aws

Entwicklerhandbuch

OpenSearch Amazon-Dienst

OpenSearch Amazon-Dienst: Entwicklerhandbuch

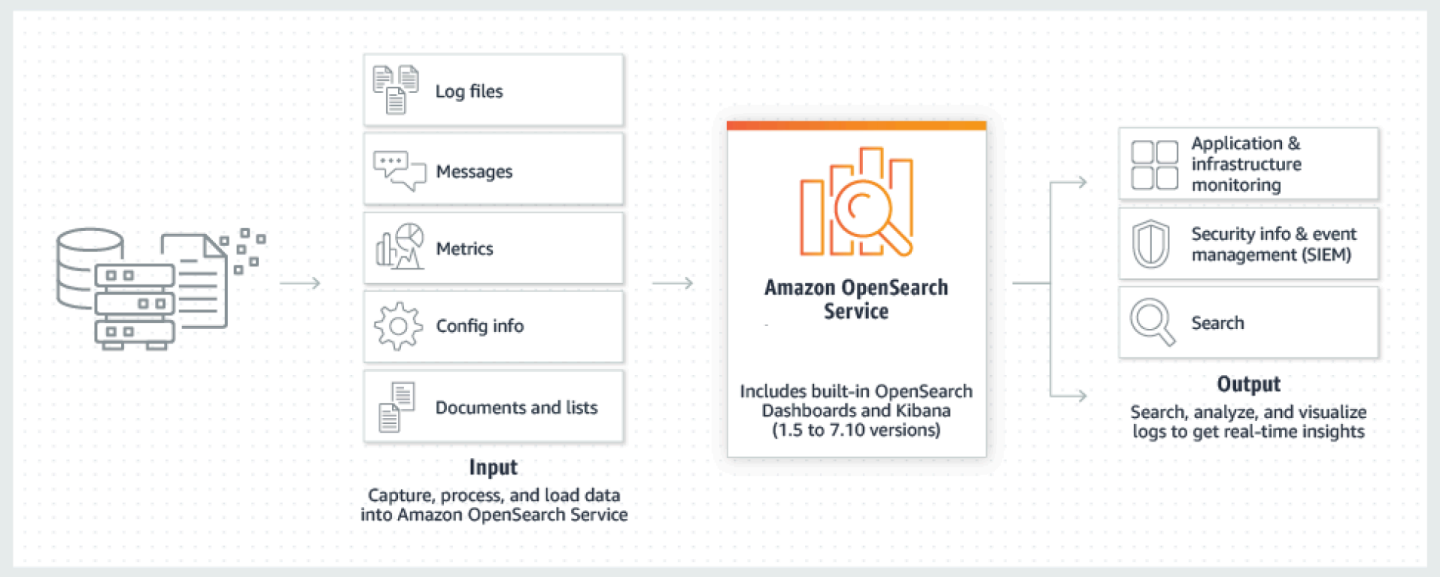
Table of Contents

Was ist Amazon OpenSearch Service?

Amazon OpenSearch Service ist ein verwalteter Service, der die Bereitstellung, den Betrieb und die Skalierung von OpenSearch Clustern in der AWS Cloud vereinfacht. Amazon OpenSearch Service unterstützt OpenSearch ältere Elasticsearch OSS (bis zu 7.10, die endgültige Open-Source-Version der Software). Wenn Sie einen Cluster erstellen, haben Sie die Option, die Suchmaschine zu verwenden.

OpenSearchist eine vollständig quelloffene Such- und Analyse-Engine für Anwendungsfälle wie Protokollanalysen, Anwendungsüberwachung in Echtzeit und Clickstream-Analyse. Weitere Informationen finden Sie in der OpenSearch Dokumentation.

Amazon OpenSearch Service stellt alle Ressourcen für Ihren OpenSearch Cluster bereit und startet ihn. Außerdem werden ausgefallene OpenSearch Serviceknoten automatisch erkannt und ersetzt, wodurch der mit selbstverwalteten Infrastrukturen verbundene Aufwand reduziert wird. Sie können Ihren Cluster mit einem einzigen API-Aufruf oder wenigen Klicks in der Konsole skalieren.



Um mit der Nutzung von OpenSearch Service zu beginnen, erstellen Sie eine OpenSearch Dienstdomäne, die einem OpenSearch Cluster entspricht. Jede EC2-Instanz im Cluster fungiert als ein OpenSearch Serviceknoten.

Sie können die OpenSearch Servicekonsole verwenden, um eine Domain innerhalb von Minuten einzurichten und zu konfigurieren. Wenn Sie den programmatischen Zugriff bevorzugen, können Sie die AWS CLI, die AWS SDKs oder Terraform verwenden.

Funktionen von Amazon OpenSearch Service

OpenSearch Der Service umfasst die folgenden Funktionen:

Skalieren

- Zahlreiche Konfigurationen von CPU, Arbeitsspeicher und Speicherkapazität, bekannt als Instance-Typen, einschließlich kostengünstiger Graviton-Instances
- Bis zu 3 PB angeschlossener Speicher
- Kostengünstiger UltraWarmKaltspeicher für schreibgeschützte Daten

Sicherheit

- AWS Identity and Access Management (IAM) Zugriffskontrolle
- Einfache Integration mit Amazon VPC und VPC-Sicherheitsgruppen
- Verschlüsselung ruhender Daten und node-to-node Verschlüsselung
- Amazon Cognito-, HTTP Basic- oder SAML-Authentifizierung für Dashboards OpenSearch
- Sicherheit auf Index-Ebene, Dokumentebene und Feldebene
- Prüfungsprotokolle
- Dashboards-Multi-Tenancy

Stabilität

- Mehrere geografische Standorte für Ihre Ressourcen, bezeichnet als Regionen und Availability Zones
- Knotenzuweisung über zwei oder drei Availability Zones in derselben AWS Region, bekannt als Multi-AZ
- Dedizierte Hauptknoten für die Auslagerung von Cluster-Management-Aufgaben
- Automatisierte Snapshots zur Sicherung und Wiederherstellung OpenSearch von Service-Domains

Flexibilität

- SQL-Unterstützung für die Integration mit Business-Intelligence-(BI-)Anwendungen
- Benutzerdefinierte Pakete zur Verbesserung der Suchergebnisse

Integration in beliebte Services

- Datenvisualisierung mithilfe von Dashboards OpenSearch
- Integration mit Amazon CloudWatch zur Überwachung von OpenSearch Service-Domain-Metriken und zur Einstellung von Alarmen
- Integration mit AWS CloudTrail API-Aufrufen von OpenSearch Service-Domains zur Überprüfung der Konfiguration
- Integration mit Amazon S3, Amazon Kinesis und Amazon DynamoDB zum Laden von Streaming-Daten in Service OpenSearch
- Warnungen von Amazon SNS, wenn Ihre Daten bestimmte Schwellenwerte überschreiten

Wann sollte ich den Service OpenSearch im Vergleich zu Amazon OpenSearch Service verwenden?

Anhand der folgenden Tabelle können Sie entscheiden, ob der bereitgestellte Amazon OpenSearch Service oder der selbstverwaltete Service die richtige Wahl für Sie OpenSearch ist.

OpenSearch	OpenSearch Amazon-Dienst
• Ihr Unternehmen ist bereit, selbst bereitgestellte Cluster manuell zu überwachen und zu verwalten, und verfügt über Mitarbeiter mit den entsprechenden Fähigkeiten. • Sie möchten die vollständige Kontrolle über Ihren Code auf Kompilierebene haben. • Ihr Unternehmen bevorzugt Open-Source-Software oder verwendet ausschließlich Open-Source-Software. • Sie verfolgen eine Multi-Cloud-Strategie, die Technologien erfordert, die nicht anbieterspezifisch sind.	• Sie möchten Ihre Infrastruktur nicht manuell verwalten, überwachen und warten. • Sie suchen einfache Möglichkeiten, die steigenden Analysekosten zu bewältigen, indem Sie Ihre Daten auf mehrere Speicherebenen verteilen und dabei die Stabilität und die niedrigen Kosten von Amazon S3 nutzen. • Sie möchten die Vorteile von Integrationen mit anderen Anbietern AWS-Services wie DynamoDB, Amazon DocumentDB (mit MongoDB-Kompatibilität), IAM und nutzen. CloudWatch CloudFormation • Sie möchten bei präventiver Wartung und bei Produktionsproblemen einfach auf AWS Support Unterstützung zugreifen können.

OpenSearch	OpenSearch Amazon-Dienst
• Ihr Team ist in der Lage, alle kritischen Produktionsprobleme zu lösen. • Sie möchten die Flexibilität haben, das Produkt nach Ihren Wünschen zu verwenden, zu modifizieren und zu erweitern. • Sie möchten sofort auf neue Funktione n zugreifen können, sobald sie veröffentlicht werden.	• Sie möchten Funktionen wie Selbstheilung, proaktive Wartung, Ausfallsicherheit und Backups nutzen.

Amazon OpenSearch Serverlos

Amazon OpenSearch Serverless ist eine serverlose On-Demand-Konfiguration mit auto Skalierung für Amazon OpenSearch Service. Serverless beseitigt die betriebliche Komplexität der Bereitstellung, Konfiguration und Optimierung Ihrer Cluster. OpenSearch Weitere Informationen finden Sie unter Amazon OpenSearch Serverlos.

OpenSearch Einnahme durch Amazon

Amazon OpenSearch Ingestion ist ein vollständig verwalteter Datensammler, der von Data Prepper unterstützt wird und Protokoll- und Ablaufverfolgungsdaten in Echtzeit an Amazon OpenSearch Service-Domains und OpenSearch serverlose Sammlungen übermittelt. Es ermöglicht Ihnen, Daten für nachgelagerte Analysen und Visualisierungen zu filtern, anzureichern, zu transformieren, zu normalisieren und zu aggregieren. Weitere Informationen finden Sie unter Amazon OpenSearch Ingestion.

Unterstützte Versionen von und OpenSearch Elasticsearch

OpenSearch Der Service unterstützt derzeit die folgenden OpenSearch Versionen:

- 2.13, 2.11, 2.9, 2.7, 2.5, 2.3, 1.3, 1.2, 1.1, 1.0

OpenSearch Der Service unterstützt auch die folgenden älteren Elasticsearch OSS-Versionen:

- 7.10, 7.9, 7.8, 7.7, 7.4, 7.1
- 6.8, 6.7, 6.5, 6.4, 6.3, 6.2, 6.0
- 5.6, 5.5, 5.3, 5.1
- 2.3
- 1.5

Weitere Informationen finden Sie unter the section called “Unterstützte Vorgänge”, the section called “Funktionen nach Engine-Version” und the section called “Plug-ins nach Engine-Version”.

Wenn Sie ein neues OpenSearch Serviceprojekt starten, empfehlen wir Ihnen dringend, die neueste unterstützte OpenSearch Version zu wählen. Wenn eine vorhandene Domain eine ältere Elasticsearch-Version verwendet, können Sie die Domain entweder behalten oder Ihre Daten migrieren. Weitere Informationen finden Sie unter the section called “Aktualisieren von Domains”.

Preise für Amazon OpenSearch Service

Bei OpenSearch Service zahlen Sie für jede Nutzungsstunde einer EC2-Instance und für die Gesamtgröße aller EBS-Speichervolumes, die Ihren Instances zugeordnet sind. Es fallen auch AWS die üblichen Datenübertragungsgebühren an.

Es gibt jedoch einige wichtige Datenübertragungsausnahmen. Wenn eine Domain mehrere Availability Zones verwendet, stellt der OpenSearch Service den Datenverkehr zwischen den Availability Zones nicht in Rechnung. Während der Shard-Zuweisung und des Rebalancing findet innerhalb einer Domain ein erheblicher Datentransfer statt. OpenSearch Warten Sie für diesen Verkehr weder Zähler noch Rechnungen. Ebenso berechnet der OpenSearch Service keine Datenübertragungen zwischen UltraWarm/cold nodes und Amazon S3.

Vollständige Preisinformationen finden Sie unter Amazon OpenSearch Service-Preise. Weitere Informationen zu den Kosten bei Konfigurationsänderungen finden Sie unter the section called “Gebühren für Konfigurationsänderungen”.

Erste Schritte mit Amazon OpenSearch Service

Melden Sie sich zunächst für ein AWS-Konto an, falls Sie noch keines haben. Nachdem Sie ein Konto eingerichtet haben, schließen Sie das Tutorial „Erste Schritte“ für Amazon OpenSearch Service ab. Lesen Sie die folgenden einführenden Themen, wenn Sie weitere Informationen benötigen, während Sie sich Wissen über den Service aneignen:

- Domain erstellen
- Festlegen der Domain-Größe entsprechend Ihrer Workload
- Steuern Sie den Zugriff auf Ihre Domain mithilfe einer Domainszugriffsrichtlinie oder einer differenzierten Zugriffssteuerung
- Indizieren Sie Daten manuell oder aus anderen AWS Diensten
- Verwenden Sie OpenSearch Dashboards, um Ihre Daten zu durchsuchen und Visualisierungen zu erstellen

Informationen zur Migration von einem OpenSearch selbstverwalteten Cluster zu OpenSearch Service finden Sie unter. the section called “Migrieren zuOpenSearchBedienung”

Zugehörige Services

OpenSearch Der Service wird häufig mit den folgenden Diensten verwendet:

Amazon CloudWatch

OpenSearch Service-Domains senden automatisch Messwerte an, CloudWatch sodass Sie den Zustand und die Leistung der Domain überwachen können. Weitere Informationen finden Sie unter Überwachung von OpenSearch Cluster-Metriken mit Amazon CloudWatch.

CloudWatch Protokolle können auch in die andere Richtung gehen. Sie können CloudWatch Logs so konfigurieren, dass Daten zur Analyse an den OpenSearch Service gestreamt werden. Weitere Informationen hierzu finden Sie unter the section called “Laden von Streaming-Daten aus Amazon CloudWatch”.

AWS CloudTrail

Verwenden Sie diese Option AWS CloudTrail , um einen Verlauf der API-Aufrufe der OpenSearch Dienstkonfiguration und der damit verbundenen Ereignisse für Ihr Konto abzurufen. Weitere Informationen finden Sie unter Überwachen von OpenSearch Amazon--Service-API-Aufrufen mit AWS CloudTrail.

Amazon Kinesis

Kinesis ist ein vollständig verwalteter Service für die Verarbeitung riesiger Streaming-Datenmengen in Echtzeit. Weitere Informationen finden Sie unter the section called “So laden Sie Streaming-Daten aus Amazon Kinesis Data Streams” und the section called “Laden von Streaming-Daten aus Amazon Data Firehose”.

Amazon S3

Amazon Simple Storage Service (Amazon S3) bietet Speicher für das Internet. Dieser Leitfaden bietet Lambda-Beispiel-Code für die Integration mit Amazon S3. Weitere Informationen finden Sie unter the section called “So laden Sie Streaming-Daten aus Amazon S3”.

AWS IAM

AWS Identity and Access Management (IAM) ist ein Webdienst, mit dem Sie den Zugriff auf Ihre OpenSearch Service-Domains verwalten können. Weitere Informationen finden Sie unter the section called “Identitäts- und Zugriffsverwaltung”.

AWS Lambda

AWS Lambda ist ein Rechendienst, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Dieser Leitfaden bietet Lambda-Beispiel-Code für das Streamen von Daten aus DynamoDB, Amazon S3 und Kinesis. Weitere Informationen finden Sie unter the section called “Laden von Streaming-Daten in den OpenSearch Service”.

Amazon-DynamoDB

Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt. Weitere Informationen zum Streamen von Daten an den OpenSearch Dienst finden Sie unterthe section called “So laden Sie Streaming-Daten aus Amazon DynamoDB”.

Amazon QuickSight

Sie können Daten aus OpenSearch Service mithilfe von QuickSight Amazon-Dashboards visualisieren. Weitere Informationen finden Sie unter Verwenden von Amazon OpenSearch Service mit Amazon QuickSight im QuickSight Amazon-Benutzerhandbuch.

> **Note**
>
> OpenSearch beinhaltet bestimmten Apache-lizenzierten Elasticsearch-Code von Elasticsearch B.V. und anderen Quellcode. Elasticsearch B.V. ist nicht die Quelle dieses anderen Quellcodes. ELASTICSEARCH ist eine eingetragene Marke von Elasticsearch B.V.

Amazon OpenSearch Service einrichten

Themen

Melde dich an für ein AWS-Konto

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/signup.
2. Folgen Sie den Online-Anweisungen.

   Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Aus Sicherheitsgründen sollten Sie einem Benutzer Administratorzugriff zuweisen und nur den Root-Benutzer verwenden, um Aufgaben auszuführen, für die Root-Benutzerzugriff erforderlich ist.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Sie können jederzeit Ihre aktuelle Kontoaktivität anzeigen und Ihr Konto verwalten. Rufen Sie dazu https://aws.amazon.com/ auf und klicken Sie auf Mein Konto.

Erstellen Sie einen Benutzer mit Administratorzugriff

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich AWS Management Consoleals Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

   Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter Anmelden als Root-Benutzer im AWS-Anmeldung Benutzerhandbuch zu.
2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

   Anweisungen finden Sie unter Aktivieren eines virtuellen MFA-Geräts für Ihren AWS-Konto Root-Benutzer (Konsole) im IAM-Benutzerhandbuch.

Erstellen Sie einen Benutzer mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.
2. Gewähren Sie einem Benutzer in IAM Identity Center Administratorzugriff.

   Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie unter Benutzerzugriff mit der Standardeinstellung konfigurieren IAM-Identity-Center-Verzeichnis im AWS IAM Identity Center Benutzerhandbuch.

Melden Sie sich als Benutzer mit Administratorzugriff an

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

  Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Zugriffsportal.

Weisen Sie weiteren Benutzern Zugriff zu

1. Erstellen Sie in IAM Identity Center einen Berechtigungssatz, der bewährten Methode zur Anwendung von Berechtigungen mit den geringsten Rechten folgt.

Anweisungen finden Sie im Benutzerhandbuch unter Einen Berechtigungssatz erstellen.AWS IAM Identity Center

2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

   Anweisungen finden Sie im AWS IAM Identity Center Benutzerhandbuch unter Gruppen hinzufügen.

Erteilen Sie Berechtigungen

In Produktionsumgebungen empfehlen wir, detailliertere Richtlinien zu verwenden. Weitere Informationen zur Zugriffsverwaltung finden Sie unter Zugriffsverwaltung für AWS Ressourcen im IAM-Benutzerhandbuch.

Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

- Benutzer und Gruppen in AWS IAM Identity Center:

  Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center -Benutzerhandbuch.
- Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

  Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anweisungen unter Erstellen einer Rolle für einen externen Identitätsanbieter (Verbund) im IAM-Benutzerhandbuch.
- IAM-Benutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Folgen Sie den Anweisungen unter Erstellen einer Rolle für einen IAM-Benutzer im IAM-Benutzerhandbuch.
  - (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

Erteilen programmgesteuerten Zugriffs

Benutzer benötigen programmatischen Zugriff, wenn sie mit AWS außerhalb des AWS Management Console interagieren möchten. Die Art und Weise, wie programmatischer Zugriff gewährt wird, hängt vom Benutzertyp ab, der zugreift. AWS

Um Benutzern programmgesteuerten Zugriff zu gewähren, wählen Sie eine der folgenden Optionen.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
Mitarbeiteridentität (Benutzer, die in IAM Identity Center verwaltet werden)	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an die AWS CLI, AWS SDKs oder APIs zu signieren. AWS	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen zu den AWS CLI finden Sie unter Konfiguration der AWS CLI zu AWS IAM Identity Center verwendenden im AWS Command Line Interface Benutzerhandbuch. • Informationen zu AWS SDKs, Tools und AWS APIs finden Sie unter IAM Identity Center-Authentifizierung im Referenzhandbuch für AWS SDKs und Tools.
IAM	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an die AWS CLI, AWS SDKs oder APIs zu signieren. AWS	Folgen Sie den Anweisungen unter Verwenden temporäre r Anmeldeinformationen mit AWS Ressourcen im IAM-Benutzerhandbuch.
IAM	(Nicht empfohlen) Verwenden Sie langfristige Anmeldeinformationen, um programmatische Anfragen an die AWS CLI, AWS SDKs oder APIs zu signieren. AWS	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen dazu finden Sie unter Authentifizierung mithilfe von IAM-Benut zeranmeldedaten im Benutzerhandbuch. AWS

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
		CLIAWS Command Line Interface • Informationen zu AWS SDKs und Tools finden Sie unter Authentifizieren mit langfristigen Anmeldeinformationen im Referenzhandbuch für AWS SDKs und Tools. • Informationen zu AWS APIs finden Sie unter Verwaltung von Zugriffsschlüsseln für IAM-Benutzer im IAM-Benutzerhandbuch.

Installieren und konfigurieren Sie AWS CLI

Wenn Sie OpenSearch Service-APIs verwenden möchten, müssen Sie die neueste Version von AWS Command Line Interface (AWS CLI) installieren. Sie AWS CLI müssen den OpenSearch Service nicht von der Konsole aus verwenden, und Sie können auch ohne die CLI loslegen, indem Sie die Schritte unter befolgenErste Schritte mit AmazonOpenSearchBedienung.

Um das einzurichten AWS CLI

1. Informationen zur Installation der neuesten Version von AWS CLI für macOS, Linux oder Windows finden Sie unter Installation oder Aktualisierung der neuesten Version von AWS CLI.
2. Informationen zur Konfiguration AWS CLI und sicheren Einrichtung Ihres Zugriffs, einschließlich OpenSearch Service AWS-Services, finden Sie unter Schnellkonfiguration mit `aws configure`.
3. Um das Setup zu überprüfen, geben Sie an der DataBrew Befehlszeile den folgenden Befehl ein.

```
aws opensearch help
```

AWS CLI Befehle verwenden den Standard AWS-Region aus Ihrer Konfiguration, sofern Sie ihn nicht mit einem Parameter oder einem Profil festlegen. Um Ihren AWS-Region mit einem Parameter festzulegen, können Sie den `--region` Parameter zu jedem Befehl hinzufügen.

Um Ihr AWS-Region Profil festzulegen, fügen Sie zunächst ein benanntes Profil in die `~/.aws/config` Datei oder die `%UserProfile%/.aws/config` Datei ein (für Microsoft Windows). Folgen Sie den Schritten unter Benannte Profile für AWS CLI. Legen Sie als Nächstes Ihre AWS-Region und andere Einstellungen mit einem Befehl fest, der dem im folgenden Beispiel ähnelt.

```
[profile opensearch]
aws_access_key_id = ACCESS-KEY-ID-OF-IAM-USER
aws_secret_access_key = SECRET-ACCESS-KEY-ID-OF-IAM-USER
region = us-east-1
output = text
```

Öffnen Sie die -Konsole

Die meisten konsolenorientierten Themen in diesem Abschnitt beginnen in der OpenSearch Servicekonsole. Wenn Sie noch nicht bei Ihrem angemeldet sind AWS-Konto, melden Sie sich an, öffnen Sie dann die OpenSearch Servicekonsole und fahren Sie mit dem nächsten Abschnitt fort, um mit den ersten Schritten mit OpenSearch Service fortzufahren.

Erste Schritte mit AmazonOpenSearchBedienung

Dieses Tutorial zeigt Ihnen, wie Sie Amazon verwendenOpenSearchDienst zum Erstellen und Konfigurieren einer Testdomain. EinOpenSearchServicedomäne ist ein Synonym fürOpenSearchCluster. Domains sind Cluster mit den Einstellungen, Instance-Typen, Instance-Anzahl und Speicherressourcen, die Sie angeben.

Dieses Tutorial führt Sie durch die grundlegenden Schritte, um eineOpenSearchDie Servicedomäne ist schnell eingerichtet und läuft schnell. Weitere detaillierte Informationen finden Sie unter Erstellen und Verwalten von Domains und in anderen Themen in diesem Handbuch. Für Informationen zur Migration zuOpenSearchService von einem selbstverwaltetenOpenSearchCluster, siehethe section called “Migrieren zuOpenSearchBedienung”.

Sie können die Schritte in diesem Tutorial ausführen, indem Sie denOpenSearchServicekonsole, dieAWS CLI, oder dieAWSSDK. Weitere Informationen zum Installieren und Einrichten der AWS CLI finden Sie im AWS Command Line Interface-Benutzerhandbuch.

Schritt 1: Erstellen Sie ein AmazonOpenSearchDienstdomäne

> **Important**
>
> Dies ist ein übersichtliches Tutorial zur Konfiguration einestestenAmazonasOpenSearchDienstdomäne. Verwenden Sie diesen Prozess nicht zum Erstellen von Produktionsdomänen. Eine ausführliche Beschreibung des Verfahrens erhalten Sie unter Erstellen und Verwalten von Domains.

EinOpenSearchServicedomäne ist ein Synonym fürOpenSearchCluster. Domains sind Cluster mit den Einstellungen, Instance-Typen, Instance-Anzahl und Speicherressourcen, die Sie angeben. Sie können eine erstellenOpenSearchDienstdomäne mithilfe der Konsole, derAWS CLI, oder dieAWSSDKs.

Um eine zu erstellenOpenSearchDienstdomäne, die die Konsole verwendet

1. Rufen Sie die Webseite unter http://aws.amazon.com auf und klicken Sie auf In der Konsole anmelden.
2. UnterAnalytik, wähleAmazonasOpenSearchBedienung.

3. Wählen Sie Domäne erstellen aus.
4. Geben Sie einen Namen für die Domäne an. In den Beispielen in diesem Tutorial wird der Name Filme verwendet.
5. Wählen Sie für die Methode zur DomainerstellungStandard erstellen.

> **Note**
>
> Um eine Produktionsdomäne schnell mit Best Practices zu konfigurieren, können SieEinfach erstellen. Für die Entwicklungs- und Testzwecke dieses Tutorials verwenden wirStandard erstellen.

6. Wählen Sie für VorlagenEntwicklung/Test.
7. Wählen Sie für die BereitstellungsoptionDomain mit Standby.
8. Wählen Sie für Version die neueste Version aus.
9. Ignoriere vorerst dieDatenknoten,Warme und kalte Datenspeicherung,Dedizierte Masterknoten,Snapshot-Konfiguration, undBenutzerdefinierter EndpunktAbschnitte.
10. Aus Gründen der Einfachheit nutzen Sie in diesem Tutorial eine Domäne mit öffentlichem Zugriff. Wählen Sie unter Netzwerk die Option Öffentlicher Zugriff aus.
11. Behalten Sie in den feinkörnigen Zugriffskontrolleinstellungen dieErmöglichen Sie eine differenzierte ZugriffskontrolleDas Kontrollkästchen ist aktiviert. AuswählenMaster-Benutzer erstellenund geben Sie einen Benutzernamen und ein Passwort ein.
12. Ignorieren Sie vorerst die Abschnitte SAML-Authentifizierung und Amazon-Cognito-Authentifizierung.
13. Wählen Sie für Zugriffsrichtlinie die Option Nur differenzierte Zugriffssteuerung verwenden aus. In diesem Tutorial ist die differenzierte Zugriffskontrolle für die Authentifizierung zuständig, nicht die Domänenzugriffsrichtlinie.
14. Ignorieren Sie die restlichen Einstellungen und wählen Sie Erstellen. Die Initialisierung neuer Domänen dauert in der Regel 15–30 Minuten, kann jedoch je nach Konfiguration auch länger dauern. Wählen Sie sie nach der Initialisierung der Domäne aus, um den Konfigurationsbereich zu öffnen. Beachten Sie den Domänenendpunkt unter Allgemeine Informationen (z. B. `https://search-my-domain.us-east-1.es.amazonaws.com`), den Sie im nächsten Schritt verwenden.

Weiter:Laden Sie Daten auf eine hochOpenSearchServicedomäne für die Indexierung

Schritt 2: Daten auf Amazon hochladenOpenSearchService für die Indexierung

> **Important**
>
> Dies ist ein übersichtliches Tutorial zum Hochladen einer kleinen Menge an Testdaten auf AmazonOpenSearchBedienung. Weitere Informationen zum Hochladen von Daten in einer Produktionsdomäne finden Sie unter Indizierung von Daten.

Sie können Daten auf eine hochladenOpenSearchDienstdomäne, die die Befehlszeile oder die meisten Programmiersprachen verwendet.

Die folgenden Beispielanforderungen nutzen der Einfachheit halber und aus Gründen der Übersichtlichkeit curl, einen häufig verwendeten HTTP-Client. Clients wie curl können das Signieren von Anforderungen, das erforderlich ist, wenn Ihre Zugriffsrichtlinien IAM-Benutzer und -Rollen angeben, nicht durchführen. Um diesen Vorgang erfolgreich abzuschließen, müssen Sie eine detaillierte Zugriffskontrolle mit einem primären Benutzernamen und Passwort verwenden, wie Sie es in konfiguriert habenSchritt 1.

Sie können curl unter Windows installieren und an der Eingabeaufforderung verwenden, stattdessen wird aber ein Tool wie Cygwin oder das Windows-Subsystem für Linux empfohlen. In macOS und den meisten Linux-Verteilungen ist curl vorinstalliert.

Option 1: Hochladen eines einzelnen Dokuments

Führen Sie den folgenden Befehl aus, um ein einzelnes Dokument zur Domäne movies (Filme) hinzuzufügen:

```
curl -XPUT -u 'master-user:master-user-password' 'domain-endpoint/movies/_doc/1' -d
 '{"director": "Burton, Tim", "genre": ["Comedy","Sci-Fi"], "year": 1996, "actor":
 ["Jack Nicholson","Pierce Brosnan","Sarah Jessica Parker"], "title": "Mars Attacks!"}'
 -H 'Content-Type: application/json'
```

Geben Sie im Befehl den Benutzernamen und das Passwort ein, die Sie in erstellt habenSchritt 1.

Eine ausführliche Erläuterung dieses Befehls und wie signierte Anfragen gestellt werden finden Sie unterOpenSearchService, siheIndizierung von Daten.

Option 2: Hochladen mehrerer Dokumente

Um eine JSON-Datei hochzuladen, die mehrere Dokumente enthält, in eineOpenSearchDienstdomäne

1. Erstellen Sie eine Datei mit dem Namen `bulk_movies.json`. Fügen Sie den folgenden Inhalt in die Datei ein und fügen Sie einen nachstehenden Zeilenumbruch hinzu:

```
{ "index" : { "_index": "movies", "_id" : "2" } }
{"director": "Frankenheimer, John", "genre": ["Drama", "Mystery", "Thriller",
 "Crime"], "year": 1962, "actor": ["Lansbury, Angela", "Sinatra, Frank", "Leigh,
 Janet", "Harvey, Laurence", "Silva, Henry", "Frees, Paul", "Gregory, James",
 "Bissell, Whit", "McGiver, John", "Parrish, Leslie", "Edwards, James", "Flowers,
 Bess", "Dhiegh, Khigh", "Payne, Julie", "Kleeb, Helen", "Gray, Joe", "Nalder,
 Reggie", "Stevens, Bert", "Masters, Michael", "Lowell, Tom"], "title": "The
 Manchurian Candidate"}
{ "index" : { "_index": "movies", "_id" : "3" } }
{"director": "Baird, Stuart", "genre": ["Action", "Crime", "Thriller"], "year":
 1998, "actor": ["Downey Jr., Robert", "Jones, Tommy Lee", "Snipes, Wesley",
 "Pantoliano, Joe", "Jacob, Ir\u00e8ne", "Nelligan, Kate", "Roebuck, Daniel",
 "Malahide, Patrick", "Richardson, LaTanya", "Wood, Tom", "Kosik, Thomas",
 "Stellate, Nick", "Minkoff, Robert", "Brown, Spitfire", "Foster, Reese",
 "Spielbauer, Bruce", "Mukherji, Kevin", "Cray, Ed", "Fordham, David", "Jett,
 Charlie"], "title": "U.S. Marshals"}
{ "index" : { "_index": "movies", "_id" : "4" } }
{"director": "Ray, Nicholas", "genre": ["Drama", "Romance"], "year": 1955, "actor":
 ["Hopper, Dennis", "Wood, Natalie", "Dean, James", "Mineo, Sal", "Backus, Jim",
 "Platt, Edward", "Ray, Nicholas", "Hopper, William", "Allen, Corey", "Birch,
 Paul", "Hudson, Rochelle", "Doran, Ann", "Hicks, Chuck", "Leigh, Nelson",
 "Williams, Robert", "Wessel, Dick", "Bryar, Paul", "Sessions, Almira", "McMahon,
 David", "Peters Jr., House"], "title": "Rebel Without a Cause"}
```

2. Führen Sie den folgenden Befehl im lokalen Verzeichnis aus, in dem die Datei gespeichert ist, um sie in die Domäne Film hochzuladen:

```
curl -XPOST -u 'master-user:master-user-password' 'domain-endpoint/_bulk' --data-
binary @bulk_movies.json -H 'Content-Type: application/json'
```

Weitere Informationen zum Massendateiformat finden Sie unter Indizierung von Daten.

Weiter:Suchen von Dokumenten

Schritt 3: Dokumente in Amazon suchenOpenSearchBedienung

So suchen Sie in Amazon nach DokumentenOpenSearchServicedomäne, verwenden Sie dieOpenSearchSuch-API. Alternativ können SieOpenSearchDashboardsum Dokumente in der Domain zu durchsuchen.

So suchen Sie Dokumente über die Befehlszeile

Führen Sie den folgenden Befehl aus, um die Domäne movies (Filme) nach dem Wort mars zu durchsuchen:

```
curl -XGET -u 'master-user:master-user-password' 'domain-endpoint/movies/_search?
q=mars&pretty=true'
```

Wenn Sie die Massendaten auf der vorherigen Seite verwenden, suchen Sie stattdessen lieber nach rebel.

Es wird eine Antwort ähnlich der folgenden angezeigt:

```
{
  "took" : 5,
  "timed_out" : false,
  "_shards" : {
    "total" : 5,
    "successful" : 5,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : {
      "value" : 1,
      "relation" : "eq"
    },
    "max_score" : 0.2876821,
    "hits" : [
      {
        "_index" : "movies",
        "_type" : "_doc",
        "_id" : "1",
        "_score" : 0.2876821,
        "_source" : {
```

```
          "director" : "Burton, Tim",
          "genre" : [
            "Comedy",
            "Sci-Fi"
          ],
          "year" : 1996,
          "actor" : [
            "Jack Nicholson",
            "Pierce Brosnan",
            "Sarah Jessica Parker"
          ],
          "title" : "Mars Attacks!"
        }
      }
    ]
  }
}
```

Suchen Sie nach Dokumenten mitOpenSearchDashboards

OpenSearchDashboards ist ein beliebtes Open-Source-Visualisierungstool, das für die Verwendung mit entwickelt wurdeOpenSearch. Es bietet eine hilfreiche Benutzeroberfläche für Sie, um Ihre Indizes zu suchen und zu überwachen.

Um Dokumente von einem zu durchsuchenOpenSearchServicedomäne, die Dashboards verwendet

1. Navigiere zumOpenSearchDashboard-URL für Ihre Domain. Sie finden die URL im Dashboard der Domain in derOpenSearchServicekonsole. Die URL weist das folgende Format auf:

   ```
   domain-endpoint/_dashboards/
   ```

2. Melden Sie sich mit Ihrem primären Benutzernamen und Passwort an.
3. Um Dashboards verwenden zu können, müssen Sie mindestens ein Indexmuster erstellen. Dashboards identifiziert anhand dieser Muster, welche Indizes Sie analysieren möchten. Öffnen Sie das linke Navigationspanel, wählen Sie Stack-Management, wählen Sie Indexmuster und dann Indexmuster erstellen. Geben Sie für dieses Tutorial Filme ein.
4. Wählen Sie Nächster Schritt aus und klicken Sie auf Indexmuster erstellen. Nachdem das Muster erstellt wurde, können Sie die verschiedenen Dokumentfelder anzeigen, z. B. `actor` und `director`.

5. Gehen Sie zurück zur Seite Indexmuster und stellen Sie sicher, dass `movies` als Standard eingestellt ist. Wenn dies nicht der Fall ist, wählen Sie das Muster aus und wählen Sie das Sternsymbol, um es zum Standardwert zu machen.
6. Um mit der Suche nach Ihren Daten zu beginnen, öffnen Sie erneut das linke Navigationsfeld und wählen Sie Entdecken.
7. Geben Sie in der Suchleiste mars ein, wenn Sie ein einzelnes Dokument hochgeladen haben, oder rebel, wenn Sie mehrere Dokumente hochgeladen haben, und drücken Sie dann die Eingabetaste. Sie können versuchen, andere Begriffe wie Schauspieler- oder Regisseurnamen zu durchsuchen.

Weiter:Domäne löschen

Schritt 4: Löschen Sie ein AmazonOpenSearchDienstdomäne

Da die in diesem Tutorial erstellte Domäne Filme nur Testzwecken dient, sollten Sie sie löschen, wenn Sie mit dem Experimentieren fertig sind, um unnötige Gebühren zu vermeiden.

Um eine zu löschenOpenSearchDienstdomäne von der Konsole aus

1. Loggen Sie sich ein beiAmazonasOpenSearchBedienungKonsole.
2. Wählen Sie unter Domänen die Filmdomäne aus.
3. Wählen Sie Löschen und bestätigen Sie das Löschen.

Nächste Schritte

Nun, da Sie wissen, wie Sie eine Domäne und Indexdaten erstellen, können Sie einige der folgenden Übungen ausprobieren:

- Erfahren Sie mehr über erweiterte Optionen zum Erstellen einer Domäne. Weitere Informationen finden Sie unter Erstellen und Verwalten von Domains.
- Erfahren Sie, wie Sie die Indizes in Ihrer Domain verwalten. Weitere Informationen finden Sie unter Verwalten von Indexen.
- Probieren Sie eines der Tutorials für die Arbeit mit Amazon ausOpenSearchBedienung. Weitere Informationen finden Sie unter Tutorials.

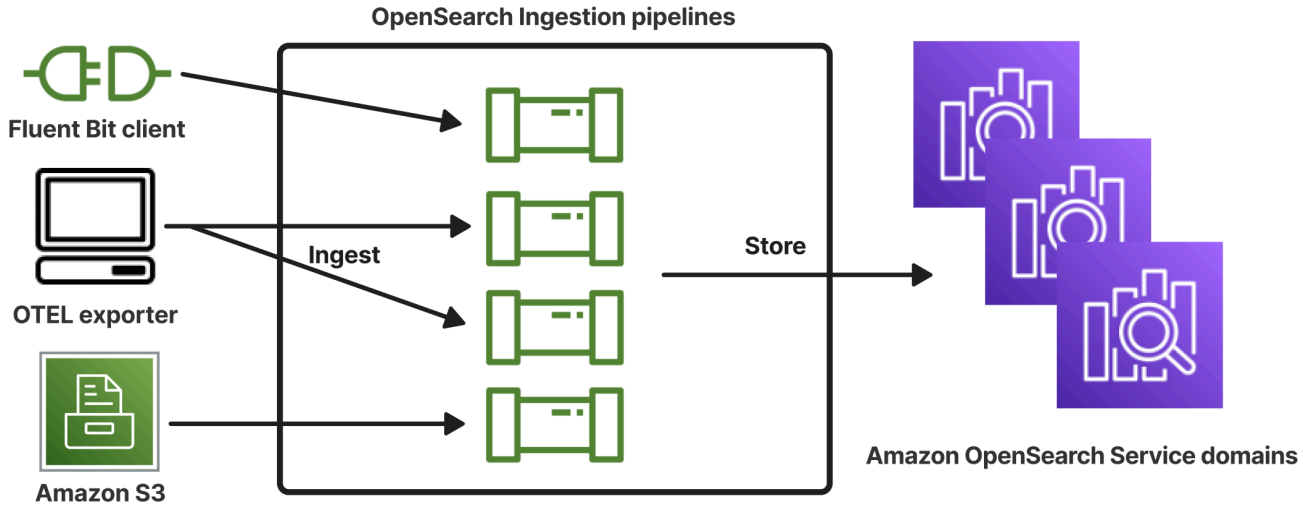
OpenSearch Einnahme durch Amazon

Amazon OpenSearch Ingestion ist ein vollständig verwalteter, serverloser Datensammler, der Protokoll-, Metrik- und Trace-Daten in Echtzeit an Amazon OpenSearch Service-Domains und OpenSearch serverlose Sammlungen liefert.

Mit OpenSearch Ingestion müssen Sie keine Drittanbieterlösungen wie Logstash oder Jaeger mehr verwenden, um Daten in Ihre Service-Domains und serverlosen Sammlungen aufzunehmen. OpenSearch OpenSearch Sie konfigurieren Ihre Datenproduzenten so, dass sie Daten an Ingestion senden. OpenSearch Anschließend werden die Daten automatisch an die von Ihnen angegebene Domain oder Sammlung gesendet. Sie können OpenSearch Ingestion auch so konfigurieren, dass Ihre Daten vor der Bereitstellung transformiert werden.

Außerdem müssen Sie sich mit OpenSearch Ingestion keine Gedanken über die Bereitstellung von Servern, die Verwaltung und das Patchen von Software oder die Skalierung Ihres Serverclusters machen. Sie stellen Ingestion-Pipelines direkt innerhalb des bereit AWS Management Console, und Ingestion kümmert sich um deren Verwaltung und OpenSearch Skalierung.

OpenSearch Ingestion ist ein Teil von Amazon Service. OpenSearch Es wird von Data Prepper unterstützt, einem Open-Source-Datensammler, der Daten für nachgelagerte Analysen und Visualisierungen filtern, anreichern, transformieren, normalisieren und aggregieren kann.



Themen

- Die wichtigsten Konzepte
- Vorteile der OpenSearch Einnahme
- Einschränkungen

- Unterstützte Data Prepper-Versionen
- Skalierung von Pipelines
- OpenSearch Preise für die Aufnahme
- Unterstützt AWS-Regionen
- OpenSearch Kontingente für die Inanspruchnahme
- Rollen und Benutzer in Amazon OpenSearch Ingestion einrichten
- Erste Schritte Schritte Schritte Schritte Schritte Schritte Schritte Schritte Schritte Schritte Schritte Schritte Schritte Schritte OpenSearch
- Überblick über die Pipeline-Funktionen in Amazon OpenSearch Ingestion
- Amazon OpenSearch Ingestion-Pipelines erstellen
- Amazon OpenSearch Ingestion-Pipelines anzeigen
- Aktualisierung der Amazon OpenSearch Ingestion-Pipelines
- Amazon OpenSearch Ingestion-Pipelines beenden und starten
- Löschen von Amazon OpenSearch Ingestion-Pipelines
- Unterstützte Plugins und Optionen für Amazon OpenSearch Ingestion-Pipelines
- Arbeiten mit Amazon OpenSearch Ingestion-Pipeline-Integrationen
- Migrieren von Daten zwischen Domains und Sammlungen mithilfe von Amazon OpenSearch Ingestion
- Verwendung der AWS SDKs zur Interaktion mit Amazon Ingestion OpenSearch
- Sicherheit bei Amazon OpenSearch Ingestion
- Kennzeichnen von Amazon OpenSearch Ingestion-Pipelines
- Protokollierung und Überwachung OpenSearch von Amazon Ingestion mit Amazon CloudWatch
- Bewährte Methoden für Amazon OpenSearch Ingestion

Die wichtigsten Konzepte

Wenn Sie mit OpenSearch Ingestion beginnen, können Sie davon profitieren, die folgenden Konzepte zu verstehen:

Pipeline

Aus Sicht der OpenSearch Datenerfassung bezieht sich eine Pipeline auf einen einzelnen bereitgestellten Datensammelpunkt, den Sie in Service erstellen. OpenSearch Sie können

sich das als die gesamte YAML-Konfigurationsdatei vorstellen, die eine oder mehrere Unter-Pipelines enthält. Schritte zum Erstellen einer Ingestion-Pipeline finden Sie unter. the section called “Pipelines erstellen”

Sub-Pipeline

Sie definieren Sub-Pipelines in einer YAML-Konfigurationsdatei. Jede Subpipeline ist eine Kombination aus einer Quelle, einem Puffer, null oder mehr Prozessoren und einer oder mehreren Senken. Sie können mehrere Sub-Pipelines in einer einzigen YAML-Datei definieren, jede mit eigenen Quellen, Prozessoren und Senken. Um die Überwachung mit CloudWatch und anderen Diensten zu erleichtern, empfehlen wir Ihnen, einen Pipeline-Namen anzugeben, der sich von allen Unter-Pipelines unterscheidet.

Sie können mehrere Sub-Pipelines in einer einzigen YAML-Datei aneinanderreihen, sodass die Quelle für eine Sub-Pipeline eine andere Sub-Pipeline und ihre Senke eine dritte Sub-Pipeline ist. Ein Beispiel finden Sie unter the section called “OpenTelemetry Kollektor”.

Quelle

Die Eingabekomponente einer Subpipeline. Sie definiert den Mechanismus, über den eine Pipeline Datensätze verarbeitet. Die Quelle kann Ereignisse verarbeiten, indem sie sie entweder über HTTPS empfängt oder sie von externen Endpunkten wie Amazon S3 liest. Es gibt zwei Arten von Quellen: Push-basierte und Pull-basierte. Push-basierte Quellen, wie HTTP - und oTel-Protokolle, streamen Datensätze an Aufnahmeendpunkte. Pull-basierte Quellen wie OTel Trace und S3 rufen Daten aus der Quelle ab.

Prozessoren

Zwischenverarbeitungseinheiten, die Datensätze filtern, transformieren und in ein gewünschtes Format anreichern können, bevor sie auf der Senke veröffentlicht werden. Der Prozessor ist eine optionale Komponente einer Pipeline. Wenn Sie keinen Prozessor definieren, werden Datensätze in dem Format veröffentlicht, das in der Quelle definiert ist. Sie können mehr als einen Prozessor haben. In einer Pipeline werden Prozessoren in der Reihenfolge ausgeführt, in der Sie sie definieren.

Sink

Die Ausgabekomponente einer Subpipeline. Sie definiert ein oder mehrere Ziele, an denen eine Unterpipeline Datensätze veröffentlicht. OpenSearch Ingestion unterstützt OpenSearch Dienstdomänen als Senken. Es unterstützt auch Sub-Pipelines als Senken. Das bedeutet, dass Sie mehrere Sub-Pipelines innerhalb einer einzigen OpenSearch Ingestion-Pipeline (YAML-

Datei) aneinanderreihen können. Selbstverwaltete OpenSearch Cluster werden nicht als Senken unterstützt.

Buffer

Der Teil eines Prozessors, der als Schicht zwischen Quelle und Senke fungiert. Sie können einen Puffer in Ihrer Pipeline nicht manuell konfigurieren. OpenSearch Die Aufnahme verwendet eine Standard-Pufferkonfiguration.

Route

Der Teil eines Prozessors, der es Pipeline-Autoren ermöglicht, nur Ereignisse, die bestimmten Bedingungen entsprechen, an verschiedene Senken zu senden.

Eine gültige Sub-Pipeline-Definition muss eine Quelle und eine Senke enthalten. Weitere Informationen zu jedem dieser Pipeline-Elemente finden Sie in der Konfigurationsreferenz.

Vorteile der OpenSearch Einnahme

OpenSearch Die Einnahme hat die folgenden Hauptvorteile:

- Eliminiert die Notwendigkeit, eine selbst bereitgestellte Pipeline manuell zu verwalten.
- Skaliert Ihre Pipelines automatisch auf der Grundlage der von Ihnen definierten Kapazitätsgrenzen.
- Hält Ihre Pipeline mit Sicherheits- und Bug-Patches auf dem neuesten Stand.
- Bietet die Option, Pipelines mit Ihrer Virtual Private Cloud (VPC) zu verbinden, um eine zusätzliche Sicherheitsebene zu schaffen.
- Ermöglicht das Stoppen und Starten von Pipelines, um die Kosten zu kontrollieren.
- Bietet Pipeline-Konfigurations-Blueprints für beliebte Anwendungsfälle, damit Sie schneller loslegen können.
- Ermöglicht Ihnen die programmgesteuerte Interaktion mit Ihren Pipelines über die verschiedenen AWS SDKs und die Ingestion-API. OpenSearch
- Unterstützt die Leistungsüberwachung in Amazon CloudWatch und die Fehlerprotokollierung in CloudWatch Logs.

Einschränkungen

OpenSearch Für die Aufnahme gelten die folgenden Einschränkungen:

- Sie können Daten nur in Domains aufnehmen, auf denen OpenSearch 1.0 oder höher oder Elasticsearch 6.8 oder höher ausgeführt wird. Wenn Sie die Trace-Quelle oTEL verwenden, empfehlen wir die Verwendung von Elasticsearch 7.9 oder höher, damit Sie das Dashboards-Plugin verwenden können. OpenSearch
- Wenn eine Pipeline in eine OpenSearch Dienstdomäne schreibt, die sich innerhalb einer VPC befindet, muss die Pipeline in derselben Domäne AWS-Region wie die Domäne erstellt werden.
- Sie können nur eine einzelne Datenquelle innerhalb einer Pipeline-Definition konfigurieren.
- Sie können selbstverwaltete OpenSearch Cluster nicht als Senken angeben.
- Sie können keinen benutzerdefinierten Endpunkt als Senke angeben. Sie können immer noch in eine Domäne schreiben, für die benutzerdefinierte Endpunkte aktiviert sind, aber Sie müssen ihren Standardendpunkt angeben.
- Sie können Ressourcen innerhalb von Opt-in-Regionen nicht als Quellen oder Senken angeben.
- Es gibt einige Einschränkungen in Bezug auf die Parameter, die Sie in eine Pipeline-Konfiguration aufnehmen können. Weitere Informationen finden Sie unter the section called “Konfigurationsanforderungen und Einschränkungen”.

Unterstützte Data Prepper-Versionen

OpenSearch Ingestion unterstützt derzeit die folgenden Hauptversionen von Data Prepper:

- 2.x

Wenn Sie eine Pipeline erstellen, verwenden Sie die erforderliche `version` Option, um die zu verwendende Hauptversion von Data Prepper anzugeben. Zum Beispiel. `version: "2"` OpenSearch Ingestion ruft die neueste unterstützte Nebenversion dieser Hauptversion ab und stellt die Pipeline mit dieser Version bereit. Weitere Informationen finden Sie unter the section called “Angabe der Pipeline-Version”.

Derzeit werden OpenSearch Ingestion-Pipelines mit Version 2.7 von Data Prepper bereitgestellt. Informationen finden Sie in den Versionshinweisen zu 2.7. Informationen zu den Funktionen und Bugfixes, die in jeder Version von Data Prepper enthalten sind, finden Sie auf der Releases-Seite. Nicht jede Nebenversion einer bestimmten Hauptversion wird von OpenSearch Ingestion unterstützt.

Wenn Sie die YAML-Konfigurationsdatei einer Pipeline aktualisieren und eine neue Nebenversion von Data Prepper unterstützt wird, aktualisiert OpenSearch Ingestion die Pipeline automatisch auf die

neueste unterstützte Nebenversion der Hauptversion, die in der Pipeline-Konfiguration angegeben ist. Möglicherweise haben Sie `version: "2"` in Ihrer Pipeline-Konfiguration und OpenSearch Ingestion die Pipeline zunächst mit Version 2.6.0 bereitgestellt. Wenn Unterstützung für Version 2.7.0 hinzugefügt wird und Sie eine Änderung an der Pipeline-Konfiguration vornehmen, aktualisiert OpenSearch Ingestion die Pipeline auf Version 2.7.0. Dieser Prozess hält Ihre Pipeline mit den neuesten Bugfixes und Leistungsverbesserungen auf dem neuesten Stand. OpenSearch Ingestion kann die Hauptversion Ihrer Pipeline nur aktualisieren, wenn Sie die `version` Option in der Pipeline-Konfiguration manuell ändern. Weitere Informationen finden Sie unter the section called “Pipelines werden aktualisiert”.

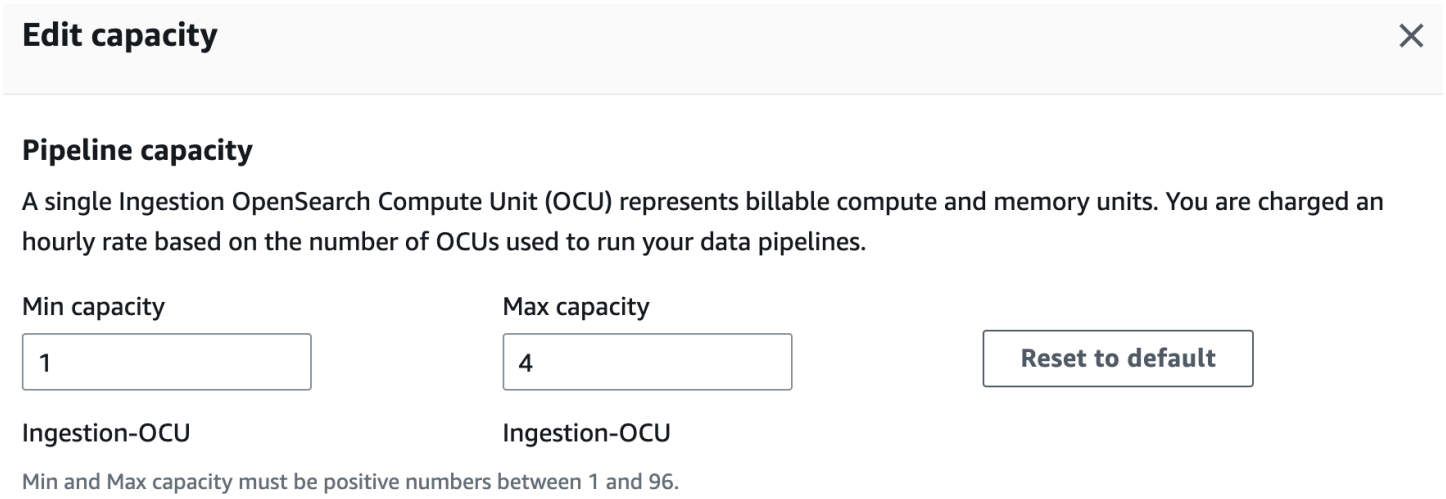
Skalierung von Pipelines

Sie müssen die Pipeline-Kapazität nicht selbst bereitstellen und verwalten. OpenSearch Ingestion skaliert Ihre Pipeline-Kapazität automatisch entsprechend Ihrer geschätzten Arbeitslast auf der Grundlage der von Ihnen angegebenen minimalen und maximalen OpenSearch Ingestion-Recheneinheiten (Ingestion-OCUs).

Jede Ingestion-OCU ist eine Kombination aus etwa 8 GiB Arbeitsspeicher und 2 vCPUs. Sie können die minimalen und maximalen OCU-Werte für eine Pipeline angeben, und OpenSearch Ingestion skaliert Ihre Pipeline-Kapazität automatisch auf der Grundlage dieser Grenzwerte.

Sie können die folgenden Werte angeben:

- Mindestkapazität — Die Pipeline kann die Kapazität auf diese Anzahl von Ingestion-OCUs reduzieren. Die angegebene Mindestkapazität ist auch die Startkapazität für eine Pipeline.
- Maximale Kapazität — Die Pipeline kann die Kapazität auf bis zu dieser Anzahl von Ingestion-OCUs erhöhen.



Stellen Sie sicher, dass die maximale Kapazität für eine Pipeline hoch genug ist, um Arbeitslastspitzen zu bewältigen, und dass die Mindestkapazität niedrig genug ist, um die Kosten zu minimieren, wenn die Pipeline nicht ausgelastet ist. Basierend auf Ihren Einstellungen skaliert OpenSearch Ingestion automatisch die Anzahl der Ingestion-OCUs für Ihre Pipeline, um die Ingestion-Arbeitslast zu verarbeiten. Zu einem bestimmten Zeitpunkt werden Ihnen nur die Ingestion-OCUs in Rechnung gestellt, die von Ihrer Pipeline aktiv genutzt werden.

Die Ihrer OpenSearch Ingestion-Pipeline zugewiesene Kapazität wird je nach den Verarbeitungsanforderungen Ihrer Pipeline und der durch Ihre Client-Anwendung generierten Last nach oben und unten skaliert. Wenn die Kapazität begrenzt ist, wird die OpenSearch Aufnahme skaliert, indem mehr Recheneinheiten (GiB Arbeitsspeicher) zugewiesen werden. Wenn Ihre Pipeline kleinere Workloads oder gar keine Daten verarbeitet, kann sie auf die minimal konfigurierten Ingestion-OCUs herunterskaliert werden.

Sie können mindestens 1 Ingestion-OCU, maximal 96 Ingestion-OCUs für statusfreie Pipelines und maximal 48 Ingestion-OCUs für statusbehaftete Pipelines angeben. Wir empfehlen mindestens 2 Ingestion-OCUs für Push-basierte Quellen. Wenn die persistente Pufferung aktiviert ist, können Sie mindestens 2 und maximal 384 Ingestion-OCUs angeben.

Bei einer Standard-Log-Pipeline mit einer einzigen Quelle, einem einfachen Grok-Muster und einer Senke kann jede Recheneinheit bis zu 2 MiB pro Sekunde unterstützen. Bei komplexeren Protokoll-Pipelines mit mehreren Prozessoren unterstützt jede Recheneinheit möglicherweise weniger Aufnahmelast. Basierend auf der Pipeline-Kapazität und der Ressourcennutzung setzt der Prozess der OpenSearch Ingestion-Skalierung ein.

Um eine hohe Verfügbarkeit zu gewährleisten, sind die Ingestion-OCUs auf mehrere Availability Zones (AZs) verteilt. Die Anzahl der AZs hängt von der von Ihnen angegebenen Mindestkapazität ab.

Wenn Sie beispielsweise mindestens 2 Recheneinheiten angeben, werden die Ingestion-OCUs, die zu einem bestimmten Zeitpunkt verwendet werden, gleichmäßig auf 2 AZs verteilt. Wenn Sie mindestens 3 oder mehr Recheneinheiten angeben, sind die Ingestion-OCUs gleichmäßig auf 3 AZs verteilt. Wir empfehlen, dass Sie mindestens zwei Ingestion-OCUs bereitstellen, um eine Verfügbarkeit von 99,9% für Ihre Ingest-Pipelines sicherzustellen.

Ingestion-OCUs werden Ihnen nicht in Rechnung gestellt, wenn sich eine Pipeline in den Bundesstaaten,, und befindet. `Create failed` `Creating` `Deleting` `Stopped`

Anweisungen zum Konfigurieren und Abrufen von Kapazitätseinstellungen für eine Pipeline finden Sie unter. the section called “Pipelines erstellen”

OpenSearch Preise für die Aufnahme

Zu einem bestimmten Zeitpunkt zahlen Sie nur für die Anzahl der Ingestion-OCUs, die einer Pipeline zugewiesen sind, unabhängig davon, ob Daten durch die Pipeline fließen. OpenSearch Ingestion passt sich Ihren Workloads sofort an, indem die Pipeline-Kapazität je nach Nutzung nach oben oder unten skaliert wird.

Vollständige Preisinformationen finden Sie unter Amazon OpenSearch Service-Preise.

Unterstützt AWS-Regionen

OpenSearch Die Aufnahme ist in einem Teil des Services verfügbar AWS-Regionen , in dem der OpenSearch Service verfügbar ist. Eine Liste der unterstützten Regionen finden Sie unter Amazon OpenSearch Service-Endpunkte und Kontingente in der Allgemeine AWS-Referenz.

OpenSearch Kontingente für die Inanspruchnahme

Eine Liste der Standardkontingente für OpenSearch Ingestion-Ressourcen finden Sie unter Amazon OpenSearch Service-Kontingente.

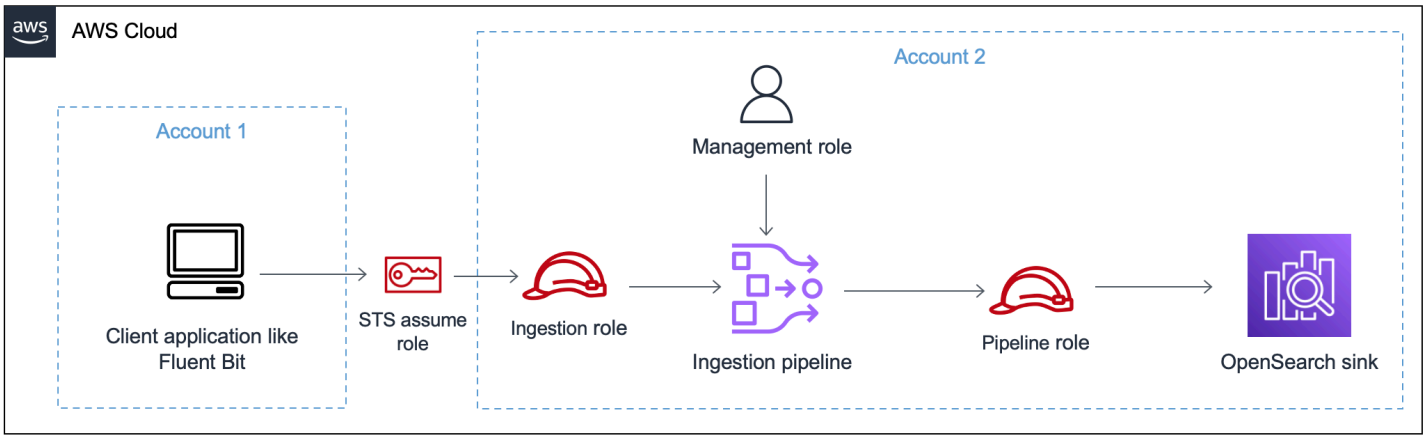
Rollen und Benutzer in Amazon OpenSearch Ingestion einrichten

Amazon OpenSearch Ingestion verwendet eine Vielzahl von Berechtigungsmodellen und IAM-Rollen, um Quellanwendungen das Schreiben in Pipelines und Pipelines das Schreiben in Senken zu ermöglichen. Bevor Sie mit der Datenaufnahme beginnen können, müssen Sie je nach Anwendungsfall eine oder mehrere IAM-Rollen mit spezifischen Berechtigungen erstellen.

Für die Einrichtung einer erfolgreichen Pipeline sind mindestens die folgenden Rollen erforderlich.

Name	Beschreibung
Rolle in der Verwaltung	Jeder Prinzipal, der Pipelines verwaltet (in der Regel ein „Pipeline-Administrator“), benötigt Verwaltungszugriff, der Berechtigungen wie `osis:CreatePipeline` und `osis:UpdatePipeline` beinhaltet. Diese Berechtigungen ermöglichen es einem Benutzer, Pipelines zu verwalten, aber nicht unbedingt Daten in sie zu schreiben.
Rolle „Pipeline“	Die Pipeline-Rolle, die Sie in der YAML-Konfiguration der Pipeline angeben, bietet die erforderlichen Berechtigungen für eine Pipeline, um in die Domain oder Collection-Senke zu schreiben und aus Pull-basierten Quellen zu lesen. Weitere Informationen finden Sie unter den folgenden Themen: • the section called “Pipelines Zugriff auf Domains gewähren” • the section called “Pipelines Zugriff auf Sammlungen gewähren”
Rolle „Ingestion“	Die Rolle „Ingestion“ enthält die `osis:Ingest` Berechtigung für die Pipeline-Ressource. Diese Berechtigung ermöglicht es Push-basierten Quellen, Daten in eine Pipeline aufzunehmen.

Die folgende Abbildung zeigt ein typisches Pipeline-Setup, bei dem eine Datenquelle wie Amazon S3 oder Fluent Bit in eine Pipeline in einem anderen Konto schreibt. In diesem Fall muss der Client die Rolle der Datenerfassung übernehmen, um auf die Pipeline zugreifen zu können. Weitere Informationen finden Sie unter the section called “Kontoübergreifende Erfassung”.



Eine einfache Anleitung zur Einrichtung finden Sie unter. the section called “Tutorial: Daten in eine Domain aufnehmen”

Topics

- the section called “Rolle in der Verwaltung”
- the section called “Rolle bei der Aufnahme”
- the section called “Rolle „Pipeline“”
- the section called “Kontoübergreifende Erfassung”

Rolle in der Verwaltung

Zusätzlich zu den grundlegenden `osis:*` Berechtigungen, die zum Erstellen und Ändern einer Pipeline erforderlich sind, benötigen Sie auch die `iam:PassRole` Berechtigung für die Pipeline-Rollenressource. JederAWS-Service, der eine Rolle akzeptiert, muss diese Berechtigung verwenden. OpenSearch Ingestion übernimmt die Rolle jedes Mal, wenn Daten in eine Datensenke geschrieben werden müssen. Auf diese Weise können Administratoren sicherstellen, dass nur autorisierte Benutzer OpenSearch Ingestion mit einer Rolle konfigurieren können, die Berechtigungen gewährt. Weitere Informationen finden Sie unter Einem Benutzer Berechtigungen zur Übergabe einer Rolle an einen gewähren. AWS-Service

Wenn Sie die verwenden AWS Management Console (mithilfe von Blueprints und späterer Überprüfung Ihrer Pipeline), benötigen Sie die folgenden Berechtigungen, um eine Pipeline zu erstellen und zu aktualisieren:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Resource":"*",
         "Action":[
            "osis:CreatePipeline",
            "osis:GetPipelineBlueprint",
            "osis:ListPipelineBlueprints",
            "osis:GetPipeline",
            "osis:ListPipelines",
            "osis:GetPipelineChangeProgress",
            "osis:ValidatePipeline",
```

```
            "osis:UpdatePipeline"
         ]
      },
      {
         "Resource":[
            "arn:aws:iam::{your-account-id}:role/pipeline-role"
         ],
         "Effect":"Allow",
         "Action":[
            "iam:PassRole"
         ]
      }
   ]
}
```

Wenn Sie die verwenden AWS CLI (ohne Ihre Pipeline vorab zu validieren oder Blueprints zu verwenden), benötigen Sie die folgenden Berechtigungen, um eine Pipeline zu erstellen und zu aktualisieren:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Resource":"*",
         "Action":[
            "osis:CreatePipeline",
            "osis:UpdatePipeline"
         ]
      },
      {
         "Resource":[
            "arn:aws:iam::{your-account-id}:role/pipeline-role"
         ],
         "Effect":"Allow",
         "Action":[
            "iam:PassRole"
         ]
      }
   ]
}
```

Rolle „Pipeline“

Eine Pipeline benötigt bestimmte Berechtigungen, um in ihre Senke schreiben zu können. Diese Berechtigungen hängen davon ab, ob es sich bei der Senke um eine OpenSearch Dienstdomäne oder eine OpenSearch serverlose Sammlung handelt.

Darüber hinaus benötigt eine Pipeline möglicherweise Berechtigungen zum Abrufen von Inhalten aus der Quellanwendung (wenn es sich bei der Quelle um ein Pull-basiertes Plug-in handelt) und Berechtigungen zum Schreiben in eine S3-Warteschlange mit unerlaubter Nachricht, sofern konfiguriert.

Themen

In eine Domainsenke schreiben

Eine OpenSearch Ingestion-Pipeline benötigt die Berechtigung, in eine OpenSearch Dienstdomäne zu schreiben, die als Senke konfiguriert ist. Zu diesen Berechtigungen gehört die Fähigkeit, die Domain zu beschreiben und HTTP-Anfragen an sie zu senden.

Um Ihrer Pipeline die erforderlichen Berechtigungen zum Schreiben in eine Senke zu gewähren, erstellen Sie zunächst eine AWS Identity and Access Management (IAM-) Rolle mit den erforderlichen Berechtigungen. Diese Berechtigungen sind für öffentliche Pipelines und VPC-Pipelines identisch. Geben Sie dann die Pipeline-Rolle in der Domänenzugriffsrichtlinie an, damit die Domäne Schreibanforderungen von der Pipeline annehmen kann.

Geben Sie abschließend den Rollen-ARN als Wert der Option sts_role_arn in der Pipeline-Konfiguration an:

```
version: "2"
source:
  http:
    ...
processor:
  ...
sink:
```

```
  - opensearch:
      ...
      aws:
        sts_role_arn: arn:aws:iam::{your-account-id}:role/pipeline-role
```

Anweisungen zum Ausführen der einzelnen Schritte finden Sie unter Zulassen des Zugriffs von Pipelines auf Domänen.

In eine Sammelsenke schreiben

Eine OpenSearch Ingestion-Pipeline benötigt die Berechtigung, in eine OpenSearch serverlose Sammlung zu schreiben, die als Senke konfiguriert ist. Zu diesen Berechtigungen gehört die Fähigkeit, die Sammlung zu beschreiben und HTTP-Anfragen an sie zu senden.

Erstellen Sie zunächst eine IAM-Rolle, die über die `aoss:BatchGetCollection` Berechtigung für alle Ressourcen verfügt (*). Nehmen Sie diese Rolle anschließend in eine Datenzugriffsrichtlinie auf und gewähren Sie ihr Berechtigungen zum Erstellen von Indizes, Aktualisieren von Indizes, Beschreiben von Indizes und Schreiben von Dokumenten innerhalb der Sammlung. Geben Sie abschließend den Rollen-ARN als Wert der Option sts_role_arn in der Pipeline-Konfiguration an.

Anweisungen zum Ausführen der einzelnen Schritte finden Sie unter Zulassen des Zugriffs von Pipelines auf Sammlungen.

Schreiben in eine Warteschleife mit unzustellbaren Briefen

Wenn Sie Ihre Pipeline so konfigurieren, dass sie in eine Warteschlange mit unerlaubten Buchstaben (DLQ) schreibt, müssen Sie die `sts_role_arn` Option in die DLQ-Konfiguration aufnehmen. Die in dieser Rolle enthaltenen Berechtigungen ermöglichen der Pipeline den Zugriff auf den S3-Bucket, den Sie als Ziel für DLQ-Ereignisse angeben.

Sie müssen dasselbe `sts_role_arn` in allen Pipeline-Komponenten verwenden. Daher müssen Sie Ihrer Pipeline-Rolle, die den DLQ-Zugriff ermöglicht, eine separate Berechtigungsrichtlinie hinzufügen. Der Rolle muss mindestens die `S3:PutObject` Aktion für die Bucket-Ressource gestattet werden:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
      "Sid": "WriteToS3DLQ",
      "Effect": "Allow",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::my-dlq-bucket/*"
    }
  ]
}
```

Anschließend können Sie die Rolle in der DLQ-Konfiguration der Pipeline angeben:

```
  ...
  sink:
    opensearch:
      dlq:
        s3:
          bucket: "my-dlq-bucket"
          key_path_prefix: "dlq-files"
          region: "us-west-2"
          sts_role_arn: "arn:aws:iam::123456789012:role/pipeline-role"
```

Rolle bei der Aufnahme

Alle Quell-Plugins, die OpenSearch Ingestion derzeit unterstützt, mit Ausnahme von S3, verwenden eine Push-basierte Architektur. Das bedeutet, dass die Quellanwendung die Daten in die Pipeline überträgt, anstatt dass die Pipeline die Daten aus der Quelle bezieht.

Daher müssen Sie Ihren Quellanwendungen die erforderlichen Berechtigungen zum Ingestieren von Daten in eine OpenSearch Ingestion-Pipeline gewähren. Der Rolle, die die Anfrage signiert, muss mindestens die Berechtigung für die `osis:Ingest` Aktion erteilt werden, sodass sie Daten an eine Pipeline senden kann. Dieselben Berechtigungen sind für öffentliche Endpunkte und VPC-Pipeline-Endpoints erforderlich.

Die folgende Beispielrichtlinie ermöglicht es dem zugehörigen Principal, Daten in eine einzelne Pipeline mit dem Namen aufzunehmen: `my-pipeline`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PermitsWriteAccessToPipeline",
```

```
      "Effect": "Allow",
      "Action": "osis:Ingest",
      "Resource": "arn:aws:osis:us-west-2:{your-account-id}:pipeline/my-pipeline"
    }
  ]
}
```

Weitere Informationen finden Sie unter the section called “Arbeiten mit Pipeline-Integrationen”.

Kontoübergreifende Erfassung

Möglicherweise müssen Sie Daten von einem anderen Konto, z. B. einem AnwendungskontoAWS-Konto, in eine Pipeline aufnehmen. Um die kontoübergreifende Erfassung zu konfigurieren, definieren Sie eine Aufnahmerolle innerhalb desselben Kontos wie die Pipeline und richten Sie eine Vertrauensbeziehung zwischen der Aufnahmerolle und dem Anwendungskonto ein:

```
{
  "Version": "2012-10-17",
  "Statement": [{
     "Effect": "Allow",
     "Principal": {
       "AWS": "arn:aws:iam::{external-account-id}:root"
      },
     "Action": "sts:AssumeRole"
  }]
}
```

Konfigurieren Sie dann Ihre Anwendung so, dass sie die Aufnahmerolle übernimmt. Das Anwendungskonto muss der Anwendungsrolle AssumeRoleBerechtigungen für die Aufnahmerolle im Pipeline-Konto gewähren.

Ausführliche Schritte und Beispiele für IAM-Richtlinien finden Sie unter. the section called “Bereitstellung von kontenübergreifendem Zugriff auf Datenerfassung”

Amazon OpenSearch Ingestion-Pipelines Zugriff auf Domains gewähren

Eine Amazon OpenSearch Ingestion-Pipeline benötigt die Berechtigung, in die OpenSearch Service-Domain zu schreiben, die als Senke konfiguriert ist. Um Zugriff zu gewähren, konfigurieren Sie eine AWS Identity and Access Management (IAM-) Rolle mit einer restriktiven Berechtigungsrichtlinie, die den Zugriff auf die Domain beschränkt, an die eine Pipeline Daten sendet. Beispielsweise möchten

Sie eine Erfassungspipeline möglicherweise nur auf die Domäne und die Indizes beschränken, die zur Unterstützung ihres Anwendungsfalls erforderlich sind.

Bevor Sie die Rolle in Ihrer Pipeline-Konfiguration angeben, müssen Sie sie mit einer entsprechenden Vertrauensstellung konfigurieren und ihr dann innerhalb der Domänenzugriffsrichtlinie Zugriff auf die Domäne gewähren.

Themen

Schritt 1: Erstellen Sie eine Pipeline-Rolle

Der Rolle, die Sie im Parameter sts_role_arn einer Pipeline-Konfiguration angeben, muss eine Berechtigungsrichtlinie angehängt sein, die es ihr ermöglicht, Daten an die Domänensenke zu senden. Außerdem muss sie über eine Vertrauensstellung verfügen, die es OpenSearch Ingestion ermöglicht, die Rolle zu übernehmen. Anweisungen zum Anhängen einer Richtlinie an eine Rolle finden Sie unter Hinzufügen von IAM-Identitätsberechtigungen im IAM-Benutzerhandbuch.

Die folgende Beispielrichtlinie zeigt die geringste Berechtigung, die Sie in der Rolle sts_role_arn einer Pipeline-Konfiguration für das Schreiben in eine einzelne Domäne gewähren können:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "es:DescribeDomain",
            "Resource": "arn:aws:es:*:{your-account-id}:domain/*"
        },
        {
            "Effect": "Allow",
            "Action": "es:ESHttp*",
            "Resource": "arn:aws:es:*:{your-account-id}:domain/{domain-namedomain}/*"
        }
    ]
```

```
}
```

Wenn Sie die Rolle wiederverwenden möchten, um in mehrere Domänen zu schreiben, können Sie die Richtlinie weiter fassen, indem Sie den Domänennamen durch ein Platzhalterzeichen () ersetzen. *

Die Rolle muss über die folgende Vertrauensstellung verfügen, sodass OpenSearch Ingestion die Pipeline-Rolle übernehmen kann:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"osis-pipelines.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

Darüber hinaus empfehlen wir, dass Sie der Richtlinie die Schlüssel `aws:SourceAccount` und die `aws:SourceArn` Bedingungsschlüssel hinzufügen, um sich vor dem Problem mit dem verwirrten Stellvertreter zu schützen. Das Quellkonto ist der Besitzer der Pipeline.

Beispielsweise können Sie der Richtlinie den folgenden Bedingungsblock hinzufügen:

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "{your-account-id}"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:osis:{region}:{your-account-id}:pipeline/*"
    }
}
```

Schritt 2: Nehmen Sie die Pipeline-Rolle in die Domänenzugriffsrichtlinie auf

Damit eine Pipeline Daten in eine Domäne schreiben kann, muss die Domäne über eine Zugriffsrichtlinie auf Domänenebene verfügen, die der Pipeline-Rolle sts_role_arn den Zugriff darauf ermöglicht.

Die folgende Beispielrichtlinie für den Domänenzugriff ermöglicht es der Pipeline-Rolle mit dem Namen`pipeline-role`, die Sie im vorherigen Schritt erstellt haben, Daten in die angegebene Domäne zu schreiben: `ingestion-domain`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::{your-account-id}:role/{pipeline-role}"
      },
      "Action": ["es:DescribeDomain", "es:ESHttp*"],
      "Resource": "arn:aws:es:{region}:{your-account-id}:domain/{domain-name}/*"
    }
  ]
}
```

Schritt 3: Ordnen Sie die Pipeline-Rolle zu (nur für Domänen, die eine differenzierte Zugriffskontrolle verwenden)

Wenn Ihre Domain eine differenzierte Zugriffskontrolle für die Authentifizierung verwendet, müssen Sie zusätzliche Schritte unternehmen, um Ihrer Pipeline Zugriff auf eine Domain zu gewähren. Die Schritte unterscheiden sich je nach Ihrer Domain-Konfiguration:

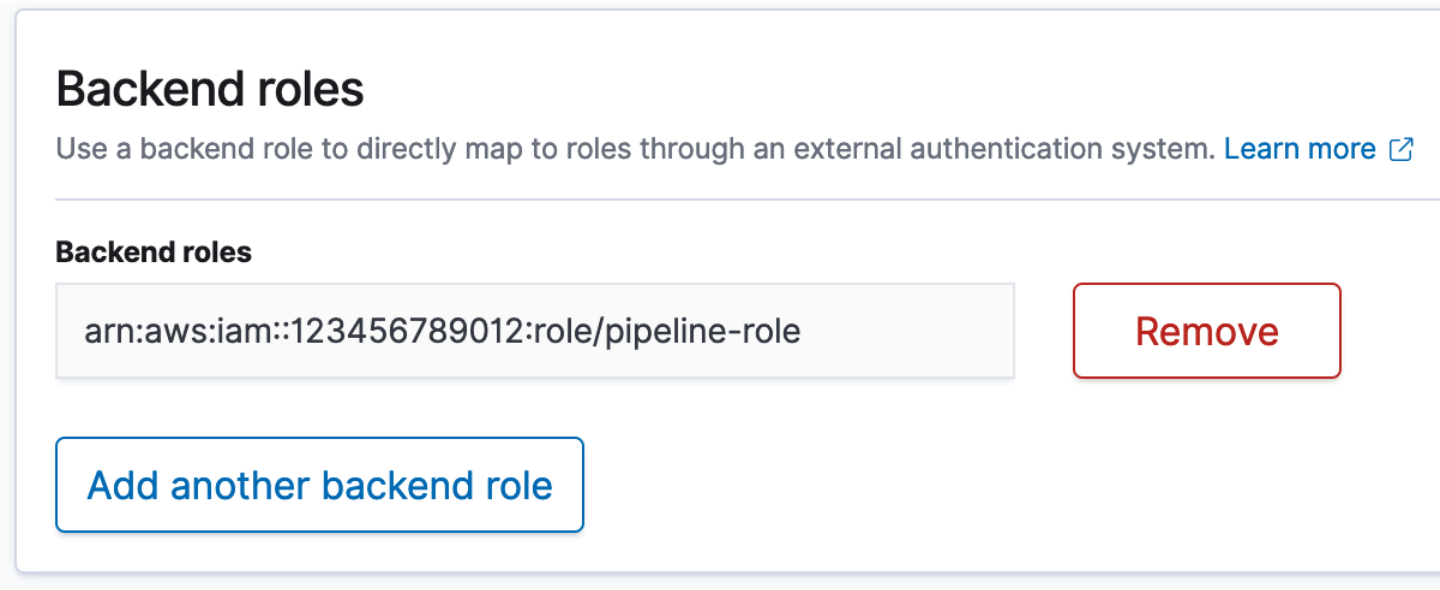
Szenario 1: Verschiedene Master-Rolle und Pipeline-Rolle — Wenn Sie einen IAM-Amazon-Ressourcennamen (ARN) als Master-Benutzer verwenden und dieser sich von der Pipeline-Rolle (`sts_role_arn`) unterscheidet, müssen Sie die Pipeline-Rolle der OpenSearch `all_access` Backend-Rolle zuordnen. Dadurch wird die Pipeline-Rolle im Wesentlichen als zusätzlicher Masterbenutzer hinzugefügt. Weitere Informationen finden Sie unter Zusätzliche Masterbenutzer.

Szenario 2: Hauptbenutzer in der internen Benutzerdatenbank — Wenn Ihre Domain einen Masterbenutzer in der internen Benutzerdatenbank und die HTTP-Basisauthentifizierung für OpenSearch Dashboards verwendet, können Sie den Hauptbenutzernamen und das Kennwort

nicht direkt an die Pipeline-Konfiguration übergeben. Stattdessen müssen Sie die Pipeline-Rolle (`sts_role_arn`) der OpenSearch `all_access` Backend-Rolle zuordnen. Dadurch wird im Wesentlichen die Pipeline-Rolle als zusätzlicher Masterbenutzer hinzugefügt. Weitere Informationen finden Sie unter Zusätzliche Masterbenutzer.

Szenario 3: Gleiche Master-Rolle und Pipeline-Rolle (ungewöhnlich) — Wenn Sie einen IAM-ARN als Master-Benutzer verwenden und es sich um denselben ARN handelt, den Sie als Pipeline-Rolle (`sts_role_arn`) verwenden, müssen Sie keine weiteren Maßnahmen ergreifen. Die Pipeline verfügt über die erforderlichen Berechtigungen, um in die Domain zu schreiben. Dieses Szenario ist ungewöhnlich, da die meisten Umgebungen eine Administratorrolle oder eine andere Rolle als Masterrolle verwenden.

Die folgende Abbildung zeigt, wie die Pipeline-Rolle einer Backend-Rolle zugeordnet wird:



Schritt 4: Geben Sie die Rolle in der Pipeline-Konfiguration an

Um erfolgreich eine Pipeline zu erstellen, müssen Sie die Pipeline-Rolle, die Sie in Schritt 1 erstellt haben, als Parameter sts_role_arn in Ihrer Pipeline-Konfiguration angeben. Die Pipeline übernimmt diese Rolle, um Anfragen an die Service-Domänensenke zu signieren. OpenSearch

Geben Sie im `sts_role_arn` Feld den ARN der IAM-Pipeline-Rolle an:

```
version: "2"
log-pipeline:
  source:
    http:
```

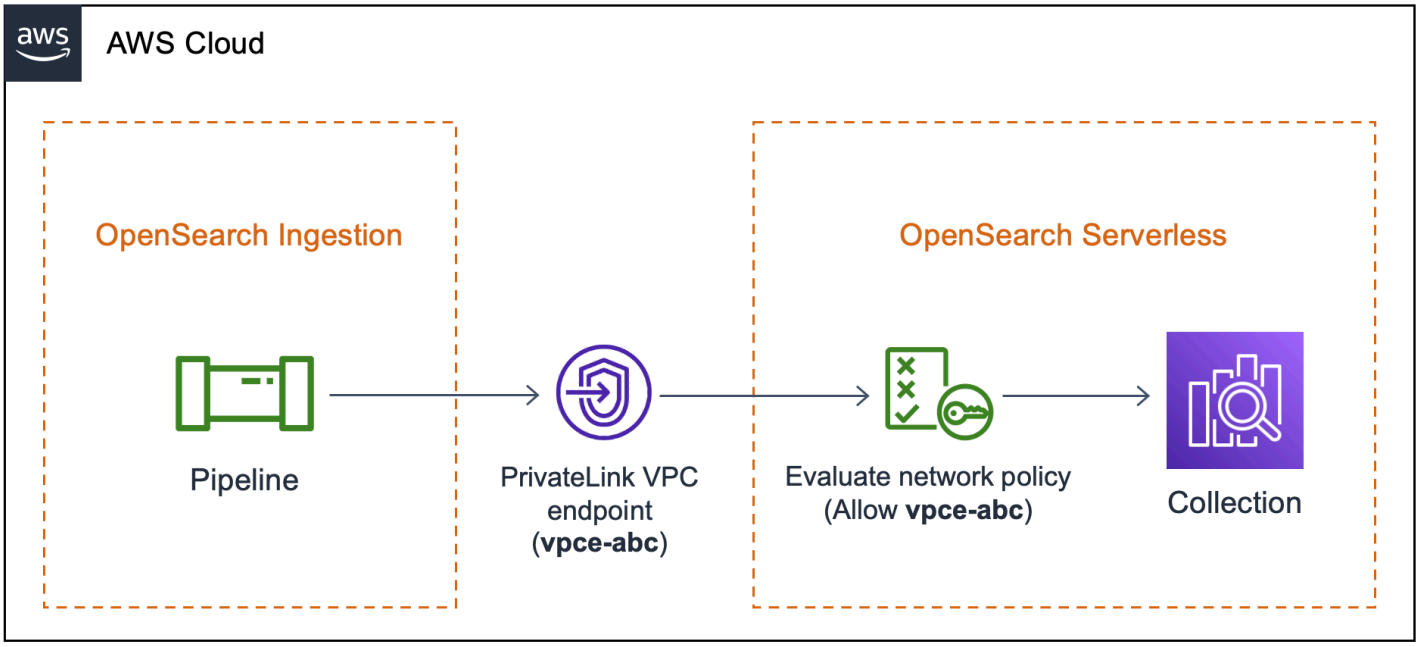
```
      path: "/${pipelineName}/logs"
  processor:
    - grok:
        match:
          log: [ "%{COMMONAPACHELOG}" ]
  sink:
    - opensearch:
        hosts: [ "https://search-{domain-name}.us-east-1.es.amazonaws.com" ]
        index: "my-index"
        aws:
          region: "{region}"
          sts_role_arn: "arn:aws:iam::{your-account-id}:role/{pipeline-role}"
```

Eine vollständige Referenz der erforderlichen und nicht unterstützten Parameter finden Sie unter. the section called “Unterstützte Plugins und Optionen”

Amazon OpenSearch Ingestion-Pipelines Zugriff auf Sammlungen gewähren

Eine Amazon OpenSearch Ingestion-Pipeline kann in eine OpenSearch serverlose öffentliche Sammlung oder VPC-Sammlung schreiben. Um Zugriff auf die Sammlung zu gewähren, konfigurieren Sie eine AWS Identity and Access Management (IAM-) Pipeline-Rolle mit einer Berechtigungsrichtlinie, die Zugriff auf die Sammlung gewährt. Bevor Sie die Rolle in Ihrer Pipeline-Konfiguration angeben, müssen Sie sie mit einer entsprechenden Vertrauensbeziehung konfigurieren und ihr dann über eine Datenzugriffsrichtlinie Datenzugriffsberechtigungen gewähren.

Während der Pipelineerstellung stellt OpenSearch Ingestion eine AWS PrivateLink Verbindung zwischen der Pipeline und der OpenSearch Serverless-Sammlung her. Der gesamte Datenverkehr von der Pipeline durchläuft diesen VPC-Endpunkt und wird an die Sammlung weitergeleitet. Um die Sammlung zu erreichen, muss dem Endpunkt über eine Netzwerkzugriffsrichtlinie Zugriff auf die Sammlung gewährt werden.



Themen

Einschränkungen

Die folgenden Einschränkungen gelten für Pipelines, die in OpenSearch serverlose Sammlungen schreiben:

- Der OTel Trace Group Processor funktioniert derzeit nicht mit OpenSearch serverlosen Sammelsenken.
- Derzeit unterstützt OpenSearch Ingestion nur den `_template` Legacy-Vorgang, während OpenSearch Serverless den Composable-Vorgang unterstützt. `_index_template` Wenn Ihre Pipeline-Konfiguration die `index_type` Option enthält, muss sie daher auf eingestellt sein. `management_disabled`

Bereitstellung des Netzwerkzugriffs auf Pipelines

Jeder Sammlung, die Sie in OpenSearch Serverless erstellen, ist mindestens eine Netzwerkzugriffsrichtlinie zugeordnet. Netzwerkzugriffsrichtlinien bestimmen, ob auf die Sammlung über das Internet von öffentlichen Netzwerken aus zugegriffen werden kann oder ob privat darauf zugegriffen werden muss. Weitere Informationen zu Netzwerkrichtlinien finden Sie unterthe section called “Netzwerkzugriff”.

Innerhalb einer Netzwerkzugriffsrichtlinie können Sie nur OpenSearch serverlos verwaltete VPC-Endpunkte angeben. Weitere Informationen finden Sie unter the section called “VPC-Endpunkte”. Damit die Pipeline jedoch in die Sammlung schreiben kann, muss die Richtlinie auch Zugriff auf den VPC-Endpunkt gewähren, den OpenSearch Ingestion automatisch zwischen der Pipeline und der Sammlung erstellt. Wenn Sie also eine Pipeline erstellen, die über eine OpenSearch serverlose Sammelsenke verfügt, müssen Sie den Namen der zugehörigen Netzwerkrichtlinie mithilfe der Option angeben. `network_policy_name`

Beispielsweise:

```
...
sink:
   - opensearch:
       hosts: [ "https://{collection-id}.{region}.aoss.amazonaws.com" ]
       index: "my-index"
        aws:
          serverless: true
          serverless_options:
            network_policy_name: "{network-policy-name}"
```

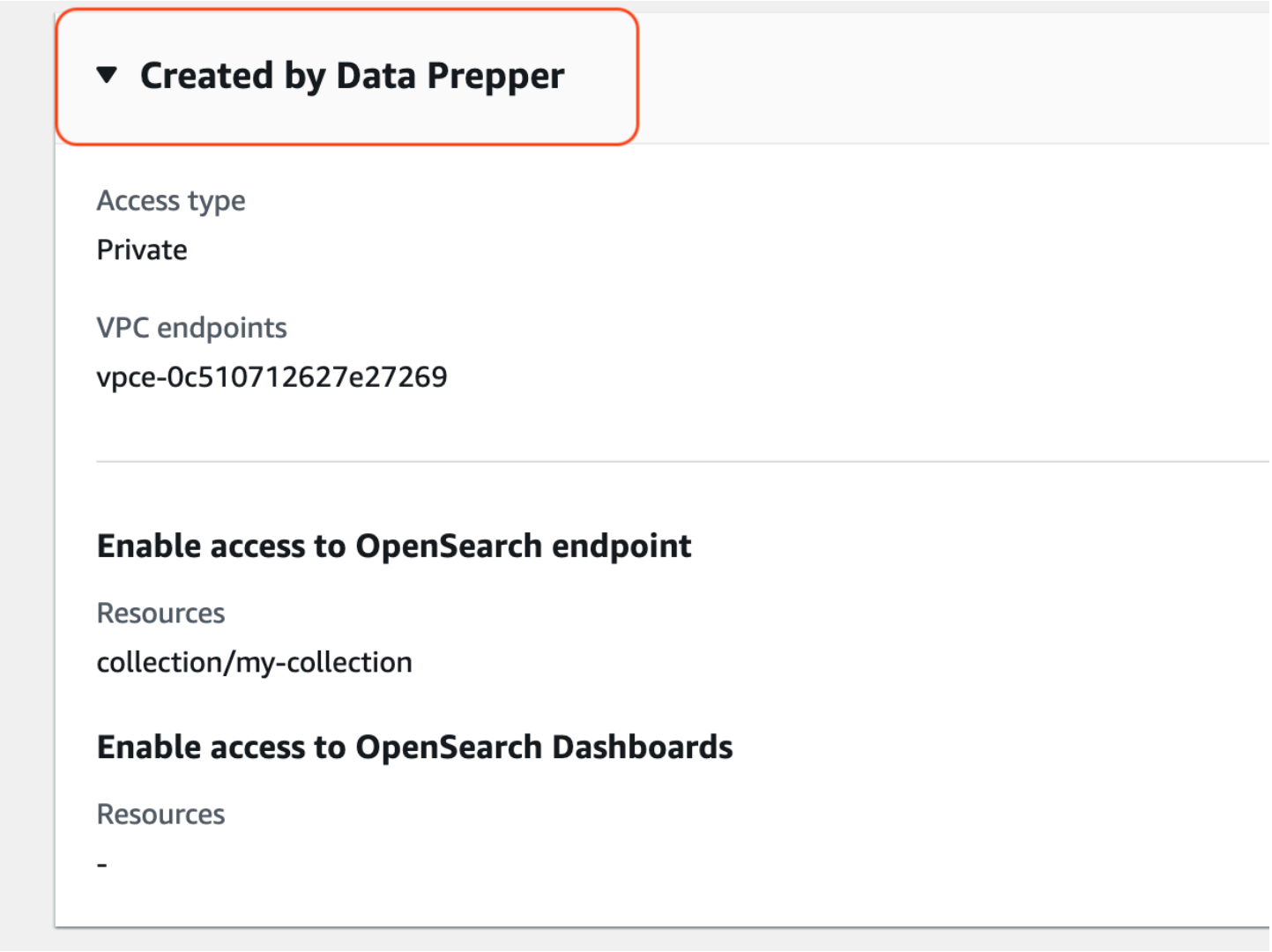
Bei der Erstellung der Pipeline überprüft OpenSearch Ingestion, ob die angegebene Netzwerkrichtlinie vorhanden ist. Wenn sie nicht existiert, wird sie von OpenSearch Ingestion erstellt. Falls sie existiert, aktualisiert OpenSearch Ingestion sie, indem ihr eine neue Regel hinzugefügt wird. Die Regel gewährt Zugriff auf den VPC-Endpunkt, der die Pipeline und die Sammlung verbindet.

Beispielsweise:

```
{
   "Rules":[
      {
         "Resource":[
            "collection/my-collection"
```

```
         ],
         "ResourceType":"collection"
      }
   ],
   "SourceVPCEs":[
      "vpce-0c510712627e27269" # The ID of the VPC endpoint that OpenSearch Ingestion
 creates between the pipeline and collection
   ],
   "Description":"Created by Data Prepper"
}
```

In der Konsole erhalten alle Regeln, die OpenSearch Ingestion Ihren Netzwerkrichtlinien hinzufügt, den Namen Created by Data Prepper:



> **Note**
>
> Im Allgemeinen hat eine Regel, die den öffentlichen Zugriff auf eine Sammlung festlegt, Vorrang vor einer Regel, die privaten Zugriff festlegt. Wenn für die Richtlinie bereits öffentlicher Zugriff konfiguriert war, ändert diese neue Regel, die OpenSearch Ingestion hinzufügt, das Verhalten der Richtlinie also nicht. Weitere Informationen finden Sie unter the section called “Vorrang der Richtlinie”.

Wenn Sie die Pipeline beenden oder löschen, löscht OpenSearch Ingestion den VPC-Endpunkt zwischen der Pipeline und der Sammlung. Es ändert auch die Netzwerkrichtlinie, um den VPC-Endpunkt aus der Liste der zulässigen Endpunkte zu entfernen. Wenn Sie die Pipeline neu starten, erstellt sie den VPC-Endpunkt neu und aktualisiert die Netzwerkrichtlinie erneut mit der Endpunkt-ID.

Schritt 1: Erstellen Sie eine Pipeline-Rolle

Für die Rolle, die Sie im Parameter sts_role_arn einer Pipeline-Konfiguration angeben, muss eine Berechtigungsrichtlinie angehängt sein, die es ihr ermöglicht, Daten an die Sammlungssenke zu senden. Außerdem muss sie über eine Vertrauensstellung verfügen, die es OpenSearch Ingestion ermöglicht, die Rolle zu übernehmen. Anweisungen zum Anhängen einer Richtlinie an eine Rolle finden Sie unter Hinzufügen von IAM-Identitätsberechtigungen im IAM-Benutzerhandbuch.

Die folgende Beispielrichtlinie zeigt die geringste Berechtigung, die Sie in der Rolle sts_role_arn einer Pipeline-Konfiguration für das Schreiben in Sammlungen bereitstellen können:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": [
                "aoss:APIAccessAll",
                "aoss:BatchGetCollection",
                "aoss:CreateSecurityPolicy",
                "aoss:GetSecurityPolicy",
                "aoss:UpdateSecurityPolicy"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

Die Rolle muss über die folgende Vertrauensstellung verfügen, damit Ingestion sie übernehmen kann OpenSearch :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "osis-pipelines.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Schritt 2: Erstellen einer Sammlung

Erstellen Sie eine OpenSearch serverlose Sammlung mit den folgenden Einstellungen. Anweisungen zum Erstellen einer Sammlung finden Sie unterthe section called “Erstellen von Sammlungen”.

Richtlinie für den Datenzugriff

Erstellen Sie eine Datenzugriffsrichtlinie für die Sammlung, die der Pipeline-Rolle die erforderlichen Berechtigungen gewährt. Beispielsweise:

```
[
  {
    "Rules": [
      {
        "Resource": [
          "index/{collection-name}/*"
        ],
        "Permission": [
          "aoss:CreateIndex",
          "aoss:UpdateIndex",
          "aoss:DescribeIndex",
          "aoss:WriteDocument"
```

```
        ],
        "ResourceType": "index"
      }
    ],
    "Principal": [
      "arn:aws:iam::{account-id}:role/{pipeline-role}"
    ],
    "Description": "Pipeline role access"
  }
]
```

> **Note**
>
> Geben Sie in dem `Principal` Element den Amazon-Ressourcennamen (ARN) der Pipeline-Rolle an, die Sie im vorherigen Schritt erstellt haben.

Richtlinie für den Netzwerkzugriff

Erstellen Sie eine Netzwerkzugriffsrichtlinie für die Sammlung. Sie können Daten in eine öffentliche Sammlung oder eine VPC-Sammlung aufnehmen. Die folgende Richtlinie bietet beispielsweise Zugriff auf einen einzelnen, serverlos verwalteten OpenSearch VPC-Endpunkt:

```
[
   {
      "Description":"Rule 1",
      "Rules":[
         {
            "ResourceType":"collection",
            "Resource":[
               "collection/{collection-name}"
            ]
         }
      ],
      "AllowFromPublic": false,
      "SourceVPCEs":[
         "vpce-050f79086ee71ac05"
      ]
   }
]
```

> **Important**
>
> Sie müssen den Namen der Netzwerkrichtlinie innerhalb der `network_policy_name` Option in der Pipeline-Konfiguration angeben. Zum Zeitpunkt der Pipeline-Erstellung aktualisiert OpenSearch Ingestion diese Netzwerkrichtlinie, um den Zugriff auf den VPC-Endpunkt zu ermöglichen, der automatisch zwischen der Pipeline und der Sammlung erstellt wird. In Schritt 3 finden Sie ein Beispiel für eine Pipeline-Konfiguration. Weitere Informationen finden Sie unter the section called “Bereitstellung des Netzwerkzugriffs auf Pipelines”.

Schritt 3: Erstellen Sie eine Pipeline

Erstellen Sie abschließend eine Pipeline, in der Sie die Pipeline-Rolle und die Sammlungsdetails angeben. Die Pipeline übernimmt diese Rolle, um Anfragen an die OpenSearch Serverless Collection Sink zu signieren.

Stellen Sie Folgendes sicher:

- Geben Sie für die `hosts` Option den Endpunkt der Sammlung an, die Sie in Schritt 2 erstellt haben.
- Geben Sie für die `sts_role_arn` Option den Amazon-Ressourcennamen (ARN) der Pipeline-Rolle an, die Sie in Schritt 1 erstellt haben.
- Stellen Sie die `serverless` Option auf ein`true`.
- Stellen Sie die `network_policy_name` Option auf den Namen der Netzwerkrichtlinie ein, die der Sammlung zugeordnet ist. OpenSearch Die Aufnahme aktualisiert diese Netzwerkrichtlinie automatisch, um den Zugriff von der VPC aus zu ermöglichen, die sie zwischen der Pipeline und der Sammlung erstellt. Weitere Informationen finden Sie unter the section called “Bereitstellung des Netzwerkzugriffs auf Pipelines”.

```
version: "2"
log-pipeline:
  source:
    http:
        path: "/log/ingest"
  processor:
    - date:
        from_time_received: true
```

```
        destination: "@timestamp"
  sink:
    - opensearch:
        hosts: [ "https://{collection-id}.{region}.aoss.amazonaws.com" ]
        index: "my-index"
        aws:
          serverless: true
          serverless_options:
            network_policy_name: "{network-policy-name}" # If the policy doesn't exist,
a new policy is created.
          region: "us-east-1"
          sts_role_arn: "arn:aws:iam::{account-id}:role/{pipeline-role}"
```

Eine vollständige Referenz der erforderlichen und nicht unterstützten Parameter finden Sie unter. the section called “Unterstützte Plugins und Optionen”

Erste Schritte Schritte Schritte Schritte Schritte Schritte Schritte Schritte Schritte Schritte Schritte Schritte Schritte Schritte Schritte OpenSearch

Amazon OpenSearch Ingestion unterstützt das Einlesen von Daten in verwaltete OpenSearch Service-Domänen und OpenSearch serverlose Sammlungen. Die folgenden Tutorials führen Sie durch die grundlegenden Schritte, um eine Pipeline auszuführen.

> **Note**
>
> Die Erstellung der Pipeline schlägt fehl, wenn Sie nicht die richtigen Berechtigungen einrichten. Informieren Sie the section called “Rollen und Benutzer einrichten” sich über die erforderlichen Rollen, bevor Sie eine Pipeline erstellen.

Themen

Tutorial: Daten mithilfe von Amazon OpenSearch Ingestion in eine Domain aufnehmen

Dieses Tutorial zeigt Ihnen, wie Sie Amazon OpenSearch Ingestion verwenden, um eine einfache Pipeline zu konfigurieren und Daten in eine Amazon OpenSearch Service-Domain aufzunehmen. Eine Pipeline ist eine Ressource, die OpenSearch Ingestion bereitstellt und verwaltet. Sie können eine Pipeline verwenden, um Daten für nachgelagerte Analysen und Visualisierungen in OpenSearch Service zu filtern, anzureichern, zu transformieren, zu normalisieren und zu aggregieren.

Dieses Tutorial führt Sie durch die grundlegenden Schritte, um eine Pipeline schnell zum Laufen zu bringen. Detailliertere Informationen erhalten Sie unter the section called “Pipelines erstellen”.

In diesem Tutorial führen Sie die folgenden Schritte durch:

1. Erstellen Sie die Pipeline-Rolle.
2. Erstellen Sie eine Domäne.
3. Erstellen Sie eine Pipeline.
4. Nehmen Sie einige Beispieldaten auf.

Im Rahmen des Tutorials erstellen Sie die folgenden Ressourcen:

- Eine Pipeline mit dem Namen `ingestion-pipeline`
- Eine Domain mit dem Name`ingestion-domain`, in die die Pipeline schreiben wird
- Eine IAM-Rolle mit dem Name`PipelineRole`, die die Pipeline übernimmt, um in die Domäne zu schreiben

Erforderliche Berechtigungen

Um dieses Tutorial abschließen zu können, benötigen Sie die richtigen IAM-Berechtigungen. Ihrem Benutzer oder Ihrer Rolle muss eine identitätsbasierte Richtlinie mit den folgenden Mindestberechtigungen angehängt sein. Mit diesen Berechtigungen können Sie eine Pipeline-Rolle (`iam:Create`) erstellen, eine Domäne erstellen oder ändern (`es:*`) und mit Pipelines () arbeiten. `osis:*`

Darüber hinaus ist die `iam:PassRole` Berechtigung für die Pipeline-Rollenressource erforderlich. Mit dieser Berechtigung können Sie die Pipeline-Rolle an OpenSearch Ingestion übergeben, sodass Ingestion Daten in die Domäne schreiben kann.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Resource":"*",
         "Action":[
            "osis:*",
            "iam:Create*",
            "es:*"
         ]
      },
      {
         "Resource":[
            "arn:aws:iam::{your-account-id}:role/PipelineRole"
         ],
         "Effect":"Allow",
         "Action":[
            "iam:PassRole"
         ]
      }
   ]
}
```

Schritt 1: Erstellen Sie die Pipeline-Rolle

Erstellen Sie zunächst eine Rolle, die die Pipeline für den Zugriff auf die OpenSearch Service-Domänensenke übernimmt. Sie werden diese Rolle später in diesem Tutorial in die Pipeline-Konfiguration aufnehmen.

Um die Pipeline-Rolle zu erstellen

1. Öffnen Sie die AWS Identity and Access Management Konsole unter https://console.aws.amazon.com/iamv2/.
2. Wählen Sie Richtlinien und dann Richtlinie erstellen aus.
3. In diesem Tutorial werden Sie Daten in eine Domain mit dem Namen aufnehmen`ingestion-domain`, die Sie im nächsten Schritt erstellen werden. Wählen Sie JSON aus und fügen Sie die folgende Richtlinie in den Editor ein. `{your-account-id}`Ersetzen Sie es durch Ihre Konto-ID und ändern Sie gegebenenfalls die Region.

   ```
   {
   ```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "es:DescribeDomain",
            "Resource": "arn:aws:es:us-east-1:{your-account-id}:domain/ingestion-
domain"
        },
        {
            "Effect": "Allow",
            "Action": "es:ESHttp*",
            "Resource": "arn:aws:es:us-east-1:{your-account-id}:domain/ingestion-
domain/*"
        }
    ]
}
```

Wenn Sie Daten in eine bestehende Domain schreiben möchten, `ingestion-domain` ersetzen Sie sie durch den Namen Ihrer Domain.

> **Note**
>
> Der Einfachheit halber verwenden wir in diesem Tutorial eine ziemlich breite Zugriffsrichtlinie. In Produktionsumgebungen empfehlen wir jedoch, dass Sie eine restriktivere Zugriffsrichtlinie auf Ihre Pipeline-Rolle anwenden. Ein Beispiel für eine Richtlinie, die die erforderlichen Mindestberechtigungen bereitstellt, finden Sie unterthe section called “Pipelines Zugriff auf Domains gewähren”.

4. Wählen Sie Weiter, dann Weiter und geben Sie Ihrer Richtlinie einen Namen für Pipeline-Policy.
5. Wählen Sie Richtlinie erstellen aus.
6. Erstellen Sie als Nächstes eine Rolle und fügen Sie ihr die Richtlinie hinzu. Wählen Sie Roles (Rollen) und anschließend Create role (Rolle erstellen).
7. Wählen Sie Benutzerdefinierte Vertrauensrichtlinie und fügen Sie die folgende Richtlinie in den Editor ein:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
```

```
            "Principal":{
               "Service":"osis-pipelines.amazonaws.com"
            },
            "Action":"sts:AssumeRole"
         }
      ]
}
```

8. Wählen Sie Weiter aus. Suchen Sie dann nach der Pipeline-Richtlinie (die Sie gerade erstellt haben) und wählen Sie sie aus.
9. Wählen Sie Weiter und geben Sie der Rolle einen Namen. PipelineRole
10. Wählen Sie Rolle erstellen aus.

Merken Sie sich den Amazon-Ressourcennamen (ARN) der Rolle (z. B.`arn:aws:iam::`*`{your-account-id}`*`:role/PipelineRole`). Sie benötigen ihn, wenn Sie Ihre Pipeline erstellen.

Schritt 2: Erstellen Sie eine Domain

Erstellen Sie als Nächstes eine Domain mit dem Name`ingestion-domain`, in die Daten aufgenommen werden sollen.

Rufen Sie die Amazon OpenSearch Service-Konsole unter https://console.aws.amazon.com/aos/home auf und erstellen Sie eine Domain, die die folgenden Anforderungen erfüllt:

- Läuft OpenSearch 1.0 oder höher oder Elasticsearch 7.4 oder höher
- Verwendet öffentlichen Zugriff
- Verwendet keine differenzierte Zugriffskontrolle

> **Note**
>
> Diese Anforderungen sollen die Einfachheit dieses Tutorials gewährleisten. In Produktionsumgebungen können Sie eine Domain mit VPC-Zugriff konfigurieren und/oder eine differenzierte Zugriffskontrolle verwenden. Informationen zur Verwendung einer detaillierten Zugriffskontrolle finden Sie unter Zuordnung der Pipeline-Rolle.

Die Domäne muss über eine Zugriffsrichtlinie verfügen, die Berechtigungen gewährt`PipelineRole`, die Sie im vorherigen Schritt erstellt haben. Die Pipeline übernimmt diese Rolle (in der Pipeline-

Konfiguration mit dem Namen sts_role_arn bezeichnet), um Daten an die Service-Domänensenke zu senden. OpenSearch

Stellen Sie sicher, dass für die Domäne die folgende Zugriffsrichtlinie auf Domänenebene gilt, die den Zugriff auf die Domäne gewährt. `PipelineRole` Ersetzen Sie die Region und die Konto-ID durch Ihre eigene:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::{your-account-id}:role/PipelineRole"
      },
      "Action": "es:*",
      "Resource": "arn:aws:es:us-east-1:{your-account-id}:domain/ingestion-domain/*"
    }
  ]
}
```

Weitere Informationen zum Erstellen von Zugriffsrichtlinien auf Domänenebene finden Sie unter Ressourcenbasierte Zugriffsrichtlinien.

Wenn Sie bereits eine Domäne erstellt haben, ändern Sie deren bestehende Zugriffsrichtlinie, um die oben genannten Berechtigungen für bereitzustellen. `PipelineRole`

> **Note**
>
> Denken Sie an den Domänenendpunkt (z. B.`https://search-ingestion-domain.us-east-1.es.amazonaws.com`). Sie werden ihn im nächsten Schritt verwenden, um Ihre Pipeline zu konfigurieren.

Schritt 3: Erstellen Sie eine Pipeline

Nachdem Sie nun über eine Domäne und eine Rolle mit den entsprechenden Zugriffsrechten verfügen, können Sie eine Pipeline erstellen.

So erstellen Sie eine Pipeline

1. Wählen Sie in der Amazon OpenSearch Service-Konsole im linken Navigationsbereich Pipelines aus.
2. Wählen Sie Create pipeline (Pipeline erstellen) aus.
3. Geben Sie der Pipeline Ingestion-Pipeline den Namen und behalten Sie die Kapazitätseinstellungen als Standardwerte bei.
4. In diesem Tutorial erstellen Sie eine einfache Sub-Pipeline namens, die `log-pipeline` das Http-Quell-Plugin verwendet. Dieses Plugin akzeptiert Protokolldaten in einem JSON-Array-Format. Sie geben eine einzelne OpenSearch Service-Domain als Senke an und nehmen alle Daten in den `application_logs` Index auf.

   Fügen Sie unter Pipeline-Konfiguration die folgende YAML-Konfiguration in den Editor ein:

```
version: "2"
log-pipeline:
  source:
    http:
      path: "/${pipelineName}/test_ingestion_path"
  processor:
    - date:
        from_time_received: true
        destination: "@timestamp"
  sink:
    - opensearch:
        hosts: [ "https://search-ingestion-domain.us-east-1.es.amazonaws.com" ]
        index: "application_logs"
        aws:
          sts_role_arn: "arn:aws:iam::{your-account-id}:role/PipelineRole"
          region: "us-east-1"
```

> **Note**
>
> Die `path` Option gibt den URI-Pfad für die Aufnahme an. Diese Option ist für Pull-basierte Quellen erforderlich. Weitere Informationen finden Sie unter the section called “Angeben des Aufnahmepfads”.

5. Ersetzen Sie die `hosts` URL durch den Endpunkt der Domain, die Sie im vorherigen Abschnitt erstellt (oder geändert) haben. Ersetzen Sie den `sts_role_arn` Parameter durch den ARN von`PipelineRole`.
6. Wählen Sie „Pipeline validieren“ und stellen Sie sicher, dass die Validierung erfolgreich ist.
7. Der Einfachheit halber konfigurieren Sie in diesem Tutorial den öffentlichen Zugriff für die Pipeline. Wählen Sie unter Netzwerk die Option Öffentlicher Zugriff aus.

   Informationen zur Konfiguration des VPC-Zugriffs finden Sie unterthe section called “Konfiguration des VPC-Zugriffs für Pipelines”.
8. Lassen Sie die Protokollveröffentlichung aktiviert, falls Sie beim Durcharbeiten dieses Tutorials auf Probleme stoßen. Weitere Informationen finden Sie unter the section called “Überwachen der Pipeline-Protokolle”.

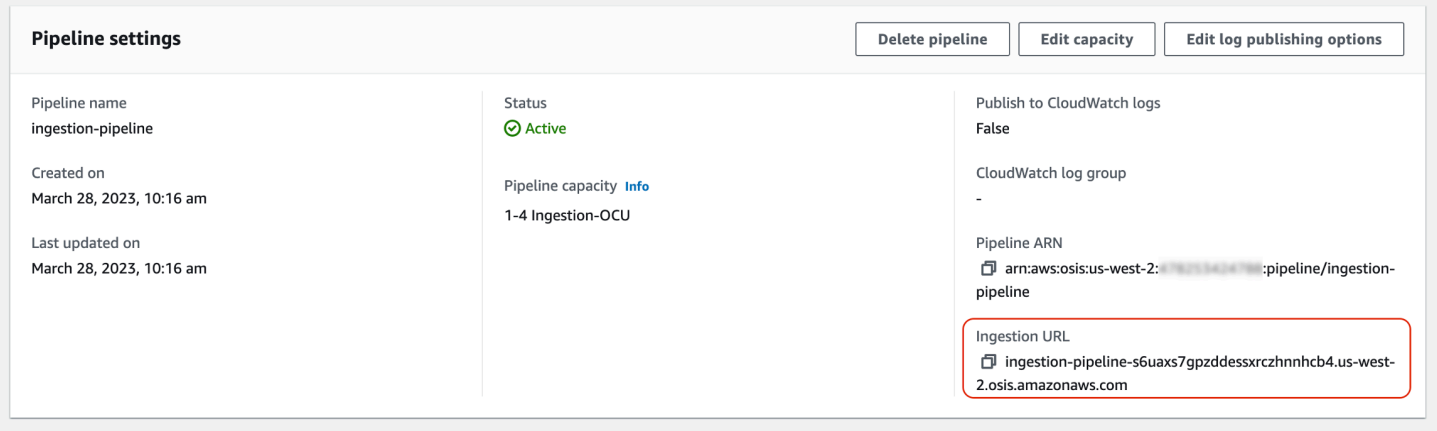
   Geben Sie den folgenden Namen für die Protokollgruppe an: `/aws/vendedlogs/OpenSearchIngestion/ingestion-pipeline/audit-logs`
9. Wählen Sie Weiter aus. Überprüfen Sie Ihre Pipeline-Konfiguration und wählen Sie Create Pipeline aus. Es dauert 5—10 Minuten, bis die Pipeline aktiv wird.

Schritt 4: Nehmen Sie einige Beispieldaten auf

Wenn der Pipeline-Status lautet`Active`, können Sie damit beginnen, Daten in die Pipeline aufzunehmen. Sie müssen alle HTTP-Anfragen an die Pipeline mit Signature Version 4 signieren. Verwenden Sie ein HTTP-Tool wie Postman oder awscurl, um einige Daten an die Pipeline zu senden. Wie bei der direkten Indizierung von Daten in einer Domain erfordert die Aufnahme von Daten in eine Pipeline immer entweder eine IAM-Rolle oder einen IAM-Zugriffsschlüssel und einen geheimen Schlüssel.

> **Note**
>
> Der Principal, der die Anfrage signiert, muss über die IAM-Berechtigung verfügen. `osis:Ingest`

Rufen Sie zunächst die Aufnahme-URL von der Seite mit den Pipeline-Einstellungen ab:



Nehmen Sie dann einige Beispieldaten auf. Die folgende Anfrage verwendet awscurl, um eine einzelne Protokolldatei an den Index zu senden: `application_logs`

```
awscurl --service osis --region us-east-1 \
    -X POST \
    -H "Content-Type: application/json" \
    -d
 '[{"time":"2014-08-11T11:40:13+00:00","remote_addr":"122.226.223.69","status":"404","request":
 http://www.k2proxy.com//hello.html HTTP/1.1","http_user_agent":"Mozilla/4.0
 (compatible; WOW64; SLCC2;)"}]' \
    https://{pipeline-endpoint}.us-east-1.osis.amazonaws.com/log-pipeline/
test_ingestion_path
```

Sie sollten eine `200 OK` Antwort sehen. Wenn Sie einen Authentifizierungsfehler erhalten, liegt das möglicherweise daran, dass Sie Daten von einem anderen Konto als dem der Pipeline aufnehmen. Siehe the section called “Behebung von Problemen mit Berechtigungen”.

Fragen Sie nun den `application_logs` Index ab, um sicherzustellen, dass Ihr Protokolleintrag erfolgreich aufgenommen wurde:

```
awscurl --service es --region us-east-1 \
     -X GET \
     https://search-{ingestion-domain}.us-east-1.es.amazonaws.com/application_logs/
_search | json_pp
```

Beispielantwort:

```
{
   "took":984,
```

```
   "timed_out":false,
   "_shards":{
      "total":1,
      "successful":5,
      "skipped":0,
      "failed":0
   },
   "hits":{
      "total":{
         "value":1,
         "relation":"eq"
      },
      "max_score":1.0,
      "hits":[
         {
            "_index":"application_logs",
            "_type":"_doc",
            "_id":"z6VY_IMBRpceX-DU6V4O",
            "_score":1.0,
            "_source":{
               "time":"2014-08-11T11:40:13+00:00",
               "remote_addr":"122.226.223.69",
               "status":"404",
               "request":"GET http://www.k2proxy.com//hello.html HTTP/1.1",
               "http_user_agent":"Mozilla/4.0 (compatible; WOW64; SLCC2;)",
               "@timestamp":"2022-10-21T21:00:25.502Z"
            }
         }
      ]
   }
}
```


Behebung von Problemen mit Berechtigungen

Wenn Sie die Schritte im Tutorial befolgt haben und immer noch Authentifizierungsfehler auftreten, wenn Sie versuchen, Daten aufzunehmen, liegt das möglicherweise daran, dass sich die Rolle, die in eine Pipeline schreibt, in einer anderen Rolle befindet AWS-Konto als die Pipeline selbst. In diesem Fall müssen Sie eine Rolle erstellen und übernehmen, die Ihnen speziell das Ingestieren von Daten ermöglicht. Anweisungen finden Sie unter the section called “Bereitstellung von kontenübergreifendem Zugriff auf Datenerfassung”.

Zugehörige Ressourcen

In diesem Tutorial wurde ein einfacher Anwendungsfall für die Aufnahme eines einzelnen Dokuments über HTTP vorgestellt. In Produktionsszenarien konfigurieren Sie Ihre Client-Anwendungen (wie Fluent Bit, Kubernetes oder OpenTelemetry Collector) so, dass Daten an eine oder mehrere Pipelines gesendet werden. Ihre Pipelines werden wahrscheinlich komplexer sein als das einfache Beispiel in diesem Tutorial.

Informationen zu den ersten Schritten zur Konfiguration Ihrer Clients und zur Datenaufnahme finden Sie in den folgenden Ressourcen:

- Pipelines erstellen und verwalten
- Konfiguration Ihrer Clients für das Senden von Daten an Ingestion OpenSearch
- Data Prepper-Dokumentation

Tutorial: Erfassen von Daten in eine Sammlung mithilfe von Amazon OpenSearch Ingestion

In diesem Tutorial erfahren Sie, wie Sie mit Amazon OpenSearch Ingestion eine einfache Pipeline konfigurieren und Daten in eine Amazon OpenSearch -Serverless-Sammlung aufnehmen. Eine Pipeline ist eine Ressource, die OpenSearch Ingestion bereitstellt und verwaltet. Sie können eine Pipeline verwenden, um Daten für nachgelagerte Analysen und Visualisierungen in OpenSearch Service zu filtern, zu anreichern, zu transformieren, zu normalisieren und zu aggregieren.

Ein Tutorial, das zeigt, wie Daten in eine bereitgestellte OpenSearch Service-Domain aufgenommen werden, finden Sie unter the section called “Tutorial: Daten in eine Domain aufnehmen”.

In diesem Tutorial führen Sie die folgenden Schritte durch:

1. Erstellen Sie die Pipeline-Rolle .
2. Erstellen Sie eine Sammlung.
3. Erstellen Sie eine Pipeline .
4. Nehmen Sie einige Beispieldaten auf.

Im Tutorial erstellen Sie die folgenden Ressourcen:

- Eine Pipeline mit dem Namen `ingestion-pipeline-serverless`

- Eine Sammlung mit dem Namen `ingestion-collection` , in die die Pipeline schreibt
- Eine IAM-Rolle mit dem Namen `PipelineRole` , die die Pipeline übernimmt, um in die Sammlung zu schreiben

Erforderliche Berechtigungen

Um dieses Tutorial abzuschließen, müssen Sie über die richtigen IAM-Berechtigungen verfügen. Ihr Benutzer oder Ihre Rolle muss über eine angefügte identitätsbasierte Richtlinie mit den folgenden Mindestberechtigungen verfügen. Mit diesen Berechtigungen können Sie eine Pipeline-Rolle erstellen (`iam:Create*`), eine Sammlung erstellen oder ändern (`aoss:*`) und mit Pipelines arbeiten (`osis:*`).

Darüber hinaus ist die -`iam:PassRole`Berechtigung für die Pipeline-Rollenressource erforderlich. Mit dieser Berechtigung können Sie die Pipeline-Rolle an OpenSearch Ingestion übergeben, damit sie Daten in die Sammlung schreiben kann.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Resource":"*",
         "Action":[
            "osis:*",
            "iam:Create*",
            "aoss:*"
         ]
      },
      {
         "Resource":[
            "arn:aws:iam::{your-account-id}:role/PipelineRole"
         ],
         "Effect":"Allow",
         "Action":[
            "iam:PassRole"
         ]
      }
   ]
}
```

Schritt 1: Erstellen der Pipeline-Rolle

Erstellen Sie zunächst eine Rolle, die die Pipeline übernimmt, um auf die OpenSearch Serverless-Sammlungssenke zuzugreifen. Sie nehmen diese Rolle später in die Pipeline-Konfiguration auf.

So erstellen Sie die Pipeline-Rolle

1. Öffnen Sie die -AWS Identity and Access ManagementKonsole unter https://console.aws.amazon.com/iamv2/.
2. Wählen Sie Richtlinien und dann Richtlinie erstellen aus.
3. Wählen Sie JSON und fügen Sie die folgende Richtlinie in den Editor ein.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "aoss:BatchGetCollection",
        "aoss:APIAccessAll"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:aoss:{region}:{your-account-id}:collection/{collection-
id}"
    },
    {
      "Action": [
        "aoss:CreateSecurityPolicy",
        "aoss:GetSecurityPolicy",
        "aoss:UpdateSecurityPolicy"
      ],
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aoss:collection": "{collection-name}"
        }
      }
    }
  ]
}
```

4. Wählen Sie Weiter, wählen Sie Weiter und benennen Sie Ihre Richtlinie collection-pipeline-policy.

5. Wählen Sie Richtlinie erstellen aus.
6. Erstellen Sie als Nächstes eine Rolle und fügen Sie ihr die Richtlinie an. Wählen Sie Roles (Rollen) und anschließend Create role (Rolle erstellen).
7. Wählen Sie Benutzerdefinierte Vertrauensrichtlinie und fügen Sie die folgende Richtlinie in den Editor ein:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"osis-pipelines.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

8. Wählen Sie Weiter aus. Suchen Sie dann nach collection-pipeline-policy (die Sie gerade erstellt haben) und wählen Sie sie aus.
9. Wählen Sie Weiter und benennen Sie die Rolle PipelineRole.
10. Wählen Sie Rolle erstellen aus.

Denken Sie an den Amazon-Ressourcennamen (ARN) der Rolle (z. B. `arn:aws:iam::{your-account-id}:role/PipelineRole`). Sie benötigen ihn, wenn Sie Ihre Pipeline erstellen.

Schritt 2: Erstellen einer Sammlung

Erstellen Sie als Nächstes eine Sammlung, in die Daten aufgenommen werden sollen. Wir benennen die Sammlung `ingestion-collection`.

1. Navigieren Sie zur Amazon- OpenSearch Service-Konsole unter https://console.aws.amazon.com/aos/home.
2. Wählen Sie in der linken Navigation Sammlungen und dann Sammlung erstellen aus.
3. Benennen Sie die Sammlungsaufnahme-Sammlung .
4. Ändern Sie unter Netzwerkzugriffseinstellungen den Zugriffstyp in Öffentlich.

5. Behalten Sie alle anderen Einstellungen als Standardwerte bei und wählen Sie Next (Weiter) aus.
6. Wählen Sie für Definitionsmethode die Option JSON aus und fügen Sie die folgende Richtlinie in den Editor ein. Diese Richtlinie führt zwei Dinge aus:

   - Ermöglicht der Pipeline-Rolle, in die Sammlung zu schreiben.
   - Ermöglicht Ihnen das Lesen aus der Sammlung. Später, nachdem Sie einige Beispieldaten in die Pipeline aufgenommen haben, fragen Sie die Sammlung ab, um sicherzustellen, dass die Daten erfolgreich aufgenommen und in den Index geschrieben wurden.

   ```
   [
     {
       "Rules": [
         {
           "Resource": [
             "index/ingestion-collection/*"
           ],
           "Permission": [
             "aoss:CreateIndex",
             "aoss:UpdateIndex",
             "aoss:DescribeIndex",
             "aoss:ReadDocument",
             "aoss:WriteDocument"
           ],
           "ResourceType": "index"
         }
       ],
       "Principal": [
         "arn:aws:iam::{your-account-id}:role/PipelineRole",
         "arn:aws:iam::{your-account-id}:role/Admin"
       ],
       "Description": "Rule 1"
     }
   ]
   ```

7. Ersetzen Sie die `Principal` Elemente. Der erste Prinzipal sollte die Pipeline-Rolle angeben, die Sie erstellt haben. Die zweite sollte einen Benutzer oder eine Rolle angeben, mit der Sie die Sammlung später abfragen können.
8. Wählen Sie Weiter aus. Benennen Sie die Zugriffsrichtlinie pipeline-domain-access und wählen Sie erneut Weiter aus.

9. Überprüfen Sie Ihre Sammlungskonfiguration und wählen Sie Submit (Senden) aus.

Wenn die Sammlung aktiv ist, notieren Sie sich den OpenSearch Endpunkt unter Endpunkt (z. B. `https://{collection-id}.us-east-1.aoss.amazonaws.com`). Sie benötigen ihn, wenn Sie Ihre Pipeline erstellen.

Schritt 3: Erstellen einer Pipeline

Nachdem Sie nun eine Sammlung und eine Rolle mit den entsprechenden Zugriffsrechten haben, können Sie eine Pipeline erstellen.

So erstellen Sie eine Pipeline

1. Wählen Sie in der Amazon- OpenSearch Service-Konsole im linken Navigationsbereich Pipelines aus.
2. Wählen Sie Create pipeline (Pipeline erstellen) aus.
3. Benennen Sie die Pipeline Serverless-Inestion und behalten Sie die Kapazitätseinstellungen als Standardwerte bei.
4. In diesem Tutorial erstellen wir eine einfache Unterpipeline namens `log-pipeline`, die das HTTP-Quell-Plugin verwendet. Das Plugin akzeptiert Protokolldaten in einem JSON-Array-Format. Wir geben eine einzelne OpenSearch Serverless-Sammlung als Senke an und nehmen alle Daten in den `my_logs` Index auf.

   Fügen Sie unter Pipeline-Konfiguration die folgende YAML-Konfiguration in den Editor ein:

```
version: "2"
log-pipeline:
  source:
    http:
      path: "/${pipelineName}/test_ingestion_path"
  processor:
    - date:
        from_time_received: true
        destination: "@timestamp"
  sink:
    - opensearch:
        hosts: [ "https://{collection-id}.us-east-1.aoss.amazonaws.com" ]
        index: "my_logs"
        aws:
          sts_role_arn: "arn:aws:iam::{your-account-id}:role/PipelineRole"
```

```
        region: "us-east-1"
        serverless: true
```

5. Ersetzen Sie die `hosts` URL durch den Endpunkt der Sammlung, die Sie im vorherigen Abschnitt erstellt haben. Ersetzen Sie den `sts_role_arn` Parameter durch den ARN von `PipelineRole`. Ändern Sie optional die `region`.
6. Wählen Sie Pipeline validieren und stellen Sie sicher, dass die Validierung erfolgreich ist.
7. Der Einfachheit halber konfigurieren wir in diesem Tutorial den öffentlichen Zugriff für die Pipeline. Wählen Sie unter Netzwerk die Option Öffentlicher Zugriff aus.

   Informationen zum Konfigurieren des VPC-Zugriffs finden Sie unter the section called “Konfiguration des VPC-Zugriffs für Pipelines”.
8. Lassen Sie die Protokollveröffentlichung aktiviert, falls Sie während des Abschlusses dieses Tutorials auf Probleme stoßen. Weitere Informationen finden Sie unter the section called “Überwachen der Pipeline-Protokolle”.

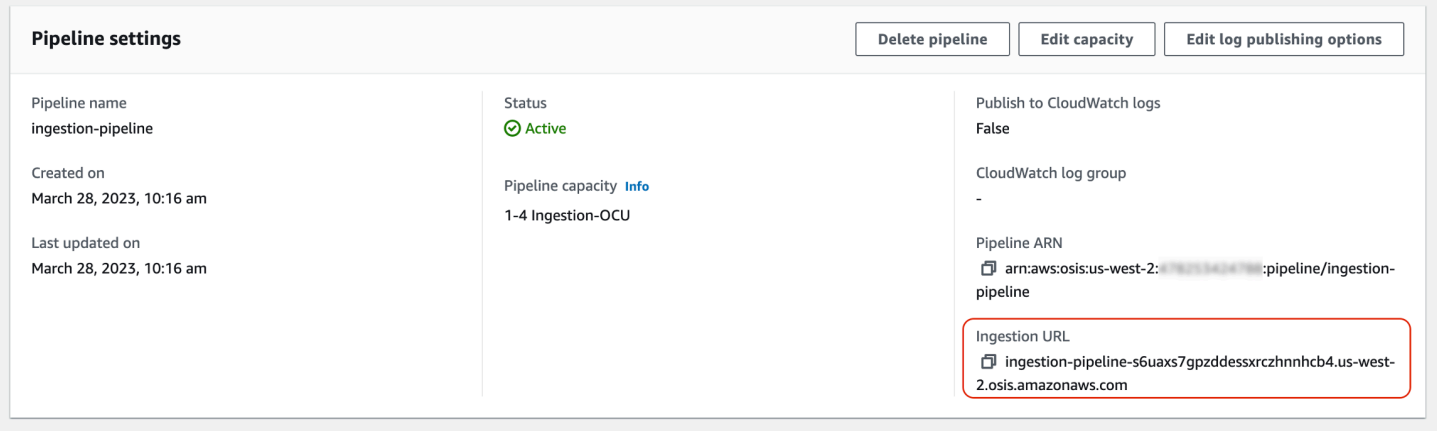
   Geben Sie den folgenden Protokollgruppennamen an: `/aws/vendedlogs/OpenSearchIngestion/serverless-ingestion/audit-logs`
9. Wählen Sie Weiter aus. Überprüfen Sie Ihre Pipeline-Konfiguration und wählen Sie Pipeline erstellen aus. Es dauert 5–10 Minuten, bis die Pipeline aktiv wird.

Schritt 4: Erfassen einiger Beispieldaten

Wenn der Pipeline-Status lautet`Active`, können Sie mit der Aufnahme von Daten beginnen. Sie müssen alle HTTP-Anfragen an die Pipeline mit Signature Version 4 signieren. Verwenden Sie ein HTTP-Tool wie Postman oder awscurl, um einige Daten an die Pipeline zu senden. Wie bei der direkten Indizierung von Daten in einer Sammlung erfordert die Aufnahme von Daten in eine Pipeline immer entweder eine IAM-Rolle oder einen IAM-Zugriffsschlüssel und einen geheimen Schlüssel .

> **Note**
>
> Der Prinzipal, der die Anforderung signiert, muss über die `osis:Ingest` IAM-Berechtigung verfügen.

Rufen Sie zunächst die Aufnahme-URL von der Seite Pipeline-Einstellungen ab:



Nehmen Sie dann einige Beispieldaten auf. Die folgende Beispielanforderung verwendet awscurl, um eine einzelne Protokolldatei an den `my_logs` Index zu senden:

```
awscurl --service osis --region us-east-1 \
    -X POST \
    -H "Content-Type: application/json" \
    -d
 '[{"time":"2014-08-11T11:40:13+00:00","remote_addr":"122.226.223.69","status":"404","request":
 http://www.k2proxy.com//hello.html HTTP/1.1","http_user_agent":"Mozilla/4.0
 (compatible; WOW64; SLCC2;)"}]' \
    https://{pipeline-endpoint}.us-east-1.osis.amazonaws.com/log-pipeline/
test_ingestion_path
```

Sie sollten eine `200 OK` Antwort sehen.

Fragen Sie nun den `my_logs` Index ab, um sicherzustellen, dass der Protokolleintrag erfolgreich aufgenommen wurde:

```
awscurl --service aoss --region us-east-1 \
     -X GET \
     https://{collection-id}.us-east-1.aoss.amazonaws.com/my_logs/_search | json_pp
```

Beispielantwort:

```
{
   "took":348,
   "timed_out":false,
   "_shards":{
      "total":0,
```

```
      "successful":0,
      "skipped":0,
      "failed":0
   },
   "hits":{
      "total":{
         "value":1,
         "relation":"eq"
      },
      "max_score":1.0,
      "hits":[
         {
            "_index":"my_logs",
            "_id":"1%3A0%3ARJgDvIcBTy5m12xrKE-y",
            "_score":1.0,
            "_source":{
               "time":"2014-08-11T11:40:13+00:00",
               "remote_addr":"122.226.223.69",
               "status":"404",
               "request":"GET http://www.k2proxy.com//hello.html HTTP/1.1",
               "http_user_agent":"Mozilla/4.0 (compatible; WOW64; SLCC2;)",
               "@timestamp":"2023-04-26T05:22:16.204Z"
            }
         }
      ]
   }
}
```


Zugehörige Ressourcen

In diesem Tutorial wurde ein einfacher Anwendungsfall für die Aufnahme eines einzelnen Dokuments über HTTP vorgestellt. In Produktionsszenarien konfigurieren Sie Ihre Clientanwendungen (wie Fluent Bit, Kubernetes oder OpenTelemetry Collector), um Daten an eine oder mehrere Pipelines zu senden. Ihre Pipelines werden wahrscheinlich komplexer sein als das einfache Beispiel in diesem Tutorial.

Informationen zu den ersten Schritten mit der Konfiguration Ihrer Clients und der Erfassung von Daten finden Sie in den folgenden Ressourcen:

- Erstellen und Verwalten von Pipelines
- Konfigurieren Ihrer Clients zum Senden von Daten an OpenSearch Ingestion
- Dokumentation zu Data Prepper

Überblick über die Pipeline-Funktionen in Amazon OpenSearch Ingestion

Amazon OpenSearch Ingestion stellt Pipelines bereit, die aus einer Quelle, einem Puffer, null oder mehr Prozessoren und einer oder mehreren Senken bestehen. Ingestion-Pipelines werden von Data Prepper als Daten-Engine unterstützt. Einen Überblick über die verschiedenen Komponenten einer Pipeline finden Sie unter. the section called “Die wichtigsten Konzepte”

Die folgenden Abschnitte bieten einen Überblick über einige der am häufigsten verwendeten Funktionen in Amazon OpenSearch Ingestion.

> **Note**
>
> Dies ist keine vollständige Liste der Funktionen, die für Pipelines verfügbar sind. Eine umfassende Dokumentation aller verfügbaren Pipeline-Funktionen finden Sie in der Data Prepper-Dokumentation. Beachten Sie, dass OpenSearch Ingestion einige Einschränkungen hinsichtlich der Plugins und Optionen auferlegt, die Sie verwenden können. Weitere Informationen finden Sie unter the section called “Unterstützte Plugins und Optionen”.

Themen

Dauerhafte Pufferung

Ein persistenter Puffer speichert Ihre Daten in einem festplattenbasierten Puffer über mehrere Availability Zones hinweg, um die Haltbarkeit Ihrer Daten zu erhöhen. Mithilfe der persistenten Pufferung können Sie Daten für alle unterstützten Push-basierten Quellen aufnehmen, ohne einen

eigenständigen Puffer einrichten zu müssen. Dazu gehören HTTP und OpenTelemetry Quellen für Protokolle, Traces und Metriken.

Um die persistente Pufferung zu aktivieren, wählen Sie beim Erstellen oder Aktualisieren einer Pipeline die Option Persistenten Puffer aktivieren aus. Weitere Informationen finden Sie unterthe section called “Pipelines erstellen”. OpenSearch Die Aufnahme bestimmt automatisch die erforderliche Pufferkapazität auf der Grundlage der OpenSearch Ingestion-Recheneinheiten (Ingestion-OCUs), die Sie für die Pipeline angeben.

Standardmäßig verwenden Pipelines eine, um Pufferdaten zu verschlüsseln. AWS-eigener Schlüssel Diese Pipelines benötigen keine zusätzlichen Berechtigungen für die Pipeline-Rolle. Alternativ können Sie einen vom Kunden verwalteten Schlüssel angeben und der Pipeline-Rolle die folgenden IAM-Berechtigungen hinzufügen:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "KeyAccess",
            "Effect": "Allow",
            "Action": [
              "kms:Decrypt",
              "kms:GenerateDataKeyWithoutPlaintext"
            ],
            "Resource": "arn:aws:kms:{region}:{aws-account-
id}:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ]
}
```

Weitere Informationen finden Sie unter Kundenverwaltete Schlüssel im AWS Key Management Service Entwicklerhandbuch.

> **Note**
>
> Wenn Sie die persistente Pufferung deaktivieren, wird Ihre Pipeline so aktualisiert, dass sie vollständig mit speicherinterner Pufferung läuft.

Optimierung der maximalen Payload-Größe für Anfragen

Wenn Sie die persistente Pufferung für eine Pipeline aktivieren, beträgt die maximale Größe der Anforderungsnutzlast standardmäßig 1 MB. Der Standardwert bietet die beste Leistung. Sie können diesen Wert jedoch erhöhen, wenn Ihre Kunden Anfragen senden, die 1 MB überschreiten. Um die maximale Nutzlastgröße einzustellen, legen Sie die `max_request_length` Option in der Quellkonfiguration fest. Genau wie die persistente Pufferung wird diese Option nur für HTTP und OpenTelemetry Quellen für Protokolle, Traces und Metriken unterstützt.

Die einzigen gültigen Werte für `max_request_length` diese Option sind 1 MB, 1,5 MB, 2 MB, 2,5 MB, 3 MB, 3,5 MB und 4 MB. Wenn Sie einen anderen Wert angeben, erhalten Sie eine Fehlermeldung.

Das folgende Beispiel zeigt, wie die maximale Nutzlastgröße innerhalb einer Pipeline-Konfiguration konfiguriert wird:

```
...
log-pipeline:
  source:
    http:
      path: "/${pipelineName}/logs"
      max_request_length: 4mb
  processor:
...
```

Wenn Sie die persistente Pufferung für eine Pipeline nicht aktivieren, ist der Wert der `max_request_length` Option standardmäßig für alle Quellen auf 10 MB voreingestellt und kann nicht geändert werden.

Aufteilen

Sie können eine OpenSearch Ingestion-Pipeline so konfigurieren, dass eingehende Ereignisse in eine Unterpipeline aufgeteilt werden, sodass Sie verschiedene Arten der Verarbeitung desselben eingehenden Ereignisses durchführen können.

Die folgende Beispielpipeline teilt eingehende Ereignisse in zwei Unter-Pipelines auf. Jede Unterpipeline verwendet ihren eigenen Prozessor, um die Daten anzureichern und zu bearbeiten, und sendet die Daten dann an verschiedene Indizes. OpenSearch

```
version: "2"
```

```
log-pipeline:
  source:
    http:
    ...
  sink:
    - pipeline:
        name: "logs_enriched_one_pipeline"
    - pipeline:
        name: "logs_enriched_two_pipeline"

logs_enriched_one_pipeline:
  source:
    log-pipeline
  processor:
   ...
  sink:
    - opensearch:
        # Provide a domain or collection endpoint
        # Enable the 'serverless' flag if the sink is an OpenSearch Serverless
 collection
        aws:
          ...
        index: "enriched_one_logs"

logs_enriched_two_pipeline:
  source:
    log-pipeline
  processor:
   ...
  sink:
    - opensearch:
        # Provide a domain or collection endpoint
        # Enable the 'serverless' flag if the sink is an OpenSearch Serverless
 collection
        aws:
          ...
          index: "enriched_two_logs"
```

Verkettung

Sie können mehrere Sub-Pipelines miteinander verketten, um die Datenverarbeitung und -anreicherung in Abschnitten durchzuführen. Mit anderen Worten, Sie können ein eingehendes Ereignis mit bestimmten Verarbeitungsfunktionen in einer Subpipeline anreichern, es dann zur

weiteren Anreicherung mit einem anderen Prozessor an eine andere Subpipeline senden und es schließlich an dessen Senke senden. OpenSearch

Im folgenden Beispiel reichert die `log_pipeline` Subpipeline ein eingehendes Protokollereignis mit einer Reihe von Prozessoren an und sendet das Ereignis dann an einen Index mit dem Namen. OpenSearch `enriched_logs` Die Pipeline sendet dasselbe Ereignis an die `log_advanced_pipeline` Subpipeline, die es verarbeitet und an einen anderen OpenSearch Index mit dem Namen sendet. `enriched_advanced_logs`

```
version: "2"
log-pipeline:
  source:
    http:
    ...
  processor:
    ...
  sink:
    - opensearch:
        # Provide a domain or collection endpoint
        # Enable the 'serverless' flag if the sink is an OpenSearch Serverless
 collection
        aws:
          ...
          index: "enriched_logs"
    - pipeline:
        name: "log_advanced_pipeline"

log_advanced_pipeline:
  source:
    log-pipeline
  processor:
   ...
  sink:
    - opensearch:
        # Provide a domain or collection endpoint
        # Enable the 'serverless' flag if the sink is an OpenSearch Serverless
 collection
        aws:
          ...
          index: "enriched_advanced_logs"
```

Warteschlangen für unzustellbare Nachrichten

Dead-Letter-Warteschlangen (DLQs) sind Ziele für Ereignisse, bei denen eine Pipeline nicht in eine Senke schreiben kann. In OpenSearch Ingestion müssen Sie einen Amazon S3 S3-Bucket mit entsprechenden Schreibberechtigungen angeben, der als DLQ verwendet werden soll. Sie können jeder Senke innerhalb einer Pipeline eine DLQ-Konfiguration hinzufügen. Wenn eine Pipeline auf Schreibfehler stößt, erstellt sie DLQ-Objekte im konfigurierten S3-Bucket. DLQ-Objekte existieren in einer JSON-Datei als Array von fehlgeschlagenen Ereignissen.

Eine Pipeline schreibt Ereignisse in den DLQ, wenn eine der folgenden Bedingungen erfüllt ist:

- Die `max_retries` für die OpenSearch Spüle benötigte Menge ist aufgebraucht. OpenSearch Für diese Option sind mindestens 16 für die Einnahme erforderlich.
- Ereignisse werden aufgrund eines Fehlers von der Senke zurückgewiesen.

Konfiguration

Um eine Warteschlange mit unerlaubten Briefen für eine Subpipeline zu konfigurieren, geben Sie die `dlq` Option in der `opensearch` Senkenkonfiguration an:

```
apache-log-pipeline:
  ...
  sink:
    opensearch:
      dlq:
        s3:
          bucket: "my-dlq-bucket"
          key_path_prefix: "dlq-files"
          region: "us-west-2"
          sts_role_arn: "arn:aws:iam::123456789012:role/dlq-role"
```

Dateien, die in diesen S3-DLQ geschrieben werden, haben das folgende Benennungsmuster:

```
dlq-v${version}-${pipelineName}-${pluginId}-${timestampIso8601}-${uniqueId}
```

Weitere Informationen finden Sie unter Dead-Letter-Warteschlangen (DLQ).

Anweisungen zur Konfiguration der Rolle finden Sie unter`sts_role_arn`. the section called “Schreiben in eine Warteschleife mit unzustellbaren Briefen”

Beispiel

Betrachten Sie die folgende Beispiel-DLQ-Datei:

```
dlq-v2-apache-log-pipeline-opensearch-2023-04-05T15:26:19.152938Z-e7eb675a-
f558-4048-8566-dac15a4f8343
```

Hier ist ein Beispiel für Daten, die nicht in die Senke geschrieben werden konnten und die zur weiteren Analyse an den DLQ S3-Bucket gesendet werden:

```
Record_0
pluginId            "opensearch"
pluginName          "opensearch"
pipelineName        "apache-log-pipeline"
failedData
index    "logs"
indexId   null
status    0
message  "Number of retries reached the limit of max retries (configured value 15)"
document
log      "sample log"
timestamp     "2023-04-14T10:36:01.070Z"

Record_1
pluginId            "opensearch"
pluginName          "opensearch"
pipelineName        "apache-log-pipeline"
failedData
index               "logs"
indexId   null
status    0
message  "Number of retries reached the limit of max retries (configured value 15)"
document
log                 "another sample log"
timestamp           "2023-04-14T10:36:01.071Z"
```

Indexverwaltung

Amazon OpenSearch Ingestion bietet viele Funktionen zur Indexverwaltung, darunter die folgenden.

Erstellen von Indizes

Sie können einen Indexnamen in einer Pipeline-Senke angeben, und OpenSearch Ingestion erstellt den Index, wenn die Pipeline bereitgestellt wird. Wenn bereits ein Index vorhanden ist, verwendet die Pipeline ihn, um eingehende Ereignisse zu indizieren. Wenn Sie eine Pipeline beenden und neu starten oder wenn Sie ihre YAML-Konfiguration aktualisieren, versucht die Pipeline, neue Indizes zu erstellen, sofern diese noch nicht vorhanden sind. Eine Pipeline kann niemals einen Index löschen.

Die folgenden Beispielsenken erstellen zwei Indizes, wenn die Pipeline bereitgestellt wird:

```
sink:
  - opensearch:
      index: apache_logs
  - opensearch:
      index: nginx_logs
```

Generieren von Indexnamen und -mustern

Sie können dynamische Indexnamen generieren, indem Sie Variablen aus den Feldern eingehender Ereignisse verwenden. Verwenden Sie in der Senkenkonfiguration das Format, `string${}` um die Interpolation von Zeichenketten zu signalisieren, und verwenden Sie einen JSON-Zeiger, um Felder aus Ereignissen zu extrahieren. Die Optionen für `index_type` sind `custom` oder. `management_disabled` Da die `index_type` Standardeinstellung `custom` für OpenSearch Domänen und `management_disabled` für OpenSearch serverlose Sammlungen ist, kann sie nicht konfiguriert werden.

Die folgende Pipeline wählt beispielsweise das `metadataType` Feld aus eingehenden Ereignissen aus, um Indexnamen zu generieren.

```
pipeline:
  ...
  sink:
    opensearch:
      index: "metadata-${metadataType}"
```

Die folgende Konfiguration generiert weiterhin jeden Tag oder jede Stunde einen neuen Index.

```
pipeline:
  ...
  sink:
```

```
    opensearch:
      index: "metadata-${metadataType}-%{yyyy.MM.dd}"

pipeline:
  ...
  sink:
    opensearch:
      index: "metadata-${metadataType}-%{yyyy.MM.dd.HH}"
```

Der Indexname kann auch eine einfache Zeichenfolge mit einem Datums-/Uhrzeitmuster als Suffix sein, z. B. `my-index-%{yyyy.MM.dd}` Wenn die Senke Daten an sendet OpenSearch, ersetzt sie das Datums-/Uhrzeitmuster durch die UTC-Zeit und erstellt für jeden Tag einen neuen Index, z. B. `my-index-2022.01.25` Weitere Informationen finden Sie in der DateTimeFormatterKlasse.

Dieser Indexname kann auch eine formatierte Zeichenfolge sein (mit oder ohne ein Datums-/Uhrzeit-Mustersuffix), z. B. `my-${index}-name` Wenn die Senke Daten an sendet OpenSearch, ersetzt sie den `"${index}"` Teil durch den Wert in dem Ereignis, das gerade verarbeitet wird. Wenn das Format `"${index1/index2/index3}"` zutrifft, ersetzt es das Feld `index1/index2/index3` durch seinen Wert im Ereignis.

Dokument-IDs werden generiert

Eine Pipeline kann beim Indizieren von Dokumenten eine Dokument-ID generieren. OpenSearch Sie kann diese Dokument-IDs aus den Feldern in eingehenden Ereignissen ableiten.

In diesem Beispiel wird das `uuid` Feld aus einem eingehenden Ereignis verwendet, um eine Dokument-ID zu generieren.

```
pipeline:
  ...
  sink:
    opensearch:
      index_type: custom
      index: "metadata-${metadataType}-%{yyyy.MM.dd}"
      document_id_field: "uuid"
```

Im folgenden Beispiel führt der Prozessor „Einträge hinzufügen“ die Felder `uuid` `other_field` aus dem eingehenden Ereignis zusammen, um eine Dokument-ID zu generieren.

Die `create` Aktion stellt sicher, dass Dokumente mit identischen IDs nicht überschrieben werden. Die Pipeline löscht doppelte Dokumente, ohne dass ein erneuter Versuch oder ein DLQ-Ereignis

erforderlich ist. Dies ist für Pipeline-Autoren, die diese Aktion verwenden, durchaus zu erwarten, da das Ziel darin besteht, die Aktualisierung vorhandener Dokumente zu vermeiden.

```
pipeline:
  ...
  processor:
   - add_entries:
      entries:
        - key: "my_doc_id_field"
          format: "${uuid}-${other_field}"
  sink:
    - opensearch:
       ...
       action: "create"
       document_id_field: "my_doc_id_field"
```

Möglicherweise möchten Sie die Dokument-ID eines Ereignisses auf ein Feld aus einem Unterobjekt festlegen. Im folgenden Beispiel verwendet das OpenSearch Sink-Plug-In das Unterobjekt, um eine Dokument-ID `info/id` zu generieren.

```
sink:
  - opensearch:
       ...
       document_id_field: info/id
```

Bei dem folgenden Ereignis generiert die Pipeline ein Dokument, bei dem das `_id` Feld wie folgt gesetzt `json001` ist:

```
{
   "fieldA":"arbitrary value",
   "info":{
      "id":"json001",
      "fieldA":"xyz",
      "fieldB":"def"
   }
}
```

Routing-IDs werden generiert

Sie können die `routing_field` Option innerhalb des OpenSearch Sink-Plug-ins verwenden, um den Wert einer Dokument-Routing-Eigenschaft (`_routing`) auf einen Wert aus einem eingehenden Ereignis festzulegen.

Routing unterstützt die JSON-Zeigersyntax, sodass auch verschachtelte Felder verfügbar sind, nicht nur Felder der obersten Ebene.

```
sink:
  - opensearch:
        ...
        routing_field: metadata/id
        document_id_field: id
```

Bei dem folgenden Ereignis generiert das Plugin ein Dokument, bei dem das `_routing` Feld auf gesetzt ist: `abcd`

```
{
   "id":"123",
   "metadata":{
      "id":"abcd",
      "fieldA":"valueA"
   },
   "fieldB":"valueB"
}
```

Anweisungen zum Erstellen von Indexvorlagen, die Pipelines bei der Indexerstellung verwenden können, finden Sie unter Indexvorlagen.

E-Bestätigung nd-to-end

OpenSearch Die Datenaufnahme gewährleistet die Haltbarkeit und Zuverlässigkeit von Daten, indem deren Übertragung von der Quelle bis zu den Senken in zustandslosen Pipelines mithilfe von Quittierung nachverfolgt wird. end-to-end Derzeit unterstützt nur das S3-Quell-Plugin die Bestätigung. end-to-end

Bei der end-to-end Bestätigung erstellt das Pipeline-Quell-Plugin einen Bestätigungssatz zur Überwachung einer Reihe von Ereignissen. Es erhält eine positive Bestätigung, wenn diese

Ereignisse erfolgreich an ihre Senken gesendet wurden, oder eine negative Bestätigung, wenn eines der Ereignisse nicht an ihre Senken gesendet werden konnte.

Im Falle eines Fehlers oder Absturzes einer Pipeline-Komponente oder wenn eine Quelle keine Bestätigung erhält, läuft die Quelle ab und ergreift die erforderlichen Maßnahmen, wie z. B. einen erneuten Versuch oder die Protokollierung des Fehlers. Wenn für die Pipeline mehrere Senken oder mehrere Sub-Pipelines konfiguriert sind, werden Bestätigungen auf Ereignisebene erst gesendet, nachdem das Ereignis an alle Senken in allen Unter-Pipelines gesendet wurde. Wenn für eine Senke ein DLQ konfiguriert ist, verfolgt die Bestätigungsfunktion auch Ereignisse, die in den DLQ geschrieben wurden. end-to-end

Um die end-to-end Bestätigung zu aktivieren, fügen Sie die Option in die `acknowledgments` Quellkonfiguration ein:

```
s3-pipeline:
  source:
    s3:
      acknowledgments: true
...
```

Gegendruck an der Quelle

In einer Pipeline kann es zu Gegendruck kommen, wenn sie mit der Verarbeitung von Daten beschäftigt ist oder wenn ihre Senken vorübergehend ausgefallen sind oder nur langsam Daten aufnehmen. OpenSearch Je nachdem, welches Quell-Plugin eine Pipeline verwendet, gibt es bei der Datenaufnahme unterschiedliche Methoden, mit Gegendruck umzugehen.

HTTP-Quelle

Pipelines, die das HTTP-Quell-Plugin verwenden, behandeln Gegendruck unterschiedlich, je nachdem, welche Pipeline-Komponente überlastet ist:

- Puffer — Wenn die Puffer voll sind, gibt die Pipeline den HTTP-Status `REQUEST_TIMEOUT` mit dem Fehlercode 408 zurück zum Quellendpunkt. Sobald Puffer freigegeben werden, beginnt die Pipeline erneut mit der Verarbeitung von HTTP-Ereignissen.
- Quell-Threads — Wenn alle HTTP-Quell-Threads mit der Ausführung von Anfragen beschäftigt sind und die Größe der Warteschlange für unbearbeitete Anfragen die maximal zulässige Anzahl von Anfragen überschritten hat, gibt die Pipeline den HTTP-Status `TOO_MANY_REQUESTS` mit dem Fehlercode 429 zurück an den Quellendpunkt. Wenn die Anforderungswarteschlange die maximal

zulässige Warteschlangengröße unterschreitet, beginnt die Pipeline erneut mit der Verarbeitung der Anfragen.

Die Quelle

Wenn die Puffer für Pipelines, die OpenTelemetry Quellen verwenden (OTel-Logs, oTel-Metriken und oTel-Trace), voll sind, beginnt die Pipeline, den HTTP-Status `REQUEST_TIMEOUT` mit dem Fehlercode 408 an den Quellendpunkt zurückzugeben. Sobald Puffer freigegeben werden, beginnt die Pipeline erneut mit der Verarbeitung von Ereignissen.

S3-Quelle

Wenn die Puffer für Pipelines mit einer S3-Quelle voll sind, beenden die Pipelines die Verarbeitung von SQS-Benachrichtigungen. Sobald die Puffer freigegeben sind, beginnen die Pipelines wieder mit der Verarbeitung von Benachrichtigungen.

Wenn eine Senke ausgefallen ist oder keine Daten aufnehmen kann und die end-to-end Bestätigung für die Quelle aktiviert ist, stoppt die Pipeline die Verarbeitung von SQS-Benachrichtigungen, bis sie eine erfolgreiche Bestätigung von allen Senken erhält.

Amazon OpenSearch Ingestion-Pipelines erstellen

Eine Pipeline ist der Mechanismus, den Amazon OpenSearch Ingestion verwendet, um Daten von ihrer Quelle (wo die Daten herkommen) zu ihrer Senke (wo die Daten hingehen) zu verschieben. Bei OpenSearch Ingestion wird die Senke immer eine einzelne Amazon OpenSearch Service-Domain sein, während die Quelle Ihrer Daten Clients wie Amazon S3, Fluent Bit oder Collector sein kann. OpenTelemetry

Weitere Informationen finden Sie in der Dokumentation unter Pipelines. OpenSearch

Themen

- Voraussetzungen und erforderliche Rollen
- Erforderliche Berechtigungen
- Angabe der Pipeline-Version
- Angeben des Aufnahmepfads
- Pipelines erstellen
- Den Status der Pipeline-Erstellung verfolgen

- Verwenden von Blueprints zum Erstellen einer Pipeline

Voraussetzungen und erforderliche Rollen

Um eine OpenSearch Ingestion-Pipeline zu erstellen, benötigen Sie die folgenden Ressourcen:

- Eine IAM-Rolle, die OpenSearch Ingestion übernimmt, um in die Senke zu schreiben. Sie werden diesen Rollen-ARN in Ihre Pipeline-Konfiguration aufnehmen.
- Eine OpenSearch Service-Domain oder eine OpenSearch Serverless-Sammlung, die als Senke fungiert. Wenn Sie in eine Domain schreiben, muss sie OpenSearch 1.0 oder höher oder Elasticsearch 7.4 oder höher ausführen. Die Senke muss über eine Zugriffsrichtlinie verfügen, die Ihrer IAM-Pipeline-Rolle die entsprechenden Berechtigungen gewährt.

Anweisungen zum Erstellen dieser Ressourcen finden Sie in den folgenden Themen:

- the section called “Pipelines Zugriff auf Domains gewähren”
- the section called “Pipelines Zugriff auf Sammlungen gewähren”

> **Note**
>
> Wenn Sie in eine Domäne schreiben, die eine differenzierte Zugriffskontrolle verwendet, müssen Sie zusätzliche Schritte ausführen. Siehe the section called “Schritt 3: Ordnen Sie die Pipeline-Rolle zu (nur für Domänen, die eine differenzierte Zugriffskontrolle verwenden)”.

Erforderliche Berechtigungen

OpenSearch Ingestion verwendet die folgenden IAM-Berechtigungen für die Erstellung von Pipelines:

- `osis:CreatePipeline`— Erstellen Sie eine Pipeline.
- `osis:ValidatePipeline`— Prüft, ob eine Pipeline-Konfiguration gültig ist.
- `iam:PassRole`— Übergeben Sie die Pipeline-Rolle an OpenSearch Ingestion, damit diese Daten in die Domain schreiben kann. Diese Berechtigung muss für die Pipeline-Rollenressource (den ARN, den Sie für die `sts_role_arn` Option in der Pipeline-Konfiguration angeben) gelten, oder einfach, `*` wenn Sie in jeder Pipeline unterschiedliche Rollen verwenden möchten.

Die folgende Richtlinie gewährt beispielsweise die Berechtigung zum Erstellen einer Pipeline:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Resource":"*",
         "Action":[
            "osis:CreatePipeline",
            "osis:ListPipelineBlueprints",
            "osis:ValidatePipeline"
         ]
      },
      {
         "Resource":[
            "arn:aws:iam::{your-account-id}:role/{pipeline-role}"
         ],
         "Effect":"Allow",
         "Action":[
            "iam:PassRole"
         ]
      }
   ]
}
```

OpenSearch Die Erfassung umfasst auch eine sogenannte Berechtigung, die erforderlich ist`osis:Ingest`, um signierte Anfragen mithilfe von Signature Version 4 an die Pipeline zu senden. Weitere Informationen finden Sie unter the section called “Eine Aufnahmerolle erstellen”.

> **Note**
>
> Darüber hinaus muss der erste Benutzer, der eine Pipeline in einem Konto erstellt, über Berechtigungen für die `iam:CreateServiceLinkedRole` Aktion verfügen. Weitere Informationen finden Sie unter Pipeline-Rollenressource.

Weitere Informationen zu den einzelnen Berechtigungen finden Sie in der Serviceautorisierungsreferenz unter Aktionen, Ressourcen und OpenSearch Bedingungsschlüssel für die Datenerfassung.

Angabe der Pipeline-Version

Wenn Sie eine Pipeline konfigurieren, müssen Sie die Hauptversion von Data Prepper angeben, die die Pipeline ausführen soll. Um die Version anzugeben, nehmen Sie die `version` Option in Ihre Pipeline-Konfiguration auf:

```
version: "2"
log-pipeline:
  source:
    ...
```

Wenn Sie Create wählen, ermittelt OpenSearch Ingestion die neueste verfügbare Nebenversion der von Ihnen angegebenen Hauptversion und stellt die Pipeline mit dieser Version bereit. Wenn Sie beispielsweise angeben `version: "2"` und die neueste unterstützte Version von Data Prepper 2.1.1 ist, stellt OpenSearch Ingestion Ihrer Pipeline Version 2.1.1 zur Verfügung. Wir zeigen die Nebenversion, die in Ihrer Pipeline läuft, nicht öffentlich an.

Um Ihre Pipeline zu aktualisieren, wenn eine neue Hauptversion von Data Prepper verfügbar ist, bearbeiten Sie die Pipeline-Konfiguration und geben Sie die neue Version an. Sie können eine Pipeline nicht auf eine frühere Version herunterstufen.

> **Note**
>
> OpenSearch Ingestion unterstützt neue Versionen von Data Prepper nicht sofort, sobald sie veröffentlicht werden. Es wird eine gewisse Verzögerung zwischen der Veröffentlichung einer neuen Version und der Unterstützung in Ingestion geben. OpenSearch Darüber hinaus unterstützt OpenSearch Ingestion möglicherweise bestimmte Haupt- oder Nebenversionen ausdrücklich nicht. Eine umfangreiche Liste finden Sie unter the section called “Unterstützte Data Prepper-Versionen”.

Jedes Mal, wenn Sie eine Änderung an Ihrer Pipeline vornehmen, die eine blaue/grüne Bereitstellung initiiert, kann OpenSearch Ingestion sie auf die neueste Nebenversion der Hauptversion aktualisieren, die derzeit in der Pipeline-YAML-Datei konfiguriert ist. Weitere Informationen finden Sie unter. the section called “Blaue/grüne Bereitstellungen für Pipeline-Updates” OpenSearch Durch die Aufnahme kann die Hauptversion Ihrer Pipeline nur geändert werden, wenn Sie die `version` Option in der Pipeline-Konfiguration explizit aktualisieren.

Angeben des Aufnahmepfads

Für pullbasierte Quellen wie OTel Trace und oTEL metrics erfordert OpenSearch Ingestion die zusätzliche `path` Option in Ihrer Quellkonfiguration. Der Pfad ist eine Zeichenfolge wie`/log/ingest`, die den URI-Pfad für die Aufnahme darstellt. Dieser Pfad definiert den URI, den Sie verwenden, um Daten an die Pipeline zu senden.

Nehmen wir beispielsweise an, Sie geben die folgende Subpipeline für einen Eintrag für eine Eingabe-Pipeline mit dem Namen an: `logs`

```
entry-pipeline:
  source:
    http:
      path: "/my/test_path"
```

Wenn Sie Daten in die Pipeline aufnehmen, müssen Sie den folgenden Endpunkt in Ihrer Client-Konfiguration angeben:. `https://logs-abcdefgh.us-west-2.osis.amazonaws.com/my/test_path`

Der Pfad muss mit einem Schrägstrich (/) beginnen und kann die Sonderzeichen '-', '_', 'enthalten . 'und'/'sowie der `${pipelineName}` Platzhalter. Wenn Sie `${pipelineName}` (z. B.`path: "/${pipelineName}/test_path"`) verwenden, wird die Variable durch den Namen der zugehörigen Subpipeline ersetzt. In diesem Beispiel wäre `https://logs.us-west-2.osis.amazonaws.com/entry-pipeline/test_path` es.

Pipelines erstellen

In diesem Abschnitt wird beschrieben, wie Sie OpenSearch Ingestion-Pipelines mithilfe der OpenSearch Servicekonsole und der erstellen. AWS CLI

Konsole

So erstellen Sie eine Pipeline

1. Melden Sie sich bei der Amazon OpenSearch Service-Konsole unter https://console.aws.amazon.com/aos/home an.
2. Wählen Sie im linken Navigationsbereich Pipelines und dann Pipeline erstellen aus.
3. Geben Sie einen Namen für die Pipeline ein.

4. (Optional) Wählen Sie „Persistenten Puffer aktivieren“. Ein persistenter Puffer speichert Ihre Daten in einem festplattenbasierten Puffer für mehrere AZs. Weitere Informationen finden Sie unter Persistent Buffering. Wenn Sie persistenten Puffer aktivieren, wählen Sie den AWS Key Management Service Schlüssel zum Verschlüsseln der Pufferdaten aus.
5. Konfigurieren Sie die minimale und maximale Pipeline-Kapazität in Ingestion OpenSearch Compute Units (OCUs). Weitere Informationen finden Sie unter the section called “Skalierung von Pipelines”.
6. Geben Sie unter Pipeline-Konfiguration Ihre Pipeline-Konfiguration im YAML-Format an. Eine einzelne Pipeline-Konfigurationsdatei kann 1—10 Unter-Pipelines enthalten. Jede Subpipeline ist eine Kombination aus einer einzelnen Quelle, null oder mehr Prozessoren und einer einzelnen Senke. Bei OpenSearch der Datenaufnahme muss es sich bei der Senke immer um eine OpenSearch Dienstdomäne handeln. Eine Liste der unterstützten Optionen finden Sie unter. the section called “Unterstützte Plugins und Optionen”

   > **Note**
   >
   > Sie müssen die `sigv4` Optionen `sts_role_arn` und in jede Unterpipeline aufnehmen. Die Pipeline übernimmt die in `sts_role_arn` zum Signieren von Anfragen an die Domäne definierte Rolle. Weitere Informationen finden Sie unter the section called “Pipelines Zugriff auf Domains gewähren”.

   Die folgende Beispielkonfigurationsdatei verwendet die HTTP-Quelle und die Grok-Plug-ins, um unstrukturierte Protokolldaten zu verarbeiten und an eine OpenSearch Service-Domain zu senden. Die Sub-Pipeline ist benannt. `log-pipeline`

```
version: "2"
log-pipeline:
  source:
    http:
      path: "/log/ingest"
  processor:
    - grok:
        match:
          log: [ '%{COMMONAPACHELOG}' ]
    - date:
        from_time_received: true
        destination: "@timestamp"
  sink:
```

```
    - opensearch:
        hosts: [ "https://search-my-domain.us-east-1.es.amazonaws.com" ]
        index: "apache_logs"
        aws:
          sts_role_arn: "arn:aws:iam::123456789012:role/{pipeline-role}"
          region: "us-east-1"
```

> **Note**
>
> Wenn Sie mehrere Senken innerhalb einer YAML-Pipeline-Definition angeben, müssen sie alle derselben OpenSearch Dienstdomäne angehören. Eine OpenSearch Ingestion-Pipeline kann nicht in mehrere verschiedene Domänen schreiben.

Sie können Ihre eigene Pipeline-Konfiguration erstellen oder Datei hochladen auswählen und eine bestehende Konfiguration für eine selbstverwaltete Data Prepper-Pipeline importieren. Alternativ können Sie einen Konfigurations-Blueprint verwenden.

7. Nachdem Sie Ihre Pipeline konfiguriert haben, wählen Sie Pipeline validieren aus, um zu bestätigen, dass Ihre Konfiguration korrekt ist. Wenn die Validierung fehlschlägt, beheben Sie die Fehler und führen Sie die Validierung erneut aus.
8. Wählen Sie unter Netzwerkkonfiguration entweder VPC-Zugriff oder Öffentlicher Zugriff aus. Fahren Sie bei Wahl von Public access (Öffentlicher Zugriff) mit dem nächsten Schritt fort. Wenn Sie VPC-Zugriff wählen, konfigurieren Sie die folgenden Einstellungen:

Einstellung	Beschreibung
Endpunktv erwaltung	Wählen Sie aus, ob Sie Ihre VPC-Endpoints selbst erstellen möchten oder ob Sie sie von OpenSearch Ingestion für Sie erstellen lassen möchten. Endpoint Management verwendet standardmäßig Endpoints, die von Ingestion verwaltet werden. OpenSearch
VPC	Wählen Sie für die Virtual Private Cloud (VPC) die ID, die Sie verwenden möchten. Die VPC und die Pipeline müssen identisch AWS-Region sein.
Subnets	Wählen Sie ein oder mehrere Subnetze aus. OpenSearch Der Service platziert einen VPC-Endpunkt und elastische Netzwerkschnittstellen in den Subnetzen.

Einstellung	Beschreibung
Sicherheitsgruppen	Wählen Sie eine oder mehrere VPC-Sicherheitsgruppen aus, die es Ihrer gewünschten Anwendung ermöglichen, die OpenSearch Ingestion-Pipeline auf den von der Pipeline bereitgestellten Ports (80 oder 443) und Protokollen (HTTP oder HTTPs) zu erreichen.
VPC-Anhangsoptionen	Wenn Ihre Quelle ein selbstverwalteter Endpunkt ist, fügen Sie Ihre Pipeline einer VPC hinzu. Wählen Sie eine der bereitgestellten Standard-CIDR-Optionen oder verwenden Sie ein benutzerdefiniertes CIDR.

Weitere Informationen finden Sie unter the section called “Konfiguration des VPC-Zugriffs für Pipelines”.

9. (Optional) Fügen Sie Ihrer Pipeline unter Tags ein oder mehrere Tags (Schlüssel-Wert-Paare) hinzu. Weitere Informationen finden Sie unter the section called “Kennzeichnen von Rohrleitungen”.
10. (Optional) Aktivieren Sie unter Optionen zur Protokollveröffentlichung die Veröffentlichung von Pipeline-Protokollen in Amazon CloudWatch Logs. Wir empfehlen, die Protokollveröffentlichung zu aktivieren, damit Sie Pipeline-Probleme einfacher beheben können. Weitere Informationen finden Sie unter the section called “Überwachen der Pipeline-Protokolle”.
11. Wählen Sie Weiter.
12. Überprüfen Sie Ihre Pipeline-Konfiguration und wählen Sie Erstellen aus.

OpenSearch Ingestion führt einen asynchronen Prozess zum Erstellen der Pipeline aus. Sobald der Pipeline-Status lautet`Active`, können Sie mit der Datenaufnahme beginnen.

AWS CLI

Der Befehl create-pipeline akzeptiert die Pipeline-Konfiguration als Zeichenfolge oder in einer .yaml-Datei. Wenn Sie die Konfiguration als Zeichenfolge angeben, muss jede neue Zeile mit einem Escapezeichen versehen werden. `\n` Beispiel: `"log-pipeline:\n source:\n http:\n processor:\n - grok:\n ...`

Der folgende Beispielbefehl erstellt eine Pipeline mit der folgenden Konfiguration:

- Mindestens 4 Ingestion-OCUs, maximal 10 Ingestion-OCUs

- Bereitgestellt in einer Virtual Private Cloud (VPC)
- Veröffentlichung von Protokollen aktiviert

```
aws osis create-pipeline \
  --pipeline-name my-pipeline \
  --min-units 4 \
  --max-units 10 \
  --log-publishing-options
 IsLoggingEnabled=true,CloudWatchLogDestination={LogGroup="MyLogGroup"} \
  --vpc-options
 SecurityGroupIds={sg-12345678,sg-9012345},SubnetIds=subnet-1212234567834asdf \
  --pipeline-configuration-body "file://pipeline-config.yaml"
```

OpenSearch Bei der Aufnahme wird ein asynchroner Prozess zum Erstellen der Pipeline ausgeführt. Sobald der Pipeline-Status lautet`Active`, können Sie mit der Datenaufnahme beginnen. Verwenden Sie den GetPipelineBefehl, um den Status der Pipeline zu überprüfen.

OpenSearch Aufnahme-API

Rufen Sie den Vorgang auf, um eine OpenSearch Ingestion-Pipeline mithilfe der OpenSearch Ingestion-API zu erstellen. CreatePipeline

Nachdem Ihre Pipeline erfolgreich erstellt wurde, können Sie Ihren Client konfigurieren und mit der Aufnahme von Daten in Ihre Service-Domain beginnen. OpenSearch Weitere Informationen finden Sie unter the section called “Arbeiten mit Pipeline-Integrationen”.

Den Status der Pipeline-Erstellung verfolgen

Sie können den Status einer Pipeline verfolgen, während sie von OpenSearch Ingestion bereitgestellt und für die Datenaufnahme vorbereitet wird.

Konsole

Nachdem Sie eine Pipeline zum ersten Mal erstellt haben, durchläuft sie mehrere Phasen, während OpenSearch Ingestion sie für die Datenaufnahme vorbereitet. Um die verschiedenen Phasen der Pipeline-Erstellung zu sehen, wählen Sie den Namen der Pipeline aus, um die Seite mit den Pipeline-Einstellungen aufzurufen. Wählen Sie unter Status die Option Details anzeigen aus.

Eine Pipeline durchläuft die folgenden Phasen, bevor sie für die Datenaufnahme verfügbar ist:

- Validierung — Überprüfung der Pipeline-Konfiguration. Wenn diese Phase abgeschlossen ist, waren alle Validierungen erfolgreich.
- Umgebung erstellen — Ressourcen vorbereiten und bereitstellen. Wenn diese Phase abgeschlossen ist, wurde die neue Pipeline-Umgebung erstellt.
- Pipeline bereitstellen — Bereitstellung der Pipeline. Wenn diese Phase abgeschlossen ist, wurde die Pipeline erfolgreich bereitgestellt.
- Zustand der Pipeline überprüfen — Überprüfung des Zustands der Pipeline. Wenn diese Phase abgeschlossen ist, wurden alle Integritätsprüfungen bestanden.
- Datenverkehr aktivieren — Ermöglicht der Pipeline, Daten aufzunehmen. Wenn diese Phase abgeschlossen ist, können Sie mit der Aufnahme von Daten in die Pipeline beginnen.

CLI

Verwenden Sie den get-pipeline-change-progressBefehl, um den Status einer Pipeline zu überprüfen. Die folgende AWS CLI Anfrage überprüft den Status einer Pipeline mit dem Namen`my-pipeline`:

```
aws osis get-pipeline-change-progress \
    --pipeline-name my-pipeline
```

Antwort:

```
{
   "ChangeProgressStatuses": {
      "ChangeProgressStages": [
         {
            "Description": "Validating pipeline configuration",
            "LastUpdated": 1.671055851E9,
            "Name": "VALIDATION",
            "Status": "PENDING"
         }
      ],
      "StartTime": 1.671055851E9,
      "Status": "PROCESSING",
      "TotalNumberOfStages": 5
   }
}
```

OpenSearch Aufnahme-API

Rufen Sie den Vorgang auf, um den Status der Pipeline-Erstellung mithilfe der OpenSearch Ingestion-API zu verfolgen. GetPipelineChangeProgress

Verwenden von Blueprints zum Erstellen einer Pipeline

Anstatt eine Pipeline-Definition von Grund auf neu zu erstellen, können Sie Konfigurations-Blueprints verwenden. Dabei handelt es sich um vorkonfigurierte YAML-Vorlagen für gängige Aufnahmeszenarien wie Trace Analytics oder Apache-Protokolle. Mithilfe von Konfigurations-Blueprints können Sie Pipelines einfach bereitstellen, ohne eine Konfiguration von Grund auf neu erstellen zu müssen.

Konsole

Um einen Pipeline-Blueprint zu verwenden

1. Melden Sie sich bei der Amazon OpenSearch Service-Konsole unter https://console.aws.amazon.com/aos/home an.
2. Wählen Sie im linken Navigationsbereich Pipelines und dann Pipeline erstellen aus.
3. Wählen Sie einen Blueprint aus. Die Pipeline-Konfiguration wird mit einer Sub-Pipeline für den von Ihnen ausgewählten Anwendungsfall gefüllt.
4. Lesen Sie den auskommentierten Text, der Sie durch die Konfiguration des Blueprints führt.

> **Important**
>
> Der Pipeline-Blueprint ist in seiner jetzigen Form nicht gültig. Sie müssen einige Änderungen vornehmen, z. B. den Rollen-ARN AWS-Region und den für die Authentifizierung zu verwendenden Rollen-ARN angeben, da andernfalls die Pipeline-Validierung fehlschlägt.

CLI

Senden Sie eine list-pipeline-blueprintsAnfrage, um eine Liste aller verfügbaren Blueprints mithilfe von zu erhalten. AWS CLI

```
aws osis list-pipeline-blueprints
```

Die Anfrage gibt eine Liste aller verfügbaren Blueprints zurück.

Verwenden Sie den folgenden Befehl, um detailliertere Informationen zu einem bestimmten Blueprint zu erhalten: get-pipeline-blueprint

```
aws osis get-pipeline-blueprint --blueprint-name AWS-ApacheLogPipeline
```

Diese Anfrage gibt den Inhalt des Apache-Protokoll-Pipeline-Blueprints zurück:

```
{
   "Blueprint":{
      "PipelineConfigurationBody":"###\n  # Limitations: https://docs.aws.amazon.com/
opensearch-service/latest/ingestion/ingestion.html#ingestion-limitations\n###\n###\n
 # apache-log-pipeline:\n    # This pipeline receives logs via http (e.g. FluentBit),
 extracts important values from the logs by matching\n    # the value in the 'log' key
 against the grok common Apache log pattern. The grokked logs are then sent\n    # to
 OpenSearch to an index named 'logs'\n###\n\nversion: \"2\"\napache-log-pipeline:\n
 source:\n    http:\n      # Provide the path for ingestion. ${pipelineName} will be
 replaced with pipeline name configured for this pipeline.\n      # In this case it
 would be \"/apache-log-pipeline/logs\". This will be the FluentBit output URI value.
\n      path: \"/${pipelineName}/logs\"\n  processor:\n    - grok:\n        match:\n
          log: [ \"%{COMMONAPACHELOG_DATATYPED}\" ]\n  sink:\n    - opensearch:\n
   # Provide an AWS OpenSearch Service domain endpoint\n        # hosts: [ \"https://
search-mydomain-1a2a3a4a5a6a7a8a9a0a9a8a7a.us-east-1.es.amazonaws.com\" ]\n
 aws:\n          # Provide a Role ARN with access to the domain. This role should have
 a trust relationship with osis-pipelines.amazonaws.com\n          # sts_role_arn:
 \"arn:aws:iam::123456789012:role/Example-Role\"\n          # Provide the region of the
 domain.\n          # region: \"us-east-1\"\n          # Enable the 'serverless' flag
 if the sink is an Amazon OpenSearch Serverless collection\n          # serverless:
 true\n        index: \"logs\"\n        # Enable the S3 DLQ to capture any failed
 requests in an S3 bucket\n        # dlq:\n          # s3:\n            # Provide an
 S3 bucket\n            # bucket: \"your-dlq-bucket-name\"\n            # Provide a key
 path prefix for the failed requests\n            # key_path_prefix: \"${pipelineName}/
logs/dlq\"\n            # Provide the region of the bucket.\n            # region:
 \"us-east-1\"\n            # Provide a Role ARN with access to the bucket. This role
 should have a trust relationship with osis-pipelines.amazonaws.com\n            #
 sts_role_arn: \"arn:aws:iam::123456789012:role/Example-Role\"\n",
      "BlueprintName":"AWS-ApacheLogPipeline"
   }
}
```

OpenSearch Aufnahme-API

Um Informationen zu Pipeline-Blueprints mithilfe der OpenSearch Ingestion-API zu erhalten, verwenden Sie die Operationen und. ListPipelineBlueprintsGetPipelineBlueprint

Amazon OpenSearch Ingestion-Pipelines anzeigen

Sie können die Details zu einer Amazon OpenSearch Ingestion-Pipeline mithilfe derAWS Management Console, der oder der AWS CLI OpenSearch Ingestion-API einsehen.

Konsole

So zeigen Sie eine Pipeline an

1. Melden Sie sich bei der OpenSearch Amazon--Service-Konsole unter https://console.aws.amazon.com/aos/home an.
2. Klicken Sie auf Pipelines im linken Navigationsbereich.
3. (Optional) Um Pipelines mit einem bestimmten Status anzuzeigen, wählen Sie „Beliebiger Status“ und dann einen Status aus, nach dem gefiltert werden soll.

   Eine Pipeline kann die folgenden Status haben:

   - `Creating`— Die Pipeline wird erstellt.
   - `Active`— Die Pipeline ist aktiv und bereit, Daten aufzunehmen.
   - `Updating`— Die Pipeline wird aktualisiert.
   - `Deleting`— Die Pipeline wird gelöscht.
   - `Create failed`— Die Pipeline konnte nicht erstellt werden.
   - `Update failed`— Die Pipeline konnte nicht aktualisiert werden.
   - `Starting`— Die Pipeline läuft.
   - `Start failed`— Die Pipeline konnte nicht gestartet werden.
   - `Stopping`— Die Pipeline wird gestoppt.
   - `Stopped`— Die Pipeline ist gestoppt und kann jederzeit neu gestartet werden.

Ingestion OCUs werden Ihnen nicht in Rechnung gestellt, wenn sich eine Pipeline in den BundesstaatenCreate failed,Creating, Deleting und befindet. Stopped

CLI

Um Pipelines mit dem anzuzeigenAWS CLI, senden Sie eine List-Pipelines-Anfrage:

```
aws osis list-pipelines
```

Die Anfrage gibt eine Liste aller vorhandenen Pipelines zurück:

```
{
    "NextToken": null,
    "Pipelines": [
        {,
            "CreatedAt": 1.671055851E9,
            "LastUpdatedAt": 1.671055851E9,
            "MaxUnits": 4,
            "MinUnits": 2,
            "PipelineArn": "arn:aws:osis:us-west-2:123456789012:pipeline/log-pipeline",
            "PipelineName": "log-pipeline",
            "Status": "ACTIVE",
            "StatusReason": {
                "Description": "The pipeline is ready to ingest data."
            }
        },
            "CreatedAt": 1.671055851E9,
            "LastUpdatedAt": 1.671055851E9,
            "MaxUnits": 2,
            "MinUnits": 8,
            "PipelineArn": "arn:aws:osis:us-west-2:123456789012:pipeline/another-
pipeline",
            "PipelineName": "another-pipeline",
            "Status": "CREATING",
            "StatusReason": {
                "Description": "The pipeline is being created. It is not able to ingest
 data."
            }
        }
    ]
}
```

Verwenden Sie den Befehl get-pipeline, um Informationen über eine einzelne Pipeline abzurufen:

```
aws osis get-pipeline --pipeline-name "my-pipeline"
```

Die Anfrage gibt Konfigurationsinformationen für die angegebene Pipeline zurück:


```
{
    "Pipeline": {
        "PipelineName": "my-pipeline",
        "PipelineArn": "arn:aws:osis:us-east-1:123456789012:pipeline/my-pipeline",
        "MinUnits": 9,
        "MaxUnits": 10,
        "Status": "ACTIVE",
        "StatusReason": {
            "Description": "The pipeline is ready to ingest data."
        },
        "PipelineConfigurationBody": "log-pipeline:\n source:\n http:\n processor:\n
 - grok:\n match:\nlog: [ '%{COMMONAPACHELOG}' ]\n - date:\n from_time_received: true
\n destination: \"@timestamp\"\n  sink:\n - opensearch:\n hosts: [ \"https://search-
mdp-performance-test-duxkb4qnycd63rpy6svmvyvfpi.us-east-1.es.amazonaws.com\" ]\n index:
 \"apache_logs\"\n aws_sts_role_arn: \"arn:aws:iam::123456789012:role/my-domain-role
\"\n  aws_region: \"us-east-1\"\n  aws_sigv4: true",,
        "CreatedAt": "2022-10-01T15:28:05+00:00",
        "LastUpdatedAt": "2022-10-21T21:41:08+00:00",
        "IngestEndpointUrls": [
            "my-pipeline-123456789012.us-east-1.osis.amazonaws.com"
        ]
    }
}
```


OpenSearchAufnahme-API

Um die OpenSearch Ingestion-Pipelines mithilfe der OpenSearch Ingestion-API anzuzeigen, rufen Sie die Operationen and auf. ListPipelinesGetPipeline

Aktualisierung der Amazon OpenSearch Ingestion-Pipelines

Sie können Amazon OpenSearch Ingestion-Pipelines mithilfe der AWS Management Console, der oder der AWS CLI OpenSearch Ingestion-API aktualisieren. OpenSearch Ingestion initiiert eine blaue/grüne Bereitstellung, wenn Sie die YAML-Konfiguration einer Pipeline aktualisieren. Weitere Informationen finden Sie unter the section called “Blaue/grüne Bereitstellungen für Pipeline-Updates”.

Themen

- Überlegungen
- Erforderliche Berechtigungen

- Pipelines werden aktualisiert
- Blaue/grüne Bereitstellungen für Pipeline-Updates

Überlegungen

Beachten Sie Folgendes, wenn Sie eine Pipeline aktualisieren:

- Sie können die Kapazitätsgrenzen einer Pipeline, die Optionen zur Protokollveröffentlichung und die YAML-Konfiguration bearbeiten. Sie können ihren Namen oder ihre Netzwerkeinstellungen nicht bearbeiten.
- Wenn Ihre Pipeline in eine VPC-Domänensenke schreibt, können Sie nicht zurückgehen und die Senke in eine andere VPC-Domäne ändern, nachdem die Pipeline erstellt wurde. Sie müssen die Pipeline löschen und mit der neuen Senke neu erstellen. Sie können die Senke immer noch von einer VPC-Domain zu einer Public Domain, von einer Public Domain zu einer VPC-Domain oder von einer Public Domain zu einer anderen Public Domain wechseln.
- Sie können die Pipeline-Senke jederzeit zwischen einer öffentlichen OpenSearch Dienstdomäne und einer OpenSearch serverlosen Sammlung wechseln.
- Wenn Sie die YAML-Konfiguration einer Pipeline aktualisieren, initiiert OpenSearch Ingestion eine blaue/grüne Bereitstellung. Weitere Informationen finden Sie unter the section called “Blaue/grüne Bereitstellungen für Pipeline-Updates”.
- Wenn Sie die YAML-Konfiguration einer Pipeline aktualisieren, aktualisiert OpenSearch Ingestion Ihre Pipeline automatisch auf die neueste unterstützte Nebenversion der Hauptversion von Data Prepper, die in der Pipeline-Konfiguration angegeben ist. Dieser Prozess hält Ihre Pipeline mit den neuesten Bugfixes und Leistungsverbesserungen auf dem neuesten Stand.
- Sie können immer noch Aktualisierungen an Ihrer Pipeline vornehmen, wenn sie gestoppt ist.

Erforderliche Berechtigungen

OpenSearch Ingestion verwendet die folgenden IAM-Berechtigungen für die Aktualisierung von Pipelines:

- `osis:UpdatePipeline`— Aktualisieren Sie eine Pipeline.
- `osis:ValidatePipeline`— Prüfen Sie, ob eine Pipeline-Konfiguration gültig ist.
- `iam:PassRole`— Übergeben Sie die Pipeline-Rolle an OpenSearch Ingestion, damit sie Daten in die Domain schreiben kann. Diese Berechtigung ist nur erforderlich, wenn Sie die

YAML-Konfiguration der Pipeline aktualisieren, nicht, wenn Sie andere Einstellungen wie die Veröffentlichung von Protokollen oder Kapazitätsgrenzen ändern.

Die folgende Richtlinie gewährt beispielsweise die Erlaubnis, eine Pipeline zu aktualisieren:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Resource":"*",
         "Action":[
            "osis:UpdatePipeline",
            "osis:ValidatePipeline"
         ]
      },
      {
         "Resource":[
            "arn:aws:iam::{your-account-id}:role/{pipeline-role}"
         ],
         "Effect":"Allow",
         "Action":[
            "iam:PassRole"
         ]
      }
   ]
}
```

Pipelines werden aktualisiert

Sie können Amazon OpenSearch Ingestion-Pipelines mithilfe der AWS Management Console, der oder der AWS CLI OpenSearch Ingestion-API aktualisieren.

Konsole

Um eine Pipeline zu aktualisieren

1. Melden Sie sich bei der Amazon OpenSearch Service-Konsole unter https://console.aws.amazon.com/aos/home an.
2. Wählen Sie im linken Navigationsbereich Pipelines aus.

3. Wählen Sie eine Pipeline aus, um ihre Einstellungen zu öffnen. Sie können die Kapazitätsgrenzen einer Pipeline, die Optionen zur Protokollveröffentlichung und die YAML-Konfiguration bearbeiten. Sie können ihren Namen oder ihre Netzwerkeinstellungen nicht bearbeiten.
4. Wenn Sie die gewünschten Änderungen vorgenommen haben, wählen Sie Save (Speichern) aus.

CLI

Um eine Pipeline mit dem zu aktualisieren AWS CLI, senden Sie eine Update-Pipeline-Anfrage. Die folgende Beispielanforderung lädt eine neue Konfigurationsdatei hoch und aktualisiert die Mindest- und Höchstkapazitätswerte:

```
aws osis update-pipeline \
  --pipeline-name "my-pipeline" \
  --pipline-configuration-body "file://new-pipeline-config.yaml" \
  --min-units 11 \
  --max-units 18
```

OpenSearch Aufnahme-API

Rufen Sie den Vorgang auf, um eine OpenSearch Ingestion-Pipeline mithilfe der OpenSearch Ingestion-API zu aktualisieren. UpdatePipeline

Blaue/grüne Bereitstellungen für Pipeline-Updates

OpenSearch Die Aufnahme leitet einen blauen/grünen Bereitstellungsprozess ein, wenn Sie die YAML-Konfiguration einer Pipeline aktualisieren.

Blau/Grün bezieht sich auf die Praxis, eine neue Umgebung für Pipeline-Updates zu erstellen und den Datenverkehr nach Abschluss dieser Updates an die neue Umgebung weiterzuleiten. Die Praxis minimiert die Ausfallzeiten und verwaltet die ursprüngliche Umgebung für den Fall, dass die Bereitstellung in der neuen Umgebung fehlgeschlagen ist. Blaue/grüne Bereitstellungen selbst haben keine Auswirkungen auf die Leistung, aber die Leistung kann sich ändern, wenn sich Ihre Pipeline-Konfiguration so ändert, dass die Leistung beeinträchtigt wird.

OpenSearch Die Aufnahme blockiert die auto-scaling bei Blau/Grün-Bereitstellungen. Ihnen wird weiterhin nur der Datenverkehr zur alten Pipeline in Rechnung gestellt, bis dieser zur neuen Pipeline

umgeleitet wird. Sobald der Verkehr umgeleitet wurde, wird Ihnen nur die neue Pipeline in Rechnung gestellt. Ihnen werden niemals zwei Pipelines gleichzeitig in Rechnung gestellt.

Wenn Sie die YAML-Konfigurationsdatei einer Pipeline aktualisieren, kann OpenSearch Ingestion Ihre Pipeline automatisch auf die neueste unterstützte Nebenversion der Hauptversion von Data Prepper aktualisieren, die in der Pipeline-Konfiguration angegeben ist. Möglicherweise haben Sie `version: "2"` in Ihrer Pipeline-Konfiguration und OpenSearch Ingestion die Pipeline zunächst mit Version 2.1.0 bereitgestellt. Wenn Unterstützung für Version 2.1.1 hinzugefügt wird und Sie eine Änderung an Ihrer Pipeline-Konfiguration vornehmen, aktualisiert OpenSearch Ingestion Ihre Pipeline auf Version 2.1.1.

Dieser Prozess hält Ihre Pipeline mit den neuesten Bugfixes und Leistungsverbesserungen auf dem neuesten Stand. OpenSearch Ingestion kann die Hauptversion Ihrer Pipeline nur aktualisieren, wenn Sie die `version` Option in der Pipeline-Konfiguration manuell ändern.

Amazon OpenSearch Ingestion-Pipelines beenden und starten

Mithilfe des Stoppens und Startens OpenSearch von Amazon Ingestion Pipelines können Sie die Kosten für Entwicklungs- und Testumgebungen verwalten. Sie können eine Pipeline vorübergehend stoppen, anstatt sie jedes Mal, wenn Sie die Pipeline verwenden, einzurichten und zu entfernen.

Themen

Übersicht über das Stoppen und Starten einer OpenSearch Ingestion-Pipeline

Sie können eine Pipeline in Zeiten stoppen, in denen Sie keine Daten in sie aufnehmen müssen. Bei Bedarf können Sie die Pipeline jederzeit erneut starten. Durch das Starten und Stoppen werden die Einrichtungs- und ENTFERnungsvorgänge für Pipelines erleichtert, die in der Entwicklung, für Tests oder ähnliche Aktivitäten verwendet werden, die keine kontinuierliche Verfügbarkeit erfordern.

Während Ihre Pipeline gestoppt ist, werden Ihnen keine Ingestion OCU-Stunden in Rechnung gestellt. Sie können gestoppte Pipelines weiterhin aktualisieren, und sie erhalten automatische Nebenversionsupdates und Sicherheitspatches.

Verwenden Sie die Funktion zum Starten und Stoppen nicht, wenn Ihre Pipeline aktiv bleiben muss, jedoch überschüssigen Kapazitäten hat. Wenn Ihre Pipeline zu teuer oder nicht sehr ausgelastet ist, sollten Sie erwägen, die maximalen Kapazitätsgrenzen zu reduzieren. Weitere Informationen finden Sie unter the section called “Skalierung von Pipelines”.

Stoppen einer OpenSearch Ingestion-Pipeline

Um eine OpenSearch Ingestion-Pipeline zu verwenden oder die Verwaltung durchzuführen, beginnen Sie immer mit einer aktiven Pipeline, beenden dann die Pipeline und starten die Pipeline dann erneut. Während Ihre Pipeline gestoppt ist, werden Ihnen die Stunden der Ingestion OCU nicht in Rechnung gestellt.

Konsole

Zum Anhalten einer Pipeline

1. Melden Sie sich bei der OpenSearch Amazon-Servicekonsole unter https://console.aws.amazon.com/aos/home an.
2. Wählen Sie im Navigationsbereich Pipelines und wählen Sie dann eine Pipeline aus. Sie können den Stoppvorgang von dieser Seite ausführen oder zur Detailseite für die Pipeline navigieren, die Sie stoppen möchten.
3. Wählen Sie unter Aktionen die Option Pipeline beenden aus.

   Wenn eine Pipeline nicht gestoppt und gestartet werden kann, ist die Aktion Pipeline beenden nicht verfügbar.

AWS CLI

Zum Anhalten einer Pipeline über die AWS CLI rufen Sie den Befehl stop-pipeline mit den folgenden Parametern auf:

- `--pipeline-name`— der Name der Pipeline.

Example

```
aws osis stop-pipeline --pipeline-name my-pipeline
```

OpenSearchAufnahme-API

Zum Anhalten einer Pipeline über die OpenSearch Ingestion-API rufen Sie die StopPipelineOperation mit dem folgenden Parameter auf:

- `PipelineName`— der Name der Pipeline.

Eine OpenSearch Ingestion-Pipeline starten

Ausgangspunkt für den Start einer OpenSearch Ingestion-Pipeline ist immer eine Pipeline, die sich bereits im gestoppten Zustand befindet. Die Pipeline behält ihre Konfigurationseinstellungen, wie z. B. Kapazitätsgrenzen, Netzwerkeinstellungen und Optionen zur Protokollveröffentlichung, bei.

Der Neustart einer Pipeline dauert in der Regel mehrere Minuten.

Konsole

Zum Starten einer Pipeline

1. Melden Sie sich bei der OpenSearch Amazon-Servicekonsole unter https://console.aws.amazon.com/aos/home an.
2. Wählen Sie im Navigationsbereich Pipelines und wählen Sie dann eine Pipeline aus. Sie können den Startvorgang von dieser Seite ausführen oder zur Detailseite für die zu startende Pipeline navigieren.
3. Wählen Sie unter Aktionen die Option Pipeline starten aus.

AWS CLI

Zum Starten einer Pipeline über die AWS CLI rufen Sie den Befehl start-pipeline mit den folgenden Parametern auf:

- `--pipeline-name`— der Name der Pipeline.

Example

```
aws osis start-pipeline --pipeline-name my-pipeline
```

OpenSearchAufnahme-API

Um eine OpenSearch Ingestion-Pipeline mithilfe der OpenSearch Ingestion-API zu starten, rufen Sie den StartPipelineVorgang mit dem folgenden Parameter auf:

- `PipelineName`— der Name der Pipeline.

Löschen von Amazon OpenSearch Ingestion-Pipelines

Sie können eine Amazon OpenSearch Ingestion-Pipeline mithilfe derAWS Management Console, der oder der AWS CLI OpenSearch Ingestion-API löschen. Sie können eine Pipeline nicht löschen, wenn sie den Status `Creating` oder hat`Updating`.

Konsole

So löschen Sie eine Pipeline

1. Melden Sie sich bei der Amazon OpenSearch Service Console unter https://console.aws.amazon.com/aos/home an.
2. Wählen Sie im linken Navigationsbereich Pipelines aus.
3. Wählen Sie die Pipeline aus, die Sie löschen möchten, und klicken Sie auf Löschen.
4. Bestätigen Sie den Löschvorgang und wählen Sie Delete (Löschen) aus.

CLI

Um eine Pipeline mit dem zu löschenAWS CLI, senden Sie eine Delete-Pipeline-Anfrage:

```
aws osis delete-pipeline --pipeline-name "my-pipeline"
```

OpenSearchAufnahme-API

Um eine OpenSearch Ingestion-Pipeline mithilfe der OpenSearch Ingestion-API zu löschen, rufen Sie den DeletePipelineVorgang mit dem folgenden Parameter auf:

- `PipelineName`— der Name der Pipeline.

Unterstützte Plugins und Optionen für Amazon OpenSearch Ingestion-Pipelines

Amazon OpenSearch Ingestion unterstützt im Vergleich zu Open Source Data Prepper eine Untergruppe von Quellen, Prozessoren und Senken. Darüber hinaus gibt es einige Einschränkungen, die OpenSearch Ingestion in Bezug auf die verfügbaren Optionen für jedes unterstützte Plugin festlegt. In den folgenden Abschnitten werden die Plugins und die zugehörigen Optionen beschrieben, die OpenSearch Ingestion unterstützt.

> **Note**
>
> OpenSearch Ingestion unterstützt keine Puffer-Plugins, da es automatisch einen Standardpuffer konfiguriert. Sie erhalten einen Validierungsfehler, wenn Sie einen Puffer in Ihre Pipeline-Konfiguration aufnehmen.

Themen

Unterstützte Plug-ins

OpenSearch Ingestion unterstützt die folgenden Data Prepper-Plugins:

Quellen:

- Amazon DocumentDB
- DynamoDB
- OpenSearch

- HTTP
- Kafka
- Hotelprotokolle

- Otel-Metriken
- Hotel-Trace
- S3

Prozessoren:

- Aggregate
- Anomaliedetektor
- CSV
- Date (Datum)
- Dekomprimieren
- Sezieren
- Ereignisse löschen
- Geo-IP
- Grok
- Schlüsselwert
- Von der Karte zur Liste
- Ereignis mutieren (Reihe von Prozessoren)
- Zeichenfolge mutieren (Reihe von Prozessoren)
- Verschleiern
- Hotel-Metriken
- Otel Trace-Gruppe
- Hotel Trace
- Ion analysieren
- Analysieren Sie JSON
- Analysieren Sie XML
- Wählen Sie Einträge aus
- Service-Karte
- Peer Forwarder nachverfolgen
- Kürzen

- Benutzeragent

Senkt:

- OpenSearch(unterstützt OpenSearch Service, OpenSearch Serverless und Elasticsearch 6.8 oder höher)
- S3

Sink-Codecs:

- Avro
- NDJSON
- JSON
- Parkett

Stateless versus statusbehaftete Prozessoren

Zustandslose Prozessoren führen Operationen wie Transformationen und Filterung durch, während statusbehaftete Prozessoren Operationen wie Aggregationen ausführen, die sich an das Ergebnis der vorherigen Ausführung erinnern. OpenSearch Ingestion unterstützt die Stateful-Prozessoren Aggregate und Service-MAP. Alle anderen unterstützten Prozessoren sind statuslos.

Für Pipelines, die nur statuslose Prozessoren enthalten, liegt die maximale Kapazitätsgrenze bei 96 Ingestion-OCUs. Wenn eine Pipeline Stateful-Prozessoren enthält, beträgt die maximale Kapazitätsgrenze 48 Ingestion-OCUs. Wenn für eine Pipeline jedoch die persistente Pufferung aktiviert ist, kann sie maximal 384 Ingestion-OCUs mit nur statusfreien Prozessoren oder 192 Ingestion-OCUs haben, wenn sie Stateful-Prozessoren enthält. Weitere Informationen finden Sie unter the section called “Skalierung von Pipelines”.

E-Bestätigung wird nur für statusfreie Prozessoren unterstützt. nd-to-end Weitere Informationen finden Sie unter the section called “E-Bestätigung nd-to-end ”.

Konfigurationsanforderungen und Einschränkungen

Sofern unten nicht anders angegeben, sind alle in der Data Prepper-Konfigurationsreferenz für die oben aufgeführten unterstützten Plugins beschriebenen Optionen in OpenSearch Ingestion-Pipelines

zulässig. In den folgenden Abschnitten werden die Einschränkungen erläutert, die OpenSearch Ingestion bestimmten Plugin-Optionen auferlegt.

> **Note**
>
> OpenSearch Ingestion unterstützt keine Puffer-Plugins, da es automatisch einen Standardpuffer konfiguriert. Sie erhalten einen Validierungsfehler, wenn Sie einen Puffer in Ihre Pipeline-Konfiguration aufnehmen.

Viele Optionen werden intern von OpenSearch Ingestion konfiguriert und verwaltet, z. B. `authentication` und. `acm_certificate_arn` Andere Optionen, wie z. B. `thread_count` und, haben Auswirkungen auf die Leistung`request_timeout`, wenn sie manuell geändert werden. Daher werden diese Werte intern festgelegt, um eine optimale Leistung Ihrer Pipelines sicherzustellen.

Schließlich können einige Optionen nicht an OpenSearch Ingestion übergeben werden, z. B. `ism_policy_file` und`sink_template`, da es sich bei der Ausführung im Open-Source-Data Prepper um lokale Dateien handelt. Diese Werte werden nicht unterstützt.

Themen

- Allgemeine Pipeline-Optionen
- Grok-Prozessor
- HTTP-Quelle
- OpenSearch sinken
- Quelle für oTel-Metriken, Quelle für oTel-Trace-Daten und Quelle für oTel-Protokolle
- Prozessor für die OT-Trace-Gruppe
- Otel-Trace-Prozessor
- Service-Map-Prozessor
- S3-Quelle

Allgemeine Pipeline-Optionen

Die folgenden allgemeinen Pipeline-Optionen werden von OpenSearch Ingestion festgelegt und in Pipeline-Konfigurationen nicht unterstützt:

- `workers`
- `delay`

Grok-Prozessor

Die folgenden Grok-Prozessoroptionen werden nicht unterstützt:

- `patterns_directories`
- `patterns_files_glob`

HTTP-Quelle

Für das HTTP-Quell-Plugin gelten die folgenden Anforderungen und Einschränkungen:

- Die `path` Option ist erforderlich. Der Pfad ist eine Zeichenfolge wie`/log/ingest`, die den URI-Pfad für die Protokollaufnahme darstellt. Dieser Pfad definiert den URI, den Sie verwenden, um Daten an die Pipeline zu senden. z. B. `https://log-pipeline.us-west-2.osis.amazonaws.com`*`/log/ingest`*. Der Pfad muss mit einem Schrägstrich (/) beginnen und kann die Sonderzeichen '-', '_', 'enthalten . 'und'/'sowie der `${pipelineName}` Platzhalter.
- Die folgenden HTTP-Quelloptionen werden von OpenSearch Ingestion festgelegt und in Pipeline-Konfigurationen nicht unterstützt:
  - `port`
  - `ssl`
  - `ssl_key_file`
  - `ssl_certificate_file`
  - `aws_region`
  - `authentication`
  - `unauthenticated_health_check`
  - `use_acm_certificate_for_ssl`
  - `thread_count`
  - `request_timeout`
  - `max_connection_count`
  - `max_pending_requests`

- `health_check_service`
- `acm_private_key_password`
- `acm_certificate_timeout_millis`
- `acm_certificate_arn`

OpenSearch sinken

Das OpenSearchSink-Plugin hat die folgenden Anforderungen und Einschränkungen.

- Die `aws` Option ist erforderlich und muss die folgenden Optionen enthalten:
  - `sts_role_arn`
  - `region`
  - `hosts`
  - `serverless`(wenn es sich bei der Senke um eine OpenSearch serverlose Sammlung handelt)
- Die `sts_role_arn` Option muss für jede Senke innerhalb einer YAML-Definitionsdatei auf dieselbe Rolle verweisen.
- Die `hosts` Option muss einen OpenSearch Dienstdomänenendpunkt oder einen OpenSearch serverlosen Sammlungsendpunkt angeben. Alle Hosts in einer YAML-Definitionsdatei müssen auf denselben Endpunkt verweisen. Sie können keinen benutzerdefinierten Endpunkt für eine Domain angeben. Es muss sich um den Standardendpunkt handeln.
- Wenn es sich bei der `hosts` Option um einen serverlosen Erfassungsendpunkt handelt, müssen Sie die `serverless` Option auf `true` setzen. Wenn Ihre YAML-Definitionsdatei die `index_type` Option enthält, muss sie außerdem auf gesetzt sein`management_disabled`, andernfalls schlägt die Validierung fehl.
- Die folgenden Optionen werden nicht unterstützt:
  - `username`
  - `password`
  - `cert`
  - `proxy`
  - `dlq_file`— Wenn Sie fehlgeschlagene Ereignisse in eine Warteschlange (Dead Letter Queue, DLQ) auslagern möchten, müssen Sie die `dlq` Option verwenden und einen S3-Bucket angeben.
  - `ism_policy_file`

- `socket_timeout`
- `template_file`
- `insecure`
- `bulk_size`

Quelle für oTel-Metriken, Quelle für oTel-Trace-Daten und Quelle für oTel-Protokolle

Für die Plug-ins oTEL metrics source, oTEL trace source und oTEL logs source gelten die folgenden Anforderungen und Einschränkungen:

- Die `path` Option ist erforderlich. Der Pfad ist eine Zeichenfolge wie`/log/ingest`, die den URI-Pfad für die Protokollaufnahme darstellt. Dieser Pfad definiert den URI, den Sie verwenden, um Daten an die Pipeline zu senden. z. B. `https://log-pipeline.us-west-2.osis.amazonaws.com`*`/log/ingest`*. Der Pfad muss mit einem Schrägstrich (/) beginnen und kann die Sonderzeichen '-', '_', 'enthalten . 'und'/'sowie der `${pipelineName}` Platzhalter.
- Die folgenden Optionen werden von OpenSearch Ingestion festgelegt und in Pipeline-Konfigurationen nicht unterstützt:
  - `port`
  - `ssl`
  - `sslKeyFile`
  - `sslKeyCertChainFile`
  - `authentication`
  - `unauthenticated_health_check`
  - `useAcmCertForSSL`
  - `unframed_requests`
  - `proto_reflection_service`
  - `thread_count`
  - `request_timeout`
  - `max_connection_count`
  - `acmPrivateKeyPassword`
  - `acmCertIssueTimeOutMillis`
  - `health_check_service`

- `acmCertificateArn`
- `awsRegion`

Prozessor für die OT-Trace-Gruppe

Für den OTel Trace Group Processor gelten die folgenden Anforderungen und Einschränkungen:

- Die `aws` Option ist erforderlich und muss die folgenden Optionen enthalten:
  - `sts_role_arn`
  - `region`
  - `hosts`
- Die `sts_role_arn` Option gibt dieselbe Rolle an wie die Pipeline-Rolle, die Sie in der OpenSearch Senkenkonfiguration angeben.
- Die `insecure` Optionen `usernamepassword`,`cert`, und werden nicht unterstützt.
- Die `aws_sigv4` Option ist erforderlich und muss auf true gesetzt werden.
- Die `serverless` Option im OpenSearch Sink-Plugin wird nicht unterstützt. Der Otel Trace Group Processor funktioniert derzeit nicht mit OpenSearch serverlosen Sammlungen.
- Die Anzahl der `otel_trace_group` Prozessoren im Pipeline-Konfigurationstext darf 8 nicht überschreiten.

Otel-Trace-Prozessor

Für den OTel Trace-Prozessor gelten die folgenden Anforderungen und Einschränkungen:

- Der Wert der `trace_flush_interval` Option darf 300 Sekunden nicht überschreiten.

Service-Map-Prozessor

Für den Service-MAP-Prozessor gelten die folgenden Anforderungen und Einschränkungen:

- Der Wert der `window_duration` Option darf 300 Sekunden nicht überschreiten.

S3-Quelle

Das S3-Quell-Plugin hat die folgenden Anforderungen und Einschränkungen:

- Die `aws` Option ist erforderlich und muss `sts_role_arn` Optionen enthaltenregion.
- Der Wert der `records_to_accumulate` Option darf 200 nicht überschreiten.
- Der Wert der `maximum_messages` Option darf 10 nicht überschreiten.
- Falls angegeben, muss die `disable_bucket_ownership_validation` Option auf False gesetzt werden.
- Falls angegeben, muss die `input_serialization` Option auf gesetzt werden`parquet`.

Arbeiten mit Amazon OpenSearch Ingestion-Pipeline-Integrationen

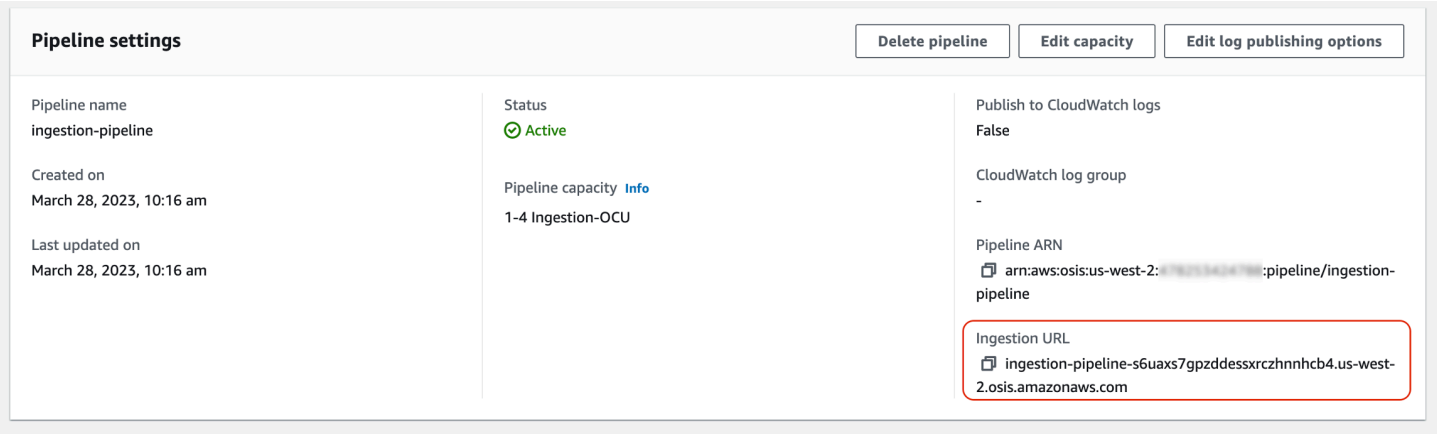
Um Daten erfolgreich in eine Amazon OpenSearch Ingestion-Pipeline aufzunehmen, müssen Sie Ihre Client-Anwendung (die Quelle) so konfigurieren, dass sie Daten an den Pipeline-Endpunkt sendet. Ihre Quelle könnten Clients wie Fluent Bit Logs, der OpenTelemetry Collector oder ein einfacher S3-Bucket sein. Die genaue Konfiguration ist für jeden Client unterschiedlich.

Die wichtigsten Unterschiede bei der Quellkonfiguration (im Vergleich zum direkten Senden von Daten an eine OpenSearch Dienstdomäne oder eine OpenSearch serverlose Sammlung) sind der AWS Dienstname (`osis`) und der Host-Endpunkt, der der Pipeline-Endpunkt sein muss.

Themen

Aufbau des Aufnahmeendpunkts

Um Daten in eine Pipeline aufzunehmen, senden Sie sie an den Aufnahmeendpunkt. Um die Aufnahme-URL zu finden, navigieren Sie zur Seite mit den Pipeline-Einstellungen und kopieren Sie die Aufnahme-URL:



Um den vollständigen Aufnahmeendpunkt für pullbasierte Quellen wie OTel Trace und oTEL Metrics zu erstellen, fügen Sie den Aufnahmepfad aus Ihrer Pipeline-Konfiguration zur Aufnahme-URL hinzu.

Nehmen wir beispielsweise an, dass Ihre Pipeline-Konfiguration den folgenden Aufnahmepfad hat:

```
entry-pipeline:
  source:
    http:
      path: "/my/test_path"
```

Der vollständige Aufnahmeendpunkt, den Sie in Ihrer Client-Konfiguration angeben, hat das folgende Format:. `https://ingestion-pipeline-abcdefg.us-west-2.osis.amazonaws.com/my/test_path`

Weitere Informationen finden Sie unter the section called “Angeben des Aufnahmepfads”.

Eine Aufnahmerolle erstellen

Alle Anfragen zur OpenSearch Datenerfassung müssen mit Signature Version 4 signiert sein. Der Rolle, die die Anfrage signiert, muss mindestens die Berechtigung für die `osis:Ingest` Aktion erteilt werden, sodass sie Daten an eine OpenSearch Ingestion-Pipeline senden kann.

Die folgende AWS Identity and Access Management (IAM-) Richtlinie ermöglicht es der entsprechenden Rolle beispielsweise, Daten an eine einzelne Pipeline zu senden:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "osis:Ingest",
      "Resource": "arn:aws:osis:us-east-1:{account-id}:pipeline/pipeline-name"
    }
  ]
}
```

> **Note**
>
> Um die Rolle für alle Pipelines zu verwenden, ersetzen Sie den ARN im `Resource` Element durch einen Platzhalter (*).

Bereitstellung von kontenübergreifendem Zugriff auf Datenerfassung

> **Note**
>
> Sie können kontenübergreifenden Zugriff auf die Erfassung nur für öffentliche Pipelines bereitstellen, nicht für VPC-Pipelines.

Möglicherweise müssen Sie Daten von einem anderen Konto in eine Pipeline aufnehmen AWS-Konto, z. B. von einem Konto, in dem Ihre Quellanwendung gespeichert ist. Wenn sich der Principal, der in eine Pipeline schreibt, in einem anderen Konto befindet als die Pipeline selbst, müssen Sie den Principal so konfigurieren, dass er einer anderen IAM-Rolle vertraut, um Daten in die Pipeline aufzunehmen.

Um kontoübergreifende Aufnahmeberechtigungen zu konfigurieren

1. Erstellen Sie die Aufnahmerolle mit der entsprechenden `osis:Ingest` Berechtigung (im vorherigen Abschnitt beschrieben) innerhalb derselben Pipeline. AWS-Konto Anweisungen finden Sie unter IAM-Rollen erstellen.
2. Fügen Sie der Aufnahmerolle eine Vertrauensrichtlinie hinzu, die es einem Principal in einem anderen Konto ermöglicht, sie zu übernehmen:

```
{
  "Version": "2012-10-17",
  "Statement": [{
     "Effect": "Allow",
     "Principal": {
       "AWS": "arn:aws:iam::{external-account-id}:root"
      },
     "Action": "sts:AssumeRole"
  }]
}
```

3. Konfigurieren Sie in dem anderen Konto Ihre Client-Anwendung (z. B. Fluent Bit) so, dass sie die Aufnahmerolle übernimmt. Damit dies funktioniert, muss das Anwendungskonto dem Anwendungsbenutzer oder der Rolle der Anwendung die Berechtigungen zur Übernahme der Aufnahmerolle gewähren.

   Das folgende Beispiel für eine identitätsbasierte Richtlinie ermöglicht es dem angehängten Prinzipal, `ingestion-role` vom Pipeline-Konto auszugehen:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::{account-id}:role/ingestion-role"
    }
  ]
}
```

Die Client-Anwendung kann dann den AssumeRoleVorgang verwenden, um Daten anzunehmen `ingestion-role` und in die zugehörige Pipeline aufzunehmen.

Verwenden einer OpenSearch Ingestion-Pipeline mit Amazon DynamoDB

Sie können eine OpenSearch Ingestion-Pipeline mit DynamoDB verwenden, um DynamoDB-Tabellenereignisse (wie Erstellen, Aktualisieren und Löschen) in Amazon Service-Domänen und Sammlungen zu streamen. OpenSearch Die OpenSearch Ingestion-Pipeline umfasst eine CDC-

Infrastruktur (Change Data Capture), um eine hochskalierbare Methode mit niedriger Latenz für das kontinuierliche Streamen von Daten aus einer DynamoDB-Tabelle bereitzustellen.

Es gibt zwei Möglichkeiten, DynamoDB als Quelle für die Datenverarbeitung zu verwenden — mit und ohne einen vollständigen anfänglichen Snapshot.

Ein vollständiger Anfangssnapshot ist eine Sicherung einer Tabelle, die DynamoDB mit der point-in-time Wiederherstellungsfunktion (PITR) erstellt. DynamoDB lädt diesen Snapshot auf Amazon S3 hoch. Von dort aus sendet eine OpenSearch Ingestion-Pipeline ihn an einen Index in einer Domain oder partitioniert ihn in mehrere Indizes in einer Domain. Damit die Daten in DynamoDB OpenSearch konsistent bleiben, synchronisiert die Pipeline alle Erstellungs-, Aktualisierungs- und Löschereignisse in der DynamoDB-Tabelle mit den Dokumenten, die im Index oder den Indizes gespeichert sind. OpenSearch

Wenn Sie einen vollständigen Anfangssnapshot verwenden, nimmt Ihre OpenSearch Ingestion-Pipeline zuerst den Snapshot auf und beginnt dann, Daten aus DynamoDB Streams zu lesen. Es holt schließlich auf und gewährleistet nahezu in Echtzeit die Datenkonsistenz zwischen DynamoDB und. OpenSearch Wenn Sie diese Option wählen, müssen Sie sowohl PITR als auch einen DynamoDB-Stream in Ihrer Tabelle aktivieren.

Sie können auch die OpenSearch Ingestion-Integration mit DynamoDB verwenden, um Ereignisse ohne Snapshot zu streamen. Wählen Sie diese Option, wenn Sie bereits einen vollständigen Snapshot von einem anderen Mechanismus haben oder wenn Sie nur aktuelle Ereignisse aus einer DynamoDB-Tabelle mit DynamoDB Streams streamen möchten. Wenn Sie diese Option wählen, müssen Sie nur einen DynamoDB-Stream in Ihrer Tabelle aktivieren.

Weitere Informationen zu dieser Integration finden Sie unter DynamoDB Zero-ETL-Integration mit Amazon OpenSearch Service im Entwicklerhandbuch.Amazon DynamoDB

Themen

Voraussetzungen

Um Ihre Pipeline einzurichten, benötigen Sie eine DynamoDB-Tabelle mit aktivierten DynamoDB Streams. Ihr Stream sollte den Stream-View-Typ verwenden. `NEW_IMAGE` OpenSearch Ingestion-Pipelines können jedoch auch Ereignisse streamen, `NEW_AND_OLD_IMAGES` sofern dieser Stream-View-Typ zu Ihrem Anwendungsfall passt.

Wenn Sie Snapshots verwenden, müssen Sie auch die point-in-time Wiederherstellung für Ihre Tabelle aktivieren. Weitere Informationen finden Sie unter Erstellen einer Tabelle, Aktivieren der point-in-time Wiederherstellung und Aktivieren eines Streams im Amazon DynamoDB DynamoDB-Entwicklerhandbuch.

Schritt 1: Konfigurieren Sie die Pipeline-Rolle

Nachdem Sie Ihre DynamoDB-Tabelle eingerichtet haben, richten Sie die Pipeline-Rolle ein, die Sie in Ihrer Pipeline-Konfiguration verwenden möchten, und fügen Sie der Rolle die folgenden DynamoDB-Berechtigungen hinzu:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "allowRunExportJob",
            "Effect": "Allow",
            "Action": [
                "dynamodb:DescribeTable",
                "dynamodb:DescribeContinuousBackups",
                "dynamodb:ExportTableToPointInTime"
            ],
            "Resource": [
                "arn:aws:dynamodb:us-east-1:{account-id}:table/my-table"
            ]
        },
        {
            "Sid": "allowCheckExportjob",
            "Effect": "Allow",
            "Action": [
                "dynamodb:DescribeExport"
            ],
            "Resource": [
                "arn:aws:dynamodb:us-east-1:{account-id}:table/my-table/export/*"
            ]
```

```
        },
        {
            "Sid": "allowReadFromStream",
            "Effect": "Allow",
            "Action": [
                "dynamodb:DescribeStream",
                "dynamodb:GetRecords",
                "dynamodb:GetShardIterator"
            ],
            "Resource": [
                "arn:aws:dynamodb:us-east-1:{account-id}:table/my-table/stream/*"
            ]
        },
        {
            "Sid": "allowReadAndWriteToS3ForExport",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:AbortMultipartUpload",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": [
                "arn:aws:s3:::my-bucket/{exportPath}/*"
            ]
        }
    ]
}
```

Sie können auch einen vom AWS KMS Kunden verwalteten Schlüssel verwenden, um die Exportdatendateien zu verschlüsseln. Um die exportierten Objekte zu entschlüsseln, geben Sie `s3_sse_kms_key_id` für die Schlüssel-ID in der Exportkonfiguration der Pipeline das folgende Format an:. `arn:aws:kms:us-west-2:{account-id}:key/my-key-id` Die folgende Richtlinie umfasst die erforderlichen Berechtigungen für die Verwendung eines vom Kunden verwalteten Schlüssels:

```
{
    "Sid": "allowUseOfCustomManagedKey",
    "Effect": "Allow",
    "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
```

```
    ],
    "Resource": arn:aws:kms:us-west-2:{account-id}:key/my-key-id
}
```

Schritt 2: Erstellen Sie die Pipeline

Anschließend können Sie eine OpenSearch Ingestion-Pipeline wie die folgende konfigurieren, die DynamoDB als Quelle angibt. Diese Beispielpipeline nimmt Daten aus `table-a` dem PITR-Snapshot auf, gefolgt von Ereignissen aus DynamoDB Streams. Die Startposition von `LATEST` gibt an, dass die Pipeline die neuesten Daten aus DynamoDB Streams lesen soll.

```
version: "2"
cdc-pipeline:
  source:
    dynamodb:
      tables:
      - table_arn: "arn:aws:dynamodb:us-west-2:{account-id}:table/table-a"
        export:
          s3_bucket: "my-bucket"
          s3_prefix: "export/"
        stream:
          start_position: "LATEST"
      aws:
        region: "us-west-2"
        sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
  sink:
  - opensearch:
      hosts: ["https://search-mydomain.us-east-1.es.amazonaws.com"]
      index: "${getMetadata(\"table_name\")}"
      index_type: custom
      normalize_index: true
      document_id: "${getMetadata(\"primary_key\")}"
      action: "${getMetadata(\"opensearch_action\")}"
      document_version: "${getMetadata(\"document_version\")}"
      document_version_type: "external"
```

Sie können einen vorkonfigurierten DynamoDB-Blueprint verwenden, um diese Pipeline zu erstellen. Weitere Informationen finden Sie unter the section called “Verwenden von Blueprints zum Erstellen einer Pipeline”.

Datenkonsistenz

OpenSearch Die Datenaufnahme unterstützt end-to-end die Bestätigung, um die Datenbeständigkeit sicherzustellen. Wenn eine Pipeline Snapshots oder Streams liest, erstellt sie dynamisch Partitionen für die Parallelverarbeitung. Die Pipeline markiert eine Partition als abgeschlossen, wenn sie nach der Aufnahme aller Datensätze in der OpenSearch Domäne oder Sammlung eine Bestätigung erhält.

Wenn Sie Daten in eine OpenSearch serverlose Suchsammlung aufnehmen möchten, können Sie in der Pipeline eine Dokument-ID generieren. Wenn Sie Daten in eine OpenSearch serverlose Zeitreihensammlung aufnehmen möchten, beachten Sie, dass die Pipeline keine Dokument-ID generiert.

Eine OpenSearch Ingestion-Pipeline ordnet außerdem eingehende Ereignisaktionen den entsprechenden Massenindizierungsaktionen zu, um das Ingestieren von Dokumenten zu erleichtern. Dadurch bleiben die Daten konsistent, sodass jede Datenänderung in DynamoDB mit den entsprechenden Dokumentänderungen in abgeglichen wird. OpenSearch

Datentypen zuordnen

OpenSearch Der Service ordnet Datentypen in jedem eingehenden Dokument dynamisch dem entsprechenden Datentyp in DynamoDB zu. Die folgende Tabelle zeigt, wie OpenSearch Service verschiedene Datentypen automatisch zuordnet.

Datentyp	OpenSearch	DynamoDB
Zahl	OpenSearch ordnet numerische Daten automatisch zu. Wenn es sich bei der Zahl um eine ganze Zahl OpenSearc h handelt, wird sie einem langen Wert zugeordnet. Wenn es sich bei der Zahl um eine Bruchzahl handelt, wird OpenSearch sie einem Gleitkommawert zugeordnet. OpenSearch ordnet verschiedene Attribute dynamisch auf der Grundlage des ersten gesendeten Dokuments zu. Wenn Sie in DynamoDB eine Mischung aus Datentypen für dasselbe Attribut	DynamoDB unterstützt Zahlen.

Datentyp	OpenSearch	DynamoDB
	haben, z. B. sowohl eine ganze Zahl als auch eine Bruchzahl, schlägt die Zuordnung möglicherweise fehl. Wenn Ihr erstes Dokument beispielsweise ein Attribut hat, das eine ganze Zahl ist, und ein späteres Dokument dasselbe Attribut wie eine Bruchzahl hat, OpenSearch kann das zweite Dokument nicht aufgenommen werden. In diesen Fällen sollten Sie eine explizite Zuordnungsvorlage bereitstellen, z. B. die folgende: `{ "template": { "mappings": { "properties": { "MixedNumberAttribute": { "type": "float" } } } } }` Wenn Sie doppelte Genauigkeit benötigen, verwenden Sie eine Feldzuordnung vom Typ Zeichenfolge. Es gibt keinen äquivalenten numerischen Typ, der eine Genauigkeit von 38 Ziffern unterstützt. OpenSearch	

Datentyp	OpenSearch	DynamoDB
Zahlensatz	OpenSearch ordnet einen Zahlensatz automatisch einem Array von Langwerten oder Gleitkommawerten zu. Wie bei den Skalarzahlen hängt dies davon ab, ob es sich bei der ersten aufgenommenen Zahl um eine ganze Zahl oder um eine Bruchzahl handelt. Sie können Zuordnungen für Zahlensätze auf die gleiche Weise bereitstellen, wie Sie skalare Zeichenketten zuordnen.	DynamoDB unterstützt Typen, die Gruppen von Zahlen darstellen.
String	OpenSearch ordnet Zeichenkettenwerte automatisch als Text zu. In einigen Situationen, z. B. bei Aufzählungswerten, können Sie sie dem Schlüsselworttyp zuordnen. Das folgende Beispiel zeigt, wie ein benanntes DynamoDB-Attribut einem Schlüsselwort `PartType` zugeordnet wird OpenSearch . `{ "template": { "mappings": { "properties": { "PartType": { "type": "keyword" } } } } }`	DynamoDB unterstützt Zeichenketten.

Datentyp	OpenSearch	DynamoDB
Zeichenkettensatz	OpenSearch ordnet einen Zeichenkettensatz automatisch einem Zeichenketten-Array zu. Sie können Zuordnungen für Zeichenkettensätze auf die gleiche Weise bereitstellen, wie Sie skalare Zeichenketten zuordnen.	DynamoDB unterstützt Typen, die Sätze von Zeichenketten darstellen.
Binär	OpenSearch ordnet Binärdaten automatisch als Text zu. Sie können ein Mapping bereitstellen, in das Sie diese als Binärfelder schreiben können OpenSearch. Das folgende Beispiel zeigt, wie ein benanntes DynamoDB-Attribut einem `ImageData` OpenSearch Binärfeld zugeordnet wird. `{ "template": { "mappings": { "properties": { "ImageData": { "type": "binary" } } } } }`	DynamoDB unterstützt binäre Typattribute.
Binärer Satz	OpenSearch ordnet eine Binärmenge automatisch einem Array von Binärdaten als Text zu. Sie können Zuordnungen für Zahlensätze auf die gleiche Weise bereitstellen, wie Sie skalare Binärwerte zuordnen.	DynamoDB unterstützt Typen, die Sätze von Binärwerten darstellen.

Datentyp	OpenSearch	DynamoDB
Boolesch	OpenSearch ordnet einen booleschen DynamoDB-Typ einem booleschen Typ zu. OpenSearch	DynamoDB unterstützt Attribute vom Typ Boolean.
Null	OpenSearch kann Dokumente mit dem DynamoDB-Nulltyp aufnehmen. Es speichert den Wert als Nullwert im Dokument. Für diesen Typ gibt es keine Zuordnung, und dieses Feld ist weder indexiert noch durchsuchbar. Wenn derselbe Attributname für einen Null-Typ verwendet wird und später zu einem anderen Typ, wie z. B. einer Zeichenfolge, geändert OpenSearch wird, wird eine dynamische Zuordnung für den ersten Wert, der nicht Null ist, erstellt. Nachfolgende Werte können immer noch DynamoDB-Nullwerte sein.	DynamoDB unterstützt Attribute vom Typ Null.

Datentyp	OpenSearch	DynamoDB
Zuordnung	OpenSearch ordnet DynamoDB-Zuordnungsattribute verschachtelten Feldern zu. Dieselben Zuordnungen gelten für ein verschachteltes Feld. Das folgende Beispiel ordnet eine Zeichenfolge in einem verschachtelten Feld einem Schlüsselworttyp in zu: OpenSearch `{ "template": { "mappings": { "properties": { "AdditionalDescriptions": { "properties": { "PartType": { "type": "keyword" } } } } } } }`	DynamoDB unterstützt Map-Typ-Attribute.

Datentyp	OpenSearch	DynamoDB
Auflisten	OpenSearch liefert unterschiedliche Ergebnisse für DynamoDB-Listen, je nachdem, was in der Liste steht. Wenn eine Liste alle Skalartypen desselben Typs enthält (z. B. eine Liste aller Zeichenketten), wird die Liste als Array dieses Typs OpenSearch aufgenommen. Dies funktioniert für die Typen Zeichenfolge, Zahl, Boolean und Null. Die Einschränkungen für jeden dieser Typen sind dieselben wie die Einschränkungen für einen Skalar dieses Typs. Sie können auch Zuordnungen für Kartenlisten bereitstellen, indem Sie dieselbe Zuordnung verwenden, die Sie für eine Karte verwenden würden. Sie können keine Liste mit gemischten Typen bereitstellen.	DynamoDB unterstützt Listentypattribute.

Datentyp	OpenSearch	DynamoDB
Einstellen	OpenSearch liefert unterschiedliche Ergebnisse für DynamoDB-Sets, je nachdem, was in der Gruppe enthalten ist. Wenn eine Menge alle Skalartypen desselben Typs enthält (z. B. eine Menge aller Zeichenketten), wird die Menge als Array dieses Typs OpenSearch aufgenommen. Dies funktioniert für die Typen Zeichenfolge, Zahl, Boolean und Null. Die Einschränkungen für jeden dieser Typen sind dieselben wie die Einschränkungen für einen Skalar dieses Typs. Sie können auch Zuordnungen für Kartengruppen bereitstellen, indem Sie dieselbe Zuordnung verwenden, die Sie für eine Karte verwenden würden. Sie können keinen Satz gemischter Typen bereitstellen.	DynamoDB unterstützt Typen, die Mengen darstellen.

Wir empfehlen, dass Sie die Dead-Letter-Warteschlange (DLQ) in Ihrer Ingestion-Pipeline konfigurieren. OpenSearch Wenn Sie die Warteschlange konfiguriert haben, sendet OpenSearch Service alle fehlgeschlagenen Dokumente, die aufgrund von Fehlern bei der dynamischen Zuordnung nicht aufgenommen werden konnten, an die Warteschlange.

Falls automatische Zuordnungen fehlschlagen, können Sie `template_type` und `template_content` in Ihrer Pipeline-Konfiguration verwenden, um explizite Zuordnungsregeln zu definieren. Alternativ können Sie Zuordnungsvorlagen direkt in Ihrer Suchdomain oder Sammlung erstellen, bevor Sie die Pipeline starten.

Einschränkungen

Beachten Sie die folgenden Einschränkungen, wenn Sie eine OpenSearch Ingestion-Pipeline für DynamoDB einrichten:

- Die OpenSearch Ingestion-Integration mit DynamoDB unterstützt derzeit keine regionsübergreifende Aufnahme. Ihre DynamoDB-Tabelle und die OpenSearch Ingestion-Pipeline müssen identisch sein. AWS-Region
- Ihre DynamoDB-Tabelle und die OpenSearch Ingestion-Pipeline müssen identisch sein. AWS-Konto
- Eine OpenSearch Ingestion-Pipeline unterstützt nur eine DynamoDB-Tabelle als Quelle.
- DynamoDB Streams speichert Daten nur bis zu 24 Stunden in einem Protokoll. Wenn die Aufnahme von einem ersten Snapshot einer großen Tabelle 24 Stunden oder länger dauert, kommt es zu einem anfänglichen Datenverlust. Um diesen Datenverlust zu minimieren, schätzen Sie die Größe der Tabelle und konfigurieren Sie die entsprechenden Recheneinheiten der OpenSearch Datenerfassungspipelines.

Verwenden einer OpenSearch Ingestion-Pipeline mit Amazon DocumentDB

Sie können eine OpenSearch Ingestion-Pipeline mit Amazon DocumentDB verwenden, um Dokumentänderungen (wie Erstellen, Aktualisieren und Löschen) an Amazon OpenSearch Service-Domains und -Sammlungen zu streamen. Die OpenSearch Ingestion-Pipeline kann CDC-Mechanismen (Change Data Capture) nutzen, sofern sie in Ihrem Amazon DocumentDB-Cluster verfügbar sind, oder API-Abfragen, um eine hochskalierte Methode zum kontinuierlichen Streamen von Daten aus einem Amazon DocumentDB-Cluster mit niedriger Latenz bereitzustellen.

Es gibt zwei Möglichkeiten, Amazon DocumentDB als Quelle für die Verarbeitung von Daten zu verwenden — mit und ohne einen vollständigen anfänglichen Snapshot.

Ein vollständiger erster Snapshot ist eine Massenabfrage einer gesamten Amazon DocumentDB-Sammlung. Amazon DocumentDB lädt diesen Snapshot auf Amazon S3 hoch. Von dort aus sendet eine OpenSearch Ingestion-Pipeline ihn an einen Index in einer Domain oder partitioniert ihn in mehrere Indizes in einer Domain. Damit die Daten in Amazon DocumentDB OpenSearch konsistent bleiben, synchronisiert die Pipeline alle Erstellungs-, Aktualisierungs- und Löschereignisse in der Amazon DocumentDB-Sammlung mit den Dokumenten, die im OpenSearch Index oder den Indizes gespeichert sind.

Wenn Sie einen vollständigen Anfangssnapshot verwenden, nimmt Ihre OpenSearch Ingestion-Pipeline zuerst den Snapshot auf und beginnt dann, Daten aus Amazon DocumentDB DocumentDB-Change-Streams zu lesen. Es holt schließlich auf und gewährleistet nahezu in Echtzeit die Datenkonsistenz zwischen Amazon DocumentDB und. OpenSearch

Sie können auch die OpenSearch Ingestion-Integration mit Amazon DocumentDB verwenden, um Ereignisse ohne Snapshot zu streamen. Wählen Sie diese Option, wenn Sie bereits einen vollständigen Snapshot von einem anderen Mechanismus haben oder wenn Sie nur aktuelle Ereignisse aus einer Amazon DocumentDB-Sammlung mit Change-Streams streamen möchten.

Bei beiden Optionen müssen Sie einen Change-Stream in Ihrer Amazon DocumentDB-Sammlung aktivieren, wenn Sie einen Stream in Ihrer Pipeline-Konfiguration aktivieren. Wenn Sie nur Volllast oder Export verwenden, müssen Sie keinen Change-Stream aktivieren.

Voraussetzungen

Bevor Sie Ihre OpenSearch Ingestion-Pipeline erstellen, führen Sie die folgenden Schritte aus:

1. Erstellen Sie einen Amazon DocumentDB-Cluster mit der Berechtigung zum Lesen von Daten, indem Sie die Schritte unter Erstellen eines Amazon DocumentDB-Clusters im Amazon DocumentDB DocumentDB-Entwicklerhandbuch befolgen. Wenn Sie eine CDC-Infrastruktur verwenden, stellen Sie sicher, dass Sie Ihren Amazon DocumentDB-Cluster für die Veröffentlichung von Change-Streams konfigurieren.
2. Richten Sie die Authentifizierung in Ihrem Amazon DocumentDB-Cluster mit AWS Secrets Manager ein. Aktivieren Sie die Rotation von Geheimnissen, indem Sie die Schritte unter Automatisches Rotieren von Passwörtern für Amazon DocumentDB befolgen. Weitere Informationen finden Sie unter Datenbankzugriff mit rollenbasierter Zugriffskontrolle und Sicherheit in Amazon DocumentDB.
3. Wenn Sie einen Change-Stream verwenden, um Datenänderungen in Ihrer Amazon DocumentDB-Sammlung zu abonnieren, vermeiden Sie Datenverlust, indem Sie den Aufbewahrungszeitraum mithilfe des `change_stream_log_retention_duration` Parameters auf bis zu 7 Tage verlängern. Change-Streams-Ereignisse werden standardmäßig für 3 Stunden gespeichert, nachdem das Ereignis aufgezeichnet wurde, was für große Sammlungen nicht ausreichend ist. Informationen zum Ändern der Aufbewahrungsdauer von Change-Stream-Protokollen finden Sie unter Aufbewahrungsdauer für Change-Stream-Protokolle ändern.
4. Erstellen Sie eine OpenSearch Dienstdomäne oder eine OpenSearch serverlose Sammlung. Weitere Informationen finden Sie unter OpenSearch Dienstdomänen erstellen und Sammlungen erstellen.

5. Fügen Sie Ihrer Domain eine ressourcenbasierte Richtlinie oder Ihrer Sammlung eine Datenzugriffsrichtlinie hinzu. Diese Zugriffsrichtlinien ermöglichen es OpenSearch Ingestion, Daten aus Ihrem Amazon DocumentDB-Cluster in Ihre Domain oder Sammlung zu schreiben.

   Die folgende Beispielrichtlinie für den Domänenzugriff ermöglicht es der Pipeline-Rolle, die Sie im nächsten Schritt erstellen, Daten in eine Domain zu schreiben. Stellen Sie sicher, dass Sie das `resource` mit Ihrem eigenen ARN aktualisieren.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::{pipeline-account-id}:role/pipeline-role"
      },
      "Action": [
        "es:DescribeDomain",
        "es:ESHttp*"
      ],
      "Resource": [
        "arn:aws:es:{region}:{account-id}:domain/domain-name"
      ]
    }
  ]
}
```

   Informationen zum Erstellen einer IAM-Rolle mit den richtigen Berechtigungen für den Zugriff auf Schreibdaten für die Sammlung oder Domain finden Sie unter Erforderliche Berechtigungen für Domänen und Erforderliche Berechtigungen für Sammlungen.

Schritt 1: Konfigurieren Sie die Pipeline-Rolle

Nachdem Sie die Voraussetzungen für Ihre Amazon DocumentDB-Pipeline eingerichtet haben, konfigurieren Sie die Pipeline-Rolle, die Sie in Ihrer Pipeline-Konfiguration verwenden möchten, und fügen Sie der Rolle die folgenden Amazon DocumentDB DocumentDB-Berechtigungen hinzu:

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Sid": "allowS3ListObjectAccess",
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::{s3_bucket}"
            ],
            "Condition": {
                "StringLike": {
                    "s3:prefix": "{s3_prefix}/*"
                }
            }
        },
        {
            "Sid": "allowReadAndWriteToS3ForExportStream",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::{s3_bucket}/{s3_prefix}/*"
            ]
        },
        {
            "Sid": "SecretsManagerReadAccess",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": ["arn:aws:secretsmanager:{region}:{account-id}:secret:secret-
name"]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachNetworkInterface",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteNetworkInterfacePermission",
```

```
                "ec2:DetachNetworkInterface",
                "ec2:DescribeNetworkInterfaces"
            ],
            "Resource": [
                "arn:aws:ec2:*:{account-id}:network-interface/*",
                "arn:aws:ec2:*:{account-id}:subnet/*",
                "arn:aws:ec2:*:{account-id}:security-group/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:Describe*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
               "StringEquals":
                    {
                        "aws:RequestTag/OSISManaged": "true"
                    }
            }
        }
    ]
}
```

Sie müssen die oben genannten Amazon EC2 EC2-Berechtigungen für die IAM-Rolle bereitstellen, mit der Sie die OpenSearch Ingestion-Pipeline erstellen, da die Pipeline diese Berechtigungen verwendet, um eine Netzwerkschnittstelle in Ihrer VPC zu erstellen und zu löschen. Die Pipeline kann nur über diese Netzwerkschnittstelle auf den Amazon DocumentDB-Cluster zugreifen.

Schritt 2: Erstellen Sie die Pipeline

Anschließend können Sie eine OpenSearch Ingestion-Pipeline wie die folgende konfigurieren, die Amazon DocumentDB als Quelle spezifiziert. Beachten Sie, dass die `getMetadata` Funktion zum Auffüllen des Indexnamens einen Metadatenschlüssel verwendet*`documentdb_collection`*. Wenn Sie einen anderen Indexnamen ohne die `getMetadata` Methode verwenden möchten, können Sie die Konfiguration `index: "`*`my_index_name`*`"` verwenden.

```
version: "2"
documentdb-pipeline:
  source:
    documentdb:
      acknowledgments: true
      host: "https://docdb-cluster-id.us-east-1.docdb.amazonaws.com"
      port: 27017
      authentication:
        username: ${aws_secrets:secret:username}
        password: ${aws_secrets:secret:password}
      aws:
        sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
      s3_bucket: "bucket-name"
      s3_region: "bucket-region"
      s3_prefix: "path" #optional path for storing the temporary data
      collections:
        - collection: "dbname.collection"
          export: true
          stream: true
  sink:
  - opensearch:
      hosts: ["https://search-mydomain.us-east-1.es.amazonaws.com"]
      index: "${getMetadata(\"documentdb_collection\")}"
      index_type: custom
      document_id: "${getMetadata(\"primary_key\")}"
      action: "${getMetadata(\"opensearch_action\")}"
      document_version: "${getMetadata(\"document_version\")}"
      document_version_type: "external"
extension:
  aws:
    secrets:
      secret:
        secret_id: "my-docdb-secret"
        region: "us-east-1"
        sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
```

```
        refresh_interval: PT1H
```

Sie können einen vorkonfigurierten Amazon DocumentDB-Blueprint verwenden, um diese Pipeline zu erstellen. Weitere Informationen finden Sie unter the section called “Verwenden von Blueprints zum Erstellen einer Pipeline”.

Wenn Sie die verwenden, AWS Management Console um Ihre Pipeline zu erstellen, müssen Sie Ihre Pipeline auch an Ihre VPC anhängen, um Amazon DocumentDB als Quelle verwenden zu können. Suchen Sie dazu den Abschnitt Netzwerkkonfiguration, aktivieren Sie das Kontrollkästchen An VPC anhängen und wählen Sie Ihr CIDR aus einer der bereitgestellten Standardoptionen oder wählen Sie Ihre eigene aus.

Um ein benutzerdefiniertes CIDR bereitzustellen, wählen Sie im Dropdownmenü die Option Andere aus. Um eine Kollision der IP-Adressen zwischen OpenSearch Ingestion und Amazon DocumentDB zu vermeiden, stellen Sie sicher, dass sich die Amazon DocumentDB VPC CIDR von der CIDR für Ingestion unterscheidet. OpenSearch

Weitere Informationen finden Sie unter VPC-Zugriff für eine Pipeline konfigurieren.

Datenkonsistenz

Die Pipeline gewährleistet die Datenkonsistenz, indem sie kontinuierlich Änderungen vom Amazon DocumentDB-Cluster abfragt oder empfängt und die entsprechenden Dokumente im OpenSearch Index aktualisiert.

OpenSearch Die Datenaufnahme unterstützt die end-to-end Bestätigung, um die Beständigkeit der Daten sicherzustellen. Wenn eine Pipeline Snapshots oder Streams liest, erstellt sie dynamisch Partitionen für die Parallelverarbeitung. Die Pipeline markiert eine Partition als abgeschlossen, wenn sie nach der Aufnahme aller Datensätze in der OpenSearch Domäne oder Sammlung eine Bestätigung erhält.

Wenn Sie Daten in eine OpenSearch serverlose Suchsammlung aufnehmen möchten, können Sie in der Pipeline eine Dokument-ID generieren. Wenn Sie Daten in eine OpenSearch serverlose Zeitreihensammlung aufnehmen möchten, beachten Sie, dass die Pipeline keine Dokument-ID generiert. Daher müssen Sie diese `document_id: "${getMetadata(\"primary_key\")}"` in Ihrer Pipeline-Senkenkonfiguration weglassen.

Eine OpenSearch Ingestion-Pipeline ordnet auch eingehende Ereignisaktionen entsprechenden Massenindizierungsaktionen zu, um das Ingestieren von Dokumenten zu erleichtern. Dadurch bleiben

die Daten konsistent, sodass jede Datenänderung in Amazon DocumentDB mit den entsprechenden Dokumentänderungen in abgeglichen wird. OpenSearch

Datentypen zuordnen

OpenSearch Der Service ordnet Datentypen in jedem eingehenden Dokument dynamisch dem entsprechenden Datentyp in Amazon DocumentDB zu. Die folgende Tabelle zeigt, wie OpenSearch Service verschiedene Datentypen automatisch zuordnet.

Datentyp	OpenSearch	Amazon DocumentDB
Ganzzahl	OpenSearch ordnet Amazon DocumentDB DocumentDB-Integer-Werte automatisch OpenSearch Ganzzahlen zu. OpenSearch ordnet das Feld dynamisch auf der Grundlage des ersten gesendeten Dokuments zu. Wenn Sie eine Mischung von Datentypen für dasselbe Attribut in Amazon DocumentDB haben, schlägt die automatische Zuordnung möglicherweise fehl. Wenn Ihr erstes Dokument beispielsweise ein Long-Attribut hat und ein späteres Dokument dasselbe Attribut als Ganzzahl hat, OpenSearch kann das zweite Dokument nicht aufgenommen werden. In diesen Fällen sollten Sie eine explizite Zuordnungsvorlage bereitstellen, die den flexibelsten Zahlentyp auswählt, z. B. den folgenden: `{ "template": { "mappings": { "properties": { "MixedNumberField": { "type": "float"`	Amazon DocumentDB unterstützt Ganzzahlen.

Datentyp	OpenSearch	Amazon DocumentDB
	`}` `}` `}` `}` `}`	

Datentyp	OpenSearch	Amazon DocumentDB
Long	OpenSearch ordnet Amazon DocumentDB DocumentDB-Long-Werte automatisch OpenSearch Long-Werten zu. OpenSearch ordnet das Feld dynamisch auf der Grundlage des ersten gesendeten Dokuments zu. Wenn Sie eine Mischung von Datentypen für dasselbe Attribut in Amazon DocumentDB haben, schlägt die automatische Zuordnung möglicherweise fehl. Wenn Ihr erstes Dokument beispielsweise ein Long-Attribut hat und ein späteres Dokument dasselbe Attribut als Ganzzahl hat, OpenSearch kann das zweite Dokument nicht aufgenommen werden. In diesen Fällen sollten Sie eine explizite Zuordnungsvorlage bereitstellen, die den flexibelsten Zahlentyp auswählt, z. B. den folgenden: `{ "template": { "mappings": { "properties": { "MixedNumberField": { "type": "float" } } } } }`	Amazon DocumentDB unterstützt Longs.

Datentyp	OpenSearch	Amazon DocumentDB
String	OpenSearch ordnet Zeichenkettenwerte automatisch als Text zu. In einigen Situationen, z. B. bei Aufzählungswerten, können Sie sie dem Schlüsselworttyp zuordnen. Das folgende Beispiel zeigt, wie ein Amazon DocumentDB-Attribut mit dem Namen einem OpenSearch Schlüssel wort `PartType` zugeordnet wird. `{ "template": { "mappings": { "properties": { "PartType": { "type": "keyword" } } } } }`	Amazon DocumentDB unterstützt Zeichenketten.

Datentyp	OpenSearch	Amazon DocumentDB
Double	OpenSearch ordnet Amazon DocumentDB DocumentDB-Doppelwerte automatisch OpenSearch Doubles zu. OpenSearch ordnet das Feld dynamisch auf der Grundlage des ersten gesendeten Dokuments zu. Wenn Sie eine Mischung von Datentypen für dasselbe Attribut in Amazon DocumentDB haben, schlägt die automatische Zuordnung möglicherweise fehl. Wenn Ihr erstes Dokument beispielsweise ein Long-Attribut hat und ein späteres Dokument dasselbe Attribut als Ganzzahl hat, OpenSearch kann das zweite Dokument nicht aufgenommen werden. In diesen Fällen sollten Sie eine explizite Zuordnungsvorlage bereitstellen, die den flexibelsten Zahlentyp auswählt, z. B. den folgenden: `{ "template": { "mappings": { "properties": { "MixedNumberField": { "type": "float" } } } } }`	Amazon DocumentDB unterstützt Doubles.

Datentyp	OpenSearch	Amazon DocumentDB
Datum	Standardmäßig wird das Datum einer Ganzzahl in zugeordnet. OpenSearch Sie können eine benutzerdefinierte Zuordnungsvorlage definieren, um ein Datum einem OpenSearch Datum zuzuordnen. `{ "template": { "mappings": { "properties": { "myDateField": { "type": "date", "format": "epoch_second" } } } } }`	Amazon DocumentDB unterstützt Datumsangaben.

Datentyp	OpenSearch	Amazon DocumentDB
Zeitstempel	Standardmäßig wird der Zeitstempel einer Ganzzahl in zugeordnet. OpenSearch Sie können eine benutzerdefinierte Zuordnungsvorlage definieren, um ein Datum einem Datum zuzuordnen. OpenSearch `{ "template": { "mappings": { "properties": { "myTimestampField": { "type": "date", "format": "epoch_second" } } } } }`	Amazon DocumentDB unterstützt Zeitstempel.
Boolesch	OpenSearch ordnet einen booleschen Amazon DocumentDB-Typ einem OpenSearch booleschen Typ zu.	Amazon DocumentDB unterstützt Attribute vom Typ Boolean.

Datentyp	OpenSearch	Amazon DocumentDB
Dezimal	OpenSearch ordnet Amazon DocumentDB DocumentDB-Zuordnungsattribute verschachtelten Feldern zu. Dieselben Zuordnungen gelten für ein verschachteltes Feld. Das folgende Beispiel ordnet eine Zeichenfolge in einem verschachtelten Feld einem Schlüsselworttyp in zu: OpenSearch `{ "template": { "mappings": { "properties": { "myDecimalField": { "type": "double" } } } } }` Mit dieser benutzerdefinierten Zuordnung können Sie das Feld mit doppelter Genauigkeit abfragen und aggregieren. Der ursprüngliche Wert behält die volle Genauigkeit in der `_source` Eigenschaft des OpenSearch Dokuments bei. Ohne diese Zuordnung wird standardmäßig Text OpenSearch verwendet.	Amazon DocumentDB unterstützt Dezimalzahlen.

Datentyp	OpenSearch	Amazon DocumentDB
Regulärer Ausdruck	Der Regex-Typ erstellt verschachtelte Felder. Dazu gehören und. *<myFieldName>* `.pattern` *<myFieldName>* `.options`	Amazon DocumentDB unterstützt reguläre Ausdrücke.
Binäre Daten	OpenSearch ordnet Amazon DocumentDB-Binärdaten automatisch OpenSearch Text zu. Sie können eine Zuordnung angeben, in OpenSearch die Sie diese als Binärfelder schreiben können. Das folgende Beispiel zeigt, wie ein `imageData` benanntes Amazon DocumentDB-Feld einem OpenSearch Binärfeld zugeordnet wird. `{ "template": { "mappings": { "properties": { "imageData": { "type": "binary" } } } } }`	Amazon DocumentDB unterstützt binäre Datenfelder.
ObjectId	Felder mit einem ObjectID-Typ werden OpenSearch Textfeldern zugeordnet. Der Wert entspricht der Zeichenkettendarstellung der ObjectID.	Amazon DocumentDB unterstützt ObjectIDs.

Datentyp	OpenSearch	Amazon DocumentDB
Null	OpenSearch kann Dokumente mit dem Nulltyp Amazon DocumentDB aufnehmen. Es speichert den Wert als Nullwert im Dokument. Für diesen Typ gibt es keine Zuordnung, und dieses Feld ist weder indexiert noch durchsuchbar. Wenn derselbe Attributname für einen Null-Typ verwendet wird und später zu einem anderen Typ, wie z. B. einer Zeichenfolge, geändert OpenSearch wird, wird eine dynamische Zuordnung für den ersten Wert, der nicht Null ist, erstellt. Nachfolgende Werte können immer noch Nullwerte von Amazon DocumentDB sein.	Amazon DocumentDB unterstützt Felder vom Typ Null.
Undefined	OpenSearch kann Dokumente mit dem undefinierten Typ Amazon DocumentDB aufnehmen. Es speichert den Wert als Nullwert im Dokument. Für diesen Typ gibt es keine Zuordnung, und dieses Feld ist weder indexiert noch durchsuchbar. Wenn derselbe Feldname für einen undefinierten Typ verwendet wird und später zu einem anderen Typ, z. B. einer Zeichenfolge, geändert OpenSearch wird, wird eine dynamische Zuordnung für den ersten nicht definierten Wert erstellt. Nachfolgende Werte können immer noch undefinierte Amazon DocumentDB DocumentDB-Werte sein.	Amazon DocumentDB unterstützt undefinierte Typfelder.

Datentyp	OpenSearch	Amazon DocumentDB
MinKey	OpenSearch kann Dokumente mit dem MinKey-Typ Amazon DocumentDB aufnehmen. Es speichert den Wert als Nullwert im Dokument. Für diesen Typ gibt es keine Zuordnung, und dieses Feld ist weder indexiert noch durchsuch bar. Wenn derselbe Feldname für einen MinKey-Typ verwendet wird und später zu einem anderen Typ, z. B. einer Zeichenfolge, geändert OpenSearch wird, wird eine dynamische Zuordnung für den ersten Nicht-Minkey-Wert erstellt. Nachfolgende Werte können immer noch Amazon DocumentDB MinKey-Werte sein.	Amazon DocumentDB unterstützt Felder vom Typ MinKey.
MaxKey	OpenSearch kann Dokumente mit dem Typ Amazon DocumentDB MaxKey aufnehmen. Es speichert den Wert als Nullwert im Dokument. Für diesen Typ gibt es keine Zuordnung, und dieses Feld ist weder indexiert noch durchsuch bar. Wenn derselbe Feldname für einen MaxKey-Typ verwendet wird und später zu einem anderen Typ, z. B. einer Zeichenfolge, geändert OpenSearch wird, wird eine dynamische Zuordnung für den ersten Nicht-MaxKey-Wert erstellt. Nachfolgende Werte können weiterhin Amazon DocumentDB MaxKey-Werte sein.	Amazon DocumentDB unterstützt Felder vom Typ MaxKey.

Wir empfehlen Ihnen, die Dead-Letter-Warteschlange (DLQ) in Ihrer Ingestion-Pipeline zu konfigurieren. OpenSearch Wenn Sie die Warteschlange konfiguriert haben, sendet OpenSearch Service alle fehlgeschlagenen Dokumente, die aufgrund von Fehlern bei der dynamischen Zuordnung nicht aufgenommen werden konnten, an die Warteschlange.

Falls automatische Zuordnungen fehlschlagen, können Sie `template_type` und `template_content` in Ihrer Pipeline-Konfiguration verwenden, um explizite Zuordnungsregeln zu definieren. Alternativ können Sie Zuordnungsvorlagen direkt in Ihrer Suchdomain oder Sammlung erstellen, bevor Sie die Pipeline starten.

Einschränkungen

Beachten Sie die folgenden Einschränkungen, wenn Sie eine OpenSearch Ingestion-Pipeline für Amazon DocumentDB einrichten:

- Die OpenSearch Ingestion-Integration mit Amazon DocumentDB unterstützt derzeit keine regionsübergreifende Aufnahme. Ihr Amazon DocumentDB-Cluster und Ihre OpenSearch Ingestion-Pipeline müssen identisch sein. AWS-Region
- Die OpenSearch Ingestion-Integration mit Amazon DocumentDB unterstützt derzeit keine kontoübergreifende Erfassung. Ihr Amazon DocumentDB-Cluster und Ihre OpenSearch Ingestion-Pipeline müssen identisch sein. AWS-Konto
- Eine OpenSearch Ingestion-Pipeline unterstützt nur einen Amazon DocumentDB-Cluster als Quelle.
- Die OpenSearch Ingestion-Integration mit Amazon DocumentDB unterstützt speziell instanzbasierte Amazon DocumentDB-Cluster. Elastische Amazon DocumentDB-Cluster werden nicht unterstützt.
- Die OpenSearch Ingestion-Integration wird nur AWS Secrets Manager als Authentifizierungsmechanismus für Ihren Amazon DocumentDB-Cluster unterstützt.
- Sie können die bestehende Pipeline-Konfiguration nicht aktualisieren, um Daten aus einer anderen Datenbank oder Sammlung aufzunehmen. Stattdessen müssen Sie eine neue Pipeline erstellen.

Verwendung einer OpenSearch Ingestion-Pipeline mit der Confluent Kafka Cloud

Sie können Confluent Kafka als Quelle in OpenSearch Ingestion verwenden, um Daten von einem Confluent Kafka-Cluster in eine Amazon Service-Domain oder eine Amazon OpenSearch Serverless-

Sammlung zu streamen. OpenSearch OpenSearch Ingestion unterstützt die Verarbeitung von Streaming-Daten aus selbstverwaltetem Kafka in öffentlichen und privaten Netzwerkräumen.

Konnektivität zur öffentlichen Kafka-Cloud von Confluent

Sie können OpenSearch Ingestion-Pipelines verwenden, um Daten aus einem Confluent-Kafka-Cluster mit öffentlicher Konfiguration zu streamen (der DNS-Name des Bootstrap-Servers muss öffentlich aufgelöst werden). Dazu benötigen Sie eine OpenSearch Ingestion-Pipeline, einen konfluenten Kafka-Cluster als Quelle und eine Amazon OpenSearch Service-Domain oder eine Amazon OpenSearch Serverless-Sammlung als Ziel.

Um Daten zu migrieren, benötigen Sie Folgendes:

- Ein Confluent-Kafka-Cluster, der als Quelle fungiert. Der Cluster sollte die Daten enthalten, die Sie migrieren möchten.
- Eine Amazon OpenSearch Service-Domain oder eine Amazon OpenSearch Serverless-Sammlung, die als Ziel dient.
- Für den Kafka-Cluster sollte die Authentifizierung mit den Anmeldeinformationen von aktiviert sein. AWS Secrets Manager

Voraussetzungen

Um die AWS Secrets Manager basierte Authentifizierung auf Ihrem selbstverwalteten OpenSearch oder Elasticsearch-Quellcluster zu aktivieren, müssen Sie

- Richten Sie die Authentifizierung auf Ihrem Confluent-Kafka-Cluster ein, AWS Secrets Manager indem Sie die Schritte unter Rotate Secrets befolgen. AWS Secrets Manager
- Erstellen Sie eine Pipeline-Rolle in IAM mit der Berechtigung, in eine Amazon OpenSearch Service-Domain oder eine Amazon OpenSearch Serverless-Sammlung zu schreiben. Sie müssen auch die Berechtigung zum Lesen der Anmeldeinformationen angeben. AWS Secrets Manager So gehen Sie vor:
  - Fügen Sie Ihrer Amazon OpenSearch Service-Domain eine ressourcenbasierte Richtlinie oder Ihrer Sammlung eine Datenzugriffsrichtlinie hinzu. Diese Zugriffsrichtlinien ermöglichen es OpenSearch Ingestion, Daten aus Ihrem selbstverwalteten OpenSearch oder Elasticsearch-Quellcluster in Ihre Amazon OpenSearch Service-Domain oder Ihre Amazon Serverless-Sammlung zu schreiben. OpenSearch
- Erstellen Sie eine OpenSearch Ingestion-Pipeline, indem Sie sich auf den Blueprint beziehen.

Nachdem Sie diese Schritte abgeschlossen haben, beginnt Ihre Pipeline automatisch mit der Verarbeitung der Daten aus Ihrem Quell-Cluster und nimmt sie in Ihre Amazon OpenSearch Service-Domain oder Ihr Amazon OpenSearch Serverless-Sammelziel auf. Sie können verschiedene Prozessoren in der OpenSearch Ingestion-Pipeline verwenden, um beliebige Transformationen an den aufgenommenen Daten durchzuführen.

IAM-Rollen und -Berechtigungen

Die folgende Beispielrichtlinie für den Domänenzugriff ermöglicht es der Pipeline-Rolle, die Sie im nächsten Schritt erstellen, Daten in eine Amazon OpenSearch Service-Domain zu schreiben. Stellen Sie sicher, dass Sie die Ressource mit Ihrem eigenen ARN aktualisieren.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::{pipeline-account-id}:role/pipeline-role"
      },
      "Action": [
        "es:DescribeDomain",
        "es:ESHttp*"
      ],
      "Resource": [
        "arn:aws:es:{region}:{account-id}:domain/domain-name"
      ]
    }
  ]
}
```

Für die Verwaltung der Netzwerkschnittstelle ist die folgende Berechtigung erforderlich:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachNetworkInterface",
```

```
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteNetworkInterfacePermission",
                "ec2:DetachNetworkInterface",
                "ec2:DescribeNetworkInterfaces"
            ],
            "Resource": [
                "arn:aws:ec2:*:{account-id}:network-interface/*",
                "arn:aws:ec2:*:{account-id}:subnet/*",
                "arn:aws:ec2:*:{account-id}:security-group/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:Describe*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [ "ec2:CreateTags" ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
               "StringEquals": { "aws:RequestTag/OSISManaged": "true" }
            }
        }
    ]
}
```

Die folgende Berechtigung ist erforderlich, um Geheimnisse aus dem AWS Secrets Manager Dienst zu lesen:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Sid": "SecretsManagerReadAccess",
            "Effect": "Allow",
            "Action": ["secretsmanager:GetSecretValue"],
            "Resource": ["arn:aws:secretsmanager:<region>:<account-id>:secret:<secret-
name>"]
        }
    ]
}
```

Die folgenden Berechtigungen sind erforderlich, um in eine Amazon OpenSearch Service-Domain zu schreiben:

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::{your-account-id}:role/{pipeline-role}"
      },
      "Action": ["es:DescribeDomain", "es:ESHttp*"],
      "Resource": "arn:aws:es:{region}:{your-account-id}:domain/{domain-name}/*"
    }
  ]
}
```

Eine Pipeline erstellen

Nachdem Sie die Richtlinie an die Pipeline-Rolle angehängt haben, verwenden Sie den Datenmigrationspipeline-Blueprint von Confluent Kafka, um die Pipeline zu erstellen. Dieser Blueprint enthält eine Standardkonfiguration für die Migration von Daten zwischen Kafka und Ihrem Ziel.

- Sie können mehrere Amazon OpenSearch Service-Domains als Ziele für Ihre Daten angeben. Diese Funktion ermöglicht das bedingte Routing oder die Replikation eingehender Daten in mehrere Amazon OpenSearch Servicedomains.
- Sie können Daten von einem Confluent Kafka-Quellcluster zu einer Amazon OpenSearch Serverless VPC-Sammlung migrieren. Stellen Sie sicher, dass Sie in der Pipeline-Konfiguration eine Netzwerkzugriffsrichtlinie angeben.
- Sie können die Confluent Schema Registry verwenden, um ein Confluent-Schema zu definieren.

Die folgende Beispiel-Pipeline nimmt Daten aus einem Confluent-Kafka-Cluster in eine Amazon Service-Domain auf: OpenSearch

```
version: "2"
kafka-pipeline:
  source:
    kafka:
      # Encryption is always required
      encryption:
        type: "ssl"
      topics:
        - name: "topic_4"
          group_id: "demoGroup"
      bootstrap_servers:
        # TODO: for public confluent kafka use public booststrap server dns
        - "<<bootstrap-server>>.us-west-2.aws.private.confluent.cloud:9092"
      authentication:
        sasl:
          plain:
            username: "${{aws_secrets:confluent-kafka-secret:username}}"
            password: "${{aws_secrets:confluent-kafka-secret:password}}"
      # Schema is optional
      schema:
        type: confluent
        registry_url: https://<<registry-url>>.us-west-2.aws.confluent.cloud
        api_key: "${{aws_secrets:schema-secret:schema_registry_api_key}}"
        api_secret: "${{aws_secrets:schema-secret:schema_registry_api_secret}}"
        basic_auth_credentials_source: "USER_INFO"
sink:
    - opensearch:
        hosts: [ "https://<<opensearchdomain>>.us-west-2.es.amazonaws.com" ]
        index: "enterprise-confluent-demo"
        aws:
          sts_role_arn: "arn:aws:iam::1234567890:role/os-os-test-role"
          region: "<<aws-region>>"
 extension:
  aws:
    secrets:
      confluent-kafka-secret:
        secret_id: "enterprise-kafka-credentials"
        region: "<<aws-region>>"
        sts_role_arn: "arn:aws:iam::1234567890:role/os-os-test-role"
      schema-secret:
```

```
        secret_id: "self-managed-kafka-schema"
        region: "<<aws-region>>"
        sts_role_arn: "arn:aws:iam::1234567890:role/os-os-test-role"
```

Konnektivität zur Confluent Kafka Cloud in VPC

Sie können OpenSearch Ingestion-Pipelines verwenden, um Daten aus einem Confluent-Kafka-Cluster mit öffentlicher Konfiguration zu streamen. Richten Sie dazu eine OpenSearch Ingestion-Pipeline mit Confluent Kafka als Quelle und einer Amazon OpenSearch Service-Domain oder einer Amazon OpenSearch Serverless-Sammlung als Ziel ein. Die Pipeline verarbeitet alle Streaming-Daten aus Ihrem Kafka-Cluster und nimmt die Daten in den Zielcluster auf.

Confluent Kafka-Netzwerkkonfiguration

OpenSearch Ingestion unterstützt Confluent Kafka-Cluster, die in allen unterstützten Netzwerkmodi in Confluent konfiguriert sind. Die folgenden Modi der Netzwerkkonfiguration werden als Quelle in Ingestion unterstützt. OpenSearch

- AWS VPC-Peering
- AWS PrivateLink für dedizierte Cluster
- AWS PrivateLink für Unternehmenscluster
- AWS Transit Gateway

Sie können Confluent Managed Kafka als Quelle für die Erfassung von Daten aus einer Confluent-Cloud verwenden. Um dies zu erreichen, richten Sie eine Pipeline ein, in der Sie Kafka als Quelle und eine Amazon OpenSearch Service-Domain oder Amazon OpenSearch Serverless Collection als Senke konfigurieren. Dies erleichtert die Migration von Daten von Kafka zum angegebenen Ziel. Die Migration unterstützt auch die Verwendung einer konfluenten Registrierung oder gar keiner Registrierung.

Um die Datenmigration durchzuführen, benötigen Sie die folgenden Ressourcen:

- Ein Confluent-Kafka-Cluster, der als Quelle fungiert und die Daten enthält, die Sie migrieren möchten.
- Ein Zielziel, z. B. eine Amazon OpenSearch Service-Domain oder eine Amazon OpenSearch Serverless-Sammlung als Senke.
- Eine VPC-ID von Amazon VPC, die Zugriff auf Confluent VPC hat.

- Für den Kafka-Cluster sollte die Authentifizierung mit den Anmeldeinformationen von aktiviert sein. AWS Secrets Manager

Voraussetzungen

Um die Aufnahme auf Ihrem Kafka-Cluster einzurichten, ist Folgendes erforderlich:

- Sie müssen die AWS Secrets Manager basierte Authentifizierung auf Ihrem Kafka-Cluster aktivieren.
  - Richten Sie die Authentifizierung auf Ihrem Kafka-Cluster mit ein. AWS Secrets Manager Aktivieren Sie die Rotation von Geheimnissen, indem Sie die Schritte unter AWS Secrets Manager Geheimnisse rotieren befolgen.
- Sie müssen den VPC-CIDR angeben, der vom OpenSearch Ingestion-Dienst verwendet werden soll.
  - Wenn Sie die AWS Management Console verwenden, um Ihre Pipeline zu erstellen, müssen Sie auch die Amazon OpenSearch Ingestion-Pipeline an Ihre VPC anhängen, um Confluent Kafka als Quelle verwenden zu können. Suchen Sie dazu den Abschnitt Netzwerkkonfiguration, aktivieren Sie das Kontrollkästchen An VPC anhängen und wählen Sie Ihr CIDR aus oder geben Sie manuell ein beliebiges /24 CIDR ein, das von der Erfassung verwendet werden soll. OpenSearch Das CIDR, das von OpenSearch Ingestion verwendet werden soll, sollte sich von dem VPC-CIDR unterscheiden, auf dem das von Confluent verwaltete Kafka ausgeführt wird. Weitere Informationen zu Confluent Kafka CIDR, die Sie vermeiden sollten, finden Sie hier. Im Folgenden finden Sie die Standard-CIDR-Optionen, die vom OpenSearch Ingestion Service zur Herstellung von Netzwerkkonnektivität verwendet werden können.
    - 10.99.20.0/24
    - 192.168.36,0/24
    - 172,21,56,0/24
- Sie müssen in IAM eine Pipeline-Rolle mit Berechtigungen für die Amazon OpenSearch Service-Domain oder Amazon OpenSearch Serverless Collection und der Berechtigung zum Lesen der Geheimnisse erstellen. AWS Secrets Manager
  - Fügen Sie Ihrer Amazon OpenSearch Servicedomain eine ressourcenbasierte Richtlinie oder Ihrer Sammlung eine Amazon OpenSearch Serverless-Datenzugriffsrichtlinie hinzu. Diese Zugriffsrichtlinien ermöglichen es OpenSearch Ingestion, Daten von Ihrem Kafka in Ihre Amazon OpenSearch Service-Domain oder Amazon OpenSearch Serverless-Sammlung zu schreiben.

- Für Confluent Kafka mit Konnektivität konfigurieren Sie AWS PrivateLink

  VPC-DHCP-Optionen. DNS-Hostnamen und DNS-Auflösung sollten aktiviert sein.

  - Domainname: aws.private.confluent.cloud

    domain-name-servers: Amazon hat DNS bereitgestellt

IAM-Rollen und -Berechtigungen

Die folgende Beispielrichtlinie für den Domänenzugriff ermöglicht es der Pipeline-Rolle, Daten in eine Amazon OpenSearch Service-Domain zu schreiben.

> **Note**
>
> Sie müssen das `resource` mit Ihrem eigenen ARN aktualisieren.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::{pipeline-account-id}:role/pipeline-role"
      },
      "Action": [
        "es:DescribeDomain",
        "es:ESHttp*"
      ],
      "Resource": [
        "arn:aws:es:{region}:{account-id}:domain/domain-name"
      ]
    }
  ]
}
```

Das folgende Beispiel enthält die für die Verwaltung Ihrer Netzwerkschnittstelle erforderlichen Berechtigungen:

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachNetworkInterface",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteNetworkInterfacePermission",
                "ec2:DetachNetworkInterface",
                "ec2:DescribeNetworkInterfaces"
            ],
            "Resource": [
                "arn:aws:ec2:*:{account-id}:network-interface/*",
                "arn:aws:ec2:*:{account-id}:subnet/*",
                "arn:aws:ec2:*:{account-id}:security-group/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:Describe*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [ "ec2:CreateTags" ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
               "StringEquals": { "aws:RequestTag/OSISManaged": "true" }
            }
        }
    ]
```

Das folgende Beispiel bietet Berechtigungen, die zum Lesen von Geheimnissen erforderlich sind AWS Secrets Manager:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SecretsManagerReadAccess",
            "Effect": "Allow",
            "Action": ["secretsmanager:GetSecretValue"],
            "Resource": ["arn:aws:secretsmanager:<region>:<account-id>:secret:<secret-
name>"]
        }
    ]
}
```

Das folgende Beispiel bietet die erforderlichen Berechtigungen, um in eine Amazon OpenSearch Service-Domain zu schreiben:

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::{your-account-id}:role/{pipeline-role}"
      },
      "Action": ["es:DescribeDomain", "es:ESHttp*"],
      "Resource": "arn:aws:es:{region}:{your-account-id}:domain/{domain-name}/*"
    }
  ]
}
```

Eine Pipeline erstellen

Nachdem Sie die Richtlinie an die Pipeline-Rolle angehängt haben, können Sie den Datenmigrationspipeline-Blueprint von Confluent Kafka verwenden, um Ihre Pipeline zu erstellen. Dieser Blueprint enthält eine Standardkonfiguration für die Migration von Daten zwischen Kafka und Ihrem Ziel.

- Sie können mehrere Amazon OpenSearch Service-Domains als Ziele für Ihre Daten angeben. Diese Funktion ermöglicht die bedingte Weiterleitung oder Replikation eingehender Daten in mehrere Amazon OpenSearch Services.

- Sie können Daten von einem Confluent Kafka-Quellcluster zu einer Amazon OpenSearch Serverless VPC-Sammlung migrieren. Stellen Sie sicher, dass Sie in der Pipeline-Konfiguration eine Netzwerkzugriffsrichtlinie angeben.
- Sie können die Confluent-Schemaregistrierung verwenden, um ein Confluent-Schema zu definieren.

Beispiel für eine Pipeline-Konfiguration

```
version: "2"
kafka-pipeline:
  source:
    kafka:
      # Encryption is always required
      encryption:
        type: "ssl"
      topics:
        - name: "topic_4"
          group_id: "demoGroup"
      bootstrap_servers:
        # TODO: for public confluent kafka use public booststrap server dns
        - "<<bootstrap-server>>.us-west-2.aws.private.confluent.cloud:9092"
      authentication:
        sasl:
          plain:
            username: "${{aws_secrets:confluent-kafka-secret:username}}"
            password: "${{aws_secrets:confluent-kafka-secret:password}}"
      # Schema is optional
      schema:
        type: confluent
        registry_url: https://<<registry-url>>.us-west-2.aws.confluent.cloud
        api_key: "${{aws_secrets:schema-secret:schema_registry_api_key}}"
        api_secret: "${{aws_secrets:schema-secret:schema_registry_api_secret}}"
        basic_auth_credentials_source: "USER_INFO"
  sink:
    - opensearch:
        hosts: [ "https://<<opensearchdomain>>.us-west-2.es.amazonaws.com" ]
        index: "enterprise-confluent-demo"
        aws:
          sts_role_arn: "arn:aws:iam::1234567890:role/os-os-test-role"
          region: "<<aws-region>>"
 extension:
  aws:
```

```
    secrets:
      confluent-kafka-secret:
        secret_id: "enterprise-kafka-credentials"
        region: "<<aws-region>>"
        sts_role_arn: "arn:aws:iam::1234567890:role/os-os-test-role"
      schema-secret:
        secret_id: "self-managed-kafka-schema"
        region: "<<aws-region>>"
        sts_role_arn: "arn:aws:iam::1234567890:role/os-os-test-role"
```

Verwenden einer OpenSearch Ingestion-Pipeline mit Amazon Managed Streaming for Apache Kafka

Sie können das Kafka-Plugin verwenden, um Daten aus Amazon Managed Streaming for Apache Kafka (Amazon MSK) in Ihre Ingestion-Pipeline aufzunehmen. OpenSearch Mit Amazon MSK können Sie Anwendungen erstellen und ausführen, die Apache Kafka zur Verarbeitung von Streaming-Daten verwenden. OpenSearch Ingestion verwendet, um eine Verbindung AWS PrivateLink zu Amazon MSK herzustellen. Sie können Daten sowohl aus Amazon MSK- als auch aus Amazon MSK Serverless-Clustern aufnehmen. Der einzige Unterschied zwischen den beiden Prozessen besteht in den erforderlichen Schritten, die Sie ergreifen müssen, bevor Sie Ihre Pipeline einrichten.

Themen

Voraussetzungen für Amazon MSK

Bevor Sie Ihre OpenSearch Ingestion-Pipeline erstellen, führen Sie die folgenden Schritte aus:

1. Erstellen Sie einen von Amazon MSK bereitgestellten Cluster, indem Sie den Schritten unter Cluster erstellen im Amazon Managed Streaming for Apache Kafka Developer Guide folgen.

Wählen Sie als Broker-Typ eine beliebige Option außer `t3` Typen aus, da diese von Ingestion nicht unterstützt werden. OpenSearch

2. Wenn der Cluster den Status Aktiv hat, folgen Sie den Schritten unter Multi-VPC-Konnektivität aktivieren.
3. Folgen Sie den Schritten unter Anhängen einer Clusterrichtlinie an den MSK-Cluster, um eine der folgenden Richtlinien anzuhängen, je nachdem, ob Ihr Cluster und Ihre Pipeline identisch sind. AWS-Konto Diese Richtlinie ermöglicht es OpenSearch Ingestion, eine AWS PrivateLink Verbindung zu Ihrem Amazon MSK-Cluster herzustellen und Daten aus Kafka-Themen zu lesen. Stellen Sie sicher, dass Sie das `resource` mit Ihrem eigenen ARN aktualisieren.

   Die folgenden Richtlinien gelten, wenn sich Ihr Cluster und Ihre Pipeline in derselben Einheit befinden AWS-Konto:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "osis.amazonaws.com"
      },
      "Action": [
        "kafka:CreateVpcConnection",
        "kafka:DescribeClusterV2"
      ],
      "Resource": "arn:aws:kafka:us-east-1:{account-id}:cluster/cluster-name/cluster-
id"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "osis-pipelines.amazonaws.com"
      },
      "Action": [
        "kafka:CreateVpcConnection",
        "kafka:GetBootstrapBrokers",
        "kafka:DescribeClusterV2"
      ],
      "Resource": "arn:aws:kafka:us-east-1:{account-id}:cluster/cluster-name/cluster-
id"
    }
```

```
  ]
}
```

Wenn sich Ihr Amazon MSK-Cluster in einer anderen Pipeline AWS-Konto als Ihrer Pipeline befindet, fügen Sie stattdessen die folgende Richtlinie bei. Beachten Sie, dass kontenübergreifender Zugriff nur mit bereitgestellten Amazon MSK-Clustern und nicht mit Amazon MSK Serverless-Clustern möglich ist. Der ARN für AWS `principal` sollte der ARN für dieselbe Pipeline-Rolle sein, die Sie für Ihre Pipeline-YAML-Konfiguration angeben:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "osis.amazonaws.com"
      },
      "Action": [
        "kafka:CreateVpcConnection",
        "kafka:DescribeClusterV2"
      ],
      "Resource": "arn:aws:kafka:us-east-1:{msk-account-id}:cluster/cluster-
name/cluster-id"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "osis-pipelines.amazonaws.com"
      },
      "Action": [
        "kafka:CreateVpcConnection",
        "kafka:GetBootstrapBrokers",
        "kafka:DescribeClusterV2"
      ],
      "Resource": "arn:aws:kafka:us-east-1:{msk-account-id}:cluster/cluster-
name/cluster-id"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::{pipeline-account-id}:role/pipeline-role"
      },
```

```
      "Action": [
        "kafka-cluster:*",
        "kafka:*"
      ],
      "Resource": [
        "arn:aws:kafka:us-east-1:{msk-account-id}:cluster/cluster-name/cluster-id",
        "arn:aws:kafka:us-east-1:{msk-account-id}:topic/cluster-name/cluster-id/*",
        "arn:aws:kafka:us-east-1:{msk-account-id}:group/cluster-name/*"
      ]
    }
  ]
}
```

4. Erstellen Sie ein Kafka-Thema, indem Sie den Schritten unter Thema erstellen folgen. Stellen Sie sicher, dass *BootstrapServerString* es sich um eine der Bootstrap-URLs für private Endpunkte (Single-VPC) handelt. Der Wert für `--replication-factor` sollte 2 oder sein3, basierend auf der Anzahl der Zonen, über die Ihr Amazon MSK-Cluster verfügt. Der Wert für `--partitions` sollte mindestens `10` sein.
5. Erzeugen und konsumieren Sie Daten, indem Sie die Schritte unter Daten produzieren und konsumieren befolgen. Stellen Sie auch hier sicher, dass *BootstrapServerString* es sich um eine Ihrer privaten Endpunkt-Bootstrap-URLs (Single-VPC) handelt.

Voraussetzungen für Amazon MSK Serverless

Bevor Sie Ihre OpenSearch Ingestion-Pipeline erstellen, führen Sie die folgenden Schritte aus:

1. Erstellen Sie einen serverlosen Amazon MSK-Cluster, indem Sie den Schritten unter Create an MSK Serverless Cluster im Amazon Managed Streaming for Apache Kafka Developer Guide folgen.
2. Wenn der Cluster den Status Aktiv hat, folgen Sie den Schritten unter Eine Cluster-Richtlinie an den MSK-Cluster anhängen, um die folgende Richtlinie anzuhängen. Stellen Sie sicher, dass Sie das `resource` mit Ihrem eigenen ARN aktualisieren.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "osis.amazonaws.com"
```

```
      },
      "Action": [
        "kafka:CreateVpcConnection",
        "kafka:DescribeClusterV2"
      ],
      "Resource": "arn:aws:kafka:us-east-1:{account-id}:cluster/cluster-name/cluster-
id"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "osis-pipelines.amazonaws.com"
      },
      "Action": [
        "kafka:CreateVpcConnection",
        "kafka:GetBootstrapBrokers",
        "kafka:DescribeClusterV2"
      ],
      "Resource": "arn:aws:kafka:us-east-1:{account-id}:cluster/cluster-name/cluster-
id"
    }
  ]
}
```

Diese Richtlinie ermöglicht es OpenSearch Ingestion, eine AWS PrivateLink Verbindung zu Ihrem Amazon MSK Serverless-Cluster herzustellen und Daten aus Kafka-Themen zu lesen. Diese Richtlinie gilt, wenn sich Ihr Cluster und Ihre Pipeline im selben System befinden. Dies muss zutreffen AWS-Konto, da Amazon MSK Serverless keinen kontoübergreifenden Zugriff unterstützt.

3. Erstellen Sie ein Kafka-Thema, indem Sie den Schritten unter Thema erstellen folgen. Stellen Sie sicher, dass *`BootstrapServerString`* es sich um eine Ihrer SASL-IAM-Bootstrap-URLs (Simple Authentication and Security Layer) handelt. Der Wert für `--replication-factor` sollte `2` oder sein`3`, basierend auf der Anzahl der Zonen, über die Ihr Amazon MSK Serverless-Cluster verfügt. Der Wert für `--partitions` sollte mindestens sein. `10`
4. Erzeugen und konsumieren Sie Daten, indem Sie die Schritte unter Daten produzieren und konsumieren befolgen. Stellen Sie auch hier sicher, dass *`BootstrapServerString`* es sich um eine Ihrer SASL-IAM-Bootstrap-URLs (Simple Authentication and Security Layer) handelt.

Schritt 1: Konfigurieren Sie die Pipeline-Rolle

Nachdem Sie Ihren von Amazon MSK bereitgestellten oder serverlosen Cluster eingerichtet haben, fügen Sie der Pipeline-Rolle, die Sie in Ihrer Pipeline-Konfiguration verwenden möchten, die folgenden Kafka-Berechtigungen hinzu:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kafka-cluster:Connect",
                "kafka-cluster:AlterCluster",
                "kafka-cluster:DescribeCluster",
                "kafka:DescribeClusterV2",
                "kafka:GetBootstrapBrokers"
            ],
            "Resource": [
                "arn:aws:kafka:us-east-1:{account-id}:cluster/cluster-name/cluster-id"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kafka-cluster:*Topic*",
                "kafka-cluster:ReadData"
            ],
            "Resource": [
                "arn:aws:kafka:us-east-1:{account-id}:topic/cluster-name/cluster-
id/topic-name"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kafka-cluster:AlterGroup",
                "kafka-cluster:DescribeGroup"
            ],
            "Resource": [
                "arn:aws:kafka:us-east-1:{account-id}:group/cluster-name/*"
            ]
        }
```

```
    ]
}
```

Schritt 2: Erstellen Sie die Pipeline

Anschließend können Sie eine OpenSearch Ingestion-Pipeline wie die folgende konfigurieren, die Kafka als Quelle angibt:

```
version: "2"
log-pipeline:
  source:
    kafka:
      acknowledgements: true
      topics:
      - name: "topic-name"
        group_id: "group-id"
      aws:
        msk:
          arn: "arn:aws:kafka:{region}:{account-id}:cluster/cluster-name/cluster-id"
        region: "us-west-2"
        sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
  processor:
  - grok:
      match:
        message:
        - "%{COMMONAPACHELOG}"
  - date:
      destination: "@timestamp"
      from_time_received: true
  sink:
  - opensearch:
      hosts: ["https://search-domain-endpoint.us-east-1.es.amazonaws.com"]
      index: "index_name"
      aws_sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
      aws_region: "us-east-1"
      aws_sigv4: true
```

Sie können einen vorkonfigurierten Amazon MSK-Blueprint verwenden, um diese Pipeline zu erstellen. Weitere Informationen finden Sie unter the section called “Verwenden von Blueprints zum Erstellen einer Pipeline”.

Schritt 3: (Optional) Verwenden Sie die Schemaregistrierung AWS Glue

Wenn Sie OpenSearch Ingestion mit Amazon MSK verwenden, können Sie das AVRO-Datenformat für Schemas verwenden, die in der Schema Registry gehostet werden. AWS Glue Mit der AWS Glue Schema Registry können Sie Datenstromschemas zentral erkennen, steuern und weiterentwickeln.

Um diese Option zu verwenden, aktivieren Sie das Schema `type` in Ihrer Pipeline-Konfiguration:

```
schema:
  type: "aws_glue"
```

Sie müssen in Ihrer Pipeline-Rolle auch Lesezugriffsberechtigungen bereitstellen AWS Glue . Sie können die AWS verwaltete Richtlinie namens verwenden AWSGlueSchemaRegistryReadonlyAccess. Darüber hinaus muss sich Ihre Registrierung in derselben AWS-Konto Region wie Ihre OpenSearch Ingestion-Pipeline befinden.

Schritt 4: (Optional) Empfohlene Recheneinheiten (OCUs) für die Amazon MSK-Pipeline konfigurieren

Jede Recheneinheit hat einen Nutzer pro Thema. Makler gleichen die Partitionen zwischen diesen Verbrauchern für ein bestimmtes Thema aus. Wenn jedoch die Anzahl der Partitionen die Anzahl der Verbraucher übersteigt, hostet Amazon MSK mehrere Partitionen auf jedem Verbraucher. OpenSearch Ingestion verfügt über eine integrierte auto Skalierung, mit der je nach CPU-Auslastung oder Anzahl ausstehender Datensätze in der Pipeline nach oben oder unten skaliert werden kann.

Um eine optimale Leistung zu erzielen, verteilen Sie Ihre Partitionen für die Parallelverarbeitung auf viele Recheneinheiten. Wenn Themen eine große Anzahl von Partitionen haben (z. B. mehr als 96, was die maximale Anzahl von OCUs pro Pipeline darstellt), empfehlen wir, eine Pipeline mit 1 —96 OCUs zu konfigurieren. Das liegt daran, dass sie bei Bedarf automatisch skaliert wird. Wenn ein Thema eine geringe Anzahl von Partitionen hat (z. B. weniger als 96), sollten Sie die maximale Recheneinheit der Anzahl der Partitionen anpassen.

Wenn eine Pipeline mehr als ein Thema enthält, wählen Sie das Thema mit der höchsten Anzahl von Partitionen als Referenz für die Konfiguration der maximalen Recheneinheiten aus. Durch Hinzufügen einer weiteren Pipeline mit einem neuen Satz von OCUs zu demselben Thema und derselben Nutzergruppe können Sie den Durchsatz nahezu linear skalieren.

Verwenden einer OpenSearch Ingestion-Pipeline mit Amazon S3

Mit OpenSearch Ingestion können Sie Amazon S3 als Quelle oder als Ziel verwenden. Wenn Sie Amazon S3 als Quelle verwenden, senden Sie Daten an eine OpenSearch Ingestion-Pipeline. Wenn Sie Amazon S3 als Ziel verwenden, schreiben Sie Daten aus einer OpenSearch Ingestion-Pipeline in einen oder mehrere S3-Buckets.

Themen

Amazon S3 als Quelle

Es gibt zwei Möglichkeiten, Amazon S3 als Quelle für die Datenverarbeitung zu verwenden — mit der S3-SQS-Verarbeitung und mit geplanten Scans.

Verwenden Sie die S3-SQS-Verarbeitung, wenn Sie Dateien fast in Echtzeit scannen möchten, nachdem sie in S3 geschrieben wurden. Sie können Amazon S3 S3-Buckets so konfigurieren, dass sie jedes Mal ein Ereignis auslösen, wenn ein Objekt im Bucket gespeichert oder geändert wird. Verwenden Sie einen einmaligen oder wiederkehrenden geplanten Scan, um Daten in einem S3-Bucket stapelweise zu verarbeiten.

Themen

Voraussetzungen

Um Amazon S3 als Quelle für eine OpenSearch Ingestion-Pipeline sowohl für einen geplanten Scan als auch für eine S3-SQS-Verarbeitung zu verwenden, erstellen Sie zunächst einen S3-Bucket.

> **Note**
>
> Wenn sich der S3-Bucket, der als Quelle in der OpenSearch Ingestion-Pipeline verwendet wird, in einem anderen befindet AWS-Konto, müssen Sie auch kontoübergreifende

Leseberechtigungen für den Bucket aktivieren. Dadurch kann die Pipeline die Daten lesen und verarbeiten. Informationen zum Aktivieren kontoübergreifender Berechtigungen finden Sie unter Bucket-Besitzer, der kontoübergreifende Bucket-Berechtigungen erteilt im Amazon S3 S3-Benutzerhandbuch.
Wenn sich Ihre S3-Buckets in mehreren Konten befinden, verwenden Sie eine Map. `bucket_owners` Ein Beispiel finden Sie in der Dokumentation unter Kontoübergreifender S3-Zugriff. OpenSearch

Um die S3-SQS-Verarbeitung einzurichten, müssen Sie außerdem die folgenden Schritte ausführen:

1. Erstellen Sie eine Amazon SQS SQS-Warteschlange.
2. Aktivieren Sie Ereignisbenachrichtigungen im S3-Bucket mit der SQS-Warteschlange als Ziel.

Schritt 1: Konfigurieren Sie die Pipeline-Rolle

Im Gegensatz zu anderen Quell-Plugins, die Daten in eine Pipeline übertragen, verfügt das S3-Quell-Plug-In über eine lesebasierte Architektur, bei der die Pipeline Daten aus der Quelle bezieht.

Damit eine Pipeline aus S3 lesen kann, müssen Sie daher eine Rolle in der S3-Quellkonfiguration der Pipeline angeben, die Zugriff sowohl auf den S3-Bucket als auch auf die Amazon SQS SQS-Warteschlange hat. Die Pipeline übernimmt diese Rolle, um Daten aus der Warteschlange zu lesen.

Note

Die Rolle, die Sie in der S3-Quellkonfiguration angeben, muss die Pipeline-Rolle sein. Daher muss Ihre Pipeline-Rolle zwei separate Berechtigungsrichtlinien enthalten — eine zum Schreiben in eine Senke und eine zum Abrufen aus der S3-Quelle. Sie müssen dasselbe `sts_role_arn` in allen Pipeline-Komponenten verwenden.

Die folgende Beispielrichtlinie zeigt die erforderlichen Berechtigungen für die Verwendung von S3 als Quelle:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
      "Effect": "Allow",
      "Action":[
          "s3:ListBucket",
          "s3:GetBucketLocation",
          "s3:GetObject"
       ],
      "Resource": "arn:aws:s3:::my-bucket/*"
    },
    {
       "Effect":"Allow",
       "Action":"s3:ListAllMyBuckets",
       "Resource":"arn:aws:s3:::*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "sqs:DeleteMessage",
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility"
      ],
      "Resource": "arn:aws:sqs:us-west-2:{account-id}:MyS3EventSqsQueue"
    }
  ]
}
```

Sie müssen diese Berechtigungen an die IAM-Rolle anhängen, die Sie in der `sts_role_arn` Option in der Konfiguration des S3-Quell-Plug-ins angeben:

```
version: "2"
source:
  s3:
    ...
    aws:
      ...
      sts_role_arn: arn:aws:iam::{account-id}:role/pipeline-role
processor:
  ...
sink:
  - opensearch:
      ...
```

Schritt 2: Erstellen Sie die Pipeline

Nachdem Sie Ihre Berechtigungen eingerichtet haben, können Sie je nach Ihrem Amazon OpenSearch S3-Anwendungsfall eine Ingestion-Pipeline konfigurieren.

S3-SQS-Verarbeitung

Um die S3-SQS-Verarbeitung einzurichten, konfigurieren Sie Ihre Pipeline so, dass sie S3 als Quelle angibt, und richten Sie Amazon SQS-Benachrichtigungen ein:

```
version: "2"
s3-pipeline:
  source:
    s3:
      notification_type: "sqs"
      codec:
        newline: null
      sqs:
        queue_url: "https://sqs.us-east-1.amazonaws.com/{account-id}/ingestion-queue"
      compression: "none"
      aws:
        region: "us-east-1"
        # IAM role that the pipeline assumes to read data from the queue. This role
 must be the same as the pipeline role.
        sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
  processor:
  - grok:
      match:
        message:
        - "%{COMMONAPACHELOG}"
  - date:
      destination: "@timestamp"
      from_time_received: true
  sink:
  - opensearch:
      hosts: ["https://search-domain-endpoint.us-east-1.es.amazonaws.com"]
      index: "index-name"
      aws:
        # IAM role that the pipeline assumes to access the domain sink
        sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
        region: "us-east-1"
```

Wenn Sie bei der Verarbeitung kleiner Dateien auf Amazon S3 eine geringe CPU-Auslastung feststellen, sollten Sie erwägen, den Durchsatz zu erhöhen, indem Sie den Wert der `workers` Option ändern. Weitere Informationen finden Sie in den Konfigurationsoptionen des S3-Plug-ins.

Geplanter Scan

Um einen geplanten Scan einzurichten, konfigurieren Sie Ihre Pipeline mit einem Zeitplan auf Scanebene, der für alle Ihre S3-Buckets gilt, oder auf Bucket-Ebene. Ein Zeitplan auf Bucket-Ebene oder eine Konfiguration mit Scan-Intervallen überschreibt immer eine Konfiguration auf Scan-Ebene.

Sie können geplante Scans entweder mit einem einmaligen Scan konfigurieren, der sich ideal für die Datenmigration eignet, oder mit einem wiederkehrenden Scan, der sich ideal für die Stapelverarbeitung eignet.

Verwenden Sie die vorkonfigurierten Amazon S3-Blueprints, um Ihre Pipeline für das Lesen aus Amazon S3 zu konfigurieren. Sie können den `scan` Teil Ihrer Pipeline-Konfiguration bearbeiten, um Ihre Planungsanforderungen zu erfüllen. Weitere Informationen finden Sie unter the section called “Verwenden von Blueprints zum Erstellen einer Pipeline”.

Einmaliger Scan

Ein einmaliger geplanter Scan wird einmal ausgeführt. In Ihrer YAML-Konfiguration können Sie mit einem `start_time` und angebenend_time, wann die Objekte im Bucket gescannt werden sollen. Alternativ können `range` Sie das Zeitintervall im Verhältnis zur aktuellen Uhrzeit angeben, in dem die Objekte im Bucket gescannt werden sollen.

Zum Beispiel ein Bereich, der so eingestellt ist, dass alle Dateien PT4H gescannt werden, die in den letzten vier Stunden erstellt wurden. Um einen einmaligen Scan so zu konfigurieren, dass er ein zweites Mal ausgeführt wird, müssen Sie die Pipeline beenden und neu starten. Wenn Sie keinen Bereich konfiguriert haben, müssen Sie auch die Start- und Endzeiten aktualisieren.

Die folgende Konfiguration richtet einen einmaligen Scan für alle Buckets und alle Objekte in diesen Buckets ein:

```
version: "2"
log-pipeline:
  source:
    s3:
      codec:
        csv:
      compression: "none"
```

```
      aws:
        region: "us-east-1"
        sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
      acknowledgments: true
      scan:
        buckets:
          - bucket:
              name: my-bucket-1
              filter:
                include_prefix:
                  - Objects1/
                exclude_suffix:
                  - .jpeg
                  - .png
          - bucket:
              name: my-bucket-2
              key_prefix:
                include:
                  - Objects2/
                exclude_suffix:
                  - .jpeg
                  - .png
      delete_s3_objects_on_read: false
  processor:
    - date:
        destination: "@timestamp"
        from_time_received: true
  sink:
    - opensearch:
        hosts: ["https://search-domain-endpoint.us-east-1.es.amazonaws.com"]
        index: "index-name"
        aws:
          sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
          region: "us-east-1"
        dlq:
          s3:
            bucket: "my-bucket-1"
            region: "us-east-1"
            sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
```

Die folgende Konfiguration richtet einen einmaligen Scan für alle Buckets während eines bestimmten Zeitfensters ein. Das bedeutet, dass S3 nur die Objekte verarbeitet, deren Erstellungszeiten in dieses Fenster fallen.

```
scan:
  start_time: 2023-01-21T18:00:00.000Z
  end_time: 2023-04-21T18:00:00.000Z
  buckets:
    - bucket:
        name: my-bucket-1
        filter:
          include:
            - Objects1/
          exclude_suffix:
            - .jpeg
            - .png
    - bucket:
        name: my-bucket-2
        filter:
          include:
            - Objects2/
          exclude_suffix:
            - .jpeg
            - .png
```

Die folgende Konfiguration richtet einen einmaligen Scan sowohl auf Scan- als auch auf Bucket-Ebene ein. Start- und Endzeiten auf Bucket-Ebene haben Vorrang vor Start- und Endzeiten auf Scan-Ebene.

```
scan:
  start_time: 2023-01-21T18:00:00.000Z
  end_time: 2023-04-21T18:00:00.000Z
  buckets:
    - bucket:
        start_time: 2023-01-21T18:00:00.000Z
        end_time: 2023-04-21T18:00:00.000Z
        name: my-bucket-1
        filter:
          include:
            - Objects1/
          exclude_suffix:
            - .jpeg
            - .png
    - bucket:
        start_time: 2023-01-21T18:00:00.000Z
        end_time: 2023-04-21T18:00:00.000Z
```

```
        name: my-bucket-2
        filter:
          include:
            - Objects2/
          exclude_suffix:
            - .jpeg
            - .png
```

Beim Stoppen einer Pipeline werden alle bereits vorhandenen Verweise darauf entfernt, welche Objekte vor dem Stopp von der Pipeline gescannt wurden. Wenn eine einzelne Scan-Pipeline gestoppt wird, werden alle Objekte nach dem Start erneut gescannt, auch wenn sie bereits gescannt wurden. Wenn Sie eine einzelne Scan-Pipeline beenden müssen, empfiehlt es sich, Ihr Zeitfenster zu ändern, bevor Sie die Pipeline erneut starten.

Wenn Sie Objekte nach Start- und Endzeit filtern müssen, ist das Stoppen und Starten der Pipeline die einzige Option. Wenn Sie nicht nach Start- und Endzeit filtern müssen, können Sie Objekte nach Namen filtern. Um nach Namen zu filtern, müssen Sie Ihre Pipeline nicht beenden und starten. Verwenden `include_prefix` Sie dazu und. `exclude_suffix`

Wiederkehrender Scan

Bei einem wiederkehrenden geplanten Scan werden Ihre angegebenen S3-Buckets in regelmäßigen, geplanten Intervallen gescannt. Sie können diese Intervalle nur auf Scanebene konfigurieren, da einzelne Konfigurationen auf Bucket-Ebene nicht unterstützt werden.

In Ihrer YAML-Konfiguration `interval` gibt der die Häufigkeit des wiederkehrenden Scans an und kann zwischen 30 Sekunden und 365 Tagen liegen. Der erste dieser Scans erfolgt immer, wenn Sie die Pipeline erstellen. Das `count` definiert die Gesamtzahl der Scan-Instanzen.

Die folgende Konfiguration richtet einen wiederkehrenden Scan mit einer Verzögerung von 12 Stunden zwischen den Scans ein:

```
scan:
  scheduling:
    interval: PT12H
    count: 4
  buckets:
    - bucket:
        name: my-bucket-1
        filter:
          include:
```

```
            - Objects1/
          exclude_suffix:
            - .jpeg
            - .png
    - bucket:
        name: my-bucket-2
        filter:
          include:
            - Objects2/
          exclude_suffix:
            - .jpeg
            - .png
```

Amazon S3 als Ziel

Um Daten aus einer OpenSearch Ingestion-Pipeline in einen S3-Bucket zu schreiben, verwenden Sie den vorkonfigurierten S3-Blueprint, um eine Pipeline mit einer S3-Senke zu erstellen. Diese Pipeline leitet selektive Daten an eine OpenSearch Senke weiter und sendet gleichzeitig alle Daten zur Archivierung in S3. Weitere Informationen finden Sie unter the section called “Verwenden von Blueprints zum Erstellen einer Pipeline”.

Wenn Sie Ihre S3-Senke erstellen, können Sie Ihre bevorzugte Formatierung anhand einer Vielzahl von Senken-Codecs angeben. Wenn Sie beispielsweise Daten im Spaltenformat schreiben möchten, wählen Sie den Parquet- oder Avro-Codec. Wenn Sie ein zeilenbasiertes Format bevorzugen, wählen Sie JSON oder ND-JSON. Um Daten in einem bestimmten Schema nach S3 zu schreiben, können Sie mithilfe des Avro-Formats auch ein Inline-Schema innerhalb von Sink-Codecs definieren.

Das folgende Beispiel definiert ein Inline-Schema in einer S3-Senke:

```
- s3:
  codec:
    parquet:
      schema: >
        {
           "type" : "record",
           "namespace" : "org.vpcFlowLog.examples",
           "name" : "VpcFlowLog",
           "fields" : [
             { "name" : "version", "type" : "string"},
             { "name" : "srcport", "type": "int"},
             { "name" : "dstport", "type": "int"},
             { "name" : "start", "type": "int"},
```

```
            { "name" : "end", "type": "int"},
            { "name" : "protocol", "type": "int"},
            { "name" : "packets", "type": "int"},
            { "name" : "bytes", "type": "int"},
            { "name" : "action", "type": "string"},
            { "name" : "logStatus", "type" : "string"}
          ]
        }
```

Wenn Sie dieses Schema definieren, geben Sie eine Obermenge aller Schlüssel an, die in den verschiedenen Ereignistypen vorhanden sein könnten, die Ihre Pipeline an eine Senke übermittelt.

Wenn bei einem Ereignis beispielsweise die Möglichkeit besteht, dass ein Schlüssel fehlt, fügen Sie diesen Schlüssel mit einem `null` Wert in Ihr Schema ein. Nullwertdeklarationen ermöglichen es dem Schema, ungleichmäßige Daten zu verarbeiten (wobei einige Ereignisse diese Schlüssel haben und andere nicht). Wenn bei eingehenden Ereignissen diese Schlüssel vorhanden sind, werden ihre Werte in Senken geschrieben.

Diese Schemadefinition fungiert als Filter, der nur das Senden definierter Schlüssel an Senken ermöglicht und undefinierte Schlüssel aus eingehenden Ereignissen löscht.

Sie können auch `include_keys` und `exclude_keys` in Ihrer Senke verwenden, um Daten zu filtern, die an andere Senken weitergeleitet werden. Diese beiden Filter schließen sich gegenseitig aus, sodass Sie in Ihrem Schema jeweils nur einen Filter verwenden können. Darüber hinaus können Sie sie nicht in benutzerdefinierten Schemas verwenden.

Verwenden Sie den vorkonfigurierten Senkenfilter-Blueprint, um Pipelines mit solchen Filtern zu erstellen. Weitere Informationen finden Sie unter the section called “Verwenden von Blueprints zum Erstellen einer Pipeline”.

Amazon S3 Cross-Konto als Quelle

Sie können bei Amazon S3 kontenübergreifenden Zugriff gewähren, sodass OpenSearch Ingestion-Pipelines auf S3-Buckets in einem anderen Konto als Quelle zugreifen können. Informationen zum Aktivieren des kontoübergreifenden Zugriffs finden Sie unter Bucket-Besitzer, der kontoübergreifende Bucket-Berechtigungen erteilt im Amazon S3 S3-Benutzerhandbuch. Nachdem Sie den Zugriff gewährt haben, stellen Sie sicher, dass Ihre Pipeline-Rolle über die erforderlichen Berechtigungen verfügt.

Anschließend können Sie eine YAML-Konfiguration erstellen, `bucket_owners` um den kontoübergreifenden Zugriff auf einen Amazon S3 S3-Bucket als Quelle zu ermöglichen:

```
s3-pipeline:
 source:
  s3:
   notification_type: "sqs"
   codec:
    csv:
     delimiter: ","
     quote_character: "\""
     detect_header: True
   sqs:
    queue_url: "https://sqs.ap-northeast-1.amazonaws.com/401447383613/test-s3-queue"
   bucket_owners:
    my-bucket-01: 123456789012
    my-bucket-02: 999999999999
   compression: "gzip"
```

Verwenden einer OpenSearch Ingestion-Pipeline mit Amazon Security Lake

Sie können das S3-Quell-Plugin verwenden, um Daten von Amazon Security Lake in Ihre OpenSearch Ingestion-Pipeline aufzunehmen. Security Lake zentralisiert automatisch Sicherheitsdaten aus AWS Umgebungen, lokalen Umgebungen und SaaS-Anbietern in einem speziell dafür entwickelten Data Lake. Sie können ein Abonnement erstellen, das Daten aus Security Lake in Ihre OpenSearch Ingestion-Pipeline repliziert, die sie dann in Ihre Service-Domain oder Serverless-Sammlung schreibt. OpenSearch OpenSearch

Verwenden Sie den vorkonfigurierten Security Lake-Blueprint, um Ihre Pipeline so zu konfigurieren, dass sie aus Security Lake liest. Der Blueprint enthält eine Standardkonfiguration für die Aufnahme von Open Cybersecurity Schema Framework (OCSF) -Parquet-Dateien aus Security Lake. Weitere Informationen finden Sie unter the section called “Verwenden von Blueprints zum Erstellen einer Pipeline”.

Themen

- Voraussetzungen
- Schritt 1: Konfigurieren Sie die Pipeline-Rolle
- Schritt 2: Erstellen Sie die Pipeline

Voraussetzungen

Bevor Sie Ihre OpenSearch Ingestion-Pipeline erstellen, führen Sie die folgenden Schritte aus:

- Aktivieren Sie Security Lake.
- Erstellen Sie einen Abonnenten in Security Lake.
  - Wählen Sie die Quellen aus, die Sie in Ihre Pipeline aufnehmen möchten.
  - Fügen Sie für Abonnentenanmeldedaten die ID des Ortes hinzu AWS-Konto , in dem Sie die Pipeline erstellen möchten. Geben Sie für die externe ID an`OpenSearchIngestion-{accountid}`.
  - Wählen Sie als Datenzugriffsmethode die Option S3 aus.
  - Wählen Sie für Benachrichtigungsdetails die Option SQS-Warteschlange aus.

Wenn Sie einen Abonnenten erstellen, erstellt Security Lake automatisch zwei Inline-Berechtigungsrichtlinien — eine für S3 und eine für SQS. Die Richtlinien haben das folgende Format: und. `AmazonSecurityLake-{12345}-S3` `AmazonSecurityLake-{12345}-SQS` Damit Ihre Pipeline auf die Abonnentenquellen zugreifen kann, müssen Sie Ihrer Pipeline-Rolle die erforderlichen Berechtigungen zuordnen.

Schritt 1: Konfigurieren Sie die Pipeline-Rolle

Erstellen Sie eine neue Berechtigungsrichtlinie in IAM, die nur die erforderlichen Berechtigungen aus den beiden Richtlinien kombiniert, die Security Lake automatisch erstellt hat. Die folgende Beispielrichtlinie zeigt die geringste Berechtigung, die für eine OpenSearch Ingestion-Pipeline zum Lesen von Daten aus mehreren Security Lake-Quellen erforderlich ist:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetObject"
         ],
         "Resource":[
            "arn:aws:s3:::aws-security-data-lake-{region}-abcde/aws/
LAMBDA_EXECUTION/1.0/*",
            "arn:aws:s3:::aws-security-data-lake-{region}-abcde/aws/S3_DATA/1.0/*",
            "arn:aws:s3:::aws-security-data-lake-{region}-abcde/aws/VPC_FLOW/1.0/*",
            "arn:aws:s3:::aws-security-data-lake-{region}-abcde/aws/ROUTE53/1.0/*",
            "arn:aws:s3:::aws-security-data-lake-{region}-abcde/aws/SH_FINDINGS/1.0/*"
         ]
      },
```

```
      {
         "Effect":"Allow",
         "Action":[
            "sqs:ReceiveMessage",
            "sqs:DeleteMessage"
         ],
         "Resource":[
            "arn:aws:sqs:{region}:{account-id}:AmazonSecurityLake-abcde-Main-Queue"
         ]
      }
   ]
}
```

> **Important**
>
> Security Lake verwaltet die Pipeline-Rollenrichtlinie nicht für Sie. Wenn Sie Quellen zu Ihrem Security Lake-Abonnement hinzufügen oder daraus entfernen, müssen Sie die Richtlinie manuell aktualisieren. Security Lake erstellt Partitionen für jede Protokollquelle, sodass Sie der Pipeline-Rolle manuell Berechtigungen hinzufügen oder entfernen müssen.

Sie müssen diese Berechtigungen der IAM-Rolle zuordnen, die Sie in der `sts_role_arn` Option in der Konfiguration des S3-Quell-Plug-ins unter `sqs` angeben.

```
version: "2"
source:
  s3:
    ...
    sqs:
      queue_url: "https://sqs.{region}.amazonaws.com/{account-id}/
AmazonSecurityLake-abcde-Main-Queue"
    aws:
      ...
      sts_role_arn: arn:aws:iam::{account-id}:role/pipeline-role
processor:
  ...
sink:
  - opensearch:
      ...
```

Schritt 2: Erstellen Sie die Pipeline

Nachdem Sie der Pipeline-Rolle die Berechtigungen hinzugefügt haben, verwenden Sie den vorkonfigurierten S3-Blueprint, um die Pipeline zu erstellen. Weitere Informationen finden Sie unter the section called “Verwenden von Blueprints zum Erstellen einer Pipeline”.

Sie müssen die `queue_url` Option in der `s3` Quellkonfiguration angeben. Dabei handelt es sich um die Amazon SQS SQS-Warteschlangen-URL, aus der gelesen werden soll. Um die URL zu formatieren, suchen Sie den Abonnement-Endpunkt in der Abonnentenkonfiguration und wechseln Sie `arn:aws:` zu`https://`. z. B. `https://sqs.`*`{region}`*`.amazonaws.com/`*`{account-id}`*`/AmazonSecurityLake-`*`abdcef`*`-Main-Queue`.

`sts_role_arn`Das, was Sie in der S3-Quellkonfiguration angeben, muss der ARN der Pipeline-Rolle sein.

Verwenden einer OpenSearch Ingestion-Pipeline mit Fluent Bit

Diese Fluent Bit-Beispielkonfigurationsdatei sendet Protokolldaten von Fluent Bit an eine Ingestion-Pipeline. OpenSearch Weitere Informationen zur Erfassung von Protokolldaten finden Sie unter Log Analytics in der Data Prepper-Dokumentation.

Beachten Sie Folgendes:

- Der `host` Wert muss Ihr Pipeline-Endpunkt sein. z. B. *`pipeline-endpoint`*`.us-east-1.osis.amazonaws.com`.
- Der `aws_service`-Wert muss `osis` lauten.
- Der `aws_role_arn` Wert ist der ARN der AWS IAM-Rolle, den der Client annehmen und für die Signature Version 4-Authentifizierung verwenden soll.

```
[INPUT]
  name                  tail
  refresh_interval      5
  path                  /var/log/test.log
  read_from_head        true

[OUTPUT]
  Name http
  Match *
  Host pipeline-endpoint.us-east-1.osis.amazonaws.com
  Port 443
```

```
  URI /log/ingest
  Format json
  aws_auth true
  aws_region us-east-1
  aws_service osis
  aws_role_arn arn:aws:iam::{account-id}:role/ingestion-role
  Log_Level trace
  tls On
```

Anschließend können Sie eine OpenSearch Ingestion-Pipeline wie die folgende konfigurieren, deren Quelle HTTP ist:

```
version: "2"
unaggregated-log-pipeline:
  source:
    http:
      path: "/log/ingest"
  processor:
    - grok:
        match:
          log:
            - "%{TIMESTAMP_ISO8601:timestamp} %{NOTSPACE:network_node}
 %{NOTSPACE:network_host} %{IPORHOST:source_ip}:%{NUMBER:source_port:int} ->
 %{IPORHOST:destination_ip}:%{NUMBER:destination_port:int} %{GREEDYDATA:details}"
    - grok:
        match:
          details:
            - "'%{NOTSPACE:http_method} %{NOTSPACE:http_uri}' %{NOTSPACE:protocol}"
            - "TLS%{NOTSPACE:tls_version} %{GREEDYDATA:encryption}"
            - "%{NUMBER:status_code:int} %{NUMBER:response_size:int}"
    - delete_entries:
        with_keys: ["details", "log"]

  sink:
    - opensearch:
        hosts: ["https://search-domain-endpoint.us-east-1.es.amazonaws.com"]
        index: "index_name"
        index_type: custom
        bulk_size: 20
        aws:
          # IAM role that the pipeline assumes to access the domain sink
          sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
          region: "us-east-1"
```

Verwenden einer OpenSearch Ingestion-Pipeline mit Fluentd

Fluentd ist ein Open-Source-Ökosystem zur Datenerfassung, das SDKs für verschiedene Sprachen und Unterprojekte wie Fluent Bit bereitstellt. Diese Fluentd-Beispielkonfigurationsdatei sendet Protokolldaten von Fluentd an eine Ingestion-Pipeline. OpenSearch Weitere Informationen zur Erfassung von Protokolldaten finden Sie unter Log Analytics in der Data Prepper-Dokumentation.

Beachten Sie Folgendes:

- Der `endpoint` Wert muss Ihr Pipeline-Endpunkt sein. z. B. *`pipeline-endpoint`*`.us-east-1.osis.amazonaws.com/apache-log-pipeline/logs`.
- Der `aws_service`-Wert muss `osis` lauten.
- Der `aws_role_arn` Wert ist der ARN der AWS IAM-Rolle, den der Client annehmen und für die Signature Version 4-Authentifizierung verwenden soll.

```
<source>
  @type tail
  path logs/sample.log
  path_key log
  tag apache
  <parse>
    @type none
  </parse>
</source>

<filter apache>
  @type record_transformer
  <record>
    log ${record["message"]}
  </record>
</filter>

<filter apache>
  @type record_transformer
  remove_keys message
</filter>

<match apache>
  @type http
  endpoint pipeline-endpoint.us-east-1.osis.amazonaws.com/apache-log-pipeline/logs
  json_array true
```

```
  <auth>
    method aws_sigv4
    aws_service osis
    aws_region us-east-1
    aws_role_arn arn:aws:iam::{account-id}:role/ingestion-role
  </auth>

  <format>
    @type json
  </format>

  <buffer>
    flush_interval 1s
  </buffer>
</match>
```

Anschließend können Sie eine OpenSearch Ingestion-Pipeline wie die folgende konfigurieren, deren Quelle HTTP ist:

```
version: "2"
apache-log-pipeline:
  source:
    http:
      path: "/${pipelineName}/logs"
  processor:
    - grok:
        match:
          log:
            - "%{TIMESTAMP_ISO8601:timestamp} %{NOTSPACE:network_node}
 %{NOTSPACE:network_host} %{IPORHOST:source_ip}:%{NUMBER:source_port:int} ->
 %{IPORHOST:destination_ip}:%{NUMBER:destination_port:int} %{GREEDYDATA:details}"
  sink:
    - opensearch:
        hosts: ["https://search-domain-endpoint.us-east-1.es.amazonaws.com"]
        index: "index_name"
        aws_sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
        aws_region: "us-east-1"
        aws_sigv4: true
```

Verwenden einer OpenSearch Ingestion-Pipeline mit Collector OpenTelemetry

Diese OpenTelemetry Beispielkonfigurationsdatei exportiert Trace-Daten aus dem OpenTelemetry Collector und sendet sie an eine OpenSearch Ingestion-Pipeline. Weitere Informationen zur Erfassung von Trace-Daten finden Sie unter Trace Analytics in der Data Prepper-Dokumentation.

Beachten Sie Folgendes:

- Der `endpoint` Wert muss Ihren Pipeline-Endpunkt enthalten. z. B. `https://pipeline-endpoint.us-east-1.osis.amazonaws.com`.
- Der `service`-Wert muss `osis` lauten.
- Die `compression` Option für den OTLP/HTTP-Exporter muss mit der `compression` Option in der Quelle der Pipeline übereinstimmen. OpenTelemetry

```
extensions:
  sigv4auth:
    region: "us-east-1"
    service: "osis"

receivers:
  jaeger:
    protocols:
      grpc:

exporters:
  otlphttp:
    traces_endpoint: "https://pipeline-endpoint.us-east-1.osis.amazonaws.com/v1/traces"
    auth:
      authenticator: sigv4auth
    compression: none

service:
  extensions: [sigv4auth]
  pipelines:
    traces:
      receivers: [jaeger]
      exporters: [otlphttp]
```

Sie können dann eine OpenSearch Ingestion-Pipeline wie die folgende konfigurieren, die das OTel Trace-Plugin als Quelle angibt:

```
version: "2"
otel-trace-pipeline:
  source:
    otel_trace_source:
      path: "/v1/traces"
  processor:
    - trace_peer_forwarder:
  sink:
    - pipeline:
        name: "trace-pipeline"
    - pipeline:
        name: "service-map-pipeline"
trace-pipeline:
  source:
    pipeline:
      name: "otel-trace-pipeline"
  processor:
    - otel_traces:
  sink:
    - opensearch:
        hosts: ["https://search-domain-endpoint.us-east-1.es.amazonaws.com"]
        index_type: trace-analytics-raw
        aws:
          # IAM role that OpenSearch Ingestion assumes to access the domain sink
          sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
          region: "us-east-1"

service-map-pipeline:
  source:
    pipeline:
      name: "otel-trace-pipeline"
  processor:
    - service_map:
  sink:
    - opensearch:
        hosts: ["https://search-domain-endpoint.us-east-1.es.amazonaws.com"]
        index_type: trace-analytics-service-map
        aws:
          # IAM role that the pipeline assumes to access the domain sink
          sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
```

```
          region: "us-east-1"
```

Ein weiteres Beispiel für eine Pipeline finden Sie im vorkonfigurierten Blueprint für Trace-Analysen. Weitere Informationen finden Sie unter the section called “Verwenden von Blueprints zum Erstellen einer Pipeline”.

Nächste Schritte

Nachdem Sie Ihre Daten in eine Pipeline exportiert haben, können Sie sie von der OpenSearch Service-Domäne abfragen, die als Senke für die Pipeline konfiguriert ist. Die folgenden Ressourcen können Ihnen den Einstieg erleichtern:

- Beobachtbarkeit
- the section called “Trace Analytics”
- the section called “Piped Processing Language”

Migrieren von Daten zwischen Domains und Sammlungen mithilfe von Amazon OpenSearch Ingestion

Sie können OpenSearch Ingestion-Pipelines verwenden, um Daten zwischen Amazon OpenSearch Service-Domains oder OpenSearch serverlosen VPC-Sammlungen zu migrieren. Dazu richten Sie eine Pipeline ein, in der Sie eine Domain oder Sammlung als Quelle und eine andere Domain oder Sammlung als Senke konfigurieren. Dadurch werden Ihre Daten effektiv von einer Domain oder Sammlung zur anderen migriert.

Um Daten zu migrieren, benötigen Sie die folgenden Ressourcen:

- Eine OpenSearch Quelldienstdomäne oder eine OpenSearch serverlose VPC-Sammlung. Diese Domain oder Sammlung enthält die Daten, die Sie migrieren möchten. Wenn Sie eine Domain verwenden, muss sie OpenSearch Version 1.0 oder höher oder Elasticsearch Version 7.4 oder höher ausführen. Die Domain muss außerdem über eine Zugriffsrichtlinie verfügen, die Ihrer Pipeline-Rolle die entsprechenden Berechtigungen gewährt.
- Eine separate Domain oder VPC-Sammlung, in die Sie Ihre Daten migrieren möchten. Diese Domain oder Sammlung fungiert als Pipeline-Senke.
- Eine Pipeline-Rolle, die OpenSearch Ingestion zum Lesen und Schreiben in Ihre Sammlung oder Domain verwendet. Sie nehmen den Amazon-Ressourcennamen (ARN) dieser Rolle in Ihre Pipeline-Konfiguration auf. Weitere Informationen finden Sie in den folgenden Ressourcen:

- the section called “Pipelines Zugriff auf Domains gewähren”
- the section called “Pipelines Zugriff auf Sammlungen gewähren”

Themen

Einschränkungen

Die folgenden Einschränkungen gelten, wenn Sie OpenSearch Service-Domains oder OpenSearch Serverless-Sammlungen als Senken kennzeichnen:

- Eine Pipeline kann nicht in mehr als eine VPC-Domäne schreiben.
- Sie können nur Daten zu oder aus OpenSearch serverlosen Sammlungen migrieren, die VPC-Zugriff verwenden. Öffentliche Sammlungen werden nicht unterstützt.
- Sie können keine Kombination aus VPC und öffentlichen Domänen in einer einzigen Pipeline-Konfiguration angeben.
- In einer einzigen Pipeline-Konfiguration können Sie maximal 20 Senken verwenden, die keine Pipeline sind.
- Sie können in einer einzigen Pipeline-Konfiguration maximal drei verschiedene AWS-Regionen Senken angeben.
- Bei einer Pipeline mit mehreren Senken kann es im Laufe der Zeit zu einer Verringerung der Verarbeitungsgeschwindigkeit kommen, wenn eine der Senken zu lange ausgefallen ist oder nicht über genügend Kapazität für den Empfang eingehender Daten verfügt.

OpenSearch Dienst als Quelle

Aus der Domäne oder Sammlung, die Sie als Quelle angeben, werden die Daten migriert.

Eine Pipeline-Rolle in IAM erstellen

Um Ihre OpenSearch Ingestion-Pipeline zu erstellen, müssen Sie zunächst eine Pipeline-Rolle erstellen, um Lese- und Schreibzugriff zwischen Domänen oder Sammlungen zu gewähren. Führen Sie dazu die folgenden Schritte aus:

1. Erstellen Sie eine neue Berechtigungsrichtlinie in IAM, um sie an die Pipeline-Rolle anzuhängen. Stellen Sie sicher, dass Sie Berechtigungen zum Lesen von der Quelle und zum Schreiben in die Senke zulassen. Weitere Informationen zum Einrichten von IAM-Pipelineberechtigungen für OpenSearch Dienstdomänen finden Sie unter the section called “Pipelines Zugriff auf Domains gewähren” undthe section called “Pipelines Zugriff auf Sammlungen gewähren”.
2. Geben Sie innerhalb der Pipeline-Rolle die folgenden Berechtigungen an, um aus der Quelle zu lesen:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":"es:ESHttpGet",
         "Resource":[
            "arn:aws:es:us-east-1:{account-id}:domain/{domain-name}/",
            "arn:aws:es:us-east-1:{account-id}:domain/{domain-name}/_cat/indices",
            "arn:aws:es:us-east-1:{account-id}:domain/{domain-name}/_search",
            "arn:aws:es:us-east-1:{account-id}:domain/{domain-name}/_search/scroll",
            "arn:aws:es:us-east-1:{account-id}:domain/{domain-name}/*/_search"
         ]
      },
      {
         "Effect":"Allow",
         "Action":"es:ESHttpPost",
         "Resource":[
            "arn:aws:es:us-east-1:{account-id}:domain/{domain-name}/*/_search/
point_in_time",
            "arn:aws:es:us-east-1:{account-id}:domain/{domain-name}/*/_search/scroll"
         ]
      },
      {
         "Effect":"Allow",
         "Action":"es:ESHttpDelete",
         "Resource":[
```

```
            "arn:aws:es:us-east-1:{account-id}:domain/{domain-name}/_search/
point_in_time",
            "arn:aws:es:us-east-1:{account-id}:domain/{domain-name}/_search/scroll"
         ]
      }
   ]
}
```

Eine Pipeline erstellen

Nachdem Sie die Richtlinie an die Pipeline-Rolle angehängt haben, verwenden Sie den AWSOpenSearchDataMigrationPipelineMigrations-Blueprint, um die Pipeline zu erstellen. Dieser Blueprint enthält eine Standardkonfiguration für die Migration von Daten zwischen OpenSearch Dienstdomänen oder Sammlungen. Weitere Informationen finden Sie unter the section called “Verwenden von Blueprints zum Erstellen einer Pipeline”.

> **Note**
>
> OpenSearch Die Aufnahme verwendet Ihre Quelldomänenversion und -verteilung, um zu bestimmen, welcher Mechanismus für die Migration verwendet werden soll. Einige Versionen unterstützen diese Option. `point_in_time` OpenSearch Serverless verwendet die `search_after` Option, weil sie `point_in_time` oder `scroll` nicht unterstützt.

Während des Migrationsprozesses werden möglicherweise gerade neue Indizes erstellt, oder Dokumente werden während der Migration aktualisiert. Aus diesem Grund müssen Sie möglicherweise entweder einen einzelnen Scan oder mehrere Scans Ihrer Domainindexdaten durchführen, um neue oder aktualisierte Daten zu erhalten.

Geben Sie die Anzahl der auszuführenden Scans an, indem Sie das `index_read_count` und `interval` in der Pipeline-Konfiguration konfigurieren. Das folgende Beispiel zeigt, wie mehrere Scans durchgeführt werden:

```
scheduling:
    interval: "PT2H"
    index_read_count: 3
    start_time: "2023-06-02T22:01:30.00Z"
```

OpenSearch Ingestion verwendet die folgende Konfiguration, um sicherzustellen, dass Ihre Daten in denselben Index geschrieben werden und dieselbe Dokument-ID beibehalten wird:

```
index: "${getMetadata(\"opensearch-index\")}"
document_id: "${getMetadata(\"opensearch-document_id\")}"
```

Angabe mehrerer OpenSearch Service-Domain-Senken

Sie können mehrere öffentliche OpenSearch Dienstdomänen als Ziele für Ihre Daten angeben. Sie können diese Funktion verwenden, um bedingtes Routing durchzuführen oder eingehende Daten in mehrere OpenSearch Dienstdomänen zu replizieren. Sie können bis zu 10 verschiedene öffentliche OpenSearch Dienstdomänen als Senken angeben.

Im folgenden Beispiel werden eingehende Daten bedingt an verschiedene OpenSearch Dienstdomänen weitergeleitet:

```
...
  route:
    - 2xx_status: "/response >= 200 and /response < 300"
    - 5xx_status: "/response >= 500 and /response < 600"
  sink:
    - opensearch:
        hosts: [ "https://search-response-2xx.us-east-1.es.amazonaws.com" ]
        aws:
          sts_role_arn: "arn:aws:iam::123456789012:role/Example-Role"
          region: "us-east-1"
        index: "response-2xx"
        routes:
          - 2xx_status
    - opensearch:
        hosts: [ "https://search-response-5xx.us-east-1.es.amazonaws.com" ]
        aws:
          sts_role_arn: "arn:aws:iam::123456789012:role/Example-Role"
          region: "us-east-1"
        index: "response-5xx"
        routes:
          - 5xx_status
```

Migrieren von Daten zu einer OpenSearch serverlosen VPC-Sammlung

Sie können OpenSearch Ingestion verwenden, um Daten von einer OpenSearch Quell-Servicedomäne oder einer OpenSearch serverlosen Sammlung zu einer VPC-Sammelsenke zu migrieren. Sie müssen in der Pipeline-Konfiguration eine Netzwerkzugriffsrichtlinie angeben. Weitere Informationen zur Datenaufnahme in OpenSearch serverlose VPC-Sammlungen finden Sie unter. the section called “Tutorial: Daten in eine Sammlung aufnehmen”

So migrieren Sie Daten zu einer VPC-Sammlung

1. Erstellen Sie eine OpenSearch serverlose Sammlung. Anweisungen finden Sie unter the section called “Tutorial: Daten in eine Sammlung aufnehmen”.
2. Erstellen Sie eine Netzwerkrichtlinie für die Sammlung, die den VPC-Zugriff sowohl auf den Sammlungsendpunkt als auch auf den Dashboards-Endpunkt festlegt. Anweisungen finden Sie unter the section called “Netzwerkzugriff”.
3. Erstellen Sie die Pipeline-Rolle, falls Sie noch keine haben. Anweisungen finden Sie unter the section called “Rolle „Pipeline“”.
4. Erstellen Sie die Pipeline. Detaillierte Anweisungen finden Sie unter the section called “Verwenden von Blueprints zum Erstellen einer Pipeline”.

Verwendung der AWS SDKs zur Interaktion mit Amazon Ingestion OpenSearch

Dieser Abschnitt enthält ein Beispiel für die Verwendung der AWS SDKs zur Interaktion mit Amazon OpenSearch Ingestion. Das Codebeispiel zeigt, wie Sie eine Domain und eine Pipeline erstellen und dann Daten in die Pipeline aufnehmen.

Themen

- Python

Python

Das folgende Beispielskript verwendet die, AWS SDK for Python (Boto3)um eine IAM-Pipeline-Rolle, eine Domäne, in die Daten geschrieben werden, und eine Pipeline, über die Daten aufgenommen werden, zu erstellen. Anschließend wird mithilfe der `requests` HTTP-Bibliothek eine Beispielprotokolldatei in die Pipeline aufgenommen.

Führen Sie die folgenden Befehle aus, um die erforderlichen Abhängigkeiten zu installieren:

```
pip install boto3
pip install botocore
pip install requests
pip install requests-auth-aws-sigv4
```

Ersetzen Sie innerhalb des Skripts die Konto-IDs in den Zugriffsrichtlinien durch Ihre AWS-Konto ID. Optional können Sie auch das `region` ändern.

```
import boto3
import botocore
from botocore.config import Config
import requests
from requests_auth_aws_sigv4 import AWSSigV4
import time

# Build the client using the default credential configuration.
# You can use the CLI and run 'aws configure' to set access key, secret
# key, and default region.

my_config = Config(
    # Optionally lets you specify a Region other than your default.
    region_name='us-east-1'
)

opensearch = boto3.client('opensearch', config=my_config)
iam = boto3.client('iam', config=my_config)
osis = boto3.client('osis', config=my_config)

domainName = 'test-domain'  # The name of the domain
pipelineName = 'test-pipeline' # The name of the pipeline

def createPipelineRole(iam, domainName):
    """Creates the pipeline role"""
    response = iam.create_policy(
        PolicyName='pipeline-policy',
        PolicyDocument=f'{{\"Version\":\"2012-10-17\",\"Statement\":[{{\"Effect
\":\"Allow\",\"Action\":\"es:DescribeDomain\",\"Resource\":\"arn:aws:es:us-
east-1:123456789012:domain\/{domainName}\"}},{{\"Effect\":\"Allow\",\"Action\":
\"es:ESHttp*\",\"Resource\":\"arn:aws:es:us-east-1:123456789012:domain\/{domainName}\/*
\"}}]}}'
    )
```

```
    policyarn = response['Policy']['Arn']

    response = iam.create_role(
        RoleName='PipelineRole',
        AssumeRolePolicyDocument='{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect
\":\"Allow\",\"Principal\":{\"Service\":\"osis-pipelines.amazonaws.com\"},\"Action\":
\"sts:AssumeRole\"}]}'
    )
    rolename=response['Role']['RoleName']

    response = iam.attach_role_policy(
        RoleName=rolename,
        PolicyArn=policyarn
    )

    print('Creating pipeline role...')
    time.sleep(10)
    print('Role created: ' + rolename)

def createDomain(opensearch, domainName):
    """Creates a domain to ingest data into"""
    response = opensearch.create_domain(
        DomainName=domainName,
        EngineVersion='OpenSearch_2.3',
        ClusterConfig={
            'InstanceType': 't2.small.search',
            'InstanceCount': 5,
            'DedicatedMasterEnabled': True,
            'DedicatedMasterType': 't2.small.search',
            'DedicatedMasterCount': 3
        },
        # Many instance types require EBS storage.
        EBSOptions={
            'EBSEnabled': True,
            'VolumeType': 'gp2',
            'VolumeSize': 10
        },
        AccessPolicies=f'{{\"Version\":\"2012-10-17\",\"Statement\":[{{\"Effect\":
\"Allow\",\"Principal\":{{\"AWS\":\"arn:aws:iam::123456789012:role\/PipelineRole
\"}},\"Action\":\"es:*\",\"Resource\":\"arn:aws:es:us-east-1:123456789012:domain\/
{domainName}\/*\"}}]}}',
        NodeToNodeEncryptionOptions={
            'Enabled': True
        }
```

```
    )
    return(response)

def waitForDomainProcessing(opensearch, domainName):
    """Waits for the domain to be active"""
    try:
        response = opensearch.describe_domain(
            DomainName=domainName
        )
        # Every 30 seconds, check whether the domain is processing.
        while 'Endpoint' not in response['DomainStatus']:
            print('Creating domain...')
            time.sleep(60)
            response = opensearch.describe_domain(
                DomainName=domainName)

        # Once we exit the loop, the domain is ready for ingestion.
        endpoint = response['DomainStatus']['Endpoint']
        print('Domain endpoint ready to receive data: ' + endpoint)
        createPipeline(osis, endpoint)

    except botocore.exceptions.ClientError as error:
        if error.response['Error']['Code'] == 'ResourceNotFoundException':
            print('Domain not found.')
        else:
            raise error

def createPipeline(osis, endpoint):
    """Creates a pipeline using the domain and pipeline role"""
    try:
        definition = f'version: \"2\"\nlog-pipeline:\n  source:\n    http:\n      path:
 \"/${{pipelineName}}/logs\"\n  processor:\n    - date:\n        from_time_received:
 true\n        destination: \"@timestamp\"\n  sink:\n    - opensearch:\n        hosts:
 [ \"https://{endpoint}\" ]\n        index: \"application_logs\"\n        aws:\n
     sts_role_arn: \"arn:aws:iam::123456789012:role/PipelineRole\"\n          region:
 \"us-east-1\"'
        response = osis.create_pipeline(
            PipelineName=pipelineName,
            MinUnits=4,
            MaxUnits=9,
            PipelineConfigurationBody=definition
        )

        response = osis.get_pipeline(
```

```
                PipelineName=pipelineName
        )

        # Every 30 seconds, check whether the pipeline is active.
        while response['Pipeline']['Status'] == 'CREATING':
            print('Creating pipeline...')
            time.sleep(30)
            response = osis.get_pipeline(
                PipelineName=pipelineName)

        # Once we exit the loop, the pipeline is ready for ingestion.
        ingestionEndpoint = response['Pipeline']['IngestEndpointUrls'][0]
        print('Pipeline ready to ingest data at endpoint: ' + ingestionEndpoint)
        ingestData(ingestionEndpoint)

    except botocore.exceptions.ClientError as error:
        if error.response['Error']['Code'] == 'ResourceAlreadyExistsException':
            print('Pipeline already exists.')
            response = osis.get_pipeline(
                PipelineName=pipelineName
            )
            ingestionEndpoint = response['Pipeline']['IngestEndpointUrls'][0]
            ingestData(ingestionEndpoint)
        else:
            raise error


def ingestData(ingestionEndpoint):
    """Ingests a sample log file into the pipeline"""
    endpoint = 'https://' + ingestionEndpoint
    r = requests.request('POST', f'{endpoint}/log-pipeline/logs',

 data='[{"time":"2014-08-11T11:40:13+00:00","remote_addr":"122.226.223.69","status":"404","requ
 http://www.k2proxy.com//hello.html HTTP/1.1","http_user_agent":"Mozilla/4.0
 (compatible; WOW64; SLCC2;)"}]',
    auth=AWSSigV4('osis'))
    print('Ingesting sample log file into pipeline')
    print('Response: ' + r.text)

def main():
    createPipelineRole(iam, domainName)
    createDomain(opensearch, domainName)
    waitForDomainProcessing(opensearch, domainName)
```

```
if __name__ == "__main__":
    main()
```

Sicherheit bei Amazon OpenSearch Ingestion

Die Sicherheit in der Cloud hat bei AWS höchste Priorität. Als AWS-Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die zur Erfüllung der Anforderungen von Organisationen entwickelt wurden, für die Sicherheit eine kritische Bedeutung hat.

Sicherheit gilt zwischen AWS und Ihnen eine geteilte Verantwortung. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud – AWS ist dafür verantwortlich, die Infrastruktur zu schützen, mit der AWS-Services in der AWS-Cloud ausgeführt werden. AWS stellt Ihnen außerdem Services bereit, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der AWS-Compliance-Programme regelmäßig.
- Sicherheit in der Cloud – Ihr Verantwortungsumfang wird durch den AWS-Service bestimmt, den Sie verwenden. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

In dieser Dokumentation wird erläutert, wie das Modell der geteilten Verantwortung bei der Verwendung von OpenSearch Ingestion zum Tragen kommt. Die folgenden Themen zeigen, wie Sie OpenSearch Ingestion konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere AWS -Services nutzen können, die Ihnen helfen, Ihre OpenSearch Ingestion-Ressourcen zu überwachen und zu sichern.

Themen

Konfiguration des VPC-Zugriffs für Amazon OpenSearch Ingestion-Pipelines

Sie können über einen VPC-Endpunkt mit Schnittstelle auf Ihre Amazon OpenSearch Ingestion-Pipelines zugreifen. Eine VPC ist ein virtuelles Netzwerk, das Ihrem AWS-Konto gewidmet ist. Es ist

logisch von anderen virtuellen Netzwerken in der AWS Cloud isoliert. Der Zugriff auf eine Pipeline über einen VPC-Endpunkt ermöglicht eine sichere Kommunikation zwischen OpenSearch Ingestion und anderen Diensten innerhalb der VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS

OpenSearch Die Aufnahme stellt diese private Verbindung her, indem ein Schnittstellenendpunkt erstellt wird, der von betrieben wird. AWS PrivateLink Wir erstellen in jedem Subnetz, das Sie bei der Pipelineerstellung angeben, eine Endpunkt-Netzwerkschnittstelle. Dabei handelt es sich um vom Anforderer verwaltete Netzwerkschnittstellen, die als Einstiegspunkt für den Datenverkehr dienen, der für die Ingestion-Pipeline bestimmt ist. OpenSearch Sie können sich auch dafür entscheiden, die Schnittstellenendpunkte selbst zu erstellen und zu verwalten.

Mit einer VPC können Sie den Datenfluss durch Ihre OpenSearch Ingestion-Pipelines innerhalb der Grenzen der VPC erzwingen, anstatt über das öffentliche Internet. Pipelines, die sich nicht in einer VPC befinden, senden und empfangen Daten über öffentlich zugängliche Endpunkte und das Internet.

Eine Pipeline mit VPC-Zugriff kann in öffentliche Domänen oder OpenSearch VPC-Dienstdomänen sowie in öffentliche oder serverlose OpenSearch VPC-Sammlungen schreiben.

Themen

Überlegungen

Beachten Sie Folgendes, wenn Sie den VPC-Zugriff für eine Pipeline konfigurieren.

- Eine Pipeline muss sich nicht in derselben VPC wie ihre Senke befinden. Sie müssen auch keine Verbindung zwischen den beiden VPCs herstellen. OpenSearch Ingestion kümmert sich für Sie darum, sie zu verbinden.
- Sie können nur eine VPC für Ihre Pipeline angeben.

- Im Gegensatz zu öffentlichen Pipelines muss sich eine VPC-Pipeline in derselben AWS-Region Domäne oder Sammelsenke befinden, in die sie schreibt.
- Sie können wählen, ob Sie eine Pipeline in einem, zwei oder drei Subnetzen Ihrer VPC bereitstellen möchten. Die Subnetze sind auf dieselben Availability Zones verteilt, in denen Ihre Ingestion OpenSearch Compute Units (OCUs) bereitgestellt werden.
- Wenn Sie nur eine Pipeline in einem Subnetz bereitstellen und die Availability Zone ausfällt, können Sie keine Daten aufnehmen. Um eine hohe Verfügbarkeit zu gewährleisten, empfehlen wir, Pipelines mit zwei oder drei Subnetzen zu konfigurieren.
- Die Angabe einer Sicherheitsgruppe ist optional. Wenn Sie keine Sicherheitsgruppe angeben, verwendet OpenSearch Ingestion die Standardsicherheitsgruppe, die in der VPC angegeben ist.

Einschränkungen

Für Pipelines mit VPC-Zugriff gelten die folgenden Einschränkungen.

- Sie können die Netzwerkkonfiguration einer Pipeline nicht ändern, nachdem Sie sie erstellt haben. Wenn Sie eine Pipeline innerhalb einer VPC starten, können Sie sie später nicht in einen öffentlichen Endpunkt ändern und umgekehrt.
- Sie können Ihre Pipeline entweder mit einem Schnittstellen-VPC-Endpunkt oder einem öffentlichen Endpunkt starten, aber Sie können nicht beides tun. Wenn Sie eine Pipeline erstellen, müssen Sie sich für das eine oder das andere entscheiden.
- Nachdem Sie eine Pipeline mit VPC-Zugriff bereitgestellt haben, können Sie sie nicht auf eine andere VPC verschieben, und Sie können ihre Subnetze oder Sicherheitsgruppeneinstellungen nicht ändern.
- Wenn Ihre Pipeline in eine Domain oder Sammlungssenke schreibt, die VPC-Zugriff verwendet, können Sie nicht später zurückkehren und die Senke (VPC oder öffentlich) ändern, nachdem die Pipeline erstellt wurde. Sie müssen die Pipeline löschen und mit einer neuen Senke neu erstellen. Sie können immer noch von einer öffentlichen Senke zu einer Senke mit VPC-Zugriff wechseln.
- Sie können keinen kontenübergreifenden Aufnahmezugriff auf VPC-Pipelines gewähren.

Voraussetzungen

Bevor Sie eine Pipeline mit VPC-Zugriff bereitstellen können, müssen Sie Folgendes tun:

- Erstellen einer VPC

Um Ihre VPC zu erstellen, können Sie die Amazon VPC-Konsole, die AWS CLI oder eines der AWS SDKs verwenden. Weitere Informationen finden Sie unter Arbeiten mit freigegebenen VPCs im Amazon-VPC-Benutzerhandbuch. Wenn bereits eine VPC vorhanden ist, können Sie diesen Schritt überspringen.

- Reservieren von IP-Adressen

  OpenSearch Bei der Aufnahme wird in jedem Subnetz, das Sie bei der Pipelineerstellung angeben, eine elastic network interface platziert. Jeder Netzwerkschnittstelle ist eine IP-Adresse zugewiesen. Sie müssen eine IP-Adresse pro Subnetz für die Netzwerkschnittstellen reservieren.

Konfiguration des VPC-Zugriffs für eine Pipeline

Sie können den VPC-Zugriff für eine Pipeline in der OpenSearch Servicekonsole oder mithilfe der AWS CLI aktivieren.

Konsole

Sie konfigurieren den VPC-Zugriff während der Pipelineerstellung. Wählen Sie unter Netzwerk die Option VPC-Zugriff und konfigurieren Sie die folgenden Einstellungen:

Einstellung	Beschreibung
Endpunktverwaltung	Wählen Sie aus, ob Sie Ihre VPC-Endpoints selbst erstellen möchten oder ob Sie sie von OpenSearch Ingestion für Sie erstellen lassen möchten.
VPC	Wählen Sie für die Virtual Private Cloud (VPC) die ID, die Sie verwenden möchten. Die VPC und die Pipeline müssen identisch AWS-Region sein.
Subnets	Wählen Sie ein oder mehrere Subnetze aus. OpenSearch Der Service platziert einen VPC-Endpunkt und elastische Netzwerkschnittstellen in den Subnetzen.
Sicherheitsgruppen	Wählen Sie eine oder mehrere VPC-Sicherheitsgruppen aus, die es Ihrer gewünschten Anwendung ermöglichen, die OpenSearch Ingestion-Pipeline auf den von der Pipeline bereitgestellten Ports (80 oder 443) und Protokollen (HTTP oder HTTPs) zu erreichen.

Einstellung	Beschreibung
VPC-Anhangsoptionen	Wenn es sich bei Ihrer Quelle um einen selbstverwalteten Endpunkt handelt, fügen Sie Ihre Pipeline einer VPC hinzu. Wählen Sie eine der bereitgestellten Standard-CIDR-Optionen oder verwenden Sie ein benutzerdefiniertes CIDR.

CLI

Um den VPC-Zugriff mit dem zu konfigurieren AWS CLI, geben Sie den `--vpc-options` Parameter an:

```
aws osis create-pipeline \
  --pipeline-name vpc-pipeline \
  --min-units 4 \
  --max-units 10 \
  --vpc-options
 SecurityGroupIds={sg-12345678,sg-9012345},SubnetIds=subnet-1212234567834asdf \
  --pipeline-configuration-body "file://pipeline-config.yaml"
```

Selbstverwaltete VPC-Endpunkte

Wenn Sie eine Pipeline erstellen, können Sie Endpoint Management verwenden, um eine Pipeline mit selbstverwalteten Endpunkten oder dienstverwalteten Endpunkten zu erstellen. Endpoint Management ist optional und verwendet standardmäßig Endgeräte, die von Ingestion verwaltet werden. OpenSearch

Informationen zum Erstellen einer Pipeline mit einem selbstverwalteten VPC-Endpunkt in der AWS Management Console finden Sie unter Pipelines mit der OpenSearch Servicekonsole erstellen. Um eine Pipeline mit einem selbstverwalteten VPC-Endpunkt in der zu erstellen AWS CLI, können Sie den `--vpc-options` Parameter im Befehl create-pipeline verwenden:

```
--vpc-options SubnetIds=subnet-abcdef01234567890,VpcEndpointManagement=CUSTOMER
```

Sie können selbst einen Endpunkt für Ihre Pipeline erstellen, wenn Sie Ihren Endpunktdienst angeben. Um Ihren Endpunktdienst zu finden, verwenden Sie den Befehl get-pipeline, der eine Antwort ähnlich der folgenden zurückgibt:

```
"vpcEndpointService" : "com.amazonaws.osis.us-east-1.pipeline-
id-1234567890abcdef1234567890",
```

```
"vpcEndpoints" : [
  {
    "vpcId" : "vpc-1234567890abcdef0",
    "vpcOptions" : {
      "subnetIds" : [ "subnet-abcdef01234567890", "subnet-021345abcdef6789" ],
      "vpcEndpointManagement" : "CUSTOMER"
    }
  }
```

Verwenden Sie die Antwort `vpcEndpointService` von der Antwort, um einen VPC-Endpunkt mit dem AWS Management Console oder AWS CLI zu erstellen.

Wenn Sie selbstverwaltete VPC-Endpoints verwenden, müssen Sie die DNS-Attribute `enableDnsSupport` und `enableDnsHostnames` in Ihrer VPC aktivieren. Beachten Sie, dass Sie, wenn Sie eine Pipeline mit einem selbstverwalteten Endpunkt haben, den Sie beenden und neu starten, den VPC-Endpunkt in Ihrem Konto neu erstellen müssen.

Service-verknüpfte Rolle für den VPC-Zugriff

Eine Service-verknüpfte Rolle ist ein spezieller Typ der IAM-Rolle zum Übertragen von Berechtigungen an einen Service, damit dieser Ressourcen für Sie erstellen und verwalten kann. Wenn Sie sich für einen vom Service verwalteten VPC-Endpunkt entscheiden, benötigt OpenSearch Ingestion eine serviceverknüpfte Rolle, die aufgerufen wird, AWSServiceRoleForAmazonOpenSearchIngestionServiceum auf Ihre VPC zuzugreifen, den Pipeline-Endpunkt zu erstellen und Netzwerkschnittstellen in einem Subnetz Ihrer VPC zu platzieren.

Wenn Sie sich für einen selbstverwalteten VPC-Endpunkt entscheiden, erfordert OpenSearch Ingestion eine serviceverknüpfte Rolle namens. AWSServiceRoleForOpensearchIngestionSelfManagedVpce Weitere Informationen zu diesen Rollen, ihren Berechtigungen und wie Sie sie löschen können, finden Sie unter. the section called “Rolle zur Erstellung von Pipelines”

OpenSearch Die Aufnahme erstellt die Rolle automatisch, wenn Sie eine Aufnahme-Pipeline erstellen. Damit diese automatische Erstellung erfolgreich ist, muss der Benutzer, der die erste Pipeline in einem Konto erstellt, über Berechtigungen für die Aktion verfügen. `iam:CreateServiceLinkedRole` Weitere Informationen finden Sie unter Berechtigungen von Service-verknüpften Rollen im IAM-Benutzerhandbuch. Sie können die Rolle in der AWS Identity and Access Management (IAM-) Konsole anzeigen, nachdem sie erstellt wurde.

Identity and Access Management für Amazon OpenSearch Ingestion

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu kontrollieren. AWS IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Ingestion-Ressourcen zu verwenden OpenSearch . IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

Identitätsbasierte Richtlinien für die Datenerfassung OpenSearch

Unterstützt Richtlinien auf Identitätsbasis.	Ja

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für Ingestion OpenSearch

Beispiele für identitätsbasierte Richtlinien zur Datenerfassung finden OpenSearch Sie unter. the section called “Beispiele für identitätsbasierte Richtlinien”

Politische Maßnahmen für Ingestion OpenSearch

Unterstützt Richtlinienaktionen	Ja

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Bei Richtlinienaktionen in OpenSearch Ingestion wird vor der Aktion das folgende Präfix verwendet:

```
osis
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [
      "osis:action1",
      "osis:action2"
         ]
```

Sie können mehrere Aktionen mit Platzhalterzeichen (*) angeben. Beispielsweise können Sie alle Aktionen festlegen, die mit dem Wort `List` beginnen, einschließlich der folgenden Aktion:

```
"Action": "osis:List*"
```

Beispiele für identitätsbasierte Richtlinien OpenSearch bei Ingestion finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Serverless OpenSearch

Richtlinienressourcen für Ingestion OpenSearch

Unterstützt Richtlinienressourcen	Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das bedeutet die Festlegung, welcher Prinzipal Aktionen für welche Ressourcen unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"
```

Schlüssel zu den Richtlinienbedingungen für Amazon OpenSearch Ingestion

Unterstützt servicespezifische Richtlini enbedingungsschlüssel	Nein

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen AND-Operation

aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, AWS wertet die Bedingung mithilfe einer logischen OR Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Eine Liste der OpenSearch Ingestion-Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für Amazon OpenSearch Ingestion in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von Amazon OpenSearch Ingestion definierte Aktionen.

ABAC mit Ingestion OpenSearch

Unterstützt ABAC (Tags in Richtlinien)	Ja

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In werden AWS diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter Was ist ABAC? im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Weitere Informationen zum Taggen von OpenSearch Ingestion-Ressourcen finden Sie unter. the section called “Kennzeichnen von Rohrleitungen”

Temporäre Anmeldeinformationen mit Ingestion verwenden OpenSearch

Unterstützt temporäre Anmeldeinformationen	Ja

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen, die mit temporären Anmeldeinformationen AWS-Services funktionieren AWS-Services , finden Sie im IAM-Benutzerhandbuch unter Diese Option funktioniert mit IAM.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Passwort anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter Wechseln zu einer Rolle (Konsole) im IAM-Benutzerhandbuch.

Mithilfe der AWS API AWS CLI oder können Sie temporäre Anmeldeinformationen manuell erstellen. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

Dienstbezogene Rollen für Ingestion OpenSearch

Unterstützt serviceverknüpfte Rollen	Ja

Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene

Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

OpenSearch Bei der Aufnahme wird eine dienstbezogene Rolle mit dem Namen verwendet. `AWSServiceRoleForAmazonOpenSearchIngestionService` Die angegebene serviceverknüpfte Rolle `AWSServiceRoleForOpensearchIngestionSelfManagedVpce` ist auch für Pipelines mit selbstverwalteten VPC-Endpunkten verfügbar. Einzelheiten zum Erstellen und Verwalten von serviceverknüpften OpenSearch Ingestion-Rollen finden Sie unter. the section called “Rolle zur Erstellung von Pipelines”

Beispiele für identitätsbasierte Richtlinien für Ingestion OpenSearch

Standardmäßig sind Benutzer und Rollen nicht berechtigt, Ingestion-Ressourcen zu erstellen oder zu ändern. OpenSearch Sie können auch keine Aufgaben mithilfe der AWS Management Console, AWS Command Line Interface (AWS CLI) oder AWS API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Einzelheiten zu den von Amazon OpenSearch Ingestion definierten Aktionen und Ressourcentypen, einschließlich des Formats der ARNs für jeden Ressourcentyp, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon OpenSearch Ingestion in der Service Authorization Reference.

Themen

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien sind sehr leistungsfähig. Sie bestimmen, ob jemand OpenSearch Ingestion-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann

zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

Identitätsbasierte Richtlinien legen fest, ob jemand OpenSearch Ingestion-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um Ihren Benutzern und Workloads zunächst Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien oder AWS -verwaltete Richtlinien für Auftrags-Funktionen im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere

und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung zum IAM Access Analyzer im IAM-Benutzerhandbuch.

- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Konfigurieren eines MFA-geschützten API-Zugriffs im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Ingestion in der Konsole verwenden OpenSearch

Um über die OpenSearch Servicekonsole auf OpenSearch Ingestion zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Informationen zu den OpenSearch Ingestion-Ressourcen in Ihrem Konto aufzulisten und einzusehen. AWS Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (wie IAM-Rollen) mit dieser Richtlinie.

Sie müssen Benutzern, die nur die API AWS CLI oder die API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. AWS Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die Sie ausführen möchten.

Die folgende Richtlinie ermöglicht es einem Benutzer, über die OpenSearch Servicekonsole auf OpenSearch Ingestion zuzugreifen:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Resource": "*",
            "Effect": "Allow",
            "Action": [
                "osis:ListPipelines",
                "osis:GetPipeline",
                "osis:ListPipelineBlueprints",
                "osis:GetPipelineBlueprint",
                "osis:GetPipelineChangeProgress"
            ]
```

```
        }
    ]
}
```

Alternativ können Sie die the section called “AmazonOpenSearchIngestionReadOnlyAccess” AWS verwaltete Richtlinie verwenden, die nur Lesezugriff auf alle OpenSearch Ingestion-Ressourcen für einen gewährt. AWS-Konto

Verwaltung von OpenSearch Ingestion-Pipelines

Diese Richtlinie ist ein Beispiel für eine „Pipeline-Admin“ -Richtlinie, die es einem Benutzer ermöglicht, Amazon OpenSearch Ingestion-Pipelines zu verwalten und zu verwalten. Der Benutzer kann Pipelines erstellen, anzeigen und löschen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Resource": "arn:aws:osis:region:123456789012:pipeline/*",
            "Action": [
                "osis:CreatePipeline",
                "osis:DeletePipeline",
                "osis:UpdatePipeline",
                "osis:ValidatePipeline",
                "osis:StartPipeline",
                "osis:StopPipeline"
            ],
            "Effect": "Allow"
        },
        {
            "Resource": "*",
            "Action": [
                "osis:ListPipelines",
                "osis:GetPipeline",
                "osis:ListPipelineBlueprints",
                "osis:GetPipelineBlueprint",
                "osis:GetPipelineChangeProgress"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Daten in eine OpenSearch Ingestion-Pipeline aufnehmen

Diese Beispielrichtlinie ermöglicht es einem Benutzer oder einer anderen Entität, Daten in eine Amazon OpenSearch Ingestion-Pipeline in ihrem Konto aufzunehmen. Der Benutzer kann die Pipelines nicht ändern.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Resource": "arn:aws:osis:region:123456789012:pipeline/*",
            "Action": [
                "osis:Ingest"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Protokollieren von Amazon OpenSearch Ingestion-API-Aufrufen mit AWS CloudTrail

Amazon OpenSearch Ingestion ist in einen Service integriertAWS CloudTrail, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem AWS -Service in OpenSearch Ingestion durchgeführten Aktionen bietet.

CloudTrailerfasst alle API-Aufrufe für OpenSearch Ingestion als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe aus dem OpenSearch Ingestion-Bereich der OpenSearch Servicekonsole und Code-Aufrufe an die OpenSearch Ingestion-API-Vorgänge.

Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket, einschließlich Ereignisse für OpenSearch Ingestion aktivieren. Auch wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse in der CloudTrail-Konsole in Event history (Ereignisverlauf) anzeigen.

Mit den von CloudTrail gesammelten Informationen können Sie die an gestellte AnfrageOpenSearch, die IP-Adresse, von der die Anfrage gestellt wurde, den Zeitpunkt der Anfrage und zusätzliche Details bestimmen.

Weitere Informationen zu CloudTrail finden Sie im AWS CloudTrail-Benutzerhandbuch.

OpenSearchInformationen zur Einnahme in CloudTrail

CloudTrail wird beim Erstellen Ihres Kontos auf AWS-Konto aktiviert. Die in OpenSearch Ingestion auftretenden Aktivitäten werden als CloudTrail Ereignis zusammen mit anderen AWS -Serviceereignissen im Ereignisverlauf aufgezeichnet. Sie können die neusten Ereignisse in Ihr(em) AWS-Konto anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail-Ereignisverlauf.

Zur kontinuierlichen Aufzeichnung der Ereignisse in Ihrem -KontoAWS-Konto, einschließlich der Ereignisse für OpenSearch Ingestion, einen Trail. Ein Trail ermöglicht CloudTrail es Protokolldateien in einem Amazon-S3-Bucket bereitzustellen. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen.

Der Trail protokolliert Ereignisse aus allen Regionen in der AWS-Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon S3 Bucket bereit. Darüber hinaus können Sie andere AWS-Services konfigurieren, um die in den CloudTrail-Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie unter:

- Übersicht zum Erstellen eines Trails
- In CloudTrail unterstützte Services und Integrationen
- Konfigurieren von Amazon SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail-Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail-Protokolldateien aus mehreren Konten

Alle OpenSearch Ingestion-Aktionen werden von der Ingestion-API-Referenz protokolliert CloudTrail und sind in OpenSearchdieser dokumentiert. Zum Beispiel werden durch Aufrufe der `CreateCollection`-, `ListCollections`- und `DeleteCollection`-Aktionen Einträge in den CloudTrail-Protokolldateien generiert.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen helfen Ihnen beim Bestimmen der Folgenden Elemente:

- Ob die Anfrage mit Stammbenutzer- oder AWS Identity and Access Management (IAM)-Anmeldeinformationen ausgeführt wurde.
- Ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer ausgeführt wurde.

- Gibt an, ob die Anforderung aus einem anderen AWS-Service gesendet wurde

Weitere Informationen finden Sie unter CloudTrail-Element userIdentity.

Grundlagen zu OpenSearch -Protokolldateieinträgen

Ein Trail ist eine Konfiguration, durch die Ereignisse als Protokolldateien an den von Ihnen angegebenen Amazon-S3-Bucket übermittelt werden. CloudTrail-Protokolldateien können einen oder mehrere Einträge enthalten.

Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar. Es enthält unter anderem Informationen über die angeforderte Aktion, etwaige Anforderungsparameter und das Datum und die Uhrzeit der Aktion. CloudTrail-Protokolleinträge sind kein geordnetes Stacktrace der öffentlichen API-Aufrufe und erscheinen daher nicht in einer bestimmten Reihenfolge.

Das folgende Beispiel zeigt einen CloudTrail-Protokolleintrag, der die Aktion `DeletePipeline` demonstriert.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn":"arn:aws:iam::123456789012:user/test-user",
        "accountId": "123456789012",
        "accessKeyId": "access-key",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/Admin",
                "accountId": "123456789012",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-04-21T16:48:33Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-04-21T16:49:22Z",
```

```
    "eventSource": "osis.amazonaws.com",
    "eventName": "UpdatePipeline",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "123.456.789.012",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36",
    "requestParameters": {
        "pipelineName": "my-pipeline",
        "pipelineConfigurationBody": "version: \"2\"\nlog-pipeline:\n  source:\n
 http:\n        path: \"/test/logs\"\n  processor:\n    - grok:\n        match:\n
        log: [ '%{COMMONAPACHELOG}' ]\n    - date:\n        from_time_received: true
\n        destination: \"@timestamp\"\n  sink:\n    - opensearch:\n        hosts:
 [ \"https://search-b5zd22mwxhggheqpj5ftslgyle.us-west-2.es.amazonaws.com\" ]\n
  index: \"apache_logs2\"\n        aws_sts_role_arn: \"arn:aws:iam::709387180454:role/
canary-bootstrap-OsisRole-J1BARLD26QKN\"\n        aws_region: \"us-west-2\"\n
 aws_sigv4: true\n"
    },
    "responseElements": {
        "pipeline": {
            "pipelineName": "my-pipeline",sourceIPAddress
            "pipelineArn": "arn:aws:osis:us-west-2:123456789012:pipeline/my-pipeline",
            "minUnits": 1,
            "maxUnits": 1,
            "status": "UPDATING",
            "statusReason": {
                "description": "An update was triggered for the pipeline. It is still
 available to ingest data."
            },
            "pipelineConfigurationBody": "version: \"2\"\nlog-pipeline:\n  source:\n
    http:\n        path: \"/test/logs\"\n  processor:\n    - grok:\n        match:
\n          log: [ '%{COMMONAPACHELOG}' ]\n    - date:\n        from_time_received:
 true\n        destination: \"@timestamp\"\n  sink:\n    - opensearch:\n        hosts:
 [ \"https://search-b5zd22mwxhggheqpj5ftslgyle.us-west-2.es.amazonaws.com\" ]\n
  index: \"apache_logs2\"\n        aws_sts_role_arn: \"arn:aws:iam::709387180454:role/
canary-bootstrap-OsisRole-J1BARLD26QKN\"\n        aws_region: \"us-west-2\"\n
 aws_sigv4: true\n",
            "createdAt": "Mar 29, 2023 1:03:44 PM",
            "lastUpdatedAt": "Apr 21, 2023 9:49:21 AM",
            "ingestEndpointUrls": [
                "my-pipeline-tu33ldsgdltgv7x7tjqiudvf7m.us-west-2.osis.amazonaws.com"
            ]
        }
    },
    "requestID": "12345678-1234-1234-1234-987654321098",
```

```
    "eventID": "12345678-1234-1234-1234-987654321098",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "709387180454",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "osis.us-west-2.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}
```

Kennzeichnen von Amazon OpenSearch Ingestion-Pipelines

Mit Tags können Sie einer OpenSearch Amazon-Ingestion-Pipeline beliebige Informationen zuweisen, damit Sie diese Informationen kategorisieren und filtern können. Ein Tag ist ein Metadaten-Etikett, das von Ihnen oder von AWS einer AWS-Ressource zugewiesen wird. Jedes Tag besteht aus einem Schlüssel und einem Wert. Für Tags, die Sie zuweisen, definieren Sie einen Schlüssel und einen Wert. So können Sie beispielsweise den Schlüssel als `stage` und den Wert für eine Ressource als `test` definieren.

Tags sind für folgende Aktivitäten nützlich:

- Identify and organize your AWS resources. Viele AWS-Services unterstützen das Markieren mit Tags (kurz: Tagging). So können Ressourcen aus verschiedenen Services dasselbe Tag zuweisen, um anzugeben, dass die Ressourcen verbunden sind. Beispielsweise könnten Sie einer OpenSearch Ingestion-Pipeline dasselbe Tag zuweisen, das Sie einer OpenSearch Amazon--Service-Domäne zuweisen.
- Überwachen von AWS-Kosten. You activate these tags on the AWS Billing and Cost Management dashboard. AWS uses the tags to categorize your costs and deliver a monthly cost allocation report to you. Weitere Informationen finden Sie unter Verwendung von Kostenzuordnungs-Tags im AWS Billing-Benutzerhandbuch.
- Beschränken Sie den Zugriff auf Pipelines mithilfe einer attributbasierten Zugriffskontrolle. Weitere Informationen finden Sie unter Steuern des Zugriffs auf Tags im IAM-Benutzerhandbuch.

Bei OpenSearch Ingestion ist die primäre Ressource eine Pipeline. Sie können die OpenSearch Servicekonsole, die AWS CLI, die OpenSearch Ingestion-APIs oder die AWS -SDKs verwenden, um Tags zu einer Pipeline hinzuzufügen, zu verwalten und daraus zu entfernen.

Themen

Erforderliche Berechtigungen

OpenSearchIngestion verwendet die folgenden AWS Identity and Access Management Access Analyzer (IAM-) Berechtigungen für das Taggen von Pipelines:

- `osis:TagResource`
- `osis:ListTagsForResource`
- `osis:UntagResource`

Weitere Informationen zu jeder Berechtigung finden Sie unter Aktionen, Ressourcen und Konditionsschlüssel für OpenSearch Ingestion in der Referenz zur Serviceberechtigung.

Arbeiten mit Tags (Konsole)

Die Konsole ist die einfachste Möglichkeit, eine Pipeline zu markieren.

Um ein Tag zu erstellen

1. Melden Sie sich bei der OpenSearch Amazon--Service-Konsole unter https://console.aws.amazon.com/aos/home an.
2. Klicken Sie auf Ingestion im linken Navigationsbereich.
3. Wählen Sie die Pipeline aus, der Sie Tags hinzufügen möchten, und gehen Sie zur Registerkarte Tags.
4. Wählen Sie Verwalten und neues Tag hinzufügen.
5. Geben Sie einen Tag-Schlüssel und einen optionalen Wert ein.
6. Wählen Sie Speichern.

Um ein Tag zu löschen, führen Sie die gleichen Schritte aus und wählen Sie Entfernen auf der Seite Tags verwalten.

Weitere Informationen zur Verwendung der Konsole für die Arbeit mit Tags finden Sie unter Tag Editor im AWSHandbuch „Erste Schritte“ der Managementkonsole.

Arbeiten mit Tags (AWS CLI)

Um eine Pipeline mit dem zu AWS CLI taggen, senden Sie eine `TagResource` Anfrage:

```
aws osis tag-resource
  --arn arn:aws:osis:us-east-1:123456789012:pipeline/my-pipeline
  --tags Key=service,Value=osis Key=source,Value=otel
```

Entfernen Sie Tags aus einer Pipeline mit dem `UntagResource` folgenden Befehl:

```
aws osis untag-resource
  --arn arn:aws:osis:us-east-1:123456789012:pipeline/my-pipeline
  --tag-keys service
```

Zeigen Sie die vorhandenen Tags für eine Pipeline mit dem `ListTagsForResource` folgenden Befehl an:

```
aws osis list-tags-for-resource
  --arn arn:aws:osis:us-east-1:123456789012:pipeline/my-pipeline
```

Protokollierung und Überwachung OpenSearch von Amazon Ingestion mit Amazon CloudWatch

Amazon OpenSearch Ingestion veröffentlicht Kennzahlen und Protokolle auf Amazon. CloudWatch

Themen

- Überwachen der Pipeline-Protokolle
- Überwachung von Pipeline-Metriken

Überwachen der Pipeline-Protokolle

Sie können die Protokollierung für Amazon OpenSearch Ingestion-Pipelines aktivieren, um Fehler- und Warnmeldungen anzuzeigen, die während des Pipelinebetriebs und der Erfassungsaktivitäten ausgegeben werden. OpenSearchIngestion veröffentlicht alle Protokolle in Amazon CloudWatch Logs. CloudWatchProtokolle können Informationen in den Protokolldateien überwachen und Sie benachrichtigen, wenn bestimmte Schwellenwerte erreicht werden. Sie können Ihre Protokolldaten auch in einem sehr robusten Speicher archivieren. Weitere Informationen finden Sie im Amazon CloudWatch Logs-Benutzerhandbuch.

Die Protokolle von OpenSearch Ingestion können auf eine fehlgeschlagene Verarbeitung von Anfragen, Authentifizierungsfehler von der Quelle bis zur Senke und andere Warnungen hinweisen, die bei der Fehlerbehebung hilfreich sein können. Für seine Logs verwendet OpenSearch Ingestion die Loglevels von`INFO`, `WARN``ERROR`, und. `FATAL` Wir empfehlen, die Protokollveröffentlichung für alle Pipelines zu aktivieren.

Erforderliche Berechtigungen

So aktivieren Sie OpenSearch Ingestion, um Protokolle an CloudWatch Protokolle zu senden. Sie müssen als Benutzer angemeldet sein, der über bestimmte IAM-Berechtigungen verfügt.

Sie benötigen die folgenden CloudWatch Protokollberechtigungen, um Ressourcen für die Protokollübermittlung zu erstellen und zu aktualisieren:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Resource": "*",
            "Action": [
                "logs:CreateLogDelivery",
                "logs:PutResourcePolicy",
                "logs:UpdateLogDelivery",
                "logs:DeleteLogDelivery",
                "logs:DescribeResourcePolicies",
                "logs:GetLogDelivery",
                "logs:ListLogDeliveries"
            ]
        }
    ]
```

```
}
```

Aktivieren der Protokollveröffentlichung

Sie können die Protokollveröffentlichung in vorhandenen Pipelines oder beim Erstellen einer Pipeline aktivieren. Schritte zum Aktivieren der Protokollveröffentlichung während der Pipelineerstellung finden Sie unterthe section called “Pipelines erstellen”.

Konsole

So aktivieren Sie die Veröffentlichung von Protokollen in einer vorhandenen Pipeline

1. Melden Sie sich bei der Amazon OpenSearch Service-Konsole unter https://console.aws.amazon.com/aos/home an.
2. Wählen Sie im linken Navigationsbereich Ingestion und wählen Sie die Pipeline aus, für die Sie Protokolle aktivieren möchten.
3. Wählen Sie Optionen für die Protokollveröffentlichung bearbeiten aus.
4. Wählen Sie In CloudWatch Protokollen veröffentlichen aus.
5. Erstellen Sie entweder eine neue Protokollgruppe oder wählen Sie eine bestehende. Es wird empfohlen, den Namen als Pfad zu formatieren, z. `/aws/vendedlogs/OpenSearchIngestion/pipeline-name/audit-logs` B. Dieses Format erleichtert die Anwendung einer CloudWatch Zugriffsrichtlinie, die allen Protokollgruppen unter einem bestimmten Pfad Berechtigungen gewährt, z. `/aws/vendedlogs/OpenSearchService/OpenSearchIngestion` B.

   > **Important**
   >
   > Sie müssen das Präfix `vendedlogs` in den Namen der Protokollgruppe aufnehmen, andernfalls schlägt die Erstellung fehl.

6. Wählen Sie Speichern.

CLI

So aktivieren Sie die folgende AnfrageAWS CLI, um die Protokollveröffentlichung mit dem zu aktivieren:

```
aws osis update-pipeline \
```

```
  --pipeline-name my-pipeline \
  --log-publishing-options  IsLoggingEnabled=true,CloudWatchLogDestination={LogGroup="/
aws/vendedlogs/OpenSearchIngestion/pipeline-name"}
```

Überwachung von Pipeline-Metriken

Sie können Amazon OpenSearch Ingestion-Pipelines mit Amazon überwachenCloudWatch, wobei Rohdaten erfasst und in lesbare Metriken nahezu in Echtzeit verarbeitet werden. Diese Statistiken werden 15 Monate gespeichert, damit Sie auf Verlaufsinformationen zugreifen können und einen besseren Überblick darüber erhalten, wie Ihre Webanwendung oder der Service ausgeführt werden. Sie können auch Alarme einrichten, die auf bestimmte Grenzwerte achten und Benachrichtigungen senden oder Aktivitäten auslösen, wenn diese Grenzwerte erreicht werden. Weitere Informationen finden Sie im CloudWatchAmazon-Benutzerhandbuch.

Die OpenSearch Ingestion-Konsole zeigt eine Reihe von Diagrammen an, die auf den Rohdaten aus CloudWatch der Registerkarte Leistung für jede Pipeline basieren.

OpenSearchIngestion meldet Metriken von den meisten unterstützten Plugins. Wenn bestimmte Plugins unten keine eigene Tabelle haben, bedeutet das, dass sie keine Plugin-spezifischen Metriken melden. Pipeline-Metriken werden im `AWS/OSIS` Namespace veröffentlicht.

Themen

- Allgemeine Metriken
- Buffer-Metriken
- Signature V4-Metriken
- Metriken für begrenzte Blockierungspuffer
- Metriken von Otel Trace Source
- Quellkennzahlen für Hotelkennzahlen
- HTTP-Metriken
- S3-Metriken
- Gesamtmetriken
- Metriken zu Datum
- Grok-Metriken
- Otel Trace Rohmetriken

- Metriken zu Hotel-Trace-Gruppen
- Zustandsorientierte Metriken der Servicemap
- OpenSearch-Metriken
- System- und Metriken

Allgemeine Metriken

Die folgenden Metriken gelten für alle Prozessoren und Senken.

Jeder Metrik sind der Name der Subpipeline und der Name des Plugins vorangestellt, und zwar im Format < sub_pipeline_name >< plugin >< metric_name >. Der vollständige Name der `recordsIn.count` Metrik für eine Subpipeline mit dem Namen `my-pipeline` und dem Datumsprozessor wäre `my-pipeline.date.recordsIn.count` beispielsweise.

Metrisches Suffix	Beschreibung
`recordsIn.count`	Der Eingang von Datensätzen in eine Pipeline-Komponente. Diese Metrik gilt für Prozessoren und Spülbecken. Relevante Statistiken: Summe Abmessung: `PipelineName`
`recordsOut.count`	Der Ausgang von Datensätzen aus einer Pipeline-Komponente. Diese Metrik gilt für Prozessoren und Quellen. Relevante Statistiken: Summe Abmessung: `PipelineName`
`timeElapsed.count`	Eine Anzahl von Datenpunkten, die während der Ausführung einer Pipeline-Komponente aufgezeichnet wurden. Diese Metrik gilt für Prozessoren und Spülbecken. Relevante Statistiken: Summe Abmessung: `PipelineName`

Metrisches Suffix	Beschreibung
`timeElapsed.sum`	Die Gesamtzeit, die während der Ausführung einer Pipeline-Komponente verstrichen ist. Diese Metrik gilt für Prozessoren und Senken in Millisekunden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`timeElapsed.max`	Die maximale Zeit, die während der Ausführung einer Pipeline-Komponente verstrichen ist. Diese Metrik gilt für Prozessoren und Senken in Millisekunden. Relevante Statistiken: Maximum Abmessung: `PipelineName`

Buffer-Metriken

Die folgenden Metriken gelten für den standardmäßigen begrenzten Blockierungspuffer, den OpenSearch Ingestion automatisch für alle Pipelines konfiguriert.

Jeder Metrik sind der Name der Subpipeline und der Name des Puffers vorangestellt, und zwar im Format < sub_pipeline_name >< buffer_name >< metric_name >. Der vollständige Name der `recordsWritten.count` Metrik für eine Subpipeline mit dem Namen `my-pipeline` wäre `my-pipeline.BlockingBuffer.recordsWritten.count` beispielsweise.

Metrisches Suffix	Beschreibung
`recordsWritten.count`	Die Anzahl der Datensätze, die in einen Puffer geschrieb en wurden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`recordsRead.count`	Die Anzahl der aus einem Puffer gelesenen Datensätze.

Metrisches Suffix	Beschreibung
	Relevante Statistiken: Summe Abmessung: `PipelineName`
`recordsInFlight.value`	Die Anzahl der ungeprüften Datensätze, die aus einem Puffer gelesen wurden. Relevante Statistiken: Durchschnitt Abmessung: `PipelineName`
`recordsInBuffer.value`	Die Anzahl der Datensätze, die sich derzeit in einem Puffer befinden. Relevante Statistiken: Durchschnitt Abmessung: `PipelineName`
`recordsProcessed.count`	Die Anzahl der Datensätze, die aus einem Puffer gelesen und von einer Pipeline verarbeitet wurden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`recordsWriteFailed.count`	Die Anzahl der Datensätze, die die Pipeline nicht in die Spüle schreiben konnte. Relevante Statistiken: Summe Abmessung: `PipelineName`
`writeTimeElapsed.count`	Eine Anzahl von Datenpunkten, die beim Schreiben in einen Puffer aufgezeichnet wurden. Relevante Statistiken: Summe Abmessung: `PipelineName`

Metrisches Suffix	Beschreibung
`writeTimeElapsed.sum`	Die Gesamtzeit, die beim Schreiben in einen Puffer verstrichen ist, in Millisekunden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`writeTimeElapsed.max`	Die maximale Zeit, die beim Schreiben in einen Puffer verstrichen ist, in Millisekunden. Relevante Statistiken: Maximum Abmessung: `PipelineName`
`writeTimeouts.count`	Die Anzahl der Schreib-Timeouts in einen Puffer. Relevante Statistiken: Summe Abmessung: `PipelineName`
`readTimeElapsed.count`	Eine Anzahl von Datenpunkten, die beim Lesen aus einem Puffer aufgezeichnet wurden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`readTimeElapsed.sum`	Die Gesamtzeit, die beim Lesen aus einem Puffer verstrich en ist, in Millisekunden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`readTimeElapsed.max`	Die maximale Zeit, die beim Lesen aus einem Puffer verstrichen ist, in Millisekunden. Relevante Statistiken: Maximum Abmessung: `PipelineName`

Metrisches Suffix	Beschreibung
`checkpointTimeElapsed.count`	Eine Anzahl von Datenpunkten, die beim Checkpoints aufgezeichnet wurden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`checkpointTimeElapsed.sum`	Die Gesamtzeit, die beim Checkpoints verstrichen ist, in Millisekunden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`checkpointTimeElapsed.max`	Die maximale Zeit, die beim Checkpoints verstrichen ist, in Millisekunden. Relevante Statistiken: Maximum Abmessung: `PipelineName`

Signature V4-Metriken

Die folgenden Metriken gelten für den Aufnahmeendpunkt einer Pipeline und sind den Quell-Plugins (`httpotel_trace`, und`otel_metrics`) zugeordnet. Alle Anfragen an den Aufnahmeendpunkt müssen mit Signature Version 4 signiert werden. Diese Metriken können Ihnen dabei helfen, Autorisierungsprobleme zu identifizieren, wenn Sie eine Verbindung zu Ihrer Pipeline herstellen, oder bestätigen, dass Sie sich erfolgreich authentifizieren.

Jeder Metrik ist der Name der Subpipeline und vorangestellt. `osis_sigv4_auth` Zum Beispiel *`sub_pipeline_name`*`.osis_sigv4_auth.httpAuthSuccess.count`.

Metrisches Suffix	Beschreibung
`httpAuthSuccess.count`	Die Anzahl der erfolgreichen Signature V4-Anfragen an die Pipeline. Relevante Statistiken: Summe

Metrisches Suffix	Beschreibung
	Abmessung: `PipelineName`
`httpAuthFailure.count`	Die Anzahl der fehlgeschlagenen Signature V4-Anfragen an die Pipeline. Relevante Statistiken: Summe Abmessung: `PipelineName`
`httpAuthServerError.count`	Die Anzahl der Signature V4-Anfragen an die Pipeline, die Serverfehler zurückgegeben haben. Relevante Statistiken: Summe Abmessung: `PipelineName`

Metriken für begrenzte Blockierungspuffer

Die folgenden Metriken gelten für den begrenzten Blockierungspuffer. Jeder Metrik ist der Name der Subpipeline und vorangestellt. `BlockingBuffer` Zum Beispiel *`sub_pipeline_name`*`.BlockingBuffer.bufferUsage.value`.

Metrisches Suffix	Beschreibung
`bufferUsage.value`	Prozentuale Nutzung von `buffer_size` basierend auf der Anzahl der Datensätze im Puffer. `buffer_size` steht für die maximale Anzahl von Datensätzen, die in den Puffer geschrieben wurden, sowie für Datensätze während des Fluges, die nicht überprüft wurden. Relevante Statistiken: Durchschnitt Abmessung: `PipelineName`

Metriken von Otel Trace Source

Die folgenden Metriken gelten für die OTel-Trace-Quelle. Jeder Metrik ist der Name der Subpipeline und vorangestellt. `otel_trace_source` Zum Beispiel *`sub_pipeline_name`*`.otel_trace_source.requestTimeouts.count`.

Metrisches Suffix	Beschreibung
`requestTimeouts.count`	Die Anzahl der Anfragen, die das Zeitlimit überschritten haben. Relevante Statistiken: Summe Abmessung: `PipelineName`
`requestsReceived.count`	Die Anzahl der vom Plugin empfangenen Anfragen. Relevante Statistiken: Summe Abmessung: `PipelineName`
`successRequests.count`	Die Anzahl der Anfragen, die vom Plugin erfolgreich bearbeitet wurden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`badRequests.count`	Die Anzahl der Anfragen mit einem ungültigen Format, die vom Plugin verarbeitet wurden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`requestsTooLarge.count`	Die Anzahl der Anfragen, deren Anzahl der Abschnitte im Inhalt größer ist als die Pufferkapazität. Relevante Statistiken: Summe Abmessung: `PipelineName`

Metrisches Suffix	Beschreibung
`internalServerError.count`	Die Anzahl der vom Plugin verarbeiteten Anfragen mit einem benutzerdefinierten Ausnahmetyp. Relevante Statistiken: Summe Abmessung: `PipelineName`
`requestProcessDuration.count`	Eine Anzahl von Datenpunkten, die während der Verarbeitung von Anfragen durch das Plugin aufgezeichnet wurden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`requestProcessDuration.sum`	Die Gesamtlatenz der vom Plugin verarbeiteten Anfragen in Millisekunden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`requestProcessDuration.max`	Die maximale Latenz der vom Plugin verarbeiteten Anfragen in Millisekunden. Relevante Statistiken: Maximum Abmessung: `PipelineName`
`payloadSize.count`	Eine Anzahl der Verteilung der Nutzlastgrößen eingehender Anfragen in Byte. Relevante Statistiken: Summe Abmessung: `PipelineName`

Metrisches Suffix	Beschreibung
`payloadSize.sum`	Die Gesamtverteilung der Nutzlastgrößen eingehender Anfragen in Byte. Relevante Statistiken: Summe Abmessung: `PipelineName`
`payloadSize.max`	Die maximale Verteilung der Nutzlastgrößen eingehender Anfragen in Byte. Relevante Statistiken: Maximum Abmessung: `PipelineName`

Quellkennzahlen für Hotelkennzahlen

Die folgenden Metriken gelten für die Metriken von OTEL. Jeder Metrik ist der Name der Subpipeline und vorangestellt. `otel_metrics_source` Zum Beispiel *`sub_pipeline_name`*`.otel_metrics_source.requestTimeouts.count`.

Metrisches Suffix	Beschreibung
`requestTimeouts.count`	Die Gesamtzahl der Anfragen an das Plugin, die das Zeitlimit überschritten haben. Relevante Statistiken: Summe Abmessung: `PipelineName`
`requestsReceived.count`	Die Gesamtzahl der vom Plugin empfangenen Anfragen. Relevante Statistiken: Summe Abmessung: `PipelineName`
`successRequests.count`	Die Anzahl der vom Plugin erfolgreich verarbeiteten Anfragen (200 Antwortstatuscode).

Metrisches Suffix	Beschreibung
	Relevante Statistiken: Summe Abmessung: `PipelineName`
`requestProcessDuration.count`	Eine Zählung der Latenz der vom Plugin verarbeiteten Anfragen in Sekunden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`requestProcessDuration.sum`	Die Gesamtlatenz der vom Plugin verarbeiteten Anfragen in Millisekunden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`requestProcessDuration.max`	Die maximale Latenz der vom Plugin verarbeiteten Anfragen in Millisekunden. Relevante Statistiken: Maximum Abmessung: `PipelineName`
`payloadSize.count`	Eine Anzahl der Verteilung der Nutzlastgrößen eingehender Anfragen in Byte. Relevante Statistiken: Summe Abmessung: `PipelineName`
`payloadSize.sum`	Die Gesamtverteilung der Nutzlastgrößen eingehender Anfragen in Byte. Relevante Statistiken: Summe Abmessung: `PipelineName`

Metrisches Suffix	Beschreibung
`payloadSize.max`	Die maximale Verteilung der Nutzlastgrößen eingehender Anfragen in Byte. Relevante Statistiken: Maximum Abmessung: `PipelineName`

HTTP-Metriken

Die folgenden Metriken gelten für die HTTP-Quelle. Jeder Metrik ist der Name der Subpipeline und vorangestellt. `http` Zum Beispiel *`sub_pipeline_name`*`.http.requestsReceived.count`.

Metrisches Suffix	Beschreibung
`requestsReceived.count`	Die Anzahl der vom `/log/ingest` -Endpunkt empfangenen Anfragen. Relevante Statistiken: Summe Abmessung: `PipelineName`
`requestsRejected.count`	Die Anzahl der vom Plugin abgelehnten Anfragen (429 Antwortstatuscode). Relevante Statistiken: Summe Abmessung: `PipelineName`
`successRequests.count`	Die Anzahl der vom Plugin erfolgreich verarbeiteten Anfragen (200 Antwortstatuscode). Relevante Statistiken: Summe Abmessung: `PipelineName`
`badRequests.count`	Die Anzahl der Anfragen mit ungültigem Inhaltstyp oder Format (400-Antwortstatuscode), die vom Plugin verarbeit et wurden.

Metrisches Suffix	Beschreibung
	Relevante Statistiken: Summe Abmessung: `PipelineName`
`requestTimeouts.count`	Die Anzahl der Anfragen, bei denen das Timeout auf dem HTTP-Quellserver abgelaufen ist (415 Antwortstatuscode). Relevante Statistiken: Summe Abmessung: `PipelineName`
`requestsTooLarge.count`	Die Anzahl der Anfragen, bei denen die Größe der Ereignisse im Inhalt größer ist als die Pufferkapazität (413-Antwortstatuscode). Relevante Statistiken: Summe Abmessung: `PipelineName`
`internalServerError.count`	Die Anzahl der vom Plugin verarbeiteten Anfragen mit einem benutzerdefinierten Ausnahmetyp (500-Antw ortstatuscode). Relevante Statistiken: Summe Abmessung: `PipelineName`
`requestProcessDura tion.count`	Eine Zählung der Latenz der vom Plugin verarbeiteten Anfragen in Sekunden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`requestProcessDura tion.sum`	Die Gesamtlatenz der vom Plugin verarbeiteten Anfragen in Millisekunden. Relevante Statistiken: Summe Abmessung: `PipelineName`

Metrisches Suffix	Beschreibung
`requestProcessDuration.max`	Die maximale Latenz der vom Plugin verarbeiteten Anfragen in Millisekunden. Relevante Statistiken: Maximum Abmessung: `PipelineName`
`payloadSize.count`	Eine Anzahl der Verteilung der Nutzlastgrößen eingehender Anfragen in Byte. Relevante Statistiken: Summe Abmessung: `PipelineName`
`payloadSize.sum`	Die Gesamtverteilung der Nutzlastgrößen eingehender Anfragen in Byte. Relevante Statistiken: Summe Abmessung: `PipelineName`
`payloadSize.max`	Die maximale Verteilung der Nutzlastgrößen eingehender Anfragen in Byte. Relevante Statistiken: Maximum Abmessung: `PipelineName`

S3-Metriken

Die folgenden Metriken gelten für die S3-Quelle. Jeder Metrik ist der Name der Subpipeline und vorangestellt. `s3` Zum Beispiel *`sub_pipeline_name`*`.s3.s3ObjectsFailed.count`.

Metrisches Suffix	Beschreibung
`s3ObjectsFailed.count`	Die Gesamtzahl der S3-Objekte, die das Plugin nicht lesen konnte.

Metrisches Suffix	Beschreibung
	Relevante Statistiken: Summe Abmessung: `PipelineName`
`s3ObjectsNotFound.count`	Die Anzahl der S3-Objekte, die das Plugin aufgrund eines `Not Found` Fehlers von S3 nicht lesen konnte. Diese Metriken werden ebenfalls zur `s3ObjectsFailed` Metrik gezählt. Relevante Statistiken: Summe Abmessung: `PipelineName`
`s3ObjectsAccessDenied.count`	Die Anzahl der S3-Objekte, die das Plugin aufgrund eines `Access Denied` `Forbidden` Oder-Fehlers von S3 nicht lesen konnte. Diese Metriken werden ebenfalls zur `s3ObjectsFailed` Metrik gezählt. Relevante Statistiken: Summe Abmessung: `PipelineName`
`s3ObjectReadTimeElapsed.count`	Die Zeit, die das Plugin benötigt, um eine GET-Anfrage für ein S3-Objekt auszuführen, es zu analysieren und Ereignisse in den Puffer zu schreiben. Relevante Statistiken: Summe Abmessung: `PipelineName`
`s3ObjectReadTimeElapsed.sum`	Die Gesamtzeit, die das Plugin benötigt, um eine GET-Anfrage für ein S3-Objekt auszuführen, sie zu analysieren und Ereignisse in den Puffer zu schreiben, in Millisekunden. Relevante Statistiken: Summe Abmessung: `PipelineName`

Metrisches Suffix	Beschreibung
`s3ObjectReadTimeElapsed.max`	Die maximale Zeit, die das Plugin benötigt, um eine GET-Anfrage für ein S3-Objekt auszuführen, sie zu analysieren und Ereignisse in den Puffer zu schreiben, in Millisekunden. Relevante Statistiken: Maximum Abmessung: `PipelineName`
`s3ObjectSizeBytes.count`	Die Anzahl der Verteilung der S3-Objektgrößen in Byte. Relevante Statistiken: Summe Abmessung: `PipelineName`
`s3ObjectSizeBytes.sum`	Die Gesamtverteilung der S3-Objektgrößen in Byte. Relevante Statistiken: Summe Abmessung: `PipelineName`
`s3ObjectSizeBytes.max`	Die maximale Verteilung der S3-Objektgrößen in Byte. Relevante Statistiken: Maximum Abmessung: `PipelineName`
`s3ObjectProcessedBytes.count`	Die Anzahl der vom Plugin verarbeiteten S3-Objekte in Byte. Relevante Statistiken: Summe Abmessung: `PipelineName`
`s3ObjectProcessedBytes.sum`	Die Gesamtverteilung der vom Plugin verarbeiteten S3-Objekte in Byte. Relevante Statistiken: Summe Abmessung: `PipelineName`

Metrisches Suffix	Beschreibung
`s3ObjectProcessedBytes.max`	Die maximale Verteilung der vom Plugin verarbeiteten S3-Objekte in Byte. Relevante Statistiken: Maximum Abmessung: `PipelineName`
`s3ObjectsEvents.count`	Die Anzahl der vom Plugin empfangenen S3-Ereignisse. Relevante Statistiken: Summe Abmessung: `PipelineName`
`s3ObjectsEvents.sum`	Die Gesamtverteilung der vom Plugin empfangenen S3-Ereignisse. Relevante Statistiken: Summe Abmessung: `PipelineName`
`s3ObjectsEvents.max`	Die maximale Verteilung der vom Plugin empfangenen S3-Ereignisse. Relevante Statistiken: Maximum Abmessung: `PipelineName`
`sqsMessageDelay.count`	Eine Anzahl von Datenpunkten, die aufgezeichnet wurden, während S3 eine Ereigniszeit für die Erstellung eines Objekts aufzeichnet, bis zu dem es vollständig analysiert wurde. Relevante Statistiken: Summe Abmessung: `PipelineName`

Metrisches Suffix	Beschreibung
`sqsMessageDelay.sum`	Die Gesamtzeit zwischen dem Zeitpunkt, an dem S3 eine Ereigniszeit für die Erstellung eines Objekts aufzeichn et, und dem Zeitpunkt, an dem es vollständig analysiert wurde, in Millisekunden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`sqsMessageDelay.max`	Die maximale Zeitspanne zwischen dem Zeitpunkt, an dem S3 eine Ereigniszeit für die Erstellung eines Objekts aufzeichnet, und dem Zeitpunkt, an dem es vollständig analysiert wurde, in Millisekunden. Relevante Statistiken: Maximum Abmessung: `PipelineName`
`s3ObjectsSucceeded.count`	Die Anzahl der S3-Objekte, die das Plugin erfolgreich gelesen hat. Relevante Statistiken: Summe Abmessung: `PipelineName`
`sqsMessagesReceived.count`	Die Anzahl der Amazon SQS SQS-Nachrichten, die das Plugin aus der Warteschlange empfangen hat. Relevante Statistiken: Summe Abmessung: `PipelineName`
`sqsMessagesDeleted.count`	Die Anzahl der Amazon SQS SQS-Nachrichten, die vom Plugin aus der Warteschlange gelöscht wurden. Relevante Statistiken: Summe Abmessung: `PipelineName`

Metrisches Suffix	Beschreibung
`sqsMessagesFailed.count`	Die Anzahl der Amazon SQS SQS-Nachrichten, die das Plugin nicht analysieren konnte. Relevante Statistiken: Summe Abmessung: `PipelineName`

Gesamtmetriken

Die folgenden Metriken gelten für den Aggregatprozessor. Jeder Metrik ist der Name der Subpipeline und vorangestellt. `aggregate` Zum Beispiel *`sub_pipeline_name`*`.aggregate.actionHandleEventsOut.count`.

Metrisches Suffix	Beschreibung
`actionHandleEvents Out.count`	Die Anzahl der Ereignisse, die vom `handleEvent` Aufruf an die konfigurierte Aktion zurückgegeben wurden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`actionHandleEvents Dropped.count`	Die Anzahl der Ereignisse, die vom `handleEvent` Aufruf an die konfigurierte Aktion zurückgegeben wurden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`actionHandleEvents ProcessingErrors.count`	Die Anzahl der Aufrufe `handleEvent` für die konfiguri erte Aktion, die zu einem Fehler geführt haben. Relevante Statistiken: Summe Abmessung: `PipelineName`
`actionConcludeGrou pEventsOut.count`	Die Anzahl der Ereignisse, die vom `concludeGroup` Aufruf an die konfigurierte Aktion zurückgegeben wurden.

Metrisches Suffix	Beschreibung
	Relevante Statistiken: Summe Abmessung: `PipelineName`
`actionConcludeGroupEventsDropped.count`	Die Anzahl der Ereignisse, die vom `condludeGroup` Aufruf zur konfigurierten Aktion nicht zurückgegeben wurden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`actionConcludeGroupEventsProcessingErrors.count`	Die Anzahl der Aufrufe `concludeGroup` für die konfigurierte Aktion, die zu einem Fehler geführt haben. Relevante Statistiken: Summe Abmessung: `PipelineName`
`currentAggregateGroups.value`	Die aktuelle Anzahl von Gruppen. Dieser Indikator nimmt ab, wenn Gruppen geschlossen werden, und steigt, wenn ein Ereignis die Bildung einer neuen Gruppe einleitet. Relevante Statistiken: Durchschnitt Abmessung: `PipelineName`

Metriken zu Datum

Die folgenden Metriken gelten für den Datumsprozessor. Jeder Metrik ist der Name der Subpipeline und vorangestellt. `date` Zum Beispiel *`sub_pipeline_name`*`.date.dateProcessingMatchSuccess.count`.

Metrisches Suffix	Beschreibung
`dateProcessingMatchSuccess.count`	Die Anzahl der Datensätze, die mindestens einem der in der `match` Konfigurationsoption angegebenen Muster entsprechen.

Metrisches Suffix	Beschreibung
	Relevante Statistiken: Summe Abmessung: `PipelineName`
`dateProcessingMatchFailure.count`	Die Anzahl der Datensätze, die keinem der in der `match` Konfigurationsoption angegebenen Muster entsprachen. Relevante Statistiken: Summe Abmessung: `PipelineName`

Grok-Metriken

Die folgenden Metriken gelten für den Grok-Prozessor. Jeder Metrik ist der Name der Subpipeline und vorangestellt. `grok` Zum Beispiel *`sub_pipeline_name`*`.grok.grokProcessingMatch.count`.

Metrisches Suffix	Beschreibung
`grokProcessingMatch.count`	Die Anzahl der Datensätze, bei denen mindestens ein Muster gefunden wurde, das mit der `match` Konfigurationsoption übereinstimmt. Relevante Statistiken: Summe Abmessung: `PipelineName`
`grokProcessingMismatch.count`	Die Anzahl der Datensätze, die keinem der in der `match` Konfigurationsoption angegebenen Muster entsprachen. Relevante Statistiken: Summe Abmessung: `PipelineName`
`grokProcessingErrors.count`	Die Anzahl der Fehler bei der Datensatzverarbeitung. Relevante Statistiken: Summe

Metrisches Suffix	Beschreibung
	Abmessung: `PipelineName`
`grokProcessingTimeouts.count`	Die Anzahl der Datensätze, bei denen beim Abgleich ein Timeout aufgetreten ist. Relevante Statistiken: Summe Abmessung: `PipelineName`
`grokProcessingTime.count`	Eine Anzahl von Datenpunkten, die aufgezeichnet wurden, während ein einzelner Datensatz mit Mustern aus der `match` Konfigurationsoption übereinstimmte. Relevante Statistiken: Summe Abmessung: `PipelineName`
`grokProcessingTime.sum`	Die Gesamtzeit, die jeder einzelne Datensatz benötigt, um ihn mit Mustern aus der `match` Konfigurationsoption abzugleichen, in Millisekunden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`grokProcessingTime.max`	Die maximale Zeit, die jeder einzelne Datensatz benötigt, um mit Mustern aus der `match` Konfigurationsoption abgeglichen zu werden, in Millisekunden. Relevante Statistiken: Maximum Abmessung: `PipelineName`

Otel Trace Rohmetriken

Die folgenden Metriken gelten für den OTel Trace-Rohprozessor. Jeder Metrik ist der Name der Subpipeline und vorangestellt. `otel_trace_raw` Zum Beispiel *`sub_pipeline_name`*`.otel_trace_raw.traceGroupCacheCount.value`.

Metrisches Suffix	Beschreibung
`traceGroupCacheCount.value`	Die Anzahl der Trace-Gruppen im Trace-Group-Cache. Relevante Statistiken: Summe Abmessung: `PipelineName`
`spanSetCount.value`	Die Anzahl der Span-Sets in der Span-Set-Sammlung. Relevante Statistiken: Summe Abmessung: `PipelineName`

Metriken zu Hotel-Trace-Gruppen

Die folgenden Metriken gelten für den OTEL Trace Group Processor. Jeder Metrik ist der Name der Subpipeline und vorangestellt. `otel_trace_group` Zum Beispiel *`sub_pipeline_name`*`.otel_trace_group.recordsInMissingTraceGroup.count`.

Metrisches Suffix	Beschreibung
`recordsInMissingTraceGroup.count`	Die Anzahl der Eingangsdatensätze, denen Trace-Gruppenfelder fehlen. Relevante Statistiken: Summe Abmessung: `PipelineName`
`recordsOutFixedTraceGroup.count`	Die Anzahl der Ausgangsdatensätze mit Trace-Gruppenfeldern, die erfolgreich gefüllt wurden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`recordsOutMissingTraceGroup.count`	Die Anzahl der ausgehenden Datensätze, denen Trace-Gruppenfelder fehlen. Relevante Statistiken: Summe

Metrisches Suffix	Beschreibung
	Abmessung: `PipelineName`

Zustandsorientierte Metriken der Servicemap

Die folgenden Metriken gelten für den Service-MAP-Stateful-Prozessor. Jeder Metrik ist der Name der Subpipeline und vorangestellt. `service-map-stateful` Zum Beispiel *`sub_pipeline_name`*`.service-map-stateful.spansDbSize.count`.

Metrisches Suffix	Beschreibung
`spansDbSize.value`	Die speicherinternen Bytegrößen von erstrecken sich in MapDB über die aktuelle und die vorherige Fensterdauer. Relevante Statistiken: Durchschnitt Abmessung: `PipelineName`
`traceGroupDbSize.value`	Die speicherinternen Bytegrößen von Trace-Gruppen in MapDB für die aktuelle und vorherige Fensterdauer. Relevante Statistiken: Durchschnitt Abmessung: `PipelineName`
`spansDbCount.value`	Die Anzahl der Bereiche in MapDB für die Dauer des aktuellen und des vorherigen Fensters. Relevante Statistiken: Summe Abmessung: `PipelineName`
`traceGroupDbCount.value`	Die Anzahl der Trace-Gruppen in MapDB während der aktuellen und vorherigen Fensterdauer. Relevante Statistiken: Summe Abmessung: `PipelineName`

Metrisches Suffix	Beschreibung
`relationshipCount.value`	Die Anzahl der Beziehungen, die während der aktuellen und der vorherigen Fensterdauer gespeichert wurden. Relevante Statistiken: Summe Abmessung: `PipelineName`

OpenSearch-Metriken

Die folgenden Metriken gelten für die OpenSearchSpüle. Jeder Metrik ist der Name der Subpipeline und vorangestellt. `opensearch` Zum Beispiel *`sub_pipeline_name`*`.opensearch.bulkRequestErrors.count`.

Metrisches Suffix	Beschreibung
`bulkRequestErrors.count`	Die Gesamtzahl der Fehler, die beim Senden von Massenanfragen aufgetreten sind. Relevante Statistiken: Summe Abmessung: `PipelineName`
`documentsSuccess.count`	Die Anzahl der Dokumente, die erfolgreich per Massenanfrage an den OpenSearch Service gesendet wurden, einschließlich Wiederholungsversuchen. Relevante Statistiken: Summe Abmessung: `PipelineName`
`documentsSuccessFirstAttempt.count`	Die Anzahl der Dokumente, die beim ersten Versuch erfolgreich per Massenanfrage an den OpenSearch Service gesendet wurden. Relevante Statistiken: Summe Abmessung: `PipelineName`

Metrisches Suffix	Beschreibung
`documentErrors.count`	Die Anzahl der Dokumente, die nicht im Rahmen von Massenanfragen gesendet wurden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`bulkRequestFailed.count`	Die Anzahl der fehlgeschlagenen Massenanforderungen. Relevante Statistiken: Summe Abmessung: `PipelineName`
`bulkRequestNumberOfRetries.count`	Die Anzahl der Wiederholungen fehlgeschlagener Massenanforderungen. Relevante Statistiken: Summe Abmessung: `PipelineName`
`bulkBadRequestErrors.count`	Die Anzahl der `Bad Request` Fehler, die beim Senden von Massenanfragen aufgetreten sind. Relevante Statistiken: Summe Abmessung: `PipelineName`
`bulkRequestNotAllowedErrors.count`	Die Anzahl der `Request Not Allowed` Fehler, die beim Senden von Massenanfragen aufgetreten sind. Relevante Statistiken: Summe Abmessung: `PipelineName`
`bulkRequestInvalidInputErrors.count`	Die Anzahl der `Invalid Input` Fehler, die beim Senden von Massenanfragen aufgetreten sind. Relevante Statistiken: Summe Abmessung: `PipelineName`

Metrisches Suffix	Beschreibung
`bulkRequestNotFoundErrors.count`	Die Anzahl der `Request Not Found` Fehler, die beim Senden von Massenanfragen aufgetreten sind. Relevante Statistiken: Summe Abmessung: `PipelineName`
`bulkRequestTimeoutErrors.count`	Die Anzahl der `Request Timeout` Fehler, die beim Senden von Massenanfragen aufgetreten sind. Relevante Statistiken: Summe Abmessung: `PipelineName`
`bulkRequestServerErrors.count`	Die Anzahl der `Server Error` Fehler, die beim Senden von Massenanfragen aufgetreten sind. Relevante Statistiken: Summe Abmessung: `PipelineName`
`bulkRequestSizeBytes.count`	Eine Anzahl der Verteilung der Nutzlastgrößen von Massenanfragen in Byte. Relevante Statistiken: Summe Abmessung: `PipelineName`
`bulkRequestSizeBytes.sum`	Die Gesamtverteilung der Nutzlastgrößen von Massenanfragen in Byte. Relevante Statistiken: Summe Abmessung: `PipelineName`

Metrisches Suffix	Beschreibung
`bulkRequestSizeBytes.max`	Die maximale Verteilung der Nutzlastgrößen von Massenanfragen in Byte. Relevante Statistiken: Maximum Abmessung: `PipelineName`
`bulkRequestLatency.count`	Eine Anzahl von Datenpunkten, die aufgezeichnet wurden, während Anfragen an das Plugin gesendet werden, einschließlich Wiederholungsversuchen. Relevante Statistiken: Summe Abmessung: `PipelineName`
`bulkRequestLatency.sum`	Die Gesamtlatenz der an das Plugin gesendeten Anfragen, einschließlich Wiederholungen, in Millisekunden. Relevante Statistiken: Summe Abmessung: `PipelineName`
`bulkRequestLatency.max`	Die maximale Latenz von Anfragen, die an das Plugin gesendet werden, einschließlich Wiederholungsversuchen, in Millisekunden. Relevante Statistiken: Maximum Abmessung: `PipelineName`
`s3.dlqS3RecordsSuccess.count`	Die Anzahl der Datensätze, die erfolgreich an die S3-Warteschlange für unzulässige Briefe gesendet wurden. Relevante Statistiken: Summe Abmessung: `PipelineName`

Metrisches Suffix	Beschreibung
`s3.dlqS3RecordsFailed.count`	Die Anzahl der Datensätze, die nicht an die S3-Wartes chlange für unzulässige Briefe gesendet werden konnten. Relevante Statistiken: Summe Abmessung: `PipelineName`
`s3.dlqS3RequestSuccess.count`	Die Anzahl erfolgreicher Anfragen an die S3-Wartes chlange für unzulässige Briefe. Relevante Statistiken: Summe Abmessung: `PipelineName`
`s3.dlqS3RequestFailed.count`	Die Anzahl der fehlgeschlagenen Anfragen an die S3-Warteschlange für unzulässige Briefe. Relevante Statistiken: Summe Abmessung: `PipelineName`
`s3.dlqS3RequestLatency.count`	Eine Anzahl von Datenpunkten, die aufgezeichnet wurden, während Anfragen an die S3-Warteschlange für unzustell bare Briefe gesendet werden, einschließlich Wiederhol ungsversuchen. Relevante Statistiken: Summe Abmessung: `PipelineName`
`s3.dlqS3RequestLatency.sum`	Die Gesamtlatenz der an die S3-Warteschlange gesendete n Anfragen, einschließlich Wiederholungsversuchen, in Millisekunden. Relevante Statistiken: Summe Abmessung: `PipelineName`

Metrisches Suffix	Beschreibung
`s3.dlqS3RequestLatency.max`	Die maximale Latenz von Anfragen, die an die S3-Wartes chlange für unzustellbare Briefe gesendet werden, einschließlich Wiederholungsversuchen, in Millisekunden. Relevante Statistiken: Maximum Abmessung: `PipelineName`
`s3.dlqS3RequestSizeBytes.count`	Eine Zählung der Verteilung der Nutzlastgrößen von Anfragen an die S3-Warteschlange für unzulässige Briefe in Byte. Relevante Statistiken: Summe Abmessung: `PipelineName`
`s3.dlqS3RequestSizeBytes.sum`	Die Gesamtverteilung der Nutzlastgrößen von Anfragen an die S3-Warteschlange für unzulässige Briefe in Byte. Relevante Statistiken: Summe Abmessung: `PipelineName`
`s3.dlqS3RequestSizeBytes.max`	Die maximale Verteilung der Nutzlastgrößen von Anfragen an die S3-Warteschlange für unzulässige Briefe in Byte. Relevante Statistiken: Maximum Abmessung: `PipelineName`

System- und Metriken

Die folgenden Metriken gelten für das gesamte OpenSearch Aufnahmesystem. Diesen Metriken ist nichts vorangestellt.

Metrik	Beschreibung
`system.cpu.usage.value`	Der Prozentsatz der verfügbaren CPU-Auslastung für alle Datenknoten. Relevante Statistiken: Durchschnitt Abmessung:`PipelineName` ,`area`, `id`
`system.cpu.count.value`	Die Gesamtmenge der CPU-Auslastung für alle Datenknoten. Relevante Statistiken: Durchschnitt Abmessung:`PipelineName` ,`area`, `id`
`jvm.memory.max.value`	Die maximale Speichermenge, die für die Speicherverwaltung verwendet werden kann, in Byte. Relevante Statistiken: Durchschnitt Abmessung:`PipelineName` ,`area`, `id`
`jvm.memory.used.value`	Gesamtumfang des verwendeten Arbeitsspeichers in Byte. Relevante Statistiken: Durchschnitt Größe:`PipelineName` ,`area`, `id` Schild
`jvm.memory.committed.value`	Die Speichermenge, die für die Verwendung durch die Java Virtual Machine (JVM) bereitgestellt wird, in Byte. Relevante Statistiken: Durchschnitt Abmessung:`PipelineName` ,`area`, `id`
`computeUnits`	Die Anzahl der Ingestion OpenSearch Compute Units (Ingestion OCUs), die von einer Pipeline verwendet werden. Relevante Statistiken: Max, Summe, Durchschnitt

Metrik	Beschreibung
	Abmessung: `PipelineName`

Bewährte Methoden für Amazon OpenSearch Ingestion

Dieses Thema bietet bewährte Methoden für die Erstellung und Verwaltung von Amazon OpenSearch Ingestion-Pipelines und enthält allgemeine Richtlinien, die für viele Anwendungsfälle gelten. Jede Workload ist einzigartig und weist einzigartige Merkmale auf, sodass keine generische Empfehlung für jeden Anwendungsfall genau richtig ist.

Themen

Allgemeine bewährte Methoden

Die folgenden allgemeinen bewährten Methoden gelten für die Erstellung und Verwaltung von Pipelines.

- Um eine hohe Verfügbarkeit sicherzustellen, konfigurieren Sie VPC-Pipelines mit zwei oder drei Subnetzen. Wenn Sie eine Pipeline nur in einem Subnetz bereitstellen und die Availability Zone ausfällt, können Sie keine Daten aufnehmen.
- Wir empfehlen, die Anzahl der Sub-Pipelines innerhalb jeder Pipeline auf 5 oder weniger zu beschränken.
- Wenn Sie das S3-Quell-Plugin verwenden, verwenden Sie S3-Dateien mit gleichmäßiger Größe, um eine optimale Leistung zu erzielen.
- Wenn Sie das S3-Quell-Plugin verwenden, fügen Sie für eine optimale Leistung 30 Sekunden zusätzliches Sichtbarkeits-Timeout pro 0,25 GB Dateigröße im S3-Bucket hinzu.
- Fügen Sie Ihrer Pipeline-Konfiguration eine Warteschlange (Dead-Letter Queue, DLQ) hinzu, damit Sie fehlgeschlagene Ereignisse auslagern und sie für Analysen zugänglich machen können. Wenn Ihre Senken Daten aufgrund falscher Zuordnungen oder anderer Probleme zurückweisen, können Sie die Daten an den DLQ weiterleiten, um das Problem zu beheben und zu beheben.

Empfohlene Alarme CloudWatch

CloudWatch Alarme führen eine Aktion aus, wenn eine CloudWatch Metrik für einen bestimmten Zeitraum einen bestimmten Wert überschreitet. Sie können beispielsweise vorgeben, dass Ihnen AWS eine E-Mail sendet, wenn Ihr Cluster-Integritätsstatus länger als eine Minute `red` ist. Dieser Abschnitt enthält einige empfohlene Alarme für Amazon OpenSearch Ingestion und wie Sie darauf reagieren können.

Weitere Informationen zur Konfiguration von Alarmen finden Sie unter CloudWatchAmazon-Alarme erstellen im CloudWatch Amazon-Benutzerhandbuch.

Alarm	Problem
`computeUnits` Der Höchstwert ist = der `maxUnits` für 15 Minuten konfigurierte Wert, 3 aufeinand erfolgende Male	Die Pipeline hat die maximale Kapazität erreicht und muss möglicher weise `maxUnits` aktualisiert werden. Erhöhen Sie die maximale Kapazität Ihrer Pipeline
`opensearc h.documen tErrors.c ount` Summe ist = *`{sub_pipe line_name }`* `.opensear ch.record sIn.count` Summe für 1 Minute, 1 aufeinanderfolgendes Mal	Die Pipeline kann nicht in die OpenSearch Senke schreiben. Überprüfen Sie die Pipeline-Berechtigungen und stellen Sie sicher, dass die Domain oder Sammlung fehlerfrei ist. Sie können auch die Dead-Letter-Wartes chlange (DLQ) auf fehlgeschlagene Ereignisse überprüfen, sofern sie konfiguriert ist.
`bulkReque stLatency .max` max ist >= x für 1 Minute, 1 Mal hintereinander	Die Pipeline weist beim Senden von Daten an die OpenSearch Senke eine hohe Latenz auf. Dies ist wahrscheinlich auf eine zu geringe Größe der Senke oder auf eine schlechte Sharding-Strategie zurückzuführen, wodurch die Senke ins Hintertreffen gerät. Eine anhaltend hohe Latenz

Alarm	Problem
	kann sich auf die Leistung der Pipeline auswirken und wird wahrschei nlich zu einem Gegendruck auf die Clients führen.
`httpAuthF ailure.co unt` Summe >= 1 für 1 Minute, 1 Mal hintereinander	Aufnahmeanfragen werden nicht authentifiziert. Vergewissern Sie sich, dass auf allen Clients die Authentifizierung mit Signature Version 4 korrekt aktiviert ist.
`system.cp u.usage.v alue` durchschn ittlich >= 80% für 15 Minuten, dreimal hintereinander	Eine anhaltend hohe CPU-Auslastung kann problematisch sein. Erwägen Sie, die maximale Kapazität für die Pipeline zu erhöhen.
`bufferUsa ge.value` durchschn ittlich >= 80% für 15 Minuten, dreimal hintereinander	Eine anhaltend hohe Puffernutzung kann problematisch sein. Erwägen Sie, die maximale Kapazität für die Pipeline zu erhöhen.

Andere Alarme, die Sie in Betracht ziehen könnten

Erwägen Sie, je nachdem, welche Amazon OpenSearch Ingestion-Funktionen Sie regelmäßig verwenden, die folgenden Alarme zu konfigurieren.

Alarm	Problem
`dynamodb. exportJob Failure.c ount` Summe 1	Der Versuch, einen Export nach Amazon S3 auszulösen, ist fehlgesch lagen.
`opensearc h.EndtoEn`	Der `EndtoEndLatency` ist höher als gewünscht für das Lesen aus DynamoDB-Streams. Dies kann durch einen unterskalierten OpenSearc

Alarm	Problem
dLatency.avg Durchschnitt > X für 15 Minuten, 4 aufeinanderfolgende Male	h Cluster oder eine maximale Pipeline-OCU-Kapazität verursacht werden, die für den WCU-Durchsatz in der DynamoDB-Tabelle zu niedrig ist. EndtoEndLatency wird nach einem Export höher sein, sollte aber im Laufe der Zeit abnehmen, wenn es sich an die neuesten DynamoDB-Streams anpasst.
dyanmodb.changeEventsProcessed.count Summe == 0 für X Minuten	Es werden keine Datensätze aus DynamoDB-Streams gesammelt. Dies könnte daran liegen, dass in der Tabelle keine Aktivität vorhanden ist oder dass ein Problem beim Zugriff auf DynamoDB-Streams aufgetreten ist.
opensearch.s3.dlqS3RecordsSuccess.count Summe >= opensearch.documentSuccess.count Summe für 1 Minute, 1 aufeinanderfolgendes Mal	Es wird eine größere Anzahl von Datensätzen an den DLQ gesendet als an die Senke. OpenSearch Überprüfen Sie die Metriken des OpenSearch Sink-Plug-ins, um die Ursache zu untersuchen und zu ermitteln.
grok.grokProcessingTimeouts.count sum = RecordsIn.count sum für 1 Minute, 5 aufeinanderfolgende Male	Bei allen Daten tritt ein Timeout auf, während der Grok-Prozessor versucht, ein Muster zu finden. Dies wirkt sich wahrscheinlich auf die Leistung aus und verlangsamt Ihre Pipeline. Erwägen Sie, Ihre Muster anzupassen, um Timeouts zu reduzieren.

Alarm	Problem
`grok.grokProcessingErrors.count` Die Summe ist >= 1 für 1 Minute, 1 aufeinanderfolgendes Mal	Der Grok-Prozessor kann die Muster nicht mit den Daten in der Pipeline abgleichen, was zu Fehlern führt. Überprüfen Sie Ihre Daten und die Grok-Plug-in-Konfigurationen, um sicherzustellen, dass der Musterabgleich erwartet wird.
`grok.grokProcessingMismatch.count` sum = RecordsIn.count sum für 1 Minute, 5 aufeinanderfolgende Male	Der Grok-Prozessor ist nicht in der Lage, Muster mit den Daten in der Pipeline abzugleichen. Überprüfen Sie Ihre Daten und die Grok-Plug-in-Konfigurationen, um sicherzustellen, dass der Musterabgleich erwartet wird.
`date.dateProcessingMatchFailure.count` sum = RecordsIn.count sum für 1 Minute, 5 aufeinanderfolgende Male	Der Datumsprozessor kann den Daten in der Pipeline keine Muster zuordnen. Überprüfen Sie Ihre Daten- und Date-Plugin-Konfigurationen, um sicherzustellen, dass das Muster erwartet wird.
`s3.s3ObjectsFailed.count` Summe >= 1 für 1 Minute, 1 aufeinanderfolgendes Mal	Dieses Problem tritt entweder auf, weil das S3-Objekt nicht existiert oder die Pipeline nicht über ausreichende Rechte verfügt. Überprüfen Sie die `s3ObjectsAccessDenied.count` Metriken `s3ObjectsNotFound.count` und ermitteln Sie die Ursache. Vergewissern Sie sich, dass das S3-Objekt vorhanden ist, und/oder aktualisieren Sie die Berechtigungen.

Alarm	Problem
`s3.sqsMessagesFailed.count` Summe >= 1 für 1 Minute, 1 Mal hintereinander	Das S3-Plugin konnte eine Amazon SQS SQS-Nachricht nicht verarbeiten. Wenn Sie in Ihrer SQS-Warteschlange eine DLQ aktiviert haben, überprüfen Sie die fehlgeschlagene Nachricht. Die Warteschlange empfängt möglicherweise ungültige Daten, die die Pipeline zu verarbeiten versucht.
`http.badRequests.count` Summe >= 1 für 1 Minute, 1 Mal hintereinander	Der Client sendet eine fehlerhafte Anfrage. Vergewissern Sie sich, dass alle Clients die richtige Payload senden.
`http.requestsTooLarge.count` Summe >= 1 für 1 Minute, 1 Mal hintereinander	Anfragen vom HTTP-Quell-Plugin enthalten zu viele Daten, wodurch die Pufferkapazität überschritten wird. Passen Sie die Batchgröße für Ihre Kunden an.
`http.internalServerError.count` Summe >= 0 für 1 Minute, 1 Mal hintereinander	Das HTTP-Quell-Plugin hat Probleme beim Empfang von Ereignissen.
`http.requestTimeouts.count` Summe >= 0 für 1 Minute, 1 Mal hintereinander	Quell-Timeouts sind wahrscheinlich das Ergebnis einer unzureichenden Bereitstellung der Pipeline. Erwägen Sie, die Pipeline `maxUnits` zu erweitern, um die zusätzliche Arbeitslast zu bewältigen.

Alarm	Problem
`otel_trace.badRequests.count` Summe >= 1 für 1 Minute, 1 Mal hintereinander	Der Client sendet eine fehlerhafte Anfrage. Vergewissern Sie sich, dass alle Clients die richtige Payload senden.
`otel_trace.requestsTooLarge.count` Summe >= 1 für 1 Minute, 1 Mal hintereinander	Anfragen vom Otel Trace-Quell-Plugin enthalten zu viele Daten, wodurch die Pufferkapazität überschritten wird. Passen Sie die Batchgröße für Ihre Kunden an.
`otel_trace.internalServerError.count` Summe >= 0 für 1 Minute, 1 Mal hintereinander	Das Quell-Plugin von Otel Trace hat Probleme beim Empfang von Ereignissen.
`otel_trace.requestTimeouts.count` Summe >= 0 für 1 Minute, 1 aufeinanderfolgendes Mal	Quell-Timeouts sind wahrscheinlich das Ergebnis einer unzureichenden Bereitstellung der Pipeline. Erwägen Sie, die Pipeline `maxUnits` zu erweitern, um die zusätzliche Arbeitslast zu bewältigen.
`otel_metrics.requestTimeouts.count` Summe >= 0 für 1 Minute, 1 Mal hintereinander	Quell-Timeouts sind wahrscheinlich das Ergebnis einer unzureichenden Bereitstellung der Pipeline. Erwägen Sie, die Pipeline `maxUnits` zu erweitern, um die zusätzliche Arbeitslast zu bewältigen.

Amazon OpenSearch Serverlos

Amazon OpenSearch Serverless ist eine On-Demand-Konfiguration mit auto-scaling für Amazon OpenSearch Service. Eine OpenSearch serverlose Sammlung ist ein OpenSearch Cluster, der die Rechenkapazität auf der Grundlage der Anforderungen Ihrer Anwendung skaliert. Dies steht im Gegensatz zu vom OpenSearch Dienst bereitgestellten OpenSearch Domänen, für die Sie die Kapazität manuell verwalten.

OpenSearch Serverless bietet eine einfache, kostengünstige Option für seltene, intermittierende oder unvorhersehbare Workloads. Es ist kostengünstig, da es die Rechenkapazität automatisch an die Nutzung Ihrer Anwendung anpasst.

OpenSearch Serverlose Sammlungen verfügen über dasselbe verteilte und hochverfügbare Speichervolumen mit hoher Kapazität, das von bereitgestellten Dienstdomänen verwendet wird. OpenSearch

OpenSearch Serverlose Sammlungen sind immer verschlüsselt. Sie können den Verschlüsselungsschlüssel auswählen, aber Sie können die Verschlüsselung nicht deaktivieren. Weitere Informationen finden Sie unter the section called “Verschlüsselung”.

Themen

Vorteile

OpenSearch Serverless bietet die folgenden Vorteile:

- Einfacher als bereitgestellt — OpenSearch Serverless macht die Verwaltung von OpenSearch Clustern und Kapazitäten weitgehend überflüssig. Es skaliert und optimiert Ihre Cluster automatisch und kümmert sich um die Lebenszyklusverwaltung von Shards und Indizes. Es verwaltet auch Servicesoftwareupdates und OpenSearch Versionsupgrades. Alle Updates und Upgrades sind unterbrechungsfrei.
- Kostengünstig — Wenn Sie OpenSearch Serverless verwenden, zahlen Sie nur für die Ressourcen, die Sie verbrauchen. Dadurch entfällt die Notwendigkeit einer Vorabbereitstellung und Überbereitstellung für Spitzenlasten.
- Hochverfügbar — OpenSearch Serverless unterstützt Produktionsworkloads mit Redundanz zum Schutz vor Ausfällen der Availability Zone und Infrastrukturausfällen.
- Skalierbar — OpenSearch Serverless skaliert Ressourcen automatisch, um gleichbleibend hohe Datenaufnahmeraten und Antwortzeiten bei Abfragen aufrechtzuerhalten.

Was ist Amazon OpenSearch Serverless?

Amazon OpenSearch Serverless ist eine serverlose On-Demand-Konfiguration für Amazon OpenSearch Service. Serverless beseitigt die betriebliche Komplexität der Bereitstellung, Konfiguration und Optimierung Ihrer Cluster. OpenSearch Dies ist eine gute Option für Unternehmen, die ihre OpenSearch Cluster nicht selbst verwalten möchten, oder für Organisationen, die nicht über die speziellen Ressourcen oder das Fachwissen verfügen, um große Cluster zu betreiben. Mit OpenSearch Serverless können Sie problemlos große Datenmengen durchsuchen und analysieren, ohne sich um die zugrunde liegende Infrastruktur und das Datenmanagement kümmern zu müssen.

Eine OpenSearch serverlose Sammlung ist eine Gruppe von OpenSearch Indizes, die zusammenarbeiten, um eine bestimmte Arbeitslast oder einen bestimmten Anwendungsfall zu unterstützen. Sammlungen sind einfacher zu verwenden als selbstverwaltete OpenSearch Cluster, für die eine manuelle Bereitstellung erforderlich ist.

Sammlungen verfügen über dasselbe verteilte und hochverfügbare Speichervolumen mit hoher Kapazität, das auch von bereitgestellten OpenSearch Dienstdomänen verwendet wird. Sie verringern jedoch die Komplexität, da sie keine manuelle Konfiguration und Optimierung erfordern. Daten werden bei der Übertragung innerhalb einer Sammlung verschlüsselt. OpenSearch Serverless unterstützt auch OpenSearch Dashboards, die eine intuitive Oberfläche für die Datenanalyse bieten.

Serverlose Sammlungen laufen OpenSearch derzeit in Version 2.0.x. Sobald neue Versionen veröffentlicht werden, aktualisiert OpenSearch Serverless Ihre Sammlungen automatisch, um neue Funktionen, Fehlerkorrekturen und Leistungsverbesserungen zu nutzen.

Themen

Anwendungsfälle für Serverless OpenSearch

OpenSearch Serverless unterstützt zwei Hauptanwendungsfälle:

- Protokollanalyse – Das Segment Protokollanalyse befasst sich mit der Analyse großer Mengen an halbstrukturierten, maschinell generierten Zeitreihendaten, um Einblicke in das Betriebs- und Benutzerverhalten zu erhalten.
- Volltextsuche – Das Segment der Volltextsuche unterstützt Anwendungen in Ihren internen Netzwerken (Content-Management-Systeme, Rechtsdokumente) und mit dem Internet verbundene Anwendungen, wie z. B. die Inhaltssuche von E-Commerce-Websites.

Wenn Sie eine Sammlung erstellen, wählen Sie einen dieser Anwendungsfälle aus. Weitere Informationen finden Sie unter the section called “Auswahl eines Sammlungstyps”.

Erste Schritte

Um mit OpenSearch Serverless zu beginnen, erstellen Sie mit der OpenSearch Servicekonsole, dem oder einem der AWS CLI SDKs eine oder mehrere Sammlungen. AWS Ein Tutorial, das Ihnen hilft, eine Sammlung schnell auszuführen, finden Sie unter the section called “Erste Schritte mit Serverless OpenSearch ”.

OpenSearch Serverless unterstützt dieselben Ingest- und Abfrage-API-Operationen wie die OpenSearch Open-Source-Suite, sodass Sie Ihre vorhandenen Clients und Anwendungen weiterhin verwenden können. Ihre Clients müssen mit OpenSearch 2.x kompatibel sein, um mit Serverless

arbeiten zu können. OpenSearch Weitere Informationen finden Sie unter the section called “Erfassung von Daten in Sammlungen”.

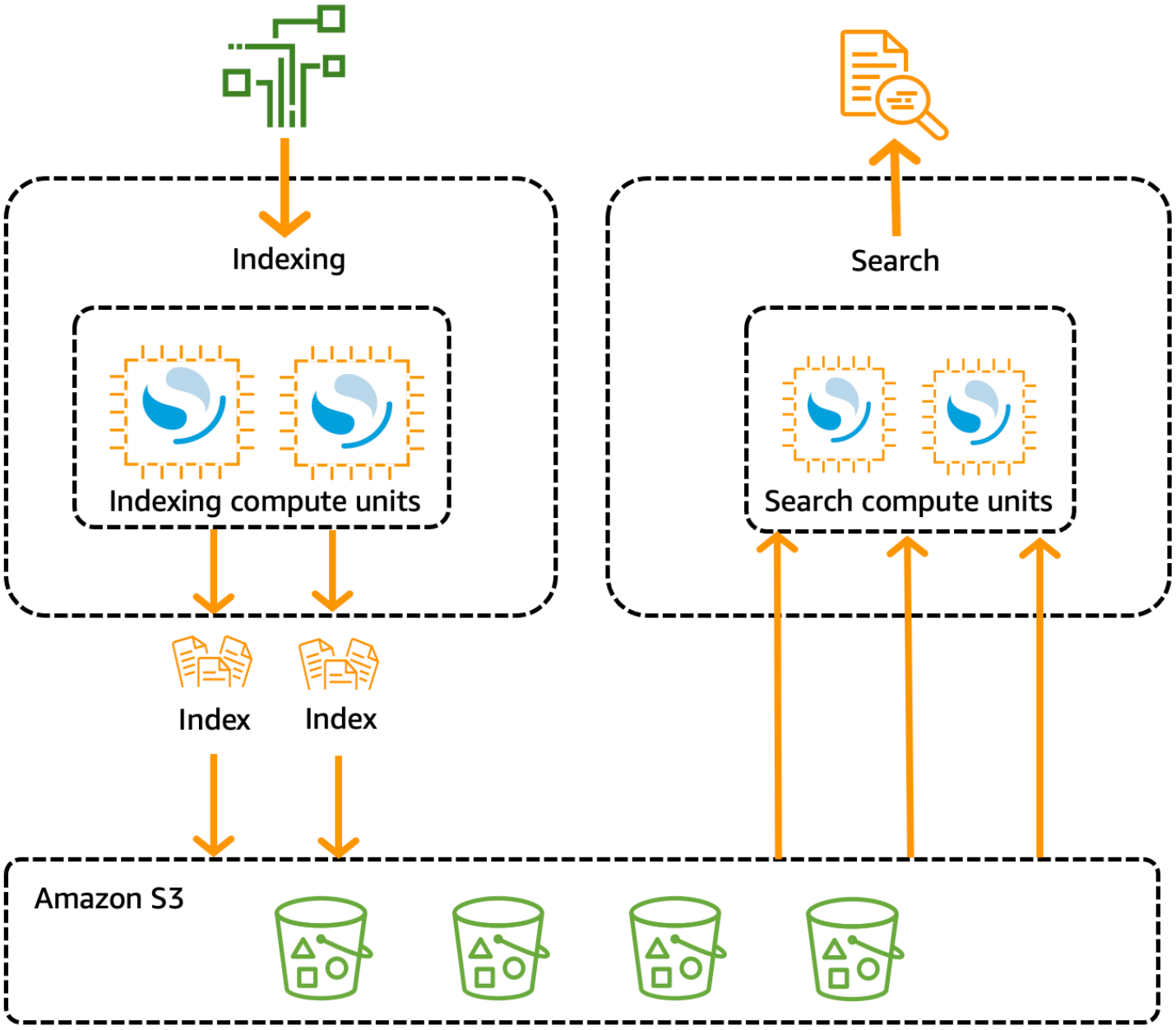
Funktionsweise

Herkömmliche OpenSearch Cluster verfügen über einen einzigen Satz von Instanzen, die sowohl Indizierungs- als auch Suchvorgänge ausführen, und der Indexspeicher ist eng mit der Rechenkapazität verknüpft. Im Gegensatz dazu verwendet OpenSearch Serverless eine cloudnative Architektur, die die Indexierungskomponenten (Ingest) von den Such- (Abfrage-) Komponenten trennt, wobei Amazon S3 der primäre Datenspeicher für Indizes ist.

Diese entkoppelte Architektur ermöglicht es Ihnen, Such- und Indizierungsfunktionen unabhängig voneinander und unabhängig von den indizierten Daten in S3 zu skalieren. Die Architektur bietet auch eine Isolierung für Aufnahme- und Abfragevorgänge, so dass sie ohne Ressourcenkonflikte gleichzeitig ausgeführt werden können.

Wenn Sie Daten in eine Sammlung schreiben, verteilt OpenSearch Serverless sie an die Recheneinheiten für die Indexierung. Die indizierenden Recheneinheiten nehmen die eingehenden Daten auf und verschieben die Indizes zu S3. Wenn Sie eine Suche nach den Sammlungsdaten durchführen, leitet OpenSearch Serverless Anfragen an die Recheneinheiten für die Suche weiter, die die abgefragten Daten enthalten. Die Recheneinheiten für die Suche laden die indizierten Daten direkt von S3 herunter (wenn sie nicht bereits lokal zwischengespeichert sind), führen Suchvorgänge aus und führen Aggregationen durch.

Das folgende Image veranschaulicht diese entkoppelte Architektur:



OpenSearch Serverlose Rechenkapazität für Datenaufnahme, Suche und Abfrage wird in Recheneinheiten (OCUs) gemessen. OpenSearch Jede OCU ist eine Kombination aus 6 GB Speicher und entsprechender virtueller CPU (vCPU) und erstellt eine Daten-Pipeline zu Amazon S3. Jede OCU enthält ausreichend flüchtigen Hot-Speicher für 120 GiB Indexdaten.

Wenn Sie Ihre erste Sammlung erstellen, instanziiert OpenSearch Serverless zwei OCUs — eine für die Indizierung und eine für die Suche. Um eine hohe Verfügbarkeit zu gewährleisten, wird auch eine Reihe von Standby-Knoten in einer anderen Availability Zone gestartet. Zu Entwicklungs- und Testzwecken können Sie die Einstellung Redundanz aktivieren für eine Sammlung deaktivieren, wodurch die beiden Standby-Replikate entfernt und nur zwei OCUs instanziiert werden.

Standardmäßig sind die redundanten aktiven Replikate aktiviert, was bedeutet, dass insgesamt vier OCUs für die erste Sammlung in einem Konto instanziiert werden.

Diese OCUs sind auch dann vorhanden, wenn an den Sammlungsendpunkten keine Aktivität stattfindet. Alle nachfolgenden Sammlungen nutzen diese OCUs gemeinsam. Wenn Sie weitere Sammlungen in demselben Konto erstellen, fügt OpenSearch Serverless nur dann zusätzliche OCUs für die Suche und Aufnahme hinzu, wenn dies zur Unterstützung der Sammlungen erforderlich ist, und zwar entsprechend den von Ihnen angegebenen Kapazitätsgrenzen. Die Kapazität wird mit sinkender Computernutzung wieder herunterskaliert.

Informationen zur Abrechnung dieser OCUs finden Sie unter the section called “Preise für Serverless OpenSearch ”.

Auswahl eines Sammlungstyps

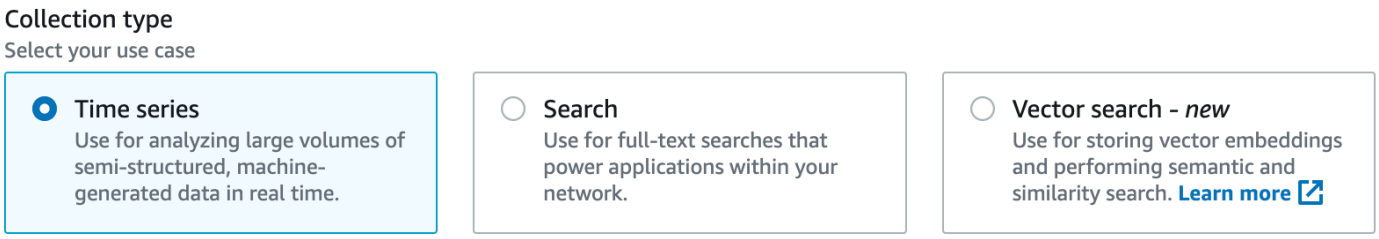
OpenSearch Serverless unterstützt drei primäre Erfassungstypen:

Time series (Zeitreihen) – Das Segment der Protokollanalyse, das sich auf die Analyse großer Mengen halbstrukturierter, maschinengenerierter Daten in Echtzeit konzentriert, um Betriebs-, Sicherheits-, Benutzerverhaltens- und Geschäftseinblicke zu erhalten.

Search (Suche) – Volltextsuche, die Anwendungen in Ihren internen Netzwerken (Content-Management-Systeme, Rechtsdokumente) und mit dem Internet verbundene Anwendungen unterstützt, z. B. die Suche auf E-Commerce-Websites und Inhaltssuche.

Vektorsuche — Semantische Suche nach Vektor-Einbettungen, die das Vektordatenmanagement vereinfacht und erweiterte Sucherlebnisse mit maschinellem Lernen (ML) und generative KI-Anwendungen wie Chatbots, persönliche Assistenten und Betrugserkennung ermöglicht.

Sie wählen einen Sammlungstyp aus, wenn Sie zum ersten Mal eine Sammlung erstellen:



Der ausgewählte Sammlungstyp hängt von der Art der Daten ab, die Sie in die Sammlung aufnehmen möchten, und davon, wie Sie diese abfragen möchten. Sie können den Sammlungstyp nach dem Erstellen nicht mehr ändern.

Die Sammlungstypen weisen die folgenden bemerkenswerten Unterschiede auf:

- Bei Such - und Vektorsuchsammlungen werden alle Daten im Hot-Storage gespeichert, um schnelle Antwortzeiten bei Abfragen zu gewährleisten. Zeitreihen-Sammlungen verwenden eine Kombination aus Hot- und Warm-Speicher, wobei die aktuellsten Daten im Hot-Speicher aufbewahrt werden, um die Reaktionszeiten bei Abfragen für Daten mit häufigerem Zugriff zu optimieren.
- Bei Sammlungen mit Zeitreihen und Vektorsuche können Sie weder anhand einer benutzerdefinierten Dokument-ID indexieren noch anhand von Upsert-Anfragen aktualisieren. Dieser Vorgang ist Suchanwendungsfällen vorbehalten. Sie können stattdessen anhand der Dokument-ID aktualisieren. Weitere Informationen finden Sie unter the section called “Unterstützte OpenSearch API-Operationen und Berechtigungen”.
- Für Such - und Zeitreihensammlungen können Sie keine Indizes vom Typ k-NN verwenden.

Preise für Serverless OpenSearch

Bei OpenSearch Serverless werden Ihnen die folgenden Komponenten in Rechnung gestellt:

- Datenerfassungsleistung
- Such- und Abfrageleistung
- In Amazon S3 verbleibender Speicher

OCUs werden auf Stundenbasis mit sekundengenauer Granularität in Rechnung gestellt. In Ihrem Kontoauszug finden Sie einen Eintrag für Rechenleistung in OCU-Stunden mit einer Kennzeichnung für Datenerfassung und einer Kennzeichnung für Suche. Außerdem werden Ihnen die in Amazon S3 gespeicherten Daten monatlich in Rechnung gestellt. Die Nutzung von OpenSearch Dashboards wird Ihnen nicht in Rechnung gestellt.

Ihnen werden mindestens 2 OCU [0,5 OCU x 2] für die Aufnahme und 1 OCU [0,5 OCU x 2] für die Suche in Rechnung gestellt, wenn Sie eine Sammlung erstellen und redundante aktive Replikate aktivieren. Ihnen wird mindestens 1 OCU [0,5 OCU x 2] für die erste Sammlung in Ihrem Konto in Rechnung gestellt, wenn Sie redundante aktive Replikate deaktivieren. Alle nachfolgenden Sammlungen können diese OCUs gemeinsam nutzen.

OpenSearch Serverless fügt zusätzliche OCUs in Schritten von 1 OCU hinzu, basierend auf der Rechenleistung und dem Speicherplatz, die zur Unterstützung Ihrer Sammlungen benötigt

werden. Sie können eine maximale Anzahl von OCUs für Ihr Konto konfigurieren, um die Kosten zu kontrollieren.

> **Note**
>
> Sammlungen, die einzigartig sind, AWS KMS keys können OCUs nicht mit anderen Sammlungen teilen.

OpenSearch Serverlose Versuche, die minimal erforderlichen Ressourcen zu verwenden, um wechselnden Workloads Rechnung zu tragen. Die Anzahl der zu einem bestimmten Zeitpunkt bereitgestellten OCUs kann variieren und ist nicht exakt. Im Laufe der Zeit wird sich der von OpenSearch Serverless verwendete Algorithmus weiter verbessern, um die Systemnutzung besser zu minimieren.

Vollständige Preisinformationen finden Sie unter Amazon OpenSearch Service-Preise.

Unterstützt AWS-Regionen

OpenSearch Serverless ist in einem Teil AWS-Regionen dieses OpenSearch Dienstes verfügbar. Eine Liste der unterstützten Regionen finden Sie unter Amazon OpenSearch Service-Endpunkte und Kontingente in der Allgemeine AWS-Referenz.

Einschränkungen

OpenSearch Serverless hat die folgenden Einschränkungen:

- Einige OpenSearch API-Operationen werden nicht unterstützt. Siehe the section called “Unterstützte OpenSearch API-Operationen und Berechtigungen”.
- Einige OpenSearch Plugins werden nicht unterstützt. Siehe the section called “ OpenSearch Unterstützte Plugins”.
- Derzeit gibt es keine Möglichkeit, Ihre Daten automatisch von einer verwalteten OpenSearch Dienstdomäne zu einer serverlosen Sammlung zu migrieren. Sie müssen Ihre Daten von einer Domain zu einer Sammlung neu indizieren.
- Kontoübergreifender Zugriff auf Sammlungen wird nicht unterstützt. Sie können Sammlungen von anderen Konten nicht in Ihre Verschlüsselungs- oder Datenzugriffsrichtlinien aufnehmen.
- Benutzerdefinierte OpenSearch Plugins werden nicht unterstützt.

- Sie können keine Snapshots von OpenSearch serverlosen Sammlungen erstellen oder wiederherstellen.
- Regionsübergreifende Suche und Replikation werden nicht unterstützt.
- Die Anzahl der Serverless-Ressourcen, die Sie in einem einzigen Konto und einer Region haben können, ist begrenzt. Siehe OpenSearch Serverlose Kontingente.
- Das Aktualisierungsintervall für Indizes in Vektorsuchsammlungen beträgt ungefähr 60 Sekunden. Das Aktualisierungsintervall für Indizes in Such- und Zeitreihensammlungen beträgt ungefähr 10 Sekunden.
- Die Anzahl der Shards, die Anzahl der Intervalle und das Aktualisierungsintervall können nicht geändert werden und werden von Serverless verwaltet. OpenSearch Die Sharding-Strategie basiert auf der Art der Erfassung und dem Datenverkehr. Beispielsweise skaliert eine Zeitreihen-Sammlung primäre Shards auf der Grundlage von Engpässen im Schreibdatenverkehr.
- Geodatenfunktionen, die in OpenSearch Versionen bis 2.1 verfügbar sind, werden unterstützt.

Vergleich von OpenSearch Service und Serverless OpenSearch

Bei OpenSearch Serverless unterscheiden sich einige Konzepte und Funktionen von den entsprechenden Funktionen für eine bereitgestellte OpenSearch Dienstdomäne. Ein wichtiger Unterschied besteht beispielsweise darin, dass OpenSearch Serverless nicht über das Konzept eines Clusters oder Knotens verfügt.

In der folgenden Tabelle wird beschrieben, wie sich wichtige Funktionen und Konzepte in OpenSearch Serverless von den entsprechenden Funktionen in einer bereitgestellten OpenSearch Dienstdomäne unterscheiden.

Funktion	OpenSearch Dienst	OpenSearch Serverlos
Domains im Vergleich zu Sammlungen	Indizes werden in Domänen gespeichert, bei denen es sich um vorab bereitgestellte OpenSearch Cluster handelt. Weitere Informationen finden Sie unter Erstellen und Verwalten von Domains.	Indizes werden in Sammlungen gespeicherte, bei denen es sich um logische Gruppierungen von Indizes handelt, die einen bestimmten Workload oder Anwendungsfall darstellen. Weitere Informationen finden Sie unter the section called “Erstellen, Auflisten und Löschen von Sammlungen”.

Funktion	OpenSearch Dienst	OpenSearch Serverlos
Knotentypen und Kapazitätsverwaltung	Sie erstellen einen Cluster mit Knotentypen, die Ihren Kosten- und Leistungsspezifikationen entsprechen. Sie müssen Ihren eigenen Speicherbedarf berechnen und einen Instance-Typ für Ihre Domain auswählen. Weitere Informationen finden Sie unter the section called “Größenanpassung von Domains”.	OpenSearch Serverless skaliert automatisch und stellt zusätzliche Recheneinheiten für Ihr Konto auf der Grundlage Ihrer Kapazitätsnutzung bereit. Weitere Informationen finden Sie unter the section called “Verwalten von Kapazitätsgrenzen”.
Fakturierung	Sie zahlen für jede Nutzungsstunde einer EC2-Instance und für die kumulierte Größe aller EBS-Speichervolumes, die an Ihre Instances angefügt sind. Weitere Informationen finden Sie unter the section called “Preisgestaltung”.	Die Rechenleistung für die Datenerfassung, die Rechenleistung für Suche und Abfrage sowie der in S3 beibehaltene Speicherplatz werden Ihnen in OCU-Stunden in Rechnung gestellt. Weitere Informationen finden Sie unter the section called “Preise für Serverless OpenSearch ”.
Verschlüsselung	Die Verschlüsselung im Ruhezustand ist für Domains optional. Weitere Informationen finden Sie unter the section called “Verschlüsselung im Ruhezustand”.	Die Verschlüsselung im Ruhezustand ist für Sammlungen erforderlich. Weitere Informationen finden Sie unter the section called “Verschlüsselung”.

Funktion	OpenSearch Dienst	OpenSearch Serverlos
Datenzugriffskontrolle	Der Zugriff auf die Daten innerhalb von Domains wird durch IAM-Richtlinien und eine differenzierte Zugriffskontrolle bestimmt.	Der Zugriff auf Daten innerhalb von Sammlungen wird durch Datenzugriffsrichtlinien bestimmt.
Unterstützte Operationen OpenSearch	OpenSearch Der Service unterstützt eine Teilmenge aller OpenSearch API-Operationen. Weitere Informationen finden Sie unter the section called “Unterstützte Vorgänge”.	OpenSearch Serverless unterstützt eine andere Teilmenge von OpenSearch API-Vorgängen. Weitere Informationen finden Sie unter the section called “Unterstützte Vorgänge und Plugins”.
Anmeldung für Dashboards	Melden Sie sich mit einem Benutzernamen und einem Passwort an. Weitere Informationen finden Sie unter the section called “Als Masterbenutzer auf OpenSearch Dashboards zugreifen”.	Wenn Sie in der AWS Konsole angemeldet sind und zu Ihrer Dashboard-URL navigieren, melden Sie sich automatisch an. Weitere Informationen finden Sie unter the section called “Zugreifen auf OpenSearch Dashboards”.
APIs	Interagieren Sie mithilfe der OpenSearch Service-API-Operationen programmgesteuert mit dem OpenSearch Service.	Interagieren Sie programmgesteuert mit OpenSearch Serverless mithilfe der Serverless-API-Operationen. OpenSearch

Funktion	OpenSearch Dienst	OpenSearch Serverlos
Netzwerkzugriff	Die Netzwerkeinstellungen für eine Domain gelten sowohl für den Domain-Endpunkt als auch für den Dashboard-Endpunkt. OpenSearch Der Netzwerkzugriff für beide ist eng gekoppelt.	Die Netzwerkeinstellungen für den Domänenendpunkt und den OpenSearch Dashboards-Endpunkt sind entkoppelt. Sie können sich dafür entscheiden, den Netzwerkzugriff für Dashboards nicht zu konfigurieren. OpenSearch Weitere Informationen finden Sie unter the section called “Netzwerkzugriff”.
Signieren von Anforderungen	Verwenden Sie die REST-Clients auf OpenSearch hoher und niedriger Ebene, um Anfragen zu signieren. Geben Sie den Service-Namen als `es` an.	Derzeit unterstützt OpenSearch Serverless eine Untergruppe von Clients, die OpenSearch Service unterstützt. Geben Sie beim Signieren von Anfragen den Service-Namen als `aoss` an. Der `x-amz-content-sha256` -Header ist erforderlich. Weitere Informationen finden Sie unter the section called “Andere Kunden”.
OpenSearch Versionsupgrades	Sie aktualisieren Ihre Domains manuell, sobald neue Versionen von OpenSearch verfügbar sind. Sie sind dafür verantwortlich, dass Ihre Domain die Upgrade-Voraussetzungen erfüllt und dass Sie alle grundlegenden Änderungen vorgenommen haben.	OpenSearch Serverless aktualisiert Ihre Sammlungen automatisch auf neue OpenSearch Versionen. Upgrades werden nicht unbedingt durchgeführt, sobald eine neue Version verfügbar ist.
Service-Software-Updates	Sie wenden Service-Software-Updates manuell auf Ihre Domain an, sobald sie verfügbar sind.	OpenSearch Serverless aktualisiert Ihre Sammlungen automatisch, um die neuesten Bugfixes, Funktionen und Leistungsverbesserungen zu nutzen.

Funktion	OpenSearch Dienst	OpenSearch Serverlos
VPC-Zugriff	Sie können Ihre Domain innerhalb einer VPC bereitstellen. Sie können auch zusätzlich vom OpenSearch Service verwaltete VPC-Endpunkte für den Zugriff auf die Domain erstellen.	Sie erstellen einen oder OpenSearch mehrere serverlos verwaltete VPC-Endpoints für Ihr Konto. Anschließend nehmen Sie diese Endpunkte in die Netzwerkrichtlinien auf.
SAML-Authentifizierung	Sie aktivieren die SAML-Authentifizierung auf Domain-Basis. Weitere Informationen finden Sie unter the section called “SAML-Authentifizierung für Dashboards OpenSearch ”.	Sie konfigurieren einen oder mehrere SAML-Anbieter auf Kontoebene und nehmen anschließend die zugehörigen Benutzer- und Gruppen-IDs in die Datenzugriffsrichtlinien auf. Weitere Informationen finden Sie unter the section called “SAML-Authentifizierung”.
Transport Layer Security (TLS)	OpenSearch Der Service unterstützt TLS 1.2, es wird jedoch empfohlen, TLS 1.3 zu verwenden.	OpenSearch Serverless unterstützt TLS 1.2, es wird jedoch empfohlen, TLS 1.3 zu verwenden.

Erste Schritte mit Amazon OpenSearch Serverless

Dieses Tutorial führt Sie durch die grundlegenden Schritte, um eine Amazon OpenSearch Serverless-Suchsammlung schnell zum Laufen zu bringen. Eine Suchsammlung ermöglicht es Ihnen, Anwendungen in Ihren internen Netzwerken und mit dem Internet verbundene Anwendungen wie die Suche nach E-Commerce-Websites und die Inhaltssuche zu unterstützen.

Informationen zur Verwendung einer Vektorsuchsammlung finden Sie unter. the section called “Arbeiten mit Vektorsuchsammlungen” Ausführlichere Informationen zur Verwendung von Sammlungen finden Sie unter the section called “Erstellen, Auflisten und Löschen von Sammlungen” und den anderen Themen in diesem Handbuch.

In diesem Tutorial führen Sie die folgenden Schritte durch:

1. Konfigurieren von Berechtigungen
2. Erstellen einer Sammlung
3. Hochladen und Suchen von Daten
4. Löschen der Sammlung

Schritt 1: Konfigurieren von Berechtigungen

Um dieses Tutorial abschließen und OpenSearch Serverless im Allgemeinen verwenden zu können, benötigen Sie die richtigen IAM-Berechtigungen. In diesem Tutorial werden Sie eine Sammlung erstellen, Daten hochladen und suchen und die Sammlung anschließend löschen.

Ihr Benutzer oder Ihre Rolle muss über eine angefügte identitätsbasierte Richtlinie mit den folgenden Mindestberechtigungen verfügen:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "aoss:CreateCollection",
        "aoss:ListCollections",
        "aoss:BatchGetCollection",
        "aoss:DeleteCollection",
        "aoss:CreateAccessPolicy",
        "aoss:ListAccessPolicies",
        "aoss:UpdateAccessPolicy",
        "aoss:CreateSecurityPolicy",
        "aoss:GetSecurityPolicy",
        "aoss:UpdateSecurityPolicy",
        "iam:ListUsers",
        "iam:ListRoles"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Weitere Informationen zu OpenSearch Serverless IAM-Berechtigungen finden Sie unter. the section called “Identitäts- und Zugriffsverwaltung”

Schritt 2: Erstellen einer Sammlung

Eine Sammlung ist eine Gruppe von OpenSearch Indizes, die zusammenarbeiten, um eine bestimmte Arbeitslast oder einen bestimmten Anwendungsfall zu unterstützen.

Um eine OpenSearch serverlose Sammlung zu erstellen

1. Öffnen Sie die Amazon OpenSearch Service-Konsole unter https://console.aws.amazon.com/aos/home.
2. Wählen Sie im linken Navigationsbereich Collections (Sammlungen) und wählen Sie Create collection (Sammlung erstellen) aus.
3. Benennen Sie die Sammlung movies (Filme).
4. Wählen Sie für den Sammlungstyp Search (Suche) aus. Weitere Informationen finden Sie unter Auswahl eines Sammlungstyps.
5. Wählen Sie unter Sicherheit die Option Standard create aus.
6. Wählen Sie unter Verschlüsselung die Option Verwenden aus AWS-eigener Schlüssel. Dies ist der AWS KMS key , den OpenSearch Serverless verwendet, um Ihre Daten zu verschlüsseln.
7. Konfigurieren Sie unter Network (Netzwerk) die Netzwerkeinstellungen für die Sammlung.
   - Wählen Sie für den Zugriffstyp Public (Öffentlich) aus.
   - Wählen Sie als Ressourcentyp sowohl Zugriff auf OpenSearch Endpunkte aktivieren als auch Zugriff auf Dashboards aktivieren aus. OpenSearch Da Sie Daten mithilfe von OpenSearch Dashboards hochladen und suchen, müssen Sie beide aktivieren.
8. Wählen Sie Weiter aus.
9. Richten Sie unter Configure data access (Datenzugriff konfigurieren) die Zugriffseinstellungen für die Sammlung ein. Datenzugriffsrichtlinien ermöglichen Benutzern und Rollen den Zugriff auf die Daten innerhalb einer Sammlung. In diesem Tutorial erteilen wir einem einzelnen Benutzer die Berechtigungen, die zum Indizieren und Durchsuchen von Daten in der Filme-Sammlung erforderlich sind.

   Erstellen Sie eine einzelne Regel, die den Zugriff auf die Filme-Sammlung ermöglicht. Nennen Sie die Regel Movies collection access (Zugriff auf Filme-Sammlung).
10. Wählen Sie Principals, IAM-Benutzer und -Rollen hinzufügen und wählen Sie den Benutzer oder die Rolle aus, mit der Sie sich bei OpenSearch Dashboards anmelden und Daten indexieren möchten. Wählen Sie Speichern.
11. Wählen Sie unter Index permissions (Indexberechtigungen) alle Berechtigungen aus.

12. Wählen Sie Weiter aus.
13. Wählen Sie für die Zugriffsrichtlinieneinstellungen die Option Create a new data access policy (Neue Datenzugriffsrichtlinie erstellen) aus und nennen Sie die Richtlinie movies (Filme).
14. Wählen Sie Weiter aus.
15. Überprüfen Sie Ihre Sammlungseinstellungen und wählen Sie Submit (Senden) aus. Warten Sie einige Minuten, bis der Sammlungsstatus `Active` erreicht ist.

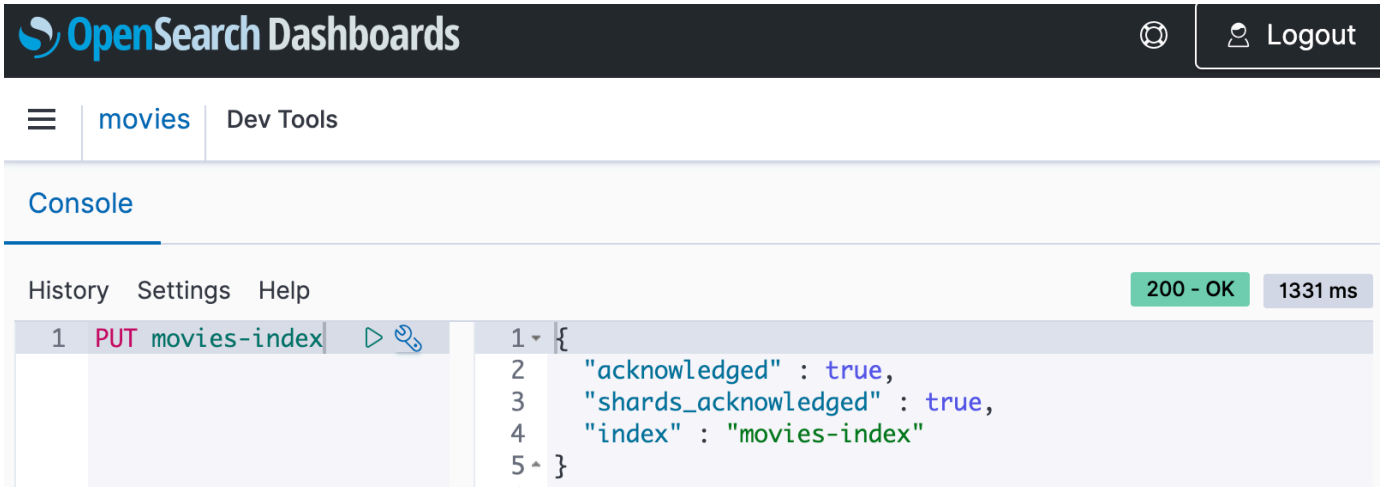
Schritt 3: Daten hochladen und suchen

Sie können Daten mit Postman oder cURL in eine OpenSearch serverlose Sammlung hochladen. Der Kürze halber verwenden diese Beispiele Dev Tools in der Dashboards-Konsole. OpenSearch

So indizieren und durchsuchen Sie Daten in der Filme-Sammlung

1. Wählen Sie im linken Navigationsbereich Collections (Sammlungen) und wählen Sie die movies (Filme)-Sammlung aus, um ihre Detailseite zu öffnen.
2. Wählen Sie die OpenSearch Dashboard-URL für die Sammlung aus. Die URL nimmt das Format `https://dashboards.{region}.aoss.amazonaws.com/_login/?collectionId={collection-id}` an.
3. Öffnen Sie in OpenSearch Dashboards den linken Navigationsbereich und wählen Sie Dev Tools aus.
4. Um einen einzelnen Index mit dem Namen movies-index zu erstellen, senden Sie die folgende Anfrage:

```
PUT movies-index
```



5. Um ein einzelnes Dokument in movies-index zu indizieren, senden Sie die folgende Anfrage:

```
PUT movies-index/_doc/1
{
  "title": "Shawshank Redemption",
  "genre": "Drama",
  "year": 1994
}
```

6. Um Daten in OpenSearch Dashboards zu suchen, müssen Sie mindestens ein Indexmuster konfigurieren. OpenSearch verwendet diese Muster, um zu identifizieren, welche Indizes Sie analysieren möchten. Öffnen Sie den linken Navigationsbereich, wählen Sie Stack-Verwaltung, wählen Sie Indexmuster und anschließend die Option Indexmuster erstellen aus. Geben Sie für dieses Tutorial Filme ein.
7. Wählen Sie Nächster Schritt aus und klicken Sie auf Indexmuster erstellen. Nachdem das Muster erstellt wurde, können Sie die verschiedenen Dokumentfelder anzeigen, z. B. `title` und `genre`.
8. Um mit der Suche nach Ihren Daten zu beginnen, öffnen Sie erneut den linken Navigationsbereich und wählen Sie Discover (Entdecken) aus, oder verwenden Sie die Such-API in Dev Tools.

Schritt 4: Sammlung löschen

Da die Filme-Sammlung zu Testzwecken dient, sollten Sie sie löschen, wenn Sie mit dem Experimentieren fertig sind.

Um eine OpenSearch serverlose Sammlung zu löschen

1. Gehen Sie zurück zur Amazon OpenSearch Service-Konsole.
2. Wählen Sie im linken Navigationsbereich Collections (Sammlungen) und anschließend die movies (Filme)-Samlung aus.
3. Wählen Sie Löschen und bestätigen Sie das Löschen.

Nächste Schritte

Da Sie nun wissen, wie Sie eine Sammlung erstellen und Daten indizieren, möchten Sie vielleicht einige der folgenden Übungen ausprobieren:

- Weitere erweiterte Optionen zum Erstellen einer Sammlung finden Sie hier. Weitere Informationen finden Sie unter the section called “Erstellen, Auflisten und Löschen von Sammlungen”.
- Erfahren Sie, wie Sie Sicherheitsrichtlinien konfigurieren, um die Sammlungssicherheit in großem Umfang zu verwalten. Weitere Informationen finden Sie unter the section called “Sicherheit bei Serverless OpenSearch ”.
- Entdecken Sie andere Möglichkeiten, Daten in Sammlungen zu indizieren. Weitere Informationen finden Sie unter the section called “Erfassung von Daten in Sammlungen”.

Amazon OpenSearch Serverless-Sammlungen erstellen und verwalten

Sie können Amazon OpenSearch Serverless-Sammlungen mithilfe der Konsole, der and-API, der AWS SDKs AWS CLI und erstellen. AWS CloudFormation

Themen

- Amazon OpenSearch Serverless-Sammlungen erstellen, auflisten und löschen
- Arbeiten mit Vektorsuchsammlungen
- Verwenden von Datenlebenszyklusrichtlinien mit Amazon OpenSearch Serverless
- Verwendung der AWS SDKs zur Interaktion mit Amazon Serverless OpenSearch
- AWS CloudFormationZum Erstellen von Amazon OpenSearch Serverless-Sammlungen verwenden

Amazon OpenSearch Serverless-Sammlungen erstellen, auflisten und löschen

Eine Sammlung in Amazon OpenSearch Serverless ist eine logische Gruppierung von einem oder mehreren Indizes, die einen Analyse-Workload darstellen. OpenSearch Der Service verwaltet und optimiert die Sammlung automatisch und erfordert nur minimale manuelle Eingaben.

Themen

Erforderliche Berechtigungen

OpenSearch Serverless verwendet die folgenden AWS Identity and Access Management (IAM-) Berechtigungen zum Erstellen und Verwalten von Sammlungen. Sie können IAM-Bedingungen festlegen, um Benutzer auf bestimmte Sammlungen zu beschränken.

- `aoss:CreateCollection` – Erstellt Sie eine Sammlung.
- `aoss:ListCollections` – Listet Sammlungen im aktuellen Konto auf.
- `aoss:BatchGetCollection` – Ruft Details zu einer oder mehreren Sammlungen ab.
- `aoss:UpdateCollection` – Ändert eine Sammlung.
- `aoss:DeleteCollection` – Löscht eine Sammlung.

Das folgende Beispiel für eine identitätsbasierte Zugriffsrichtlinie stellt die Mindestberechtigungen bereit, die ein Benutzer benötigt, um eine einzelne Sammlung mit dem Namen `Logs` zu verwalten:

```
[
   {
      "Sid":"Allows managing logs collections",
      "Effect":"Allow",
      "Action":[
         "aoss:CreateCollection",
```

```
            "aoss:ListCollections",
            "aoss:BatchGetCollection",
            "aoss:UpdateCollection",
            "aoss:DeleteCollection",
            "aoss:CreateAccessPolicy",
            "aoss:CreateSecurityPolicy"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "aoss:collection":"Logs"
            }
         }
      }
]
```

`aoss:CreateAccessPolicy` und `aoss:CreateSecurityPolicy` sind enthalten, da Verschlüsselungs-, Netzwerk- und Datenzugriffsrichtlinien erforderlich sind, damit eine Sammlung ordnungsgemäß funktioniert. Weitere Informationen finden Sie unter the section called “Identitäts- und Zugriffsverwaltung”.

> **Note**
>
> Wenn Sie die erste Sammlung in Ihrem Konto erstellen, benötigen Sie auch die `iam:CreateServiceLinkedRole`-Berechtigung. Weitere Informationen finden Sie unter the section called “Rolle bei der Sammlungserstellung”.

Erstellen von Sammlungen

Sie können die Konsole oder die verwenden, um eine serverlose Sammlung AWS CLI zu erstellen. In diesen Schritten wird beschrieben, wie Sie eine Suche oder eine Zeitreihensammlung erstellen. Informationen zum Erstellen einer Vektorsuchsammlung finden Sie unterthe section called “Arbeiten mit Vektorsuchsammlungen”.

Eine Sammlung erstellen (Konsole)

So erstellen Sie eine Sammlung mithilfe der Konsole

1. Navigieren Sie zur Amazon OpenSearch Service-Konsole unter https://console.aws.amazon.com/aos/home/.

2. Erweitern Sie im linken Navigationsbereich Serverless und wählen Sie Collections (Sammlungen) aus.
3. Wählen Sie Create Connection (Verbindung erstellen) aus.
4. Geben Sie einen Namen und eine Beschreibung für die Sammlung an. Der Name muss die folgenden Kriterien erfüllen:

   - ist einzigartig für Ihr Konto und AWS-Region
   - Beginnt mit einem Kleinbuchstaben
   - Enthält zwischen 3 und 32 Zeichen
   - Enthält nur Kleinbuchstaben a–z, die Zahlen 0–9 und den Bindestrich (-)
5. Auswahl eines Sammlungstyps:

   - Search (Suche) – Volltextsuche, die Anwendungen in Ihren internen Netzwerken und Anwendungen mit Internetzugriff unterstützt. Alle Suchdaten werden im Hot-Speicher gespeichert, um schnelle Antwortzeiten auf Abfragen zu stellen.
   - Time series (Zeitreihen) – Segment der Protokollanalyse, das sich auf die Analyse großer Mengen halbstrukturierter, maschinell generierter Daten konzentriert. Daten werden mindestens 24 Stunden in Hot-Indizes gespeichert, der Rest verbleibt im Warmspeicher.
   - Vektorsuche — Semantische Suche nach Vektoreinbettungen, die die Verwaltung von Vektordaten vereinfacht. Unterstützt erweiterte Sucherlebnisse mit maschinellem Lernen (ML) und generative KI-Anwendungen wie Chatbots, persönliche Assistenten und Betrugserkennung.

   Weitere Informationen finden Sie unter the section called “Auswahl eines Sammlungstyps”.
6. Wählen Sie unter Bereitstellungstyp die Redundanzeinstellung für Ihre Sammlung aus. Standardmäßig wird jede Sammlung mit Redundanz erstellt, was bedeutet, dass die Indexierungs- und OpenSearch Suchcompute-Einheiten (OCUs) jeweils ihre eigenen Standby-Replikate in einer anderen Availability Zone haben. Zu Entwicklungs- und Testzwecken können Sie die Redundanz deaktivieren, wodurch die Anzahl der OCUs in Ihrer Sammlung auf zwei reduziert wird. Weitere Informationen finden Sie unter the section called “Funktionsweise”.
7. Wählen Sie unter Verschlüsselung einen AWS KMS Schlüssel aus, mit dem Sie Ihre Daten verschlüsseln möchten. OpenSearch Serverless benachrichtigt Sie, wenn der von Ihnen eingegebene Sammlungsname einem in einer Verschlüsselungsrichtlinie definierten Muster entspricht. Sie können diese Übereinstimmung beibehalten oder mit eindeutigen

Verschlüsselungseinstellungen überschreiben. Weitere Informationen finden Sie unter the section called “Verschlüsselung”.

8. Konfigurieren Sie unter Network access settings (Netzwerkzugriffseinstellungen) den Netzwerkzugriff für die Sammlung.

   - Wählen Sie als Zugriffstyp öffentlich oder privat aus. Geben Sie anschließend an, welche VPC-Endpoints auf die AWS-Services Sammlung zugreifen können.
     - VPC-Endpunkte für den Zugriff — Geben Sie einen oder mehrere VPC-Endpunkte an, über die der Zugriff ermöglicht werden soll. Informationen zum Erstellen eines VPC-Endpunkts finden Sie unter the section called “VPC-Endpunkte”.
     - AWS-Service privater Zugriff — Wählen Sie einen oder mehrere unterstützte Dienste aus, auf die Sie zugreifen möchten.
   - Wählen Sie unter Ressourcentyp aus, ob auf die Sammlung über ihren OpenSearchEndpunkt (um API-Aufrufe über curl, Postman usw. zu tätigen), über den OpenSearch Dashboards-Endpunkt (um mit Visualisierungen zu arbeiten und API-Aufrufe über die Konsole zu tätigen) oder über beide zugegriffen werden kann.

   > **Note**
   >
   > AWS-Service Der private Zugriff gilt nur für den Endpunkt, nicht für den OpenSearch Dashboards-Endpunkt. OpenSearch

   OpenSearch Serverless benachrichtigt Sie, wenn der von Ihnen eingegebene Sammlungsname einem in einer Netzwerkrichtlinie definierten Muster entspricht. Sie können diese Übereinstimmung beibehalten oder mit benutzerdefinierten Netzwerkeinstellungen überschreiben. Weitere Informationen finden Sie unter the section called “Netzwerkzugriff”.

9. (Optional) Fügen Sie der Sammlung ein oder mehrere Tags hinzu. Weitere Informationen finden Sie unter the section called “Markieren von Sammlungen”.
10. Wählen Sie Weiter.
11. Konfigurieren Sie Datenzugriffsregeln für die Sammlung, die festlegen, wer auf die Daten innerhalb der Sammlung zugreifen kann. Für jede Regel, die Sie erstellen, führen Sie die folgenden Schritte aus:

- Wählen Sie Add principals (Prinzipale hinzufügen) und wählen Sie eine oder mehrere IAM-Rollen oder SAML users and groups (SAML-Benutzer und -Gruppen) aus, denen Sie Datenzugriff gewähren möchten.
- Unter Grant permissions (Berechtigungen gewähren) wählen Sie die Alias-, Vorlagen- und Indexberechtigungen aus, um die zugehörigen Prinzipale zu erteilen. Eine vollständige Liste der Berechtigungen und des von ihnen gewährten Zugriffs finden Sie unter the section called “Unterstützte OpenSearch API-Operationen und Berechtigungen”.

OpenSearch Serverless benachrichtigt Sie, wenn der von Ihnen eingegebene Sammlungsname einem in einer Datenzugriffsrichtlinie definierten Muster entspricht. Sie können diese Übereinstimmung beibehalten oder mit eindeutigen Datenzugriffseinstellungen überschreiben. Weitere Informationen finden Sie unter the section called “Datenzugriffskontrolle”.

12. Wählen Sie Weiter.
13. Wählen Sie unter Data access policy settings (Einstellungen für die Datenzugriffsrichtlinie) aus, was mit den Regeln geschehen soll, die Sie gerade erstellt haben. Sie können sie entweder verwenden, um eine neue Datenzugriffsrichtlinie zu erstellen, oder sie zu einer vorhandenen Richtlinie hinzufügen.
14. Überprüfen Sie Ihre Sammlungskonfiguration und wählen Sie Submit (Senden) aus.

Der Erfassungsstatus ändert sich in, wenn `Creating` OpenSearch Serverless die Sammlung erstellt.

Eine Sammlung erstellen (CLI)

Bevor Sie eine Sammlung mit dem erstellen AWS CLI, benötigen Sie eine Verschlüsselungsrichtlinie mit einem Ressourcenmuster, das dem beabsichtigten Namen der Sammlung entspricht. Wenn Sie beispielsweise Ihre Sammlungs-Protokollanwendung benennen möchten, können Sie eine Verschlüsselungsrichtlinie wie die folgende erstellen:

```
aws opensearchserverless create-security-policy \
  --name logs-policy \
  --type encryption --policy "{\"Rules\":[{\"ResourceType\":\"collection\",\"Resource
\":[\"collection\/logs-application\"]}],\"AWSOwnedKey\":true}"
```

Wenn Sie die Richtlinie für weitere Sammlungen verwenden möchten, können Sie die Regel breiter fassen, wie z. B. `collection/logs*` oder `collection/*`.

Außerdem müssen Sie Netzwerkeinstellungen für die Sammlung in Form einer Netzwerkrichtlinie konfigurieren. Unter Verwendung des vorherigen Beispiels für die Protokollanwendung könnten Sie die folgende Netzwerkrichtlinie erstellen:

```
aws opensearchserverless create-security-policy \
  --name logs-policy \
  --type network --policy "[{\"Description\":\"Public access for logs collection
\",\"Rules\":[{\"ResourceType\":\"dashboard\",\"Resource\":[\"collection\/logs-
application\"]},{\"ResourceType\":\"collection\",\"Resource\":[\"collection\/logs-
application\"]}],\"AllowFromPublic\":true}]"
```

> **Note**
>
> Sie können Netzwerkrichtlinien erstellen, nachdem Sie eine Sammlung erstellt haben. Wir empfehlen jedoch, dies vorher zu tun.

Um eine Sammlung zu erstellen, senden Sie eine CreateCollectionAnfrage:

```
aws opensearchserverless create-collection --name "logs-application" --type SEARCH --
description "A collection for storing log data"
```

Geben Sie für `type` entweder `SEARCH` oder `TIMESERIES` an. Weitere Informationen finden Sie unter the section called “Auswahl eines Sammlungstyps”.

Beispielantwort

```
{
    "createCollectionDetail": {
        "id": "07tjusf2h91cunochc",
        "name": "books",
        "description":"A collection for storing log data",
        "status": "CREATING",
        "type": "SEARCH",
        "kmsKeyArn": "auto",
        "arn": "arn:aws:aoss:us-east-1:123456789012:collection/07tjusf2h91cunochc",
        "createdDate": 1665952577473
    }
}
```

Wenn Sie in der Anfrage keinen Sammlungstyp angeben, wird standardmäßig `TIMESERIES` verwendet. Wenn Ihre Sammlung mit einem AWS-eigener Schlüssel verschlüsselt ist, handelt es sich bei `kmsKeyArn` um `auto` und nicht um einen ARN.

> **Important**
>
> Nachdem Sie eine Sammlung erstellt haben, können Sie nicht darauf zugreifen, es sei denn, sie entspricht einer Datenzugriffsrichtlinie. Anweisungen zum Erstellen von Datenzugriffsrichtlinien finden Sie unter the section called “Datenzugriffskontrolle”.

Zugreifen auf OpenSearch Dashboards

Nachdem Sie eine Sammlung mit dem erstellt haben AWS Management Console, können Sie zur OpenSearch Dashboard-URL der Sammlung navigieren. Sie finden die Dashboard-URL, indem Sie im linken Navigationsbereich Sammlungen und dann die Sammlung auswählen, um die zugehörige Detailseite zu öffnen. Die URL nimmt das Format `https://dashboards.us-east-1.aoss.amazonaws.com/_login/?collectionId=07tjusf2h91cunochc` an. Sobald Sie zur URL navigieren, melden Sie sich automatisch bei Dashboards an.

Wenn Sie die OpenSearch Dashboard-URL bereits verfügbar haben, aber nicht auf der sind AWS Management Console, wird beim Aufrufen der Dashboard-URL über den Browser zur Konsole weitergeleitet. Sobald Sie Ihre AWS Anmeldeinformationen eingegeben haben, melden Sie sich automatisch bei Dashboards an. Informationen zum Zugriff auf Sammlungen für SAML finden Sie unter Zugreifen auf OpenSearch Dashboards mit SAML.

Das Timeout der OpenSearch Dashboard-Konsole beträgt eine Stunde und ist nicht konfigurierbar.

> **Note**
>
> Am 10. Mai 2023 OpenSearch wurde ein gemeinsamer globaler Endpunkt für OpenSearch Dashboards eingeführt. Sie können jetzt im Browser mit einer URL, die das Format annimmt, zu OpenSearch Dashboards navigieren. `https://dashboards.us-east-1.aoss.amazonaws.com/_login/?collectionId=07tjusf2h91cunochc` Um die Abwärtskompatibilität zu gewährleisten, werden wir die bestehenden sammlungsspezifischen OpenSearch Dashboard-Endpunkte weiterhin mit diesem Format unterstützen. `https://07tjusf2h91cunochc.us-east-1.aoss.amazonaws.com/_dashboards`

Anzeigen von Sammlungen

Sie können die vorhandenen Sammlungen in Ihrem AWS-Konto auf der Registerkarte Sammlungen der Amazon OpenSearch Service-Konsole einsehen.

Um Sammlungen zusammen mit ihren IDs aufzulisten, senden Sie eine ListCollectionsAnfrage.

```
aws opensearchserverless list-collections
```

Beispielantwort

```
{
   "collectionSummaries":[
      {
         "arn":"arn:aws:aoss:us-east-1:123456789012:collection/07tjusf2h91cunochc",
         "id":"07tjusf2h91cunochc",
         "name":"my-collection",
         "status":"CREATING"
      }
   ]
}
```

Um die Suchergebnisse einzuschränken, verwenden Sie Sammlungsfilter. Diese Anfrage filtert die Antwort auf Sammlungen im `ACTIVE`-Zustand:

```
aws opensearchserverless list-collections --collection-filters '{ "status": "ACTIVE" }'
```

Um detailliertere Informationen zu einer oder mehreren Sammlungen, einschließlich des OpenSearch Endpunkts und des OpenSearch Dashboards-Endpunkts, zu erhalten, senden Sie eine BatchGetCollectionAnfrage:

```
aws opensearchserverless batch-get-collection --ids ["07tjusf2h91cunochc",
 "1iu5usc4rame"]
```

> **Note**
>
> Sie können `--names` oder `--ids` in die Anfrage aufnehmen, aber nicht beides.

Beispielantwort

```
{
   "collectionDetails":[
      {
         "id": "07tjusf2h91cunochc",
         "name": "my-collection",
         "status": "ACTIVE",
         "type": "SEARCH",
         "description": "",
         "arn": "arn:aws:aoss:us-east-1:123456789012:collection/07tjusf2h91cunochc",
         "kmsKeyArn": "arn:aws:kms:us-
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab",
         "createdDate": 1667446262828,
         "lastModifiedDate": 1667446300769,
         "collectionEndpoint": "https://07tjusf2h91cunochc.us-
east-1.aoss.amazonaws.com",
         "dashboardEndpoint": "https://07tjusf2h91cunochc.us-east-1.aoss.amazonaws.com/
_dashboards"
      },
      {
         "id": "178ukvtg3i82dvopdid",
         "name": "another-collection",
         "status": "ACTIVE",
         "type": "TIMESERIES",
         "description": "",
         "arn": "arn:aws:aoss:us-east-1:123456789012:collection/178ukvtg3i82dvopdid",
         "kmsKeyArn": "arn:aws:kms:us-
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab",
         "createdDate": 1667446262828,
         "lastModifiedDate": 1667446300769,
         "collectionEndpoint": "https://178ukvtg3i82dvopdid.us-
east-1.aoss.amazonaws.com",
         "dashboardEndpoint": "https://178ukvtg3i82dvopdid.us-
east-1.aoss.amazonaws.com/_dashboards"
      }
   ],
   "collectionErrorDetails":[]
}
```


Löschen von Sammlungen

Beim Löschen einer Sammlung werden alle Daten und Indizes in der Sammlung gelöscht. Sie können Sammlungen nicht wiederherstellen, nachdem Sie diese gelöscht haben.

So löschen Sie eine Sammlung über die Konsole

1. Wählen Sie im Bereich Sammlungen der Amazon OpenSearch Service-Konsole die Sammlung aus, die Sie löschen möchten.
2. Wählen Sie Löschen und bestätigen Sie das Löschen.

Um eine Sammlung mit dem zu löschen AWS CLI, senden Sie eine DeleteCollectionAnfrage:

```
aws opensearchserverless delete-collection --id 07tjusf2h91cunochc
```

Beispielantwort

```
{
   "deleteCollectionDetail":{
      "id":"07tjusf2h91cunochc",
      "name":"my-collection",
      "status":"DELETING"
   }
}
```

Arbeiten mit Vektorsuchsammlungen

Der Sammlungstyp der Vektorsuche in OpenSearch Serverless bietet eine skalierbare und leistungsstarke Funktion zur Ähnlichkeitssuche. Es macht es Ihnen leicht, moderne, erweiterte Sucherlebnisse für maschinelles Lernen (ML) und Anwendungen für generative künstliche Intelligenz (KI) zu entwickeln, ohne die zugrunde liegende Vektordatenbankinfrastruktur verwalten zu müssen.

Zu den Anwendungsfällen für Vektorsuchsammlungen gehören Bildersuchen, Dokumentensuchen, Musikabruf, Produktempfehlungen, Videosuchen, standortbezogene Suchen, Betrugserkennung und Anomalieerkennung.

Da die Vektor-Engine für OpenSearch Serverless auf der Suchfunktion k-Nearest Neighbor (k-NN) basiert OpenSearch, erhalten Sie dieselbe Funktionalität mit der Einfachheit einer serverlosen Umgebung. Die Engine unterstützt die k-NN-API-Operationen. OpenSearch Mit diesen Vorgängen können Sie Volltextsuche, erweiterte Filterung, Aggregationen, Geodatenabfragen, verschachtelte Abfragen zum schnelleren Abrufen von Daten und verbesserte Suchergebnisse nutzen.

Die Vektor-Engine bietet Entfernungsmetriken wie euklidische Entfernung, Kosinusähnlichkeit und Punktproduktähnlichkeit und kann 16.000 Dimensionen aufnehmen. Sie können Felder

mit verschiedenen Datentypen für Metadaten wie Zahlen, Boolesche Werte, Datumsangaben, Stichwörter und Geopunkte speichern. Sie können auch Felder mit Text für beschreibende Informationen speichern, um gespeicherten Vektoren mehr Kontext zu verleihen. Durch die gemeinsame Zuordnung der Datentypen wird die Komplexität reduziert, die Wartbarkeit erhöht und Datenduplizierungen, Probleme mit der Versionskompatibilität und Lizenzprobleme vermieden.

Erste Schritte mit Sammlungen für die Vektorsuche

In diesem Tutorial führen Sie die folgenden Schritte aus, um Vektoreinbettungen in Echtzeit zu speichern, zu suchen und abzurufen:

1. Konfigurieren von Berechtigungen
2. Erstellen einer Sammlung
3. Hochladen und Suchen von Daten
4. Löschen der Sammlung

Schritt 1: Konfigurieren von Berechtigungen

Um dieses Tutorial abzuschließen (und OpenSearch Serverless im Allgemeinen zu verwenden), benötigen Sie die richtigen AWS Identity and Access Management (IAM-) Berechtigungen. In diesem Tutorial erstellen Sie eine Sammlung, laden Daten hoch, suchen nach Daten und löschen dann die Sammlung.

Ihr Benutzer oder Ihre Rolle muss über eine angefügte identitätsbasierte Richtlinie mit den folgenden Mindestberechtigungen verfügen:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "aoss:CreateCollection",
        "aoss:ListCollections",
        "aoss:BatchGetCollection",
        "aoss:DeleteCollection",
        "aoss:CreateAccessPolicy",
        "aoss:ListAccessPolicies",
        "aoss:UpdateAccessPolicy",
        "aoss:CreateSecurityPolicy",
        "iam:ListUsers",
```

```
        "iam:ListRoles"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Weitere Informationen zu OpenSearch serverlosen IAM-Berechtigungen finden Sie unter. the section called “Identitäts- und Zugriffsverwaltung”

Schritt 2: Erstellen einer Sammlung

Eine Sammlung ist eine Gruppe von OpenSearch Indizes, die zusammenarbeiten, um eine bestimmte Arbeitslast oder einen bestimmten Anwendungsfall zu unterstützen.

Um eine OpenSearch serverlose Sammlung zu erstellen

1. Öffnen Sie die Amazon OpenSearch Service-Konsole unter https://console.aws.amazon.com/aos/home.
2. Wählen Sie im linken Navigationsbereich Collections (Sammlungen) und wählen Sie Create collection (Sammlung erstellen) aus.
3. Nennen Sie das Sammelhaus.
4. Wählen Sie als Sammlungstyp die Option Vektorsuche aus. Weitere Informationen finden Sie unter the section called “Auswahl eines Sammlungstyps”.
5. Deaktivieren Sie unter Bereitstellungstyp die Option Redundanz aktivieren (aktive Replikate). Dadurch wird eine Sammlung im Entwicklungs- oder Testmodus erstellt und die Anzahl der OpenSearch Recheneinheiten (OCUs) in Ihrer Sammlung auf zwei reduziert. Wenn Sie in diesem Tutorial eine Produktionsumgebung erstellen möchten, lassen Sie das Kontrollkästchen aktiviert.
6. Wählen Sie unter Sicherheit die Option Einfach erstellen aus, um Ihre Sicherheitskonfiguration zu optimieren. Alle Daten in der Vector Engine werden bei der Übertragung und im Ruhezustand standardmäßig verschlüsselt. Die Vektor-Engine unterstützt detaillierte IAM-Berechtigungen, sodass Sie definieren können, wer Verschlüsselungen, Netzwerke, Sammlungen und Indizes erstellen, aktualisieren und löschen darf.
7. Wählen Sie Weiter aus.
8. Überprüfen Sie Ihre Sammlungseinstellungen und wählen Sie Submit (Senden) aus. Warten Sie einige Minuten, bis der Sammlungsstatus `Active` erreicht ist.

Schritt 3: Daten hochladen und suchen

Ein Index ist eine Sammlung von Dokumenten mit einem gemeinsamen Datenschema, das es Ihnen ermöglicht, Ihre Vektoreinbettungen und andere Felder zu speichern, zu suchen und abzurufen. Sie können Daten erstellen und in Indizes in einer OpenSearch serverlosen Sammlung hochladen, indem Sie die Dev Tools-Konsole in OpenSearch Dashboards oder ein HTTP-Tool wie Postman oder awscurl verwenden. In diesem Tutorial werden Dev Tools verwendet.

So indizieren und durchsuchen Sie Daten in der Filme-Sammlung

1. Um einen einzelnen Index für Ihre neue Sammlung zu erstellen, senden Sie die folgende Anfrage an die Dev Tools-Konsole. Standardmäßig wird dadurch ein Index mit einer `nmslib` Engine und einer euklidischen Distanz erstellt.

```
PUT housing-index
{
   "settings": {
      "index.knn": true
   },
   "mappings": {
      "properties": {
         "housing-vector": {
            "type": "knn_vector",
            "dimension": 3
         },
         "title": {
            "type": "text"
         },
         "price": {
            "type": "long"
         },
         "location": {
            "type": "geo_point"
         }
      }
   }
}
```

2. Um ein einzelnes Dokument in den Housing-Index zu indexieren, senden Sie die folgende Anfrage:

```
POST housing-index/_doc
```

```
{
  "housing-vector": [
    10,
    20,
    30
  ],
  "title": "2 bedroom in downtown Seattle",
  "price": "2800",
  "location": "47.71, 122.00"
}
```

3. Um nach Immobilien zu suchen, die denen in Ihrem Index ähnlich sind, senden Sie die folgende Abfrage:

```
GET housing-index/_search
{
    "size": 5,
    "query": {
        "knn": {
            "housing-vector": {
                "vector": [
                    10,
                    20,
                    30
                ],
                "k": 5
            }
        }
    }
}
```

Schritt 4: Sammlung löschen

Da die Wohnungssammlung zu Testzwecken dient, sollten Sie sie unbedingt löschen, wenn Sie mit dem Experimentieren fertig sind.

Um eine OpenSearch serverlose Sammlung zu löschen

1. Gehen Sie zurück zur Amazon OpenSearch Service-Konsole.
2. Wählen Sie im linken Navigationsbereich Sammlungen und dann die Eigenschaftensammlung aus.

3. Wählen Sie Löschen und bestätigen Sie den Löschvorgang.

Gefilterte Suche

Sie können Filter verwenden, um Ihre semantischen Suchergebnisse zu verfeinern. Um einen Index zu erstellen und eine gefilterte Suche in Ihren Dokumenten durchzuführen, ersetzen Sie die folgenden Anweisungen anstelle von Daten hochladen und suchen aus dem vorherigen Tutorial. Die anderen Schritte bleiben gleich. Weitere Informationen zu Filtern finden Sie unter k-NN-Suche mit Filtern.

So indizieren und durchsuchen Sie Daten in der Filme-Sammlung

1. Um einen einzelnen Index für Ihre Sammlung zu erstellen, senden Sie die folgende Anfrage in der Dev Tools-Konsole:

```
PUT housing-index-filtered
{
  "settings": {
    "index.knn": true
  },
  "mappings": {
    "properties": {
      "housing-vector": {
        "type": "knn_vector",
        "dimension": 3,
        "method": {
          "engine": "faiss",
          "name": "hnsw"
        }
      },
      "title": {
        "type": "text"
      },
      "price": {
        "type": "long"
      },
      "location": {
        "type": "geo_point"
      }
    }
  }
```

```
}
```

2. Um ein einzelnes Dokument zu indexieren housing-index-filtered, senden Sie die folgende Anfrage:

```
POST housing-index-filtered/_doc
{
  "housing-vector": [
    10,
    20,
    30
  ],
  "title": "2 bedroom in downtown Seattle",
  "price": "2800",
  "location": "47.71, 122.00"
}
```

3. Um nach Ihren Daten nach einer Wohnung in Seattle zu einem bestimmten Preis und in einer bestimmten Entfernung von einem geografischen Punkt zu suchen, senden Sie die folgende Anfrage:

```
GET housing-index-filtered/_search
{
  "size": 5,
  "query": {
    "knn": {
      "housing-vector": {
        "vector": [
          0.1,
          0.2,
          0.3
        ],
        "k": 5,
        "filter": {
          "bool": {
            "must": [
              {
                "query_string": {
                  "query": "Find me 2 bedroom apartment in Seattle under $3000 ",
                  "fields": [
                    "title"
                  ]
                }
```

```
              },
              {
                "range": {
                  "price": {
                    "lte": 3000
                  }
                }
              },
              {
                "geo_distance": {
                  "distance": "100miles",
                  "location": {
                    "lat": 48,
                    "lon": 121
                  }
                }
              }
            ]
          }
        }
      }
    }
  }
}
```

Workloads im Milliardenbereich

Vektorsuchsammlungen unterstützen Workloads mit Milliarden von Vektoren. Sie müssen zu Skalierungszwecken keine Neuindizierung durchführen, da Auto Scaling dies für Sie erledigt. Wenn Sie über Millionen von Vektoren (oder mehr) mit einer hohen Anzahl von Dimensionen verfügen und mehr als 200 OCUs benötigen, wenden Sie sich an den AWS Support, um die maximale Anzahl an OpenSearch Recheneinheiten (OCUs) für Ihr Konto zu erhöhen.

Einschränkungen

Für Sammlungen mit Vektorsuche gelten die folgenden Einschränkungen:

- Sammlungen für die Vektorsuche unterstützen die Apache Lucene ANN-Engine nicht.
- Sammlungen mit Vektorsuche unterstützen nur den HNSW-Algorithmus mit Faiss und nicht IVF und IVFQ.

- Sammlungen für die Vektorsuche unterstützen die API-Operationen Warmup, Statistik und Modelltraining nicht.
- Sammlungen für die Vektorsuche unterstützen keine Inline- oder gespeicherten Skripts.
- Informationen zur Indexanzahl sind in den Sammlungen AWS Management Console für die Vektorsuche nicht verfügbar.
- Das Aktualisierungsintervall für Indizes für Vektorsuchsammlungen beträgt 60 Sekunden.

Nächste Schritte

Da Sie nun wissen, wie Sie eine Vektorsuchsammlung erstellen und Daten indexieren, möchten Sie vielleicht einige der folgenden Übungen ausprobieren:

- Verwenden Sie den OpenSearch Python-Client, um mit Vektorsuchsammlungen zu arbeiten. Sehen Sie sich dieses Tutorial unter an GitHub.
- Verwenden Sie den OpenSearch Java-Client, um mit Vektorsuchsammlungen zu arbeiten. Sehen Sie sich dieses Tutorial unter an GitHub.
- Für LangChain die Verwendung OpenSearch als Vektorspeicher eingerichtet. LangChain ist ein Open-Source-Framework für die Entwicklung von Anwendungen, die auf Sprachmodellen basieren. Weitere Informationen finden Sie in der LangChain Dokumentation.

Verwenden von Datenlebenszyklusrichtlinien mit Amazon OpenSearch Serverless

Eine Datenlebenszyklus-Richtlinie für eine Amazon OpenSearch Serverless-Zeitreihenerfassung bestimmt die Lebensdauer der Daten in dieser Sammlung. OpenSearch Serverless speichert die Daten für den von Ihnen konfigurierten Zeitraum.

Sie können für jeden Index jeder Zeitreihensammlung in Ihrem AWS-Konto eine separate Datenlebenszyklusrichtlinie konfigurieren. OpenSearch Serverless bewahrt Dokumente mindestens für den Aufbewahrungszeitraum, den Sie in der Richtlinie konfiguriert haben, in Indizes auf. Anschließend werden sie automatisch nach bestem Wissen und Gewissen gelöscht, in der Regel innerhalb von 48 Stunden oder innerhalb von 10% der Aufbewahrungsfrist, je nachdem, welcher Zeitraum länger ist.

Nur Zeitreihenerfassungen unterstützen Richtlinien für den Datenlebenszyklus. Sie werden von Sammlungen mit Such - oder Vektorsuche nicht unterstützt.

Themen

Richtlinien für den Datenlebenszyklus

In einer Datenlebenszyklus-Richtlinie geben Sie eine Reihe von Regeln an. Mit der Datenlebenszyklus-Richtlinie können Sie die Aufbewahrungsdauer von Daten verwalten, die Indizes oder Sammlungen zugeordnet sind, die diesen Regeln entsprechen. Diese Regeln definieren den Aufbewahrungszeitraum für Daten in einem Index oder einer Gruppe von Indizes. Jede Regel besteht aus einem Ressourcentyp (`index`), einem Aufbewahrungszeitraum und einer Liste von Ressourcen (Indizes), für die der Aufbewahrungszeitraum gilt.

Sie definieren den Aufbewahrungszeitraum mit einem der folgenden Formate:

- `"MinIndexRetention": "24h"`— OpenSearch Serverless speichert Indexdaten für den angegebenen Zeitraum in Stunden oder Tagen. Sie können für diesen Zeitraum einen Zeitraum von `24h` bis `3650d` festlegen.
- `"NoMinIndexRetention": true`— OpenSearch Serverless speichert Indexdaten auf unbestimmte Zeit.

In der folgenden Beispielrichtlinie legt die erste Regel eine Aufbewahrungsfrist von 15 Tagen für alle Indizes innerhalb der Sammlung fest. `marketing` Die zweite Regel legt fest, dass für alle Indexnamen, die `log` in der `finance` Sammlung mit 1 beginnen, keine Aufbewahrungsfrist festgelegt ist und dass sie auf unbestimmte Zeit aufbewahrt werden.

```
{
   "lifeCyclePolicyDetail": {
      "type": "retention",
      "name": "my-policy",
```

```
      "policyVersion": "MTY4ODI0NTM2OTk1N18x",
      "policy": {
         "Rules": [
            {
            "ResourceType":"index",
            "Resource":[
               "index/marketing/*"
            ],
            "MinIndexRetention": "15d"
         },
         {
            "ResourceType":"index",
            "Resource":[
               "index/finance/log*"
            ],
            "NoMinIndexRetention": true
         }
         ]
      },
      "createdDate": 1688245369957,
      "lastModifiedDate": 1688245369957
   }
}
```

In der folgenden Beispiel-Richtlinienregel speichert OpenSearch Serverless die Daten in allen Indizes für alle Sammlungen innerhalb des Kontos auf unbestimmte Zeit.

```
{
   "Rules": [
      {
         "ResourceType": "index",
         "Resource": [
            "index/*/*"
         ]
      }
   ],
   "NoMinIndexRetention": true
}
```

Erforderliche Berechtigungen

Lifecycle-Richtlinien für OpenSearch Serverless verwenden die folgenden AWS Identity and Access Management (IAM-) Berechtigungen. Sie können IAM-Bedingungen angeben, um Benutzer auf

Datenlebenszyklus-Richtlinien zu beschränken, die bestimmten Sammlungen und Indizes zugeordnet sind.

- `aoss:CreateLifecyclePolicy`— Erstellen Sie eine Datenlebenszyklus-Richtlinie.
- `aoss:ListLifecyclePolicies`— Listet alle Datenlebenszyklus-Richtlinien im aktuellen Konto auf.
- `aoss:BatchGetLifecyclePolicy`— Zeigen Sie eine Datenlebenszyklus-Richtlinie an, die einem Konto- oder Richtliniennamen zugeordnet ist.
- `aoss:BatchGetEffectiveLifecyclePolicy`— Eine Datenlebenszyklus-Richtlinie für eine bestimmte Ressource anzeigen (`index`ist die einzige unterstützte Ressource).
- `aoss:UpdateLifecyclePolicy`— Ändern Sie eine bestimmte Datenlebenszyklus-Richtlinie und ändern Sie deren Aufbewahrungseinstellung oder Ressource.
- `aoss:DeleteLifecyclePolicy`— Löscht eine Datenlebenszyklus-Richtlinie.

Die folgende identitätsbasierte Zugriffsrichtlinie ermöglicht es einem Benutzer, alle Datenlebenszyklusrichtlinien einzusehen und Richtlinien anhand des Ressourcenmusters zu aktualisieren: `collection/application-logs`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "aoss:UpdateLifecyclePolicy"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aoss:collection": "application-logs"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "aoss:ListLifecyclePolicies",
                "aoss:BatchGetLifecyclePolicy"
            ],
```

```
            "Resource": "*"
        }
    ]
}
```

Vorrang der Richtlinie

Es kann Situationen geben, in denen sich die Richtlinienregeln für den Datenlebenszyklus innerhalb oder zwischen Richtlinien überschneiden. In diesem Fall überschreibt eine Regel mit einem spezifischeren Ressourcennamen oder einem spezifischeren Muster für einen Index eine Regel mit einem allgemeineren Ressourcennamen oder Muster für alle Indizes, die beiden Regeln gemeinsam sind.

In der folgenden Richtlinie gelten beispielsweise zwei Regeln für einen Index. `index/sales/logstash` In diesem Fall hat die zweite Regel Vorrang, da sie `index/sales/log*` am längsten entsprich`index/sales/logstash`. Daher legt OpenSearch Serverless keine Aufbewahrungsfrist für den Index fest.

```
{
      "Rules":[
         {
            "ResourceType":"index",
            "Resource":[
               "index/sales/*",
            ],
            "MinIndexRetention": "15d"
         },
         {
            "ResourceType":"index",
            "Resource":[
               "index/sales/log*",
            ],
            "NoMinIndexRetention": true
         }
      ]
   }
```

Richtliniensyntax

Geben Sie eine oder mehrere Regeln an. Diese Regeln definieren die Datenlebenszykluseinstellungen für Ihre OpenSearch Serverless-Indizes.

Jede Regel enthält die folgenden Elemente. Sie können `NoMinIndexRetention` in jeder Regel entweder `MinIndexRetention` oder angeben, aber nicht beides.

Element	Beschreibung
Ressourcentyp	Der Ressourcentyp, für den die Regel gilt. Die einzige unterstützte Option für Datenlebe nszyklus-Richtlinien ist`index`.
Resource	Eine Liste von Ressourcennamen und/ oder Mustern. Muster bestehen aus einem Präfix und einem Platzhalter (*), sodass die zugehörigen Berechtigungen auf mehrere Ressourcen angewendet werden können. Zum Beispiel `index/`*`<collection-name|p attern>`* `/`*`<index-name|pattern>`* .
MinIndexRetention	Der Mindestzeitraum, in Tagen (d) oder Stunden (h), für die Aufbewahrung des Dokuments im Index. Die Untergrenze ist `24h` und die Obergrenze ist`3650d`.
NoMinIndexRetention	Wenn`true`, OpenSearch Serverless speichert Dokumente auf unbestimmte Zeit.

Im Folgenden sind einige Beispiele aufgeführt:

```
{
  "Rules": [
    {
      "ResourceType": "index",
      "Resource": [
        "index/autoparts-inventory/*"
      ],
      "MinIndexRetention": "20d"
    },
    {
      "ResourceType": "index",
      "Resource": [
```

```
        "index/auto*/gear"
      ],
      "MinIndexRetention": "24h"
    },
    {
      "ResourceType": "index",
      "Resource": [
        "index/autoparts-inventory/tires"
      ],
      "NoMinIndexRetention": true
    }
  ]
}
```

Richtlinien für den Datenlebenszyklus erstellen () AWS CLI

Verwenden Sie den CreateLifecyclePolicyBefehl, um mithilfe der OpenSearch serverlosen API-Operationen eine Datenlebenszyklus-Richtlinie zu erstellen. Dieser Befehl akzeptiert sowohl Inline-Richtlinien als auch JSON-Dateien. Inline-Richtlinien müssen als JSON-Zeichenfolge mit Escape-Zeichen codiert werden.

Die folgende Anfrage erstellt eine Datenlebenszyklus-Richtlinie:

```
aws opensearchserverless create-lifecycle-policy \
    --name my-policy \
    --type retention \
    --policy "{\"Rules\":[{\"ResourceType\":\"index\",\"Resource\":[\"index/autoparts-inventory/*\"],\"MinIndexRetention\": \"81d\"},{\"ResourceType\":\"index\",\"Resource\":[\"index/sales/orders*\"],\"NoMinIndexRetention\":true}]}"
```

Verwenden Sie das Format `--policy file://my-policy.json` die Richtlinie in einer JSON-Datei bereitzustellen

Datenlebenszyklus-Richtlinien anzeigen

Bevor Sie eine Sammlung erstellen, sollten Sie sich eine Vorschau der vorhandenen Datenlebenszyklus-Richtlinien in Ihrem Konto ansehen, um zu sehen, welche über ein Ressourcenmuster verfügen, das dem Namen Ihrer Sammlung entspricht. In der folgenden ListLifecyclePoliciesAnfrage werden alle Datenlebenszyklus-Richtlinien in Ihrem Konto aufgeführt:

```
aws opensearchserverless list-lifecycle-policies --type retention
```

Die Anfrage gibt Informationen zu allen konfigurierten Datenlebenszyklus-Richtlinien zurück. Um die in der einen bestimmten Richtlinie definierten Musterregeln einzusehen, suchen Sie die Richtlinieninformationen im Inhalt des `lifecyclePolicySummaries` Elements in der Antwort. Notieren Sie sich das `name` Ende `type` dieser Richtlinie und verwenden Sie diese Eigenschaften in einer BatchGetLifecyclePolicyAnfrage, um eine Antwort mit den folgenden Richtliniendetails zu erhalten:

```
{
    "lifecyclePolicySummaries": [
        {
            "type": "retention",
            "name": "my-policy",
            "policyVersion": "MTY2MzY5MTY1MDA3Ml8x",
            "createdDate": 1663691650072,
            "lastModifiedDate": 1663691650072
        }
    ]
}
```

Um die Ergebnisse auf Richtlinien zu beschränken, die bestimmte Sammlungen oder Indizes enthalten, können Sie Ressourcenfilter einbeziehen:

```
aws opensearchserverless list-lifecycle-policies --type retention --resources
 "index/autoparts-inventory/*"
```

Verwenden Sie den BatchGetLifecyclePolicyBefehl, um detaillierte Informationen zu einer bestimmten Richtlinie anzuzeigen.

Aktualisierung der Richtlinien für den Datenlebenszyklus

Wenn Sie eine Datenlebenszyklus-Richtlinie ändern, wirkt sich dies auf alle zugehörigen Sammlungen aus. Um eine Datenlebenszyklus-Richtlinie in der OpenSearch Serverless-Konsole zu aktualisieren, erweitern Sie Datenlebenszyklus-Richtlinien, wählen Sie die zu ändernde Richtlinie aus und klicken Sie auf Bearbeiten. Nehmen Sie Ihre Änderungen vor und wählen Sie Save (Speichern).

Verwenden Sie den Befehl, um eine Datenlebenszyklus-Richtlinie mithilfe der OpenSearch Serverless API zu aktualisieren. UpdateLifecyclePolicy Sie müssen eine Richtlinienversion in die Anfrage aufnehmen. Sie können die Richtlinienversion mithilfe der `ListLifecyclePolicies`- oder `BatchGetLifecyclePolicy`-Befehle abrufen. Durch die Angabe der neuesten Richtlinienversion

wird sichergestellt, dass Sie nicht versehentlich eine von einem anderen Benutzer vorgenommene Änderung überschreiben.

Die folgende Anfrage aktualisiert eine Datenlebenszyklus-Richtlinie mit einem neuen JSON-Richtliniendokument:

```
aws opensearchserverless update-lifecycle-policy \
    --name my-policy \
    --type retention \
    --policy-version MTY2MzY5MTY1MDA3Ml8x \
    --policy file://my-new-policy.json
```

Zwischen der Aktualisierung der Richtlinie und der Durchsetzung der neuen Aufbewahrungsfristen kann es zu einer Verzögerung von einigen Minuten kommen.

Löschen von Datenlebenszyklus-Richtlinien

Wenn Sie eine Datenlebenszyklus-Richtlinie löschen, gilt sie nicht mehr für passende Indizes. Um eine Richtlinie in der OpenSearch Serverless-Konsole zu löschen, wählen Sie die Richtlinie aus und klicken Sie auf Löschen.

Sie können auch den DeleteLifecyclePolicyfolgenden Befehl verwenden:

```
aws opensearchserverless delete-lifecycle-policy --name my-policy --type retention
```

Verwendung der AWS SDKs zur Interaktion mit Amazon Serverless OpenSearch

Dieser Abschnitt enthält Beispiele für die Verwendung der AWS SDKs für die Interaktion mit Amazon OpenSearch Serverless. Diese Codebeispiele zeigen, wie Sicherheitsrichtlinien und Sammlungen erstellt und Sammlungen abgefragt werden.

> **Note**
>
> Wir sind gerade dabei, diese Codebeispiele zu erstellen. Wenn Sie ein Codebeispiel (Java, Go usw.) beisteuern möchten, öffnen Sie bitte eine Pull-Anfrage direkt im GitHubRepository.

Themen

- Python

- JavaScript

Python

Das folgende Beispielskript verwendet das AWS SDK for Python (Boto3) sowie den opensearch-py-Client für Python, um Verschlüsselungs-, Netzwerk- und Datenzugriffsrichtlinien zu erstellen, eine passende Sammlung zu erstellen und einige Beispieldaten zu indizieren.

Führen Sie die folgenden Befehle aus, um die erforderlichen Abhängigkeiten zu installieren:

```
pip install opensearch-py
pip install boto3
pip install botocore
pip install requests-aws4auth
```

Ersetzen Sie innerhalb des Skripts das `Principal`-Element durch den Amazon-Ressourcennamen (ARN) des Benutzers oder der Rolle, die die Anfrage signiert. Optional können Sie auch das `region` ändern.

```
from opensearchpy import OpenSearch, RequestsHttpConnection
from requests_aws4auth import AWS4Auth
import boto3
import botocore
import time

# Build the client using the default credential configuration.
# You can use the CLI and run 'aws configure' to set access key, secret
# key, and default region.

client = boto3.client('opensearchserverless')
service = 'aoss'
region = 'us-east-1'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key,
                   region, service, session_token=credentials.token)


def createEncryptionPolicy(client):
    """Creates an encryption policy that matches all collections beginning with tv-"""
    try:
        response = client.create_security_policy(
            description='Encryption policy for TV collections',
```

```
            name='tv-policy',
            policy="""
                {
                    \"Rules\":[
                        {
                            \"ResourceType\":\"collection\",
                            \"Resource\":[
                                \"collection\/tv-*\"
                            ]
                        }
                    ],
                    \"AWSOwnedKey\":true
                }
                """,
            type='encryption'
        )
        print('\nEncryption policy created:')
        print(response)
    except botocore.exceptions.ClientError as error:
        if error.response['Error']['Code'] == 'ConflictException':
            print(
                '[ConflictException] The policy name or rules conflict with an existing
 policy.')
        else:
            raise error


def createNetworkPolicy(client):
    """Creates a network policy that matches all collections beginning with tv-"""
    try:
        response = client.create_security_policy(
            description='Network policy for TV collections',
            name='tv-policy',
            policy="""
                [{
                    \"Description\":\"Public access for TV collection\",
                    \"Rules\":[
                        {
                            \"ResourceType\":\"dashboard\",
                            \"Resource\":[\"collection\/tv-*\"]
                        },
                        {
                            \"ResourceType\":\"collection\",
                            \"Resource\":[\"collection\/tv-*\"]
```

```
                        }
                    ],
                    \"AllowFromPublic\":true
                }]
                """,
            type='network'
        )
        print('\nNetwork policy created:')
        print(response)
    except botocore.exceptions.ClientError as error:
        if error.response['Error']['Code'] == 'ConflictException':
            print(
                '[ConflictException] A network policy with this name already exists.')
        else:
            raise error


def createAccessPolicy(client):
    """Creates a data access policy that matches all collections beginning with tv-"""
    try:
        response = client.create_access_policy(
            description='Data access policy for TV collections',
            name='tv-policy',
            policy="""
                [{
                    \"Rules\":[
                        {
                            \"Resource\":[
                                \"index\/tv-*\/*\"
                            ],
                            \"Permission\":[
                                \"aoss:CreateIndex\",
                                \"aoss:DeleteIndex\",
                                \"aoss:UpdateIndex\",
                                \"aoss:DescribeIndex\",
                                \"aoss:ReadDocument\",
                                \"aoss:WriteDocument\"
                            ],
                            \"ResourceType\": \"index\"
                        },
                        {
                            \"Resource\":[
                                \"collection\/tv-*\"
                            ],
```

```
                            \"Permission\":[
                                \"aoss:CreateCollectionItems\"
                            ],
                            \"ResourceType\": \"collection\"
                        }
                    ],
                    \"Principal\":[
                        \"arn:aws:iam::123456789012:role\/Admin\"
                    ]
                }]
                """,
            type='data'
        )
        print('\nAccess policy created:')
        print(response)
    except botocore.exceptions.ClientError as error:
        if error.response['Error']['Code'] == 'ConflictException':
            print(
                '[ConflictException] An access policy with this name already exists.')
        else:
            raise error


def createCollection(client):
    """Creates a collection"""
    try:
        response = client.create_collection(
            name='tv-sitcoms',
            type='SEARCH'
        )
        return(response)
    except botocore.exceptions.ClientError as error:
        if error.response['Error']['Code'] == 'ConflictException':
            print(
                '[ConflictException] A collection with this name already exists. Try
 another name.')
        else:
            raise error


def waitForCollectionCreation(client):
    """Waits for the collection to become active"""
    response = client.batch_get_collection(
        names=['tv-sitcoms'])
```

```
    # Periodically check collection status
    while (response['collectionDetails'][0]['status']) == 'CREATING':
        print('Creating collection...')
        time.sleep(30)
        response = client.batch_get_collection(
            names=['tv-sitcoms'])
    print('\nCollection successfully created:')
    print(response["collectionDetails"])
    # Extract the collection endpoint from the response
    host = (response['collectionDetails'][0]['collectionEndpoint'])
    final_host = host.replace("https://", "")
    indexData(final_host)


def indexData(host):
    """Create an index and add some sample data"""
    # Build the OpenSearch client
    client = OpenSearch(
        hosts=[{'host': host, 'port': 443}],
        http_auth=awsauth,
        use_ssl=True,
        verify_certs=True,
        connection_class=RequestsHttpConnection,
        timeout=300
    )
    # It can take up to a minute for data access rules to be enforced
    time.sleep(45)

    # Create index
    response = client.indices.create('sitcoms-eighties')
    print('\nCreating index:')
    print(response)

    # Add a document to the index.
    response = client.index(
        index='sitcoms-eighties',
        body={
            'title': 'Seinfeld',
            'creator': 'Larry David',
            'year': 1989
        },
        id='1',
    )
    print('\nDocument added:')
```

```
    print(response)


def main():
    createEncryptionPolicy(client)
    createNetworkPolicy(client)
    createAccessPolicy(client)
    createCollection(client)
    waitForCollectionCreation(client)


if __name__ == "__main__":
    main()
```

JavaScript

Das folgende Beispielskript verwendet das SDK für JavaScript in Node.js sowie den opensearch-js-Client fürJavaScript, um Verschlüsselungs-, Netzwerk- und Datenzugriffsrichtlinien zu erstellen, eine passende Sammlung zu erstellen, einen Index zu erstellen und einige Beispieldaten zu indexieren.

Führen Sie die folgenden Befehle aus, um die erforderlichen Abhängigkeiten zu installieren:

```
npm i aws-sdk
npm i aws4
npm i @opensearch-project/opensearch
```

Ersetzen Sie innerhalb des Skripts das `Principal`-Element durch den Amazon-Ressourcennamen (ARN) des Benutzers oder der Rolle, die die Anfrage signiert. Optional können Sie auch das `region` ändern.

```
var AWS = require('aws-sdk');
var aws4 = require('aws4');
var {
    Client,
    Connection
} = require("@opensearch-project/opensearch");
var {
    OpenSearchServerlessClient,
    CreateSecurityPolicyCommand,
    CreateAccessPolicyCommand,
    CreateCollectionCommand,
    BatchGetCollectionCommand
```

```
} = require("@aws-sdk/client-opensearchserverless");
var client = new OpenSearchServerlessClient();

async function execute() {
    await createEncryptionPolicy(client)
    await createNetworkPolicy(client)
    await createAccessPolicy(client)
    await createCollection(client)
    await waitForCollectionCreation(client)
}

async function createEncryptionPolicy(client) {
    // Creates an encryption policy that matches all collections beginning with 'tv-'
    try {
        var command = new CreateSecurityPolicyCommand({
            description: 'Encryption policy for TV collections',
            name: 'tv-policy',
            type: 'encryption',
            policy: " \
        { \
            \"Rules\":[ \
                { \
                    \"ResourceType\":\"collection\", \
                    \"Resource\":[ \
                        \"collection\/tv-*\" \
                    ] \
                } \
            ], \
            \"AWSOwnedKey\":true \
        }"
        });
        const response = await client.send(command);
        console.log("Encryption policy created:");
        console.log(response['securityPolicyDetail']);
    } catch (error) {
        if (error.name === 'ConflictException') {
            console.log('[ConflictException] The policy name or rules conflict with an
 existing policy.');
        } else
            console.error(error);
    };
}

async function createNetworkPolicy(client) {
```

```
    // Creates a network policy that matches all collections beginning with 'tv-'
    try {
        var command = new CreateSecurityPolicyCommand({
            description: 'Network policy for TV collections',
            name: 'tv-policy',
            type: 'network',
            policy: " \
            [{ \
                \"Description\":\"Public access for television collection\", \
                \"Rules\":[ \
                    { \
                        \"ResourceType\":\"dashboard\", \
                        \"Resource\":[\"collection\/tv-*\"] \
                    }, \
                    { \
                        \"ResourceType\":\"collection\", \
                        \"Resource\":[\"collection\/tv-*\"] \
                    } \
                ], \
                \"AllowFromPublic\":true \
            }]"
        });
        const response = await client.send(command);
        console.log("Network policy created:");
        console.log(response['securityPolicyDetail']);
    } catch (error) {
        if (error.name === 'ConflictException') {
            console.log('[ConflictException] A network policy with that name already
 exists.');
        } else
            console.error(error);
    };
}

async function createAccessPolicy(client) {
    // Creates a data access policy that matches all collections beginning with 'tv-'
    try {
        var command = new CreateAccessPolicyCommand({
            description: 'Data access policy for TV collections',
            name: 'tv-policy',
            type: 'data',
            policy: " \
            [{ \
                \"Rules\":[ \
```

```
                    { \
                        \"Resource\":[ \
                            \"index\/tv-*\/*\" \
                        ], \
                        \"Permission\":[ \
                            \"aoss:CreateIndex\", \
                            \"aoss:DeleteIndex\", \
                            \"aoss:UpdateIndex\", \
                            \"aoss:DescribeIndex\", \
                            \"aoss:ReadDocument\", \
                            \"aoss:WriteDocument\" \
                        ], \
                        \"ResourceType\": \"index\" \
                    }, \
                    { \
                        \"Resource\":[ \
                            \"collection\/tv-*\" \
                        ], \
                        \"Permission\":[ \
                            \"aoss:CreateCollectionItems\" \
                        ], \
                        \"ResourceType\": \"collection\" \
                    } \
                ], \
                \"Principal\":[ \
                    \"arn:aws:iam::123456789012:role\/Admin\" \
                ] \
            }]"
        });
        const response = await client.send(command);
        console.log("Access policy created:");
        console.log(response['accessPolicyDetail']);
    } catch (error) {
        if (error.name === 'ConflictException') {
            console.log('[ConflictException] An access policy with that name already
 exists.');
        } else
            console.error(error);
    };
}

async function createCollection(client) {
    // Creates a collection to hold TV sitcoms indexes
    try {
```

```
        var command = new CreateCollectionCommand({
            name: 'tv-sitcoms',
            type: 'SEARCH'
        });
        const response = await client.send(command);
        return (response)
    } catch (error) {
        if (error.name === 'ConflictException') {
            console.log('[ConflictException] A collection with this name already
 exists. Try another name.');
        } else
            console.error(error);
    };
}

async function waitForCollectionCreation(client) {
    // Waits for the collection to become active
    try {
        var command = new BatchGetCollectionCommand({
            names: ['tv-sitcoms']
        });
        var response = await client.send(command);
        while (response.collectionDetails[0]['status'] == 'CREATING') {
            console.log('Creating collection...')
            await sleep(30000) // Wait for 30 seconds, then check the status again
            function sleep(ms) {
                return new Promise((resolve) => {
                    setTimeout(resolve, ms);
                });
            }
            var response = await client.send(command);
        }
        console.log('Collection successfully created:');
        console.log(response['collectionDetails']);
        // Extract the collection endpoint from the response
        var host = (response.collectionDetails[0]['collectionEndpoint'])
        // Pass collection endpoint to index document request
        indexDocument(host)
    } catch (error) {
        console.error(error);
    };
}

async function indexDocument(host) {
```

```
    var client = new Client({
        node: host,
        Connection: class extends Connection {
            buildRequestObject(params) {
                var request = super.buildRequestObject(params)
                request.service = 'aoss';
                request.region = 'us-east-1'; // e.g. us-east-1
                var body = request.body;
                request.body = undefined;
                delete request.headers['content-length'];
                request.headers['x-amz-content-sha256'] = 'UNSIGNED-PAYLOAD';
                request = aws4.sign(request, AWS.config.credentials);
                request.body = body;

                return request
            }
        }
    });

    // Create an index
    try {
        var index_name = "sitcoms-eighties";

        var response = await client.indices.create({
            index: index_name
        });

        console.log("Creating index:");
        console.log(response.body);

        // Add a document to the index
        var document = "{ \"title\": \"Seinfeld\", \"creator\": \"Larry David\", \"year
\": \"1989\" }\n";

        var response = await client.index({
            index: index_name,
            body: document
        });

        console.log("Adding document:");
        console.log(response.body);
    } catch (error) {
        console.error(error);
```

```
    };
}

execute()
```

AWS CloudFormationZum Erstellen von Amazon OpenSearch Serverless-Sammlungen verwenden

Sie können AWS CloudFormation damit Amazon OpenSearch Serverless Ressourcen wie Sammlungen, Sicherheitsrichtlinien und VPC-Endpunkte erstellen. Eine umfassende OpenSearch CloudFormation Serverless-Referenz finden Sie unter Amazon OpenSearch Serverless im AWS CloudFormationBenutzerhandbuch.

Die folgende CloudFormation Beispielvorlage erstellt eine einfache Datenzugriffsrichtlinie, Netzwerkrichtlinie und Sicherheitsrichtlinie sowie eine entsprechende Sammlung. Dies ist eine gute Möglichkeit, Amazon OpenSearch Serverless schnell zum Laufen zu bringen und die notwendigen Elemente bereitzustellen, um eine Sammlung zu erstellen und zu verwenden.

> **Important**
>
> In diesem Beispiel wird der öffentliche Netzwerkzugriff verwendet, was für Produktionsworkloads nicht empfohlen wird. Wir empfehlen die Verwendung des VPC-Zugriffs, um Ihre Sammlungen zu schützen. Weitere Informationen finden Sie unter AWS::OpenSearchServerless::VpcEndpoint und the section called “VPC-Endpunkte”.

```
AWSTemplateFormatVersion: 2010-09-09
Description: 'Amazon OpenSearch Serverless template to create an IAM user, encryption
 policy, data access policy and collection'
Resources:
  IAMUSer:
    Type: 'AWS::IAM::User'
    Properties:
      UserName:  aossadmin
  DataAccessPolicy:
    Type: 'AWS::OpenSearchServerless::AccessPolicy'
    Properties:
      Name: quickstart-access-policy
      Type: data
      Description: Access policy for quickstart collection
```

```
      Policy: !Sub >-
        [{"Description":"Access for cfn user","Rules":
[{"ResourceType":"index","Resource":["index/*/*"],"Permission":["aoss:*"]},
        {"ResourceType":"collection","Resource":["collection/quickstart"],"Permission":
["aoss:*"]}],
        "Principal":["arn:aws:iam::${AWS::AccountId}:user/aossadmin"]}]
  NetworkPolicy:
    Type: 'AWS::OpenSearchServerless::SecurityPolicy'
    Properties:
      Name: quickstart-network-policy
      Type: network
      Description: Network policy for quickstart collection
      Policy: >-
        [{"Rules":[{"ResourceType":"collection","Resource":["collection/
quickstart"]}, {"ResourceType":"dashboard","Resource":["collection/
quickstart"]}],"AllowFromPublic":true}]
  EncryptionPolicy:
    Type: 'AWS::OpenSearchServerless::SecurityPolicy'
    Properties:
      Name: quickstart-security-policy
      Type: encryption
      Description: Encryption policy for quickstart collection
      Policy: >-
        {"Rules":[{"ResourceType":"collection","Resource":["collection/
quickstart"]}],"AWSOwnedKey":true}
  Collection:
    Type: 'AWS::OpenSearchServerless::Collection'
    Properties:
      Name: quickstart
      Type: TIMESERIES
      Description: Collection to holds timeseries data
    DependsOn: EncryptionPolicy
Outputs:
  IAMUser:
    Value: !Ref IAMUSer
  DashboardURL:
    Value: !GetAtt Collection.DashboardEndpoint
  CollectionARN:
    Value: !GetAtt Collection.Arn
```

Verwaltung von Kapazitätsgrenzen für Amazon OpenSearch Serverless

Mit Amazon OpenSearch Serverless müssen Sie die Kapazität nicht selbst verwalten. OpenSearch Serverless skaliert die Rechenkapazität für Ihr Konto automatisch auf der Grundlage der aktuellen Arbeitslast. Serverlose Rechenkapazität wird in OpenSearch Recheneinheiten (OCUs) gemessen. Jede OCU ist eine Kombination aus 6 GB Speicher und entsprechender virtueller CPU (vCPU) und erstellt eine Daten-Pipeline zu Amazon S3. Weitere Informationen zur entkoppelten Architektur in OpenSearch Serverless finden Sie unter. the section called “Funktionsweise”

Wenn Sie Ihre erste Sammlung erstellen, instanziiert OpenSearch Serverless insgesamt vier OCUs (zwei für die Indizierung und zwei für die Suche). Diese OCUs sind immer vorhanden, auch wenn keine Indizierungs- oder Suchaktivitäten stattfinden. Alle nachfolgenden Sammlungen können diese OCUs gemeinsam nutzen (mit Ausnahme von Sammlungen mit eindeutigen AWS KMS Schlüsseln, die ihren eigenen Satz von vier OCUs instanziieren). Bei Bedarf skaliert OpenSearch Serverless automatisch und fügt zusätzliche OCUs hinzu, wenn Ihre Indexierungs- und Suchnutzung zunimmt. Wenn der Datenverkehr auf Ihrem Sammlungsendpunkt abnimmt, wird die Kapazität wieder auf die für Ihre Datengröße erforderliche OCU-Mindestanzahl reduziert. Es wird höchstens auf 1 OCU [0,5 OCU x 2] für die Indizierung und 1 OCU [0,5 OCU x 2] für die Suche herunterskaliert.

Bei Such - und Vektorsuchsammlungen werden alle Daten in Hot-Indizes gespeichert, um schnelle Antwortzeiten bei Abfragen zu gewährleisten. Zeitreihenerfassungen verwenden eine Kombination aus heißem und warmem Speicher, wobei die neuesten Daten im Hot-Storage aufbewahrt werden, um die Antwortzeiten bei Abfragen für Daten, auf die häufiger zugegriffen wird, zu optimieren. Weitere Informationen finden Sie unter the section called “Auswahl eines Sammlungstyps”.

> **Note**
>
> Eine Vektorsuchsammlung kann keine gemeinsamen OCUs mit Such - und Zeitreihensammlungen verwenden, selbst wenn die Vektorsuchsammlung denselben KMS-Schlüssel wie die Such - oder Zeitreihensammlungen verwendet. Für Ihre erste Vektorsammlung wird ein neuer Satz von OCUs erstellt. Die OCUs von Vektorsammlungen werden von denselben KMS-Schlüsselsammlungen gemeinsam genutzt.

Um die Kapazität Ihrer Sammlungen zu verwalten und die Kosten zu kontrollieren, können Sie die maximale Indexierungs- und Suchkapazität für das Girokonto und die Region insgesamt angeben.

OpenSearch Serverless skaliert Ihre Sammlungsressourcen automatisch auf der Grundlage dieser Spezifikationen.

Da die Indizierungs- und Suchkapazität separat skaliert werden, geben Sie für beide Limits auf Kontoebene an:

- Maximale Indexkapazität — OpenSearch Serverless kann die Indexkapazität auf bis zu dieser Anzahl von OCUs erhöhen.
- Maximale Suchkapazität — OpenSearch Serverless kann die Suchkapazität auf bis zu diese Anzahl von OCUs erhöhen.

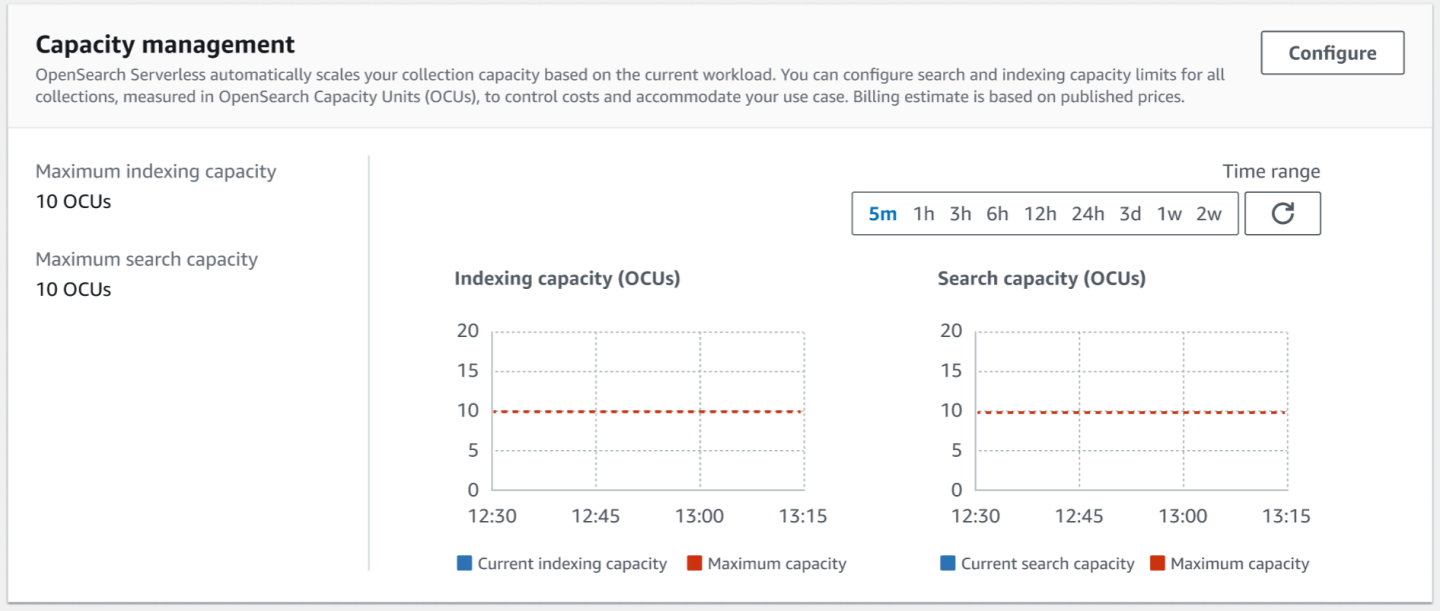
> **Note**
>
> Derzeit gelten Kapazitätseinstellungen nur auf Kontoebene. Sie können keine Kapazitätsgrenzen pro Sammlung konfigurieren.

Ihr Ziel sollte es sein, sicherzustellen, dass die maximale Kapazität hoch genug ist, um Spitzen im Workload zu bewältigen. Basierend auf Ihren Einstellungen skaliert OpenSearch Serverless automatisch die Anzahl der OCUs für Ihre Sammlungen, um den Indexierungs- und Suchaufwand zu verarbeiten.

Themen

Konfigurieren von Kapazitätseinstellungen

Um die Kapazitätseinstellungen in der OpenSearch Serverless-Konsole zu konfigurieren, erweitern Sie Serverless im linken Navigationsbereich und wählen Sie Dashboard aus. Geben Sie unter Capacity management (Kapazitätsverwaltung) die maximale Indizierungs- und Suchkapazität an:



Um die Kapazität mit dem zu konfigurieren AWS CLI, senden Sie eine UpdateAccountSettingsAnfrage:

```
aws opensearchserverless update-account-settings \
    --capacity-limits '{ "maxIndexingCapacityInOCU": 8,"maxSearchCapacityInOCU": 9 }'
```

Maximale Kapazitätsgrenzen

Für alle drei Arten von Sammlungen beträgt die maximale Standardkapazität 10 OCUs für die Indizierung und 10 OCUs für die Suche. Die zulässige Mindestkapazität für ein Konto beträgt 1 OCU [0,5 OCU x 2] für die Indexierung und 1 OCU [0,5 OCU x 2] für die Suche. Für alle Sammlungen beträgt die maximal zulässige Kapazität 200 OCUs für die Indexierung und 200 OCUs für die Suche. Sie können die OCU-Anzahl so konfigurieren, dass sie eine beliebige Zahl von 1 bis zur maximal zulässigen Kapazität ist, und zwar in Vielfachen von 2.

Jede OCU verfügt über ausreichend kurzlebigen Hot-Speicher für 120 GiB Indexdaten. OpenSearch Serverless unterstützt bis zu 1 TiB an Daten pro Index in Such - und Vektorsuchsammlungen und 10 TiB an heißen Daten pro Index in einer Zeitreihensammlung. Bei Zeitreihen-Sammlungen können Sie immer noch mehr Daten aufnehmen, die dann als warme Daten in S3 gespeichert werden können.

Eine Liste aller Kontingente finden Sie unter OpenSearch Serverlose Kontingente.

Überwachung der Kapazitätsnutzung

Sie können die Metriken `Search0CU` und die CloudWatch Kennzahlen `Indexing0CU` auf Kontoebene überwachen, um zu verstehen, wie Ihre Sammlungen skalieren. Wir empfehlen Ihnen, Warnungen zu konfigurieren, um sich benachrichtigen zu lassen wenn sich Ihr Konto einem Schwellenwert für kapazitätsbezogene Metriken nähert. So können Sie Ihre Kapazitätseinstellungen entsprechend anpassen.

Sie können diese Metriken auch verwenden, um festzustellen, ob Ihre Einstellungen für die maximale Kapazität angemessen sind oder ob Sie diese anpassen müssen. Analysieren Sie diese Metriken, um Ihre Bemühungen auf die Optimierung der Effizienz Ihrer Sammlungen zu konzentrieren. Weitere Informationen zu den Metriken, an die OpenSearch Serverless sendet, finden Sie CloudWatch unter. the section called “Überwachen von OpenSearch Serverless”

Daten in Amazon OpenSearch Serverless-Sammlungen aufnehmen

Diese Abschnitte enthalten Einzelheiten zu den unterstützten Ingest-Pipelines für die Datenaufnahme in Amazon Serverless Collections. OpenSearch Sie behandeln auch einige der Clients, mit denen Sie mit den API-Vorgängen interagieren können. OpenSearch Ihre Clients sollten mit OpenSearch 2.x kompatibel sein, um sie in OpenSearch Serverless integrieren zu können.

Themen

- Signieren von HTTP-Anforderungen mit anderen Clients

Erforderliche Mindestberechtigungen

Um Daten in eine OpenSearch serverlose Sammlung aufzunehmen, muss dem Principal, der die Daten schreibt, in einer Datenzugriffsrichtlinie die folgenden Mindestberechtigungen zugewiesen werden:

```
[
   {
      "Rules":[
         {
            "ResourceType":"index",
            "Resource":[
               "index/target-collection/logs"
            ],
            "Permission":[
               "aoss:CreateIndex",
               "aoss:WriteDocument",
               "aoss:UpdateIndex"
            ]
         }
      ],
      "Principal":[
         "arn:aws:iam::123456789012:user/my-user"
      ]
   }
]
```

Die Berechtigungen können umfassender sein, wenn Sie in zusätzliche Indizes schreiben möchten. Anstatt beispielsweise einen einzelnen Zielindex anzugeben, können Sie die Berechtigung für alle Indizes (index/*target-collection*/*) oder eine Teilmenge von Indizes (index/*target-collection*/*logs**) erteilen.

Eine Referenz aller verfügbaren OpenSearch API-Operationen und der zugehörigen Berechtigungen finden Sie unter. the section called “Unterstützte Vorgänge und Plugins”

OpenSearch Einnahme

Anstatt einen Drittanbieter-Client zu verwenden, um Daten direkt an eine OpenSearch serverlose Sammlung zu senden, können Sie Amazon OpenSearch Ingestion verwenden. Sie konfigurieren

Ihre Datenproduzenten so, dass sie Daten an OpenSearch Ingestion senden, und Ingestion übermittelt die Daten automatisch an die von Ihnen angegebene Sammlung. Sie können OpenSearch Ingestion auch so konfigurieren, dass Ihre Daten vor der Bereitstellung transformiert werden. Weitere Informationen finden Sie unter OpenSearch Einnahme durch Amazon.

Eine OpenSearch Ingestion-Pipeline benötigt die Berechtigung, in eine OpenSearch serverlose Sammlung zu schreiben, die als Senke konfiguriert ist. Zu diesen Berechtigungen gehört die Möglichkeit, die Sammlung zu beschreiben und HTTP-Anfragen an sie zu senden. Anweisungen zur Verwendung von OpenSearch Ingestion zum Hinzufügen von Daten zu einer Sammlung finden Sie unter. the section called “Pipelines Zugriff auf Sammlungen gewähren”

Informationen zu den ersten Schritten mit OpenSearch Ingestion finden Sie unter. the section called “Tutorial: Daten in eine Sammlung aufnehmen”

Fluent Bit

Sie können das Bild AWS für Fluent Bit und das OpenSearch Ausgabe-Plugin verwenden, um Daten in serverlose Sammlungen aufzunehmen. OpenSearch

> **Note**
>
> Sie benötigen Version 2.30.0 oder höher des AWS for Fluent Bit-Images, um die Integration mit Serverless durchführen zu können. OpenSearch

Beispielkonfiguration:

Dieser Beispielausgabeabschnitt der Konfigurationsdatei zeigt, wie eine OpenSearch serverlose Sammlung als Ziel verwendet wird. Die wichtige Ergänzung ist der `AWS_Service_Name`-Parameter, der `aoss` ist. `Host` ist der Sammlungsendpunkt.

```
[OUTPUT]
    Name  opensearch
    Match *
    Host  collection-endpoint.us-west-2.aoss.amazonaws.com
    Port  443
    Index  my_index
    Trace_Error On
    Trace_Output On
    AWS_Auth On
    AWS_Region <region>
```

```
    AWS_Service_Name aoss
    tls     On
    Suppress_Type_Name On
```

Amazon Data Firehose

Firehose unterstützt OpenSearch Serverless als Lieferziel. Anweisungen zum Senden von Daten an OpenSearch Serverless finden Sie unter Creating a Kinesis Data Firehose Delivery Stream and Choose OpenSearch Serverless for Your Destination im Amazon Data Firehose Developer Guide.

Die IAM-Rolle, die Sie Firehose für die Lieferung zur Verfügung stellen, muss in einer Datenzugriffsrichtlinie mit der `aoss:WriteDocument` Mindestberechtigung für die Zielsammlung angegeben werden, und Sie müssen über einen bereits vorhandenen Index verfügen, an den Daten gesendet werden können. Weitere Informationen finden Sie unter the section called “Erforderliche Mindestberechtigungen”.

Bevor Sie Daten an OpenSearch Serverless senden, müssen Sie möglicherweise Transformationen an den Daten durchführen. Weitere Informationen über die Verwendung von Lambda-Funktionen zur Ausführung dieser Aufgabe finden Sie unter Amazon Kinesis Data Firehose Datentransformation im selben Handbuch.

Fluentd

Sie können das OpenSearch Fluentd-Plugin verwenden, um Daten von Ihrer Infrastruktur, Ihren Containern und Netzwerkgeräten zu sammeln und sie an serverlose Sammlungen zu senden. OpenSearch Calyptia wartet eine Distribution von Fluentd, die alle nachgelagerten Abhängigkeiten von Ruby und SSL enthält.

Um Fluentd zum Senden von Daten an Serverless zu verwenden OpenSearch

1. Laden Sie Version 1.4.2 oder höher von Calyptia Fluentd unter https://www.fluentd.org/download herunter. Diese Version enthält standardmäßig das OpenSearch Plugin, das Serverless unterstützt. OpenSearch
2. Installieren Sie das Paket . Befolgen Sie die Anweisungen in der Fluentd-Dokumentation basierend auf Ihrem Betriebssystem:

   - Red Hat Enterprise Linux / CentOS / Amazon Linux
   - Debian / Ubuntu
   - Windows

- MacOSX

3. Fügen Sie eine Konfiguration hinzu, die Daten an OpenSearch Serverless sendet. Diese Beispielkonfiguration sendet die Meldung „test“ an eine einzelne Sammlung. Stellen Sie Folgendes sicher:

   - Geben Sie für `host` den Endpunkt Ihrer OpenSearch serverlosen Sammlung an.
   - Legen Sie für `aws_service_name` die Option `aoss` fest.

```
<source>
@type sample
tag test
test {"hello":"world"}
</source>

<match test>
@type opensearch
host https://collection-endpoint.us-east-1.aoss.amazonaws.com
port 443
index_name fluentd
aws_service_name aoss
</match>
```

4. Führen Sie Calyptia Fluentd aus, um mit dem Senden von Daten an die Sammlung zu beginnen. Auf einem Mac können Sie beispielsweise den folgenden Befehl ausführen:

```
sudo launchctl load /Library/LaunchDaemons/calyptia-fluentd.plist
```

Go

Der folgende Beispielcode verwendet den opensearch-go-Client für Go, um eine sichere Verbindung zur angegebenen OpenSearch Serverless-Sammlung herzustellen und einen einzelnen Index zu erstellen. Sie müssen Werte für `region` und `host` angeben.

```
package main

import (
  "context"
```

```
  "log"
  "strings"
  "github.com/aws/aws-sdk-go-v2/aws"
  "github.com/aws/aws-sdk-go-v2/config"
  opensearch "github.com/opensearch-project/opensearch-go/v2"
  opensearchapi "github.com/opensearch-project/opensearch-go/v2/opensearchapi"
  requestsigner "github.com/opensearch-project/opensearch-go/v2/signer/awsv2"
)

const endpoint = "" // serverless collection endpoint

func main() {
 ctx := context.Background()

 awsCfg, err := config.LoadDefaultConfig(ctx,
  config.WithRegion("<AWS_REGION>"),
  config.WithCredentialsProvider(
   getCredentialProvider("<AWS_ACCESS_KEY>", "<AWS_SECRET_ACCESS_KEY>",
 "<AWS_SESSION_TOKEN>"),
  ),
 )
 if err != nil {
  log.Fatal(err) // don't log.fatal in a production-ready app
 }

 // create an AWS request Signer and load AWS configuration using default config folder
 or env vars.
 signer, err := requestsigner.NewSignerWithService(awsCfg, "aoss") // "aoss" for Amazon
 OpenSearch Serverless
 if err != nil {
  log.Fatal(err) // don't log.fatal in a production-ready app
 }

 // create an opensearch client and use the request-signer
 client, err := opensearch.NewClient(opensearch.Config{
  Addresses: []string{endpoint},
  Signer:    signer,
 })
 if err != nil {
  log.Fatal("client creation err", err)
 }

 indexName := "go-test-index"
```

```
  // define index mapping
 mapping := strings.NewReader(`{
  "settings": {
    "index": {
         "number_of_shards": 4
         }
       }
  }`)

 // create an index
 createIndex := opensearchapi.IndicesCreateRequest{
  Index: indexName,
    Body: mapping,
 }
 createIndexResponse, err := createIndex.Do(context.Background(), client)
 if err != nil {
  log.Println("Error ", err.Error())
  log.Println("failed to create index ", err)
  log.Fatal("create response body read err", err)
 }
 log.Println(createIndexResponse)

 // delete the index
 deleteIndex := opensearchapi.IndicesDeleteRequest{
  Index: []string{indexName},
 }

 deleteIndexResponse, err := deleteIndex.Do(context.Background(), client)
 if err != nil {
  log.Println("failed to delete index ", err)
  log.Fatal("delete index response body read err", err)
 }
 log.Println("deleting index", deleteIndexResponse)
}

func getCredentialProvider(accessKey, secretAccessKey, token string)
 aws.CredentialsProviderFunc {
 return func(ctx context.Context) (aws.Credentials, error) {
  c := &aws.Credentials{
   AccessKeyID:     accessKey,
   SecretAccessKey: secretAccessKey,
   SessionToken:    token,
  }
  return *c, nil
```

```
 }
}
```

Java

Der folgende Beispielcode verwendet den opensearch-java-Client für Java, um eine sichere Verbindung zur angegebenen OpenSearch Serverless-Sammlung herzustellen und einen einzelnen Index zu erstellen. Sie müssen Werte für `region` und `host` angeben.

Der wichtige Unterschied zu OpenSearch Service-Domains ist der Dienstname (`aoss`anstelle von). `es`

```
// import OpenSearchClient to establish connection to OpenSearch Serverless collection
import org.opensearch.client.opensearch.OpenSearchClient;

SdkHttpClient httpClient = ApacheHttpClient.builder().build();
// create an opensearch client and use the request-signer
OpenSearchClient client = new OpenSearchClient(
    new AwsSdk2Transport(
        httpClient,
        "...us-west-2.aoss.amazonaws.com", // serverless collection endpoint
        "aoss" // signing service name
        Region.US_WEST_2, // signing service region
        AwsSdk2TransportOptions.builder().build()
    )
);

String index = "sample-index";

// create an index
CreateIndexRequest createIndexRequest = new
 CreateIndexRequest.Builder().index(index).build();
CreateIndexResponse createIndexResponse = client.indices().create(createIndexRequest);
System.out.println("Create index reponse: " + createIndexResponse);

// delete the index
DeleteIndexRequest deleteIndexRequest = new
 DeleteIndexRequest.Builder().index(index).build();
DeleteIndexResponse deleteIndexResponse = client.indices().delete(deleteIndexRequest);
System.out.println("Delete index reponse: " + deleteIndexResponse);

httpClient.close();
```

Der folgende Beispielcode stellt erneut eine sichere Verbindung her und durchsucht dann einen Index.

```
import org.opensearch.client.opensearch.OpenSearchClient;

SdkHttpClient httpClient = ApacheHttpClient.builder().build();

OpenSearchClient client = new OpenSearchClient(
    new AwsSdk2Transport(
        httpClient,
        "...us-west-2.aoss.amazonaws.com", // serverless collection endpoint
        "aoss" // signing service name
        Region.US_WEST_2, // signing service region
        AwsSdk2TransportOptions.builder().build()
    )
);

Response response = client.generic()
    .execute(
        Requests.builder()
            .endpoint("/" + "users" + "/_search?typed_keys=true")
            .method("GET")
            .json("{"
                + "    \"query\": {"
                + "        \"match_all\": {}"
                + "    }"
                + "}")
            .build());

httpClient.close();
```

JavaScript

Im folgenden Beispielcode wird der opensearch-js-Client verwendet, JavaScript um eine sichere Verbindung zur angegebenen OpenSearch Serverless-Sammlung herzustellen, einen einzelnen Index zu erstellen, ein Dokument hinzuzufügen und den Index zu löschen. Sie müssen Werte für `node` und `region` angeben.

Der wichtige Unterschied zu OpenSearch Dienstdomänen ist der Dienstname (`aoss`anstelle von). `es`

Version 3

In diesem Beispiel wird Version 3 des SDK für JavaScript in Node.js verwendet.

```
const { defaultProvider } = require('@aws-sdk/credential-provider-node');
const { Client } = require('@opensearch-project/opensearch');
const { AwsSigv4Signer } = require('@opensearch-project/opensearch/aws');

async function main() {
    // create an opensearch client and use the request-signer
    const client = new Client({
        ...AwsSigv4Signer({
            region: 'us-west-2',
            service: 'aoss',
            getCredentials: () => {
                const credentialsProvider = defaultProvider();
                return credentialsProvider();
            },
        }),
        node: '' # // serverless collection endpoint
    });

    const index = 'movies';

    // create index if it doesn't already exist
    if (!(await client.indices.exists({ index })).body) {
        console.log((await client.indices.create({ index })).body);
    }

    // add a document to the index
    const document = { foo: 'bar' };
    const response = await client.index({
        id: '1',
        index: index,
        body: document,
    });
    console.log(response.body);

    // delete the index
    console.log((await client.indices.delete({ index })).body);
}

main();
```

Version 2

In diesem Beispiel wird Version 2 des SDK für JavaScript in Node.js verwendet.

```
const AWS = require('aws-sdk');
const { Client } = require('@opensearch-project/opensearch');
const { AwsSigv4Signer } = require('@opensearch-project/opensearch/aws');

async function main() {
    // create an opensearch client and use the request-signer
    const client = new Client({
        ...AwsSigv4Signer({
            region: 'us-west-2',
            service: 'aoss',
            getCredentials: () =>
                new Promise((resolve, reject) => {
                    AWS.config.getCredentials((err, credentials) => {
                        if (err) {
                            reject(err);
                        } else {
                            resolve(credentials);
                        }
                    });
                }),
        }),
        node: '' # // serverless collection endpoint
    });

    const index = 'movies';

    // create index if it doesn't already exist
    if (!(await client.indices.exists({ index }),body) {
        console.log((await client.indices.create({
            index
        })).body);
    }

    // add a document to the index
    const document = {
        foo: 'bar'
    };
    const response = await client.index({
        id: '1',
        index: index,
```

```
        body: document,
    });
    console.log(response.body);

    // delete the index
    console.log((await client.indices.delete({ index })).body);
}

main();
```

Logstash

Sie können das OpenSearch Logstash-Plugin verwenden, um Logs in OpenSearch serverlosen Sammlungen zu veröffentlichen.

Um Logstash zu verwenden, um Daten an Serverless zu senden OpenSearch

1. Installieren Sie Version 2.0.0 oder höher des logstash-output-opensearchPlugins mit Docker oder Linux.

   Docker

   Docker hostet die Logstash OSS-Software mit dem vorinstallierten Ausgabe-Plugin: opensearchproject/ OpenSearch -output-plugin. logstash-oss-with-opensearch Sie können das Image wie jedes andere Image abrufen:

   ```
   docker pull opensearchproject/logstash-oss-with-opensearch-output-plugin:latest
   ```

   Linux

   Installieren Sie zunächst die neueste Version von Logstash, falls Sie dies noch nicht getan haben. Installieren Sie anschließend Version 2.0.0 des Ausgabe-Plugins:

   ```
   cd logstash-8.5.0/
   bin/logstash-plugin install --version 2.0.0 logstash-output-opensearch
   ```

   Wenn das Plugin bereits installiert ist, aktualisieren Sie es auf die neueste Version:

   ```
   bin/logstash-plugin update logstash-output-opensearch
   ```

Ab Version 2.0.0 des Plugins verwendet das SDK Version 3. AWS Wenn du eine Logstash-Version vor 8.4.0 verwendest, musst du alle vorinstallierten AWS Plugins entfernen und das Plugin installieren: `logstash-integration-aws`

```
/usr/share/logstash/bin/logstash-plugin remove logstash-input-s3
/usr/share/logstash/bin/logstash-plugin remove logstash-input-sqs
/usr/share/logstash/bin/logstash-plugin remove logstash-output-s3
/usr/share/logstash/bin/logstash-plugin remove logstash-output-sns
/usr/share/logstash/bin/logstash-plugin remove logstash-output-sqs
/usr/share/logstash/bin/logstash-plugin remove logstash-output-cloudwatch

/usr/share/logstash/bin/logstash-plugin install --version 0.1.0.pre logstash-
integration-aws
```

2. Damit das OpenSearch Ausgabe-Plugin mit OpenSearch Serverless funktioniert, müssen Sie die folgenden Änderungen am Ausgabebereich von logstash.conf vornehmen: `opensearch`

   - Geben Sie `aoss` als `service_name` unter `auth_type` an.
   - Geben Sie Ihren Sammlungsendpunkt für `hosts` an.
   - Fügen Sie die Parameter `default_server_major_version` und `legacy_template` hinzu. Diese Parameter sind erforderlich, damit das Plugin mit Serverless funktioniert. OpenSearch

```
output {
  opensearch {
    hosts => "collection-endpoint:443"
    auth_type => {
      ...
      service_name => 'aoss'
    }
    default_server_major_version => 2
    legacy_template => false
  }
}
```

Diese Beispielkonfigurationsdatei verwendet ihre Eingabe aus Dateien in einem S3-Bucket und sendet sie an eine OpenSearch Serverless-Sammlung:

```
input {
```

```
  s3  {
    bucket => "my-s3-bucket"
    region => "us-east-1"
  }
}

output {
  opensearch {
    ecs_compatibility => disabled
    hosts => "https://my-collection-endpoint.us-east-1.aoss.amazonaws.com:443"
    index => my-index
    auth_type => {
      type => 'aws_iam'
      aws_access_key_id => 'your-access-key'
      aws_secret_access_key => 'your-secret-key'
      region => 'us-east-1'
      service_name => 'aoss'
    }
    default_server_major_version => 2
    legacy_template => false
  }
}
```

3. Führen Sie dann Logstash mit der neuen Konfiguration aus, um das Plugin zu testen:

```
bin/logstash -f config/test-plugin.conf
```

Python

Der folgende Beispielcode verwendet den opensearch-py-Client für Python, um eine sichere Verbindung zur angegebenen OpenSearch Serverless-Sammlung herzustellen, einen einzelnen Index zu erstellen und diesen Index zu durchsuchen. Sie müssen Werte für `region` und `host` angeben.

Der wichtige Unterschied zu OpenSearch Dienstdomänen ist der Dienstname (`aoss`anstelle von). `es`

```
from opensearchpy import OpenSearch, RequestsHttpConnection, AWSV4SignerAuth
import boto3

host = ''  # serverless collection endpoint, without https://
region = ''  # e.g. us-east-1
```

```
service = 'aoss'
credentials = boto3.Session().get_credentials()
auth = AWSV4SignerAuth(credentials, region, service)

# create an opensearch client and use the request-signer
client = OpenSearch(
    hosts=[{'host': host, 'port': 443}],
    http_auth=auth,
    use_ssl=True,
    verify_certs=True,
    connection_class=RequestsHttpConnection,
    pool_maxsize=20,
)

# create an index
index_name = 'books-index'
create_response = client.indices.create(
    index_name
)

print('\nCreating index:')
print(create_response)

# index a document
document = {
  'title': 'The Green Mile',
  'director': 'Stephen King',
  'year': '1996'
}

response = client.index(
    index = 'books-index',
    body = document,
    id = '1'
)


# delete the index
delete_response = client.indices.delete(
    index_name
)

print('\nDeleting index:')
```

```
print(delete_response)
```

Ruby

Das `opensearch-aws-sigv4` Gem bietet standardmäßig Zugriff auf OpenSearch Serverless und OpenSearch Service. Es hat alle Funktionen des opensearch-ruby-Clients, da es von diesem Gem abhängig ist.

Geben Sie bei der Instanziierung des Sigv4-Signers `aoss` als Servicenamen an:

```
require 'opensearch-aws-sigv4'
require 'aws-sigv4'

signer = Aws::Sigv4::Signer.new(service: 'aoss',
                                region: 'us-west-2',
                                access_key_id: 'key_id',
                                secret_access_key: 'secret')

# create an opensearch client and use the request-signer
client = OpenSearch::Aws::Sigv4Client.new(
  { host: 'https://your.amz-opensearch-serverless.endpoint',
    log: true },
  signer)

# create an index
index = 'prime'
client.indices.create(index: index)

# insert data
client.index(index: index, id: '1', body: { name: 'Amazon Echo',
                                            msrp: '5999',
                                            year: 2011 })

# query the index
client.search(body: { query: { match: { name: 'Echo' } } })

# delete index entry
client.delete(index: index, id: '1')

# delete the index
client.indices.delete(index: index)
```

Signieren von HTTP-Anforderungen mit anderen Clients

Die folgenden Anforderungen gelten für das Signieren von Anfragen an OpenSearch serverlose Sammlungen, wenn Sie HTTP-Anfragen mit anderen Clients erstellen.

- Sie müssen den Service-Namen als `aoss` angeben.
- Der `x-amz-content-sha256`-Header ist für alle Anforderungen der AWS Signature Version 4 erforderlich. Es stellt einen Hash der Anforderungsnutzlast bereit. Wenn eine Anforderungsnutzlast vorhanden ist, legen Sie den Wert auf den kryptografischen Hash des Secure Hash Algorithm (SHA) (SHA256) fest. Wenn keine Anforderungsnutzlast vorhanden ist, setzen Sie den Wert auf `e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855`, was der Hash einer leeren Zeichenfolge ist.

Themen

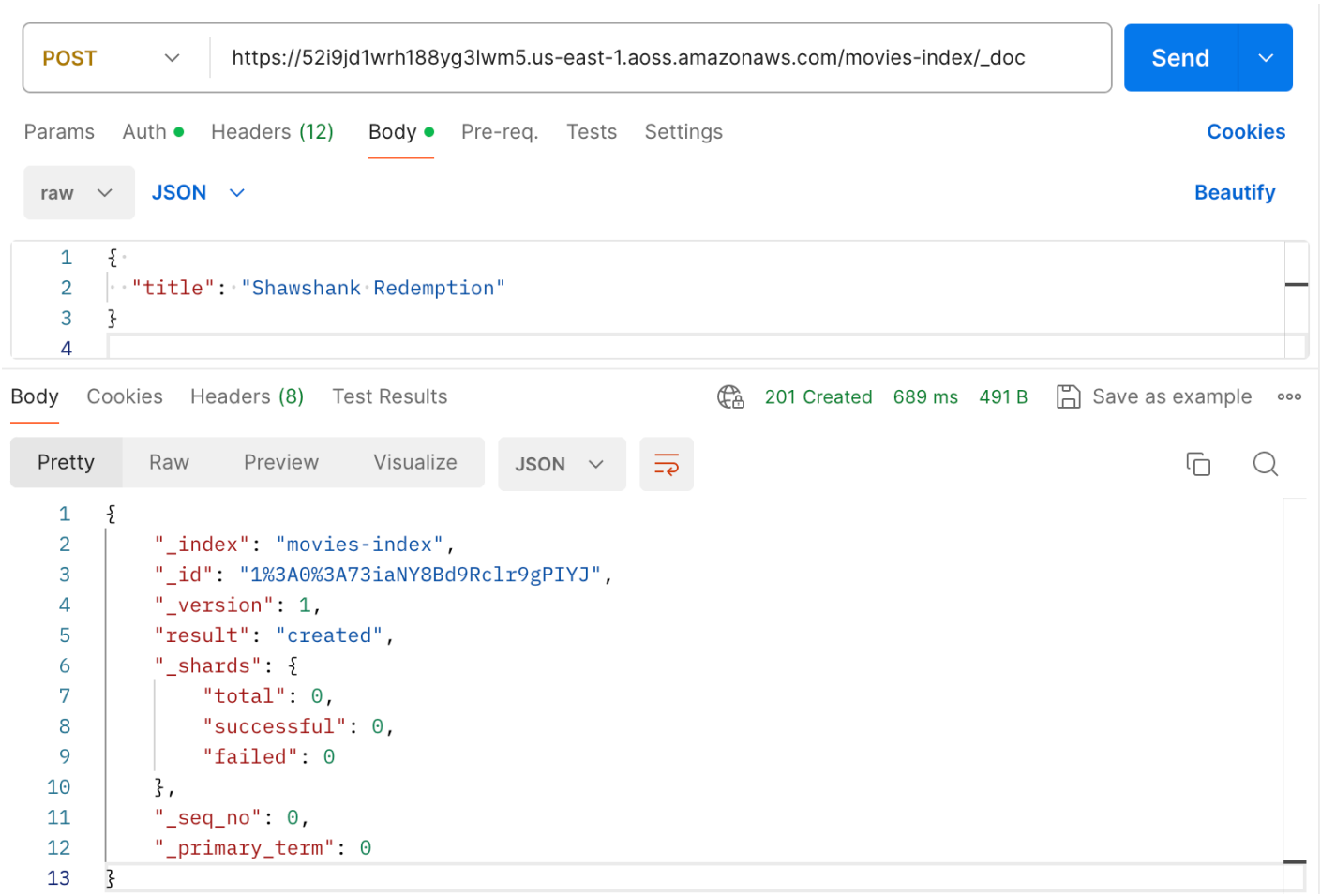
Indizierung mit cURL

Die folgende Beispielanforderung verwendet die Client URL Request Library (cURL), um ein einzelnes Dokument an einen Index zu senden, der `movies-index` innerhalb einer Sammlung benannt ist:

```
curl -XPOST \
    --user "$AWS_ACCESS_KEY_ID":"$AWS_SECRET_ACCESS_KEY" \
    --aws-sigv4 "aws:amz:us-east-1:aoss" \
    --header "x-amz-content-sha256: $REQUEST_PAYLOAD_SHA_HASH" \
    --header "x-amz-security-token: $AWS_SESSION_TOKEN" \
    "https://my-collection-endpoint.us-east-1.aoss.amazonaws.com/movies-index/_doc" \
    -H "Content-Type: application/json" -d '{"title": "Shawshank Redemption"}'
```

Indizierung mit Postman

Die folgende Abbildung zeigt, wie Sie mit Postman Anfragen an eine Sammlung senden. Anweisungen zur Authentifizierung finden Sie unter Workflow zur Authentifizierung mit AWS Signatur in Postman.



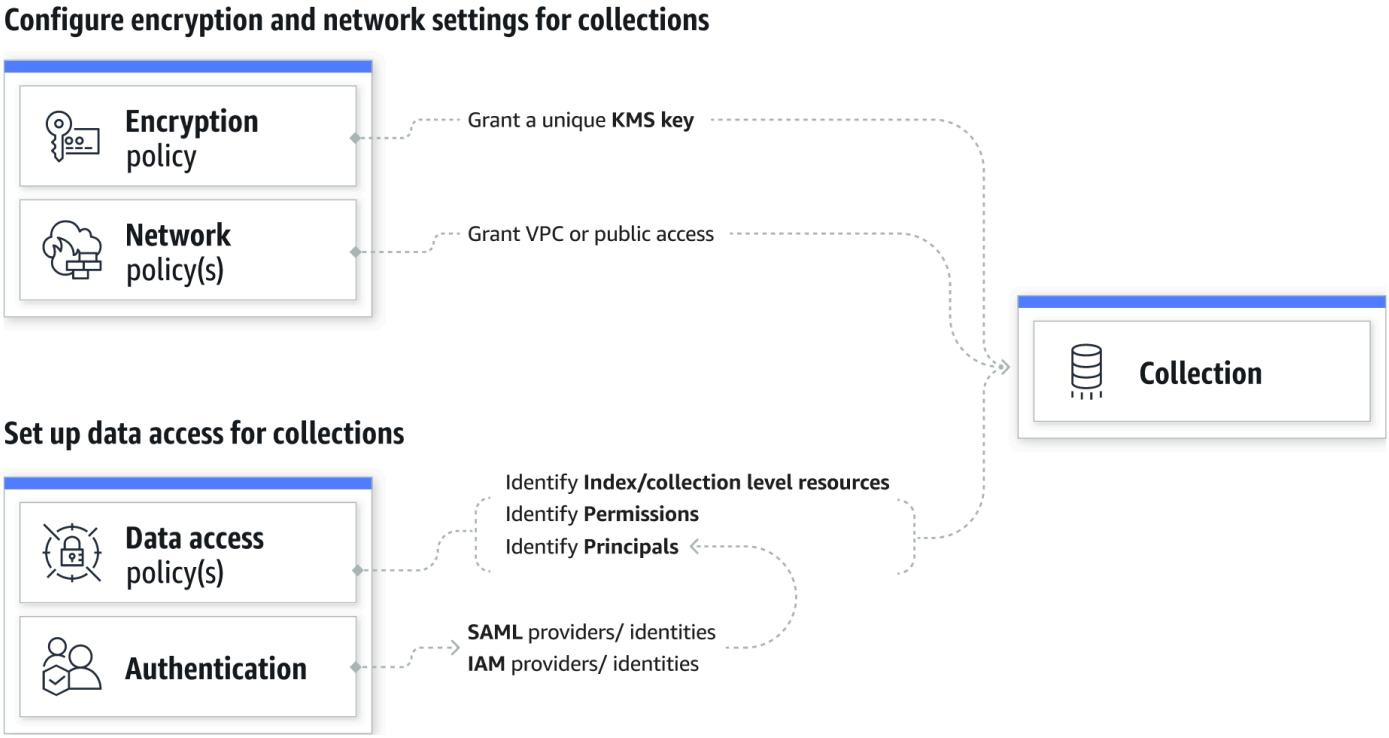
Überblick über die Sicherheit in Amazon OpenSearch Serverless

Die Sicherheit in Amazon OpenSearch Serverless unterscheidet sich in folgenden Punkten grundlegend von der Sicherheit in Amazon OpenSearch Service:

Funktion	OpenSearch Service	OpenSearch Serverlos
Datenzugr iffskontrolle	Der Datenzugriff wird durch IAM-Richt linien und eine differenzierte Zugangsko ntrolle festgelegt.	Der Datenzugriff wird durch Datenzugriffsrichtlinien festgeleg t.
Verschlüsselung im Ruhezustand	Die Verschlüsselung im Ruhezustand ist für Domains optional.	Die Verschlüsselung im Ruhezustand ist für Sammlunge n erforderlich.

Funktion	OpenSearch Service	OpenSearch Serverlos
Einrichtung und Verwaltung der Sicherheit	Sie müssen Netzwerk, Verschlüsselung und Datenzugriff für jede Domain einzeln konfigurieren.	Sie können Sicherheitsrichtli nien verwenden, um Sicherhei tseinstellungen für mehrere Sammlungen in großem Umfang zu verwalten.

Das folgende Diagramm veranschaulicht die Sicherheitskomponenten, aus denen eine funktionale Sammlung besteht. Eine Sammlung muss über einen zugewiesenen Verschlüsselungsschlüssel, Netzwerkzugriffseinstellungen und eine passende Datenzugriffsrichtlinie verfügen, die ihren Ressourcen Berechtigungen gewährt.



Themen

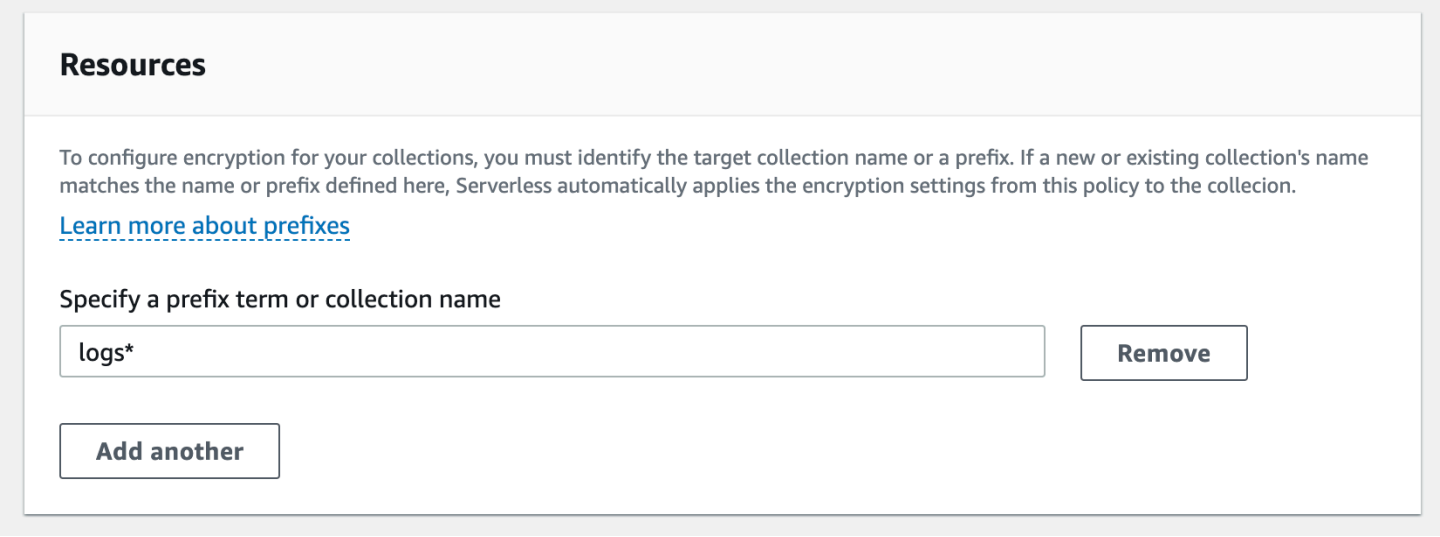
- Verschlüsselungsrichtlinien
- Netzwerkrichtlinien
- Daten-Zugriffsrichtlinien
- IAM und SAML-Authentifizierung
- Sicherheit der Infrastruktur

- Erste Schritte mit Sicherheit in Amazon OpenSearch Serverless
- Identity and Access Management für Amazon OpenSearch Serverless
- Verschlüsselung in Amazon OpenSearch Serverless
- Netzwerkzugriff für Amazon OpenSearch Serverless
- Datenzugriffskontrolle für Amazon OpenSearch Serverless
- Greifen Sie über einen Schnittstellenendpunkt auf Amazon OpenSearch Serverless zu ()AWS PrivateLink
- SAML-Authentifizierung für Amazon OpenSearch Serverless
- Konformitätsvalidierung für Amazon OpenSearch Serverless

Verschlüsselungsrichtlinien

Verschlüsselungsrichtlinien definieren, ob Ihre Sammlungen mit einem AWS-eigener Schlüssel oder einem vom Kunden verwalteten Schlüssel verschlüsselt werden. Verschlüsselungsrichtlinien bestehen aus zwei Komponenten: einem Ressourcenmuster und einem Verschlüsselungsschlüssel. Das Ressourcenmuster legt fest, für welche Sammlung oder Sammlungen die Richtlinie gilt. Der Verschlüsselungsschlüssel legt fest, wie die zugehörigen Sammlungen gesichert werden.

Um eine Richtlinie auf mehrere Sammlungen anzuwenden, fügen Sie der Richtlinienregel ein Platzhalterzeichen (*) hinzu. Die folgende Richtlinie gilt beispielsweise für alle Sammlungen, deren Namen mit „logs“ beginnen.



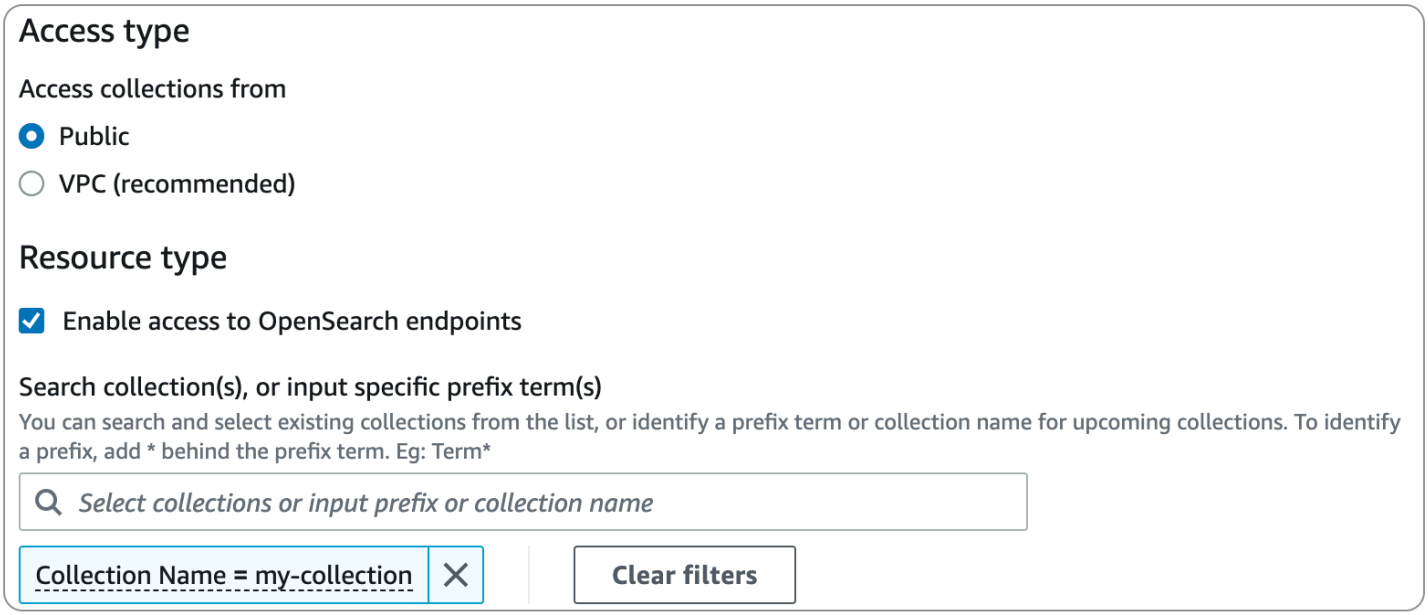
Verschlüsselungsrichtlinien optimieren den Prozess der Erstellung und Verwaltung von Sammlungen, insbesondere wenn Sie dies programmgesteuert tun. Sie können eine Sammlung erstellen,

indem Sie einfach einen Namen angeben. Bei der Erstellung wird dieser automatisch ein Verschlüsselungsschlüssel zugewiesen.

Netzwerkrichtlinien

Netzwerkrichtlinien definieren, ob Ihre Sammlungen privat oder über das Internet von öffentlichen Netzwerken aus zugänglich sind. Auf private Sammlungen kann über OpenSearch serverlos verwaltete VPC-Endpunkte oder über spezifische Endpunkte AWS-Services wie Amazon Bedrock über privaten Zugriff zugegriffen werden.AWS-Service Genau wie Verschlüsselungsrichtlinien können auch Netzwerkrichtlinien für mehrere Sammlungen gelten, so dass Sie den Netzwerkzugriff für viele Sammlungen in großem Umfang verwalten können.

Netzwerkrichtlinien bestehen aus zwei Komponenten: einem Zugriffstyp und einem Ressourcentyp. Der Zugriffstyp kann entweder öffentlich oder privat sein. Der Ressourcentyp bestimmt, ob der von Ihnen gewählte Zugriff für den Sammlungsendpunkt, den OpenSearch Dashboards-Endpunkt oder für beide gilt.



Wenn Sie den VPC-Zugriff innerhalb einer Netzwerkrichtlinie konfigurieren möchten, müssen Sie zunächst einen oder OpenSearch mehrere serverlos verwaltete VPC-Endpoints erstellen. Mit diesen Endpunkten können Sie wie in Ihrer VPC auf OpenSearch Serverless zugreifen, ohne ein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder eine Verbindung verwenden zu müssen. AWS Direct Connect

Der private Zugriff auf AWS-Services kann nur für den Endpunkt der Sammlung gelten, nicht für den OpenSearch Endpunkt der OpenSearch Dashboards. AWS-Services kann kein Zugriff auf OpenSearch Dashboards gewährt werden.

Daten-Zugriffsrichtlinien

Datenzugriffsrichtlinien definieren, wie Ihre Benutzer auf die Daten in Ihren Sammlungen zugreifen. Datenzugriffsrichtlinien unterstützen Sie bei der Verwaltung von Sammlungen in großem Umfang, indem sie automatisch Zugriffsberechtigungen für Sammlungen und Indizes zuweisen, die einem bestimmten Muster übereinstimmen. Mehrere Richtlinien können für eine einzelne Ressource gelten.

Datenzugriffsrichtlinien bestehen aus einer Reihe von Regeln mit jeweils drei Komponenten: einem Ressourcentyp, gewährte Ressourcen und einer Reihe von Berechtigungen. Der Ressourcentyp kann eine Sammlung oder ein Index sein. Bei den gewährten Ressourcen kann es sich um Sammlungs-/Indexnamen oder Muster mit einem Platzhalter (*) handeln. Die Liste der Berechtigungen gibt an, auf welche OpenSearch API-Operationen die Richtlinie Zugriff gewährt. Darüber hinaus enthält die Richtlinie eine Liste von Prinzipalen, die die IAM-Rollen, -Benutzer und SAML-Identitäten angeben, denen Zugriff gewährt werden soll.

Weitere Informationen zum Format einer Datenzugriffsrichtlinie finden Sie in der Richtliniensyntax.

Bevor Sie eine Datenzugriffsrichtlinie erstellen, müssen Sie über eine oder mehrere IAM-Rollen oder -Benutzer oder SAML-Identitäten verfügen, auf die Sie in der Richtlinie Zugriff gewähren können. Einzelheiten finden Sie im nächsten Abschnitt.

IAM und SAML-Authentifizierung

IAM-Prinzipale und SAML-Identitäten sind eine der Bausteine einer Datenzugriffsrichtlinie. Innerhalb der `principal`-Anweisung einer Zugriffsrichtlinie können Sie IAM-Rollen, IAM-Benutzer und SAML-

Identitäten angeben. Diesen Prinzipalen werden dann die Berechtigungen gewährt, die Sie in den zugeordneten Richtlinienregeln angeben.

```
[
   {
      "Rules":[
         {
            "ResourceType":"index",
            "Resource":[
               "index/marketing/orders*"
            ],
            "Permission":[
               "aoss:*"
            ]
         }
      ],
      "Principal":[
         "arn:aws:iam::123456789012:user/Dale",
         "arn:aws:iam::123456789012:role/RegulatoryCompliance",
         "saml/123456789012/myprovider/user/Annie"
      ]
   }
]
```

Sie konfigurieren die SAML-Authentifizierung direkt in OpenSearch Serverless. Weitere Informationen finden Sie unter the section called “SAML-Authentifizierung”.

Sicherheit der Infrastruktur

Amazon OpenSearch Serverless ist durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf Amazon OpenSearch Serverless zuzugreifen. Clients müssen Transport Layer Security (TLS) unterstützen. Wir benötigen TLS 1.2 und empfehlen TLS 1.3. Eine Liste der unterstützten Verschlüsselungen für TLS 1.3 finden Sie unter TLS-Protokolle und Chiffren in der Elastic Load Balancing Balancing-Dokumentation.

Darüber hinaus müssen Sie Anfragen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signieren, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Erste Schritte mit Sicherheit in Amazon OpenSearch Serverless

Die folgenden Tutorials helfen Ihnen bei den ersten Schritten mit Amazon OpenSearch Serverless. In beiden Tutorials werden die gleichen grundlegenden Schritte ausgeführt, aber eines verwendet die Konsole, während das andere die AWS CLI verwendet.

Beachten Sie, dass die Anwendungsfälle in diesen Tutorials vereinfacht sind. Die Netzwerk- und Sicherheitsrichtlinien sind relativ offen. Bei Produktions-Workloads empfehlen wir, robustere Sicherheitsfunktionen wie SAML-Authentifizierung, VPC-Zugriff und restriktive Datenzugriffsrichtlinien zu konfigurieren.

Themen

- Tutorial: Erste Schritte mit der Sicherheit in Amazon OpenSearch Serverless (Konsole)
- Tutorial: Erste Schritte mit der Sicherheit in Amazon OpenSearch Serverless (CLI)

Tutorial: Erste Schritte mit der Sicherheit in Amazon OpenSearch Serverless (Konsole)

Dieses Tutorial führt Sie durch die grundlegenden Schritte zum Erstellen und Verwalten von Sicherheitsrichtlinien mit der Amazon OpenSearch -Serverless-Konsole.

In diesem Tutorial führen Sie die folgenden Schritte aus:

1. Konfigurieren von Berechtigungen
2. Erstellen einer Verschlüsselungsrichtlinie
3. Eine Netzwerkrichtlinie erstellen
4. Konfigurieren einer Datenzugriffsrichtlinie
5. Erstellen einer Sammlung
6. Hochladen und Suchen von Daten

Das Tutorial führt Sie durch das Einrichten einer Sammlung mithilfe der AWS Management Console. Die gleichen Schritte mit der AWS CLI finden Sie unter the section called “Tutorial: Erste Schritte mit Sicherheit (CLI)”.

Schritt 1: Konfigurieren von Berechtigungen

> **Note**
>
> Sie können diesen Schritt überspringen, wenn Sie bereits eine umfassendere identitätsbasierte Richtlinie verwenden, z. B. `Action":"aoss:*"` oder `Action":"*"`. In Produktionsumgebungen empfehlen wir jedoch, dem Prinzipal der geringsten Berechtigung zu folgen und nur die für die Ausführung einer Aufgabe erforderlichen Mindestberechtigungen zuzuweisen.

Um dieses Tutorial und OpenSearch Serverless im Allgemeinen verwenden zu können, müssen Sie über die richtigen IAM-Berechtigungen verfügen. Ihr Benutzer oder Ihre Rolle muss über eine angefügte identitätsbasierte Richtlinie mit den folgenden Mindestberechtigungen verfügen:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "aoss:ListCollections",
        "aoss:BatchGetCollection",
        "aoss:CreateCollection",
        "aoss:CreateSecurityPolicy",
        "aoss:GetSecurityPolicy",
        "aoss:ListSecurityPolicies",
        "aoss:CreateAccessPolicy",
        "aoss:GetAccessPolicy",
        "aoss:ListAccessPolicies"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Eine vollständige Liste der OpenSearch Serverless-Berechtigungen finden Sie unter the section called “Identitäts- und Zugriffsverwaltung”.

Schritt 2: Erstellen einer Verschlüsselungsrichtlinie

Verschlüsselungsrichtlinien geben den AWS KMS Schlüssel an, den OpenSearch Serverless zum Verschlüsseln der Sammlung verwendet. Sie können Sammlungen mit einem Von AWS verwalteter Schlüssel oder einem anderen Schlüssel verschlüsseln. Der Einfachheit halber verschlüsseln wir in diesem Tutorial unsere Sammlung mit einem Von AWS verwalteter Schlüssel.

So erstellen Sie eine Verschlüsselungsrichtlinie

1. Öffnen Sie die Amazon- OpenSearch Service-Konsole unter https://console.aws.amazon.com/aos/home.
2. Erweitern Sie im linken Navigationsbereich Serverless und wählen Sie Encryption policies (Verschlüsselungsrichtlinien).
3. Wählen Sie Create encryption policy (Verschlüsselungsrichtlinie erstellen).
4. Benennen Sie die Richtlinie books-policy (Bücher-Richtlinie). Geben Sie als Beschreibung Encryption policy for books collection (Verschlüsselungsrichtlinie für die Bücher-Sammlung) ein.
5. Geben Sie unter Resources (Ressourcen) den Namen books (Bücher) ein, den Sie Ihrer Sammlung geben werden. Wenn Sie die Richtlinie weiter fassen möchten, können Sie ein Sternchen (`books*`) einfügen, damit die Richtlinie für alle Sammlungen gilt, die mit dem Wort „Bücher“ beginnen.
6. Lassen Sie für Verschlüsselung die Option AWS Eigenen Schlüssel verwenden ausgewählt.
7. Wählen Sie Erstellen.

Schritt 3: Erstellen einer Netzwerkrichtlinie

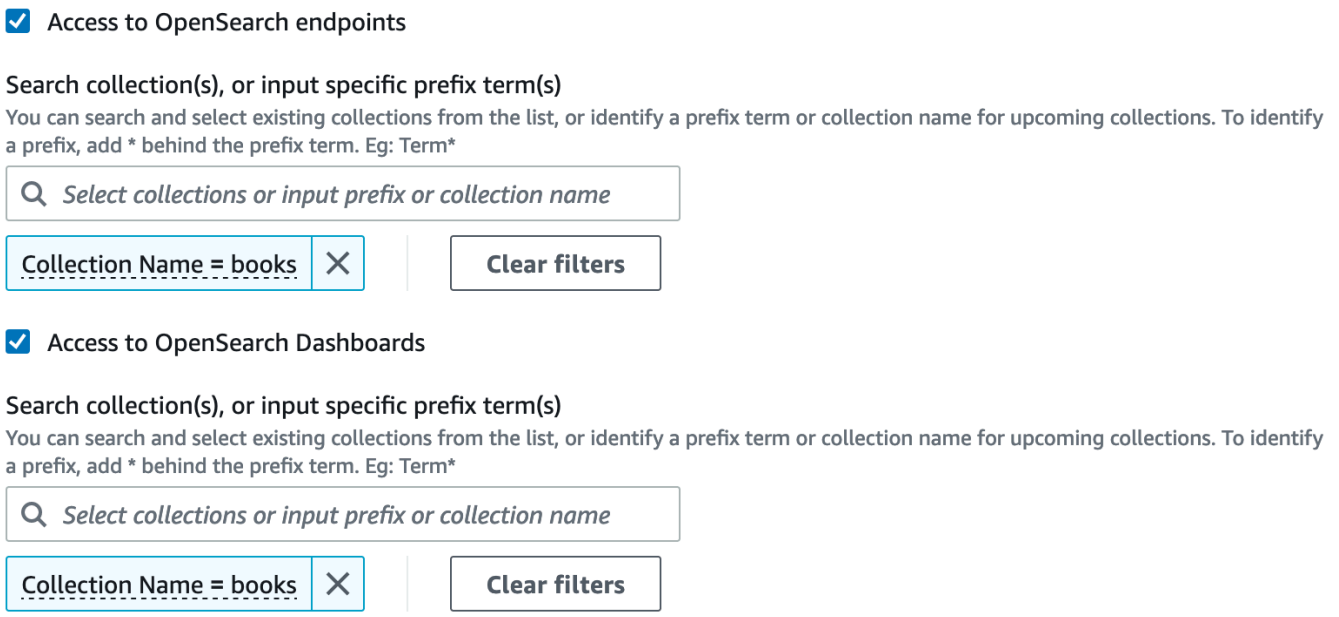
Netzwerkrichtlinien bestimmen, ob Ihre Sammlung über das Internet von öffentlichen Netzwerken aus zugänglich ist oder ob über OpenSearch Serverless-verwaltete VPC-Endpunkte darauf zugegriffen werden muss. In diesem Tutorial konfigurieren wir den öffentlichen Zugriff.

So erstellen Sie eine Netzwerkrichtlinie

1. Wählen Sie im linken Navigationsbereich Network policies (Netzwerkrichtlinien) und dann Create network policy (Netzwerkrichtlinie erstellen) aus.
2. Benennen Sie die Richtlinie books-policy (Bücher-Richtlinie). Geben Sie als Beschreibung Network policy for books collection (Netzwerkrichtlinie für Bücher-Sammlung) ein.
3. Benennen Sie unter Rule 1 (Regel 1) die Regel Public access for books collection (Öffentlicher Zugriff für Bücher-Sammlung).

4. Der Einfachheit halber konfigurieren wir in diesem Tutorial den öffentlichen Zugriff für die Bücher-Sammlung. Wählen Sie für den Zugriffstyp Public (Öffentlich) aus.
5. Wir greifen von OpenSearch Dashboards aus auf die Sammlung zu. Dazu müssen Sie den Netzwerkzugriff für Dashboards und den OpenSearch Endpunkt konfigurieren, andernfalls funktioniert Dashboards nicht.

   Aktivieren Sie für den Ressourcentyp sowohl Zugriff auf OpenSearch Endpunkte als auch Zugriff auf OpenSearch Dashboards.
6. Geben Sie in beiden Eingabefeldern Collection Name = books (Sammlungsname = Bücher) ein. Diese Einstellung schränkt die Richtlinie so ein, dass sie nur für eine einzelne Sammlung gilt (`books`). Ihre Regel sollte folgendermaßen aussehen:



7. Wählen Sie Erstellen.

Schritt 4: Erstellen einer Datenzugriffsrichtlinie

Ihre Sammlungsdaten sind erst dann zugänglich, wenn Sie den Zugriff auf die Daten konfigurieren. Datenzugriffsrichtlinien sind von der identitätsbasierten IAM-Richtlinie, die Sie in Schritt 1 konfiguriert haben, getrennt. Diese ermöglichen den Benutzern den Zugriff auf die tatsächlichen Daten innerhalb einer Sammlung.

In diesem Tutorial gewähren wir einem einzelnen Benutzer die Berechtigungen, die zum Indizieren von Daten in der Bücher-Sammlung erforderlich sind.

So erstellen Sie eine Datenzugriffsrichtlinie

1. Wählen Sie im linken Navigationsbereich Data access policies (Datenzugriffsrichtlinien) und anschließend Create access policy (Zugriffsrichtlinie erstellen) aus.
2. Benennen Sie die Richtlinie books-policy (Bücher-Richtlinie). Geben Sie als Beschreibung Data access policy for books collection (Datenzugriffsrichtlinie für die Bücher-Sammlung) ein.
3. Wählen Sie JSON als Methode zur Richtliniendefinition aus und fügen Sie die folgende Richtlinie in den JSON-Editor ein.

   Ersetzen Sie den Prinzipal-ARN durch den ARN des Kontos, mit dem Sie sich bei OpenSearch Dashboards anmelden und Daten indizieren.

   ```
   [
      {
         "Rules":[
            {
               "ResourceType":"index",
               "Resource":[
                  "index/books/*"
               ],
               "Permission":[
                  "aoss:CreateIndex",
                  "aoss:DescribeIndex",
                  "aoss:ReadDocument",
                  "aoss:WriteDocument",
                  "aoss:UpdateIndex",
                  "aoss:DeleteIndex"
               ]
            }
         ],
         "Principal":[
            "arn:aws:iam::123456789012:user/my-user"
         ]
      }
   ]
   ```

   Diese Richtlinie gewährt einem einzelnen Benutzer die Mindestberechtigungen, die erforderlich sind, um einen Index in der Bücher-Sammlung zu erstellen, einige Daten zu indizieren und danach zu suchen.
4. Wählen Sie Erstellen.

Schritt 5: Erstellen einer Sammlung

Nachdem Sie die Verschlüsselungs- und Netzwerkrichtlinien konfiguriert haben, können Sie eine passende Sammlung erstellen und die Sicherheitseinstellungen werden automatisch darauf angewendet.

So erstellen Sie eine OpenSearch -Serverless-Sammlung

1. Wählen Sie im linken Navigationsbereich Collections (Sammlungen) und wählen Sie Create collection (Sammlung erstellen) aus.
2. Benennen Sie die Sammlung books (Bücher).
3. Wählen Sie als Sammlungstyp Search (Suchen) aus.
4. Unter Verschlüsselung informiert OpenSearch Serverless Sie darüber, dass der Name der Sammlung mit der `books-policy`Verschlüsselungsrichtlinie übereinstimmt.
5. Unter Netzwerkzugriffseinstellungen informiert OpenSearch Serverless Sie darüber, dass der Name der Sammlung mit der `books-policy` Netzwerkrichtlinie übereinstimmt.
6. Wählen Sie Weiter aus.
7. Unter Optionen für Datenzugriffsrichtlinien informiert OpenSearch Serverless Sie darüber, dass der Name der Sammlung mit der `books-policy` Datenzugriffsrichtlinie übereinstimmt.
8. Wählen Sie Weiter aus.
9. Überprüfen Sie die Sammlungskonfiguration und wählen Sie Submit (Senden) aus. Die Initialisierung von Sammlungen dauert in der Regel weniger als eine Minute.

Schritt 6: Hochladen und Suchen von Daten

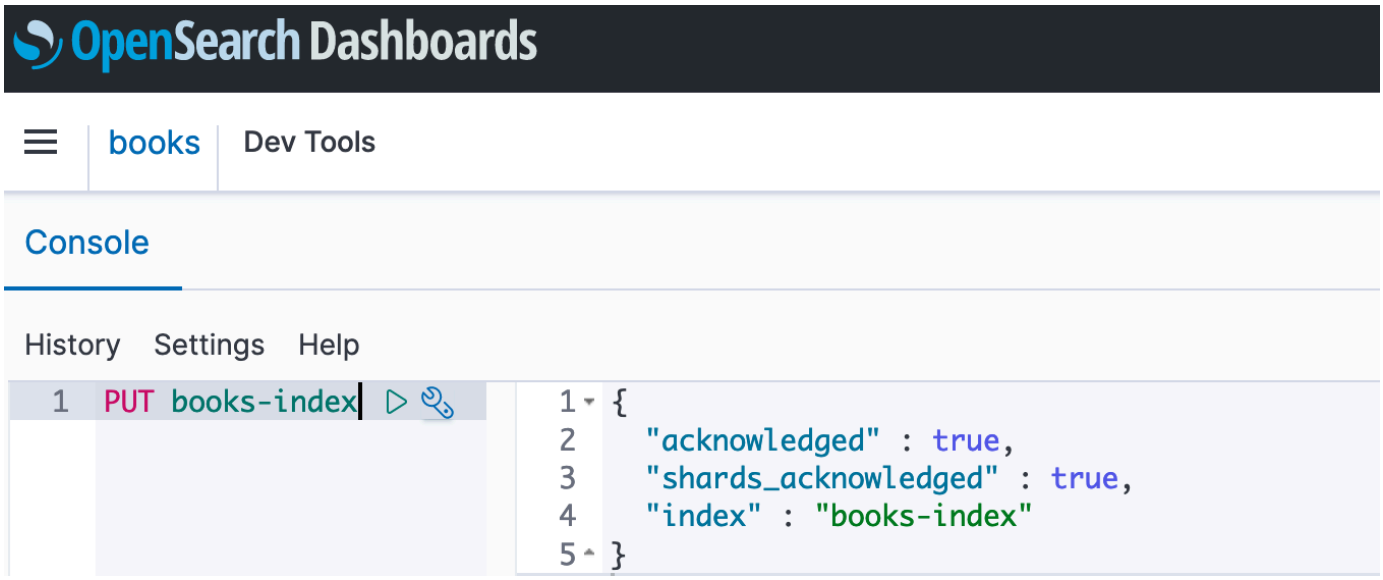
Sie können Daten mit Postman oder curl in eine OpenSearch -Serverless-Sammlung hochladen. Der Kürze halber verwenden diese Beispiele Entwicklungs-Tools in der OpenSearch Dashboards-Konsole.

So indizieren und suchen Sie Daten in einer Sammlung

1. Wählen Sie im linken Navigationsbereich Collections (Sammlungen) und dann die Bücher-Sammlung aus, um die Detailseite zu öffnen.
2. Wählen Sie die OpenSearch Dashboards-URL für die Sammlung aus. Die URL nimmt das Format `https://collection-id.us-east-1.aoss.amazonaws.com/_dashboards` an.

3. Melden Sie sich bei OpenSearch Dashboards mit den AWS Zugriffs- und geheimen Schlüsseln für den Prinzipal an, den Sie in Ihrer Datenzugriffsrichtlinie angegeben haben.
4. Öffnen Sie in OpenSearch Dashboards das linke Navigationsmenü und wählen Sie Entwicklungstools aus.
5. Führen Sie den folgenden Befehl aus, um einen einzelnen Index mit dem Namen books-index zu erstellen:

```
PUT books-index
```



6. Führen Sie den folgenden Befehl aus, um ein einzelnes Dokument in books-index zu indizieren:

```
PUT books-index/_doc/1
{
  "title": "The Shining",
  "author": "Stephen King",
  "year": 1977
}
```

7. Um Daten in OpenSearch Dashboards zu suchen, müssen Sie mindestens ein Indexmuster konfigurieren. OpenSearch verwendet diese Muster, um zu identifizieren, welche Indizes Sie analysieren möchten. Öffnen Sie das Dashboards-Hauptmenü, wählen Sie Stack-Management, wählen Sie Indexmuster und dann Indexmuster erstellen. Geben Sie für dieses Tutorial books-index ein.

8. Wählen Sie Nächster Schritt aus und klicken Sie auf Indexmuster erstellen. Nachdem das Muster erstellt wurde, können Sie die verschiedenen Dokumentfelder anzeigen, z. B. `author` und `title`.
9. Um mit der Suche nach Ihren Daten zu beginnen, öffnen Sie erneut das Hauptmenü und wählen Sie Discover (Erkunden) oder verwenden Sie die Such-API.

Tutorial: Erste Schritte mit der Sicherheit in Amazon OpenSearch Serverless (CLI)

In diesem Tutorial werden Sie aus Sicherheitsgründen durch die Schritte geführt, die im Tutorial für die ersten Schritte der Konsole beschrieben sind. Es verwendet jedoch die AWS CLI anstelle der OpenSearch Servicekonsole.

In diesem Tutorial führen Sie die folgenden Schritte durch:

1. Erstellen einer IAM-Berechtigungsrichtlinie
2. Veranlassen der IAM-Richtlinie an eine IAM-Rolle
3. Eine Verschlüsselungsrichtlinie erstellen
4. Eine Netzwerkrichtlinie erstellen
5. Eine Sammlung erstellen
6. Konfigurieren einer Datenzugriffsrichtlinie
7. Abrufen des Sammlungsendpunkts
8. Hochladen von Daten in Ihre Verbindung
9. Suchen von Daten in Ihrer Sammlung

Ziel dieses Tutorials ist es, eine einzelne OpenSearch Serverless-Sammlung mit relativ einfachen Einstellungen für Verschlüsselung, Netzwerk und Datenzugriff einzurichten. Beispielsweise konfigurieren wir den Zugriff auf ein öffentliches Netzwerk, ein Von AWS verwalteter Schlüssel für Verschlüsselung und eine vereinfachte Datenzugriffsrichtlinie, die einem einzelnen Benutzer minimale Berechtigungen gewährt.

Erwägen Sie in einem Produktionsumgebung die Implementierung einer robusteren Konfiguration, einschließlich SAML-Authentifizierung, eines benutzerdefinierten Verschlüsselungsschlüssels und VPC-Zugriff.

So beginnen Sie mit Sicherheitsrichtlinien in OpenSearch Serverless

1.

> **Note**
>
> Sie können diesen Schritt überspringen, wenn Sie bereits eine umfassendere identitätsbasierte Richtlinie verwenden, z. B. `Action":"aoss:*"` oder `Action":"*"`. In Produktionsumgebungen empfehlen wir jedoch, dem Prinzipal der geringsten Berechtigung zu folgen und nur die für die Ausführung einer Aufgabe erforderlichen Mindestberechtigungen zuzuweisen.

Erstellen Sie zunächst eine Richtlinie AWS Identity and Access Management mit den Mindestberechtigungen, die für die Durchführung der Schritte in diesem Tutorial erforderlich sind. Wir werden die Richtlinie `TutorialPolicy` nennen:

```
aws iam create-policy \
  --policy-name TutorialPolicy \
  --policy-document "{\"Version\": \"2012-10-17\",\"Statement\":
 [{\"Action\": [\"aoss:ListCollections\",\"aoss:BatchGetCollection\",
\"aoss:CreateCollection\",\"aoss:CreateSecurityPolicy\",\"aoss:GetSecurityPolicy\",
\"aoss:ListSecurityPolicies\",\"aoss:CreateAccessPolicy\",\"aoss:GetAccessPolicy\",
\"aoss:ListAccessPolicies\"],\"Effect\": \"Allow\",\"Resource\": \"*\"}]}"
```

Beispielantwort

```
{
    "Policy": {
        "PolicyName": "TutorialPolicy",
        "PolicyId": "ANPAW6WRAECKG6QJWUV7U",
        "Arn": "arn:aws:iam::123456789012:policy/TutorialPolicy",
        "Path": "/",
        "DefaultVersionId": "v1",
        "AttachmentCount": 0,
        "PermissionsBoundaryUsageCount": 0,
        "IsAttachable": true,
        "CreateDate": "2022-10-16T20:57:18+00:00",
        "UpdateDate": "2022-10-16T20:57:18+00:00"
    }
}
```

2. Fügen Sie `TutorialPolicy` der IAM-Rolle an, die die Daten in der Sammlung indizieren und durchsuchen wird. Wir benennen den Benutzer `TutorialRole`:

```
aws iam attach-role-policy \
  --role-name TutorialRole \
  --policy-arn arn:aws:iam::123456789012:policy/TutorialPolicy
```

3. Bevor Sie eine Sammlung erstellen, müssen Sie eine Verschlüsselungsrichtlinie erstellen, die ein AWS-eigener Schlüssel der in einem späteren Schritt erstellten Bücher-Sammlung zuweist.

   Senden Sie die folgende Anfrage, um eine Verschlüsselungsrichtlinie für die Bücher-Sammlung zu erstellen:

```
aws opensearchserverless create-security-policy \
  --name books-policy \
  --type encryption --policy "{\"Rules\":[{\"ResourceType\":\"collection\",
\"Resource\":[\"collection\/books\"]}],\"AWSOwnedKey\":true}"
```

   Beispielantwort

```
{
    "securityPolicyDetail": {
        "type": "encryption",
        "name": "books-policy",
        "policyVersion": "MTY2OTI0MDAwNTk5MF8x",
        "policy": {
            "Rules": [
                {
                    "Resource": [
                        "collection/books"
                    ],
                    "ResourceType": "collection"
                }
            ],
            "AWSOwnedKey": true
        },
        "createdDate": 1669240005990,
        "lastModifiedDate": 1669240005990
    }
}
```

4. Erstellen Sie eine Netzwerkrichtlinie, die öffentlichen Zugriff auf die Bücher-Sammlung gewährt:

```
aws opensearchserverless create-security-policy --name books-policy --type network
 \
  --policy "[{\"Description\":\"Public access for books collection\",\"Rules
\":[{\"ResourceType\":\"dashboard\",\"Resource\":[\"collection\/books\"]},
{\"ResourceType\":\"collection\",\"Resource\":[\"collection\/books\"]}],
\"AllowFromPublic\":true}]"
```

Beispielantwort

```
{
    "securityPolicyDetail": {
        "type": "network",
        "name": "books-policy",
        "policyVersion": "MTY2OTI0MDI1Njk1NV8x",
        "policy": [
            {
                "Rules": [
                    {
                        "Resource": [
                            "collection/books"
                        ],
                        "ResourceType": "dashboard"
                    },
                    {
                        "Resource": [
                            "collection/books"
                        ],
                        "ResourceType": "collection"
                    }
                ],
                "AllowFromPublic": true,
                "Description": "Public access for books collection"
            }
        ],
        "createdDate": 1669240256955,
        "lastModifiedDate": 1669240256955
    }
}
```

5. Erstellen Sie die Bücher-Sammlung:

```
aws opensearchserverless create-collection --name books --type SEARCH
```

Beispielantwort

```
{
    "createCollectionDetail": {
        "id": "8kw362bpwg4gx9b2f6e0",
        "name": "books",
        "status": "CREATING",
        "type": "SEARCH",
        "arn": "arn:aws:aoss:us-
east-1:123456789012:collection/8kw362bpwg4gx9b2f6e0",
        "kmsKeyArn": "auto",
        "createdDate": 1669240325037,
        "lastModifiedDate": 1669240325037
    }
}
```

6. Erstellen Sie eine Datenzugriffsrichtlinie, die Mindestberechtigungen zum Indizieren und Suchen von Daten in der Bücher-Sammlung bereitstellt. Ersetzen Sie den Prinzipal-ARN durch den ARN von `TutorialRole` aus Schritt 1:

```
aws opensearchserverless create-access-policy \
  --name books-policy \
  --type data \
  --policy "[{\"Rules\":[{\"ResourceType\":\"index\",\"Resource\":
[\"index\/books\/books-index\"],\"Permission\":[\"aoss:CreateIndex
\",\"aoss:DescribeIndex\",\"aoss:ReadDocument\",\"aoss:WriteDocument
\",\"aoss:UpdateIndex\",\"aoss:DeleteIndex\"]}],\"Principal\":
[\"arn:aws:iam::123456789012:role\/TutorialRole\"]}]"
```

Beispielantwort

```
{
    "accessPolicyDetail": {
        "type": "data",
        "name": "books-policy",
        "policyVersion": "MTY2OTI0MDM5NDY1M18x",
        "policy": [
            {
```

```
                "Rules": [
                    {
                        "Resource": [
                            "index/books/books-index"
                        ],
                        "Permission": [
                            "aoss:CreateIndex",
                            "aoss:DescribeIndex",
                            "aoss:ReadDocument",
                            "aoss:WriteDocument",
                            "aoss:UpdateDocument",
                            "aoss:DeleteDocument"
                        ],
                        "ResourceType": "index"
                    }
                ],
                "Principal": [
                    "arn:aws:iam::123456789012:role/TutorialRole"
                ]
            }
        ],
        "createdDate": 1669240394653,
        "lastModifiedDate": 1669240394653
    }
}
```

`TutorialRole` sollte nun in der Lage sein, Dokumente in der Bücher-Sammlung zu indizieren und zu durchsuchen.

7. Um die OpenSearch API aufzurufen, benötigen Sie den Sammlungsendpunkt. Senden Sie die folgende Anfrage, um den `collectionEndpoint`-Parameter abzurufen:

```
aws opensearchserverless batch-get-collection --names books
```

Beispielantwort

```
{
    "collectionDetails": [
        {
            "id": "8kw362bpwg4gx9b2f6e0",
            "name": "books",
            "status": "ACTIVE",
```

```
            "type": "SEARCH",
            "description": "",
            "arn": "arn:aws:aoss:us-
east-1:123456789012:collection/8kw362bpwg4gx9b2f6e0",
            "createdDate": 1665765327107,
            "collectionEndpoint": "https://8kw362bpwg4gx9b2f6e0.us-
east-1.aoss.amazonaws.com",
            "dashboardEndpoint": "https://8kw362bpwg4gx9b2f6e0.us-
east-1.aoss.amazonaws.com/_dashboards"
        }
    ],
    "collectionErrorDetails": []
}
```

> **Note**
>
> Sie können den Sammlungsendpunkt erst sehen, wenn sich der Sammlungsstatus zu `ACTIVE` ändert. Möglicherweise müssen Sie mehrere Aufrufe durchführen, um den Status zu überprüfen, bis die Sammlung erfolgreich erstellt wurde.

8. Verwenden Sie ein HTTP-Tool wie Postman oder curl, um Daten in der Bücher-Sammlung zu indizieren. Wir erstellen einen Index mit dem Namen books-index und fügen ein einzelnes Dokument hinzu.

   Senden Sie die folgende Anforderung mit den Anmeldeinformationen für `TutorialRole` an den Sammlungsendpunkt, den Sie im vorherigen Schritt abgerufen haben.

   ```
   PUT https://8kw362bpwg4gx9b2f6e0.us-east-1.aoss.amazonaws.com/books-index/_doc/1
   {
     "title": "The Shining",
     "author": "Stephen King",
     "year": 1977
   }
   ```

   Beispielantwort

   ```
   {
     "_index" : "books-index",
     "_id" : "1",
     "_version" : 1,
     "result" : "created",
   ```

```
  "_shards" : {
    "total" : 0,
    "successful" : 0,
    "failed" : 0
  },
  "_seq_no" : 0,
  "_primary_term" : 0
}
```

9. Verwenden Sie die Such-API, um mit der Suche nach Daten in Ihrer Sammlung zu beginnen. Die folgende Abfrage führt eine einfache Suche durch:

```
GET https://8kw362bpwg4gx9b2f6e0.us-east-1.aoss.amazonaws.com/books-index/_search
```

Beispielantwort

```
{
    "took": 405,
    "timed_out": false,
    "_shards": {
        "total": 6,
        "successful": 6,
        "skipped": 0,
        "failed": 0
    },
    "hits": {
        "total": {
            "value": 2,
            "relation": "eq"
        },
        "max_score": 1.0,
        "hits": [
            {
                "_index": "books-index:0::3xJq14MBUaOS0wL26UU9:0",
                "_id": "F_bt4oMBLle5pYmm5q4T",
                "_score": 1.0,
                "_source": {
                    "title": "The Shining",
                    "author": "Stephen King",
                    "year": 1977
                }
            }
        ]
```

```
    }
}
```

Identity and Access Management für Amazon OpenSearch Serverless

AWS Identity and Access Management (IAM) ist ein AWS-Service, mit dem Administratoren den Zugriff auf AWS-Ressourcen sicher steuern können. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um serverlose Ressourcen zu verwenden. OpenSearch IAM ist ein AWS-Service, den Sie ohne zusätzliche Kosten verwenden können.

Themen

Identitätsbasierte Richtlinien für Serverless OpenSearch

Unterstützt Richtlinien auf Identitätsbasis.	Ja

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen,

unter denen Aktionen zugelassen oder abgelehnt werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für Serverless OpenSearch

Beispiele für identitätsbasierte Richtlinien OpenSearch ohne Server finden Sie unter. the section called “Beispiele für identitätsbasierte Richtlinien”

Richtlinienaktionen für Serverless OpenSearch

Unterstützt Richtlinienaktionen	Ja

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie die zugehörige AWS-API-Operation. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keine passende API-Operation gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Bei Richtlinienaktionen in OpenSearch Serverless wird vor der Aktion das folgende Präfix verwendet:

```
aoss
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [
      "aoss:action1",
      "aoss:action2"
         ]
```

Sie können mehrere Aktionen mit Platzhalterzeichen (*) angeben. Beispielsweise können Sie alle Aktionen festlegen, die mit dem Wort `Describe` beginnen, einschließlich der folgenden Aktion:

```
"Action": "aoss:List*"
```

Beispiele für identitätsbasierte OpenSearch Richtlinien ohne Server finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Serverless OpenSearch

Richtlinienressourcen für Serverless OpenSearch

Unterstützt Richtlinienressourcen	Ja

Administratoren können mithilfe von AWS-JSON-Richtlinien festlegen, wer zum Zugriff auf was berechtigt ist. Das bedeutet die Festlegung, welcher Prinzipal Aktionen für welche Ressourcen unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"
```

Schlüssel für Richtlinienbedingungen für Amazon OpenSearch Serverless

Unterstützt servicespezifische Richtlini enbedingungsschlüssel	Ja

Administratoren können mithilfe von AWS-JSON-Richtlinien festlegen, wer zum Zugriff auf was berechtigt ist. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte

Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen AND-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, wertet AWS die Bedingung mittels einer logischen OR-Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und servicespezifische Bedingungsschlüssel. Eine Liste aller globalen AWS-Bedingungsschlüssel finden Sie unter Globale AWS-Bedingungskontextschlüssel im IAM-Benutzerhandbuch.

Neben der attributebasierten Zugriffskontrolle (ABAC) unterstützt OpenSearch Serverless die folgenden Bedingungsschlüssel:

- `aoss:collection`
- `aoss:CollectionId`
- `aoss:index`

Sie können diese Bedingungsschlüssel auch beim Bereitstellen von Berechtigungen für Zugriffsrichtlinien und Sicherheitsrichtlinien verwenden. Beispiel:

```
[
   {
      "Effect":"Allow",
      "Action":[
         "aoss:CreateAccessPolicy",
         "aoss:CreateSecurityPolicy"
      ],
      "Resource":"*",
      "Condition":{
         "StringLike":{
            "aoss:collection":"log"
         }
```

```
      }
   }
]
```

In diesem Beispiel gilt die Bedingung für Richtlinien, die Regeln enthalten, die mit einem Sammlungsnamen oder -muster übereinstimmen. Die Bedingungen haben das folgende Verhalten:

- `StringEquals` – Gilt für Richtlinien mit Regeln, die die exakte Ressourcenzeichenfolge „log“ (d. h. `collection/log`) enthalten.
- `StringLike` – Gilt für Richtlinien mit Regeln, die eine Ressourcenzeichenfolge enthalten, die die Zeichenfolge „log“ enthält (d. h. `collection/log`, aber auch `collection/logs-application` oder `collection/applogs123`).

> **Note**
>
> Bedingungsschlüssel für Sammlungen gelten nicht auf der Indexebene. In der obigen Richtlinie würde die Bedingung beispielsweise nicht auf eine Zugriffs- oder Sicherheitsrichtlinie gelten, die die Ressourcenzeichenfolge `index/logs-application/*` enthält.

Eine Liste der OpenSearch Serverless-Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für Amazon OpenSearch Serverless in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von Amazon OpenSearch Serverless definierte Aktionen.

ABAC mit Serverless OpenSearch

Unterstützt ABAC (Tags in Richtlinien)	Ja

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In AWS werden diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und mehrere AWS-Ressourcen anfügen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, oder `aws:TagKeys`Bedingung verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter Was ist ABAC? im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Weitere Informationen zum Taggen von OpenSearch serverlosen Ressourcen finden Sie unter. the section called “Markieren von Sammlungen”

Temporäre Anmeldeinformationen mit Serverless verwenden OpenSearch

Unterstützt temporäre Anmeldeinformationen	Ja

Einige AWS-Services Featureieren nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, darunter welche AWS-Services mit temporären Anmeldeinformationen Featureieren, finden Sie unter AWS-Services, die mit IAM Featureieren im IAM-Benutzerhandbuch.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen Methode als einem Benutzernamen und einem Passwort bei der AWS Management Console anmelden. Wenn Sie beispielsweise über den Single Sign-On (SSO)-Link Ihres Unternehmens auf AWS zugreifen, erstellt dieser Prozess automatisch temporäre Anmeldeinformationen. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter Wechseln zu einer Rolle (Konsole) im IAM-Benutzerhandbuch.

Sie können mithilfe der AWS CLI- oder AWS-API manuell temporäre Anmeldeinformationen erstellen. Sie können dann diese temporären Anmeldeinformationen verwenden, um auf AWS zuzugreifen.

AWS empfiehlt, dass Sie temporäre Anmeldeinformationen dynamisch generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

Mit Diensten verknüpfte Rollen für Serverless OpenSearch

Unterstützt serviceverknüpfte Rollen	Ja

Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einem AWS-Service verknüpft ist. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem AWS-Konto angezeigt und gehören zum Service. Ein IAM-Administrator kann die Berechtigungen für serviceverbundene Rollen anzeigen, aber nicht bearbeiten.

Einzelheiten zum Erstellen und Verwalten OpenSearch serverloser dienstbezogener Rollen finden Sie unter. the section called “Rolle bei der Sammlungserstellung”

Beispiele für identitätsbasierte Richtlinien für Serverless OpenSearch

Standardmäßig sind Benutzer und Rollen nicht berechtigt, serverlose Ressourcen zu erstellen oder zu ändern OpenSearch . Sie können auch keine Aufgaben über die AWS Management Console, die AWS Command Line Interface (AWS CLI) oder die AWS-API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Einzelheiten zu den von Amazon OpenSearch Serverless definierten Aktionen und Ressourcentypen, einschließlich des Formats der ARNs für jeden Ressourcentyp, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon OpenSearch Serverless in der Service Authorization Reference.

Themen

- Bewährte Methoden für Richtlinien

- OpenSearch Serverless in der Konsole verwenden
- Verwaltung serverloser Sammlungen OpenSearch
- Serverlose Sammlungen anzeigen OpenSearch
- Verwendung von OpenSearch API-Vorgängen

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien sind sehr leistungsfähig. Sie bestimmen, ob jemand OpenSearch serverlose Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

Identitätsbasierte Richtlinien legen fest, ob jemand OpenSearch serverlose Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Erste Schritte mit AWS-verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen – Um Ihren Benutzern und Workloads Berechtigungen zu gewähren, verwenden Sie die AWS-verwaltete Richtlinien die Berechtigungen für viele allgemeine Anwendungsfälle gewähren. Sie sind in Ihrem AWS-Konto verfügbar. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie AWS-kundenverwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS-verwaltete Richtlinien oder AWS-verwaltete Richtlinien für Auftragsfunktionen im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können

auch Bedingungen verwenden, um Zugriff auf Service-Aktionen zu gewähren, wenn diese durch ein bestimmtes AWS-Service, wie beispielsweise AWS CloudFormation, verwendet werden. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.

- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung zum IAM Access Analyzer im IAM-Benutzerhandbuch.
- Bedarf einer Multi-Faktor-Authentifizierung (MFA) – Wenn Sie ein Szenario haben, das IAM-Benutzer oder Root-Benutzer in Ihrem AWS-Konto erfordert, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Konfigurieren eines MFA-geschützten API-Zugriffs im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

OpenSearch Serverless in der Konsole verwenden

Um über die OpenSearch Servicekonsole auf OpenSearch Serverless zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den OpenSearch Serverless-Ressourcen in Ihrem AWS Konto aufzulisten und einzusehen. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (wie IAM-Rollen) mit dieser Richtlinie.

Für Benutzer, die nur Aufrufe an die AWS CLI oder AWS-API durchführen, müssen Sie keine Mindestberechtigungen in der Konsole erteilen. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die Sie ausführen möchten.

Die folgende Richtlinie ermöglicht einem Benutzer den Zugriff auf OpenSearch Serverless innerhalb der OpenSearch Servicekonsole:

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Resource": "*",
            "Effect": "Allow",
            "Action": [
                "aoss:ListCollections",
                "aoss:BatchGetCollection",
                "aoss:ListAccessPolicies",
                "aoss:ListSecurityConfigs",
                "aoss:ListSecurityPolicies",
                "aoss:ListTagsForResource",
                "aoss:ListVpcEndpoints",
                "aoss:GetAccessPolicy",
                "aoss:GetAccountSettings",
                "aoss:GetSecurityConfig",
                "aoss:GetSecurityPolicy"
            ]
        }
    ]
}
```

Verwaltung serverloser Sammlungen OpenSearch

Diese Richtlinie ist ein Beispiel für eine „Sammlungsadministrator“ -Richtlinie, die es einem Benutzer ermöglicht, Amazon OpenSearch Serverless-Sammlungen zu verwalten und zu verwalten. Der Benutzer kann Sammlungen erstellen, anzeigen und löschen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Resource": "arn:aws:aoss:region:123456789012:collection/*",
            "Action": [
                "aoss:CreateCollection",
                "aoss:DeleteCollection",
                "aoss:UpdateCollection"
            ],
            "Effect": "Allow"
        },
        {
            "Resource": "*",
            "Action": [
```

```
                "aoss:BatchGetCollection",
                "aoss:ListCollections",
                "aoss:CreateAccessPolicy",
                "aoss:CreateSecurityPolicy"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Serverlose Sammlungen anzeigen OpenSearch

Diese Beispielrichtlinie ermöglicht es einem Benutzer, Details für alle Amazon OpenSearch Serverless-Sammlungen in seinem Konto einzusehen. Der Benutzer kann die Sammlungen oder die zugeordneten Sicherheitsrichtlinien nicht ändern.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Resource": "*",
            "Action": [
                "aoss:ListAccessPolicies",
                "aoss:ListCollections",
                "aoss:ListSecurityPolicies",
                "aoss:ListTagsForResource",
                "aoss:BatchGetCollection"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Verwendung von OpenSearch API-Vorgängen

API-Operationen auf Datenebene bestehen aus den Funktionen, die Sie in OpenSearch Serverless verwenden, um Echtzeitwerte aus dem Dienst abzuleiten. API-Operationen auf der Kontrollebene bestehen aus den Funktionen, mit denen Sie die Umgebung einrichten.

Um vom Browser aus auf Amazon OpenSearch Serverless Data Plane APIs und OpenSearch Dashboards zuzugreifen, müssen Sie zwei IAM-Berechtigungen für Sammelressourcen hinzufügen. Diese Berechtigungen sind und. `aoss:APIAccessAll` `aoss:DashboardsAccessAll`

> **Note**
>
> Ab dem 10. Mai 2023 benötigt OpenSearch Serverless diese beiden neuen IAM-Berechtigungen für Sammlungsressourcen. Die `aoss:APIAccessAll` Berechtigung ermöglicht den Zugriff auf die Datenebene, und die `aoss:DashboardsAccessAll` Berechtigung ermöglicht OpenSearch Dashboards vom Browser aus. Wenn die beiden neuen IAM-Berechtigungen nicht hinzugefügt werden, wird ein 403-Fehler angezeigt.

Diese Beispielrichtlinie ermöglicht es einem Benutzer, auf Datenebenen-APIs für eine bestimmte Sammlung in seinem Konto zuzugreifen und auf OpenSearch Dashboards für alle Sammlungen in seinem Konto zuzugreifen.

```
{
    "Version": "2012-10-17",
    "Statement": [
         {
            "Effect": "Allow",
            "Action": "aoss:APIAccessAll",
            "Resource": "arn:aws:aoss:region:account-id:collection/collection-id"
        },
        {
            "Effect": "Allow",
            "Action": "aoss:DashboardsAccessAll",
            "Resource": "arn:aws:aoss:region:account-id:dashboards/default"
        }
    ]
}
```

Beides `aoss:APIAccessAll` und `aoss:DashboardsAccessAll` gewährt volle IAM-Berechtigungen für die Sammlungsressourcen, während die Dashboard-Berechtigung auch Zugriff auf Dashboards gewährt OpenSearch . Jede Berechtigung funktioniert unabhängig voneinander, sodass eine ausdrückliche Verweigerung `aoss:APIAccessAll` nicht den `aoss:DashboardsAccessAll` Zugriff auf die Ressourcen, einschließlich der Entwicklungstools, blockiert. Das Gleiche gilt für die Option „Ablehnen`aoss:DashboardsAccessAll`“.

OpenSearch Serverless unterstützt nur die Quell-IP-Adresse in der Bedingungseinstellung in der IAM-Richtlinie des Prinzipals für Aufrufe auf Datenebene:

```
"Condition": {
```

```
    "IpAddress": {
         "aws:SourceIp": "52.95.4.14"
    }
}
```

Verschlüsselung in Amazon OpenSearch Serverless

Verschlüsselung im Ruhezustand

Jede Amazon OpenSearch Serverless-Sammlung, die Sie erstellen, ist durch Verschlüsselung ruhender Daten geschützt. Diese Sicherheitsfunktion verhindert unbefugten Zugriff auf Ihre Daten. Encryption at Rest verwendet AWS Key Management Service (AWS KMS), um Ihre Verschlüsselungsschlüssel zu speichern und zu verwalten. Es verwendet den Advanced-Encryption-Standard-Algorithmus mit 256-Bit-Schlüsseln (AES-256) zur Durchführung der Verschlüsselung.

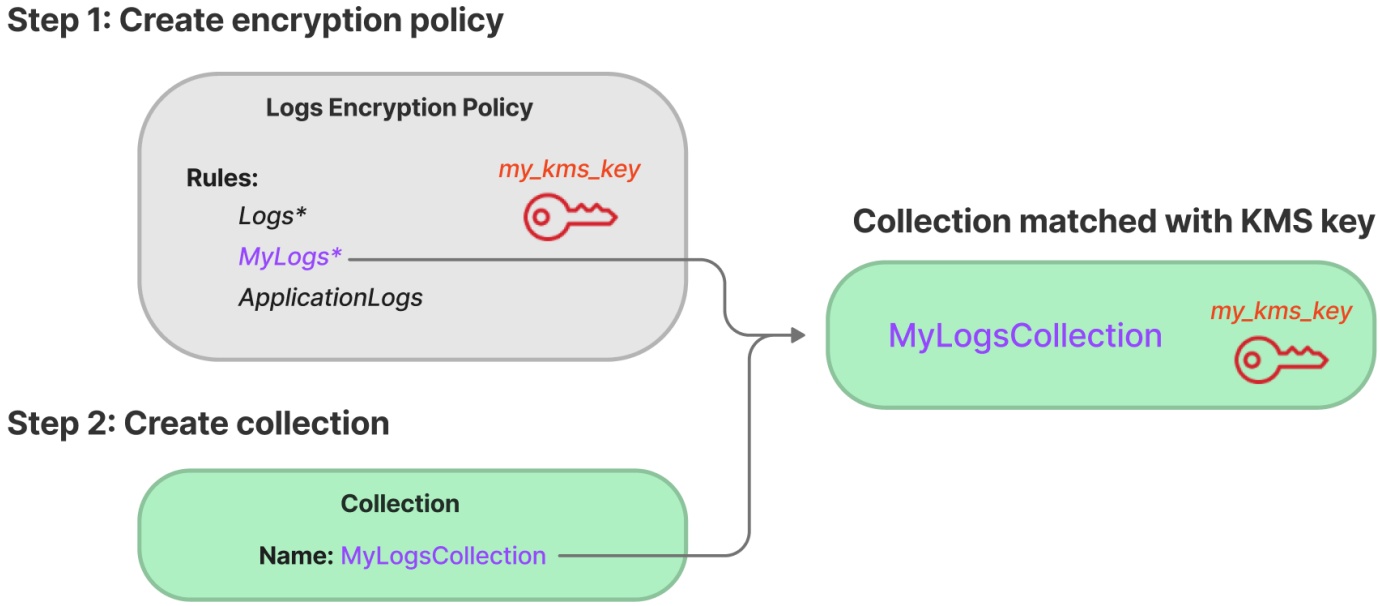
Themen

Verschlüsselungsrichtlinien

Mit Verschlüsselungsrichtlinien können Sie viele Sammlungen in großem Umfang verwalten. Dazu weisen Sie neu erstellten Sammlungen, die einem bestimmten Namen oder Muster entsprechen, automatisch einen Verschlüsselungsschlüssel zu.

Wenn Sie eine Verschlüsselungsrichtlinie erstellen, können Sie entweder ein Präfix angeben, bei dem es sich um eine auf Platzhaltern basierende Abgleichregel wie `MyCollection*` handelt, oder einen einzelnen Sammlungsnamen eingeben. Wenn Sie dann eine Sammlung erstellen, die mit

diesem Namen oder Präfixmuster übereinstimmt, werden ihr automatisch die Richtlinie und der entsprechende KMS-Schlüssel zugewiesen.



Verschlüsselungsrichtlinien unterstützen die folgenden Elemente:

- `Rules` – eine oder mehrere Regeln für den Sammlungsabgleich, jeweils mit den folgenden Unterelementen:
  - `ResourceType` – Derzeit ist die einzige Option „Sammlung“. Verschlüsselungsrichtlinien gelten nur für Sammlungsressourcen.
  - `Resource` – Ein oder mehrere Sammlungsnamen oder Muster, auf die die Richtlinie angewendet wird, im Format `collection/<collection name|pattern>`.
- `AWSOwnedKey` – Ob ein AWS-eigener Schlüssel verwendet werden soll.
- `KmsARN` – Wenn Sie `AWSOwnedKey` auf „falsch“ festlegen, geben Sie den Amazon-Ressourcennamen (ARN) des KMS-Schlüssels an, mit dem die zugehörigen Sammlungen verschlüsselt werden sollen. Wenn Sie diesen Parameter angeben, ignoriert OpenSearch Serverless den `AWSOwnedKey` Parameter.

Die folgende Beispielrichtlinie weist jeder zukünftigen Sammlung mit dem Namen `autopartsinventory` sowie Sammlungen, die mit dem Begriff „Vertrieb“ beginnen, einen vom Kunden verwalteten Schlüssel zu:

```
{
   "Rules":[
```

```
      {
         "ResourceType":"collection",
         "Resource":[
            "collection/autopartsinventory",
            "collection/sales*"
         ]
      }
   ],
   "AWSOwnedKey":false,
   "KmsARN":"arn:aws:encryption:us-east-1:123456789012:key/93fd6da4-a317-4c17-
bfe9-382b5d988b36"
}
```

Selbst wenn eine Richtlinie mit einem Sammlungsnamen übereinstimmt, können Sie diese automatische Zuweisung während der Sammlungserstellung außer Kraft setzen, wenn das Ressourcenmuster einen Platzhalter (*) enthält. Wenn Sie sich dafür entscheiden, die automatische Schlüsselzuweisung außer Kraft zu setzen, erstellt OpenSearch Serverless für Sie eine Verschlüsselungsrichtlinie mit dem Namen auto-< ***collection-name*** > und hängt sie der Sammlung an. Die Richtlinie gilt zunächst nur für eine einzelne Sammlung, Sie können sie jedoch ändern, um weitere Sammlungen einzubeziehen.

Wenn Sie Richtlinienregeln so ändern, dass sie nicht mehr mit einer Sammlung übereinstimmen, wird die Zuweisung des zugeordneten KMS-Schlüssels zu dieser Sammlung nicht aufgehoben. Die Sammlung bleibt immer mit ihrem ursprünglichen Verschlüsselungsschlüssel verschlüsselt. Wenn Sie den Verschlüsselungsschlüssel für eine Sammlung ändern möchten, müssen Sie die Sammlung neu erstellen.

Wenn Regeln aus mehreren Richtlinien mit einer Sammlung übereinstimmen, wird die spezifischere Regel verwendet. Wenn beispielsweise eine Richtlinie eine Regel für `collection/log*` und eine andere für `collection/logSpecial` enthält, wird der Verschlüsselungsschlüssel für die zweite Richtlinie verwendet, da dieser spezifischer ist.

Sie können in einer Richtlinie keinen Namen oder ein Präfix verwenden, wenn es bereits in einer anderen Richtlinie vorhanden ist. OpenSearch Serverless zeigt einen Fehler an, wenn Sie versuchen, identische Ressourcenmuster in verschiedenen Verschlüsselungsrichtlinien zu konfigurieren.

Überlegungen

Berücksichtigen Sie Folgendes, wenn Sie die Verschlüsselung für Ihre Sammlungen konfigurieren:

- Die Verschlüsselung im Ruhezustand ist für alle Serverless-Sammlungen erforderlich.

- Sie haben die Möglichkeit, einen vom Kunden verwalteten Schlüssel oder ein AWS-eigener Schlüssel zu verwenden. Wenn Sie sich für einen vom Kunden verwalteten Schlüssel entscheiden, empfehlen wir Ihnen, die automatische Schlüsselrotation zu aktivieren.
- Sie können den Verschlüsselungsschlüssel für eine Sammlung nicht ändern, nachdem die Sammlung erstellt wurde. Wählen Sie sorgfältig aus, welche Sie verwenden AWS KMS möchten, wenn Sie zum ersten Mal eine Sammlung einrichten.
- Eine Sammlung kann nur mit einer einzigen Verschlüsselungsrichtlinie übereinstimmen.
- Sammlungen mit eindeutigen KMS-Schlüsseln können OpenSearch Recheneinheiten (OCUs) nicht mit anderen Sammlungen gemeinsam nutzen. Jede Sammlung mit einem eindeutigen Schlüssel erfordert ihre eigenen 4 OCUs.
- Wenn Sie den KMS-Schlüssel in einer Verschlüsselungsrichtlinie aktualisieren, hat die Änderung keine Auswirkungen auf bestehende übereinstimmende Sammlungen mit bereits zugewiesenen KMS-Schlüsseln.
- OpenSearch Serverless überprüft die Benutzerberechtigungen für vom Kunden verwaltete Schlüssel nicht explizit. Wenn ein Benutzer über die Berechtigung verfügt, über eine Datenzugriffsrichtlinie auf eine Sammlung zuzugreifen, kann er die mit dem zugehörigen Schlüssel verschlüsselten Daten aufnehmen und abfragen.

Erforderliche Berechtigungen

Die Verschlüsselung im Ruhezustand für OpenSearch Serverless verwendet die folgenden AWS Identity and Access Management (IAM-) Berechtigungen. Sie können IAM-Bedingungen festlegen, um Benutzer auf bestimmte Sammlungen zu beschränken.

- `aoss:CreateSecurityPolicy` – Erstellt eine Verschlüsselungsrichtlinie.
- `aoss:ListSecurityPolicies` – Listet alle Verschlüsselungsrichtlinien und Sammlungen auf, denen diese angefügt sind.
- `aoss:GetSecurityPolicy` – Zeigt Details zu einer bestimmten Verschlüsselungsrichtlinie an.
- `aoss:UpdateSecurityPolicy` – Erstellt eine Verschlüsselungsrichtlinie.
- `aoss:DeleteSecurityPolicy` – Löscht eine Verschlüsselungsrichtlinie.

Das folgende Beispiel für eine identitätsbasierte Zugriffsrichtlinie stellt die Mindestberechtigungen bereit, die ein Benutzer zum Verwalten von Verschlüsselungsrichtlinien mit dem Ressourcenmuster `collection/application-logs` benötigt.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "aoss:CreateSecurityPolicy",
            "aoss:UpdateSecurityPolicy",
            "aoss:DeleteSecurityPolicy",
            "aoss:GetSecurityPolicy"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "aoss:collection":"application-logs"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":[
            "aoss:ListSecurityPolicies"
         ],
         "Resource":"*"
      }
   ]
}
```

Schlüsselrichtlinie für einen kundenverwalteten Schlüssel

Wenn Sie einen vom Kunden verwalteten Schlüssel zum Schutz einer Sammlung auswählen, erhält OpenSearch Serverless die Erlaubnis, den KMS-Schlüssel im Namen des Prinzipals zu verwenden, der die Auswahl trifft. Dieser Prinzipal, ein Benutzer oder eine Rolle, muss über die für OpenSearch Serverless erforderlichen Berechtigungen für den KMS-Schlüssel verfügen. Sie können diese Berechtigungen in einer Schlüsselrichtlinie oder einer IAM-Richtlinie bereitstellen.

OpenSearch Serverless benötigt mindestens die folgenden Berechtigungen für einen vom Kunden verwalteten Schlüssel:

- km: DescribeKey
- km: CreateGrant

Beispielsweise:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:DescribeKey",
        "kms:CreateGrant"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "kms:ViaService": "aoss.us-east-1.amazonaws.com"
        },
        "Bool": {
          "kms:GrantIsForAWSResource": "true"
        }
      }
    }
  ]
}
```

OpenSearch Serverless erstellt einen Grant mit den Berechtigungen kms: GenerateDataKey und kms:Decrypt.

Weitere Informationen finden Sie unter Verwenden von Schlüsselrichtlinien in AWS KMS im Entwicklerhandbuch für AWS Key Management Service .

So verwendet Serverless Grants in OpenSearch AWS KMS

OpenSearch Für Serverless ist ein Zuschuss erforderlich, um einen vom Kunden verwalteten Schlüssel verwenden zu können.

Wenn Sie in Ihrem Konto eine Verschlüsselungsrichtlinie mit einem neuen Schlüssel erstellen, erstellt OpenSearch Serverless in Ihrem Namen einen Zuschuss, indem es eine CreateGrantAnfrage an sendet. AWS KMS Grants in AWS KMS werden verwendet, um OpenSearch serverlosen Zugriff auf einen KMS-Schlüssel in einem Kundenkonto zu gewähren.

OpenSearch Serverless setzt voraus, dass der Zuschuss Ihren vom Kunden verwalteten Schlüssel für die folgenden internen Operationen verwenden kann:

- Senden Sie DescribeKeyAnfragen an, AWS KMS um zu überprüfen, ob die angegebene symmetrische, vom Kunden verwaltete Schlüssel-ID gültig ist.
- Senden Sie GenerateDataKeyAnfragen an den KMS-Schlüssel, um Datenschlüssel zu erstellen, mit denen Objekte verschlüsselt werden können.
- Senden Sie Entschlüsselungsanforderungen an AWS KMS , um die verschlüsselten Datenschlüssel zu entschlüsseln, sodass sie zum Verschlüsseln Ihrer Daten verwendet werden können.

Sie können den Zugriff auf die Genehmigung jederzeit widerrufen oder den Zugriff des Services auf den vom Kunden verwalteten Schlüssel entfernen. Wenn Sie dies tun, kann OpenSearch Serverless auf keine der mit dem vom Kunden verwalteten Schlüssel verschlüsselten Daten zugreifen. Dies wirkt sich auf alle Vorgänge aus, die von diesen Daten abhängig sind, was zu `AccessDeniedException` Fehlern und Ausfällen in den asynchronen Workflows führt.

OpenSearch Serverless zieht Zuschüsse in einem asynchronen Workflow zurück, wenn ein bestimmter vom Kunden verwalteter Schlüssel keinen Sicherheitsrichtlinien oder Sammlungen zugeordnet ist.

Erstellen von Verschlüsselungsrichtlinien (Konsole)

In einer Verschlüsselungsrichtlinie geben Sie einen KMS-Schlüssel und eine Reihe von Erfassungsmustern an, auf die die Richtlinie angewendet wird. Allen neuen Sammlungen, die mit einem der in der Richtlinie definierten Muster übereinstimmen, wird beim Erstellen der Sammlung der entsprechende KMS-Schlüssel zugewiesen. Wir empfehlen Ihnen, Verschlüsselungsrichtlinien zu erstellen, bevor Sie mit dem Erstellen von Sammlungen beginnen.

Um eine Richtlinie für serverlose Verschlüsselung zu erstellen OpenSearch

1. Öffnen Sie die Amazon OpenSearch Service-Konsole unter https://console.aws.amazon.com/aos/home.
2. Erweitern Sie im linken Navigationsbereich Serverless und wählen Sie Encryption policies (Verschlüsselungsrichtlinien) aus.
3. Wählen Sie Create encryption policy (Verschlüsselungsrichtlinie erstellen).
4. Geben Sie einen Namen und eine Beschreibung für die Richtlinie an.
5. Geben Sie unter Resources (Ressourcen) ein oder mehrere Ressourcenmuster für diese Verschlüsselungsrichtlinie ein. Alle neu erstellten Sammlungen im aktuellen AWS-Konto und in der aktuellen Region, die mit einem der Muster übereinstimmen, werden dieser Richtlinie

automatisch zugewiesen. Wenn Sie beispielsweise `ApplicationLogs` (ohne Platzhalter) eingeben und später eine Sammlung mit diesem Namen erstellen, werden die Richtlinie und der entsprechende KMS-Schlüssel dieser Sammlung zugewiesen.

Sie können auch ein Präfix wie `Logs*` angeben, das die Richtlinie allen neuen Sammlungen zuweist, deren Namen mit `Logs` beginnen. Durch die Verwendung von Platzhaltern können Sie die Verschlüsselungseinstellungen für mehrere Sammlungen in großem Umfang verwalten.

6. Wählen Sie unter Encryption (Verschlüsselung) einen zu verwendenden KMS-Schlüssel aus.
7. Wählen Sie Erstellen.

Nächster Schritt: Erstellen von Sammlungen

Nachdem Sie eine oder mehrere Verschlüsselungsrichtlinien konfiguriert haben, können Sie mit der Erstellung von Sammlungen beginnen, die den in diesen Richtlinien definierten Regeln entsprechen. Anweisungen finden Sie unter the section called “Erstellen von Sammlungen”.

Im Schritt Verschlüsselungen bei der Erstellung der Sammlung informiert Sie OpenSearch Serverless darüber, dass der von Ihnen eingegebene Name dem in einer Verschlüsselungsrichtlinie definierten Muster entspricht, und weist der Sammlung automatisch den entsprechenden KMS-Schlüssel zu. Wenn das Ressourcenmuster einen Platzhalter (*) enthält, können Sie die Übereinstimmung überschreiben und Ihren eigenen Schlüssel auswählen.

Erstellen von Verschlüsselungsrichtlinien (AWS CLI)

Um mithilfe der OpenSearch serverlosen API-Operationen eine Verschlüsselungsrichtlinie zu erstellen, geben Sie Ressourcenmuster und einen Verschlüsselungsschlüssel im JSON-Format an. Die CreateSecurityPolicyAnfrage akzeptiert sowohl Inline-Richtlinien als auch JSON-Dateien.

Verschlüsselungsrichtlinien haben folgendes Format. Diese Beispieldatei `my-policy.json` stimmt mit jeder zukünftigen Sammlung mit dem Namen `autopartsinventory` überein, ebenso wie mit allen Sammlungen, deren Namen mit `sales` beginnen.

```
{
   "Rules":[
      {
         "ResourceType":"collection",
         "Resource":[
            "collection/autopartsinventory",
            "collection/sales*"
```

```
         ]
      }
   ],
   "AWSOwnedKey":false,
   "KmsARN":"arn:aws:encryption:us-east-1:123456789012:key/93fd6da4-a317-4c17-
bfe9-382b5d988b36"
}
```

Um einen Service-eigenen Schlüssel zu verwenden, legen Sie `AWSOwnedKey` auf `true` fest:

```
{
   "Rules":[
      {
         "ResourceType":"collection",
         "Resource":[
            "collection/autopartsinventory",
            "collection/sales*"
         ]
      }
   ],
   "AWSOwnedKey":true
}
```

Die folgende Anfrage erstellt die Verschlüsselungsrichtlinie:

```
aws opensearchserverless create-security-policy \
    --name sales-inventory \
    --type encryption \
    --policy file://my-policy.json
```

Verwenden Sie dann den CreateCollectionAPI-Vorgang, um eine oder mehrere Sammlungen zu erstellen, die einem der Ressourcenmuster entsprechen.

Anzeigen von Verschlüsselungsrichtlinien

Bevor Sie eine Sammlung erstellen, möchten Sie möglicherweise eine Vorschau der vorhandenen Verschlüsselungsrichtlinien in Ihrem Konto anzeigen, um zu sehen, welche ein Ressourcenmuster hat, das mit dem Namen Ihrer Sammlung übereinstimmt. In der folgenden ListSecurityPoliciesAnfrage werden alle Verschlüsselungsrichtlinien in Ihrem Konto aufgeführt:

```
aws opensearchserverless list-security-policies --type encryption
```

Die Anfrage gibt Informationen über alle konfigurierten Verschlüsselungsrichtlinien zurück. Verwenden Sie den Inhalt des `policy`-Elements, um die Musterregeln anzuzeigen, die in der Richtlinie definiert sind:

```
{
   "securityPolicyDetails": [
      {
         "createdDate": 1663693217826,
         "description": "Sample encryption policy",
         "lastModifiedDate": 1663693217826,
         "name": "my-policy",
         "policy": "{\"Rules\":[{\"ResourceType\":\"collection\",\"Resource\":
[\"collection/autopartsinventory\",\"collection/sales*\"]}],\"AWSOwnedKey\":true}",
         "policyVersion": "MTY2MzY5MzIxNzgyNl8x",
         "type": "encryption"
      }
   ]
}
```

Verwenden Sie den GetSecurityPolicyBefehl, um detaillierte Informationen zu einer bestimmten Richtlinie, einschließlich des KMS-Schlüssels, anzuzeigen.

Aktualisieren von Verschlüsselungsrichtlinien

Wenn Sie den KMS-Schlüssel in einer Verschlüsselungsrichtlinie aktualisieren, gilt die Änderung nur für neu erstellte Sammlungen, die mit dem konfigurierten Namen oder Muster übereinstimmen. Bestehende Sammlungen, denen bereits KMS-Schlüssel zugewiesen sind, sind davon nicht betroffen.

Dasselbe gilt für Regeln zum Richtlinienabgleich. Wenn Sie eine Regel hinzufügen, ändern oder löschen, gilt die Änderung nur für neu erstellte Sammlungen. Vorhandene Sammlungen verlieren ihren zugewiesenen KMS-Schlüssel nicht, wenn Sie die Regeln einer Richtlinie so ändern, dass sie nicht mehr mit dem Namen einer Sammlung übereinstimmen.

Um eine Verschlüsselungsrichtlinie in der OpenSearch Serverless-Konsole zu aktualisieren, wählen Sie Verschlüsselungsrichtlinien, wählen Sie die zu ändernde Richtlinie aus und klicken Sie auf Bearbeiten. Nehmen Sie Ihre Änderungen vor und wählen Sie Save (Speichern).

Verwenden Sie den Vorgang, um eine Verschlüsselungsrichtlinie mithilfe der OpenSearch Serverless API zu aktualisieren. UpdateSecurityPolicy Die folgende Anfrage aktualisiert eine Verschlüsselungsrichtlinie mit einem neuen Richtlinien-JSON-Dokument:

```
aws opensearchserverless update-security-policy \
    --name sales-inventory \
    --type encryption \
    --policy-version 2 \
    --policy file://my-new-policy.json
```

Aktualisieren von Verschlüsselungsrichtlinien

Wenn Sie eine Verschlüsselungsrichtlinie löschen, sind alle Sammlungen, die derzeit den in der Richtlinie definierten KMS-Schlüssel verwenden, nicht betroffen. Um eine Richtlinie in der OpenSearch Serverless-Konsole zu löschen, wählen Sie die Richtlinie aus und klicken Sie auf Löschen.

Sie können auch den DeleteSecurityPolicyVorgang verwenden:

```
aws opensearchserverless delete-security-policy --name my-policy --type encryption
```

Verschlüsselung während der Übertragung

In OpenSearch Serverless werden alle Pfade in einer Sammlung während der Übertragung mithilfe von Transport Layer Security 1.2 (TLS) mit einer dem Industriestandard entsprechenden AES-256-Verschlüsselung verschlüsselt. Der Zugriff auf alle APIs und Dashboards für Opensearch erfolgt ebenfalls über TLS 1.2. TLS ist eine Reihe von branchenüblichen kryptografischen Protokollen, die zur Verschlüsselung von Informationen verwendet werden, die über das Netzwerk ausgetauscht werden.

Netzwerkzugriff für Amazon OpenSearch Serverless

Die Netzwerkeinstellungen für eine Amazon OpenSearch Serverless-Sammlung bestimmen, ob auf die Sammlung über das Internet von öffentlichen Netzwerken aus zugegriffen werden kann oder ob privat darauf zugegriffen werden muss.

Der private Zugriff kann für eine oder beide der folgenden Bedingungen gelten:

- OpenSearch Serverlos verwaltete VPC-Endpunkte
- Unterstützt AWS-Services wie Amazon Bedrock

Sie können den Netzwerkzugriff für den Endpunkt einer Sammlung und den entsprechenden OpenSearchOpenSearch Dashboard-Endpunkt separat konfigurieren.

Der Netzwerkzugriff ist der Isolationsmechanismus, mit dem Sie den Zugriff aus verschiedenen Quellnetzwerken ermöglichen können. Wenn beispielsweise der OpenSearch Dashboard-Endpunkt einer Sammlung öffentlich zugänglich ist, der OpenSearch API-Endpunkt jedoch nicht, kann ein Benutzer nur über Dashboards auf die Sammlungsdaten zugreifen, wenn er von einem öffentlichen Netzwerk aus eine Verbindung herstellt. Wenn sie versuchen, die OpenSearch APIs direkt von einem öffentlichen Netzwerk aus aufzurufen, werden sie blockiert. Die Netzwerkeinstellungen können für solche Permutationen von Quelle zu Ressource-Typ verwendet werden. Amazon OpenSearch Serverless unterstützt sowohl IPv4- als auch IPv6-Konnektivität.

Themen

Netzwerkrichtlinien

Mit Netzwerkrichtlinien können Sie viele Sammlungen in großem Umfang verwalten, indem Sie Sammlungen, die den in der Richtlinie definierten Regeln entsprechen, automatisch Netzwerkzugriffseinstellungen zuweisen.

In einer Netzwerkrichtlinie legen Sie eine Reihe von Regeln fest. Diese Regeln definieren Zugriffsberechtigungen für Sammelendpunkte und Dashboard-Endpunkte. OpenSearch Jede Regel besteht aus einem Zugriffstyp (öffentlich oder privat) und einem Ressourcentyp (Sammlungs- und/oder OpenSearch Dashboard-Endpunkt). Für jeden Ressourcentyp (`collection` and `dashboard`) legen Sie eine Reihe von Regeln fest, die definieren, für welche Sammlungen die Richtlinie gilt.

In dieser Beispielrichtlinie spezifiziert die erste Regel den VPC-Endpunktzugriff sowohl auf den Sammlungsendpunkt als auch auf den Dashboards-Endpunkt für alle Sammlungen, die mit dem Begriff beginnen. `marketing*` Es spezifiziert auch den Zugriff auf Amazon Bedrock.

> **Note**
>
> Der private Zugriff auf AWS-Services z. B. Amazon Bedrock gilt nur für den Endpunkt der Sammlung, nicht für den OpenSearch Endpunkt der OpenSearch Dashboards. Selbst wenn dies der Fall `ResourceType` ist`dashboard`, AWS-Services kann kein Zugriff auf Dashboards gewährt werden. OpenSearch

Die zweite Regel legt den öffentlichen Zugriff auf die `finance`-Sammlung fest, jedoch nur für den Sammlungsendpunkt (kein Zugriff auf Dashboards).

```
[
   {
      "Description":"Marketing access",
      "Rules":[
         {
            "ResourceType":"collection",
            "Resource":[
               "collection/marketing*"
            ]
         },
         {
            "ResourceType":"dashboard",
            "Resource":[
               "collection/marketing*"
            ]
         }
      ],
      "AllowFromPublic":false,
      "SourceVPCEs":[
         "vpce-050f79086ee71ac05"
      ],
      "SourceServices":[
         "bedrock.amazonaws.com"
      ],
   },
   {
      "Description":"Sales access",
      "Rules":[
         {
            "ResourceType":"collection",
            "Resource":[
```

```
                "collection/finance"
            ]
         }
      ],
      "AllowFromPublic":true
   }
]
```

Diese Richtlinie gewährt der Öffentlichkeit nur Zugriff auf OpenSearch Dashboards für Sammlungen, die mit „Finanzen“ beginnen. Alle Versuche, direkt auf die OpenSearch API zuzugreifen, schlagen fehl.

```
[
  {
    "Description": "Dashboards access",
    "Rules": [
      {
        "ResourceType": "dashboard",
        "Resource": [
          "collection/finance*"
        ]
      }
    ],
    "AllowFromPublic": true
  }
]
```

Netzwerkrichtlinien können sowohl für bestehende Sammlungen als auch für zukünftige Sammlungen gelten. Sie können beispielsweise eine Sammlung erstellen und dann eine Netzwerkrichtlinie mit einer Regel erstellen, die dem Sammlungsnamen entspricht. Vor dem Erstellen von Sammlungen müssen Sie keine Netzwerkrichtlinien erstellen.

Überlegungen

Berücksichtigen Sie Folgendes, wenn Sie den Netzwerkzugriff für Ihre Sammlungen konfigurieren:

- Wenn Sie den VPC-Endpunktzugriff für eine Sammlung konfigurieren möchten, müssen Sie zunächst mindestens einen OpenSearch serverlos verwalteten VPC-Endpunkt erstellen.
- Der private Zugriff auf gilt AWS-Services nur für den Endpunkt der Sammlung, nicht für den OpenSearch Dashboard-Endpunkt. OpenSearch Selbst wenn dies der Fall `ResourceType` ist`dashboard`, AWS-Services kann kein Zugriff auf OpenSearch Dashboards gewährt werden.

- Wenn eine Sammlung von öffentlichen Netzwerken aus zugänglich ist, ist sie auch von allen OpenSearch serverlos verwalteten VPC-Endpunkten und allen zugänglich. AWS-Services
- Für eine einzelne Sammlung können mehrere Netzwerkrichtlinien gelten. Weitere Informationen finden Sie unter the section called “Vorrang der Richtlinie”.

Für die Konfiguration von Netzwerkrichtlinien sind Berechtigungen erforderlich

Der Netzwerkzugriff für OpenSearch Serverless verwendet die folgenden AWS Identity and Access Management (IAM-) Berechtigungen. Sie können IAM-Bedingungen festlegen, um Benutzer auf Netzwerkrichtlinien zu beschränken, die bestimmten Sammlungen zugeordnet sind.

- `aoss:CreateSecurityPolicy` – Erstellt eine Netzwerkzugriffsrichtlinie.
- `aoss:ListSecurityPolicies` – Listet alle Netzwerkrichtlinien im aktuellen Konto auf.
- `aoss:GetSecurityPolicy` – Zeigt die Spezifikation einer Netzwerkzugriffsrichtlinie an.
- `aoss:UpdateSecurityPolicy` – Ändert eine bestimmte Netzwerkzugriffsrichtlinie und ändert die VPC-ID oder die Bezeichnung für den öffentlichen Zugriff.
- `aoss:DeleteSecurityPolicy` – Löscht eine Netzwerkzugriffsrichtlinie (nachdem sie von allen Sammlungen getrennt wurde).

Die folgende identitätsbasierte Zugriffsrichtlinie ermöglicht es einem Benutzer, alle Netzwerkrichtlinien anzuzeigen und Richtlinien mit dem Ressourcenmuster `collection/application-logs` zu aktualisieren:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "aoss:UpdateSecurityPolicy"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aoss:collection": "application-logs"
                }
            }
        },
```

```
        {
            "Effect": "Allow",
            "Action": [
                "aoss:ListSecurityPolicies",
                "aoss:GetSecurityPolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

> **Note**
>
> Darüber hinaus benötigt OpenSearch Serverless die `aoss:DashboardsAccessAll` Berechtigungen `aoss:APIAccessAll` und für die Erfassung von Ressourcen. Weitere Informationen finden Sie unter the section called “Verwendung von OpenSearch API-Vorgängen”.

Vorrang der Richtlinie

Es kann Situationen geben, in denen sich Netzwerkrichtlinienregeln innerhalb oder zwischen Richtlinien überschneiden. In diesem Fall überschreibt eine Regel, die den öffentlichen Zugriff festlegt, eine Regel, die privaten Zugriff für alle Sammlungen festlegt, die beiden Regeln gemeinsam sind.

In der folgenden Richtlinie weisen beispielsweise beide Regeln der `finance`-Sammlung Netzwerkzugriff zu, aber eine Regel legt den VPC-Zugriff fest, während die andere den öffentlichen Zugriff festlegt. In dieser Situation überschreibt der öffentliche Zugriff den VPC-Zugriff nur für die Finanzsammlung (weil er in beiden Regeln vorhanden ist), sodass die Finanzsammlung über öffentliche Netzwerke zugänglich ist. Die Verkaufssammlung verfügt über VPC-Zugriff vom angegebenen Endpunkt aus.

```
[
   {
      "Description":"Rule 1",
      "Rules":[
         {
            "ResourceType":"collection",
            "Resource":[
```

```
                "collection/sales",
                "collection/finance"
            ]
         }
      ],
      "AllowFromPublic":false,
      "SourceVPCEs":[
         "vpce-050f79086ee71ac05"
      ]
   },
   {
      "Description":"Rule 2",
      "Rules":[
         {
            "ResourceType":"collection",
            "Resource":[
               "collection/finance"
            ]
         }
      ],
      "AllowFromPublic":true
   }
]
```

Wenn mehrere VPC-Endpunkte aus unterschiedlichen Regeln auf eine Sammlung zutreffen, sind die Regeln additiv und die Sammlung ist von allen angegebenen Endpunkten aus zugänglich. Wenn Sie `AllowFromPublic` auf oder festlegen, `true` aber auch eines `SourceVPCEs` oder mehrere angeben`SourceServices`, ignoriert OpenSearch Serverless die VPC-Endpunkte und Dienstkennungen, sodass die zugehörigen Sammlungen öffentlich zugänglich sind.

Erstellen von Netzwerkrichtlinien (Konsole)

Netzwerkrichtlinien können sowohl für bestehende Richtlinien als auch für zukünftige Richtlinien gelten. Wir empfehlen, dass Sie Netzwerkrichtlinien erstellen, bevor Sie mit dem Erstellen von Sammlungen beginnen.

Um eine serverlose Netzwerkrichtlinie zu erstellen OpenSearch

1. Öffnen Sie die Amazon OpenSearch Service-Konsole unter https://console.aws.amazon.com/aos/home.
2. Erweitern Sie im linken Navigationsbereich Serverless und wählen Sie Network policies (Netzwerkrichtlinien) aus.

3. Wählen Sie Create network policy (Netzwerkrichtlinie erstellen) aus.
4. Geben Sie einen Namen und eine Beschreibung für die Sammlung an.
5. Geben Sie eine oder mehrere Regeln an. Diese Regeln definieren die Zugriffsberechtigungen für Ihre OpenSearch serverlosen Sammlungen und deren OpenSearch Dashboard-Endpunkte.

   Jede Regel enthält die folgenden Elemente:

Element	Beschreibung
Rule name (Regelname)	Ein Name, der den Inhalt der Regel beschreibt. Beispiel: „VPC-Zugriff für Marketingteam“.
Access type (Art des Zugriffs)	Wählen Sie entweder öffentlichen oder privaten Zugriff. Wählen Sie dann eine oder beide der folgenden Optionen aus: • VPC-Endpunkte für den Zugriff — Geben Sie einen oder OpenSearch mehrere serverlos verwaltete VPC-Endpunkte an — verwaltete VPC-Endpunkte. • AWS-Service privater Zugriff — Wählen Sie einen oder AWS-Services mehrere unterstützte Optionen aus.
Ressourcentyp	Wählen Sie aus, ob Sie Zugriff auf OpenSearch Endpunkte (was Aufrufe an die OpenSearch API ermöglicht), auf OpenSearc h Dashboards (die den Zugriff auf Visualisi erungen und die Benutzeroberfläche für OpenSearch Plugins ermöglichen) oder auf beides gewähren möchten. **Note** AWS-Service Der private Zugriff gilt nur für den Endpunkt der Sammlung,

Element	Beschreibung
	nicht für den OpenSearch Endpunkt der Dashboards. OpenSearch Auch wenn Sie OpenSearch Dashboards auswählen, AWS-Services kann nur Endpunktzugriff gewährt werden.

Für jeden ausgewählten Ressourcentyp können Sie vorhandene Sammlungen auswählen, für die die Richtlinieneinstellungen gelten, und/oder ein oder mehrere Ressourcenmuster erstellen. Ressourcenmuster bestehen aus einem Präfix und einem Platzhalter (*) und definieren, für welche Sammlungen die Richtlinieneinstellungen gelten.

Wenn Sie beispielsweise ein Muster mit dem Namen `Marketing*` einfügen, werden auf alle neuen oder vorhandenen Sammlungen, deren Namen mit „Marketing“ beginnen, automatisch die Netzwerkeinstellungen in dieser Richtlinie angewendet. Ein einzelner Platzhalter (`*`) wendet die Richtlinie auf alle aktuellen und zukünftigen Sammlungen an.

Darüber hinaus können Sie den Namen einer future Sammlung ohne Platzhalter angeben, z. B. `Finance` OpenSearch Serverless wendet die Richtlinieneinstellungen auf jede neu erstellte Sammlung mit genau diesem Namen an.

6. Wenn Sie mit der Konfiguration Ihrer Richtlinie zufrieden sind, wählen Sie Create (Erstellen).

Erstellen von Netzwerkrichtlinien (AWS CLI)

Um mithilfe der OpenSearch serverlosen API-Operationen eine Netzwerkrichtlinie zu erstellen, geben Sie Regeln im JSON-Format an. Die CreateSecurityPolicyAnfrage akzeptiert sowohl Inline-Richtlinien als auch JSON-Dateien. Alle Sammlungen und Muster müssen das Format `collection/<collection name|pattern>` aufweisen.

> **Note**
>
> Der Ressourcentyp erlaubt `dashboards` nur Zugriff auf OpenSearch Dashboards. Damit OpenSearch Dashboards funktionieren, müssen Sie jedoch auch den Zugriff auf Sammlungen aus denselben Quellen zulassen. Ein Beispiel finden Sie in der zweiten Richtlinie unten.

Um den privaten Zugriff festzulegen, fügen Sie eines oder beide der folgenden Elemente hinzu:

- `SourceVPCEs`— Geben Sie einen oder mehrere OpenSearch serverlos verwaltete VPC-Endpunkte an.
- `SourceServices`— Geben Sie die Kennung eines oder mehrerer unterstützter Geräte an. AWS-Services Derzeit werden die folgenden Dienstkennungen unterstützt:
  - `bedrock.amazonaws.com`— Amazonas-Grundgestein

Die folgende Beispielnetzwerkrichtlinie bietet privaten Zugriff auf einen VPC-Endpunkt und Amazon Bedrock auf Sammlungsendpunkte nur für Sammlungen, die mit dem Präfix beginnen. `log*` Authentifizierte Benutzer können sich nicht bei OpenSearch Dashboards anmelden. Sie können nur programmgesteuert auf den Sammlungsendpunkt zugreifen.

```
[
   {
      "Description":"Private access for log collections",
      "Rules":[
         {
            "ResourceType":"collection",
            "Resource":[
               "collection/log*"
            ]
         }
      ],
      "AllowFromPublic":false,
      "SourceVPCEs":[
         "vpce-050f79086ee71ac05"
      ],
      "SourceServices":[
         "bedrock.amazonaws.com"
      ],
   }
]
```

Die folgende Richtlinie gewährt öffentlichen Zugriff auf den OpenSearch Endpunkt und die OpenSearch Dashboards für eine einzelne Sammlung mit dem Namen. `finance` Wenn die Sammlung nicht vorhanden ist, werden die Netzwerkeinstellungen auf die Sammlung angewendet, wenn und sobald sie erstellt wird.

```
[
```

```
   {
      "Description":"Public access for finance collection",
      "Rules":[
         {
            "ResourceType":"dashboard",
            "Resource":[
               "collection/finance"
            ]
         },
         {
            "ResourceType":"collection",
            "Resource":[
               "collection/finance"
            ]
         }
      ],
      "AllowFromPublic":true
   }
]
```

Die folgende Anfrage erstellt die oben genannte Netzwerkrichtlinie:

```
aws opensearchserverless create-security-policy \
    --name sales-inventory \
    --type network \
    --policy "[{\"Description\":\"Public access for finance collection\",\"Rules
\":[{\"ResourceType\":\"dashboard\",\"Resource\":[\"collection\/finance\"]},
{\"ResourceType\":\"collection\",\"Resource\":[\"collection\/finance\"]}],
\"AllowFromPublic\":true}]"
```

Verwenden Sie das Format `--policy file://my-policy.json` die Richtlinie in einer JSON-Datei bereitzustellen

Anzeigen von Netzwerkrichtlinien

Bevor Sie eine Sammlung erstellen, möchten Sie möglicherweise eine Vorschau der vorhandenen Netzwerkrichtlinien in Ihrem Konto anzeigen, um zu sehen, welche ein Ressourcenmuster hat, das mit dem Namen Ihrer Sammlung übereinstimmt. Die folgende ListSecurityPoliciesAnfrage listet alle Netzwerkrichtlinien in Ihrem Konto auf:

```
aws opensearchserverless list-security-policies --type network
```

Die Anfrage gibt Informationen zu allen konfigurierten Netzwerkrichtlinien zurück. Um die in einer bestimmten Richtlinie definierten Musterregeln einzusehen, suchen Sie die Richtlinieninformationen im Inhalt des `securityPolicySummaries` Elements in der Antwort. Notieren Sie sich das `name` Ende `type` dieser Richtlinie und verwenden Sie diese Eigenschaften in einer GetSecurityPolicyAnfrage, um eine Antwort mit den folgenden Richtliniendetails zu erhalten:

```
{
    "securityPolicyDetail": [
        {
            "type": "network",
            "name": "my-policy",
            "policyVersion": "MTY2MzY5MTY1MDA3Ml8x",
            "policy": "[{\"Description\":\"My network policy rule\",\"Rules\":
[{\"ResourceType\":\"dashboard\",\"Resource\":[\"collection/*\"]}],\"AllowFromPublic
\":true}]",
            "createdDate": 1663691650072,
            "lastModifiedDate": 1663691650072
        }
    ]
}
```

Verwenden Sie den GetSecurityPolicyBefehl, um detaillierte Informationen zu einer bestimmten Richtlinie anzuzeigen.

Aktualisieren von Netzwerkrichtlinien

Wenn Sie die VPC-Endpunkte oder die Bezeichnung des öffentlichen Zugriffs für ein Netzwerk ändern, sind alle zugehörigen Sammlungen betroffen. Um eine Netzwerkrichtlinie in der OpenSearch Serverless-Konsole zu aktualisieren, erweitern Sie Netzwerkrichtlinien, wählen Sie die zu ändernde Richtlinie aus und klicken Sie auf Bearbeiten. Nehmen Sie Ihre Änderungen vor und wählen Sie Save (Speichern).

Verwenden Sie den Befehl, um eine Netzwerkrichtlinie mithilfe der OpenSearch Serverless API zu aktualisieren. UpdateSecurityPolicy Sie müssen eine Richtlinienversion in die Anfrage aufnehmen. Sie können die Richtlinienversion mithilfe der `ListSecurityPolicies`- oder `GetSecurityPolicy`-Befehle abrufen. Durch die Angabe der neuesten Richtlinienversion wird sichergestellt, dass Sie nicht versehentlich eine von einem anderen Benutzer vorgenommene Änderung überschreiben.

Die folgende Anfrage aktualisiert eine Netzwerkrichtlinie mit einem neuen JSON-Richtliniendokument:

```
aws opensearchserverless update-security-policy \
    --name sales-inventory \
    --type network \
    --policy-version MTY2MzY5MTY1MDA3Ml8x \
    --policy file://my-new-policy.json
```

Löschen von Netzwerkrichtlinien

Bevor Sie eine Netzwerkrichtlinie löschen können, müssen Sie sie von allen Sammlungen trennen. Um eine Richtlinie in der OpenSearch Serverless-Konsole zu löschen, wählen Sie die Richtlinie aus und klicken Sie auf Löschen.

Sie können auch den DeleteSecurityPolicyfolgenden Befehl verwenden:

```
aws opensearchserverless delete-security-policy --name my-policy --type network
```

Datenzugriffskontrolle für Amazon OpenSearch Serverless

Mit der Datenzugriffskontrolle in Amazon OpenSearch Serverless können Sie Benutzern den Zugriff auf Sammlungen und Indizes ermöglichen, unabhängig von ihrem Zugriffsmechanismus oder ihrer Netzwerkquelle. Sie können IAM-Rollen und SAML-Identitäten Zugriff gewähren.

Sie verwalten Zugriffsberechtigungen über Datenzugriffsrichtlinien, die für Sammlungen und Indexressourcen gelten. Datenzugriffsrichtlinien unterstützen Sie bei der Verwaltung von Sammlungen in großem Umfang, indem sie automatisch Zugriffsberechtigungen für Sammlungen und Indizes zuweisen, die einem bestimmten Muster übereinstimmen. Für eine einzelne Ressource können mehrere Datenzugriffsrichtlinien gelten. Beachten Sie, dass Sie über eine Datenzugriffsrichtlinie für Ihre Sammlung verfügen müssen, um auf Ihre OpenSearch Dashboard-URL zugreifen zu können.

Themen

- Datenzugriffsrichtlinien im Vergleich zu IAM-Richtlinien
- Für die Konfiguration von Datenzugriffsrichtlinien sind IAM-Berechtigungen erforderlich
- Richtliniensyntax
- Unterstützte Richtlinienberechtigungen
- Beispieldatensätze auf Dashboards OpenSearch

- Erstellen von Datenzugriffsrichtlinien (Konsole)
- Erstellen von Datenzugriffsrichtlinien (AWS CLI)
- Ansicht von Datenzugriffsrichtlinien
- Aktualisieren von Datenzugriffsrichtlinien
- Löschen von Datenzugriffsrichtlinien
- Kontoübergreifender Datenzugriff

Datenzugriffsrichtlinien im Vergleich zu IAM-Richtlinien

Datenzugriffsrichtlinien sind logisch von AWS Identity and Access Management (IAM-) Richtlinien getrennt. IAM-Berechtigungen steuern den Zugriff auf die Serverless API-Operationen wie z. B. `CreateCollection` und `ListAccessPolicies`. Datenzugriffsrichtlinien steuern den Zugriff auf die von OpenSearch Serverless unterstützten OpenSearch Operationen wie oder. `PUT <index>` `GET _cat/indices`

Die IAM-Berechtigungen, die den Zugriff auf API-Operationen der Datenzugriffsrichtlinie steuern, wie z. B. `aoss:CreateAccessPolicy` and `aoss:GetAccessPolicy` (im nächsten Abschnitt beschrieben), wirken sich nicht auf die in einer Datenzugriffsrichtlinie angegebene Berechtigung aus.

Angenommen, eine IAM-Richtlinie verweigert einem Benutzer beispielsweise das Erstellen von Datenzugriffsrichtlinien für `collection-a`, erlaubt ihm jedoch, Datenzugriffsrichtlinien für alle Sammlungen (`*`) zu erstellen:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "aoss:CreateAccessPolicy"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "aoss:collection": "collection-a"
                }
            }
        },
```

```
        {
            "Effect": "Allow",
            "Action": [
                "aoss:CreateAccessPolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

Wenn der Benutzer eine Datenzugriffsrichtlinie erstellt, die bestimmte Berechtigungen für alle Sammlungen (`collection/*` oder `index/*/*`) gewährt, gilt die Richtlinie für alle Sammlungen, einschließlich Sammlung A.

> **Important**
>
> Die Erteilung von Berechtigungen im Rahmen einer Datenzugriffsrichtlinie reicht nicht aus, um auf Daten in Ihrer OpenSearch serverlosen Sammlung zuzugreifen. Einem zugehörigen Principal muss außerdem Zugriff auf die IAM-Berechtigungen `aoss:APIAccessAll` und gewährt werden. `aoss:DashboardsAccessAll` Beide Berechtigungen gewähren vollen Zugriff auf Sammlungsressourcen, während die Dashboard-Berechtigung auch Zugriff OpenSearch auf Dashboards gewährt. Wenn ein Principal nicht über diese beiden IAM-Berechtigungen verfügt, erhält er 403-Fehler, wenn er versucht, Anfragen an die Sammlung zu senden. Weitere Informationen finden Sie unter the section called “Verwendung von OpenSearch API-Vorgängen”.

Für die Konfiguration von Datenzugriffsrichtlinien sind IAM-Berechtigungen erforderlich

Die Datenzugriffskontrolle für OpenSearch Serverless verwendet die folgenden IAM-Berechtigungen. Sie können IAM-Bedingungen festlegen, um Benutzer auf bestimmte Zugriffsrichtliniennamen zu beschränken.

- `aoss:CreateAccessPolicy` – Erstellt eine Zugriffsrichtlinie.
- `aoss:ListAccessPolicies` – Listet alle Zugriffsrichtlinien auf.
- `aoss:GetAccessPolicy` – Zeigt Details zu einer bestimmten Zugriffsrichtlinie an.
- `aoss:UpdateAccessPolicy` – Ändert eine Zugriffsrichtlinie.
- `aoss:DeleteAccessPolicy` – Löscht eine Zugriffsrichtlinie.

Die folgende identitätsbasierte Zugriffsrichtlinie ermöglicht es einem Benutzer, alle Zugriffsrichtlinien anzuzeigen und Richtlinien zu aktualisieren, die das Ressourcenmuster `collection/logs` enthalten.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "aoss:ListAccessPolicies",
                "aoss:GetAccessPolicy"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "aoss:UpdateAccessPolicy"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aoss:collection": [
                        "logs"
                    ]
                }
            }
        }
    ]
}
```

> **Note**
>
> Darüber hinaus benötigt OpenSearch Serverless die `aoss:DashboardsAccessAll` Berechtigungen `aoss:APIAccessAll` und für die Erfassung von Ressourcen. Weitere Informationen finden Sie unter the section called “Verwendung von OpenSearch API-Vorgängen”.

Richtliniensyntax

Eine Datenzugriffsrichtlinie enthält eine Reihe von Regeln, die jeweils die folgenden Elemente enthalten:

Element	Beschreibung
`ResourceType`	Der Ressourcentyp (Sammlung oder Index), für den die Berechtigungen gelten. Alias- und Vorlagenberechtigungen befinden sich auf Sammlungsebene, während Berechtigungen zum Erstellen, Ändern und Suchen von Daten auf Indexebene liegen. Weitere Informationen finden Sie unter Unterstützte Richtlinienberechtigungen.
`Resource`	Eine Liste von Ressourcennamen und/oder Mustern. Muster sind Präfixe gefolgt von einem Platzhalter (*), wodurch die zugehörigen Berechtigungen auf mehrere Ressourcen angewendet werden können. • Sammlungen haben das Format `collection/ <name|pattern>` . • Indizes haben das Format `index/<collection-name|pattern> /<index-name|pattern/>` .
`Permission`	Eine Liste der Berechtigungen, die für die angegebenen Ressourcen gewährt werden sollen. Eine vollständige Liste der Berechtigungen und der zulässigen API-Operationen finden Sie unter the section called “Unterstützte OpenSearch API-Operationen und Berechtigungen”.
`Principal`	Eine Liste mit einem oder mehreren Prinzipalen, denen Zugriff gewährt werden soll. Prinzipale können IAM-Rollen-ARNs oder SAML-Identitäten sein. Diese Prinzipien müssen dem aktuellen AWS-Konto entsprechen. Datenzugriffsrichtlinien unterstützen den kontoübergreifenden Zugriff nicht direkt, Sie können jedoch eine Rolle in Ihre Richtlinie aufnehmen, die ein Benutzer aus einem anderen Land in dem Konto, dem die Sammlung gehört, übernehmen AWS-Konto kann. Weitere Informationen finden Sie unter the section called “Kontoübergreifender Datenzugriff”.

Die folgende Beispielrichtlinie gewährt Alias- und Vorlagenberechtigungen für die Sammlung mit dem Namen `autopartsinventory` sowie alle Sammlungen, die mit dem Präfix `sales*`

beginnen. Es gewährt auch Lese- und Schreibberechtigungen für alle Indizes innerhalb der `autopartsinventory`-Sammlung und alle Indizes in der `salesorders`-Sammlung, die mit dem Präfix `orders*` beginnen.

```
[
   {
      "Description": "Rule 1",
      "Rules":[
         {
            "ResourceType":"collection",
            "Resource":[
               "collection/autopartsinventory",
               "collection/sales*"
            ],
            "Permission":[
               "aoss:CreateCollectionItems",
               "aoss:UpdateCollectionItems",
               "aoss:DescribeCollectionItems"
            ]
         },
         {
            "ResourceType":"index",
            "Resource":[
               "index/autopartsinventory/*",
               "index/salesorders/orders*"
            ],
            "Permission":[
               "aoss:*"
            ]
         }
      ],
      "Principal":[
         "arn:aws:iam::123456789012:user/Dale",
         "arn:aws:iam::123456789012:role/RegulatoryCompliance",
         "saml/123456789012/myprovider/user/Annie",
         "saml/123456789012/anotherprovider/group/Accounting"
      ]
   }
]
```

Sie können den Zugriff innerhalb einer Richtlinie nicht explizit verweigern. Daher sind alle Richtlinienberechtigungen additiv. Wenn beispielsweise eine Richtlinie einem Benutzer

`aoss:ReadDocument` und eine andere Richtlinie `aoss:WriteDocument` gewährt, verfügt der Benutzer über beide Berechtigungen. Wenn eine dritte Richtlinie denselben Benutzer `aoss:*` gewährt, kann der Benutzer alle Aktionen für den zugeordneten Index ausführen. Restriktivere Berechtigungen überschreiben weniger restriktive nicht.

Unterstützte Richtlinienberechtigungen

Die folgenden Berechtigungen werden in Datenzugriffsrichtlinien unterstützt. Informationen zu den OpenSearch API-Vorgängen, die einzelnen Berechtigungen zulassen, finden Sie unterthe section called “Unterstützte OpenSearch API-Operationen und Berechtigungen”.

Sammlungssberechtigungen

- `aoss:CreateCollectionItems`
- `aoss:DeleteCollectionItems`
- `aoss:UpdateCollectionItems`
- `aoss:DescribeCollectionItems`
- `aoss:*`

Indexberechtigungen

- `aoss:ReadDocument`
- `aoss:WriteDocument`
- `aoss:CreateIndex`
- `aoss:DeleteIndex`
- `aoss:UpdateIndex`
- `aoss:DescribeIndex`
- `aoss:*`

Beispieldatensätze auf Dashboards OpenSearch

OpenSearch Dashboards bietet Beispieldatensätze mit Visualisierungen, Dashboards und anderen Tools, die Ihnen helfen, Dashboards zu erkunden, bevor Sie Ihre eigenen Daten hinzufügen.
Um Indizes aus diesen Beispieldaten zu erstellen, benötigen Sie eine Datenzugriffsrichtlinie, die

Berechtigungen für den Datensatz bereitstellt, mit dem Sie arbeiten möchten. Die folgende Richtlinie verwendet einen Platzhalter (*), um Berechtigungen für alle drei Beispieldatensätze zu gewähren.

```
[
  {
    "Rules": [
      {
        "Resource": [
          "index/<collection-name>/opensearch_dashboards_sample_data_*"
        ],
        "Permission": [
          "aoss:CreateIndex",
          "aoss:DescribeIndex",
          "aoss:ReadDocument"
        ],
        "ResourceType": "index"
      }
    ],
    "Principal": [
      "arn:aws:iam::<account-id>:user/<user>"
    ]
  }
]
```

Erstellen von Datenzugriffsrichtlinien (Konsole)

Sie können eine Datenzugriffsrichtlinie mit dem visuellen Editor oder im JSON-Format erstellen. Allen neuen Sammlungen, die mit einem der in der Richtlinie definierten Muster übereinstimmen, werden beim Erstellen der Sammlung die entsprechenden Berechtigungen zugewiesen.

Um eine Richtlinie für den OpenSearch serverlosen Datenzugriff zu erstellen

1. Öffnen Sie die Amazon OpenSearch Service-Konsole unter https://console.aws.amazon.com/aos/home.
2. Erweitern Sie im linken Navigationsbereich Serverless und wählen Sie Data access control (Datenzugriffssteuerung) aus.
3. Wählen Sie Create access policy (Zugriffsrichtlinie erstellen) aus.
4. Geben Sie einen Namen und eine Beschreibung für die Richtlinie an.
5. Geben Sie einen Namen für die erste Regel in Ihrer Richtlinie an. Beispiel: „Zugriff auf die Protokollsammlung“.

6. Wählen Sie Add principals (Prinzipale hinzufügen) und wählen Sie eine oder mehrere IAM-Rollen oder SAML users and groups (SAML-Benutzer und -Gruppen) aus, denen Sie Datenzugriff gewähren möchten.

   > **Note**
   >
   > Um Prinzipale aus den Dropdown-Menüs auswählen zu können, müssen Sie über die `iam:ListUsers`- und `iam:ListRoles`-Berechtigungen (für IAM-Prinzipale) und die `aoss:ListSecurityConfigs`-Berechtigung (für SAML-Identitäten) verfügen.

7. Wählen Sie Grant (Gewähren) und wählen Sie die Alias-, Vorlagen- und Indexberechtigungen aus, um die zugehörigen Prinzipale zu erteilen. Eine vollständige Liste der Berechtigungen und des von ihnen gewährten Zugriffs finden Sie unter the section called “Unterstützte OpenSearch API-Operationen und Berechtigungen”.
8. (Optional) Konfigurieren Sie zusätzliche Regeln für die Richtlinie.
9. Wählen Sie Erstellen. Zwischen der Erstellung der Richtlinie und dem Erzwingen von Berechtigungen kann eine Verzögerung von etwa einer Minute liegen. Wenn es länger als 5 Minuten dauert, wenden Sie sich an AWS Support.

> **Important**
>
> Wenn Ihre Richtlinie nur Indexberechtigungen (und keine Sammlungsberechtigungen) umfasst, wird Ihnen möglicherweise trotzdem eine Meldung mit dem Hinweis `Collection cannot be accessed yet. Configure data access policies so that users can access the data within this collection` für passende Sammlungen angezeigt. Sie können diese Warnung ignorieren. Zulässige Prinzipale können weiterhin ihre zugewiesenen indexbezogenen Operationen für die Sammlung ausführen.

Erstellen von Datenzugriffsrichtlinien (AWS CLI)

Verwenden Sie den `CreateAccessPolicy` Befehl, um eine Datenzugriffsrichtlinie mithilfe der OpenSearch Serverless API zu erstellen. Der Befehl akzeptiert sowohl Inline-Richtlinien als auch .json-Dateien. Inline-Richtlinien müssen als JSON-Zeichenfolge mit Escape-Zeichen codiert werden.

Die folgende Anfrage erstellt eine Datenzugriffsrichtlinie:

```
aws opensearchserverless create-access-policy \
    --name marketing \
    --type data \
    --policy "[{\"Rules\":[{\"ResourceType\":\"collection\",\"Resource\":
[\"collection/autopartsinventory\",\"collection/sales*\"],\"Permission\":
[\"aoss:UpdateCollectionItems\"]},{\"ResourceType\":\"index\",\"Resource\":
[\"index/autopartsinventory/*\",\"index/salesorders/orders*\"],\"Permission
\":[\"aoss:ReadDocument\",\"aoss:DescribeIndex\"]}],\"Principal\":
[\"arn:aws:iam::123456789012:user/Shaheen\"]}]"
```

Verwenden Sie das Format `--policy file://my-policy.json`, um die Richtlinie in einer .json-Datei bereitzustellen.

Die in der Richtlinie enthaltenen Prinzipale können jetzt die OpenSearch Operationen verwenden, für die ihnen Zugriff gewährt wurde.

Ansicht von Datenzugriffsrichtlinien

Bevor Sie eine Sammlung erstellen, möchten Sie möglicherweise eine Vorschau der vorhandenen Datenzugriffsrichtlinien in Ihrem Konto anzeigen, um zu sehen, welche ein Ressourcenmuster hat, das mit dem Namen Ihrer Sammlung übereinstimmt. In der folgenden ListAccessPoliciesAnfrage werden alle Datenzugriffsrichtlinien in Ihrem Konto aufgeführt:

```
aws opensearchserverless list-access-policies --type data
```

Die Anfrage gibt Informationen über alle konfigurierten Datenzugriffsrichtlinien zurück. Die Musterregeln, die in einer bestimmten Richtlinie definiert sind, finden Sie im Inhalt des `accessPolicySummaries` Elements in der Antwort. Notieren Sie sich das `name` Ende `type` dieser Richtlinie und verwenden Sie diese Eigenschaften in einer GetAccessPolicyAnfrage, um eine Antwort mit den folgenden Richtliniendetails zu erhalten:

```
{
    "accessPolicyDetails": [
        {
            "type": "data",
            "name": "my-policy",
            "policyVersion": "MTY2NDA1NDE4MDg1OF8x",
            "description": "My policy",
            "policy": "[{\"Rules\":[{\"ResourceType\":\"collection\",
\"Resource\":[\"collection/autopartsinventory\",\"collection/sales*\"],
\"Permission\":[\"aoss:UpdateCollectionItems\"]},{\"ResourceType\":\"index\",
```

```
\"Resource\":[\"index/autopartsinventory/*\",\"index/salesorders/orders*\"],
\"Permission\":[\"aoss:ReadDocument\",\"aoss:DescribeIndex\"]}],\"Principal\":
[\"arn:aws:iam::123456789012:user/Shaheen\"]}]",
            "createdDate": 1664054180858,
            "lastModifiedDate": 1664054180858
        }
    ]
}
```

Sie können Ressourcenfilter einbeziehen, um die Ergebnisse auf Richtlinien zu beschränken, die bestimmte Sammlungen oder Indizes enthalten:

```
aws opensearchserverless list-access-policies --type data --resource
 "index/autopartsinventory/*"
```

Verwenden Sie den GetAccessPolicyBefehl, um Details zu einer bestimmten Richtlinie anzuzeigen.

Aktualisieren von Datenzugriffsrichtlinien

Wenn Sie eine Datenzugriffsrichtlinie aktualisieren, wirkt sich dies auf alle zugehörigen Sammlungen aus. Um eine Datenzugriffsrichtlinie in der OpenSearch Serverless-Konsole zu aktualisieren, wählen Sie Datenzugriffskontrolle, wählen Sie die zu ändernde Richtlinie aus und klicken Sie auf Bearbeiten. Nehmen Sie Ihre Änderungen vor und wählen Sie Save (Speichern).

Um eine Datenzugriffsrichtlinie mithilfe der OpenSearch Serverless API zu aktualisieren, senden Sie eine `UpdateAccessPolicy` Anfrage. Sie müssen eine Richtlinienversion einbeziehen, die Sie mit den `ListAccessPolicies`- oder `GetAccessPolicy`-Befehlen abrufen können. Durch die Angabe der neuesten Richtlinienversion wird sichergestellt, dass Sie nicht versehentlich eine von einem anderen Benutzer vorgenommene Änderung überschreiben.

Die folgende UpdateAccessPolicyAnfrage aktualisiert eine Datenzugriffsrichtlinie mit einem neuen JSON-Richtliniendokument:

```
aws opensearchserverless update-access-policy \
    --name sales-inventory \
    --type data \
    --policy-version MTY2NDA1NDE4MDg1OF8x \
    --policy file://my-new-policy.json
```

Zwischen dem Aktualisieren der Richtlinie und dem Erzwingen der neuen Berechtigungen kann es einige Minuten Verzögerung geben.

Löschen von Datenzugriffsrichtlinien

Wenn Sie eine Datenzugriffsrichtlinie löschen, verlieren alle zugehörigen Sammlungen den in der Richtlinie definierten Zugriff. Stellen Sie sicher, dass Ihre IAM- und SAML-Benutzer über den entsprechenden Zugriff auf die Sammlung verfügen, bevor Sie eine Richtlinie löschen. Um eine Richtlinie in der OpenSearch Serverless-Konsole zu löschen, wählen Sie die Richtlinie aus und klicken Sie auf Löschen.

Sie können auch den DeleteAccessPolicyfolgenden Befehl verwenden:

```
aws opensearchserverless delete-access-policy --name my-policy --type data
```

Kontoübergreifender Datenzugriff

Sie können zwar keine Datenzugriffsrichtlinie mit kontoübergreifender Identität oder kontoübergreifender Erfassung erstellen, aber Sie können mit der Option „Rolle übernehmen“ dennoch einen kontoübergreifenden Zugriff einrichten. Wenn Sie beispielsweise *account-a* Eigentümer einer Sammlung sind, für die Zugriff *account-b* erforderlich ist, *account-b* kann der Benutzer von aus eine Rolle darin übernehmen. *account-a* Die Rolle muss über die IAM-Berechtigungen verfügen `aoss:APIAccessAll` und `aoss:DashboardsAccessAll` in der Datenzugriffsrichtlinie enthalten sein. *account-a*

Greifen Sie über einen Schnittstellenendpunkt auf Amazon OpenSearch Serverless zu ()AWS PrivateLink

Sie können AWS PrivateLink es verwenden, um eine private Verbindung zwischen Ihrer VPC und Amazon OpenSearch Serverless herzustellen. Sie können auf OpenSearch Serverless zugreifen, als wäre es in Ihrer VPC, ohne ein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder AWS Direct Connect eine Verbindung zu verwenden. Instances in Ihrer VPC benötigen keine öffentlichen IP-Adressen, um auf OpenSearch Serverless zuzugreifen.

Sie stellen diese private Verbindung her, indem Sie einen Schnittstellen-Endpunkt erstellen, der von AWS PrivateLink unterstützt wird. Wir erstellen eine Endpunkt-Netzwerkschnittstelle in jedem Subnetz, das Sie für den Schnittstellen-Endpunkt angeben. Dabei handelt es sich um vom Anforderer verwaltete Netzwerkschnittstellen, die als Einstiegspunkt für den Datenverkehr dienen, der für Serverless bestimmt ist. OpenSearch

Weitere Informationen finden Sie unter Zugriff auf AWS-Services über AWS PrivateLink im AWS PrivateLink -Leitfaden.

Themen

DNS-Auflösung der Sammlungsendpunkte

Wenn Sie einen VPC-Endpunkt erstellen, erstellt der Service eine neue Amazon Route 53 private gehostete Zone und fügt sie der VPC hinzu. Diese private gehostete Zone besteht aus einem Datensatz zur Auflösung des DNS-Wildcard-Eintrags für OpenSearch serverlose Sammlungen (`*.aoss.us-east-1.amazonaws.com`) in die für den Endpunkt verwendeten Schnittstellenadressen. Sie benötigen nur einen OpenSearch serverlosen VPC-Endpunkt in einer VPC, um auf alle Sammlungen und Dashboards in jeder VPC zuzugreifen. AWS-Region Jeder VPC mit einem Endpunkt für OpenSearch Serverless ist eine eigene private Hosting-Zone zugeordnet.

OpenSearch Serverless erstellt außerdem einen öffentlichen Route 53-Platzhalter-DNS-Eintrag für alle Sammlungen in der Region. Der DNS-Name wird in die öffentlichen IP-Adressen von OpenSearch Serverless aufgelöst. Clients in VPCs, die keinen OpenSearch serverlosen VPC-Endpunkt haben, oder Clients in öffentlichen Netzwerken können den öffentlichen Route 53-Resolver verwenden und mit diesen IP-Adressen auf die Sammlungen und Dashboards zugreifen. Der IP-Adresstyp (IPv4, IPv6 oder Dualstack) des VPC-Endpunkts wird anhand der Subnetze bestimmt, die beim Erstellen eines Schnittstellenendpunkts für Serverless bereitgestellt werden. OpenSearch

> **Note**
>
> Sie können Ihren vorhandenen IPv4-VPC-Endpunkt auf Dualstack aktualisieren, indem Sie den Befehl in der update-vpc-endpointverwenden. AWS CLI

Die DNS-Resolver-Adresse für eine bestimmte VPC ist die zweite IP-Adresse der VPC CIDR. Jeder Client in der VPC muss diesen Resolver verwenden, um die VPC-Endpunktadresse für jede

Sammlung abzurufen. Der Resolver verwendet eine private gehostete Zone, die von Serverless erstellt wurde. OpenSearch Es reicht aus, diesen Resolver für alle Sammlungen in einem beliebigen Konto zu verwenden. Es ist auch möglich, den VPC-Resolver für einige Sammlungsendpunkte und den öffentlichen Resolver für andere zu verwenden, obwohl dies normalerweise nicht erforderlich ist.

VPCs und Netzwerkzugriffsrichtlinien

Um OpenSearch APIs und Dashboards für Ihre Sammlungen Netzwerkberechtigungen zu gewähren, können Sie Richtlinien für den OpenSearch serverlosen Netzwerkzugriff verwenden. Sie können diesen Netzwerkzugriff entweder von Ihren VPC-Endpunkten oder dem öffentlichen Internet aus steuern. Da Ihre Netzwerkrichtlinie nur die Zugriffsberechtigungen steuert, müssen Sie auch eine Datenzugriffsrichtlinie einrichten, die die Erlaubnis festlegt, mit den Daten in einer Sammlung und ihren Indizes zu arbeiten. Stellen Sie sich einen OpenSearch serverlosen VPC-Endpunkt als Zugriffspunkt für den Service, eine Netzwerkzugriffsrichtlinie als Zugriffspunkt auf Netzwerkebene für Sammlungen und Dashboards und eine Datenzugriffsrichtlinie als Zugriffspunkt für eine detaillierte Zugriffskontrolle für jeden Vorgang mit Daten in der Sammlung vor.

Da Sie in einer Netzwerkrichtlinie mehrere VPC-Endpunkt-IDs angeben können, empfehlen wir, für jede VPC, die auf eine Sammlung zugreifen muss, einen VPC-Endpunkt zu erstellen. Diese VPCs können zu anderen AWS Konten gehören als das Konto, dem die OpenSearch Serverless-Sammlung und die Netzwerkrichtlinie gehören. Es wird nicht empfohlen, eine VPC-zu-VPC-Peering- oder eine andere Proxylösung zwischen zwei Konten zu erstellen, sodass die VPC eines Kontos den VPC-Endpunkt eines anderen Kontos verwenden kann. Dies ist weniger sicher und kostengünstiger als wenn jede VPC über einen eigenen Endpunkt verfügt. Die erste VPC wird für den Administrator der anderen VPC, der in der Netzwerkrichtlinie den Zugriff auf den Endpunkt dieser VPC eingerichtet hat, nicht ohne weiteres sichtbar sein.

VPCs und Endpunktrichtlinien

Amazon OpenSearch Serverless unterstützt Endpunktrichtlinien für VPCs. Eine Endpunktrichtlinie ist eine ressourcenbasierte IAM-Richtlinie, die Sie an einen VPC-Endpunkt anhängen, um zu steuern, welche AWS Principals den Endpunkt für den Zugriff auf Ihren Service verwenden können. AWS Weitere Informationen finden Sie unter Steuern des Zugriffs auf VPC-Endpoints mithilfe von Endpunktrichtlinien.

Um eine Endpunktrichtlinie zu verwenden, müssen Sie zunächst einen Schnittstellenendpunkt erstellen. Sie können einen Schnittstellenendpunkt entweder mit der OpenSearch Serverless-Konsole oder der OpenSearch Serverless-API erstellen. Nachdem Sie Ihren Schnittstellenendpunkt erstellt

haben, müssen Sie die Endpunktrichtlinie zum Endpunkt hinzufügen. Weitere Informationen finden Sie unter Zugriff auf Amazon OpenSearch Serverless über einen Schnittstellenendpunkt (AWS PrivateLink).

> **Note**
>
> Sie können eine Endpunktrichtlinie nicht direkt in der OpenSearch Service-Konsole definieren.

Eine Endpunktrichtlinie überschreibt oder ersetzt keine anderen identitätsbasierten Richtlinien, ressourcenbasierten Richtlinien, Netzwerkrichtlinien oder Datenzugriffsrichtlinien, die Sie möglicherweise konfiguriert haben. Weitere Informationen zur Aktualisierung von Endpunktrichtlinien finden Sie unter Steuern des Zugriffs auf VPC-Endpunkte mithilfe von Endpunktrichtlinien.

Standardmäßig gewährt eine Endpunktrichtlinie vollen Zugriff auf Ihren VPC-Endpunkt.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*"
        }
    ]
}
```

Obwohl die standardmäßige VPC-Endpunktrichtlinie vollen Endpunktzugriff gewährt, können Sie eine VPC-Endpunktrichtlinie konfigurieren, um den Zugriff auf bestimmte Rollen und Benutzer zu ermöglichen. Sehen Sie sich dazu das folgende Beispiel an:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "123456789012",
```

```
                    "987654321098"
                ]
            },
            "Action": "*",
            "Resource": "*"
        }
    ]
}
```

Sie können eine OpenSearch serverlose Sammlung angeben, die als bedingtes Element in Ihre VPC-Endpunktrichtlinie aufgenommen werden soll. Sehen Sie sich dazu das folgende Beispiel an:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:CollectionName": [
                        "coll-abc"
                    ]
                }
            }
        }
    ]
}
```

Sie können SAML-Identitäten in Ihrer VPC-Endpunktrichtlinie verwenden, um den VPC-Endpunktzugriff zu bestimmen. Sie müssen (*) im Hauptbereich Ihrer VPC-Endpunktrichtlinie einen Platzhalter verwenden. Sehen Sie sich dazu das folgende Beispiel an:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
```

```
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:SamlGroups": [
                        "saml/123456789012/idp123/group/football",
                        "saml/123456789012/idp123/group/soccer",
                        "saml/123456789012/idp123/group/cricket"
                    ]
                }
            }
        }
    ]
}
```

Darüber hinaus können Sie Ihre Endpunktrichtlinie so konfigurieren, dass sie eine bestimmte SAML-Prinzipalrichtlinie enthält. Sehen Sie sich dazu Folgendes an:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:SamlPrincipal": [
                        "saml/123456789012/idp123/user/user1234"]
                    }
                }
            }
        ]
    }
```

Weitere Informationen zur Verwendung der SAML-Authentifizierung mit Amazon OpenSearch Serverless finden Sie unter SAML-Authentifizierung für Amazon Serverless. OpenSearch

Sie können auch IAM- und SAML-Benutzer in dieselbe VPC-Endpunktrichtlinie aufnehmen. Sehen Sie sich dazu das folgende Beispiel an:

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:SamlGroups": [
                        "saml/123456789012/idp123/group/football",
                        "saml/123456789012/idp123/group/soccer",
                        "saml/123456789012/idp123/group/cricket"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "123456789012"
                ]
            },
            "Action": "*",
            "Resource": "*"
        }
    ]
}
```

Überlegungen

Bevor Sie einen Schnittstellenendpunkt für OpenSearch Serverless einrichten, sollten Sie Folgendes berücksichtigen:

- OpenSearch Serverless unterstützt Aufrufe aller unterstützten OpenSearch API-Operationen (nicht Konfigurations-API-Operationen) über den Schnittstellenendpunkt.
- Nachdem Sie einen Schnittstellenendpunkt für OpenSearch Serverless erstellt haben, müssen Sie ihn dennoch in die Netzwerkzugriffsrichtlinien aufnehmen, damit er auf serverlose Sammlungen zugreifen kann.
- Standardmäßig ist der vollständige Zugriff auf OpenSearch Serverless über den Schnittstellenendpunkt zulässig. Sie können den Endpunkt-Netzwerkschnittstellen eine

Sicherheitsgruppe zuordnen, um den Datenverkehr zu OpenSearch Serverless über den Schnittstellenendpunkt zu steuern.

- Ein einzelner AWS-Konto kann maximal 50 OpenSearch serverlose VPC-Endpunkte haben.
- Wenn Sie in einer Netzwerkrichtlinie den öffentlichen Internetzugriff auf die API oder die Dashboards Ihrer Sammlung aktivieren, ist Ihre Sammlung von jeder VPC und über das öffentliche Internet zugänglich.
- Wenn Sie sich vor Ort und außerhalb der VPC befinden, können Sie einen DNS-Resolver nicht direkt für die OpenSearch serverlose VPC-Endpunktlösung verwenden. Wenn Sie VPN-Zugriff benötigen, benötigt die VPC einen DNS-Proxy-Resolver, den externe Clients verwenden können. Route 53 bietet eine Option für eingehende Endpunkte, mit der Sie DNS-Abfragen an Ihre VPC von Ihrem lokalen Netzwerk oder einer anderen VPC aus auflösen können.
- Die private gehostete Zone, die OpenSearch Serverless erstellt und an die VPC anhängt, wird vom Service verwaltet, sie wird jedoch in Ihren Amazon Route 53 Ressourcen angezeigt und Ihrem Konto in Rechnung gestellt.
- Weitere Überlegungen finden Sie unter Überlegungen im AWS PrivateLink -Leitfaden.

Erforderliche Berechtigungen

Der VPC-Zugriff für OpenSearch Serverless verwendet die folgenden AWS Identity and Access Management (IAM-) Berechtigungen. Sie können IAM-Bedingungen festlegen, um Benutzer auf bestimmte Sammlungen zu beschränken.

- `aoss:CreateVpcEndpoint` – Erstellt einen VPC-Endpunkt.
- `aoss:ListVpcEndpoints` – Listet alle VPC-Endpunkte auf.
- `aoss:BatchGetVpcEndpoint` – Zeigt Details zu einer Untergruppe von VPC-Endpunkten an.
- `aoss:UpdateVpcEndpoint` – Ändert einen VPC-Endpunkt.
- `aoss:DeleteVpcEndpoint` – Löscht einen VPC-Endpunkt.

Darüber hinaus benötigen Sie die folgenden Amazon-EC2- und Route-53-Berechtigungen, um einen VPC-Endpunkt zu erstellen.

- `ec2:CreateTags`
- `ec2:CreateVpcEndpoint`
- `ec2:DeleteVpcEndPoints`

- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:DescribeVpcEndpoints`
- `ec2:DescribeVpcs`
- `ec2:ModifyVpcEndPoint`
- `route53:AssociateVPCWithHostedZone`
- `route53:ChangeResourceRecordSets`
- `route53:CreateHostedZone`
- `route53:DeleteHostedZone`
- `route53:GetChange`
- `route53:GetHostedZone`
- `route53:ListHostedZonesByName`
- `route53:ListHostedZonesByVPC`
- `route53:ListResourceRecordSets`

Erstellen Sie einen Schnittstellenendpunkt für Serverless OpenSearch

Sie können einen Schnittstellenendpunkt für OpenSearch Serverless entweder mit der Konsole oder der OpenSearch Serverless API erstellen.

Um einen Schnittstellenendpunkt für eine serverlose Sammlung zu erstellen OpenSearch

1. Öffnen Sie die Amazon OpenSearch Service-Konsole unter https://console.aws.amazon.com/aos/home.
2. Erweitern Sie im linken Navigationsbereich Serverless und wählen Sie VPC endpoints (VPC-Endpunkte) aus.
3. Wählen Sie Create VPC endpoint (VPC-Endpunkt) erstellen.
4. Geben Sie einen Namen für den Endpunkt an.
5. Wählen Sie für VPC die VPC aus, von der aus Sie auf OpenSearch Serverless zugreifen möchten.
6. Wählen Sie für Subnetze ein Subnetz aus, von dem aus Sie auf Serverless zugreifen möchten. OpenSearch
   - Die IP-Adresse und der DNS-Typ des Endpunkts basieren auf dem Subnetztyp

- Dualstack: Wenn alle Subnetze sowohl IPv4- als auch IPv6-Adressbereiche haben
- IPv6: Wenn alle Subnetze nur IPv6-Subnetze sind
- IPv4: Wenn alle Subnetze IPv4-Adressbereiche haben

7. Wählen Sie für Sicherheitsgruppen die Sicherheitsgruppen aus, die den Security groups (Endpunkt-Netzwerkschnittstellen) zugeordnet werden sollen. Dies ist ein entscheidender Schritt, bei dem Sie die Ports, Protokolle und Quellen für eingehenden Datenverkehr einschränken, den Sie für Ihren Endpunkt autorisieren. Stellen Sie sicher, dass die Sicherheitsgruppenregeln den Ressourcen, die den VPC-Endpunkt für die Kommunikation mit OpenSearch Serverless verwenden, die Kommunikation mit der Endpunkt-Netzwerkschnittstelle ermöglichen.
8. Wählen Sie Endpunkt erstellen aus.

Verwenden Sie den Befehl, um einen VPC-Endpunkt mithilfe der OpenSearch Serverless API zu erstellen. `CreateVpcEndpoint`

> **Note**
>
> Nachdem Sie einen Endpunkt erstellt haben, notieren Sie sich seine ID, z. B. `vpce-050f79086ee71ac05`. Um dem Endpunkt Zugriff auf Ihre Sammlungen zu gewähren, müssen Sie diese ID in eine oder mehrere Netzwerkzugriffsrichtlinien aufnehmen.

Nächster Schritt: Einem Endpunkt Zugriff auf eine Sammlung gewähren

Nachdem Sie einen Schnittstellen-Endpunkt erstellt haben, müssen Sie ihm über Netzwerkzugriffsrichtlinien Zugriff auf Sammlungen gewähren. Weitere Informationen finden Sie unter the section called “Netzwerkzugriff”.

SAML-Authentifizierung für Amazon OpenSearch Serverless

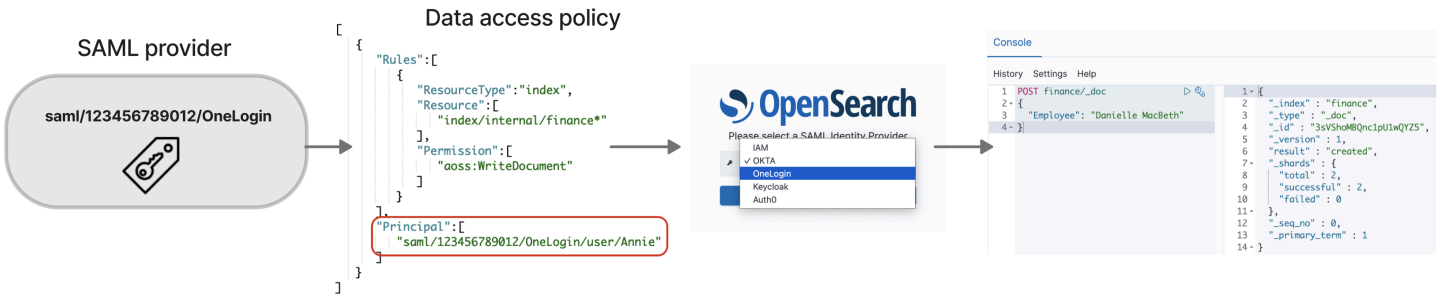
Mit der SAML-Authentifizierung für Amazon OpenSearch Serverless können Sie Ihren vorhandenen Identitätsanbieter verwenden, um Single Sign-On (SSO) für die OpenSearch Dashboards-Endpunkte von Serverless-Sammlungen bereitzustellen.

Mit der SAML-Authentifizierung können Sie Identitätsanbieter von Drittanbietern verwenden, um sich bei OpenSearch Dashboards anzumelden, um Daten zu indizieren und zu durchsuchen. OpenSearch Serverless unterstützt Anbieter, die den SAML-2.0-Standard verwenden, z. B. IAM Identity Center, Okta, Keycloak, Active Directory Federation Services (AD FS) und Auth0. Sie können

IAM Identity Center so konfigurieren, dass Benutzer und Gruppen aus anderen Identitätsquellen wie Okta OneLoginund Microsoft Entra ID synchronisiert werden. Eine Liste der von IAM Identity Center unterstützten Identitätsquellen und Schritte zu deren Konfiguration finden Sie unter Erste Schritte im IAM-Identity-Center-Benutzerhandbuch.

> **Note**
>
> Die SAML-Authentifizierung dient nur dem Zugriff auf OpenSearch Dashboards über einen Webbrowser. Authentifizierte Benutzer können Anforderungen an die OpenSearch API-Operationen nur über Entwicklungs-Tools in OpenSearch Dashboards stellen. Mit Ihren SAML-Anmeldeinformationen können Sie keine direkten HTTP-Anfragen an die - OpenSearch API-Operationen stellen.

Zum Einrichten der SAML-Authentifizierung konfigurieren Sie zuerst einen SAML-Identitätsanbieter (IdP). Anschließend nehmen Sie einen oder mehrere Benutzer von diesem IdP in eine Datenzugriffsrichtlinie auf. Diese Richtlinie gewährt ihr bestimmte Berechtigungen für Sammlungen und/oder Indizes. Ein Benutzer kann sich dann bei OpenSearch Dashboards anmelden und die Aktionen ausführen, die in der Datenzugriffsrichtlinie zulässig sind.



Themen

- Überlegungen
- Erforderliche Berechtigungen
- Erstellen von SAML-Anbietern (Konsole)
- Zugreifen auf OpenSearch Dashboards
- Gewährung von Zugriff für SAML-Identitäten auf Sammlungsdaten
- Erstellen von SAML-Anbietern (AWS CLI)
- Anzeigen von SAML-Anbietern
- Aktualisieren von SAML-Anbietern

- Löschen von SAML-Anbietern

Überlegungen

Berücksichtigen Sie beim Konfigurieren der SAML-Authentifizierung Folgendes:

- Signierte und verschlüsselte Anfragen werden nicht unterstützt.
- Verschlüsselte Aussagen werden nicht unterstützt.
- Vom Identitätsanbieter initiierte Authentifizierung und Abmeldung werden nicht unterstützt.

Erforderliche Berechtigungen

Die SAML-Authentifizierung für OpenSearch Serverless verwendet die folgenden AWS Identity and Access Management (IAM)-Berechtigungen:

- `aoss:CreateSecurityConfig` – Erstellt einen SAML-Anbieter.
- `aoss:ListSecurityConfig` – Listet alle SAML-Anbieter im aktuellen Konto auf.
- `aoss:GetSecurityConfig` – Zeigt Informationen zum SAML-Anbieter an.
- `aoss:UpdateSecurityConfig` – Ändert eine bestimmte SAML-Anbieterkonfiguration, einschließlich der XML-Metadaten.
- `aoss:DeleteSecurityConfig` – Löscht einen SAML-Anbieter.

Die folgende identitätsbasierte Zugriffsrichtlinie ermöglicht einem Benutzer die Verwaltung aller IdP-Konfigurationen:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "aoss:CreateSecurityConfig",
                "aoss:DeleteSecurityConfig",
                "aoss:GetSecurityConfig",
                "aoss:UpdateSecurityConfig",
                "aoss:ListSecurityConfigs"
            ],
            "Effect": "Allow",
            "Resource": "*"
```

```
        }
    ]
}
```

Beachten Sie, dass das `Resource`-Element ein Platzhalter sein muss.

Erstellen von SAML-Anbietern (Konsole)

In diesen Schritten wird erläutert, wie SAML-Anbieter erstellt werden. Dadurch wird die SAML-Authentifizierung mit vom Serviceanbieter (SP) initiierter Authentifizierung für OpenSearch Dashboards aktiviert. Die vom Identitätsanbieter initiierte Authentifizierung wird nicht unterstützt.

So aktivieren Sie die SAML-Authentifizierung für OpenSearch Dashboards

1. Melden Sie sich bei der Amazon- OpenSearch Service-Konsole unter https://console.aws.amazon.com/aos/home an.
2. Erweitern Sie im linken Navigationsbereich Serverless und wählen Sie SAML authentication (SAML-Authentifizierung) aus.
3. Wählen Sie Add SAML provider (SAML-Anbieter hinzufügen).
4. Geben Sie einen Namen und eine Beschreibung für die Sammlung an.

   > **Note**
   >
   > Der von Ihnen angegebene Name ist öffentlich zugänglich und wird in einem Dropdown-Menü angezeigt, wenn sich Benutzer bei OpenSearch Dashboards anmelden. Stellen Sie sicher, dass der Name leicht erkennbar ist und keine vertraulichen Informationen über Ihren Identitätsanbieter preisgibt.

5. Kopieren Sie unter Configure your IdP (Konfigurieren Ihres IdP) die URL des Assertion Consumer Service (ACS).
6. Verwenden Sie die ACS-URL, die Sie gerade kopiert haben, um Ihren Identitätsanbieter zu konfigurieren. Terminologie und Schritte variieren je nach Anbieter. Schlagen Sie in der Dokumentation Ihres Anbieters nach.

   In Okta erstellen Sie beispielsweise eine „SAML 2.0-Webanwendung“ und geben die ACS-URL als Single Sign On URL (Single-Sign-On-URL), Recipient URL (Empfänger-URL) und Destination URL (Ziel-URL) an. Für Auth0 geben Sie es in Allowed Callback URLs (Zulässige Rückruf-URLs) an.

7. Geben Sie die Zielgruppeneinschränkung an, falls Ihr IdP ein Feld dafür aufweist. Die Zielgruppenbeschränkung ist ein Wert innerhalb der SAML-Aussagen, der angibt, für wen die Aussagen bestimmt ist. Geben Sie für OpenSearch Serverless an`aws:opensearch:<aws account id>`. Beispiel: `aws:opensearch:123456789012`

   Der Name des Feldes für die Zielgruppenbeschränkung variiert je nach Anbieter. Für Okta ist es der Audience URI (SP Entity ID) (Zielgruppen-URI (SP-Entitäts-ID)). Für IAM Identity Center ist es die Application SAML audience (SAML-Zielgruppe der Anwendung).

8. Wenn Sie IAM Identity Center verwenden, müssen Sie außerdem die folgende Attributzuordnung angeben: `Subject=${user:name}`, mit einem Format von `unspecified`.

9. Nachdem Sie Ihren Identitätsanbieter konfiguriert haben, wird eine IdP-Metadatendatei generiert. Diese XML-Datei enthält Informationen zum Anbieter, z. B. ein TLS-Zertifikat, Single Sign-On-Endpunkte und die Entitäts-ID des Identitätsanbieters.

   Kopieren Sie den Text aus der IdP-Metadaten-Datei und fügen Sie ihn in das Feld Provide metadata from your IdP (Metadaten von Ihrem IdP bereitstellen) ein. Wählen Sie alternativ Aus XML-Datei importieren und laden Sie die Datei hoch. Die Metadatendatei sollte ungefähr so aussehen:

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor entityID="entity-id"
 xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
  <md:IDPSSODescriptor WantAuthnRequestsSigned="false"
 protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>tls-certificate</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>s
    </md:KeyDescriptor>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</
md:NameIDFormat>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</
md:NameIDFormat>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
POST" Location="idp-sso-url"/>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
Redirect" Location="idp-sso-url"/>
  </md:IDPSSODescriptor>
```

```
</md:EntityDescriptor>
```

10. Lassen Sie das Feld Benutzerdefiniertes Benutzer-ID-Attribut leer, um das -`NameID`Element der SAML-Assertion für den Benutzernamen zu verwenden. Wenn Ihre Assertion dieses Standardelement nicht verwendet und stattdessen den Benutzernamen als benutzerdefiniertes Attribut enthält, geben Sie dieses Attribut hier an. Bei Attributen wird zwischen Groß- und Kleinschreibung unterschieden. Es wird nur ein einzelnes Benutzerattribut unterstützt.

    Das folgende Beispiel zeigt ein Überschreibungsattribut für `NameID` in der SAML-Aussage:

    ```
    <saml2:Attribute Name="UserId" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
    format:basic">
      <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:type="xs:string">annie</saml2:AttributeValue>
    </saml2:Attribute>
    ```

11. (Optional) Geben Sie im Feld Group attribute (Gruppenattribut) ein benutzerdefiniertes Attribut an, z. B. `role` oder `group`. Es wird nur ein einzelnes Gruppenattribut unterstützt. Es gibt kein Standard-Gruppenattribut. Wenn Sie keine angeben, können Ihre Datenzugriffsrichtlinien nur Benutzerprinzipale enthalten.

    Das folgende Beispiel zeigt ein Gruppenattribut in der SAML-Aussage:

    ```
    <saml2:Attribute Name="department"
     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:type="xs:string">finance</saml2:AttributeValue>
    </saml2:Attribute>
    ```

12. Standardmäßig meldet OpenSearch Dashboards Benutzer nach 24 Stunden ab. Sie können diesen Wert auf eine beliebige Zahl zwischen 1 und 12 Stunden (15 und 720 Minuten) konfigurieren, indem Sie das OpenSearch Dashboards-Timeout angeben. Wenn Sie versuchen, das Timeout auf oder weniger als 15 Minuten festzulegen, wird Ihre Sitzung auf eine Stunde zurückgesetzt.
13. Wählen Sie Create SAML provider (SAML-Anbieter erstellen).

Zugreifen auf OpenSearch Dashboards

Nachdem Sie einen SAML-Anbieter konfiguriert haben, können alle Benutzer und Gruppen, die diesem Anbieter zugeordnet sind, zum OpenSearch Dashboards-Endpunkt navigieren. Die Dashboards-URL hat das Format *`collection-endpoint`*`/_dashboards/` für alle Sammlungen .

Wenn Sie SAML aktiviert haben, werden Sie über den Link in der zur IdP-Auswahlseite AWS Management Console weitergeleitet, auf der Sie sich mit Ihren SAML-Anmeldeinformationen anmelden können. Verwenden Sie zunächst das Dropdown-Menü, um einen Identitätsanbieter auszuwählen:

Melden Sie sich anschließend mit den Anmeldeinformationen Ihres Identitätsanbieters an.

Wenn Sie SAML nicht aktiviert haben, AWS Management Console werden Sie über den Link in der angewiesen, sich als IAM-Benutzer oder -Rolle anzumelden, ohne dass SAML verfügbar ist.

Gewährung von Zugriff für SAML-Identitäten auf Sammlungsdaten

Nachdem Sie einen SAML-Anbieter erstellt haben, müssen Sie den zugrunde liegenden Benutzern und Gruppen immer noch Zugriff auf die Daten in Ihren Sammlungen gewähren. Sie gewähren Zugriff über Datenzugriffsrichtlinien. Solange Sie Benutzern keinen Zugriff gewähren, können diese keine Daten in Ihren Sammlungen lesen, schreiben oder löschen.

Erstellen Sie zum Gewähren des Zugriffs eine Datenzugriffsrichtlinie und geben Sie Ihre SAML-Benutzer- und/oder -Gruppen-IDs in der `Principal`-Anweisung an:

```
[
   {
      "Rules":[
       ...
      ],
      "Principal":[
         "saml/987654321098/myprovider/user/Shaheen",
         "saml/987654321098/myprovider/group/finance"
      ]
   }
]
```

Sie können Zugriff auf Sammlungen, Indizes oder beides gewähren. Wenn Sie möchten, dass verschiedene Benutzer über unterschiedliche Berechtigungen verfügen, erstellen Sie mehrere Regeln. Eine Liste der verfügbaren Berechtigungen finden Sie unter Unterstützte Richtlinienberechtigungen. Weitere Informationen zum Formatieren einer Zugriffsrichtlinie finden Sie unter Richtliniensyntax.

Erstellen von SAML-Anbietern (AWS CLI)

Senden Sie eine -CreateSecurityConfigAnforderung, um einen SAML-Anbieter mit der OpenSearch Serverless-API zu erstellen:

```
aws opensearchserverless create-security-config \
    --name myprovider \
    --type saml \
    --saml-options file://saml-auth0.json
```

Geben Sie `saml-options`, einschließlich der Metadaten-XML, als Schlüsselwert-Zuordnung in einer .json-Datei an. Die Metadaten-XML muss als JSON-Escape-Zeichenfolge codiert werden.

```
{
   "sessionTimeout": 70,
   "groupAttribute": "department",
   "userAttribute": "userid",
   "metadata": "<EntityDescriptor xmlns=\"urn:oasis:names:tc:SAML:2.0:metadata
\" ... ... ... IDPSSODescriptor>\r\n<\/EntityDescriptor>"
}
```

Anzeigen von SAML-Anbietern

Die folgende ListSecurityConfigs Anforderung listet alle SAML-Anbieter in Ihrem Konto auf:

```
aws opensearchserverless list-security-configs --type saml
```

Die Anfrage gibt Informationen zu allen vorhandenen SAML-Anbietern zurück, einschließlich der vollständigen IdP-Metadaten, die Ihr Identitätsanbieter generiert:

```
{
   "securityConfigDetails": [
      {
         "configVersion": "MTY2NDA1MjY4NDQ5M18x",
         "createdDate": 1664054180858,
         "description": "Example SAML provider",
         "id": "saml/123456789012/myprovider",
         "lastModifiedDate": 1664054180858,
         "samlOptions": {
            "groupAttribute": "department",
            "metadata": "<EntityDescriptor xmlns=\"urn:oasis:names:tc:SAML:2.0:metadata
\" ... ... ... IDPSSODescriptor>\r\n<\/EntityDescriptor>",
            "sessionTimeout": 120,
            "userAttribute": "userid"
         }
      }
   ]
}
```

Um Details zu einem bestimmten Anbieter anzuzeigen, einschließlich des `configVersion` für zukünftige Updates, senden Sie eine `GetSecurityConfig`-Anfrage.

Aktualisieren von SAML-Anbietern

Um einen SAML-Anbieter über die OpenSearch Serverless-Konsole zu aktualisieren, wählen Sie SAML-Authentifizierung, wählen Sie Ihren Identitätsanbieter und dann Bearbeiten aus. Sie können alle Felder ändern, einschließlich der Metadaten und derb benutzerdefinierten Attribute.

Um einen Anbieter über die OpenSearch Serverless-API zu aktualisieren, senden Sie eine -UpdateSecurityConfigAnforderung und fügen Sie die ID der zu aktualisierenden Richtlinie ein. Sie müssen auch eine Konfigurationsversion angeben, die Sie mithilfe der `ListSecurityConfigs`- oder `GetSecurityConfig`-Befehle abrufen können. Die Angabe der neuesten Version stellt sicher, dass Sie nicht versehentlich eine Änderung überschreiben, die von jemand anderem vorgenommen wurde.

Die folgende Anfrage aktualisiert die SAML-Optionen für einen Anbieter:

```
aws opensearchserverless update-security-config \
    --id saml/123456789012/myprovider \
    --type saml \
    --saml-options file://saml-auth0.json \
    --config-version MTY2NDA1MjY4NDQ5M18x
```

Geben Sie Ihre SAML-Konfigurationsoptionen als Schlüsselwert-Zuordnung in einer .json-Datei an.

> **Important**
>
> Aktualisierungen von SAML-Optionen erfolgen nicht inkrementell. Wenn Sie bei einer Aktualisierung keinen Wert für einen Parameter im `SAMLOptions`-Objekt angeben, werden die vorhandenen Werte mit leeren Werten überschrieben. Wenn die aktuelle Konfiguration beispielsweise einen Wert für `userAttribute` enthält und Sie dann eine Aktualisierung vornehmen und diesen Wert nicht angeben, wird der Wert aus der Konfiguration entfernt. Stellen Sie sicher, dass Sie die vorhandenen Werte kennen, bevor Sie eine Aktualisierung durch Aufrufen der `GetSecurityConfig`-Operation vornehmen.

Löschen von SAML-Anbietern

Wenn Sie einen SAML-Anbieter löschen, sind alle Verweise auf zugeordnete Benutzer und Gruppen in Ihren Datenzugriffsrichtlinien nicht mehr funktionsfähig. Um Verwirrung zu vermeiden, empfehlen

wir Ihnen, alle Verweise auf den Endpunkt in Ihren Zugriffsrichtlinien zu entfernen, bevor Sie den Endpunkt löschen.

Um einen SAML-Anbieter mit der OpenSearch Serverless-Konsole zu löschen, wählen Sie Authentifizierung, wählen Sie den Anbieter und dann Löschen aus.

Senden Sie eine -DeleteSecurityConfigAnforderung, um einen Anbieter über die OpenSearch Serverless-API zu löschen:

```
aws opensearchserverless delete-security-config --id saml/123456789012/myprovider
```

Konformitätsvalidierung für Amazon OpenSearch Serverless

Externe Prüfer bewerten die Sicherheit und Konformität von Amazon OpenSearch Serverless im Rahmen mehrerer AWS Compliance-Programme. Zu diesen Programmen gehören SOC, PCI und HIPAA.

Informationen darüber, ob AWS-Service ein in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter AWS-Services Umfang nach Compliance-Programm AWS-Services unter . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen unter .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- Schnellstartanleitungen zu Sicherheit und Compliance — In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Implementierung von Basisumgebungen beschrieben AWS , bei denen Sicherheit und Compliance im Mittelpunkt stehen.
- Architecting for HIPAA Security and Compliance on Amazon Web Services — In diesem Whitepaper wird beschrieben, wie Unternehmen HIPAA-fähige Anwendungen erstellen AWS können.

> **Note**
>
> AWS-Services Nicht alle sind HIPAA-fähig. Weitere Informationen finden Sie in der Referenz für HIPAA-berechtigte Services.

- AWS Compliance-Ressourcen — Diese Sammlung von Arbeitsmappen und Leitfäden gilt möglicherweise für Ihre Branche und Ihren Standort.
- AWS Leitfäden zur Einhaltung von Vorschriften für Kunden — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.
- Evaluierung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub— Auf diese AWS-Service Weise erhalten Sie einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerungsreferenz.
- Amazon GuardDuty — Dies AWS-Service erkennt potenzielle Bedrohungen für Ihre Workloads AWS-Konten, Container und Daten, indem es Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen wie PCI DSS zu erfüllen, indem es die in bestimmten Compliance-Frameworks vorgeschriebenen Anforderungen zur Erkennung von Eindringlingen erfüllt.
- AWS Audit Manager— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Markieren von Amazon-OpenSearch-Serverless-Sammlungen

Mit Tags können Sie einer Amazon-OpenSearch-Serverless-Sammlung beliebige Informationen zuweisen, damit Sie diese Informationen kategorisieren und filtern können. Ein Tag ist ein Metadaten-Etikett, das von Ihnen oder von AWS einer AWS-Ressource zugewiesen wird.

Jedes Tag besteht aus einem Schlüssel und einem Wert. Für Tags, die Sie zuweisen, definieren Sie einen Schlüssel und einen Wert. So können Sie beispielsweise den Schlüssel als `stage` und den Wert für eine Ressource als `test` definieren.

Mithilfe von Tags können Sie Folgendes tun:

- Identifizieren und organisieren Sie Ihre AWS-Ressourcen. Viele AWS-Services unterstützen das Markieren mit Tags (kurz: Tagging). So können Ressourcen aus verschiedenen Services dasselbe Tag zuweisen, um anzugeben, dass die Ressourcen verbunden sind. Beispielsweise könnten Sie einer OpenSearch-Serverless-Sammlung dasselbe Tag zuweisen, das Sie einer Amazon-OpenSearch-Service-Domäne zuweisen.
- Überwachen von AWS-Kosten. You activate these tags on the AWS Billing and Cost Management dashboard. AWS uses the tags to categorize your costs and deliver a monthly cost allocation report to you. Weitere Informationen finden Sie unter Verwendung von Kostenzuordnungs-Tags im AWS Billing-Benutzerhandbuch.

Die primäre Ressource in OpenSearch Serverless ist eine Sammlung. Sie können die OpenSearch-Service-Konsole, das AWS CLI, die OpenSearch-Serverless-API-Operationen oder die AWS-SDKs verwenden, um Tags zu einer Sammlung hinzuzufügen, zu verwalten und daraus zu entfernen.

Erforderliche Berechtigungen

OpenSearch Serverless verwendet die folgenden AWS Identity and Access Management Access Analyzer (IAM)-Berechtigungen zum Markieren von Sammlungen:

- `aoss:TagResource`
- `aoss:ListTagsForResource`
- `aoss:UntagResource`

Arbeiten mit Tags (Konsole)

Die Konsole ist die einfachste Möglichkeit, eine Sammlung zu markieren.

So erstellen Sie ein Tag (Konsole)

1. Melden Sie sich bei der Amazon OpenSearch Service Konsole unter https://console.aws.amazon.com/aos/home an.

2. Erweitern Sie im linken Navigationsbereich Serverless und wählen Sie Collections (Sammlungen) aus.
3. Wählen Sie die Sammlung aus, der Sie Tags hinzufügen möchten, und gehen Sie zur Registerkarte Tags.
4. Wählen Sie Verwalten und neues Tag hinzufügen.
5. Geben Sie einen Tag-Schlüssel und einen optionalen Wert ein.
6. Wählen Sie Save (Speichern).

Um ein Tag zu löschen, führen Sie die gleichen Schritte aus und wählen Sie Entfernen auf der Seite Tags verwalten.

Weitere Informationen zur Verwendung der Konsole für die Arbeit mit Tags finden Sie unter Tag Editor im AWSHandbuch „Erste Schritte“ der Managementkonsole.

Arbeiten mit Tags (AWS CLI)

Um eine Sammlung mit dem AWS CLI zu markieren, senden Sie eine TagResource-Anfrage:

```
aws opensearchserverless tag-resource
  --resource-arn arn:aws:aoss:us-east-1:123456789012:collection/my-collection
  --tags Key=service,Value=aoss Key=source,Value=logs
```

Zeigen Sie die vorhandenen Tags für eine Sammlung mit dem ListTagsForResource-Befehl an:

```
aws opensearchserverless list-tags-for-resource
  --resource-arn arn:aws:aoss:us-east-1:123456789012:collection/my-collection
```

Entfernen Sie Tags aus einer Sammlung mit dem UntagResource-Befehl:

```
aws opensearchserverless untag-resource
  --resource-arn arn:aws:aoss:us-east-1:123456789012:collection/my-collection
  --tag-keys service
```

Unterstützte Operationen und Plugins in Amazon OpenSearch Serverless

Amazon OpenSearch Serverless unterstützt eine Vielzahl von OpenSearch Plug-ins sowie einen Teil der Indexierungs-, Such- und Metadaten-API-Operationen, die in verfügbar sind. OpenSearch Sie können die Berechtigungen in der linken Spalte der Tabelle in Datenzugriffsrichtlinien aufnehmen, um den Zugriff auf bestimmte Vorgänge zu beschränken.

Themen

Unterstützte OpenSearch API-Operationen und Berechtigungen

In der folgenden Tabelle sind die API-Operationen aufgeführt, die OpenSearch Serverless unterstützt, zusammen mit den entsprechenden Datenzugriffsrichtlinienberechtigungen:

Berechtigung der Datenzugriffsrichtlinie	OpenSearch API-Operationen	Beschreibung und Vorbehalte
`aoss:CreateIndex`	PUT <index>	Erstellen Sie Indizes. Weitere Informationen finden Sie unter Index erstellen. **Note** Diese Berechtigung gilt auch für die Erstellung von Indizes mit den Beispieldaten auf OpenSearch Dashboards.

Berechtigung der Datenzugriffsrichtlinie	OpenSearch API-Operationen	Beschreibung und Vorbehalte
`aoss:DescribeIndex`	• GET <index> • GET <index>/_mapping • GET <index>/_mappings • GET <index>/_setting • GET <index>/_setting/<setting> • GET <index>/_settings • GET <index>/_settings/<setting> • GET _cat/indices • GET _mapping • GET _mappings • GET _resolve/index/<index> • KOPF <index>	Beschreiben Sie Indizes. Weitere Informationen finden Sie in den folgenden Ressourcen: • Get index • Eine Zuordnung abrufen • Einstellungen abrufen • Der Index ist vorhanden • CAT-Indizes (Die Antwort enthält keine `health status` Or-Felder.)

Berechtigung der Datenzugriffsrichtlinie	OpenSearch API-Operationen	Beschreibung und Vorbehalte
`aoss:WriteDocument`	• LÖSCHEN SIE <index>/_doc/<id> • POST <index>/_bulk • POST <index>/_create/<id> (nur für Suchsammlungstypen) • POST <index>/_doc • POST <index>/_update/<id> (nur für Suchsammlungstypen) • POST _bulk • PUT <index>/_create/<id> (nur für Suchsammlungstypen) • PUT <index>/_doc/<id> (nur für Suchsammlungstypen)	Schreiben und Aktualisieren Sie Dokumente. Weitere Informationen finden Sie in den folgenden Ressourcen: • Masse • Datenindex **Note** Einige Operationen sind nur für Sammlungen des Typs `SEARCH` zulässig. Weitere Informationen finden Sie unter the section called “Auswahl eines Sammlungstyps”.

Berechtigung der Datenzugriffsrichtlinie	OpenSearch API-Operationen	Beschreibung und Vorbehalte
`aoss:ReadDocument`	• GET <index>/_analyze • GET <index>/_doc/<id> • GET <index>/_explain/<id> • GET <index>/_mget • GET <index>/_source/<id> • GET <index>/_count • GET <index>/_field_caps • GET <index>/_msearch • GET <index>/_rank_eval • GET <index>/_search • GET <index>/_validate/<query> • GET _analyze • GET _field_caps • GET _mget • GET _search • HEAD <index>/_doc/<id> • HEAD <index>/_source/<id> • POST <index>/_analyze • POST <index>/_explain/<id> • POST <index>/_count • POST <index>/_field_caps • POST <index>/_rank_eval • POST <index>/_search • POST _analyze • POST _field_caps • POST _search	Lesen Sie Dokumente . Weitere Informationen finden Sie in den folgenden Ressourcen: • Textanalyse durchführen • Dokument abrufen • Count • DSL abfragen • Auswertung der Evaluierung • API analysieren • Explain

Berechtigung der Datenzugriffsrichtlinie	OpenSearch API-Operationen	Beschreibung und Vorbehalte
`aoss:DeleteIndex`	DELETE <target>	Löschen Sie Indizes. Weitere Informationen finden Sie unter Index löschen.
`aoss:UpdateIndex`	• POST _mapping • POST <index>/_mapping/ • POST <index>/_mappings/ • POST <index>/_setting • POST <index>/_settings • POST _setting • POST _settings • PUT _mapping • GET <index>/_mapping • GET <index>/_mappings/ • GET <index>/_setting • GET <index>/_settings • PUT _setting • PUT _settings	Aktualisieren von Index-Einstellungen. Weitere Informationen finden Sie in den folgenden Ressourcen: • Zuweisung • Einstellungen aktualisieren
`aoss:CreateCollectionItems`	POST _aliases	Erstellen Sie Index-Aliase. Weitere Informationen finden Sie unter Aliasse erstellen.

Berechtigung der Datenzugriffsrichtlinie	OpenSearch API-Operationen	Beschreibung und Vorbehalte
`aoss:DescribeCollectionItems`	• GET <index>/_alias/<alias> • GET _alias • GET _alias/<alias> • GET _cat/aliases • GET _cat/templates • GET _cat/templates/<template_name> • GET _component_template • GET _component_template/<component-template> • GET _index_template • GET _index_template/<index-template> • HEAD _alias/<alias> • HEAD _component_template/<component-template> • HEAD _index_template/<name> • HEAD <index>/_alias/<alias>	Beschreiben Sie Aliase und Index-Vorlagen. Weitere Informationen finden Sie in den folgenden Ressourcen: • Verwalten von Aliase • Index-Vorlagen

Berechtigung der Datenzugriffsrichtlinie	OpenSearch API-Operationen	Beschreibung und Vorbehalte
`aoss:UpdateCollectionItems`	• POST <index>/_alias/<alias> • POST <index>/_aliases/<alias> • POST _component_template/<component-template> • POST _index_template/<index-template> • PUT <index>/_alias/<alias> • PUT <index>/_aliases/<alias> • PUT _component_template/<component-template> • PUT _index_template/<index-template>	Aktualisieren Sie Aliase und Index-Vorlagen. Weitere Informationen finden Sie in den folgenden Ressourcen: • Aliase indizieren • Index-Vorlagen
`aoss:DeleteCollectionItems`	• DELETE <index>/_alias/<alias> • DELETE _component_template/<component-template> • DELETE _index_template/<index-template> • DELETE <index>/_aliases/<alias>	Löschen Sie Aliase und Index-Vorlagen. Weitere Informationen finden Sie in den folgenden Ressourcen: • Aliase löschen • Eine Vorlage löschen

OpenSearch Unterstützte Plugins

OpenSearch Serverlose Sammlungen sind mit den folgenden Plugins aus der OpenSearch Community vorkonfiguriert. Serverless stellt Plugins automatisch bereit und verwaltet sie für Sie.

Analyse-Plugins

- ICU Analysis
- Japanese (kuromoji) Analysis
- Koreanische (Nori)-Analyse
- Phonetic Analysis

- Smart Chinese Analysis
- Stempel Polish Analysis
- Ukrainische Analyse

Mapper-Plugins

- Mapper Size
- Mapper Murmur3
- Mapper-annotierter Text

Skript-Plugins

- Painless
- Expression
- Mustache

Darüber hinaus enthält OpenSearch Serverless alle Plugins, die als Module ausgeliefert werden.

Überwachen von Amazon OpenSearch Serverless

Die Überwachung ist wichtig, um die Zuverlässigkeit, Verfügbarkeit und Leistung von Amazon OpenSearch Serverless und Ihren anderen - AWS Lösungen aufrechtzuerhalten. AWS bietet die folgenden Überwachungstools, um OpenSearch Serverless zu überwachen, Missstände zu melden und gegebenenfalls automatische Maßnahmen zu ergreifen:

- Amazon CloudWatch überwacht Ihre AWS Ressourcen und die Anwendungen, auf denen Sie ausgeführt werden, AWS in Echtzeit. Sie können Kennzahlen erfassen und verfolgen, benutzerdefinierte Dashboards erstellen und Alarme festlegen, die Sie benachrichtigen oder Maßnahmen ergreifen, wenn eine bestimmte Metrik einen von Ihnen festgelegten Schwellenwert erreicht.

  Sie können beispielsweise die CPU-Auslastung oder andere Metriken Ihrer Amazon EC2 CloudWatch verfolgen lassen und bei Bedarf automatisch neue Instances starten. Weitere Informationen finden Sie im Amazon- CloudWatch Benutzerhandbuch.
- AWS CloudTrail erfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihrer AWS-Konto. Es stellt die Protokolldateien in einem von Ihnen angegebenen Amazon-S3-Bucket

bereit. Sie können feststellen, welche Benutzer und Konten aufgerufen haben AWS, von welcher Quell-IP-Adresse die Aufrufe stammen und wann die Aufrufe erfolgt sind. Weitere Informationen finden Sie im AWS CloudTrail -Benutzerhandbuch.

- Amazon EventBridge stellt einen Stream von Systemereignissen in nahezu Echtzeit bereit, der Änderungen in Ihren OpenSearch Service-Domains beschreibt. Sie können Regeln erstellen, die bestimmte Ereignisse überwachen und automatisierte Aktionen in anderen auslösen, AWS-Services wenn diese Ereignisse auftreten. Weitere Informationen finden Sie im Amazon-EventBridge Benutzerhandbuch.

Überwachen von OpenSearch Serverless mit Amazon CloudWatch

Sie können Amazon OpenSearch Serverless mit überwachen CloudWatch, das Rohdaten sammelt und sie in lesbare Metriken verarbeitet, die nahezu in Echtzeit vorliegen. Diese Statistiken werden 15 Monate gespeichert, damit Sie auf Verlaufsinformationen zugreifen können und einen besseren Überblick darüber erhalten, wie Ihre Webanwendung oder der Service ausgeführt werden.

Sie können auch Alarme einrichten, die auf bestimmte Grenzwerte achten und Benachrichtigungen senden oder Aktivitäten auslösen, wenn diese Grenzwerte erreicht werden. Weitere Informationen finden Sie im Amazon- CloudWatch Benutzerhandbuch.

OpenSearch Serverless meldet die folgenden Metriken im -`AWS/AOSS`Namespace.

Metrik	Beschreibung
`ActiveCollection`	Zeigt an, ob eine Sammlung aktiv ist. Ein Wert von 1 bedeutet, dass sich die Sammlung in einem `ACTIVE`-Status befindet. Dieser Wert wird bei erfolgreicher Erstellung einer Sammlung ausgegeben und verbleibt 1, bis Sie die Sammlung löschen. Die Metrik darf keinen Wert von 0 haben. Relevante Statistiken: Maximum Dimensionen: `ClientId`, `CollectionId` , `CollectionName` Frequenz: 60 Sekunden

Metrik	Beschreibung
`DeletedDocuments`	Die Gesamtzahl der gelöschten Dokumente. Relevante Statistiken: Durchschnitt, Summe Dimensionen: `ClientId`, `CollectionId` , `CollectionName` , `IndexId`, `IndexName` Frequenz: 60 Sekunden
`IndexingOCU`	Die Anzahl der OpenSearch Compute Units (OCUs), die zum Erfassen von Sammlungsdaten verwendet werden. Diese Metrik gilt auf Kontoebene. Relevante Statistiken: Summe Dimensionen: `ClientId` Frequenz: 60 Sekunden
`IngestionDataRate`	Die Indexierungsrate in GB pro Sekunde für eine Sammlung oder einen Index. Diese Metrik gilt nur für Anfragen zur Massenindexierung. Relevante Statistiken: Summe Dimensionen: `ClientId`, `CollectionId` , `CollectionName` , `IndexId`, `IndexName` Frequenz: 60 Sekunden

Metrik	Beschreibung
`IngestionDocumentErrors`	Die Gesamtzahl von Dokumentfehlern während der Erfassung für eine Sammlung oder einen Index. Nach einer erfolgreichen Massenindizierungsanfrage verarbeiten Autoren die Anfrage und geben Fehler für alle fehlgesch lagenen Dokumente innerhalb der Anfrage aus. Relevante Statistiken: Summe Dimensionen: `ClientId`, `CollectionId` , `Collectio nName` , `IndexId`, `IndexName` Frequenz: 60 Sekunden
`IngestionDocumentRate`	Die Rate pro Sekunde, mit der Dokumente in eine Sammlung oder einen Index aufgenommen werden. Diese Metrik gilt nur für Anfragen zur Massenindizierung. Relevante Statistiken: Summe Dimensionen: `ClientId`, `CollectionId` , `Collectio nName` , `IndexId`, `IndexName` Frequenz: 60 Sekunden
`IngestionRequestErrors`	Die Gesamtzahl der Massenindizierungsanforderu ngsfehler an eine Sammlung. OpenSearch Serverless gibt diese Metrik aus, wenn eine Massenindizierungsanforderu ng aus irgendeinem Grund fehlschlägt, z. B. aufgrund eines Authentifizierungs- oder Verfügbarkeitsproblems. Relevante Statistiken: Summe Dimensionen: `ClientId`, `CollectionId` , `Collectio nName` Frequenz: 60 Sekunden

Metrik	Beschreibung
IngestionRequestLatency	Die Latenz in Sekunden für Massenschreibvorgänge in eine Sammlung. Relevante Statistiken: Minimum, Maximum, Durchschnitt Dimensionen: ClientId, CollectionId , CollectionName Frequenz: 60 Sekunden
IngestionRequestRate	Die Gesamtzahl der von einer Sammlung empfangenen Massenschreibvorgänge. Relevante Statistiken: Minimum, Maximum, Durchschnitt Dimensionen: ClientId, CollectionId , CollectionName Frequenz: 60 Sekunden
IngestionRequestSuccess	Die Gesamtzahl der erfolgreichen Indizierungsvorgänge einer Sammlung. Relevante Statistiken: Summe Dimensionen: ClientId, CollectionId , CollectionName Frequenz: 60 Sekunden
SearchableDocuments	Die Gesamtzahl der durchsuchbaren Dokumente in einer Sammlung oder einem Index. Relevante Statistiken: Summe Dimensionen: ClientId, CollectionId , CollectionName , IndexId, IndexName Frequenz: 60 Sekunden

Metrik	Beschreibung
`SearchRequestErrors`	Die Gesamtzahl der Abfragefehler pro Minute für eine Sammlung. Relevante Statistiken: Summe Dimensionen: `ClientId`, `CollectionId` , `CollectionName` Frequenz: 60 Sekunden
`SearchRequestLatency`	Die durchschnittliche Zeit in Millisekunden, die zum Abschließen eines Suchvorgangs für eine Sammlung benötigt wird. Relevante Statistiken: Minimum, Maximum, Durchschnitt Dimensionen: `ClientId`, `CollectionId` , `CollectionName` Frequenz: 60 Sekunden
`SearchOCU`	Die Anzahl der OpenSearch Compute Units (OCUs), die zum Durchsuchen von Sammlungsdaten verwendet werden. Diese Metrik gilt auf Kontoebene. Relevante Statistiken: Summe Dimensionen: `ClientId` Frequenz: 60 Sekunden

Metrik	Beschreibung
`SearchRequestRate`	Die Gesamtzahl der Suchanfragen pro Minute für eine Sammlung. Relevante Statistiken: Durchschnitt, Maximum, Summe Dimensionen: `ClientId`, `CollectionId` , `CollectionName` Frequenz: 60 Sekunden
`StorageUsedInS3`	Die Menge des verwendeten Amazon S3-Speichers in Byte. OpenSearch Serverless speichert indizierte Daten in Amazon S3. Sie müssen den Zeitraum von einer Minute auswählen, um einen genauen Wert zu erhalten. Relevante Statistiken: Summe Dimensionen: `ClientId`, `CollectionId` , `CollectionName` , `IndexId`, `IndexName` Frequenz: 60 Sekunden
`2xx, 3xx, 4xx, 5xx`	Die Anzahl der Anforderungen an die Sammlung, die zu dem angegebenen HTTP-Antwortcode (2xx, 3xx, 4xx, 5xx) geführt haben. Relevante Statistiken: Summe Dimensionen: `ClientId`, `CollectionId` , `CollectionName` Frequenz: 60 Sekunden

Protokollieren von OpenSearch Serverless-API-Aufrufen mit AWS CloudTrail

Amazon OpenSearch Serverless ist in integriert, einem Service AWS CloudTrail, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem - AWS Service in Serverless durchgeführten Aktionen bietet.

CloudTrail erfasst alle API-Aufrufe für OpenSearch Serverless als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe aus dem Abschnitt Serverless der OpenSearch Servicekonsole und Codeaufrufe der OpenSearch Serverless-API-Operationen.

Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3-Bucket aktivieren, einschließlich Ereignissen für OpenSearch Serverless. Wenn Sie keinen Trail konfigurieren, können Sie trotzdem die neuesten Ereignisse in der CloudTrail Konsole unter Ereignisverlauf anzeigen.

Anhand der von CloudTrailgesammelten Informationen können Sie die an OpenSearch Serverless gestellte Anfrage, die IP-Adresse, von der die Anfrage gestellt wurde, den Initiator der Anfrage, den Zeitpunkt der Anfrage und zusätzliche Details bestimmen.

Weitere Informationen zu CloudTrailfinden Sie im AWS CloudTrail -Benutzerhandbuch.

OpenSearch Serverless-Informationen in CloudTrail

CloudTrail wird auf Ihrem aktiviert AWS-Konto , wenn Sie das Konto erstellen. Wenn eine Aktivität in OpenSearch Serverless auftritt, wird diese Aktivität in einem - CloudTrail Ereignis zusammen mit anderen - AWS Serviceereignissen im Ereignisverlauf aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem anzeigen, suchen und herunterladen AWS-Konto. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail Ereignisverlauf .

Erstellen Sie für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS-Konto, einschließlich Ereignissen für OpenSearch Serverless, einen Trail. Ein Trail ermöglicht CloudTrail die Bereitstellung von Protokolldateien an einen Amazon S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen.

Der Trail protokolliert Ereignisse aus allen Regionen in der - AWS Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon S3-Bucket bereit. Darüber hinaus können Sie andere - AWS Services konfigurieren, um die in den CloudTrail Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie hier:

- Übersicht zum Erstellen eines Trails
- CloudTrail Von unterstützte Services und Integrationen
- Konfigurieren von Amazon SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien aus mehreren Konten

Alle OpenSearch Serverless-Aktionen werden von protokolliert CloudTrail und sind in der OpenSearch Serverless-API-Referenz dokumentiert. Aufrufe der `DeleteCollection` Aktionen `CreateCollection`, `ListCollections`sund erzeugen beispielsweise Einträge in den CloudTrail Protokolldateien.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen helfen Ihnen beim Bestimmen der Folgenden Elemente:

- Ob die Anforderung mit Root- oder AWS Identity and Access Management (IAM)-Benutzeranmeldeinformationen ausgeführt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anforderung von einem anderen - AWS Service gestellt wurde.

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

Grundlegendes zu Serverless OpenSearch -Protokolldateieinträgen

Ein Trail ist eine Konfiguration, die die Bereitstellung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge.

Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar. Sie enthält Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordnetes Stacktrace der öffentlichen API-Aufrufe und erscheinen daher nicht in einer bestimmten Reihenfolge.

Das folgende Beispiel zeigt einen - CloudTrail Protokolleintrag, der die `CreateCollection` Aktion demonstriert.

```
{
   "eventVersion":"1.08",
```

```
   "userIdentity":{
      "type":"AssumedRole",
      "principalId":"AIDACKCEVSQ6C2EXAMPLE",
      "arn":"arn:aws:iam::123456789012:user/test-user",
      "accountId":"123456789012",
      "accessKeyId":"access-key",
      "sessionContext":{
         "sessionIssuer":{
            "type":"Role",
            "principalId":"AIDACKCEVSQ6C2EXAMPLE",
            "arn":"arn:aws:iam::123456789012:role/Admin",
            "accountId":"123456789012",
            "userName":"Admin"
         },
         "webIdFederationData":{

         },
         "attributes":{
            "creationDate":"2022-04-08T14:11:34Z",
            "mfaAuthenticated":"false"
         }
      }
   },
   "eventTime":"2022-04-08T14:11:49Z",
   "eventSource":"aoss.amazonaws.com",
   "eventName":"CreateCollection",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"AWS Internal",
   "userAgent":"aws-cli/2.1.30 Python/3.8.8 Linux/5.4.176-103.347.amzn2int.x86_64 exe/
x86_64.amzn.2 prompt/off command/aoss.create-collection",
   "errorCode":"HttpFailureException",
   "errorMessage":"An unknown error occurred",
   "requestParameters":{
      "accountId":"123456789012",
      "name":"test-collection",
      "description":"A sample collection",
      "clientToken":"d3a227d2-a2a7-49a6-8fb2-e5c8303c0718"
   },
   "responseElements": null,
   "requestID":"12345678-1234-1234-1234-987654321098",
   "eventID":"12345678-1234-1234-1234-987654321098",
   "readOnly":false,
   "eventType":"AwsApiCall",
   "managementEvent":true,
```

```
    "recipientAccountId":"123456789012",
    "eventCategory":"Management",
    "tlsDetails":{
       "clientProvidedHostHeader":"user.aoss-sample.us-east-1.amazonaws.com"
    }
}
```

Überwachen von OpenSearch Serverless-Ereignissen mit Amazon EventBridge

Amazon OpenSearch Service lässt sich in Amazon integrieren EventBridge , um Sie über bestimmte Ereignisse zu informieren, die sich auf Ihre Domains auswirken. Ereignisse von - AWS Services werden nahezu EventBridge in Echtzeit an übermittelt. Die gleichen Ereignisse werden auch an Amazon CloudWatch Events , den Vorgänger von Amazon , gesendet EventBridge. Sie können Regeln schreiben, um anzugeben, welche Ereignisse für Sie von Interesse sind und welche automatisierten Aktionen zu ergreifen sind, wenn ein Ereignis mit einer Regel übereinstimmt. Beispiele für Aktionen, die Sie automatisch aktivieren können, sind die folgenden:

- Aufrufen einer - AWS Lambda Funktion
- Aufrufen eines Amazon EC2-Ausführungsbefehls
- Weiterleiten des Ereignisses an Amazon Kinesis Data Streams
- Aktivieren eines AWS Step Functions-Zustandsautomaten
- Benachrichtigen eines Amazon SNS-Themas oder einer Amazon SQS-Warteschlange

Weitere Informationen finden Sie unter Erste Schritte mit Amazon EventBridge im Amazon-EventBridge Benutzerhandbuch.

Einrichten von Benachrichtigungen

Sie können AWS Benutzerbenachrichtigungen verwenden, um Benachrichtigungen zu erhalten, wenn ein OpenSearch -Serverless-Ereignis eintritt. Ein Ereignis ist ein Indikator für eine Änderung in der OpenSearch Serverless-Umgebung, z. B. wenn Sie das maximale Limit Ihrer OCU-Nutzung erreichen. Amazon EventBridge empfängt das Ereignis und leitet eine Benachrichtigung an das AWS Management Console Notifications Center und die von Ihnen ausgewählten Übermittlungskanäle weiter. Sie erhalten eine Benachrichtigung, wenn ein Ereignis einer von Ihnen angegebenen Regel entspricht.

OpenSearch Ereignisse für Datenverarbeitungseinheiten (OCU)

OpenSearch Serverless sendet Ereignisse an , EventBridge wenn eines der folgenden OCU-bezogenen Ereignisse eintritt.

OCU-Nutzung nähert sich dem Höchstlimit

OpenSearch Serverless sendet dieses Ereignis, wenn Ihre OCU-Auslastung 75 % Ihres Kapazitätslimits erreicht. Ihre OCU-Nutzung wird basierend auf Ihrem konfigurierten Kapazitätslimit und Ihrem aktuellen OCU-Verbrauch berechnet.

Beispiel

Im Folgenden finden Sie ein Beispielereignis dieses Typs (Such-OCU):

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "OCU Utilization Approaching Max Limit",
  "source": "aws.aoss",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "eventTime" : 1678943345789,
    "description": "Your search OCU usage is at 75% and is approaching the configured
 maximum limit."
  }
}
```

Im Folgenden finden Sie ein Beispielereignis dieses Typs (Index-OCU):

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "OCU Utilization Approaching Max Limit",
  "source": "aws.aoss",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
```

```
  "detail": {
    "eventTime" : 1678943345789,
    "description": "Your indexing OCU usage is at 75% and is approaching the configured
 maximum limit."
  }
```

OCU-Nutzung hat das maximale Limit erreicht

OpenSearch Serverless sendet dieses Ereignis, wenn Ihre OCU-Nutzung für die Suche oder Indizierung 100 % Ihres Kapazitätslimits erreicht. Ihre OCU-Nutzung wird basierend auf Ihrem konfigurierten Kapazitätslimit und Ihrem aktuellen OCU-Verbrauch berechnet.

Beispiel

Im Folgenden finden Sie ein Beispielereignis dieses Typs (Such-OCU):

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "OCU Utilization Reached Max Limit",
  "source": "aws.aoss",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "eventTime" : 1678943345789,
    "description": "Your search OCU usage has reached the configured maximum limit."
  }
}
```

Im Folgenden finden Sie ein Beispielereignis dieses Typs (Index-OCU):

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "OCU Utilization Reached Max Limit",
  "source": "aws.aoss",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
```

```
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "eventTime" : 1678943345789,
    "description": "Your indexing OCU usage has reached the configured maximum limit."
  }
}
```

Amazon OpenSearch Service-Domains erstellen und verwalten

In diesem Kapitel wird beschrieben, wie Amazon OpenSearch Service-Domains erstellt und verwaltet werden. Eine Domain ist das AWS bereitgestellte Äquivalent eines OpenSearch Open-Source-Clusters. Wenn Sie eine Domain erstellen, geben Sie deren Einstellungen, Instanztypen, Instanzzahlen und Speicherzuweisung an. Weitere Informationen zu Open-Source-Clustern finden Sie in der OpenSearch Dokumentation unter Cluster erstellen.

Im Gegensatz zu den kurzen Anweisungen im Erste Schritte-Tutorial werden in diesem Kapitel alle Optionen beschrieben und relevante Referenzinformationen bereitgestellt. Sie können jedes Verfahren anhand der Anweisungen für die OpenSearch Servicekonsole, die AWS Command Line Interface (AWS CLI) oder die AWS SDKs abschließen.

OpenSearch Dienstdomänen erstellen

In diesem Abschnitt wird beschrieben, wie Sie OpenSearch Dienstdomänen mithilfe der OpenSearch Servicekonsole oder AWS CLI mithilfe des `create-domain` Befehls erstellen.

OpenSearch Dienstdomänen erstellen (Konsole)

Gehen Sie wie folgt vor, um mithilfe der Konsole eine OpenSearch Dienstdomäne zu erstellen.

So erstellen Sie eine OpenSearch Dienstdomäne (Konsole)

1. Rufen Sie die Webseite unter http://aws.amazon.com auf und klicken Sie auf In der Konsole anmelden.
2. Wählen Sie unter Analytics Amazon OpenSearch Service aus.
3. Wählen Sie Domain erstellen aus.
4. Geben Sie für Domain name (Domainname) einen Domainnamen ein. Der Name muss die folgenden Kriterien erfüllen:
   - Einzigartig für Ihr Konto und AWS-Region
   - Beginnt mit einem Kleinbuchstaben
   - Enthält zwischen drei und 28 Zeichen

- Enthält die nur Kleinbuchstaben a–z, die Nummern 0–9 und den Bindestrich (-)

5. Wählen Sie für die Methode zur Domainerstellung die Option Standard create aus.
6. Wählen Sie für Vorlagen die Option aus, die dem Zweck Ihrer Domain am besten entspricht:

   - Produktionsdomänen für Workloads, die hohe Verfügbarkeit und Leistung erfordern. Diese Domänen verwenden Multi-AZ (mit oder ohne Standby) und dedizierte Masterknoten für eine höhere Verfügbarkeit.
   - Entwicklung/Test für Entwicklung oder Test. Diese Domains können Multi-AZ (mit oder ohne Standby) oder eine einzelne Availability Zone verwenden.

   > **Important**
   >
   > Unterschiedliche Bereitstellungstypen präsentieren verschiedene Optionen auf nachfolgenden Seiten. Diese Schritte beinhalten alle Optionen.

7. Wählen Sie unter Bereitstellungsoption (en) die Option Domäne mit Standby aus, um eine 3-AZ-Domäne zu konfigurieren, wobei Knoten in einer der Zonen als Standby reserviert sind. Diese Option setzt eine Reihe von bewährten Methoden durch, z. B. eine bestimmte Anzahl von Datenknoten, die Anzahl der Master-Knoten, den Instanztyp, die Anzahl der Replikate und die Einstellungen für Softwareupdates.
8. Wählen Sie unter Version die Version OpenSearch oder das Legacy-Elasticsearch-OSS aus, das Sie verwenden möchten. Wir empfehlen Ihnen, die neueste Version von OpenSearch zu wählen. Weitere Informationen finden Sie unter the section called “Unterstützte Versionen”.

   (Optional) Wenn Sie eine OpenSearch Version für Ihre Domain ausgewählt haben, wählen Sie Kompatibilitätsmodus aktivieren, damit die Version als 7.10 OpenSearch gemeldet wird. Dadurch können bestimmte Elasticsearch OSS-Clients und -Plugins, die die Version überprüfen, bevor sie eine Verbindung herstellen, weiterhin mit dem Service arbeiten.
9. Wählen Sie unter Instance type (Instance-Typ) einen Instance-Typ für Ihre Datenknoten aus. Weitere Informationen finden Sie unter the section called “Unterstützte Instance-Typen”.

   > **Note**
   >
   > Nicht alle Availability Zones unterstützen alle Instance-Typen. Wenn Sie Multi-AZ mit oder ohne Standby wählen, empfehlen wir, Instance-Typen der aktuellen Generation wie R5 oder I3 zu wählen.

10. Wählen Sie unter Number of instances (Anzahl der Instances) die Anzahl der Datenknoten aus.

    Höchstwerte finden Sie unter Kontingente für OpenSearch Dienstdomänen und Instanzen. Cluster mit einem Knoten sind für die Entwicklung und das Testen verwendbar, jedoch nicht für Produktions-Workloads. Weitere Anleitungen finden Sie unter the section called “Größenanpassung von Domains” und the section called “Konfigurieren einer Multi-AZ-Domain”.
11. Wählen Sie als Speichertyp Amazon EBS aus. Die in der Liste verfügbaren Volume-Typen hängen von dem Instance-Typ ab, den Sie ausgewählt haben. Eine Anleitung zum Erstellen besonders großer Domains finden Sie unter the section called “Petabyte-Größe”.
12. Konfigurieren Sie für EBS-Speicher die folgenden zusätzlichen Einstellungen. Einige Einstellungen werden je nach gewähltem Volumentyp möglicherweise nicht angezeigt.

Einstellung	Beschreibung
EBS-Volume-Typ	Wählen Sie zwischen universelle (SSD) – gp3 und universelle (SSD) – gp2, oder bereitgestellte IOPS (SSD) der vorherigen Generation, und Magnetic (Standard).
EBS-Speichergröße pro Knoten	Geben Sie die Größe des EBS-Volumes ein, das Sie jedem Datenknoten zuordnen möchten. EBS volume size (EBS-Volume-Größe) bezieht sich auf einen Knoten. Sie können die Gesamtclustergröße für die OpenSearch Service-Domain berechnen, indem Sie die Anzahl der Datenknoten mit der EBS-Volume-Größe multiplizieren. Die Mindest- und Maximalgröße eines EBS-Volumes hängt sowohl vom angegebenen EBS-Volume-Typ als auch vom Instance-Typ ab, dem es zugeordnet ist. Weitere Informationen finden Sie unter EBS-Volume-Größenbeschränkungen.
Bereitgestellte IOPS	Wenn Sie einen bereitgestellten IOPS-SSD-Volume-Typ ausgewählt haben, geben Sie die Anzahl der E/A-Vorgänge pro Sekunde (IOPS) ein, die das Volume unterstützen kann.

13. (Optional) Wenn Sie einen gp3 Volumetyp ausgewählt haben, erweitern Sie Erweiterte Einstellungen und geben Sie gegen Aufpreis zusätzliche IOPS (bis zu 16.000 für jede bereitgestellte 3 TiB-Volumengröße pro Datenknoten) und den Durchsatz (bis zu 1.000 MiB/s für jede bereitgestellte 3 TiB-Volumengröße pro Datenknoten) an, die über das im Speicherpreis

enthaltene Maß hinausgehen. Weitere Informationen finden Sie in den Amazon OpenSearch Service-Preisen.

14. (Optional) Um den UltraWarm Speicher zu aktivieren, wählen Sie UltraWarm Datenknoten aktivieren. Jeder Instance-Typ verfügt über eine maximale Speichermenge, die er adressieren kann. Multiplizieren Sie diesen Betrag mit der Anzahl der Warm-Datenknoten für den gesamten adressierbaren Warm-Speicher.
15. (Optional) Um Cold Storage zu aktivieren, wählen Sie Cold Storage aktivieren. Sie müssen die Option aktivieren UltraWarm , um Cold Storage zu aktivieren.
16. Wenn Sie Multi-AZ mit Standby verwenden, sind bereits drei dedizierte Master-Knoten aktiviert. Wählen Sie den gewünschten Master-Knotentyp aus. Wenn Sie sich für eine Multi-AZ-Domain ohne Standby-Domain entschieden haben, wählen Sie Dedizierte Masterknoten aktivieren und wählen Sie den Typ und die Anzahl der gewünschten Master-Knoten aus. Dedizierte Hauptknoten erhöhen die Cluster-Stabilität und sind für Domains mit einer höheren Instance-Anzahl als 10 erforderlich. Für Produktions-Domains werden drei dedizierte Hauptknoten empfohlen.

    > **Note**
    >
    > Sie können für Ihre dedizierte Hauptknoten und Ihre Datenknoten verschiedene Instance-Typen wählen. Sie können beispielsweise universelle oder speicheroptimierte Instances für Ihre Datenknoten, aber für die Datenverarbeitung optimierte Instances für Ihre dedizierten Hauptknoten auswählen.

17. (Optional) Für Domains, die OpenSearch oder Elasticsearch 5.3 und höher ausgeführt werden, ist die Snapshot-Konfiguration irrelevant. Weitere Informationen zu automatisierten Snapshots finden Sie unter the section called “Erstellen von Index-Snapshots”.
18. Wenn Sie einen benutzerdefinierten Endpunkt anstelle des standardmäßigen `https://search-`*`mydomain-1a2a3a4a5a6a7a8a9a0a9a8a7a`*`.`*`us-east-1`*`.es.amazonaws.com` verwenden möchten, wählen Sie Benutzerdefinierten Endpunkt aktivieren und geben Sie einen Namen und ein Zertifikat an. Weitere Informationen finden Sie unter the section called “Erstellen eines benutzerdefinierten Endpunkts”.
19. Wählen Sie für Netzwerk entweder VPC-Zugriff oder Öffentlicher Zugriff. Fahren Sie bei Wahl von Public access (Öffentlicher Zugriff) mit dem nächsten Schritt fort. Wenn Sie VPC-Zugriff ausgewählt haben, stellen Sie zunächst sicher, dass die Voraussetzungen erfüllt sind und führen Sie dann die folgenden Schritte aus:

Einstellung	Beschreibung
VPC	Wählen Sie für die Virtual Private Cloud (VPC) die ID, die Sie verwenden möchten. Die VPC und die Domain müssen identisch sein AWS-Region, und Sie müssen eine VPC auswählen, bei der die Tenancy auf Standard gesetzt ist. OpenSearch Der Service unterstützt noch keine VPCs, die eine dedizierte Tenancy verwenden.
Subnetz	Wählen Sie Add subnet (Subnetz hinzufügen). Wenn Sie Multi-AZ aktiviert haben, müssen Sie zwei oder drei Subnetze auswählen. OpenSearch Der Service platziert einen VPC-Endpunkt und elastische Netzwerkschnittstellen in den Subnetzen. Sie müssen eine ausreichende Anzahl von IP-Adressen in dem oder den Subnetzen für die Netzwerkschnittstellen reservieren. Weitere Informationen finden Sie unter Reservieren von IP-Adressen in einem VPC-Subnetz.
Sicherheitsgruppen	Wählen Sie eine oder mehrere VPC-Sicherheitsgruppen aus, die es Ihrer gewünschten Anwendung ermöglichen, die OpenSearch Service-Domain über die von der Domain bereitgestellten Ports (80 oder 443) und Protokolle (HTTP oder HTTPS) zu erreichen. Weitere Informationen finden Sie unter the section called “VPC-Unterstützung”.
IAM Role (IAM-Rolle)	Behalten Sie die Standardrolle bei. OpenSearch Der Service verwendet diese vordefinierte Rolle (auch als dienstverknüpfte Rolle bezeichnet), um auf Ihre VPC zuzugreifen und einen VPC-Endpunkt und Netzwerkschnittstellen im Subnetz der VPC zu platzieren. Weitere Informationen finden Sie unter Serviceverknüpfte Rolle für den VPC-Zugriff.
Typ der IP-Adresse	Wählen Sie entweder Dual Stack oder IPv4 als IP-Adresstyp. Dual Stack ermöglicht Ihnen die gemeinsame Nutzung von Domänenressourcen für alle IPv4- und IPv6-Adresstypen. Dies ist die empfohlene Option. Wenn Sie Ihren IP-Adresstyp auf Dual-Stack einstellen, können Sie Ihren Adresstyp später nicht mehr ändern.

20. Aktivieren oder deaktivieren Sie die abgestimmte Zugriffskontrolle:

- Wenn Sie IAM für die Benutzerverwaltung verwenden möchten, wählen Sie IAM-ARN als Haupt-Benutzer festlegen, und geben Sie den ARN für eine IAM-Rolle an.
- Wenn Sie die interne Benutzerdatenbank verwenden möchten, wählen Sie Masterbenutzer erstellen und geben Sie einen Benutzernamen und ein Passwort an.

Für welche Option Sie sich auch entscheiden, der Masterbenutzer kann auf alle Indizes im Cluster und auf alle OpenSearch APIs zugreifen. Hinweise zur Auswahl der Option finden Sie unter the section called “Die wichtigsten Konzepte”.

Wenn Sie die differenzierte Zugriffskontrolle deaktivieren, können Sie den Zugriff auf Ihre Domain weiterhin steuern, indem Sie sie in einer VPC platzieren, eine restriktive Zugriffsrichtlinie anwenden oder beides tun. Sie müssen node-to-node Verschlüsselung und Verschlüsselung im Ruhezustand aktivieren, um eine differenzierte Zugriffskontrolle verwenden zu können.

> **Note**
>
> Wir empfehlen dringend, eine abgestimmte Zugriffskontrolle zu aktivieren, um die Daten in Ihrer Domain zu schützen. Eine abgestimmte Zugriffssteuerung bietet Sicherheit auf Cluster-, Index-, Dokument- und Feldebene.

21. (Optional) Wenn Sie die SAML-Authentifizierung für OpenSearch Dashboards verwenden möchten, wählen Sie SAML-Authentifizierung aktivieren und konfigurieren Sie die SAML-Optionen für die Domain. Anweisungen finden Sie unter the section called “SAML-Authentifizierung für Dashboards OpenSearch ”.
22. (Optional) Wenn Sie die Amazon Cognito Cognito-Authentifizierung für OpenSearch Dashboards verwenden möchten, wählen Sie Amazon Cognito Cognito-Authentifizierung aktivieren. Wählen Sie dann den Amazon Cognito Cognito-Benutzerpool und den Identitätspool aus, den Sie für die OpenSearch Dashboard-Authentifizierung verwenden möchten. Eine Anleitung zum Erstellen dieser Ressourcen finden Sie unter the section called “Amazon Cognito Cognito-Authentifizierung für Dashboards OpenSearch ”.
23. Wählen Sie für die Zugriffsrichtlinie eine Zugriffsrichtlinie aus oder konfigurieren Sie eine eigene. Wenn Sie eine benutzerdefinierte Richtlinie erstellen möchten, können Sie sie selbst konfigurieren oder aus einer anderen Domain importieren. Weitere Informationen finden Sie unter the section called “Identitäts- und Zugriffsverwaltung”.

> **Note**
>
> Wenn der VPC-Zugriff aktiviert wurde, können Sie keine IP-basierten Richtlinien verwenden. Sie können stattdessen mit Sicherheitsgruppen steuern, welche IP-Adressen auf die Domain zugreifen dürfen. Weitere Informationen finden Sie unter the section called “Zugriffsrichtlinien für VPC-Domänen”.

24. (Optional) Wenn alle Anfragen an die Domain über HTTPS eingehen sollen, wählen Sie HTTPS für allen Datenverkehr zur Domain erfordern. Um die node-to-node Verschlüsselung zu aktivieren, wählen Sie ode-to-nodeN-Verschlüsselung aus. Weitere Informationen finden Sie unter the section called “Keine ode-to-node Verschlüsselung”. Um die Verschlüsselung von Daten im Ruhezustand zu aktivieren, wählen Sie Verschlüsselung von Daten im Ruhezustand aktivieren aus. Diese Optionen sind vorausgewählt, wenn Sie sich für die Bereitstellungsoption Multi-AZ mit Standby entschieden haben.
25. (Optional) Wählen Sie AWS Eigenen Schlüssel verwenden aus, damit der OpenSearch Service in Ihrem Namen einen AWS KMS Verschlüsselungsschlüssel erstellt (oder verwenden Sie den bereits erstellten). Wählen Sie andernfalls Ihren eigenen KMS-Schlüssel aus. Weitere Informationen finden Sie unter the section called “Verschlüsselung im Ruhezustand”.
26. Wählen Sie für das Fenster außerhalb der Spitzenzeiten eine Startzeit aus, um Service-Software-Updates und Auto-Tune-Optimierungen zu planen, für die eine blaue/grüne Bereitstellung erforderlich ist. Updates außerhalb der Spitzenzeiten tragen dazu bei, die Belastung der dedizierten Master-Knoten eines Clusters in Zeiten mit hohem Datenverkehr zu minimieren.
27. Wählen Sie für Auto-Tune aus, ob der OpenSearch Service speicherbezogene Konfigurationsänderungen an Ihrer Domain vorschlagen darf, um Geschwindigkeit und Stabilität zu verbessern. Weitere Informationen finden Sie unter the section called “Automatische Optimierung”.

    (Optional) Wählen Sie das Zeitfenster außerhalb der Spitzenzeiten, um ein wiederkehrendes Zeitfenster zu planen, in dem Auto-Tune die Domain aktualisiert.
28. (Optional) Wählen Sie Automatisches Softwareupdate, um automatische Softwareupdates zu aktivieren.
29. (Optional) Fügen Sie Tags hinzu, um Ihre Domain zu beschreiben, damit Sie diese Informationen kategorisieren und filtern können. Weitere Informationen finden Sie unter the section called “Markieren von Domänen”.

30. (Optional) Erweitern und konfigurieren Sie Erweiterte Clustereinstellungen. Eine Zusammenfassung dieser Optionen finden Sie unter the section called “Erweiterte Clustereinstellungen”.
31. Wählen Sie Erstellen.

OpenSearch Dienstdomänen erstellen (AWS CLI)

Anstatt eine OpenSearch Dienstdomäne mithilfe der Konsole zu erstellen, können Sie die verwenden AWS CLI. Informationen zur Syntax finden Sie unter Amazon OpenSearch Service in der AWS CLI-Befehlsreferenz a.

Beispielbefehle

Dieses erste Beispiel zeigt die folgende Konfiguration der OpenSearch Service-Domain:

- Erstellt eine OpenSearch Dienstdomäne namens mylogs mit OpenSearch Version 1.2
- Füllt die Domain mit zwei Instances des Instance-Typs `r6g.large.search`
- Verwendet ein 100 GiB universelle (SSD)-EBS gp3-Volume als Speicher für jeden Datenknoten
- Ermöglicht anonymen Zugriff, aber nur von einer einzigen IP-Adresse: 192.0.2.0/32

```
aws opensearch create-domain \
    --domain-name mylogs \
    --engine-version OpenSearch_1.2 \
    --cluster-config  InstanceType=r6g.large.search,InstanceCount=2 \
    --ebs-options
 EBSEnabled=true,VolumeType=gp3,VolumeSize=100,Iops=3500,Throughput=125 \
    --access-policies '{"Version": "2012-10-17", "Statement": [{"Action": "es:*",
 "Principal":"*","Effect": "Allow", "Condition": {"IpAddress":{"aws:SourceIp":
["192.0.2.0/32"]}}}]}'
```

Das nächste Beispiel zeigt die folgende Konfiguration der OpenSearch Dienstdomäne:

- Erstellt eine OpenSearch Service-Domain namens mylogs mit Elasticsearch Version 7.10
- Füllt die Domain mit sechs Instances des Instance-Typs `r6g.large.search`
- Verwendet ein 100 GiB universelle (SSD)-EBS gp2-Volume als Speicher für jeden Datenknoten
- Beschränkt den Zugriff auf den Service auf einen einzelnen Benutzer, der anhand der Benutzer-ID 5555555555 identifiziert wird AWS-Konto

- Verteilt Instances auf mehrere Availability Zones

```
aws opensearch create-domain \
    --domain-name mylogs \
    --engine-version Elasticsearch_7.10 \
    --cluster-config
 InstanceType=r6g.large.search,InstanceCount=6,ZoneAwarenessEnabled=true,ZoneAwarenessConfig={A
 \
    --ebs-options EBSEnabled=true,VolumeType=gp2,VolumeSize=100 \
    --access-policies '{"Version": "2012-10-17", "Statement": [ { "Effect": "Allow",
 "Principal": {"AWS": "arn:aws:iam::555555555555:root" }, "Action":"es:*", "Resource":
 "arn:aws:es:us-east-1:555555555555:domain/mylogs/*" } ] }'
```

Das nächste Beispiel zeigt die folgende Konfiguration der Dienstdomäne: OpenSearch

- Erstellt eine OpenSearch Dienstdomäne namens mylogs mit OpenSearch Version 1.0
- Füllt die Domain mit zehn Instances des Instance-Typs `r6g.xlarge.search`
- Füllt die Domain mit drei Instances des Instance-Typs `r6g.large.search`, die als dedizierte Hauptknoten dienen
- Verwendet ein 100-GiB-EBS-Volume für bereitgestellte IOPS als Speicher, konfiguriert mit einer Basisleistung von 1000 IOPS für jeden Datenknoten
- Beschränkt den Zugriff auf einen Benutzer und eine Unterressource, die `_search`-API

```
aws opensearch create-domain \
    --domain-name mylogs \
    --engine-version OpenSearch_1.0 \
    --cluster-config
 InstanceType=r6g.xlarge.search,InstanceCount=10,DedicatedMasterEnabled=true,DedicatedMasterTyp
 \
    --ebs-options EBSEnabled=true,VolumeType=io1,VolumeSize=100,Iops=1000 \
    --access-policies '{"Version": "2012-10-17", "Statement": [ { "Effect": "Allow",
 "Principal": { "AWS": "arn:aws:iam::555555555555:root" }, "Action": "es:*",
 "Resource": "arn:aws:es:us-east-1:555555555555:domain/mylogs/_search" } ] }'
```

> **Note**
>
> Wenn Sie versuchen, eine OpenSearch Dienstdomäne zu erstellen und eine Domäne mit demselben Namen bereits vorhanden ist, meldet die CLI keinen Fehler. Stattdessen gibt sie die Details der vorhandenen Domain zurück.

OpenSearch Dienstdomänen (AWS SDKs) erstellen

Die AWS SDKs (mit Ausnahme der Android- und iOS-SDKs) unterstützen alle in der Amazon OpenSearch Service API-Referenz definierten Aktionen, einschließlich. `CreateDomain` Einen Beispiel-Code finden Sie unter the section called “Verwenden der AWS-SDKs”. Weitere Informationen zur Installation und Verwendung der AWS SDKs finden Sie unter AWS Software Development Kits.

OpenSearch Dienstdomänen erstellen ()AWS CloudFormation

OpenSearch Service ist in einen Service integriert AWS CloudFormation, der Sie bei der Modellierung und Einrichtung Ihrer AWS Ressourcen unterstützt, sodass Sie weniger Zeit mit der Erstellung und Verwaltung Ihrer Ressourcen und Infrastruktur verbringen müssen. Sie erstellen eine Vorlage, die die OpenSearch Domäne beschreibt, die Sie erstellen möchten, und die Domäne für Sie CloudFormation bereitstellt und konfiguriert. Weitere Informationen, einschließlich Beispielen für JSON- und YAML-Vorlagen für OpenSearch Domains, finden Sie in der Amazon OpenSearch Service-Referenz zum Ressourcentyp im AWS CloudFormation Benutzerhandbuch.

Konfigurieren von Zugriffsrichtlinien

Amazon OpenSearch Service bietet verschiedene Möglichkeiten, den Zugriff auf Ihre OpenSearch Service-Domains zu konfigurieren. Weitere Informationen finden Sie unter the section called “Identitäts- und Zugriffsverwaltung” und the section called “Differenzierte Zugriffskontrolle”.

Die Konsole stellt vorkonfigurierte Zugriffsrichtlinien bereit, die Sie an die spezifischen Anforderungen der jeweiligen Domain anpassen können. Sie können auch Zugriffsrichtlinien aus anderen OpenSearch Service-Domains importieren. Informationen zur Interaktion dieser Zugriffsrichtlinien mit dem VPC-Zugriff finden Sie unter the section called “Zugriffsrichtlinien für VPC-Domänen”.

So konfigurieren Sie Zugriffsrichtlinien (Konsole)

1. Rufen Sie die Webseite https://aws.amazon.com auf und klicken Sie dann auf Sign In to the Console (Bei der Konsole anmelden).
2. Wählen Sie unter Analytics Amazon OpenSearch Service aus.
3. Wählen Sie im Navigationsbereich unter Domains die Domain aus, die Sie aktualisieren möchten.
4. Klicken Sie auf Aktionen und Sicherheitskonfiguration bearbeiten.
5. Bearbeiten Sie die Zugriffsrichtlinien-JSON, um eine vorkonfigurierte Option zu importieren.
6. Wählen Sie Änderungen speichern aus.

Erweiterte Clustereinstellungen

Verwenden Sie erweiterte Optionen, um Folgendes zu konfigurieren:

Indizes in Anforderungstexten

Gibt an, ob explizite Verweise auf Indizes im Text von HTTP-Anforderungen zulässig sind. Wenn für diese Eigenschaft `false` festgelegt wird, wird verhindert, dass Benutzer die Zugriffskontrolle für Unterressourcen umgehen können. Der Standardwert ist `true`. Weitere Informationen finden Sie unter the section called “Erweiterte Optionen und Überlegungen zur API”.

Zuweisung des Felddaten-Cache

Gibt den Prozentsatz des Java-Heap-Space an, der den Felddaten zugewiesen ist. Standardmäßig beträgt diese Einstellung 20 % des JVM-Heaps.

> **Note**
>
> Viele Kunden fragen rotierende tägliche Indizes ab. Wir empfehlen, dass Sie Benchmark-Tests mit `indices.fielddata.cache.size` beginnen, die auf 40 % des JVM-Heap für die meisten dieser Anwendungsfälle konfiguriert sind. Für sehr große Indizes benötigen Sie möglicherweise einen Datencache für große Felder.

Maximale Anzahl der Klauseln

Gibt die maximale erlaubte Anzahl der Klauseln in einer booleschen Lucene-Abfrage an. Der Standardwert ist 1.024. Abfragen mit mehr als der erlaubten Anzahl Klauseln erzeugen den Fehler `TooManyClauses`. Weitere Informationen finden Sie in der Lucene-Dokumentation.

Konfigurationsänderungen in Amazon OpenSearch Service vornehmen

Amazon OpenSearch Service verwendet bei der Aktualisierung von Domains einen blauen/grünen Bereitstellungsprozess. Eine blaue/grüne Bereitstellung erzeugt eine inaktive Umgebung für Domain-Updates, die die Produktionsumgebung kopiert und Benutzer nach Abschluss dieser Updates an die neue Umgebung weiterleitet. In einer Blau/Grün-Umgebung ist die blaue Umgebung die aktuelle Produktionsumgebung. Die grüne Umgebung ist die inaktive Umgebung.

Daten werden von der blauen Umgebung in die grüne Umgebung migriert. Wenn die neue Umgebung bereit ist, wechselt der OpenSearch Service die Umgebungen, um die grüne Umgebung zur neuen Produktionsumgebung zu machen. Der Switchover erfolgt ohne Datenverlust. Auf diese Weise werden Ausfallzeiten minimiert und die ursprüngliche Umgebung für den Fall beibehalten, dass die Bereitstellung in der neuen Umgebung nicht erfolgreich ist.

Themen

Änderungen, die normalerweise eine Blau/Grün-Bereitstellung auslösen

Die folgenden Operationen führen zu blaugrünen Bereitstellungen:

- Ändern des Instance-Typs
- Aktivieren der differenzierten Zugriffskontrolle
- Ausführen von Service-Softwareupdates
- Aktivieren oder Deaktivieren von dedizierten Master-Knoten
- Multi-AZ ohne Standby aktivieren oder deaktivieren
- Ändern des Speichertyps, des Volumetyps oder der Datenträgergröße
- Auswählen von verschiedenen VPC-Subnetzen
- Hinzufügen oder Entfernen von VPC-Sicherheitsgruppen
- Amazon Cognito Cognito-Authentifizierung für Dashboards aktivieren oder deaktivieren OpenSearch
- Auswählen eines anderen Amazon-Cognito-Benutzerpools oder Identitätenpools
- Ändern von erweiterten Einstellungen
- Upgrade auf eine neue OpenSearch Version (OpenSearch Dashboards sind möglicherweise während eines Teils oder des gesamten Upgrades nicht verfügbar)
- Aktivierung der Verschlüsselung von Daten im Ruhezustand oder node-to-node Verschlüsselung
- Aktivierung UltraWarm oder Deaktivierung von Cold Storage
- Deaktivieren der automatischen Abstimmung und Zurücksetzen der Änderungen
- Ein optionales Plugin einer Domain zuordnen und ein optionales Plugin von einer Domain trennen
- Erhöhung der Anzahl der dedizierten Master-Knoten für Multi-AZ-Domains mit zwei dedizierten Master-Knoten
- Verringerung der Größe des EBS-Volumes
- Änderung der EBS-Volume-Größe, der IOPS oder des Durchsatzes, wenn die letzte Änderung, die Sie vorgenommen haben, gerade läuft oder vor weniger als 6 Stunden stattgefunden hat
- Aktivierung der Veröffentlichung von Audit-Logs für. CloudWatch

Bei Multi-AZ mit Standby-Domains können Sie jeweils nur eine Änderungsanforderung stellen. Wenn eine Änderung bereits im Gange ist, wird die neue Anfrage abgelehnt. Sie können den Status der aktuellen Änderung mit der `DescribeDomainChangeProgress` API überprüfen.

Änderungen, die normalerweise keine Blau/Grün-Bereitstellung auslösen

Die folgenden Operationen führen in den meistenFällen nicht zu Blau/Grün-Bereitstellungen:

- Änderung der Zugriffsrichtlinie
- Ändern des benutzerdefinierten Endpunkts
- Änderung der TLS-Richtlinie (Transport Layer Security)
- Ändern der automatisierten Snapshot-Stunde
- Aktivieren oder Deaktivieren von Require HTTPS (Erzwingung von HTTPS)
- Aktivieren der automatischen Optimierung oder Deaktivierung, ohne die Änderungen rückgängig zu machen
- Wenn Ihre Domain über dedizierte Master-Knoten verfügt, ändern Sie den Datenknoten oder die Anzahl der UltraWarm Knoten
- Wenn Ihre Domain über dedizierte Master-Knoten verfügt, ändern Sie den Typ oder die Anzahl der dedizierten Master-Instances (außer bei Multi-AZ-Domänen mit zwei dedizierten Masterknoten)
- Aktivierung oder Deaktivierung der Veröffentlichung von Fehlerprotokollen oder langsamen Protokollen für CloudWatch
- Deaktivierung der Veröffentlichung von Audit-Logs auf CloudWatch
- Erhöhung der Volumegröße auf bis zu 3 TiB pro Datenknoten, Änderung des Volumetyps, der IOPS oder des Durchsatzes
- Hinzufügen und Entfernen von Tags

> **Note**
>
> Abhängig von Ihrer Service-Softwareversion gibt es einige Ausnahmen. Wenn Sie sichergehen möchten, dass eine Änderung nicht zu einer blauen/grünen Bereitstellung führt, führen Sie vor der Aktualisierung Ihrer Domain einen Probelauf durch, sofern diese Option verfügbar ist. Einige Änderungen bieten keine Option für einen Probelauf. Wir empfehlen generell, dass Sie außerhalb der Hauptverkehrszeiten Änderungen an Ihrem Cluster vornehmen.

Feststellen, ob eine Änderung eine Blau/Grün-Bereitstellung verursacht

Sie können einige Arten von geplanten Konfigurationsänderungen testen, um festzustellen, ob sie zu einer blauen/grünen Bereitstellung führen, ohne sich auf diese Änderungen festlegen zu müssen. Führen Sie, bevor Sie eine Kofigurationsänderung initiieren, über die Konsole oder ein API eine Validierungsprüfung durch, um sicherzustellen, dass Ihre Domain für ein Update in Frage kommt.

Console

Um eine Konfigurationsänderung zu validieren

1. Navigieren Sie zur Amazon OpenSearch Service-Konsole unterhttps://console.aws.amazon.com/aos/.
2. Wählen Sie im linken Navigationsbereich die Option Domains aus.
3. Wählen Sie die Domain aus, für die Sie eine Konfigurationsänderung vornehmen möchten. Dadurch wird die Detailseite der Domain geöffnet. Wählen Sie das Dropdown-Menü Actions (Aktionen) und dann Edit cluster configuration (Clusterkonfiguration bearbeiten) aus.
4. Auf der Seite Edit cluster configuration (Clusterkonfiguration bearbeiten) können Sie Änderungen am Instance-Typ, der Anzahl der Knoten und allen anderen Konfigurationen vornehmen. Nachdem Sie Ihre Änderungen im Übersichtsbereich bestätigt haben, wählen Sie Run (Ausführen) aus.
5. Sobald Ihr Probelauf abgeschlossen ist, werden die Ergebnisse zusammen mit einer Testlauf-ID automatisch unten auf der Seite angezeigt. Diese Ergebnisse informieren Sie darüber, in welche Kategorie Ihre Änderung fällt:

   - Löst eine Blau/Grün-Bereitstellung aus
   - Erfordert keine Blau/Grün-Bereitstellung
   - Enthält Überprüfungsfehler, die Sie beheben müssen, bevor Sie Ihre Änderungen speichern können

   Beachten Sie, dass jeder Testlauf den vorherigen überschreibt. Um die Details der einzelnen Testläufe zu einem späteren Zeitpunkt nachschlagen zu können, müssen Sie Ihre Testlauf-ID speichern. Jeder Testlauf ist 90 Tage lang verfügbar bzw. bis Sie ein Konfigurationsupdate vornehmen.
6. Um mit Ihrem Konfigurationsupdate fortzufahren, wählen Sie Save changes (Änderungen speichern) aus. Wählen Sie andernfalls Abbrechen. Mit jeder Option gelangen Sie zurück zur Registerkarte Cluster configuration (Cluster-Konfiguration). Auf dieser Registerkarte können Sie Dry run details (Testlaufdetails) auswählen, um die Details Ihres letzten Testlaufs zu sehen. Diese Seite enthält auch einen side-by-side Vergleich zwischen der Konfiguration vor dem Testlauf und der Testlaufkonfiguration.

API

Sie können eine Testlaufvalidierung über die Konfigurations-API durchführen. Um Ihre Änderungen mit der API zu testen, stellen Sie `DryRun` auf `true` und `DryRunMode` auf `Verbose` ein. Im Modus „Verbose“ wird zusätzlich eine Validierungsprüfung durchgeführt, um festzustellen, ob durch die Änderung eine Blau/Grün-Bereitstellung ausgelöst wird. Mit dieser UpdateDomainConfigAnfrage wird beispielsweise der Bereitstellungstyp getestet, der sich aus der Aktivierung von Folgendem ergibt UltraWarm:

```
POST https://es.us-east-1.amazonaws.com/2021-01-01/opensearch/domain/my-domain/
config
{
   "ClusterConfig": {
    "WarmCount": 3,
    "WarmEnabled": true,
    "WarmType": "ultrawarm1.large.search"
   },
   "DryRun": true,
   "DryRunMode": "Verbose"
}
```

Die Anforderung führt eine Validierungsprüfung durch und gibt die Art der Bereitstellung zurück, die die Änderung verursachen wird, führt das Update jedoch nicht tatsächlich durch:

```
{
   "ClusterConfig": {
     ...
    },
   "DryRunResults": {
      "DeploymentType": "Blue/Green",
      "Message": "This change will require a blue/green deployment."
    }
}
```

Mögliche Bereitstellungstypen sind:

- `Blue/Green` – Die Änderung bewirkt eine Blau/Grün-Bereitstellung.
- `DynamicUpdate` – Die Änderung bewirkt keine Blau/Grün-Bereitstellung.
- `Undetermined` – Die Domain befindet sich noch in einem Verarbeitungsstatus, sodass der Bereitstellungstyp nicht bestimmt werden kann.

- None – Keine Konfigurationsänderung.

Schlägt die Überprüfung fehl, wird eine Liste der Validierungsfehler zurückgegeben.

```
{
   "ClusterConfig":{
      "..."
   },
   "DryRunProgressStatus":{
      "CreationDate":"2023-01-12T01:14:33.847Z",
      "DryRunId":"db00ca39-48b2-4774-bbd3-252cf094d205",
      "DryRunStatus":"failed",
      "UpdateDate":"2023-01-12T01:14:33.847Z",
      "ValidationFailures":[
         {
            "Code":"Cluster.Index.WriteBlock",
            "Message":"Cluster has index write blocks."
         }
      ]
   }
}
```

Wenn der Status immer noch lautet`pending`, können Sie die Testlauf-ID in Ihrer UpdateDomainConfig Antwort bei nachfolgenden DescribeDryRunProgressAufrufen verwenden, um den Status der Validierung zu überprüfen.

```
GET https://es.us-east-1.amazonaws.com/2021-01-01/opensearch/domain/my-domain/
dryRun?dryRunId=my-dry-run-id
{
    "DryRunConfig": null,
    "DryRunProgressStatus": {
        "CreationDate": "2023-01-12T01:14:42.998Z",
        "DryRunId": "db00ca39-48b2-4774-bbd3-252cf094d205",
        "DryRunStatus": "succeeded",
        "UpdateDate": "2023-01-12T01:14:49.334Z",
        "ValidationFailures": null
    },
    "DryRunResults": {
        "DeploymentType": "Blue/Green",
        "Message": "This change will require a blue/green deployment."
    }
```

```
}
```

Um eine Testlaufanalyse ohne Validierungsprüfung durchzuführen, stellen Sie `DryRunMode` auf `Basic` ein, wenn Sie die Konfigurations-API verwenden.

Python

Der folgende Python-Code verwendet die UpdateDomainConfigAPI, um eine Testlauf-Validierungsprüfung durchzuführen, und wenn die Prüfung erfolgreich ist, ruft er dieselbe API ohne einen Probelauf auf, um das Update zu starten. Schlägt die Prüfung fehl, druckt das Skript den Fehler aus und stoppt.

```
import time
import boto3

client = boto3.client('opensearch')

response = client.UpdateDomainConfig(
    ClusterConfig={
        'WarmCount': 3,
        'WarmEnabled': True,
        'WarmCount': 123,
    },
    DomainName='test-domain',
    DryRun=True,
    DryRunMode='Verbose'
)

dry_run_id = response.DryRunProgressStatus.DryRunId

retry_count = 0

while True:

    if retry_count == 5:
        print('An error occured')
        break

    dry_run_progress_response = client.DescribeDryRunProgress('test-domain',
 dry_run_id)
    dry_run_status = dry_run_progress_response.DryRunProgressStatus.DryRunStatus

    if dry_run_status == 'succeeded':
```

```
        client.UpdateDomainConfig(
            ClusterConfig={
            'WarmCount': 3,
            'WarmEnabled': True,
            'WarmCount': 123,
        })
        break

    elif dry_run_status == 'failed':
        validation_failures_list =
dry_run_progress_response.DryRunProgressStatus.ValidationFailures
        for item in validation_failures_list:
            print(f"Code: {item['Code']}, Message: {item['Message']}")
        break

    retry_count += 1
    time.sleep(30)
```

Initiierung und Nachverfolgung einer Konfigurationsänderung

> **Note**
>
> Sie können jeweils eine Konfigurationsänderung beantragen. Sie können auch mehrere Konfigurationsänderungen in einer einzigen Anfrage zusammenfassen. Warten Sie, bis der Status Ihrer Domain erreicht ist, `Active` bevor Sie weitere Konfigurationsänderungen anfordern.

In der Amazon OpenSearch Service-Konsole können Sie die Felder Domain-Verarbeitungsstatus und Konfigurationsänderungsstatus aufrufen, um Domain- und Konfigurationsänderungen nachzuverfolgen. Sie können Domain- und Konfigurationsänderungen auch anhand der `ConfigChangeStatus` Parameter `DomainProcessingStatus` und in den API-Antworten verfolgen. Weitere Informationen zum DomainStatusDatentyp finden Sie in der OpenSearch Service-API-Referenz.

Sichtbarkeit des Domain-Verarbeitungsstatus: Sie können den Konfigurationsstatus einer Domain ganz einfach ermitteln, indem Sie sich das Feld Domain-Verarbeitungsstatus in der Konsole ansehen. In ähnlicher Weise kann der `DomainProcessingStatus` API-Parameter verwendet werden, um den Status zu identifizieren. Die folgenden Werte sind Verarbeitungsstatus für eine Domain:

- `Active`: Derzeit wird keine Konfigurationsänderung durchgeführt. Sie können eine neue Anfrage zur Konfigurationsänderung einreichen.
- `Creating`: Die Domain wird erstellt.
- `Modifying`: Konfigurationsänderungen, wie das Hinzufügen neuer Datenknoten, EBS-, GP3-, IOPS-Bereitstellung oder Einrichtung von KMS-Schlüsseln, sind im Gange.

> **Note**
>
> Möglicherweise wird der Status `Modifying` in Situationen angezeigt, in denen für eine Domain eine Shard-Verschiebung erforderlich ist, um die Konfigurationsänderungen abzuschließen. Aus Gründen der Abwärtskompatibilität wird das Verhalten des `Processing` Parameters in den API-Antworten unverändert beibehalten und auf False gesetzt, sobald die Änderungen an der Kernkonfiguration abgeschlossen sind, ohne auf den Abschluss der Shard-Bewegung zu warten.

- `Upgrading Engine Version`: Ein Upgrade der Engine-Version ist im Gange.
- `Updating Service Software`: Ein Service-Software-Update ist in Bearbeitung.
- `Deleting`: Die Domain wird gelöscht.
- `Isolated`: Die Domain ist gesperrt.

Sichtbarkeit des Konfigurationsstatus: Konfigurationsänderungen können vom Betreiber (z. B. Hinzufügen eines neuen Datenknotens, Änderung des Instanztyps) oder vom Dienst (z. B. Auto-Tune und Updates außerhalb der Hauptverkehrszeiten) initiiert werden. Den Status der letzten Konfigurationsänderungen finden Sie im Feld Configuration Change Status der Amazon OpenSearch Service-Konsole und in der `ConfigChangeStatus` API-Antwort. Die folgenden Werte geben den Konfigurationsstatus einer Domain an:

- `Pending`: Eine Anfrage zur Änderung der Konfiguration wurde eingereicht.
- `Initializing`: Der Dienst initialisiert eine Anfrage zur Konfigurationsänderung.
- `Validating`: Der Service validiert die angeforderten Änderungen und die erforderlichen Ressourcen.
- `Awaiting user inputs`: Gilt, wenn der Betreiber erwartet, dass einige Konfigurationsänderungen, wie z. B. die Änderung des Instanztyps, weiter vorangetrieben werden. Sie können Konfigurationsänderungen bearbeiten.
- `Applying changes`: Der Dienst wendet die angeforderten Konfigurationsänderungen an.

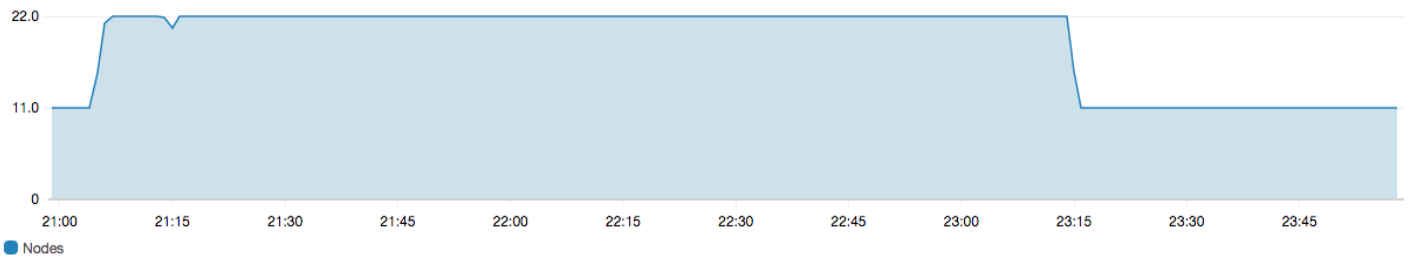
- `Cancelled`: Die Konfigurationsänderung wurde storniert. Wenn Sie den Status „Überprüfung fehlgeschlagen“ erhalten, können Sie in der Konsole auf Abbrechen klicken oder den `CancelDomainConfigChange` API-Vorgang aufrufen. Wenn Sie dies tun, werden alle vorgenommenen Änderungen rückgängig gemacht.
- `Completed`: Die angeforderten Konfigurationsänderungen wurden erfolgreich abgeschlossen.
- `Validation Failed`: Die angeforderten Änderungen konnten nicht überprüft werden. Es wurden keine Konfigurationsänderungen vorgenommen.

> **Note**
>
> Fehler bei der Überprüfung können auf rote Indizes in Ihrer Domain, auf die Nichtverfügbarkeit eines ausgewählten Instanztyps oder auf zu wenig Festplattenspeicher zurückzuführen sein. Eine Liste der Validierungsfehler finden Sie unter. the section called “Beheben von Validierungsfehlern” Während eines Fehlers bei der Überprüfung können Sie die Konfigurationsänderungen abbrechen, erneut versuchen oder bearbeiten.

API-Zusammenfassung: Sie können die `DescribeDomainConfig` API-Operationen, und verwenden `DescribeDomainDescribeDomainChangeProgress`, um den Status der Konfigurationsupdates detailliert abzurufen. Darüber hinaus können Sie `CancelDomainConfigChange` damit die Updates stornieren, falls die Überprüfung fehlschlägt. Weitere Informationen finden Sie in der Dokumentation zur OpenSearch Service-API

Wenn die Konfigurationsänderungen abgeschlossen sind, wird der Domänenstatus wieder auf geändert`Active`.

Sie können die Cluster-Integrität und die CloudWatch Amazon-Metriken überprüfen und feststellen, dass die Anzahl der Knoten im Cluster während der Domain-Aktualisierung vorübergehend zunimmt — häufig verdoppelt — wird. In der folgenden Abbildung sehen Sie, wie sich die Anzahl der Knoten während einer Konfigurationsänderung verdoppelt und sich wieder auf 11 verringert, wenn die Aktualisierung abgeschlossen ist.



Dieser temporäre Anstieg kann die dedizierten Master-Knoten des Clusters belasten, da sie möglicherweise plötzlich viel mehr Knoten zu verwalten haben. Dies kann auch die Such- und Indizierungslatenzen erhöhen, da der OpenSearch Service Daten vom alten Cluster auf den neuen kopiert. Es ist wichtig, genügend Kapazität im Cluster bereitzustellen, um den erhöhten Verwaltungsaufwand zu bewältigen, der mit diesen blau/grünen Bereitstellungen verbunden ist.

> **Important**
>
> Es fallen keine zusätzlichen Gebühren bei Konfigurationsänderungen und Service-Wartung an. Sie zahlen nur für die Anzahl der Knoten, die Sie für Ihren Cluster anfordern. Weitere Einzelheiten finden Sie unter the section called “Gebühren für Konfigurationsänderungen”.

Um eine Überlastung der dedizierten Master-Knoten zu verhindern, können Sie die Nutzung anhand der CloudWatch Amazon-Metriken überwachen. Weitere Informationen über empfohlene Maximalwerte finden Sie unter the section called “Empfohlene CloudWatch Alarme”.

Stufen einer Konfigurationsänderung

Nachdem Sie eine Konfigurationsänderung initiiert haben, führt OpenSearch Service eine Reihe von Schritten durch, um Ihre Domain zu aktualisieren. Sie können den Fortschritt der Konfigurationsänderung in der Konsole unter Status der Konfigurationsänderung einsehen. Die genauen Schritte, die eine Aktualisierung durchläuft, hängen von der Art der Änderung ab, die Sie vornehmen. Sie können eine Konfigurationsänderung auch mithilfe des DescribeDomainChangeProgressAPI-Vorgangs überwachen.

Die folgenden Schritte sind mögliche Stufen, die eine Aktualisierung während einer Konfigurationsänderung durchlaufen kann:

Stufenname	Beschreibung
Validierung	Überprüfen, ob die Domain für ein Update berechtigt ist, und ggf. Erkennen

Stufenname	Beschreibung
	von Validierungsproblemen.
Erstellen einer neuen Umgebung	Erfüllen der erforderlichen Voraussetzungen und Erstellen der erforderlichen Ressourcen, um die Blau/Grün-Bereitstellung zu starten.
Provisioning neuer Knoten	Erstellen einer neuen Gruppe von Instances in der neuen Umgebung.
Routing des Datenverkehrs auf neue Knoten	Umleiten des Datenverkehrs auf die neu erstellten Datenknoten.
Routing des Datenverkehrs auf alte Knoten	Deaktivieren des Datenverkehrs auf den alten Datenknoten.

Stufenname	Beschreibung
Vorbereiten von Knoten auf das Entfernen	Vorbereiten der Entfernung von Knoten. Dieser Schritt wird nur ausgeführt, wenn Sie Ihre Domain herunterskalieren (z. B. von 8 Knoten auf 6 Knoten).
Kopieren von Shards auf neue Knoten	Verschieben von Shards von den alten Knoten auf die neuen Knoten.
Beenden von Knoten	Beenden und Löschen alter Knoten, nachdem die Shards entfernt wurden.
Löschen von älteren Ressourcen	Löschen von Ressourcen, die mit der alten Umgebung verknüpft sind (z. B. Load Balancer).

Stufenname	Beschreibung
Dynamisches Update	Wird angezeigt, wenn die Aktualisierung keine Blau/Grün-Bereitstellung erfordert und dynamisch angewendet werden kann.
Anwenden von speziellen Änderungen im Zusammenhang mit dem Master	Wird angezeigt, wenn der Typ oder die Anzahl der dedizierten Master-Instances geändert wird.
Volumenbezogene Änderungen werden übernommen	Wird angezeigt, wenn Volumengröße, Typ, IOPS und Durchsatz geändert werden.

Auswirkungen von Blau/Grün-Bereitstellungen auf die Leistung

Während der blauen/grünen Bereitstellung ist Ihr Amazon OpenSearch Service-Cluster für eingehende Such- und Indexierungsanfragen verfügbar. Es können jedoch die folgenden Leistungsprobleme auftreten:

- Vorübergehender Anstieg der Auslastung auf Leader-Knoten, da Cluster mehr Knoten verwalten müssen.
- Höhere Latenz bei der Suche und Indizierung, da der OpenSearch Service Daten von alten Knoten auf neue Knoten kopiert.
- Zunehmende Ablehnungen für eingehende Anfragen, da die Clusterlast bei blauen/grünen Bereitstellungen zunimmt.
- Um Latenzprobleme und Ablehnungen von Anfragen zu vermeiden, sollten Sie blaue/grüne Bereitstellungen ausführen, wenn der Cluster intakt ist und wenig Netzwerkverkehr herrscht.

Gebühren für Konfigurationsänderungen

Wenn Sie die Konfiguration für eine Domäne ändern, erstellt OpenSearch Service einen neuen Cluster, wie unter beschrieben. the section called “Konfigurationsänderungen” Bei der Migration von alt auf neu fallen die folgenden Gebühren an:

- Wenn Sie den Instance-Typ ändern, bezahlen Sie für beide Cluster für die erste Stunde. Nach der ersten Stunde bezahlen Sie nur für den neuen Cluster. EBS-Volumes werden nicht zweimal belastet, da sie Teil Ihres Clusters sind. Daher folgt die Abrechnung der Instance-Abrechnung.

  Beispiel: Sie ändern die Konfiguration von drei `m3.xlarge`-Instances zu vier `m4.large`-Instances. In der ersten Stunde bezahlen Sie für beide Cluster (3 * `m3.xlarge` + 4 * `m4.large`). Nach der ersten Stunde bezahlen Sie nur für den neuen Cluster (4 * `m4.large`).
- Wenn Sie den Instance-Typ nicht ändern, bezahlen Sie nur für den größten Cluster für die erste Stunde. Nach der ersten Stunde bezahlen Sie nur für den neuen Cluster.

  Beispiel: Sie ändern die Konfiguration von sechs `m3.xlarge`-Instances zu drei `m3.xlarge`-Instances. In der ersten Stunde bezahlen Sie für den größten Cluster (6 * `m3.xlarge`). Nach der ersten Stunde bezahlen Sie nur für den neuen Cluster (3 * `m3.xlarge`).

Beheben von Validierungsfehlern

Wenn Sie eine Konfigurationsänderung initiieren OpenSearch oder ein Upgrade der Elasticsearch-Version durchführen, führt OpenSearch Service zunächst eine Reihe von Validierungsprüfungen durch, um sicherzustellen, dass Ihre Domain für ein Update in Frage kommt. Wenn eine dieser Prüfungen fehlschlägt, erhalten Sie in der Konsole eine Benachrichtigung mit den spezifischen Problemen, die Sie beheben müssen, bevor Sie Ihre Domain aktualisieren. In der folgenden Tabelle

sind die möglichen Domain-Probleme aufgeführt, die bei OpenSearch Service auftreten könnten, sowie die Schritte zu deren Behebung.

Problem	Fehlercode	Fehlerbehebungsschritte
Sicherheitsgruppe wurde nicht gefunden	`SecurityGroupNotFound`	Die mit Ihrer OpenSearch Dienstdomäne verknüpfte Sicherheitsgruppe ist nicht vorhanden. Um dieses Problem zu lösen, erstellen Sie eine Sicherheitsgruppe mit dem angegebenen Namen.
Subnetz nicht gefunden	`SubnetNotFound`	Das mit Ihrer OpenSearch Service-Domain verknüpfte Subnetz ist nicht vorhanden. Um dieses Problem zu lösen, erstellen Sie ein Subnetz in Ihrer VPC.
Serviceverknüpfte Rolle nicht konfiguriert	`SLRNotConfigured`	Die dienstverknüpfte Rolle für OpenSearch Service ist nicht konfiguriert. Die dienstbezogene Rolle ist von OpenSearch Service vordefiniert und umfasst alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen. Wenn die Rolle nicht vorhanden ist, müssen Sie sie ggf. manuell erstellen.
Nicht genügend IP-Adressen	`InsufficientFreeIPsForSubnets`	Eines oder mehrere Ihrer VPC-Subnetze verfügen nicht über genügend IP-Adressen, um Ihre Domain zu aktualisieren. Informationen dazu, wie viele IP-Adressen Sie benötigen, finden Sie unter the section called “Reservieren von IP-Adressen in einem VPC-Subnetz”.
Cognito-Benutzerpool ist nicht vorhanden	`CognitoUserPoolNotFound`	OpenSearch Der Service kann den Amazon Cognito Cognito-Benutzerpool nicht finden. Stellen Sie sicher, dass Sie einen Benutzerpool erstellt haben und die korrekte ID verwenden. Die ID können Sie mithilfe der Amazon-Cognito-Konsole oder dem folgenden AWS CLI -Befehl bestimmen: `aws cognito-idp list-user-pools --max-results 60 --region us-east-1`
Cognito-Identitätspool ist	`CognitoIdentityPoo`	OpenSearch Der Dienst kann den Cognito-Identitätspool nicht finden. Stellen Sie sicher, dass Sie einen Benutzerpool erstellt haben und die

Problem	Fehlercode	Fehlerbehebungsschritte
nicht vorhanden	`lNotFound`	korrekte ID verwenden. Die ID können Sie mithilfe der Amazon-Cognito-Konsole oder dem folgenden AWS CLI -Befehl bestimmen: `aws cognito-identity list-identity-pools --max-results 60 --region us-east-1`
Cognito-Domain nicht für Benutzerpool gefunden	`CognitoDomainNotFound`	Der Benutzerpool verfügt nicht über einen Domain-Namen. Sie können eine mit der Amazon Cognito Cognito-Konsole oder mit dem folgenden AWS CLI Befehl konfigurieren: `aws cognito-idp create-user-pool-domain --domain my-domain --user-pool-id id`
Cognito-Rolle nicht konfiguriert	`CognitoRoleNotConfigured`	Die IAM-Rolle, die dem OpenSearch Service die Berechtigung erteilt, die Benutzer- und Identitätspools von Amazon Cognito zu konfigurieren und für die Authentifizierung zu verwenden, ist nicht konfiguriert. Konfigurieren Sie die Rolle mit passenden Berechtigungen und einer entsprechenden Vertrauensstellung. Sie können die Konsole verwenden, die die Standardrolle CognitoAccessForAmazonOpenSearchfür Sie erstellt, oder Sie können eine Rolle mithilfe des AWS CLI oder des AWS SDK manuell konfigurieren.
Benutzerpool kann nicht beschrieben werden	`UserPoolNotDescribable`	Die angegebene Amazon-Cognito-Rolle hat keine Berechtigung, den mit Ihrer Domain verknüpften Benutzerpool zu beschreiben. Vergewissern Sie sich, dass die Richtlinie für Rollenberechtigungen die Aktion `cognito-identity:DescribeUserPool` zulässt. Siehe the section called “Informationen über die CognitoAccessForAmazonOpenSearch-Rolle” für die vollständige Berechtigungsrichtlinie.

Problem	Fehlercode	Fehlerbehebungsschritte
Identität spool kann nicht beschrieb en werden	`IdentityP oolNotDes cribable`	Die angegebene Amazon-Cognito-Rolle hat keine Berechtigung, den mit Ihrer Domain verknüpften Identitätspool zu beschreiben. Vergewissern Sie sich, dass die Richtlinie für Rollenberechtigungen die Aktion `cognito-identity:DescribeIdentityPool` zulässt. Siehe the section called “Informationen über die CognitoAc cessForAmazonOpenSearch-Rolle” für die vollständige Berechtig ungsrichtlinie.
Benutzer und Identität spool können nicht beschrieb en werden	`CognitoPo olsNotDes cribable`	Die angegebene Amazon-Cognito-Rolle hat keine Berechtigung, die mit Ihrer Domain verknüpften Benutzer- und Identitätspools zu beschreiben. Vergewissern Sie sich, dass die Richtlinie für Rollenber echtigungen die Aktionen `cognito-identity:DescribeId entityPool` und `cognito-identity:DescribeUs erPool` zulässt. Siehe the section called “Informationen über die CognitoAccessForAmazonOpenSearch-Rolle” für die vollständige Berechtigungsrichtlinie.
KMS-Schlü ssel nicht aktiviert	`KMSKeyNot Enabled`	Der Schlüssel AWS Key Management Service (AWS KMS), der zur Verschlüsselung Ihrer Domain verwendet wird, ist deaktiviert. Aktivieren Sie den Schlüssel sofort erneut.
Benutzerd efinierte s Zertifika t befindet sich nicht im Status „ISSUED“ (A LLT)	`InvalidCe rtificate`	Wenn Ihre Domain einen benutzerdefinierten Endpunkt verwendet , sichern Sie ihn, indem Sie entweder ein SSL-Zertifikat in AWS Certificate Manager (ACM) generieren oder eines Ihrer eigenen importieren. Der Zertifikatsstatus muss Issued (Ausgestellt) sein. Wenn dieser Fehler angezeigt wird, überprüfen Sie den Status Ihres Zertifikats in der ACM-Konsole. Wenn der Status „Expired“ (Abgelaufen), „Failed“ (Fehlgeschlagen), „Inactive“ (Inaktiv) oder „Pending“ (Ausstehend) ist, siehe die ACM-Dokumentation zur Fehlerbehebung, um das Problem zu lösen.

Problem	Fehlercode	Fehlerbehebungsschritte
Nicht genügend Kapazität zum Starten des ausgewählten Instance-Typs	`InsufficientInstanceCapacity`	Die angeforderte Kapazität des Instance-Typs ist nicht verfügbar. Möglicherweise haben Sie fünf `i3.16xlarge.search` Knoten angefordert, aber OpenSearch Service hat nicht genügend `i3.16xlarge.search` Hosts zur Verfügung, sodass die Anfrage nicht erfüllt werden kann. Überprüfen Sie die unterstützten Instanztypen in OpenSearch Service und wählen Sie einen anderen Instanztyp aus.
Rote Indizes im Cluster	`RedCluster`	Ein oder mehrere Indizes in Ihrem Cluster haben einen roten Status, was zu einem allgemeinen roten Cluster-Status führt. Informationen zur Behebung dieses Problems finden Sie unter the section called “Roter Cluster-Status”.
Speicherschutzschalter, zu viele Anfragen	`TooManyRequests`	Es gibt zu viele Such- und Schreibanfragen für Ihre Domain, sodass OpenSearch Service die Konfiguration nicht aktualisieren kann. Sie können die Anzahl der Anforderungen reduzieren, Instances bis zu 64 GiB RAM vertikal skalieren oder eine horizontale Skalierung durchführen, indem Sie Instances hinzufügen.
Neue Konfiguration kann keine Daten aufnehmen (wenig Speicherplatz)	`InsufficientStorageCapacity`	Die konfigurierte Speichergröße kann nicht alle Daten in Ihrer Domain enthalten. Um dieses Problem zu lösen, wählen Sie ein größeres Volume, löschen Sie nicht verwendete Indizes oder erhöhen Sie die Anzahl der Knoten im Cluster, um sofort Speicherplatz freizugeben.

Problem	Fehlercode	Fehlerbehebungsschritte

An bestimmte Knoten angeheftete Shards	`ShardMovementBlocked`	Ein oder mehrere Indizes in Ihrer Domain sind an bestimmte Knoten angehängt und können nicht neu zugewiesen werden. Dies ist höchstwahrscheinlich darauf zurückzuführen, dass Sie die Shard-Zuweisungsfilterung konfiguriert haben, mit der Sie angeben können, welche Knoten die Shards eines bestimmten Indexes hosten dürfen.
		
		Um dieses Problem zu beheben, entfernen Sie Filter für die Shard-Zuweisung aus allen betroffenen Indizes:
		
		`PUT my-index/_settings`
		`{`
		`  "settings": {`
		`  "index.routing.allocation.require._name": null`
		`  }`
		`}`

Neue Konfiguration kann nicht alle Shards enthalten (Shard-Anzahl)	`TooManyShards`	Die Anzahl der Shards in Ihrer Domain ist zu hoch, sodass OpenSearch Service sie nicht in die neue Konfiguration verschieben kann. Um dieses Problem zu beheben, skalieren Sie Ihre Domain horizontal, indem Sie Knoten mit demselben Konfigurationstyp wie Ihre aktuellen Cluster-Knoten hinzufügen. Beachten Sie: Die maximale EBS-Volume-Größe hängt vom Instance-Typ des Knotens ab. Um dieses Problem künftig zu vermeiden, siehe the section called “Auswahl der Anzahl der Shards” und definieren Sie eine Sharding-Strategie, die sich für Ihren Anwendungsfall eignet.
Das mit Ihrer Domain verknüpfte Subnetz unterstützt keine IPv4-Adressen	`ResultCodeIPv4BlockNotExists`	Um dieses Problem zu beheben, erstellen Sie ein Subnetz oder aktualisieren Sie das vorhandene Subnetz in Ihrer VPC entsprechend dem konfigurierten IP-Adresstyp der Domain. Wenn Ihre Domain einen reinen IPv4-Adresstyp verwendet, verwenden Sie ein reines IPv4-Subnetz. Wenn Ihre Domain den Dual-Stack-Modus verwendet, verwenden Sie ein Dual-Stack-Subnetz.

Problem	Fehlercode	Fehlerbehebungsschritte
Das Ihrer Domain zugeordnete Subnetz unterstützt keine IPv6-Adressen	`ResultCodeIPv6BlockNotExists`	Um dieses Problem zu beheben, erstellen Sie ein Subnetz oder aktualisieren Sie das vorhandene Subnetz in Ihrer VPC entsprechend dem konfigurierten IP-Adresstyp der Domain. Wenn Ihre Domain einen reinen IPv4-Adresstyp verwendet, verwenden Sie ein reines IPv4-Subnetz. Wenn Ihre Domain den Dual-Stack-Modus verwendet, verwenden Sie ein Dual-Stack-Subnetz.

Service-Software-Updates in Amazon OpenSearch Service

> **Note**
>
> Erläuterungen zu den Änderungen und Ergänzungen, die in jedem größeren (nicht Patch-) Service-Software-Update vorgenommen wurden, finden Sie in den Versionshinweisen.

Amazon OpenSearch Service veröffentlicht regelmäßig Service-Software-Updates, die Funktionen hinzufügen oder Ihre Domains anderweitig verbessern. Das Feld Notifications (Benachrichtigungen) in der Konsole ist der einfachste Weg, um festzustellen, ob ein Update verfügbar ist oder um den Status eines Updates zu überprüfen. Jede Benachrichtigung enthält Details zum Service-Software-Update. Alle Service-Softwareupdates verwenden Blau/Grün-Bereitstellungen, um Ausfallzeiten zu minimieren.

Service-Software-Updates unterscheiden sich von OpenSearch Versions-Upgrades. Informationen zum Upgrade auf eine neuere Version von finden Sie OpenSearchunter the section called “Aktualisieren von Domains”.

Themen

- Optionale und erforderliche Updates
- Patch-Updates
- Überlegungen
- Starten eines Service-Software-Updates
- Planen von Software-Updates in Zeiten außerhalb der Spitzenzeiten

- Überwachen von Service-Software-Updates
- Wenn Domains nicht für ein Update in Frage kommen

Optionale und erforderliche Updates

OpenSearch Der Service verfügt über zwei große Kategorien von Service-Software-Updates:

Optionale Updates

Optionale Service-Software-Updates enthalten im Allgemeinen Verbesserungen und Unterstützung für neue Funktionen oder Funktionen. Optionale Updates werden auf Ihren Domains nicht erzwungen und es gibt keine feste Frist, um sie zu installieren. Die Verfügbarkeit des Updates wird per E-Mail und Konsolenbenachrichtigung mitgeteilt. Sie können wählen, ob Sie das Update sofort anwenden oder es auf ein geeigneteres Datum und eine angemessenere Uhrzeit verschieben möchten. Sie können sie auch während des Zeitfensters außerhalb der Spitzenlast der Domain planen. Die meisten Softwareupdates sind optional.

Unabhängig davon, ob Sie ein Update planen oder nicht, aktualisiert OpenSearch Service Ihre Servicesoftware automatisch für Sie, wenn Sie eine Änderung an der Domain vornehmen, die eine Blau/Grün-Bereitstellung verursacht.

Sie können Ihre Domain so konfigurieren, dass optionale Updates außerhalb der Spitzenzeiten automatisch angewendet werden. Wenn diese Option aktiviert ist, wartet OpenSearch Service mindestens 13 Tage ab dem Zeitpunkt, an dem ein optionales Update verfügbar ist, und plant dann das Update nach 72 Stunden (drei Tagen). Sie erhalten eine Konsolenbenachrichtigung, wenn das Update geplant ist, und Sie können wählen, ob Sie es für einen späteren Zeitpunkt verschieben möchten.

Um automatische Softwareupdates zu aktivieren, wählen Sie Automatisches Softwareupdate aktivieren, wenn Sie Ihre Domain erstellen oder aktualisieren. Um dieselbe Einstellung mit der zu konfigurieren AWS CLI, legen `true` Sie `--software-update-options` beim Erstellen oder Aktualisieren Ihrer Domain auf fest.

Erforderliche Aktualisierungen

Zu den erforderlichen Service-Softwareupdates gehören im Allgemeinen kritische Sicherheitskorrekturen oder andere obligatorische Updates, um die kontinuierliche Integrität und Funktionalität Ihrer Domain sicherzustellen. Beispiele für erforderliche Updates sind Log4j Common Vulnerabilities and Exposures (CVEs) und die Durchsetzung von Instance Metadata Service Version

2 (IMDSv2). Die Anzahl der obligatorischen Updates in einem Jahr beträgt normalerweise weniger als drei.

OpenSearch Der Service plant diese Updates automatisch und benachrichtigt Sie 72 Stunden (drei Tage) vor der geplanten Aktualisierung per E-Mail und Konsolenbenachrichtigung. Sie können wählen, ob Sie das Update sofort anwenden oder es auf ein geeigneteres Datum und eine angemessenere Uhrzeit innerhalb des zulässigen Zeitrahmens verschieben möchten. Sie können sie auch im nächsten Zeitfenster außerhalb der Spitzenlast der Domäne planen. Wenn Sie keine Maßnahmen für ein erforderliches Update ergreifen und keine Domänenänderungen vornehmen, die eine Blau/Grün-Bereitstellung verursachen, kann OpenSearch Service das Update jederzeit innerhalb des Zeitfensters außerhalb der Spitzenlast der Domäne über die angegebene Frist (in der Regel 14 Tage nach Verfügbarkeit) hinaus initiieren.

Unabhängig davon, wann das Update geplant ist, aktualisiert OpenSearch Service Ihre Domain automatisch für Sie, wenn Sie eine Änderung an der Domain vornehmen, die eine Blau/Grün-Bereitstellung verursacht.

Patch-Updates

Bei Service-Softwareversionen, die mit „-P“ und einer Nummer enden, wie etwa R20211203-*P4*, handelt es sich um Patch-Versionen. Patches werden vermutlich Leistungsverbesserungen, kleinere Bugfixes und Behebungen von Sicherheitslücken oder Verbesserungen der Sicherheitslage beinhalten. Patch-Versionen enthalten keine neuen Funktionen oder bahnbrechenden Änderungen und haben im Allgemeinen keine direkten oder spürbaren Auswirkungen auf die Benutzer. Die Service-Software-Benachrichtigung informiert Sie darüber, ob eine Patch-Version optional oder obligatorisch ist.

Überlegungen

Beachten Sie beim Aktualisieren Ihrer Domain folgende Punkte:

- Durch die manuelle Aktualisierung Ihrer Domain können Sie die Vorteile neuer Funktionen schneller nutzen. Wenn Sie Aktualisieren wählen, platziert Service die Anforderung in einer Warteschlange und beginnt mit der Aktualisierung, wenn es Zeit hat. OpenSearch
- Wenn Sie ein Service-Software-Update initiieren, sendet OpenSearch Service eine Benachrichtigung, wenn das Update gestartet wird und wenn es abgeschlossen ist.
- Software-Updates verwenden Blau/Grün-Bereitstellungen, um Ausfallzeiten zu minimieren. Aktualisierungen können die dedizierten Hauptknoten eines Clusters vorübergehend belasten.

Stellen Sie daher sicher, dass ausreichende Kapazität für den zugeordneten Overhead beibehalten wird.

- Aktualisierungen werden normalerweise innerhalb von Minuten abgeschlossen, können aber auch mehrere Stunden oder sogar Tage dauern, wenn Ihr System stark ausgelastet ist. Erwägen Sie, Ihre Domain während des konfigurierten Zeitfensters außerhalb der Spitzenlast zu aktualisieren, um lange Aktualisierungszeiträume zu vermeiden.

Starten eines Service-Software-Updates

Sie können ein Service-Software-Update über die OpenSearch Servicekonsole, die AWS CLIoder eines der SDKs anfordern.

Konsole

So fordern Sie ein Service-Software-Update an

1. Öffnen Sie die Amazon- OpenSearch Service-Konsole unter https://console.aws.amazon.com/aos/home.
2. Wählen Sie den Domänennamen aus, um dessen Konfiguration zu öffnen.
3. Wählen Sie Aktionen, Aktualisieren und eine der folgenden Optionen aus:

   - Update jetzt anwenden – plant sofort, dass die Aktion in der aktuellen Stunde ausgeführt wird, wenn Kapazität verfügbar ist. Wenn keine Kapazität verfügbar ist, stellen wir andere verfügbare Zeitfenster zur Auswahl zur Verfügung.
   - Planen Sie es im Out-Peak-Fenster – Nur verfügbar, wenn das Out-Peak-Fenster für die Domain aktiviert ist. Plant die Aktualisierung, die während des konfigurierten Zeitfensters außerhalb der Spitzenlast der Domain stattfindet. Es gibt keine Garantie dafür, dass das Update im nächsten unmittelbaren Zeitfenster durchgeführt wird. Abhängig von der Kapazität kann dies in nachfolgenden Tagen passieren. Weitere Informationen finden Sie unter the section called “Fenster außerhalb der Spitzenlast”.
   - Zeitplan für ein bestimmtes Datum und eine bestimmte Uhrzeit – Plant die Aktualisierung für ein bestimmtes Datum und eine bestimmte Uhrzeit. Wenn die von Ihnen angegebene Zeit aus Kapazitätsgründen nicht verfügbar ist, können Sie einen anderen Zeitraum auswählen.

Wenn Sie das Update für ein späteres Datum planen (innerhalb oder außerhalb des Zeitfensters außerhalb der Spitze der Domain), können Sie es jederzeit verschieben. Anweisungen finden Sie unter the section called “Neuplanung von Aktionen”.

4. Wählen Sie Bestätigen aus.

AWS CLI

Senden Sie eine start-service-software-update AWS CLI Anfrage, um ein Service-Software-Update zu initiieren. In diesem Beispiel wird die Aktualisierung sofort zur Warteschlange hinzugefügt:

```
aws opensearch start-service-software-update \
  --domain-name my-domain \
  --schedule-at "NOW"
```

Antwort:

```
{
    "ServiceSoftwareOptions": {
        "CurrentVersion": "R20220928-P1",
        "NewVersion": "R20220928-P2",
        "UpdateAvailable": true,
        "Cancellable": true,
        "UpdateStatus": "PENDING_UPDATE",
        "Description": "",
        "AutomatedUpdateDate": "1969-12-31T16:00:00-08:00",
        "OptionalDeployment": true
    }
}
```

Tip

Nachdem Sie ein Update angefordert haben, haben Sie ein kurzes Zeitfenster, in dem Sie es abbrechen können. Die Dauer dieses `PENDING_UPDATE` Zustands kann stark variieren und hängt von Ihrem AWS-Region und der Anzahl der gleichzeitigen Updates ab, die der OpenSearch Service durchführt. Um ein Update abzubrechen, verwenden Sie die -Konsole oder den `-cancel-service-software-update` AWS CLI Befehl.

Wenn die Anforderung mit einem fehlschlägt`BaseException`, bedeutet dies, dass die von Ihnen angegebene Zeit aus Kapazitätsgründen nicht verfügbar ist und Sie eine andere Zeit angeben müssen. OpenSearch Der Service bietet alternative verfügbare Slot-Vorschläge in der Antwort.

AWS SDKs

Dieses Python-Beispielskript verwendet die Methoden describe_domain und start_service_software_update aus dem , AWS SDK for Python (Boto3) um zu überprüfen, ob eine Domain für ein Service-Software-Update in Frage kommt, und startet in diesem Fall das Update. Sie müssen einen Wert für `domain_name` angeben.

```
import boto3
from botocore.config import Config
import time

# Build the client using the default credential configuration.
# You can use the CLI and run 'aws configure' to set access key, secret
# key, and default region.

my_config = Config(
    # Optionally lets you specify a Region other than your default.
    region_name='us-east-1'
)

domain_name = ''  # The name of the domain to check and update

client = boto3.client('opensearch', config=my_config)


def getUpdateStatus(client):
    """Determines whether the domain is eligible for an update"""
    response = client.describe_domain(
        DomainName=domain_name
    )
    sso = response['DomainStatus']['ServiceSoftwareOptions']
    if sso['UpdateStatus'] == 'ELIGIBLE':
        print('Domain [' + domain_name + '] is eligible for a service software update
 from version ' +
              sso['CurrentVersion'] + ' to version ' + sso['NewVersion'])
        updateDomain(client)
    else:
        print('Domain is not eligible for an update at this time.')
```

```
def updateDomain(client):
    """Starts a service software update for the eligible domain"""
    response = client.start_service_software_update(
        DomainName=domain_name
    )
    print('Updating domain [' + domain_name + '] to version ' +
          response['ServiceSoftwareOptions']['NewVersion'] + '...')
    waitForUpdate(client)


def waitForUpdate(client):
    """Waits for the domain to finish updating"""
    response = client.describe_domain(
        DomainName=domain_name
    )
    status = response['DomainStatus']['ServiceSoftwareOptions']['UpdateStatus']
    if status == 'PENDING_UPDATE' or status == 'IN_PROGRESS':
        time.sleep(30)
        waitForUpdate(client)
    elif status == 'COMPLETED':
        print('Domain [' + domain_name +
              '] successfully updated to the latest software version')
    else:
        print('Domain is not currently being updated.')

def main():
    getUpdateStatus(client)
```

Planen von Software-Updates in Zeiten außerhalb der Spitzenzeiten

Jede nach dem 16. Februar 2023 erstellte OpenSearch Service-Domain hat ein tägliches 10-Stunden-Fenster zwischen 22:00 Uhr und 8:00 Uhr Ortszeit, für die wir das außerhalb der Hauptverkehrszeit liegende Fenster in Betracht ziehen. OpenSearch Der Service verwendet dieses Fenster, um Service-Software-Updates für die Domain zu planen. Aktualisierungen außerhalb der Spitzenzeiten tragen dazu bei, die Belastung der dedizierten Hauptknoten eines Clusters während Zeiträumen mit höherem Datenverkehr zu minimieren. Der OpenSearch Service kann ohne Ihre Zustimmung keine Aktualisierungen außerhalb dieses 10-Stunden-Fensters initiieren.

- Für optional eUpdates benachrichtigt OpenSearch Service Sie über die Verfügbarkeit des Updates und fordert Sie auf, das Update in einem bevorstehenden Zeitfenster außerhalb der Spitzenzeiten zu planen.

- Für erforderliche Updates plant OpenSearch Service die Aktualisierung automatisch während eines bevorstehenden Zeitfensters außerhalb der Spitzenzeiten und benachrichtigt Sie drei Tage im Voraus. Sie können die Aktualisierung (für innerhalb oder außerhalb des Zeitfensters außerhalb der Spitzenlast) verschieben, jedoch nur innerhalb des erforderlichen Zeitrahmens, damit die Aktualisierung abgeschlossen werden kann.

Für jede Domain können Sie die Standardstartzeit um 22:00 Uhr mit einer benutzerdefinierten Zeit überschreiben. Anweisungen finden Sie unter the section called “Konfigurieren eines benutzerdefinierten Fensters außerhalb der Spitzenlast”.

Konsole

So planen Sie ein Update während eines bevorstehenden Zeitfensters außerhalb der Spitzenzeiten

1. Öffnen Sie die Amazon- OpenSearch Service-Konsole unter https://console.aws.amazon.com/aos/home.
2. Wählen Sie den Domänennamen aus, um dessen Konfiguration zu öffnen.
3. Wählen Sie Aktionen, Aktualisieren.
4. Wählen Sie Planen im Fenster außerhalb der Spitzenzeiten aus.
5. Wählen Sie Bestätigen aus.

Sie können die geplante Aktion auf der Registerkarte Off-Peak-Fenster anzeigen und sie jederzeit neu planen. Siehe the section called “Anzeigen geplanter Aktionen”.

CLI

Um ein Update während eines bevorstehenden Fensters außerhalb der Spitzenzeiten mit der zu planen AWS CLI, senden Sie eine -StartServiceSoftwareUpdateAnforderung und geben Sie `OFF_PEAK_WINDOW` für den `--schedule-at`Parameter an:

```
aws opensearch start-service-software-update \
  --domain-name my-domain \
  --schedule-at "OFF_PEAK_WINDOW"
```

Überwachen von Service-Software-Updates

OpenSearch Der Service sendet eine Benachrichtigung, wenn ein Service-Software-Update verfügbar, erforderlich, gestartet, abgeschlossen oder fehlgeschlagen ist. Sie können diese

Benachrichtigungen im Bereich Benachrichtigungen der OpenSearch Servicekonsole anzeigen. Der Schweregrad der Benachrichtigung ist`Informational`, wenn das Update optional ist und`High` wenn es erforderlich ist.

OpenSearch Der Service sendet auch Service-Softwareereignisse an Amazon EventBridge. Sie können verwenden, EventBridge um Regeln zu konfigurieren, die eine E-Mail senden oder eine bestimmte Aktion ausführen, wenn ein Ereignis empfangen wird. Ein Beispiel-Walkthrough finden Sie unte the section called “Tutorial: Senden von SNS-Warnungen für verfügbare Updates”.

Informationen zum Format der einzelnen Service-Software-Ereignisse, die an Amazon gesendet werden EventBridge, finden Sie unter the section called “Aktualisieren der Software”.

Wenn Domains nicht für ein Update in Frage kommen

Ihre Domain ist für ein Service-Software-Update nicht berechtigt, wenn sie sich in einem der folgenden Zustände befindet:

Status	Beschreibung
Domain in Verarbeitung	Die Domain befindet sich in der Mitte einer Konfigurationsänderung. Überprüfen Sie die Update-Berechtigung, nachdem die Operation abgeschlossen ist.
Roter Cluster-Status	Ein oder mehrere Indizes im Cluster sind rot. Fehlerbehandlungsschritte finden Sie unter the section called “Roter Cluster-Status”.
Hohe Fehlerrate	Der OpenSearch Cluster gibt eine große Anzahl von 5xx-Fehlern zurück, wenn er versucht, Anfragen zu verarbeiten. Dieses Problem ist in der Regel das Ergebnis zu vieler gleichzeitiger Lese- oder Schreibanforderungen. Erwägen Sie, den Datenverkehr zu dem Cluster zu reduzieren oder Ihre Domain zu skalieren.
Split brain	Split brain bedeutet, dass Ihr OpenSearch Cluster über mehr als einen Hauptknoten verfügt und sich in zwei Cluster aufgeteilt hat, die sich nicht von selbst wieder hinzufügen. Sie können split brain vermeiden, indem Sie die empfohlene Anzahl der dedizierten Hauptknoten verwenden. Für Hilfe zur Wiederherstellung von split brain wenden Sie sich an AWS Support.

Status	Beschreibung
Problem mit der Amazon Cognito Integration	Ihre Domain verwendet die Authentifizierung für OpenSearch Dashboards und OpenSearch der Service kann keine oder mehrere Amazon Cognito-Ressourcen finden. Dieses Problem tritt in der Regel auf, wenn der Amazon-Cognito-Benutzerpool fehlt. Um das Problem zu beheben, erstellen Sie die fehlende Ressource neu und konfigurieren Sie die OpenSearch Service-Domain für ihre Verwendung.
Andere -Service-Probleme	Probleme mit dem OpenSearch Service selbst können dazu führen, dass Ihre Domain als nicht für ein Update berechtigt angezeigt wird. Wenn keine der vorangehenden Bedingungen für Ihre Domain gelten und das Problem mehr als einen Tag bestehen bleibt, wenden Sie sich bitte an AWS Support.

Definieren von Off-Peak-Fenstern für Amazon OpenSearch Service

Wenn Sie eine Amazon- OpenSearch Service-Domain erstellen, definieren Sie ein tägliches 10-Stunden-Fenster, das als außerhalb der Spitzenzeiten betrachtet wird. Der OpenSearch Service verwendet dieses Fenster, um Service-Softwareaktualisierungen und Auto-Tune-Optimierungen zu planen, die nach Möglichkeit eine Blau/Grün-Bereitstellung während relativ kürzerer Datenverkehrszeiten erfordern. Blau/Grün bezieht sich auf den Prozess der Erstellung einer neuen Umgebung für Domain-Updates und der Weiterleitung von Benutzern an die neue Umgebung, nachdem diese Updates abgeschlossen sind.

Obwohl Blau/Grün-Bereitstellungen unterbrechungsfrei sind, empfehlen wir Ihnen, diese Bereitstellungen während des konfigurierten Zeitfensters außerhalb der Spitzenlast der Domain zu planen, um potenzielle Leistungseinbußen zu minimieren, während Ressourcen für eine Blau/Grün-Bereitstellung genutzt werden. Aktualisierungen wie Knotenaustausch oder solche, die sofort in der Domain bereitgestellt werden müssen, verwenden nicht das Fenster außerhalb der Spitzenlast.

Sie können die Startzeit für das Fenster außerhalb der Spitzenlast ändern, aber Sie können die Länge des Fensters nicht ändern.

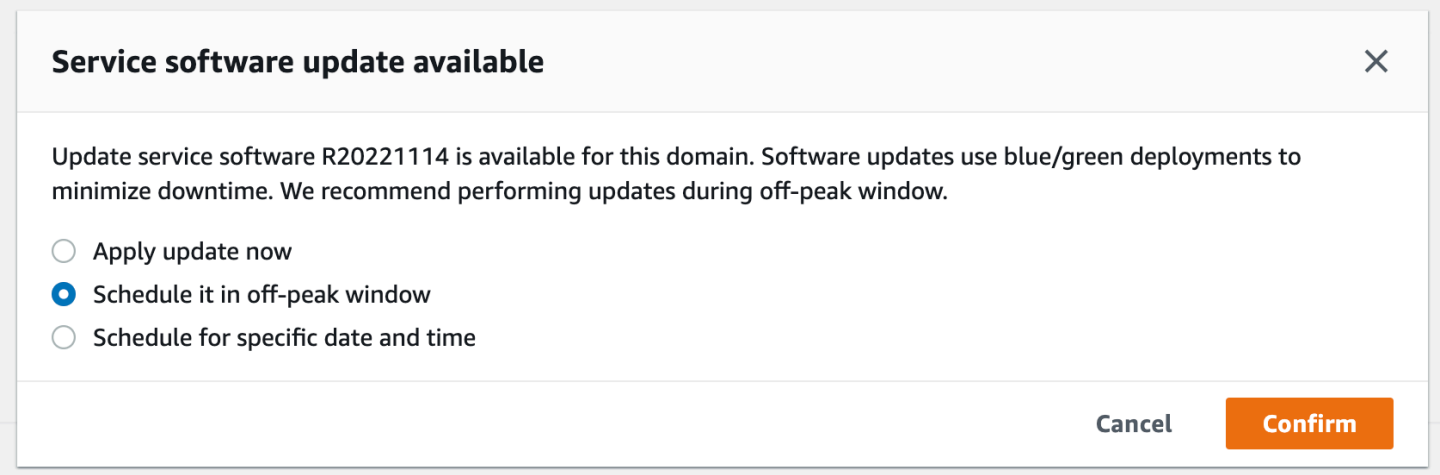
> **Note**
>
> Off-Peak-Fenster wurden am 16. Februar 2023 eingeführt. Für alle Domänen, die vor diesem Datum erstellt wurden, ist das Fenster außerhalb der Spitzenlast standardmäßig deaktiviert. Sie müssen das Fenster außerhalb der Spitzenzeiten für diese Domains manuell aktivieren und konfigurieren. Für alle Domains, die nach diesem Datum erstellt wurden, ist das Fenster außerhalb der Spitzenlast standardmäßig aktiviert. Sie können das Fenster außerhalb der Spitzenlast für eine Domäne nicht deaktivieren, nachdem sie aktiviert wurde.

Themen

Software-Updates außerhalb der Spitzenlast

OpenSearch Der Service verfügt über zwei große Kategorien von Service-Software-Updates – optional und erforderlich. Beide Typen erfordern Blau/Grün-Bereitstellungen. Optionale Updates werden in Ihren Domains nicht erzwungen, während erforderliche Updates automatisch installiert werden, wenn Sie vor Ablauf der angegebenen Frist keine Maßnahmen ergreifen (in der Regel zwei Wochen nach Verfügbarkeit). Weitere Informationen finden Sie unter the section called “Optionale und erforderliche Updates”.

Wenn Sie ein optional esUpdate initiieren, haben Sie die Möglichkeit, das Update sofort anzuwenden, für ein nachfolgendes Zeitfenster außerhalb der Spitzenzeiten zu planen oder ein benutzerdefiniertes Datum und eine benutzerdefinierte Uhrzeit anzugeben, um es anzuwenden.



Für erforderliche Updates plant OpenSearch Service automatisch ein Datum und eine Uhrzeit außerhalb der Spitzenzeiten, um das Update durchzuführen. Sie erhalten drei Tage vor dem geplanten Update eine Benachrichtigung und können wählen, ob Sie den Zeitplan für ein späteres Datum und eine spätere Uhrzeit innerhalb des erforderlichen Bereitstellungszeitraums verschieben möchten. Anweisungen finden Sie unter the section called “Neuplanung von Aktionen”.

Optimierungen der automatischen Optimierung außerhalb der Spitzenzeiten

Zuvor verwendete die automatische Optimierung Wartungsfenster, um Änderungen zu planen, die eine Blau/Grün-Bereitstellung erforderten. Domains, für die vor der Einführung von Off-Peak-Fenstern bereits die automatische Optimierung und Wartungsfenster aktiviert waren, verwenden weiterhin Wartungsfenster für diese Updates, es sei denn, Sie migrieren sie zur Verwendung des Off-Peak-Fensters.

Wir empfehlen Ihnen, Ihre Domains so zu migrieren, dass sie das Fenster außerhalb der Spitzenlast verwenden, da es verwendet wird, um andere Aktivitäten in der Domain zu planen, z. B. Service-Softwate-Updates. Anweisungen finden Sie unter the section called “Migrieren von Wartungsfenstern zur automatischen Optimierung”. Sie können nach der Migration Ihrer Domain zum Out-Peak-Fenster nicht wieder zur Verwendung von Wartungsfenstern zurückkehren.

Alle Domains, die nach dem 16. Februar 2023 erstellt wurden, verwenden das Fenster außerhalb der Spitzenlast und nicht ältere Wartungsfenster, um Blau/Grün-Bereitstellungen zu planen. Sie können das Zeitfenster außerhalb der Spitzenlast für eine Domain nicht deaktivieren. Eine Liste der Auto-Tune-Optimierungen, die Blau/Grün-Bereitstellungen erfordern, finden Sie unter the section called “Änderungsarten”.

Aktivieren des Fensters außerhalb der Spitzenlast

Für alle Domains, die vor dem 16. Februar 2023 erstellt wurden (als Off-Peak-Fenster eingeführt wurden), ist die Funktion standardmäßig deaktiviert. Sie müssen es für diese Domains manuell aktivieren. Sie können das Fenster außerhalb der Spitzenlast nicht deaktivieren, nachdem es aktiviert wurde.

Konsole

So aktivieren Sie das Zeitfenster außerhalb der Spitzenlast für eine Domain

1. Öffnen Sie die Amazon- OpenSearch Service-Konsole unter https://console.aws.amazon.com/aos/home.
2. Wählen Sie den Namen der Domain aus, um ihre Konfiguration zu öffnen.
3. Navigieren Sie zur Registerkarte Off-Peak-Fenster und wählen Sie Bearbeiten aus.
4. Geben Sie eine benutzerdefinierte Startzeit in UTC (Coordinated Universal Time) an. Um beispielsweise eine Startzeit von 23:30 Uhr in der Region USA West (Oregon) zu konfigurieren, geben Sie 07:30 an.
5. Wählen Sie Änderungen speichern aus.

CLI

Senden Sie eine -UpdateDomainConfigAnforderungAWS CLI, um das Fenster außerhalb der Spitzenlast mit der zu ändern:

```
aws opensearch update-domain-config \
  --domain-name my-domain \
  --off-peak-window-options 'Enabled=true,
 OffPeakWindow={WindowStartTime={Hours=02,Minutes=00}}'
```

Wenn Sie keine Startzeit für ein benutzerdefiniertes Fenster angeben, wird standardmäßig 00:00 UTC verwendet.

Konfigurieren eines benutzerdefinierten Fensters außerhalb der Spitzenlast

Sie geben ein benutzerdefiniertes Off-Peak-Fenster für Ihre Domain in UTC (Coordinated Universal Time) an. Wenn Sie beispielsweise möchten, dass das Zeitfenster außerhalb der Spitzenzeiten um 23:00 Uhr für eine Domain in der Region USA Ost (Nord-Virginia) beginnt, geben Sie 04:00 UTC an.

Konsole

So ändern Sie das Zeitfenster außerhalb der Spitzenlast für eine Domain

1. Öffnen Sie die Amazon- OpenSearch Service-Konsole unter https://console.aws.amazon.com/aos/home.
2. Wählen Sie den Namen der Domain aus, um ihre Konfiguration zu öffnen.
3. Navigieren Sie zur Registerkarte „Off-Peak-Fenster“. Sie können das konfigurierte Zeitfenster außerhalb der Spitzenlast und eine Liste der bevorstehenden geplanten Aktionen für die Domain anzeigen.
4. Wählen Sie Bearbeiten und geben Sie eine neue Startzeit in UTC an. Um beispielsweise eine Startzeit von 21:00 Uhr in der Region USA Ost (Nord-Virginia) zu konfigurieren, geben Sie 02:00 UCT an.
5. Wählen Sie Änderungen speichern aus.

CLI

Um ein benutzerdefiniertes Zeitfenster außerhalb der Spitzenlast mit der zu konfigurierenAWS CLI, senden Sie eine -UpdateDomainConfigAnforderung und geben Sie Stunde und Minute im 24-Stunden-Zeitformat an.

Die folgende Anforderung ändert beispielsweise die Startzeit des Fensters auf 2:00 Uhr UTC:

```
aws opensearch update-domain-config \
  --domain-name my-domain \
  --off-peak-window-options 'OffPeakWindow={WindowStartTime={Hours=02,Minutes=00}}'
```

Wenn Sie keine Startzeit für das Fenster angeben, wird standardmäßig die Ortszeit 22:00 Uhr für die verwendetAWS-Region, in der die Domain erstellt wird.

Anzeigen geplanter Aktionen

Sie können alle Aktionen anzeigen, die derzeit für jede Ihrer Domains geplant, in Bearbeitung oder ausstehend sind. Aktionen können den Schweregrad `HIGH`, `MEDIUM`und haben`LOW`.

Aktionen können die folgenden Status haben:

- `Pending update` – Die Aktion befindet sich in der zu verarbeitenden Warteschlange.

- `In progress` – Die Aktion ist derzeit in Bearbeitung.
- `Failed` – Die Aktion konnte nicht abgeschlossen werden.
- `Completed` – Die Aktion wurde erfolgreich abgeschlossen.
- `Not eligible` – Nur für Service-Software-Updates. Die Aktualisierung kann nicht fortgesetzt werden, da sich der Cluster in einem fehlerhaften Zustand befindet.
- `Eligible` – Nur für Service-Software-Updates. Die Domain ist für ein Update berechtigt.

Konsole

Die OpenSearch Servicekonsole zeigt alle geplanten Aktionen innerhalb der Domänenkonfiguration zusammen mit dem Schweregrad und dem aktuellen Status jeder Aktion an.

So zeigen Sie geplante Aktionen für eine Domäne an

1. Öffnen Sie die Amazon- OpenSearch Service-Konsole unter https://console.aws.amazon.com/aos/home.
2. Wählen Sie den Namen der Domain aus, um ihre Konfiguration zu öffnen.
3. Navigieren Sie zur Registerkarte Off-Peak-Fenster.
4. Zeigen Sie unter Geplante Aktionen alle Aktionen an, die derzeit für die Domäne geplant, in Bearbeitung oder ausstehend sind.

CLI

Um geplante Aktionen mit der anzuzeigenAWS CLI, senden Sie eine -ListScheduledActionsAnforderung:

```
aws opensearch list-scheduled-actions \
  --domain-name my-domain
```

Antwort:

```
{
    "ScheduledActions": [
        {
            "Cancellable": true,
            "Description": "The Deployment type is : BLUE_GREEN.",
            "ID": "R20220721-P13",
            "Mandatory": false,
```

```
            "Severity": "HIGH",
            "ScheduledBy": "CUSTOMER",
            "ScheduledTime": 1.673871601E9,
            "Status": "PENDING_UPDATE",
            "Type": "SERVICE_SOFTWARE_UPDATE",
        },
        {
            "Cancellable": true,
            "Description": "Amazon Opensearch will adjust the young generation JVM
 arguments on your domain to improve performance",
            "ID": "Auto-Tune",
            "Mandatory": true,
            "Severity": "MEDIUM",
            "ScheduledBy": "SYSTEM",
            "ScheduledTime": 1.673871601E9,
            "Status": "PENDING_UPDATE",
            "Type": "JVM_HEAP_SIZE_TUNING",
        }
    ]
}
```


Neuplanung von Aktionen

OpenSearch Der Service benachrichtigt Sie über geplante Service-Softwareupdates und automatische Optimierungen. Sie können die Änderung sofort anwenden oder für ein späteres Datum und eine spätere Uhrzeit verschieben.

> **Note**
>
> OpenSearch Der Service kann die Aktion innerhalb einer Stunde nach der von Ihnen ausgewählten Zeit planen. Wenn Sie beispielsweise ein Update um 17 Uhr anwenden möchten, kann es zwischen 17 und 18 Uhr angewendet werden.

Konsole

So planen Sie eine Aktion neu

1. Öffnen Sie die Amazon- OpenSearch Service-Konsole unter https://console.aws.amazon.com/aos/home.
2. Wählen Sie den Namen der Domain aus, um ihre Konfiguration zu öffnen.

3. Navigieren Sie zur Registerkarte Fenster außerhalb der Spitzenlast.
4. Wählen Sie unter Geplante Aktionen die Aktion aus und wählen Sie Neu planen aus.
5. Wählen Sie eine der folgenden Optionen:

   - Update jetzt anwenden – plant sofort, dass die Aktion in der aktuellen Stunde ausgeführt wird, wenn Kapazität verfügbar ist. Wenn keine Kapazität verfügbar ist, stellen wir andere verfügbare Zeitfenster zur Auswahl zur Verfügung.
   - Planen im Zeitfenster außerhalb der Spitzenlast – Markiert die Aktion, die während eines bevorstehenden Zeitfensters außerhalb der Spitzenlast aufgenommen werden soll. Es gibt keine Garantie dafür, dass die Änderung im nächsten Fenster implementiert wird. Abhängig von der Kapazität kann dies in nachfolgenden Tagen passieren.
   - Zeitplan für dieses Update ändern – Ermöglicht Ihnen die Angabe eines benutzerdefinierten Datums und einer benutzerdefinierten Uhrzeit, um die Änderung anzuwenden. Wenn die von Ihnen angegebene Zeit aus Kapazitätsgründen nicht verfügbar ist, können Sie einen anderen Zeitfenster auswählen.
   - Geplante Aktualisierung abbrechen – Bricht die Aktualisierung ab. Diese Option ist nur für optionale Service-Software-Updates verfügbar. Sie ist nicht für automatische Optimierungsaktionen oder obligatorische Softwareupdates verfügbar.
6. Wählen Sie Änderungen speichern aus.

CLI

Um eine Aktion mit der neu zu planenAWS CLI, senden Sie eine -UpdateScheduledActionAnforderung. Senden Sie eine -`ListScheduledActions`Anforderung, um die Aktions-ID abzurufen.

Die folgende Anforderung plant ein Service-Software-Update für ein bestimmtes Datum und eine bestimmte Uhrzeit:

```
aws opensearch update-scheduled-action \
  --domain-name my-domain \
  --action-id R20220721-P13 \
  --action-type "SERVICE_SOFTWARE_UPDATE" \
  --desired-start-time 1677348395000 \
  --schedule-at TIMESTAMP
```

Antwort:

```
{
   "ScheduledAction": {
      "Cancellable": true,
      "Description": "Cluster status is updated.",
      "Id": "R20220721-P13",
      "Mandatory": false,
      "ScheduledBy": "CUSTOMER",
      "ScheduledTime": 1677348395000,
      "Severity": "HIGH",
      "Status": "PENDING_UPDATE",
      "Type": "SERVICE_SOFTWARE_UPDATE"
   }
}
```

Wenn die Anforderung mit einem fehlschlägt`SlotNotAvailableException`, bedeutet dies, dass die von Ihnen angegebene Zeit aus Kapazitätsgründen nicht verfügbar ist und Sie eine andere Zeit angeben müssen. OpenSearch Der Service bietet alternative verfügbare Slot-Vorschläge in der Antwort.

Migrieren von Wartungsfenstern zur automatischen Optimierung

Wenn eine Domain vor dem 16. Februar 2023 erstellt wurde, könnte sie Wartungsfenster verwenden, um Auto-Tune-Optimierungen zu planen, die eine Blau/Grün-Bereitstellung erfordern. Sie können Ihre vorhandenen Auto-Tune-Domains so migrieren, dass stattdessen das Fenster außerhalb der Spitzenzeiten verwendet wird.

> **Note**
>
> Sie können nach der Migration Ihrer Domain zur Verwendung von Out-Peak-Fenstern nicht wieder zur Verwendung von Wartungsfenstern zurückkehren.

Konsole

So migrieren Sie eine Domain zur Verwendung des Fensters außerhalb der Spitzenlast

1. Wählen Sie in der Amazon- OpenSearch Service-Konsole den Namen der Domain aus, um ihre Konfiguration zu öffnen.
2. Gehen Sie zur Registerkarte Automatische Optimierung und wählen Sie Bearbeiten aus.
3. Wählen Sie In ein Fenster außerhalb der Spitzenlast migrieren aus.

4. Geben Sie für Startzeit (UTC) eine tägliche Startzeit für das Zeitfenster außerhalb der Spitzenzeiten in UTC (Universal Coordinated Time) an.
5. Wählen Sie Änderungen speichern aus.

CLI

Senden Sie eine -UpdateDomainConfigAnforderungAWS CLI, um mithilfe der von einem Wartungsfenster mit automatischer Optimierung zum Fenster außerhalb der Spitzenlast zu migrieren:

```
aws opensearch update-domain-config \
  --domain-name my-domain \
  --auto-tune-options
 DesiredState=ENABLED,UseOffPeakWindow=true,MaintenanceSchedules=[]
```

Das Fenster außerhalb der Spitzenlast muss aktiviert sein, damit Sie eine Domain vom Wartungsfenster für die automatische Optimierung zum Fenster außerhalb der Spitzenlast migrieren können. Sie können das Fenster außerhalb der Spitzenlast in einer separaten Anforderung oder in derselben Anforderung aktivieren. Detaillierte Anweisungen finden Sie unter the section called “Aktivieren des Fensters außerhalb der Spitzenlast”.

Benachrichtigungen in Amazon OpenSearch Service

Benachrichtigungen in Amazon OpenSearch Service enthalten wichtige Informationen über die Leistung und den Zustand Ihrer Domains. OpenSearch Service benachrichtigt Sie über Service-Software-Updates, automatische Optimierungsverbesserungen, Cluster-Zustandsereignisse und Domainfehler. Benachrichtigungen sind für alle Versionen von OpenSearch und Elasticsearch OSS verfügbar.

Sie können Benachrichtigungen im Bereich Benachrichtigungen der OpenSearch Servicekonsole anzeigen. Alle Benachrichtigungen für OpenSearch Service werden auch in Amazon EventBridge angezeigt. Eine vollständige Liste der Benachrichtigungen und Beispielereignisse finden Sie unter the section called “Überwachung von Ereignissen”.

Themen

- Einstieg in die Verwendung von Benachrichtigungen
- Schweregrad
- EventBridge Beispielereignis

Einstieg in die Verwendung von Benachrichtigungen

Benachrichtigungen werden automatisch aktiviert, wenn Sie eine Domain erstellen. Gehen Sie zum Bereich Benachrichtigungen der OpenSearch Servicekonsole, um Benachrichtigungen zu überwachen und zu bestätigen. Jede Benachrichtigung enthält Informationen wie die Uhrzeit, zu der sie veröffentlicht wurde, die Domain, auf die sie sich bezieht, einen Schweregrad und Statuslevel sowie eine kurze Erklärung. Sie können frühere Benachrichtigungen für bis zu 90 Tage in der Konsole anzeigen.

Nachdem Sie auf das Benachrichtigungsfeld zugegriffen oder eine Benachrichtigung bestätigt haben, erhalten Sie möglicherweise eine Fehlermeldung, dass Sie keine Berechtigungen zum Ausführen von `es:ListNotifications` oder `es:UpdateNotificationStatus` haben. Um dieses Problem zu beheben, erteilen Sie Ihrem Benutzer oder Ihrer Rolle die folgenden Berechtigungen in IAM:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "es:UpdateNotificationStatus",
      "es:ListNotifications"
    ],
    "Resource": "arn:aws:es:*:123456789012:domain/*"
  }]
}
```

Die IAM-Konsole löst einen Fehler aus („IAM erkennt eine oder mehrere Aktionen nicht“), den Sie sicher ignorieren können. Sie können die `es:UpdateNotificationStatus`-Aktion auch auf bestimmte Domains beschränken. Weitere Informationen hierzu finden Sie unter the section called “Richtlinienelementreferenz”.

Schweregrad

Benachrichtigungen im OpenSearch Service können informativ sein, die sich auf jede bereits ausgeführte Aktion oder den Betrieb Ihrer Domäne beziehen, oder umsetzbare , bei denen Sie bestimmte Maßnahmen ergreifen müssen, z. B. das Anwenden eines obligatorischen Sicherheitspatches. Jeder Benachrichtigung ist ein Schweregrad zugeordnet, der `Informational`, `Low`, `Medium`, `High`, oder `Critical` sein kann. In der folgenden Tabelle werden alle Schweregrade zusammengefasst:

Schweregrad	Beschreibung	Beispiele
`Informational`	Informationen zum Betrieb Ihrer Domain.	• Service-Softwareaktualisierung verfügbar • Automatische Optimierung gestartet
`Low`	Eine empfohlene Maßnahme, hat jedoch keine negativen Auswirkungen auf die Domain-Verfügbarkeit oder -leistung, wenn keine Maßnahmen ergriffen werden.	• Automatische Optimierung abgebrochen • Warnung mit hoher Shard-Anzahl
`Medium`	Es kann Auswirkungen haben, wenn die empfohlene Aktion nicht ausgeführt wird, aber es gibt ein erweitertes Zeitfenster für die auszuführende Aktion.	• Service-Softwareaktualisierung fehlgeschlagen • Limit für Shard-Anzahl überschritten
`High`	Dringende Maßnahmen sind erforderlich, um nachteilige Auswirkungen zu vermeiden.	• Aktualisierung der Servicesoftware erforderlich • KMS-Schlüssel unzugänglich
`Critical`	Sofortiges Handeln ist erforderlich, um nachteilige Auswirkungen zu vermeiden oder zu reparieren.	Aktuell keine verfügbar

EventBridge Beispielereignis

Das folgende Beispiel zeigt ein - OpenSearch Service-Benachrichtigungsereignis, das an Amazon gesendet wird EventBridge. Die Benachrichtigung hat den Schweregrad von `Informational`, da das Update optional ist:

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Available",
    "severity": "Informational",
    "description": "Service software update [R20200330-p1] available."
  }
}
```

Konfiguration einer Multi-AZ-Domain in Amazon Service OpenSearch

Um Datenverlust zu verhindern und die Ausfallzeiten des Amazon OpenSearch Service-Clusters im Falle einer Serviceunterbrechung zu minimieren, können Sie Knoten auf zwei oder drei Availability Zones in derselben Region verteilen, eine Konfiguration, die als Multi-AZ bezeichnet wird. Availability Zones sind isolierte Standorte innerhalb jeder AWS Region.

Für Domains, auf denen Produktionsworkloads ausgeführt werden, empfehlen wir die Bereitstellungsoption Multi-AZ mit Standby, mit der die folgende Konfiguration erstellt wird:

- Die Domain wurde in drei Zonen bereitgestellt.
- Instance-Typen der aktuellen Generation für dedizierte Master- und Datenknoten.
- Drei dedizierte Masterknoten und drei (oder ein Vielfaches von drei) Datenknoten.
- Mindestens zwei Replikate für jeden Index in Ihrer Domain oder ein Vielfaches von drei Kopien von Daten (einschließlich Primärknoten und Replikaten).

Der Rest dieses Abschnitts enthält Erläuterungen und Kontext zu diesen Konfigurationen.

Multi-AZ mit Standby

Multi-AZ mit Standby ist eine Bereitstellungsoption für Amazon OpenSearch Service-Domains, die eine Verfügbarkeit von 99,99%, konsistente Leistung für Produktionsworkloads und eine vereinfachte Domainkonfiguration und -verwaltung bietet. Wenn Sie Multi-AZ mit Standby verwenden, sind Domains widerstandsfähig gegen Infrastrukturausfälle, ohne dass sich dies auf Leistung oder Verfügbarkeit auswirkt. Diese Bereitstellungsoption erfüllt diesen Standard, indem sie eine Reihe von bewährten Methoden vorschreibt, z. B. eine bestimmte Anzahl von Datenknoten, die Anzahl der Master-Knoten, den Instanztyp, die Anzahl der Replikate, die Einstellungen für Softwareupdates und die Aktivierung von Auto-Tune.

Wenn Sie Multi-AZ mit Standby verwenden, erstellt OpenSearch Service eine Domain, die sich über drei Availability Zones erstreckt, wobei jede Zone eine vollständige Kopie der Daten enthält und die Daten gleichmäßig auf jede der Zonen verteilt sind. Ihre Domain reserviert Knoten in einer dieser Zonen als Standby-Knoten, was bedeutet, dass sie keine Suchanfragen bearbeiten. Wenn OpenSearch Service einen Fehler in der zugrunde liegenden Infrastruktur feststellt, aktiviert er die Standby-Knoten automatisch in weniger als einer Minute. Die Domain bedient weiterhin Indizierungs- und Suchanfragen, und jede Auswirkung beschränkt sich auf die Zeit, die für die Durchführung des Failovers benötigt wird. Es findet keine Umverteilung von Daten oder Ressourcen statt, sodass die Clusterleistung nicht beeinträchtigt wird und das Risiko einer verminderten Verfügbarkeit entfällt. Multi-AZ mit Standby ist ohne zusätzliche Kosten erhältlich.

Sie haben zwei Möglichkeiten, eine Domain mit Standby auf dem AWS Management Console zu erstellen. Zunächst können Sie eine Domäne mit der Erstellungsmethode Easy Create erstellen. Der OpenSearch Service verwendet dann automatisch eine vordefinierte Konfiguration, die Folgendes umfasst:

- Drei Availability Zones, von denen eine als Standby fungiert
- Drei dedizierte Master-Knoten und Datenknoten
- Auto-Tune ist auf der Domain aktiviert
- GP3-Speicher für die Datenknoten

Sie können auch die Erstellungsmethode „Standard“ wählen und als Bereitstellungsoption „Domäne mit Standby“ auswählen. Auf diese Weise können Sie Ihre Domain individuell anpassen und gleichzeitig wichtige Standby-Funktionen wie drei Zonen und drei Masterknoten vorschreiben. Wir empfehlen, eine Anzahl von Datenknoten zu wählen, die einem Vielfachen von drei (der Anzahl der Availability Zones) entspricht.

Sobald Sie Ihre Domain erstellt haben, können Sie zu den Seiten mit den Domain-Details navigieren und auf der Registerkarte Cluster-Konfiguration überprüfen, ob 3-AZ mit Standby unter Availability Zone (n) angezeigt wird.

Wenn Sie Probleme bei der Migration einer vorhandenen Domain zu Multi-AZ mit Standby haben, finden Sie im Leitfaden zur Fehlerbehebung weitere Informationen unter Fehler bei der Migration zu Multi-AZ mit Standby.

Einschränkungen

Beachten Sie beim Einrichten einer Domain mit Multi-AZ mit Standby die folgenden Einschränkungen:

- Die Gesamtzahl der Shards auf einem Knoten darf 1000 nicht überschreiten, die Gesamtzahl der Shards in einem Cluster darf 75000 nicht überschreiten und die Größe eines einzelnen Shards darf 65 GB nicht überschreiten.
- Multi-AZ mit Standby funktioniert nur mit den Instance-Typen`m5`,`c5`,,`r5`, `r6gc6g`, `m6g` und. `r6gd` `i3` Weitere Informationen zu unterstützten Instances finden Sie unter Unterstützte Instance-Typen.
- Sie können nur bereitgestellte IOps-SSD, Allzweck-SSD (GP3) oder instanzgestützten Speicher mit Standby verwenden.
- Wenn Sie die Aktivierung UltraWarmauf einer Multi-AZ mit Standby-Domain durchführen, muss die Anzahl der warmen Knoten ein Vielfaches der Anzahl der verwendeten Availability Zones sein.

Multi-AZ ohne Standby

OpenSearch Der Service unterstützt weiterhin Multi-AZ ohne Standby, was eine Verfügbarkeit von 99,9% bietet. Die Knoten sind über die Availability Zone (n) verteilt, und die Verfügbarkeit hängt von der Anzahl der Availability Zones und Datenkopien ab. Während Sie bei Standby Ihre Domain nach bewährten Methoden konfigurieren müssen, können Sie ohne Standby Ihre eigene Anzahl von Availability Zones, Nodes und Replicas wählen. Wir empfehlen diese Option nur, wenn Sie über bestehende Workflows verfügen, die durch die Erstellung von Domains mit Standby gestört würden.

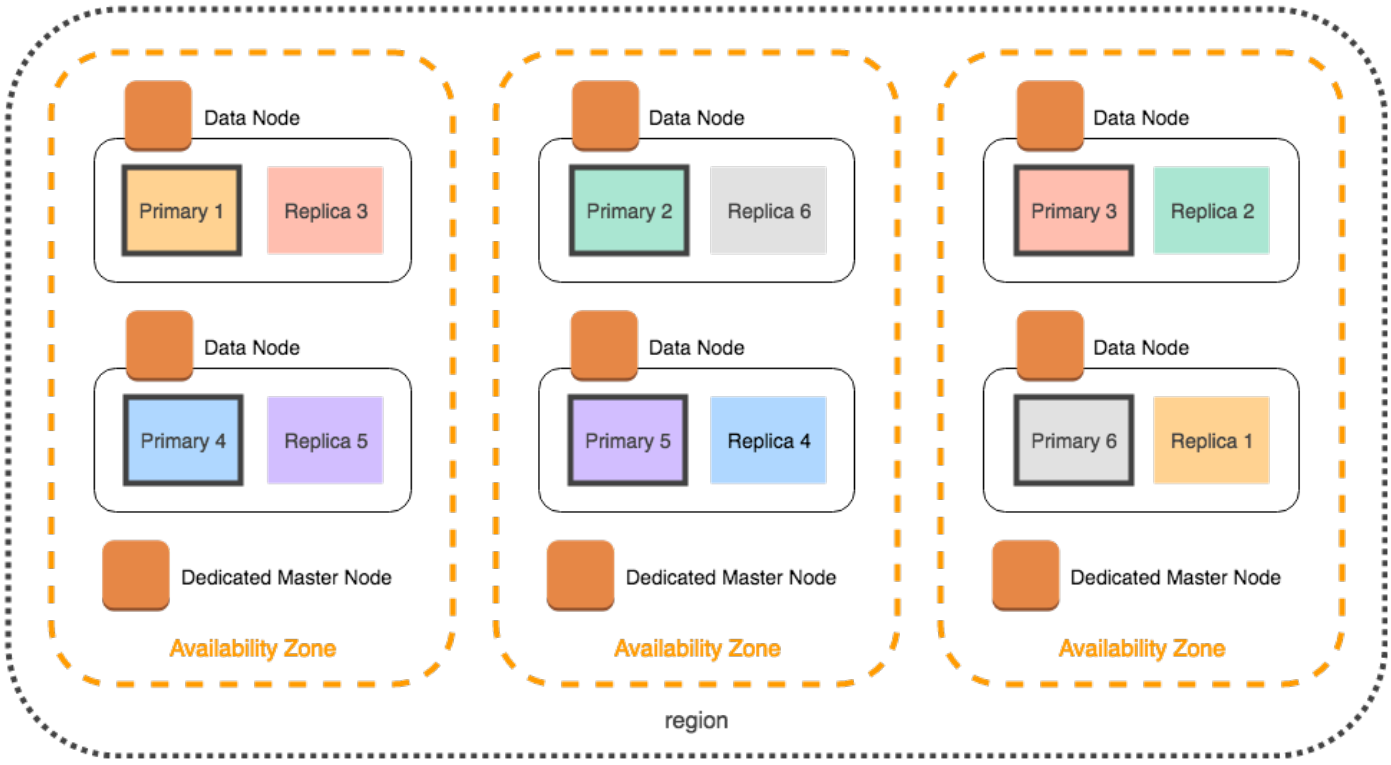
Wenn Sie sich für diese Option entscheiden, empfehlen wir dennoch, drei Availability Zones auszuwählen, um auch bei Knoten-, Festplatten- und Single-AZ-Ausfällen widerstandsfähig zu bleiben. Wenn ein Fehler auftritt, verteilt der Cluster die Daten auf die verbleibenden Ressourcen neu, um Verfügbarkeit und Redundanz aufrechtzuerhalten. Diese Datenverschiebung erhöht die Ressourcennutzung im Cluster und kann sich auf die Leistung auswirken. Wenn der Cluster nicht

richtig dimensioniert ist, kann es zu einer verminderten Verfügbarkeit kommen, was den Zweck von Multi-AZ weitgehend zunichte macht.

Die einzige Möglichkeit, eine Domain ohne Standby auf dem zu konfigurieren, AWS Management Console besteht darin, die Erstellungsmethode Standard zu wählen und Domäne ohne Standby als Bereitstellungsoption auszuwählen.

Shard-Verteilung

Wenn Sie Multi-AZ ohne Standby aktivieren, sollten Sie mindestens ein Replikat für jeden Index in Ihrem Cluster erstellen. Ohne Replikate kann OpenSearch Service keine Kopien Ihrer Daten an andere Availability Zones verteilen. Die Standardkonfiguration für jeden Index ist eine Replikat-Anzahl von 1. Wie das folgende Diagramm zeigt, bemüht sich OpenSearch Service nach besten Kräften, primäre Shards und die entsprechenden Replikat-Shards auf verschiedene Zonen zu verteilen.

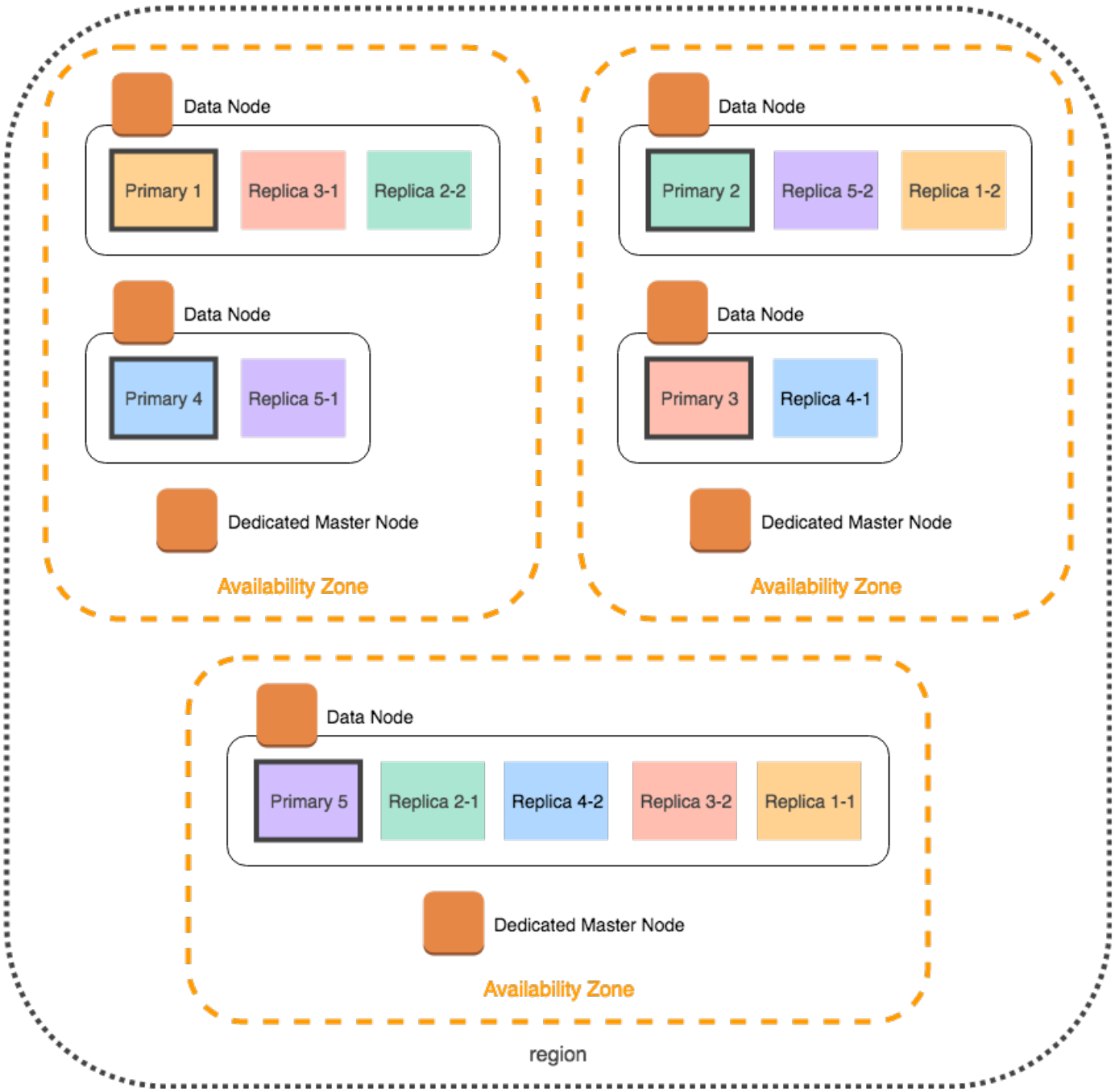


Der OpenSearch Service verteilt die Shards nicht nur nach Availability Zone, sondern auch nach Knoten. Dennoch können bestimmte Domain-Konfigurationen zu einer unausgewogenen Anzahl von Shards führen. Betrachten Sie sich die folgende Domain:

- 5 Datenknoten
- 5 Primär-Shards

- 2 Replikate
- 3 Availability Zones

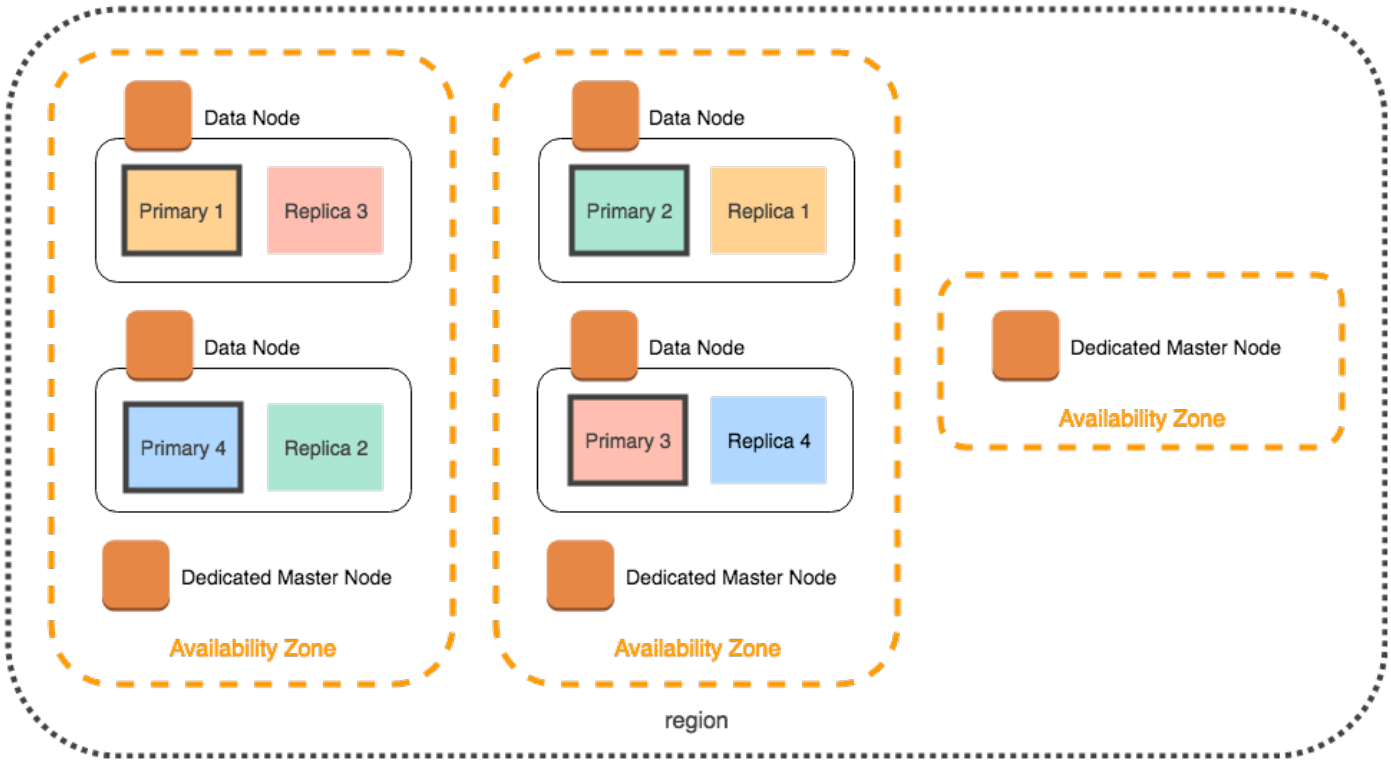
In dieser Situation muss OpenSearch Service einen Knoten überlasten, um die primären Shards und die Replikat-Shards auf die Zonen zu verteilen, wie in der folgenden Abbildung dargestellt.



Um solche Situationen zu vermeiden, die einzelne Knoten belasten und die Leistung beeinträchtigen können, empfehlen wir, Multi-AZ mit Standby zu wählen oder eine Instanzzahl zu wählen, die ein Vielfaches von drei ist, wenn Sie zwei oder mehr Replikate pro Index haben möchten.

Verteilung dedizierter Hauptknoten

Selbst wenn Sie bei der Konfiguration Ihrer Domain zwei Availability Zones auswählen, verteilt OpenSearch Service die dedizierten Master-Knoten automatisch auf drei Availability Zones. Diese Verteilung wirkt Cluster-Ausfallzeiten entgegen, falls in einer Zone eine Service-Unterbrechung auftritt. Wenn Sie die empfohlenen drei dedizierten Master-Knoten verwenden und eine Availability Zone ausfällt, verfügt Ihr Cluster weiterhin über ein Quorum (2) dedizierter Master-Knoten und kann einen neuen Master auswählen. Diese Konfiguration wird in der folgenden Abbildung veranschaulicht.



Wenn Sie den Instance-Typ einer älteren Generation auswählen, der nicht in drei Availability Zones verfügbar ist, treffen die folgenden Szenarien zu:

- Wenn Sie drei Availability Zones für die Domain ausgewählt haben, gibt OpenSearch Service einen Fehler aus. Wählen Sie einen anderen Instance-Typ aus und versuchen Sie es erneut.
- Wenn Sie zwei Availability Zones für die Domain ausgewählt haben, verteilt OpenSearch Service die dedizierten Master-Knoten auf zwei Zonen.

Unterbrechungen bei Availability Zones

Unterbrechungen bei Availability Zones sind selten, können aber auftreten. In der folgenden Tabelle sind die verschiedenen Multi-AZ-Konfigurationen und Verhaltensweisen während einer Unterbrechung aufgeführt. Die letzte Zeile in der Tabelle bezieht sich auf Multi-AZ mit Standby, während alle anderen Zeilen Konfigurationen haben, die nur für Multi-AZ ohne Standby gelten.

Anzahl der Availability Zones in einer Region	Anzahl der von Ihnen ausgewählten Availability Zones	Anzahl der dedizierten Hauptknoten	Verhalten bei einer Unterbrechung bei einer Availability Zone
2 oder mehr	2	0	Ausfallzeit. Ihr Cluster verliert die Hälfte seiner Datenknoten und muss mindestens einen in der verbleibenden Availability Zone ersetzen, bevor er einen Master auswählen kann.
2	2	3	50/50-Wahrscheinlichkeit von Ausfallzeiten. OpenSearch Der Service verteilt zwei dedizierte Master-Knoten in eine Availability Zone und einen in die andere: • Wenn bei der Availability Zone mit einem dedizierten Master-Knoten eine Unterbrechung auftritt, können die zwei dedizierten Master-Knoten in der verbleibenden Availability Zone einen Master auswählen. • Wenn die Availability Zone mit zwei dedizierten Hauptknoten unterbrochen wird, ist der Cluster nicht verfügbar, bis die verbleibende Availability Zone wiederhergestellt ist.
3 oder mehr	2	3	Keine Ausfallzeiten. OpenSearch Der Service verteilt die dedizierten Masterknoten automatisch auf drei Availability Zones, sodass die

Anzahl der Availability Zones in einer Region	Anzahl der von Ihnen ausgewählten Availability Zones	Anzahl der dedizierten Hauptknoten	Verhalten bei einer Unterbrechung bei einer Availability Zone
			verbleibenden zwei dedizierten Masterknoten einen Master auswählen können.
3 oder mehr	3	0	Keine Ausfallzeit Etwa zwei Drittel Ihrer Datenknoten sind weiterhin zur Wahl eines Masters verfügbar.
3 oder mehr	3	3	Keine Ausfallzeit Die verbleibenden zwei dedizierten Master-Knoten können einen Master auswählen.

In allen Konfigurationen, unabhängig von der Ursache, können Knotenausfälle dazu führen, dass die verbleibenden Datenknoten des Clusters einer Phase erhöhter Belastung ausgesetzt sind, während der OpenSearch Service automatisch neue Knoten konfiguriert, um die jetzt fehlenden zu ersetzen.

Beispiel: Tritt bei einer Availability Zone in einer Konfiguration mit drei Zonen ein Unterbrechung auf, müssen zwei Drittel der Datenknoten genauso so viele Anforderungen an den Cluster wie zuvor verarbeiten. Während sie diese Anforderungen verarbeiten, replizieren die verbleibenden Knoten außerdem Shards auf neuen Knoten, während diese online gehen. Die Leistung kann dadurch noch weiter beeinträchtigt werden. Wenn Verfügbarkeit für Ihre Workload unerlässlich ist, erwägen Sie, dieses Problem durch Hinzufügen von Ressourcen zu Ihrem Cluster zu mildern.

> **Note**
>
> OpenSearch Der Service verwaltet Multi-AZ-Domänen transparent, sodass Sie Störungen in der Availability Zone nicht manuell simulieren können.

Starten Ihrer Amazon- OpenSearch Service-Domains innerhalb einer VPC

Sie können - AWS Ressourcen wie Amazon- OpenSearch Service-Domains in einer Virtual Private Cloud (VPC) starten. Eine VPC ist ein virtuelles Netzwerk, das speziell für Ihr bestimmt ist AWS-Konto. Sie ist logisch von den anderen virtuellen Netzwerken in der AWS Cloud getrennt. Das Platzieren einer - OpenSearch Service-Domain in einer VPC ermöglicht eine sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher innerhalb der - AWS Cloud.

> **Note**
>
> Wenn Sie Ihre OpenSearch Service-Domain in einer VPC platzieren, muss Ihr Computer eine Verbindung mit der VPC herstellen können. Diese Verbindung besteht oft in Form eines VPN, eines Transit Gateways, eines verwalteten Netzwerks oder eines Proxy-Servers. Sie können nicht direkt von außerhalb der VPC auf Ihre Domänen zugreifen.

Themen

VPC im Vergleich zu öffentlichen Domänen

Im Folgenden sind einige der Möglichkeiten aufgeführt, wie sich VPC-Domänen von öffentlichen Domänen unterscheiden. Jeder Unterschied wird weiter unten detailliert beschrieben.

- Domänen, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domänen, die öffentliche Endpunkte nutzen, über eine zusätzliche Sicherheitsebene.
- Während auf öffentliche Domänen von jedem mit dem Internet verbundenen Gerät aus zugegriffen werden kann, benötigen VPC-Domänen eine Form von VPN oder Proxy.
- Im Vergleich zu öffentlichen Domänen werden für VPC-Domänen in der -Konsole weniger Informationen angezeigt. Insbesondere werden auf der Registerkarte Clusterzustand keine Shard-Informationen aufgeführt. Zudem fehlt die Registerkarte Indizes ganz.

- Die Domänenendpunkte haben unterschiedliche Formen (`https://search-domain-name` im Vergleich mit `https://vpc-domain-name`).
- Sie können keine IP-basierten Zugriffsrichtlinien auf Domänen anwenden, die sich in einer VPC befinden, da Sicherheitsgruppen bereits IP-basierte Zugriffsrichtlinien erzwingen.

Einschränkungen

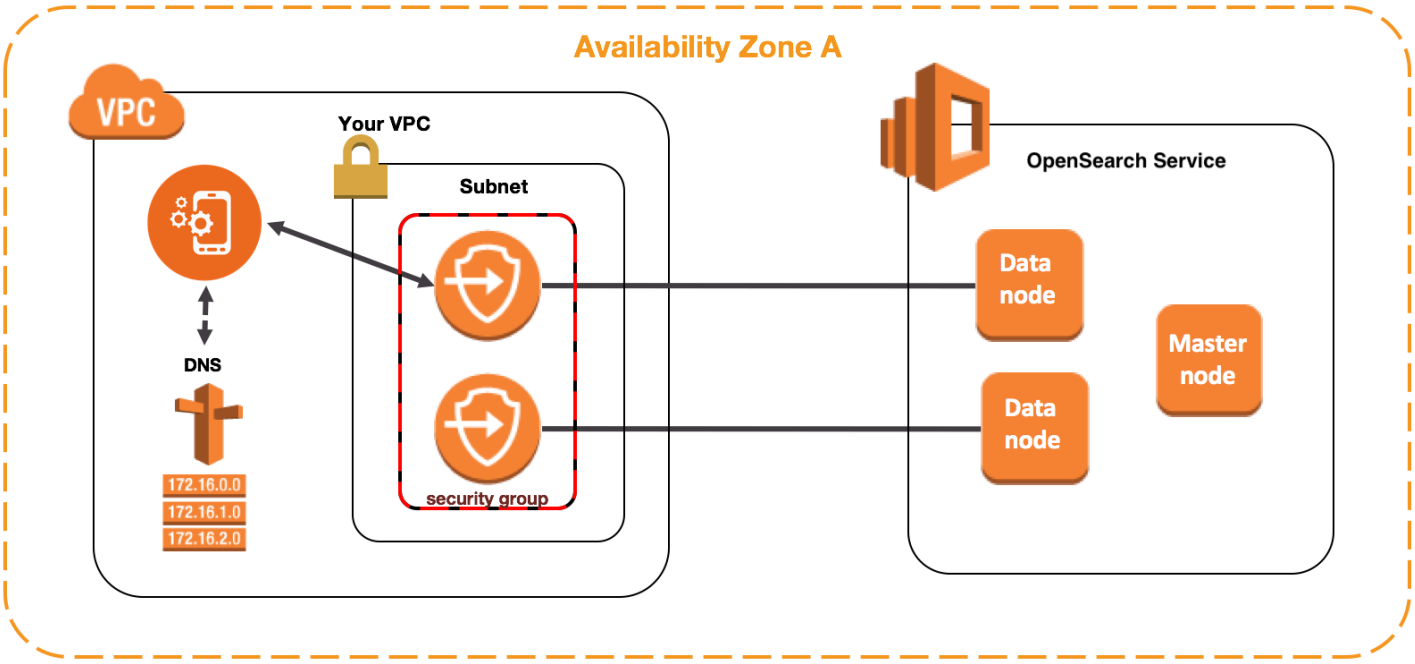
Für den Betrieb einer - OpenSearch Service-Domain innerhalb einer VPC gelten die folgenden Einschränkungen:

- Wenn Sie eine neue Domäne in einer VPC verwenden, können Sie später nicht zu einem öffentlichen Endpunkt wechseln. Dasselbe gilt auch umgekehrt: Wenn Sie eine Domäne mit einem öffentlichen Endpunkt erstellen, können Sie diese später nicht in eine VPC aufnehmen. Sie müssen stattdessen eine neue Domäne erstellen und die Daten übernehmen.
- Sie können entweder die Domäne in eine VPC aufnehmen oder einen öffentlichen Endpunkt verwenden, beides zugleich ist aber nicht möglich. Sie müssen eine der beiden Möglichkeiten beim Erstellen der Domäne auswählen.
- Sie können Ihre Domäne nicht in einer VPC starten, die Dedicated Tenancy verwendet. Sie müssen eine VPC verwenden, deren Tenancy auf Standard gesetzt ist.
- Nachdem Sie eine Domäne in eine VPC aufgenommen haben, kann sie nicht in eine andere VPC verlagert werden, aber Sie können die Subnetze und Sicherheitsgruppeneinstellungen ändern.
- Um auf die Standardinstallation von OpenSearch Dashboards für eine Domain zuzugreifen, die sich in einer VPC befindet, müssen Benutzer Zugriff auf die VPC haben. Der Zugriff auf eine VPC unterscheidet sich je nach Netzwerkkonfiguration, aber wahrscheinlich muss dazu eine Verbindung mit einem VPN bzw. verwalteten Netzwerk hergestellt oder ein Proxyserver oder Transit Gateway verwendet werden. Weitere Informationen finden Sie unter the section called “Zugriffsrichtlinien für VPC-Domänen”, im Amazon VPC User Guide und unter the section called “Steuern des Zugriffs auf Dashboards OpenSearch ”.

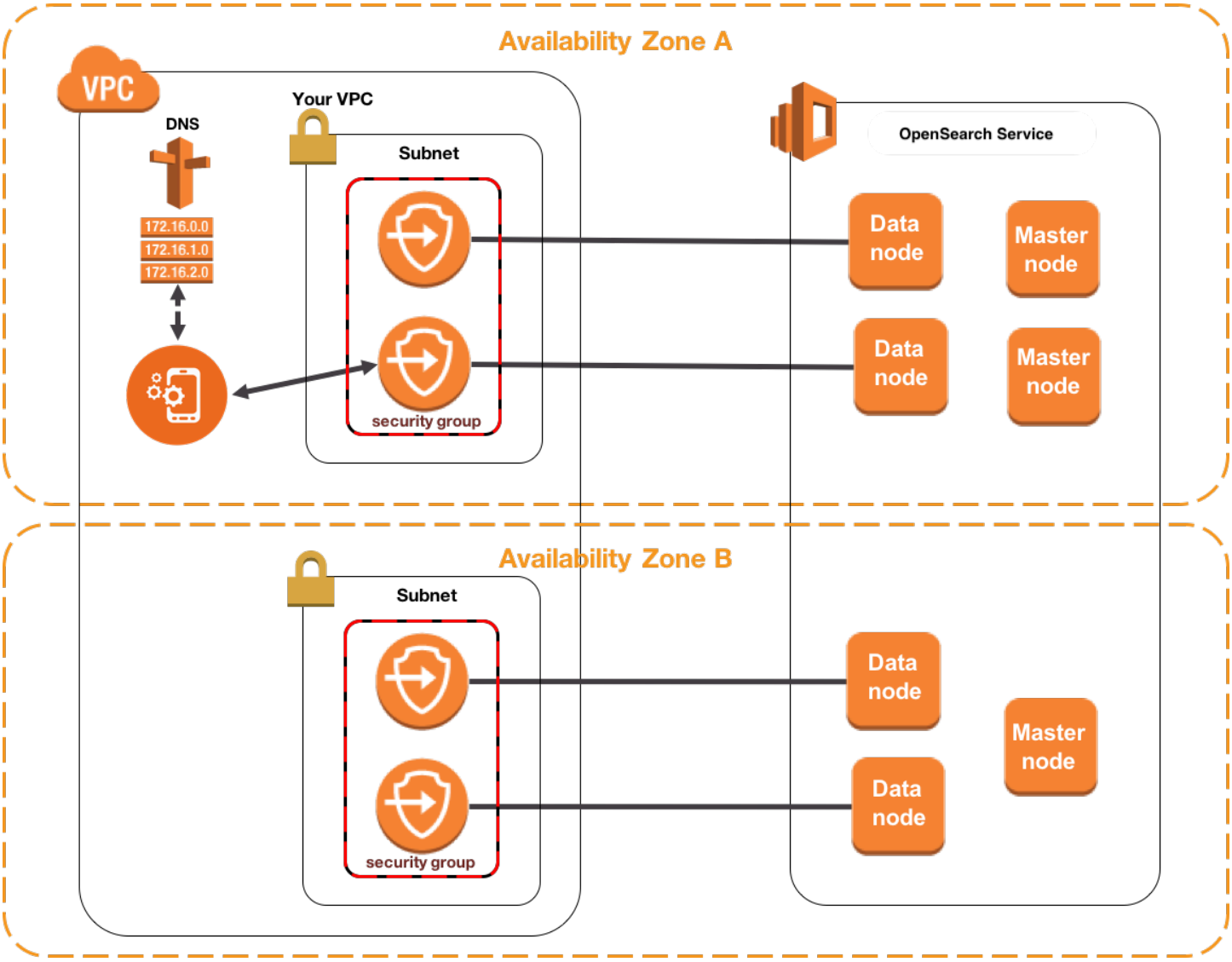
Architektur

Zur Unterstützung von VPCs platziert OpenSearch Service einen Endpunkt in einem, zwei oder drei Subnetzen Ihrer VPC. Wenn Sie mehrere Availability Zones für Ihre Domäne aktivieren, muss sich jedes Subnetz in einer anderen Availability Zone in derselben Region befinden. Wenn Sie nur eine Availability Zone verwenden, platziert OpenSearch Service einen Endpunkt nur in einem Subnetz.

Die folgende Abbildung zeigt die VPC-Architektur für eine Availability Zone:



Die folgende Abbildung zeigt die VPC-Architektur für zwei Availability Zones:



OpenSearch Der Service platziert auch eine Elastic-Network-Schnittstelle (ENI) in der VPC für jeden Ihrer Datenknoten. OpenSearch Der Service weist jeder ENI eine private IP-Adresse aus dem IPv4-Adressbereich Ihres Subnetzes zu. Der Service weist den IP-Adressen außerdem einen öffentlichen DNS-Hostnamen (Domänenendpunkt) zu. Sie müssen einen öffentlichen DNS-Service zum Auflösen des Endpunkts (DNS-Hostname) in die IP-Adressen der Datenknoten verwenden:

- Wenn Ihre VPC den von Amazon bereitgestellten DNS-Server verwendet, indem die `enableDnsSupport` Option auf `true` (Standardwert) gesetzt wird, ist die Auflösung für den OpenSearch Service-Endpunkt erfolgreich.
- Wenn Ihre VPC einen privaten DNS-Server verwendet und der Server die öffentlichen autoritativen DNS-Server erreichen kann, um DNS-Hostnamen aufzulösen, ist die Auflösung für den OpenSearch Service-Endpunkt ebenfalls erfolgreich.

Da sich die IP-Adressen ändern können, sollten Sie den Domänenendpunkt regelmäßig auflösen, damit stets der Zugriff auf die richtigen Datenknoten gewährleistet ist. Wir empfehlen, das DNS-Auflösungsintervall auf eine Minute einzustellen. Wenn Sie einen Client verwenden, sollten Sie zudem sicherstellen, dass dessen DNS-Cache gelöscht wird.

Migrieren vom öffentlichen Zugriff zum VPC-Zugriff

Beim Erstellen einer Domäne legen Sie fest, ob für den Zugriff ein öffentlicher Endpunkt oder eine VPC verwendet wird. Nach der Erstellung können Sie nicht mehr zwischen den beiden Möglichkeiten wechseln. Sie müssen stattdessen eine neue Domäne erstellen und dann entweder eine manuelle Neuindizierung oder Datenmigration durchführen. Snapshots bieten eine bequeme Möglichkeit für das Migrieren von Daten. Informationen zum Erstellen und Wiederherstellen von Snapshots finden Sie unter the section called “Erstellen von Index-Snapshots”.

Zugriffsrichtlinien für VPC-Domänen

Das Platzieren Ihrer OpenSearch Service-Domain in einer VPC bietet eine inhärente, starke Sicherheitsebene. Wenn Sie eine Domäne mit öffentlichem Zugriff erstellen, hat der Endpunkt das folgende Format:

```
https://search-domain-name-identifier.region.es.amazonaws.com
```

Wie aus der Bezeichnung "öffentlich" zu schließen ist, kann auf diesen Endpunkt von jedem mit dem Internet verbundenen Gerät zugegriffen werden. Sie können jedoch (und sollten) den Zugriff darauf kontrollieren. Wenn Sie in einem Webbrowser auf den Endpunkt zugreifen, erhalten Sie unter Umständen die Nachricht `Not Authorized`. Die Anforderung erreicht jedoch die Domäne.

Wenn Sie eine Domäne mit VPC-Zugriff erstellen, gleicht der Endpunkt einem öffentlichen Endpunkt:

```
https://vpc-domain-name-identifier.region.es.amazonaws.com
```

Wenn Sie versuchen, auf den Endpunkt in einem Webbrowser zuzugreifen, tritt möglicherweise jedoch eine Zeitüberschreitung der Anforderung auf. Selbst zum Ausführen grundlegender `GET`-Anforderungen muss Ihr Computer eine Verbindung mit dem VPC herstellen können. Diese Verbindung besteht oft in Form eines VPN, eines Transit Gateways, eines verwalteten Netzwerks oder eines Proxy-Servers. Details zu den verschiedenen möglichen Verbindungsformen finden Sie unter Beispiele für VPC im Amazon-VPC-Benutzerhandbuch. Ein auf die Entwicklung ausgerichtetes Beispiel finden Sie unter the section called “Testen von VPC-Domänen”.

Zusätzlich zu dieser Verbindungsanforderung lassen VPCs Sie den Zugriff auf die Domäne über Sicherheitsgruppen verwalten. Diese Kombination von Sicherheitsfunktionen reicht für viele Anwendungsfälle aus, und die Verwendung einer offenen Zugriffsrichtlinie für die Domäne mag ausreichend erscheinen.

Das Arbeiten mit einer offenen Zugriffsrichtlinie bedeutet nicht, dass jeder im Internet auf die OpenSearch Service-Domain zugreifen kann. Vielmehr bedeutet dies, dass die Domain die Anforderung akzeptiert, wenn eine Anforderung die OpenSearch Service-Domain erreicht und die zugehörigen Sicherheitsgruppen dies zulassen. Die einzige Ausnahme gibt es bei der Verwendung einer differenzierten Zugriffskontrolle oder einer Zugriffsrichtlinie, die IAM-Rollen angibt. Damit die Domäne eine Anforderung in diesen Situationen annehmen kann, müssen die Sicherheitsgruppen dies zulassen und sie muss mit gültigen Anmeldeinformationen signiert sein.

> **Note**
>
> Da Sicherheitsgruppen bereits IP-basierte Zugriffsrichtlinien durchsetzen, können Sie IP-basierte Zugriffsrichtlinien nicht auf OpenSearch Service-Domains anwenden, die sich in einer VPC befinden. Wenn Sie öffentlichen Zugriff verwenden, sind IP-basierte Richtlinien weiterhin verfügbar.

Bevor Sie beginnen: Voraussetzungen für den VPC-Zugriff

Bevor Sie eine Verbindung zwischen einer VPC und Ihrer neuen OpenSearch Service-Domain aktivieren können, müssen Sie Folgendes tun:

- Erstellen einer VPC

  Um Ihre VPC zu erstellen, können Sie die Amazon-VPC-Konsole, die AWS -CLI oder eines der -AWS SDKs verwenden. Weitere Informationen finden Sie unter Arbeiten mit freigegebenen VPCs im Amazon-VPC-Benutzerhandbuch. Wenn bereits eine VPC vorhanden ist, können Sie diesen Schritt überspringen.
- Reservieren von IP-Adressen

  OpenSearch Der Service ermöglicht die Verbindung einer VPC mit einer Domain, indem Netzwerkschnittstellen in einem Subnetz der VPC platziert werden. Jeder Netzwerkschnittstelle ist eine IP-Adresse zugewiesen. Sie müssen im Subnetz eine ausreichende Anzahl von IP-Adressen für die Netzwerkschnittstellen reservieren. Weitere Informationen finden Sie unter Reservieren von IP-Adressen in einem VPC-Subnetz.

Testen von VPC-Domänen

Die erweiterte Sicherheit einer VPC kann die Herstellung einer Verbindung zu Ihrer Domäne und die Durchführung von Tests zu einer Herausforderung machen. Wenn Sie bereits über eine - OpenSearch Service-VPC-Domain verfügen und lieber keinen VPN-Server erstellen möchten, versuchen Sie den folgenden Vorgang:

1. Wählen Sie für die Zugriffsrichtlinie Ihrer Domäne die Option Nur differenzierte Zugriffssteuerung verwenden aus. Sie können diese Einstellung jederzeit aktualisieren, nachdem Sie den Test abgeschlossen haben.
2. Erstellen Sie eine Amazon Linux Amazon EC2-Instance in derselben VPC, demselben Subnetz und derselben Sicherheitsgruppe wie Ihre OpenSearch Service-Domain.

   Da diese Instance für Testzwecke vorgesehen ist und nur sehr wenig Arbeit leisten muss, wählen Sie einen kostengünstigen Instance-Typ, beispielsweise `t2.micro`. Weisen Sie der Instance eine öffentliche IP-Adresse zu und erstellen Sie entweder ein neues Schlüsselpaar oder wählen Sie ein vorhandenes aus. Wenn Sie einen neuen Schlüssel erstellen, laden Sie sie in Ihr `~/.ssh`-Verzeichnis herunter.

   Weitere Informationen zum Erstellen von Instances finden Sie unter Erste Schritte mit Amazon EC2 Linux Instances.
3. Fügen Sie Ihrer VPC ein Internet-Gateway hinzu.
4. Fügen Sie in der Routing-Tabelle für Ihre VPC eine neue Route hinzu. Geben Sie für Destination (Ziel) einen CIDR-Block an, der die öffentliche IP-Adresse Ihres Computers enthält. Geben Sie für Target (Ziel) das Internet-Gateway an, das Sie gerade erstellt haben.

   Sie können beispielsweise `123.123.123.123/32` nur für Ihren Computer oder `123.123.123.0/24` für mehrere Computer angeben.
5. Für die Sicherheitsgruppe geben Sie zwei Regeln für eingehenden Datenverkehr an:

Typ	Protocol (Protokoll)	Port-Bereich	Quelle
SSH (22)	TCP (6)	22	*your-cidr-block*
HTTPS (443)	TCP (6)	443	*your-security-group-id*

Die erste Regel ermögicht Ihnen, SSH in Ihre EC2-Instance zu integrieren. Die zweite ermöglicht es der EC2-Instance, über HTTPS mit der OpenSearch Service-Domain zu kommunizieren.

6. Führen Sie vom Terminal folgenden Befehl aus:

```
ssh -i ~/.ssh/your-key.pem ec2-user@your-ec2-instance-public-ip -N -L
 9200:vpc-domain-name.region.es.amazonaws.com:443
```

   Dieser Befehl erstellt einen SSH-Tunnel, der Anfragen über die EC2-Instance an https://localhost:9200 an Ihre OpenSearch Service-Domain weiterleitet. Die Angabe von Port 9200 im Befehl simuliert eine lokale OpenSearch Installation, verwendet jedoch den gewünschten Port. OpenSearch Der Service akzeptiert nur Verbindungen über Port 80 (HTTP) oder 443 (HTTPS).

   Der Befehl stellt kein Feedback bereit und wird unbegrenzt ausgeführt. Um ihn anzuhalten, drücken Sie `Ctrl + C`.

7. Navigieren Sie zu https://localhost:9200/_dashboards/ in Ihrem Webbrowser. Möglicherweise müssen Sie eine Sicherheitsausnahme bestätigen.

   Alternativ können Sie Anfragen an https://localhost:9200 unter Verwendung von curl, Postman oder Ihrer bevorzugten Programmiersprache senden.

> **Tip**
>
> Wenn curl-Fehler auftreten, weil ein Zertifikat nicht übereinstimmt, versuchen Sie das `--insecure`-Flag.

Reservieren von IP-Adressen in einem VPC-Subnetz

OpenSearch Der Service verbindet eine Domain mit einer VPC, indem Netzwerkschnittstellen in einem Subnetz der VPC platziert werden (oder mehrere Subnetze der VPC, wenn Sie mehrere Availability Zones aktivieren). Jeder Netzwerkschnittstelle ist eine IP-Adresse zugewiesen. Bevor Sie Ihre OpenSearch Service-Domain erstellen, müssen Sie über eine ausreichende Anzahl von IP-Adressen in jedem Subnetz verfügen, um die Netzwerkschnittstellen unterzubringen.

Die Grundformel lautet: Die Anzahl der IP-Adressen, die OpenSearch Service in jedem Subnetz reserviert, ist das Dreifache der Anzahl der Datenknoten geteilt durch die Anzahl der Availability Zones.

Beispiele

- Wenn eine Domäne über neun Datenknoten in drei Availability Zones verfügt, beträgt die IP-Anzahl pro Subnetz 9 * 3 / 3 = 9.
- Wenn eine Domäne über acht Datenknoten in zwei Availability Zones verfügt, beträgt die IP-Anzahl pro Subnetz 8 * 3 / 2 = 12.
- Wenn eine Domäne sechs Datenknoten in einer Availability Zone hat, beträgt die IP-Anzahl pro Subnetz 6 * 3 / 1 = 18.

Wenn Sie die Domain erstellen, reserviert OpenSearch Service die IP-Adressen, verwendet einige für die Domain und reserviert den Rest für Blau/Grün-Bereitstellungen. Die Netzwerkschnittstellen und deren IP-Adressen werden im Bereich Netzwerkschnittstellen der Amazon-EC2-Konsole angezeigt. Die Spalte Beschreibung zeigt, welcher OpenSearch Service-Domain die Netzwerkschnittstelle zugeordnet ist.

> **Tip**
>
> Wir empfehlen Ihnen, dedizierte Subnetze für die reservierten OpenSearch Service-IP-Adressen zu erstellen. Dadurch werden Überschneidungen mit anderen Anwendungen und Services vermieden und es ist gewährleistet, dass bei einer künftigen Skalierung des Clusters zusätzliche IP-Adressen reserviert werden können. Weitere Informationen erhalten Sie unter Erstellen eines Subnetzes in Ihrer VPC.

Service-verknüpfte Rolle für den VPC-Zugriff

Eine serviceverknüpfte Rolle ist eine einzigartige Art von IAM-Rolle, die Berechtigungen an einen Service delegiert, damit er -Ressourcen in Ihrem Namen erstellen und verwalten kann. OpenSearch Der Service benötigt eine serviceverknüpfte Rolle, um auf Ihre VPC zuzugreifen, den Domänenendpunkt zu erstellen und Netzwerkschnittstellen in einem Subnetz Ihrer VPC zu platzieren.

OpenSearch Der Service erstellt die Rolle automatisch, wenn Sie die OpenSearch Servicekonsole verwenden, um eine Domain innerhalb einer VPC zu erstellen. Damit diese automatische Erstellung möglich ist, müssen Sie über Berechtigungen für die Aktion `iam:CreateServiceLinkedRole` verfügen. Weitere Informationen finden Sie unter Berechtigungen von Service-verknüpften Rollen im IAM-Benutzerhandbuch.

Nachdem OpenSearch Service die Rolle erstellt hat, können Sie sie (`AWSServiceRoleForAmazonOpenSearchService`) mithilfe der IAM-Konsole anzeigen.

Ausführliche Informationen zu den Berechtigungen dieser Rolle, und wie Sie sie löschen, finden Sie unter the section called “Verwenden von serviceverknüpften Rollen”.

Index-Snapshots in Amazon OpenSearch Service erstellen

Snapshots in Amazon OpenSearch Service sind Backups der Indizes und des Status eines Clusters. Der Status beinhaltet Cluster-Einstellungen, Knoteninformationen, Index-Einstellungen und die Shard-Zuweisung.

OpenSearch Service-Snapshots gibt es in den folgenden Formen:

- Automatisierte Snapshots dienen nur zur Cluster-Wiederherstellung. Sie können sie verwenden, um Ihre Domain im Falle eines roten Cluster-Status oder Datenverlusts wiederherzustellen. Weitere Informationen finden Sie weiter unten unter Snapshots wiederherstellen. OpenSearch Der Service speichert automatisierte Snapshots ohne zusätzliche Kosten in einem vorkonfigurierten Amazon S3 S3-Bucket.
- Manuelle Snapshots dienen zur Cluster-Wiederherstellung oder zum Verschieben von Daten von einem Cluster zu einem anderen. Sie müssen manuelle Snapshots initiieren. Diese Snapshots werden in Ihrem eigenen Amazon-S3-Bucket gespeichert und es fallen die S3-Standardgebühren an. Wenn Sie über einen Snapshot aus einem selbstverwalteten OpenSearch Cluster verfügen, können Sie diesen Snapshot verwenden, um zu einer OpenSearch Service-Domain zu migrieren. Weitere Informationen finden Sie unter Migration zu Amazon OpenSearch Service.

Alle OpenSearch Service-Domains erstellen automatische Snapshots, aber die Häufigkeit unterscheidet sich in folgenden Punkten:

- Für Domains, die OpenSearch oder Elasticsearch 5.3 und höher laufen, OpenSearch erstellt Service stündlich automatisierte Snapshots und speichert bis zu 336 davon 14 Tage lang. Stündliche Snapshots sind aufgrund ihrer inkrementellen Natur weniger störend. Sie bieten auch einen neueren Wiederherstellungspunkt für den Fall von Problemen mit Domains.
- Bei Domains, auf denen Elasticsearch 5.1 und früher ausgeführt wird, erstellt OpenSearch Service täglich automatische Snapshots zu der von Ihnen angegebenen Stunde, speichert bis zu 14 davon und speichert keine Snapshot-Daten länger als 30 Tage.

Wenn Ihr Cluster in den roten Status wechselt, schlagen alle automatisierten Snapshots fehl, während der Cluster-Status bestehen bleibt. Wenn Sie das Problem nicht innerhalb von zwei Wochen beheben, können die Daten in Ihrem Cluster dauerhaft verloren gehen. Fehlerbehandlungsschritte finden Sie unter the section called “Roter Cluster-Status”.

Themen

Voraussetzungen

Um Snapshots manuell zu erstellen, müssen Sie mit IAM und Amazon S3 arbeiten. Stellen Sie sicher, dass Sie die folgenden Voraussetzungen erfüllen, bevor Sie versuchen, einen Snapshot zu erstellen:

Voraussetzung	Beschreibung
S3-Bucket	Erstellen Sie einen S3-Bucket, um manuelle Snapshots für Ihre OpenSearch Service-Domain zu speichern. Weitere Anleitungen finden Sie unter Erstellen eines Buckets im Benutzerhandbuch für Amazon Simple Storage Service. Merken Sie sich den Namen des Buckets, um ihn an den folgenden Stellen zu verwenden: • Die `Resource`-Anweisung der IAM-Richtlinie, die Ihrer IAM-Rolle beigefügt ist • Der Python-Client, der zum Registrieren eines Snapshot-Repositorys verwendet wurde (wenn Sie diese Methode verwenden)

Voraussetzung	Beschreibung
	Important Wenden Sie keine S3 Glacier-Lebenszyklusregel auf diesen Bucket an. Manuelle Snapshots bieten keine Unterstützung für die Speicherklasse S3 Glacier.

Voraussetzung	Beschreibung
IAM-Rolle	Erstellen Sie eine IAM-Rolle, um Berechtigungen an den Service zu delegieren. OpenSearch Detaillierte Anleitungen finden Sie unter Erstellen einer IAM-Rolle (Konsole) im IAM-Benutzerhandbuch. Das restliche Kapitel bezieht sich auf diese Rolle als `TheSnapshotRole` . Anfügen einer IAM-Richtlinie Hängen Sie die folgende Richtlinie an `TheSnapshotRole` an, um den Zugriff auf den S3-Bucket zuzulassen: `{ "Version": "2012-10-17", "Statement": [{ "Action": [ "s3:ListBucket" ], "Effect": "Allow", "Resource": [ "arn:aws:s3::: s3-bucket-name " ] }, { "Action": [ "s3:GetObject", "s3:PutObject", "s3:DeleteObject" ], "Effect": "Allow", "Resource": [ "arn:aws:s3::: s3-bucket-name /*" ] } ] }` Anweisungen zum Anfügen einer Richtlinie an eine Rolle finden Sie unter Hinzufügen von IAM-Identitätsberechtigungen im IAM-Benutzerhandbuch.

Voraussetzung	Beschreibung

	Bearbeiten der Vertrauensstellung
	
	Bearbeiten Sie die Vertrauensstellung von`TheSnapshotRole` , um OpenSearch Service in der `Principal` Anweisung anzugeben, wie im folgenden Beispiel gezeigt:
	
	`{`
	`  "Version": "2012-10-17",`
	`  "Statement": [{`
	`  "Sid": "",`
	`  "Effect": "Allow",`
	`  "Principal": {`
	`  "Service": "es.amazonaws.com"`
	`  },`
	`  "Action": "sts:AssumeRole"`
	`  }]`
	
	`}`
	
	Anweisungen zum Bearbeiten der Vertrauensstellung finden Sie unter Ändern einer Rollenvertrauensrichtlinie im IAM-Benutzerhandbuch.

Voraussetzung	Beschreibung

Berechtigungen	Um das Snapshot-Repository zu registrieren, müssen Sie in der Lage sein, es an OpenSearch Service `TheSnapshotRole` weiterzuleiten. Sie benötigen außerdem Zugriff auf die Aktion `es:ESHttpPut` . Um diese beiden Berechtigungen zu erteilen, fügen Sie die folgende Richtlinie an die IAM-Rolle an, deren Anmeldeinformationen zum Signieren der Anforderung verwendet werden:
	
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": "iam:PassRole", "Resource": "arn:aws:iam:: 123456789012 :role/TheSnapshotRole " }, { "Effect": "Allow", "Action": "es:ESHttpPut", "Resource": "arn:aws:es: region:123456789012 :domain/domain-name /*" } ] }`
	
	Wenn Ihr Benutzer oder Ihre Rolle nicht über die `iam:PassRole` erforderlichen Berechtigungen verfügt`TheSnapshotRole` , tritt möglicherweise der folgende Fehler auf, wenn Sie im nächsten Schritt versuchen, ein Repository zu registrieren:
	
	`$ python register-repo.py {"Message":"User: arn:aws:iam:: 123456789012 :user/MyUserAccount is not authorized to perform: iam:PassRole on resource: arn:aws:iam:: 123456789012 :role/TheSnapshotRole "}`

Registrieren eines manuellen Snapshot-Repositorys

Sie müssen ein Snapshot-Repository bei OpenSearch Service registrieren, bevor Sie manuelle Index-Snapshots erstellen können. Für diesen einmaligen Vorgang müssen Sie Ihre AWS Anfrage

mit Zugangsdaten signieren, die für den Zugriff berechtigt sind`TheSnapshotRole`, wie unter beschriebenthe section called “Voraussetzungen”.

Schritt 1: Ordnen Sie die Snapshot-Rolle in OpenSearch Dashboards zu (wenn Sie eine differenzierte Zugriffskontrolle verwenden)

Eine differenzierte Zugriffskontrolle führt einen zusätzlichen Schritt bei der Registrierung eines Repositorys ein. Auch wenn Sie die HTTP-Basisauthentifizierung für alle anderen Zwecke verwenden, müssen Sie die `manage_snapshots`-Rolle Ihrer IAM-Rolle mit `iam:PassRole`-Berechtigungen zuordnen, um `TheSnapshotRole` zu übergeben.

1. Navigieren Sie zum OpenSearch Dashboards-Plugin für Ihre Service-Domain. OpenSearch Sie finden den Dashboards-Endpunkt in Ihrem Domain-Dashboard in der OpenSearch Service-Konsole.
2. Wählen Sie im Hauptmenü Sicherheit, Rollen, und wählen Sie die Rolle manage_snapshots.
3. Wählen Sie Zugeordnete Benutzer, Mapping verwalten.
4. Fügen Sie den ARN der Rolle hinzu, die über Berechtigungen zum Weitergeben von `TheSnapshotRole` verfügt. Platzieren Sie Rollen-ARNs unter Backend roles (Backend-Rollen).

   ```
   arn:aws:iam::123456789123:role/role-name
   ```

5. Wählen Sie Zuordnen und bestätigen Sie, dass der Benutzer oder die Rolle unter Zugeordnete Benutzer angezeigt wird.

Schritt 2: Registrieren eines Repositorys

Auf der folgenden Registerkarte „Snapshots“ wird veranschaulicht, wie Sie ein Snapshot-Verzeichnis registrieren. Spezifische Optionen für die Verschlüsselung eines manuellen Snapshots und die Registrierung eines Snapshots nach der Migration zu einer neuen Domain finden Sie auf den entsprechenden Registerkarten.

Snapshots

Um ein Snapshot-Repository zu registrieren, senden Sie eine PUT-Anfrage an den Endpunkt der OpenSearch Service-Domäne. Sie können curl, den Python-Beispielclient, Postman oder eine andere Methode verwenden, um eine signierte Anfrage zur Registrierung des Snapshot-Repositorys zu senden. Beachten Sie, dass Sie in der OpenSearch Dashboards-Konsole keine PUT-Anfrage verwenden können, um das Repository zu registrieren.

Die Anfrage hat das folgende Format:

```
PUT domain-endpoint/_snapshot/my-snapshot-repo-name
{
  "type": "s3",
  "settings": {
    "bucket": "s3-bucket-name",
    "base_path": "my/snapshot/directory",
    "region": "region",
    "role_arn": "arn:aws:iam::123456789012:role/TheSnapshotRole"
  }
}
```

> **Note**
>
> Repository-Namen dürfen nicht mit „cs-“ beginnen. Darüber hinaus sollten Sie nicht von mehreren Domains in dasselbe Repository schreiben. Nur eine Domain sollte Schreibzugriff auf das Repository haben.

Wenn sich Ihre Domain in einer Virtual Private Cloud (VPC) befindet, muss Ihr Computer mit der VPC verbunden sein, damit die Anforderung zur erfolgreichen Registrierung des Snapshot-Repositorys erfolgt. Der Zugriff auf eine VPC unterscheidet sich je nach Netzwerkkonfiguration, wahrscheinlich muss eine Verbindung mit einem VPN oder Unternehmensnetzwerk hergestellt werden. Um zu überprüfen, ob Sie die OpenSearch Service-Domain erreichen können, navigieren Sie `https://your-vpc-domain.region.es.amazonaws.com` in einem Webbrowser zu und überprüfen Sie, ob Sie die Standard-JSON-Antwort erhalten.

Wenn sich Ihr Amazon S3 S3-Bucket in einer anderen AWS-Region als Ihrer OpenSearch Domain befindet, fügen Sie den Parameter `"endpoint": "s3.amazonaws.com"` zur Anfrage hinzu.

Encrypted snapshots

Sie können derzeit keine AWS Key Management Service (KMS-) Schlüssel zum Verschlüsseln manueller Snapshots verwenden, aber Sie können sie mit serverseitiger Verschlüsselung (SSE) schützen.

Um SSE mit S3-verwalteten Schlüsseln für den Bucket zu aktivieren, den Sie als Snapshot-Repository verwenden, fügen Sie dem `"settings"` Block der `"server_side_encryption": true` PUT-Anforderung etwas hinzu. Weitere Informationen finden Sie unter Schützen von Daten

durch serverseitige Verschlüsselung mit Amazon S3-verwalteten Verschlüsselungsschlüsseln im Amazon Simple Storage Service-Benutzerhandbuch.

Alternativ können Sie AWS KMS Schlüssel für die serverseitige Verschlüsselung für den S3-Bucket verwenden, den Sie als Snapshot-Repository verwenden. Wenn Sie diesen Ansatz verwenden, stellen Sie sicher, dass Sie dem AWS KMS Schlüssel, der zur Verschlüsselung des S3-Buckets verwendet wird, die `TheSnapshotRole` Erlaubnis erteilen. Weitere Informationen finden Sie unter Schlüsselrichtlinien in AWS KMS.

Domain migration

Das Registrieren eines Snapshot-Repositorys ist ein einmaliger Vorgang. Um jedoch von einer Domain zu einer anderen zu migrieren, müssen Sie dasselbe Snapshot-Repository auf der alten und der neuen Domain registrieren. Der Repository-Name ist beliebig.

Berücksichtigen Sie die folgenden Richtlinien, wenn Sie zu einer neuen Domain migrieren oder dasselbe Repository bei mehreren Domains registrieren:

- Fügen Sie beim Registrieren des Repositorys in der neuen Domain `"readonly": true` zum `"settings"`-Block der PUT-Anforderung hinzu. Diese Einstellung verhindert, dass Sie versehentlich Daten aus der alten Domain überschreiben. Nur eine Domain sollte Schreibzugriff auf das Repository haben.
- Wenn Sie Daten zu einer Domain in einer anderen AWS-Region migrieren (z. B. von einer alten Domain und einem Bucket in us-east-2 zu einer neuen Domain in us-west-2), `"region": "region"` ersetzen Sie sie `"endpoint": "s3.amazonaws.com"` in der PUT-Anweisung durch und wiederholen Sie die Anfrage.

Verwenden des Python-Beispielclients

Der Python-Client ist einfacher zu automatisieren als eine einfache HTTP-Anfrage und bietet eine bessere Wiederverwendbarkeit. Wenn Sie diese Methode zum Registrieren eines Snapshot-Repositorys verwenden, speichern Sie den folgenden Python-Beispielcode als Python-Datei, z. B. `register-repo.py`. Der Client benötigt die Pakete AWS SDK for Python (Boto3), Anforderungen und requests-aws4auth. Der Client enthält auskommentierte Beispiele für andere Snapshot-Vorgänge.

Aktualisieren Sie die folgenden Variablen im Beispiel-Code: `host`, `region`, `path`, und`payload`.

```
import boto3
import requests
```

```
from requests_aws4auth import AWS4Auth

host = '' # domain endpoint
region = '' # e.g. us-west-1
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)

# Register repository

path = '/_snapshot/my-snapshot-repo-name' # the OpenSearch API endpoint
url = host + path

payload = {
  "type": "s3",
  "settings": {
    "bucket": "s3-bucket-name",
    "base_path": "my/snapshot/directory",
    "region": "us-west-1",
    "role_arn": "arn:aws:iam::123456789012:role/snapshot-role"
  }
}

headers = {"Content-Type": "application/json"}

r = requests.put(url, auth=awsauth, json=payload, headers=headers)

print(r.status_code)
print(r.text)

# # Take snapshot
#
# path = '/_snapshot/my-snapshot-repo-name/my-snapshot'
# url = host + path
#
# r = requests.put(url, auth=awsauth)
#
# print(r.text)
#
# # Delete index
#
# path = 'my-index'
# url = host + path
```

```
#
# r = requests.delete(url, auth=awsauth)
#
# print(r.text)
#
# # Restore snapshot (all indexes except Dashboards and fine-grained access control)
#
# path = '/_snapshot/my-snapshot-repo-name/my-snapshot/_restore'
# url = host + path
#
# payload = {
#   "indices": "-.kibana*,-.opendistro_security,-.opendistro-*",
#   "include_global_state": False
# }
#
# headers = {"Content-Type": "application/json"}
#
# r = requests.post(url, auth=awsauth, json=payload, headers=headers)
#
# print(r.text)
#
# # Restore snapshot (one index)
#
# path = '/_snapshot/my-snapshot-repo-name/my-snapshot/_restore'
# url = host + path
#
# payload = {"indices": "my-index"}
#
# headers = {"Content-Type": "application/json"}
#
# r = requests.post(url, auth=awsauth, json=payload, headers=headers)
#
# print(r.text)
```

Manuelle Snapshots erstellen

Snapshots erfolgen nicht augenblicklich. Sie sind zeitaufwändig und stellen keine perfekte Ansicht des Clusters dar. point-in-time Während ein Snapshot erstellt wird, können Sie weiterhin Dokumente indizieren und andere Anfragen an den Cluster stellen, aber neue Dokumente und Aktualisierungen bestehender Dokumente werden nicht im Allgemeinen in den Snapshot aufgenommen. Der Snapshot enthält primäre Shards, so wie sie bei der OpenSearch Initiierung des Snapshots vorhanden waren. Je nach der Größe Ihres Snapshot-Thread-Pools umfassen die Snapshots ggf. verschiedene Shards

zu geringfügig unterschiedlichen Zeitpunkten. Bewährte Methoden für Snapshots finden Sie unterthe section called “Verbessern Sie die Snapshot-”.

Snapshot-Speicher und -Leistung

OpenSearch Snapshots sind inkrementell, d. h. sie speichern nur Daten, die sich seit dem letzten erfolgreichen Snapshot geändert haben. Diese inkrementelle Beschaffenheit bedeutet, dass der Unterschied in der Festplattennutzung zwischen häufigen und seltenen Snapshots oft minimal ist. Mit anderen Worten, die Erstellung stündlicher Snapshots für eine Woche (mit insgesamt 168 Snapshots) verbraucht möglicherweise nicht viel mehr Speicherplatz als ein einzelner Snapshot am Ende der Woche. Und je häufiger Sie Snapshots erstellen, desto weniger Zeit nimmt ihre Fertigstellung in Anspruch. Tägliche Snapshots können beispielsweise 20–30 Minuten dauern, während stündliche Snapshots innerhalb weniger Minuten abgeschlossen sein können. Manche OpenSearch Benutzer machen Schnappschüsse bis zu jeder halben Stunde.

Aufnehmen eines Snapshots

Beim Erstellen eines Snapshots geben Sie die folgenden Informationen an:

- Den Namen Ihres Snapshot-Repositorys
- Einen Namen für den Snapshot

In den Beispielen dieses Kapitels wird aufgrund der Einfachheit und Übersichtlichkeit der gängige HTTP-Client curl verwendet. Informationen zum Übergeben eines Benutzernamens und eines Passworts für Ihre Curl-Anfrage finden Sie im Tutorial Erste Schritte.

Wenn Ihre Zugriffsrichtlinien Benutzer oder Rollen angeben, müssen Sie Ihre Snapshot-Anfragen signieren. Für curl können Sie die `--aws-sigv4`Option mit Version 7.75.0 oder höher verwenden. Sie können auch die auskommentierten Beispiele im Python-Beispielclient verwenden, um signierte HTTP-Anfragen an dieselben Endpunkte zu stellen, die die curl-Befehle verwenden.

Führen Sie die folgenden Schritte aus, um einen manuellen Snapshot zu erstellen:

1. Sie können keinen Snapshot erstellen, wenn gerade ein Snapshot ausgeführt wird. Um dies zu überprüfen, führen Sie den folgenden Befehl aus:

   ```
   curl -XGET 'domain-endpoint/_snapshot/_status'
   ```

2. Führen Sie den folgenden Befehl aus, um einen manuellen Snapshot zu erstellen:

```
curl -XPUT 'domain-endpoint/_snapshot/repository-name/snapshot-name'
```

Um bestimmte Indizes ein- oder auszuschließen und andere Einstellungen festzulegen, fügen Sie einen Anforderungstext hinzu. Informationen zur Anforderungsstruktur finden Sie in der Dokumentation unter Schnappschüsse erstellen. OpenSearch

> **Note**
>
> Die Zeit, die für die Erstellung eines Snapshots benötigt wird, nimmt mit der Größe der OpenSearch Dienstdomäne zu. Bei lange laufenden Snapshot-Operationen tritt gelegentlich der folgende Fehler auf: `504 GATEWAY_TIMEOUT`. In der Regel können Sie diese Fehler ignorieren und warten, bis der Vorgang erfolgreich abgeschlossen werden kann. Führen Sie den folgenden Befehl aus, um den Status aller Snapshots in Ihrer Domain zu überprüfen:
>
> ```
> curl -XGET 'domain-endpoint/_snapshot/repository-name/_all?pretty'
> ```

Wiederherstellen von Snapshots

Bevor Sie einen Snapshot wiederherstellen, stellen Sie sicher, dass die Zieldomäne kein Multi-AZ mit Standby verwendet. Wenn Standby aktiviert ist, schlägt der Wiederherstellungsvorgang fehl.

> **Warning**
>
> Wenn Sie Indexaliase verwenden, sollten Sie entweder die Schreibanforderungen an einen Alias beenden oder den Alias auf einen anderen Index umstellen, bevor Sie seinen Index löschen. Hierdurch lässt sich folgendes Szenario vermeiden:
>
> 1. Sie löschen einen Index und dadurch auch dessen Alias.
> 2. Eine fehlerhafte Schreibanforderung an einen jetzt gelöschten Alias erstellt einen neuen Index mit demselben Namen wie der Alias.
> 3. Sie können den Alias aufgrund eines Namenskonflikts mit dem neuen Index nicht mehr verwenden. Wenn Sie den Alias zu einem anderen Index wechseln, geben Sie bei der Wiederherstellung von einem Snapshot `"include_aliases": false` an.

So stellen Sie einen Snapshot wieder her

1. Ermitteln Sie den Snapshot, den Sie wiederherstellen möchten. Stellen Sie sicher, dass alle Einstellungen für diesen Index, z. B. benutzerdefinierte Analyzer-Pakete oder Einstellungen für Zuweisungsanforderungen, mit der Domäne kompatibel sind. Verwenden Sie den folgenden Befehl, um alle Snapshot-Repositorys anzuzeigen:

   ```
   curl -XGET 'domain-endpoint/_snapshot?pretty'
   ```

   Nachdem Sie das Repository ermittelt haben, können Sie mit dem folgenden Befehl alle gespeicherten Snapshots anzeigen:

   ```
   curl -XGET 'domain-endpoint/_snapshot/repository-name/_all?pretty'
   ```

   > **Note**
   >
   > Die meisten automatischen Snapshots werden im `cs-automated`-Repository gespeichert. Wenn Ihre Domain Daten im Ruhezustand verschlüsselt, werden sie im `cs-automated-enc` Repository abgelegt. Wenn das gewünschte Repository für manuelle Snapshots nicht angezeigt wird, registrieren Sie es in der Domain.

2. (Optional) Löschen Sie einen oder mehrere Indizes in der OpenSearch Service-Domäne oder benennen Sie ihn um, wenn Namenskonflikte zwischen den Indizes im Cluster und den Indizes im Snapshot auftreten. Sie können keinen Snapshot Ihrer Indizes in einem OpenSearch Cluster wiederherstellen, der bereits Indizes mit denselben Namen enthält.

   Sie haben die folgenden Optionen, wenn Sie Konflikte bei der Indexbenennung haben:

   - Löschen Sie die Indizes in der vorhandenen OpenSearch Service-Domain und stellen Sie dann den Snapshot wieder her.
   - Benennen Sie die Indizes um, wenn Sie sie aus dem Snapshot wiederherstellen, und indizieren Sie sie später neu. Informationen zum Umbenennen von Indizes finden Sie in dieser Beispielanforderung in der OpenSearch Dokumentation.
   - Stellen Sie den Snapshot in einer anderen OpenSearch Dienstdomäne wieder her (nur mit manuellen Snapshots möglich).

   Der folgende Befehl löscht alle vorhandenen Indizes in einer Domain:

```
curl -XDELETE 'domain-endpoint/_all'
```

Wenn Sie jedoch nicht alle Indizes wiederherstellen möchten, können Sie einfach einen löschen:

```
curl -XDELETE 'domain-endpoint/index-name'
```

3. Um einen Snapshot wiederherzustellen, führen Sie den folgenden Befehl aus:

```
curl -XPOST 'domain-endpoint/_snapshot/repository-name/snapshot-name/_restore'
```

Aufgrund spezieller Berechtigungen für die OpenSearch Dashboards und detaillierter Zugriffskontrollindizes schlagen Versuche, alle Indizes wiederherzustellen, möglicherweise fehl, insbesondere wenn Sie versuchen, die Wiederherstellung anhand eines automatisierten Snapshots durchzuführen. Im folgenden Beispiel wird nur der Index `my-index` aus `2020-snapshot` im Snapshot-Repository `cs-automated` wiederhergestellt:

```
curl -XPOST 'domain-endpoint/_snapshot/cs-automated/2020-snapshot/_restore' \
-d '{"indices": "my-index"}' \
-H 'Content-Type: application/json'
```

Alternativ können Sie alle Indizes außer den Dashboards-Indizes und den Indizes der differenzierten Zugriffskontrolle wiederherstellen:

```
curl -XPOST 'domain-endpoint/_snapshot/cs-automated/2020-snapshot/_restore' \
-d '{"indices": "-.kibana*,-.opendistro*"}' \
-H 'Content-Type: application/json'
```

Mithilfe der Parameter und können Sie einen Snapshot wiederherstellen, ohne die zugehörigen Daten zu löschen. `rename_pattern` `rename_replacement` Weitere Informationen zu diesen Parametern finden Sie in den Anforderungsfeldern der Restore Snapshot API und in der OpenSearch Dokumentation als Beispielanforderung.

> **Note**
>
> Wenn nicht alle primären Shards für die entsprechenden Indizes zur Verfügung stehen, könnte ein Snapshot den `state` von `PARTIAL` aufweisen. Dieser Wert gibt an, dass Daten

aus mindestens einem Shard nicht erfolgreich gespeichert wurden. Sie können aus einem Teil-Snapshot wiederherstellen, aber Sie müssen möglicherweise fehlende Indizes aus älteren Snapshots wiederherstellen.

Löschen von manuellen Snapshots

Führen Sie den folgenden Befehl aus, um einen manuellen Snapshot zu löschen:

```
DELETE _snapshot/repository-name/snapshot-name
```

Automatisieren von Snapshots mit Snapshot Management

Sie können in OpenSearch Dashboards eine Snapshot Management (SM) -Richtlinie einrichten, um das regelmäßige Erstellen und Löschen von Snapshots zu automatisieren. SM kann Snapshots von einer Gruppe von Indizes erstellen, wohingegen Index State Management nur einen Snapshot pro Index erstellen kann. Um SM in OpenSearch Service verwenden zu können, müssen Sie Ihr eigenes Amazon S3 S3-Repository registrieren. Anweisungen zur Registrierung Ihres Repositorys finden Sie unter Manuelles Snapshot-Repository registrieren.

Vor SM bot OpenSearch Service eine kostenlose, automatisierte Snapshot-Funktion an, die immer noch standardmäßig aktiviert ist. Diese Funktion sendet Snapshots an das vom Service verwaltete Repository`cs-*`. Um die Funktion zu deaktivieren, wenden Sie sich an. AWS Support

Weitere Informationen zur SM-Funktion finden Sie in der OpenSearch Dokumentation unter Snapshot-Verwaltung.

SM unterstützt derzeit nicht die Erstellung von Snapshots für mehrere Indextypen. Wenn Sie beispielsweise versuchen, einen Snapshot für mehrere Indizes zu erstellen, wobei * sich einige Indizes in der Warm-Tier befinden, schlägt die Snapshot-Erstellung fehl. Wenn Ihr Snapshot mehrere Indextypen enthalten soll, verwenden Sie die ISM-Snapshot-Aktion, bis SM diese Option unterstützt.

Konfigurieren von Berechtigungen

Wenn Sie von einer früheren OpenSearch Service-Domain-Version auf 2.5 aktualisieren, sind die Sicherheitsberechtigungen für die Snapshot-Verwaltung möglicherweise nicht für die Domäne definiert. Benutzer ohne Administratorrechte müssen dieser Rolle zugeordnet werden, um die Snapshot-Verwaltung in Domänen mit detaillierter Zugriffskontrolle verwenden zu können. Gehen Sie wie folgt vor, um die Snapshot-Verwaltungsrolle manuell zu erstellen:

1. Gehen Sie in OpenSearch Dashboards zu Sicherheit und wählen Sie Berechtigungen aus.
2. Wählen Sie Aktionsgruppe erstellen und konfigurieren Sie die folgenden Gruppen:

Group name (Gruppenname)	Berechtigungen
`snapshot_management_full_access`	• `cluster:admin/opensearch/snapshot_management/*` • `cluster:admin/opensearch/notifications/feature/publish` • `cluster:admin/repository/*` • `cluster:admin/snapshot/*`
`snapshot_management_read_access`	• `cluster:admin/opensearch/snapshot_management/policy/get` • `cluster:admin/opensearch/snapshot_management/policy/search` • `cluster:admin/opensearch/snapshot_management/policy/explain` • `cluster:admin/repository/get` • `cluster:admin/snapshot/get`

3. Wählen Sie Rollen und Rolle erstellen.
4. Nennen Sie die Rolle snapshot_management_role.
5. Wählen Sie für Clusterberechtigungen oder aus. `snapshot_management_full_access` `snapshot_management_read_access`
6. Wählen Sie Erstellen.
7. Nachdem Sie die Rolle erstellt haben, ordnen Sie sie einer beliebigen Benutzer- oder Backend-Rolle zu, die Snapshots verwaltet.

Überlegungen

Beachten Sie bei der Konfiguration der Snapshot-Verwaltung Folgendes:

- Pro Repository ist eine Richtlinie zulässig.
- Für eine Richtlinie sind bis zu 400 Snapshots zulässig.

- Diese Funktion kann nicht ausgeführt werden, wenn Ihre Domain den Status Rot hat, unter hohem JVM-Druck steht (85% oder mehr) oder wenn die Snapshot-Funktion nicht mehr funktioniert. Wenn die allgemeine Indexierungs- und Suchleistung Ihres Clusters beeinträchtigt wird, kann dies auch für SM gelten.
- Ein Snapshot-Vorgang beginnt erst, nachdem der vorherige Vorgang abgeschlossen ist, sodass keine gleichzeitigen Snapshot-Vorgänge durch eine Richtlinie aktiviert werden.
- Mehrere Richtlinien mit demselben Zeitplan können zu einem Anstieg der Ressourcen führen. Wenn sich die Snapshot-Indizes der Richtlinien überschneiden, können die Snapshot-Operationen auf Festplattenebene nur sequentiell ausgeführt werden, was zu einem kaskadierten Leistungsproblem führen kann. Wenn sich die Richtlinien ein Repository teilen, kommt es zu einer Zunahme von Schreibvorgängen in dieses Repository.
- Wir empfehlen Ihnen, die Automatisierung von Snapshot-Vorgängen nicht öfter als einmal pro Stunde einzuplanen, es sei denn, Sie haben einen speziellen Anwendungsfall.

Automatisieren von Snapshots mit Index-Statusmanagement

Sie können die Operation Index-Statusmanagement (ISM) `snapshot` verwenden, um automatisch Snapshots von Indizes basierend auf Änderungen des Alters, der Größe oder der Anzahl der Dokumente auszulösen. ISM eignet sich am besten, wenn Sie einen Snapshot pro Index benötigen. Informationen zum Erstellen eines Snapshots einer Gruppe von Indizes finden Sie unterAutomatisieren von Snapshots mit Snapshot Management.

Um SM in OpenSearch Service verwenden zu können, müssen Sie Ihr eigenes Amazon S3 S3-Repository registrieren. Ein Beispiel für eine Richtlinie, die den Vorgang `snapshot` verwendet, finden Sie unter Beispielrichtlinien.

Verwenden von Curator für Snapshots

Wenn ISM für die Index- und Snapshot-Verwaltung nicht funktioniert, können Sie stattdessen Curator verwenden. Es bietet eine erweiterte Filterfunktionalität zur Vereinfachung der Verwaltungsaufgaben auf komplexen Clustern. Verwenden Sie pip zum Installieren von Curator:

```
pip install elasticsearch-curator
```

Sie können Curator als Befehlszeilenschnittstelle (Command Line Interface, CLI) oder Python-API verwenden. Wenn Sie die Python-API verwenden, müssen Sie Version 7.13.4 oder früher des Legacy-elasticsearch-py-Clients verwenden. Sie unterstützt den opensearch-py-Client nicht.

Wenn Sie die CLI verwenden, exportieren Sie Ihre Anmeldeinformationen über die Befehlszeile und konfigurieren Sie `curator.yml` wie folgt:

```
client:
  hosts: search-my-domain.us-west-1.es.amazonaws.com
  port: 443
  use_ssl: True
  aws_region: us-west-1
  aws_sign_request: True
  ssl_no_validate: False
  timeout: 60

logging:
  loglevel: INFO
```

Aktualisieren von Amazon- OpenSearch Service-Domains

> **Note**
>
> OpenSearch - und Elasticsearch-Versions-Upgrades unterscheiden sich von Service-Software-Updates. Informationen zum Aktualisieren der Servicesoftware für Ihre OpenSearch Service-Domain finden Sie unter the section called “Service-Software-Updates”.

Amazon OpenSearch Service bietet direkte Upgrades für Domains, auf denen OpenSearch 1.0 oder höher oder Elasticsearch 5.1 oder höher ausgeführt wird. Wenn Sie Services wie Amazon Data Firehose oder Amazon CloudWatch Logs verwenden, um Daten an OpenSearch Service zu streamen, überprüfen Sie vor der OpenSearch Migration, ob diese Services die neuere Version von unterstützen.

Themen

- Verwenden eines Snapshots zum Migrieren von Daten

Unterstützte Upgrade-Pfade

Derzeit unterstützt OpenSearch Service die folgenden Upgrade-Pfade:

Von Version	Auf Version
OpenSearch 1.3 oder 2.x	OpenSearch 2.x Version 2.3 enthält die folgenden grundlegenden Änderungen: • Der `type` Parameter wurde in Version 2.0 von allen OpenSearch API-Endpunkten entfernt. Weitere Informationen finden Sie unter grundlegende Änderungen. • Wenn Ihre Domäne Indizes (Hot oder Cold) enthält UltraWarm, die ursprüngl ich in Elasticsearch 6.8 erstellt wurden, sind diese Indizes nicht mit OpenSearc h 2.3 kompatibel. Bevor Sie auf Version 2.3 aktualisieren, müssen Sie die nicht kompatibl en Indizes neu indizieren. Bei inkompatiblen UltraWarm oder Cold-Indizes migrieren Sie sie in den Hot Storage, indizieren die Daten neu und migrieren Sie sie dann wieder in den Warm- oder Cold Storage. Alternativ können Sie die Indizes auch löschen, wenn Sie sie nicht mehr benötigen. Wenn Sie Ihre Domain versehentlich auf Version 2.3 aktualisieren, ohne diese Schritte vorher auszuführen, können Sie die nicht kompatiblen Indizes nicht aus ihrer aktuellen Speicherebene migrieren. Ihre einzige Möglichkeit besteht darin, sie zu löschen.
OpenSearch 1.x	OpenSearch 1.x
Elasticsearch 7.x	Elasticsearch 7.x oder OpenSearch 1.x

Von Version	Auf Version
	Important OpenSearch 1.x führt zahlreiche grundlegende Änderungen ein. Details hierzu finden Sie unter Amazon OpenSearch Service umbenennen.
Elasticsearch 6.8	Elasticsearch 7.x oder OpenSearch 1.x **Important** Elasticsearch 7.0 und OpenSearch 1.0 enthalten zahlreiche grundlegende Änderungen. Bevor Sie ein direktes Upgrade initiieren, empfehlen wir, einen manuellen Snapshot der 6.x-Domain zu erstellen, sie auf einer Test-7.x- oder OpenSearch 1.x-Domain wiederherzustellen und diese Testdomain zur Identifizierung potenzieller Upgrade-Probleme zu verwenden. Informationen zu grundlegenden Änderungen in OpenSearch 1.0 finden Sie unter Amazon OpenSearch Service umbenennen. Wie in Elasticsearch 6.x können Indizes nur einen Mapping-Typ enthalten, aber dieser Typ muss jetzt den Namen `_doc` haben. Daher benötigen bestimmte APIs keinen Mapping-Typ mehr im Anforderungstext (z. B. die `_bulk`-API). Für neue Indizes haben selbst gehostete Elasticsearch 7.x und OpenSearch 1.x eine Standard-Shard-Anzahl von One. OpenSearch Service-Domains auf Elasticsearch 7.x und höher, wobei der vorherige Standardwert von fünf beibehalten wird.
Elasticsearch 6.x	Elasticsearch 6.x

Von Version	Auf Version
Elasticsearch 5.6	Elasticsearch 6.x **Important** Indizes, die in Version 6.x erstellt wurden, unterstützen keine mehrfache n Mapping-Typen mehr. Indizes, die in Version 5.x erstellt wurden, unterstützen noch mehrfache Mapping-Typen, wenn sie in einem 6.x Cluster wiederhergestellt werden. Sehen Sie nach, ob Ihr Code nur einen einzigen Mapping-Typ pro Index erstellt. Um Ausfallzeiten während des Upgrades von Elasticsearch 5.6 auf 6.x zu minimieren, indiziert OpenSearch Service den `.kibana` Index auf neu`.kibana-6` , löscht `.kibana`, erstellt einen Alias mit dem Namen `.kibana`und ordnet den neuen Index dem neuen Alias zu.
Elasticsearch 5.x	Elasticsearch 5.x

Der Upgrade-Prozess besteht aus drei Schritten:

1. Prüfungen vor dem Upgrade – OpenSearch Der Service prüft auf Probleme, die ein Upgrade blockieren können, und fährt nicht mit dem nächsten Schritt fort, es sei denn, diese Prüfungen sind erfolgreich.
2. Snapshot – OpenSearch Der Service erstellt einen Snapshot des OpenSearch oder Elasticsearch-Clusters und fährt nicht mit dem nächsten Schritt fort, es sei denn, der Snapshot ist erfolgreich. Wenn das Upgrade fehlschlägt, verwendet OpenSearch Service diesen Snapshot, um den Cluster in seinen ursprünglichen Zustand wiederherzustellen. Weitere Informationen finden Sie unter the section called “Nach einem Upgrade ist kein Downgrade möglich”.
3. Upgrade – Der OpenSearch Service startet das Upgrade, was zwischen 15 Minuten und mehreren Stunden dauern kann. OpenSearch Dashboards sind möglicherweise während eines Teils oder des gesamten Upgrades nicht verfügbar.

Starten eines Upgrades (Konsole)

Der Upgrade-Vorgang kann nicht rückgängig gemacht und weder angehalten noch abgebrochen werden. Während eines Upgrades können Sie keine Änderungen an der Konfiguration der Domain vornehmen. Bevor Sie das Upgrade starten, müssen Sie überprüfen, ob Sie fortfahren möchten. Sie können diese Schritte auch zum Ausführen der Pre-Upgrade-Prüfung verwenden ohne tatsächlich das Upgrade zu starten.

Wenn der Cluster über dedizierte Hauptknoten verfügt, werden OpenSearch Upgrades ohne Ausfallzeiten abgeschlossen. Andernfalls reagiert der Cluster nach dem Upgrade möglicherweise mehrere Sekunden lang nicht mehr, während er einen Master-Knoten wählt.

So aktualisieren Sie eine Domain auf eine neuere Version von OpenSearch oder Elasticsearch

1. Erstellen Sie einen manuellen Snapshot Ihrer Domain. Dieser Snapshot dient als Backup, das Sie auf einer neuen Domain wiederherstellen können, wenn Sie zu mit der vorherigen OpenSearch Version zurückkehren möchten.
2. Rufen Sie die Webseite unter http://aws.amazon.com auf und klicken Sie auf In der Konsole anmelden.
3. Wählen Sie unter Analyse die Option Amazon OpenSearch Service aus.
4. Wählen Sie im Navigationsbereich unter My domains (Meine Domains) die Domain aus, die Sie upgraden möchten.
5. Wählen Sie Aktionen und Aktualisieren aus.
6. Wählen Sie die Version aus, auf die aktualisiert werden soll. Wenn Sie auf eine - OpenSearch Version aktualisieren, wird die Option Kompatibilitätsmodus aktivieren angezeigt. Wenn Sie diese Einstellung aktivieren, OpenSearch meldet seine Version als 7.10, damit Elasticsearch-OSS-Clients und Plugins wie Logstash weiterhin mit Amazon OpenSearch Service arbeiten können. Sie können diese Einstellung später deaktivieren.
7. Wählen Sie Upgrade.
8. Überprüfen Sie den Status im Domain-Dashboard, um den Status des Upgrades zu überwachen.

Starten eines Upgrades (CLI)

Sie können die folgenden Vorgänge verwenden, um die richtige Version von OpenSearch oder Elasticsearch für Ihre Domain zu identifizieren, ein direktes Upgrade zu starten, die Vor-Upgrade-Prüfung durchzuführen und den Fortschritt anzuzeigen:

- `get-compatible-versions` (`GetCompatibleVersions`)
- `upgrade-domain` (`UpgradeDomain`)
- `get-upgrade-status` (`GetUpgradeStatus`)
- `get-upgrade-history` (`GetUpgradeHistory`)

Weitere Informationen finden Sie in der AWS -CLI-Befehlsreferenz und in der Amazon- OpenSearch Service-API-Referenz .

Starten eines Upgrades (SDK)

In diesem Beispiel wird der Python-OpenSearchServiceLow-Level-Client von verwendet, AWS SDK for Python (Boto) um zu überprüfen, ob eine Domain für ein Upgrade auf eine bestimmte Version berechtigt ist, sie zu aktualisieren und den Upgrade-Status kontinuierlich zu überprüfen.

```
import boto3
from botocore.config import Config
import time

# Build the client using the default credential configuration.
# You can use the CLI and run 'aws configure' to set access key, secret
# key, and default Region.

DOMAIN_NAME = ''  # The name of the domain to upgrade
TARGET_VERSION = ''  # The version you want to upgrade the domain to. For example,
 OpenSearch_1.1

my_config = Config(
    # Optionally lets you specify a Region other than your default.
    region_name='us-east-1'
)
client = boto3.client('opensearch', config=my_config)


def check_versions():
    """Determine whether domain is eligible for upgrade"""
    response = client.get_compatible_versions(
        DomainName=DOMAIN_NAME
    )
    compatible_versions = response['CompatibleVersions']
    for i in range(len(compatible_versions)):
        if TARGET_VERSION in compatible_versions[i]["TargetVersions"]:
```

```
            print('Domain is eligible for upgrade to ' + TARGET_VERSION)
            upgrade_domain()
            print(response)
        else:
            print('Domain not eligible for upgrade to ' + TARGET_VERSION)


def upgrade_domain():
    """Upgrades the domain"""
    response = client.upgrade_domain(
        DomainName=DOMAIN_NAME,
        TargetVersion=TARGET_VERSION
    )
    print('Upgrading domain to ' + TARGET_VERSION + '...' + response)
    time.sleep(5)
    wait_for_upgrade()


def wait_for_upgrade():
    """Get the status of the upgrade"""
    response = client.get_upgrade_status(
        DomainName=DOMAIN_NAME
    )
    if (response['UpgradeStep']) == 'UPGRADE' and (response['StepStatus']) ==
 'SUCCEEDED':
        print('Domain successfully upgraded to ' + TARGET_VERSION)
    elif (response['StepStatus']) == 'FAILED':
        print('Upgrade failed. Please try again.')
    elif (response['StepStatus']) == 'SUCCEEDED_WITH_ISSUES':
        print('Upgrade succeeded with issues')
    elif (response['StepStatus']) == 'IN_PROGRESS':
        time.sleep(30)
        wait_for_upgrade()


def main():
    check_versions()


if __name__ == "__main__":
    main()
```

Beheben von Validierungsfehlern

Wenn Sie ein Versionsupgrade von OpenSearch oder Elasticsearch initiieren, führt OpenSearch Service zunächst eine Reihe von Validierungsprüfungen durch, um sicherzustellen, dass Ihre Domain für ein Upgrade in Frage kommt. Wenn eine dieser Prüfungen fehlschlägt, erhalten Sie eine Benachrichtigung mit den spezifischen Problemen, die Sie beheben müssen, bevor Sie Ihre Domain aktualisieren. Eine Liste potenzieller Probleme und Schritte zu deren Behebung finden Sie unter the section called “Beheben von Validierungsfehlern”.

Fehlerbehebung bei einem Upgrade

Direkte -Upgrades erfordern gesunde Domains. Ihre Domain ist womöglich nicht für ein Upgrade berechtigt oder kann aus einer Vielzahl von Gründen nicht upgegradet werden. Die folgende Tabelle zeigt die gängigsten Probleme.

Problem	Beschreibung
Optionales Plugin wird nicht unterstützt	Wenn Sie eine Domain mit optionalen Plug-Ins aktualisieren, aktualisiert OpenSearch Service auch automatisch die Plug-Ins. Daher muss die Zielversion für Ihre Domain auch diese optionalen Plug-Ins unterstützen. Wenn auf der Domain ein optionales Plugin installiert ist, das für die Zielversion nicht verfügbar ist, schlägt die Upgrade-Anforderung fehl.
Zu viele Shards pro Knoten	OpenSearch, sowie 7.x-Versionen von Elasticsearch haben eine Standardeinstellung von nicht mehr als 1 000 Shards pro Knoten. Wenn ein Knoten in Ihrem aktuellen Cluster diese Einstellung überschreitet, erlaubt OpenSearch Ihnen Service kein Upgrade. Informationen zu den Optionen für die Fehlerbehebung finden Sie unter the section called “Maximales Shard-Limit überschritten”.
Domain in Verarbeitung	Die Domain befindet sich in der Mitte einer Konfigurationsänderung. Überprüfen Sie die Upgrade-Berechtigung, nachdem die Operation abgeschlossen ist.
Roter Cluster-Status	Ein oder mehrere Indizes im Cluster sind rot. Fehlerbehandlungsschritte finden Sie unter the section called “Roter Cluster-Status”.
Hohe Fehlerrate	Der Cluster gibt beim Versuch, Anfragen zu verarbeiten, eine große Anzahl von 5xx-Fehlern zurück. Dieses Problem ist in der Regel das

Problem	Beschreibung
	Ergebnis zu vieler gleichzeitiger Lese- oder Schreibanforderungen. Erwägen Sie, den Datenverkehr zu dem Cluster zu reduzieren oder Ihre Domain zu skalieren.
Split brain	Split brain bedeutet, dass Ihr Cluster über mehr als einen Master-Kn oten verfügt und sich in zwei Cluster aufgeteilt hat, die sich nicht von selbst wieder hinzufügen. Sie können split brain vermeiden, indem Sie die empfohlene Anzahl der dedizierten Hauptknoten verwenden. Für Hilfe zur Wiederherstellung von split brain wenden Sie sich an AWS Support.
Master-Knoten wurde nicht gefunden.	OpenSearch Der Service kann den Hauptknoten des Clusters nicht finden. Wenn Ihre Domain Multi-AZ verwendet, kann ein Ausfall einer Availability Zone dazu geführt haben, dass der Cluster das Quorum verliert und keinen neuen Hauptknoten wählen kann. Wenn sich das Problem nicht von selbst löst, wenden Sie sich bitte an AWS Support.
Zu viele ausstehende Aufgaben	Der Master-Knoten ist stark ausgelastet und hat viele ausstehende Aufgaben. Erwägen Sie, den Datenverkehr zu dem Cluster zu reduzieren oder Ihre Domain zu skalieren.
Beeinträchtigtes Speicher-Volume	Das Datenträger-Volume eines oder mehrerer Knoten funktioniert nicht ordnungsgemäß. Dieses Problem tritt oft zusammen mit anderen Problemen, wie z. B. eine hohe Fehlerrate oder zu viele ausstehende Aufgaben, auf. Wenn es isoliert auftritt und sich nicht von selbst löst, wenden Sie sich bitte an AWS Support.
Problem mit KMS-Schlüssel	Der KMS-Schlüssel für die Verschlüsselung der Domain ist entweder nicht zugänglich oder fehlt. Weitere Informationen finden Sie unter the section called “Überwachen von Domains, die Daten im Ruhezustand verschlüsseln”.

Problem	Beschreibung
Snapshot in Arbeit	Die Domain erstellt derzeit einen Snapshot. Überprüfen Sie die Upgrade-Berechtigung, nachdem der Snapshot abgeschlossen ist. Überprüfen Sie auch, ob Sie manuelle Snapshot-Repositorys auflisten, Snapshots innerhalb dieser Repositorys auflisten und manuelle Snapshots erstellen können. Wenn OpenSearch der Service nicht überprüfen kann, ob ein Snapshot ausgeführt wird, können Upgrades fehlschlagen.
Snapshot-Timeout oder -Fehler	Der Pre-Upgrade-Snapshot hat zu lange gedauert oder ist fehlgesch lagen. Überprüfen Sie die Cluster-Gesundheit und versuchen Sie es erneut. Wenn das Problem weiterhin besteht, wenden Sie sich bitte an AWS Support.
Inkompatible Indizes	Ein oder mehrere Indizes sind nicht kompatibel mit der Zielversion. Dieses Problem kann auftreten, wenn Sie die Indizes von einer älteren Version von OpenSearch oder Elasticsearch migriert haben. Indizieren Sie die Indizes neu und versuchen Sie es erneut.
Hohe Festplatt ennutzung	Die Festplattennutzung für den Cluster übersteigt 90 %. Löschen Sie Daten oder skalieren Sie die Domain und versuchen Sie es erneut.
Hohe JVM-Nutzung	Die JVM-Speicherbelastung übersteigt 75 %. Reduzieren Sie den Datenverkehr an den Cluster oder skalieren Sie die Domain und versuchen Sie es erneut.
OpenSearch Dashboards-Aliaspr oblem	`.dashboards` ist bereits als Alias konfiguriert und wird einem inkompatiblen Index zugeordnet, wahrscheinlich einem von einer früheren Version von OpenSearch Dashboards. Indizieren Sie neu und versuchen Sie es erneut.
Roter Dashboard-Status	OpenSearch Der Dashboards-Status ist rot. Verwenden Sie Dashboard s, wenn das Upgrade abgeschlossen ist. Wenn der rote Status weiterhin besteht, beheben Sie den Fehler manuell und versuchen Sie es erneut.

Problem	Beschreibung
Cluster-übergreifende Kompatibilität	Sie können ein Upgrade nur dann durchführen, wenn die Cluster-ü bergreifende Kompatibilität zwischen der Quell- und Ziel-Domain nach dem Upgrade aufrechterhalten wird. Während des Upgrade-Vorgangs werden alle inkompatiblen Verbindungen identifiziert. Um fortzufahren, aktualisieren Sie entweder die Remote-Domain oder löschen Sie die inkompatiblen Verbindungen. Beachten Sie, dass Sie, wenn die Replikati on für die Domain aktiv ist, nicht fortsetzen können, nachdem Sie die Verbindung gelöscht haben.
Problem mit dem anderen OpenSearch Service	Probleme mit dem OpenSearch Service selbst können dazu führen, dass Ihre Domain als nicht für ein Upgrade berechtigt angezeigt wird. Wenn keine der vorangehenden Bedingungen für Ihre Domain gelten und das Problem mehr als einen Tag bestehen bleibt, wenden Sie sich bitte an AWS Support.

Verwenden eines Snapshots zum Migrieren von Daten

Direkte Upgrades sind die einfachere, schnellere und zuverlässigere Möglichkeit, eine Domain auf eine neuere OpenSearch oder Elasticsearch-Version zu aktualisieren. Snapshots sind eine gute Option, wenn Sie aus einer Version von Elasticsearch vor 5.1 migrieren oder einen völlig neuen Cluster migrieren möchten.

Die folgende Tabelle zeigt, wie Sie Snapshots verwenden, um Daten zu einer Domain zu migrieren, die eine andere - OpenSearch oder Elasticsearch-Version verwendet. Informationen zum Erstellen und Wiederherstellen von Snapshots finden Sie unter the section called “Erstellen von Index-Snapshots”.

Von Version	Auf Version	Migrationsprozess
OpenSearch 1.3 oder 2.x	OpenSearch 2.x	1. Überprüfen Sie die grundlegenden Änderungen für OpenSearch 2.3, um festzustellen, ob Sie Anpassung en an Ihren Indizes oder Anwendungen vornehmen müssen. 2. Erstellen Sie einen manuellen Snapshot der Domain 1.3 oder 2.x.

Von Version	Auf Version	Migrationsprozess

		3. Erstellen Sie eine 2.x-Domain, die eine höhere Version als Ihre ursprüngliche 1.3- oder 2.x-Domain hat.
		4. Stellen Sie den Snapshot aus der ursprünglichen Domäne in der 2.x-Domäne wieder her. Während des Vorgangs müssen Sie möglicherweise Ihren `.opensearch` Index unter einem neuen Namen wiederherstellen:
		`POST _snapshot/ <repository-name> /<snapshot-name>/_restore`
		`{`
		`"indices": "*",`
		`"ignore_unavailable": true,`
		`"rename_pattern": ".opensearch",`
		`"rename_replacement": ".backup-opensearch"`
		`}`
		Anschließend können Sie `.backup-opensearch` in der neuen Domain neu indizieren und als Alias für `.opensearch` verwenden. Beachten Sie, dass der `_restore` REST-Aufruf nicht enthält, `include_global_state` da der Standardwert in false `_restore` ist. Daher enthält die Testdomäne keine Indexvorlagen und hat nicht den vollständigen Status aus dem Backup.
		5. Wenn Sie Ihre ursprüngliche Domain nicht mehr benötigen, löschen Sie sie. Andernfalls fallen weitere Kosten für die Domain an.

Von Version	Auf Version	Migrationsprozess

OpenSearch 1.x	OpenSearch 1.x	1. Erstellen Sie einen manuellen Snapshot der 1.x-Domain.
		2. Erstellen Sie eine 1.x-Domain, die eine höhere Version als Ihre ursprüngliche 1.x-Domain hat.
		3. Stellen Sie den Snapshot aus der ursprünglichen Domäne in der neuen 1.x-Domäne wieder her. Während des Vorgangs müssen Sie möglicherweise Ihren `.opensearch` Index unter einem neuen Namen wiederherstellen:
		`POST _snapshot/ <repository-name> /<snapshot-name>/_restore`
		`{`
		`  "indices": "*",`
		`  "ignore_unavailable": true,`
		`  "rename_pattern": ".opensearch",`
		`  "rename_replacement": ".backup-opensearch"`
		`}`
		Anschließend können Sie `.backup-opensearch` in der neuen Domain neu indizieren und als Alias für `.opensearch` verwenden. Beachten Sie, dass der `_restore` REST-Aufruf nicht enthält, `include_global_state` da der Standardwert in false `_restore` ist. Daher enthält die Testdomäne keine Indexvorlagen und hat nicht den vollständigen Status aus dem Backup.
		4. Wenn Sie Ihre ursprüngliche Domain nicht mehr benötigen, löschen Sie sie. Andernfalls fallen weitere Kosten für die Domain an.

Von Version	Auf Version	Migrationsprozess

Elasticsearch 6.x oder 7.x	OpenSearch 1.x	1. Überprüfen Sie die grundlegenden Änderungen für OpenSearch 1.0, um festzustellen, ob Sie Anpassungen an Ihren Indizes oder Anwendungen vornehmen müssen.
		2. Erstellen Sie einen manuellen Snapshot der Elasticsearch 7.x or 6.x-Domain.
		3. Erstellen Sie eine OpenSearch 1.x-Domain.
		4. Stellen Sie den Snapshot von der Elasticsearch-Domäne in der OpenSearch Domäne wieder her. Während des Vorgangs müssen Sie möglicherweise Ihren `.elasticsearch` Index unter einem neuen Namen wiederherstellen:
		`POST _snapshot/ <repository-name> /<snapshot-name>/_restore`
		`{`
		`  "indices": "*",`
		`  "ignore_unavailable": true,`
		`  "rename_pattern": ".elasticsearch",`
		`  "rename_replacement": ".backup-opensearch"`
		`}`
		Anschließend können Sie `.backup-opensearch` in der neuen Domain neu indizieren und als Alias für `.elasticsearch` verwenden. Beachten Sie, dass der `_restore` REST-Aufruf nicht enthält, `include_global_state` da der Standardwert in false `_restore` ist. Daher enthält die Testdomäne keine Indexvorlagen und hat nicht den vollständigen Status aus dem Backup.
		5. Wenn Sie Ihre ursprüngliche Domain nicht mehr benötigen, löschen Sie sie. Andernfalls fallen weitere Kosten für die Domain an.

Von Version	Auf Version	Migrationsprozess

Elasticsearch 6.x	Elasticsearch 7.x	1. Lesen Sie funktionsgefährdende Änderungen in 7.0 nach, um zu prüfen, ob Sie Ihre Indizes oder Anwendungen anpassen müssen.
		2. Erstellen Sie einen manuellen Snapshot der 6.x-Domain.
		3. Erstellen Sie eine 7.x-Domain.
		4. Stellen Sie den Snapshot von der ursprünglichen Domain in der 7.x-Domain wieder her. Während der Operation müssen Sie wahrscheinlich den `.opensearch` -Index unter einem neuen Namen wiederher stellen:
		`POST _snapshot/ <repository-name> /<snapshot-name>/_restore`
		`{`
		`  "indices": "*",`
		`  "ignore_unavailable": true,`
		`  "rename_pattern": ".elasticsearch",`
		`  "rename_replacement": ".backup-elasticsearch"`
		`}`
		Anschließend können Sie `.backup-elasticsearch` in der neuen Domain neu indizieren und als Alias für `.elasticsearch` verwenden. Beachten Sie, dass der `_restore` REST-Aufruf nicht enthält, `include_global_state` da der Standardwert in false `_restore` ist. Daher enthält die Testdomäne keine Indexvorlagen und hat nicht den vollständigen Status aus dem Backup.
		5. Wenn Sie Ihre ursprüngliche Domain nicht mehr benötigen, löschen Sie sie. Andernfalls fallen weitere Kosten für die Domain an.

Von Version	Auf Version	Migrationsprozess
Elasticsearch 6.x	Elasticsearch 6.8	1. Erstellen Sie einen manuellen Snapshot der 6.x-Domain. 2. Erstellen Sie eine 6.8-Domain. 3. Stellen Sie den Snapshot von der ursprünglichen Domain in der 6.8-Domain wieder her. 4. Wenn Sie Ihre ursprüngliche Domain nicht mehr benötigen, löschen Sie sie. Andernfalls fallen weitere Kosten für die Domain an.
Elasticsearch 5.x	Elasticsearch 6.x	1. Lesen Sie funktionsgefährdende Änderungen in 6.0 nach, um zu prüfen, ob Sie Ihre Indizes oder Anwendungen anpassen müssen. 2. Erstellen Sie einen manuellen Snapshot der 5.x-Domain. 3. Erstellen Sie eine 6.x-Domain. 4. Stellen Sie den Snapshot von der ursprünglichen Domain in der 6.x-Domain wieder her. 5. Falls Sie Ihre 5.x-Domain nicht mehr benötigen, löschen Sie diese. Andernfalls fallen weitere Kosten für die Domain an.
Elasticsearch 5.x	Elasticsearch 5.6	1. Erstellen Sie einen manuellen Snapshot der 5.x-Domain. 2. Erstellen Sie eine 5.6-Domain. 3. Stellen Sie den Snapshot von der ursprünglichen Domain in der 5.6-Domain wieder her. 4. Wenn Sie Ihre ursprüngliche Domain nicht mehr benötigen, löschen Sie sie. Andernfalls fallen weitere Kosten für die Domain an.

Von Version	Auf Version	Migrationsprozess
Elasticsearch 2.3	Elasticsearch 6.x	Elasticsearch 2.3-Snapshots sind nicht kompatibel mit 6.x. Zur direkten Migration Ihrer Daten von 2.3 auf 6.x müssen Sie Ihre Indizes in der neuen Domain manuell wiederherstellen. Alternativ können Sie die Schritte 2.3 bis 5.x in dieser Tabelle befolgen, `_reindex`-Operationen in der neuen 5.x-Domain ausführen, um Ihre 2.3-Indizes in 5.x-Indizes zu konvertieren, und folgen dann den Schritten 5.x bis 6.x.
Elasticsearch 2.3	Elasticsearch 5.x	1. Lesen Sie funktionsgefährdende Änderungen in 5.0 nach, um zu prüfen, ob Sie Ihre Indizes oder Anwendungen anpassen müssen. 2. Erstellen Sie einen manuellen Snapshot der 2.3-Domain. 3. Erstellen Sie eine 5.x-Domain. 4. Stellen Sie den Snapshot der 2.3-Domain auf der 5.x-Domain wieder her. 5. Wenn Sie Ihre 2.3-Domain nicht mehr benötigen, löschen Sie sie. Andernfalls fallen weitere Kosten für die Domain an.

Von Version	Auf Version	Migrationsprozess
Elasticsearch 1.5	Elasticsearch 5.x	Elasticsearch 1.5-Snapshots sind nicht kompatibel mit 5.x. Zur Migration Ihrer Daten von 1.5 auf 5.x müssen Sie Ihre Indizes in der neuen Domain manuell wiederherstellen. **Important** 1.5-Snapshots sind mit 2.3 kompatibel, OpenSearch Service-2.3-Domains unterstützen den `_reindex` Vorgang jedoch nicht. Da Sie diese nicht neu indizieren können, können Indizes aus einer 1.5-Domain von 2.3-Snapshots dennoch nicht in 5.x-Domains wiederhergestellt werden.

Von Version	Auf Version	Migrationsprozess
Elasticsearch 1.5	Elasticsearch 2.3	1. Verwenden Sie das Migrations-Plugin, um herauszufinden, ob Sie direkt auf Version 2.3 upgraden können. Möglicherweise müssen Sie Ihre Daten vor der Migration ändern. a. Öffnen Sie in einem Webbrowser `http://domain-endpoint /_plugin/migration/` . b. Wählen Sie Run checks now (Prüfungen jetzt ausführen) aus. c. Überprüfen Sie die Ergebnisse und, falls erforderlich, befolgen Sie die Anweisungen, um Änderungen an Ihren Daten vorzunehmen. 2. Erstellen Sie einen manuellen Snapshot der 1.5-Domain. 3. Erstellen Sie eine 2.3-Domain. 4. Stellen Sie den Snapshot der 1.5-Domain auf der 2.3-Domain wieder her. 5. Wenn Sie Ihre 1.5-Domain nicht mehr benötigen, löschen Sie sie. Andernfalls fallen weitere Kosten für die Domain an.

Einen benutzerdefinierten Endpunkt für Amazon OpenSearch Service erstellen

Wenn Sie einen benutzerdefinierten Endpunkt für Ihre Amazon OpenSearch Service-Domain erstellen, können Sie leichter auf Ihre URLs OpenSearch und Ihre OpenSearch Dashboard-URLs verweisen. Sie können das Branding Ihres Unternehmens einbeziehen oder einfach einen kürzeren easier-to-remember Endpunkt als den Standard-Endpunkt verwenden.

Wenn Sie jemals zu einer neuen Domäne wechseln müssen, aktualisieren Sie einfach Ihren DNS, um auf die neue URL zu verweisen und verwenden Sie den gleichen Endpunkt wie zuvor.

Sie sichern benutzerdefinierte Endpunkte, indem Sie entweder ein Zertifikat in AWS Certificate Manager (ACM) generieren oder eines Ihrer eigenen importieren.

Benutzerdefinierte Endpunkte für neue Domänen

Sie können mithilfe der OpenSearch Servicekonsole oder der Konfigurations-API einen benutzerdefinierten Endpunkt für eine neue OpenSearch Service-Domain aktivieren. AWS CLI

So passen Sie Ihren Endpunkt an (Konsole)

1. Wählen Sie in der OpenSearch Servicekonsole Create domain aus und geben Sie einen Namen für die Domain ein.
2. Wählen Sie unter Benutzerdefinierter Endpunkt die Option Benutzerdefinierten Endpunkt aktivieren aus.
3. Geben Sie für Benutzerdefinierter Hostname Ihren bevorzugten benutzerdefinierten Endpunkt-Hostnamen ein. Der Hostname sollte ein vollständig qualifizierter Domänenname (Fully Qualified Domäne Name, FQDN) sein, z. B. www.yourDomäne.com oder example.yourDomäne.com.

   > **Note**
   >
   > Wenn Sie kein Platzhalterzertifikat haben, müssen Sie ein neues Zertifikat für die Unterdomänen Ihres benutzerdefinierten Endpunkts anfordern.

4. Wählen Sie als AWS -Zertifikat das SSL-Zertifikat aus, das Sie für die Domäne verwenden möchten. Wenn keine Zertifikate verfügbar sind, können Sie eines in ACM importieren oder ACM für die Bereitstellung eines Zertifikats verwenden. Weitere Informationen finden Sie unter Ausstellen und Verwalten von Zertifikaten im AWS -Certificate-Manager-Benutzerhandbuch.

   > **Note**
   >
   > Das Zertifikat muss den benutzerdefinierten Endpunktnamen haben und sich in demselben Konto wie Ihre OpenSearch Service-Domain befinden. Der Zertifikatsstatus sollte AUSGESTELLT sein.

   - Befolgen Sie die restlichen Schritte, um Ihre Domäne zu erstellen und wählen Sie Erstellen aus.

- Wählen Sie die Domäne aus, wenn die Verarbeitung abgeschlossen ist, um Ihren benutzerdefinierten Endpunkt anzuzeigen.

Um die CLI oder die Konfigurations-API zu verwenden, nutzen Sie die `CreateDomain`- und `UpdateDomainConfig`-Operationen. Weitere Informationen finden Sie in der AWS CLI Befehlsreferenz und der Amazon OpenSearch Service API-Referenz.

Benutzerdefinierte Endpunkte für vorhandene Domänen

Um einer vorhandenen OpenSearch Service-Domain einen benutzerdefinierten Endpunkt hinzuzufügen, wählen Sie Bearbeiten und führen Sie die obigen Schritte 2 bis 4 aus.

Nächste Schritte

Nachdem Sie einen benutzerdefinierten Endpunkt für Ihre OpenSearch Service-Domain aktiviert haben, können Sie eine CNAME-Zuordnung in Amazon Route 53 (oder Ihrem bevorzugten DNS-Dienstanbieter) erstellen. Durch die Erstellung einer CNAME-Zuordnung können Sie den Datenverkehr an Ihren benutzerdefinierten Endpunkt und dessen Subdomänen weiterleiten. Ohne diese Zuordnung können Sie den Datenverkehr nicht an Ihren benutzerdefinierten Endpunkt weiterleiten. Schritte zum Erstellen dieser Zuordnung in Route 53 finden Sie unter Konfiguration von DNS-Routing für eine neue Domain und Erstellen einer neuen Hosting-Zone für eine Subdomain. Weitere Anbieter finden Sie in der entsprechenden Dokumentation.

Erstellen Sie einen CNAME-Eintrag, der den benutzerdefinierten Endpunkt auf den automatisch generierten Domänenendpunkt verweist. Wenn es sich bei Ihrer Domain um einen Dual-Stack handelt, können Sie Ihren CNAME-Eintrag auf einen der beiden vom Dienst generierten Endpunkte verweisen. Die Dual-Stack-Fähigkeit Ihres benutzerdefinierten Endpunkts hängt von dem vom Dienst generierten Endpunkt ab, auf den Sie den CNAME-Eintrag verweisen. Der benutzerdefinierte Endpunkt-Hostname ist der Name des CNAME-Datensatzes und der Hostname des Domain-Endpunkts ist der Wert des CNAME-Datensatzes.

Wenn Sie die SAML-Authentifizierung für OpenSearch Dashboards verwenden, müssen Sie Ihren IdP mit der neuen SSO-URL aktualisieren.

Sie können Amazon Route 53 verwenden, um einen Alias-Eintragstyp zu erstellen, der den benutzerdefinierten Endpunkt Ihrer Domain auf einen Dual-Stack-Suchendpunkt verweist. Um einen Alias-Eintragstyp zu erstellen, müssen Sie Ihre Domain so konfigurieren, dass sie den Dual-Stack-IP-Adresstyp verwendet. Sie können dies mithilfe der Route 53-API tun.

Um mithilfe der Route 53-API einen Alias-Datensatztyp zu erstellen, geben Sie das Alias-Ziel Ihrer Domain an. Sie finden das Alias-Ziel Ihrer Domain im Feld Hosted Zone (Dual Stack) im Abschnitt „Benutzerdefinierter Endpunkt“ der OpenSearch Service-Konsole oder indem Sie die `DescribeDomain` API verwenden und den Wert von kopieren`DomainEndpointV2HostedZoneId`.

Auto-Tune für Amazon Service OpenSearch

Auto-Tune in Amazon OpenSearch Service verwendet Leistungs- und Nutzungsmetriken aus Ihrem OpenSearch Cluster, um speicherbezogene Konfigurationsänderungen vorzuschlagen, einschließlich Warteschlangen- und Cachegrößen sowie Einstellungen für Java Virtual Machine (JVM) auf Ihren Knoten. Diese optionalen Änderungen verbessern die Clustergeschwindigkeit und -stabilität.

Einige Änderungen werden sofort implementiert, während andere außerhalb der Spitzenzeiten Ihrer Domain geplant sind. Sie können jederzeit zu den standardmäßigen OpenSearch Serviceeinstellungen zurückkehren. Während Auto-Tune Leistungskennzahlen für Ihre Domain sammelt und analysiert, können Sie die zugehörigen Empfehlungen in der OpenSearch Servicekonsole auf der Seite Benachrichtigungen einsehen.

Auto-Tune ist kommerziell für Domains verfügbar, AWS-Regionen auf denen eine beliebige OpenSearch Version oder Elasticsearch 6.7 oder höher mit einem unterstützten Instanztyp ausgeführt wird.

Themen

Änderungsarten

Die automatische Optimierung hat zwei große Kategorien von Änderungen:

- Unterbrechungsfreie Änderungen, die bei der Ausführung des Clusters vorgenommen werden.
- Änderungen, für die eine blaue/grüne Bereitstellung erforderlich ist, die dann angewendet wird, wenn die Domain nicht in Spitzenzeiten arbeitet.

Basierend auf den Leistungsmetriken Ihrer Domain kann die automatische Optimierung Anpassungen an den folgenden Einstellungen vorschlagen:

Änderungstyp	Kategorie	Beschreibung
JVM-Heap-Größe	Blau/Grün	Standardmäßig verwendet OpenSearch Service 50% des RAM einer Instanz für den JVM-Heap, bis zu einer Heap-Größe von 32 GiB. Wenn Sie diesen Prozentsatz erhöhen, erhalten OpenSearch Sie mehr Speicher, es bleibt jedoch weniger für das Betriebssystem und andere Prozesse übrig. Größere Werte können die Anzahl der Garbage-Collection-Pausen verringern, aber die Länge dieser Pausen erhöhen.
JVM-Einstellungen für junge Generation	Blau/Grün	JVM-„junge Generation“-Einstellungen beeinflussen die Häufigkeit von kleineren Garbage Collections. Häufigere kleinere Sammlungen können die Anzahl der großen Sammlungen und Pausen verringern.
Warteschlangengröße	Unterbrechungsfrei	Standardmäßig ist die Größe der Suchwarteschlange `1000` und die Größe der Schreibwarteschlange `10000`. Die automatische Optimierung skaliert automatisch die Such- und Schreibwarteschlangen, wenn zusätzlicher Heap zur Bearbeitung von Anforderungen verfügbar ist.
Cache-Größe	Unterbrechungsfrei	Die Feld-Cache überwacht Datenstrukturen auf Heap. Daher ist es wichtig, die Verwendung des Caches zu überwachen. Die automatische Optimierung skaliert die Größe des Felddaten-Caches, um Probleme mit dem Arbeitsspeicher und dem Leistungsschalter zu vermeiden. Die Shard-Anforderungs-Cache wird auf Knotenebene verwaltet und hat eine standardmäßige maximale Größe von 1 % des Heaps. Die automatische Optimierung skaliert die Größe des Shard-Anforderungscaches, um mehr Such- und Indexanforderungen zu

Änderungstyp	Kategorie	Beschreibung
		akzeptieren, als das, was der konfigurierte Cluster verarbeiten kann.
Anforderungsgröße	Unterbrechungsfrei	Wenn die aggregierte Größe der laufenden Anfragen 10% der gesamten JVM übersteigt (2% für `t2` Instance-Typen und 1% für`t3.small`), werden standardmäßig alle neuen `_search` AND-Anfragen OpenSearch gedrosselt, bis die vorhandenen `_bulk` Anfragen abgeschlossen sind. Die automatische Optimierung optimiert diesen Schwellenwert automatisch, normalerweise zwischen 5 und 15 %, basierend auf der Menge an JVM, die derzeit auf dem System belegt ist. Wenn beispielsweise der JVM-Speicherdruck hoch ist, kann Auto-Tune den Schwellenwert auf 5 % reduzieren und sie erhalten dann möglicherweise mehr Ablehnungen, bis sich der Cluster stabilisiert hat und der Schwellenwert steigt.

Aktivieren oder Deaktivieren der automatischen Optimierung

OpenSearch Der Service aktiviert Auto-Tune standardmäßig für neue Domänen. Um Auto-Tune für bestehende Domains zu aktivieren oder zu deaktivieren, empfehlen wir die Verwendung der Konsole, was den Vorgang vereinfacht. Aktivieren der automatischen Optimierung verursacht keine Blau/Grün-Bereitstellung.

Sie können die automatische Optimierung derzeit mit AWS CloudFormation nicht aktivieren oder deaktivieren.

Konsole

Um Auto-Tune auf einer vorhandenen Domain zu aktivieren

1. Öffnen Sie die Amazon OpenSearch Service-Konsole unter https://console.aws.amazon.com/aos/home.
2. Wählen Sie im Navigationsbereich unter Domains den Domainnamen aus, um die Cluster-Konfiguration zu öffnen.

3. Wählen Sie Einschalten, falls Auto-Tune noch nicht aktiviert ist.
4. Wählen Sie optional Zeitfenster außerhalb der Spitzenzeiten aus, um Optimierungen zu planen, die eine blaue/grüne Bereitstellung während des für die Domain konfigurierten Zeitfensters außerhalb der Spitzenzeiten erfordern. Weitere Informationen finden Sie unter the section called “Planung von Verbesserungen bei Auto-Tune”.
5. Wählen Sie Save Changes (Änderungen speichern).

CLI

Um Auto-Tune mit dem zu aktivieren, senden Sie eine AnfrageAWS CLI: UpdateDomainConfig

```
aws opensearch update-domain-config \
  --domain-name my-domain \
  --auto-tune-options DesiredState=ENABLED
```

Planung von Verbesserungen bei Auto-Tune

Vor dem 16. Februar 2023 nutzte Auto-Tune Wartungsfenster, um Änderungen zu planen, die eine blaue/grüne Implementierung erforderten. Wartungsfenster werden jetzt nicht mehr unterstützt, sondern das Zeitfenster außerhalb der Spitzenzeiten. Dabei handelt es sich um einen täglichen Zeitblock von 10 Stunden, in dem Ihre Domain in der Regel wenig Traffic verzeichnet. Sie können die Standardstartzeit für das Fenster außerhalb der Spitzenzeiten ändern, aber Sie können die Länge nicht ändern.

Alle Domains, für die Auto-Tune-Wartungsfenster vor der Einführung von Zeitfenstern außerhalb der Spitzenzeiten am 16. Februar 2023 aktiviert waren, können ältere Wartungsfenster weiterhin ohne Unterbrechung verwenden. Wir empfehlen Ihnen jedoch, Ihre bestehenden Domains zu migrieren, um stattdessen das Zeitfenster außerhalb der Spitzenzeiten für die Domainwartung zu nutzen. Detaillierte Anweisungen finden Sie unter the section called “Migrieren von Wartungsfenstern zur automatischen Optimierung”.

Konsole

Um Auto-Tune-Aktionen außerhalb der Spitzenzeiten zu planen

1. Öffnen Sie die Amazon OpenSearch Service-Konsole unter https://console.aws.amazon.com/aos/home.

2. Wählen Sie im Navigationsbereich unter Domains den Domainnamen aus, um die Cluster-Konfiguration zu öffnen.
3. Gehen Sie zur Registerkarte Auto-Tune und wählen Sie Bearbeiten aus.
4. Wählen Sie Einschalten, falls Auto-Tune noch nicht aktiviert ist.
5. Wählen Sie unter Optimierungen außerhalb der Spitzenzeiten planen die Option Zeitfenster außerhalb der Spitzenzeiten aus.
6. Wählen Sie Änderungen speichern aus.

CLI

Um Ihre Domain so zu konfigurieren, dass Auto-Tune-Aktionen während des konfigurierten Zeitfensters außerhalb der Spitzenzeiten geplant werden, fügen Sie der Anfrage Folgendes bei: `UseOffPeakWindow` UpdateDomainConfig

```
aws opensearch update-domain-config \
  --domain-name my-domain \
  --auto-tune-options
 DesiredState=ENABLED,UseOffPeakWindow=true,MaintenanceSchedules=null
```

Überwachen von Auto-Tune-Änderungen

Sie können Auto-Tune-Statistiken in überwachen. Amazon CloudWatch Eine vollständige Liste der Metriken finden Sie unter the section called “Metriken automatisch abstimmen”.

OpenSearch Der Service sendet Auto-Tune-Ereignisse an Amazon. EventBridge Sie können Regeln konfigurieren EventBridge , die beim Empfang eines Ereignisses eine E-Mail senden oder eine bestimmte Aktion ausführen. Informationen zum Format der einzelnen Auto-Tune-Ereignisse, an die gesendet wurden EventBridge, finden Sie unterthe section called “Automatische Optimierung von Ereignissen”.

Markieren von Amazon- OpenSearch Service-Domains

Mit Tags können Sie einer Amazon- OpenSearch Service-Domäne beliebige Informationen zuweisen, damit Sie diese Informationen kategorisieren und filtern können. Ein Tag ist ein Schlüssel-Wert-Paar, das Sie definieren und einer - OpenSearch Service-Domain zuordnen. Sie können diese Tags verwenden, um Kosten zu verfolgen, indem Sie Ausgaben für ähnlich markierte Ressourcen

gruppieren. AWS wendet keine semantische Bedeutung auf Ihre Tags an. Tags werden streng als Zeichenfolgen interpretiert. Alle Tags haben die folgenden Elemente:

Tag-Element	Beschreibung	Erforderlich
Tag-Schlüssel	Der Tag-Schlüssel ist der Name des Markierungen. Der Schlüssel muss für die OpenSearch Service-Domain, an die er angefügt ist, eindeutig sein. Eine Liste der grundlegenden Einschränkungen auf Tag-Schlüsseln und -Werten finden Sie unter Einschränkungen benutzerdefinierter Tags.	Ja
Tag-Wert	Der Tag-Wert ist der Zeichenfolgenwert des Tags. Tag-Werte können `null` sein und müssen in einem Tag-Satz nicht einzigartig sein. Sie können beispielsweise über ein Schlüssel-Wert-Paar in einem Tag-Satz "Projekt/Trinity" und "Kostenstelle/Trinity" verfügen. Eine Liste der grundlegenden Einschränkungen auf Tag-Schlüsseln und -Werten finden Sie unter Einschränkungen benutzerdefinierter Tags.	Nein

Jede OpenSearch Service-Domain hat einen Tag-Satz, der alle Tags enthält, die dieser OpenSearch Service-Domain zugewiesen sind. weist OpenSearch Service- AWS Domains nicht automatisch Tags zu. Ein Tag-Satz kann zwischen 0 und 50 Tags enthalten. Wenn Sie einer Domäne einen Tag mit demselben Schlüssel wie ein vorhandenes Tag hinzufügen, wird der alte Wert vom neuen Wert überschrieben.

Tag-Beispiel

Sie können einen Schlüssel verwenden, um eine Kategorie zu definieren, und der Wert könnte ein Element in dieser Kategorie sein. Sie könnten beispielsweise einen Tag-Schlüssel von `project` und einen Tag-Wert von definieren`Salix`, was darauf hinweist, dass die OpenSearch Service-Domain dem Salix-Projekt zugewiesen ist. Sie können auch Tags verwenden, um OpenSearch Service-Domains so zu kennzeichnen, dass sie für Tests oder Produktion verwendet werden, indem Sie einen Schlüssel wie `environment=test` oder verwenden`environment=production`. Versuchen Sie, einen konsistenten Satz von Tag-Schlüsseln zu verwenden, um die Nachverfolgung von Metadaten zu erleichtern, die mit OpenSearch Service-Domains verknüpft sind.

Sie können auch Tags verwenden, um Ihre AWS Rechnung so zu organisieren, dass sie Ihrer eigenen Kostenstruktur entspricht. Melden Sie sich dazu an, um Ihre AWS-Konto Rechnung mit Tag-Schlüsselwerten zu erhalten. Um dann die Kosten kombinierter Ressourcen anzuzeigen, organisieren Sie Ihre Fakturierungsinformationen nach Ressourcen mit gleichen Tag-Schlüsselwerten. Sie können beispielsweise mehrere OpenSearch Service-Domains mit Schlüssel-Wert-Paaren markieren und dann Ihre Abrechnungsinformationen so organisieren, dass die Gesamtkosten für jede Domain über mehrere Services hinweg angezeigt werden. Weitere Informationen finden Sie unter Verwendung von Kostenzuordnungs-Tags in der AWS -Fakturierungs- und Kostenverwaltungs-Dokumentation.

> **Note**
>
> Tags werden für Autorisierungszwecke im Cache gespeichert. Aus diesem Grund können Ergänzungen und Aktualisierungen von Tags in OpenSearch Service-Domains einige Minuten dauern, bis sie verfügbar sind.

Arbeiten mit Tags (Konsole)

Die Konsole ist die einfachste Möglichkeit, eine Domäne zu markieren.

So erstellen Sie ein Tag (Konsole)

1. Rufen Sie die Webseite https://aws.amazon.com auf und klicken Sie dann auf Sign In to the Console (Bei der Konsole anmelden).
2. Wählen Sie unter Analyse die Option Amazon OpenSearch Service aus.
3. Wählen Sie die Domäne aus, zu der Sie Tags hinzufügen möchten und gehen Sie zur Registerkarte Tags.
4. Wählen Sie Verwalten und neues Tag hinzufügen.
5. Geben Sie einen Tag-Schlüssel und einen optionalen Wert ein.
6. Wählen Sie Speichern.

Um ein Tag zu löschen, führen Sie die gleichen Schritte aus und wählen Sie Entfernen auf der Seite Tags verwalten.

Weitere Informationen zur Verwendung der Konsole für die Arbeit mit Tags finden Sie unter Tag Editor im AWS Handbuch „Erste Schritte“ der Managementkonsole.

Arbeiten mit Tags (AWS CLI)

Sie können Ressourcen-Tags mithilfe der AWS CLI mit dem --add-tags Befehl erstellen.

Syntax

```
add-tags --arn=<domain_arn> --tag-list Key=<key>,Value=<value>
```

Parameter	Beschreibung
`--arn`	Amazon-Ressourcenname für die OpenSearch Service-Domäne, an die das Tag angefügt ist.
`--tag-list`	Satz an durch Leerzeichen getrennten Schlüssel-Wert-Paaren im folgendem Format: `Key=<key>,Value=<value>`

Beispiel

Im folgenden Beispiel werden zwei Tags für die logs-Domäne erstellt:

```
aws opensearch add-tags --arn arn:aws:es:us-east-1:379931976431:domain/logs --tag-list
 Key=service,Value=OpenSearch Key=instances,Value=m3.2xlarge
```

Sie können Tags aus einer - OpenSearch Service-Domain mit dem --remove-tags Befehl entfernen.

Syntax

```
remove-tags --arn=<domain_arn> --tag-keys Key=<key>,Value=<value>
```

Parameter	Beschreibung
`--arn`	Amazon-Ressourcenname (ARN) für die OpenSearch Service-D omäne, an die das Tag angefügt ist.
`--tag-keys`	Satz von durch Leerzeichen getrennten Schlüssel-Wert-Paaren, die Sie aus der OpenSearch Service-Domain entfernen möchten.

Beispiel

Das folgende Beispiel entfernt zwei Tags aus der logs-Domäne, die im vorherigen Beispiel erstellt wurden:

```
aws opensearch remove-tags --arn arn:aws:es:us-east-1:379931976431:domain/logs --tag-keys service instances
```

Sie können die vorhandenen Tags für eine - OpenSearch Service-Domain mit dem --list-tags Befehl anzeigen:

Syntax

```
list-tags --arn=<domain_arn>
```

Parameter	Beschreibung
`--arn`	Amazon-Ressourcenname (ARN) für die OpenSearch Service-Domäne, an die die Tags angefügt sind.

Beispiel

Im folgenden Beispiel werden alle Ressourcen-Tags für die logs-Domäne aufgelistet:

```
aws opensearch list-tags --arn arn:aws:es:us-east-1:379931976431:domain/logs
```

Arbeiten mit Tags (AWS SDKs)

Die - AWS SDKs (außer den Android- und iOS-SDKs) unterstützen alle in der Amazon- OpenSearch Service-API-Referenz definierten Aktionen, einschließlich der `RemoveTags` Operationen `ListTags`, und `AddTags`. Weitere Informationen zur Installation und Verwendung der AWS SDKs finden Sie unter AWS Software Development Kits.

Python

In diesem Beispiel wird der OpenSearchService Low-Level-Python-Client aus dem AWS SDK for Python (Boto) verwendet, um einer Domain ein Tag hinzuzufügen, das an die Domain angehängte Tag aufzulisten und ein Tag aus der Domain zu entfernen. Sie müssen Werte für `DOMAIN_ARN`, `TAG_KEY` und `TAG_VALUE` angeben.

```
import boto3
```

```
from botocore.config import Config  # import configuration

DOMAIN_ARN = ''  # ARN for the domain. i.e "arn:aws:es:us-east-1:123456789012:domain/
my-domain
TAG_KEY = ''  # The name of the tag key. i.e 'Smileyface'
TAG_VALUE = ''  # The value assigned to the tag. i.e 'Practicetag'

# defines the configurations parameters such as region

my_config = Config(region_name='us-east-1')
client = boto3.client('opensearch', config=my_config)


# defines the client variable

def addTags():
    """Adds tags to the domain"""

    response = client.add_tags(ARN=DOMAIN_ARN,
                               TagList=[{'Key': TAG_KEY,
                                         'Value': TAG_VALUE}])

    print(response)


def listTags():
    """List tags that have been added to the domain"""

    response = client.list_tags(ARN=DOMAIN_ARN)
    print(response)


def removeTags():
    """Remove tags that have been added to the domain"""

    response = client.remove_tags(ARN=DOMAIN_ARN, TagKeys=[TAG_KEY])

    print('Tag removed')
    return response
```

Durchführung administrativer Aktionen auf Amazon OpenSearch Service-Domains

Amazon OpenSearch Service bietet mehrere Verwaltungsoptionen, mit denen Sie detailliert steuern können, ob Sie Probleme mit Ihrer Domain beheben müssen. Zu diesen Optionen gehören die Möglichkeit, den OpenSearch Prozess auf einem Datenknoten neu zu starten, und die Möglichkeit, einen Datenknoten neu zu starten.

OpenSearch Der Service überwacht die Integritätsparameter des Knotens und ergreift bei Anomalien Korrekturmaßnahmen, um die Domänen stabil zu halten. Mit den administrativen Optionen zum Neustarten des OpenSearch Prozesses auf einem Knoten und zum Neustarten eines Knotens selbst haben Sie die Kontrolle über einige dieser Abhilfemaßnahmen.

Sie können das AWS Management Console AWS CLI, oder das AWS SDK verwenden, um diese Aktionen durchzuführen. In den folgenden Abschnitten wird beschrieben, wie Sie diese Aktionen mit der Konsole ausführen.

Starten Sie den OpenSearch Prozess auf einem Knoten neu

Um den OpenSearch Prozess auf einem Knoten neu zu starten

1. Navigieren Sie zur OpenSearch Servicekonsole unterhttps://console.aws.amazon.com/aos/.
2. Wählen Sie im linken Navigationsbereich die Option Domains aus. Wählen Sie den Namen der Domain, mit der Sie arbeiten möchten.
3. Nachdem die Seite mit den Domänendetails geöffnet wurde, navigieren Sie zur Registerkarte Instanzstatus.
4. Wählen Sie unter Datenknoten die Schaltfläche neben dem Knoten aus, auf dem Sie den Prozess neu starten möchten.
5. Wählen Sie das Drop-down-Menü Aktionen aus und wählen Sie Restart OpenSearch / Elasticsearch-Prozess aus.
6. Wählen Sie im Modal die Option Bestätigen aus.
7. Um den Status der von Ihnen initiierten Aktion zu sehen, wählen Sie den Namen des Knotens aus. Nachdem die Seite mit den Knotendetails geöffnet wurde, wählen Sie unter dem Namen des Knotens die Registerkarte Ereignisse aus, um eine Liste der mit diesem Knoten verknüpften Ereignisse anzuzeigen.

Starten Sie einen Datenknoten neu

Um einen Datenknoten neu zu starten

1. Navigieren Sie zur OpenSearch Servicekonsole unterhttps://console.aws.amazon.com/aos/.
2. Wählen Sie im linken Navigationsbereich die Option Domains aus. Wählen Sie den Namen der Domain, mit der Sie arbeiten möchten.
3. Nachdem die Seite mit den Domänendetails geöffnet wurde, navigieren Sie zur Registerkarte Instanzstatus.
4. Wählen Sie unter Datenknoten die Schaltfläche neben dem Knoten aus, auf dem Sie den Prozess neu starten möchten.
5. Wählen Sie das Drop-down-Menü Aktionen aus und wählen Sie Knoten neu starten aus.
6. Wählen Sie im Modal die Option Bestätigen aus.
7. Um den Status der von Ihnen initiierten Aktion zu sehen, wählen Sie den Namen des Knotens aus. Nachdem die Seite mit den Knotendetails geöffnet wurde, wählen Sie unter dem Namen des Knotens die Registerkarte Ereignisse aus, um eine Liste der mit diesem Knoten verknüpften Ereignisse anzuzeigen.

Starten Sie das Dashboard oder den Kibana-Prozess auf einem Knoten neu

Um den Dashboard- oder Kibana-Prozess auf einem Knoten neu zu starten

1. Navigieren Sie zur OpenSearch Servicekonsole unterhttps://console.aws.amazon.com/aos/.
2. Wählen Sie im linken Navigationsbereich die Option Domains aus. Wählen Sie den Namen der Domain, mit der Sie arbeiten möchten.
3. Nachdem die Seite mit den Domänendetails geöffnet wurde, navigieren Sie zur Registerkarte Instanzstatus.
4. Wählen Sie unter Datenknoten die Schaltfläche neben dem Knoten aus, auf dem Sie den Prozess neu starten möchten.
5. Wählen Sie das Drop-down-Menü Aktionen aus und wählen Sie Dashboard/Kibana-Prozess neu starten aus.
6. Wählen Sie im Modal die Option Bestätigen aus.
7. Um den Status der von Ihnen initiierten Aktion zu sehen, wählen Sie den Namen des Knotens aus. Nachdem die Seite mit den Knotendetails geöffnet wurde, wählen Sie unter dem Namen

des Knotens die Registerkarte Ereignisse aus, um eine Liste der mit diesem Knoten verknüpften Ereignisse anzuzeigen.

Einschränkungen

Für Verwaltungsoptionen gelten die folgenden Einschränkungen:

- Verwaltungsoptionen werden auf Elasticsearch-Versionen 7.x und höher unterstützt.
- Administrative Optionen unterstützen keine Domains mit Multi-AZ und aktiviertem Standby.
- Der OpenSearch Neustart des Elasticsearch-Prozesses und der Neustart des Datenknotens werden auf Domains mit drei oder mehr Datenknoten unterstützt.
- Die Prozessunterstützung für Dashboards und Kibana wird auf Domains mit zwei oder mehr Datenknoten unterstützt.
- Um den OpenSearch Prozess auf einem Knoten neu zu starten oder einen Knoten neu zu starten, darf sich die Domain nicht im roten Status befinden und für alle Indizes müssen Replikate konfiguriert sein.

Arbeiten mit direkten Anfragen von Amazon OpenSearch Service mit Amazon S3

Sie können direkte Abfragen von Amazon OpenSearch Service verwenden, um Daten in Amazon S3 abzufragen. Amazon OpenSearch Service bietet eine direkte Abfrageintegration mit Amazon S3, um Betriebsprotokolle in Amazon S3 und Data Lakes auf Basis von Amazon S3 zu analysieren, ohne zwischen Diensten wechseln zu müssen. Sie können jetzt Daten in Cloud-Objektspeichern analysieren und gleichzeitig die Betriebsanalysen und Visualisierungen von Service nutzen. OpenSearch

Mit direkten Abfragen mit Amazon S3 müssen Sie keine komplexen ETL-Pipelines mehr aufbauen und müssen keine Kosten mehr tragen, Daten sowohl im OpenSearch Service- als auch im Amazon S3 S3-Speicher zu duplizieren. Sie können auch Integrationen gängiger Protokollvorlagen installieren, die vordefinierte Dashboards enthalten, und Datenbeschleunigungen konfigurieren, die auf diesen Protokolltyp zugeschnitten sind. Die Vorlagen umfassen VPC Flow Logs, AWS CloudTrail Logs und Amazon S3 S3-Logs. Zu den Beschleunigungen gehören das Überspringen von Indizes, materialisierten Ansichten und abgedeckten Indizes.

Themen

Preisgestaltung

Sie zahlen für bestehende OpenSearch Service- und Amazon S3 S3-Ressourcen, die zur Erstellung und Verarbeitung direkter Abfragen verwendet werden. Abfragen, die an Amazon S3 gesendet

werden, verwenden fakturierbare Rechenleistung und werden als OpenSearch Compute Units (OCUs) pro Stunde angezeigt.

Es gibt zwei Arten von direkten Abfragen mit Amazon S3: interaktive Abfragen und beschleunigte Abfragen. Interaktive Abfragen führen Analysen Ihrer Daten in Amazon S3 durch. Wenn Sie eine neue Abfrage ausführen, startet OpenSearch Service eine neue Sitzung, die mindestens drei Minuten dauert. OpenSearch Der Dienst hält die Sitzung aktiv, um sicherzustellen, dass nachfolgende Abfragen schnell ausgeführt werden. Beschleunigungsabfragen verwenden Compute, um Indizes im OpenSearch Service zu verwalten. Diese Abfragen dauern in der Regel länger, da sie unterschiedliche Datenmengen in OpenSearch Service aufnehmen, sodass interaktive Abfragen schneller ausgeführt werden können.

Weitere Informationen finden Sie unter Amazon OpenSearch Service Pricing.

Einschränkungen

Die folgenden Einschränkungen gelten für direkte OpenSearch Serviceanfragen mit Amazon S3.

- Ihre OpenSearch Domain muss Version 2.13 oder höher sein, um direkte OpenSearch Service-Anfragen zu unterstützen.
- Auf OpenSearch Serverless nicht verfügbar.
- Ihre OpenSearch Domain und AWS Glue Data Catalog müssen sich in derselben AWS-Konto befinden. Ihr Amazon S3 S3-Bucket kann sich in einem anderen Konto befinden (erfordert, dass die Bedingung zu Ihrer IAM-Richtlinie hinzugefügt wird), muss sich jedoch in derselben Domain befinden AWS-Region wie Ihre Domain.
- Einige Datentypen werden nicht unterstützt. Die unterstützten Datentypen sind auf Parquet, CSV und JSON beschränkt.
- OpenSearch Service Direct-Abfragen mit Amazon S3 unterstützen nur Spark-Tabellen, die mit Query Workbench generiert wurden. In AWS Glue Data Catalog oder Athena generierte Tabellen werden vom Spark-Streaming nicht unterstützt. Dies ist erforderlich, um Beschleunigungen aufrechtzuerhalten und Indizes auf dem neuesten Stand zu halten.
- Daten müssen vor der Abfrage reduziert werden, oder Sie müssen SQL in OpenSearch Service verwenden, um Ihre verschachtelten Spalten in spezielle Spalten umzuwandeln.
- Fehlende Spalten erfordern möglicherweise die Verwendung der `COALESCE` SQL-Funktion, um Ergebnisse zurückzugeben.

- Wenn sich die Struktur Ihrer Daten ändert, sind Aktualisierungen für die AWS Glue Tabelle sowie bestehende Beschleunigungen erforderlich.
- OpenSearch Für Instance-Typen gelten je nach Instance-Typ Beschränkungen für Netzwerknutzlasten (10 v. 100).
- AWS CloudFormation Vorlagen werden noch nicht unterstützt.

Empfehlungen

Wir empfehlen Ihnen, bei der Verwendung von Direct Query wie folgt vorzugehen:

- Nehmen Sie Daten mithilfe der Partitionsformate Jahr, Monat, Tag und Stunde in Amazon S3 auf, um Abfragen zu beschleunigen.
- Verwenden Sie Limits für Ihre Abfragen, um sicherzustellen, dass Sie nicht zu viele Daten zurückholen.
- Verwenden Sie Index State Management (falls zutreffend), um Speicherplatz für materialisierte Ansichten und umfassende Indizes bereitzustellen.
- Löschen Sie Beschleunigungsjobs und Indizes, wenn sie nicht mehr benötigt werden.
- Verwenden Sie beim Erstellen von Skipping-Indizes Bloom-Filter für hohe Kardinalität und Min-/Max-Filter für große Bereiche. Es wird empfohlen, den Wertesatz für ein Feld mit hoher Kardinalität zu verwenden.
- Verwenden Sie Referenzhandbücher, um Daten nach Amazon S3 zu exportieren. Sie können AWS Logs wie CloudFrontCloudTrail, und Elastic Load Balancing verwenden.

Kontingente

Ihr Konto hat die folgenden Kontingente für direkte OpenSearch Serviceanfragen mit Amazon S3. Jedes Mal, wenn Sie eine Anfrage starten, öffnet OpenSearch Service eine Sitzung und hält sie mindestens zehn Minuten lang aufrecht. Dadurch wird die Abfragelatenz reduziert, da die Startzeit der Sitzung bei nachfolgenden Abfragen entfällt.

Beschreibung	Maximal	Kann überschreiben
Verbindungen pro Domain	10	Ja
Datenquellen pro Domain	20	Ja

Beschreibung	Maximal	Kann überschreiben
Indizes pro Domain	5	Ja
Gleichzeitige Sitzungen pro Datenquelle	10	Ja
Maximale OCU pro Abfrage	60	Ja
Maximale Ausführungszeit für Abfragen (Minuten)	30	Ja
Maximale OCUs pro Beschleunigung	20	Ja
Maximaler kurzlebiger Speicher	20	Ja

Unterstützte Regionen

Die folgenden Regionen sind für direkte OpenSearch Serviceanfragen mit Amazon S3 verfügbar: Asien-Pazifik (Hongkong), Asien-Pazifik (Mumbai), Asien-Pazifik (Seoul), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney), Asien-Pazifik (Tokio), Kanada (Zentral), Europa (Frankfurt), Europa (Irland), Europa (Stockholm), USA Ost (Nord-Virginia), USA Ost (Ohio) und USA West (Oregon).

Erstellen von Amazon OpenSearch Service-Datenquellenintegrationen mit Amazon S3

Sie können eine neue Amazon S3 S3-Direktabfrage-Datenquelle für OpenSearch Service über die AWS Management Console oder die API erstellen. Jede neue Datenquelle verwendet die, um Tabellen AWS Glue Data Catalog zu verwalten, die Amazon S3 S3-Buckets darstellen.

Themen

- Voraussetzungen
- Richten Sie eine neue Datenquelle für direkte Abfragen ein
- Ordnen Sie die AWS Glue Data Catalog Rolle zu (wenn nach dem Erstellen der Datenquelle eine detaillierte Zugriffskontrolle aktiviert ist)

- Nächste Schritte

Voraussetzungen

Bevor Sie eine Datenquelle erstellen können, benötigen Sie eine OpenSearch Domain mit Version 2.13 oder höher. Anweisungen zur Einrichtung finden Sie unterthe section called “ OpenSearch Dienstdomänen erstellen”.

Richten Sie eine neue Datenquelle für direkte Abfragen ein

Sie können eine Datenquelle für direkte Abfragen in einer Domain mit der AWS Management Console oder der Service-API einrichten. OpenSearch

AWS Management Console

1. Navigieren Sie zur Amazon OpenSearch Service-Konsole unterhttps://console.aws.amazon.com/aos/.
2. Wählen Sie im linken Navigationsbereich die Option Domains aus.
3. Wählen Sie die Domain aus, für die Sie eine neue Datenquelle einrichten möchten. Dadurch wird die Detailseite der Domain geöffnet. Wählen Sie die Registerkarte Verbindungen unter den allgemeinen Domänendetails und suchen Sie den Abschnitt Direkte Abfrage.
4. Wählen Sie Erstellen.
5. Geben Sie auf der Seite zur Erstellung der Datenquelle einen Namen für Ihre neue Datenquelle ein. Wählen Sie unter Datenquellentyp die Option Amazon S3 aus. Wählen Sie eine bestehende IAM-Rolle aus, für die Einschränkungen gelten, auf die in Amazon S3 AWS Glue Data Catalog und Amazon S3 zugegriffen werden kann.
6. Wählen Sie Erstellen. Dadurch wird der Bildschirm mit den Datenquellendetails mit einer OpenSearch Dashboard-URL geöffnet. Sie können zu dieser URL navigieren, um die nächsten Schritte abzuschließen.

OpenSearch Service-API

Verwenden Sie den AddDataSourceAPI-Vorgang, um eine neue Datenquelle in Ihrer Domain zu erstellen.

```
POST https://es.region.amazonaws.com/2021-01-01/opensearch/domain/domain-name/
dataSource
```

```
{
   "DataSourceType": {
        "s3GlueDataCatalog": {
            "RoleArn": "arn:aws:iam::account-id:role/Admin"
        }
    }
   "Description": "data-source-description",
   "Name": "my-data-source"
}
```

Die folgende Beispielrichtlinie zeigt die Berechtigungen mit den geringsten Rechten, die zum Erstellen und Verwalten einer Datenquelle erforderlich sind. Wenn Sie über umfassendere Berechtigungen verfügen, wie z. `s3:*` B. die `AdminstratorAccess` Richtlinie, umfassen diese Berechtigungen die Berechtigungen mit den geringsten Rechten in der Beispielrichtlinie.

Die Integration benötigt Zugriff, um in Amazon S3 zu schreiben und AWS Glue Data Catalog. Für Amazon S3 benötigen wir Schreibzugriff, um beim Aufbau von Beschleunigungen einen Checkpoint-Standort beizubehalten. Denn wir benötigen Schreibzugriff AWS Glue Data Catalog, um Datenbanken, Tabellen und Partitionen, die für die Integration benötigt werden, innerhalb OpenSearch von Service zu verwalten.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"HttpActionsForOpenSearchDomain",
         "Effect":"Allow",
         "Action":"es:ESHttp*",
         "Resource":"arn:aws:es:<region>:<account>:domain/<domain_name>/*"
      },
      {
         "Sid":"AmazonOpenSearchS3GlueDirectQueryReadAllS3Buckets",
         "Effect":"Allow",
         "Action":[
            "s3:GetObject",
            "s3:GetObjectVersion",
            "s3:ListBucket"
         ],
         "Condition":{
            "StringEquals":{
               "aws:ResourceAccount":"<account>"
```

```
            }
         },
         "Resource":"*"
      },
      {
         "Sid":"AmazonOpenSearchDirectQueryGlueCreateAccess",
         "Effect":"Allow",
         "Action":[
            "glue:CreateDatabase",
            "glue:CreatePartition",
            "glue:CreateTable",
            "glue:BatchCreatePartition"
         ],
         "Resource":"*"
      },
      {
         "Sid":"AmazonOpenSearchS3GlueDirectQueryModifyAllGlueResources",
         "Effect":"Allow",
         "Action":[
            "glue:DeleteDatabase",
            "glue:DeletePartition",
            "glue:DeleteTable",
            "glue:GetDatabase",
            "glue:GetDatabases",
            "glue:GetPartition",
            "glue:GetPartitions",
            "glue:GetTable",
            "glue:GetTableVersions",
            "glue:GetTables",
            "glue:UpdateDatabase",
            "glue:UpdatePartition",
            "glue:UpdateTable",
            "glue:BatchGetPartition",
            "glue:BatchDeletePartition",
            "glue:BatchDeleteTable"
         ],
         "Resource":[
            "arn:aws:glue:us-east-1:<account>:table/*",
            "arn:aws:glue:us-east-1:<account>:database/*",
            "arn:aws:glue:us-east-1:<account>catalog"
         ],
         "Condition":{
            "StringEquals":{
               "aws:ResourceAccount":"<account>"
```

```
            }
         }
      },
      {
         "Sid":"ReadAndWriteActionsForS3CheckpointBucket",
         "Effect":"Allow",
         "Action":[
            "s3:ListMultipartUploadParts",
            "s3:DeleteObject",
            "s3:GetObject",
            "s3:PutObject",
            "s3:GetBucketLocation",
            "s3:ListBucket"
         ],
         "Condition":{
            "StringEquals":{
               "aws:ResourceAccount":"<account>"
            }
         },
         "Resource":[
            "arn:aws:s3:::<checkpoint_bucket_name>",
            "arn:aws:s3:::<checkpoint_bucket_name>/*"
         ]
      }
   ]
}
```

Um Amazon S3 S3-Buckets in verschiedenen Konten zu unterstützen, müssen Sie eine Bedingung in die Amazon S3 S3-Richtlinie aufnehmen und das entsprechende Konto hinzufügen.

```
"Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{accountId}}"
                }
```

Für die Rolle muss außerdem die folgende Vertrauensrichtlinie gelten, in der die Ziel-ID angegeben ist.

```
{
    "Version":"2012-10-17",
    "Statement":[
       {
```

```
          "Effect":"Allow",
          "Principal":{
             "Service": "directquery.opensearchservice.amazonaws.com"
          },
          "Action":"sts:AssumeRole"
       }
     ]
}
```

Anweisungen zum Erstellen der Rolle finden Sie unter Erstellen einer Rolle mit benutzerdefinierten Vertrauensrichtlinien.

Wenn Sie in OpenSearch Service eine differenzierte Zugriffskontrolle aktiviert haben, wird automatisch eine neue OpenSearch differenzierte Zugriffssteuerungsrolle für Ihre Datenquelle erstellt. Der Name der neuen detaillierten Zugriffskontrollrolle lautet. `AWS OpenSearchDirectQuery <name of data source>`

Standardmäßig hat die Rolle nur Zugriff auf Datenquellenindizes für direkte Abfragen. Sie können die Rolle zwar so konfigurieren, dass der Zugriff auf Ihre Datenquelle eingeschränkt oder gewährt wird, es wird jedoch empfohlen, den Zugriff dieser Rolle nicht anzupassen. Wenn Sie die Datenquelle löschen, wird diese Rolle gelöscht. Dadurch wird allen anderen Benutzern der Zugriff entzogen, sofern sie der Rolle zugeordnet sind.

Ordnen Sie die AWS Glue Data Catalog Rolle zu (wenn nach dem Erstellen der Datenquelle eine detaillierte Zugriffskontrolle aktiviert ist)

Wenn Sie nach dem Erstellen einer Datenquelle die detaillierte Zugriffskontrolle aktiviert haben, müssen Sie Benutzer ohne Administratorrechte einer IAM-Rolle mit AWS Glue Data Catalog Zugriff zuordnen, um direkte Abfragen ausführen zu können. Gehen Sie wie folgt vor, um manuell eine `glue_access` Backend-Rolle zu erstellen, die Sie der IAM-Rolle zuordnen können:

> **Note**
>
> Indizes werden für alle Abfragen der Datenquelle verwendet. Ein Benutzer mit Lesezugriff auf den Anforderungsindex für eine bestimmte Datenquelle kann alle Abfragen für diese Datenquelle lesen. Ein Benutzer mit Lesezugriff auf den Ergebnisindex kann Ergebnisse für alle Abfragen dieser Datenquelle lesen.

1. Wählen Sie im Hauptmenü der OpenSearch Dashboards Sicherheit, Rollen und Rollen erstellen aus.
2. Nennen Sie die Rolle glue_access.
3. Wählen Sie für Clusterberechtigungen,`indices:data/write/bulk*`, `indices:data/read/scroll` aus. `indices:data/read/scroll/clear`
4. Geben Sie für Index die folgenden Indizes ein, auf die Sie dem Benutzer mit der Rolle Zugriff gewähren möchten:

   - `.query_execution_request_`*`<name of data source>`*
   - `query_execution_result_`*`<name of data source>`*
   - `flint_*`
5. Wählen Sie für Indexberechtigungen die Option aus`indices_all`.
6. Wählen Sie Erstellen.
7. Wählen Sie Zugeordnete Benutzer, Mapping verwalten.
8. Fügen Sie unter Backend-Rollen den ARN der AWS Glue Rolle hinzu, für die eine Berechtigung zum Aufrufen Ihrer Domain erforderlich ist.

   ```
   arn:aws:iam::account-id:role/role-name
   ```
9. Wählen Sie Map aus und vergewissern Sie sich, dass die Rolle unter Zugeordnete Benutzer angezeigt wird.

Weitere Informationen zum Zuordnen von Rollen finden Sie unterthe section called “Rollen an Benutzer zuweisen”.

Nächste Schritte

Nachdem Sie eine Datenquelle erstellt haben, stellt Ihnen OpenSearch Service eine OpenSearch Dashboard-URL zur Verfügung. Sie verwenden diese, um die Zugriffskontrolle zu konfigurieren, Tabellen zu definieren, protokollbasierte Dashboards für gängige Protokolltypen einzurichten und Ihre Daten abzufragen.

Konfiguration einer Datenquelle in Dashboards OpenSearch

Nachdem Sie Ihre Datenquelle erstellt haben, können Sie Sicherheitseinstellungen konfigurieren, Ihre Amazon S3 S3-Tabellen definieren oder eine beschleunigte Datenindizierung einrichten. In diesem

Abschnitt werden Sie durch verschiedene Anwendungsfälle mit Ihrer Datenquelle in OpenSearch Dashboards geführt, bevor Sie Ihre Daten abfragen.

Um die folgenden Abschnitte zu konfigurieren, müssen Sie zunächst in OpenSearch Dashboards zu Ihrer Datenquelle navigieren. Wählen Sie in der linken Navigationsleiste unter Verwaltung die Option Datenquellen aus. Wählen Sie unter Datenquellen verwalten den Namen der Datenquelle aus, die Sie in der Konsole erstellt haben.

Einrichten der Zugriffssteuerung

Suchen Sie auf der Detailseite für Ihre Datenquelle den Abschnitt Zugriffskontrollen und wählen Sie Bearbeiten aus. Wenn Sie das Sicherheits-Plugin installiert haben, wählen Sie Eingeschränkt und wählen Sie aus, welchen rollenbasierten Gruppen Sie Zugriff auf die neue Datenquelle gewähren möchten. Sie können auch Nur Administrator wählen, wenn Sie möchten, dass nur der Administrator Zugriff auf die Datenquelle hat.

> **Important**
>
> Indizes werden für alle Abfragen der Datenquelle verwendet. Ein Benutzer mit Lesezugriff auf den Anforderungsindex für eine bestimmte Datenquelle kann alle Abfragen für diese Datenquelle lesen. Ein Benutzer mit Lesezugriff auf den Ergebnisindex kann Ergebnisse für alle Abfragen dieser Datenquelle lesen.

Richten Sie Integrationen für beliebte AWS Protokolltypen ein

OpenSearch Dashboards erleichtern den schnellen Einstieg in die Verwendung gängiger Protokolltypen, die in Amazon S3 mithilfe von Rohprotokollen gespeichert sind, mit Ausnahme von Amazon VPC Flow-Protokollen, die im Parquet-Format unterstützt werden. OpenSearch Dashboards bietet Integrationen, die den Zugriff auf Ressourcen wie AWS Glue Data Catalog Tabellen, gespeicherte Abfragen und Dashboards ermöglichen. Diese Ressourcen basieren auf OpenSearch Beschleunigungen und werden nach der Installation automatisch aktualisiert. Sie können Integrationen auf der Seite mit den Datenquellendetails oder über die linke Navigationsleiste einrichten. So gehen Sie vor:

1. Wählen Sie den Protokolltyp aus, den Sie installieren möchten. Stellen Sie sicher, dass der Protokolltyp, den Sie installieren, das Amazon S3 S3-Tag hat.

2. Wählen Sie als Verbindungstyp Amazon S3 S3-Verbindung aus, falls diese noch nicht ausgewählt ist.
3. Wählen Sie den Namen der Datenquelle, auf der Sie die Integration installieren möchten, den Amazon S3 S3-Speicherort für die Daten, den Checkpoint, den Sie zur Aufrechterhaltung des Beschleunigungsindizierungsstatus verwenden möchten, und die gewünschten Ressourcen basierend auf Ihrem Anwendungsfall aus.

> **Note**
>
> Bei der Erstellung der IAM-Rolle haben Sie eine Amazon S3 S3-Ressource für einen Checkpoint angegeben, der über Schreibaktionsberechtigungen für den Checkpoint-Standort verfügt. Sie müssen auf einen Amazon S3 S3-Bucket-Standort verweisen, der Schreibzugriff für den Checkpoint-Standort hat. Wenn Sie dies nicht tun, schlagen die Beschleunigungen fehl, die durch die Integration installiert werden.

> **Note**
>
> Für die Integration von Amazon VPC Flow Log muss ein Patch mithilfe von OpenSearch Dashboards installiert werden. Es kann einige Minuten dauern, bis die Dashboards, die Sie installiert haben, gefüllt sind.

Referenzhandbücher zum Exportieren von Daten nach Amazon S3

Sie können die folgenden Referenzhandbücher verwenden, um Daten nach Amazon S3 zu exportieren:

Quellen:

- Apache Access
- CloudFront
- CloudTrail

- Elastic Load Balancing
- Amazon S3

- AWS WAF
- Amazon VPC-Ablauf
- NGINX

Erstellen Sie Spark-Tabellen mit Query Workbench

Direkte Abfragen von OpenSearch Service an Amazon S3 verwenden Spark-Tabellen innerhalb von AWS Glue Data Catalog. Sie können Tabellen in der Query Workbench erstellen, ohne die OpenSearch Dashboards verlassen zu müssen.

Um bestehende Datenbanken und Tabellen in Ihrer Datenquelle zu verwalten oder neue Tabellen zu erstellen, für die Sie direkte Abfragen verwenden möchten, wählen Sie Query Workbench aus der linken Navigationsleiste und wählen Sie die Amazon S3 S3-Datenquelle aus der Dropdownliste Datenquelle aus.

Führen Sie die folgende Abfrage aus, um eine Tabelle für in S3 gespeicherte VPC Flow-Protokolle im Parquet-Format einzurichten:

```
CREATE TABLE
datasourcename.gluedatabasename.vpclogstable (version INT, account_id STRING,
 interface_id STRING,
srcaddr STRING, dstaddr STRING, srcport INT, dstport INT, protocol INT, packets
 BIGINT,
bytes BIGINT, start BIGINT, end BIGINT, action STRING, log_status STRING,
`aws-account-id` STRING, `aws-service` STRING, `aws-region` STRING, year STRING,
month STRING, day STRING, hour STRING)

USING parquet PARTITIONED BY (aws-account-id, aws-service, aws-region, year, month,
day, hour)

LOCATION "s3://accountnum-vpcflow/AWSLogs"
```

Führen Sie nach dem Erstellen der Tabelle die folgende Abfrage aus, um sicherzustellen, dass sie mit direkten Abfragen kompatibel ist:

```
MSCK REPAIR TABLE  datasourcename.databasename.vpclogstable
```

Beschleunigte Abfragen

Wählen Sie auf der Detailseite für Ihre Datenquelle die Option Leistung beschleunigen aus. Um eine schnelle Nutzung Ihrer Daten in Amazon S3 zu gewährleisten, können Sie drei verschiedene Arten von Beschleunigungen einrichten, um Daten im OpenSearch Service zu indizieren: Überspringen von Indizes, materialisierte Ansichten und Abdecken von Indizes.

Indizes überspringen

Mit einem Skipping-Index können Sie nur die Metadaten der in Amazon S3 gespeicherten Daten indizieren. Wenn Sie eine Tabelle mit einem Übersprungindex abfragen, referenziert der Abfrageplaner den Index und schreibt die Abfrage neu, um die Daten effizient zu finden, anstatt alle Partitionen und Dateien zu scannen. Auf diese Weise kann der Übersprungindex den spezifischen Speicherort der gespeicherten Daten schnell eingrenzen.

Wählen Sie auf der Seite mit den Datenquellendetails die Option Leistung beschleunigen aus. Dort können Sie beginnen, indem Sie die Datenbank und Tabelle auswählen, die Sie beschleunigen möchten. Alternativ können Sie sich dafür entscheiden, automatisch einen Skipping-Index zu generieren. Wenn Sie Felder zur Beschleunigung lieber manuell hinzufügen möchten, können Sie dies tun, indem Sie auf die Schaltfläche Felder hinzufügen klicken. Beim Hinzufügen der Felder werden Sie gefragt, welche Art von Skipping-Index Sie hinzufügen möchten. Sie müssen aus einer der folgenden Optionen wählen:

- Partition: Verwendet Datenpartitionsdetails zum Auffinden von Daten (am besten für partitionierte Spalten wie Jahr, Monat, Tag, Stunde)
- MinMax: Verwendet die Unter- und Obergrenze der indizierten Spalte, um nach Daten zu suchen (am besten für numerische Spalten)
- ValueSet: Verwendet einen eindeutigen Wertesatz zum Auffinden von Daten (am besten für Spalten mit niedriger bis mäßiger Kardinalität, die eine exakte Übereinstimmung erfordern)
- BloomFilter: Verwendet einen Bloom-Filter, um Daten zu finden (am besten für Spalten mit hoher Kardinalität, für die keine exakte Übereinstimmung erforderlich ist)

Sie können mit Query Workbench auch manuell einen Skipping-Index für Ihre Tabelle erstellen. Wählen Sie einfach die S3-Datenquelle aus der Datenquellen-Dropdownliste aus und fügen Sie die folgende Abfrage hinzu:

```
CREATE SKIPPING INDEX
```

```
ON datasourcename.gluedatabasename.vpclogstable(
 `srcaddr` BLOOM_FILTER,
 `dstaddr` BLOOM_FILTER,
 `day` PARTITION,
 `account_id`BLOOM_FILTER
 ) WITH (
index_settings = '{"number_of_shards":5,"number_of_replicas":1}',
auto_refresh = true,
checkpoint_location = 's3://accountnum-vpcflow/AWSLogs/checkpoint'
)
```

Materialisierte Ansichten

Mit materialisierten Ansichten können Sie komplexe Abfragen wie Aggregationen verwenden, um Dashboard-Visualisierungen zu unterstützen. Materialisierte Ansichten nehmen je nach Abfrage eine kleine Menge Ihrer Daten in Servicestorage auf. OpenSearch OpenSearch Service erstellt dann aus den aufgenommenen Daten einen Index, den Sie für Visualisierungen verwenden können. Sie können den Index der materialisierten Ansicht wie the section called “Indexstatusmanagement” jeden anderen Index mit verwalten. OpenSearch

Da Sie einen Zielindex angeben, werden Sie aufgefordert, dem Index einen Namen zu geben und das Watermark Delay hinzuzufügen, das festlegt, wie spät Daten eingehen und trotzdem verarbeitet werden können.

Verwenden Sie die folgende Abfrage, um eine neue materialisierte Ansicht für die VPC-Flow-Logtabelle zu erstellen, die Sie in erstellt haben: the section called “Erstellen Sie Spark-Tabellen mit Query Workbench”

```
CREATE MATERIALIZED VIEW {table_name}__week_live_mview AS
  SELECT
    cloud.account_uid AS `aws.vpc.cloud_account_uid`,
    cloud.region AS `aws.vpc.cloud_region`,
    cloud.zone AS `aws.vpc.cloud_zone`,
    cloud.provider AS `aws.vpc.cloud_provider`,

    CAST(IFNULL(src_endpoint.port, 0) AS LONG) AS `aws.vpc.srcport`,
    CAST(IFNULL(src_endpoint.svc_name, 'Unknown') AS STRING)  AS `aws.vpc.pkt-src-aws-
service`,
    CAST(IFNULL(src_endpoint.ip, '0.0.0.0') AS STRING)  AS `aws.vpc.srcaddr`,
    CAST(IFNULL(src_endpoint.interface_uid, 'Unknown') AS STRING)  AS `aws.vpc.src-
interface_uid`,
    CAST(IFNULL(src_endpoint.vpc_uid, 'Unknown') AS STRING)  AS `aws.vpc.src-vpc_uid`,
```

```
    CAST(IFNULL(src_endpoint.instance_uid, 'Unknown') AS STRING)  AS `aws.vpc.src-
instance_uid`,
    CAST(IFNULL(src_endpoint.subnet_uid, 'Unknown') AS STRING)  AS `aws.vpc.src-
subnet_uid`,

    CAST(IFNULL(dst_endpoint.port, 0) AS LONG) AS `aws.vpc.dstport`,
    CAST(IFNULL(dst_endpoint.svc_name, 'Unknown') AS STRING) AS `aws.vpc.pkt-dst-aws-
service`,
    CAST(IFNULL(dst_endpoint.ip, '0.0.0.0') AS STRING)  AS `aws.vpc.dstaddr`,
    CAST(IFNULL(dst_endpoint.interface_uid, 'Unknown') AS STRING)  AS `aws.vpc.dst-
interface_uid`,
    CAST(IFNULL(dst_endpoint.vpc_uid, 'Unknown') AS STRING)  AS `aws.vpc.dst-vpc_uid`,
    CAST(IFNULL(dst_endpoint.instance_uid, 'Unknown') AS STRING)  AS `aws.vpc.dst-
instance_uid`,
    CAST(IFNULL(dst_endpoint.subnet_uid, 'Unknown') AS STRING)  AS `aws.vpc.dst-
subnet_uid`,
    CASE
      WHEN regexp(dst_endpoint.ip, '(10\\..*)|(192\\.168\\..*)|(172\\.1[6-9]\\..*)|
(172\\.2[0-9]\\..*)|(172\\.3[0-1]\\.*)')
        THEN 'ingress'
      ELSE 'egress'
      END AS `aws.vpc.flow-direction`,

    CAST(IFNULL(connection_info['protocol_num'], 0) AS INT) AS
 `aws.vpc.connection.protocol_num`,
    CAST(IFNULL(connection_info['tcp_flags'], '0') AS STRING)  AS
 `aws.vpc.connection.tcp_flags`,
    CAST(IFNULL(connection_info['protocol_ver'], '0') AS STRING)  AS
 `aws.vpc.connection.protocol_ver`,
    CAST(IFNULL(connection_info['boundary'], 'Unknown') AS STRING)  AS
 `aws.vpc.connection.boundary`,
    CAST(IFNULL(connection_info['direction'], 'Unknown') AS STRING)  AS
 `aws.vpc.connection.direction`,

    CAST(IFNULL(traffic.packets, 0) AS LONG) AS `aws.vpc.packets`,
    CAST(IFNULL(traffic.bytes, 0) AS LONG) AS `aws.vpc.bytes`,

    CAST(FROM_UNIXTIME(time / 1000) AS TIMESTAMP) AS `@timestamp`,
    CAST(FROM_UNIXTIME(start_time / 1000) AS TIMESTAMP) AS `start_time`,
    CAST(FROM_UNIXTIME(start_time / 1000) AS TIMESTAMP) AS `interval_start_time`,
    CAST(FROM_UNIXTIME(end_time / 1000) AS TIMESTAMP) AS `end_time`,
    status_code AS `aws.vpc.status_code`,

    severity AS `aws.vpc.severity`,
```

```
    class_name AS `aws.vpc.class_name`,
    category_name AS `aws.vpc.category_name`,
    activity_name AS `aws.vpc.activity_name`,
    disposition AS `aws.vpc.disposition`,
    type_name AS `aws.vpc.type_name`,

    region AS `aws.vpc.region`,
    accountid AS `aws.vpc.account-id`
  FROM
  datasourcename.gluedatabasename.vpclogstable
WITH (
  auto_refresh = true,
  refresh_interval = '15 Minute',
  checkpoint_location = 's3://accountnum-vpcflow/AWSLogs/checkpoint',
  watermark_delay = '1 Minute',
)
```

Indizes abdecken

Mit einem Deckindex können Sie Daten aus einer bestimmten Spalte in einer Tabelle aufnehmen. Dies ist der leistungsstärkste der drei Indexierungstypen. Da OpenSearch Service alle Daten aus der gewünschten Spalte aufnimmt, erzielen Sie eine bessere Leistung und können erweiterte Analysen durchführen.

Genau wie bei materialisierten Ansichten erstellt OpenSearch Service einen neuen Index aus den umfassenden Indexdaten. Sie können diesen neuen Index für Dashboard-Visualisierungen und andere OpenSearch Servicefunktionen wie Anomalieerkennung oder Geodatenfunktionen verwenden. Sie können den Index der Deckungsansicht mit verwaltenthe section called “Indexstatusmanagement”, genauso wie mit jedem anderen Index. OpenSearch

Verwenden Sie die folgende Abfrage, um einen neuen Covering-Index für die VPC-Flow-Log-Tabelle zu erstellen, die Sie in the section called “Erstellen Sie Spark-Tabellen mit Query Workbench” erstellt haben:

```
CREATE INDEX vpc_covering_index
ON datasourcename.gluedatabasename.vpclogstable (version, account_id, interface_id,
srcaddr, dstaddr, srcport, dstport, protocol, packets,
bytes, start, action, log_status STRING,
`aws-account-id`, `aws-service`, `aws-region`, year,
month, day, hour )
WITH (
  auto_refresh = true,
```

```
  refresh_interval = '15 minute',
  checkpoint_location = 's3://accountnum-vpcflow/AWSLogs/checkpoint'
)
```

Daten in Dashboards abfragen OpenSearch

Nachdem Sie Ihre Tabellen eingerichtet und die gewünschte optionale Abfragebeschleunigung konfiguriert haben, können Sie nun mit der Analyse Ihrer Daten beginnen. Um Ihre Daten abzufragen, wählen Sie die Datenquelle aus dem Dropdownmenü auf der Discover-Seite oder der Observability-Seite in OpenSearch Dashboards aus.

Wenn Sie einen Skipping-Index verwenden oder noch keinen Index erstellt haben, können Sie SQL oder Piped Processing Language (PPL) verwenden, um Ihre Daten abzufragen. Wenn Sie eine materialisierte Ansicht oder einen umfassenden Index konfiguriert haben, verfügen Sie bereits über einen Index und können die Dashboards Query Language (DQL) in allen Dashboards verwenden. Sie können PPL auch mit dem Observability-Plugin und SQL mit dem Query Workbench-Plugin verwenden. Derzeit unterstützen nur die Observability- und Query Workbench-Plugins PPL und SQL. Informationen zum Abfragen von Daten mithilfe der OpenSearch Service-API finden Sie in der Async-API-Dokumentation.

SQL

Verwenden Sie die folgende Abfrage, um eine SQL-Beispielabfrage für die VPC-Flow-Logtabelle auszuführen, die Sie in the section called “Erstellen Sie Spark-Tabellen mit Query Workbench” erstellt haben:

```
SELECT srcaddr, SUM (CAST(bytes AS LONG)) as total_bytes
 FROM datasourcename.gluedatabasename.vpclogstable GROUP BY srcaddrORDER BY total_bytes
 DESCLIMIT 10;
```

PPL

Verwenden Sie die folgenden Abfragen, um PPL-Beispielabfragen für die VPC-Protokolltabelle auszuführen, die Sie in erstellt haben: the section called “Erstellen Sie Spark-Tabellen mit Query Workbench”

```
source = datasourcename.gluedatabasename.vpclogstable | fields account_id, srcaddr,
 dstaddr, action | head 10
```

Empfehlungen

Es kann vorkommen, dass die Ergebnisse nicht wie erwartet zurückgegeben werden. Wenn Sie Probleme haben, empfehlen wir Ihnen, die folgenden Maßnahmen zu ergreifen:

- `SELECT*` Anweisungen liefern keine Ergebnisse — überprüfen Sie Ihre Tabelle, um zu sehen, ob sie verschachtelte Struc-Spalten enthält, die aufgelöst werden müssen.
- Wenn Sie mehrere Tabellen auswählen, verwenden Sie die `SQL UNION` Anweisung, um auf mehrere Tabellen zu verweisen.
- Beschleunigungen sind so eingestellt, dass eine bestimmte Anzahl von Workern für die Ausführung einer Abfrage verwendet wird. Wenn Abfragen langsam zurückkehren, können Sie manuell mehr Worker für die Ausführung von Abfragen zuweisen, um die Leistung zu erhöhen.
- Verwenden Sie beim Erstellen von Skipping-Indizes Bloom-Filter für hohe Kardinalität und Min-/Max-Filter für große Bereiche, um Platz in der Domäne zu sparen. Es wird empfohlen, den Wert auf ein Feld mit moderater Kardinalität festzulegen, wenn Sie eine exakte Übereinstimmung erzielen möchten.
- Weitere Informationen zu häufig verwendeten SQL-Abfragen finden Sie unter AWS Service Logs.

Eine Datenquelle verwalten

Die Verwaltung Ihrer Datenquelle ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von Datenquellen für direkte Abfragen und Ihrer anderen AWS Lösungen. AWS stellt die folgenden Tools bereit, um Fehler zu überwachen, zu melden und gegebenenfalls automatische Maßnahmen zu ergreifen.

Themen

- Überwachung mit CloudWatch Metrik-Datenquellen
- Datenquellen aktivieren und deaktivieren
- Überwachung mit Budget AWS
- Löschen einer Amazon OpenSearch Service-Datenquelle mit Amazon S3

Überwachung mit CloudWatch Metrik-Datenquellen

Sie können die Direktabfrage überwachen mit CloudWatch. CloudWatch sammelt Rohdaten und verarbeitet sie zu lesbaren Metriken, die nahezu in Echtzeit verfügbar sind. Diese Statistiken werden

15 Monate gespeichert, damit Sie auf Verlaufsinformationen zugreifen können und einen besseren Überblick darüber erhalten, wie Ihre Webanwendung oder der Service ausgeführt werden.

Sie können auch Alarme einrichten, um bestimmte Schwellenwerte zu überwachen und Benachrichtigungen zu senden oder Maßnahmen zu ergreifen, wenn diese Schwellenwerte erreicht werden. Weitere Informationen finden Sie unter Was ist Amazon CloudWatch.

Direct Query meldet die folgenden Messwerte:

Metrik	Beschreibung
AsyncQueryCreateAPI	Die Gesamtzahl der Anfragen, die an die API gestellt wurden, um asynchrone Abfragen zu erstellen. Relevante Statistiken: Durchschnitt, Maximum, Summe Abmessungen:`ClientId`, `DomainName` Frequenz: 60 Sekunden
AsyncQueryGetApiRequestCount	Die Gesamtzahl der Anfragen an die API zum Abrufen asynchroner Abfrageergebnisse. Relevante Statistiken: Durchschnitt, Maximum, Summe Abmessungen:`ClientId`, `DomainName` Frequenz: 60 Sekunden
AsyncQueryCancelApiRequestCount	Die Gesamtzahl der Anfragen, die an die API gestellt wurden, um asynchrone Abfragen abzubrechen. Relevante Statistiken: Durchschnitt, Maximum, Summe Abmessungen:`ClientId`, `DomainName`

Metrik	Beschreibung
	Frequenz: 60 Sekunden
Ein syncQueryGet ApiFailed RequestCusErrCount	Die Anzahl der fehlgeschlagenen Anfragen beim Abrufen asynchroner Abfrageergebnisse aufgrund von kundenbezogenen Fehlern (z. B. ungültige Abfrage-ID). Relevante Statistiken: Durchschnitt, Maximum, Summe Abmessungen:`ClientId`, `DomainName` Frequenz: 60 Sekunden
AsyncQueryCancelApiFailedRequestCusErrCount	Die Anzahl der fehlgeschlagenen Anfragen beim Abrufen asynchroner Abfrageergebnisse aufgrund von kundenbezogenen Fehlern (z. B. ungültige Abfrage-ID). Relevante Statistiken: Durchschnitt, Maximum, Summe Abmessungen:`ClientId`, `DomainName` Frequenz: 60 Sekunden
AsyncQueryCancelApiFailedRequestSysErrCount	Die Anzahl der fehlgeschlagenen Anfragen bei der Erstellung asynchroner Abfragen aufgrund von kundenbezogenen Fehlern. Relevante Statistiken: Durchschnitt, Maximum, Summe Abmessungen:, `ClientId` `DomainName` Frequenz: 60 Sekunden

Metrik	Beschreibung
Ein syncQueryGet ApiFailed RequestSysErrCount	Die Anzahl der fehlgeschlagenen Anfragen beim Abrufen asynchroner Abfrageergebnisse aufgrund systembedingter Fehler. Relevante Statistiken: Durchschnitt, Maximum, Summe Abmessungen:, `ClientId` `DomainName` Frequenz: 60 Sekunden

Datenquellen aktivieren und deaktivieren

Für Situationen, in denen Sie die Verwendung von Direktabfragen für eine Datenquelle beenden möchten, können Sie sich dafür entscheiden, die Datenquelle zu deaktivieren. Durch das Deaktivieren einer Datenquelle wird die Ausführung vorhandener Abfragen abgeschlossen und die Ausführung aller neuen Abfragen durch den Benutzer gestoppt.

Die Einrichtung von Beschleunigungen zur Steigerung der Abfrageleistung, wie z. B. das Überspringen von Indizes, materialisierten Ansichten und das Abdecken von Indizes, wird auf manuell gesetzt, sobald eine Datenquelle deaktiviert wird. Sobald eine Datenquelle nach der Deaktivierung auf aktiv gesetzt wurde, werden Benutzerabfragen wie erwartet ausgeführt. Beschleunigungen, die zuvor eingerichtet und auf manuell eingestellt waren, müssen manuell konfiguriert werden, damit sie wieder nach einem Zeitplan ausgeführt werden.

Überwachung mit Budget AWS

Amazon OpenSearch Service füllt OCU-Nutzungsdaten auf Kontoebene in den Cost Explorer von Billing and Cost Management ein. Kunden können die OCU-Nutzung auf Kontoebene abrechnen und Schwellenwerte sowie Warnmeldungen festlegen, wenn Schwellenwerte überschritten werden.

Das Format des Verwendungstyps, nach dem im Cost Explorer gefiltert werden soll, sieht wie folgt aus: DirectQuery OCU (RegionCodeOCU-Stunden). Kunden, die benachrichtigt werden möchten, wenn die DirectQuery OCU-Nutzung (OCU-Hours) ihren Schwellenwert erreicht, können ein AWS Budgets-Konto erstellen und eine Warnung konfigurieren, die auf dem von ihnen festgelegten Schwellenwert basiert. Optional können Kunden ein Amazon SNS SNS-Thema einrichten, das eine Datenquelle abschaltet, falls ein Schwellenwertkriterium erfüllt wird.

> **Note**
>
> Die Nutzungsdaten in AWS Budgets sind nicht in Echtzeit verfügbar und können sich um bis zu 8 Stunden verzögern.

Löschen einer Amazon OpenSearch Service-Datenquelle mit Amazon S3

Wenn Sie eine Datenquelle löschen, entfernt Amazon OpenSearch Service sie aus Ihrer Domain. OpenSearch Service entfernt auch Indizes, die mit der Datenquelle verknüpft sind. Ihre Transaktionsdaten werden nicht aus Amazon S3 gelöscht, aber Amazon S3 sendet keine neuen Daten an OpenSearch Service.

Sie können eine Datenquellenintegration mithilfe der AWS Management Console oder der OpenSearch Service-API löschen.

AWS Management Console

So löschen Sie eine Datenquelle:

1. Navigieren Sie zur Amazon OpenSearch Service-Konsole unterhttps://console.aws.amazon.com/aos/.
2. Wählen Sie im linken Navigationsbereich Domains aus.
3. Wählen Sie die Domäne aus, für die Sie eine Datenquelle löschen möchten. Dadurch wird die Detailseite der Domain geöffnet. Wählen Sie die Registerkarte Verbindungen unter den allgemeinen Informationen und suchen Sie den Abschnitt Direkte Abfrage.
4. Wählen Sie die Datenquelle aus, die Sie löschen möchten, wählen Sie Löschen und bestätigen Sie den Löschvorgang.

OpenSearch Service-API

Verwenden Sie den DeleteDataSourceAPI-Vorgang, um eine vorhandene Datenquelle in Ihrer Domain zu löschen.

```
POST https://es.region.amazonaws.com/2021-01-01/opensearch/domain/domain-name/
dataSource/data-source-name
```

Überwachen von Amazon OpenSearch Service Domänen Domänen

Überwachung ist wichtig, um die Zuverlässigkeit, Verfügbarkeit und Leistung von Amazon OpenSearch Service und Ihren anderen AWS -Lösungen aufrechtzuerhalten. AWSstellt die folgenden Überwachungswerkzeuge zur Verfügung, mit denen Sie OpenSearch Service-Ressourcen überwachen, Missstände melden können:

Amazon CloudWatch

Amazon CloudWatch überwacht Ihre OpenSearch Serviceressourcen in Echtzeit. Sie können Metriken erfassen und verfolgen, benutzerdefinierte Dashboards erstellen und Alarme festlegen, die Sie benachrichtigen oder Maßnahmen ergreifen, wenn eine Metrik einen bestimmten Schwellenwert erreicht. Weitere Informationen finden Sie im Benutzerhandbuch für Amazon Benutzerhandbuch für Amazon Benutzerhandbuch für Amazon CloudWatch Benutzerhandbuch für Amazon Benutzerhandbuch für Amazon Benutzerhandbuch

CloudWatchAmazon-Protokolle

Mit Amazon CloudWatch Logs können Sie Ihre OpenSearch Protokolldateien überwachen, speichern und darauf zugreifen. CloudWatchLogs überwacht die Informationen in Protokolldateien und kann Sie benachrichtigen, wenn bestimmte Schwellenwerte erreicht werden. Weitere Informationen finden Sie im Amazon Logs-Benutzerhandbuch für Amazon Logs Benutzerhandbuch für Amazon CloudWatch Logs Benutzerhandbuch für Amazon Logs

Amazon EventBridge

Amazon EventBridge liefert nahezu in Echtzeit einen Strom von Systemereignissen, die Änderungen in Ihren OpenSearch Service Domänen beschreiben. Sie können Regeln erstellen, die bestimmte Ereignisse überwachen und automatisierte Aktionen in anderen AWS-Services auslösen, wenn diese Ereignisse auftreten. Weitere Informationen finden Sie im Benutzerhandbuch für Amazon Benutzerhandbuch für Amazon Benutzerhandbuch für Amazon EventBridge Benutzerhandbuch für Amazon Benutzerhandbuch für Amazon Benutzerhandbuch

AWS CloudTrail

AWS CloudTrailerfasst Konfigurations-API-Aufrufe an OpenSearch Service als Ereignisse. Es kann diese Ereignisse an einen von Ihnen angegebenen Amazon-S3-Bucket übermitteln. Anhand dieser Informationen können Sie feststellen, welche Benutzer und Konten Anfragen

gestellt haben, die Quell-IP-Adresse, von der die Anfragen gestellt wurden und wann die Anfragen aufgetreten sind. Weitere Informationen finden Sie im AWS CloudTrail-Benutzerhandbuch.

Themen

Überwachung von OpenSearch Cluster-Metriken mit Amazon CloudWatch

Amazon OpenSearch Service veröffentlicht Daten von Ihren Domains bei Amazon CloudWatch. CloudWatch ermöglicht es Ihnen, Statistiken über diese Datenpunkte in Form eines geordneten Satzes von Zeitreihendaten, den so genannten Metriken, abzurufen. OpenSearch Der Service sendet die meisten Messwerte CloudWatch in 60-Sekunden-Intervallen an. Wenn Sie universelle oder magnetische EBS-Volumes verwenden, werden die EBS-Volume-Metriken nur alle fünf Minuten aktualisiert. Alle kumulativen Metriken (z. `ThreadpoolWriteRejeceted` B.`ThreadpoolSearchRejected`) befinden sich im Arbeitsspeicher und verlieren ihren Status. Metriken werden bei einem Node-Drop, einem Node-Bounce, einem Node-Austausch und einer Blau/Grün-Implementierung zurückgesetzt. Weitere Informationen zu Amazon CloudWatch finden Sie im CloudWatch Amazon-Benutzerhandbuch.

Die OpenSearch Servicekonsole zeigt eine Reihe von Diagrammen an, die auf den Rohdaten von basieren CloudWatch. Je nach Ihren Anforderungen ziehen Sie es möglicherweise vor, die Clusterdaten CloudWatch anstelle der Diagramme in der Konsole anzuzeigen. Der Service archiviert die Metriken für zwei Wochen, bevor sie verworfen werden. Die Metriken werden ohne Aufpreis zur Verfügung gestellt, es fallen CloudWatch jedoch Gebühren für die Erstellung von Dashboards und Alarmen an. Weitere Informationen finden Sie unter CloudWatchAmazon-Preise.

OpenSearch Service veröffentlicht die folgenden Kennzahlen für CloudWatch:

- the section called “Cluster-Metriken”
- the section called “Dedizierte Hauptknoten-Metriken”

- the section called “EBS-Volume-Metriken”
- the section called “Instance-Metriken”
- the section called “UltraWarm Metriken”
- the section called “Cold-Storage-Metriken”
- the section called “Warnungsmetriken”
- the section called “Metriken zur Anomalieerkennung”
- the section called “Asynchrone Suchmetriken”
- the section called “SQL-Metriken”
- the section called “k-NN-Metriken”
- the section called “Metriken für Cluster-übergreifende Suchen”
- the section called “Cluster-übergreifende Replikationsmetriken”
- the section called “Learning-to-Rank-Metriken”
- the section called “Metriken für Piped Processing Language”

Metriken anzeigen in CloudWatch

CloudWatch Metriken werden zuerst nach dem Service-Namespace und dann nach den verschiedenen Dimensionskombinationen innerhalb der einzelnen Namespaces gruppiert.

Um Metriken mit der Konsole anzuzeigen CloudWatch

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Suchen Sie im linken Navigationsbereich nach Metrics (Metriken) und wählen Sie All metrics (Alle Metriken) aus. Wählen Sie den ES/ OpenSearchService Namespace aus.
3. Wählen Sie eine Dimension aus, um die entsprechenden Metriken anzuzeigen. Metriken für einzelne Knoten befinden sich in der `ClientId, DomainName, NodeId`-Dimension. Cluster-Metriken befinden sich in der `Per-Domain, Per-Client Metrics`-Dimension. Einige Knotenmetriken werden auf Clusterebene aggregiert und somit in beide Dimensionen eingeschlossen. Shard-Metriken befinden sich in der `ClientId, DomainName, NodeId, ShardRole`-Dimension.

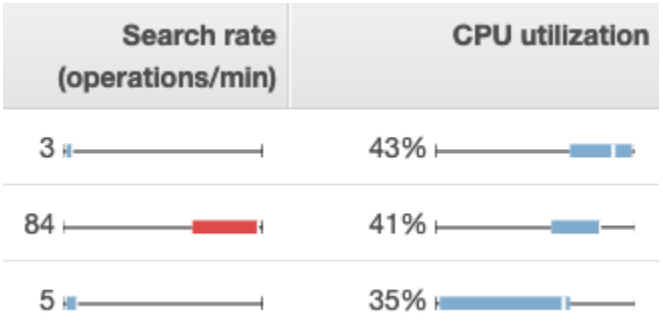
Um eine Liste von Metriken anzuzeigen, verwenden Sie AWS CLI

Führen Sie den folgenden Befehl aus:

```
aws cloudwatch list-metrics --namespace "AWS/ES"
```

Interpretieren von Zustandstabellen im OpenSearch Service

Verwenden Sie die Registerkarten Clusterstatus und Instanzstatus, um Metriken in OpenSearch Service anzuzeigen. Die Registerkarte Instanzstatus verwendet Boxdiagramme, um einen at-a-glance Überblick über den Zustand der einzelnen OpenSearch Knoten zu geben:



- Jedes farbige Feld zeigt den Wertebereich für den Knoten im angegebenen Zeitraum.
- Blaue Felder stehen für Werte, die mit anderen Knoten konsistent sind. Rote Felder stellen Ausreißer dar.
- Die weiße Linie innerhalb der einzelnen Felder zeigt den aktuellen Wert des Knotens.
- Die "Whisker" auf beiden Seiten jedes Feldes zeigen die minimalen und maximalen Werte für alle Knoten über den Zeitraum.

Wenn Sie Änderungen an der Konfiguration Ihrer Domain vornehmen, verdoppelt sich häufig die Größe der Liste mit den einzelnen Instances auf den Registerkarten Cluster health (Cluster-Zustand) und Instance health (Instance-Zustand) für einen kurzen Zeitraum, bevor wieder die richtige Zahl angezeigt wird. Eine Erklärung dieser Verhaltensweise finden Sie unter the section called “Konfigurationsänderungen”.

Cluster-Metriken

Amazon OpenSearch Service bietet die folgenden Metriken für Cluster.

Metrik	Beschreibung
`ClusterStatus.green`	Ein Wert von 1 gibt an, dass alle Index-Shards zu Knoten im Cluster zugeordnet sind.

Metrik	Beschreibung
	Relevante Statistiken: Maximum
`ClusterStatus.yellow`	Ein Wert von 1 bedeutet, dass die primären Shards für alle Indizes den Knoten im Cluster zugewiesen sind, die Replikat-Shards für mindestens einen Index jedoch nicht. Weitere Informationen finden Sie unter the section called “Gelber Cluster-Status”. Relevante Statistiken: Maximum
`ClusterStatus.red`	Ein Wert von 1 gibt an, dass die Primär- und Replikat-Shards für mindestens einen Index keinen Knoten im Cluster zugeordnet sind. Weitere Informationen finden Sie unter the section called “Roter Cluster-Status”. Relevante Statistiken: Maximum
`Shards.active`	Die Gesamtzahl der aktiven primären und Replikat-Shards. Relevante Statistiken: Maximum, Summe
`Shards.unassigned`	Die Anzahl der Shards, die Knoten im Cluster nicht zugeordnet sind. Relevante Statistiken: Maximum, Summe
`Shards.delayedUnassigned`	Die Anzahl der Shards, deren Knotenzuordnung durch die Timeout-Einstellungen verzögert wurde. Relevante Statistiken: Maximum, Summe
`Shards.activePrimary`	Die Anzahl der aktiven primären Shards. Relevante Statistiken: Maximum, Summe
`Shards.initializing`	Die Anzahl der Shards, die derzeit initialisiert werden. Relevante Statistiken: Summe

Metrik	Beschreibung
`Shards.relocating`	Die Anzahl der Shards, die derzeit verschoben werden. Relevante Statistiken: Summe
`Nodes`	Die Anzahl der Knoten im OpenSearch Service-Cluster, einschließlich dedizierter Master-Knoten und UltraWarm Knoten. Weitere Informationen finden Sie unter the section called “Konfigurationsänderungen”. Relevante Statistiken: Maximum
`SearchableDocuments`	Die Gesamtzahl der durchsuchbaren Dokumente in allen Datenknoten im Cluster. Relevante Statistiken: Minimum, Maximum, Durchschnitt
`DeletedDocuments`	Die Gesamtzahl der zum Löschen markierten Dokumente in allen Datenknoten im Cluster. Diese Dokumente erscheinen nicht mehr in den Suchergebnissen, sondern entfernen OpenSearch nur gelöschte Dokumente bei der Segmentzusammenführung von der Festplatte. Diese Metrik steigt nach Löschanfragen und sinkt nach Segmentzusammenführungen. Relevante Statistiken: Minimum, Maximum, Durchschnitt
`CPUUtilization`	Der Prozentsatz der CPU-Nutzung für Datenknoten im Cluster. „Maximum“ zeigt den Knoten mit der höchsten CPU-Nutzung an. „Average“ (Durchschnitt) stellt alle Knoten im Cluster dar. Diese Metrik ist auch für einzelne Knoten verfügbar. Relevante Statistiken: Maximum, Durchschnitt

Metrik	Beschreibung
`FreeStorageSpace`	Der freie Platz für Datenknoten im Cluster. `Sum` zeigt den gesamten freien Speicherplatz für den Cluster an, Sie müssen jedoch den Zeitraum bei einer Minute belassen, um einen genauen Wert zu erhalten. `Minimum` und `Maximum` zeigen die Knoten mit dem wenigsten bzw. dem meisten freien Speicherplatz an. Diese Metrik ist auch für einzelne Knoten verfügbar. OpenSearch Der Service gibt eine aus`ClusterBlockException` , wenn diese Metrik erreicht `0` ist. Zum Wiederherstellen müssen Sie entweder Indizes löschen, größere Instances hinzufügen oder EBS-basierten Speicher zu vorhandenen Instances hinzufügen. Weitere Informationen hierzu finden Sie unter the section called “Zu wenig verfügbarer Speicherplatz”. Die OpenSearch Servicekonsole zeigt diesen Wert in GiB an. Die CloudWatch Amazon-Konsole zeigt es in MiB an. **Note** `FreeStorageSpace` wird immer niedriger sein als die Werte, die die `_cat/allocation` APIs OpenSearch `_cluster/stats` und. OpenSearch Der Service reserviert einen Prozentsatz des Speicherplatzes auf jeder Instanz für interne Operationen. Weitere Informationen finden Sie unter Berechnen von Speicheranforderungen. Relevante Statistiken: Minimum, Maximum, Durchschnitt, Summe
`ClusterUsedSpace`	Der insgesamt für den Cluster verwendete Speicherplatz. Sie müssen den Zeitraum bei einer Minute belassen, um einen korrekten Wert zu erhalten. Die OpenSearch Servicekonsole zeigt diesen Wert in GiB an. Die CloudWatch Amazon-Konsole zeigt es in MiB an. Relevante Statistiken: Minimum, Maximum

Metrik	Beschreibung
`ClusterIndexWritesBlocked`	Gibt an, ob Ihr Cluster eingehende Schreibanforderungen akzeptiert oder blockiert. Ein Wert von 0 bedeutet, dass der Cluster Anforderungen akzeptiert. Ein Wert von 1 bedeutet, dass Anforderungen blockiert werden. Einige der häufigsten Faktoren sind folgende: `FreeStorageSpace` ist zu gering, oder `JVMMemoryPressure` ist zu hoch. Um dieses Problem zu lösen, sollten Sie erwägen, mehr Speicherplatz hinzuzufügen oder Ihren Cluster zu skalieren. Relevante Statistiken: Maximum
`JVMMemoryPressure`	Der maximale Prozentsatz des Java-Heaps, der für alle Datenknoten im Cluster verwendet wird. OpenSearch Der Dienst verwendet die Hälfte des RAM einer Instanz für den Java-Heap, bis zu einer Heap-Größe von 32 GiB. Sie können Instances bis zu 64 GiB RAM vertikal skalieren. Dann können Sie eine horizontale Skalierung durchführen, indem Sie Instances hinzufügen. Siehe the section called “Empfohlene CloudWatch Alarme”. Relevante Statistiken: Maximum **Note** Die Logik für diese Metrik wurde in der Service-Software R20220323 geändert. Weitere Informationen finden Sie in den Versionshinweisen.
`OldGenJVMMemoryPressure`	Der maximale Prozentsatz des Java-Heaps, der für die „alte Generation“ auf allen Datenknoten im Cluster verwendet wird. Diese Metrik ist auch auf Knotenebene verfügbar. Relevante Statistiken: Maximum

Metrik	Beschreibung
AutomatedSnapshotFailure	Die Anzahl fehlgeschlagener automatischer Snapshots für den Cluster. Der Wert 1 gibt an, dass keine automatischen Snapshots für die Domain in den vorherigen 36 Stunden erstellt wurden. Relevante Statistiken: Minimum, Maximum
CPUCreditBalance	Das verbleibende CPU-Guthaben für die Datenknoten im Cluster. Ein CPU-Guthaben stellt die Leistung eines gesamten CPU-Kerns für eine Minute zur Verfügung. Weitere Informationen finden Sie unter CPU-Guthaben im Amazon-EC2-Entwicklerhandbuch. Diese Metrik ist nur für die T2-Instance-Typen verfügbar. Relevante Statistiken: Minimum
OpenSearchDashboardsHealthyNodes	Ein Gesundheitscheck für OpenSearch Dashboards. Wenn Minimum, Maximum und Durchschnitt alle gleich 1 sind, verhalten sich Dashboards normal. Wenn Sie 10 Knoten mit einem Maximum von 1, Minimum von 0 und Durchschnitt von 0,7 haben, bedeutet dies, dass 7 Knoten (70 %) gesund und 3 Knoten (30 %) ungesund sind. Relevante Statistiken: Minimum, Maximum, Durchschnitt
OpensearchDashboardsReportingFailedRequestSysErrCount	Die Anzahl der Anfragen zur Generierung von OpenSearch Dashboard-Berichten, die aufgrund von Serverproblemen oder Funktionseinschränkungen fehlgeschlagen sind. Relevante Statistiken: Summe
OpensearchDashboardsReportingFailedRequestUserErrCount	Die Anzahl der Anfragen zur Generierung von OpenSearch Dashboards-Berichten, die aufgrund von Client-Problemen fehlgeschlagen sind. Relevante Statistiken: Summe

Metrik	Beschreibung
OpensearchDashboardsReportingRequestCount	Die Gesamtzahl der Anfragen zur Generierung von OpenSearch Dashboards-Berichten. Relevante Statistiken: Summe
OpensearchDashboardsReportingSuccessCount	Die Anzahl der erfolgreichen Anfragen zur Generierung von OpenSearch Dashboard-Berichten. Relevante Statistiken: Summe
KMSKeyError	Ein Wert von 1 gibt an, dass der AWS KMS Schlüssel, der zum Verschlüsseln von Daten im Ruhezustand verwendet wird, deaktiviert wurde. Aktivieren Sie den Schlüssel wieder, um den normalen Betrieb für die Domain wiederherzustellen. In der Konsole wird diese Metrik nur für Domains angezeigt, in denen Daten im Ruhezustand verschlüsselt werden. Relevante Statistiken: Minimum, Maximum
KMSKeyInaccessible	Der Wert 1 gibt an, dass der AWS KMS Schlüssel, der zum Verschlüsseln von Daten im Ruhezustand verwendet wurde, gelöscht wurde oder dass seine Berechtigungen für den Dienst aufgehoben wurden. OpenSearch Für Domains, die sich in diesem Zustand befinden, ist die Wiederherstellung nicht möglich. Aber wenn Sie über einen manuellen Snapshot verfügen, können Sie diesen verwenden, um die Daten der Domain zu einer neuen Domain zu migrieren. In der Konsole wird diese Metrik nur für Domains angezeigt, in denen Daten im Ruhezustand verschlüsselt werden. Relevante Statistiken: Minimum, Maximum

Metrik	Beschreibung
`InvalidHostHeaderRequests`	Die Anzahl der HTTP-Anfragen an den OpenSearch Cluster, die einen ungültigen (oder fehlenden) Host-Header enthielten. Gültige Anfragen enthalten den Domain-Hostnamen als Host-Header-Wert. OpenSearch Der Dienst lehnt ungültige Anfragen für Domänen mit öffentlichem Zugriff ab, für die es keine restriktive Zugriffsrichtlinie gibt. Wir empfehlen, auf alle Domains eine restriktive Zugriffsr ichtlinie anzuwenden. Wenn Sie große Werte für diese Metrik sehen, stellen Sie sicher, dass Ihre OpenSearch Kunden den Domain-Hostnamen (und nicht beispielsweise die IP-Adresse) in ihren Anfragen angeben. Relevante Statistiken: Summe
`OpenSearchRequests (previously ElasticsearchRequests)`	Die Anzahl der Anfragen an den OpenSearch Cluster. Relevante Statistiken: Summe
`2xx, 3xx, 4xx, 5xx`	Die Anzahl der Anforderungen an die Domain, die zum jeweiligen HTTP-Antwortcode (2xx, 3xx, 4xx, 5xx) geführt haben. Relevante Statistiken: Summe

Metrik	Beschreibung
`ThroughputThrottle`	Gibt an, ob Festplatten gedrosselt wurden oder nicht. Eine Drosselung tritt auf, wenn der kombinierte Durchsatz von `ReadThroughputMicroBursting` und höher als der maximale Durchsatz, `WriteThroughputMicroBursting` ist. `MaxProvisionedThroughput` `MaxProvisionedThroughput` ist der niedrigere Wert des Instanzdurchsatzes oder des bereitgestellten Volumendurchsatzes. Ein Wert von 1 gibt an, dass Festplatten gedrosselt wurden. Ein Wert von 0 zeigt ein normales Verhalten an. Informationen zum Instance-Durchsatz finden Sie unter Amazon EBS-optimierte Instances. Informationen zum Volumendurchsatz finden Sie unter Amazon EBS-Volumetypen. Relevante Statistiken: Minimum, Maximum
`IopsThrottle`	Gibt an, ob die Anzahl der Eingabe-/Ausgabevorgänge pro Sekunde (IOPS) in der Domain gedrosselt wurde. Eine Drosselung erfolgt, wenn die IOPS des Datenknotens die maximal zulässige Grenze des EBS-Volumes oder der EC2-Instance des Datenknotens überschreiten. Informationen zu Instance-IOPS finden Sie unter Amazon EBS-optimierte Instances. Informationen zu Volume-IOPS finden Sie unter Amazon EBS-Volumetypen. Relevante Statistiken: Minimum, Maximum

Dedizierte Hauptknoten-Metriken

Amazon OpenSearch Service bietet die folgenden Metriken für dedizierte Master-Knoten.

Metrik	Beschreibung
`MasterCPUUtilization`	Der maximale Prozentsatz der CPU-Ressourcen, die von den dedizierten Hauptknoten verwendet werden. Wir empfehlen,

Metrik	Beschreibung
	die Größe des Instance-Typs zu erhöhen, wenn diese Metrik 60 Prozent erreicht. Relevante Statistiken: Maximum
`MasterFreeStorageSpace`	Diese Metrik ist nicht relevant und kann ignoriert werden. Der Service verwendet keine Hauptknoten als Datenknoten.
`MasterJVMMemoryPressure`	Der maximale Prozentsatz des Java-Heap, der für alle dedizierten Hauptknoten im Cluster verwendet wird. Wir empfehlen die Verlagerung auf einen größeren Instance-Typen, wenn diese Metrik 85 Prozent erreicht. Relevante Statistiken: Maximum **Note** Die Logik für diese Metrik wurde in der Service-Software R20220323 geändert. Weitere Informationen finden Sie in den Versionshinweisen.
`MasterOldGenJVMMemoryPressure`	Der maximale Prozentsatz des Java-Heap pro Hauptknoten, der für die „alte Generation“ verwendet wird. Relevante Statistiken: Maximum
`MasterCPUCreditBalance`	Das verbleibende CPU-Guthaben für die dedizierte Hauptknoten im Cluster. Ein CPU-Guthaben stellt die Leistung eines gesamten CPU-Kerns für eine Minute zur Verfügung. Weitere Informationen finden Sie unter CPU-Guthaben im Amazon-EC2-Entwicklerhandbuch. Diese Metrik ist nur für die T2-Instance-Typen verfügbar. Relevante Statistiken: Minimum

Metrik	Beschreibung
`MasterReachableFromNode`	Eine Zustandsprüfung für `MasterNotDiscovered` -Ausnahmen. Ein Wert von 1 zeigt ein normales Verhalten an. Ein Wert von 0 zeigt an, dass `/_cluster/health/` fehlschlägt. Ausfälle bedeuten, dass der Master-Knoten vom Quellknoten aus nicht erreichbar ist. Sie sind normalerweise das Ergebnis eines Problems mit der Netzwerkkonnektivität oder eines AWS Abhängigkeitsproblems. Relevante Statistiken: Maximum
`MasterSysMemoryUtilization`	Der Prozentsatz des Arbeitsspeichers des Hauptknotens, der verwendet wird. Relevante Statistiken: Maximum

EBS-Volume-Metriken

Amazon OpenSearch Service bietet die folgenden Metriken für EBS-Volumes.

Metrik	Beschreibung
`ReadLatency`	Die Latenz für Lesevorgänge auf EBS-Volumes in Sekunden. Diese Metrik ist auch für einzelne Knoten verfügbar. Relevante Statistiken: Minimum, Maximum, Durchschnitt
`WriteLatency`	Die Latenz für Schreibvorgänge auf EBS-Volumes in Sekunden. Diese Metrik ist auch für einzelne Knoten verfügbar. Relevante Statistiken: Minimum, Maximum, Durchschnitt
`ReadThroughput`	Der Durchsatz für Lesevorgänge auf EBS-Volumes in Byte pro Sekunde. Diese Metrik ist auch für einzelne Knoten verfügbar. Relevante Statistiken: Minimum, Maximum, Durchschnitt

Metrik	Beschreibung
`ReadThroughputMicroBursting`	Der Durchsatz in Byte pro Sekunde für Lesevorgänge auf EBS-Volumes, wenn Micro-Bursting berücksichtigt wird. Diese Metrik ist auch für einzelne Knoten verfügbar. Micro-Bursting tritt auf, wenn ein EBS-Volume hohe IOPS- oder Durchsatzraten für deutlich kürzere Zeiträume (weniger als eine Minute) aufweist. Relevante Statistiken: Minimum, Maximum, Durchschnitt
`WriteThroughput`	Der Durchsatz für Schreibvorgänge auf EBS-Volumes in Byte pro Sekunde. Diese Metrik ist auch für einzelne Knoten verfügbar. Relevante Statistiken: Minimum, Maximum, Durchschnitt
`WriteThroughputMicroBursting`	Der Durchsatz in Byte pro Sekunde für Schreibvorgänge auf EBS-Volumes, wenn Micro-Bursting berücksichtigt wird. Diese Metrik ist auch für einzelne Knoten verfügbar. Micro-Bursting tritt auf, wenn ein EBS-Volume hohe IOPS- oder Durchsatzraten für deutlich kürzere Zeiträume (weniger als eine Minute) aufweist. Relevante Statistiken: Minimum, Maximum, Durchschnitt
`DiskQueueDepth`	Die Anzahl der ausstehenden Eingabe- und Ausgabe(I/O)-Anforderungen für ein EBS-Volume. Relevante Statistiken: Minimum, Maximum, Durchschnitt
`ReadIOPS`	Die Anzahl der Eingabe- und Ausgabe(I/O)-Vorgänge pro Sekunde für Lesevorgänge in EBS-Volumes. Diese Metrik ist auch für einzelne Knoten verfügbar. Relevante Statistiken: Minimum, Maximum, Durchschnitt

Metrik	Beschreibung
`ReadIOPSMicroBursting`	Die Anzahl der Eingabe- und Ausgabevorgänge (I/O) pro Sekunde für Lesevorgänge auf EBS-Volumes, wenn Micro-Bursting berücksichtigt wird. Diese Metrik ist auch für einzelne Knoten verfügbar. Micro-Bursting tritt auf, wenn ein EBS-Volume hohe IOPS- oder Durchsatzraten für deutlich kürzere Zeiträume (weniger als eine Minute) überbrückt. Relevante Statistiken: Minimum, Maximum, Durchschnitt
`WriteIOPS`	Die Anzahl der Eingabe- und Ausgabe(I/O)-Vorgänge pro Sekunde für Schreibvorgänge in EBS-Volumes. Diese Metrik ist auch für einzelne Knoten verfügbar. Relevante Statistiken: Minimum, Maximum, Durchschnitt
`WriteIOPSMicroBursting`	Die Anzahl der Eingabe- und Ausgabevorgänge (I/O) pro Sekunde für Schreibvorgänge auf EBS-Volumes, wenn Micro-Bursting berücksichtigt wird. Diese Metrik ist auch für einzelne Knoten verfügbar. Micro-Bursting tritt auf, wenn ein EBS-Volume hohe IOPS- oder Durchsatzraten für deutlich kürzere Zeiträume (weniger als eine Minute) übertrifft. Relevante Statistiken: Minimum, Maximum, Durchschnitt
`BurstBalance`	Der Prozentsatz der Ein- und Ausgabe (E/A)-Guthaben, die im Burst-Bucket für ein EBS-Volume verbleiben. Ein Wert von 100 bedeutet, dass das Volumen die maximale Anzahl von Credits erreicht hat. Wenn dieser Prozentsatz unter 70 % fällt, lesen Sie the section called “Niedrige EBS-Burst-Balance”. Das Burst-Balance bleibt für Domains mit GP3-Volume-Typen und Domains mit GP2-Volumes mit einer Volume-Größe von über 1.000 GiB bei 0. Relevante Statistiken: Minimum, Maximum, Durchschnitt

Instance-Metriken

Amazon OpenSearch Service bietet die folgenden Metriken für jede Instance in einer Domain. OpenSearch Service aggregiert diese Instance-Metriken auch, um einen Einblick in den allgemeinen

Zustand des Clusters zu erhalten. Sie können dieses Verhalten mithilfe der Statistik über Beispielzähler in der Konsole überprüfen. Beachten Sie, dass jede Metrik in der folgenden Tabelle relevante Statistiken für den Knoten und den Cluster enthält.

> **Important**
>
> Verschiedene Versionen von Elasticsearch nutzen unterschiedliche Threadpools für die Verarbeitung von Aufrufen der `_index`-API. Elasticsearch 1.5 und 2.3 nutzen den Index-Threadpool. Elasticsearch 5. x, 6.0 und 6.2 verwenden den Bulk-Thread-Pool. OpenSearch und Elasticsearch 6.3 und höher verwenden den Write-Thread-Pool. Derzeit enthält die OpenSearch Service-Konsole kein Diagramm für den Bulk-Thread-Pool. Verwenden Sie `GET _cluster/settings?include_defaults=true`, um die Thread-Pool- und Warteschlangengrößen für Ihren Cluster zu überprüfen.

Metrik	Beschreibung
`ConcurrentSearchRate`	Die Gesamtzahl der Suchanfragen mit gleichzeitiger Segmentsuche pro Minute für alle Shards auf einem Datenknoten. Eine einzelner Aufruf der `_search`-API gibt möglicherweise Ergebnisse von vielen unterschiedlichen Shards zurück. Befinden sich fünf dieser Shards in einem Knoten, meldet der Knoten für diese Metrik 5, auch wenn der Client nur eine Anfrage durchgeführt hat. Relevante Statistiken für Knoten: Durchschnitt Relevante Statistiken für Cluster: Durchschnitt, Maximum, Summe
`ConcurrentSearchLatency`	Der Unterschied in der Gesamtzeit in Millisekunden, die bei allen Suchen mit gleichzeitiger Segmentsuche in einem Knoten zwischen Minute N und Minute (N-1) benötigt wird. Relevante Statistiken für Knoten: Durchschnitt Relevante Statistiken für Cluster: Durchschnitt, Maximum
`IndexingLatency`	Die Differenz in Millisekunden in der Gesamtzeit aller Indizierungsvorgänge in einem Knoten zwischen Minute N und Minute (N-1).

Metrik	Beschreibung
	Relevante Statistiken für Knoten: Durchschnitt Relevante Statistiken für Cluster: Durchschnitt, Maximum
`IndexingRate`	Die Anzahl der Indizierungsvorgänge pro Minute. Ein einzelner Aufruf der `_bulk`-API, der zwei Dokumente und zwei Aktualisierungen hinzufügt, zählt als vier Vorgänge, die auf mehrere Knoten verteilt werden können. Wenn dieser Index über ein oder mehrere Replikate verfügt und sich auf einer OpenSearch Domain ohne optimierte Instances befindet, zeichnen andere Knoten im Cluster ebenfalls insgesamt vier Indizierungsvorgänge auf. Bei OpenSearch Domänen mit optimierten Instanzen zeichnen andere Knoten mit Replikaten keine Vorgänge auf. Löschungen von Dokumenten werden bei dieser Metrik nicht gezählt. Relevante Statistiken für Knoten: Durchschnitt Relevante Statistiken für Cluster: Durchschnitt, Maximum, Summe
`SearchLatency`	Der Unterschied in der Gesamtzeit in Millisekunden, die bei allen Suchen in einem Knoten zwischen Minute N und Minute (N-1) benötigt wird. Relevante Statistiken für Knoten: Durchschnitt Relevante Statistiken für Cluster: Durchschnitt, Maximum
`SearchRate`	Die Gesamtanzahl von Suchabfragen pro Minute für alle Shards in einem Datenknoten. Eine einzelner Aufruf der `_search`-API gibt möglicherweise Ergebnisse von vielen unterschiedlichen Shards zurück. Befinden sich fünf dieser Shards in einem Knoten, meldet der Knoten für diese Metrik 5, auch wenn der Client nur eine Anfrage durchgeführt hat. Relevante Statistiken für Knoten: Durchschnitt Relevante Statistiken für Cluster: Durchschnitt, Maximum, Summe

Metrik	Beschreibung
`SegmentCount`	Die Anzahl der Segmente auf einem Datenknoten. Je mehr Segmente Sie haben, desto länger dauert jede Suche. OpenSearch führt gelegentlich kleinere Segmente zu einem größeren zusammen. Relevante Statistiken für Knoten: Maximum, Durchschnitt Relevante Statistiken für Cluster: Summe, Maximum, Durchschnitt
`SysMemoryUtilization`	Der Prozentsatz des Arbeitsspeichers einer Instance, die in dem Cluster verwendet wird. Hohe Werte für diese Metrik sind normal und stellen normalerweise kein Problem mit Ihrem Cluster dar. Einen besseren Indikator für potenzielle Leistungs- und Stabilitätsprobleme finden Sie in der `JVMMemoryPressure` -Metrik. Relevante Statistiken für Knoten: Minimum, Maximum, Durchschnitt Relevante Statistiken für Cluster: Minimum, Maximum, Durchschnitt
`JVMGCYoungCollectionCount`	Die Anzahl der Ausführungen der automatischen Speicherbereinigung (Garbage Collection) "young generation". Eine stets zunehmende große Anzahl von Ausführungen ist ein normaler Aspekt bei Clustervorgängen. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe, Maximum, Durchschnitt
`JVMGCYoungCollectionTime`	Die Dauer in Millisekunden, die ein Cluster für die Ausführungen der automatischen Speicherbereinigung (Garbage Collection) „young generation“ aufgewendet hat. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe, Maximum, Durchschnitt

Metrik	Beschreibung
JVMGCOldCollectionCount	Die Anzahl der Ausführungen der automatischen Speicherbereinigung (Garbage Collection) "old generation". In einem Cluster mit genügend Ressourcen sollte diese Zahl relativ klein bleiben und selten zunehmen. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe, Maximum, Durchschnitt
JVMGCOldCollectionTime	Die Dauer in Millisekunden, die ein Cluster für die Ausführungen der automatischen Speicherbereinigung (Garbage Collection) „old generation“ aufgewendet hat. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe, Maximum, Durchschnitt
OpenSearchDashboardsConcurrentConnections	Die Anzahl der aktiven gleichzeitigen Verbindungen zu OpenSearch Dashboards. Wenn diese Zahl konstant hoch ist, sollten Sie Ihren Cluster skalieren. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe, Maximum, Durchschnitt
OpenSearchDashboardsHealthyNode	Eine Zustandsprüfung für den einzelnen OpenSearch Dashboards-Knoten. Ein Wert von 1 zeigt ein normales Verhalten an. Ein Wert von 0 zeigt an, dass auf Dashboards nicht zugegriffen werden kann. Relevante Statistiken für Knoten: Minimum Relevante Statistiken für Cluster: Minimum, Maximum, Durchschnitt

Metrik	Beschreibung
OpenSearchDashboardsHeapTotal	Die Menge des den OpenSearch Dashboards zugewiesenen Heap-Speichers in MiB. Verschiedene EC2-Instance-Typen können sich auf die genaue Speicherzuweisung auswirken. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe, Maximum, Durchschnitt
OpenSearchDashboardsHeapUsed	Die absolute Menge an Heap-Speicher, die von OpenSearch Dashboards in MiB verwendet wird. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe, Maximum, Durchschnitt
OpenSearchDashboardsHeapUtilization	Der maximale Prozentsatz des verfügbaren Heap-Speichers, der von Dashboards verwendet wird. OpenSearch Erhöht dieser Wert über 80 %, erwägen Sie eine Skalierung Ihres Clusters. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Minimum, Maximum, Durchschnitt
OpenSearchDashboardsOS1MinuteLoad	Die durchschnittliche CPU-Last von einer Minute für Dashboards. OpenSearch Die CPU-Last sollte idealerweise unter 1,00 liegen. Während temporäre Spitzen in Ordnung sind, empfehlen wir, die Größe des Instance-Typs zu erhöhen, wenn diese Metrik konsistent über 1,00 liegt. Relevante Statistiken für Knoten: Durchschnitt Relevante Statistiken für Cluster: Durchschnitt, Maximum

Metrik	Beschreibung
OpenSearchDashboardsRequestTotal	Die Gesamtzahl der HTTP-Anfragen an OpenSearch Dashboards. Wenn Ihr System langsam ist oder eine hohe Anzahl von Dashboards-Anforderungen angezeigt wird, sollten Sie die Größe des Instance-Typs erhöhen. Relevante Knoten-Statistiken: Summe Relevante Statistiken für Cluster: Summe
OpenSearchDashboardsResponseTimesMaxInMillis	Die maximale Zeit in Millisekunden, die OpenSearch Dashboards benötigen, um auf eine Anfrage zu antworten. Wenn Anforderungen konsistent lange brauchen, bis Ergebnisse zurückgegeben werden, sollten Sie die Größe des Instance-Typs erhöhen. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Maximum, Durchschnitt
SearchTaskCancelled	Die Anzahl der Stornierungen von Koordinatorknoten. Relevante Knoten-Statistiken: Summe Relevante Statistiken für Cluster: Summe
SearchShardTaskCancelled	Die Anzahl der Stornierungen von Datenknoten. Relevante Knoten-Statistiken: Summe Relevante Cluster-Statistiken: Summe,
ThreadpoolForce_mergeQueue	Die maximale Anzahl von Aufgaben in einer Warteschlange im Threadpool erzwungener Zusammenführungen. Wenn die Größe der Warteschlange gleichbleibend hoch ist, erwägen Sie eine Skalierung Ihres Clusters. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe, Maximum, Durchschnitt

Metrik	Beschreibung
ThreadpoolForce_mergeRejected	Die Anzahl abgewiesener Aufgaben im Threadpool erzwungener Zusammenführungen. Wenn die Anzahl stätig wächst, erwägen Sie eine Skalierung Ihres Clusters. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe
ThreadpoolForce_mergeThreads	Die Größe des Threadpools erzwungener Zusammenführungen. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Durchschnitt, Summe
ThreadpoolIndexQueue	Die Anzahl von Aufgaben in einer Warteschlange im Index-Threadpool. Wenn die Größe der Warteschlange gleichbleibend hoch ist, erwägen Sie eine Skalierung Ihres Clusters. Die maximale Größe der Index-Warteschlange beträgt 200. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe, Maximum, Durchschnitt
ThreadpoolIndexRejected	Die Anzahl abgewiesener Aufgaben im Index-Threadpool. Wenn die Anzahl stätig wächst, erwägen Sie eine Skalierung Ihres Clusters. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe
ThreadpoolIndexThreads	Die Größe des Index-Threadpools. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Durchschnitt, Summe

Metrik	Beschreibung
ThreadpoolSearchQueue	Die Anzahl von Aufgaben in einer Warteschlange im Such-Threadpool. Wenn die Größe der Warteschlange gleichbleibend hoch ist, erwägen Sie eine Skalierung Ihres Clusters. Die maximale Größe der Such-Warteschlange beträgt 1.000. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe, Maximum, Durchschnitt
ThreadpoolSearchRejected	Die Anzahl abgewiesener Aufgaben im Such-Threadpool. Wenn die Anzahl stätig wächst, erwägen Sie eine Skalierung Ihres Clusters. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe
ThreadpoolSearchThreads	Die Größe des Such-Threadpools. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Durchschnitt, Summe
Threadpoolsql-workerQueue	Die Anzahl von Aufgaben in einer Warteschlange im SQL-Such-Threadpool. Wenn die Größe der Warteschlange gleichbleibend hoch ist, erwägen Sie eine Skalierung Ihres Clusters. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe, Maximum, Durchschnitt
Threadpoolsql-workerRejected	Die Anzahl abgewiesener Aufgaben im SQL-Such-Threadpool. Wenn die Anzahl stätig wächst, erwägen Sie eine Skalierung Ihres Clusters. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe

Metrik	Beschreibung
`Threadpoolsql-workerThreads`	Die Größe des SQL-Such-Threadpools. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Durchschnitt, Summe
`ThreadpoolBulkQueue`	Die Anzahl von Aufgaben in einer Warteschlange im Massen-Threadpool. Wenn die Größe der Warteschlange gleichbleibend hoch ist, erwägen Sie eine Skalierung Ihres Clusters. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe, Maximum, Durchschnitt
`ThreadpoolBulkRejected`	Die Anzahl abgewiesener Aufgaben im Massen-Threadpool. Wenn die Anzahl stätig wächst, erwägen Sie eine Skalierung Ihres Clusters. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe
`ThreadpoolBulkThreads`	Die Größe des Massen-Threadpools. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Durchschnitt, Summe
`ThreadpoolIndexSearcherQueue`	Die Anzahl der Aufgaben in der Warteschlange im Thread-Pool der Indexsuche. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe, Maximum, Durchschnitt

Metrik	Beschreibung
ThreadpoolIndexSearcherRejected	Die Anzahl der abgelehnten Aufgaben im Threadpool der Indexsuche. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe
ThreadpoolIndexSearcherThreads	Die Größe des Threadpools für die Indexsuche. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Durchschnitt, Summe
ThreadpoolWriteThreads	Die Größe des Schreib-Threadpools. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Durchschnitt, Summe
ThreadpoolWriteQueue	Die Anzahl von Aufgaben in einer Warteschlange im Schreib-Threadpool. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Durchschnitt, Summe

Metrik	Beschreibung
`ThreadpoolWriteRejected`	Die Anzahl abgewiesener Aufgaben im Schreib-Threadpool. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Durchschnitt, Summe **Note** Da die Standardgröße der Schreibwarteschlange in Version 7.1 von 200 auf 10000 erhöht wurde, ist diese Metrik nicht mehr der einzige Indikator für Ablehnungen durch OpenSearch Service. Verwenden Sie die `CoordinatingWriteRejected` , `PrimaryWriteRejected` und `ReplicaWriteRejected` -Metriken, um Ablehnungen in Version 7.1 und höher zu überwachen.
`CoordinatingWriteRejected`	Die Gesamtzahl der Ablehnungen erfolgte auf dem koordinierenden Knoten aufgrund des Indexierungsdrucks seit dem letzten OpenSearch Start des Serviceprozesses. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Durchschnitt, Summe Diese Metrik ist in Version 7.1 und höher verfügbar.
`PrimaryWriteRejected`	Die Gesamtzahl der Ablehnungen auf den primären Shards ist auf den Indexierungsdruck seit dem letzten Start des Serviceprozesses zurückzuführen. OpenSearch Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Durchschnitt, Summe Diese Metrik ist in Version 7.1 und höher verfügbar.

Metrik	Beschreibung
`ReplicaWriteRejected`	Die Gesamtzahl der Ablehnungen auf den Replikat-Shards ist auf den Indexierungsdruck seit dem letzten Start des Serviceprozesses zurückzuführen. OpenSearch Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Durchschnitt, Summe Diese Metrik ist in Version 7.1 und höher verfügbar.

UltraWarm Metriken

Amazon OpenSearch Service bietet die folgenden Metriken für UltraWarmKnoten.

Metrik	Beschreibung
`WarmCPUUtilization`	Der Prozentsatz der CPU-Auslastung für UltraWarm Knoten im Cluster. „Maximum“ zeigt den Knoten mit der höchsten CPU-Nutzung an. Der Durchschnitt steht für alle UltraWarm Knoten im Cluster. Diese Metrik ist auch für einzelne UltraWarm Knoten verfügbar. Relevante Statistiken: Maximum, Durchschnitt
`WarmFreeStorageSpace`	Die Menge an Warm-Speicherplatz in MiB. Weil Amazon S3 anstelle von angeschlossenen Festplatten UltraWarm verwendet `Sum` wird, ist dies die einzig relevante Statistik. Sie müssen den Zeitraum bei einer Minute belassen, um einen korrekten Wert zu erhalten. Relevante Statistiken: Summe
`WarmSearchableDocuments`	Die Gesamtzahl der durchsuchbaren Dokumente in allen Warm-Indizes im Cluster. Sie müssen den Zeitraum bei einer Minute belassen, um einen korrekten Wert zu erhalten. Relevante Statistiken: Summe

Metrik	Beschreibung
`WarmSearchLatency`	Der Unterschied in der Gesamtzeit in Millisekunden für alle Suchanfragen UltraWarm zwischen Minute N und Minute (N-1). Relevante Statistiken für Knoten: Durchschnitt Relevante Statistiken für Cluster: Durchschnitt, Maximum
`WarmSearchRate`	Die Gesamtzahl der Suchanfragen pro Minute für alle Shards auf einem Knoten. UltraWarm Eine einzelner Aufruf der `_search`-API gibt möglicherweise Ergebnisse von vielen unterschiedlichen Shards zurück. Befinden sich fünf dieser Shards in einem Knoten, meldet der Knoten für diese Metrik 5, auch wenn der Client nur eine Anfrage durchgeführt hat. Relevante Statistiken für Knoten: Durchschnitt Relevante Statistiken für Cluster: Durchschnitt, Maximum, Summe
`WarmStorageSpaceUtilization`	Die Gesamtmenge an Warm-Speicherplatz, in MiB, die vom Cluster belegt wird. Relevante Statistiken: Maximum
`HotStorageSpaceUtilization`	Die Gesamtmenge an „Hot Storage“-Speicherplatz, die vom Cluster belegt wird. Relevante Statistiken: Maximum
`WarmSysMemoryUtilization`	Der Prozentsatz des Arbeitsspeichers des Warm-Knotens, der verwendet wird. Relevante Statistiken: Maximum
`HotToWarmMigrationQueueSize`	Die Anzahl der Indizes, die derzeit darauf warten, vom Hot- zum Warm-Speicher zu migrieren. Relevante Statistiken: Maximum

Metrik	Beschreibung
`WarmToHot Migration QueueSize`	Die Anzahl der Indizes, die derzeit darauf warten, vom Warm zum Hot Storage zu migrieren. Relevante Statistiken: Maximum
`HotToWarm Migration FailureCount`	Die Gesamtzahl der fehlgeschlagenen Hot-zu-Warm-Migrationen. Relevante Statistiken: Summe
`HotToWarm Migration ForceMerg eLatency`	Die durchschnittliche Latenz der erzwungenen Verschmelzungsphas e des Migrationsprozesses. Wenn diese Phase durchweg zu lange dauert, ziehen Sie in Betracht, `index.ultrawarm.migration.f orce_merge.max_num_segments` zu erhöhen. Relevante Statistiken: Durchschnitt
`HotToWarm Migration SnapshotL atency`	Die durchschnittliche Latenz der Snapshot-Phase des Migration sprozesses. Wenn dieser Schritt konsistent zu lange dauert, stellen Sie sicher, dass die Shards entsprechend dimensioniert und im gesamten Cluster verteilt sind. Relevante Statistiken: Durchschnitt
`HotToWarm Migration Processin gLatency`	Die durchschnittliche Latenz erfolgreicher Hot-to-Warm-Migrationen, ohne die in der Warteschlange verbrachte Zeit. Dieser Wert ist die Summe der Zeit, die benötigt wird, um die Phasen Zusammenführung zu erzwingen, Snapshot und Shard-Verlagerung des Migrationsprozesses abzuschließen. Relevante Statistiken: Durchschnitt
`HotToWarm Migration SuccessCount`	Die Gesamtzahl der erfolgreichen Hot-zu-Warm-Migrationen. Relevante Statistiken: Summe

Metrik	Beschreibung
`HotToWarmMigrationSuccessLatency`	Die durchschnittliche Latenz erfolgreicher Hot-to-Warm-Migrationen, mit der in der Warteschlange verbrachten Zeit. Relevante Statistiken: Durchschnitt
`WarmThreadpoolSearchThreads`	Die Größe des UltraWarm Such-Thread-Pools. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Durchschnitt, Summe
`WarmThreadpoolSearchRejected`	Die Anzahl der abgelehnten Aufgaben im UltraWarm Such-Thread-Pool. Wenn diese Zahl kontinuierlich zunimmt, sollten Sie erwägen, weitere UltraWarm Knoten hinzuzufügen. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe
`WarmThreadpoolSearchQueue`	Die Anzahl der Aufgaben in der Warteschlange im UltraWarm Such-Thread-Pool. Wenn die Warteschlangengröße konstant hoch ist, sollten Sie erwägen, weitere UltraWarm Knoten hinzuzufügen. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe, Maximum, Durchschnitt
`WarmJVMMemoryPressure`	Der maximale Prozentsatz des Java-Heaps, der für die UltraWarm Knoten verwendet wird. Relevante Statistiken: Maximum **Note** Die Logik für diese Metrik wurde in der Service-Software R20220323 geändert. Weitere Informationen finden Sie in den Versionshinweisen.

Metrik	Beschreibung
`WarmOldGenJVMMemoryPressure`	Der maximale Prozentsatz des Java-Heaps, der für die „alte Generation“ pro UltraWarm Knoten verwendet wird. Relevante Statistiken: Maximum
`WarmJVMGCYoungCollectionCount`	Gibt an, wie oft die Garbage-Collection der „jungen Generation“ auf UltraWarm Knoten ausgeführt wurde. Eine stets zunehmende große Anzahl von Ausführungen ist ein normaler Aspekt bei Clustervorgängen. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe, Maximum, Durchschnitt
`WarmJVMGCYoungCollectionTime`	Die Zeit in Millisekunden, die der Cluster mit der Garbage-Collection der „jungen Generation“ auf Knoten verbracht hat. UltraWarm Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe, Maximum, Durchschnitt
`WarmJVMGCOldCollectionCount`	Die Häufigkeit, mit der die Speicherbereinigung der „alten Generation“ auf Knoten ausgeführt wurde. UltraWarm In einem Cluster mit genügend Ressourcen sollte diese Zahl relativ klein bleiben und selten zunehmen. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe, Maximum, Durchschnitt
`WarmConcurrentSearchRate`	Die Gesamtzahl der Suchanfragen mit gleichzeitiger Segmentsuche pro Minute für alle Shards auf einem UltraWarm Knoten. Eine einzelner Aufruf der `_search`-API gibt möglicherweise Ergebnisse von vielen unterschiedlichen Shards zurück. Befinden sich fünf dieser Shards in einem Knoten, meldet der Knoten für diese Metrik 5, auch wenn der Client nur eine Anfrage durchgeführt hat. Relevante Statistiken für Knoten: Durchschnitt Relevante Statistiken für Cluster: Summe, Maximum, Durchschnitt

Metrik	Beschreibung
`WarmConcurrentSearchLatency`	Der Unterschied in der Gesamtzeit in Millisekunden, die bei allen Suchen mit gleichzeitiger Segmentsuche in einem UltraWarm Knoten zwischen Minute N und Minute (N-1) benötigt wird. Relevante Statistiken für Knoten: Durchschnitt Relevante Statistiken für Cluster: Maximum, Durchschnitt
`WarmThreadpoolIndexSearcherQueue`	Die Anzahl der Aufgaben in der Warteschlange im Threadpool der Indexsuche. UltraWarm Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe, Maximum, Durchschnitt
`WarmThreadpoolIndexSearcherRejected`	Die Anzahl der abgelehnten Aufgaben im Threadpool der UltraWarm Indexsuche. Relevante Statistiken für Knoten: Maximum Relevante Statistiken für Cluster: Summe
`WarmThreadpoolIndexSearcherThreads`	Die Größe des Threadpools für die UltraWarm Indexsuche. Relevante Statistiken für Knoten: Maximum Relevante Cluster-Statistiken: Summe, Durchschnitt

Cold-Storage-Metriken

Amazon OpenSearch Service bietet die folgenden Kennzahlen für Cold Storage.

Metrik	Beschreibung
`ColdStorageSpaceUtilization`	Die Gesamtmenge an Cold-Storage-Platz, in MiB, die vom Cluster belegt wird. Relevante Statistiken: Maximum

Metrik	Beschreibung
`ColdToWarmMigrationFailureCount`	Die Gesamtzahl der fehlgeschlagenen Cold-zu-Warm-Migrationen. Relevante Statistiken: Summe
`ColdToWarmMigrationLatency`	Die Zeitspanne für erfolgreiche Cold-zu-Warm-Migrationen. Relevante Statistiken: Durchschnitt
`ColdToWarmMigrationQueueSize`	Die Anzahl der Indizes, die derzeit darauf warten, vom Cold- zum Warm-Speicher zu migrieren. Relevante Statistiken: Maximum
`ColdToWarmMigrationSuccessCount`	Die Gesamtzahl der erfolgreichen Cold-zu-Warm-Migrationen. Relevante Statistiken: Summe
`WarmToColdMigrationFailureCount`	Die Gesamtzahl der fehlgeschlagenen Warm-zu-Cold-Migrationen. Relevante Statistiken: Summe
`WarmToColdMigrationLatency`	Die Zeitspanne für erfolgreiche Warm-zu-Cold-Migrationen. Relevante Statistiken: Durchschnitt
`WarmToColdMigrationQueueSize`	Die Anzahl der Indizes, die derzeit darauf warten, vom Warm zum Cold Storage zu migrieren. Relevante Statistiken: Maximum
`WarmToColdMigrationSuccessCount`	Die Gesamtzahl der erfolgreichen Warm-zu-Cold-Migrationen. Relevante Statistiken: Summe

OR1-Metriken

Amazon OpenSearch Service bietet die folgenden Metriken für OR1-Instances.

Metrik	Beschreibung
`RemoteStorageUsedSpace`	Die Gesamtmenge an Amazon S3 S3-Speicherplatz in MiB, die der Cluster verwendet. Relevante Statistiken: Summe
`RemoteStorageWriteRejected`	Die Gesamtzahl der Anfragen, die aufgrund von Remote-Speicher- und Replikationsdruck auf primären Shards abgelehnt wurden. Dies wird ab dem letzten Start des OpenSearch Serviceprozesses berechnet. Relevante Statistiken: Summe

Warnungsmetriken

Amazon OpenSearch Service bietet die folgenden Metriken für Benachrichtigungen.

Metrik	Beschreibung
`AlertingDegraded`	Ein Wert von 1 bedeutet, dass entweder der Warnungsindex rot ist, oder ein oder mehrere Knoten nicht im Zeitplan sind. Ein Wert von 0 zeigt ein normales Verhalten an. Relevante Statistiken: Maximum
`AlertingIndexExists`	Ein Wert von 1 bedeutet, dass der `.opensearch-alerting-config` -Index existiert. Ein Wert von 0 bedeutet, dass dies nicht der Fall ist. Bis Sie die Warnfunktion zum ersten Mal verwenden, bleibt dieser Wert bei 0. Relevante Statistiken: Maximum
`AlertingIndexStatus.green`	Der Zustand des Index. Ein Wert von 1 bedeutet „grün“. Der Wert 0 bedeutet, dass der Index entweder nicht existiert oder nicht grün ist. Relevante Statistiken: Maximum

Metrik	Beschreibung
`AlertingIndexStatus.red`	Der Zustand des Index. Ein Wert von 1 bedeutet „rot“. Der Wert 0 bedeutet, dass der Index entweder nicht existiert oder nicht rot ist. Relevante Statistiken: Maximum
`AlertingIndexStatus.yellow`	Der Zustand des Index. Ein Wert von 1 bedeutet „gelb“. Der Wert 0 bedeutet, dass der Index entweder nicht vorhanden ist oder nicht gelb ist. Relevante Statistiken: Maximum
`AlertingNodesNotOnSchedule`	Ein Wert von 1 bedeutet, dass einige Aufgaben nicht termingerecht ausgeführt werden. Der Wert 0 bedeutet, dass alle Alarmaufgaben termingerecht ausgeführt werden (oder dass keine Alarmaufgaben vorhanden sind). Sehen Sie in der OpenSearch Service-Konsole nach oder stellen Sie eine `_nodes/stats` Anfrage, um festzustellen, ob Knoten eine hohe Ressourcenauslastung aufweisen. Relevante Statistiken: Maximum
`AlertingNodesOnSchedule`	Ein Wert von 1 bedeutet, dass alle Alarmaufgaben termingerecht ausgeführt werden (oder dass keine Alarmaufgaben vorhanden sind). Der Wert 0 bedeutet, dass einige Aufgaben nicht termingerecht ausgeführt werden. Relevante Statistiken: Maximum
`AlertingScheduledJobEnabled`	Der Wert 1 bedeutet, dass die `opensearch.scheduled_jobs.enabled` -Clustereinstellung „true“ ist. Der Wert 0 bedeutet, dass diese „false“ ist und geplante Aufgaben deaktiviert sind. Relevante Statistiken: Maximum

Metriken zur Anomalieerkennung

Amazon OpenSearch Service bietet die folgenden Metriken für die Erkennung von Anomalien.

Metrik	Beschreibung
`ADPluginUnhealthy`	Ein Wert von 1 bedeutet, dass das Plug-in zur Anomalieerkennung nicht ordnungsgemäß funktioniert, entweder wegen einer hohen Anzahl von Fehlern oder weil einer der Indizes, die es verwendet, rot ist. Ein Wert 0 gibt an, dass das Plug-in wie erwartet funktioniert. Relevante Statistiken: Maximum
`ADExecuteRequestCount`	Die Anzahl der Anfragen zur Erkennung von Anomalien. Relevante Statistiken: Summe
`ADExecuteFailureCount`	Die Anzahl der fehlgeschlagenen Anfragen zur Erkennung von Anomalien. Relevante Statistiken: Summe
`ADHCExecuteFailureCount`	Die Anzahl der fehlgeschlagenen Anforderungen zum Erkennen von Anomalien für Detektoren mit hoher Kardinalität. Relevante Statistiken: Summe
`ADHCExecuteRequestCount`	Die Anzahl der Anforderungen zum Erkennen von Anomalien für Detektoren mit hoher Kardinalität. Relevante Statistiken: Summe
`ADAnomalyResultsIndexStatusIndexExists`	Ein Wert 1 bedeutet, dass der Index, auf den der `.opensearch-anomaly-results` -Alias verweist, vorhanden ist. Bis Sie die Funktion zur Anomalieerkennung zum ersten Mal verwenden, bleibt dieser Wert 0. Relevante Statistiken: Maximum
`ADAnomalyResultsIndexStatus.red`	Ein Wert 1 bedeutet, dass der Index, auf den der `.opensearch-anomaly-results` -Alias zeigt, rot ist. Ein Wert von 0 bedeutet, dass dies nicht der Fall ist. Bis Sie die Funktion zur Anomalieerkennung zum ersten Mal verwenden, bleibt dieser Wert 0.

Metrik	Beschreibung
	Relevante Statistiken: Maximum
ADAnomaly Detectors IndexStat usIndexExists	Ein Wert von 1 bedeutet, dass der `.opensearch-anomaly-detectors` -Index existiert. Ein Wert von 0 bedeutet, dass dies nicht der Fall ist. Bis Sie die Funktion zur Anomalieerkennung zum ersten Mal verwenden, bleibt dieser Wert 0. Relevante Statistiken: Maximum
ADAnomaly Detectors IndexStat us.red	Ein Wert von 1 bedeutet, dass der `.opensearch-anomaly-detectors` -Index rot ist. Ein Wert von 0 bedeutet, dass dies nicht der Fall ist. Bis Sie die Funktion zur Anomalieerkennung zum ersten Mal verwenden, bleibt dieser Wert 0. Relevante Statistiken: Maximum
ADModelsC heckpoint IndexStat usIndexExists	Ein Wert von 1 bedeutet, dass der `.opensearch-anomaly-checkpoints` -Index existiert. Ein Wert von 0 bedeutet, dass dies nicht der Fall ist. Bis Sie die Funktion zur Anomalieerkennung zum ersten Mal verwenden, bleibt dieser Wert 0. Relevante Statistiken: Maximum
ADModelsC heckpoint IndexStat us.red	Ein Wert von 1 bedeutet, dass der `.opensearch-anomaly-checkpoints` -Index rot ist. Ein Wert von 0 bedeutet, dass dies nicht der Fall ist. Bis Sie die Funktion zur Anomalieerkennung zum ersten Mal verwenden, bleibt dieser Wert 0. Relevante Statistiken: Maximum

Asynchrone Suchmetriken

Amazon OpenSearch Service bietet die folgenden Metriken für die asynchrone Suche.

Asynchrone Suchkoordinator-Knotenstatistik (pro Koordinator-Knoten)

Metrik	Beschreibung
`AsynchronousSearchSubmissionRate`	Die Anzahl der asynchronen Suchen, die in der letzten Minute gesendet wurden.
`AsynchronousSearchInitializedRate`	Die Anzahl der asynchronen Suchen, die in der letzten Minute initialisiert wurden.
`AsynchronousSearchRunningCurrent`	Die Anzahl der derzeit ausgeführten asynchronen Suchen.
`AsynchronousSearchCompletionRate`	Die Anzahl der asynchronen Suchen, die in der letzten Minute erfolgreich beendet wurden.
`AsynchronousSearchFailureRate`	Die Anzahl der asynchronen Suchen, die in der letzten Minute beendet wurden und fehlgeschlagen sind.
`AsynchronousSearchPersistRate`	Die Anzahl der asynchronen Suchen, die in der letzten Minute beibehalten wurden.
`AsynchronousSearchPersistFailedRate`	Die Anzahl der asynchronen Suchen, deren Beibehaltung in der letzten Minute fehlgeschlagen ist.
`AsynchronousSearchRejected`	Die Gesamtzahl der seit der Knotenbetriebszeit abgelehnten asynchronen Suchen.

Metrik	Beschreibung
`AsynchronousSearchCancelled`	Die Gesamtzahl der seit der Knotenbetriebszeit abgebrochenen asynchronen Suchen.
`AsynchronousSearchMaxRunningTime`	Die Dauer der längsten asynchronen Suche auf einem Knoten in der letzten Minute.

Asynchrone Suchcluster-Statistiken

Metrik	Beschreibung
`AsynchronousSearchStoreHealth`	Der Zustand des Speichers im anhaltenden Index (Rot/Nicht-Rot) in der letzten Minute.
`AsynchronousSearchStoreSize`	Die Größe des Systemindex über alle Shards in der letzten Minute.
`AsynchronousSearchStoredResponseCount`	Die Anzahl der gespeicherten Antworten im Systemindex in der letzten Minute.

Metriken automatisch abstimmen

Amazon OpenSearch Service bietet die folgenden Metriken für Auto-Tune.

Metrik	Beschreibung
`AutoTuneChangesHistoryHeapSize`	Die Änderungshistorie in MiB für Werte zur Optimierung der Heap-Größe.

Metrik	Beschreibung
AutoTuneChangesHistoryJVMYoungGenArgs	Die Änderungshistorie für JVM-Argumente YongGen .
AutoTuneFailed	Ein boolescher Wert, der angibt, ob die Auto-Tune-Änderung fehlgeschlagen ist.
AutoTuneSucceeded	Ein boolescher Wert, der angibt, ob die Auto-Tune-Änderung erfolgreich war.
AutoTuneValue	Der Änderungsverlauf der Warteschlange (Anzahl) und die Cache-Tunings ändern den Verlauf (in MiB) für unterbrechungsfreie Änderungen.

Multi-AZ mit Standby-Metriken

Amazon OpenSearch Service bietet die folgenden Metriken für Multi-AZ mit Standby.

Metriken auf Knotenebene für Datenknoten in aktiven Availability Zones

Metrik	Beschreibung
CPUUtilization	Der Prozentsatz der CPU-Nutzung für Datenknoten im Cluster. „Maximum“ zeigt den Knoten mit der höchsten CPU-Nutzung an. „Average“ (Durchschnitt) stellt alle Knoten im Cluster dar. Diese Metrik ist auch für einzelne Knoten verfügbar.
FreeStorageSpace	Der freie Platz für Datenknoten im Cluster. Sum zeigt den gesamten freien Speicherplatz für den Cluster an, Sie müssen jedoch den Zeitraum bei einer Minute belassen, um einen genauen Wert zu erhalten. Minimum und Maximum zeigen die Knoten mit dem wenigsten bzw. dem meisten freien Speicherplatz an. Diese Metrik ist auch für einzelne Knoten verfügbar. OpenSearch Der Service gibt eine ausClusterBlockException , wenn diese Metrik erreicht 0 ist. Zum Wiederherstellen müssen Sie entweder Indizes löschen, größere Instances hinzufügen oder EBS-basierten Speicher zu vorhandenen Instances

Metrik	Beschreibung
	hinzufügen. Weitere Informationen hierzu finden Sie unter the section called “Zu wenig verfügbarer Speicherplatz”. Die OpenSearch Servicekonsole zeigt diesen Wert in GiB an. Die CloudWatch Amazon-Konsole zeigt es in MiB an.
`JVMMemory Pressure`	Der maximale Prozentsatz des Java-Heaps, der für alle Datenknoten im Cluster verwendet wird. OpenSearch Der Dienst verwendet die Hälfte des RAM einer Instanz für den Java-Heap, bis zu einer Heap-Größe von 32 GiB. Sie können Instances bis zu 64 GiB RAM vertikal skalieren . Dann können Sie eine horizontale Skalierung durchführen, indem Sie Instances hinzufügen. Siehe the section called “Empfohlene CloudWatch Alarme”.
`SysMemory Utilization`	Der Prozentsatz des Arbeitsspeichers einer Instance, die in dem Cluster verwendet wird. Hohe Werte für diese Metrik sind normal und stellen normalerweise kein Problem mit Ihrem Cluster dar. Einen besseren Indikator für potenzielle Leistungs- und Stabilitätsprobleme finden Sie in der `JVMMemoryPressure` -Metrik.
`IndexingLatency`	Der Unterschied zwischen Minute N und Minute (N-1) in Millisekunden in der Gesamtzeit aller Indizierungsvorgänge in einem Knoten.
`IndexingRate`	Die Anzahl der Indizierungsvorgänge pro Minute.
`SearchLatency`	Der Unterschied in der Gesamtzeit in Millisekunden, die bei allen Suchvorgängen in einem Knoten zwischen Minute N und Minute (N-1) gemessen wird.
`SearchRate`	Die Gesamtanzahl von Suchabfragen pro Minute für alle Shards in einem Datenknoten.
`Threadpoo lSearchQueue`	Die Anzahl von Aufgaben in einer Warteschlange im Such-Threadpool. Wenn die Größe der Warteschlange gleichbleibend hoch ist, erwägen Sie eine Skalierung Ihres Clusters. Die maximale Größe der Such-Wart eschlange beträgt 1.000.

Metrik	Beschreibung
`ThreadpoolWriteQueue`	Die Anzahl von Aufgaben in einer Warteschlange im Schreib-Threadpool.
`ThreadpoolSearchRejected`	Die Anzahl abgewiesener Aufgaben im Such-Threadpool. Wenn die Anzahl stätig wächst, erwägen Sie eine Skalierung Ihres Clusters.
`ThreadpoolWriteRejected`	Die Anzahl abgewiesener Aufgaben im Schreib-Threadpool.

Metriken auf Clusterebene für Cluster in aktiven Availability Zones

Metrik	Beschreibung
`DataNodes`	Die Gesamtzahl der aktiven Shards und Standby-Shards.
`DataNodesShards.active`	Die Gesamtzahl der aktiven primären und Replikat-Shards.
`DataNodesShards.unassigned`	Die Anzahl der Shards, die Knoten im Cluster nicht zugeordnet sind.
`DataNodesShards.initializing`	Die Anzahl der Shards, die derzeit initialisiert werden.
`DataNodesShards.relocating`	Die Anzahl der Shards, die derzeit verschoben werden.

Metriken zur Rotation der Verfügbarkeits

Wenn`ActiveReads.`*`Availability-Zone`* `=` `1`, dann ist die Zone aktiv.
Wenn`ActiveReads.`*`Availability-Zone`* `=` `0`, dann befindet sich die Zone im Standby-Modus.

Metriken zum aktuellen Zeitpunkt

Amazon OpenSearch Service bietet die folgenden Metriken für Point-in-Time-Suchen (PIT).

Statistiken zum PIT-Koordinatorknoten (pro Koordinatorknoten)

Metrik	Beschreibung
`CurrentPointInTime`	Die Anzahl der aktiven PIT-Suchkontexte im Knoten.
`TotalPointInTime`	Die Anzahl der abgelaufenen PIT-Suchkontexte seit der Betriebszeit des Knotens.
`AvgPointInTimeAliveTime`	Die durchschnittliche Verfügbarkeit von PIT-Suchkontexten seit der Betriebszeit des Knotens.
`HasActivePointInTime`	Ein Wert von 1 gibt an, dass es seit der Verfügbarkeit des Knotens aktive PIT-Kontexte auf Knoten gibt. Ein Wert von 0 bedeutet, dass keine vorhanden sind.
`HasUsedPointInTime`	Ein Wert von 1 gibt an, dass seit der Betriebszeit des Knotens abgelaufene PIT-Kontexte auf Knoten vorhanden sind. Ein Wert von 0 bedeutet, dass keine vorhanden sind.

SQL-Metriken

Amazon OpenSearch Service bietet die folgenden Metriken für die SQL-Unterstützung.

Metrik	Beschreibung
`SQLFailedRequestCountByCusErr`	Die Anzahl der Anforderungen an die `_sql`-API, die aufgrund eines Clientproblems fehlgeschlagen sind. Beispielsweise kann eine Anforderung den HTTP-Statuscode 400 aufgrund eines `IndexNotFoundException` zurückgeben. Relevante Statistiken: Summe

Metrik	Beschreibung
SQLFailedRequestCountBySysErr	Die Anzahl der Anforderungen an die _sql-API, die aufgrund eines Serverproblems oder einer Funktionseinschränkung fehlgeschlagen sind. Beispielsweise kann eine Anforderung den HTTP-Statuscode 503 aufgrund eines VerificationException zurückgeben. Relevante Statistiken: Summe
SQLRequestCount	Die Anzahl der Anforderungen an die _sql-API. Relevante Statistiken: Summe
SQLDefaultCursorRequestCount	Ähnlich wieSQLRequestCount , zählt aber nur Paginierungsanfragen. Relevante Statistiken: Summe
SQLUnhealthy	Ein Wert von 1 gibt an, dass das SQL-Plug-In als Antwort auf bestimmte Anfragen 5 xx Antwortcodes zurückgibt oder ungültige Query-DSL an weitergibt. OpenSearch Andere Anfragen sollten weiterhin erfolgreich sein. Der Wert 0 zeigt an, dass keine aktuellen Fehler vorliegen. Wenn Sie einen dauerhaften Wert von 1 sehen, beheben Sie die Anforderungen, die Ihre Clients an das Plug-in stellen. Relevante Statistiken: Maximum

k-NN-Metriken

Amazon OpenSearch Service umfasst die folgenden Metriken für das K-Nearest Neighbor (k-NN) - Plugin.

Metrik	Beschreibung
KNNCacheCapacityReached	Metrik pro Knoten, ob die Cache-Kapazität erreicht wurde. Diese Metrik ist nur für die ungefähre k-NN-Suche relevant. Relevante Statistiken: Maximum

Metrik	Beschreibung
KNNCircuitBreakerTriggered	Metrik pro Cluster, ob der Leistungsschalter ausgelöst wird. Wenn Knoten einen Wert von 1 für KNNCacheCapacityReached zurückgibt, wird dieser Wert auch 1 zurückgeben. Diese Metrik ist nur für die ungefähre k-NN-Suche relevant. Relevante Statistiken: Maximum
KNNEvictionCount	Metrik pro Knoten für die Anzahl der Diagramme, die aufgrund von Speichereinschränkungen oder Leerlaufzeit aus dem Cache entfernt wurden. Explizite Bereinigungen, die aufgrund des Indexlöschens auftreten, werden nicht gezählt. Diese Metrik ist nur für die ungefähre k-NN-Suche relevant. Relevante Statistiken: Summe
KNNGraphIndexErrors	Metrik pro Knoten für die Anzahl der Anforderungen, um das knn_vector -Feld eines Dokuments in ein Diagramm hinzufügen, das einen Fehler erzeugt hat. Relevante Statistiken: Summe
KNNGraphIndexRequests	Metrik pro Knoten für die Anzahl der Anforderungen, um das knn_vector -Feld eines Dokuments in ein Diagramm hinzufügen. Relevante Statistiken: Summe
KNNGraphMemoryUsage	Metrik pro Knoten für die aktuelle Cachegröße (Gesamtgröße aller Diagramme im Speicher) in Kilobyte. Diese Metrik ist nur für die ungefähre k-NN-Suche relevant. Relevante Statistiken: Durchschnitt
KNNGraphQueryErrors	Metrik pro Knoten für die Anzahl der Diagrammabfragen, die einen Fehler verursacht haben. Relevante Statistiken: Summe

Metrik	Beschreibung
KNNGraphQueryRequests	Metrik pro Knoten für die Anzahl der Diagrammabfragen. Relevante Statistiken: Summe
KNNHitCount	Metrik pro Knoten für die Anzahl der Cache-Treffer. Ein Cache-Treffer tritt auf, wenn ein Benutzer ein Diagramm abfragt, das bereits in den Speicher geladen ist. Diese Metrik ist nur für die ungefähre k-NN-Suche relevant. Relevante Statistiken: Summe
KNNLoadExceptionCount	Metrik pro Knoten für die Häufigkeit, mit der eine Ausnahme aufgetreten ist, während versucht wurde, ein Diagramm in den Cache zu laden. Diese Metrik ist nur für die ungefähre k-NN-Suche relevant. Relevante Statistiken: Summe
KNNLoadSuccessCount	Metrik pro Knoten, wie oft das Plug-In ein Diagramm erfolgreich in den Cache geladen hat. Diese Metrik ist nur für die ungefähre k-NN-Suche relevant. Relevante Statistiken: Summe
KNNMissCount	Metrik pro Knoten für die Anzahl der Cache-Fehlschläge. Ein Cache-Fehlschlag tritt auf, wenn ein Benutzer ein Diagramm abfragt, das noch nicht in den Speicher geladen ist. Diese Metrik ist nur für die ungefähre k-NN-Suche relevant. Relevante Statistiken: Summe
KNNQueryRequests	Metrik pro Knoten für die Anzahl der Abfrageanforderungen, die das k–NN-Plug-In empfangen hat. Relevante Statistiken: Summe

Metrik	Beschreibung
KNNScriptCompilationErrors	Metrik pro Knoten für die Anzahl der Fehler während der Skript-Kompilierung. Diese Statistik ist nur relevant für die Suche nach k-NN-Skripten. Relevante Statistiken: Summe
KNNScriptCompilations	Metrik pro Knoten für die Anzahl der Kompilierung des k-NN-Skripts. Dieser Wert sollte normalerweise 1 oder 0 sein, aber wenn der Cache mit den kompilierten Skripten gefüllt ist, wird das k-NN-Skript möglicherweise neu kompiliert. Diese Statistik ist nur relevant für die Suche nach k-NN-Skripten. Relevante Statistiken: Summe
KNNScriptQueryErrors	Metrik pro Knoten für die Anzahl der Fehler bei Skriptabfragen. Diese Statistik ist nur relevant für die Suche nach k-NN-Skripten. Relevante Statistiken: Summe
KNNScriptQueryRequests	Metrik pro Knoten für die Gesamtzahl der Skriptabfragen. Diese Statistik ist nur relevant für die Suche nach k-NN-Skripten. Relevante Statistiken: Summe
KNNTotalLoadTime	Die Zeit in Nanosekunden, die k-NN benötigt hat, um Diagramme in den Cache zu laden. Diese Metrik ist nur für die ungefähre k-NN-Suche relevant. Relevante Statistiken: Summe

Metriken für Cluster-übergreifende Suchen

Amazon OpenSearch Service bietet die folgenden Metriken für die clusterübergreifende Suche.

Metriken der Quell-Domain

Metrik	Dimension	Beschreibung
`CrossClusterOutboundConnections`	`ConnectionId`	Anzahl der verbundenen Knoten. Wenn Ihre Antwort eine oder mehrere übersprungene Domains enthält, verwenden Sie diese Metrik, um alle fehlerhaften Verbindungen nachzuverfolgen. Wenn diese Zahl auf 0 fällt, ist die Verbindung fehlerhaft.
`CrossClusterOutboundRequests`	`ConnectionId`	Anzahl der an die Ziel-Domain gesendeten Suchabfragen. Verwenden Sie dies, um zu überprüfen, ob die Last von Cluster-übergreifenden Suchabfragen Ihre Domain überfordert, korrelieren Sie jede Spitze in dieser Metrik mit jeder JVM/CPU-Spitze.

Metrik der Ziel-Domain

Metrik	Dimension	Beschreibung
`CrossClusterInboundRequests`	`ConnectionId`	Anzahl der eingehenden Verbindungsanforderungen, die von der Quell-Domain empfangen wurden.

Fügen Sie einen CloudWatch Alarm für den Fall hinzu, dass Sie unerwartet eine Verbindung verlieren. Schritte zum Erstellen eines Alarms finden Sie unter Erstellen eines CloudWatch Alarms auf der Grundlage eines statischen Schwellenwerts.

Cluster-übergreifende Replikationsmetriken

Amazon OpenSearch Service bietet die folgenden Metriken für die clusterübergreifende Replikation.

Metrik	Beschreibung
`ReplicationRate`	Die durchschnittliche Rate der Replikationsvorgänge pro Sekunde. Diese Metrik ähnelt der `IndexingRate` -Metrik.

Metrik	Beschreibung
LeaderCheckPoint	Die Summe der Leader-Checkpoint-Werte für eine bestimmte Verbindung über alle replizierenden Indizes. Sie können diese Metrik verwenden, um die Latenz der Replikation zu messen.
FollowerCheckPoint	Die Summe der Follower-Checkpoint-Werte für eine bestimmte Verbindung über alle replizierenden Indizes. Sie können diese Metrik verwenden, um die Latenz der Replikation zu messen.
ReplicationNumSyncingIndices	Die Anzahl der Indizes, die den Replikationsstatus SYNCING haben.
ReplicationNumBootstrappingIndices	Die Anzahl der Indizes, die den Replikationsstatus BOOTSTRAPPING haben.
ReplicationNumPausedIndices	Die Anzahl der Indizes, die den Replikationsstatus PAUSED haben.
ReplicationNumFailedIndices	Die Anzahl der Indizes, die den Replikationsstatus FAILED haben.
CrossClusterOutboundReplicationRequests	Die Anzahl der Replikationstransportanfragen auf der Follower-Domain. Transportanfragen sind intern und treten bei jedem Aufruf eines Replikations-API-Vorgangs auf. Sie treten auch auf, wenn die Follower-Domain Änderungen gegenüber der Leader-Domain abfragt.
CrossClusterInboundReplicationRequests	Die Anzahl der Replikationstransportanfragen in der Leader-Domäne. Transportanfragen sind intern und treten bei jedem Aufruf eines Replikations-API-Vorgangs auf.

Metrik	Beschreibung
`AutoFollowNumSuccessStartReplication`	Die Anzahl der Follower-Indizes, die durch eine Replikationsregel für eine bestimmte Verbindung erfolgreich erstellt wurden.
`AutoFollowNumFailedStartReplication`	Die Anzahl der Follower-Indizes, die von einer Replikationsregel nicht erstellt werden konnten, wenn ein übereinstimmendes Muster vorhanden war. Dieses Problem kann aufgrund eines Netzwerkproblems auf dem Remote-Cluster oder eines Sicherheitsproblems auftreten (d. h. die zugeordnete Rolle hat keine Berechtigung zum Starten der Replikation).
`AutoFollowLeaderCallFailure`	Ob es fehlgeschlagene Abfragen vom Follower-Index zum Leader-Index gegeben hat, um neue Daten abzurufen. Ein Wert von 1 bedeutet, dass es in der letzten Minute 1 oder mehr fehlgeschlagene Anrufe gegeben hat.

Learning-to-Rank-Metriken

Amazon OpenSearch Service bietet die folgenden Kennzahlen für Learning to Rank.

Metrik	Beschreibung
`LTRRequestTotalCount`	Gesamtzahl der Ranglistenanforderungen.
`LTRRequestErrorCount`	Gesamtzahl der fehlgeschlagenen Anforderungen.
`LTRStatus.red`	Verfolgt, ob einer der Indizes, die zum Ausführen des Plug-Ins benötigt werden, rot ist.
`LTRMemoryUsage`	Der Gesamtspeicher, der vom Plug-In verwendet wird.

Metrik	Beschreibung
`LTRFeatureMemoryUsageInBytes`	Die Menge an Arbeitsspeicher in Byte, die von den Learning-to-Rank-Funktionsfeldern verwendet wird.
`LTRFeaturesetMemoryUsageInBytes`	Die Menge an Arbeitsspeicher in Byte, die von allen Learning-to-Rank-Funktionssets verwendet wird.
`LTRModelMemoryUsageInBytes`	Die Menge an Arbeitsspeicher in Byte, die von allen Learning-to-Rank-Modellen verwendet wird.

Metriken für Piped Processing Language

Amazon OpenSearch Service bietet die folgenden Metriken für Piped Processing Language.

Metrik	Beschreibung
`PPLFailedRequestCountByCusErr`	Die Anzahl der Anforderungen an die `_ppl`-API, die aufgrund eines Clientproblems fehlgeschlagen sind. Beispielsweise kann eine Anforderung den HTTP-Statuscode 400 aufgrund eines `IndexNotFoundException` zurückgeben.
`PPLFailedRequestCountBySysErr`	Die Anzahl der Anforderungen an die `_ppl`-API, die aufgrund eines Serverproblems oder einer Funktionseinschränkung fehlgeschlagen sind. Beispielsweise kann eine Anforderung den HTTP-Statuscode 503 aufgrund eines `VerificationException` zurückgeben.
`PPLRequestCount`	Die Anzahl der Anforderungen an die `_ppl`-API.

OpenSearch Protokolle mit Amazon CloudWatch Logs überwachen

Amazon OpenSearch Service stellt die folgenden OpenSearch Protokolle über Amazon CloudWatch Logs zur Verfügung:

- Fehlerprotokolle
- Langsame Protokolle für Suchanfragen
- Langsame Protokolle teilen
- Prüfungsprotokolle

Search Shard Slow-Logs, Indexing Shard Slow-Logs und Fehlerprotokolle sind nützlich, um Leistungs- und Stabilitätsprobleme zu beheben. Prüfungsprotokolle verfolgen Benutzeraktivitäten zu Compliance-Zwecken. Alle Protokolle sind standardmäßig deaktiviert. Wenn diese Option aktiviert ist, gelten die Standardpreise CloudWatch .

> **Note**
>
> Fehlerprotokolle sind nur für OpenSearch Elasticsearch-Versionen 5.1 und höher verfügbar. Langsame Logs sind für alle Versionen OpenSearch und für Elasticsearch verfügbar.

OpenSearch Verwendet für seine Logs Apache Log4j 2 und die integrierten Log-Levels (vom geringsten bis zum schwersten) von`TRACE`,`DEBUG`, `INFO``WARN`, `ERROR` und. `FATAL`

Wenn Sie Fehlerprotokolle aktivieren, veröffentlicht OpenSearch Service die Protokollzeilen von `WARN``ERROR`, und `FATAL` bis. CloudWatch OpenSearch Service veröffentlicht auch mehrere Ausnahmen von der `DEBUG` Ebene, darunter die folgenden:

- `org.opensearch.index.mapper.MapperParsingException`
- `org.opensearch.index.query.QueryShardException`
- `org.opensearch.action.search.SearchPhaseExecutionException`
- `org.opensearch.common.util.concurrent.OpenSearchRejectedExecutionException`
- `java.lang.IllegalArgumentException`

Fehlerprotokolle können bei der Fehlerbehebung in zahlreichen Situationen helfen, unter anderem:

- Probleme bei der Kompilierung von Painless-Skripts
- Ungültige Abfragen
- Probleme bei der Indizierung
- Snapshot-Fehler

- Migrationsfehler beim Indexstatusmanagement

Themen

Aktivieren der Veröffentlichung von Protokollen (Konsole)

Die OpenSearch Servicekonsole ist die einfachste Methode, um die Veröffentlichung von Protokollen zu ermöglichen CloudWatch.

Um die Veröffentlichung von Protokollen in CloudWatch (Konsole) zu aktivieren

1. Rufen Sie die Webseite https://aws.amazon.com auf und klicken Sie dann auf Sign In to the Console (Bei der Konsole anmelden).
2. Wählen Sie unter Analytics Amazon OpenSearch Service aus.
3. Wählen Sie die Domain aus, die Sie aktualisieren möchten.
4. Wählen Sie auf der Registerkarte Protokolle einen Protokolltyp aus und wählen Sie Aktivieren aus.
5. Erstellen Sie eine neue CloudWatch Protokollgruppe oder wählen Sie eine bestehende aus.

   > **Note**
   >
   > Wenn Sie die mehrere Protokolle aktivieren möchten, sollten Sie jedes Protokoll in einer eigenen Protokollgruppe veröffentlichen. Diese Trennung ermöglicht ein einfacheres Scannen der Protokolle.

6. Wählen Sie eine Zugriffsrichtlinie mit den entsprechenden Berechtigungen aus, oder erstellen Sie eine Richtlinie mit dem in der Konsole verfügbaren JSON:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "es.amazonaws.com"
      },
      "Action": [
        "logs:PutLogEvents",
        "logs:CreateLogStream"
      ],
      "Resource": "cw_log_group_arn:*"
    }
  ]
}
```

Wir empfehlen Ihnen, die `aws:SourceAccount`- und `aws:SourceArn`-Bedingungsschlüssel zur Richtlinie hinzuzufügen, um sich vor dem Problem des verwirrten Stellvertreters zu schützen. Das Quellkonto ist der Eigentümer der Domain und der Quell-ARN ist der ARN der Domain. Ihre Domain muss zum Hinzufügen dieser Bedingungsschlüssel über Service-Software R20211203 oder höher verfügen.

Beispielsweise können Sie der Richtlinie den folgenden Bedingungsblock hinzufügen:

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account-id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:es:region:account-id:domain/domain-name"
    }
}
```

Important

CloudWatch Logs unterstützt 10 Ressourcenrichtlinien pro Region. Wenn Sie beabsichtigen, Protokolle für mehrere OpenSearch Dienstdomänen zu aktivieren, sollten Sie eine umfassendere Richtlinie erstellen und wiederverwenden, die mehrere Protokollgruppen umfasst, um zu verhindern, dass dieses Limit erreicht wird.

Anweisungen zum Aktualisieren Ihrer Richtlinie finden Sie unter the section called "Aktivieren der Veröffentlichung von Protokollen (AWS CLI)".

7. Wählen Sie Enable (Aktivieren) aus.

   Der Status Ihrer Domain ändert sich von Active (Aktiv) zu Processing (In Verarbeitung). Der Status muss auf Active (Aktiv) zurückgesetzt werden, bevor die Veröffentlichung von Protokollen aktiviert wird. Diese Änderung dauert in der Regel 30 Minuten, kann jedoch je nach Domain-Konfiguration auch länger dauern.

Wenn Sie eines der Shard Slow-Logs aktiviert haben, finden Sie weitere Informationen unterthe section called "Schwellenwerte für Shard Slow Log festlegen". Wenn Sie Prüfungsprotokolle aktiviert haben, siehe the section called "Schritt 2: Aktivieren Sie die Audit-Logs in den OpenSearch Dashboards". Wenn Sie nur Fehlerprotokolle aktiviert haben, müssen Sie keine weiteren Konfigurationsschritte ausführen.

Aktivieren der Veröffentlichung von Protokollen (AWS CLI)

Bevor Sie die Protokollveröffentlichung aktivieren können, benötigen Sie eine CloudWatch Protokollgruppe. Wenn Sie noch keine Gruppe vorliegen haben, können Sie mit dem folgenden Befehl eine Gruppe erstellen:

```
aws logs create-log-group --log-group-name my-log-group
```

Geben Sie den folgenden Befehl ein, um den ARN der Protokollgruppe zu ermitteln, und notieren Sie sich den ARN:

```
aws logs describe-log-groups --log-group-name my-log-group
```

Jetzt können Sie dem OpenSearch Dienst Schreibberechtigungen für die Protokollgruppe erteilen. Sie müssen die ARN der Protokollgruppe nahe am Ende des Befehls bereitstellen:

```
aws logs put-resource-policy \
  --policy-name my-policy \
  --policy-document '{ "Version": "2012-10-17", "Statement": [{ "Sid": "",
 "Effect": "Allow", "Principal": { "Service": "es.amazonaws.com"}, "Action":
[ "logs:PutLogEvents","logs:CreateLogStream"],"Resource": "cw_log_group_arn:*"}]}'
```

> **Important**
>
> CloudWatch Logs unterstützt 10 Ressourcenrichtlinien pro Region. Wenn Sie planen, Shard Slow Logs für mehrere OpenSearch Dienstdomänen zu aktivieren, sollten Sie eine umfassendere Richtlinie erstellen und wiederverwenden, die mehrere Protokollgruppen umfasst, um zu verhindern, dass dieses Limit erreicht wird.

Wenn Sie diese Richtlinie zu einem späteren Zeitpunkt überprüfen müssen, verwenden Sie den `aws logs describe-resource-policies`-Befehl. Um die Richtlinie zu aktualisieren, geben Sie denselben `aws logs put-resource-policy`-Befehl für ein neues Richtliniendokument aus.

Schließlich können Sie die Option `--log-publishing-options` zum Aktivieren der Veröffentlichung verwenden. Die Syntax für die Option ist identisch für die `create-domain`- und `update-domain-config`-Befehle.

Parameter	Zulässige Werte
`--log-publishing-options`	`SEARCH_SLOW_LOGS={CloudWatchLogsLogGroupArn=` *`cw_log_group_arn`* `,Enabled=true|false}`
	`INDEX_SLOW_LOGS={CloudWatchLogsLogGroupArn=` *`cw_log_group_arn`* `,Enabled=true|false}`
	`ES_APPLICATION_LOGS={CloudWatchLogsLogGroupArn=` *`cw_log_group_arn`* `,Enabled=true|false}`
	`AUDIT_LOGS={CloudWatchLogsLogGroupArn=` *`cw_log_group_arn`* `,Enabled=true|false}`

> **Note**
>
> Wenn Sie die mehrere Protokolle aktivieren möchten, sollten Sie jedes Protokoll in einer eigenen Protokollgruppe veröffentlichen. Diese Trennung ermöglicht ein einfacheres Scannen der Protokolle.

Beispiel

Das folgende Beispiel ermöglicht die Veröffentlichung von Shard Slow-Protokollen für die Suche und Indizierung von Shard Slow für die angegebene Domäne:

```
aws opensearch update-domain-config \
  --domain-name my-domain \
  --log-publishing-options
 "SEARCH_SLOW_LOGS={CloudWatchLogsLogGroupArn=arn:aws:logs:us-east-1:123456789012:log-group:my-log-
group,Enabled=true},INDEX_SLOW_LOGS={CloudWatchLogsLogGroupArn=arn:aws:logs:us-east-1:123456789012:log-group:my-other-log-group,Enabled=true}"
```

Um das Veröffentlichen in zu deaktivieren CloudWatch, führen Sie denselben Befehl mit aus. `Enabled=false`

Wenn Sie eines der Shard Slow-Logs aktiviert haben, finden Sie weitere Informationen unterthe section called “Schwellenwerte für Shard Slow Log festlegen”. Wenn Sie Prüfungsprotokolle aktiviert haben, siehe the section called “Schritt 2: Aktivieren Sie die Audit-Logs in den OpenSearch Dashboards”. Wenn Sie nur Fehlerprotokolle aktiviert haben, müssen Sie keine weiteren Konfigurationsschritte ausführen.

Aktivieren der Veröffentlichung von Protokollen (AWS -SDKs)

Bevor Sie die Protokollveröffentlichung aktivieren können, müssen Sie zunächst eine CloudWatch Protokollgruppe erstellen, ihren ARN abrufen und dem OpenSearch Dienst Schreibberechtigungen für diese Gruppe erteilen. Die entsprechenden Vorgänge sind in der Amazon CloudWatch Logs API-Referenz dokumentiert:

- `CreateLogGroup`
- `DescribeLogGroup`
- `PutResourcePolicy`

Sie können auf diese Operationen mit den AWS -SDKs zugreifen.

Die AWS SDKs (außer den Android- und iOS-SDKs) unterstützen alle Operationen, die in der Amazon OpenSearch Service API-Referenz definiert sind, einschließlich der `--log-publishing-options` Option für `CreateDomain` und. `UpdateDomainConfig`

Wenn Sie eines der Shard Slow-Logs aktiviert haben, finden Sie weitere Informationen unter. the section called “Schwellenwerte für Shard Slow Log festlegen” Wenn Sie nur Fehlerprotokolle aktiviert haben, müssen Sie keine weiteren Konfigurationsschritte ausführen.

Aktivieren der Veröffentlichung von Protokollen (CloudFormation)

In diesem Beispiel erstellen wir eine Protokollgruppe mit dem Namen`opensearch-logs`, weisen die entsprechenden Berechtigungen CloudFormation zu und erstellen dann eine Domäne, in der die Protokollveröffentlichung für Anwendungsprotokolle, Shard-Slow-Logs für die Suche und Indexierung von Slow-Logs aktiviert ist.

Bevor Sie die Protokollveröffentlichung aktivieren können, müssen Sie eine CloudWatch Protokollgruppe erstellen:

```
Resources:
  OpenSearchLogGroup:
    Type: AWS::Logs::LogGroup
    Properties:
      LogGroupName: opensearch-logs
Outputs:
  Arn:
    Value:
      'Fn::GetAtt':
        - OpenSearchLogGroup
        - Arn
```

Die Vorlage gibt den ARN der Protokollgruppe aus. In diesem Fall ist der ARN `arn:aws:logs:us-east-1:123456789012:log-group:opensearch-logs`.

Erstellen Sie mithilfe des ARN eine Ressourcenrichtlinie, die dem OpenSearch Dienst Schreibberechtigungen für die Protokollgruppe erteilt:

```
Resources:
 OpenSearchLogPolicy:
   Type: AWS::Logs::ResourcePolicy
   Properties:
     PolicyName: my-policy
     PolicyDocument: "{ \"Version\": \"2012-10-17\", \"Statement\": [{ \"Sid\": \"\",
 \"Effect\": \"Allow\", \"Principal\": { \"Service\": \"es.amazonaws.com\"}, \"Action
\":[ \"logs:PutLogEvents\",\"logs:CreateLogStream\"],\"Resource\": \"arn:aws:logs:us-
east-1:123456789012:log-group:opensearch-logs:*\"}]}"
```

Erstellen Sie abschließend den folgenden CloudFormation Stack, der eine OpenSearch Dienstdomäne mit Protokollveröffentlichung generiert. Die Zugriffsrichtlinie ermöglicht es dem Benutzer AWS-Konto , alle HTTP-Anfragen an die Domain zu stellen.

```
Resources:
  OpenSearchServiceDomain:
    Type: "AWS::OpenSearchService::Domain"
    Properties:
      DomainName: my-domain
      EngineVersion: "OpenSearch_1.0"
      ClusterConfig:
        InstanceCount: 2
        InstanceType: "r6g.xlarge.search"
        DedicatedMasterEnabled: true
        DedicatedMasterCount: 3
        DedicatedMasterType: "r6g.xlarge.search"
      EBSOptions:
        EBSEnabled: true
        VolumeSize: 10
        VolumeType: "gp2"
      AccessPolicies:
        Version: "2012-10-17"
        Statement:
            Effect: "Allow"
            Principal:
                AWS: "arn:aws:iam::123456789012:user/es-user"
            Action: "es:*"
            Resource: "arn:aws:es:us-east-1:123456789012:domain/my-domain/*"
      LogPublishingOptions:
        ES_APPLICATION_LOGS:
          CloudWatchLogsLogGroupArn: "arn:aws:logs:us-east-1:123456789012:log-
group:opensearch-logs"
          Enabled: true
        SEARCH_SLOW_LOGS:
          CloudWatchLogsLogGroupArn: "arn:aws:logs:us-east-1:123456789012:log-
group:opensearch-logs"
          Enabled: true
        INDEX_SLOW_LOGS:
          CloudWatchLogsLogGroupArn: "arn:aws:logs:us-east-1:123456789012:log-
group:opensearch-logs"
          Enabled: true
```

Ausführliche Syntaxinformationen finden Sie unter Optionen für die Protokollveröffentlichung im AWS CloudFormation -Benutzerhandbuch.

Schwellenwerte für langsame Protokollierung von Suchanfragen festlegen

Protokolle für langsame Suchanfragen sind für die Suche in OpenSearch Dienstdomänen verfügbar, die auf Version 2.13 und höher ausgeführt werden. Die Protokollschwellenwerte für langsame Suchanfragen sind für die Gesamtdauer der Anfrage konfiguriert. Dies unterscheidet sich von langsamen Protokollen für Shard-Anfragen, die so konfiguriert sind, dass einzelne Shard Zeit in Anspruch nehmen.

Sie können Logs für langsame Suchanfragen mit Clustereinstellungen angeben. Dies unterscheidet sich von Shard Slow Logs, die Sie mit Indexeinstellungen aktivieren. Sie können beispielsweise die folgenden Einstellungen über die OpenSearch REST-API angeben:

```
PUT domain-endpoint/_cluster/settings
{
  "transient": {
    "cluster.search.request.slowlog.threshold.warn": "5s",
    "cluster.search.request.slowlog.threshold.info": "2s"
  }
}
```

Schwellenwerte für Shard Slow Log festlegen

OpenSearch deaktiviert standardmäßig Shard Slow Logs. Nachdem Sie die Veröffentlichung von Shard Slow-Logs auf aktiviert haben CloudWatch, müssen Sie immer noch Schwellenwerte für die Protokollierung für jeden Index angeben. OpenSearch Diese Schwellenwerte definieren genau, was auf welcher Protokollebene protokolliert werden soll.

Sie können diese Einstellungen beispielsweise über die OpenSearch REST-API angeben:

```
PUT domain-endpoint/index/_settings
{
  "index.search.slowlog.threshold.query.warn": "5s",
  "index.search.slowlog.threshold.query.info": "2s"
}
```

Langsame Logs testen

Um zu testen, ob sowohl die Protokolle für Suchanfragen als auch für Shard Slow erfolgreich veröffentlicht werden, sollten Sie mit sehr niedrigen Werten beginnen, um zu überprüfen, ob die Protokolle auch angezeigt werden CloudWatch, und dann die Schwellenwerte auf sinnvollere Werte erhöhen.

Wenn die Protokolle nicht angezeigt werden, überprüfen Sie Folgendes:

- Existiert die CloudWatch Protokollgruppe? Überprüfen Sie die CloudWatch Konsole.
- Hat OpenSearch Service die Rechte, in die Protokollgruppe zu schreiben? Überprüfen Sie die OpenSearch Servicekonsole.
- Ist die OpenSearch Dienstdomäne für die Veröffentlichung in der Protokollgruppe konfiguriert? Überprüfen Sie die OpenSearch Servicekonsole, verwenden Sie die AWS CLI `describe-domain-config` Option oder rufen Sie `DescribeDomainConfig` über eines der SDKs an.
- Sind die Schwellenwerte für die OpenSearch Protokollierung so niedrig, dass Ihre Anfragen sie überschreiten?

  Verwenden Sie den folgenden Befehl, um die Schwellenwerte für die langsame Protokollierung Ihrer Suchanfrage für eine Domain zu überprüfen:

  ```
  GET domain-endpoint/_cluster/settings?flat_settings
  ```

  Verwenden Sie den folgenden Befehl, um die Schwellenwerte für das Shard Slow-Log für einen Index zu überprüfen:

  ```
  GET domain-endpoint/index/_settings?pretty
  ```

Wenn Sie Slow-Protokolle für einen Index deaktivieren möchten, setzen Sie alle geänderten Schwellenwerte wieder auf die Standardwerte von `-1` zurück.

Wenn Sie die Veröffentlichung CloudWatch über die OpenSearch Service Console deaktivieren oder AWS CLI nicht die Erstellung OpenSearch von Protokollen beenden, sondern nur die Veröffentlichung dieser Protokolle beenden. Überprüfen Sie unbedingt Ihre Indexeinstellungen, falls Sie die Shard Slow-Logs nicht mehr benötigen, und Ihre Domain-Einstellungen, falls Sie die Slow-Logs für Suchanfragen nicht mehr benötigen.

Anzeigen von -Protokollen

Das Anzeigen der Anwendung und die langsame Anmeldung CloudWatch sind wie die Anzeige jedes anderen CloudWatch Protokolls. Weitere Informationen finden Sie unter Protokolldaten anzeigen im Amazon CloudWatch Logs-Benutzerhandbuch.

Hier finden Sie einige Überlegungen zur Anzeige der Protokolle:

- OpenSearch Service veröffentlicht nur die ersten 255.000 Zeichen jeder Zeile an CloudWatch. Alle verbleibenden Inhalte werden abgeschnitten. Bei Prüfungsprotokollen sind es 10 000 Zeichen pro Nachricht.
- In CloudWatch haben die Namen der Protokolldatenströme die Suffixe`-index-slow-logs`,,, und `-search-slow-logs-application-logs`, `-audit-logs` um den Inhalt leichter zu identifizieren.

Überwachung von Auditprotokollen in Amazon OpenSearch Service

Wenn Ihre Amazon OpenSearch Service-Domain eine differenzierte Zugriffskontrolle verwendet, können Sie Audit-Logs für Ihre Daten aktivieren. Audit-Logs sind hochgradig anpassbar und ermöglichen es Ihnen, Benutzeraktivitäten in Ihren OpenSearch Clustern nachzuverfolgen, einschließlich erfolgreicher und fehlgeschlagener Authentifizierungen OpenSearch, Anfragen an, Indexänderungen und eingehende Suchanfragen. Die Standardkonfiguration verfolgt einen beliebten Satz von Benutzeraktionen. Wir empfehlen jedoch, die Einstellungen genau an Ihre Bedürfnisse anzupassen.

Genau wie OpenSearch Anwendungsprotokolle und langsame Protokolle veröffentlicht OpenSearch Service CloudWatch Auditprotokolle in Logs. Wenn diese Option aktiviert ist, gelten die CloudWatch Standardpreise.

> **Note**
>
> Um Audit-Logs zu aktivieren, muss Ihre Benutzerrolle der `security_manager` Rolle zugeordnet sein, die Ihnen Zugriff auf die OpenSearch `plugins/_security` REST-API gewährt. Weitere Informationen hierzu finden Sie unter the section called “Hauptbenutzer ändern”.

Themen

Einschränkungen

Prüfungsprotokolle haben folgende Einschränkungen:

- Prüfungsprotokolle enthalten keine clusterübergreifenden Suchanforderungen, die von der Domain-Zugriffsrichtlinie des Ziels abgelehnt wurden.
- Die Maximalgröße jeder Prüfungsprotokollmeldung beträgt 10 000 Zeichen. Die Prüfungsprotokollmeldung wird abgeschnitten, wenn sie diesen Grenzwert überschreitet.

Aktivieren von Prüfprotokollen

Die Aktivierung des Prüfungsprotokolls für einen Cluster ist ein zweistufiger Prozess. Zunächst konfigurieren Sie Ihre Domain so, dass Audit-Logs in Logs veröffentlicht werden CloudWatch . Anschließend aktivieren Sie Audit-Logs in OpenSearch Dashboards und konfigurieren sie so, dass sie Ihren Anforderungen entsprechen.

> **Important**
>
> Wenn beim Ausführen dieser Schritte ein Fehler auftritt, finden Sie unter the section called “Prüfungsprotokolle können nicht aktiviert werden” Informationen zur Fehlerbehebung.

Schritt 1: Aktivieren von Überwachungsprotokolle und Konfigurieren einer Zugriffsrichtlinie

In diesen Schritten wird beschrieben, wie Sie mithilfe der Konsole Prüfungsprotokolle aktivieren. Sie können sie auch mithilfe der oder der AWS CLIOpenSearch Service-API aktivieren.

Um Audit-Logs für eine OpenSearch Service-Domain (Konsole) zu aktivieren

1. Wählen Sie die Domain aus, um ihre Konfiguration zu öffnen, und wechseln Sie dann zur Registerkarte Protokolle.
2. Wählen Sie Prüfungsprotokolle und dann Aktivieren aus.
3. Erstellen Sie eine CloudWatch Protokollgruppe oder wählen Sie eine bestehende aus.
4. Wählen Sie eine Zugriffsrichtlinie mit den entsprechenden Berechtigungen aus, oder erstellen Sie eine Richtlinie mit dem in der Konsole verfügbaren JSON:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "es.amazonaws.com"
      },
      "Action": [
        "logs:PutLogEvents",
        "logs:CreateLogStream"
      ],
      "Resource": "cw_log_group_arn"
    }
  ]
}
```

Wir empfehlen Ihnen, die `aws:SourceAccount`- und `aws:SourceArn`-Bedingungsschlüssel zur Richtlinie hinzuzufügen, um sich vor dem Problem des verwirrten Stellvertreters zu schützen. Das Quellkonto ist der Eigentümer der Domain und der Quell-ARN ist der ARN der Domain. Ihre Domain muss zum Hinzufügen dieser Bedingungsschlüssel über Service-Software R20211203 oder höher verfügen.

Beispielsweise können Sie der Richtlinie den folgenden Bedingungsblock hinzufügen:

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account-id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:es:region:account-id:domain/domain-name"
```

```
    }
}
```

5. Wählen Sie Aktivieren aus.

Schritt 2: Aktivieren Sie die Audit-Logs in den OpenSearch Dashboards

Nachdem Sie die Auditprotokolle in der OpenSearch Servicekonsole aktiviert haben, müssen Sie sie auch in den OpenSearch Dashboards aktivieren und entsprechend Ihren Anforderungen konfigurieren.

1. Öffnen Sie OpenSearch Dashboards und wählen Sie im Menü auf der linken Seite Sicherheit aus.
2. Wählen Sie Prüfungsprotokolle aus.
3. Wählen Sie Überwachungsprotokollierung aktivieren aus.

Die Dashboards-Benutzeroberfläche bietet vollständige Kontrolle über die Prüfungsprotokolleinstellungen unter Allgemeine Einstellungen und Compliance-Einstellungen. Eine Beschreibung aller Konfigurationsoptionen finden Sie unter Prüfungsprotokolleinstellungen.

Aktivieren Sie die Audit-Protokollierung mithilfe der AWS CLI

Der folgende AWS CLI Befehl aktiviert Audit-Logs für eine bestehende Domain:

```
aws opensearch update-domain-config --domain-name my-domain --log-publishing-options
 "AUDIT_LOGS={CloudWatchLogsLogGroupArn=arn:aws:logs:us-east-1:123456789012:log-
group:my-log-group,Enabled=true}"
```

Sie können Prüfungsprotokolle auch aktivieren, wenn Sie eine Domain erstellen. Weitere Informationen finden Sie in der AWS CLI -Befehlsreferenz.

Aktivieren der Prüfungsprotokollierung über die Konfigurations-API

Die folgende Anfrage an die Konfigurations-API aktiviert Prüfungsprotokolle für eine vorhandene Domain:

```
POST https://es.us-east-1.amazonaws.com/2021-01-01/opensearch/domain/my-domain/config
```

```
{
  "LogPublishingOptions": {
    "AUDIT_LOGS": {
      "CloudWatchLogsLogGroupArn":"arn:aws:logs:us-east-1:123456789012:log-
group1:sample-domain",
      "Enabled":true
    }
  }
}
```

Weitere Informationen finden Sie in der Amazon OpenSearch Service API-Referenz.

Protokollebenen und -Kategorien prüfen

Cluster-Kommunikation erfolgt über zwei separate Ebenen: die REST- und die Transportebene.

- Die REST-Schicht deckt die Kommunikation mit HTTP-Clients wie curl, Logstash, OpenSearch Dashboards, dem Java-High-Level-REST-Client und der Python-Anforderungsbibliothek ab — alle HTTP-Anfragen, die im Cluster ankommen.
- Die Transportebene deckt die Kommunikation zwischen Knoten ab. Nachdem beispielsweise eine Suchanfrage im Cluster (über die REST-Ebene) eintrifft, sendet der koordinierende Knoten, der die Anfrage bedient, die Anfrage an andere Knoten, empfängt deren Antworten, sammelt die erforderlichen Dokumente und fasst sie in der endgültigen Antwort zusammen. Operationen wie Shard-Zuweisung und Neuverteilung erfolgen ebenfalls über die Transportebene.

Sie können Prüfungsprotokolle für ganze Ebenen sowie einzelne Prüfungskategorien für eine Ebene aktivieren oder deaktivieren. Die folgende Tabelle enthält eine Zusammenfassung der Überwachungskategorien und die Ebene, für die sie verfügbar sind.

Kategorie	Beschreibung	Für REST verfügbar	Transportfähig
FAILED_LOGIN	Eine Anforderung enthielt ungültige Anmeldein formationen und die Authentifizierung ist fehlgeschlagen.	Ja	Ja

Kategorie	Beschreibung	Für REST verfügbar	Transportfähig
MISSING_PRIVILEGES	Ein Benutzer hatte nicht die Berechtigung, die Anforderung zu stellen.	Ja	Ja
GRANTED_PRIVILEGES	Ein Benutzer hatte die Berechtigung, die Anforderung zu stellen.	Ja	Ja
OPENSEARCH_SECURITY_INDEX_ATTEMPT	Eine Anforderung hat versucht, den `.opendistro_security` -Index zu ändern.	Nein	Ja
AUTHENTICATED	Eine Anforderung enthielt gültige Anmeldeinformationen und die Authentifizierung ist erfolgreich.	Ja	Ja

Kategorie	Beschreibung	Für REST verfügbar	Transportfähig
INDEX_EVENT	Eine Anforderung führte einen administrativen Vorgang für einen Index aus, z. B. das Erstellen eines Indexes, das Festlegen eines Alias oder das Ausführen einer erzwungenen Zusammenführung. Die vollständige Liste der `indices:admin/` Aktionen, die diese Kategorie umfasst, ist in der Dokumentation verfügbar. OpenSearch	Nein	Ja

Zusätzlich zu diesen Standardkategorien bietet die fein abgestufte Zugriffskontrolle mehrere zusätzliche Kategorien, die darauf ausgelegt sind, die Anforderungen an die Daten-Compliance zu erfüllen.

Kategorie	Beschreibung
COMPLIANCE_DOC_READ	Eine Anforderung führte ein Leseereignis für ein Dokument in einem Index aus.
COMPLIANCE_DOC_WRITE	Eine Anforderung führte ein Schreibereignis für ein Dokument in einem Index aus.
COMPLIANCE_INTERNAL_CONFIG_READ	Eine Anforderung führte ein Leseereignis auf dem `.opendistro_security` -Index aus.

Kategorie	Beschreibung
COMPLIANCE_INTERNAL_CONFIG_WRITE	Eine Anforderung führte ein Schreibereignis auf dem `.opendistro_security` -Index aus.

Es kann eine beliebige Kombination von Kategorien und Nachrichtenattributen vorliegen. Wenn Sie beispielsweise eine REST-Anforderung senden, um ein Dokument zu indizieren, werden möglicherweise die folgenden Zeilen in den Prüfungsprotokollen angezeigt:

- Authentifiziert auf REST-Ebene (Authentifizierung)
- GRANTED_PRIVILEGE auf Transportebene (Autorisierung)
- COMPLIANCE_DOC_WRITE (Dokument in einen Index geschrieben)

Prüfprotokolleinstellungen

Prüfungsprotokolle verfügen über zahlreiche Konfigurationsoptionen.

Allgemeine Einstellungen

Mit den allgemeinen Einstellungen können Sie einzelne Kategorien oder ganze Ebenen aktivieren oder deaktivieren. Wir empfehlen, GRANTED_PRIVILEGES und AUTHENTICATED als ausgeschlossene Kategorien. Andernfalls werden diese Kategorien für jede gültige Anforderung an den Cluster protokolliert.

Name	Backend-Einstellung	Beschreibung
REST-Ebene	enable_rest	Aktivieren oder Deaktivieren von Ereignissen, die auf der REST-Ebene auftreten.
REST-Kategorien	disabled_rest_categories	Geben Sie Prüfungskategorien an, die auf der REST-Ebene ignoriert werden sollen. Durch Ändern dieser Kategorien kann die Größe der Prüfungsprotokolle erheblich erhöht werden.

Name	Backend-Einstellung	Beschreibung
Transportebene	enable_transport	Aktivieren oder deaktivieren Sie Ereignisse, die auf der Transportebene auftreten.
Transportkategorien	disabled_transport_categories	Geben Sie Prüfungskategorien an, die auf der Transportebene ignoriert werden müssen. Durch Ändern dieser Kategorien kann die Größe der Prüfungsprotokolle erheblich erhöht werden.

Mit Attributeinstellungen können Sie die Detailmenge in jeder Protokollzeile anpassen.

Name	Backend-Einstellung	Beschreibung
Massenanfragen	resolve_bulk_requests	Wenn Sie diese Einstellung aktivieren, wird für jedes Dokument in einer Massenanforderung ein Protokoll generiert, das die Größe der Prüfungsprotokolle erheblich erhöhen kann.
Anforderungstext	log_request_body	Fügen Sie den Anforderungstext der Anforderungen ein.
Lösen von Indizes	resolve_indices	Alias in Indizes auflösen.

Verwenden Sie Ignorier-Einstellungen, um eine Gruppe von Benutzern oder API-Pfaden auszuschließen:

Name	Backend-Einstellung	Beschreibung
Ignorierte Benutzer	ignore_users	Geben Sie die Benutzer an, die Sie ausschließen möchten.

Name	Backend-Einstellung	Beschreibung
Ignorierte Anforderungen	ignore_requests	Geben Sie Anforderungsmuster an, die Sie ausschließen möchten.

Compliance-Einstellungen

Mit den Compliance-Einstellungen können Sie den Zugriff auf Index-, Dokument- oder Feldebene optimieren.

Name	Backend-Einstellung	Beschreibung
Compliance-Protokollierung	enable_compliance	Aktivieren oder deaktivieren Sie die Compliance-Protokollierung.

Sie können die folgenden Einstellungen für die Lese- und Schreibereignisprotokollierung festlegen.

Name	Backend-Einstellung	Beschreibung
Interne Konfigurationsprotokollierung	internal_config	Aktivieren oder deaktivieren Sie die Protokollierung von Ereignissen im `.opendistro_security` -Index.

Sie können die folgenden Einstellungen für Lese-Ereignisse festlegen.

Name	Backend-Einstellung	Beschreibung
Lesen von Metadaten	read_metadata_only	Nur Metadaten für Leseereignisse einschließen. Fügen Sie keine Dokumentfelder ein.

Name	Backend-Einstellung	Beschreibung
Ignorierte Benutzer	read_ignore_users	Schließen Sie bestimmte Benutzer nicht für Leseereignisse ein.
Beobachtete Felder	read_watched_fields	Geben Sie die Indizes und Felder an, die auf Leseereignisse überwacht werden sollen. Durch das Hinzufügen überwachter Felder wird ein Protokoll pro Dokumentzugriff generiert, wodurch die Größe der Prüfungsprotokolle erheblich vergrößert wird. Beobachtete Felder unterstützen Indexmuster und Feldmuster: `{ "index-name-pattern": [ "field-name-pattern" ], "logs*": [ "message" ], "twitter": [ "id", "user*" ] }`

Sie können die folgenden Einstellungen für Schreibereignisse festlegen.

Name	Backend-Einstellung	Beschreibung
Schreiben von Metadaten	write_metadata_only	Nur Metadaten für Schreibereignisse einschließen. Fügen Sie keine Dokumentfelder ein.
Protokoll-Differenzen	write_log_diffs	Wenn write_metadata_only false ist, schließen Sie nur die Unterschiede zwischen Schreibereignissen ein.

Name	Backend-Einstellung	Beschreibung
Ignorierte Benutzer	write_ignore_users	Geben Sie bestimmte Benutzer für Schreibereignisse nicht ein.
Angesehene Indizes	write_watched_indices	Geben Sie die Indizes oder Indexmuster an, die auf Schreibereignisse überwacht werden sollen. Durch das Hinzufügen überwachter Felder wird ein Protokoll pro Dokumentzugriff generiert, wodurch die Größe der Prüfungsprotokolle erheblich vergrößert wird.

Prüfungsprotokollbeispiel

Dieser Abschnitt enthält eine Beispielkonfiguration, eine Suchanforderung und das resultierende Prüfungsprotokoll für alle Lese- und Schreibereignisse eines Indexes.

Schritt 1: Konfigurieren von Prüfungsprotokollen

Nachdem Sie die Veröffentlichung von Audit-Logs in einer CloudWatch Logs-Gruppe aktiviert haben, navigieren Sie zur Seite „Audit-Protokollierung“ der OpenSearch Dashboards und wählen Sie Audit-Protokollierung aktivieren aus.

1. Wählen Sie unter Allgemeine Einstellungen Konfigurieren und stellen Sie sicher, dass die REST-Ebene aktiviert ist.
2. Wählen Sie in den Compliance-Einstellungen die Option Konfigurieren aus.
3. Fügen Sie unter Schreiben in Beobachtete Felder `accounts` für alle Schreibereignisse zu diesem Index hinzu.
4. Fügen Sie unter Lesen in Beobachtete Felder `ssn`- und `id-`-Felder des `accounts`-Index hinzu:

```
{
  "accounts-": [
    "ssn",
    "id-"
  ]
}
```

Schritt 2: Ausführen von Lese- und Schreibereignissen

1. Navigieren Sie zu OpenSearch Dashboards, wählen Sie Dev Tools und indexieren Sie ein Beispieldokument:

```
PUT accounts/_doc/0
{
  "ssn": "123",
  "id-": "456"
}
```

2. Um ein Leseereignis zu testen, senden Sie die folgende Anforderung:

```
GET accounts/_search
{
  "query": {
    "match_all": {}
  }
}
```

Schritt 3: Beobachten der Protokolle

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Protokollgruppen aus.
3. Wählen Sie die Protokollgruppe aus, die Sie beim Aktivieren von Prüfungsprotokollen festgelegt haben. Innerhalb der Protokollgruppe erstellt OpenSearch Service einen Protokollstream für jeden Knoten in Ihrer Domain.
4. Wählen Sie unter Protokollströme die Option Alle durchsuchen aus.
5. Die Lese- und Schreibereignisse finden Sie in den entsprechenden Protokollen. Sie können eine Verzögerung von 5 Sekunden erwarten, bevor das Protokoll angezeigt wird.

   Beispiel für Schreibprüfungsprotokoll

```
{
  "audit_compliance_operation": "CREATE",
  "audit_cluster_name": "824471164578:audit-test",
  "audit_node_name": "be217225a0b77c2bd76147d3ed3ff83c",
  "audit_category": "COMPLIANCE_DOC_WRITE",
  "audit_request_origin": "REST",
```

```
  "audit_compliance_doc_version": 1,
  "audit_node_id": "3xNJhm4XS_yTzEgDWcGRjA",
  "@timestamp": "2020-08-23T05:28:02.285+00:00",
  "audit_format_version": 4,
  "audit_request_remote_address": "3.236.145.227",
  "audit_trace_doc_id": "lxnJGXQBqZSlDB91r_uZ",
  "audit_request_effective_user": "admin",
  "audit_trace_shard_id": 8,
  "audit_trace_indices": [
    "accounts"
  ],
  "audit_trace_resolved_indices": [
    "accounts"
  ]
}
```


Beispiel für Leseprüfungsprotokoll


```
{
  "audit_cluster_name": "824471164578:audit-docs",
  "audit_node_name": "806f6050cb45437e2401b07534a1452f",
  "audit_category": "COMPLIANCE_DOC_READ",
  "audit_request_origin": "REST",
  "audit_node_id": "saSevm9ASte0-pjAtYi2UA",
  "@timestamp": "2020-08-31T17:57:05.015+00:00",
  "audit_format_version": 4,
  "audit_request_remote_address": "54.240.197.228",
  "audit_trace_doc_id": "config:7.7.0",
  "audit_request_effective_user": "admin",
  "audit_trace_shard_id": 0,
  "audit_trace_indices": [
    "accounts"
  ],
  "audit_trace_resolved_indices": [
    "accounts"
  ]
}
```


Um den Text der Anfrage einzubeziehen, kehren Sie zu den Compliance-Einstellungen in den OpenSearch Dashboards zurück und deaktivieren Sie die Option Metadaten schreiben. Um

Ereignisse eines bestimmten Benutzers auszuschließen, fügen Sie den Benutzer zu Ignorierte Benutzer hinzu.

Eine Beschreibung der einzelnen Prüfungsprotokoll-Felder finden Sie unter Referenz des Prüfungsprotokolls. Informationen zur Suche und Analyse Ihrer Audit-Protokolldaten finden Sie unter Analysieren von Protokolldaten mit CloudWatch Logs Insights im Amazon CloudWatch Logs-Benutzerhandbuch.

Konfigurieren von Prüfungsprotokollen mit der REST-API

Wir empfehlen die Verwendung von OpenSearch Dashboards zur Konfiguration von Audit-Logs, Sie können aber auch die detaillierte REST-API für die Zugriffskontrolle verwenden. Dieser Abschnitt enthält eine Beispielanforderung. Die vollständige Dokumentation zur REST-API ist in der Dokumentation verfügbar. OpenSearch

```
PUT _opendistro/_security/api/audit/config
{
  "enabled": true,
  "audit": {
    "enable_rest": true,
    "disabled_rest_categories": [
      "GRANTED_PRIVILEGES",
      "AUTHENTICATED"
    ],
    "enable_transport": true,
    "disabled_transport_categories": [
      "GRANTED_PRIVILEGES",
      "AUTHENTICATED"
    ],
    "resolve_bulk_requests": true,
    "log_request_body": true,
    "resolve_indices": true,
    "exclude_sensitive_headers": true,
    "ignore_users": [
      "kibanaserver"
    ],
    "ignore_requests": [
      "SearchRequest",
      "indices:data/read/*",
      "/_cluster/health"
    ]
  },
```

```
  "compliance": {
    "enabled": true,
    "internal_config": true,
    "external_config": false,
    "read_metadata_only": true,
    "read_watched_fields": {
      "read-index-1": [
        "field-1",
        "field-2"
      ],
      "read-index-2": [
        "field-3"
      ]
    },
    "read_ignore_users": [
      "read-ignore-1"
    ],
    "write_metadata_only": true,
    "write_log_diffs": false,
    "write_watched_indices": [
      "write-index-1",
      "write-index-2",
      "log-*",
      "*"
    ],
    "write_ignore_users": [
      "write-ignore-1"
    ]
  }
}
```

Überwachung von OpenSearch Service-Ereignissen mit Amazon EventBridge

Amazon OpenSearch Service ist in Amazon integriert EventBridge , um Sie über bestimmte Ereignisse zu informieren, die sich auf Ihre Domains auswirken. Ereignisse von AWS Diensten werden nahezu EventBridge in Echtzeit zugestellt. Dieselben Ereignisse werden auch an Amazon CloudWatch Events, den Vorgänger von Amazon, gesendet EventBridge. Sie können einfache Regeln schreiben, um anzugeben, welche Ereignisse für Sie interessant sind und welche automatisierten Aktionen durchgeführt werden sollen, wenn sich für ein Ereignis eine

Übereinstimmung mit einer Regel ergibt. Die folgenden Aktionen können beispielsweise automatisch ausgelöst werden:

- Eine AWS Lambda Funktion aufrufen
- Aufrufen eines Amazon EC2-Ausführungsbefehls
- Weiterleiten des Ereignisses an Amazon Kinesis Data Streams
- Aktivierung einer AWS Step Functions Functions-Zustandsmaschine
- Benachrichtigen eines Amazon SNS-Themas oder einer Amazon SQS-Warteschlange

Weitere Informationen finden Sie unter Erste Schritte mit Amazon EventBridge im EventBridge Amazon-Benutzerhandbuch.

Themen

Aktualisieren der Software

OpenSearch Der Service sendet Ereignisse, EventBridge wenn eines der folgenden Service-Software-Aktualisierungsereignisse eintritt.

Service-Software-Update verfügbar

OpenSearch Der Dienst sendet dieses Ereignis, wenn ein Service-Softwareupdate verfügbar ist.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Available",
    "severity": "Informational",
    "description": "Service software update R20220928 available. Service Software
 Deployment Mechanism:
                   Blue/Green. For more information on deployment configuration,
 please
                   see: https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/managedomains-configuration-changes.html"
  }
}
```

Das Update der Service-Software ist geplant

OpenSearch Der Dienst sendet dieses Ereignis, wenn ein Service-Softwareupdate geplant wurde. Bei optionalen Updates erhalten Sie die Benachrichtigung am geplanten Datum und können den Termin jederzeit verschieben. Bei erforderlichen Aktualisierungen erhalten Sie die Benachrichtigung drei Tage vor dem geplanten Datum, und Sie haben die Möglichkeit, den Termin innerhalb des obligatorischen Zeitfensters zu verschieben.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
```

```
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Scheduled",
    "severity": "High",
    "description": "A new service software update [R20200330-p1] has been scheduled at
 [21st May 2023 12:40 GMT].
                    Please see documentation for more information on scheduling
 software updates:
                    https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/service-software.html."
  }
}
```

Das Service-Software-Update wurde verschoben

OpenSearch Der Service sendet dieses Ereignis, wenn ein optionales Service-Softwareupdate verschoben wurde. Weitere Informationen finden Sie unter the section called “Optionale und erforderliche Updates”.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Rescheduled",
    "severity": "High",
    "description": "The service software update [R20200330-p1], which was originally
 scheduled for
                    [21st May 2023 12:40 GMT], has been rescheduled to [23rd May 2023
 12:40 GMT].
                    Please see documentation for more information on scheduling
 software updates:
```

```
                    https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/service-software.html."
  }
}
```

Service-Software-Update gestartet

OpenSearch Der Dienst sendet dieses Ereignis, wenn ein Service-Softwareupdate gestartet wurde.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Started",
    "severity": "Informational",
    "description": "Service software update [R20200330-p1] started.
  }
}
```

Service-Software-Update abgeschlossen

OpenSearch Der Dienst sendet dieses Ereignis, wenn ein Service-Softwareupdate abgeschlossen ist.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
```

```
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Completed",
    "severity": "Informational",
    "description": "Service software update [R20200330-p1] completed."
  }
}
```

Das Service-Software-Update wurde abgebrochen

OpenSearch Der Dienst sendet dieses Ereignis, wenn ein Service-Softwareupdate storniert wurde.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Cancelled",
    "severity": "Informational",
    "description": "The scheduled service software update [R20200330-p1] has been
 cancelled as a
                   newer update is available. Please schedule the latest update."
  }
}
```

Das geplante Service-Software-Update wurde storniert

OpenSearch Der Dienst sendet dieses Ereignis, wenn ein Dienst-Softwareupdate, das zuvor für die Domäne geplant war, storniert wurde.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Cancelled",
    "severity": "Informational",
    "description": "The scheduled service software update [R20200330-p1] has been
 cancelled."
  }
}
```

Das Service-Software-Update wurde nicht ausgeführt

OpenSearch Der Dienst sendet dieses Ereignis, wenn er ein Service-Softwareupdate nicht initiieren kann.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Unexecuted",
```

```
    "severity": "Informational",
    "description": "The scheduled service software update [R20200330-p1] cannot be
 started. Reason: [reason]"
  }
}
```

Service-Software-Update fehlgeschlagen

OpenSearch Der Dienst sendet dieses Ereignis, wenn ein Service-Softwareupdate fehlschlägt.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Failed",
    "severity": "High",
    "description": "Installation of service software update [R20200330-p1] failed.
 [reason].
  }
}
```

Aktualisierung der Servicesoftware erforderlich

OpenSearch Der Dienst sendet dieses Ereignis, wenn ein Service-Softwareupdate erforderlich ist. Weitere Informationen finden Sie unter the section called “Optionale und erforderliche Updates”.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
```

```
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Required",
    "severity": "High",
    "description": "Service software update [R20200330-p1] available. Update
                    will be automatically installed after [21st May 2023] if no
                    action is taken. Service Software Deployment Mechanism: Blue/Green.
                    For more information on deployment configuration, please see:
                    https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/managedomains-configuration-changes.html"
  }
}
```

Automatische Optimierung von Ereignissen

OpenSearch Der Dienst sendet Ereignisse, EventBridge wenn eines der folgenden Auto-Tune-Ereignisse eintritt.

Automatische Optimierung ausstehend

OpenSearch Der Dienst sendet dieses Ereignis, wenn Auto-Tune Optimierungsempfehlungen für eine verbesserte Clusterleistung und -verfügbarkeit identifiziert hat. Dieses Ereignis wird nur für Domains angezeigt, bei denen die automatische Optimierung deaktiviert ist.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version": "0",
  "id": "3acb26c8-397c-4c89-a80a-ce672a864c55",
  "detail-type": "Amazon OpenSearch Service Auto-Tune Notification",
  "source": "aws.es",
  "account": "123456789012",
```

```
  "time": "2020-10-30T22:06:31Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Auto-Tune Event",
    "severity": "Informational",
    "status": "Pending",
    "description": "Auto-Tune recommends the following new settings for your
 domain: { JVM Heap size : 60%}. Enable Auto-Tune to improve cluster stability and
 performance.",
    "scheduleTime": "{iso8601-timestamp}"
  }
}
```

Automatische Optimierung gestartet

OpenSearch Der Service sendet dieses Ereignis, wenn Auto-Tune beginnt, neue Einstellungen auf Ihre Domain anzuwenden.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version": "0",
  "id": "3acb26c8-397c-4c89-a80a-ce672a864c55",
  "detail-type": "Amazon OpenSearch Service Auto-Tune Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2020-10-30T22:06:31Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Auto-Tune Event",
    "severity": "Informational",
    "status": "Started",
    "scheduleTime": "{iso8601-timestamp}",
    "startTime": "{iso8601-timestamp}",
    "description" : "Auto-Tune is applying the following settings to your domain: { JVM
 Heap size : 60%}."
  }
}
```

Die automatische Optimierung erfordert eine geplante blau/grüne Bereitstellung

OpenSearch Der Service sendet dieses Ereignis, wenn Auto-Tune Optimierungsempfehlungen identifiziert hat, die eine geplante blaue/grüne Bereitstellung erfordern.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version": "0",
  "id": "3acb26c8-397c-4c89-a80a-ce672a864c55",
  "detail-type": "Amazon OpenSearch Service Auto-Tune Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2020-10-30T22:06:31Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Auto-Tune Event",
    "severity": "Low",
    "status": "Pending",
    "startTime": "{iso8601-timestamp}",
    "description": "Auto-Tune has identified the following settings for your domain
 that require a blue/green deployment: { JVM Heap size : 60%}.
                    You can schedule the deployment for your preferred time."
  }
}
```

Automatische Optimierung abgebrochen

OpenSearch Der Service sendet dieses Ereignis, wenn der Auto-Tune-Zeitplan storniert wurde, weil keine Tuning-Empfehlungen ausstehen.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version": "0",
  "id": "3acb26c8-397c-4c89-a80a-ce672a864c55",
```

```
  "detail-type": "Amazon OpenSearch Service Auto-Tune Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2020-10-30T22:06:31Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Auto-Tune Event",
    "severity": "Low",
    "status": "Cancelled",
    "scheduleTime": "{iso8601-timestamp}",
    "description": "Auto-Tune has cancelled the upcoming blue/green deployment."
  }
}
```

Automatische Optimierung abgeschlossen

OpenSearch Der Dienst sendet dieses Ereignis, wenn Auto-Tune die blaue/grüne Bereitstellung abgeschlossen hat und der Cluster mit den neuen JVM-Einstellungen betriebsbereit ist.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version": "0",
  "id": "3acb26c8-397c-4c89-a80a-ce672a864c55",
  "detail-type": "Amazon OpenSearch Service Auto-Tune Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2020-10-30T22:06:31Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Auto-Tune Event",
    "severity": "Informational",
    "status": "Completed",
    "completionTime": "{iso8601-timestamp}",
    "description": "Auto-Tune has completed the blue/green deployment and successfully
 applied the following settings: { JVM Heap size : 60%}."
  }
}
```

Automatische Optimierung deaktiviert und Änderungen zurückgesetzt

OpenSearch Der Dienst sendet dieses Ereignis, wenn Auto-Tune deaktiviert wurde und die vorgenommenen Änderungen rückgängig gemacht wurden.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version": "0",
  "id": "3acb26c8-397c-4c89-a80a-ce672a864c55",
  "detail-type": "Amazon OpenSearch Service Auto-Tune Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2020-10-30T22:06:31Z",
  "region": "us-east-1",
  "resources": [ "arn:aws:es:us-east-1:123456789012:domain/test-domain" ],
  "detail": {
    "event": "Auto-Tune Event",
    "severity": "Informational",
    "status": "Completed",
    "description": "Auto-Tune is now disabled. All settings have been reverted. Auto-
Tune will continue to evaluate
                    cluster performance and provide recommendations.",
    "completionTime": "{iso8601-timestamp}"
  }
}
```

Automatische Optimierung deaktiviert und Änderungen beibehalten

OpenSearch Der Dienst sendet dieses Ereignis, wenn Auto-Tune deaktiviert wurde und die vorgenommenen Änderungen beibehalten wurden.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version": "0",
  "id": "3acb26c8-397c-4c89-a80a-ce672a864c55",
  "detail-type": "Amazon OpenSearch Service Auto-Tune Notification",
  "source": "aws.es",
```

```
  "account": "123456789012",
  "time": "2020-10-30T22:06:31Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Auto-Tune Event",
    "severity": "Informational",
    "status": "Completed",
    "description": "Auto-Tune is now disabled. The most-recent settings by Auto-Tune
 have been retained.
                    Auto-Tune will continue to evaluate cluster performance and provide
 recommendations.",
    "completionTime": "{iso8601-timestamp}"
  }
}
```

Ereignisse zum Cluster-Zustand

OpenSearch Der Dienst sendet bestimmte Ereignisse an den EventBridge Zeitpunkt, an dem der Zustand Ihres Clusters beeinträchtigt ist.

Wiederherstellung roter Cluster gestartet

OpenSearch Der Dienst sendet dieses Ereignis, nachdem Ihr Clusterstatus länger als eine Stunde ununterbrochen rot angezeigt wurde. Es versucht, einen oder mehrere rote Indizes aus einem Snapshot automatisch wiederherzustellen, um den Clusterstatus zu beheben.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service Cluster Status Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2016-11-01T13:12:22Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
   "detail":{
```

```
      "event":"Automatic Snapshot Restore for Red Indices",
      "status":"Started",
      "severity":"High",
      "description":"Your cluster status is red. We have started automatic snapshot
 restore for the red indices.
                    No action is needed from your side. Red indices [red-index-0, red-
index-1]"
   }
}
```

Wiederherstellung des roten Clusters teilweise abgeschlossen

OpenSearch Der Dienst sendet dieses Ereignis, wenn er nur eine Teilmenge der roten Indizes aus einem Snapshot wiederherstellen konnte, während er versucht, einen roten Clusterstatus zu korrigieren.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service Cluster Status Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2016-11-01T13:12:22Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
   "detail":{
      "event":"Automatic Snapshot Restore for Red Indices",
      "status":"Partially Restored",
      "severity":"High",
      "description":"Your cluster status is red. We were able to restore the following
 Red indices from
                   snapshot: [red-index-0]. Indices not restored: [red-index-1].
 Please refer https://docs.aws.amazon.com/opensearch-service/latest/developerguide/
handling-errors.html#handling-errors-red-cluster-status for troubleshooting steps."
   }
}
```

Wiederherstellung roter Cluster fehlgeschlagen

OpenSearch Der Dienst sendet dieses Ereignis, wenn er beim Versuch, einen roten Clusterstatus zu korrigieren, keine Indizes wiederherstellen kann.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service Cluster Status Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2016-11-01T13:12:22Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
   "detail":{
      "event":"Automatic Snapshot Restore for Red Indices",
      "status":"Failed",
      "severity":"High",
      "description":"Your cluster status is red. We were unable to restore the Red
 indices automatically.
                    Indices not restored: [red-index-0, red-index-1]. Please refer
 https://docs.aws.amazon.com/opensearch-service/latest/developerguide/handling-
errors.html#handling-errors-red-cluster-status for troubleshooting steps."
   }
}
```

Zu löschende Shards

OpenSearch Der Dienst sendet dieses Ereignis, wenn er versucht hat, Ihren roten Clusterstatus automatisch zu korrigieren, nachdem dieser 14 Tage lang ununterbrochen rot war, aber ein oder mehrere Indizes rot bleiben. Nach weiteren 7 Tagen (insgesamt 21 Tage ununterbrochen rot) löscht der OpenSearch Service weiterhin nicht zugewiesene Shards auf allen roten Indizes.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service Cluster Status Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2022-04-09T10:36:48Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
   "detail":{
      "severity":"Medium",
      "description":"Your cluster status is red. Please fix the red indices as soon as
 possible.
                    If not fixed by 2022-04-12 01:51:47+00:00, we will delete all
 unassigned shards,
                    the unit of storage and compute, for these red indices to recover
 your domain and make it green.
                    Please refer to https://docs.aws.amazon.com/opensearch-service/
latest/developerguide/handling-errors.html#handling-errors-red-cluster-status for
 troubleshooting steps.
                    test_data, test_data1",
      "event":"Automatic Snapshot Restore for Red Indices",
      "status":"Shard(s) to be deleted"
   }
}
```

Shards gelöscht

OpenSearch Der Service sendet dieses Ereignis, nachdem Ihr Clusterstatus 21 Tage lang ununterbrochen rot war. Er löscht die nicht zugewiesenen Shards (Speicher und Berechnung) auf allen roten Indizes. Details hierzu finden Sie unter the section called “Automatische Behebung von roten Clustern”.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service Cluster Status Notification",
```

```
   "source":"aws.es",
   "account":"123456789012",
   "time":"2022-04-09T10:54:48Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
   "detail":{
      "severity":"High",
      "description":"We have deleted unassinged shards, the unit of storage and
 compute, in
                    red indices: index-1, index-2 because these indices were red for
 more than
                    21 days and could not be restored with the automated restore
 process.
                    Please refer to https://docs.aws.amazon.com/opensearch-service/
latest/developerguide/handling-errors.html#handling-errors-red-cluster-status for
 troubleshooting steps.",
      "event":"Automatic Snapshot Restore for Red Indices",
      "status":"Shard(s) deleted"
   }
}
```

Warnung mit hoher Shard-Anzahl

OpenSearch Der Service sendet dieses Ereignis, wenn die durchschnittliche Anzahl der Shards auf Ihren Hot-Data-Nodes 90% der empfohlenen Standardgrenze von 1.000 überschritten hat. Spätere Versionen von Elasticsearch OpenSearch unterstützen zwar ein konfigurierbares Limit für die maximale Anzahl an Shards pro Knoten, wir empfehlen jedoch, nicht mehr als 1.000 Shards pro Knoten zu verwenden. Siehe Auswahl der Anzahl der Shards

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2016-11-01T13:12:22Z",
  "region":"us-east-1",
```

```
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"High Shard Count",
     "status":"Warning",
     "severity":"Low",
     "description":"One or more data nodes have close to 1000 shards. To ensure optimum
 performance and stability of your
                   cluster, please refer to the best practice guidelines - https://
docs.aws.amazon.com/opensearch-service/latest/developerguide/sizing-domains.html#bp-
sharding."
  }
}
```

Limit für Shard-Anzahl überschritten

OpenSearch Der Service sendet dieses Ereignis, wenn die durchschnittliche Anzahl der Shards auf Ihren Hot-Data-Nodes den empfohlenen Standardgrenzwert von 1.000 überschritten hat. Spätere Versionen von Elasticsearch OpenSearch unterstützen zwar ein konfigurierbares Limit für die maximale Anzahl an Shards pro Knoten, wir empfehlen jedoch, nicht mehr als 1.000 Shards pro Knoten zu verwenden. Siehe Auswahl der Anzahl der Shards

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2016-11-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"High Shard Count",
     "status":"Warning",
     "severity":"Medium",
     "description":"One or more data nodes have more than 1000 shards. To ensure
 optimum performance and stability of your
                   cluster, please refer to the best practice guidelines - https://
docs.aws.amazon.com/opensearch-service/latest/developerguide/sizing-domains.html#bp-
sharding."
```

```
  }
}
```

Geringer Speicherplatz

OpenSearch Der Service sendet dieses Ereignis, wenn ein oder mehrere Knoten in Ihrem Cluster weniger als 25% des verfügbaren Speicherplatzes oder weniger als 25 GB haben.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"Low Disk Space",
     "status":"Warning",
     "severity":"Medium",
     "description":"One or more data nodes in your cluster has less than 25% of storage
 space or less than 25GB.
                  Your cluster will be blocked for writes at 20% or 20GB. Please refer
 to the documentation for more information - https://docs.aws.amazon.com/opensearch-
service/latest/developerguide/handling-errors.html#troubleshooting-cluster-block"
  }
}
```

Geringer Speicherplatz

OpenSearch Der Service sendet dieses Ereignis, wenn alle Knoten in Ihrem Cluster weniger als 10% des verfügbaren Speicherplatzes oder weniger als 10 GB haben. Wenn alle Knoten das Wasserzeichen für den niedrigen Festplattenwert überschreiten, führt jeder neue Index zu einem gelben Cluster, und wenn alle Knoten das Wasserzeichen für die hohe Festplatte unterschreiten, führt dies zu einem roten Cluster.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"Low Disk Watermark Breach",
     "status":"Warning",
     "severity":"Medium",
     "description":"Low Disk Watermark threshold is about to be breached. Once the
 threshold is breached, new index creation will be blocked on all
                   nodes to prevent the cluster status from turning red. Please
 increase disk size to suit your storage needs. For more information,
                   see https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/handling-errors.html#troubleshooting-cluster-block".
  }
}
```

EBS-Burst-Balance unter 70 %

OpenSearch Der Dienst sendet dieses Ereignis, wenn der EBS-Burst-Saldo auf einem oder mehreren Datenknoten unter 70% fällt. Eine Erschöpfung der EBS-Burst-Balance kann zu einer weit verbreiteten Nichtverfügbarkeit des Clusters und zur Drosselung von E/A-Anfragen führen, was hohe Latenzzeiten und Timeouts bei Indizierungs- und Suchanfragen zur Folge haben kann. Schritte zur Behebung dieses Problems finden Sie unter the section called “Niedrige EBS-Burst-Balance”.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
```

```
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"EBS Burst Balance",
     "status":"Warning",
     "severity":"Medium",
     "description":"EBS burst balance on one or more data nodes is below 70%.
                    Follow https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/handling-errors.html#handling-errors-low-ebs-burst
                    to fix this issue."
  }
}
```

EBS-Burst-Balance unter 20 %

OpenSearch Der Service sendet dieses Ereignis, wenn der EBS-Burst-Saldo auf einem oder mehreren Datenknoten unter 20% fällt. Eine Erschöpfung der EBS-Burst-Balance kann zu einer weit verbreiteten Nichtverfügbarkeit des Clusters und zur Drosselung von E/A-Anfragen führen, was hohe Latenzzeiten und Timeouts bei Indizierungs- und Suchanfragen zur Folge haben kann. Schritte zur Behebung dieses Problems finden Sie unter the section called “Niedrige EBS-Burst-Balance”.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"EBS Burst Balance",
     "status":"Warning",
     "severity":"High",
     "description":"EBS burst balance on one or more data nodes is below 20%.
                    Follow https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/handling-errors.html#handling-errors-low-ebs-burst
```

```
                    to fix this issue.
  }
}
```

Drosselung des Festplattendurchsatzes

OpenSearch Der Service sendet dieses Ereignis, wenn Lese- und Schreibanforderungen an Ihre Domain aufgrund der Durchsatzbeschränkungen Ihrer EBS-Volumes oder EC2-Instance gedrosselt werden. Wenn Sie diese Benachrichtigung erhalten, sollten Sie erwägen, Ihre Volumes oder Instances entsprechend den empfohlenen Best Practices zu skalieren. AWS Wenn Ihr Datenträgertyp istgp2, erhöhen Sie die Volumegröße. Wenn Ihr Datenträgertyp istgp3, sorgen Sie für mehr Durchsatz. Sie können auch überprüfen, ob Ihre Instance-Basis und der maximale EBS-Durchsatz größer oder gleich dem bereitgestellten Volumendurchsatz sind, und können entsprechend skalieren.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"Disk Throughput Throttle",
     "status":"Warning",
     "severity":"Medium",
     "description":"Your domain is experiencing throttling due to instance or volume
 throughput limitations.
                    Please consider scaling your domain to suit your throughput needs.
 In July 2023, we improved
                    the accuracy of throughput throttle calculation by replacing ‘Max
 volume throughput’ with
                    ‘Provisioned volume throughput’. Please refer to the documentation
 for more information."
  }
}
```

Große Shard-Größe

OpenSearch Der Dienst sendet dieses Ereignis, wenn ein oder mehrere Shards in Ihrem Cluster entweder 50 GiB oder 65 GiB überschritten haben. Um eine optimale Leistung und Stabilität des Clusters zu gewährleisten, sollten Sie die Shard-Größe reduzieren.

Weitere Informationen finden Sie in den Best Practices für Sharding.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"Large Shard Size",
     "status":"Warning",
     "severity":"Medium",
     "description":"One or more shards are larger than 65GiB. To ensure optimum cluster
 performance and stability, reduce shard sizes.
                   For more information, see https://docs.aws.amazon.com/opensearch-
service/latest/developerguide/monitoring-events.html#monitoring-events-large-shard-
size."
  }
}
```

Hohe JVM-Nutzung

OpenSearch Der Service sendet dieses Ereignis, wenn die `JVMMemoryPressure` Metrik für Ihre Domain 80% überschritten hat. Wenn der Wert 30 Minuten lang 92% überschreitet, werden alle Schreibvorgänge in Ihrem Cluster blockiert. Um eine optimale Clusterstabilität zu gewährleisten, reduzieren Sie den Datenverkehr zum Cluster oder skalieren Sie Ihre Domain, um ausreichend Arbeitsspeicher für Ihre Arbeitslast bereitzustellen.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"High JVM Usage",
     "status":"Warning",
     "severity":"High",
     "description":"JVM memory pressure has exceeded 80%. If it exceeds 92% for 30
 minutes, all write operations to your cluster
                   will be blocked. To ensure optimum cluster stability, reduce
 traffic to the cluster or use larger instance types.
                   For more information, see https://docs.aws.amazon.com/opensearch-
service/latest/developerguide/monitoring-events.html#monitoring-events-high-jvm."
  }
}
```

Unzureichender GC

OpenSearch Der Dienst sendet dieses Ereignis, wenn der maximale JVM-Wert über 70% liegt und der Unterschied zwischen dem Maximum und dem Minimum weniger als 30% beträgt. Dies kann darauf hindeuten, dass die JVM während der Garbage-Collection-Zyklen nicht in der Lage ist, ausreichend Speicher für Ihre Arbeitslast zurückzugewinnen. Dies kann zu immer langsameren Reaktionen und höheren Latenzen führen. In einigen Fällen kann es sogar zu Knotenausfällen aufgrund von Integritätsprüfungen kommen, bei denen das Timeout abgelaufen ist. Um eine optimale Clusterstabilität zu gewährleisten, reduzieren Sie den Datenverkehr zum Cluster oder skalieren Sie Ihre Domain, um ausreichend Arbeitsspeicher für Ihre Arbeitslast bereitzustellen.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version":"0",
```

```
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"Insufficient GC",
     "status":"Warning",
     "severity":"Medium",
     "description":"Maximum JVM is above 70% and JVM range is less than 30%. This may
 indicate insufficient garbage collection for your workload.
                   For more information, see https://docs.aws.amazon.com/opensearch-
service/latest/developerguide/monitoring-events.html#monitoring-events-insufficient-
gc."
  }
}
```

Warnung beim benutzerdefinierten Index-Routing

OpenSearch Der Dienst sendet dieses Ereignis, wenn sich Ihre Domain im Verarbeitungsstatus befindet und Indizes mit benutzerdefinierten index.routing.allocation-Einstellungen enthält, was dazu führen kann, dass blaugrüne Bereitstellungen hängen bleiben. Stellen Sie sicher, dass die Einstellungen ordnungsgemäß angewendet wurden.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"Custom Index Routing Warning",
     "status":"Warning",
     "severity":"Medium",
```

```
     "description":"Your domain is in processing state and contains indice(s) with
 custom index.routing.allocation
                    settings which can cause blue-green deployments to get stuck.
 Verify settings are applied properly.
                    For more information, see https://docs.aws.amazon.com/opensearch-
service/latest/developerguide/monitoring-events.html#monitoring-events-index-routing."
  }
}
```

Shard-Lock ist fehlgeschlagen

OpenSearch Der Service sendet dieses Ereignis, wenn Ihre Domain aufgrund nicht zugewiesener Shards mit defekt ist. `[ShardLockObtainFailedException]` Weitere Informationen finden Sie unter Wie behebe ich die In-Memory-Shard-Sperrausnahme in Amazon OpenSearch Service?

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"Failed Shard Lock",
     "status":"Warning",
     "severity":"Medium",
     "description":"Your domain is unhealthy due to unassigned shards with
 [ShardLockObtainFailedException]. For more information,
                    see https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/monitoring-events.html#monitoring-events-failed-shard-lock."
}
```

VPC-Endpunktereignisse

OpenSearch Der Service sendet bestimmte Ereignisse an Endpunkte, die sich auf AWS PrivateLink Schnittstellen EventBridge beziehen.

Erstellung eines VPC-Endpunkts fehlgeschlagen

OpenSearch Der Dienst sendet dieses Ereignis, wenn er keinen angeforderten VPC-Endpunkt erstellen kann. Dieser Fehler kann auftreten, weil Sie das Limit für die Anzahl der in einer Region zulässigen VPC-Endpunkte erreicht haben. Dieser Fehler wird auch angezeigt, wenn ein bestimmtes Subnetz oder eine Sicherheitsgruppe nicht vorhanden ist.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service VPC Endpoint Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2016-11-01T13:12:22Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
   "detail":{
      "event":"VPC Endpoint Create Validation",
      "status":"Failed",
      "severity":"High",
      "description":"Unable to create VPC endpoint aos-0d4c74c0342343 for domain
                     arn:aws:es:eu-south-1:123456789012:domain/my-domain due to the
 following validation failures: You've reached the limit on the
                     number of VPC endpoints that you can create in the AWS Region."
   }
}
```

VPC-Endpunkt-Update fehlgeschlagen

OpenSearch Der Dienst sendet dieses Ereignis, wenn er einen angeforderten VPC-Endpunkt nicht löschen kann.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
```

```
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service VPC Endpoint Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2016-11-01T13:12:22Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
   "detail":{
      "event":"VPC Endpoint Update Validation",
      "status":"Failed",
      "severity":"High",
      "description":"Unable to update VPC endpoint aos-0d4c74c0342343 for domain
                    arn:aws:es:eu-south-1:123456789012:domain/my-domain due to the
 following validation failures: <failure message>."
    }
}
```

Löschen des VPC-Endpunkts fehlgeschlagen

OpenSearch Der Dienst sendet dieses Ereignis, wenn er einen angeforderten VPC-Endpunkt nicht löschen kann.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service VPC Endpoint Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2016-11-01T13:12:22Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
   "detail":{
      "event":"VPC Endpoint Delete Validation",
      "status":"Failed",
```

```
      "severity":"High",
      "description":"Unable to delete VPC endpoint aos-0d4c74c0342343 for domain
                    arn:aws:es:eu-south-1:123456789012:domain/my-domain due to the
 following validation failures: Specified subnet doesn't exist."
    }
}
```

Ereignisse beim Ausscheiden eines Knotens

OpenSearch Der Dienst sendet Ereignisse an den EventBridge Zeitpunkt, an dem eines der folgenden Ereignisse beim Ausscheiden eines Knotens eintritt.

Stilllegung des Knotens geplant

OpenSearch Der Dienst sendet dieses Ereignis, wenn die Außerbetriebnahme eines Knotens geplant wurde.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2023-04-07T10:07:33Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Node Retirement Notification",
    "status": "Scheduled",
    "severity": "Medium",
    "description": "An automated action to retire and replace a node has been scheduled
 on your domain.
                    The node will be replaced in the next off-peak window. For more
 information, see
                    https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/monitoring-events.html."
  }
}
```

Der Ausfall des Knotens ist abgeschlossen

OpenSearch Der Dienst sendet dieses Ereignis, wenn die Außerbetriebnahme eines Knotens abgeschlossen ist.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2023-04-07T10:07:33Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Node Retirement Notification",
    "status": "Completed",
    "severity": "Medium",
    "description": "The node has been retired and replaced with a new node."
  }
}
```

Der Ausfall eines Knotens ist fehlgeschlagen

OpenSearch Der Dienst sendet dieses Ereignis, wenn die Außerbetriebnahme eines Knotens fehlschlägt.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2023-04-07T10:07:33Z",
  "region": "us-east-1",
```

```
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Node Retirement Notification",
    "status": "Failed",
    "severity": "Medium",
    "description": "Node retirement failed. No actions are required from your end. We
 will automatically
                   retry replacing the node."
  }
}
```

Ereignisse, bei denen der Knoten heruntergefahren ist

OpenSearch Der Dienst sendet diese Ereignisse, wenn aufgrund einer heruntergekommenen Hardware auf einem Knoten ein Austausch eines Knotens erforderlich ist.

Benachrichtigung über die Außerbetriebnahme eines heruntergekommenen

OpenSearch Der Service sendet dieses Ereignis, wenn die automatische Aktion zur Außerbetriebnahme und zum Austausch eines heruntergekommenen Knotens für Ihre Domain geplant wurde.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
   "version":"0",
   "id":"db233454-aad1-7676-3b15-10a84b052baa",
   "detail-type":"Amazon OpenSearch Service Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2024-01-11T08:16:06Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-node-replacement"
   ],
   "detail":{
      "severity":"Medium",
      "description":"An automated action to retire and replace a node has
 been scheduled on your domain. For more information, please see https://
docs.aws.amazon.com/opensearch-service/latest/developerguide/monitoring-events.html.",
      "event":"Degraded Node Retirement Notification",
```

```
      "status":"Scheduled"
   }
}
```

Außerbetriebnahme eines heruntergestuften Knotens abgeschlossen

OpenSearch Der Dienst sendet dieses Ereignis, wenn ein heruntergestufter Knoten ausgemustert und durch einen neuen Knoten ersetzt wurde.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
   "version":"0",
   "id":"7444215c-90f9-a52d-bcda-e85973a9a762",
   "detail-type":"Amazon OpenSearch Service Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2024-01-11T10:20:30Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-node-replacement"
   ],
   "detail":{
      "severity":"Medium",
      "description":"The node has been retired and replaced with a new node.",
      "event":"Degraded Node Retirement Notification",
      "status":"Completed"
   }
}
```

Ausfall eines heruntergestuften Knotens ist fehlgeschlagen

OpenSearch Der Dienst sendet dieses Ereignis, wenn die Außerbetriebnahme des heruntergestuften Knotens fehlgeschlagen ist.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
```

```
   "version":"0",
   "id":"c328e9bb-93b9-c0b2-b17a-df527fdf96b6",
   "detail-type":"Amazon OpenSearch Service Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2024-01-11T08:31:38Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-node-replacement"
   ],
   "detail":{
      "severity":"Medium",
      "description":"Node retirement failed. No actions are required from your end. We
 will automatically re-try replacing the node.",
      "event":"Degraded Node Retirement Notification",
      "status":"Failed"
   }
}
```

Ereignisse für Domain-Fehler

OpenSearch Der Dienst sendet Ereignisse an, EventBridge wenn einer der folgenden Domänenfehler auftritt.

Fehler bei Validierung von Domain-Updates

OpenSearch Der Dienst sendet dieses Ereignis, wenn er beim Versuch, eine Domain zu aktualisieren oder eine Konfigurationsänderung vorzunehmen, auf einen oder mehrere Validierungsfehler stößt. Wie Sie diese Fehler beheben erfahren Sie unter the section called “Beheben von Validierungsfehlern”.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service Domain Update Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2016-11-01T13:12:22Z",
```

```
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
   "detail":{
      "event":"Domain Update Validation",
      "status":"Failed",
      "severity":"High",
      "description":"Unable to perform updates to your domain due to the following
 validation failures: <failures>
                    Please see the documentation for more information https://
docs.aws.amazon.com/opensearch-service/latest/developerguide/managedomains-
configuration-changes.html#validation"
   }
}
```

KMS-Schlüssel unzugänglich

OpenSearch Der Dienst sendet dieses Ereignis, wenn er nicht auf Ihren AWS KMS Schlüssel zugreifen kann.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Domain Error Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2016-11-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"KMS Key Inaccessible",
     "status":"Error",
     "severity":"High",
     "description":"The KMS key associated with this domain is inaccessible. You are at
 risk of losing access to your domain.
                    For more information, please refer to https://docs.aws.amazon.com/
opensearch-service/latest/developerguide/encryption-at-rest.html#disabled-key."
  }
```

```
}
```

Isolierung von Domänen

OpenSearch Der Dienst sendet dieses Ereignis, wenn Ihre Domain isoliert ist und keine Anfragen empfangen, lesen oder schreiben kann, weil sie für das Netzwerk nicht erreichbar ist.

Beispiel

Es folgt ein Beispiel für diesen Ereignistyp:

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2023-11-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"Domain Isolation Notification",
     "status":"Error",
     "severity":"High",
     "description":"Your OpenSearch Service domain has been isolated. An isolated
 domain is unreachable by network and cannot receive, read, or write requests. For more
 information and assistance, please contact AWS Support at https://docs.aws.amazon.com/
opensearch-service/latest/developerguide/encryption-at-rest.html#disabled-key."
  }
}
```

Tutorial: Auf Amazon OpenSearch EventBridge Service-Ereignisse achten

In diesem Tutorial richten Sie eine einfache AWS Lambda Funktion ein, die auf Amazon OpenSearch Service-Ereignisse wartet und diese in einen CloudWatch Logs-Protokollstream schreibt.

Voraussetzungen

In diesem Tutorial wird davon ausgegangen, dass Sie über eine bestehende OpenSearch Service-Domain verfügen. Wenn Sie noch keine Domain erstellt haben, führen Sie die Schritte unter Erstellen und Verwalten von Domains aus, um eine zu erstellen.

Schritt 1: Erstellen der Lambda-Funktion

In diesem Verfahren erstellen Sie eine einfache Lambda-Funktion, die als Ziel für OpenSearch Service-Ereignismeldungen dient.

So erstellen Sie eine Lambda-Zielfunktion

1. Öffnen Sie die AWS Lambda Konsole unter https://console.aws.amazon.com/lambda/.
2. Wählen Sie Eine Funktion erstellen und Von Grund auf neu erstellen aus.
3. Geben Sie für Funktionsname den Event-Handler an.
4. Wählen Sie für Runtime (Laufzeit) die Option Python 3.8 aus.
5. Wählen Sie Funktion erstellen.
6. Bearbeiten Sie im Bereich Function code den Beispiel-Code entsprechend dem folgenden Beispiel:

   ```
   import json

   def lambda_handler(event, context):
       if event["source"] != "aws.es":
           raise ValueError("Function only supports input from events with a source
    type of: aws.es")

       print(json.dumps(event))
   ```

   Dies ist eine einfache Python 3.8-Funktion, die die vom OpenSearch Service gesendeten Ereignisse ausgibt. Wenn alles korrekt konfiguriert ist, werden die Ereignisdetails am Ende dieses Tutorials im CloudWatch Log-Protokollstream angezeigt, der dieser Lambda-Funktion zugeordnet ist.
7. Wählen Sie Bereitstellen.

Schritt 2: Registrieren von Ereignisregeln

In diesem Schritt erstellen Sie eine EventBridge Regel, die Ereignisse aus Ihren OpenSearch Service-Domänen erfasst. Diese Regel erfasst alle Ereignisse in dem Konto, in dem sie definiert ist. Die Ereignisnachrichten selbst enthalten Informationen über die Ereignisquelle, einschließlich der Domain, aus der sie stammen. Sie können diese Informationen verwenden, um Ereignisse programmgesteuert zu filtern und zu sortieren.

Um eine EventBridge Regel zu erstellen

1. Öffnen Sie die EventBridge Konsole unter https://console.aws.amazon.com/events/.
2. Wählen Sie Regel erstellen aus.
3. Nennen Sie die Regel Event-Regel.
4. Wählen Sie Weiter aus.
5. Wählen Sie für das Ereignismuster AWS Services, Amazon OpenSearch Service und All Events aus. Dieses Muster gilt für alle Ihre OpenSearch Service-Domains und für jedes OpenSearch Service-Ereignis. Alternativ können Sie ein spezifischeres Muster erstellen, damit bestimmte Ergebnisse gefiltert werden.
6. Wählen Sie Weiter aus.
7. Wählen Sie für das Ziel Lambda-Funktion aus. Wählen Sie im Funktions-Dropdown-Menü Ereignis-Handler aus.
8. Wählen Sie Weiter aus.
9. Überspringen Sie die Tags und wählen Sie erneut Weiter aus.
10. Prüfen Sie die Konfiguration und wählen Sie Regel erstellen aus.

Schritt 3: Testen der Konfiguration

Wenn Sie das nächste Mal eine Benachrichtigung im Bereich Benachrichtigungen der OpenSearch Servicekonsole erhalten und alles richtig konfiguriert ist, wird Ihre Lambda-Funktion ausgelöst und die Ereignisdaten werden in einen CloudWatch Log-Log-Stream für die Funktion geschrieben.

So testen Sie die Konfiguration

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Logs (Protokolle) und die Protokollgruppe für Ihre Lambda-Funktion aus (z. B. /aws/lambda/event-handler).
3. Wählen Sie einen Protokollstream aus, um die Ereignisdaten anzuzeigen.

Tutorial: Senden von Amazon-SNS-Warnungen für verfügbare Softwareupdates

In diesem Tutorial konfigurieren Sie eine EventBridge Amazon-Ereignisregel, die Benachrichtigungen über verfügbare Service-Software-Updates in Amazon OpenSearch Service erfasst und Ihnen eine E-Mail-Benachrichtigung über Amazon Simple Notification Service (Amazon SNS) sendet.

Voraussetzungen

In diesem Tutorial wird davon ausgegangen, dass Sie über eine bestehende OpenSearch Service-Domain verfügen. Wenn Sie noch keine Domain erstellt haben, führen Sie die Schritte unter Erstellen und Verwalten von Domains aus, um eine zu erstellen.

Schritt 1: Erstellen und Abonnieren eines Amazon-SNS-Themas

Konfigurieren Sie ein Amazon-SNS-Thema, das als Ereignisziel für Ihre neue Ereignisregel dient.

So erstellen Sie ein Amazon-SNS-Ziel

1. Öffnen Sie die Amazon SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home.
2. Klicken Sie auf Themen und Erstellen eines Themas.
3. Wählen Sie als Auftragstyp Standard aus und benennen Sie den Auftrag software-update.
4. Wählen Sie Thema erstellen aus.
5. Nachdem das Thema erstellt wurde, wählen Sie Erstellen eines Abonnements.
6. Wählen Sie unter Protocol (Protokoll) die Option Email (E-Mail) aus. Geben Sie für Endpunkt eine E-Mail-Adresse ein, auf die Sie aktuell Zugriff haben, und wählen Sie Abonnement erstellen aus.
7. Überprüfen Sie Ihr E-Mail-Konto und warten Sie auf eine E-Mail-Nachricht zur Bestätigung Ihres Abonnements. Wenn Sie sie erhalten, wählen Sie Confirm Abonnement aus.

Schritt 2: Registrieren von Ereignisregeln

Als nächstes registrieren Sie eine Ereignisregel, die nur Service-Software-Updateereignisse erfasst.

So erstellen Sie eine Ereignisregel

1. Öffnen Sie die EventBridge Konsole unter https://console.aws.amazon.com/events/.

2. Wählen Sie Regel erstellen aus.
3. Benennen Sie die Regel softwareupdate-rule.
4. Wählen Sie Weiter aus.
5. Wählen Sie für das Ereignismuster AWS Services, Amazon OpenSearch Service und Amazon OpenSearch Service Software Update Notification aus. Dieses Muster entspricht jedem Service-Software-Update-Ereignis von OpenSearch Service. Weitere Informationen zu Ereignismustern finden Sie unter EventBridge Amazon-Ereignismuster im EventBridgeAmazon-Benutzerhandbuch.
6. Optional können Sie auch auf bestimmte Schweregrade filtern. Die Schweregrade jedes Ereignisses finden Sie unter the section called “Aktualisieren der Software”.
7. Wählen Sie Weiter aus.
8. Wählen Sie für das Ziel SNS-Thema und dann Software-Update aus.
9. Wählen Sie Weiter aus.
10. Überspringen Sie die Tags und wählen Sie Weiter aus.
11. Prüfen Sie die Regelkonfiguration und wählen Sie Regel erstellen aus.

Wenn Sie das nächste Mal eine Benachrichtigung von OpenSearch Service über ein verfügbares Service-Software-Update erhalten und alles richtig konfiguriert ist, sollte Amazon SNS Ihnen eine E-Mail-Benachrichtigung über das Update senden.

Überwachen von OpenSearch Amazon--Service-API-Aufrufen mit AWS CloudTrail

Amazon OpenSearch Service ist in integriertAWS CloudTrail, einen Service, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem AWS -Service in OpenSearch Service durchgeführten Aktionen bietet. CloudTrailerfasst Konfigurations-API-Aufrufe an OpenSearch Service als Ereignisse.

> **Note**
>
> CloudTrailerfasst nur Aufrufe an die Konfigurations-API wie `CreateDomain` und`GetUpgradeStatus`. CloudTrailerfasst keine Aufrufe an die OpenSearchAPIs wie `_search` und`_bulk`. Informationen zu diesen Aufrufen finden Sie unter the section called “Überwachen der Prüfprotokolle”.

Die erfassten Aufrufe umfassen Aufrufe von der OpenSearch ServicekonsoleAWS CLI, oder einem AWS -SDK. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon-S3-Bucket, einschließlich Ereignisse für OpenSearch Service aktivieren. Auch wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse in der CloudTrail-Konsole in Event history (Ereignisverlauf) anzeigen. Mit den von CloudTrail gesammelten Informationen können Sie die an OpenSearch Service gestellte Anfrage, die IP-Adresse, von der die Anforderung gestellt wurde, den initiator der Anfrage, den Zeitpunkt der Anfrage und zusätzliche Details bestimmen.

Weitere Informationen zu CloudTrail finden Sie im AWS CloudTrail-Benutzerhandbuch.

Informationen zu Amazon OpenSearch Service in CloudTrail

CloudTrail wird beim Erstellen Ihres Kontos auf AWS-Konto aktiviert. Die in OpenSearch Service auftretenden Aktivitäten werden als CloudTrail Ereignis zusammen mit anderen AWS -Serviceereignissen im Ereignisverlauf aufgezeichnet. Sie können die neusten Ereignisse in Ihr AWS-Konto-Konto herunterladen und dort suchen und anzeigen. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail-API-Ereignisverlauf.

Erstellen Sie für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS-Konto -Konto, einschließlich Ereignisse für OpenSearch Service, einen Trail. Ein Trail ermöglicht CloudTrail die Bereitstellung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS-Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon S3 Bucket bereit. Darüber hinaus können Sie andere AWS-Services konfigurieren, um die in den CloudTrail-Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie unter:

- Erstellen eines Trails für AWS-Konto
- AWSServiceintegrationen mit Logs CloudTrail
- Konfigurieren von Amazon SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail-Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail-Protokolldateien aus mehreren Konten

Alle OpenSearch Service-Konfigurations-API-Aktionen werden von der Amazon--Service-Konfigurations-API-Referenz protokolliert CloudTrail und sind in der API-Referenz OpenSearch für Amazon Service Service dokumentiert.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Anhand der Identitätsinformationen zur Benutzeridentität können Sie Folgendes bestimmen:

- Ob die Anfrage mit Root- oder AWS Identity and Access Management (IAM)-Benutzer-Anmeldeinformationen ausgeführt wurde.
- Ob die Anfrage mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen föderierten Benutzer ausgeführt wurde
- Ob die Anforderung von einem anderen AWS-Service getätigt wurde.

Weitere Informationen finden Sie unter CloudTrail userIdentity-Element.

Erläuterungen der OpenSearch Amazon-Service-Protokolldateieinträge

Ein Trail ist eine Konfiguration, durch die Ereignisse als Protokolldateien an den von Ihnen angegebenen Amazon-S3-Bucket übermittelt werden. CloudTrail-Protokolldateien können einen oder mehrere Einträge enthalten. Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält unter anderem Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion sowie über die Anfrageparameter. CloudTrail-Protokolleinträge sind kein geordnetes Stacktrace der öffentlichen API-Aufrufe und erscheinen daher nicht in einer bestimmten Reihenfolge.

Das folgende Beispiel zeigt einen CloudTrail-Protokolleintrag, der die Operation `CreateDomain` demonstriert:

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::123456789012:user/test-user",
    "accountId": "123456789012",
    "accessKeyId": "access-key",
    "userName": "test-user",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2018-08-21T21:59:11Z"
      }
    },
    "invokedBy": "signin.amazonaws.com"
```

```
  },
  "eventTime": "2018-08-21T22:00:05Z",
  "eventSource": "es.amazonaws.com",
  "eventName": "CreateDomain",
  "awsRegion": "us-west-1",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "signin.amazonaws.com",
  "requestParameters": {
    "engineVersion": "OpenSearch_1.0",
    "clusterConfig": {
      "instanceType": "m4.large.search",
      "instanceCount": 1
    },
    "snapshotOptions": {
      "automatedSnapshotStartHour": 0
    },
    "domainName": "test-domain",
    "encryptionAtRestOptions": {},
    "eBSOptions": {
      "eBSEnabled": true,
      "volumeSize": 10,
      "volumeType": "gp2"
    },
    "accessPolicies": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect\":\"Allow
\",\"Principal\":{\"AWS\":[\"123456789012\"]},\"Action\":[\"es:*\"],\"Resource\":
\"arn:aws:es:us-west-1:123456789012:domain/test-domain/*\"}]}",
    "advancedOptions": {
      "rest.action.multi.allow_explicit_index": "true"
    }
  },
  "responseElements": {
    "domainStatus": {
      "created": true,
      "clusterConfig": {
        "zoneAwarenessEnabled": false,
        "instanceType": "m4.large.search",
        "dedicatedMasterEnabled": false,
        "instanceCount": 1
      },
      "cognitoOptions": {
        "enabled": false
      },
      "encryptionAtRestOptions": {
        "enabled": false
```

```
      },
      "advancedOptions": {
        "rest.action.multi.allow_explicit_index": "true"
      },
      "upgradeProcessing": false,
      "snapshotOptions": {
        "automatedSnapshotStartHour": 0
      },
      "eBSOptions": {
        "eBSEnabled": true,
        "volumeSize": 10,
        "volumeType": "gp2"
      },
      "engineVersion": "OpenSearch_1.0",
      "processing": true,
      "aRN": "arn:aws:es:us-west-1:123456789012:domain/test-domain",
      "domainId": "123456789012/test-domain",
      "deleted": false,
      "domainName": "test-domain",
      "accessPolicies": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect\":\"Allow
\",\"Principal\":{\"AWS\":\"arn:aws:iam::123456789012:root\"},\"Action\":\"es:*\",
\"Resource\":\"arn:aws:es:us-west-1:123456789012:domain/test-domain/*\"}]}"
    }
  },
  "requestID": "12345678-1234-1234-1234-987654321098",
  "eventID": "87654321-4321-4321-4321-987654321098",
  "eventType": "AwsApiCall",
  "recipientAccountId": "123456789012"
}
```

Sicherheit bei Amazon OpenSearch Service

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS Dienste in der AWS Cloud ausführt. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der AWS -Compliance-Programme regelmäßig. Weitere Informationen zu den Compliance-Programmen, die für Amazon OpenSearch Service gelten, finden Sie unter AWS Services in Scope by Compliance Program.
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Service, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Nutzung des OpenSearch Service anwenden können. In den folgenden Themen erfahren Sie, wie Sie den OpenSearch Service so konfigurieren, dass er Ihre Sicherheits- und Compliance-Ziele erfüllt. Sie erfahren auch, wie Sie andere AWS Dienste verwenden können, die Sie bei der Überwachung und Sicherung Ihrer OpenSearch Serviceressourcen unterstützen.

Themen

- Konfiguration der Amazon Cognito Cognito-Authentifizierung für Dashboards OpenSearch
- Verwenden von serviceverknüpften Rollen für Amazon OpenSearch Service

Datenschutz bei Amazon OpenSearch Service

Das AWS Modell der mit gilt für den Datenschutz bei Amazon OpenSearch Service. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS -Modell der geteilten Verantwortung und in der DSGVO im AWS -Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Verwenden Sie SSL/TLS, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit OpenSearch Service oder anderen AWS-Services über die Konsole, API oder SDKs arbeiten. AWS

CLI AWS Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Verschlüsselung von Daten im Ruhezustand für Amazon OpenSearch Service

OpenSearch Service-Domains bieten die Verschlüsselung von Daten im Ruhezustand, eine Sicherheitsfunktion, die dazu beiträgt, unbefugten Zugriff auf Ihre Daten zu verhindern. Die Funktion verwendet AWS Key Management Service (AWS KMS) zum Speichern und Verwalten Ihrer Verschlüsselungsschlüssel und den Advanced Encryption Standard-Algorithmus mit 256-Bit-Schlüsseln (AES-256) für die Verschlüsselung. Wenn die Funktion aktiviert ist, verschlüsselt sie die folgenden Aspekte einer Domain:

- Alle Indizes (einschließlich der Indizes im Speicher) UltraWarm
- OpenSearch Logs
- Swap-Dateien
- Alle anderen Daten im Anwendungsverzeichnis
- Automatisierte Snapshots

Die folgenden Dinge werden nicht verschlüsselt, wenn Sie die Verschlüsselung gespeicherter Daten aktivieren, aber Sie können weitere Schritte zu ihrem Schutz unternehmen:

- Manuelle Schnappschüsse: Sie können derzeit keine AWS KMS Schlüssel verwenden, um manuelle Schnappschüsse zu verschlüsseln. Sie können jedoch eine serverseitige Verschlüsselung mit in S3 verwalteten Schlüsseln oder KMS-Schlüsseln zum Verschlüsseln des Buckets verwenden, den Sie als Snapshot-Repository verwenden. Anweisungen finden Sie unter the section called “Registrieren eines manuellen Snapshot-Repositorys”.
- Langsame Protokolle und Fehlerprotokolle: Wenn Sie Protokolle veröffentlichen und diese verschlüsseln möchten, können Sie die zugehörige CloudWatch Protokollgruppe mit demselben AWS KMS Schlüssel wie die Dienstdomäne verschlüsseln. OpenSearch Weitere Informationen finden Sie unter Verschlüsseln von Protokolldaten in CloudWatch Logs using AWS KMS im Amazon CloudWatch Logs-Benutzerhandbuch.

> **Note**
>
> Sie können die Verschlüsselung im Ruhezustand für eine bestehende Domain nicht aktivieren, wenn UltraWarm oder Cold Storage auf der Domain aktiviert ist. Sie müssen zuerst Cold Storage UltraWarm deaktivieren, Verschlüsselung im Ruhezustand aktivieren und dann Cold Storage wieder aktivieren UltraWarm . Wenn Sie Indizes im Cold Storage UltraWarm oder Cold Storage behalten möchten, müssen Sie sie zunächst in den Hot-Storage verschieben, bevor Sie sie deaktivieren UltraWarm oder Cold Storage aktivieren.

OpenSearch Der Service unterstützt nur KMS-Schlüssel mit symmetrischer Verschlüsselung, keine asymmetrischen Schlüssel. Informationen zum Erstellen symmetrischer Schlüssel finden Sie unter Erstellen von Schlüsseln im AWS Key Management Service -Entwicklerhandbuch.

Unabhängig davon, ob die Verschlüsselung im Ruhezustand aktiviert ist, verschlüsseln alle Domänen automatisch benutzerdefinierte Pakete mithilfe von AES-256 und vom Service verwalteten Schlüsseln. OpenSearch

Berechtigungen

Um die OpenSearch Service-Konsole zur Konfiguration der Verschlüsselung von Daten im Ruhezustand zu verwenden, benötigen Sie Leseberechtigungen AWS KMS, z. B. für die folgende identitätsbasierte Richtlinie:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:List*",
        "kms:Describe*"
      ],
      "Resource": "*"
    }
  ]
}
```

Wenn Sie einen anderen Schlüssel als den AWS eigenen Schlüssel verwenden möchten, müssen Sie auch über die erforderlichen Berechtigungen verfügen, um Berechtigungen für den Schlüssel zu

erstellen. Diese Berechtigung erfolgt in der Regel über eine ressourcenbasierte Richtlinie, die Sie beim Erstellen des Schlüssels angeben.

Wenn Sie Ihren Schlüssel ausschließlich für OpenSearch Service behalten möchten, können Sie dieser Schlüsselrichtlinie die ViaService Bedingung kms: hinzufügen:

```
"Condition": {
  "StringEquals": {
    "kms:ViaService": "es.us-west-1.amazonaws.com"
  },
  "Bool": {
    "kms:GrantIsForAWSResource": "true"
  }
}
```

Weitere Informationen finden Sie unter Verwenden von Schlüsselrichtlinien in AWS KMS im AWS Key Management Service Entwicklerhandbuch.

Verschlüsselung gespeicherter Daten aktivieren

Für die Verschlüsselung ruhender Daten auf neuen Domains ist entweder OpenSearch Elasticsearch 5.1 oder höher erforderlich. Für die Aktivierung auf bestehenden Domains ist entweder Elasticsearch 6.7 OpenSearch oder höher erforderlich.

So aktivieren Sie die Verschlüsselung von Data-at-Rest (Konsole)

1. Öffnen Sie die Domain in der AWS Konsole und wählen Sie dann Aktionen und Sicherheitskonfiguration bearbeiten aus.
2. Wählen Sie unter Verschlüsselung die Option Verschlüsselung von Data-at-Rest aktivieren aus.
3. Wählen Sie einen AWS KMS Schlüssel aus, den Sie verwenden möchten, und klicken Sie dann auf Änderungen speichern.

Sie können die Verschlüsselung auch über die Konfigurations-API aktivieren. Die folgende Anforderung ermöglicht die Verschlüsselung von Daten im Ruhezustand, die sich auf einer vorhandenen Domain befinden:

```
{
   "ClusterConfig":{
      "EncryptionAtRestOptions":{
```

```
        "Enabled": true,
        "KmsKeyId":"arn:aws:kms:us-east-1:123456789012:alias/my-key"
      }
   }
}
```

Deaktivierter oder gelöschter KMS-Schlüssel

Wenn du den Schlüssel, mit dem du eine Domain verschlüsselt hast, deaktivierst oder löschst, kann nicht mehr auf die Domain zugegriffen werden. OpenSearch Der Dienst sendet Ihnen eine Benachrichtigung, in der Sie darüber informiert werden, dass er nicht auf den KMS-Schlüssel zugreifen kann. Aktivieren Sie den Schlüssel erneut umgehend, um auf Ihre Domain zuzugreifen.

Das OpenSearch Serviceteam kann Ihnen nicht helfen, Ihre Daten wiederherzustellen, wenn Ihr Schlüssel gelöscht wird. AWS KMS löscht Schlüssel erst nach einer Wartezeit von mindestens sieben Tagen. Wenn Ihr Schlüssel gelöscht werden soll, brechen Sie entweder die Löschung ab oder machen Sie einen manuellen Snapshot der Domain, um den Verlust Ihrer Daten zu verhindern.

Verschlüsselung gespeicherter Daten deaktivieren

Nachdem Sie eine Domain zum Verschlüsseln von Daten im Ruhezustand konfiguriert haben, können Sie die Einstellung nicht mehr deaktivieren. Stattdessen können Sie einen manuellen Snapshot der vorhandenen Domain erstellen, eine andere Domain erstellen, Ihre Daten migrieren und die alte Domain löschen.

Überwachen von Domains, die Daten im Ruhezustand verschlüsseln

Domains, die Daten im Ruhezustand verschlüsseln, haben zwei zusätzliche Metriken: `KMSKeyError` und `KMSKeyInaccessible`. Diese Metriken werden nur angezeigt, wenn die Domain ein Problem mit Ihrem Verschlüsselungsschlüssel feststellt. Vollständige Beschreibungen dieser Metriken finden Sie unter the section called “Cluster-Metriken”. Sie können sie entweder über die OpenSearch Service-Konsole oder die CloudWatch Amazon-Konsole anzeigen.

> **Tip**
>
> Jede Metrik stellt ein erhebliches Problem für eine Domain dar. Wir empfehlen daher, CloudWatch Alarme für beide zu erstellen. Weitere Informationen finden Sie unter the section called “Empfohlene CloudWatch Alarme”.

Weitere Überlegungen

- Bei der automatischen Schlüsselrotation bleiben die Eigenschaften Ihrer AWS KMS Schlüssel erhalten, sodass die Rotation keine Auswirkungen auf Ihre Fähigkeit hat, auf Ihre OpenSearch Daten zuzugreifen. Verschlüsselte OpenSearch Dienstdomänen unterstützen keine manuelle Schlüsselrotation, bei der ein neuer Schlüssel erstellt und alle Verweise auf den alten Schlüssel aktualisiert werden. Weitere Informationen finden Sie unter Rotieren von Schlüsseln im AWS Key Management Service -Entwicklerhandbuch.
- Bestimmte Instance-Typen unterstützen die Verschlüsselung gespeicherter Daten nicht. Details hierzu finden Sie unter the section called “Unterstützte Instance-Typen”.
- Domains, die gespeicherte Daten verschlüsseln, verwenden einen anderen Repository-Namen für ihre automatischen Snapshots. Weitere Informationen finden Sie unter the section called “Wiederherstellen von Snapshots”.
- Während wir dringend empfehlen, die Verschlüsselung im Ruhezustand zu aktivieren, kann dies zusätzlichen CPU-Overhead und einige Millisekunden Latenz verursachen. Die meisten Anwendungsfälle reagieren jedoch nicht empfindlich auf diese Unterschiede, und das Ausmaß der Auswirkungen hängt von der Konfiguration Ihres Clusters, Ihrer Clients und Ihres Nutzungsprofils ab.

Keine ode-to-node Verschlüsselung für Amazon OpenSearch Service

Die ode-to-node N-Verschlüsselung bietet zusätzlich zu den Standardfunktionen von Amazon OpenSearch Service eine zusätzliche Sicherheitsebene.

Jede OpenSearch Dienstdomäne — unabhängig davon, ob die Domäne VPC-Zugriff verwendet — befindet sich in einer eigenen, dedizierten VPC. Diese Architektur verhindert, dass potenzielle Angreifer den Datenverkehr zwischen Knoten abfangen, und sorgt für die Sicherheit des Clusters. OpenSearch Standardmäßig ist der Datenverkehr innerhalb der VPC jedoch nicht verschlüsselt. ode-to-node N-Verschlüsselung aktiviert die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der VPC.

Wenn Sie Daten über HTTPS an den OpenSearch Service senden, trägt die node-to-node Verschlüsselung dazu bei, dass Ihre Daten bei der OpenSearch Verteilung (und Weiterverteilung) im gesamten Cluster verschlüsselt bleiben. Wenn Daten unverschlüsselt über HTTP ankommen, verschlüsselt der OpenSearch Service sie, nachdem sie den Cluster erreicht haben. Mithilfe der Konsole oder der Konfigurations-API können Sie verlangen, AWS CLI dass der gesamte Datenverkehr zur Domain über HTTPS eingeht.

Wenn Sie eine differenzierte Zugriffskontrolle aktivieren, ist keine ode-to-node Verschlüsselung erforderlich.

Verschlüsselung aktivieren node-to-node

Für die ode-to-node Verschlüsselung neuer Domains ist eine beliebige Version von OpenSearch oder Elasticsearch 6.0 oder höher erforderlich. Für die Aktivierung der node-to-node Verschlüsselung auf bestehenden Domains ist eine beliebige Version von OpenSearch oder Elasticsearch 6.7 oder höher erforderlich. Wählen Sie die vorhandene Domain in der AWS -Konsole, Aktionen und Sicherheitskonfiguration bearbeiten aus.

Alternativ können Sie die Konfigurations-API AWS CLI oder verwenden. Weitere Informationen finden Sie in der AWS CLI Befehlsreferenz und der OpenSearch Service-API-Referenz.

Verschlüsselung wird deaktiviert node-to-node

Nachdem Sie eine Domain für die node-to-node Verschlüsselung konfiguriert haben, können Sie die Einstellung nicht deaktivieren. Stattdessen können Sie einen manuellen Snapshot der verschlüsselten Domain erstellen, eine andere Domain erstellen, Ihre Daten migrieren und die alte Domain löschen.

Identity and Access Management in Amazon OpenSearch Service

Amazon OpenSearch Service bietet verschiedene Möglichkeiten, den Zugriff auf Ihre Domains zu kontrollieren. Dieses Thema geht auf die verschiedenen Richtlinientypen, deren Interaktion miteinander und die Erstellung eigener, benutzerdefinierter Richtlinien ein.

> **Important**
>
> Die VPC-Unterstützung führt zu einigen zusätzlichen Überlegungen zur OpenSearch Dienstzugriffskontrolle. Weitere Informationen finden Sie unter the section called “Zugriffsrichtlinien für VPC-Domänen”.

Arten von Richtlinien

OpenSearch Der Service unterstützt drei Arten von Zugriffsrichtlinien:

- the section called “Ressourcenbasierte Richtlinien”
- the section called “Identitätsbasierte Richtlinien”

- the section called “IP-basierte Richtlinien”

Ressourcenbasierte Richtlinien

Beim Erstellen einer Domain fügen Sie eine ressourcenbasierte Richtlinie hinzu, die oft als Domain-Zugriffsrichtlinie bezeichnet wird. Diese Richtlinien legen fest, welche Aktionen ein Prinzipal auf den Subressourcen der Domain durchführen kann (mit Ausnahme der clusterübergreifenden Suche). Zu den Unterressourcen gehören OpenSearch Indizes und APIs. Das Element Principal gibt die Konten, Benutzer oder Rollen an, denen Zugriff gewährt ist. Das Element Resource gibt an, auf welche Unterressourcen diese Prinzipale zugreifen können.

Beispielsweise gewährt die folgende ressourcenbasierte Richtlinie `test-user` vollen Zugriff (`es:*`) auf die Unterressourcen auf `test-domain`:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::123456789012:user/test-user"
        ]
      },
      "Action": [
        "es:*"
      ],
      "Resource": "arn:aws:es:us-west-1:987654321098:domain/test-domain/*"
    }
  ]
}
```

Zwei wichtige Überlegungen treffen auf diese Richtlinie zu:

- Diese Berechtigungen gelten nur für diese Domain. Sofern Sie keine ähnlichen Richtlinien auf anderen Domains erstellen, kann `test-user` nur auf `test-domain` zugreifen.
- Das nachgestellte `/*` im `Resource`-Element ist wichtig und weist darauf hin, dass ressourcenbasierte Richtlinien nur für die Unterressourcen der Domain gelten, nicht für die Domain selbst. In ressourcenbasierten Richtlinien entspricht die `es:*`-Aktion `es:ESHttp*`.

Beispielsweise kann `test-user` zwar Anforderungen an einen Index (`GET https://search-test-domain.us-west-1.es.amazonaws.com/test-index`) richten, aber nicht die Konfiguration der Domain (`POST https://es.us-west-1.amazonaws.com/2021-01-01/opensearch/domain/test-domain/config`) aktualisieren. Beachten Sie den Unterschied zwischen den beiden Endpunkten. Für den Zugriff auf die Konfigurations-API ist eine identitätsbasierte Richtlinie erforderlich.

Sie können einen partiellen Indexnamen angeben, indem Sie einen Platzhalter hinzufügen. Dieses Beispiel identifiziert alle Indizes, die mit `commerce` beginnen:

```
arn:aws:es:us-west-1:987654321098:domain/test-domain/commerce*
```

In diesem Fall bedeutet der Platzhalter, dass `test-user` Anfragen an Indizes innerhalb von `test-domain` stellen kann, deren Namen mit `commerce` beginnen.

Um `test-user` weiter einzuschränken, können Sie die folgende Richtlinie anwenden:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::123456789012:user/test-user"
        ]
      },
      "Action": [
        "es:ESHttpGet"
      ],
      "Resource": "arn:aws:es:us-west-1:987654321098:domain/test-domain/commerce-data/
_search"
    }
  ]
}
```

Nun kann `test-user` nur noch eine Operation durchführen: die Suche nach dem Index `commerce-data`. Auf alle anderen Indizes innerhalb der Domain kann nicht zugegriffen werden, und ohne die

Berechtigung, die Aktionen `es:ESHttpPut` oder `es:ESHttpPost` zu verwenden, kann `test-user` keine Dokumente hinzufügen oder ändern.

Als nächstes möchten Sie vielleicht eine Rolle für Hauptbenutzer konfigurieren. Diese Richtlinie gewährt `power-user-role`-Zugriff auf die HTTP GET- und PUT-Methoden für alle URIs im Index:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::123456789012:role/power-user-role"
        ]
      },
      "Action": [
        "es:ESHttpGet",
        "es:ESHttpPut"
      ],
      "Resource": "arn:aws:es:us-west-1:987654321098:domain/test-domain/commerce-data/
*"
    }
  ]
}
```

Wenn sich Ihre Domain in einer VPC befindet oder eine differenzierte Zugriffssteuerung verwendet, können Sie eine offene Domain-Zugriffsrichtlinie verwenden. Andernfalls muss Ihre Domain-Zugriffsrichtlinie eine Einschränkung enthalten, entweder nach Prinzipal oder IP-Adresse.

Weitere Informationen zu allen verfügbaren Aktionen finden Sie unter the section called “Richtlinienelementreferenz”. Für eine weitaus detailliertere Kontrolle über Ihre Daten verwenden Sie eine offene Domain-Zugriffsrichtlinie mit differenzierte Zugriffssteuerung.

Identitätsbasierte Richtlinien

Im Gegensatz zu ressourcenbasierten Richtlinien, die Teil jeder OpenSearch Dienstdomäne sind, fügen Sie Benutzern oder Rollen, die den (IAM-) Dienst verwenden, identitätsbasierte Richtlinien zu. AWS Identity and Access Management Genauso wie ressourcenbasierte Richtlinien legen identitätsbasierte Richtlinien fest, welche Personen auf einen Service zugreifen können, welche

Aktionen sie ausführen können und, sofern zutreffend, für welche Ressourcen sie diese Aktionen ausführen können.

Identitätsbasierte Richtlinien sind in der Regel allgemeiner, dies muss aber nicht unbedingt so sein. Sie regeln oft nur die Konfigurations-API-Aktionen, die ein Benutzer durchführen darf. Sobald Sie diese Richtlinien eingerichtet haben, können Sie ressourcenbasierte Richtlinien (oder eine differenzierte Zugriffskontrolle) in OpenSearch Service verwenden, um Benutzern Zugriff auf Indizes und APIs zu gewähren. OpenSearch

> **Note**
>
> Benutzer mit der AWS verwalteten `AmazonOpenSearchServiceReadOnlyAccess` Richtlinie können den Cluster-Integritätsstatus auf der Konsole nicht sehen. Damit sie den Cluster-Integritätsstatus (und andere OpenSearch Daten) sehen können, fügen Sie die `es:ESHttpGet` Aktion einer Zugriffsrichtlinie hinzu und fügen Sie sie ihren Konten oder Rollen hinzu.

Da identitätsbasierte Richtlinien an Benutzer oder Rollen (Prinzipale) angefügt werden, gibt JSON keinen Prinzipal an. Die folgende Richtlinie gewährt Zugriff auf Aktionen, die mit `Describe` und `List` beginnen. Diese Kombination von Aktionen bietet schreibgeschützten Zugriff auf Domain-Konfigurationen, jedoch nicht direkt auf die in der Domain gespeicherten Daten:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "es:Describe*",
        "es:List*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Ein Administrator hat möglicherweise vollen Zugriff auf den OpenSearch Dienst und alle in allen Domänen gespeicherten Daten:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "es:*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Mit identitätsbasierten Richtlinien können Sie Tags verwenden, um den Zugriff auf die Konfigurations-API zu steuern. Die folgende Richtlinie ermöglicht es beispielsweise angehängten Prinzipalen, die Konfiguration einer Domain anzuzeigen und zu aktualisieren, wenn die Domain über das Tag `team:devops` verfügt:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": [
      "es:UpdateDomainConfig",
      "es:DescribeDomain",
      "es:DescribeDomainConfig"
    ],
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:ResourceTag/team": [
          "devops"
        ]
      }
    }
  }]
}
```

Sie können auch Tags verwenden, um den Zugriff auf die OpenSearch API zu kontrollieren. Tag-basierte Richtlinien für die OpenSearch API gelten nur für HTTP-Methoden. Mit der folgenden

Richtlinie können beispielsweise angehängte Principals GET- und PUT-Anfragen an die OpenSearch API senden, wenn die Domain über das `environment:production` Tag verfügt:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": [
      "es:ESHttpGet",
      "es:ESHttpPut"
    ],
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:ResourceTag/environment": [
          "production"
        ]
      }
    }
  }]
}
```

Für eine detailliertere Steuerung der OpenSearch API sollten Sie eine differenzierte Zugriffskontrolle in Betracht ziehen.

> **Note**
>
> Nachdem Sie einer tagbasierten Richtlinie eine oder mehrere OpenSearch APIs hinzugefügt haben, müssen Sie einen einzelnen Tagvorgang (z. B. ein Tag hinzufügen, entfernen oder ändern) ausführen, damit die Änderungen für eine Domain wirksam werden. Sie müssen die Service-Software R20211203 oder höher verwenden, um OpenSearch API-Operationen in tagbasierte Richtlinien aufzunehmen.

OpenSearch Der Service unterstützt die `RequestTag` und die `TagKeys` globalen Bedingungsschlüssel für die Konfigurations-API, nicht für die API. OpenSearch Diese Bedingungen gelten nur für API-Aufrufe, die Tags in der Anfrage enthalten, z. B. `CreateDomain`, `AddTags` und `RemoveTags`. Mit der folgenden Richtlinie können angehängte Prinzipale Domains erstellen, jedoch nur, wenn sie das `team:it`-Tag in die Anfrage aufnehmen:

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "es:CreateDomain",
      "es:AddTags"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:RequestTag/team": [
          "it"
        ]
      }
    }
  }
}
```

Weitere Informationen zur Verwendung von Tags für die Zugriffssteuerung und die Unterschiede zwischen ressourcenbasierten und identitätsbasierten Richtlinien finden Sie im IAM-Benutzerhandbuch.

IP-basierte Richtlinien

IP-basierte Richtlinien beschränken den Zugriff auf eine Domain auf eine oder mehrere IP-Adressen oder CIDR-Blöcke. Aus technischer Sicht sind IP-basierte Richtlinien kein eigener Richtlinientyp. Stattdessen sind sie einfach ressourcenbasierte Richtlinien, die einen anonymen Prinzipal angeben und ein besonderes Condition-Element einschließen.

Der Hauptvorteil IP-basierter Richtlinien besteht darin, dass sie unsignierte Anfragen an eine OpenSearch Service-Domain zulassen, sodass Sie Clients wie Curl und OpenSearch Dashboards verwenden oder über einen Proxyserver auf die Domain zugreifen können. Weitere Informationen hierzu finden Sie unter the section called “Verwenden eines Proxys für den Zugriff auf den Service über Dashboards OpenSearch OpenSearch ”.

> **Note**
>
> Wenn für die Domain VPC-Zugriff aktiviert wurde, können Sie keine IP-basierte Richtlinie konfigurieren. Sie können stattdessen mit Sicherheitsgruppen steuern, welche IP-Adressen

auf die Domain zugreifen dürfen. Weitere Informationen finden Sie unter the section called "Zugriffsrichtlinien für VPC-Domänen".

Die folgende Richtlinie gewährt allen HTTP-Anforderungen, die vom angegebenen IP-Bereich stammen, den Zugriff auf `test-domain`:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": [
        "es:ESHttp*"
      ],
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": [
            "192.0.2.0/24"
          ]
        }
      },
      "Resource": "arn:aws:es:us-west-1:987654321098:domain/test-domain/*"
    }
  ]
}
```

Wenn Ihre Domain über einen öffentlichen Endpunkt verfügt und keine differenzierte Zugriffssteuerung verwendet, empfehlen wir, IAM-Prinzipale und IP-Adressen zu kombinieren. Diese Richtlinie gewährt `test-user` HTTP-Zugriff nur, wenn die Anforderung aus dem angegebenen IP-Bereich stammt:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Principal": {
      "AWS": [
```

```
        "arn:aws:iam::987654321098:user/test-user"
      ]
    },
    "Action": [
      "es:ESHttp*"
    ],
    "Condition": {
      "IpAddress": {
        "aws:SourceIp": [
          "192.0.2.0/24"
        ]
      }
    },
    "Resource": "arn:aws:es:us-west-1:987654321098:domain/test-domain/*"
  }]
}
```

Serviceanfragen stellen und signieren OpenSearch

Auch wenn Sie eine vollständig offene, ressourcenbasierte Zugriffsrichtlinie konfigurieren, müssen alle Anfragen an die OpenSearch Dienstkonfigurations-API signiert werden. Wenn in Ihren Richtlinien IAM-Rollen oder -Benutzer angegeben sind, müssen Anfragen an die OpenSearch APIs ebenfalls mit AWS Signature Version 4 signiert werden. Die Signaturmethode ist je nach API verschieden:

- Um Aufrufe an die OpenSearch Service-Konfigurations-API zu tätigen, empfehlen wir, eines der AWS SDKs zu verwenden. Mit den SDKs wird der Vorgang erheblich vereinfacht und Sie können im Vergleich zum Erstellen und Signieren eigener Anforderungen viel Zeit sparen. Die Konfigurations-API-Endpunkte verwenden das folgende Format:

  ```
  es.region.amazonaws.com/2021-01-01/
  ```

  Beispiel: Die folgende Anforderung versendet eine Konfigurationsänderung an die `movies`-Domain, aber Sie müssen sie selbst signieren (nicht empfohlen):

  ```
  POST https://es.us-east-1.amazonaws.com/2021-01-01/opensearch/domain/movies/config
  {
    "ClusterConfig": {
      "InstanceType": "c5.xlarge.search"
    }
  }
  ```

Wenn Sie eines der SDKs verwenden, wie z. B. Boto 3, übernimmt das SDK automatisch das Signieren der Anforderung:

```
import boto3

client = boto3.client(es)
response = client.update_domain_config(
  DomainName='movies',
  ClusterConfig={
    'InstanceType': 'c5.xlarge.search'
  }
)
```

Ein Java-Codebeispiel finden Sie unter the section called “Verwenden der AWS-SDKs”.

- Um Aufrufe an die OpenSearch APIs zu tätigen, müssen Sie Ihre eigenen Anfragen signieren. Die OpenSearch APIs verwenden das folgende Format:

```
domain-id.region.es.amazonaws.com
```

Beispiel: Die folgende Anforderung durchsucht den `movies`-Index nach thor:

```
GET https://my-domain.us-east-1.es.amazonaws.com/movies/_search?q=thor
```

> **Note**
>
> Der Service ignoriert Parameter, die in URLs für HTTP POST-Anforderungen, die mit Signature Version 4 signiert sind, übergeben wurden.

Konflikte in Richtlinien

Komplexitäten entstehen, wenn Richtlinien einander widersprechen oder den Benutzer nicht explizit erwähnen. Grundlegendes zur Funktionsweise von IAM im IAM-Benutzerhandbuch enthält eine Kurzübersicht über die Richtlinienauswertungslogik:

- Standardmäßig werden alle Anforderungen verweigert.
- Dieser Standardwert kann durch eine explizite Zugriffserlaubnis überschrieben werden.

- Eine explizite Zugriffsverweigerung überschreibt jedwede Zugriffserlaubnis.

Wenn Ihnen beispielsweise eine ressourcenbasierte Richtlinie Zugriff auf eine Domain-Unterressource (einen OpenSearch Index oder eine API) gewährt, Ihnen aber eine identitätsbasierte Richtlinie den Zugriff verweigert, wird Ihnen der Zugriff verweigert. Wenn eine identitätsbasierte Richtlinien den Zugriff gewährt, eine ressourcenbasierte Richtlinie aber nicht festlegt, ob Ihnen Zugriff gewährt werden soll oder ob nicht, wird Ihnen der Zugriff gewährt. In der folgenden Tabelle sich überschneidender Richtlinien finden Sie eine vollständige Übersicht der Ergebnisse für Domains-Subressourcen.

	Zugelassen in ressourcenbasierter Richtlinie	Verweigert in ressourcenbasierter Richtlinie	Weder zugelassen noch verweigert in ressourcenbasierter Richtlinie
Allowed in identity-based policy	Sobald Sie die Details auf dieser Seite überprüft haben, klicken Sie auf	Deny	Sobald Sie die Details auf dieser Seite überprüft haben, klicken Sie auf
Denied in identity-based policy	Deny	Deny	Deny
Neither allowed nor denied in identity-based policy	Sobald Sie die Details auf dieser Seite überprüft haben, klicken Sie auf	Deny	Deny

Richtlinienelementreferenz

OpenSearch Der Service unterstützt die meisten Richtlinienelemente in der IAM-Referenz für Richtlinienelemente, mit Ausnahme von. `NotPrincipal` Die folgende Tabelle zeigt die gängigsten Elemente.

JSON-Richtlinienelement	Übersicht
`Version`	Die aktuelle Version der Richtliniensprache ist `2012-10-17` . Alle vordefinierten Zugriffsrichtlinien sollten diesen Wert angeben.
`Effect`	Dieses Element legt fest, ob die Anweisung den Zugriff auf die angegebenen Aktionen zulässt oder verweigert. Gültige Werte sind `Allow` oder `Deny`.
`Principal`	Dieses Element gibt die AWS-Konto oder die IAM-Rolle oder den Benutzer an, dem der Zugriff auf eine Ressource gewährt oder verweiger t wird. Es kann verschiedene Formen annehmen: • AWS Konten: oder `"Principal":{"AWS": ["1234567 89012"]}` `"Principal":{"AWS": ["arn:aws:iam::123 456789012:root"]}` • IAM-Benutzer: `"Principal":{"AWS": ["arn:aws:iam::123 456789012:user/test-user"]}` • IAM-Rollen: `"Principal":{"AWS": ["arn:aws:iam::123 456789012:role/test-role"]}` **Important** Durch die Angabe des Platzhalters * wird der anonyme Zugriff auf die Domain ermöglicht. Dies wird nur empfohlen, wenn Sie eine IP-basierte Bedingung hinzufügen, VPC-Support verwenden oder eine feinkörnige Zugriffssteuerung aktivieren. Prüfen Sie außerdem sorgfältig die folgenden Richtlinien, um sicherzus tellen, dass sie keinen breiten Zugang gewähren: • Identitätsbasierte Richtlinien, die mit zugehörigen AWS Prinz ipalen verknüpft sind (z. B. IAM-Rollen)

JSON-Richtlinienelement	Übersicht
	• Ressourcenbasierte Richtlinien, die mit zugehörigen AWS Ressourcen verknüpft sind (z. B. KMS-Schlüssel) AWS Key Management Service

JSON-Richtlinienelement	Übersicht
`Action`	OpenSearch Der Dienst verwendet `ESHttp*` Aktionen für OpenSearch HTTP-Methoden. Die restlichen Aktionen gelten für die Konfigurations-API. Bestimmte `es:`-Aktionen unterstützen Berechtigungen auf Ressource nebene. Sie können einem Benutzer z. B. Berechtigungen zum Löschen einer bestimmten Domain erteilen, ohne ihn zum Löschen beliebiger Domains zu berechtigen. Andere Aktionen gelten nur für den Service selbst. `es:ListDomainNames` ist im Kontext einer einzelnen Domain ohne Bedeutung und benötigt folglich einen Platzhalter. Eine Liste aller verfügbaren Aktionen und ob sie für die Domain-Su bressourcen (`test-domain/*`), für die Domain-Konfiguration () oder nur für den Service (`test-domain *`) gelten, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon OpenSearch Service in der Service Authorization Reference Ressourcenbasierte Richtlinien unterscheiden sich von Berechtig ungen auf Ressourcenebene. Ressourcenbasierte Richtlinien sind vollständige JSON-Richtlinien, die an Domains angefügt werden. Mithilfe von Berechtigungen auf Ressourcenebene können Sie Aktionen auf bestimmte Domains oder Unterressourcen einschränken. In der Praxis können Sie sich Berechtigungen auf Ressourcenebene als optionaler Teil einer ressourcen- oder identitätsbasierten Richtlinien vorstellen. Während Berechtigungen auf Ressourcenebene für `es:CreateDomain` nicht allzu sinnvoll erscheinen – denn warum sollte man einem Benutzer Berechtigungen zum Erstellen einer Domain gewähren, die bereits vorhanden ist? – können Sie mithilfe eines Platzhalters ein einfaches Benennungsschema für Ihre Domains (z. B. `"Resource": "arn:aws:es:us-west-1:987654321098:domain/my-team-name-*"`) erzwingen. Natürlich kann nichts Sie daran hindern, Aktionen zusammen mit weniger restriktiven Ressourcen einzuschließen, wie z. B. die folgenden Elemente:

JSON-Richtlinienelement	Übersicht

	<pre>{
	  "Version": "2012-10-17",
	  "Statement": [
	    {
	      "Effect": "Allow",
	      "Action": [
	        "es:ESHttpGet",
	        "es:DescribeDomain"
	      ],
	      "Resource": "*"
	    }
	  ]
	}</pre>
	Weitere Informationen zum Kombinieren von Aktionen mit Ressourcen finden Sie unter dem Element `Resource` in dieser Tabelle.

JSON-Richtlinienelement	Übersicht
`Condition`	OpenSearch Der Service unterstützt die meisten Bedingungen, die im IAM-Benutzerhandbuch unter den Kontextschlüsseln für AWS globale Bedingungen beschrieben sind. Zu den nennenswerten Ausnahmen gehört der `aws:PrincipalTag` Schlüssel, den der OpenSearch Service nicht unterstützt. Bei der Konfiguration einer IP-basierten Richtlinien geben Sie die IP-Adressen oder den CIDR-Block als Bedingung an, wie im folgenden Beispiel: `"Condition": { "IpAddress": { "aws:SourceIp": [ "192.0.2.0/32" ] } }` Wie unter erwähntthe section called “Identitätsbasierte Richtlinien”, gelten die Bedingungsschlüssel `aws:ResourceTag` `aws:RequestTag` , und die `aws:TagKeys` Bedingungsschlüssel sowohl für die Konfigurations-API als auch für die OpenSearch APIs.

JSON-Richtlinienelement	Übersicht

`Resource`	OpenSearch Der Service verwendet `Resource` Elemente auf drei grundlegende Arten:
	
	• Verwenden Sie für Aktionen, die sich auf den OpenSearch Dienst selbst beziehen`es:ListDomainNames` , z. B. um vollen Zugriff zu gewähren, die folgende Syntax:
	
	`"Resource": "*"`
	
	• Für Aktionen, die mit der Konfiguration einer Domain zusammenhängen, wie `es:DescribeDomain` , können Sie die folgende Syntax verwenden:
	
	`"Resource": "arn:aws:es:` *region*`:`*aws-account-id*`:domain/`*domain-name*`"`
	
	• Für Aktionen, die für Unterressourcen einer Domain gelten, wie `es:ESHttpGet` , können Sie die folgende Syntax verwenden:
	
	`"Resource": "arn:aws:es:` *region*`:`*aws-account-id*`:domain/`*domain-name*`/*"`
	
	Sie müssen keinen Platzhalter verwenden. OpenSearch Mit dem Service können Sie für jeden OpenSearch Index oder jede API eine andere Zugriffsrichtlinie definieren. Unter Umständen möchten Sie die Berechtigungen eines Benutzers für den Index `test-index` einschränken:
	
	`"Resource": "arn:aws:es:` *region*`:`*aws-account-id*`:domain/`*domain-name*`/test-index"`
	
	Anstelle eines uneingeschränkten Zugriffs auf `test-index` können Sie die Richtlinie auch nur auf die Such-API beschränken.

JSON-Richtlinienelement	Übersicht

	`"Resource": "arn:aws:es:region:aws-account-id:domain/domain-name /test-index/_search"`
	
	Sie können sogar den Zugriff auf einzelne Dokumente kontrollieren:
	
	`"Resource": "arn:aws:es:region:aws-account-id:domain/domain-name /test-index/test-type/1"`
	
	Wenn die Unterressource als URI OpenSearch ausgedrückt wird, können Sie im Wesentlichen den Zugriff darauf mithilfe einer Zugriffsrichtlinie steuern. Weitere Informationen dazu, auf welche Ressourcen ein Benutzer zugreifen kann, finden Sie unter the section called “Differenzierte Zugriffskontrolle”.
	
	Weitere Informationen dazu, welche Aktionen Berechtigungen auf Ressourcenebene unterstützten, finden Sie unter dem Element `Action` in dieser Tabelle.

Erweiterte Optionen und Überlegungen zur API

OpenSearch Der Dienst verfügt über mehrere erweiterte Optionen, von denen eine Auswirkungen auf die Zugriffskontrolle hat:. `rest.action.multi.allow_explicit_index` Bei ihrer Standardeinstellung „true" können Benutzer Unterressourcen-Berechtigungen unter bestimmten Bedingungen umgehen.

Beachten Sie beispielsweise die folgende ressourcenbasierte Richtlinie:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
```

```
          "arn:aws:iam::123456789012:user/test-user"
        ]
      },
      "Action": [
        "es:ESHttp*"
      ],
      "Resource": [
        "arn:aws:es:us-west-1:987654321098:domain/test-domain/test-index/*",
        "arn:aws:es:us-west-1:987654321098:domain/test-domain/_bulk"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::123456789012:user/test-user"
        ]
      },
      "Action": [
        "es:ESHttpGet"
      ],
      "Resource": "arn:aws:es:us-west-1:987654321098:domain/test-domain/restricted-
index/*"
    }
  ]
}
```

Diese Richtlinie gewährt `test-user` vollen Zugriff auf `test-index` und die OpenSearch Bulk-API. Außerdem ermöglicht sie `GET`-Anforderungen an `restricted-index`.

Wie zu erwarten, schlägt die folgende Indizierungsanforderung aufgrund eines Berechtigungsfehlers fehl:

```
PUT https://search-test-domain.us-west-1.es.amazonaws.com/restricted-index/movie/1
{
  "title": "Your Name",
  "director": "Makoto Shinkai",
  "year": "2016"
}
```

Im Gegensatz zur Index-API ermöglicht Ihnen die Massen-API, in einem einzelnen Aufruf viele Dokumente zu erstellen, zu aktualisieren und zu löschen. Sie geben diese Operationen jedoch oft

im Anforderungstext anstatt in der Anforderungs-URL an. Da OpenSearch Service URLs verwendet, um den Zugriff auf Domain-Subressourcen zu steuern, `test-user` kann er tatsächlich die Bulk-API verwenden, um Änderungen daran vorzunehmen. `restricted-index` Auch wenn der Benutzer über keine POST-Berechtigungen für den Index verfügt, ist die folgende Anforderung erfolgreich:

```
POST https://search-test-domain.us-west-1.es.amazonaws.com/_bulk
{ "index" : { "_index": "restricted-index", "_type" : "movie", "_id" : "1" } }
{ "title": "Your Name", "director": "Makoto Shinkai", "year": "2016" }
```

In diesem Fall funktioniert die Zugriffsrichtlinie nicht wie beabsichtigt. Um Benutzer daran zu hindern, diese Arten von Einschränkungen zu umgehen, können Sie `rest.action.multi.allow_explicit_index` in „false" ändern. Wenn dieser Wert „false" lautet, funktionieren alle Aufrufe der Massen-APIs mget und msearch, die im Anforderungstext Indexnamen angeben, nicht mehr. Mit anderen Worten: Aufrufe an `_bulk` funktionieren nicht mehr, aber Aufrufe an `test-index/_bulk` sind hiervon nicht betroffen. Da dieser zweite Endpunkt einen Indexnamen enthält, müssen Sie im Anforderungstext keinen angeben.

OpenSearch Dashboards ist stark von mget und msearch abhängig, sodass es nach dieser Änderung wahrscheinlich nicht mehr richtig funktioniert. Als Teillösung können Sie für `rest.action.multi.allow_explicit_index` "true" belassen und bestimmten Benutzer den Zugriff auf eine oder mehrere dieser APIs verweigern.

Weitere Informationen zum Ändern dieser Einstellung finden Sie unter the section called “Erweiterte Clustereinstellungen”.

Dementsprechend enthalt die folgende ressourcenbasierte Richtlinie zwei geringfügige Probleme:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/test-user"
      },
      "Action": "es:ESHttp*",
      "Resource": "arn:aws:es:us-west-1:987654321098:domain/test-domain/*"
    },
    {
      "Effect": "Deny",
```

```
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/test-user"
      },
      "Action": "es:ESHttp*",
      "Resource": "arn:aws:es:us-west-1:987654321098:domain/test-domain/restricted-
index/*"
    }
  ]
}
```

- Trotz der expliziten Verweigerung kann `test-user` weiterhin Aufrufe wie `GET https://search-test-domain.us-west-1.es.amazonaws.com/_all/_search` und `GET https://search-test-domain.us-west-1.es.amazonaws.com/*/_search` für den Zugriff auf die Dokumente in `restricted-index` ausführen.
- Da das `Resource`-Element auf `restricted-index/*` verweist, ist `test-user` nicht zum direkten Zugriff auf die Dokumente des Index berechtigt. Der Benutzer verfügt jedoch über Berechtigungen zum Löschen des gesamten Index. Damit der Zugriff und das Löschen verhindert werden, muss die Richtlinie stattdessen `restricted-index*` angeben.

Anstatt großzügige Berechtigungen und gezielte Verweigerungen miteinander zu mischen, ist eine sicherere Strategie, der Regel der geringsten Rechte zu folgen und nur die Berechtigungen zu gewähren, die zum Ausführen einer Aufgabe erforderlich sind. Weitere Informationen zur Steuerung des Zugriffs auf einzelne Indizes oder OpenSearch Operationen finden Sie unter. the section called “Differenzierte Zugriffskontrolle”

> **Important**
>
> Die Angabe des Platzhalters* ermöglicht den anonymen Zugriff auf Ihre Domain. Es wird nicht empfohlen, den Platzhalter zu verwenden. Überprüfen Sie außerdem sorgfältig die folgenden Richtlinien, um sicherzustellen, dass sie keinen breiten Zugriff gewähren:
>
> - Identitätsbasierte Richtlinien, die mit zugehörigen AWS Prinzipalen verknüpft sind (z. B. IAM-Rollen)
> - Ressourcenbasierte Richtlinien, die mit zugehörigen AWS Ressourcen verknüpft sind (z. B. KMS-Schlüssel) AWS Key Management Service

Konfigurieren von Zugriffsrichtlinien

- Anweisungen zum Erstellen oder Ändern von ressourcen- und IP-basierten Richtlinien in OpenSearch Service finden Sie unter. the section called “Konfigurieren von Zugriffsrichtlinien”
- Weitere Anweisungen zum Erstellen oder Ändern von identitätsbasierten Richtlinien in IAM finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Zusätzliche Beispielrichtlinien

Obwohl dieses Kapitel viele Beispielrichtlinien enthält, ist die AWS Zugriffskontrolle ein komplexes Thema, das sich am besten anhand von Beispielen verstehen lässt. Weitere Informationen finden Sie unter Beispiel für identitätsbasierte IAM-Richtlinien im IAM-Benutzerhandbuch.

Referenz zu Amazon OpenSearch Service API-Berechtigungen

Wenn Sie die Zugriffskontrolle einrichten, schreiben Sie Berechtigungsrichtlinien, die Sie einer IAM-Identität zuordnen können (identitätsbasierte Richtlinien). Weitere Informationen finden Sie in den folgenden Themen in der Service-Authorization-Referenz:

- Aktionen, Ressourcen und Bedingungsschlüssel für den Service. OpenSearch
- Aktionen, Ressourcen und Bedingungsschlüssel für OpenSearch Ingestion.

Diese Referenz enthält Informationen darüber, welche -API-Operationen in einer IAM-Richtlinie verwendet werden können. Dazu gehören auch die AWS Ressource, für die Sie die Berechtigungen erteilen können, sowie Bedingungsschlüssel, die Sie für eine differenzierte Zugriffskontrolle verwenden können.

Sie geben die Aktionen im Feld `Action` der Richtlinie, den Ressourcenwert im Feld `Resource` der Richtlinie und die Bedingungen im Feld `Condition` der Richtlinie an. Um eine Aktion für OpenSearch Service anzugeben, verwenden Sie das `es:` Präfix, gefolgt vom Namen des API-Vorgangs (z. B.`es:CreateDomain`). Um eine Aktion für OpenSearch Ingestion anzugeben, verwenden Sie das `osis:` Präfix gefolgt von der API-Operation (z. B.`osis:CreatePipeline`).

AWS verwaltete Richtlinien für Amazon OpenSearch Service

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. AWS Verwaltete Richtlinien dienen dazu, Berechtigungen für viele gängige Anwendungsfälle

bereitzustellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie allen AWS Kunden zur Verfügung stehen. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie kundenverwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das Update auf alle Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie eingeführt AWS-Service wird oder neue API-Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

AmazonOpenSearchDirectQueryGlueCreateAccess

Gewährt Amazon OpenSearch Service Direct Query Service Zugriff auf `CreateDatabaseCreatePartition`,`CreateTable`, und `BatchCreatePartition` AWS Glue API.

Sie finden die AmazonOpenSearchDirectQueryGlueCreateAccessRichtlinie in der IAM-Konsole.

AmazonOpenSearchServiceFullAccess

Gewährt vollen Zugriff auf die API-Operationen und Ressourcen der OpenSearch Dienstkonfiguration für einen AWS-Konto.

Sie finden die AmazonOpenSearchServiceFullAccessRichtlinie in der IAM-Konsole.

AmazonOpenSearchServiceReadOnlyAccess

Gewährt schreibgeschützten Zugriff auf alle OpenSearch Serviceressourcen für einen. AWS-Konto

Sie finden die AmazonOpenSearchServiceReadOnlyAccessRichtlinie in der IAM-Konsole.

AmazonOpenSearchServiceRolePolicy

Sie können `AmazonOpenSearchServiceRolePolicy` nicht an Ihre IAM-Entitäten anhängen. Diese Richtlinie ist einer dienstbezogenen Rolle zugeordnet, die es dem OpenSearch Service

ermöglicht, auf Kontoressourcen zuzugreifen. Weitere Informationen finden Sie unter the section called “Berechtigungen”.

Sie finden die AmazonOpenSearchServiceRolePolicyRichtlinie in der IAM-Konsole.

AmazonOpenSearchServiceCognitoAccess

Bietet die Mindestberechtigungen für Amazon Cognito, die erforderlich sind, um die Cognito-Authentifizierung zu aktivieren.

Sie finden die AmazonOpenSearchServiceCognitoAccessRichtlinie in der IAM-Konsole.

AmazonOpenSearchIngestionServiceRolePolicy

Sie können `AmazonOpenSearchIngestionServiceRolePolicy` nicht an Ihre IAM-Entitäten anhängen. Diese Richtlinie ist mit einer serviceverknüpften Rolle verknüpft, die es OpenSearch Ingestion ermöglicht, VPC-Zugriff für Erfassungspipelines zu aktivieren, Tags zu erstellen und aufnahmebezogene Metriken für Ihr Konto zu veröffentlichen. CloudWatch Weitere Informationen finden Sie unter the section called “Verwenden von serviceverknüpften Rollen”.

Sie finden die Richtlinie in der IAM-Konsole. AmazonOpenSearchIngestionServiceRolePolicy

OpenSearchIngestionSelfManagedVpcePolicy

Sie können `OpenSearchIngestionSelfManagedVpcePolicy` nicht an Ihre IAM-Entitäten anhängen. Diese Richtlinie ist mit einer serviceverknüpften Rolle verknüpft, die es OpenSearch Ingestion ermöglicht, selbstverwalteten VPC-Zugriff für Erfassungspipelines zu aktivieren, Tags zu erstellen und aufnahmebezogene Metriken für Ihr Konto zu veröffentlichen. CloudWatch Weitere Informationen finden Sie unter the section called “Verwenden von serviceverknüpften Rollen”.

OpenSearchIngestionSelfManagedVpcePolicySie finden die Richtlinie in der IAM-Konsole.

AmazonOpenSearchIngestionFullAccess

Gewährt vollen Zugriff auf die Operationen und Ressourcen der OpenSearch Ingestion-API für einen. AWS-Konto

Sie finden die AmazonOpenSearchIngestionFullAccessRichtlinie in der IAM-Konsole.

AmazonOpenSearchIngestionReadOnlyAccess

Gewährt schreibgeschützten Zugriff auf alle OpenSearch Ingestion-Ressourcen für einen. AWS-Konto

Sie finden die AmazonOpenSearchIngestionReadOnlyAccessRichtlinie in der IAM-Konsole.

AmazonOpenSearchServerlessServiceRolePolicy

Stellt die Amazon CloudWatch Mindestberechtigungen bereit, die erforderlich sind, um OpenSearch serverlose Metrikdaten an zu senden. CloudWatch

Sie finden die AmazonOpenSearchServerlessServiceRolePolicyRichtlinie in der IAM-Konsole.

OpenSearch Service-Updates für AWS verwaltete Richtlinien

Sehen Sie sich Details zu Aktualisierungen der AWS verwalteten Richtlinien für OpenSearch Service an, seit dieser Dienst mit der Nachverfolgung von Änderungen begonnen hat.

Änderung	Beschreibung	Datum
`OpenSearchIngestionSelfManagedVpcePolicy` hinzugefügt	Eine neue Richtlinie, die es OpenSearch Ingestion ermöglicht, selbstverwalteten VPC-Zugriff für Erfassungspipelines zu aktivieren, Tags zu erstellen und aufnahmebezogene Metriken in Ihrem Konto zu veröffentlichen. CloudWatch Informationen zum Richtlinien-JSON finden Sie unter IAM-Konsole.	12. Juni 2024
Hinzugefügt `AmazonOpenSearchDirectQueryGlueCreateAccess`	Gewährt Amazon OpenSearch Service Direct Query Service Zugriff auf `CreateDatabase` `CreatePartition` ,`CreateTable` , und `BatchCreatePartition` AWS Glue API.	6. Mai 2024

Änderung	Beschreibung	Datum
`AmazonOpenSearchServiceRolePolicy` und `AmazonElasticsearchServiceRolePolicy` wurden aktualisiert	Die für die dienstbezogene Rolle erforderlichen Berechtigungen zum Zuweisen und Aufheben der Zuweisung von IPv6-Adressen wurden hinzugefügt. Die veraltete Elasticsearch-Richtlinie wurde ebenfalls aktualisiert, um die Abwärtskompatibilität sicherzustellen.	18. Oktober 2023
`AmazonOpenSearchIngestionServiceRolePolicy` hinzugefügt	Eine neue Richtlinie, die es OpenSearch Ingestion ermöglicht, den VPC-Zugriff für Erfassungspipelines zu aktivieren, Tags zu erstellen und aufnahmebezogene Metriken in Ihrem Konto zu veröffentlichen. CloudWatch Informationen zum Richtlinien-JSON finden Sie unter IAM-Konsole.	26. April 2023
`AmazonOpenSearchIngestionFullAccess` hinzugefügt	Eine neue Richtlinie, die vollen Zugriff auf die Operationen und Ressourcen der OpenSearch Ingestion-API für einen gewährt. AWS-Konto Informationen zum Richtlinien-JSON finden Sie unter IAM-Konsole.	26. April 2023

Änderung	Beschreibung	Datum
`AmazonOpenSearchIngestionReadOnlyAccess` hinzugefügt	Eine neue Richtlinie, die Lesezugriff auf alle OpenSearch Ingestion -Ressourcen für einen gewährt. AWS-Konto Informationen zum Richtlinien-JSON finden Sie unter IAM-Konsole.	26. April 2023
`AmazonOpenSearchServerlessServiceRolePolicy` hinzugefügt	Eine neue Richtlinie, die die Mindestberechtigungen bereitstellt, die erforderlich sind, um OpenSearch serverlose Metrikdaten an zu Amazon CloudWatch senden. Informationen zum Richtlinien-JSON finden Sie unter IAM-Konsole.	29. November 2022

Änderung	Beschreibung	Datum
`AmazonOpenSearchServiceRolePolicy` und `AmazonElasticsearchServiceRolePolicy` wurden aktualisiert	Es wurden die Berechtigungen hinzugefügt, die für die serviceverknüpfte Rolle erforderlich sind, um vom OpenSearch Service verwaltete VPC-Endpunkte zu erstellen. Einige Aktionen können nur ausgeführt werden, wenn die Anforderung das Tag `OpenSearchManaged=true` enthält. Die veraltete Elasticsearch-Richtlinie wurde ebenfalls aktualisiert, um die Abwärtskompatibilität sicherzustellen.	7. November 2022
`AmazonOpenSearchServiceRolePolicy` und `AmazonElasticsearchServiceRolePolicy` wurden aktualisiert	Unterstützung für die `PutMetricData` Aktion hinzugefügt, die für die Veröffentlichung von OpenSearch Cluster-Metriken auf Amazon erforderlich ist CloudWatch. Die veraltete Elasticsearch-Richtlinie wurde ebenfalls aktualisiert, um die Abwärtskompatibilität sicherzustellen. Informationen zum Richtlinien-JSON finden Sie unter IAM-Konsole.	12. September 2022

Änderung	Beschreibung	Datum
`AmazonOpenSearchServiceRolePolicy` und `AmazonElasticsearchServiceRolePolicy` wurden aktualisiert	Unterstützung für den Ressourcentyp `acm` hinzugefügt. Die Richtlinie bietet die Mindestberechtigung AWS Certificate Manager (ACM), die für die serviceverknüpfte Rolle erforderlich ist, um ACM-Ressourcen zu verifizieren und zu validieren, um benutzerdefinierte Domänen mit aktivierten Endpunkten zu erstellen und zu aktualisieren. Die veraltete Elasticsearch-Richtlinie wurde ebenfalls aktualisiert, um die Abwärtskompatibilität sicherzustellen.	28. Juli 2022

Änderung	Beschreibung	Datum
`AmazonOpenSearchServiceCognitoAccess` und `AmazonESCognitoAccess` wurden aktualisiert	Unterstützung für die `UpdateUserPoolClient` Aktion hinzugefügt, die erforderlich ist, um die Cognito-Benutzerpoolkonfiguration während des Upgrades von Elasticsearch auf festzulegen. OpenSearch Korrigierte Berechtigungen für die `SetIdentityPoolRoles` -Aktion, um Zugriff auf alle Ressourcen zu gewähren. Die veraltete Elasticsearch-Richtlinie wurde ebenfalls aktualisiert, um die Abwärtskompatibilität sicherzustellen.	20. Dezember 2021
`AmazonOpenSearchServiceRolePolicy` aktualisiert	Unterstützung für den Ressourcentyp `security-group` hinzugefügt. Die Richtlinie stellt die Mindestberechtigungen für Amazon EC2 und Elastic Load Balancing bereit, die für die Service-verknüpfte Rolle erforderlich sind, um den VPC-Zugriff zu ermöglichen.	9. September 2021

Änderung	Beschreibung	Datum
• `AmazonOpenSearchServiceFullAccess` hinzugefügt • `AmazonESFullAccess` – Veraltet	Diese neue Richtlinie soll die alte Richtlinie ersetzen. Beide Richtlinien bieten vollen Zugriff auf die OpenSearch Service-Konfigurations-API und alle HTTP-Methoden für die OpenSearch APIs. Feinkörnige Zugriffssteuerung und ressourcenbasierte Richtlinien können den Zugriff weiterhin einschränken.	7. September 2021
• `AmazonOpenSearchServiceReadOnlyAccess` hinzugefügt • `AmazonESReadOnlyAccess` – Veraltet	Diese neue Richtlinie soll die alte Richtlinie ersetzen. Beide Richtlinien bieten nur Lesezugriff auf die OpenSearch Dienstkonfigurations-API (`es:Describe* es:List*`, und`es:Get*`) und keinen Zugriff auf die HTTP-Methoden für die OpenSearch APIs.	7. September 2021
• `AmazonOpenSearchServiceCognitoAccess` hinzugefügt • `AmazonESCognitoAccess` – Veraltet	Diese neue Richtlinie soll die alte Richtlinie ersetzen. Beide Richtlinien bieten die Mindestberechtigungen für Amazon Cognito, die erforderlich sind, um die Cognito-Authentifizierung zu aktivieren.	7. September 2021

Änderung	Beschreibung	Datum
• AmazonOpenSearchServiceRolePolicy hinzugefügt • `AmazonElasticsearchServiceRolePolicy` – Veraltet	Diese neue Richtlinie soll die alte Richtlinie ersetzen. Beide Richtlinien stellen die Mindestberechtigungen für Amazon EC2 und Elastic Load Balancing bereit, die für die Service-verknüpfte Rolle erforderlich sind, um den VPC-Zugriff zu ermöglichen.	7. September 2021
Änderungsverfolgung gestartet	Amazon OpenSearch Service verfolgt jetzt Änderungen an AWS verwalteten Richtlinien.	7. September 2021

Dienstübergreifende Confused-Deputy-Prävention

Das Confused-Deputy-Problem ist ein Sicherheitsproblem, bei dem eine juristische Stelle, die nicht über die Berechtigung zum Ausführen einer Aktion verfügt, eine privilegiertere juristische Stelle zwingen kann, die Aktion auszuführen. In AWS kann der dienstübergreifende Identitätswechsel zu Confused-Deputy-Problem führen. Ein dienstübergreifender Identitätswechsel kann auftreten, wenn ein Dienst (der Anruf-Dienst) einen anderen Dienst anruft (den aufgerufenen Dienst). Der aufrufende Service kann manipuliert werden, um seine Berechtigungen zu verwenden, um Aktionen auf die Ressourcen eines anderen Kunden auszuführen, für die er sonst keine Zugriffsberechtigung haben sollte. Um dies zu verhindern, bietet AWS Tools, mit denen Sie Ihre Daten für alle Services mit Serviceprinzipalen schützen können, die Zugriff auf Ressourcen in Ihrem Konto erhalten haben.

Wir empfehlen die Verwendung der globalen Bedingungskontext-Schlüssel `aws:SourceArn` und `aws:SourceAccount` in ressourcenbasierten Richtlinien, um die Berechtigungen, die Amazon OpenSearch Service einem anderen Service erteilt, auf eine bestimmte Ressource zu beschränken. Wenn der `aws:SourceArn`-Wert die Konto-ID nicht enthält, z. B. einen Amazon-S3-Bucket-ARN, müssen Sie beide globale Bedingungskontextschlüssel verwenden, um Berechtigungen einzuschränken. Wenn Sie beide globale Bedingungskontextschlüssel verwenden und der `aws:SourceArn`-Wert die Konto-ID enthält, müssen der `aws:SourceAccount`-

Wert und das Konto im `aws:SourceArn`-Wert dieselbe Konto-ID verwenden, wenn sie in der gleichen Richtlinienanweisung verwendet wird. Verwenden Sie `aws:SourceArn`, wenn Sie nur eine Ressource mit dem betriebsübergreifenden Zugriff verknüpfen möchten. Verwenden Sie `aws:SourceAccount`, wenn Sie zulassen möchten, dass Ressourcen in diesem Konto mit der betriebsübergreifenden Verwendung verknüpft werden.

Der Wert von `aws:SourceArn` muss der ARN der OpenSearch-Service-Domäne sein.

Der effektivste Weg, um sich vor dem Confused-Deputy-Problem zu schützen, ist die Verwendung des globalen Bedingungskontextschlüssels `aws:SourceArn` mit dem vollständigen ARN der Ressource. Wenn Sie den vollständigen ARN der Ressource nicht kennen oder wenn Sie mehrere Ressourcen angeben, verwenden Sie den globalen Kontextbedingungsschlüssel mit Platzhaltern (`aws:SourceArn`) * für die unbekannten Teile des ARN. Zum Beispiel: , , `arn:aws:es:*:123456789012:*`.

Das folgende Beispiel zeigt, wie Sie die globalen Bedingungskontext-Schlüssel `aws:SourceArn` und `aws:SourceAccount` in verwenden können, um das Confused-Deputy-Problem zu vermeiden.

```
{
   "Version":"2012-10-17",
   "Statement":{
      "Sid":"ConfusedDeputyPreventionExamplePolicy",
      "Effect":"Allow",
      "Principal":{
         "Service":"es.amazonaws.com"
      },
      "Action":"sts:AssumeRole",
      "Condition":{
         "StringEquals":{
            "aws:SourceAccount":"123456789012"
         },
         "ArnLike":{
            "aws:SourceArn":"arn:aws:es:region:123456789012:domain/my-domain"
         }
      }
   }
}
```

Feinkörnige Zugriffskontrolle in Amazon Service OpenSearch

Eine detaillierte Zugriffskontrolle bietet zusätzliche Möglichkeiten, den Zugriff auf Ihre Daten bei Amazon OpenSearch Service zu kontrollieren. Je nachdem, wer die Anforderung ausstellt, kann es sein, dass eine Suche Ergebnisse aus nur einem Index zurückgibt. Sie können bestimmte Felder in Ihren Dokumenten ausblenden oder bestimmte Dokumente ganz ausschließen.

Die differenzierte Zugriffskontrolle bietet folgende Nutzen:

- Rollenbasierte Zugriffskontrolle
- Sicherheit auf Index-, Dokument- und Feldebene
- OpenSearch Dashboards, Mehrmandantenfähigkeit
- HTTP-Basisauthentifizierung für und Dashboards OpenSearch OpenSearch

Themen

Das Gesamtbild: detaillierte Zugriffskontrolle und Servicesicherheit OpenSearch

Die Sicherheit von Amazon OpenSearch Service besteht aus drei Hauptebenen:

Netzwerk

Die erste Sicherheitsebene ist das Netzwerk, das bestimmt, ob Anfragen eine OpenSearch Service-Domain erreichen. Wenn Sie beim Erstellen einer Domain Öffentlichen Zugriff auswählen, können Anforderungen von jedem mit dem Internet verbundenen Client den Domain-Endpunkt erreichen. Wenn Sie VPC-Zugriff auswählen, müssen Clients eine Verbindung zur VPC herstellen (und die zugeordneten Sicherheitsgruppen müssen dies zulassen), damit eine Anforderung den Endpunkt erreichen kann. Weitere Informationen finden Sie unter the section called “VPC-Unterstützung”.

Domain-Zugriffsrichtlinie

Die zweite Sicherheitsebene ist die Domain-Zugriffsrichtlinie. Nachdem eine Anforderung einen Domain-Endpunkt erreicht hat, erlaubt oder verweigert die ressourcenbasierte Zugriffsrichtlinie den Anforderungszugriff auf einen bestimmten URI. Die Zugriffsrichtlinie akzeptiert oder lehnt Anfragen am „Rand“ der Domain ab, bevor sie OpenSearch sich selbst erreichen.

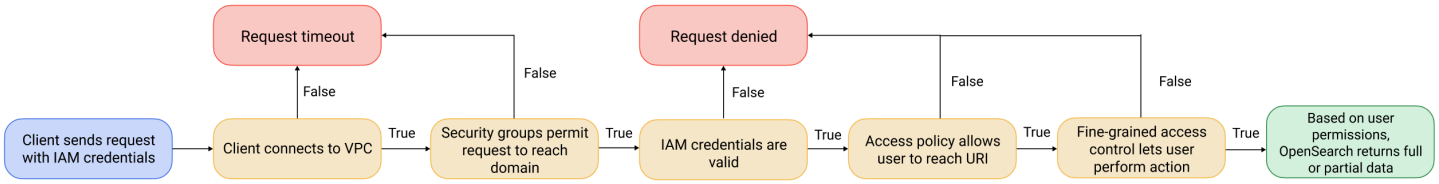
Differenzierte Zugriffskontrolle

Die dritte und letzte Sicherheitsebene ist eine differenzierte Zugriffskontrolle. Nachdem eine ressourcenbasierte Zugriffsrichtlinie eine Anforderung einen Domain-Endpunkt erreichen lässt, werden die Benutzeranmeldeinformationen durch eine differenzierte Zugriffskontrolle ausgewertet und entweder der Benutzer authentifiziert oder die Anforderung verweigert. Wenn eine differenzierte Zugriffskontrolle Zugriffssteuerung den Benutzer authentifiziert, ruft sie alle dem Benutzer zugeordneten Rollen ab und verwendet den vollständigen Satz von Berechtigungen, um zu bestimmen, wie die Anforderung behandelt werden soll.

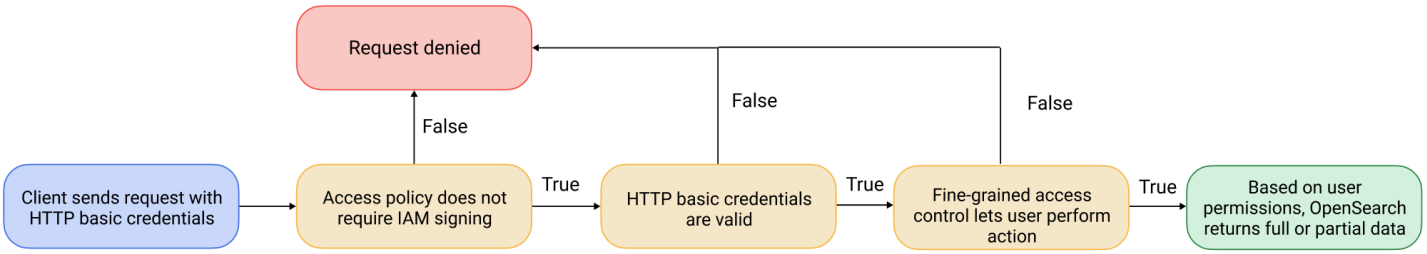
> **Note**
>
> Wenn eine ressourcenbasierte Zugriffsrichtlinie IAM-Rollen oder -Benutzer enthält, müssen Clients signierte Anfragen mit AWS Signature Version 4 senden. Daher können Zugriffsrichtlinien in Konflikt mit einer differenzierten Zugriffskontrolle stehen, insbesondere

wenn Sie die interne Benutzerdatenbank und die HTTP-Standardauthentifizierung verwenden. Sie können eine Anfrage nicht mit einem Benutzernamen und einem Passwort sowie mit IAM-Anmeldeinformationen signieren. Wenn Sie die differenzierte Zugriffskontrolle aktivieren, wird im Allgemeinen empfohlen, eine Domain-Zugriffsrichtlinie zu verwenden, die keine signierten Anforderungen erfordert.

Das folgende Diagramm veranschaulicht eine typische Konfiguration: eine VPC-Zugriff-Domain mit aktivierter differenzierter Zugriffskontrolle, eine IAM-basierte Zugriffsrichtlinie und ein IAM-Master-Benutzer.



Das folgende Diagramm veranschaulicht eine weitere typische Konfiguration: eine öffentliche Zugriff-Domain mit aktivierter differenzierter Zugriffskontrolle, eine Zugriffsrichtlinie, die keine IAM-Prinzipale verwendet, und ein Master-Benutzer in der internen Benutzerdatenbank.



Beispiel

Nehmen wir eine GET-Anfrage an `movies/_search?q=thor` an. Hat der Benutzer die Berechtigung, den `movies`-Index zu durchsuchen? Wenn ja: Hat der Benutzer die Berechtigung, alle darin befindlichen Dokumente anzuzeigen? Sollte die Antwort Felder auslassen oder anonymisieren? Für den Master-Benutzer könnte die Antwort folgendermaßen aussehen:

```
{
  "hits": {
    "total": 7,
    "max_score": 8.772789,
    "hits": [{
        "_index": "movies",
```

```
        "_type": "_doc",
        "_id": "tt0800369",
        "_score": 8.772789,
        "_source": {
          "directors": [
            "Kenneth Branagh",
            "Joss Whedon"
          ],
          "release_date": "2011-04-21T00:00:00Z",
          "genres": [
            "Action",
            "Adventure",
            "Fantasy"
          ],
          "plot": "The powerful but arrogant god Thor is cast out of Asgard to
 live amongst humans in Midgard (Earth), where he soon becomes one of their finest
 defenders.",
          "title": "Thor",
          "actors": [
            "Chris Hemsworth",
            "Anthony Hopkins",
            "Natalie Portman"
          ],
          "year": 2011
        }
      },
      ...
    ]
  }
}
```

Wenn ein Benutzer mit eingeschränkten Berechtigungen genau dieselbe Anforderung ausgibt, könnte die Antwort folgendermaßen aussehen:

```
{
  "hits": {
    "total": 2,
    "max_score": 8.772789,
    "hits": [{
        "_index": "movies",
        "_type": "_doc",
        "_id": "tt0800369",
        "_score": 8.772789,
```

```
        "_source": {
          "year": 2011,
          "release_date":
 "3812a72c6dd23eef3c750c2d99e205cbd260389461e19d610406847397ecb357",
          "plot": "The powerful but arrogant god Thor is cast out of Asgard to
 live amongst humans in Midgard (Earth), where he soon becomes one of their finest
 defenders.",
          "title": "Thor"
        }
      },
      ...
    ]
  }
}
```

Die Antwort hat weniger Treffer und weniger Felder für jeden Treffer. Außerdem ist das `release_date`-Feld anonymisiert. Wenn ein Benutzer ohne Berechtigungen dieselbe Anforderung stellt, gibt der Cluster einen Fehler zurück:

```
{
  "error": {
    "root_cause": [{
      "type": "security_exception",
      "reason": "no permissions for [indices:data/read/search] and User [name=limited-
user, roles=[], requestedTenant=null]"
    }],
    "type": "security_exception",
    "reason": "no permissions for [indices:data/read/search] and User [name=limited-
user, roles=[], requestedTenant=null]"
  },
  "status": 403
}
```

Wenn ein Benutzer ungültige Anmeldeinformationen bereitstellt, gibt der Cluster eine `Unauthorized`-Ausnahme zurück.

Die wichtigsten Konzepte

Wenn Sie mit der detaillierten Zugriffskontrolle beginnen, sollten Sie die folgenden Konzepte berücksichtigen:

- Rollen — Die wichtigste Methode zur Verwendung einer differenzierten Zugriffskontrolle. In diesem Fall unterscheiden sich die Rollen von IAM-Rollen. Rollen enthalten eine beliebige Kombination von Berechtigungen: clusterweit, indexspezifisch, auf Dokumentebene oder auf Feldebene.
- Zuordnung — Nachdem Sie eine Rolle konfiguriert haben, ordnen Sie sie einem oder mehreren Benutzern zu. Beispielsweise können Sie einem einzelnen Benutzer drei Rollen zuordnen: eine Rolle, die Zugriff auf Dashboards bietet, eine mit schreibgeschütztem Zugriff auf `index1` und eine mit Schreibzugriff auf `index2`. Sie können auch alle diese Berechtigungen in eine einzige Rolle aufnehmen.
- Benutzer — Personen oder Anwendungen, die Anfragen an den OpenSearch Cluster stellen. Benutzer verfügen über Anmeldeinformationen — entweder IAM-Zugriffsschlüssel oder einen Benutzernamen und ein Passwort —, die sie angeben, wenn sie Anfragen stellen.

Über den Masterbenutzer

Der Masterbenutzer in OpenSearch Service ist entweder eine Kombination aus Benutzername und Passwort oder ein IAM-Prinzipal, der über vollständige Berechtigungen für den zugrunde liegenden OpenSearch Cluster verfügt. Ein Benutzer gilt als Masterbenutzer, wenn er uneingeschränkten Zugriff auf den OpenSearch Cluster hat und über die Möglichkeit verfügt, interne Benutzer, Rollen und Rollenzuordnungen in Dashboards zu erstellen. OpenSearch

Ein in der OpenSearch Service Console oder über die CLI erstellter Masterbenutzer wird automatisch zwei vordefinierten Rollen zugeordnet:

- `all_access`— Bietet vollen Zugriff auf alle clusterweiten Operationen, Schreibberechtigungen für alle Clusterindizes und Schreibberechtigungen für alle Mandanten.
- `security_manager`— Ermöglicht den Zugriff auf das Security-Plugin und die Verwaltung von Benutzern und Berechtigungen.

Mit diesen beiden Rollen erhält der Benutzer Zugriff auf die Registerkarte Sicherheit in OpenSearch Dashboards, wo er Benutzer und Berechtigungen verwalten kann. Wenn Sie einen weiteren internen Benutzer erstellen und ihn nur der `all_access` Rolle zuordnen, hat der Benutzer keinen Zugriff auf den Tab Sicherheit. Sie können zusätzliche Masterbenutzer erstellen, indem Sie sie explizit `all_access` sowohl den `security_manager` Rollen als auch zuordnen. Anweisungen finden Sie unter the section called “Zusätzliche Hauptbenutzer”.

Wenn Sie einen Masterbenutzer für Ihre Domain erstellen, können Sie entweder einen vorhandenen IAM-Prinzipal angeben oder einen Masterbenutzer in der internen Benutzerdatenbank erstellen. Beachten Sie bei der Entscheidung, welche Sie verwenden möchten, Folgendes:

- IAM-Prinzipal — Wenn Sie einen IAM-Prinzipal für Ihren Masterbenutzer wählen, müssen alle Anfragen an den Cluster mit AWS Signature Version 4 signiert werden.

  OpenSearch Der Service berücksichtigt keine der Berechtigungen des IAM-Prinzipals. Der IAM-Benutzer oder die IAM-Rolle dient ausschließlich der Authentifizierung. Die Richtlinien für diesen Benutzer oder diese Rolle haben keinen Einfluss auf die Autorisierung des Masterbenutzers. Die Autorisierung erfolgt über die verschiedenen Berechtigungen im OpenSearch Security-Plugin.

  Sie können beispielsweise einem IAM-Prinzipal keine IAM-Berechtigungen zuweisen, und solange sich der Computer oder die Person bei diesem Benutzer oder dieser Rolle authentifizieren kann, hat sie die Macht des Masterbenutzers in Service. OpenSearch

  Wir empfehlen IAM, wenn Sie dieselben Benutzer auf mehreren Clustern verwenden möchten, wenn Sie Amazon Cognito für den Zugriff auf Dashboards verwenden möchten oder wenn Sie OpenSearch Clients haben, die Signature Version 4-Signaturen unterstützen.
- Interne Benutzerdatenbank — Wenn Sie in der internen Benutzerdatenbank einen Master erstellen (mit einer Kombination aus Benutzername und Passwort), können Sie die HTTP-Basisauthentifizierung (sowie IAM-Anmeldeinformationen) verwenden, um Anfragen an den Cluster zu stellen. Die meisten Clients unterstützen die Standardauthentifizierung, einschließlich Curl, die auch AWS Signature Version 4 mit der Option --aws-sigv4 unterstützt. Die interne Benutzerdatenbank wird in einem OpenSearch Index gespeichert, sodass Sie sie nicht mit anderen Clustern teilen können.

  Wir empfehlen die interne Benutzerdatenbank, wenn Sie Benutzer nicht über mehrere Cluster hinweg wiederverwenden müssen, wenn Sie HTTP-Standardauthentifizierung für den Zugriff auf Dashboards verwenden möchten (statt Amazon Cognito), oder wenn Sie Clients haben, die nur die Standardauthentifizierung unterstützen. Die interne Benutzerdatenbank ist der einfachste Weg, um mit OpenSearch Service zu beginnen.

Aktivieren der differenzierten Zugriffskontrolle

Ermöglichen Sie eine differenzierte Zugriffskontrolle mithilfe der Konsole oder der Konfigurations-API. AWS CLI Informationen zu den erforderlichen Schritten finden Sie unter Erstellen und Verwalten von Domains.

Für eine detaillierte Zugriffskontrolle ist Elasticsearch 6.7 OpenSearch oder höher erforderlich. Außerdem sind HTTPS für den gesamten Datenverkehr zur Domain, Verschlüsselung ruhender Daten und Verschlüsselung erforderlich. node-to-node Je nachdem, wie Sie die erweiterten Funktionen der detaillierten Zugriffskontrolle konfigurieren, kann die zusätzliche Verarbeitung Ihrer Anfragen Rechen- und Speicherressourcen auf einzelnen Datenknoten erfordern. Nachdem Sie die differenzierte Zugriffskontrolle aktiviert haben, können Sie sie nicht mehr deaktivieren.

Aktivieren der differenzierten Zugriffskontrolle für vorhandene Domains

Sie können eine differenzierte Zugriffskontrolle für bestehende Domains aktivieren, auf denen Elasticsearch 6.7 OpenSearch oder höher ausgeführt wird.

So aktivieren Sie die differenzierte Zugriffskontrolle für eine vorhandene Domain (Konsole)

1. Wählen Sie die Domain aus und wählen Sie Aktionen und Sicherheitskonfiguration bearbeiten.
2. „True“ zur Aktivierung der differenzierten Zugriffskontrolle.
3. Auswahl zur Erstellung des Hauptbenutzers:

   - Wenn Sie IAM für die Benutzerverwaltung verwenden möchten, wählen Sie IAM-ARN als Haupt-Benutzer festlegen, und geben Sie den ARN für eine IAM-Rolle an.
   - Wenn Sie die interne Benutzerdatenbank verwenden möchten, wählen Sie Masterbenutzer erstellen und geben Sie einen Benutzernamen und ein Passwort an.
4. (Optional) Wählen Sie Migrationszeitraum für offene/IP-basierte Zugriffsrichtlinie aktivieren aus. Diese Einstellung aktiviert einen 30-tägigen Übergangszeitraum, in dem Ihre bestehenden Benutzer weiterhin ohne Unterbrechungen auf die Domain zugreifen können, sowie vorhandene offene und IP-basierte Zugriffsrichtlinien weiterhin mit Ihrer Domain arbeiten werden. Während diesem Migrationszeitraum empfehlen wir Administratoren, die notwendigen Rollen zu erstellen und diese Benutzern für die Domain zuzuordnen. Wenn Sie identitätsbasierte Richtlinien anstelle einer offenen oder IP-basierten Zugriffsrichtlinie verwenden, können Sie diese Einstellung deaktivieren.

   Sie müssen Ihre Clients ebenfalls aktualisieren, um während des Migrationszeitraums mit einer differenzierten Zugriffskontrolle arbeiten zu können. Wenn Sie beispielsweise IAM-Rollen mit detaillierter Zugriffskontrolle zuordnen, müssen Sie Ihre Clients aktualisieren, damit sie Anfragen mit AWS Signature Version 4 signieren können. Wenn Sie die HTTP-Standardauthentifizierung mit einer differenzierten Zugriffskontrolle konfigurieren, müssen Sie Ihre Clients aktualisieren, um in Anfragen entsprechende grundlegende Anmeldeinformationen zur Authentifizierung bereitzustellen.

Während der Migrationsphase landen Benutzer, die auf den OpenSearch Dashboards-Endpunkt für die Domain zugreifen, direkt auf der Discover-Seite und nicht auf der Anmeldeseite. Administratoren und Master-Benutzer können Anmeldung auswählen, um sich mit Administrator-Anmeldeinformationen anzumelden und das Rollen-Mapping zu konfigurieren.

> **Important**
>
> OpenSearch Der Service deaktiviert den Migrationszeitraum automatisch nach 30 Tagen. Wir empfehlen die Beendigung des Migrationszeitraums, sobald Sie die erforderlichen Rollen erstellt und sie Benutzern zugeordnet haben. Nach Beendigung des Migrationszeitraums können Sie ihn nicht erneut aktivieren.

5. Wählen Sie Änderungen speichern aus.

Die Änderung löst ein Blau/Grün-Bereitstellung aus, in der der Cluster-Zustand rot wird. Alle Cluster-Operationen bleiben davon jedoch unberührt.

So aktivieren Sie die differenzierte Zugriffskontrolle für eine vorhandene Domain (CLI)

Ändern Sie `AnonymousAuthEnabled` zu `true`, um den Migrationszeitraum mit einer differenzierten Zugriffskontrolle zu aktivieren:

```
aws opensearch update-domain-config --domain-name test-domain --region us-east-1 \
      --advanced-security-options '{ "Enabled": true,
 "InternalUserDatabaseEnabled":true, "MasterUserOptions": {"MasterUserName":"master-
username","MasterUserPassword":"master-password"},"AnonymousAuthEnabled": true}'
```

Über die Rolle „default_role“

Die differenzierte Zugriffskontrolle erfordert das Rollen-Mapping. Wenn Ihre Domain identitätsbasierte Zugriffsrichtlinien verwendet, ordnet OpenSearch Service Ihre Benutzer automatisch einer neuen Rolle namens default_role zu, um Sie bei der ordnungsgemäßen Migration vorhandener Benutzer zu unterstützen. Diese temporäre Zuordnung stellt sicher, dass Ihre Benutzer weiterhin erfolgreich IAM-signierte GET- und PUT-Anfragen senden können, bis Sie Ihr eigenes Rollen-Mapping erstellen.

Die Rolle fügt Ihrer Service-Domain keine Sicherheitslücken oder -mängel hinzu. OpenSearch Wir empfehlen die Löschung der Standardrolle, sobald Sie Ihre eigenen Rollen erstellt und entsprechend zugeordnet haben.

Migrationszenarien

In der folgenden Tabelle wird das Verhalten für jede Authentifizierungsmethode vor und nach dem Aktivieren der differenzierten Zugriffskontrolle für eine vorhandene Domain beschrieben und die Schritte, die Administratoren durchführen müssen, um ihre Benutzer ordnungsgemäß Rollen zuzuordnen:

Authentifizierungsmethode	Vor der Aktivierung der differenzierten Zugriffskontrolle	Nach der Aktivierung der differenzierten Zugriffskontrolle	Aufgaben des Administrators
Identitätsbasierte Richtlinien	Alle Benutzer, die IAM-Richtlinie erfüllen, können auf die Domain zugreifen.	Sie müssen den Migrationszeitraum nicht aktivieren. OpenSearch Der Service ordnet automatisch alle Benutzer, die IAM-Richtlinie erfüllen, der Rolle default_role zu, sodass sie weiterhin auf die Domain zugreifen können.	1. Benutzerdefiniertes Rollen-Mapping für die Domain erstellen. 2. Löschen Sie die Rolle default_role.
IP-basierte Richtlinien	Alle Benutzer von den zulässigen IP-Adressen oder CIDR-Blöcken können auf die Domain zugreifen.	Während des 30-tägigen Migrationszeitraums können alle Benutzer von den zulässigen IP-Adressen oder CIDR-Blöcken weiterhin auf die Domain zugreifen.	1. Benutzerdefiniertes Rollen-Mapping für die Domain erstellen. 2. Aktualisieren Sie Ihre Clients, um je nach Konfiguration des Rollen-Mapping entweder Anmeldeinformationen für die grundlegende Authentifizierung oder IAM-Anmeldeinformationen bereitzustellen.

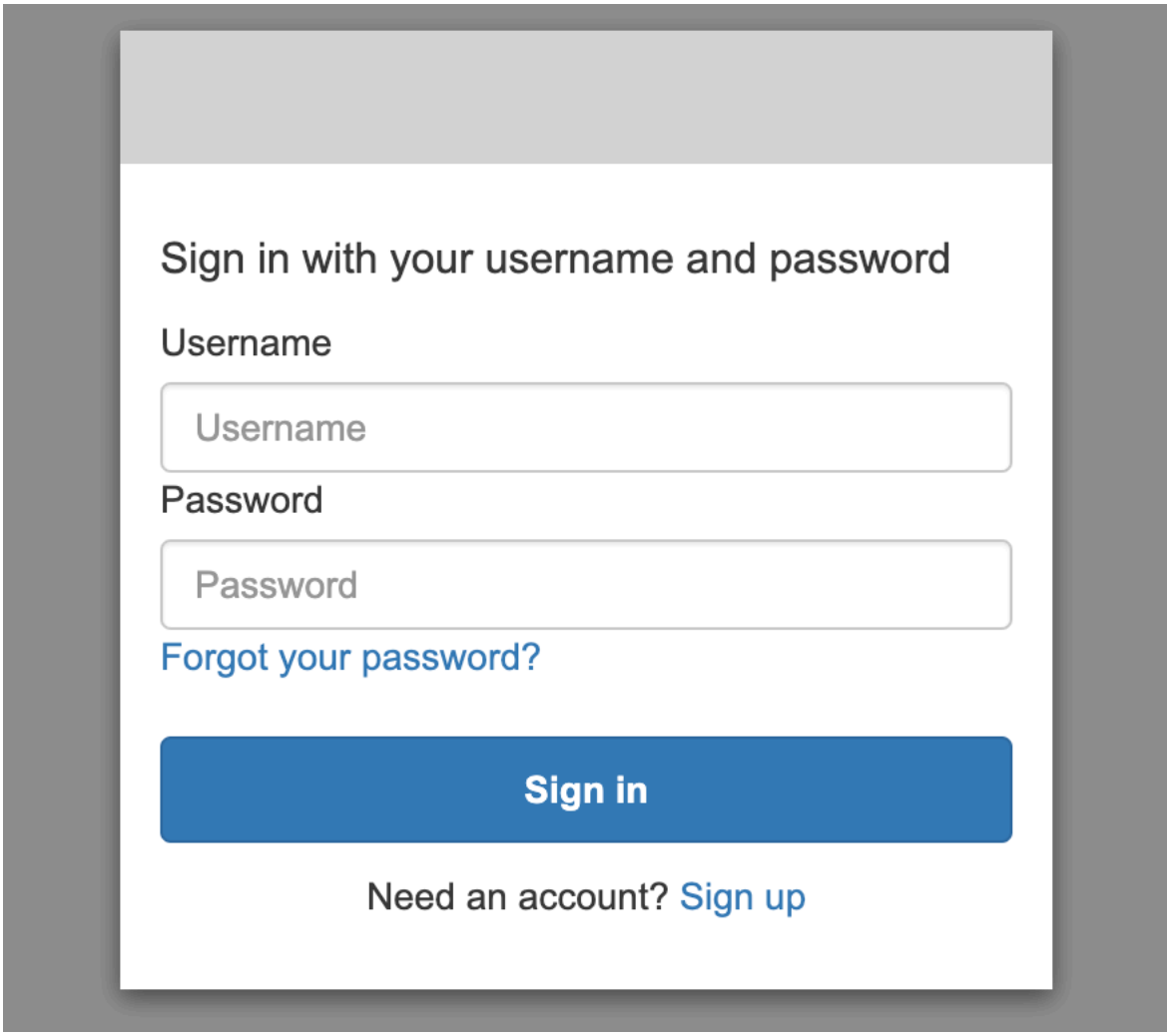
Authentifizierungsmethode	Vor der Aktivierung der differenzierten Zugriffskontrolle	Nach der Aktivierung der differenzierten Zugriffskontrolle	Aufgaben des Administrators
			3. Den Migrationszeitraum deaktivieren. Benutzer von den zulässigen IP-Adressen oder CIDR-Blöcken, die Anfragen ohne grundlegende Authentifizierung oder IAM-Anmeldeinformationen senden, verlieren den Zugriff auf die Domain.
Offene Zugriffsrichtlinien	Alle Benutzer im Internet können auf die Domain zugreifen.	Während des 30-tägigen Migrationszeitraums können alle Benutzer über das Internet weiterhin auf die Domain zugreifen.	1. Erstellen Sie Rollenzuordnungen in der Domain. 2. Aktualisieren Sie Ihre Clients, um je nach Konfiguration des Rollen-Mapping entweder Anmeldeinformationen für die grundlegende Authentifizierung oder IAM-Anmeldeinformationen bereitzustellen. 3. Den Migrationszeitraum deaktivieren. Benutzer, die Anfragen ohne grundlegende Authentifizierung oder IAM-Anmeldeinformationen senden, verlieren den Zugriff auf die Domain.

Als Masterbenutzer auf OpenSearch Dashboards zugreifen

Die differenzierte Zugriffskontrolle verfügt über ein OpenSearch Dashboards-Plugin, das Verwaltungsaufgaben vereinfacht. Mit Dashboards können Sie Benutzer, Rollen, Zuweisungen, Aktionsgruppen und Mandanten verwalten. Die Anmeldeseite von OpenSearch Dashboards und die zugrunde liegende Authentifizierungsmethode unterscheiden sich jedoch, je nachdem, wie Sie Benutzer verwalten und Ihre Domain konfiguriert haben.

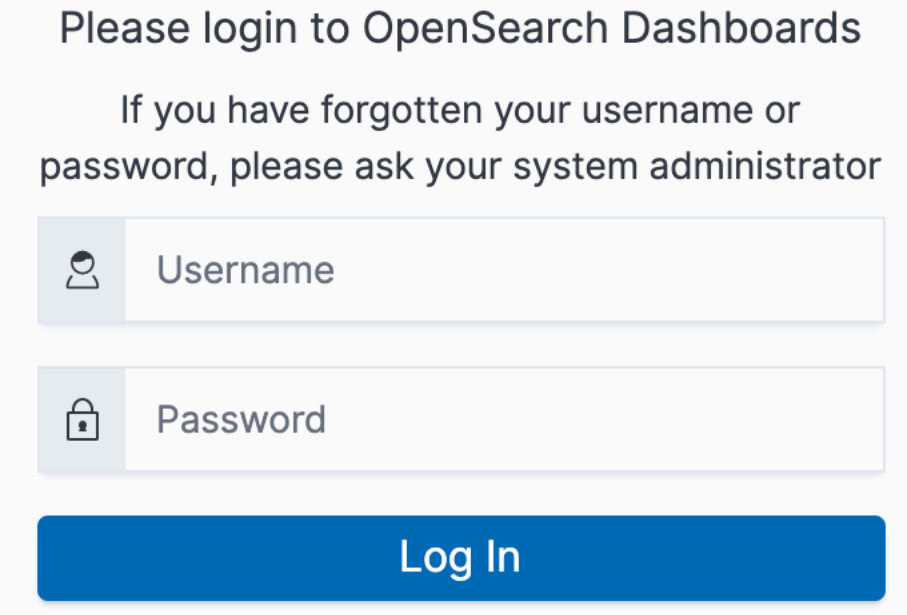
- Wenn Sie IAM für die Benutzerverwaltung verwenden möchten, verwenden Sie the section called “Amazon Cognito Cognito-Authentifizierung für Dashboards OpenSearch ”, um auf Dashboards zuzugreifen. Andernfalls zeigt Dashboards eine nicht funktionierende Anmeldeseite an. Siehe the section called “Einschränkungen”.

  Bei der Amazon-Cognito-Authentifizierung muss eine der angenommenen Rollen aus dem Identitätspool mit der IAM-Rolle übereinstimmen, die Sie für den Hauptbenutzer angegeben haben. Weitere Informationen zu dieser Konfiguration finden Sie unter the section called “(Optional) Konfigurieren von individuell festgelegtem Zugriff” und the section called “Tutorial: Detaillierte Zugriffskontrolle mit Cognito-Authentifizierung”.



- Wenn Sie die interne Benutzerdatenbank verwenden möchten, können Sie sich mit Ihrem Hauptbenutzernamen und Passwort bei Dashboards anmelden. Sie müssen über HTTPS auf Dashboards zugreifen. Amazon Cognito und SAML-Authentifizierung für Dashboards ersetzen beide diesen Anmeldebildschirm.

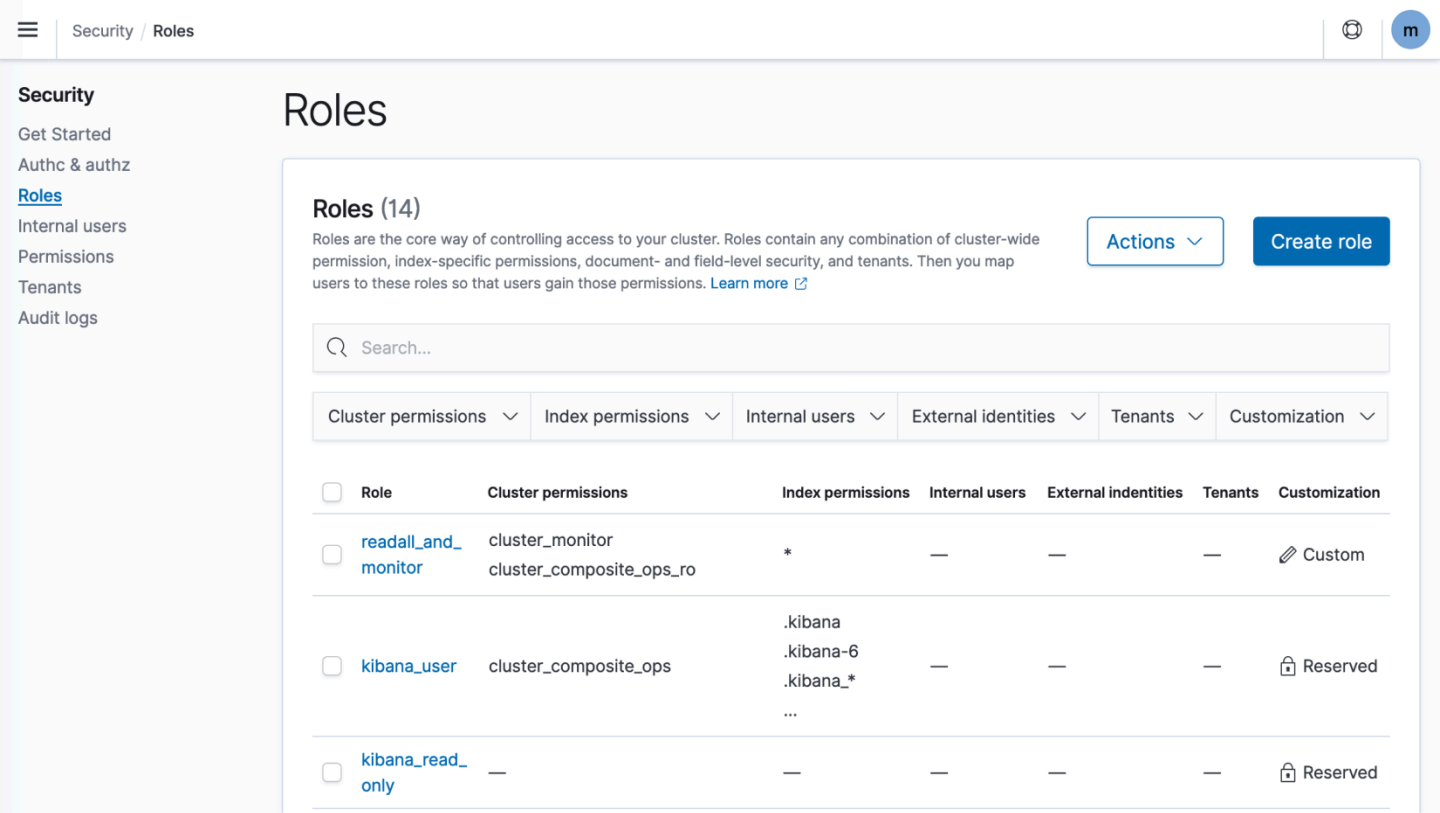
Weitere Informationen zu dieser Konfiguration finden Sie unter the section called “Tutorial: Interne Benutzerdatenbank mit einfacher Authentifizierung”.



- Falls Sie die SAML-Authentifizierung verwenden, können Sie sich mit den Anmeldeinformationen eines externen Identitätsanbieters anmelden. Weitere Informationen finden Sie unter the section called “SAML-Authentifizierung für Dashboards OpenSearch ”.

Verwalten von Berechtigungen

Wie in the section called “Die wichtigsten Konzepte” erwähnt, verwalten Sie differenzierte Zugriffskontrollberechtigungen mithilfe von Rollen, Benutzern und Zuweisungen. In diesem Abschnitt wird beschrieben, wie diese Ressourcen erstellt und angewendet werden. Wir empfehlen Ihnen, sich bei Dashboards als Hauptbenutzer anzumelden, um diese Operationen auszuführen.



> **Note**
>
> Die Berechtigungen, die Sie Ihren Benutzern gewähren möchten, variieren je nach Anwendungsfall stark. Wir können nicht alle Szenarien in dieser Dokumentation durchführbar abdecken. Achten Sie bei der Entscheidung, welche Berechtigungen Sie Ihren Benutzern gewähren möchten, darauf, die in den folgenden Abschnitten genannten OpenSearch Cluster- und Indexberechtigungen zu beachten und stets das Prinzip der geringsten Rechte zu beachten.

Erstellen von Rollen

Sie können mithilfe von OpenSearch Dashboards oder dem `_plugins/_security` Vorgang in der REST-API neue Rollen für eine detaillierte Zugriffskontrolle erstellen. Weitere Informationen finden Sie unter Rollen erstellen.

Die differenzierte Zugriffskontrolle umfasst auch eine Reihe vordefinierter Rollen. Clients wie OpenSearch Dashboards und Logstash stellen eine Vielzahl von Anfragen an OpenSearch, was es schwierig machen kann, Rollen mit den Mindestberechtigungen manuell zu erstellen.

Die `opensearch_dashboards_user` Rolle umfasst beispielsweise die Berechtigungen, die ein Benutzer benötigt, um mit Indexmustern, Visualisierungen, Dashboards und Mandanten zu arbeiten. Es wird empfohlen, sie einer beliebigen Benutzer- oder Backend-Rolle zuzuweisen, die auf Dashboards zugreift, zusammen mit zusätzlichen Rollen, die den Zugriff auf andere Indizes ermöglichen.

Amazon OpenSearch Service bietet die folgenden OpenSearch Rollen nicht an:

- `observability_full_access`
- `observability_read_access`
- `reports_read_access`
- `reports_full_access`

Amazon OpenSearch Service bietet mehrere Rollen an, die nicht verfügbar sind bei OpenSearch:

- `ultrawarm_manager`
- `ml_full_access`
- `cold_manager`
- `notifications_full_access`
- `notifications_read_access`

Sicherheit auf Clusterebene

Berechtigungen auf Clusterebene beinhalten die Möglichkeit, breite Anforderungen wie `_mget`, `_msearch` und `_bulk` zu machen, die Integrität zu überwachen, Snapshots zu erstellen und vieles mehr. Verwalten Sie diese Berechtigungen mithilfe des Abschnitts Clusterberechtigungen beim Erstellen einer Rolle. Eine vollständige Liste der Berechtigungen auf Clusterebene finden Sie unterCluster-Berechtigungen.

Anstelle einzelner Berechtigungen können Sie häufig Ihren gewünschten Sicherheitsstatus mithilfe einer Kombination der Standard-Aktionsgruppen erreichen. Eine Liste der Aktionsgruppen auf Cluster-Ebene finden Sie unter Clusterebene.

Sicherheit auf Index-Ebene

Berechtigungen auf Index-Ebene beinhalten die Möglichkeit, neue Indizes zu erstellen, Indizes zu durchsuchen, Dokumente zu lesen und zu schreiben, Dokumente zu löschen, Aliase zu verwalten

und vieles mehr. Verwalten Sie diese Berechtigungen beim Erstellen einer Rolle mithilfe des Abschnitts Index Permissions (Indexberechtigungen). Eine vollständige Liste der Berechtigungen auf Indexebene finden Sie unter Berechtigungen indizieren.

Anstelle einzelner Berechtigungen können Sie häufig Ihren gewünschten Sicherheitsstatus mithilfe einer Kombination der Standard-Aktionsgruppen erreichen. Eine Liste der Aktionsgruppen auf Index-Ebene finden Sie unter Index-Ebene.

Sicherheit auf Dokumentebene

Mit der Sicherheit auf Dokumentebene können Sie einschränken, welche Dokumente in einem Index ein Benutzer anzeigen kann. Geben Sie beim Erstellen einer Rolle ein Indexmuster und eine OpenSearch Abfrage an. Alle Benutzer, die Sie dieser Rolle zuordnen, können nur die Dokumente sehen, die mit der Abfrage übereinstimmen. Die Sicherheit auf Dokumentebene wirkt sich auf die Anzahl der Treffer aus, die Sie bei der Suche erhalten.

Weitere Informationen finden Sie unter Sicherheit auf Dokumentenebene.

Sicherheit auf Feldebene

Mit der Sicherheit auf Feldebene können Sie steuern, welche Dokumentfelder ein Benutzer anzeigen kann. Fügen Sie beim Erstellen einer Rolle eine Liste von Feldern hinzu, die entweder eingeschlossen oder ausgeschlossen werden sollen. Wenn Sie Felder einschließen, können alle Benutzer, die Sie dieser Rolle zuordnen, nur diese Felder sehen. Wenn Sie Felder ausschließen, können sie alle Felder mit Ausnahme der ausgeschlossenen sehen. Die Sicherheit auf Feldebene wirkt sich auf die Anzahl der Felder aus, die bei der Suche in Treffer enthalten sind.

Weitere Informationen finden Sie unter Sicherheit auf Feldebene.

Feldmaskierung

Die Feldmaskierung ist eine Alternative zur Sicherheit auf Feldebene, mit der Sie die Daten in einem Feld anonymisieren können, anstatt sie vollständig zu entfernen. Fügen Sie beim Erstellen einer Rolle eine Liste von Feldern hinzu, die maskiert werden sollen. Die Feldmaskierung wirkt sich darauf aus, ob beim Suchen der Inhalt eines Feldes angezeigt wird.

> **Tip**
>
> Wenn Sie die Standardmaskierung auf ein Feld anwenden, verwendet OpenSearch Service einen sicheren, zufälligen Hash, der zu ungenauen Aggregationsergebnissen führen kann.

Verwenden Sie stattdessen die musterbasierte Maskierung, um Aggregationen für maskierte Felder durchzuführen.

Erstellen von Benutzern

Wenn Sie die interne Benutzerdatenbank aktiviert haben, können Sie Benutzer mithilfe von OpenSearch Dashboards oder der `_plugins/_security` Operation in der REST-API erstellen. Weitere Informationen finden Sie unter Benutzer erstellen.

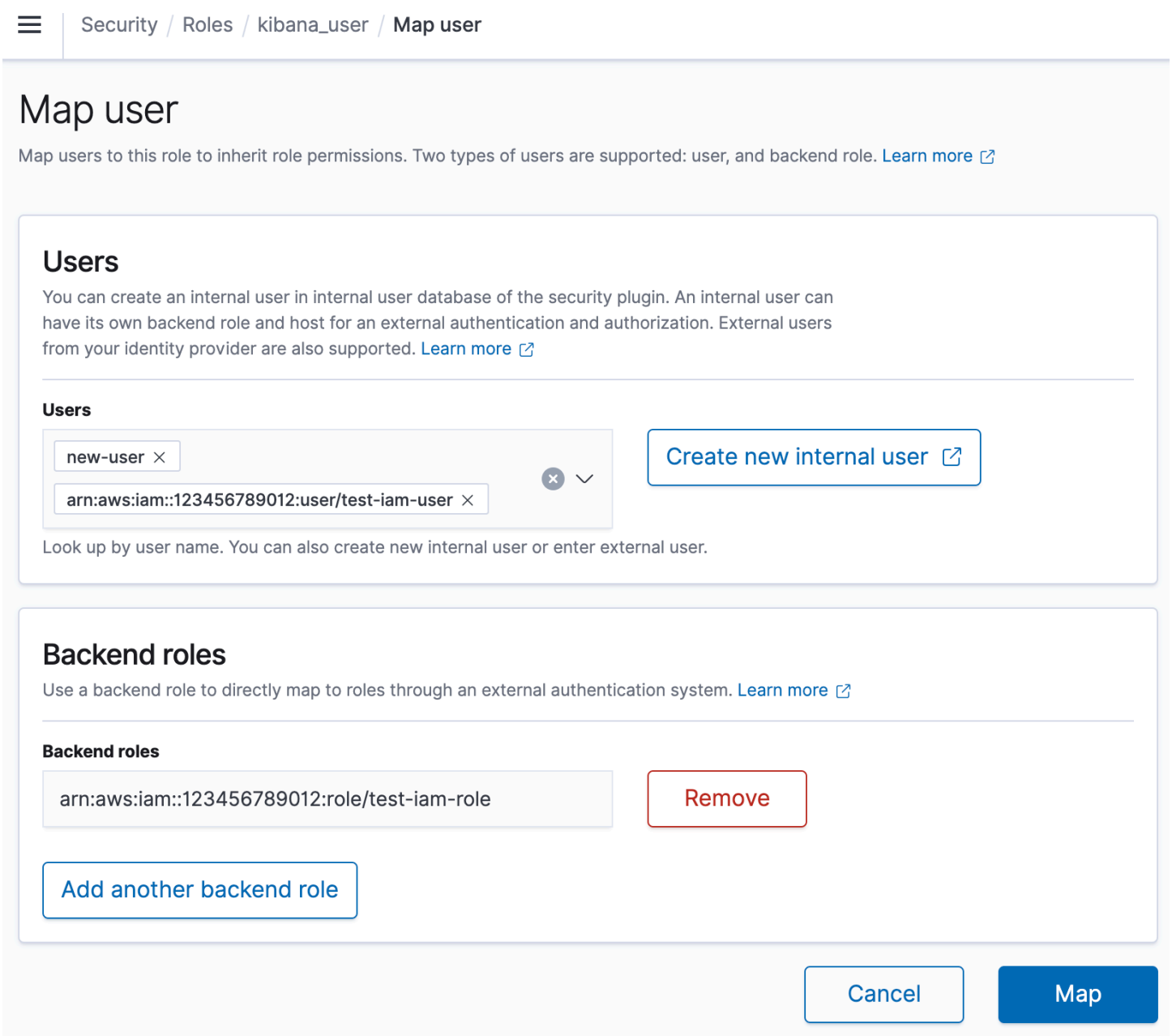
Wenn Sie sich für IAM als Ihren Hauptbenutzer entschieden haben, ignorieren Sie diesen Teil von Dashboards. Erstellen Sie stattdessen IAM-Rollen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch.

Rollen an Benutzer zuweisen

Das Rollen-Mapping ist der kritischste Aspekt der differenzierten Zugriffskontrolle. Die differenzierte Zugriffskontrolle verfügt über einige vordefinierte Rollen, die Ihnen beim Einstieg helfen. Wenn Sie jedoch nicht den Benutzern Rollen zuordnen, endet jede Anforderung an den Cluster mit einem Berechtigungsfehler.

Backend-Rollen können dazu beitragen, den Rollenzuordnungsprozess zu vereinfachen. Anstatt dieselbe Rolle 100 einzelnen Benutzern zuzuordnen, können Sie die Rolle einer einzelnen Backend-Rolle zuordnen, die sich alle 100 Benutzer teilen. Backend-Rollen können IAM-Rollen oder beliebige Zeichenfolgen sein.

- Geben Sie Benutzer, Benutzer-ARNs und Amazon-Cognito-Benutzerzeichenfolgen im Abschnitt Users (Benutzer) an. Cognito-Benutzerzeichenfolgen haben die Form von `Cognito/`*`user-pool-id`*`/`*`username`*.
- Geben Sie Backend-Rollen und IAM-Rollen-ARNs im Abschnitt Backend roles (Backend-Rollen) an.



Mithilfe von OpenSearch Dashboards oder der `_plugins/_security` Operation in der REST-API können Sie Benutzern Rollen zuordnen. Weitere Informationen finden Sie unter Zuordnen von Benutzern zu Rollen.

Aktionsgruppen erstellen

Aktionsgruppen sind Gruppen von Berechtigungen, die Sie über verschiedene Ressourcen hinweg wiederverwenden können. Sie können mithilfe von OpenSearch Dashboards oder der `_plugins/_security` Operation in der REST-API neue Aktionsgruppen erstellen, obwohl die

Standardaktionsgruppen für die meisten Anwendungsfälle ausreichend sind. Weitere Informationen zu den Standardaktionsgruppen finden Sie unter Standardaktionsgruppen.

OpenSearch Dashboards, Mehrmandantenfähigkeit

Mandanten (Tenants) sind Räume zum Speichern von Indexmustern, Visualisierungen, Dashboards und anderen Dashboards-Objekten. Mit der Mehrmandantenfähigkeit von Dashboards können Sie Ihre Arbeit sicher mit anderen Dashboard-Benutzern teilen (oder sie privat halten) und Mandanten dynamisch konfigurieren. Sie können steuern, welche Rollen Zugriff auf einen Mandanten haben, und ob diese Rollen Lese- oder Schreibzugriff haben. Der globale Mandant ist der Standardmandant. Weitere Informationen finden Sie unter Mehrmandantenfähigkeit von Dashboards. OpenSearch

So zeigen Sie Ihren aktuellen Mandanten an oder ändern Mandanten:

1. Navigieren Sie zu OpenSearch Dashboards und melden Sie sich an.
2. Wählen Sie oben rechts Ihr Benutzersymbol aus und wählen Sie Tenant wechseln.
3. Überprüfen Sie Ihren Mandanten, bevor Sie Visualisierungen oder Dashboards erstellen. Wenn Sie Ihre Arbeit mit allen anderen Dashboards-Benutzern teilen möchten, wählen Sie Global. Um Ihre Arbeit für eine Teilmenge von Dashboards-Benutzern freizugeben, wählen Sie einen anderen freigegebenen Mandanten aus. Andernfalls wählen Sie Private (Privat).

> **Note**
>
> OpenSearch Dashboards verwaltet einen separaten Index für jeden Mandanten und erstellt eine Indexvorlage namens. `tenant_template` Löschen oder ändern Sie den `tenant_template` Index nicht, da dies zu Fehlfunktionen der OpenSearch Dashboards führen kann, wenn die Indexzuordnung des Mandanten falsch konfiguriert ist.

Empfohlene Konfigurationen

Aufgrund der Interaktion der differenzierten Zugriffskontrolle mit anderen Sicherheitsfunktionen empfehlen wir mehrere differenzierte Zugriffskontrollkonfigurationen, die für die meisten Anwendungsfälle gut funktionieren.

Beschreibung	Hauptbenutzer	Domain-Zugriffsrichtlinie

Verwenden Sie IAM-Anmeldeinformationen für Aufrufe der OpenSearch APIs und verwenden Sie die SAML-Authentifizierung, um auf Dashboards zuzugreifen. Verwalten Sie differenzierte Zugriffskontrollrollen mithilfe von Dashboards oder der REST-API.	IAM-Rolle oder -Benutzer	<pre>{
		  "Version": "2012-10-17",
		  "Statement": [
		  {
		  "Effect": "Allow",
		  "Principal": {
		  "AWS": "*"
		  },
		  "Action": "es:ESHttp*",
		  "Resource": " *domain-arn* /*"
		  }
		  ]
		}</pre>

Verwenden Sie IAM-Anmeldeinformationen oder die Standardauthentifizierung für Aufrufe der APIs. OpenSearch Verwalten Sie differenzierte Zugriffskontrollrollen mithilfe von Dashboards oder der REST-API.
 	
Diese Konfiguration bietet viel Flexibilität, insbesondere wenn Sie OpenSearch Clients haben, die nur die Standardauthentifizierung unterstützen.
 	
Wenn Sie über einen vorhandenen Identitätsanbieter verfügen,
	Nutzername und Passwort	<pre>{
		  "Version": "2012-10-17",
		  "Statement": [
		  {
		  "Effect": "Allow",
		  "Principal": {
		  "AWS": "*"
		  },
		  "Action": "es:ESHttp*",
		  "Resource": " *domain-arn* /*"
		  }
		  ]
		}</pre>

Beschreibung	Hauptbenutzer	Domain-Zugriffsrichtlinie
verwenden Sie die SAML-Authentifizierung, um auf Dashboards zuzugreifen. Andernfalls verwalten Sie Dashboards-Benutzer in der internen Benutzerdatenbank.		

Verwenden Sie IAM-Anmeldeinformationen für Aufrufe der OpenSearch APIs und verwenden Sie Amazon Cognito, um auf Dashboards zuzugreifen. Verwalten Sie differenzierte Zugriffskontrollrollen mithilfe von Dashboards oder der REST-API.	IAM-Rolle oder -Benutzer	<pre>{
		  "Version": "2012-10-17",
		  "Statement": [
		  {
		  "Effect": "Allow",
		  "Principal": {
		  "AWS": "*"
		  },
		  "Action": "es:ESHttp*",
		  "Resource": " *domain-arn* /*"
		  }
		  ]
		}</pre>

Beschreibung	Hauptbenutzer	Domain-Zugriffsrichtlinie

Verwenden Sie IAM-Anmeldeinformationen für Aufrufe der OpenSearch APIs und blockieren Sie die meisten Zugriffe auf Dashboards. Verwalten Sie differenzierte Zugriffskontrollrollen mithilfe oder der REST-API.	IAM-Rolle oder -Benutzer	{
		"Version": "2012-10-17",
		"Statement": [
		{
		"Effect": "Allow",
		"Principal": {
		"AWS": "*"
		},
		"Action": "es:ESHttp*",
		"Resource": " *domain-arn* /*"
		},
		{
		"Effect": "Deny",
		"Principal": {
		"AWS": "*"
		},
		"Action": "es:ESHttp*",
		"Resource": " *domain-arn* /_dashboards*"
		}
		]
		}

Einschränkungen

Die differenzierte Zugriffskontrolle hat mehrere wichtige Einschränkungen:

- Der `hosts`-Aspekt von Rollen-Mappings, der Rollen Hostnamen oder IP-Adressen zuweist, funktioniert nicht, wenn sich die Domain innerhalb einer VPC befindet. Sie können jedoch Rollen weiterhin Benutzern und Backend-Rollen zuordnen.
- Wenn Sie IAM für den Master-Benutzer auswählen und die Amazon-Cognito- oder SAML-Authentifizierung nicht aktivieren, zeigt Dashboards eine nicht funktionierende Anmeldeseite an.
- Wenn Sie IAM für den Master-Benutzer auswählen, können Sie weiterhin Benutzer in der internen Benutzerdatenbank erstellen. Da die HTTP-Standardauthentifizierung unter dieser Konfiguration nicht aktiviert ist, werden jedoch alle mit diesen Benutzeranmeldeinformationen signierten Anforderungen abgelehnt.

- Wenn Sie SQL verwenden, um einen Index abzufragen, auf den Sie keinen Zugriff haben, erhalten Sie den Fehler „No permissions (Keine Berechtigungen)“. Wenn der Index nicht existiert, erhalten Sie den Fehler „no such index (Kein solcher Index vorhanden)“. Dieser Unterschied bei den Fehlermeldungen bedeutet, dass Sie die Existenz eines Index bestätigen können, wenn Sie zufällig seinen Namen erraten.

  Um das Problem zu minimieren, geben Sie keine vertraulichen Informationen in Indexnamen ein. Um jeden Zugriff auf SQL zu verweigern, fügen Sie der Domainszugriffsrichtlinie das folgende Element hinzu:

```
{
  "Effect": "Deny",
  "Principal": {
    "AWS": [
      "*"
    ]
  },
  "Action": [
    "es:*"
  ],
  "Resource": "arn:aws:es:us-east-1:123456789012:domain/my-domain/_plugins/_sql"
}
```

- Wenn Ihre Domain-Version 2.3 oder höher ist und Sie eine differenzierte Zugriffskontrolle aktiviert haben, führt die Einstellung auf 1 `max_clause_count` zu Problemen mit Ihrer Domain. Wir empfehlen, für dieses Konto eine höhere Zahl festzulegen.
- Wenn Sie die differenzierte Zugriffskontrolle in einer Domäne aktivieren, in der keine differenzierte Zugriffskontrolle eingerichtet ist, müssen Sie für Datenquellen, die für direkte Abfragen erstellt wurden, die detaillierten Zugriffssteuerungsrollen selbst einrichten. Weitere Informationen zum Einrichten detaillierter Zugriffsrollen finden Sie unter Erstellen von Amazon OpenSearch Service-Datenquellenintegrationen mit Amazon S3.

Hauptbenutzer ändern

Wenn Sie die Details des Master-Benutzers vergessen haben, können Sie ihn mithilfe der Konsole, AWS CLI, oder der Konfigurations-API neu konfigurieren.

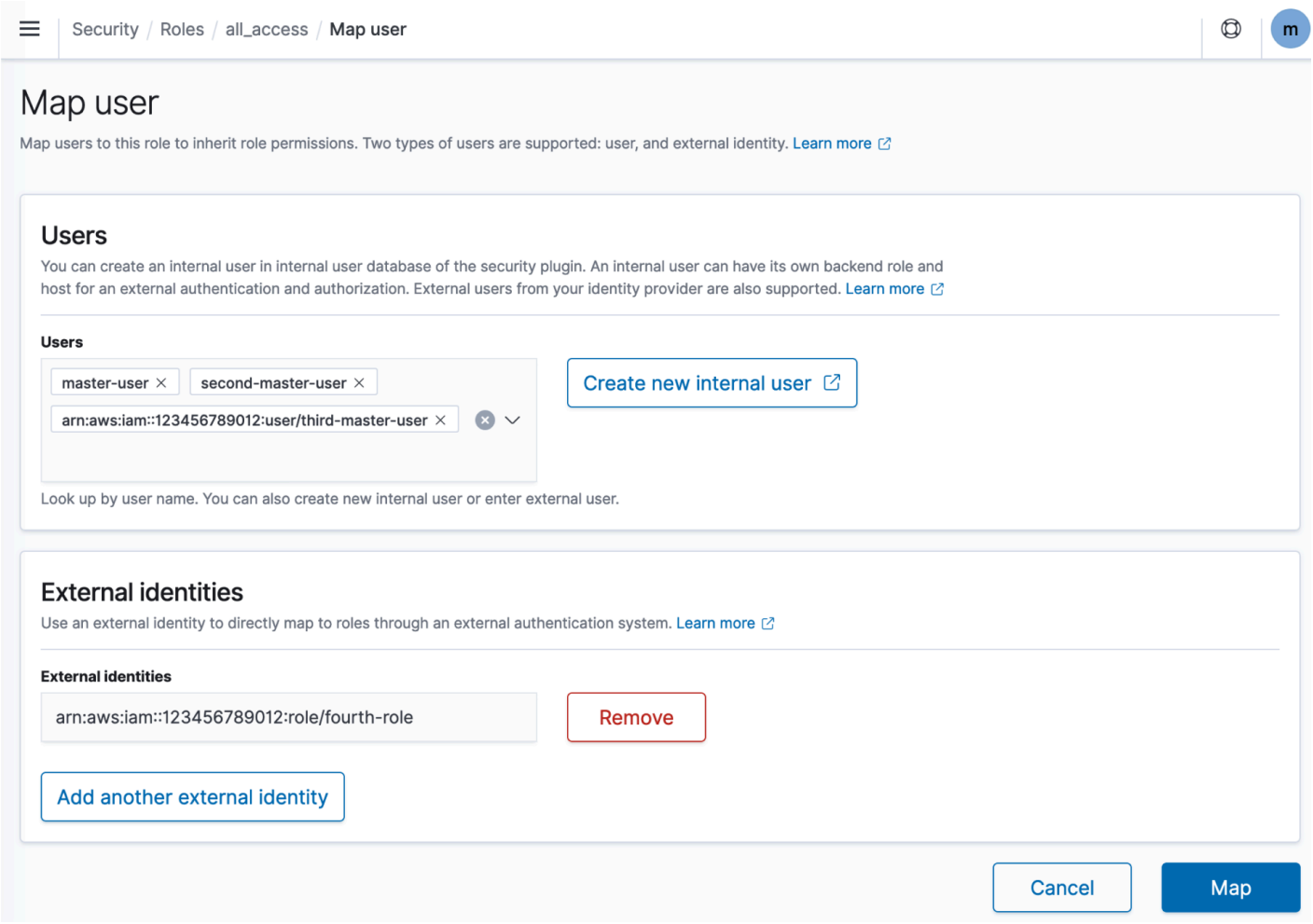
So ändern Sie den Master-Benutzer (Konsole):

1. Navigieren Sie zur Amazon OpenSearch Service-Konsole unter https://console.aws.amazon.com/aos/home/.
2. Wählen Sie Ihre Domain aus und wählen Sie Actions (Aktionen), Edit security configuration (Sicherheitskonfiguration bearbeiten).
3. Wählen Sie entweder IAM-ARN als Hauptbenutzer festlegen oder Neuen Hauptbenutzer erstellen aus.
   - Wenn Sie zuvor einen IAM-Master-Benutzer verwendet haben, ordnet die differenzierte Zugriffskontrolle die `all_access`-Rolle dem von Ihnen angegebenen neuen IAM-ARN neu zu.
   - Wenn Sie zuvor die interne Benutzerdatenbank verwendet haben, erstellt die differenzierte Zugriffskontrolle einen neuen Master-Benutzer. Sie können den neuen Master-Benutzer verwenden, um den alten zu löschen.
   - Beim Wechsel von der internen Benutzerdatenbank zu einem IAM-Hauptbenutzer werden keine Benutzer aus der internen Benutzerdatenbank gelöscht. Stattdessen deaktiviert es nur die HTTP-Basisauthentifizierung. Löschen Sie Benutzer manuell aus der internen Benutzerdatenbank oder behalten Sie sie für den Fall, dass Sie die HTTP-Basisauthentifizierung je wieder aktivieren müssen.
4. Wählen Sie Änderungen speichern aus.

Zusätzliche Hauptbenutzer

Sie bestimmen einen Master-Benutzer, wenn Sie eine Domain erstellen, aber wenn Sie möchten, können Sie diesen Master-Benutzer verwenden, um zusätzliche Master-Benutzer zu erstellen. Sie haben zwei Optionen: OpenSearch Dashboards oder die REST-API.

- Wählen Sie in Dashboards Sicherheit, Rollen und weisen Sie den neuen Hauptbenutzer den Rollen `all_access` und `security_manager` zu.



- Um die REST-API zu verwenden, senden Sie die folgenden Anforderungen:

```
PUT _plugins/_security/api/rolesmapping/all_access
{
  "backend_roles": [
    "arn:aws:iam::123456789012:role/fourth-master-user"
  ],
  "hosts": [],
  "users": [
    "master-user",
    "second-master-user",
    "arn:aws:iam::123456789012:user/third-master-user"
  ]
}
```

```
PUT _plugins/_security/api/rolesmapping/security_manager
{
```

```
  "backend_roles": [
    "arn:aws:iam::123456789012:role/fourth-master-user"
  ],
  "hosts": [],
  "users": [
    "master-user",
    "second-master-user",
    "arn:aws:iam::123456789012:user/third-master-user"
  ]
}
```

Diese Anforderungen ersetzen die aktuellen Rollen-Mappings. Führen Sie daher zuerst GET-Anforderungen aus, damit Sie alle aktuellen Rollen in die PUT-Anforderungen aufnehmen können. Die REST-API ist besonders nützlich, wenn Sie nicht auf Dashboards zugreifen können und der `all_access`-Rolle eine IAM-Rolle aus Amazon Cognito zuordnen möchten.

Manuelle Snapshots

Die differenzierte Zugriffskontrolle bringt einige zusätzliche Komplikationen bei der Erstellung manueller Snapshots mit sich. Um ein Snapshot-Repository zu registrieren – auch wenn Sie die HTTP-Basisauthentifizierung für alle anderen Zwecke verwenden – müssen Sie die `manage_snapshots`-Rolle einer IAM-Rolle zuordnen, die über `iam:PassRole` Berechtigungen zum Annehmen von `TheSnapshotRole` verfügt, wie in the section called “Voraussetzungen” definiert.

Verwenden Sie dann diese IAM-Rolle, um eine signierte Anforderung an die Domain zu senden, wie in the section called “Registrieren eines manuellen Snapshot-Repositorys” beschrieben.

Integrationen

Wenn Sie andere AWS Dienste mit OpenSearch Service verwenden, müssen Sie den IAM-Rollen für diese Dienste die entsprechenden Berechtigungen zuweisen. Beispielsweise verwenden Firehose-Lieferstreams häufig eine IAM-Rolle namens. `firehose_delivery_role` Erstellen Sie in Dashboards eine Rolle für die differenzierte Zugriffskontrolle, und ordnen Sie dieser die IAM-Rolle zu. In diesem Fall benötigt die neue Rolle die folgenden Berechtigungen:

```
{
  "cluster_permissions": [
    "cluster_composite_ops",
    "cluster_monitor"
  ],
```

```
  "index_permissions": [{
    "index_patterns": [
      "firehose-index*"
    ],
    "allowed_actions": [
      "create_index",
      "manage",
      "crud"
    ]
  }]
}
```

Berechtigungen variieren je nach den Aktionen, die jeder Service ausführt. Eine AWS IoT Regel oder AWS Lambda Funktion, die Daten indexiert, benötigt wahrscheinlich ähnliche Berechtigungen wie Firehose, während eine Lambda-Funktion, die nur Suchen durchführt, einen eingeschränkteren Satz verwenden kann.

REST-API-Unterschiede

Die detaillierte REST-API für die Zugriffskontrolle unterscheidet sich je nach Ihrer /Elasticsearch-Version geringfügig. OpenSearch Bevor Sie eine PUT-Anforderung stellen, stellen Sie eine GET-Anforderung, um den erwarteten Anforderungsinhalt zu überprüfen. Beispielsweise gibt eine GET-Anforderung an `_plugins/_security/api/user` alle Benutzer zurück, die Sie dann ändern und verwenden können, um gültige PUT-Anforderungen zu stellen.

Auf Elasticsearch 6.x sehen Anforderungen zum Erstellen von Benutzern wie folgt aus:

```
PUT _opendistro/_security/api/user/new-user
{
  "password": "some-password",
  "roles": ["new-backend-role"]
}
```

Auf OpenSearch oder Elasticsearch 7.x sehen Anfragen so aus (wechseln `_plugins` Sie zu, wenn Sie Elasticsearch verwenden): `_opendistro`

```
PUT _plugins/_security/api/user/new-user
{
  "password": "some-password",
  "backend_roles": ["new-backend-role"]
}
```

Außerdem sind Tenants Eigenschaften von Rollen in Elasticsearch 6.x:

```
GET _opendistro/_security/api/roles/all_access

{
  "all_access": {
    "cluster": ["UNLIMITED"],
    "tenants": {
      "admin_tenant": "RW"
    },
    "indices": {
      "*": {
        "*": ["UNLIMITED"]
      }
    },
    "readonly": "true"
  }
}
```

In OpenSearch und Elasticsearch 7.x handelt es sich um Objekte mit eigener URI (ändern Sie `_plugins` zu, `_opendistro` wenn Sie Elasticsearch verwenden):

```
GET _plugins/_security/api/tenants

{
  "global_tenant": {
    "reserved": true,
    "hidden": false,
    "description": "Global tenant",
    "static": false
  }
}
```

Die Dokumentation zur OpenSearch REST-API finden Sie in der API-Referenz für das Sicherheits-Plugin.

> **Tip**
>
> Wenn Sie die interne Benutzerdatenbank verwenden, können Sie curl verwenden, um Anforderungen zu stellen und Ihre Domain zu testen. Probieren Sie die folgenden Beispielbefehle aus:

```
curl -XGET -u 'master-user:master-user-password' 'domain-endpoint/_search'
curl -XGET -u 'master-user:master-user-password' 'domain-endpoint/_plugins/
_security/api/user'
```

Tutorial: Konfigurieren einer Domain mit einem IAM-Hauptbenutzer und Amazon-Cognito-Authentifizierung

Dieses Tutorial behandelt einen beliebten Amazon OpenSearch Service-Anwendungsfall für eine differenzierte Zugriffskontrolle: einen IAM-Master-Benutzer mit Amazon Cognito Cognito-Authentifizierung für Dashboards. OpenSearch

Im Tutorial konfigurieren wir eine Haupt-IAM-Rolle und eine eingeschränkte IAM-Rolle, die wir dann Benutzern in Amazon Cognito zuordnen. Der Masterbenutzer kann sich dann bei OpenSearch Dashboards anmelden, den eingeschränkten Benutzer einer Rolle zuordnen und mithilfe einer detaillierten Zugriffskontrolle die Benutzerberechtigungen einschränken.

Obwohl diese Schritte den Amazon-Cognito-Benutzerpool für die Authentifizierung verwenden, funktioniert derselbe grundlegende Prozess für jeden Cognito-Authentifizierungsanbieter, mit dem Sie verschiedenen Benutzern unterschiedliche IAM-Rollen zuweisen können.

In diesem Tutorial führen Sie die folgenden Schritte durch:

1. Erstellen von Haupt- und eingeschränkten IAM-Rollen
2. Erstellen einer Domain mit Cognito-Authentifizierung
3. Konfigurieren Sie einen Cognito-Benutzerpool und einen Identitätspool
4. Ordnen Sie Rollen in Dashboards zu OpenSearch
5. Testen der Berechtigungen

Schritt 1: Erstellen von Haupt- und eingeschränkten IAM-Rollen

Navigieren Sie zur AWS Identity and Access Management (IAM-) Konsole und erstellen Sie zwei separate Rollen:

- `MasterUserRole` – Der Hauptbenutzer, der über vollständige Berechtigungen für den Cluster verfügt und Rollen und Rollenzuordnungen verwaltet.
- `LimitedUserRole` – Eine eingeschränktere Rolle, der Sie als Hauptbenutzer eingeschränkten Zugriff gewähren.

Anweisungen zum Erstellen der Rollen finden Sie unter Erstellen einer Rolle mit benutzerdefinierten Vertrauensrichtlinien.

Beide Rollen müssen über die folgende Vertrauensrichtlinie verfügen, die es Ihrem Cognito-Identitätspool ermöglicht, die Rollen zu übernehmen:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Principal": {
      "Federated": "cognito-identity.amazonaws.com"
    },
    "Action": "sts:AssumeRoleWithWebIdentity",
    "Condition": {
      "StringEquals": {
        "cognito-identity.amazonaws.com:aud": "{identity-pool-id}"
      },
      "ForAnyValue:StringLike": {
        "cognito-identity.amazonaws.com:amr": "authenticated"
      }
    }
  }]
}
```

> **Note**
>
> Ersetzen Sie `identity-pool-id` durch die eindeutige Kennung Ihres Amazon-Cognito-Identitätspools. z. B. `us-east-1:0c6cdba7-3c3c-443b-a958-fb9feb207aa6`.

Schritt 2: Erstellen einer Domain mit Cognito-Authentifizierung

Navigieren Sie zur Amazon OpenSearch Service-Konsole unter https://console.aws.amazon.com/aos/home/ und erstellen Sie eine Domain mit den folgenden Einstellungen:

- OpenSearch 1.0 oder höher oder Elasticsearch 7.8 oder höher
- Öffentlicher Zugriff
- Detallierte Zugriffskontrolle, die mit `MasterUserRole` als Hauptbenutzer aktiviert ist (im vorherigen Schritt erstellt)
- Amazon Cognito Cognito-Authentifizierung für OpenSearch Dashboards aktiviert. Anweisungen zum Aktivieren der Cognito-Authentifizierung und zum Auswählen eines Benutzer- und Identitätspools finden Sie unter the section called “Konfigurieren einer Domain zur Verwendung der Amazon-Cognito-Authentifizierung”.
- Die folgende Domain-Zugriffsrichtlinie:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::{account-id}:root"
      },
      "Action": [
        "es:ESHttp*"
      ],
      "Resource": "arn:aws:es:{region}:{account-id}:domain/{domain-name}/*"
    }
  ]
}
```

- HTTPS für den gesamten Datenverkehr zur Domain erforderlich
- Keine Verschlüsselung ode-to-node
- Verschlüsselung gespeicherter Daten

Schritt 3: Cognito-Benutzer konfigurieren

Während Ihre Domain erstellt wird, konfigurieren Sie die Master- und eingeschränkten Benutzer in Amazon Cognito, indem Sie im Amazon Cognito Developer Guide unter Create a user pool

nachlesen. Konfigurieren Sie abschließend Ihren Identitätspool, indem Sie die Schritte unter Erstellen eines Identitätspools in Amazon Cognito befolgen. Der Benutzer- und der Identitätenpool müssen sich in derselben AWS-Region befinden.

Schritt 4: Rollen in OpenSearch Dashboards zuordnen

Nachdem Ihre Benutzer konfiguriert sind, können Sie sich als Hauptbenutzer bei OpenSearch Dashboards anmelden und Benutzer Rollen zuordnen.

1. Kehren Sie zur OpenSearch Servicekonsole zurück und navigieren Sie zur OpenSearch Dashboard-URL für die von Ihnen erstellte Domain. Die URL weist folgendes Format auf: *domain-endpoint*`/_dashboards/`.
2. Melden Sie sich mit den `master-user`-Anmeldeinformationen an.
3. Wählen Sie Add sample data (Beispieldaten hinzufügen) und fügen Sie die Beispielflugdaten hinzu.
4. Wählen Sie im linken Navigationsbereich Security (Sicherheit), Roles (Rollen), Create role (Rolle erstellen) aus.
5. Benennen Sie die Rolle `new-role`.
6. Geben Sie für Index `opensearch_dashboards_sample_data_fli*` (`kibana_sample_data_fli*` auf Elasticsearch-Domains) an.
7. Wählen Sie für Index permissions (Indexberechtigungen) die Option read (Lesen) aus.
8. Geben Sie für Sicherheitsabfrage auf Dokumentebene die folgende Abfrage an:

```
{
  "match": {
    "FlightDelay": true
  }
}
```

9. Wählen Sie für die Sicherheit auf Feldebene Ausschließen und geben Sie `FlightNum` an.
10. Fü rAnonymisierung, geben Sie `Dest` an.
11. Wählen Sie Erstellen.
12. Wählen Sie Zugeordnete Benutzer, Mapping verwalten. Fügen Sie den Amazon-Ressourcennamen (ARN) für `LimitedUserRole` als externe Identität hinzu und wählen Sie Map (Zuordnen) aus.

13. Kehren Sie zur Liste der Rollen zurück und wählen Sie opensearch_dashboards_useraus. Wählen Sie Zugeordnete Benutzer, Mapping verwalten. Fügen Sie den ARN für `LimitedUserRole` als Backend-Rolle hinzu und wählen Sie Zuordnen aus.

Schritt 5: Testen der Berechtigungen

Wenn Ihre Rollen korrekt zugeordnet sind, können Sie sich als Benutzer mit eingeschränkten Rechten anmelden und die Berechtigungen testen.

1. Navigieren Sie in einem neuen, privaten Browserfenster zur OpenSearch Dashboard-URL für die Domain, melden Sie sich mit den `limited-user` Anmeldeinformationen an und wählen Sie Auf eigene Faust erkunden aus.
2. Wählen Sie Entwicklerwerkzeuge aus und führen Sie dann die Standardsuche aus:

   ```
   GET _search
   {
     "query": {
       "match_all": {}
     }
   }
   ```

   Beachten Sie den Berechtigungsfehler. `limited-user` hat keine Berechtigungen zum Ausführen von clusterweiten Suchvorgängen.
3. Führen Sie eine weitere Suche aus:

   ```
   GET opensearch_dashboards_sample_data_flights/_search
   {
     "query": {
       "match_all": {}
     }
   }
   ```

   Beachten Sie, dass alle übereinstimmenden Dokumente ein `FlightDelay`-Feld von `true`, ein anonymisiertes `Dest`- Feld und kein `FlightNum`-Feld haben.
4. Wählen Sie in Ihrem ursprünglichen Browserfenster, angemeldet als `master-user`, Dev Tools, und führen Sie dann die gleichen Suchvorgänge durch. Beachten Sie die Unterschiede zwischen Berechtigungen, Anzahl der Treffer, übereinstimmenden Dokumenten und eingeschlossenen Feldern.

Tutorial: Konfigurieren einer Domain mit der internen Benutzerdatenbank und HTTP-Basisauthentifizierung

In diesem Tutorial wird ein weiterer beliebter, detaillierter Anwendungsfall für die Zugriffskontrolle behandelt: ein Hauptbenutzer in der internen Benutzerdatenbank und die HTTP-Basisauthentifizierung für Dashboards. OpenSearch Der Hauptbenutzer kann sich dann bei OpenSearch Dashboards anmelden, einen internen Benutzer erstellen, den Benutzer einer Rolle zuordnen und mithilfe einer detaillierten Zugriffskontrolle die Benutzerberechtigungen einschränken.

In diesem Tutorial führen Sie die folgenden Schritte durch:

1. Erstellen Sie eine Domain mit einem Masterbenutzer
2. Konfigurieren Sie einen internen Benutzer in OpenSearch Dashboards
3. Ordnen Sie Rollen in Dashboards zu OpenSearch
4. Testen der Berechtigungen

Schritt 1: Erstellen einer Domäne

Navigieren Sie zur Amazon OpenSearch Service-Konsole unter https://console.aws.amazon.com/aos/home/ und erstellen Sie eine Domain mit den folgenden Einstellungen:

- OpenSearch 1.0 oder höher oder Elasticsearch 7.9 oder höher
- Öffentlicher Zugriff
- Differenzierte Zugriffskontrolle mit einem Master-Benutzer in der internen Benutzerdatenbank (`TheMasterUser` für den Rest dieses Lernprogramms)
- Amazon Cognito-Authentifizierung für Dashboards deaktiviert
- Die folgende Zugriffsrichtlinie:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::{account-id}:root"
      },
      "Action": [
```

```
        "es:ESHttp*"
      ],
      "Resource": "arn:aws:es:{region}:{account-id}:domain/{domain-name}/*"
    }
  ]
}
```

- HTTPS für den gesamten Datenverkehr zur Domain erforderlich
- Keine ode-to-node Verschlüsselung
- Verschlüsselung gespeicherter Daten

Schritt 2: Erstellen Sie einen internen Benutzer in OpenSearch Dashboards

Da Sie nun über eine Domain verfügen, können Sie sich bei OpenSearch Dashboards anmelden und einen internen Benutzer erstellen.

1. Kehren Sie zur OpenSearch Servicekonsole zurück und navigieren Sie zur OpenSearch Dashboard-URL für die von Ihnen erstellte Domain. Die URL weist folgendes Format auf: *domain-endpoint*/_dashboards/.
2. Melden Sie sich mit dem an`TheMasterUser`.
3. Wählen Sie Add sample data (Beispieldaten hinzufügen) und fügen Sie die Beispielflugdaten hinzu.
4. Wählen Sie im linken Navigationsbereich Sicherheit, Interne Benutzer, Internen Benutzer erstellen aus.
5. Benennen Sie den Benutzer `new-user` und geben Sie ein Passwort an. Wählen Sie die Option Erstellen aus.

Schritt 3: Rollen in OpenSearch Dashboards zuordnen

Nachdem Ihr Benutzer nun konfiguriert ist, können Sie Ihren Benutzer einer Rolle zuordnen.

1. Bleiben Sie im Bereich Sicherheit der OpenSearch Dashboards und wählen Sie Rollen, Rolle erstellen aus.
2. Benennen Sie die Rolle `new-role`.
3. Geben Sie für Index `opensearch_dashboards_sample_data_fli*` (`kibana_sample_data_fli*`bei Elasticsearch-Domains) das Indexmuster an.

4. Wählen Sie für die Aktionsgruppe lesen aus.
5. Geben Sie für Sicherheitsabfrage auf Dokumentebene die folgende Abfrage an:

```
{
  "match": {
    "FlightDelay": true
  }
}
```

6. Wählen Sie für die Sicherheit auf Feldebene Ausschließen und geben Sie `FlightNum` an.
7. Fü rAnonymisierung, geben Sie `Dest` an.
8. Wählen Sie Erstellen.
9. Wählen Sie Zugeordnete Benutzer, Mapping verwalten. Fügen Sie dann `new-user` zu Benutzern hinzu und wählen Sie Zuordnen.
10. Kehren Sie zur Liste der Rollen zurück und wählen Sie opensearch_dashboards_useraus. Wählen Sie Zugeordnete Benutzer, Mapping verwalten. Fügen Sie dann `new-user` zu Benutzern hinzu und wählen Sie Zuordnen.

Schritt 4: Testen Sie die Berechtigungen

Wenn Ihre Rollen korrekt zugeordnet sind, können Sie sich als Benutzer mit eingeschränkten Rechten anmelden und die Berechtigungen testen.

1. Navigieren Sie in einem neuen, privaten Browserfenster zur OpenSearch Dashboard-URL für die Domain, melden Sie sich mit den `new-user` Anmeldeinformationen an und wählen Sie Auf eigene Faust erkunden aus.
2. Wählen Sie Entwicklerwerkzeuge aus und führen Sie dann die Standardsuche aus:

```
GET _search
{
  "query": {
    "match_all": {}
  }
}
```

   Beachten Sie den Berechtigungsfehler. `new-user` hat keine Berechtigungen zum Ausführen von clusterweiten Suchvorgängen.

3. Führen Sie eine weitere Suche aus:

```
GET dashboards_sample_data_flights/_search
{
  "query": {
    "match_all": {}
  }
}
```

   Beachten Sie, dass alle übereinstimmenden Dokumente ein `FlightDelay`-Feld von `true`, ein anonymisiertes `Dest`- Feld und kein `FlightNum`-Feld haben.

4. Wählen Sie in Ihrem ursprünglichen Browserfenster, angemeldet als `TheMasterUser`, Dev Tools, und führen Sie dann die gleichen Suchvorgänge durch. Beachten Sie die Unterschiede zwischen Berechtigungen, Anzahl der Treffer, übereinstimmenden Dokumenten und eingeschlossenen Feldern.

Konformitätsprüfung für Amazon OpenSearch Service

Externe Prüfer bewerten die Sicherheit und Konformität von Amazon OpenSearch Service im Rahmen mehrerer AWS Compliance-Programme. Zu diesen Programmen gehören SOC, PCI und HIPAA.

Wenn Sie Compliance-Anforderungen haben, sollten Sie erwägen, eine beliebige Version von OpenSearch Elasticsearch 6.0 oder höher zu verwenden. Frühere Versionen von Elasticsearch bieten keine Kombination aus Verschlüsselung ruhender Daten und node-to-node Verschlüsselung und erfüllen daher wahrscheinlich nicht Ihre Anforderungen. Sie könnten auch erwägen, eine beliebige Version von Elasticsearch 6.7 OpenSearch oder höher zu verwenden, wenn eine detaillierte Zugriffskontrolle für Ihren Anwendungsfall wichtig ist. Unabhängig davon garantiert die Wahl einer bestimmten Version OpenSearch oder einer Elasticsearch-Version bei der Erstellung einer Domain nicht die Einhaltung der Vorschriften.

Informationen darüber, ob AWS-Service ein in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter AWS-Services Umfang nach Compliance-Programm AWS-Services unter . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen unter .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- Schnellstartanleitungen zu Sicherheit und Compliance — In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Implementierung von Basisumgebungen beschrieben AWS , bei denen Sicherheit und Compliance im Mittelpunkt stehen.
- Architecting for HIPAA Security and Compliance on Amazon Web Services — In diesem Whitepaper wird beschrieben, wie Unternehmen HIPAA-fähige Anwendungen erstellen AWS können.

  > **Note**
  >
  > AWS-Services Nicht alle sind HIPAA-fähig. Weitere Informationen finden Sie in der Referenz für HIPAA-berechtigte Services.

- AWS Compliance-Ressourcen — Diese Sammlung von Arbeitsmappen und Leitfäden gilt möglicherweise für Ihre Branche und Ihren Standort.
- AWS Leitfäden zur Einhaltung von Vorschriften für Kunden — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.
- Evaluierung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub— Dies AWS-Service bietet einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerungsreferenz.
- Amazon GuardDuty — Dies AWS-Service erkennt potenzielle Bedrohungen für Ihre Workloads AWS-Konten, Container und Daten, indem es Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen

wie PCI DSS zu erfüllen, indem es die in bestimmten Compliance-Frameworks vorgeschriebenen Anforderungen zur Erkennung von Eindringlingen erfüllt.

- AWS Audit Manager— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Ausfallsicherheit in Amazon OpenSearch Service

Die globale AWS-Infrastruktur ist um AWS-Regionen und Availability Zones herum aufgebaut. AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die mit einem Netzwerk mit geringer Latenz, hohem Durchsatz und hoher Redundanz verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Availability Zones ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser hoch verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen über AWS-Regionen und Availability Zones finden Sie unter AWSGlobale Infrastruktur.

Neben der globalen AWS-Infrastruktur stellt OpenSearch Service verschiedene Funktionen bereit, um Ihren Anforderungen an Ausfallsicherheit und Datensicherung gerecht zu werden:

- Multi-AZ-Domänen und Replikat-Shards
- Automatisierte und manuelle Snapshots

JWT-Authentifizierung und Autorisierung für Amazon Service OpenSearch

Amazon OpenSearch Service ermöglicht es Ihnen jetzt, JSON Web Tokens (JWTs) für die Authentifizierung und Autorisierung zu verwenden. JWTs sind JSON-basierte Zugriffstoken, die verwendet werden, um Single Sign-On (SSO) -Zugriff zu gewähren. Sie können JWTs in OpenSearch Service verwenden, um Single Sign-On-Token zu erstellen, um Anfragen an Ihre Service-Domain zu validieren. OpenSearch Um JWTs verwenden zu können, müssen Sie eine detaillierte Zugriffskontrolle aktiviert haben und Sie müssen einen gültigen öffentlichen Schlüssel im RSA- oder ECDSA-PEM-Format angeben. Weitere Informationen zur feinkörnigen Zugriffskontrolle finden Sie unter Feinkörnige Zugriffskontrolle in Amazon Service. OpenSearch

Sie können JSON-Web-Tokens mithilfe der OpenSearch Service-Konsole, der AWS Command Line Interface (AWS CLI) oder der SDKs konfigurieren. AWS

Überlegungen

Bevor Sie JWTs mit Amazon OpenSearch Service verwenden, müssen Sie Folgendes berücksichtigen:

- Aufgrund der Größe der öffentlichen RSA-Schlüssel in der PEM-Formatierung empfehlen wir, die JWT-Authentifizierung und -Autorisierung über die AWS Konsole zu konfigurieren.
- Sie müssen gültige Benutzer und Rollen angeben, wenn Sie die Fächer- und Rollenfelder für Ihre JWTs angeben. Andernfalls werden Anfragen abgelehnt.

Ändern der Domainzugriffsrichtlinie

Bevor Sie Ihre Domain für die Verwendung der JWT-Authentifizierung und -Autorisierung konfigurieren können, müssen Sie Ihre Domänenzugriffsrichtlinie aktualisieren, damit JWT-Benutzer auf die Domain zugreifen können. Andernfalls werden alle eingehenden autorisierten JWT-Anfragen abgelehnt. Die empfohlene Domänenzugriffsrichtlinie für den vollständigen Zugriff auf die Unterressourcen (/*) lautet:

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "es:ESHttp*",
      "Resource": "domain-arn/*"
    }
  ]
}
```

Konfiguration der JWT-Authentifizierung und -Autorisierung

Sie können die JWT-Authentifizierung und -Autorisierung während der Domainerstellung oder durch Aktualisierung einer vorhandenen Domain aktivieren. Die Einrichtungsschritte variieren geringfügig, je nachdem, welche Option Sie wählen.

In den folgenden Schritten wird erklärt, wie Sie eine vorhandene Domäne für die JWT-Authentifizierung und -Autorisierung in der OpenSearch Servicekonsole konfigurieren:

1. Navigieren Sie unter Domänenkonfiguration zu JWT-Authentifizierung und Autorisierung für OpenSearch und wählen Sie JWT-Authentifizierung und Autorisierung aktivieren aus.
2. Konfigurieren Sie den öffentlichen Schlüssel, der für Ihre Domain verwendet werden soll. Dazu können Sie entweder eine PEM-Datei hochladen, die einen öffentlichen Schlüssel enthält, oder ihn manuell eingeben.

   > **Note**
   >
   > Wenn der hochgeladene oder eingegebene Schlüssel nicht gültig ist, erscheint über dem Textfeld eine Warnung, die das Problem angibt.

3. (Optional) Unter Zusätzliche Einstellungen können Sie die folgenden optionalen Felder konfigurieren

   - Betreffschlüssel — Sie können dieses Feld leer lassen, um den `sub` Standardschlüssel für Ihre JWTs zu verwenden.
   - Rollenschlüssel — Sie können dieses Feld leer lassen, um den `roles` Standardschlüssel für Ihre JWTs zu verwenden.

   Nachdem Sie Ihre Änderungen vorgenommen haben, speichern Sie Ihre Domain.

Verwenden eines JWT zum Senden einer Testanfrage

Nachdem Sie ein neues JWT mit einem bestimmten Betreff- und Rollenpaar erstellt haben, können Sie eine Testanfrage senden. Verwenden Sie dazu den privaten Schlüssel, um Ihre Anfrage über das Tool zu signieren, mit dem das JWT erstellt wurde. OpenSearch Der Service ist in der Lage, die eingehende Anfrage zu validieren, indem er diese Signatur überprüft.

> **Note**
>
> Wenn Sie einen benutzerdefinierten Betreff- oder Rollenschlüssel für Ihr JWT angegeben haben, müssen Sie die richtigen Anspruchsnamen für Ihr JWT verwenden.

Im Folgenden finden Sie ein Beispiel dafür, wie Sie ein JWT-Token verwenden, um über den Suchendpunkt Ihrer Domain auf den OpenSearch Service zuzugreifen:

```
curl -XGET "$search_endpoint" -H "Authorization: Bearer <JWT>"
```

Konfiguration der JWT-Authentifizierung und -Autorisierung ()AWS CLI

Der folgende AWS CLI Befehl aktiviert die JWT-Authentifizierung und -Autorisierung, OpenSearch sofern die Domäne vorhanden ist:

```
aws opensearch update-domain-config --domain-name <your_domain_name> --advanced-
security-options '{"JWTOptions":{"Enabled":true, "PublicKey": "<your_public_key>",
 "SubjectKey": "<your_subject_key>", "RolesKey": "<your_roles_key>"}}'
```

Konfiguration der JWT-Authentifizierung und -Autorisierung (Konfiguration über API)

Die folgende Anfrage an die Konfigurations-API aktiviert die JWT-Authentifizierung und -Autorisierung für OpenSearch eine bestehende Domain:

```
POST https://es.us-east-1.amazonaws.com/2021-01-01/opensearch/domain/my-domain/config
{
  "AdvancedSecurityOptions": {
    "JWTOptions": {
      "Enabled": true,
      "PublicKey": "public-key",
      "RolesKey": "optional-roles-key",
      "SubjectKey": "optional-subject-key"
   }
  }
}
```

Generieren eines key pair

Um JWTs für Ihre OpenSearch Domain zu konfigurieren, müssen Sie einen öffentlichen Schlüssel im PEM-Format (Privacy-Enhanced Mail) bereitstellen. Amazon OpenSearch Service unterstützt derzeit zwei asymetrische Verschlüsselungsalgorithmen bei der Verwendung von JWTs: RSA und ECDSA.

Gehen Sie wie folgt vor, um ein RSA-Schlüsselpaar mit der gemeinsamen OpenSSL-Bibliothek zu erstellen:

1. `openssl genrsa -out privatekey.pem 2048`
2. `openssl rsa -in privatekey.pem -pubout -out publickey.pem`

In diesem Beispiel enthält die `publickey.pem` Datei den öffentlichen Schlüssel für die Verwendung mit Amazon OpenSearch Service und den privaten Schlüssel zum Signieren der an den Service gesendeten JWTs. `privatekey.pem` Darüber hinaus haben Sie die Möglichkeit, den privaten Schlüssel in das häufig verwendete `pkcs8` Format zu konvertieren, falls Sie dieses für die Generierung Ihrer JWTs benötigen.

Wenn Sie die Upload-Schaltfläche verwenden, um eine PEM-Datei direkt zur Konsole hinzuzufügen, muss die Datei eine `.pem` Erweiterung haben. Andere Dateierweiterungen wie `.crt.cert`, oder `.key` werden derzeit nicht unterstützt.

Infrastruktursicherheit in Amazon OpenSearch Service

Als verwalteter Service ist Amazon OpenSearch Service durch die AWS globale Netzwerksicherheit von geschützt. Informationen zu AWS Sicherheitsservices und wie die Infrastruktur AWS schützt, finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung mit den bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastrukturschutz in Security Pillar AWS Well-Architected Framework.

Sie verwenden durch AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf OpenSearch Service zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Sie verwenden durch AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf die OpenSearch Service-Konfigurations-API zuzugreifen. Geben Sie in den Domain-Endpunkt-Optionen den `TLSSecurityPolicy`-Wert an, um die minimal erforderliche TLS-Version für die Annahme zu konfigurieren:

```
aws opensearch update-domain-config --domain-name my-domain --domain-endpoint-options
 '{"TLSSecurityPolicy": "Policy-Min-TLS-1-2-2019-07"}'
```

Einzelheiten finden Sie in der AWS CLI -Befehlsreferenz.

Abhängig von Ihrer Domänenkonfiguration müssen Sie möglicherweise auch Anfragen an die OpenSearch -APIs signieren. Weitere Informationen finden Sie unter the section called “Serviceanfragen stellen und signieren OpenSearch ”.

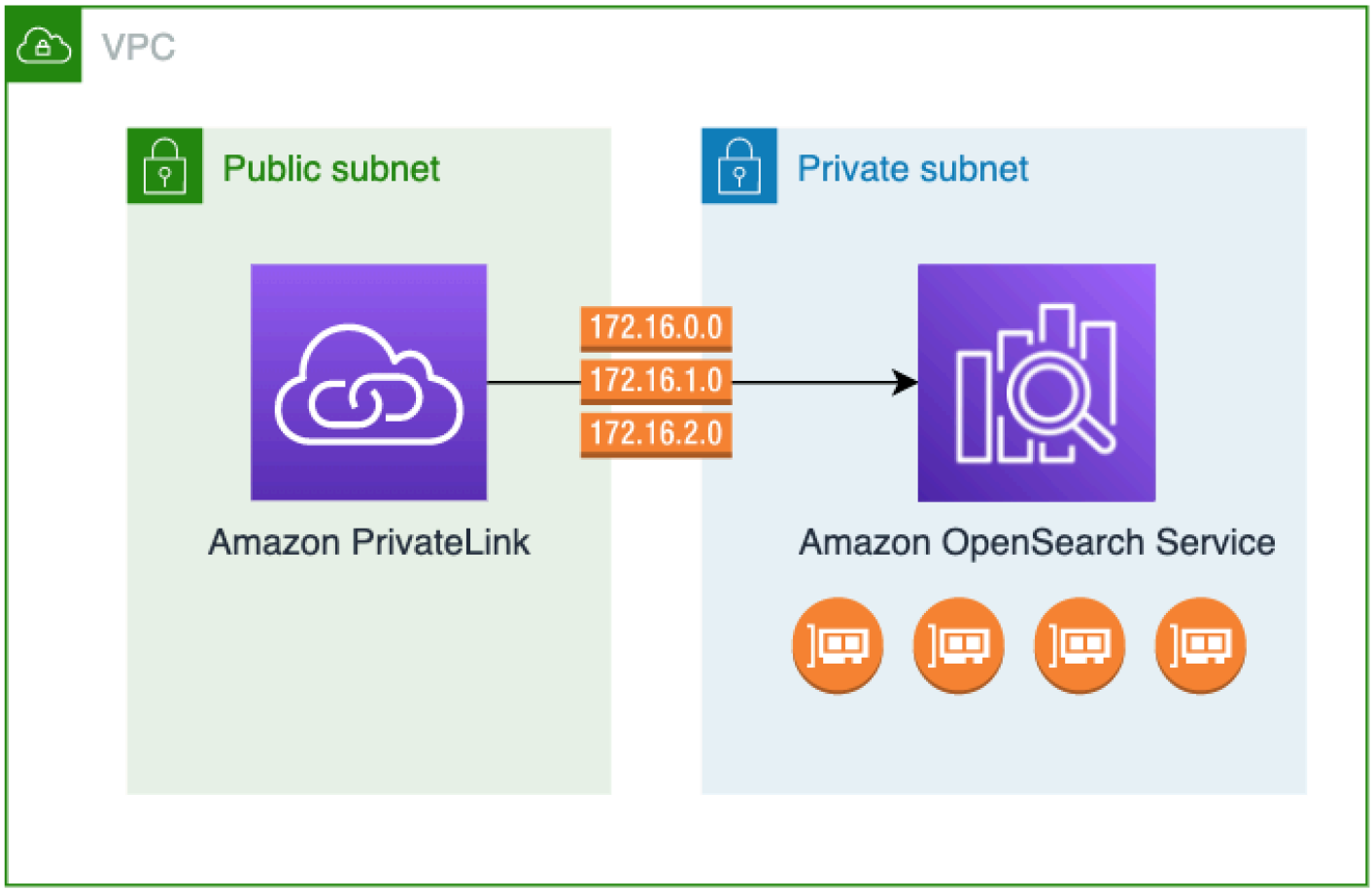
OpenSearch Der Service unterstützt Domains für öffentlichen Zugriff, die Anfragen von jedem mit dem Internet verbundenen Gerät empfangen können, und Domains für VPC-Zugriff, die vom öffentlichen Internet isoliert sind.

Zugriff auf Amazon OpenSearch Service über einen OpenSearch serviceverwalteten VPC-Endpunkt (AWS PrivateLink)

Sie können auf eine Amazon- OpenSearch Service-Domain zugreifen, indem Sie einen OpenSearch serviceverwalteten VPC-Endpunkt einrichten (unterstützt von AWS PrivateLink). Diese Endpunkte stellen eine private Verbindung zwischen Ihrer VPC und Amazon OpenSearch Service her. Sie können auf OpenSearch Service-VPC-Domains zugreifen, als wären sie in Ihrer VPC, ohne die Verwendung eines Internet-Gateways, NAT-Geräts, einer VPN-Verbindung oder einer - AWS Direct Connect Verbindung. Instances in Ihrer VPC benötigen keine öffentlichen IP-Adressen, um auf den OpenSearch Service zuzugreifen.

Sie können OpenSearch Service-Domains so konfigurieren, dass zusätzliche Endpunkte verfügbar sind, die in öffentlichen oder privaten Subnetzen innerhalb derselben VPC, einer anderen VPC oder einer anderen ausgeführt werden AWS-Konten. Auf diese Weise können Sie eine zusätzliche Sicherheitsebene für den Zugriff auf Ihre Domains hinzufügen, unabhängig davon, wo diese

ausgeführt werden, ohne dass eine Infrastruktur verwaltet werden muss. Das folgende Diagramm veranschaulicht OpenSearch serviceverwaltete VPC-Endpunkte innerhalb derselben VPC:



Sie stellen diese private Verbindung her, indem Sie einen OpenSearch serviceverwalteten Schnittstellen-VPC-Endpunkt erstellen, der von unterstützt wird AWS PrivateLink. Wir erstellen in jedem Subnetz, das Sie für den Schnittstellen-VPC-Endpunkt aktivieren, eine Endpunkt-Netzwerkschnittstelle. Dies sind serviceverwaltete Netzwerkschnittstellen, die als Eintrittspunkt für Datenverkehr dienen, der für OpenSearch Service bestimmt ist. Die AWS PrivateLink Standardpreise für Schnittstellenendpunkte gelten für OpenSearch serviceverwaltete VPC-Endpunkte, die unter abgerechnet werden AWS PrivateLink.

Sie können VPC-Endpunkte für Domänen erstellen, auf denen alle Versionen von OpenSearch und Legacy-Elasticsearch ausgeführt werden. Weitere Informationen finden Sie unter Zugriff auf AWS-Services über AWS PrivateLink im AWS PrivateLink -Leitfaden.

Überlegungen und Einschränkungen für OpenSearch Service

Bevor Sie einen Schnittstellen-VPC-Endpunkt für OpenSearch Service einrichten, lesen Sie Überlegungen im AWS PrivateLink -Handbuch.

Beachten Sie bei der Verwendung von OpenSearch serviceverwalteten VPC-Endpunkten Folgendes:

- Sie können nur Schnittstellen-VPC-Endpunkte verwenden, um eine Verbindung zu VPC-Domains herzustellen. Öffentliche Domains werden nicht unterstützt.
- VPC-Endpunkte können nur eine Verbindung zu Domains innerhalb derselben AWS-Regionherstellen.
- HTTPS ist das einzige unterstützte Protokoll für VPC-Endpunkte. HTTP ist nicht zulässig.
- OpenSearch Der Service unterstützt Aufrufe an alle unterstützten OpenSearch API-Operationen über einen Schnittstellen-VPC-Endpunkt.
- Sie können maximal 50 Endpunkte pro Konto und maximal 10 Endpunkte pro Domain konfigurieren. Eine einzelne Domain kann maximal über 10 autorisierte Prinzipale verfügen.
- Sie können derzeit nicht verwenden AWS CloudFormation , um Schnittstellen-VPC-Endpunkte zu erstellen.
- Sie können Schnittstellen-VPC-Endpunkte nur über die OpenSearch Servicekonsole oder mithilfe der OpenSearch Service-API erstellen. Sie können keine Schnittstellen-VPC-Endpunkte für OpenSearch Service mit der Amazon-VPC-Konsole erstellen.
- OpenSearch Serviceverwaltete VPC-Endpunkte sind nicht über das Internet zugänglich. Auf einen OpenSearch serviceverwalteten VPC-Endpunkt kann nur innerhalb der VPC zugegriffen werden, in der Endpunkt bereitgestellt wird, oder in allen VPCs, in denen der Endpunkt gemäß den Routing-Tabellen und Sicherheitsgruppen bereitgestellt wird.
- VPC-Endpunktrichtlinien werden für OpenSearch Service nicht unterstützt. Sie können eine Sicherheitsgruppe mit den Endpunktnetzwerkschnittstellen verknüpfen, um den Datenverkehr zum OpenSearch Service über den Schnittstellen-VPC-Endpunkt zu steuern.
- Ihre serviceverknüpfte Rolle muss sich in demselben AWS Konto befinden, das Sie zum Erstellen des VPC-Endpunkts verwenden.
- Um den OpenSearch Service-VPC-Endpunkt zu erstellen, zu aktualisieren und zu löschen, benötigen Sie zusätzlich zu Ihren Amazon- OpenSearch Service-Berechtigungen die folgenden Amazon EC2-Berechtigungen:
  - `ec2:CreateVpcEndpoint`
  - `ec2:DescribeVpcEndpoints`

- `ec2:ModifyVpcEndpoint`
- `ec2:DeleteVpcEndpoints`
- `ec2:CreateTags`
- `ec2:DescribeTags`
- `ec2:DescribeSubnets`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeVpcs`

> **Note**
>
> Derzeit können Sie die Erstellung von VPC-Endpunkten nicht auf OpenSearch Service beschränken. Wir arbeiten daran, dies in einem zukünftigen Update zu ermöglichen.

Zugriff auf eine Domain bereitstellen

Wenn sich die VPC, auf die Sie auf Ihre Domain zugreifen möchten, in einem anderen befindet AWS-Konto, müssen Sie sie vom Konto des Besitzers autorisieren, bevor Sie einen Schnittstellen-VPC-Endpunkt erstellen können.

So erlauben Sie einer VPC in einer anderen AWS-Konto den Zugriff auf Ihre Domain

1. Öffnen Sie die Amazon- OpenSearch Service-Konsole unter https://console.aws.amazon.com/aos/home/.
2. Wählen Sie im Navigationsbereich Domains aus und öffnen Sie die Domain, auf die Sie Zugriff gewähren möchten.
3. Wechseln Sie zur Registerkarte VPC endpoints (VPC-Endpunkte), auf der die Konten und entsprechenden VPCs angezeigt werden, die Zugriff auf Ihre Domain haben.
4. Wählen Sie Authorize principal (Prinzipal autorisieren) aus.
5. Geben Sie die AWS-Konto ID des Kontos ein, das auf Ihre Domain zugreifen soll. Dieser Schritt autorisiert das angegebene Konto, VPC-Endpunkte für die Domain zu erstellen.
6. Klicken Sie auf Authorize.

Erstellen eines Schnittstellen-VPC-Endpunkts für eine VPC-Domain

Sie können einen Schnittstellen-VPC-Endpunkt für OpenSearch Service entweder über die OpenSearch Servicekonsole oder die AWS Command Line Interface (AWS CLI) erstellen.

So erstellen Sie einen Schnittstellen-VPC-Endpunkt für eine - OpenSearch Service-Domain

1. Öffnen Sie die Amazon- OpenSearch Service-Konsole unter https://console.aws.amazon.com/aos/home/.
2. Wählen Sie im linken Navigationsbereich VPC endpoints (VPC-Endpunkte) aus.
3. Wählen Sie Endpunkt erstellen aus.
4. Wählen Sie aus, ob eine Domain im aktuellen AWS-Konto oder einem anderen verbunden werden soll AWS-Konto.
5. Wählen Sie die Domain aus, zu der Sie mit diesem Endpunkt eine Verbindung herstellen. Wenn sich die Domain in der aktuellen befindet AWS-Konto, wählen Sie die Domain aus der Dropdownliste aus. Wenn sich die Domain in einem anderen Konto befindet, geben Sie den Amazon-Ressourcennamen (ARN) der Domain ein, zu der eine Verbindung hergestellt werden soll. Um eine Domain in einem anderen Konto auszuwählen, muss der Eigentümer Ihnen Zugriff auf die Domain gewähren.
6. Wählen Sie für VPC die VPC aus, von der aus Sie auf OpenSearch Service zugreifen.
7. Wählen Sie für Subnetze ein oder mehrere Subnetze aus, von denen aus Sie auf den OpenSearch Service zugreifen.
8. Wählen Sie für Sicherheitsgruppen die Sicherheitsgruppen aus, die den Security groups (Endpunkt-Netzwerkschnittstellen) zugeordnet werden sollen. Dies ist ein wichtiger Schritt, in dem Sie einschränken, welche Ports, Protokolle und Quellen für eingehenden Datenverkehr Sie für Ihren Endpunkt autorisieren. Die Sicherheitsgruppenregeln müssen den Ressourcen, die den VPC-Endpunkt für die Kommunikation mit dem - OpenSearch Service verwenden, die Kommunikation mit der Endpunkt-Netzwerkschnittstelle ermöglichen.
9. Wählen Sie Endpunkt erstellen aus. Der Endpunkt sollte innerhalb von 2–5 Minuten aktiv sein.

Arbeiten mit OpenSearch serviceverwalteten VPC-Endpunkten unter Verwendung der Konfigurations-API

Verwenden Sie die folgenden API-Operationen, um OpenSearch serviceverwaltete VPC-Endpunkte zu erstellen und zu verwalten.

- CreateVpcEndpoint
- ListVpcEndpoints
- UpdateVpcEndpoint
- DeleteVpcEndpoint

Verwenden Sie die folgenden API-Operationen, um den Endpunktzugriff auf VPC-Domains zu verwalten:

- AuthorizeVpcEndpointAccess
- ListVpcEndpointAccess
- ListVpcEndpointsForDomain
- RevokeVpcEndpointAccess

SAML-Authentifizierung für Dashboards OpenSearch

Mit der SAML-Authentifizierung für OpenSearch Dashboards können Sie Ihren bestehenden Identitätsanbieter verwenden, um Single Sign-On (SSO) für Dashboards auf Amazon OpenSearch Service-Domains anzubieten, auf denen Elasticsearch 6.7 OpenSearch oder höher ausgeführt wird. Um die SAML-Authentifizierung zu verwenden, müssen Sie differenzierte Zugriffssteuerung aktivieren.

Anstatt sich über Amazon Cognito oder die interne Benutzerdatenbank zu authentifizieren, können Sie mit der SAML-Authentifizierung für OpenSearch Dashboards Identitätsanbieter von Drittanbietern verwenden, um sich bei Dashboards anzumelden, eine detaillierte Zugriffskontrolle zu verwalten, Ihre Daten zu durchsuchen und Visualisierungen zu erstellen. OpenSearch Der Service unterstützt Anbieter, die den SAML 2.0-Standard verwenden, wie Okta, Keycloak, Active Directory Federation Services (ADFS), Auth0 und. AWS IAM Identity Center

Die SAML-Authentifizierung für Dashboards ist nur für den Zugriff auf Dashboards über einen Webbrowser vorgesehen. OpenSearch Mit Ihren SAML-Anmeldeinformationen können Sie keine direkten HTTP-Anfragen an die OpenSearch APIs oder Dashboards stellen.

SAML-Konfigurationsübersicht

In dieser Dokumentation wird davon ausgegangen, dass Sie über einen vorhandenen Identitätsanbieter verfügen und damit vertraut sind. Wir können keine detaillierten

Konfigurationsschritte für Ihren genauen Anbieter bereitstellen, sondern nur für Ihre OpenSearch Service-Domain.

Der OpenSearch Anmeldevorgang für Dashboards kann eine von zwei Formen annehmen:

- Dienstanbieter (SP) initiiert: Sie navigieren zu Dashboards (z. B. `https://my-domain.us-east-1.es.amazonaws.com/_dashboards`), die Sie zum Anmeldebildschirm weiterleiten. Nachdem Sie sich angemeldet haben, leitet Sie der Identitätsanbieter zu Dashboards weiter.
- Identity Provider (IdP) initiiert: Sie navigieren zu Ihrem Identitätsanbieter, melden sich an und wählen OpenSearch Dashboards aus einem Anwendungsverzeichnis aus.

OpenSearch Der Service bietet zwei Single-Sign-On-URLs, SP-initiiert und IdP-initiiert. Sie benötigen jedoch nur die, die Ihrem gewünschten Dashboard-Anmeldeablauf entspricht. OpenSearch

Unabhängig davon, welchen Authentifizierungstyp Sie verwenden, besteht das Ziel darin, sich über Ihren Identitätsanbieter anzumelden und eine SAML-Assertion zu erhalten, die Ihren Benutzernamen (erforderlich) und alle Backend-Rollen (optional, aber empfohlen) enthält. Diese Informationen ermöglichen eine differenzierte Zugriffssteuerung, um SAML-Benutzern Berechtigungen zuzuweisen. Bei externen Identitätsanbietern werden Backend-Rollen normalerweise als „Rollen“ oder „Gruppen“ bezeichnet.

Überlegungen

Berücksichtigen Sie beim Konfigurieren der SAML-Authentifizierung Folgendes:

- Aufgrund der Größe der IdP-Metadatendatei empfehlen wir dringend, die AWS -Konsole zu verwenden, um die SAML-Authentifizierung zu konfigurieren.
- Domains unterstützen jeweils nur eine Dashboards-Authentifizierungsmethode. Wenn Sie die Amazon Cognito Cognito-Authentifizierung für OpenSearch Dashboards aktiviert haben, müssen Sie sie deaktivieren, bevor Sie die SAML-Authentifizierung aktivieren können.
- Wenn Sie einen Network Load Balancer mit SAML verwenden, müssen Sie zunächst einen benutzerdefinierten Endpunkt erstellen. Weitere Informationen finden Sie unter ???.

SAML-Authentifizierung für VPC-Domains

SAML erfordert keine direkte Kommunikation zwischen Ihrem Identitätsanbieter und Ihrem Serviceanbieter. Daher können Sie SAML auch dann verwenden, wenn Ihre OpenSearch Domain in einer privaten VPC gehostet wird, solange Ihr Browser sowohl mit Ihrem OpenSearch Cluster als

auch mit Ihrem Identitätsanbieter kommunizieren kann. Ihr Browser fungiert im Wesentlichen als Vermittler zwischen Ihrem Identitätsanbieter und Ihrem Dienstanbieter. Ein nützliches Diagramm, das den SAML-Authentifizierungsablauf erklärt, finden Sie in der Okta-Dokumentation.

Ändern der Domainzugriffsrichtlinie

Bevor Sie die SAML-Authentifizierung konfigurieren, müssen Sie die Domainzugriffsrichtlinie aktualisieren, um SAML-Benutzern Zugriff auf die Domain zu gewähren. Andernfalls werden Ihnen „Zugriff verweigert“-Fehler angezeigt.

Wir empfehlen die folgende Domain-Zugriffsrichtlinie, die vollen Zugriff auf die Unterressourcen (`/*`) in der Domain bietet:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "es:ESHttp*",
      "Resource": "domain-arn/*"
    }
  ]
}
```

Um die Richtlinie restriktiver zu gestalten, können Sie der Richtlinie eine IP-Adressbedingung hinzufügen. Diese Bedingung beschränkt den Zugriff nur auf den angegebenen IP-Adressbereich oder das angegebene Subnetz. Die folgende Richtlinie erlaubt beispielsweise den Zugriff nur vom Subnetz 192.0.2.0/24 aus:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": [
        "es:ESHttp*"
```

```
      ],
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": [
            "192.0.2.0/24"
          ]
        }
      },
      "Resource": "domain-arn/*"
    }
  ]
}
```

> **Note**
>
> Eine offene Domänenzugriffsrichtlinie erfordert, dass eine detaillierte Zugriffskontrolle für Ihre Domain aktiviert ist. Andernfalls wird der folgende Fehler angezeigt:
> `To protect domains with public access, a restrictive policy or fine-grained access control is required.`
> Wenn Sie einen Masterbenutzer oder internen Benutzer mit einem sicheren Passwort konfiguriert haben, kann es aus Sicherheitsgründen akzeptabel sein, die Richtlinie offen zu lassen und gleichzeitig eine differenzierte Zugriffskontrolle zu verwenden. Weitere Informationen finden Sie unter ???.

Konfigurieren der SP- oder IDP-initiierten Authentifizierung

In diesen Schritten wird erklärt, wie die SAML-Authentifizierung mit SP-initiierter oder IDP-initiierter Authentifizierung für Dashboards aktiviert wird. OpenSearch Informationen zum zusätzlichen Schritt, der zum Aktivieren beider Authentifizierungen erforderlich ist, finden Sie unter Konfigurieren der SP- oder IdP-initiierten Authentifizierung.

Schritt 1: SAML-Authentifizierung aktivieren

Sie können die SAML-Authentifizierung entweder während der Domainerstellung aktivieren oder indem Sie für eine vorhandene Domain Actions (Aktionen), Edit security configuration (Sicherheitskonfiguration bearbeiten) auswählen. Die folgenden Schritte unterscheiden sich geringfügig, je nachdem, welchen Sie auswählen.

Wählen Sie in der Domänenkonfiguration unter SAML-Authentifizierung für OpenSearch Dashboards/Kibana die Option SAML-Authentifizierung aktivieren aus.

Schritt 2: Ihren Identitätsanbieter konfigurieren

Führen Sie die folgenden Schritte aus, je nachdem, wann Sie die SAML-Authentifizierung konfigurieren.

Wenn Sie eine Domain erstellen

Wenn Sie gerade dabei sind, eine neue Domain zu erstellen, kann OpenSearch Service noch keine Entitäts-ID oder SSO-URLs für Dienstanbieter generieren. Ihr Identitätsanbieter benötigt diese Werte, um die SAML-Authentifizierung ordnungsgemäß zu aktivieren. Sie können jedoch erst generiert werden, nachdem die Domain erstellt wurde. Um diese Interdependenz bei der Domainerstellung zu umgehen, können Sie temporäre Werte in Ihre IdP-Konfiguration eingeben, um die erforderlichen Metadaten zu generieren, und sie dann aktualisieren, sobald Ihre Domain aktiv ist.

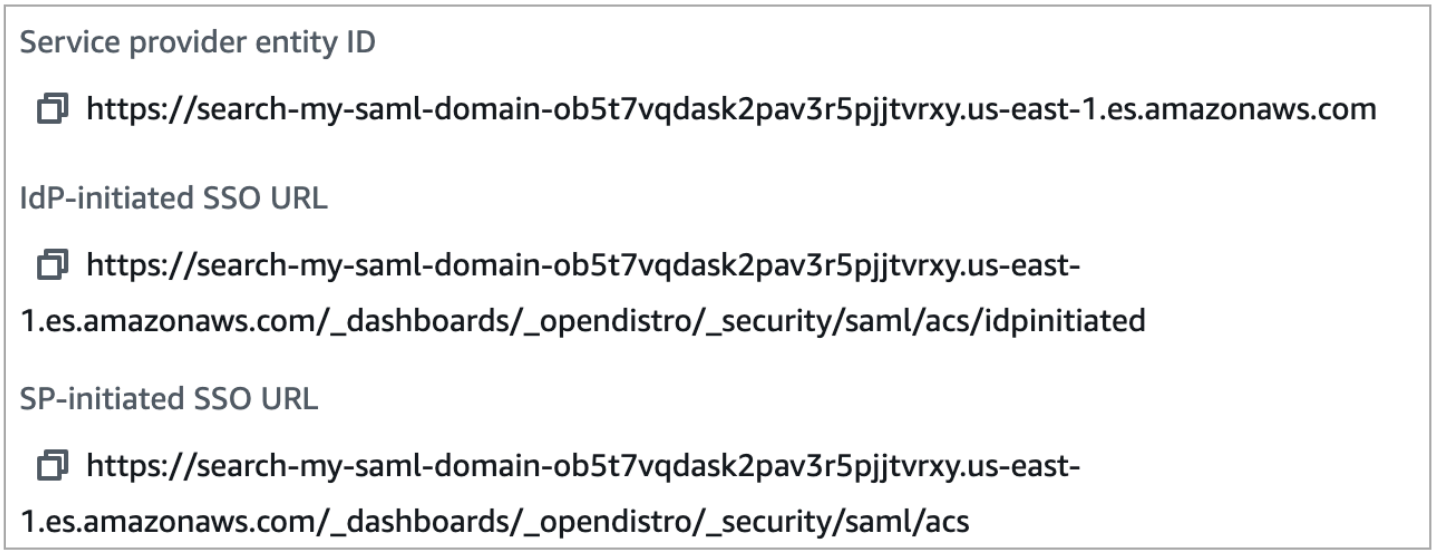
Wenn Sie einen benutzerdefinierten Endpunkt verwenden, können Sie ableiten, wie die URLs lauten werden. Wenn Ihr benutzerdefinierter Endpunkt beispielsweise `www.custom-endpoint.com` lautet, lautet die Entitäts-ID des Serviceanbieters `www.custom-endpoint.com`, die IDP-initiierte SSO-URL lautet `www.custom-endpoint.com/_dashboards/_opendistro/_security/saml/acs/idpinitiated` und die SP-initiierte SSO-URL ist `www.custom-endpoint.com/_dashboards/_opendistro/_security/saml/acs`. Sie können die Werte verwenden, um Ihren Identitätsanbieter zu konfigurieren, bevor die Domain erstellt wird. Beispiele finden Sie im nächsten Abschnitt.

Wenn Sie keinen benutzerdefinierten Endpunkt verwenden, können Sie temporäre Werte in Ihren IdP eingeben, um die erforderlichen Metadaten zu generieren, und sie später aktualisieren, nachdem die Domain aktiv ist.

In Okta können Sie beispielsweise `https://temp-endpoint.amazonaws.com` in die Felder Single Sign On URL und Audience URI (SP Entity ID) eingeben, wodurch Sie die Metadaten generieren können. Sobald die Domain aktiv ist, können Sie dann die richtigen Werte von OpenSearch Service abrufen und in Okta aktualisieren. Anweisungen finden Sie unter the section called “Schritt 6: Ihre IdP-URLs aktualisieren”.

Wenn Sie eine bestehende Domain bearbeiten

Wenn Sie die SAML-Authentifizierung für eine bestehende Domain aktivieren, kopieren Sie die Entitäts-ID des Serviceanbieters und eine der SSO-URLs. Hinweise zu der zu verwendenden URL finden Sie unter the section called “SAML-Konfigurationsübersicht”.



Verwenden Sie die Werte, um Ihren Identitätsanbieter zu konfigurieren. Dies ist der komplexeste Teil des Prozesses, und leider variieren Terminologie und Schritte je nach Anbieter stark. Schlagen Sie in der Dokumentation Ihres Anbieters nach.

In Okta erstellen Sie beispielsweise eine SAML 2.0-Webanwendung. Geben Sie für Single Sign-On-On-URL die SSO-URL an. Geben Sie für Zielgruppen-URI (SP-Entitäts-ID) die SP-Entitäts-ID an.

Anstelle von Benutzern und Backend-Rollen hat Okta Benutzer und Gruppen. Für Group Attribute Statements (Anweisungen zu Gruppenattributen) empfehlen wir, `role` zum Feld Name und den regulären Ausdruck `.+` zum Feld Filter hinzuzufügen. Diese Anweisung weist den Okta-Identitätsanbieter an, alle Benutzergruppen unter das `role`-Feld der SAML-Assertion aufzunehmen, nachdem sich ein Benutzer authentifiziert hat.

In IAM Identity Center geben Sie die SP-Entitäts-ID als SAML-Anwendungszielgruppe an. Sie müssen außerdem die folgenden Attributzuordnungen angeben: und. `Subject=${user:subject}:format=unspecified` `Role=${user:groups}:format=uri`

In Auth0 erstellen Sie eine reguläre Webanwendung und aktivieren das SAML 2.0-Add-on. In Keycloak erstellen Sie einen Client.

Schritt 3: IdP-Metadaten importen

Nachdem Sie Ihren Identitätsanbieter konfiguriert haben, wird eine IdP-Metadatendatei generiert. Diese XML-Datei enthält Informationen zum Anbieter, z. B. ein TLS-Zertifikat, Single Sign-On-Endpunkte und die Entitäts-ID des Identitätsanbieters.

Kopieren Sie den Inhalt der IdP-Metadatendatei und fügen Sie ihn in das Feld Metadaten von IdP in der OpenSearch Servicekonsole ein. Wählen Sie alternativ Aus XML-Datei importieren und laden Sie die Datei hoch. Die Metadatendatei sollte ungefähr so aussehen:

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor entityID="entity-id"
 xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
  <md:IDPSSODescriptor WantAuthnRequestsSigned="false"
 protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>tls-certificate</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</
md:NameIDFormat>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</
md:NameIDFormat>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
 Location="idp-sso-url"/>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
Redirect" Location="idp-sso-url"/>
  </md:IDPSSODescriptor>
</md:EntityDescriptor>
```

Schritt 4: SAML-Felder konfigurieren

Nachdem Sie Ihre IdP-Metadaten eingegeben haben, konfigurieren Sie die folgenden zusätzlichen Felder in der OpenSearch Servicekonsole:

- IdP entity ID – Kopieren Sie den Wert der Eigenschaft `entityID` aus Ihrer Metadatendatei und fügen Sie ihn in dieses Feld ein. Viele Identitätsanbieter zeigen diesen Wert auch als Teil einer Zusammenfassung nach der Konfiguration an. Manche Anbieter nennen ihn „Aussteller“.

- SAML-Master-Benutzername und SAML-Master-Backend-Rolle — Der Benutzer und/oder die Backend-Rolle, die Sie angeben, erhalten volle Berechtigungen für den Cluster, was einem neuen Masterbenutzer entspricht, kann diese Berechtigungen jedoch nur innerhalb von Dashboards verwenden. OpenSearch

  In Okta könnten Sie beispielsweise einen Benutzer `jdoe` haben, der zur Gruppe `admins` gehört. Wenn Sie `jdoe` zum Feld für den SAML-Hauptbenutzernamen hinzufügen, erhält nur dieser Benutzer vollständige Berechtigungen. Wenn Sie `admins` zum Feld für die SAML-Haupt-Backend-Rolle hinzufügen, erhält jeder Benutzer, der zu der `admins`-Gruppe gehört, vollständige Berechtigungen.

  > **Note**
  >
  > Der Inhalt der SAML-Assertion muss genau mit den Zeichenfolgen übereinstimmen, die Sie für den SAML-Hauptbenutzernamen und die SAML-Hauptrolle verwenden. Einige Identitätsanbieter fügen vor ihren Benutzernamen ein Präfix hinzu, was zu einer Nichtübereinstimmung führen kann. hard-to-diagnose In der Benutzeroberfläche des Identity Providers wird möglicherweise `jdoe` angezeigt, aber die SAML-Assertion kann `auth0|jdoe` enthalten. Verwenden Sie immer die Zeichenfolge aus der SAML-Assertion.

Bei vielen Identitätsanbietern können Sie während des Konfigurationsprozesses eine Beispiel-Assertion anzeigen, und Tools wie SAML-tracer können Ihnen dabei helfen, den Inhalt echter Assertionen zu untersuchen und Fehler zu beheben. Assertions sehen in etwa wie folgt aus:

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2:Assertion ID="id6722929929925935134334 0162"
 IssueInstant="2020-09-22T22:03:08.633Z" Version="2.0"
  xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
  <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">idp-issuer</
saml2:Issuer>
  <saml2:Subject>
    <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:unspecified">username</saml2:NameID>
    <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
      <saml2:SubjectConfirmationData NotOnOrAfter="2020-09-22T22:08:08.816Z"
 Recipient="domain-endpoint/_dashboards/_opendistro/_security/saml/acs"/>
    </saml2:SubjectConfirmation>
  </saml2:Subject>
```

```
  <saml2:Conditions NotBefore="2020-09-22T21:58:08.816Z"
 NotOnOrAfter="2020-09-22T22:08:08.816Z">
    <saml2:AudienceRestriction>
      <saml2:Audience>domain-endpoint</saml2:Audience>
    </saml2:AudienceRestriction>
  </saml2:Conditions>
  <saml2:AuthnStatement AuthnInstant="2020-09-22T19:54:37.274Z">
    <saml2:AuthnContext>

 <saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport<
saml2:AuthnContextClassRef>
    </saml2:AuthnContext>
  </saml2:AuthnStatement>
  <saml2:AttributeStatement>
    <saml2:Attribute Name="role" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:unspecified">
      <saml2:AttributeValue
        xmlns:xs="http://www.w3.org/2001/XMLSchema"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:type="xs:string">GroupName Match Matches regex ".+" (case-sensitive)
      </saml2:AttributeValue>
    </saml2:Attribute>
  </saml2:AttributeStatement>
</saml2:Assertion>
```

Schritt 5: (Optional) Zusätzliche Einstellungen konfigurieren

Konfigurieren Sie unter Additional settings (Zusätzliche Einstellungen) die folgenden optionalen Felder:

- Subject key (Betreffsschlüssel) – Sie können dieses Feld leer lassen, um das Element `NameID` der SAML-Assertion für den Benutzernamen zu verwenden. Wenn Ihre Assertion dieses Standardelement nicht verwendet und stattdessen den Benutzernamen als benutzerdefiniertes Attribut enthält, geben Sie dieses Attribut hier an.
- Roles key (Rollenschlüssel) – Wenn Sie Backend-Rollen verwenden möchten (empfohlen), geben Sie in diesem Feld ein Attribut aus der Assertion an, z. B. `role` oder `group`. Dies ist eine weitere Situation, in der Tools wie SAML-tracer helfen können.
- Gültigkeitsdauer der Sitzung — Standardmäßig meldet OpenSearch Dashboards Benutzer nach 24 Stunden ab. Sie können diesen Wert auf eine beliebige Zahl zwischen 60 und 1.440 (24 Stunden) einstellen, indem Sie einen neuen Wert angeben.

Wenn Sie mit Ihrer Konfiguration zufrieden sind, speichern Sie die Domain.

Schritt 6: Ihre IdP-URLs aktualisieren

Wenn Sie die SAML-Authentifizierung beim Erstellen einer Domain aktiviert haben, mussten Sie temporäre URLs in Ihrem IdP angeben, um die XML-Metadatendatei zu generieren. Nachdem sich der Domainstatus zu `Active` geändert hat, können Sie die richtigen URLs abrufen und Ihren IdP ändern.

Um die URLs abzurufen, wählen Sie die Domain aus und dann Actions (Aktionen) und Edit security configuration (Sicherheitskonfiguration bearbeiten). Unter SAML-Authentifizierung für OpenSearch Dashboards/Kibana finden Sie die richtige Entitäts-ID und die richtigen SSO-URLs des Dienstanbieters. Kopieren Sie die Werte und verwenden Sie sie, um Ihren Identitätsanbieter zu konfigurieren. Ersetzen Sie dabei die temporären URLs, die Sie in Schritt 2 angegeben haben.

Schritt 7: SAML-Benutzer Rollen zuordnen

Sobald Ihr Domainstatus Aktiv ist und Ihr IdP korrekt konfiguriert ist, navigieren Sie zu OpenSearch Dashboards.

- Wenn Sie die vom SP initiierte URL gewählt haben, navigieren Sie zu *`domain-endpoint`*`/_dashboards`. Um sich direkt bei einem bestimmten Mandanten anzumelden, können Sie `?security_tenant=`*`tenant-name`* an die URL anhängen.
- Wenn Sie die vom IdP initiierte URL ausgewählt haben, navigieren Sie zum Anwendungsverzeichnis Ihres Identitätsanbieters.

Melden Sie sich in beiden Fällen entweder als SAML-Haupt-Benutzer oder als Benutzer an, der zur SAML-Haupt-Backend-Rolle gehört. Um das Beispiel ab Schritt 7 fortzusetzen, melden Sie sich entweder als `jdoe` oder als Mitglied der Gruppe `admins` an.

Wählen Sie nach dem Laden der OpenSearch Dashboards Sicherheit, Rollen aus. Ordnen Sie dann Rollen zu, um anderen Benutzern den Zugriff auf OpenSearch Dashboards zu ermöglichen.

Sie können beispielsweise Ihren vertrauenswürdigen Kollegen `jroe` den Rollen `all_access` und `security_manager` zuordnen. Sie können die Backend-Rolle `analysts` auch den Rollen `readall` und `opensearch_dashboards_user` zuordnen.

Wenn Sie lieber die API als OpenSearch Dashboards verwenden möchten, sehen Sie sich die folgende Beispielanfrage an:

```
PATCH _plugins/_security/api/rolesmapping
[
  {
    "op": "add", "path": "/security_manager", "value": { "users": ["master-user",
 "jdoe", "jroe"], "backend_roles": ["admins"] }
  },
  {
    "op": "add", "path": "/all_access", "value": { "users": ["master-user", "jdoe",
 "jroe"], "backend_roles": ["admins"] }
  },
  {
    "op": "add", "path": "/readall", "value": { "backend_roles": ["analysts"] }
  },
  {
    "op": "add", "path": "/opensearch_dashboards_user", "value": { "backend_roles":
 ["analysts"] }
  }
]
```

Konfigurieren der SP- und der IDP-initiierten Authentifizierung

Wenn Sie sowohl SP- als auch IdP-initiierte Authentifizierung konfigurieren möchten, müssen Sie dies über Ihren Identitätsanbieter tun. In Okta können Sie beispielsweise die folgenden Schritte ausführen:

1. Gehen Sie in Ihrer SAML-Anwendung zu General (Allgemeines), SAML settings (SAML-Einstellungen).
2. Geben Sie für die Single sign on URL (Single-Sign-On-URL) Ihre IdP-initiierte SSO-URL an. z. B. `https://search-domain-hash/_dashboards/_opendistro/_security/saml/acs/idpinitiated`.
3. Aktivieren Sie Allow this app to request other SSO URLs (Dieser App erlauben, andere SSO-URLs anzufordern).
4. Fügen Sie unter Requestable SSO URLs (Anforderbare SSO-URLs) eine oder mehrere SP-initiierte SSO-URLs hinzu. z. B. `https://search-domain-hash/_dashboards/_opendistro/_security/saml/acs`.

Konfigurieren der SAML-Authentifizierung (AWS CLI)

Der folgende AWS CLI Befehl aktiviert die SAML-Authentifizierung für OpenSearch Dashboards in einer vorhandenen Domain:

```
aws opensearch update-domain-config \
  --domain-name my-domain \
  --advanced-security-options '{"SAMLOptions":{"Enabled":true,"MasterUserName":"my-idp-user","MasterBackendRole":"my-idp-group-or-role","Idp":{"EntityId":"entity-id","MetadataContent":"metadata-content-with-quotes-escaped"},"RolesKey":"optional-roles-key","SessionTimeoutMinutes":180,"SubjectKey":"optional-subject-key"}}'
```

Sie müssen alle Anführungszeichen und Zeilenumbrüche in der Metadaten-XML maskieren. Verwenden Sie z. B.<KeyDescriptor use=\"signing\">\n anstelle von <KeyDescriptor use="signing"> und einen Zeilenumbruch. Ausführliche Informationen zur Verwendung von finden Sie in der AWS CLIAWS CLI Befehlsreferenz.

Konfigurieren der SAML-Authentifizierung (Konfigurations-API)

Die folgende Anfrage an die Konfigurations-API aktiviert die SAML-Authentifizierung für OpenSearch Dashboards in einer vorhandenen Domain:

```
POST https://es.us-east-1.amazonaws.com/2021-01-01/opensearch/domain/my-domain/config
{
  "AdvancedSecurityOptions": {
    "SAMLOptions": {
      "Enabled": true,
      "MasterUserName": "my-idp-user",
      "MasterBackendRole": "my-idp-group-or-role",
      "Idp": {
        "EntityId": "entity-id",
        "MetadataContent": "metadata-content-with-quotes-escaped"
      },
      "RolesKey": "optional-roles-key",
      "SessionTimeoutMinutes": 180,
      "SubjectKey": "optional-subject-key"
    }
  }
}
```

Sie müssen alle Anführungszeichen und Zeilenumbrüche in der Metadaten-XML maskieren. Verwenden Sie z. B.<KeyDescriptor use=\"signing\">\n anstelle von <KeyDescriptor use="signing"> und einen Zeilenumbruch. Ausführliche Informationen zur Verwendung der Konfigurations-API finden Sie in der OpenSearch Service-API-Referenz.

SAML-Fehlerbehebung

Fehler	Details
Ihre Anfrage: '*/some/path* ' ist nicht erlaubt.	Vergewissern Sie sich, dass Sie Ihrem Identität sanbieter die richtige SSO-URL (Schritt 3) bereitges tellt haben.
Geben Sie ein gültiges Metadaten dokument des Identitätsanbieters an, um SAML zu aktivieren.	Ihre IdP-Metadatendatei entspricht nicht dem SAML 2.0-Standard. Überprüfen Sie mit einem Validieru ngstool auf Fehler.
SAML-Konfigurationsoptionen sind in der Konsole nicht sichtbar.	Aktualisieren Sie auf die neueste Servicesoftware.
SAML-Konfigurationsfehler: Beim Abrufen der SAML-Konfiguration ist ein Fehler aufgetreten. Bitte überprüfen Sie Ihre Einstellungen.	Dieser allgemeine Fehler kann aus vielen Gründen auftreten. • Überprüfen Sie, ob Sie Ihrem Identitätsanbieter die richtige SP-Entitäts-ID und SSO-URL bereitgestellt haben. • Generieren Sie die IdP-Metadatendatei neu und überprüfen Sie die IdP-Entitäts-ID. Fügen Sie alle aktualisierten Metadaten in der AWS Konsole hinzu. • Vergewissern Sie sich, dass Ihre Domain-Zugriffsric htlinie den Zugriff auf OpenSearch Dashboard s und `_plugins/_security/*` ermöglicht. Generell empfehlen wir eine offene Zugriffsrichtlinie für Domains, die eine differenzierte Zugriffskontrolle verwenden. • Schritte zum Konfigurieren von SAML finden Sie in der Dokumentation Ihres Identitätsanbieters.
Fehlende Rolle: Für diesen Benutzer sind keine Rollen verfügbar, bitte wenden Sie sich an Ihren Systemadm inistrator.	Sie haben sich erfolgreich authentifiziert, aber der Benutzername und alle Backend-Rollen aus der SAML-Assertion sind keinen Rollen zugeordnet und haben daher keine Berechtigungen. Bei diesen

Fehler	Details
	Mappings muss die Groß-/Kleinschreibung beachtet werden. Ihr Systemadministrator kann den Inhalt Ihrer SAML-Assertion mit einem Tool wie SAML-Tracer überprüfen und anschließend Ihre Rollenzuweisung anhand der folgenden Anfrage überprüfen: `GET _plugins/_security/api/rolesmapping`
Ihr Browser leitet kontinuierlich um oder empfängt HTTP 500-Fehler, wenn er versucht, auf Dashboards zuzugreifen. OpenSearch	Diese Fehler können auftreten, wenn Ihre SAML-Assertion eine große Anzahl von Rollen mit insgesamt etwa 1.500 Zeichen enthält. Wenn Sie beispielsweise 80 Rollen übergeben, deren durchschnittliche Länge 20 Zeichen beträgt, überschreiten Sie möglicherweise die Größenbeschränkung für Cookies in Ihrem Webbrowser. Ab OpenSearch Version 2.7 unterstützt die SAML-Assertion Rollen mit bis zu 5000 Zeichen.
Sie können sich nicht von ADFS abmelden.	ADFS erfordert, dass alle Abmeldeanfragen signiert sind, was der OpenSearch Service nicht unterstützt. `<SingleLogoutService />` Aus der IdP-Metadatendatei entfernen, um OpenSearch Service zu zwingen, seinen eigenen internen Abmeldemechanismus zu verwenden.
`Could not find entity descriptor for __PATH__.`	Die Entitäts-ID des IdP, die in der Metadaten-XML to OpenSearch Service bereitgestellt wird, unterscheidet sich von der in der SAML-Antwort. Um dieses Problem zu beheben, stellen Sie sicher, dass sie übereinstimmen. Aktivieren Sie die CW-Anwendungsfehlerprotokolle auf Ihrer Domain, um die Fehlermeldung zum Debuggen des SAML-Integrationsproblems zu finden.

Fehler	Details
`Signature validation failed. SAML response rejected.`	OpenSearch Der Dienst kann die Signatur in der SAML-Antwort mithilfe des in Metadaten-XML bereitgestellten Zertifikats des IdP nicht überprüfen. Dies könnte entweder ein manueller Fehler sein oder Ihr IdP hat sein Zertifikat rotiert. Aktualisieren Sie das neueste Zertifikat von Ihrem IdP in der Metadaten-XML, die dem OpenSearch Service über die AWS Management Console zur Verfügung gestellt wird.
`__PATH__ is not a valid audience for this response.`	Das Zielgruppenfeld in der SAML-Antwort entsprich t nicht dem Domain-Endpunkt. Um diesen Fehler zu beheben, aktualisieren Sie das SP-Zielgruppenfeld so, dass es Ihrem Domain-Endpunkt entspricht. Wenn Sie benutzerdefinierte Endpunkte aktiviert haben, sollte das Zielgruppenfeld Ihrem benutzerd efinierten Endpunkt entsprechen. Aktivieren Sie CW-Anwendungsfehlerprotokolle auf Ihrer Domain, um die Fehlermeldung zum Debuggen des SAML-Inte grationsproblems zu finden.
Ihr Browser erhält in der Antwort einen HTTP 400-Fehler mit`Invalid Request Id`.	Dieser Fehler tritt im Allgemeinen auf, wenn Sie die vom IDP initiierte URL mit dem Format konfiguriert haben. *<DashboardsURL>* `/_opendistro/_security/saml/acs` Konfigurieren Sie die URL stattdessen mit dem Format. *<DashboardsURL>* `/_opendistro/_security/saml/acs/idpinitiated`

Fehler	Details
Die Antwort wurde am __PATH__ statt am empfangen__PATH__.	Das Zielfeld in der SAML-Antwort entspricht keinem der folgenden URL-Formate: • `<DashboardsURL> /_opendistro/_security/saml/acs` • `<DashboardsURL> /_opendistro/_security/saml/acs/idpinitiated .` Geben Sie je nach verwendetem Anmeldeablauf (SP-initiiert oder IDP-initiiert) ein Zielfeld ein, das mit einer der URLs übereinstimmt. OpenSearch
Die Antwort hat ein `InResponseTo` Attribut, obwohl keines erwartet wurde. `InResponseTo`	Sie verwenden die vom IdP initiierte URL für einen SP-initiierten Anmeldeablauf. Verwenden Sie stattdessen die vom SP initiierte URL.

Deaktivieren der SAML-Authentifizierung

Um die SAML-Authentifizierung für OpenSearch Dashboards zu deaktivieren (Konsole)

1. Klicken Sie auf die Domain, wählen Sie Aktionen und Sicherheitskonfiguration bearbeiten.
2. Deaktivieren Sie das Kontrollkästchen SAML-Authentifizierung aktivieren.
3. Wählen Sie Änderungen speichern aus.
4. Nachdem die Verarbeitung der Domain abgeschlossen ist, überprüfen Sie das differenzierte Mapping der Zugriffssteuerungsrollen mit der folgenden Anfrage:

   ```
   GET _plugins/_security/api/rolesmapping
   ```

   Durch das Deaktivieren der SAML-Authentifizierung für Dashboards werden die Zuordnungen für den SAML-Haupt-Benutzernamen und/oder die SAML-Haupt-Backend-Rolle nicht entfernt. Wenn Sie diese Zuordnungen entfernen möchten, melden Sie sich mit der internen Benutzerdatenbank (sofern aktiviert) bei Dashboards an oder verwenden Sie die API, um sie zu entfernen:

   ```
   PUT _plugins/_security/api/rolesmapping/all_access
   ```

```
{
  "users": [
    "master-user"
  ]
}
```

Konfiguration der Amazon Cognito Cognito-Authentifizierung für Dashboards OpenSearch

Sie können Ihre Amazon OpenSearch Service-Standardinstallation von OpenSearch Dashboards mit Amazon Cognito authentifizieren und schützen. Die Amazon Cognito Cognito-Authentifizierung ist optional und nur für Domains OpenSearch verfügbar, die Elasticsearch 5.1 oder höher verwenden. Wenn Sie die Amazon-Cognito-Authentifizierung nicht konfigurieren, können Sie Dashboards dennoch mit einer IP-basierten Zugriffsrichtlinie und einem Proxy-Server, HTTP-Basisauthentifizierung oder SAML schützen.

Ein Großteil des Authentifizierungsprozesses findet in Amazon Cognito statt, aber dieser Abschnitt enthält Richtlinien und Anforderungen für die Konfiguration von Amazon Cognito Cognito-Ressourcen für die Verwendung mit OpenSearch Service-Domains. Die Standardpreise gelten für alle Amazon-Cognito-Ressourcen.

> **Tip**
>
> Wenn Sie eine Domain zum ersten Mal für die Verwendung der Amazon Cognito Cognito-Authentifizierung für OpenSearch Dashboards konfigurieren, empfehlen wir die Verwendung der Konsole. Amazon-Cognito-Ressourcen sind extrem anpassbar und mithilfe der Konsole können Sie die für Sie wichtigen Funktionen besser identifizieren und verstehen.

Themen

- (Optional) Anpassen der Anmeldeseite
- (Optional) Konfiguration der erweiterten Sicherheit
- Testen
- Kontingente
- Häufige Konfigurationsprobleme
- Amazon Cognito Cognito-Authentifizierung für Dashboards deaktivieren OpenSearch
- Löschen von Domains, die die Amazon Cognito Cognito-Authentifizierung für OpenSearch Dashboards verwenden

Voraussetzungen

Bevor Sie die Amazon Cognito Cognito-Authentifizierung für OpenSearch Dashboards konfigurieren können, müssen Sie mehrere Voraussetzungen erfüllen. Die OpenSearch Servicekonsole hilft dabei, die Erstellung dieser Ressourcen zu optimieren, aber das Verständnis des Zwecks der einzelnen Ressourcen hilft bei der Konfiguration und Fehlerbehebung. Für die Amazon-Cognito-Authentifizierung für Dashboards sind die folgenden Ressourcen erforderlich:

- Amazon Cognito Benutzerpool
- Amazon Cognito Identitätenpool
- IAM-Rolle, der die `AmazonOpenSearchServiceCognitoAccess`-Richtlinie zugewiesen ist (`CognitoAccessForAmazonOpenSearch`)

> **Note**
>
> Der Benutzer- und der Identitätenpool müssen sich in derselben AWS-Region befinden. Sie können denselben Benutzerpool, Identitätspool und dieselbe IAM-Rolle verwenden, um die Amazon Cognito Cognito-Authentifizierung für Dashboards zu mehreren OpenSearch Service-Domains hinzuzufügen. Weitere Informationen hierzu finden Sie unter the section called “Kontingente”.

Über den Benutzerpool

Benutzerpools haben zwei Hauptfunktionen: das Erstellen und Verwalten von Benutzerverzeichnissen und die Benutzerregistrierung und -anmeldung. Eine Anleitung zum

Erstellen eines Benutzerpools finden Sie unter Erstellen eines Benutzerpools im Amazon-Cognito-Entwicklerhandbuch.

Wenn Sie einen Benutzerpool für die Verwendung mit OpenSearch Service erstellen, sollten Sie Folgendes berücksichtigen:

- Ihr Amazon-Cognito-Benutzerpool muss über einen Domain-Namen verfügen. OpenSearch Der Service verwendet diesen Domainnamen, um Benutzer auf eine Anmeldeseite für den Zugriff auf Dashboards umzuleiten. Anders als für einen Domain-Namen kann für den Benutzerpool eine Standardkonfiguration verwendet werden.
- Sie müssen die für den Pool erforderlichen Standardattribute angeben – Attribute wie Name, Geburtsdatum, E-Mail-Adresse und Telefonnummer. Sie können diese Attribute nach dem Erstellen des Benutzerpools nicht mehr ändern. Wählen Sie daher diejenigen Attribute aus, die für Sie zum Zeitpunkt der Erstellung am relevantesten sind.
- Legen Sie beim Erstellen des Benutzerpools fest, ob Benutzer eigene Konten erstellen können, wie sicher Passwörter für Konten sein müssen und ob Multifaktor-Authentifizierung aktiviert werden soll. Wenn Sie vorhaben, einen externen Identitätsanbieter zu verwenden, sind diese Einstellungen nicht relevant. Theoretisch können Sie den Benutzerpool als Identitätsanbieter aktivieren und einen externen Identitätsanbieter aktivieren. Die meisten Personen ziehen jedoch eine Methode vor.

Benutzerpool-IDs haben die Form: *region*_*ID*. Wenn Sie beabsichtigen, die AWS CLI oder ein AWS SDK zur Konfiguration des OpenSearch Dienstes zu verwenden, notieren Sie sich die ID.

Über den Identitätenpool

Mit Identitäten-Pools können Sie Benutzern nach der Anmeldung temporäre Rollen mit beschränkten Berechtigungen zuweisen. Eine Anleitung zum Erstellen eines Identitätenpools finden Sie unter Identitätenpools im Amazon-Cognito-Entwicklerhandbuch. Beachten Sie Folgendes, wenn Sie einen Identitätspool für die Verwendung mit OpenSearch Service erstellen:

- Wenn Sie die Amazon-Cognito-Konsole verwenden, müssen Sie das Kontrollkästchen Zugriff für nicht authentifizierte Identitäten aktivieren aktivieren, um den Identitätenpool zu erstellen. Nachdem Sie den Identitätspool erstellt und die OpenSearch Service-Domain konfiguriert haben, deaktiviert Amazon Cognito diese Einstellung.
- Sie müssen keine externen Identitätsanbieter zu dem Identitäten-Pool hinzufügen. Wenn Sie OpenSearch Service für die Verwendung der Amazon Cognito Cognito-Authentifizierung

konfigurieren, konfiguriert er den Identitätspool so, dass er den Benutzerpool verwendet, den Sie gerade erstellt haben.

- Nachdem Sie den Identitäten-Pool erstellt haben, müssen Sie unauthentifizierte und authentifizierte IAM-Rollen auswählen. Diese Rollen legen die Zugriffsrichtlinien fest, die Benutzer vor und nach der Anmeldung haben. Wenn Sie die Amazon-Cognito-Konsole verwenden, kann diese die Rollen für Sie erstellen. Nachdem Sie die authentifizierte Rolle erstellt haben, notieren Sie sich deren ARN. Dieser hat die Form `arn:aws:iam::123456789012:role/Cognito_identitypoolnameAuth_Role`.

Identitäten-Pool-IDs haben die Form: *region*`:`*ID*`-`*ID*`-`*ID*`-`*ID*`-`*ID*. Wenn Sie beabsichtigen, die AWS CLI oder ein AWS SDK zur Konfiguration des OpenSearch Dienstes zu verwenden, notieren Sie sich die ID.

Informationen über die CognitoAccessForAmazonOpenSearch-Rolle

OpenSearch Der Service benötigt Berechtigungen, um die Benutzer- und Identitätspools von Amazon Cognito zu konfigurieren und für die Authentifizierung zu verwenden. Zu diesem `AmazonOpenSearchServiceCognitoAccess` Zweck können Sie eine AWS verwaltete Richtlinie verwenden. `AmazonESCognitoAccess`ist eine ältere Richtlinie, die durch die `AmazonOpenSearchServiceCognitoAccess` Umbenennung des Dienstes in Amazon OpenSearch Service ersetzt wurde. Beide Richtlinien bieten die Mindestberechtigungen für Amazon Cognito, die erforderlich sind, um die Cognito-Authentifizierung zu aktivieren. Informationen zum Richtlinien-JSON finden Sie unter IAM-Konsole.

Wenn Sie die Konsole verwenden, um Ihre OpenSearch Service-Domain zu erstellen oder zu konfigurieren, erstellt sie eine IAM-Rolle für Sie und fügt die `AmazonOpenSearchServiceCognitoAccess` Richtlinie (oder die `AmazonESCognitoAccess` Richtlinie, wenn es sich um eine Elasticsearch-Domain handelt) an die Rolle an. Der Standardname der Rolle lautet `CognitoAccessForAmazonOpenSearch`.

`AmazonOpenSearchServiceCognitoAccess`Sowohl die Richtlinien für Rollenberechtigungen `AmazonESCognitoAccess` als auch beide ermöglichen es OpenSearch Service, die folgenden Aktionen für alle Identitäts- und Benutzerpools durchzuführen:

- Aktion: `cognito-idp:DescribeUserPool`
- Aktion: `cognito-idp:CreateUserPoolClient`
- Aktion: `cognito-idp:DeleteUserPoolClient`

- Aktion: `cognito-idp:UpdateUserPoolClient`
- Aktion: `cognito-idp:DescribeUserPoolClient`
- Aktion: `cognito-idp:AdminInitiateAuth`
- Aktion: `cognito-idp:AdminUserGlobalSignOut`
- Aktion: `cognito-idp:ListUserPoolClients`
- Aktion: `cognito-identity:DescribeIdentityPool`
- Aktion: `cognito-identity:SetIdentityPoolRoles`
- Aktion: `cognito-identity:GetIdentityPoolRoles`

Wenn Sie das AWS CLI oder eines der AWS SDKs verwenden, müssen Sie Ihre eigene Rolle erstellen, die Richtlinie anhängen und den ARN für diese Rolle angeben, wenn Sie Ihre OpenSearch Service-Domain konfigurieren. Die Rolle muss über die folgende Vertrauensstellung verfügen:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "opensearchservice.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Anleitungen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service und Anfügen und Trennen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Konfigurieren einer Domain zur Verwendung der Amazon-Cognito-Authentifizierung

Nachdem Sie die Voraussetzungen erfüllt haben, können Sie eine OpenSearch Service-Domain für die Verwendung von Amazon Cognito for Dashboards konfigurieren.

> **Note**
>
> Amazon Cognito ist nicht in allen AWS-Regionen verfügbar. Eine Liste der unterstützten Regionen finden Sie unter AWS-Regionen und Endpunkte. Sie müssen nicht dieselbe Region für Amazon Cognito verwenden, die Sie für OpenSearch Service verwenden.

Konfigurieren der Amazon-Cognito-Authentifizierung (Konsole)

Da sie die CognitoAccessForAmazonOpenSearchRolle für Sie erstellt, bietet die Konsole die einfachste Konfigurationserfahrung. Zusätzlich zu den standardmäßigen OpenSearch Serviceberechtigungen benötigen Sie die folgenden Berechtigungen, um mit der Konsole eine Domain zu erstellen, die die Amazon Cognito Cognito-Authentifizierung für OpenSearch Dashboards verwendet.

```
{
  "Version": "2012-10-17",
  "Statement": [{
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeVpcs",
        "cognito-identity:ListIdentityPools",
        "cognito-idp:ListUserPools",
        "iam:CreateRole",
        "iam:AttachRolePolicy"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetRole",
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::123456789012:role/service-
role/CognitoAccessForAmazonOpenSearch"
    }
  ]
}
```

Anweisungen zum Hinzufügen von Berechtigungen zu einer Identität (Benutzer, Gruppe oder Rolle) finden Sie unter Hinzufügen von IAM-Identitätsberechtigungen (Konsole).

Wenn `CognitoAccessForAmazonOpenSearch` bereits vorhanden ist, benötigen Sie weniger Berechtigungen:

```
{
  "Version": "2012-10-17",
  "Statement": [{
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeVpcs",
        "cognito-identity:ListIdentityPools",
        "cognito-idp:ListUserPools"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetRole",
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::123456789012:role/service-
role/CognitoAccessForAmazonOpenSearch"
    }
  ]
}
```

So konfigurieren Sie die Amazon-Cognito-Authentifizierung für Dashboards (Konsole)

1. Öffnen Sie die Amazon OpenSearch Service-Konsole unter https://console.aws.amazon.com/aos/home/.
2. Wählen Sie unter Domains die Domain aus, die Sie konfigurieren möchten.
3. Klicken Sie auf Aktionen, Sicherheitskonfiguration bearbeiten.
4. Wählen Sie Amazon-Cognito-Authentifizierung aktivieren aus.
5. Wählen Sie für Region das AWS-Region aus, das Ihren Amazon-Cognito-Benutzerpool und Identitätspool enthält.
6. Wählen Sie für Cognito User Pool (Cognito-Benutzerpool) einen Benutzerpool aus oder erstellen Sie einen Benutzerpool. Anleitungen finden Sie unter the section called “Über den Benutzerpool”.

7. Wählen Sie für Cognito Identity Pool (Cognito-Identitäten-Pool) einen Identitäten-Pool aus oder erstellen Sie einen Identitäten-Pool. Anleitungen finden Sie unter the section called “Über den Identitätenpool”.

   > **Note**
   >
   > Über die Links Benutzerpool erstellen und Identitätenpool erstellen werden Sie zur Amazon-Cognito-Konsole geleitet und müssen diese Ressourcen dort manuell erstellen. Der Prozess erfolgt nicht automatisch. Weitere Informationen hierzu finden Sie unter the section called “Voraussetzungen”.

8. Verwenden Sie für IAM-Rollenname den Standardwert `CognitoAccessForAmazonOpenSearch` (empfohlen), oder geben Sie einen neuen Namen ein. Weitere Informationen zum Zweck dieser Rolle finden Sie unter the section called “Informationen über die CognitoAccessForAmazonOpenSearch-Rolle”.
9. Wählen Sie Änderungen speichern aus.

Nachdem Ihre Domain die Verarbeitung abgeschlossen hat, finden Sie unter the section called “Zulassen der authentifizierten Rolle” und the section called “Konfigurieren von Identitätsanbietern” weitere Konfigurationsschritte.

Konfigurieren der Amazon-Cognito-Authentifizierung (AWS CLI)

Verwenden Sie den `--cognito-options` Parameter, um Ihre OpenSearch Service-Domain zu konfigurieren. Die folgende Syntax wird von den `create-domain`- und `update-domain-config`-Befehlen verwendet:

```
--cognito-options Enabled=true,UserPoolId="user-pool-id",IdentityPoolId="identity-pool-id",RoleArn="arn:aws:iam::123456789012:role/CognitoAccessForAmazonOpenSearch"
```

Beispiel

Im folgenden Beispiel wird eine Domain in der Region `us-east-1` erstellt, die Amazon-Cognito-Authentifizierung für Dashboards mit der Rolle `CognitoAccessForAmazonOpenSearch` aktiviert und der Domain Zugriff auf `Cognito_Auth_Role` erlaubt:

```
aws opensearch create-domain --domain-name my-domain --region us-east-1 --access-policies '{ "Version":"2012-10-17", "Statement":[{"Effect":"Allow","Principal":{"AWS":
```

```
 ["arn:aws:iam::123456789012:role/
Cognito_Auth_Role"]},"Action":"es:ESHttp*","Resource":"arn:aws:es:us-
east-1:123456789012:domain/*" }]}' --engine-version "OpenSearch_1.0"
 --cluster-config InstanceType=m4.xlarge.search,InstanceCount=1
 --ebs-options EBSEnabled=true,VolumeSize=10 --cognito-options
 Enabled=true,UserPoolId="us-east-1_123456789",IdentityPoolId="us-
east-1:12345678-1234-1234-1234-123456789012",RoleArn="arn:aws:iam::123456789012:role/
CognitoAccessForAmazonOpenSearch"
```

Nachdem Ihre Domain die Verarbeitung abgeschlossen hat, finden Sie unter the section called “Zulassen der authentifizierten Rolle” und the section called “Konfigurieren von Identitätsanbietern” weitere Konfigurationsschritte.

Konfigurieren der Amazon-Cognito-Authentifizierung (AWS-SDKs)

Die AWS SDKs (außer den Android- und iOS-SDKs) unterstützen alle Operationen, die in der Amazon OpenSearch Service API-Referenz definiert sind, einschließlich des `CognitoOptions` Parameters für die Operationen `CreateDomain` und`UpdateDomainConfig`. Weitere Informationen über die Installation und Verwendung der AWS SDKs finden Sie unter AWS-Software-Entwicklungs-Kits.

Nachdem Ihre Domain die Verarbeitung abgeschlossen hat, finden Sie unter the section called “Zulassen der authentifizierten Rolle” und the section called “Konfigurieren von Identitätsanbietern” weitere Konfigurationsschritte.

Zulassen der authentifizierten Rolle

Standardmäßig verfügt die authentifizierte IAM-Rolle, die Sie gemäß den Richtlinien unter konfiguriert haben, the section called “Über den Identitätenpool” nicht über die erforderlichen Rechte für den Zugriff auf Dashboards. OpenSearch Sie müssen der Rolle zusätzliche Berechtigungen gewähren.

> **Note**
>
> Wenn Sie eine detaillierte Zugriffskontrolle konfiguriert haben und eine offene oder IP-basierte Zugriffsrichtlinie verwenden, können Sie diesen Schritt überspringen.

Sie können diese Berechtigungen in eine identitätsbasierte Richtlinie aufnehmen. Wenn Sie jedoch nicht möchten, dass authentifizierte Benutzer Zugriff auf alle OpenSearch Dienstdomänen haben, ist eine ressourcenbasierte Richtlinie, die an eine einzelne Domäne angehängt ist, der bessere Ansatz.

Geben Sie für `Principal` den ARN der von Cognito authentifizierten Rolle an, die Sie mit den Richtlinien in the section called “Über den Identitätenpool” konfiguriert haben.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "AWS":[
               "arn:aws:iam::123456789012:role/Cognito_identitypoolnameAuth_Role"
            ]
         },
         "Action":[
            "es:ESHttp*"
         ],
         "Resource":"arn:aws:es:region:123456789012:domain/domain-name/*"
      }
   ]
}
```

Anweisungen zum Hinzufügen einer ressourcenbasierten Richtlinie zu einer Dienstdomäne finden Sie unter. OpenSearch the section called “Konfigurieren von Zugriffsrichtlinien”

Konfigurieren von Identitätsanbietern

Wenn Sie eine Domain für die Verwendung der Amazon Cognito Cognito-Authentifizierung für Dashboards konfigurieren, fügt OpenSearch Service dem Benutzerpool einen App-Client hinzu und fügt den Benutzerpool dem Identitätspool als Authentifizierungsanbieter hinzu.

> **Warning**
>
> Der App-Client darf nicht umbenannt oder gelöscht werden.

Je nachdem, wie Sie Ihren Benutzerpool konfiguriert haben, müssen Sie Benutzerkonten entweder manuell erstellen oder Benutzer können eigene Konten erstellen. Wenn Sie mit diesen Einstellungen zufrieden sind, müssen Sie nichts weiter unternehmen. Viele Anwender verwenden jedoch lieber externe Identitätsanbieter.

Um einen SAML 2.0-Identitätsanbieter zu aktivieren, müssen Sie ein SAML-Metadatendokument bereitstellen. Um soziale Identitätsanbieter wie Login with Amazon, Facebook und Google zu aktivieren, müssen Sie über eine App-ID und einen geheimen App-Schlüssel von diesen Anbietern verfügen. Sie können Identitätsanbieter in beliebigen Kombinationen aktivieren.

Der einfachste Weg, Ihren Benutzerpool zu konfigurieren, erfolgt über die Amazon-Cognito-Konsole. Eine Anleitung finden Sie unter Verwenden des Verbunds für einen Benutzerpool und So geben Sie die Einstellungen Ihres Anwendungs-Identitätsanbieters (IdP) für Ihren Benutzerpool an im Amazon-Cognito-Entwicklerhandbuch.

(Optional) Konfigurieren von individuell festgelegtem Zugriff

Ihnen ist wahrscheinlich aufgefallen, dass mit den Standardeinstellungen des Identitätenpools jedem Benutzer, der sich anmeldet, dieselbe IAM-Rolle zugewiesen wird (`Cognito_`*`identitypool`*`Auth_Role`). Hierdurch erhalten alle Benutzer Zugriff auf dieselben AWS-Ressourcen. Wenn Sie die differenzierte Zugriffskontrolle mit Amazon Cognito verwenden möchten – etwa weil Sie wollen, dass die Analysten Ihrer Organisation schreibgeschützt auf mehrere Indizes zugreifen, Entwickler aber Schreibzugriff auf alle Indizes haben sollen – haben Sie zwei Möglichkeiten:

- Erstellen Sie Benutzergruppen, und konfigurieren Sie Ihren Identitätsanbieter so, dass die IAM-Rolle basierend auf dem Authentifizierungstoken des Benutzers ausgewählt wird (empfohlen).
- Konfigurieren Sie Ihren Identitätsanbieter so, dass die IAM-Rolle basierend auf einer oder mehreren Regeln ausgewählt wird.

Ein Walkthrough, das die differenzierte Zugriffskontrolle enthält, finden Sie unter the section called “Tutorial: Detaillierte Zugriffskontrolle mit Cognito-Authentifizierung”.

> **Important**
>
> Genau wie die Standardrolle muss Amazon Cognito Teil der Vertrauensbeziehung jeder zusätzlichen Rolle sein. Weitere Informationen finden Sie unter Erstellen von Rollen für das Rollenmapping im Amazon-Cognito-Entwicklerhandbuch.

Benutzergruppen und Token

Wenn Sie eine Benutzergruppe erstellen, wählen Sie eine IAM-Rolle für die Mitglieder dieser Gruppe aus. Informationen zum Erstellen von Gruppen finden Sie unter Benutzergruppen im Amazon-Cognito-Entwicklerhandbuch.

Nachdem Sie mindestens eine Benutzergruppe erstellt haben, können Sie Ihren Authentifizierungsanbieter so konfigurieren, dass er Benutzern die Rollen ihrer jeweiligen Gruppe anstelle der Standardrolle des Identitäten-Pools zuweist. Wählen Sie Rolle aus Token auswählen aus, und wählen Sie dann entweder Authentifizierte Standardrolle verwenden oder VERWEIGERN, um anzugeben, wie der Identitätenpool Benutzer behandelt, die nicht Teil einer Gruppe sind.

Regeln

Regeln bestehen im Grunde genommen aus einer Reihe von `if`-Anweisungen, die Amazon Cognito der Reihe nach auswertet. Wenn die E-Mail-Adresse eines Benutzers beispielsweise `@corporate` enthält, weist Amazon Cognito dem Benutzer `Role_A` zu. Wenn die E-Mail-Adresse eines Benutzers `@subsidiary` enthält, wird dem Benutzer `Role_B` zugewiesen. Andernfalls wird dem Benutzer die Standardauthentifizierungsrolle zugewiesen.

Weitere Informationen finden Sie unter Zuweisen von Rollen zu Benutzern mit dem rollenbasierten Mapping im Amazon-Cognito-Entwicklerhandbuch.

(Optional) Anpassen der Anmeldeseite

Sie können die Amazon Cognito Cognito-Konsole verwenden, um ein benutzerdefiniertes Logo hochzuladen und CSS-Änderungen an der Anmeldeseite vorzunehmen. Eine Anleitung sowie eine vollständige Liste der CSS-Eigenschaften finden Sie unter So geben Sie App-Einstellungen für die Benutzeroberfläche Ihres Benutzerpools an im Amazon-Cognito-Entwicklerhandbuch.

(Optional) Konfiguration der erweiterten Sicherheit

Amazon-Cognito-Benutzerpools unterstützen erweiterte Sicherheitsfunktionen wie Multi-Faktor-Authentifizierung, Überprüfung auf nicht mehr zuverlässige Anmeldeinformationen und die adaptive Authentifizierung. Weitere Informationen hierzu finden Sie unter Verwalten der Sicherheit im Amazon-Cognito-Entwicklerhandbuch.

Testen

Wenn Sie mit der Konfiguration zufrieden sind, stellen Sie sicher, dass die Benutzererfahrung Ihren Erwartungen entspricht.

Um auf Dashboards zuzugreifen OpenSearch

1. Navigieren Sie im Webbrowser zu `https://opensearch-domain/_dashboards`. Um sich direkt bei einem bestimmten Mandanten anzumelden, hängen Sie `?security_tenant=tenant-name` an die URL an.
2. Melden Sie sich mit Ihren bevorzugten Anmeldeinformationen an.
3. Nachdem die OpenSearch Dashboards geladen wurden, konfigurieren Sie mindestens ein Indexmuster. Dashboards identifiziert anhand dieser Muster, welche Indizes Sie analysieren möchten. Geben Sie * ein, wählen Sie Nächster Schritt aus und klicken Sie auf Create index pattern (Indexmuster erstellen).
4. Klicken Sie auf Ermitteln, um Ihre Daten zu durchsuchen.

Falls ein Schritt in diesem Prozess fehlschlägt, finden Sie unter the section called “Häufige Konfigurationsprobleme” Hilfestellung zur Problembehebung.

Kontingente

In Amazon Cognito sind Soft Limits für viele Ressourcen konfiguriert. Wenn Sie die Dashboard-Authentifizierung für eine große Anzahl von OpenSearch Service-Domains aktivieren möchten, überprüfen Sie die Kontingente in Amazon Cognito und fordern Sie bei Bedarf eine Erhöhung des Limits an.

Jede OpenSearch Service-Domain fügt dem Benutzerpool einen App-Client hinzu, wodurch dem Identitätspool ein Authentifizierungsanbieter hinzugefügt wird. Wenn Sie die OpenSearch Dashboard-Authentifizierung für mehr als 10 Domains aktivieren, stoßen Sie möglicherweise auf das Limit „maximale Amazon Cognito Cognito-Benutzerpoolanbieter pro Identitätspool“. Wenn Sie ein Limit überschreiten, können alle OpenSearch Service-Domains, die Sie für die Verwendung der Amazon Cognito Cognito-Authentifizierung für Dashboards zu konfigurieren versuchen, im Konfigurationsstatus Verarbeitung hängen bleiben.

Häufige Konfigurationsprobleme

Die folgenden Tabellen enthalten häufige Konfigurationsprobleme und deren Lösungen.

Service konfigurieren OpenSearch

Problem	Lösung
`OpenSearch Service can't create the role` (Konsole)	Sie verfügen nicht über die erforderlichen IAM-Berec htigungen. Fügen Sie die unter the section called “Konfigurieren der Amazon-Cognito-Authentifizierung (Konsole)” angegebenen Berechtigungen hinzu.
`User is not authorize d to perform: iam:PassR ole on resource CognitoAc cessForAmazonOpenSearch` (Konsole)	Sie haben keine `iam:PassRole` Berechtigungen für die CognitoAccessForAmazonOpenSearchRolle. Fügen Sie die folgende Richtlinie zu Ihrem Konto hinzu: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "iam:PassRole" ], "Resource": "arn:aws:iam:: 123456789 012:role/service-role/CognitoAccessF orAmazonOpenSearch " } ] }` Alternativ können Sie die Richtlinie `IAMFullAccess` anfügen.
`User is not authorize d to perform: cognito- identity:ListIdenti tyPools on resource`	Sie verfügen nicht über die Leseberechtigung für Amazon Cognito. Fügen Sie die Richtlinie `AmazonCog nitoReadOnly` zu Ihrem Konto hinzu.
`An error occurred (Validati onException) when calling the CreateDomain operation : OpenSearch Service`	OpenSearch Der Dienst ist in der Vertrauensstellung der `CognitoAccessForAmazonOpenSearch` Rolle nicht angegeben. Stellen Sie sicher, dass Ihre Rolle die in the section called “Informationen über die CognitoAc

Problem	Lösung
`must be allowed to use the passed role`	cessForAmazonOpenSearch-Rolle" angegebene Vertrauensstellung verwendet. Konfigurieren Sie alternativ mit der Konsole die Amazon-Cognito-Authentifizierung. In der Konsole wird eine Rolle für Sie erstellt.
`An error occurred (ValidationException) when calling the CreateDomain operation: User is not authorized to perform: cognito-idp: action on resource: user pool`	Die in `--cognito-options` angegebene Rolle verfügt nicht über die Berechtigung für den Zugriff auf Amazon Cognito. Stellen Sie sicher, dass die Rolle über die AWS verwaltete `AmazonOpenSearchServiceCognitoAccess` -Richtlinie verfügt. Konfigurieren Sie alternativ mit der Konsole die Amazon-Cognito-Authentifizierung. In der Konsole wird eine Rolle für Sie erstellt.
`An error occurred (ValidationException) when calling the CreateDomain operation: User pool does not exist`	OpenSearch Der Dienst kann den Benutzerpool nicht finden. Stellen Sie sicher, dass Sie einen Benutzerpool erstellt haben und die korrekte ID verwenden. Die ID können Sie mithilfe der Amazon-Cognito-Konsole oder dem folgenden AWS CLI-Befehl bestimmen: `aws cognito-idp list-user-pools --max-results 60 --region region`
`An error occurred (ValidationException) when calling the CreateDomain operation: IdentityPool not found`	OpenSearch Der Dienst kann den Identitätspool nicht finden. Stellen Sie sicher, dass Sie einen Benutzerpool erstellt haben und die korrekte ID verwenden. Die ID können Sie mithilfe der Amazon-Cognito-Konsole oder dem folgenden AWS CLI-Befehl bestimmen: `aws cognito-identity list-identity-pools --max-results 60 --region region`

Problem	Lösung
`An error occurred (ValidationException) when calling the CreateDomain operation: Domain needs to be specified for user pool`	Der Benutzerpool verfügt nicht über einen Domain-Namen. Sie können diesen über die Amazon-Cognito-Konsole oder mit dem folgenden AWS CLI-Befehl konfigurieren: `aws cognito-idp create-user-pool-domain --domain name --user-pool-id id`

Auf OpenSearch Dashboards zugreifen

Problem	Lösung
Die Anmeldeseite enthält nicht meinen bevorzugten Identitätsanbieter.	Vergewissern Sie sich, dass Sie den Identitätsanbieter für den OpenSearch Service App-Client aktiviert haben, wie unter beschriebenthe section called “Konfigurieren von Identitätsanbietern”.
Die Anmeldeseite sieht nicht so aus, als würde sie zu meiner Organisation gehören.	Siehe the section called “(Optional) Anpassen der Anmeldeseite”.
Meine Anmeldeinformationen funktionieren nicht.	Stellen Sie sicher, dass Sie den Identitätsanbieter wie in the section called “Konfigurieren von Identitätsanbietern” angegeben konfiguriert haben. Wenn Sie den Benutzerpool als Identitätsanbieter verwenden, überprüfen Sie, ob das Konto auf der Amazon Cognito Cognito-Konsole vorhanden ist.
OpenSearch Dashboards werden entweder gar nicht geladen oder funktionieren nicht richtig.	Die von Amazon Cognito authentifizierte Rolle benötigt die Berechtigung `es:ESHttp*` für die Domain (`/*`), um auf Dashboards zugreifen und Dashboards verwenden zu können. Stellen Sie sicher, dass Sie wie in the section called “Zulassen der authentifizierten Rolle” angegeben eine Zugriffsrichtlinie hinzugefügt haben.

Problem	Lösung
Wenn ich mich von einem Tab aus OpenSearch Dashboards abmelde, wird auf den übrigen Tabs eine Meldung angezeigt, dass das Aktualisierungstoken gesperrt wurde.	Wenn Sie sich von einer OpenSearch Dashboards-Sitzung abmelden, während Sie die Amazon Cognito Cognito-Authentifizierung verwenden, führt OpenSearch Service einen AdminUserGlobalSignOutVorgang aus, der Sie von allen aktiven OpenSearch Dashboards-Sitzungen abmeldet.
`Invalid identity pool configuration. Check assigned IAM roles for this pool.`	Amazon Cognito verfügt nicht über Berechtigungen, die IAM-Rolle im Auftrag des authentifizierten Benutzers anzunehmen. Ändern Sie die Vertrauensstellung für die Rolle, so, dass sie folgendes beinhaltet: `{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Principal": { "Federated": "cognito-identity.amazonaws.com" }, "Action": "sts:AssumeRoleWithWebIdentity", "Condition": { "StringEquals": { "cognito-identity.amazonaws.com:aud": " identity-pool-id " }, "ForAnyValue:StringLike": { "cognito-identity.amazonaws.com:amr": "authenticated" } } }] }`

Problem	Lösung
`Token is not from a supported provider of this identity pool.`	Dieser ungewöhnliche Fehler kann auftreten, wenn Sie den App-Client aus dem Benutzerpool entfernen. Versuchen Sie, Dashboards in einer neuen Browsersitzung zu öffnen.

Amazon Cognito Cognito-Authentifizierung für Dashboards deaktivieren OpenSearch

Gehen Sie wie folgt vor, um die Amazon-Cognito-Authentifizierung für Dashboards zu deaktivieren.

So deaktivieren Sie die Amazon-Cognito-Authentifizierung für Dashboards (Konsole)

1. Öffnen Sie die Amazon OpenSearch Service-Konsole unter https://console.aws.amazon.com/aos/home/.
2. Wählen Sie unter Domains die Domain aus, die Sie konfigurieren möchten.
3. Klicken Sie auf Aktionen, Sicherheitskonfiguration bearbeiten.
4. Heben Sie die Auswahl von Amazon-Cognito-Authentifizierung aktivieren auf.
5. Wählen Sie Änderungen speichern aus.

> **Important**
>
> Wenn Sie die Amazon-Cognito-Benutzer- und Identitätenpools nicht mehr brauchen, können Sie diese löschen. Andernfalls fallen weiterhin Gebühren an.

Löschen von Domains, die die Amazon Cognito Cognito-Authentifizierung für OpenSearch Dashboards verwenden

Um zu verhindern, dass Domänen, die Amazon Cognito Cognito-Authentifizierung für Dashboards verwenden, im Konfigurationsstatus Verarbeitung stecken bleiben, löschen Sie OpenSearch Service-Domains, bevor Sie die zugehörigen Amazon Cognito Cognito-Benutzer- und Identitätspools löschen.

Verwenden von serviceverknüpften Rollen für Amazon OpenSearch Service

Amazon OpenSearch Service verwendet AWS Identity and Access Management (IAM) serviceverknüpfte Rollen. Eine serviceverknüpfte Rolle ist eine einzigartige Art von IAM-Rolle, die direkt mit Service verknüpft ist. OpenSearch Dienstbezogene Rollen sind von OpenSearch Service vordefiniert und beinhalten alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

Eine dienstbezogene Rolle erleichtert die Einrichtung von OpenSearch Service, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. OpenSearch Service definiert die Berechtigungen seiner dienstbezogenen Rollen, und sofern nicht anders definiert, kann nur OpenSearch Service seine Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden. Aktualisierungen der servicebezogenen Rollen- und Berechtigungsrichtlinien finden Sie unter Dokumentverlauf für Amazon OpenSearch Service.

Informationen zu anderen Services, die serviceorientierte Rollen unterstützen, finden Sie unter AWS services that work with IAM (-Services, die mit IAM funktionieren). Suchen Sie nach den Services, für die Yes (Ja) in der Spalte Service-linked roles (Serviceorientierte Rollen) angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Themen

Verwenden von serviceverknüpften Rollen zur Erstellung von VPC-Domains

Amazon OpenSearch Service verwendet AWS Identity and Access Management (IAM) serviceverknüpfte Rollen. Eine serviceverknüpfte Rolle ist eine einzigartige Art von IAM-Rolle, die direkt mit Service verknüpft ist. OpenSearch Dienstbezogene Rollen sind von OpenSearch Service vordefiniert und beinhalten alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

OpenSearch Der Service verwendet die angegebene, mit dem Service verknüpfte Rolle AWSServiceRoleForAmazonOpenSearchService, die die Mindestberechtigungen für Amazon EC2 und Elastic Load Balancing bereitstellt, die für die Rolle erforderlich sind, um den VPC-Zugriff für eine Domain zu aktivieren.

Veraltete Elasticsearch-Rolle

Amazon OpenSearch Service verwendet eine serviceverknüpfte Rolle namens`AWSServiceRoleForAmazonOpenSearchService`. Ihre Konten enthalten möglicherweise auch eine Service-verknüpfte Rolle namens `AWSServiceRoleForAmazonElasticsearchService`, die mit den veralteten Amazon-Elasticsearch-Service-API-Endpunkten funktioniert.

Wenn die alte Elasticsearch-Rolle in Ihrem Konto nicht vorhanden ist, erstellt OpenSearch Service automatisch eine neue OpenSearch serviceverknüpfte Rolle, wenn Sie zum ersten Mal eine Domain erstellen. OpenSearch Andernfalls verwendet Ihr Konto weiterhin die Elasticsearch-Rolle. Damit diese automatische Erstellung möglich ist, müssen Sie über Berechtigungen für die Aktion `iam:CreateServiceLinkedRole` verfügen.

Berechtigungen

Die serviceverknüpfte Rolle `AWSServiceRoleForAmazonOpenSearchService` vertraut darauf, dass die folgenden Services die Rolle annehmen:

- `opensearchservice.amazonaws.com`

Die genannte Richtlinie für Rollenberechtigungen `AmazonOpenSearchServiceRolePolicy`ermöglicht es dem OpenSearch Service, die folgenden Aktionen für die angegebenen Ressourcen durchzuführen:

- Aktion: `acm:DescribeCertificate` für `*`
- Aktion: `cloudwatch:PutMetricData` für `*`
- Aktion: `ec2:CreateNetworkInterface` für `*`
- Aktion: `ec2:DeleteNetworkInterface` für `*`
- Aktion: `ec2:DescribeNetworkInterfaces` für `*`
- Aktion: `ec2:ModifyNetworkInterfaceAttribute` für `*`
- Aktion: `ec2:DescribeSecurityGroups` für `*`

- Aktion: `ec2:DescribeSubnets` für *
- Aktion: `ec2:DescribeVpcs` für *
- Aktion: `ec2:CreateTags` auf allen Netzwerkschnittstellen und VPC-Endpunkten
- Aktion: `ec2:DescribeTags` für *
- Aktion: `ec2:CreateVpcEndpoint` auf allen VPCs, Sicherheitsgruppen, Subnetze und Routentabellen sowie auf allen VPC-Endpunkten, wenn die Anfrage das Tag `OpenSearchManaged=true` enthält
- Aktion: `ec2:ModifyVpcEndpoint` auf allen VPCs, Sicherheitsgruppen, Subnetze und Routentabellen sowie auf allen VPC-Endpunkten, wenn die Anfrage das Tag `OpenSearchManaged=true` enthält
- Aktion: `ec2:DeleteVpcEndpoints` auf allen Endpunkten, wenn die Anfrage das Tag `OpenSearchManaged=true` enthält
- Aktion: `ec2:AssignIpv6Addresses` für *
- Aktion: `ec2:UnAssignIpv6Addresses` für *
- Aktion: `elasticloadbalancing:AddListenerCertificates` für *
- Aktion: `elasticloadbalancing:RemoveListenerCertificates` für *

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter Serviceverknüpfte Rollenberechtigung im IAM-Benutzerhandbuch.

Erstellen der serviceverknüpfte -Rolle

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie mit dem eine VPC-fähige Domäne erstellen AWS Management Console, erstellt OpenSearch Service die dienstverknüpfte Rolle für Sie. Damit diese automatische Erstellung möglich ist, müssen Sie über Berechtigungen für die Aktion `iam:CreateServiceLinkedRole` verfügen.

Sie können auch die IAM-Konsole, den IAM-CLI oder die IAM-API verwenden, um eine Service-verknüpfte Rolle manuell zu erstellen. Weitere Informationen finden Sie unter Erstellen einer Service-verknüpften Rolle im IAM-Benutzerhandbuch.

Bearbeiten der serviceverknüpften Rolle

OpenSearch Mit Service können Sie die dienstverknüpfte Rolle nicht bearbeiten. `AWSServiceRoleForAmazonOpenSearchService` Da möglicherweise verschiedene Entitäten

auf die Rolle verweisen, kann der Rollenname nach der Erstellung einer serviceverknüpften Rolle nicht bearbeitet werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen der serviceverknüpften -Rolle

Wenn Sie ein Feature oder einen Dienst, die bzw. der eine serviceverknüpften Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch Ihre serviceverknüpfte Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

Bereinigen der -serviceverknüpften Rolle

Bevor Sie mit IAM eine serviceverknüpfte Rolle löschen können, müssen Sie sich zunächst vergewissern, dass die Rolle über keine aktiven Sitzungen verfügt, und alle Ressourcen entfernen, die von der Rolle verwendet werden.

So überprüfen Sie in der IAM-Konsole, ob die serviceverknüpfte Rolle über eine aktive Sitzung verfügt

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich der IAM Console Roles (Rollen) aus. Wählen Sie dann den Namen (nicht das Kontrollkästchen) der Rolle `AWSServiceRoleForAmazonOpenSearchService` aus.
3. Wählen Sie auf der Seite Summary für die ausgewählte Rolle die Registerkarte Access Advisor.
4. Überprüfen Sie auf der Registerkarte Access Advisor die jüngsten Aktivitäten für die serviceverknüpfte Rolle.

> **Note**
>
> Wenn Sie sich nicht sicher sind, ob OpenSearch Service die `AWSServiceRoleForAmazonOpenSearchService` Rolle verwendet, können Sie versuchen, die Rolle zu löschen. Wenn der Service die Rolle verwendet, schlägt die Löschung fehl und Sie können die Ressourcen anzeigen, in denen die Rolle verwendet wird. Wenn die Rolle verwendet wird, müssen Sie warten, bis die Sitzung beendet wird, bevor Sie die Rolle löschen können, und/oder die Ressourcen löschen, in denen die

Rolle verwendet wird. Die Sitzung für eine serviceverknüpfte Rolle können Sie nicht widerrufen.

Manuelles Löschen einer Service-verknüpften Rolle

Löschen Sie serviceverknüpfte Rollen aus der IAM-Konsole, API oder AWS CLI. Anweisungen finden Sie unter Löschen einer Service-verknüpften Rolle im IAM-Benutzerhandbuch.

Verwenden von dienstverknüpften Rollen zum Erstellen serverloser Sammlungen OpenSearch

OpenSearch Serverless verwendet dienstgebundene AWS Identity and Access Management Rollen (IAM). Eine dienstverknüpfte Rolle ist ein einzigartiger Typ von IAM-Rolle, die direkt mit dem Dienst verknüpft ist. OpenSearch Dienstbezogene Rollen sind von OpenSearch Service vordefiniert und beinhalten alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

OpenSearch Serverless verwendet die mit dem Dienst verknüpfte Rolle mit dem Namen AWSServiceRoleForAmazonOpenSearchServerless, die die Rolle benötigt, um Metriken im Zusammenhang mit Serverless CloudWatch in Ihrem Konto zu veröffentlichen. Die zugeordnete Rollenberechtigungsrichtlinie ist benannt. AWSServiceRoleForAmazonOpenSearchServerless `AmazonOpenSearchServerlessServiceRolePolicy` Weitere Informationen zu der Richtlinie finden Sie AmazonOpenSearchServerlessServiceRolePolicyim Referenzhandbuch für AWS verwaltete Richtlinien.

Dienstbezogene Rollenberechtigungen für Serverless OpenSearch

OpenSearch Serverless verwendet die angegebene dienstverknüpfte Rolle AWSServiceRoleForAmazonOpenSearchServerless, die es OpenSearch Serverless ermöglicht, Dienste in Ihrem Namen aufzurufen AWS .

Die AWSServiceRoleForAmazonOpenSearchServerless dienstgebundene Rolle vertraut darauf, dass die folgenden Dienste die Rolle übernehmen:

- `observability.aoss.amazonaws.com`

Die genannte Rollenberechtigungsrichtlinie `AmazonOpenSearchServerlessServiceRolePolicy` ermöglicht es OpenSearch Serverless, die folgenden Aktionen an den angegebenen Ressourcen durchzuführen:

- Aktion: `cloudwatch:PutMetricData` für alle Ressourcen AWS

> **Note**
>
> Die Richtlinie beinhaltet den Bedingungsschlüssel`{"StringEquals": {"cloudwatch:namespace": "AWS/AOSS"}}`, was bedeutet, dass die dienstbezogene Rolle nur Metrikdaten an den `AWS/AOSS` CloudWatch Namespace senden kann.

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter Serviceverknüpfte Rollenberechtigung im IAM-Benutzerhandbuch.

Die dienstverknüpfte Rolle für Serverless wird erstellt OpenSearch

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie eine OpenSearch serverlose Sammlung in der AWS Management Console, der oder der AWS API erstellen AWS CLI, erstellt OpenSearch Serverless die dienstverknüpfte Rolle für Sie.

> **Note**
>
> Wenn Sie zum ersten Mal eine Sammlung erstellen, muss Ihnen das `iam:CreateServiceLinkedRole` in einer identitätsbasierten Richtlinie zugewiesen werden.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie eine OpenSearch serverlose Sammlung erstellen, erstellt Serverless die OpenSearch dienstverknüpfte Rolle erneut für Sie.

Sie können die IAM-Konsole auch verwenden, um eine serviceverknüpfte Rolle mit dem Amazon OpenSearch Serverless-Anwendungsfall zu erstellen. Erstellen Sie in der API

AWS CLI oder in der AWS API eine serviceverknüpfte Rolle mit dem Servicenamen: `observability.aoss.amazonaws.com`

```
aws iam create-service-linked-role --aws-service-name
 "observability.aoss.amazonaws.com"
```

Weitere Informationen finden Sie unter Erstellen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch. Wenn Sie diese serviceverknüpfte Rolle löschen, können Sie mit demselben Verfahren die Rolle erneut erstellen.

Bearbeiten Sie die dienstverknüpfte Rolle für Serverless OpenSearch

OpenSearch Serverless ermöglicht es Ihnen nicht, die dienstverknüpfte Rolle zu bearbeiten. AWSServiceRoleForAmazonOpenSearchServerless Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach der Erstellung einer serviceverknüpften Rolle nicht bearbeitet werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen der dienstverknüpften Rolle für Serverless OpenSearch

Wenn Sie ein Feature oder einen Service, die bzw. der eine serviceverknüpfte Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Dies verhindert, dass Sie über eine ungenutzte Entität verfügen, die nicht aktiv überwacht oder gewartet wird. Sie müssen jedoch die Ressourcen für Ihre serviceverknüpfte Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

Um die zu löschen AWSServiceRoleForAmazonOpenSearchServerless, müssen Sie zuerst alle OpenSearch Serverless-Sammlungen in Ihrem löschen. AWS-Konto

> **Note**
>
> Wenn OpenSearch Serverless die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

So löschen Sie die serviceverknüpfte Rolle mit IAM

Verwenden Sie die IAM-Konsole, die oder die AWS API AWS CLI, um die AWSServiceRoleForAmazonOpenSearchServerless serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Unterstützte Regionen für OpenSearch serverlose, serviceverknüpfte Rollen

OpenSearch Serverless unterstützt die Verwendung der AWSServiceRoleForAmazonOpenSearchServerless serviceverknüpften Rolle in jeder Region, in der Serverless verfügbar ist. OpenSearch Eine Liste der unterstützten Regionen finden Sie unter Amazon OpenSearch Serverless Endpoints and Quotas in der. Allgemeine AWS-Referenz

Verwenden von serviceverknüpften Rollen zur Erstellung von Ingestion-Pipelines OpenSearch

Amazon OpenSearch Ingestion verwendet serviceverknüpfte AWS Identity and Access Management Rollen (IAM). Eine serviceverknüpfte Rolle ist eine einzigartige Art von IAM-Rolle, die direkt mit Ingestion verknüpft ist. OpenSearch Servicebezogene Rollen sind von OpenSearch Ingestion vordefiniert und beinhalten alle Berechtigungen, die der Dienst benötigt, um andere Dienste in Ihrem Namen aufzurufen. AWS

OpenSearch Bei der Aufnahme wird die angegebene dienstverknüpfte Rolle verwendet, es sei denn AWSServiceRoleForAmazonOpenSearchIngestionService, Sie verwenden eine selbstverwaltete VPC. In diesem Fall wird die benannte dienstverknüpfte Rolle verwendet. AWSServiceRoleForOpensearchIngestionSelfManagedVpce Die beigefügte Richtlinie stellt die Berechtigungen bereit, die für die Rolle erforderlich sind, um eine virtuelle private Cloud (VPC) zwischen Ihrem Konto und OpenSearch Ingestion zu erstellen und CloudWatch Metriken in Ihrem Konto zu veröffentlichen.

Berechtigungen

Die serviceverknüpfte Rolle `AWSServiceRoleForAmazonOpenSearchIngestionService` vertraut darauf, dass die folgenden Services die Rolle annehmen:

- `osis.amazon.com`

Die genannte Richtlinie für Rollenberechtigungen `AmazonOpenSearchIngestionServiceRolePolicy` ermöglicht es OpenSearch Ingestion, die folgenden Aktionen für die angegebenen Ressourcen durchzuführen:

- Aktion: `ec2:DescribeSubnets` für *
- Aktion: `ec2:DescribeSecurityGroups` für *
- Aktion: `ec2:DeleteVpcEndpoints` für *

- Aktion: `ec2:CreateVpcEndpoint` für `*`
- Aktion: `ec2:DescribeVpcEndpoints` für `*`
- Aktion: `ec2:CreateTags` für `arn:aws:ec2:*:*:network-interface/*`
- Aktion: `cloudwatch:PutMetricData` für `cloudwatch:namespace": "AWS/OSIS"`

Die serviceverknüpfte Rolle `AWSServiceRoleForOpensearchIngestionSelfManagedVpce` vertraut darauf, dass die folgenden Services die Rolle annehmen:

- `self-managed-vpce.osis.amazon.com`

Die genannte Rollenberechtigungsrichtlinie `OpenSearchIngestionSelfManagedVpcePolicy` ermöglicht es OpenSearch Ingestion, die folgenden Aktionen an den angegebenen Ressourcen durchzuführen:

- Aktion: `ec2:DescribeSubnets` für `*`
- Aktion: `ec2:DescribeSecurityGroups` für `*`
- Aktion: `ec2:DescribeVpcEndpoints` für `*`
- Aktion: `cloudwatch:PutMetricData` für `cloudwatch:namespace": "AWS/OSIS"`

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter Serviceverknüpfte Rollenberechtigung im IAM-Benutzerhandbuch.

Die dienstbezogene Rolle für Ingestion wird erstellt OpenSearch

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie eine OpenSearch Ingestion-Pipeline in der AWS Management Console, der oder der AWS API erstellen AWS CLI, erstellt OpenSearch Ingestion die dienstbezogene Rolle für Sie.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie eine OpenSearch Ingestion-Pipeline erstellen, erstellt Ingestion erneut die dienstbezogene Rolle OpenSearch für Sie.

Die serviceverknüpfte Rolle für Ingestion bearbeiten OpenSearch

OpenSearch Bei der Aufnahme können Sie die dienstbezogene Rolle nicht bearbeiten. `AWSServiceRoleForAmazonOpenSearchIngestionService` Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen der dienstverknüpften Rolle für Ingestion OpenSearch

Wenn Sie ein Feature oder einen Service, die bzw. der eine serviceverknüpfte Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte Entität, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch die Ressourcen für Ihre serviceverknüpfte Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

Bereinigen einer serviceverknüpften Rolle

Bevor mit IAM eine serviceverknüpfte Rolle löschen können, müssen Sie zunächst alle von der Rolle verwendeten Ressourcen löschen.

> **Note**
>
> Wenn OpenSearch Ingestion die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

Um OpenSearch Ingestion-Ressourcen zu löschen, die von der oder -Rolle verwendet werden **`AWSServiceRoleForAmazonOpenSearchIngestionServiceAWSServiceRoleForOpensearchInge`**

1. Navigieren Sie zur Amazon OpenSearch Service-Konsole und wählen Sie Ingestion.
2. Löschen Sie alle Pipelines. Anweisungen finden Sie unter the section called “Löschen von Pipelines”.

Löschen Sie die mit dem Dienst verknüpfte Rolle für Ingestion OpenSearch

Sie können die OpenSearch Ingestion-Konsole verwenden, um eine dienstverknüpfte Rolle zu löschen.

So löschen Sie eine serviceverknüpfte Rolle (Konsole)

1. Navigieren Sie zur IAM-Konsole.
2. Wählen Sie Rollen und suchen Sie nach der AWSServiceRoleForAmazonOpenSearchIngestionServiceRolle oder. AWSServiceRoleForOpensearchIngestionSelfManagedVpce
3. Wählen Sie die Rolle aus und klicken Sie auf Löschen.

Beispielcode für AmazonOpenSearchBedienung

Dieses Kapitel enthält allgemeinen Beispielcode für die Arbeit mit AmazonOpenSearchService: Signieren von HTTP-Anfragen in einer Vielzahl von Programmiersprachen, Komprimieren von HTTP-Anforderungstexten und Verwenden desAWSSDKs zum Erstellen von Domains.

Themen

Elasticsearch-Client-Kompatibilität

Die neuesten Versionen der Elasticsearch-Clients enthalten möglicherweise Lizenz- oder Versionsprüfungen, die die Kompatibilität künstlich stören. Die folgende Tabelle enthält Empfehlungen dazu, welche Versionen dieser Clients verwendet werden sollten, um eine optimale Kompatibilität mit zu gewährleisten.OpenSearchBedienung.

> **Important**
>
> Diese Client-Versionen sind veraltet und werden nicht mit den neuesten Abhängigkeiten aktualisiert, einschließlich Log4j. Wir empfehlen dringend die Verwendung desOpenSearchVersionen der Clients, wenn möglich.

Client	Empfohlene Version
Java Low-Level-REST-Client	7.13.4
Java High-Level-REST-Clients	7.13.4
Python-Elasticsearch-Client	7.13.4
Ruby-Elasticsearch-Client	7.13.3
Node.js-Elasticsearch-Client	7.13.0

Komprimieren von HTTP-Anfragen in Amazon OpenSearch Service

Sie können HTTP-Anfragen und -Antworten in Amazon OpenSearch Service-Domains mithilfe der GZIP-Komprimierung komprimieren. Die gzip-Komprimierung kann Ihnen dabei helfen, die Größe Ihrer Dokumente zu reduzieren und die Bandbreitennutzung und Latenz zu senken, was zu verbesserten Übertragungsgeschwindigkeiten führt.

Die Gzip-Komprimierung wird für alle Domains unterstützt, auf denen Elasticsearch 6.0 OpenSearch oder höher ausgeführt wird. Einige OpenSearch Clients verfügen über eine integrierte Unterstützung für die Gzip-Komprimierung, und viele Programmiersprachen verfügen über Bibliotheken, die den Prozess vereinfachen.

Aktivieren der gzip-Komprimierung

Nicht zu verwechseln mit ähnlichen OpenSearch Einstellungen, `http_compression.enabled` ist OpenSearch dienstspezifisch und aktiviert oder deaktiviert die GZIP-Komprimierung auf einer Domain. Domains, die auf Elasticsearch OpenSearch 7 laufen. Bei x ist die GZIP-Komprimierung standardmäßig aktiviert, wohingegen bei Domains, auf denen Elasticsearch 6 ausgeführt wird. x hat sie standardmäßig deaktiviert.

Um die gzip-Komprimierung zu aktivieren, senden Sie die folgende Anfrage:

```
PUT _cluster/settings
{
  "persistent" : {
    "http_compression.enabled": true
  }
}
```

Anforderungen an `_cluster/settings` müssen unkomprimiert sein. Daher müssen Sie möglicherweise eine separate Client- oder Standard-HTTP-Anforderung verwenden, um Clustereinstellungen zu aktualisieren.

Senden Sie die folgende Anfrage, um zu bestätigen, dass Sie die GZIP-Komprimierung erfolgreich aktiviert haben:

```
GET _cluster/settings?include_defaults=true
```

Stellen Sie sicher, dass Sie die folgende Einstellung in der Antwort sehen:

```
...
"http_compression": {
  "enabled": "true"
}
...
```

Erforderliche Header

Wenn Sie einen gzip-komprimierten Anforderungstext einschließen, behalten Sie den Standard-`Content-Type: application/json`-Header und fügen Sie den `Content-Encoding: gzip`-Header hinzu. Um eine gzip-komprimierte Antwort zu akzeptieren, fügen Sie den `Accept-Encoding: gzip`-Header auch hinzu. Wenn ein OpenSearch Client die Gzip-Komprimierung unterstützt, schließt er diese Header wahrscheinlich automatisch ein.

Beispiel-Code (Python 3)

Im folgenden Beispiel wird opensearch-py verwendet, um die Komprimierung durchzuführen und die Anforderung zu senden. Dieser Code signiert die Anforderung mit Ihren IAM-Anmeldeinformationen.

```
from opensearchpy import OpenSearch, RequestsHttpConnection
from requests_aws4auth import AWS4Auth
import boto3

host = '' # e.g. my-test-domain.us-east-1.es.amazonaws.com
region = '' # e.g. us-west-1
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)

# Create the client.
search = OpenSearch(
    hosts = [{'host': host, 'port': 443}],
    http_auth = awsauth,
    use_ssl = True,
    verify_certs = True,
    http_compress = True, # enables gzip compression for request bodies
    connection_class = RequestsHttpConnection
)

document = {
```

```
  "title": "Moneyball",
  "director": "Bennett Miller",
  "year": "2011"
}

# Send the request.
print(search.index(index='movies', id='1', body=document, refresh=True))

# print(search.index(index='movies', doc_type='_doc', id='1', body=document,
 refresh=True))
```

Alternativ können Sie die richtigen Header angeben, den Anforderungstext selbst komprimieren und eine Standard-HTTP-Bibliothek wie Anforderungen verwenden. Dieser Code signiert die Anforderung mit grundlegenden HTTP-Anmeldeinformationen, die Ihre Domäne möglicherweise unterstützt, wenn Sie eine differenzierte Zugriffssteuerung verwenden.

```
import requests
import gzip
import json

base_url = '' # The domain with https:// and a trailing slash. For example, https://my-
test-domain.us-east-1.es.amazonaws.com/
auth = ('master-user', 'master-user-password') # For testing only. Don't store
 credentials in code.

headers = {'Accept-Encoding': 'gzip', 'Content-Type': 'application/json',
           'Content-Encoding': 'gzip'}

document = {
  "title": "Moneyball",
  "director": "Bennett Miller",
  "year": "2011"
}

# Compress the document.
compressed_document = gzip.compress(json.dumps(document).encode())

# Send the request.
path = 'movies/_doc?refresh=true'
url = base_url + path
response = requests.post(url, auth=auth, headers=headers, data=compressed_document)
print(response.status_code)
```

```
print(response.text)
```

Mit demAWSSDKs zur Interaktion mit AmazonOpenSearchBedienung

Dieser Abschnitt enthält Beispiele für die Verwendung desAWSSDKs zur Interaktion mit AmazonOpenSearchAPI zur Dienstkonfiguration. Diese Codebeispiele zeigen, wie Sie erstellen, aktualisieren und löschenOpenSearchServicedomänen.

Java

Dieser Abschnitt enthält Beispiele für Versionen 1 und 2 von AWS SDK for Java.

Version 2

In diesem Beispiel wird derOpenSearchClientBuilderKonstruktor aus Version 2 desAWS SDK for Javaum eine zu erstellenOpenSearchDomäne, aktualisiere ihre Konfiguration und lösche sie. Heben Sie die Kommentierung der Aufrufe an `waitForDomainProcessing` auf (und kommentieren Sie den Aufruf an `deleteDomain`), damit die Domäne online gehen und verwendet werden kann.

```
package com.example.samples;

import java.util.concurrent.TimeUnit;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.opensearch.OpenSearchClient;
import software.amazon.awssdk.services.opensearch.model.ClusterConfig;
import software.amazon.awssdk.services.opensearch.model.EBSOptions;
import software.amazon.awssdk.services.opensearch.model.CognitoOptions;
import software.amazon.awssdk.services.opensearch.model.NodeToNodeEncryptionOptions;
import software.amazon.awssdk.services.opensearch.model.CreateDomainRequest;
import software.amazon.awssdk.services.opensearch.model.CreateDomainResponse;
import software.amazon.awssdk.services.opensearch.model.DescribeDomainRequest;
import software.amazon.awssdk.services.opensearch.model.UpdateDomainConfigRequest;
import software.amazon.awssdk.services.opensearch.model.UpdateDomainConfigResponse;
import software.amazon.awssdk.services.opensearch.model.DescribeDomainResponse;
import software.amazon.awssdk.services.opensearch.model.DeleteDomainRequest;
import software.amazon.awssdk.services.opensearch.model.DeleteDomainResponse;
import software.amazon.awssdk.services.opensearch.model.OpenSearchException;
import software.amazon.awssdk.auth.credentials.DefaultCredentialsProvider;
```

```
/**
 * Sample class demonstrating how to use the Amazon Web Services SDK for Java to
 create, update,
 * and delete Amazon OpenSearch Service domains.
 */

public class OpenSearchSample {

    public static void main(String[] args) {

     String domainName = "my-test-domain";

     // Build the client using the default credentials chain.
        // You can use the CLI and run `aws configure` to set access key, secret
        // key, and default region.

        OpenSearchClient client = OpenSearchClient.builder()
          // Unnecessary, but lets you use a region different than your default.
          .region(Region.US_EAST_1)
          // Unnecessary, but if desired, you can use a different provider chain.
          .credentialsProvider(DefaultCredentialsProvider.create())
                    .build();

        // Create a new domain, update its configuration, and delete it.
        createDomain(client, domainName);
        //waitForDomainProcessing(client, domainName);
        updateDomain(client, domainName);
        //waitForDomainProcessing(client, domainName);
        deleteDomain(client, domainName);
    }

    /**
     * Creates an Amazon OpenSearch Service domain with the specified options.
     * Some options require other Amazon Web Services resources, such as an Amazon
 Cognito user pool
     * and identity pool, whereas others require just an instance type or instance
     * count.
     *
     * @param client
     *            The client to use for the requests to Amazon OpenSearch Service
     * @param domainName
     *            The name of the domain you want to create
     */
```

```
    public static void createDomain(OpenSearchClient client, String domainName) {

     // Create the request and set the desired configuration options

        try {

            ClusterConfig clusterConfig = ClusterConfig.builder()
                    .dedicatedMasterEnabled(true)
                    .dedicatedMasterCount(3)
                    // Small, inexpensive instance types for testing. Not
 recommended for production.
                    .dedicatedMasterType("t2.small.search")
                    .instanceType("t2.small.search")
                    .instanceCount(5)
                    .build();

            // Many instance types require EBS storage.
            EBSOptions ebsOptions = EBSOptions.builder()
                    .ebsEnabled(true)
                    .volumeSize(10)
                    .volumeType("gp2")
                    .build();

            NodeToNodeEncryptionOptions encryptionOptions =
 NodeToNodeEncryptionOptions.builder()
                    .enabled(true)
                    .build();

            CreateDomainRequest createRequest = CreateDomainRequest.builder()
                    .domainName(domainName)
                    .engineVersion("OpenSearch_1.0")
                    .clusterConfig(clusterConfig)
                    .ebsOptions(ebsOptions)
                    .nodeToNodeEncryptionOptions(encryptionOptions)
                    // You can uncomment this line and add your account ID, a
 username, and the
                    // domain name to add an access policy.
                    // .accessPolicies("{\"Version\":\"2012-10-17\",
\"Statement\":[{\"Effect\":\"Allow\",\"Principal\":{\"AWS\":
[\"arn:aws:iam::123456789012:user/user-name\"]},\"Action\":[\"es:*\"],\"Resource\":
\"arn:aws:es:region:123456789012:domain/domain-name/*\"}]}")
                    .build();

            // Make the request.
```

```
            System.out.println("Sending domain creation request...");
            CreateDomainResponse createResponse =
client.createDomain(createRequest);
            System.out.println("Domain status:
"+createResponse.domainStatus().toString());
            System.out.println("Domain ID:
"+createResponse.domainStatus().domainId());


        } catch (OpenSearchException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
    }

    /**
     * Updates the configuration of an Amazon OpenSearch Service domain with the
     * specified options. Some options require other Amazon Web Services resources,
such as an
     * Amazon Cognito user pool and identity pool, whereas others require just an
     * instance type or instance count.
     *
     * @param client
     *            The client to use for the requests to Amazon OpenSearch Service
     * @param domainName
     *            The name of the domain to update
     */

    public static void updateDomain(OpenSearchClient client, String domainName) {

     // Updates the domain to use three data instances instead of five.
        // You can uncomment the Cognito line and fill in the strings to enable
Cognito
        // authentication for OpenSearch Dashboards.

        try {

            ClusterConfig clusterConfig = ClusterConfig.builder()
                    .instanceCount(5)
                    .build();

            CognitoOptions cognitoOptions = CognitoOptions.builder()
                    .enabled(true)
                    .userPoolId("user-pool-id")
```

```
                    .identityPoolId("identity-pool-id")
                    .roleArn("role-arn")
                    .build();

            UpdateDomainConfigRequest updateRequest =
UpdateDomainConfigRequest.builder()
                    .domainName(domainName)
                    .clusterConfig(clusterConfig)
                    //.cognitoOptions(cognitoOptions)
                    .build();

            System.out.println("Sending domain update request...");
            UpdateDomainConfigResponse updateResponse =
client.updateDomainConfig(updateRequest);
            System.out.println("Domain config:
"+updateResponse.domainConfig().toString());


        } catch (OpenSearchException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
    }

    /**
     * Deletes an Amazon OpenSearch Service domain. Deleting a domain can take
     * several minutes.
     *
     * @param client
     *             The client to use for the requests to Amazon OpenSearch Service
     * @param domainName
     *             The name of the domain that you want to delete
     */

    public static void deleteDomain(OpenSearchClient client, String domainName) {

        try {

            DeleteDomainRequest deleteRequest = DeleteDomainRequest.builder()
                    .domainName(domainName)
                    .build();

            System.out.println("Sending domain deletion request...");
```

```
            DeleteDomainResponse deleteResponse =
client.deleteDomain(deleteRequest);
            System.out.println("Domain status: "+deleteResponse.toString());


        } catch (OpenSearchException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
    }

    /**
     * Waits for the domain to finish processing changes. New domains typically take
15-30 minutes
     * to initialize, but can take longer depending on the configuration. Most
updates to existing domains
     * take a similar amount of time. This method checks every 15 seconds and
finishes only when
     * the domain's processing status changes to false.
     *
     * @param client
     *            The client to use for the requests to Amazon OpenSearch Service
     * @param domainName
     *            The name of the domain that you want to check
     */

    public static void waitForDomainProcessing(OpenSearchClient client, String
domainName) {
        // Create a new request to check the domain status.
        DescribeDomainRequest describeRequest = DescribeDomainRequest.builder()
                .domainName(domainName)
                .build();

        // Every 15 seconds, check whether the domain is processing.
        DescribeDomainResponse describeResponse =
client.describeDomain(describeRequest);
        while (describeResponse.domainStatus().processing()) {
            try {
                System.out.println("Domain still processing...");
                TimeUnit.SECONDS.sleep(15);
                describeResponse = client.describeDomain(describeRequest);
            } catch (InterruptedException e) {
                e.printStackTrace();
            }
```

```
        }

        // Once we exit that loop, the domain is available
        System.out.println("Amazon OpenSearch Service has finished processing
 changes for your domain.");
        System.out.println("Domain description: "+describeResponse.toString());
    }
}
```

Version 1

In diesem Beispiel wird derAWSElasticsearchClientBuilderKonstruktor aus Version 1 desAWS SDK for Javaum eine veraltete Elasticsearch-Domain zu erstellen, ihre Konfiguration zu aktualisieren und sie zu löschen. Heben Sie die Kommentierung der Aufrufe an `waitForDomainProcessing` auf (und kommentieren Sie den Aufruf an `deleteDomain`), damit die Domäne online gehen und verwendet werden kann.

```
package com.amazonaws.samples;

import java.util.concurrent.TimeUnit;
import com.amazonaws.auth.DefaultAWSCredentialsProviderChain;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.elasticsearch.AWSElasticsearch;
import com.amazonaws.services.elasticsearch.AWSElasticsearchClientBuilder;
import com.amazonaws.services.elasticsearch.model.CreateElasticsearchDomainRequest;
import com.amazonaws.services.elasticsearch.model.CreateElasticsearchDomainResult;
import com.amazonaws.services.elasticsearch.model.DeleteElasticsearchDomainRequest;
import com.amazonaws.services.elasticsearch.model.DeleteElasticsearchDomainResult;
import
 com.amazonaws.services.elasticsearch.model.DescribeElasticsearchDomainRequest;
import com.amazonaws.services.elasticsearch.model.DescribeElasticsearchDomainResult;
import com.amazonaws.services.elasticsearch.model.EBSOptions;
import com.amazonaws.services.elasticsearch.model.ElasticsearchClusterConfig;
import com.amazonaws.services.elasticsearch.model.ResourceNotFoundException;
import
 com.amazonaws.services.elasticsearch.model.UpdateElasticsearchDomainConfigRequest;
import
 com.amazonaws.services.elasticsearch.model.UpdateElasticsearchDomainConfigResult;
import com.amazonaws.services.elasticsearch.model.VolumeType;

/**
 * Sample class demonstrating how to use the Amazon Web Services SDK for Java to
 create, update,
```

```
 * and delete Amazon OpenSearch Service domains.
 */

public class OpenSearchSample {

    public static void main(String[] args) {

        final String domainName = "my-test-domain";

        // Build the client using the default credentials chain.
        // You can use the CLI and run `aws configure` to set access key, secret
        // key, and default region.
        final AWSElasticsearch client = AWSElasticsearchClientBuilder
                .standard()
                // Unnecessary, but lets you use a region different than your
 default.
                .withRegion(Regions.US_WEST_2)
                // Unnecessary, but if desired, you can use a different provider
 chain.
                .withCredentials(new DefaultAWSCredentialsProviderChain())
                .build();

        // Create a new domain, update its configuration, and delete it.
        createDomain(client, domainName);
        // waitForDomainProcessing(client, domainName);
        updateDomain(client, domainName);
        // waitForDomainProcessing(client, domainName);
        deleteDomain(client, domainName);
    }

    /**
     * Creates an Amazon OpenSearch Service domain with the specified options.
     * Some options require other Amazon Web Services resources, such as an Amazon
 Cognito user pool
     * and identity pool, whereas others require just an instance type or instance
     * count.
     *
     * @param client
     *            The client to use for the requests to Amazon OpenSearch Service
     * @param domainName
     *            The name of the domain you want to create
     */
    private static void createDomain(final AWSElasticsearch client, final String
 domainName) {
```

```
        // Create the request and set the desired configuration options
        CreateElasticsearchDomainRequest createRequest = new
 CreateElasticsearchDomainRequest()
                .withDomainName(domainName)
                .withElasticsearchVersion("7.10")
                .withElasticsearchClusterConfig(new ElasticsearchClusterConfig()
                        .withDedicatedMasterEnabled(true)
                        .withDedicatedMasterCount(3)
                        // Small, inexpensive instance types for testing. Not
 recommended for production
                        // domains.
                        .withDedicatedMasterType("t2.small.elasticsearch")
                        .withInstanceType("t2.small.elasticsearch")
                        .withInstanceCount(5))
                // Many instance types require EBS storage.
                .withEBSOptions(new EBSOptions()
                        .withEBSEnabled(true)
                        .withVolumeSize(10)
                        .withVolumeType(VolumeType.Gp2));
                // You can uncomment this line and add your account ID, a username,
 and the
                // domain name to add an access policy.
                // .withAccessPolicies("{\"Version\":\"2012-10-17\",
\"Statement\":[{\"Effect\":\"Allow\",\"Principal\":{\"AWS\":
[\"arn:aws:iam::123456789012:user/user-name\"]},\"Action\":[\"es:*\"],\"Resource\":
\"arn:aws:es:region:123456789012:domain/domain-name/*\"}]}")


        // Make the request.
        System.out.println("Sending domain creation request...");
        CreateElasticsearchDomainResult createResponse =
 client.createElasticsearchDomain(createRequest);
        System.out.println("Domain creation response from Amazon OpenSearch
 Service:");
        System.out.println(createResponse.getDomainStatus().toString());
    }

    /**
     * Updates the configuration of an Amazon OpenSearch Service domain with the
     * specified options. Some options require other Amazon Web Services resources,
 such as an
     * Amazon Cognito user pool and identity pool, whereas others require just an
     * instance type or instance count.
```

```
    *
    * @param client
    *            The client to use for the requests to Amazon OpenSearch Service
    * @param domainName
    *            The name of the domain to update
    */
   private static void updateDomain(final AWSElasticsearch client, final String
domainName) {
       try {
           // Updates the domain to use three data instances instead of five.
           // You can uncomment the Cognito lines and fill in the strings to enable
Cognito
           // authentication for OpenSearch Dashboards.
           final UpdateElasticsearchDomainConfigRequest updateRequest = new
UpdateElasticsearchDomainConfigRequest()
                   .withDomainName(domainName)
                   // .withCognitoOptions(new CognitoOptions()
                           // .withEnabled(true)
                           // .withUserPoolId("user-pool-id")
                           // .withIdentityPoolId("identity-pool-id")
                           // .withRoleArn("role-arn")
                   .withElasticsearchClusterConfig(new ElasticsearchClusterConfig()
                           .withInstanceCount(3));

           System.out.println("Sending domain update request...");
           final UpdateElasticsearchDomainConfigResult updateResponse = client
                   .updateElasticsearchDomainConfig(updateRequest);
           System.out.println("Domain update response from Amazon OpenSearch
Service:");
           System.out.println(updateResponse.toString());
       } catch (ResourceNotFoundException e) {
           System.out.println("Domain not found. Please check the domain name.");
       }
   }

   /**
    * Deletes an Amazon OpenSearch Service domain. Deleting a domain can take
    * several minutes.
    *
    * @param client
    *            The client to use for the requests to Amazon OpenSearch Service
    * @param domainName
    *            The name of the domain that you want to delete
    */
```

```
   private static void deleteDomain(final AWSElasticsearch client, final String
domainName) {
       try {
           final DeleteElasticsearchDomainRequest deleteRequest = new
DeleteElasticsearchDomainRequest()
                   .withDomainName(domainName);

           System.out.println("Sending domain deletion request...");
           final DeleteElasticsearchDomainResult deleteResponse =
client.deleteElasticsearchDomain(deleteRequest);
           System.out.println("Domain deletion response from Amazon OpenSearch
Service:");
           System.out.println(deleteResponse.toString());
       } catch (ResourceNotFoundException e) {
           System.out.println("Domain not found. Please check the domain name.");
       }
   }

   /**
    * Waits for the domain to finish processing changes. New domains typically take
15-30 minutes
    * to initialize, but can take longer depending on the configuration. Most
updates to existing domains
    * take a similar amount of time. This method checks every 15 seconds and
finishes only when
    * the domain's processing status changes to false.
    *
    * @param client
    *            The client to use for the requests to Amazon OpenSearch Service
    * @param domainName
    *            The name of the domain that you want to check
    */
   private static void waitForDomainProcessing(final AWSElasticsearch client, final
String domainName) {
       // Create a new request to check the domain status.
       final DescribeElasticsearchDomainRequest describeRequest = new
DescribeElasticsearchDomainRequest()
               .withDomainName(domainName);

       // Every 15 seconds, check whether the domain is processing.
       DescribeElasticsearchDomainResult describeResponse =
client.describeElasticsearchDomain(describeRequest);
       while (describeResponse.getDomainStatus().isProcessing()) {
           try {
```

```
                System.out.println("Domain still processing...");
                TimeUnit.SECONDS.sleep(15);
                describeResponse =
 client.describeElasticsearchDomain(describeRequest);
            } catch (InterruptedException e) {
                e.printStackTrace();
            }
        }

        // Once we exit that loop, the domain is available
        System.out.println("Amazon OpenSearch Service has finished processing
 changes for your domain.");
        System.out.println("Domain description response from Amazon OpenSearch
 Service:");
        System.out.println(describeResponse.toString());
    }
}
```

Python

In diesem Beispiel wird derOpenSearchServicePython-Client auf niedriger Ebene vonAWS SDK for Python (Boto)um eine Domain zu erstellen, ihre Konfiguration zu aktualisieren und sie zu löschen.

```
import boto3
import botocore
from botocore.config import Config
import time

# Build the client using the default credential configuration.
# You can use the CLI and run 'aws configure' to set access key, secret
# key, and default region.

my_config = Config(
    # Optionally lets you specify a region other than your default.
    region_name='us-west-2'
)

client = boto3.client('opensearch', config=my_config)

domainName = 'my-test-domain'  # The name of the domain
```

```
def createDomain(client, domainName):
    """Creates an Amazon OpenSearch Service domain with the specified options."""
    response = client.create_domain(
        DomainName=domainName,
        EngineVersion='OpenSearch_1.0',
        ClusterConfig={
            'InstanceType': 't2.small.search',
            'InstanceCount': 5,
            'DedicatedMasterEnabled': True,
            'DedicatedMasterType': 't2.small.search',
            'DedicatedMasterCount': 3
        },
        # Many instance types require EBS storage.
        EBSOptions={
            'EBSEnabled': True,
            'VolumeType': 'gp2',
            'VolumeSize': 10
        },
        AccessPolicies="{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect\":\"Allow
\",\"Principal\":{\"AWS\":[\"arn:aws:iam::123456789012:user/user-name\"]},\"Action\":
[\"es:*\"],\"Resource\":\"arn:aws:es:us-west-2:123456789012:domain/my-test-domain/*
\"}]}",
        NodeToNodeEncryptionOptions={
            'Enabled': True
        }
    )
    print("Creating domain...")
    print(response)


def updateDomain(client, domainName):
    """Updates the domain to use three data nodes instead of five."""
    try:
        response = client.update_domain_config(
            DomainName=domainName,
            ClusterConfig={
                'InstanceCount': 3
            }
        )
        print('Sending domain update request...')
        print(response)

    except botocore.exceptions.ClientError as error:
        if error.response['Error']['Code'] == 'ResourceNotFoundException':
```

```
            print('Domain not found. Please check the domain name.')
        else:
            raise error


def deleteDomain(client, domainName):
    """Deletes an OpenSearch Service domain. Deleting a domain can take several
 minutes."""
    try:
        response = client.delete_domain(
            DomainName=domainName
        )
        print('Sending domain deletion request...')
        print(response)

    except botocore.exceptions.ClientError as error:
        if error.response['Error']['Code'] == 'ResourceNotFoundException':
            print('Domain not found. Please check the domain name.')
        else:
            raise error


def waitForDomainProcessing(client, domainName):
    """Waits for the domain to finish processing changes."""
    try:
        response = client.describe_domain(
            DomainName=domainName
        )
        # Every 15 seconds, check whether the domain is processing.
        while response["DomainStatus"]["Processing"] == True:
            print('Domain still processing...')
            time.sleep(15)
            response = client.describe_domain(
                DomainName=domainName)

        # Once we exit the loop, the domain is available.
        print('Amazon OpenSearch Service has finished processing changes for your
 domain.')
        print('Domain description:')
        print(response)

    except botocore.exceptions.ClientError as error:
        if error.response['Error']['Code'] == 'ResourceNotFoundException':
            print('Domain not found. Please check the domain name.')
```

```
        else:
            raise error


def main():
    """Create a new domain, update its configuration, and delete it."""
    createDomain(client, domainName)
    waitForDomainProcessing(client, domainName)
    updateDomain(client, domainName)
    waitForDomainProcessing(client, domainName)
    deleteDomain(client, domainName)
```

Knoten

In diesem Beispiel wird die Version 3 des SDK verwendet fürJavaScriptin Node.jsOpenSearchAuftraggeberum eine Domain zu erstellen, ihre Konfiguration zu aktualisieren und sie zu löschen.

```
var {
    OpenSearchClient,
    CreateDomainCommand,
    DescribeDomainCommand,
    UpdateDomainConfigCommand,
    DeleteDomainCommand
} = require("@aws-sdk/client-opensearch");
var sleep = require('sleep');

var client = new OpenSearchClient();

var domainName = 'my-test-domain'

// Create a new domain, update its configuration, and delete it.
createDomain(client, domainName)
waitForDomainProcessing(client, domainName)
updateDomain(client, domainName)
waitForDomainProcessing(client, domainName)
deleteDomain(client, domainName)

async function createDomain(client, domainName) {
    // Creates an Amazon OpenSearch Service domain with the specified options.
    var command = new CreateDomainCommand({
        DomainName: domainName,
        EngineVersion: 'OpenSearch_1.0',
```

```
        ClusterConfig: {
        'InstanceType': 't2.small.search',
        'InstanceCount': 5,
        'DedicatedMasterEnabled': 'True',
        'DedicatedMasterType': 't2.small.search',
        'DedicatedMasterCount': 3
        },
        EBSOptions:{
            'EBSEnabled': 'True',
            'VolumeType': 'gp2',
            'VolumeSize': 10
        },
        AccessPolicies: "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect\":\"Allow
\",\"Principal\":{\"AWS\":[\"arn:aws:iam::123456789012:user/user-name\"]},\"Action\":
[\"es:*\"],\"Resource\":\"arn:aws:es:us-east-1:123456789012:domain/my-test-domain/*
\"}]}",
         NodeToNodeEncryptionOptions:{
            'Enabled': 'True'
        }
    });
    const response = await client.send(command);
    console.log("Creating domain...");
    console.log(response);
}

async function updateDomain(client, domainName) {
    // Updates the domain to use three data nodes instead of five.
    var command = new UpdateDomainConfigCommand({
        DomainName: domainName,
        ClusterConfig: {
        'InstanceCount': 3
        }
    });
    const response = await client.send(command);
    console.log('Sending domain update request...');
    console.log(response);
}

async function deleteDomain(client, domainName) {
    // Deletes an OpenSearch Service domain. Deleting a domain can take several
 minutes.
    var command = new DeleteDomainCommand({
        DomainName: domainName
    });
```

```
    const response = await client.send(command);
    console.log('Sending domain deletion request...');
    console.log(response);
}

async function waitForDomainProcessing(client, domainName) {
    // Waits for the domain to finish processing changes.
    try {
        var command = new DescribeDomainCommand({
            DomainName: domainName
        });
        var response = await client.send(command);

        while (response.DomainStatus.Processing == true) {
            console.log('Domain still processing...')
            await sleep(15000) // Wait for 15 seconds, then check the status again
            function sleep(ms) {
                return new Promise((resolve) => {
                    setTimeout(resolve, ms);
                });
            }
            var response = await client.send(command);
        }
        // Once we exit the loop, the domain is available.
        console.log('Amazon OpenSearch Service has finished processing changes for your
 domain.');
        console.log('Domain description:');
        console.log(response);

    } catch (error) {
        if (error.name === 'ResourceNotFoundException') {
            console.log('Domain not found. Please check the domain name.');
            }
    };
}
```

Indizierung von Daten in Amazon Service OpenSearch

Da Amazon OpenSearch Service eine REST-API verwendet, gibt es zahlreiche Methoden für die Indizierung von Dokumenten. Sie können Standard-Clients wie curl oder eine beliebige Programmiersprache verwenden, die HTTP-Anforderungen senden können. Um den Prozess der Interaktion damit weiter zu vereinfachen, verfügt OpenSearch Service über Clients für viele Programmiersprachen. Fortgeschrittene Benutzer können direkt fortfahren mit the section called “Laden von Streaming-Daten in den OpenSearch Service”.

Wir empfehlen Ihnen dringend, Amazon OpenSearch Ingestion für die Datenaufnahme zu verwenden. Dabei handelt es sich um einen vollständig verwalteten Datensammler, der in Service integriert ist. OpenSearch Weitere Informationen finden Sie unter Amazon OpenSearch Ingestion.

Eine Einführung in die Indizierung finden Sie in der Dokumentation. OpenSearch

Namensbeschränkungen bei Indizes

OpenSearch Für Dienstindizes gelten die folgenden Einschränkungen bei der Benennung:

- Alle Buchstaben müssen Kleinbuchstaben sein.
- Indexnamen dürfen nicht mit _ oder - beginnen.
- Indexnamen dürfen keine Leerzeichen, Kommas, :, ", *, +, /, \, |, ?, #, > oder < enthalten.

Nehmen Sie keine vertraulichen Informationen in Index-, Typ- oder Dokument-ID-Namen auf. OpenSearch Der Dienst verwendet diese Namen in seinen Uniform Resource Identifiers (URIs). Server und Anwendungen protokollieren oft HTTP-Anforderungen. Dies kann dazu führen, dass unnötigerweise Daten preisgegeben werden, wenn URIs sensible Informationen enthalten.

```
2018-10-03T23:39:43 198.51.100.14 200 "GET https://opensearch-domain/dr-jane-doe/flu-patients-2018/202-555-0100/ HTTP/1.1"
```

Auch wenn Sie keine Berechtigungen zum Anzeigen des zugehörigen JSON-Dokuments haben, könnten Sie von dieser gefälschten Protokollzeile ableiten, dass einer von Dr. Does Patienten mit der Telefonnummer 202–555–0100 im Jahr 2018 die Grippe hatte.

Wenn der OpenSearch Dienst eine echte oder vermeintliche IP-Adresse in einem Indexnamen erkennt (z. B.`my-index-12.34.56.78.91`), maskiert er die IP-Adresse. Ein Anruf bei `_cat/indices` ergibt die folgende Antwort:

```
green open my-index-x.x.x.x.91    soY19tBERoKo71WcEScidw 5 1 0 0   2kb  1kb
```

Um unnötige Verwirrung zu vermeiden, sollten Sie es vermeiden, IP-Adressen in Indexnamen zu verwenden.

Reduzierung der Antwortgröße

Antworten der `_index`- und `_bulk`-APIs enthalten ziemlich viele Informationen. Diese Informationen können bei der Fehlerbehebung von Anfragen oder der Implementierung von Logik für Wiederholversuche nützlich sein. Sie benötigen allerdings beträchtliche Bandbreite. In diesem Beispiel führt die Indizierung eines 32-Byte-Dokuments zu einer 339-Byte-Antwort (einschließlich Kopfzeilen):

```
PUT opensearch-domain/more-movies/_doc/1
{"title": "Back to the Future"}
```

Antwort

```
{
  "_index": "more-movies",
  "_type": "_doc",
  "_id": "1",
  "_version": 4,
  "result": "updated",
  "_shards": {
    "total": 2,
    "successful": 2,
    "failed": 0
  },
  "_seq_no": 3,
  "_primary_term": 1
}
```

Diese Antwortgröße mag minimal erscheinen, aber wenn Sie 1 000 000 Dokumente pro Tag indizieren – ungefähr 11,5 Dokumente pro Sekunde – ergeben 339 Byte pro Antwort 10,17 GB Download-Datenverkehr pro Monat.

Wenn Datenübertragungskosten ein Problem darstellen, verwenden Sie den `filter_path` Parameter, um die Größe der OpenSearch Serviceantwort zu reduzieren. Achten Sie jedoch darauf, dass Sie keine Felder herausfiltern, die Sie benötigen, um fehlgeschlagene Anfragen zu identifizieren oder erneut zu versuchen. Diese Felder variieren je nach Client. Der `filter_path` Parameter funktioniert für alle OpenSearch Service-REST-APIs, ist aber besonders nützlich bei APIs, die Sie häufig aufrufen, wie z. B. die `_bulk` APIs `_index` und:

```
PUT opensearch-domain/more-movies/_doc/1?filter_path=result,_shards.total
{"title": "Back to the Future"}
```

Antwort

```
{
  "result": "updated",
  "_shards": {
    "total": 2
  }
}
```

Anstatt Felder zu integrieren, können Sie Felder mit einem `-`-Präfix ausschließen. `filter_path` unterstützt auch Platzhalter:

```
POST opensearch-domain/_bulk?filter_path=-took,-items.index._*
{ "index": { "_index": "more-movies", "_id": "1" } }
{"title": "Back to the Future"}
{ "index": { "_index": "more-movies", "_id": "2" } }
{"title": "Spirited Away"}
```

Antwort

```
{
  "errors": false,
  "items": [
    {
      "index": {
        "result": "updated",
        "status": 200
      }
    },
    {
      "index": {
```

```
        "result": "updated",
        "status": 200
      }
    }
  ]
}
```

Indexcodecs

Index-Codecs bestimmen, wie die in einem Index gespeicherten Felder komprimiert und auf der Festplatte gespeichert werden. Der Index-Codec wird durch die statische `index.codec` Einstellung gesteuert, die den Komprimierungsalgorithmus angibt. Diese Einstellung wirkt sich auf die Größe des Index-Shards und die Betriebsleistung aus.

Eine Liste der unterstützten Codecs und ihrer Leistungsmerkmale finden Sie in der Dokumentation unter Unterstützte Codecs. OpenSearch

Beachten Sie bei der Auswahl eines Index-Codec Folgendes:

- Um die Probleme zu vermeiden, die mit der Änderung der Codec-Einstellung eines vorhandenen Indexes verbunden sind, sollten Sie zunächst einen repräsentativen Workload in einer Umgebung außerhalb der Produktionsumgebung testen, bevor Sie eine neue Codec-Einstellung verwenden. Weitere Informationen finden Sie unter Ändern eines Index-Codecs.
- Sie können keine Z-Standard-Komprimierungscodecs (`"index.codec": "zstd"`oder`"index.codec": "zstd_no_dict"`) für k-NN- oder Security Analytics-Indizes verwenden.

Laden von Streaming-Daten in Amazon OpenSearch Service

Sie können OpenSearch Ingestion verwenden, um Streaming-Daten direkt in Ihre Amazon-OpenSearch Service-Domain zu laden, ohne Lösungen von Drittanbietern verwenden zu müssen. Um Daten an OpenSearch Ingestion zu senden, konfigurieren Sie Ihre Datenproduzenten und der Service stellt die Daten automatisch an die von Ihnen angegebene Domain oder Sammlung bereit. Informationen zu den ersten Schritten mit OpenSearch Ingestion finden Sie unter the section called “Tutorial: Daten in eine Sammlung aufnehmen”.

Sie können weiterhin andere Quellen verwenden, um Streaming-Daten wie Amazon Data Firehose und Amazon CloudWatch Logs zu laden, die über integrierte Unterstützung für OpenSearch Service

verfügen. Andere, wie z. B. Amazon S3, Amazon Kinesis Data Streams und Amazon DynamoDB, verwenden AWS Lambda -Funktionen als Ereignis-Handler. Die Lambda-Funktionen reagieren auf neue Daten, indem Sie sie verarbeiten und zu Ihrer Domain streamen.

> **Note**
>
> Lambda unterstützt verschiedene gängige Programmiersprachen und ist in den meisten AWS-Regionenverfügbar. Weitere Informationen finden Sie unter Erste Schritte mit Lambda im -AWS Lambda Entwicklerhandbuch und unter -AWS Service-Endpunkte im Allgemeine AWS-Referenz.

Themen

Laden von Streaming-Daten aus OpenSearch der Aufnahme

Sie können Amazon OpenSearch Ingestion verwenden, um Daten in eine - OpenSearch Service-Domain zu laden. Sie konfigurieren Ihre Datenproduzenten so, dass sie Daten an OpenSearch Ingestion senden, und es stellt die Daten automatisch an die von Ihnen angegebene Sammlung bereit. Sie können OpenSearch Ingestion auch so konfigurieren, dass Ihre Daten vor der Bereitstellung transformiert werden. Weitere Informationen finden Sie unter OpenSearch Einnahme durch Amazon.

So laden Sie Streaming-Daten aus Amazon S3

Sie können Lambda verwenden, um Daten von Amazon S3 aus an Ihre OpenSearch Service-Domain zu senden. Neue in einem S3-Bucket eintreffende Daten lösen eine Ereignisbenachrichtigung an Lambda aus, wodurch Ihr benutzerdefinierter Code zum Durchführen der Indizierung ausgeführt wird.

Diese Methode zum Streamen von Daten ist ausgesprochen flexibel. Sie können Objekt-Metadaten indizieren oder einige Elemente des Objekttextes analysieren und indizieren, sofern das Objekt Klartext ist. Dieser Abschnitt enthält unkomplizierten Python-Beispielcode für die Verwendung von regulären Ausdrücken zum Analysieren einer Protokolldatei und Indizieren der Übereinstimmungen.

Voraussetzungen

Zum Fortfahren benötigen Sie die folgenden Ressourcen.

Voraussetzung	Beschreibung
Amazon S3-Bucket	Weitere Informationen finden Sie unter Erstellen Ihres ersten S3 Buckets im Benutzerhandbuch für Amazon Simple Storage Service. Der Bucket muss sich in derselben Region wie Ihre OpenSearch Service-D omain befinden.
OpenSearch Service-D omain	Das Ziel für die Daten, nachdem sie durch Ihre Lambda-Funktion verarbeitet wurden. Weitere Informationen finden Sie unter the section called “ OpenSearch Dienstdomänen erstellen”.

Erstellen des Lambda-Bereitstellungspakets

Bereitstellungspakete sind ZIP- oder JAR-Dateien, die Ihren Code und seine Abhängigkeiten enthalten. Dieser Abschnitt enthält Python-Beispielcode. Informationen zu anderen Programmiersprachen finden Sie unter Lambda-Bereitstellungspakete im AWS Lambda - Entwicklerhandbuch.

1. Erstellen Sie ein Verzeichnis. In diesem Beispiel verwenden wir den Namen `s3-to-opensearch`.
2. Erstellen Sie im Verzeichnis eine Datei mit dem Namen `sample.py`:

```
import boto3
import re
import requests
from requests_aws4auth import AWS4Auth

region = '' # e.g. us-west-1
service = 'es'
credentials = boto3.Session().get_credentials()
```

```
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)

host = '' # the OpenSearch Service domain, e.g. https://search-mydomain.us-
west-1.es.amazonaws.com
index = 'lambda-s3-index'
datatype = '_doc'
url = host + '/' + index + '/' + datatype

headers = { "Content-Type": "application/json" }

s3 = boto3.client('s3')

# Regular expressions used to parse some simple log lines
ip_pattern = re.compile('(\d+\.\d+\.\d+\.\d+)')
time_pattern = re.compile('\[(\d+\/\w\w\w\/\d\d\d\d:\d\d:\d\d:\d\d\s-\d\d\d\d)\]')
message_pattern = re.compile('\"(.+)\"')

# Lambda execution starts here
def handler(event, context):
    for record in event['Records']:

        # Get the bucket name and key for the new file
        bucket = record['s3']['bucket']['name']
        key = record['s3']['object']['key']

        # Get, read, and split the file into lines
        obj = s3.get_object(Bucket=bucket, Key=key)
        body = obj['Body'].read()
        lines = body.splitlines()

        # Match the regular expressions to each line and index the JSON
        for line in lines:
            line = line.decode("utf-8")
            ip = ip_pattern.search(line).group(1)
            timestamp = time_pattern.search(line).group(1)
            message = message_pattern.search(line).group(1)

            document = { "ip": ip, "timestamp": timestamp, "message": message }
            r = requests.post(url, auth=awsauth, json=document, headers=headers)
```

Bearbeiten Sie die Variablen für `region` und `host`.

3. Installieren Sie pip, falls noch nicht geschehen, und installieren Sie dann die Abhängigkeiten in einem neuen `package`-Verzeichnis:

```
cd s3-to-opensearch

pip install --target ./package requests
pip install --target ./package requests_aws4auth
```

   Da in allen Lambda-Ausführungsumgebungen Boto3 installiert ist, müssen Sie es nicht in Ihr Bereitstellungspaket einschließen.

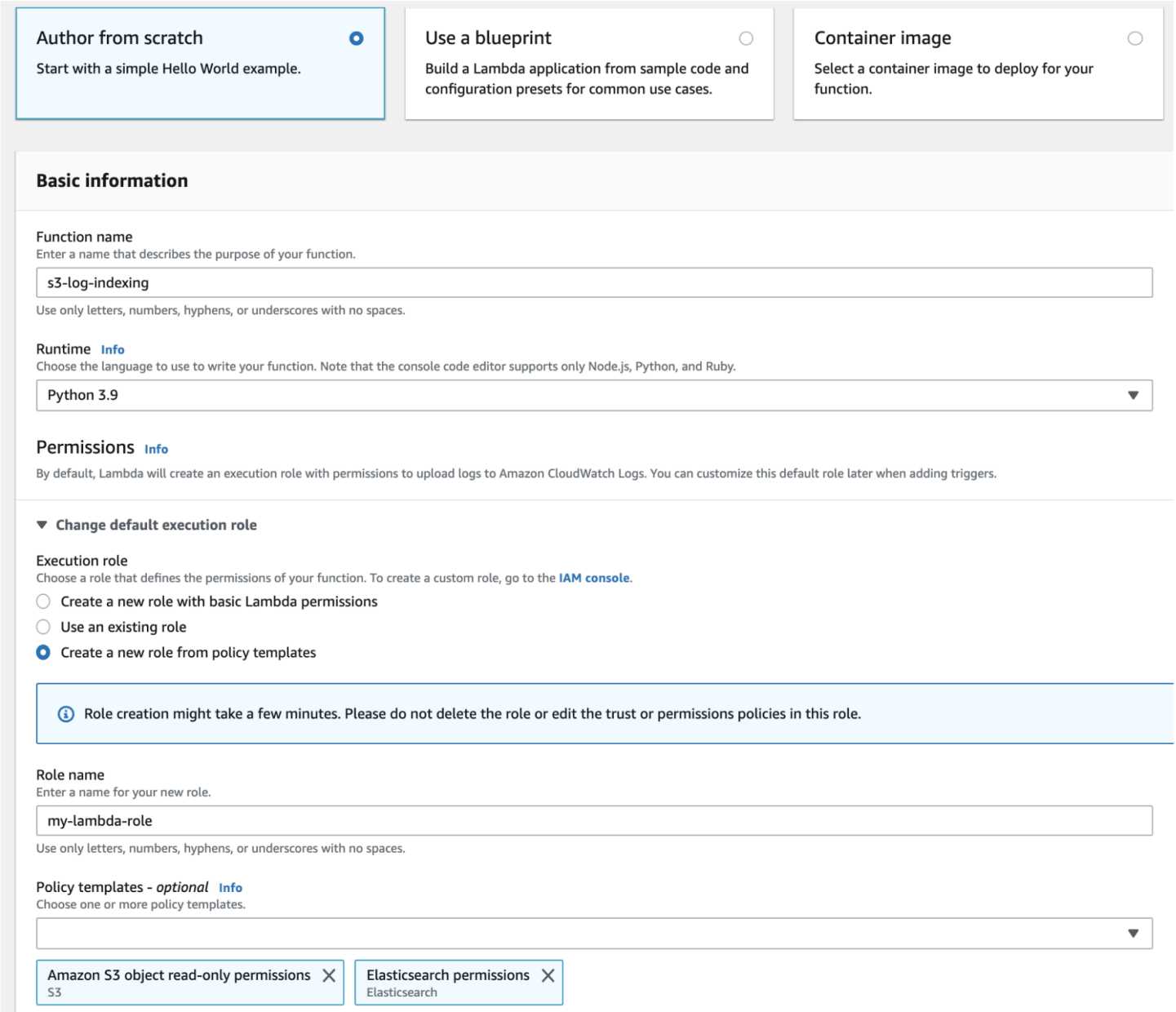
4. Paket mit Anwendungscode und Abhängigkeiten:

```
cd package
zip -r ../lambda.zip .

cd ..
zip -g lambda.zip sample.py
```

So erstellen Sie die Lambda-Funktion:

Nachdem Sie das Bereitstellungspaket erstellt haben, können Sie die Lambda-Funktion erstellen. Wenn Sie eine Funktion erstellen, wählen Sie einen Namen, eine Laufzeit (z. B. Python 3.8) und eine IAM-Rolle aus. Die IAM-Rolle definiert die Berechtigungen der Funktion. Detaillierte Anweisungen finden Sie unter Erstellen einer einfachen Lambda-Funktion im AWS Lambda -Entwicklerhandbuch.

In diesem Beispiel wird davon ausgegangen, dass Sie die Konsole verwenden. Wählen Sie Python 3.9 und eine Rolle mit S3-Leseberechtigungen und OpenSearch Service-Schreibberechtigungen aus, wie im folgenden Screenshot gezeigt:



Nachdem Sie die Funktion erstellt haben, müssen Sie einen Auslöser hinzufügen. In diesem Beispiel soll der Code immer dann ausgeführt werden, wenn im S3-Bucket ein Protokoll eintrifft:

1. Klicken Sie auf Auslöser hinzufügen und wählen Sie S3 aus.
2. Wählen Sie Ihren Bucket aus.
3. Wählen Sie unter Event type (Ereignistyp) die Option PUT aus.
4. Geben Sie für Prefix (Präfix) den Wert `logs/` ein.
5. Geben Sie für Suffix `.log` ein.
6. Bestätigen Sie die Warnung für rekursive Aufrufe und wählen Sie Hinzufügen aus.

Schließlich können Sie Ihr Bereitstellungs-Paket hochladen:

1. Wählen Sie Hochladen von und .zip-Datei und befolgen Sie dann die Anweisungen zum Hochladen Ihres Bereitstellungspakets.
2. Nachdem der Upload abgeschlossen ist, bearbeiten Sie die Laufzeit-Einstellungen und ändern Sie den Handler auf `sample.handler`. Diese Einstellung teilt Lambda die Datei (`sample.py`) und Methode (`handler`) mit, die es nach einem Auslöser ausführen soll.

An diesem Punkt verfügen Sie über einen vollständigen Satz von Ressourcen: einen Bucket für Protokolldateien, eine Funktion, die ausgeführt wird, wenn dem Bucket eine Protokolldatei hinzugefügt wird, Code, der die Analyse und Indizierung durchführt, und eine - OpenSearch Service-Domain für die Suche und Visualisierung.

Testen der Lambda-Funktion

Nachdem Sie die Funktion erstellt haben, können Sie sie durch Hochladen einer Datei in den Amazon-S3-Bucket testen. Erstellen Sie anhand der folgenden Beispielprotokollzeilen eine Datei mit dem Namen `sample.log`:

```
12.345.678.90 - [10/Oct/2000:13:55:36 -0700] "PUT /some-file.jpg"
12.345.678.91 - [10/Oct/2000:14:56:14 -0700] "GET /some-file.jpg"
```

Laden Sie die Datei in den Ordner `logs` Ihres S3-Buckets hoch. Anweisungen finden Sie unter Hochladen eines Objekts in Ihren Bucket im Benutzerhandbuch für Amazon Simple Storage Service.

Verwenden Sie dann die OpenSearch Servicekonsole oder OpenSearch Dashboards, um zu überprüfen, ob der `lambda-s3-index` Index zwei Dokumente enthält. Sie können auch eine Standard-Suchabfrage durchführen:

```
GET https://domain-name/lambda-s3-index/_search?pretty
{
  "hits" : {
    "total" : 2,
    "max_score" : 1.0,
    "hits" : [
      {
        "_index" : "lambda-s3-index",
        "_type" : "_doc",
        "_id" : "vTYXaWIBJWV_TTkEuSDg",
```

```
        "_score" : 1.0,
        "_source" : {
          "ip" : "12.345.678.91",
          "message" : "GET /some-file.jpg",
          "timestamp" : "10/Oct/2000:14:56:14 -0700"
        }
      },
      {
        "_index" : "lambda-s3-index",
        "_type" : "_doc",
        "_id" : "vjYmaWIBJWV_TTkEuCAB",
        "_score" : 1.0,
        "_source" : {
          "ip" : "12.345.678.90",
          "message" : "PUT /some-file.jpg",
          "timestamp" : "10/Oct/2000:13:55:36 -0700"
        }
      }
    ]
  }
}
```

So laden Sie Streaming-Daten aus Amazon Kinesis Data Streams

Sie können Streaming-Daten aus Kinesis Data Streams in den OpenSearch Service laden. Neue im Daten-Stream eintreffende Daten lösen eine Ereignisbenachrichtigung an Lambda aus, wodurch Ihr benutzerdefinierter Code zum Durchführen der Indizierung ausgeführt wird. Dieser Abschnitt enthält unkomplizierten Python-Beispielcode.

Voraussetzungen

Zum Fortfahren benötigen Sie die folgenden Ressourcen.

Voraussetzung	Beschreibung
Amazon Kinesis Data Stream	Die Ereignisquelle für Ihre Lambda-Funktion. Weitere Informationen finden Sie unter Kinesis Data Streams.
OpenSearch Service-Domain	Das Ziel für die Daten, nachdem sie durch Ihre Lambda-Funktion verarbeitet wurden. Weitere Informationen finden Sie unter the section called “ OpenSearch Dienstdomänen erstellen”

Voraussetzung	Beschreibung

IAM Role (IAM-Rolle)	Diese Rolle muss über grundlegende OpenSearch Service-, Kinesis- und Lambda-Berechtigungen verfügen, wie z. B. die folgenden:
	
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "es:ESHttpPost", "es:ESHttpPut", "logs:CreateLogGroup", "logs:CreateLogStream", "logs:PutLogEvents", "kinesis:GetShardIterator", "kinesis:GetRecords", "kinesis:DescribeStream", "kinesis:ListStreams" ], "Resource": "*" } ] }`
	
	Die Rolle muss über die folgende Vertrauensstellung verfügen:
	
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "Service": "lambda.amazonaws.com" }, "Action": "sts:AssumeRole" } ] }`

Voraussetzung	Beschreibung
	Weitere Informationen finden Sie unter Erstellen von IAM-Rollen im IAM-Benutzerhandbuch.

So erstellen Sie die Lambda-Funktion:

Befolgen Sie die Anweisungen in the section called “Erstellen des Lambda-Bereitstellungspakets”. Erstellen Sie jedoch ein Verzeichnis mit dem Namen `kinesis-to-opensearch` und verwenden Sie den folgenden Code für `sample.py`:

```
import base64
import boto3
import json
import requests
from requests_aws4auth import AWS4Auth

region = '' # e.g. us-west-1
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)

host = '' # the OpenSearch Service domain, e.g. https://search-mydomain.us-
west-1.es.amazonaws.com
index = 'lambda-kine-index'
datatype = '_doc'
url = host + '/' + index + '/' + datatype + '/'

headers = { "Content-Type": "application/json" }

def handler(event, context):
    count = 0
    for record in event['Records']:
        id = record['eventID']
        timestamp = record['kinesis']['approximateArrivalTimestamp']

        # Kinesis data is base64-encoded, so decode here
        message = base64.b64decode(record['kinesis']['data'])

        # Create the JSON document
        document = { "id": id, "timestamp": timestamp, "message": message }
```

```
        # Index the document
        r = requests.put(url + id, auth=awsauth, json=document, headers=headers)
        count += 1
    return 'Processed ' + str(count) + ' items.'
```

Bearbeiten Sie die Variablen für `region` und `host`.

Installieren Sie pip, falls noch nicht geschehen, und verwenden Sie dann die folgenden Befehle, um Ihre Abhängigkeiten zu installieren:

```
cd kinesis-to-opensearch

pip install --target ./package requests
pip install --target ./package requests_aws4auth
```

Befolgen Sie dann die Anweisungen in the section called “So erstellen Sie die Lambda-Funktion:”. Geben Sie jedoch die IAM-Rolle aus the section called “Voraussetzungen” und die folgenden Einstellungen für den Auslöser an:

- Kinesis-Stream: Ihr Kinesis-Stream
- Stapelgröße: 100
- Startposition: Horizont trimmen

Weitere Informationen finden Sie unter Was ist Amazon Kinesis Data Streams? im Entwicklerhandbuch für Amazon Kinesis Data Streams.

An diesem Punkt verfügen Sie über einen vollständigen Satz von Ressourcen: einen Kinesis-Datenstrom, eine Funktion, die ausgeführt wird, nachdem der Stream neue Daten empfängt und diese Daten indiziert, und eine - OpenSearch Service-Domain für die Suche und Visualisierung.

Lambda-Funktion testen

Nachdem Sie die Funktion erstellt haben, können Sie sie testen, indem Sie den Data-Stream mithilfe der AWS CLIaufzeichnen:

```
aws kinesis put-record --stream-name test --data "My test data." --partition-key
 partitionKey1 --region us-west-1
```

Verwenden Sie dann die OpenSearch Servicekonsole oder OpenSearch Dashboards, um zu überprüfen, ob ein Dokument `lambda-kine-index` enthält. Sie können außerdem die folgenden Anforderung verwenden:

```
GET https://domain-name/lambda-kine-index/_search
{
  "hits" : [
    {
      "_index": "lambda-kine-index",
      "_type": "_doc",
      "_id":
 "shardId-000000000000:49583511615762699495012960821421456686529436680496087042",
      "_score": 1,
      "_source": {
        "timestamp": 1523648740.051,
        "message": "My test data.",
        "id":
 "shardId-000000000000:49583511615762699495012960821421456686529436680496087042"
      }
    }
  ]
}
```

So laden Sie Streaming-Daten aus Amazon DynamoDB

Sie können verwenden AWS Lambda , um Daten aus Amazon DynamoDB an Ihre OpenSearch Service-Domain zu senden. Neue in der Datenbanktabelle eintreffende Daten lösen eine Ereignisbenachrichtigung an Lambda aus, wodurch Ihr benutzerdefinierte Code zum Durchführen der Indizierung ausgeführt wird.

Voraussetzungen

Zum Fortfahren benötigen Sie die folgenden Ressourcen.

Voraussetzung	Beschreibung
DynamoDB-Tabelle	Die Tabelle enthält Ihre Quelldaten. Weitere Informationen finden Sie unter Grundlegende Operationen in DynamoDB-Tabellen im Amazon-DynamoDB-Entwicklerhandbuch.

Voraussetzung	Beschreibung
	Die Tabelle muss sich in derselben Region wie Ihre OpenSearch Service-Domain befinden und einen Stream auf Neues Image festlegen. Weitere Informationen finden Sie unter Aktivieren eines Streams.
OpenSearch Service-Domain	Das Ziel für die Daten, nachdem sie durch Ihre Lambda-Funktion verarbeitet wurden. Weitere Informationen finden Sie unter the section called “ OpenSearch Dienstdomänen erstellen”.

Voraussetzung	Beschreibung
IAM-Rolle	Diese Rolle muss über grundlegende OpenSearch Service-, DynamoDB- und Lambda-Ausführungsberechtigungen verfügen, wie z. B. die folgenden: `{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["es:ESHttpPost", "es:ESHttpPut", "dynamodb:DescribeStream", "dynamodb:GetRecords", "dynamodb:GetShardIterator", "dynamodb:ListStreams", "logs:CreateLogGroup", "logs:CreateLogStream", "logs:PutLogEvents"], "Resource": "*" }] }`  Die Rolle muss über die folgende Vertrauensstellung verfügen:  `{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Principal": { "Service": "lambda.amazonaws.com" }, "Action": "sts:AssumeRole" }] }`

Voraussetzung	Beschreibung
	Weitere Informationen finden Sie unter Erstellen von IAM-Rollen im IAM-Benutzerhandbuch.

So erstellen Sie die Lambda-Funktion:

Befolgen Sie die Anweisungen in the section called “Erstellen des Lambda-Bereitstellungspakets”. Erstellen Sie jedoch ein Verzeichnis mit dem Namen `ddb-to-opensearch` und verwenden Sie den folgenden Code für `sample.py`:

```
import boto3
import requests
from requests_aws4auth import AWS4Auth

region = '' # e.g. us-east-1
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)

host = '' # the OpenSearch Service domain, e.g. https://search-mydomain.us-
west-1.es.amazonaws.com
index = 'lambda-index'
datatype = '_doc'
url = host + '/' + index + '/' + datatype + '/'

headers = { "Content-Type": "application/json" }

def handler(event, context):
    count = 0
    for record in event['Records']:
        # Get the primary key for use as the OpenSearch ID
        id = record['dynamodb']['Keys']['id']['S']

        if record['eventName'] == 'REMOVE':
            r = requests.delete(url + id, auth=awsauth)
        else:
            document = record['dynamodb']['NewImage']
            r = requests.put(url + id, auth=awsauth, json=document, headers=headers)
        count += 1
```

```
    return str(count) + ' records processed.'
```

Bearbeiten Sie die Variablen für `region` und `host`.

Installieren Sie pip, falls noch nicht geschehen, und verwenden Sie dann die folgenden Befehle, um Ihre Abhängigkeiten zu installieren:

```
cd ddb-to-opensearch

pip install --target ./package requests
pip install --target ./package requests_aws4auth
```

Befolgen Sie dann die Anweisungen in the section called “So erstellen Sie die Lambda-Funktion:”. Geben Sie jedoch die IAM-Rolle aus the section called “Voraussetzungen” und die folgenden Einstellungen für den Auslöser an:

- Tabelle: Ihre DynamoDB-Tabelle
- Stapelgröße: 100
- Startposition: Horizont trimmen

Weitere Informationen finden Sie unter Verarbeiten neuer Elemente mit DynamoDB-Streams und Lambda im Amazon-DynamoDB-Entwicklerhandbuch.

An diesem Punkt verfügen Sie über einen vollständigen Satz von Ressourcen: eine DynamoDB-Tabelle für Ihre Quelldaten, einen DynamoDB-Stream von Änderungen an der Tabelle, eine Funktion, die ausgeführt wird, nachdem sich Ihre Quelldaten geändert haben und diese Änderungen indiziert, und eine - OpenSearch Service-Domain für die Suche und Visualisierung.

Lambda-Funktion testen

Nachdem Sie die Funktion erstellt haben, können Sie sie testen, indem Sie ein neues Element zur DynamoDB-Tabelle mithilfe der AWS CLIhinzufügen:

```
aws dynamodb put-item --table-name test --item '{"director": {"S": "Kevin
 Costner"},"id": {"S": "00001"},"title": {"S": "The Postman"}}' --region us-west-1
```

Verwenden Sie dann die OpenSearch Servicekonsole oder OpenSearch Dashboards, um zu überprüfen, ob ein Dokument `lambda-index` enthält. Sie können außerdem die folgenden Anforderung verwenden:

```
GET https://domain-name/lambda-index/_doc/00001
{
    "_index": "lambda-index",
    "_type": "_doc",
    "_id": "00001",
    "_version": 1,
    "found": true,
    "_source": {
        "director": {
            "S": "Kevin Costner"
        },
        "id": {
            "S": "00001"
        },
        "title": {
            "S": "The Postman"
        }
    }
}
```

Laden von Streaming-Daten aus Amazon Data Firehose

Firehose unterstützt OpenSearch Service als Bereitstellungsziel. Anweisungen zum Laden von Streaming-Daten in den OpenSearch Service finden Sie unter Erstellen eines Kinesis-Data-Firehose-Bereitstellungsdatenstroms und Auswählen des OpenSearch Services für Ihr Ziel im Amazon-Data-Firehose-Entwicklerhandbuch.

Bevor Sie Daten in den OpenSearch Service laden, müssen Sie möglicherweise Transformationen an den Daten durchführen. Weitere Informationen über die Verwendung von Lambda-Funktionen zur Ausführung dieser Aufgabe finden Sie unter Amazon Kinesis Data Firehose Datentransformation im selben Handbuch.

Wenn Sie einen Bereitstellungsdatenstrom konfigurieren, bietet Firehose eine IAM-Rolle mit nur einem Klick, die ihm den Ressourcenzugriff gibt, den er zum Senden von Daten an den OpenSearch Service, Sichern von Daten auf Amazon S3 und Transformieren von Daten mit Lambda benötigt. Aufgrund der Komplexität bei der manuellen Erstellung einer solchen Rolle empfehlen wir die Verwendung der bereitgestellten Rolle.

Laden von Streaming-Daten aus Amazon CloudWatch

Sie können Streaming-Daten mithilfe eines CloudWatch Logs-Abonnements aus - CloudWatch Protokollen in Ihre OpenSearch Service-Domain laden. Informationen zu Amazon- CloudWatch Abonnements finden Sie unter Echtzeitverarbeitung von Protokolldaten mit Abonnements. Konfigurationsinformationen finden Sie unter Streaming von CloudWatch Protokolldaten an Amazon OpenSearch Service im Amazon CloudWatch-Entwicklerhandbuch.

So laden Sie Streaming-Daten aus AWS IoT

Sie können Daten von AWS IoT mithilfe von Regeln senden. Weitere Informationen finden Sie in der -OpenSearchAktion im AWS IoT -Entwicklerhandbuch.

Laden von Daten in Amazon OpenSearch Service mit

Die Open-Source-Version von Logstash (Logstash OSS) bietet eine bequeme Möglichkeit, die Massen-API zum Hochladen von Daten in Ihre OpenSearch Amazon--Service-Domäne zu verwenden. Der Service unterstützt alle Standard-Logstash-Eingabe-Plug-Ins, einschließlich des Amazon-S3-Eingabe-Plug-Ins. OpenSearch Der Dienst unterstützt das logstash-output-opensearchAusgabe-Plugin, das sowohl die grundlegende Authentifizierung als auch IAM-Anmeldeinformationen unterstützt. Das Plugin arbeitet mit Version 8.1 und niedriger von Logstash OSS.

Konfiguration

Die Logstash-Konfiguration variiert je nach Art der Authentifizierung, die Ihre Domäne verwendet.

Unabhängig davon, welche Authentifizierungsmethode Sie verwenden, müssen Sie im Abschnitt output der Konfigurationsdatei `ecs_compatibility` auf `disabled` festlegen. Logstash 8.0 führte eine bahnbrechende Änderung ein, bei der alle Plugins standardmäßig im ECS-Kompatibilitätsmodus ausgeführt werden. Sie müssen den Standard überschreiben, um das Legacy-Verhalten beizubehalten.

Differenzierte Zugriffskontrolle

Wenn Ihre OpenSearch Dienstdomäne eine differenzierte Zugriffskontrolle mit HTTP-Standardauthentifizierung verwendet, ähnelt die Konfiguration jedem anderen OpenSearch Cluster. Diese Beispielkonfigurationsdatei übernimmt ihre Eingabe aus der Open-Source-Version von Filebeat (Filebeat OSS):

```
input {
  beats  {
    port => 5044
  }
}

output {
  opensearch {
    hosts       => "https://domain-endpoint:443"
    user        => "my-username"
    password    => "my-password"
    index       => "logstash-logs-%{+YYYY.MM.dd}"
    ecs_compatibility => disabled
    ssl_certificate_verification => false
  }
}
```

Die Konfiguration variiert je nach Beats-Anwendung und Anwendungsfall, aber Ihre Filebeat-OSS-Konfiguration könnte folgendermaßen aussehen:

```
filebeat.inputs:
- type: log
  enabled: true
  paths:
    - /path/to/logs/dir/*.log
filebeat.config.modules:
  path: ${path.config}/modules.d/*.yml
  reload.enabled: false
setup.ilm.enabled: false
setup.ilm.check_exists: false
setup.template.settings:
  index.number_of_shards: 1
output.logstash:
  hosts: ["logstash-host:5044"]
```

IAM-Konfiguration

Wenn Ihre Domäne eine IAM-basierte Domänenzugriffsrichtlinie oder eine differenzierte Zugriffskontrolle mit einem Haupt-Benutzer verwendet, müssen Sie alle Anforderungen an den OpenSearch Service mit IAM-Anmeldeinformationen signieren. Die folgende identitätsbasierte Richtlinie gewährt alle HTTP-Anforderungen an die Unterressourcen Ihrer Domäne.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "es:ESHttp*"
      ],
      "Resource": "arn:aws:es:region:aws-account-id:domain/domain-name/*"
    }
  ]
}
```

Um Ihre Logstash-Konfiguration zu ändern, ändern Sie Ihre Konfigurationsdatei, um das Plug-In für seine Ausgabe zu verwenden. Diese Beispielkonfigurationsdatei übernimmt ihre Eingabe von Dateien in einem S3-Bucket:

```
input {
  s3 {
    bucket => "my-s3-bucket"
    region => "us-east-1"
  }
}

output {
  opensearch {
    hosts => ["domain-endpoint:443"]
    auth_type => {
      type => 'aws_iam'
      aws_access_key_id => 'your-access-key'
      aws_secret_access_key => 'your-secret-key'
      region => 'us-east-1'
      }
      index  => "logstash-logs-%{+YYYY.MM.dd}"
      ecs_compatibility => disabled
  }
}
```

Wenn Sie Ihre IAM-Anmeldeinformationen nicht in der Konfigurationsdatei angeben möchten, können Sie sie exportieren (oder `aws configure` ausführen):

```
export AWS_ACCESS_KEY_ID="your-access-key"
```

```
export AWS_SECRET_ACCESS_KEY="your-secret-key"
export AWS_SESSION_TOKEN="your-session-token"
```

Wenn sich Ihre OpenSearch Service-Domäne in einer VPC befindet, muss die Logstash-OSS-Maschine eine Verbindung zur VPC herstellen und über die VPC-Sicherheitsgruppen Zugriff auf die Domäne haben. Weitere Informationen finden Sie unter the section called “Zugriffsrichtlinien für VPC-Domänen”.

Suchen nach Daten in Amazon OpenSearch Service

Es gibt mehrere gängige Methoden für die Suche nach Dokumenten in Amazon OpenSearch Service, darunter URI-Suchen und Suchen nach Anforderungstexten. OpenSearch Der Service bietet zusätzliche Funktionen, die das Sucherlebnis verbessern, wie z. B. benutzerdefinierte Pakete, SQL-Unterstützung und asynchrone Suche. Eine umfassende OpenSearch Such-API-Referenz finden Sie in der OpenSearch Dokumentation.

> **Note**
>
> Die folgenden Beispielanfragen funktionieren mit OpenSearch APIs. Einige Anfragen funktionieren möglicherweise nicht mit älteren Elasticsearch-Versionen.

Themen

URI-Suchanfragen

Universal Resource Identifier (URI)-Suchanfragen sind die einfachste Form der Suche. Sie geben in einer URI-Suchanfrage die Abfrage als einen HTTP-Anfrageparameter an:

```
GET https://search-my-domain.us-west-1.es.amazonaws.com/_search?q=house
```

Eine Beispielantwort kann wie folgt aussehen:


```
{
  "took": 25,
  "timed_out": false,
  "_shards": {
    "total": 10,
    "successful": 10,
    "skipped": 0,
    "failed": 0
  },
  "hits": {
    "total": {
      "value": 85,
      "relation": "eq",
    },
    "max_score": 6.6137657,
    "hits": [
      {
        "_index": "movies",
        "_type": "movie",
        "_id": "tt0077975",
        "_score": 6.6137657,
        "_source": {
          "directors": [
            "John Landis"
          ],
          "release_date": "1978-07-27T00:00:00Z",
          "rating": 7.5,
          "genres": [
            "Comedy",
            "Romance"
          ],
          "image_url": "http://ia.media-imdb.com/images/M/
MV5BMTY2OTQxNTc1OF5BMl5BanBnXkFtZTYwNjA3NjI5._V1_SX400_.jpg",
          "plot": "At a 1962 College, Dean Vernon Wormer is determined to expel the
 entire Delta Tau Chi Fraternity, but those troublemakers have other plans for him.",
          "title": "Animal House",
          "rank": 527,
          "running_time_secs": 6540,
          "actors": [
```

```
            "John Belushi",
            "Karen Allen",
            "Tom Hulce"
          ],
          "year": 1978,
          "id": "tt0077975"
        }
      },
      ...
    ]
  }
}
```

Standardmäßig durchsucht diese Abfrage alle Felder aller Indizes nach dem Begriff house. Wenn Sie die Suche einschränken möchten, geben Sie einen Index- (`movies`) und ein Dokumentfeld (`title`) in der URI an:

```
GET https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search?q=title:house
```

Sie können zusätzliche Parameter in die Anfrage aufnehmen, aber die unterstützten Parameter stellen nur einen kleinen Teil der OpenSearch Suchoptionen dar. Die folgende Anfrage gibt 20 Ergebnisse (statt standardmäßig 10) zurück und sortiert nach Jahr (statt nach `_score`):

```
GET https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search?
q=title:house&size=20&sort=year:desc
```

Anforderungstextsuchen

Um komplexere Suchen durchzuführen, verwenden Sie den Hauptteil der HTTP-Anfrage und die OpenSearch domänenspezifische Sprache (DSL) für Abfragen. Mit der Abfrage DSL können Sie den gesamten Bereich der Suchoptionen angeben. OpenSearch

> **Note**
>
> Sie können keine Unicode-Sonderzeichen in einen Textfeldwert aufnehmen, andernfalls wird der Wert als mehrere durch das Sonderzeichen getrennte Werte analysiert. Diese fehlerhafte Analyse kann zu einer unbeabsichtigten Filterung von Dokumenten führen und möglicherweise die Kontrolle über deren Zugriff beeinträchtigen. Weitere Informationen finden

Sie in der OpenSearch Dokumentation unter Ein Hinweis zu Unicode-Sonderzeichen in Textfeldern.

Die folgende `match`-Abfrage ist ähnlich wie das endgültige URI-Suchanfragen-Beispiel:

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search
{
  "size": 20,
  "sort": {
    "year": {
      "order": "desc"
    }
  },
  "query": {
    "query_string": {
      "default_field": "title",
      "query": "house"
    }
  }
}
```

Note

Die `_search`-API akzeptiert HTTP `GET` und `POST` für Anforderungstextsuchen, jedoch nicht alle HTTP-Clients unterstützen das Hinzufügen eines Anforderungstexts zu einer `GET`-Anforderung. `POST` ist die universellere Wahl.

In vielen Fällen möchten Sie möglicherweise mehrere Felder durchsuchen, jedoch nicht alle Felder. Verwenden Sie die `multi_match`-Abfrage:

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search
{
  "size": 20,
  "query": {
    "multi_match": {
      "query": "house",
      "fields": ["title", "plot", "actors", "directors"]
    }
```

```
  }
}
```

Boosten der Felder

Sie können die Suchrelevanz verbessern, indem Sie bestimmte Felder "boosten". Boosts sind Multiplikatoren, die Übereinstimmungen in einem Feld stärker gewichten als die in anderen Feldern. Im folgenden Beispiel beeinflusst eine Übereinstimmung für john im `title`-Feld `_score` doppelt so viel wie eine Übereinstimmung im `plot`-Feld und vier Mal so viel wie eine Übereinstimmung im `actors`- oder `directors`-Feld. Das Ergebnis ist, dass Filme wie John Wick und John Carter oben in den Suchergebnissen und Filme mit John Travolta unten angegeben werden.

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search
{
  "size": 20,
  "query": {
    "multi_match": {
      "query": "john",
      "fields": ["title^4", "plot^2", "actors", "directors"]
    }
  }
}
```

Hervorheben der Suchergebnisse

Die `highlight` Option weist OpenSearch an, dass ein zusätzliches Objekt innerhalb des `hits` Arrays zurückgegeben werden soll, wenn die Abfrage mit einem oder mehreren Feldern übereinstimmt:

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search
{
  "size": 20,
  "query": {
    "multi_match": {
      "query": "house",
      "fields": ["title^4", "plot^2", "actors", "directors"]
    }
  },
  "highlight": {
    "fields": {
```

```
      "plot": {}
    }
  }
}
```

Wenn die Abfrage mit dem Inhalt des `plot`-Feldes übereinstimmt, könnte ein Treffer folgendermaßen aussehen:

```
{
  "_index": "movies",
  "_type": "movie",
  "_id": "tt0091541",
  "_score": 11.276199,
  "_source": {
    "directors": [
      "Richard Benjamin"
    ],
    "release_date": "1986-03-26T00:00:00Z",
    "rating": 6,
    "genres": [
      "Comedy",
      "Music"
    ],
    "image_url": "http://ia.media-imdb.com/images/M/
MV5BMTIzODEzODE2OF5BMl5BanBnXkFtZTcwNjQ3ODcyMQ@@._V1_SX400_.jpg",
    "plot": "A young couple struggles to repair a hopelessly dilapidated house.",
    "title": "The Money Pit",
    "rank": 4095,
    "running_time_secs": 5460,
    "actors": [
      "Tom Hanks",
      "Shelley Long",
      "Alexander Godunov"
    ],
    "year": 1986,
    "id": "tt0091541"
  },
  "highlight": {
    "plot": [
      "A young couple struggles to repair a hopelessly dilapidated <em>house</em>."
    ]
  }
}
```

Standardmäßig OpenSearch umschließt die übereinstimmende Zeichenfolge in Tags, stellt bis zu 100 Zeichen Kontext für den Treffer bereit und teilt den Inhalt in Sätze auf, indem Satzzeichen, Leerzeichen, Tabulatoren und Zeilenumbrüche identifiziert werden. Alle diese Einstellungen sind konfigurierbar:

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search
{
  "size": 20,
  "query": {
    "multi_match": {
      "query": "house",
      "fields": ["title^4", "plot^2", "actors", "directors"]
    }
  },
  "highlight": {
    "fields": {
      "plot": {}
    },
    "pre_tags": "<strong>",
    "post_tags": "</strong>",
    "fragment_size": 200,
    "boundary_chars": ".,!? "
  }
}
```

Count-API

Wenn Sie nicht am Inhalt Ihrer Dokumente interessiert sind und einfach nur die Anzahl der Übereinstimmungen wissen möchten, können Sie die `_count`-API anstelle der `_search`-API verwenden. Die folgende Anfrage verwendet die `query_string`-Abfrage zum Identifizieren romantischer Komödien:

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/movies/_count
{
  "query": {
    "query_string": {
      "default_field": "genres",
      "query": "romance AND comedy"
    }
  }
}
```

Eine Beispielantwort kann wie folgt aussehen:

```
{
  "count": 564,
  "_shards": {
    "total": 5,
    "successful": 5,
    "skipped": 0,
    "failed": 0
  }
}
```

Paginieren der Suchergebnisse

Wenn Sie eine große Anzahl von Suchergebnissen anzeigen müssen, können Sie die Paginierung mit verschiedenen Methoden implementieren.

Zeitpunkt

Die Point-in-Time-Funktion (PIT) ist eine Art von Suche, mit der Sie verschiedene Abfragen für einen Datensatz ausführen können, der zeitlich festgelegt ist. Dies ist die bevorzugte Paginierungsmethode OpenSearch, insbesondere für tiefe Paginierung. Sie können PIT mit OpenSearch Service Version 2.5 und höher verwenden. Weitere Informationen zu PIT finden Sie unter???.

Die `size` Parameter `from` und

Die einfachste Methode zum Paginieren ist die Verwendung der `size` Parameter `from` und. Die folgende Anfrage gibt Ergebnisse 20-39 der null-indizierten Liste von Suchergebnissen zurück:

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search
{
  "from": 20,
  "size": 20,
  "query": {
    "multi_match": {
      "query": "house",
      "fields": ["title^4", "plot^2", "actors", "directors"]
    }
  }
}
```

Weitere Informationen zur Suchpaginierung finden Sie in der Dokumentation unter Ergebnisse paginieren. OpenSearch

Abfragesprache für Dashboards

Sie können die Dashboards Query Language (DQL) verwenden, um in Dashboards nach Daten und Visualisierungen zu suchen. OpenSearch DQL verwendet vier primäre Abfragetypen: Begriffe, boolesch, Datum und Bereich und verschachteltes Feld.

Begriffsabfrage

Bei einer Begriffsabfrage müssen Sie den Begriff angeben, nach dem Sie suchen.

Geben Sie zum Durchführen einer Begriffsabfrage Folgendes ein:

```
host:www.example.com
```

Boolesche Abfrage

Sie können die booleschen Operatoren `AND`, `or` und `not` verwenden, um mehrere Abfragen zu kombinieren.

Fügen Sie zum Durchführen einer booleschen Abfrage Folgendes ein:

```
host.keyword:www.example.com and response.keyword:200
```

Datums- und Bereichsabfragen

Sie können eine Datums- und Bereichsabfrage verwenden, um ein Datum vor oder nach Ihrer Abfrage zu finden.

- > zeigt eine Suche nach einem Datum nach dem angegebenen Datum an.
- < zeigt eine Suche nach einem Datum vor dem angegebenen Datum an.

```
@timestamp > "2020-12-14T09:35:33"
```

Verschachtelte Feldabfrage

Wenn Sie ein Dokument mit verschachtelten Feldern haben, müssen Sie angeben, welche Teile des Dokuments Sie abrufen möchten. Im Folgenden finden Sie ein Beispieldokument, das verschachtelte Felder enthält:

```
{"NBA players":[
    {"player-name": "Lebron James",
      "player-position": "Power forward",
      "points-per-game": "30.3"
    },
    {"player-name": "Kevin Durant",
      "player-position": "Power forward",
      "points-per-game": "27.1"
    },
    {"player-name": "Anthony Davis",
      "player-position": "Power forward",
      "points-per-game": "23.2"
    },
    {"player-name": "Giannis Antetokounmpo",
      "player-position": "Power forward",
      "points-per-game":"29.9"
    }
  ]
}
```

Fügen Sie Folgendes ein, um ein bestimmtes Feld mit DQL abzurufen:

```
NBA players: {player-name: Lebron James}
```

Fügen Sie Folgendes ein, um mehrere Objekte aus dem verschachtelten Dokument abzurufen:

```
NBA players: {player-name: Lebron James} and NBA players: {player-name: Giannis
 Antetokounmpo}
```

Fügen Sie Folgendes ein, um innerhalb eines Bereichs zu suchen:

```
NBA players: {player-name: Lebron James} and NBA players: {player-name: Giannis
 Antetokounmpo and < 30}
```

Wenn Ihr Dokument ein Objekt enthält, das in einem anderen Objekt verschachtelt ist, können Sie dennoch Daten abrufen, indem Sie alle Ebenen angeben. Fügen Sie dazu Folgendes ein:

```
Top-Power-forwards.NBA players: {player-name:Lebron James}
```

Maßgeschneiderte Pakete für Amazon OpenSearch Service

Mit Amazon OpenSearch Service können Sie benutzerdefinierte Wörterbuchdateien wie Stoppwörter und Synonyme hochladen. Außerdem bietet Amazon Service mehrere vorgefertigte, optionale Plug-ins, die Sie mit Ihrer Domain verknüpfen können. Der Oberbegriff für diese beiden Arten von Dateien ist Pakete.

Wörterbuchdateien verbessern Ihre Suchergebnisse, indem sie OpenSearch anweisen, bestimmte häufig verwendete Wörter zu ignorieren oder Begriffe wie „gefrorener Vanillepudding“, „Gelato“ und „Eiscreme“ gleichwertig zu behandeln. Sie können außerdem die Stammverknüpfung verbessern, z. B. im Plug-In Japanese (kuromoji) Analysis.

Optionale Plugins können Ihrer Domain zusätzliche Funktionen bieten. Sie können beispielsweise das Amazon Personalize Personalize-Plugin verwenden, um personalisierte Suchergebnisse zu erhalten. Optionale Plugins verwenden den `ZIP-PLUGIN` Pakettyp. Weitere Hinweise zu optionalen Plugins finden Sie unterthe section called “Plug-ins nach Engine-Version”.

Themen

- Paketberechtigungen
- Hochladen von Paketen nach Amazon S3
- Importieren und Zuordnen von Paketen
- Verwenden von Paketen mit OpenSearch
- Pakete werden aktualisiert
- Manuelle Indexaktualisierungen für Wörterbücher
- Trennen und Entfernen von Paketen

Paketberechtigungen

Benutzer ohne Administratorzugriff benötigen bestimmte AWS Identity and Access Management (IAM-) Aktionen, um Pakete zu verwalten:

- `es:CreatePackage`- ein Paket in einer OpenSearch Serviceregion erstellen
- `es:DeletePackage`- löscht ein Paket aus einer OpenSearch Serviceregion
- `es:AssociatePackage` – Zuordnen eines Pakets zu einer Domäne
- `es:DissociatePackage` – Trennen eines Pakets von einer Domäne

Sie benötigen auch Berechtigungen für den Amazon-S3-Bucket-Pfad oder das Objekt, in dem sich das benutzerdefinierte Paket befindet.

Erteilen Sie alle Berechtigungen innerhalb von IAM, nicht in der Domänenzugriffsrichtlinie. Weitere Informationen finden Sie unter the section called “Identitäts- und Zugriffsverwaltung”.

Hochladen von Paketen nach Amazon S3

In diesem Abschnitt wird beschrieben, wie Sie benutzerdefinierte Wörterbuchpakete hochladen können, da optionale Plugin-Pakete bereits vorinstalliert sind. Bevor Sie Ihrer Domain ein benutzerdefiniertes Wörterbuch zuordnen können, müssen Sie es in einen Amazon S3 S3-Bucket hochladen. Weitere Anleitungen finden Sie unter Upload eines Objekts im Benutzerhandbuch für Amazon Simple Storage Service. Unterstützte Plugins müssen nicht hochgeladen werden.

Wenn Ihr Wörterbuch vertrauliche Informationen enthält, geben Sie beim Hochladen eine serverseitige Verschlüsselung mit von S3 verwalteten Schlüsseln an. OpenSearch Der Dienst kann nicht auf Dateien auf S3 zugreifen, die Sie mit einem Schlüssel schützen. AWS KMS

Nachdem Sie die Datei hochgeladen haben, notieren Sie deren S3-Pfad. Das Pfadformat lautet `s3://`*`bucket-name`*`/`*`file-path`*`/`*`file-name`*.

Sie können die folgende Synonymdatei für Testzwecke verwenden. Speichern Sie diese unter `synonyms.txt`.

```
danish, croissant, pastry
ice cream, gelato, frozen custard
sneaker, tennis shoe, running shoe
basketball shoe, hightop
```

Bestimmte Wörterbücher, wie Hunspell-Wörterbücher, verwenden mehrere Dateien und benötigen eigene Verzeichnisse im Dateisystem. Derzeit unterstützt OpenSearch Service nur Wörterbücher mit einer einzigen Datei.

Importieren und Zuordnen von Paketen

Die Konsole ist die einfachste Methode, ein benutzerdefiniertes Wörterbuch in Service zu importieren. OpenSearch Wenn Sie ein Wörterbuch aus Amazon S3 importieren, speichert OpenSearch Service seine eigene Kopie des Pakets und verschlüsselt diese Kopie automatisch mit AES-256 mit OpenSearch vom Service verwalteten Schlüsseln.

Optionale Plug-ins sind in OpenSearch Service bereits vorinstalliert, sodass Sie sie nicht selbst hochladen müssen. Sie müssen jedoch ein Plug-in mit einer Domain verknüpfen. Verfügbare Plug-ins sind auf dem Bildschirm Pakete in der Konsole aufgeführt.

Importieren Sie ein Paket und verknüpfen Sie es mit einer Domain mit dem AWS Management Console

1. Wählen Sie in der Amazon OpenSearch Service-Konsole Pakete aus.
2. Klicken Sie auf Packet importieren.
3. Geben Sie dem Benutzerwörterbuch einen aussagekräftigen Namen.
4. Geben Sie den S3-Pfad zu der Datei an und wählen Sie dann Absenden aus.
5. Kehren Sie zum Bildschirm Packages (Pakete) zurück.
6. Wenn der Paketstatus Available (Verfügbar) lautet, wählen Sie das Paket aus. Optionale Plugins werden automatisch verfügbar sein.
7. Wählen Sie Einer Domain zuordnen aus.
8. Wählen Sie eine Domäne aus und klicken Sie dann auf Associate (Zuordnen).
9. Wählen Sie im Navigationsbereich Ihre Domäne und dann die Registerkarte Pakete aus.
10. Wenn es sich bei dem Paket um ein benutzerdefiniertes Wörterbuch handelt, notieren Sie sich die ID, wenn das Paket verfügbar wird. Verwenden Sie `analyzers/id` als Dateipfad für Anfragen an OpenSearch.

Verwenden Sie alternativ die SDKs oder die AWS CLI Konfigurations-API, um Pakete zu importieren und zuzuordnen. Weitere Informationen finden Sie in der AWS CLI Befehlsreferenz und der Amazon OpenSearch Service API-Referenz.

Verwenden von Paketen mit OpenSearch

In diesem Abschnitt wird beschrieben, wie Sie beide Arten von Paketen verwenden können: benutzerdefinierte Wörterbücher und optionale Plugins.

Verwenden von benutzerdefinierten Wörterbüchern

Nachdem Sie eine Datei einer Domäne zugeordnet haben, können Sie sie beim Erstellen von Tokenizern und Tokenfiltern in Parametern wie `synonyms_path`, `stopwords_path` und `user_dictionary` verwenden. Der genaue Parameter ist je nach Objekt unterschiedlich. Mehrere

Objekte unterstützen `synonyms_path` und `stopwords_path`, `user_dictionary` gilt jedoch exklusiv für das kuromoji-Plugin.

Für das IK-Analysis-Plug-In (Chinesisch) können Sie eine benutzerdefinierte Wörterbuchdatei als benutzerdefiniertes Paket hochladen und sie einer Domäne zuordnen, und das Plug-In nimmt sie automatisch auf, ohne dass ein `user_dictionary`-Parameter erforderlich ist. Wenn es sich bei Ihrer Datei um eine Synonymdatei handelt, verwenden Sie den `synonyms_path`-Parameter.

Mit dem folgenden Beispiel wird eine Synonymdatei zu einem neuen Index hinzugefügt:

```
PUT my-index
{
  "settings": {
    "index": {
      "analysis": {
        "analyzer": {
          "my_analyzer": {
            "type": "custom",
            "tokenizer": "standard",
            "filter": ["my_filter"]
          }
        },
        "filter": {
          "my_filter": {
            "type": "synonym",
            "synonyms_path": "analyzers/F111111111",
            "updateable": true
          }
        }
      }
    }
  },
  "mappings": {
    "properties": {
      "description": {
        "type": "text",
        "analyzer": "standard",
        "search_analyzer": "my_analyzer"
      }
    }
  }
}
```

Diese Anforderung erstellt einen benutzerdefinierten Analysator für den Index, der den Standard-Tokenizer und einen Synonym-Tokenfilter verwendet.

- Tokenizer teilen Zeichendatenströme auf der Grundlage einer Reihe von Regeln in Token (im Allgemeinen Wörter) auf. Das einfachste Beispiel ist der Whitespace-Tokenizer, der die vorhergehenden Zeichen jedes Mal in ein Token unterteilt, wenn er auf ein Leerzeichen trifft. Ein komplexeres Beispiel ist der Standard-Tokenizer, der unter Verwendung einer Reihe von grammatikalischen Regeln in vielen Sprachen arbeitet.
- Tokenfilter fügen Token hinzu, ändern oder löschen Token. Ein Synonym-Tokenfilter beispielsweise fügt Token hinzu, wenn er ein Wort in der Synonymliste findet. Der Stopp-Tokenfilter entfernt Token, wenn er ein Wort in der Liste der Stoppwörter findet.

Diese Anfrage fügt dem Mapping auch ein Textfeld (`description`) hinzu und teilt mit, dass der neue Analyzer als Suchanalysegerät verwendet werden OpenSearch soll. Sie können sehen, dass es immer noch den Standard-Analysator als Indexanalysator verwendet.

Notieren Sie sich schließlich die Zeile `"updateable": true` im Token-Filter. Dieses Feld gilt nur für Suchanalysatoren, nicht für Indexanalysatoren und ist wichtig, wenn Sie den Suchanalysator später automatisch aktualisieren möchten.

Fügen Sie dem Index zu Testzwecken einige Dokumente hinzu:

```
POST _bulk
{ "index": { "_index": "my-index", "_id": "1" } }
{ "description": "ice cream" }
{ "index": { "_index": "my-index", "_id": "2" } }
{ "description": "croissant" }
{ "index": { "_index": "my-index", "_id": "3" } }
{ "description": "tennis shoe" }
{ "index": { "_index": "my-index", "_id": "4" } }
{ "description": "hightop" }
```

Suchen Sie diese anschließend unter Verwendung eines Synonyms:

```
GET my-index/_search
{
  "query": {
    "match": {
      "description": "gelato"
    }
```

```
  }
}
```

In diesem Fall wird die folgende Antwort OpenSearch zurückgegeben:

```
{
  "hits": {
    "total": {
      "value": 1,
      "relation": "eq"
    },
    "max_score": 0.99463606,
    "hits": [{
      "_index": "my-index",
      "_type": "_doc",
      "_id": "1",
      "_score": 0.99463606,
      "_source": {
        "description": "ice cream"
      }
    }]
  }
}
```

> **Tip**
>
> Wörterbuchdateien verwenden Java-Heap-Speicherplatz proportional zu ihrer Größe. Beispielsweise kann eine 2-GiB-Wörterbuchdatei 2 GiB Heap-Speicherplatz auf einem Knoten verbrauchen. Wenn Sie große Dateien verwenden, stellen Sie sicher, dass die Knoten über genügend Heap-Speicher verfügen, um sie aufzunehmen. Überwachen Sie die `JVMMemoryPressure`-Metrik und skalieren Sie Ihren Cluster nach Bedarf.

Verwendung optionaler Plugins

OpenSearch Mit dem Service können Sie vorinstallierte, optionale OpenSearch Plugins zur Verwendung mit Ihrer Domain verknüpfen. Ein optionales Plugin-Paket ist mit einer bestimmten OpenSearch Version kompatibel und kann nur Domains mit dieser Version zugeordnet werden. Die Liste der verfügbaren Pakete für Ihre Domain enthält alle unterstützten Plugins, die mit Ihrer Domain-Version kompatibel sind. Nachdem Sie ein Plugin mit einer Domain verknüpft haben, beginnt ein

Installationsvorgang auf der Domain. Anschließend können Sie auf das Plugin verweisen und es verwenden, wenn Sie Anfragen an den OpenSearch Service stellen.

Zum Zuordnen und Trennen eines Plugins ist eine blaue/grüne Bereitstellung erforderlich. Weitere Informationen finden Sie unter the section called “Änderungen, die normalerweise eine Blau/Grün-Bereitstellung auslösen”.

Zu den optionalen Plugins gehören Sprachanalyseprogramme und benutzerdefinierte Suchergebnisse. Das Amazon Personalize Search Ranking-Plugin verwendet beispielsweise maschinelles Lernen, um Suchergebnisse für Ihre Kunden zu personalisieren. Weitere Informationen zu diesem Plugin finden Sie unter Suchergebnisse personalisieren von. OpenSearch Eine Liste aller unterstützten Plugins finden Sie unterthe section called “Plug-ins nach Engine-Version”.

Sudachi-Plugin

Wenn Sie beim Sudachi-Plugin eine Wörterbuchdatei neu zuordnen, wirkt sich das nicht sofort auf die Domain aus. Das Wörterbuch wird aktualisiert, wenn die nächste blaue/grüne Bereitstellung im Rahmen einer Konfigurationsänderung oder eines anderen Updates auf der Domain ausgeführt wird. Alternativ können Sie ein neues Paket mit den aktualisierten Daten erstellen, mit diesem neuen Paket einen neuen Index erstellen, den vorhandenen Index erneut mit dem neuen Index indizieren und dann den alten Index löschen. Wenn Sie den Ansatz der Neuindizierung bevorzugen, verwenden Sie einen Indexalias, damit Ihr Datenverkehr nicht unterbrochen wird.

Darüber hinaus unterstützt das Sudachi-Plugin nur binäre Sudachi-Wörterbücher, die Sie mit der API-Operation hochladen können. CreatePackage Informationen zum vorgefertigten Systemwörterbuch und zum Verfahren zum Kompilieren von Benutzerwörterbüchern finden Sie in der Sudachi-Dokumentation.

Das folgende Beispiel zeigt, wie System- und Benutzerwörterbücher mit dem Sudachi-Tokenizer verwendet werden. Sie müssen diese Wörterbücher als benutzerdefinierte Pakete mit Typ hochladen `TXT-DICTIONARY` und ihre Paket-IDs in den zusätzlichen Einstellungen angeben.

```
PUT sudachi_sample
{
  "settings": {
    "index": {
      "analysis": {
        "tokenizer": {
          "sudachi_tokenizer": {
            "type": "sudachi_tokenizer",
```

```
            "additional_settings": "{\"systemDict\": \"<system-dictionary-package-
id>\",\"userDict\": [\"<user-dictionary-package-id>\"]}"
          }
          },
          "analyzer": {
            "sudachi_analyzer": {
              "filter": ["my_searchfilter"],
              "tokenizer": "sudachi_tokenizer",
              "type": "custom"
            }
          },
          "filter":{
            "my_searchfilter": {
              "type": "sudachi_split",
              "mode": "search"
            }
          }
        }
      }
    }
}
```

Pakete werden aktualisiert

In diesem Abschnitt wird nur beschrieben, wie Sie ein benutzerdefiniertes Wörterbuchpaket aktualisieren, da optionale Plugin-Pakete bereits für Sie aktualisiert wurden. Durch das Hochladen einer neuen Version eines Wörterbuchs auf Amazon S3 wird das Paket auf Amazon OpenSearch Service nicht automatisch aktualisiert. OpenSearch Service speichert eine eigene Kopie der Datei. Wenn Sie also eine neue Version auf S3 hochladen, müssen Sie sie manuell aktualisieren.

Jede Ihrer verknüpften Domänen speichert auch eine eigene Kopie der Datei. Um das Suchverhalten vorhersehbar zu halten, verwenden Domänen weiterhin ihre aktuelle Paketversion, bis Sie sie explizit aktualisieren. Um ein benutzerdefiniertes Paket zu aktualisieren, ändern Sie die Datei in Amazon S3 Control, aktualisieren Sie das Paket in OpenSearch Service und wenden Sie dann das Update an.

Aktualisieren Sie ein Paket mit dem AWS Management Console

1. Wählen Sie in der OpenSearch Servicekonsole Pakete aus.
2. Wählen Sie ein Paket und Aktualisieren aus.
3. Geben Sie den S3-Pfad zu der Datei an und wählen Sie dann Paket aktualisieren aus.
4. Kehren Sie zum Bildschirm Packages (Pakete) zurück.

5. Wenn der Paketstatus auf Verfügbar wechselt, wählen Sie das Paket aus. Wählen Sie dann eine oder mehrere verknüpfte Domänen aus, übernehmen Sie die Aktualisierung und bestätigen Sie. Warten Sie, bis sich der Zuordnungsstatus in Aktiv ändert.
6. Die nächsten Schritte hängen davon ab, wie Sie Ihre Indizes konfiguriert haben:

   - Wenn Ihre Domain läuft OpenSearch oder Elasticsearch 7.8 oder höher ist und nur Suchanalyser verwendet, bei denen das aktualisierbare Feld auf true gesetzt ist, müssen Sie keine weiteren Maßnahmen ergreifen. OpenSearch Der Service aktualisiert Ihre Indizes automatisch mithilfe der _plugins/_refresh_search_analyzers-API.
   - Wenn auf Ihrer Domain Elasticsearch 7.7 oder früher ausgeführt wird, Indexanalysatoren verwendet werden oder das Feld nicht verwendet, finden Sie weitere Informationen unter. `updateable` the section called “Manuelle Indexaktualisierungen für Wörterbücher”

Die Konsole ist zwar die einfachste Methode, Sie können aber auch die SDKs oder die AWS CLI Konfigurations-API verwenden, um Servicepakete zu aktualisieren OpenSearch . Weitere Informationen finden Sie in der AWS CLI Befehlsreferenz und der Amazon OpenSearch Service API-Referenz.

Aktualisieren Sie ein Paket mit dem AWS SDK

Anstatt ein Paket in der Konsole manuell zu aktualisieren, können Sie die SDKs verwenden, um den Update-Prozess zu automatisieren. Das folgende Python-Beispielskript lädt eine neue Paketdatei auf Amazon S3 hoch, aktualisiert das Paket in OpenSearch Service und wendet das neue Paket auf die angegebene Domain an. Nachdem bestätigt wurde, dass das Update erfolgreich war, führt es einen Beispielaufruf durch, um OpenSearch nachzuweisen, dass die neuen Synonyme angewendet wurden.

Sie müssen Werte für `host`, `region`, `file_name`, `bucket_name`, `s3_key`, `package_id`, `domain_name` und `query` angeben.

```
from requests_aws4auth import AWS4Auth
import boto3
import requests
import time
import json
import sys

host = ''  # The OpenSearch domain endpoint with https:// and a trailing slash. For
 example, https://my-test-domain.us-east-1.es.amazonaws.com/
```

```
region = ''  # For example, us-east-1
file_name = ''  # The path to the file to upload
bucket_name = ''  # The name of the S3 bucket to upload to
s3_key = ''  # The name of the S3 key (file name) to upload to
package_id = ''  # The unique identifier of the OpenSearch package to update
domain_name = ''  # The domain to associate the package with
query = ''  # A test query to confirm the package has been successfully updated

service = 'es'
credentials = boto3.Session().get_credentials()
client = boto3.client('opensearch')
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key,
                   region, service, session_token=credentials.token)


def upload_to_s3(file_name, bucket_name, s3_key):
    """Uploads file to S3"""
    s3 = boto3.client('s3')
    try:
        s3.upload_file(file_name, bucket_name, s3_key)
        print('Upload successful')
        return True
    except FileNotFoundError:
        sys.exit('File not found. Make sure you specified the correct file path.')


def update_package(package_id, bucket_name, s3_key):
    """Updates the package in OpenSearch Service"""
    print(package_id, bucket_name, s3_key)
    response = client.update_package(
        PackageID=package_id,
        PackageSource={
            'S3BucketName': bucket_name,
            'S3Key': s3_key
        }
    )
    print(response)


def associate_package(package_id, domain_name):
    """Associates the package to the domain"""
    response = client.associate_package(
        PackageID=package_id, DomainName=domain_name)
    print(response)
```

```
    print('Associating...')


def wait_for_update(domain_name, package_id):
    """Waits for the package to be updated"""
    response = client.list_packages_for_domain(DomainName=domain_name)
    package_details = response['DomainPackageDetailsList']
    for package in package_details:
        if package['PackageID'] == package_id:
            status = package['DomainPackageStatus']
            if status == 'ACTIVE':
                print('Association successful.')
                return
            elif status == 'ASSOCIATION_FAILED':
                sys.exit('Association failed. Please try again.')
            else:
                time.sleep(10)  # Wait 10 seconds before rechecking the status
                wait_for_update(domain_name, package_id)


def sample_search(query):
    """Makes a sample search call to OpenSearch"""
    path = '_search'
    params = {'q': query}
    url = host + path
    response = requests.get(url, params=params, auth=awsauth)
    print('Searching for ' + '"' + query + '"')
    print(response.text)
```

Note

Wenn Sie bei der Ausführung des Skripts mit dem die Fehlermeldung „Paket nicht gefunden“ erhalten, bedeutet dies wahrscheinlich AWS CLI, dass Boto3 die in ~/.aws/config angegebene Region verwendet, die nicht die Region ist, in der sich Ihr S3-Bucket befindet. Führen Sie entweder `aws configure` aus und geben Sie die richtige Region an, oder fügen Sie die Region explizit zum Client hinzu:

```
client = boto3.client('opensearch', region_name='us-east-1')
```

Manuelle Indexaktualisierungen für Wörterbücher

Manuelle Indexaktualisierungen gelten nur für benutzerdefinierte Wörterbücher, nicht für optionale Plugins. Um ein aktualisiertes Wörterbuch zu verwenden, müssen Sie Ihre Indizes manuell aktualisieren, wenn Sie eine der folgenden Bedingungen erfüllen:

- Ihre Domäne führt Elasticsearch 7.7 oder früher aus.
- Sie verwenden benutzerdefinierte Pakete als Indexanalysatoren.
- Sie verwenden benutzerdefinierte Pakete als Suchanalysatoren, schließen jedoch das aktualisierbare Feld nicht ein.

Um Analyzer mit den neuen Paketdateien zu aktualisieren, haben Sie zwei Möglichkeiten:

- Schließen und öffnen Sie alle Indizes, die Sie aktualisieren möchten:

```
POST my-index/_close
POST my-index/_open
```

- Indizieren Sie die Indizes neu. Erstellen Sie zunächst einen Index, der die aktualisierte Synonymdatei (oder eine völlig neue Datei) verwendet. Beachten Sie, dass nur UTF-8 unterstützt wird.

```
PUT my-new-index
{
  "settings": {
    "index": {
      "analysis": {
        "analyzer": {
          "synonym_analyzer": {
            "type": "custom",
            "tokenizer": "standard",
            "filter": ["synonym_filter"]
          }
        },
        "filter": {
          "synonym_filter": {
            "type": "synonym",
            "synonyms_path": "analyzers/F222222222"
          }
        }
```

```
      }
    }
  },
  "mappings": {
    "properties": {
      "description": {
        "type": "text",
        "analyzer": "synonym_analyzer"
      }
    }
  }
}
```

Nehmen Sie anschließend eine Neuindizierung des alten Index in diesen neuen Index vor:

```
POST _reindex
{
  "source": {
    "index": "my-index"
  },
  "dest": {
    "index": "my-new-index"
  }
}
```

Wenn Sie häufig Index-Analysen aktualisieren, verwenden Sie Indexalias um einen konsistenten Pfad zum neuesten Index beizubehalten:

```
POST _aliases
{
  "actions": [
    {
      "remove": {
        "index": "my-index",
        "alias": "latest-index"
      }
    },
    {
      "add": {
        "index": "my-new-index",
        "alias": "latest-index"
      }
```

```
    }
  ]
}
```

Wenn Sie den alten Index nicht benötigen, löschen Sie ihn:

```
DELETE my-index
```

Trennen und Entfernen von Paketen

Wenn Sie ein Paket, unabhängig davon, ob es sich um ein benutzerdefiniertes Wörterbuch oder ein optionales Plugin handelt, von einer Domain trennen, können Sie dieses Paket nicht mehr verwenden, wenn Sie neue Indizes erstellen. Nachdem ein Paket getrennt wurde, können bestehende Indizes, die das Paket verwendet haben, es nicht mehr verwenden. Sie müssen das Paket aus einem Index entfernen, bevor Sie es trennen können. Andernfalls schlägt die Trennung fehl.

Die Konsole ist die einfachste Methode, um ein Paket von einer Domäne zu trennen und es aus dem Dienst zu entfernen. OpenSearch Wenn Sie ein Paket aus dem OpenSearch Service entfernen, wird es nicht von seinem ursprünglichen Speicherort auf Amazon S3 entfernt.

Trennen Sie ein Paket von einer Domain mit dem AWS Management Console

1. Rufen Sie die Webseite https://aws.amazon.com auf und klicken Sie dann auf Sign In to the Console (Bei der Konsole anmelden).
2. Wählen Sie unter Analytics Amazon OpenSearch Service aus.
3. Wählen Sie im Navigationsbereich Ihre Domäne und dann die Registerkarte Packages (Pakete) aus.
4. Wählen Sie ein Paket aus, klicken Sie dann auf die Option Aktionen und anschließend auf Trennen. Bestätigen Sie Ihre Auswahl.
5. Warten Sie, bis das Paket nicht mehr in der Liste angezeigt wird. Möglicherweise müssen Sie Ihren Browser aktualisieren.
6. Wenn Sie das Paket mit anderen Domänen verwenden möchten, hören Sie hier auf. Um mit dem Entfernen des Pakets fortzufahren (falls es sich um ein benutzerdefiniertes Wörterbuch handelt), wählen Sie im Navigationsbereich Pakete aus.
7. Wählen Sie das Paket und anschließend Delete (Löschen) aus.

Verwenden Sie alternativ die SDKs oder die AWS CLI Konfigurations-API, um Pakete zu trennen und zu entfernen. Weitere Informationen finden Sie in der AWS CLI Befehlsreferenz und der Amazon OpenSearch Service API-Referenz.

Abfragen Ihrer Amazon OpenSearch Service-Daten mit SQL

Sie können SQL verwenden, um Ihren Amazon OpenSearch Service abzufragen, anstatt die JSON-basierte OpenSearch Abfrage DSL zu verwenden. Abfragen mit SQL sind nützlich, wenn Sie bereits mit der Sprache vertraut sind oder Ihre Domain in eine Anwendung integrieren möchten, die sie verwendet. SQL-Unterstützung ist für Domains verfügbar, auf denen Elasticsearch 6.5 OpenSearch oder höher ausgeführt wird.

> **Note**
>
> Diese Dokumentation beschreibt die Versionskompatibilität zwischen OpenSearch Service und verschiedenen Versionen des SQL-Plug-ins sowie des JDBC- und ODBC-Treibers. Informationen zur Syntax für grundlegende und komplexe Abfragen, Funktionen, Metadatenabfragen und Aggregatfunktionen finden Sie in der OpenSearchOpen-Source-Dokumentation.

In der folgenden Tabelle finden Sie die Version des SQL-Plug-ins, die von den einzelnen OpenSearch Elasticsearch-Versionen unterstützt wird.

OpenSearch

OpenSearch Version	SQL-Plug-In-Version	Bemerkenswerte Funktionen
2.13.0	2.13.0.0	
2.11.0	2.11.0.0	Unterstützung für PPL-Sprache und Abfragen hinzufügen
2.9.0	2.9.0.0	Spark-Konnektor hinzufügen und Tabellen- und PromQL-Funktionen unterstützen
2.7.0	2.7.0.0	API hinzufügen `datasource`
2.5.0	2.5.0.0	

OpenSearch Version	SQL-Plug-In-Version	Bemerkenswerte Funktionen
2.3.0	2.3.0.0	Hinzufügen von `maketime`- und `makedate`-Datum- und Uhrzeit-Funktionen
1.3.0	1.3.0.0	Support für standardmäßige Abfragelimitgröße und IN-Klausel zur Auswahl innerhalb einer Werteliste
1.2.0	1.2.0.0	Neues Protokoll für das Visualisierungs-Antwortformat hinzugefügt.
1.1.0	1.1.0.0	Match-Funktion als Filter in SQL und PPL wird unterstützt
1.0.0	1.0.0.0	Support von Abfragen eines Datenstroms

Open Distro für Elasticsearch

Elasticsearch Version	SQL-Plug-In-Version	Bemerkenswerte Funktionen
7.10	1,13,0	NULL FIRST und LAST für Fensterfunktionen, CAST () -Funktion, SHOW- und DESCRIBE-Befehle
7.9	1.11.0	Zusätzliche Datums-/Uhrzeitfunktionen hinzufügen, ORDER BY-Schlüsselwort
7.8	1.9.0	
7.7	1.8.0	
7.3	1.3.0	Mehrere Zeichenfolgen- und Zahlenoperatoren
7.1	1.1.0	

Beispielaufruf

Um Ihre Daten mit SQL abzufragen, senden Sie HTTP-Anforderungen im folgenden Format an `_sql`:

```
POST domain-endpoint/_plugins/_sql
{
  "query": "SELECT * FROM my-index LIMIT 50"
}
```

> **Note**
>
> Wenn auf Ihrer Domain Elasticsearch und nicht ausgeführt wird OpenSearch, lautet das Format. `_opendistro/_sql`

Hinweise und Unterschiede

Aufrufe an `_plugins/_sql` enthalten Indexnamen im Anforderungstext, es gelten also die gleichen Überlegungen zur Zugriffsrichtlinie wie bei den Operationen bulk, mget und msearch. Befolgen Sie wie immer das Prinzip der geringsten Rechte wenn Sie API-Operationen Berechtigungen erteilen.

Sicherheitsüberlegungen bezüglich der Verwendung von SQL mit differenzierter Zugriffskontrolle finden Sie unter Differenzierte Zugriffskontrolle in the section called “Differenzierte Zugriffskontrolle”.

Das OpenSearch SQL-Plugin enthält viele einstellbare Einstellungen. Verwenden Sie im OpenSearch Service den `_cluster/settings` Pfad, nicht den Pfad der Plugin-Einstellungen (`_plugins/_query/settings`):

```
PUT _cluster/settings
{
  "transient" : {
    "plugins.sql.enabled" : true
  }
}
```

Ersetzen Sie für ältere Elasticsearch-Domains `plugins` mit `opendistro`:

```
PUT _cluster/settings
{
  "transient" : {
    "opendistro.sql.enabled" : true
  }
}
```

SQL Workbench

Die SQL Workbench ist eine OpenSearch Dashboard-Benutzeroberfläche, mit der Sie bei Bedarf SQL-Abfragen ausführen, SQL in das REST-Äquivalent übersetzen und Ergebnisse als Text, JSON, JDBC oder CSV anzeigen und speichern können. Weitere Informationen finden Sie unter Workbench abfragen.

SQL CLI

SQL-CLI ist eine eigenständige Python-Anwendung, die Sie mit dem Befehl `opensearchsql` starten können. Schritte zum Installieren, Konfigurieren und Verwenden finden Sie unter SQL CLI.

JDBC-Treiber

Mit dem Java Database Connectivity (JDBC) -Treiber können Sie OpenSearch Service-Domains in Ihre bevorzugten Business Intelligence (BI) -Anwendungen integrieren. Um den Treiber herunterzuladen, klicken Sie hier. Weitere Informationen finden Sie im GitHub Repository.

Die folgenden Tabellen beschreiben die versionsabhängige Kompatibilität des Treibers.

OpenSearch

OpenSearch Version	JDBC-Treiberversion
2.13	1.1.0.1
2.11	1.1.0.1
2.9	1.1.0.1
2.7	1.1.0.1
2.5	1.1.0.1
2.3	1.1.0.1
1.3	1.1.0.1
1.2	1.1.0.1
1.1	1.1.0.1

OpenSearch Version	JDBC-Treiberversion
1,0	1.1.0.1

Open Distro für Elasticsearch

Elasticsearch Version	JDBC-Treiber-Version
7.10	1,13,0
7.9	1.11.0
7.8	1.9.0
7.7	1.8.0
7.4	1.4.0
7.1	1.0.0
6.8	0.9.0
6.7	0.9.0
6,5	0.9.0

ODBC-Treiber

Der Open Database Connectivity (ODBC) -Treiber ist ein schreibgeschützter ODBC-Treiber für Windows und macOS, mit dem Sie Business Intelligence- und Datenvisualisierungsanwendungen wie Microsoft Excel mit dem SQL-Plug-In verbinden können.

Sie können ein Beispiel für eine funktionierende Treiberdatei auf der Seite mit den Artefakten herunterladen. OpenSearch Informationen zur Installation des Treibers finden Sie im SQL-Repository unter GitHub.

k-Nearest Neighbor (k-NN) -Suche in Amazon Service OpenSearch

k-NN für Amazon OpenSearch Service ist die Abkürzung für den zugehörigen k-Nearest Neighbors-Algorithmus und ermöglicht es Ihnen, nach Punkten in einem Vektorraum zu suchen und die „nächsten Nachbarn“ für diese Punkte anhand der euklidischen Entfernung oder der Kosinusähnlichkeit zu finden. Anwendungsfälle umfassen Empfehlungen (z. B. eine Funktion „andere Songs, die Ihnen vielleicht gefallen“ in einer Musikanwendung), Bilderkennung und Betrugserkennung.

> **Note**
>
> Diese Dokumentation beschreibt die Versionskompatibilität zwischen OpenSearch Service und verschiedenen Versionen des k-NN-Plug-ins sowie Einschränkungen bei der Verwendung des Plug-ins mit Managed Service. OpenSearch Eine umfassende Dokumentation des k-NN-Plug-ins, einschließlich einfacher und komplexer Beispiele, Parameterreferenzen und der vollständigen API-Referenz für das Plugin, finden Sie in der OpenSearch Open-Source-Dokumentation. Die Open-Source-Dokumentation behandelt auch die Leistungsoptimierung und k-NN-spezifische Clustereinstellungen.

Verwenden Sie die folgenden Tabellen, um die Version des k-NN-Plug-ins zu finden, das auf Ihrer Amazon OpenSearch Service-Domain läuft. Jede k-NN-Plug-in-Version entspricht einer OpenSearchoder Elasticsearch-Version.

OpenSearch

OpenSearch Version	k-NN-Plug-In-Version	Nennenswerte Funktionen
2.13	2.13.0.0	
2.11	2.11.0.0	Unterstützung für `ignore_unmapped` In-k-NN-Abfragen hinzugefügt
2.9	2.9.0.0	Implementierung von k-NN-Byte-Vektoren und effizientem Filtern mit der Faiss-Engine
2.7	2.7.0.0	

OpenSearch Version	k-NN-Plug-In-Version	Nennenswerte Funktionen
2.5	2.5.0.0	Erweitert SystemIndexPlugin für den k-NN-Modellsystemindex, Lucene-spezifische Dateierweiterungen zum Kern von HybridFS hinzugefügt
2.3	2.3.0.0	
1.3	1.3.0.0	
1.2	1.2.0.0	Unterstützung für Faiss-Bibliothek hinzugefügt
1.1	1.1.0.0	
1,0	1.0.0.0	Umbenannte REST-APIs bei gleichzeitiger Unterstützung der Abwärtskompatibilität, umbenannter Namespace von `opendistro` in `opensearch`

Elasticsearch

Elasticsearch-Version	k-NN-Plug-In-Version	Nennenswerte Funktionen
7.1	1.3.0.0	Euklidische Entfernung
7.4	1.4.0.0	
7.7	1.8.0.0	Kosinusähnlichkeit
7.8	1.9.0.0	
7.9	1.11.0.0	Aufwärm-API, benutzerdefinierte Bewertung
7.10	1.13.0.0	Hamming-Distanz, L1-Norm-Distanz und Painless-Scripting

Erste Schritte mit k-NN

Um k-NN zu verwenden, müssen Sie einen Index mit der `index.knn`-Einstellung erstellen und mindestens ein Feld des `knn_vector`-Datentyps hinzufügen.

```
PUT my-index
{
  "settings": {
    "index.knn": true
  },
  "mappings": {
    "properties": {
      "my_vector1": {
        "type": "knn_vector",
        "dimension": 2
      },
      "my_vector2": {
        "type": "knn_vector",
        "dimension": 4
      }
    }
  }
}
```

Der `knn_vector`-Datentyp unterstützt eine einzelne Liste von bis zu 10.000 Gleitkommazahlen, wobei die Anzahl der Gleitkommazahlen durch den erforderlichen `dimension`-Parameter definiert wird. Nachdem Sie den Index erstellt haben, fügen Sie ihm einige Daten hinzu.

```
POST _bulk
{ "index": { "_index": "my-index", "_id": "1" } }
{ "my_vector1": [1.5, 2.5], "price": 12.2 }
{ "index": { "_index": "my-index", "_id": "2" } }
{ "my_vector1": [2.5, 3.5], "price": 7.1 }
{ "index": { "_index": "my-index", "_id": "3" } }
{ "my_vector1": [3.5, 4.5], "price": 12.9 }
{ "index": { "_index": "my-index", "_id": "4" } }
{ "my_vector1": [5.5, 6.5], "price": 1.2 }
{ "index": { "_index": "my-index", "_id": "5" } }
{ "my_vector1": [4.5, 5.5], "price": 3.7 }
{ "index": { "_index": "my-index", "_id": "6" } }
{ "my_vector2": [1.5, 5.5, 4.5, 6.4], "price": 10.3 }
{ "index": { "_index": "my-index", "_id": "7" } }
```

```
{ "my_vector2": [2.5, 3.5, 5.6, 6.7], "price": 5.5 }
{ "index": { "_index": "my-index", "_id": "8" } }
{ "my_vector2": [4.5, 5.5, 6.7, 3.7], "price": 4.4 }
{ "index": { "_index": "my-index", "_id": "9" } }
{ "my_vector2": [1.5, 5.5, 4.5, 6.4], "price": 8.9 }
```

Dann können Sie die Daten mit dem knn-Abfragetyp durchsuchen.

```
GET my-index/_search
{
  "size": 2,
  "query": {
    "knn": {
      "my_vector2": {
        "vector": [2, 3, 5, 6],
        "k": 2
      }
    }
  }
}
```

In diesem Fall ist k die Anzahl der Nachbarn, die die Abfrage zurückgeben soll, aber Sie müssen auch die `size`-Option einschließen. Andernfalls erhalten Sie k-Ergebnisse für jeden Shard (und jedes Segment) anstatt k-Ergebnisse für die gesamte Abfrage. k-NN unterstützt einen maximalen k-Wert von 10 000.

Wenn Sie die knn-Abfrage mit anderen Klauseln mischen, erhalten Sie möglicherweise weniger als k-Ergebnisse. In diesem Beispiel reduziert die `post_filter`-Klausel die Anzahl der Ergebnisse von 2 auf 1.

```
GET my-index/_search
{
  "size": 2,
  "query": {
    "knn": {
      "my_vector2": {
        "vector": [2, 3, 5, 6],
        "k": 2
      }
    }
  },
  "post_filter": {
```

```
    "range": {
      "price": {
        "gte": 6,
        "lte": 10
      }
    }
  }
}
```

Wenn Sie eine große Anzahl von Abfragen bearbeiten und gleichzeitig eine optimale Leistung beibehalten müssen, können Sie die `_msearch`API verwenden, um eine Massensuche mit JSON zu erstellen und eine einzige Anfrage zu senden, um mehrere Suchen durchzuführen:

```
GET _msearch
{ "index": "my-index"}
{ "query": { "knn": {"my_vector2":{"vector": [2, 3, 5, 6],"k":2 }} } }
{ "index": "my-index", "search_type": "dfs_query_then_fetch"}
{ "query": { "knn": {"my_vector1":{"vector": [2, 3],"k":2 }} } }
```

Das folgende Video zeigt, wie Sie Bulk-Vektorsuchen für K-NN-Abfragen einrichten.

k-NN-Unterschiede, -Optimierung und -Einschränkungen

OpenSearch ermöglicht es Ihnen, alle k-NN-Einstellungen mithilfe der `_cluster/settings` API zu ändern. Bei OpenSearch Service können Sie alle Einstellungen außer `knn.memory.circuit_breaker.enabled` und ändern`knn.circuit_breaker.triggered`. k-NN-Statistiken sind als CloudWatch Amazon-Metriken enthalten.

Vergleichen Sie insbesondere die `KNNGraphMemoryUsage` Metrik auf jedem Datenknoten mit der `knn.memory.circuit_breaker.limit` Statistik und dem verfügbaren RAM für den Instance-Typ. OpenSearch Der Dienst verwendet die Hälfte des RAM einer Instanz für den Java-Heap (bis zu einer Heap-Größe von 32 GiB). Standardmäßig verwendet KNN bis zu 50 % der verbleibenden Hälfte, sodass ein Instance-Typ mit 32 GiB RAM 8 GiB an Graphen (32 * 0,5 * 0,5) aufnehmen kann. Die Leistung kann beeinträchtigt werden, wenn die Nutzung des Graphen-Speichers diesen Wert überschreitet.

Sie können einen k-NN-Index nicht in einen Cold Storage migrieren, UltraWarmwenn der Index ungefähre k-NN () verwendet. `"index.knn": true` Wenn `index.knn` auf `false` gesetzt wird (exakt k-NN), können Sie den Index weiterhin auf andere Speicherstichen verschieben.

Clusterübergreifende Suche in Amazon Service OpenSearch

Mit der clusterübergreifenden Suche in Amazon OpenSearch Service können Sie Abfragen und Aggregationen über mehrere verbundene Domains hinweg durchführen. Es ist oft sinnvoller, mehrere kleinere Domänen anstelle einer einzigen großen Domäne zu verwenden, insbesondere wenn Sie verschiedene Arten von Workloads ausführen.

Mit Workload-spezifischen Domänen können Sie die folgenden Aufgaben ausführen:

- Optimieren Sie jede Domäne durch die Auswahl von Instance-Typen für bestimmte Workloads.
- Richten Sie Grenzen für die Fehlerisolierung über Workloads hinweg ein. Dies bedeutet, dass, wenn einer Ihrer Workloads fehlschlägt, der Fehler in dieser bestimmten Domäne bleibt und sich nicht auf Ihre anderen Workloads auswirkt.
- Skalieren Sie einfacher über Domänen hinweg.

Die clusterübergreifende Suche unterstützt OpenSearch Dashboards, sodass Sie Visualisierungen und Dashboards für alle Ihre Domains erstellen können. Sie zahlen die Standardgebühren für die AWS Datenübertragung für Suchergebnisse, die zwischen Domains übertragen werden.

> **Note**
>
> Open Source bietet OpenSearch auch Dokumentation für die clusterübergreifende Suche. Die Einrichtung unterscheidet sich für Open-Source-Cluster erheblich von denen für verwaltete Amazon OpenSearch Service-Domains. Insbesondere konfigurieren Sie in OpenSearch Service clusterübergreifende Verbindungen mit der und AWS Management Console nicht mit cURL. Zusätzlich zur detaillierten Zugriffskontrolle verwendet der verwaltete Dienst AWS Identity and Access Management (IAM) für die clusterübergreifende Authentifizierung. Daher empfehlen wir, diese Dokumentation und nicht die OpenSearch Open-Source-Dokumentation zu verwenden, um die clusterübergreifende Suche für Ihre Domains zu konfigurieren.

Themen

- Einrichten einer Verbindung
- Entfernen einer Verbindung
- Einrichten von Sicherheit und Beispiel-Walkthrough-Anleitungen
- OpenSearch Dashboards

Einschränkungen

Die Cluster-übergreifende Suche hat mehrere wichtige Einschränkungen:

- Sie können eine Elasticsearch-Domain nicht mit einer OpenSearch Domain verbinden.
- Sie können keine Verbindung zu selbstverwalteten OpenSearch /Elasticsearch-Clustern herstellen.
- Um Domains regionsübergreifend zu verbinden, müssen sich beide Domains auf Elasticsearch 7.10 oder höher oder befinden. OpenSearch
- Eine Domäne kann maximal 20 ausgehende Verbindungen haben. Ebenso kann eine Domäne maximal 20 eingehende Verbindungen haben. Mit anderen Worten, eine Domäne kann sich mit maximal 20 anderen Domänen verbinden.
- Die Quelldomain muss sich in derselben oder einer höheren Version als die Zieldomain befinden. Wenn Sie eine bidirektionale Verbindung zwischen zwei Domänen einrichten und eine oder beide aktualisieren möchten, müssen Sie zuerst eine der Verbindungen löschen.
- Sie können keine benutzerdefinierten Wörterbücher oder SQL mit Cluster-übergreifender Suche verwenden.
- Sie können es nicht verwenden AWS CloudFormation , um Domänen zu verbinden.
- Sie können die Cluster-übergreifende Suche auf M3- oder (T2 und T3) Burstable Instances nicht verwenden.

Voraussetzungen für die Cluster-übergreifende Suche

Bevor Sie die Cluster-übergreifende Suche einrichten, stellen Sie sicher, dass Ihre Domänen die folgenden Anforderungen erfüllen:

- Zwei OpenSearch Domains oder Elasticsearch-Domains in Version 6.7 oder höher
- Differenzierte Zugriffskontrolle aktiviert
- Keine ode-to-node Verschlüsselung aktiviert

Cluster-übergreifende Suche – Preise

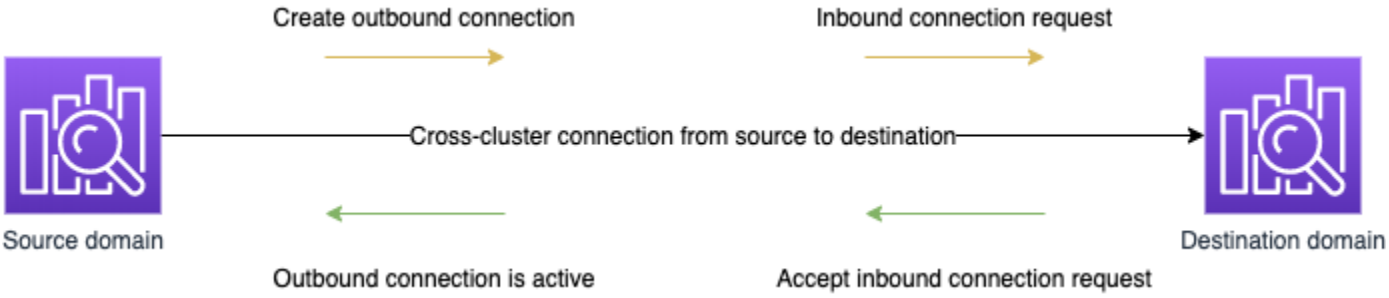
Für die Suche über Domänen hinweg fallen keine zusätzlichen Gebühren an.

Einrichten einer Verbindung

Die Domäne „Quelle“ bezieht sich auf die Domäne, von der eine Cluster-übergreifende Suchabfrage stammt. Mit anderen Worten, die Quelldomäne ist diejenige, an die Sie die erste Suchabfrage senden.

Die Domäne „Ziel“ ist die Domäne, die die Quelldomäne abfragt.

Eine Cluster-übergreifende Verbindung ist unidirektional von der Quelle zur Zieldomäne. Dies bedeutet, dass die Zieldomäne die Quelldomäne nicht abfragen kann. Sie können jedoch eine andere Verbindung in die entgegengesetzte Richtung einrichten.



Die Quelldomäne erstellt eine „ausgehende“ Verbindung zur Zieldomäne. Die Zieldomäne empfängt eine „eingehende“ Verbindungsanforderung von der Quelldomäne.

So richten Sie eine Verbindung ein

1. Wählen Sie im Domänen-Dashboard eine Domäne und anschließend die Registerkarte Verbindungen aus.
2. Wählen Sie im Abschnitt Ausgehende Verbindungen die Option Anforderung.
3. Geben Sie unter Verbindungs-Alias einen Namen für die Verbindung ein.
4. Wählen Sie, ob Sie eine Verbindung zu einer Domain in Ihrer AWS-Konto Region oder zu einem anderen Konto oder einer anderen Region herstellen möchten.

    - Um eine Verbindung zu einem Cluster in Ihrer Region AWS-Konto und Ihrer Region herzustellen, wählen Sie die Domain aus dem Drop-down-Menü aus und wählen Sie Request aus.

- Um eine Verbindung zu einem Cluster in einer anderen Region AWS-Konto oder Region herzustellen, wählen Sie den ARN der Remotedomäne aus und wählen Sie Request. Um Domains regionsübergreifend zu verbinden, müssen auf beiden Domains Elasticsearch Version 7.10 oder höher oder ausgeführt werden. OpenSearch

5. Um nicht verfügbare Cluster für Cluster-Abfragen zu überspringen, wählen Sie Nicht verfügbar überspringen aus. Diese Einstellung stellt sicher, dass Ihre clusterübergreifenden Abfragen trotz Ausfällen auf einem oder mehreren Remoteclustern Teilergebnisse zurückgeben.
6. Die Cluster-übergreifende Suche überprüft zuerst die Verbindungsanforderung, um sicherzustellen, dass die Voraussetzungen erfüllt sind. Wenn die Domänen inkompatibel sind, wechselt die Verbindungsanforderung in den Status `Validation failed`.
7. Nachdem die Verbindungsanforderung erfolgreich validiert wurde, wird sie an die Zieldomäne gesendet, wo sie genehmigt werden muss. Bis diese Genehmigung erfolgt, bleibt die Verbindung im Status `Pending acceptance`. Wenn die Verbindungsanforderung in der Zieldomäne akzeptiert wird, ändert sich der Status in `Active` und die Zieldomäne steht für Abfragen zur Verfügung.

   - Auf der Domänenseite werden die allgemeinen Domänenintegritäts- und Instance-Integritätsdetails Ihrer Zieldomäne angezeigt. Nur Domänenbesitzer haben die Flexibilität, Verbindungen zu oder von ihren Domänen zu erstellen, anzuzeigen, zu entfernen und zu überwachen.

Nachdem die Verbindung hergestellt wurde, wird jeder Datenverkehr, der zwischen den Knoten der verbundenen Domänen fließt, verschlüsselt. Wenn Sie eine VPC-Domäne mit einer Nicht-VPC-Domäne verbinden und die Nicht-VPC-Domäne ein öffentlicher Endpunkt ist, der Datenverkehr aus dem Internet empfangen kann, ist der Cluster-übergreifende Datenverkehr zwischen den Domänen immer noch verschlüsselt und sicher.

Entfernen einer Verbindung

Durch das Entfernen einer Verbindung werden alle clusterübergreifenden Operationen an ihren Indizes gestoppt.

1. Wählen Sie im Domänen-Dashboard die Registerkarte Verbindungen aus.
2. Wählen Sie die Domänenverbindungen aus, die Sie entfernen möchten und klicken Sie auf Löschen, um den Löschvorgang zu bestätigen.

Sie können diese Schritte entweder in der Quell- oder der Zieldomäne ausführen, um die Verbindung zu entfernen. Nachdem Sie die Verbindung entfernt haben, ist sie noch 15 Tage lang mit einem `Deleted`-Status sichtbar.

Sie können eine Domäne mit aktiven Cluster-übergreifenden Verbindungen nicht löschen. Um eine Domäne zu löschen, entfernen Sie zuerst alle eingehenden und ausgehenden Verbindungen aus dieser Domäne. Damit stellen Sie sicher, dass Sie die Benutzer der Cluster-übergreifenden Domäne berücksichtigen, bevor Sie die Domäne löschen.

Einrichten von Sicherheit und Beispiel-Walkthrough-Anleitungen

1. Sie senden eine Cluster-übergreifende Suchabfrage an die Quelldomäne.
2. Die Quelldomäne wertet diese Anforderung anhand ihrer Domänenzugriffsrichtlinie aus. Da die Cluster-übergreifende Suche eine differenzierte Zugriffskontrolle erfordert, wird eine Open-Access-Richtlinie für die Quelldomäne empfohlen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "*"
        ]
      },
      "Action": [
        "es:ESHttp*"
      ],
      "Resource": "arn:aws:es:region:account:domain/src-domain/*"
    }
  ]
}
```

> **Note**
>
> Wenn Sie Remote-Indizes in den Pfad einbeziehen, müssen Sie den URI im Domänen-ARN URL-codieren. Verwenden Sie beispielsweise `arn:aws:es:us-east-1:123456789012:domain/my-domain/`

`local_index,dst%3Aremote_index` anstelle von `arn:aws:es:us-east-1:123456789012:domain/my-domain/local_index,dst:remote_index`.

Wenn Sie zusätzlich zur differenzierten Zugriffskontrolle eine restriktive Zugriffsrichtlinie verwenden möchten, muss Ihre Richtlinie mindestens den Zugriff auf `es:ESHttpGet` zulassen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::123456789012:user/test-user"
        ]
      },
      "Action": "es:ESHttpGet",
      "Resource": "arn:aws:es:region:account:domain/src-domain/*"
    }
  ]
}
```

3. Die differenzierte Zugriffskontrolle für die Quelldomäne wertet die Anforderung aus:

   - Ist die Anforderung mit gültigen IAM- oder HTTP-Basisanmeldeinformationen signiert?
   - Ist dies der Fall, hat der Benutzer die Berechtigung, die Suche durchzuführen und auf die Daten zuzugreifen?

   Wenn die Anforderung nur Daten in der Zieldomäne durchsucht (z. B. `dest-alias:dest-index/_search`), benötigen Sie nur Berechtigungen für die Zieldomäne.

   Wenn die Anforderung Daten in beiden Domänen durchsucht (z. B. `source-index,dest-alias:dest-index/_search`), benötigen Sie Berechtigungen für beide Domänen.

   Bei der detaillierten Zugriffskontrolle müssen Benutzer zusätzlich zu den Standard `read` - oder `search` Berechtigungen für die `indices:admin/shards/search_shards` entsprechenden Indizes auch über die entsprechenden Berechtigungen verfügen.

4. Die Quelldomäne übergibt die Anforderung an die Zieldomäne. Die Zieldomäne wertet diese Anforderung anhand ihrer Domänenzugriffsrichtlinie aus. Sie müssen die `es:ESCrossClusterGet`-Berechtigung für die Zieldomäne angeben:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "es:ESCrossClusterGet",
      "Resource": "arn:aws:es:region:account:domain/dst-domain"
    }
  ]
}
```

Stellen Sie sicher, dass die `es:ESCrossClusterGet`-Berechtigung auf `/dst-domain` und nicht `/dst-domain/*` angewendet wird.

Diese Mindestrichtlinie erlaubt jedoch nur Cluster-übergreifende Suchvorgänge. Wenn Sie andere Operationen ausführen möchten, z. B. das Indizieren von Dokumenten und das Durchführen von Standardsuchvorgängen, benötigen Sie zusätzliche Berechtigungen. Wir empfehlen die folgende Richtlinie für die Zieldomäne:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "*"
        ]
      },
      "Action": [
        "es:ESHttp*"
      ],
      "Resource": "arn:aws:es:region:account:domain/dst-domain/*"
    },
```

```
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "es:ESCrossClusterGet",
      "Resource": "arn:aws:es:region:account:domain/dst-domain"
    }
  ]
}
```

> **Note**
>
> Alle clusterübergreifenden Suchanfragen zwischen Domänen werden bei der Übertragung standardmäßig als Teil der Verschlüsselung verschlüsselt. node-to-node

5. Die Zieldomäne führt die Suche durch und gibt die Ergebnisse an die Quelldomäne zurück.
6. Die Quelldomäne kombiniert ihre eigenen Ergebnisse (falls vorhanden) mit den Ergebnissen der Zieldomäne und gibt sie an Sie zurück.
7. Wir empfehlen Postman für Testanfragen:

   - Indizieren Sie in der Zieldomäne ein Dokument:

     ```
     POST https://dst-domain.us-east-1.es.amazonaws.com/books/_doc/1

     {
       "Dracula": "Bram Stoker"
     }
     ```

   - Wenn Sie diesen Index von der Quelldomäne abfragen möchten, fügen Sie den Verbindungsalias der Zieldomäne in die Abfrage ein.

     ```
     GET https://src-domain.us-east-1.es.amazonaws.com/<connection_alias>:books/
     _search

     {
         ...
       "hits": [
         {
           "_index": "source-destination:books",
           "_type": "_doc",
     ```

```
      "_id": "1",
      "_score": 1,
      "_source": {
        "Dracula": "Bram Stoker"
      }
    }
  ]
}
```

Sie finden den Verbindungsalias auf der Registerkarte Verbindungen in Ihrem Domänen-Dashboard.

- Wenn Sie eine Verbindung zwischen `domain-a -> domain-b` mit dem Verbindungsalias `cluster_b` und `domain-a -> domain-c` mit dem Verbindungsalias `cluster_c` einrichten, suchen Sie `domain-a`, `domain-b` und `domain-c` wie folgt:

```
GET https://src-domain.us-east-1.es.amazonaws.com/
local_index,cluster_b:b_index,cluster_c:c_index/_search
{
  "query": {
    "match": {
      "user": "domino"
    }
  }
}
```

Antwort

```
{
  "took": 150,
  "timed_out": false,
  "_shards": {
    "total": 3,
    "successful": 3,
    "failed": 0,
    "skipped": 0
  },
  "_clusters": {
    "total": 3,
    "successful": 3,
    "skipped": 0
  },
```

```
  "hits": {
    "total": 3,
    "max_score": 1,
    "hits": [
      {
        "_index": "local_index",
        "_type": "_doc",
        "_id": "0",
        "_score": 1,
        "_source": {
          "user": "domino",
          "message": "Lets unite the new mutants",
          "likes": 0
        }
      },
      {
        "_index": "cluster_b:b_index",
        "_type": "_doc",
        "_id": "0",
        "_score": 2,
        "_source": {
          "user": "domino",
          "message": "I'm different",
          "likes": 0
        }
      },
      {
        "_index": "cluster_c:c_index",
        "_type": "_doc",
        "_id": "0",
        "_score": 3,
        "_source": {
          "user": "domino",
          "message": "So am I",
          "likes": 0
        }
      }
    ]
  }
}
```


Wenn Sie sich in Ihrer Verbindungseinrichtung nicht dafür entschieden haben, nicht verfügbare Cluster zu überspringen, müssen alle Zielcluster, die Sie durchsuchen, verfügbar

sein, damit Ihre Suchanfrage erfolgreich ausgeführt werden kann. Andernfalls schlägt die gesamte Anforderung fehl, auch wenn eine der Domänen nicht verfügbar ist, werden keine Suchergebnisse zurückgegeben.

OpenSearch Dashboards

Sie können Daten aus mehreren verbundenen Domänen auf die gleiche Weise visualisieren wie aus einer einzelnen Domäne, dafür müssen Sie jedoch auf die Remote-Indizes mit `connection-alias:index` zugreifen. Ihr Indexmuster muss also mit `connection-alias:index` übereinstimmen.

Lernen, für Amazon OpenSearch Service zu ranken

OpenSearch verwendet ein probabilistisches Ranking-Framework namens BM-25, um Relevanzwerte zu berechnen. Wenn ein markantes Schlüsselwort häufiger in einem Dokument erscheint, weist BM-25 diesem Dokument eine höhere Relevanzbewertung zu. Dieses Framework berücksichtigt jedoch Benutzerverhalten wie Click-Through-Daten nicht, was die Relevanz weiter verbessern könnte.

Learning to Rank ist ein Open-Source-Plug-In, mit dem Sie mittels Machine Learning und Verhaltensdaten die Relevanz von Dokumenten optimieren können. Es verwendet Modelle aus den XGBoost- und Ranklib-Bibliotheken, um die Suchergebnisse erneut zu bewerten. Das Elasticsearch LTR-Plugin wurde ursprünglich von OpenSource Connections entwickelt, wobei wichtige Beiträge von der Wikimedia Foundation, Snagajob Engineering, Bonsai und Yelp Engineering geleistet wurden. Die OpenSearch Version des Plugins ist vom Elasticsearch LTR-Plugin abgeleitet.

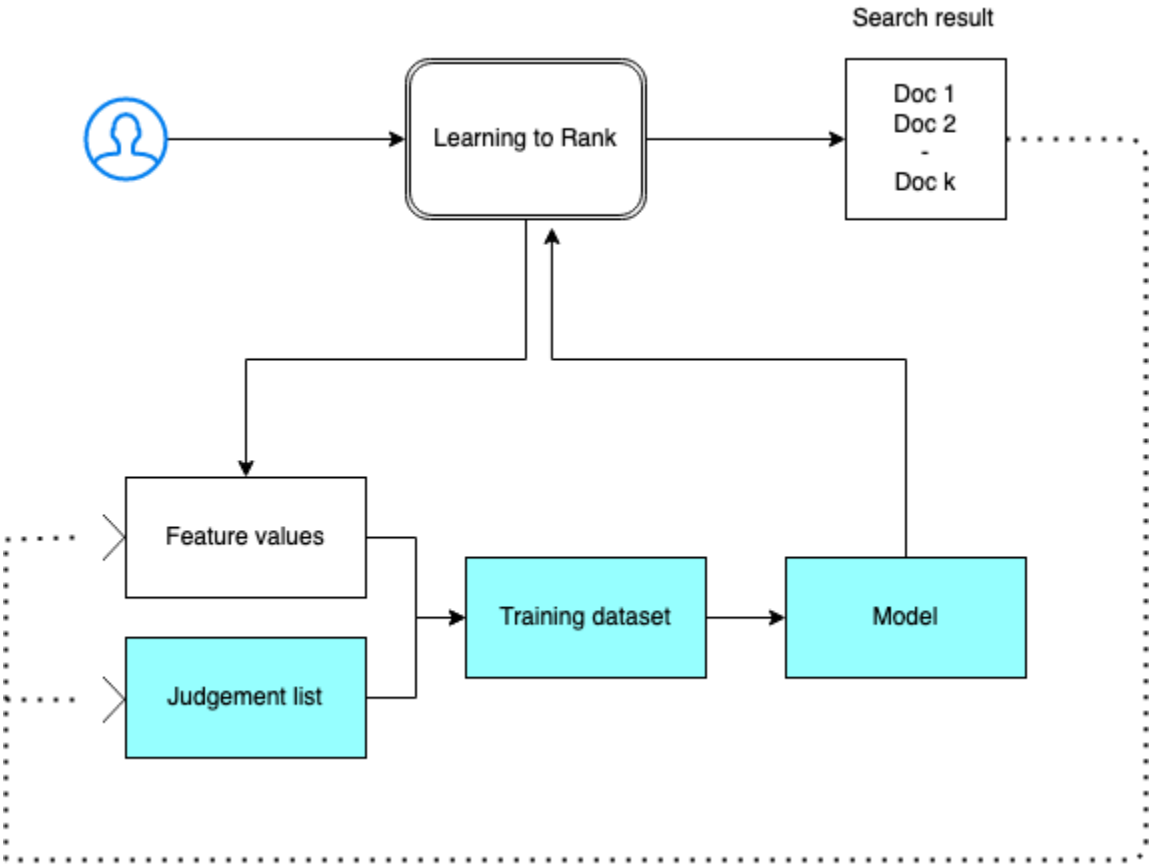
Für Learning to Rank ist Elasticsearch 7.7 OpenSearch oder höher erforderlich. Um das Plug-In „Learning to Rank“ verwenden zu können, benötigen Sie volle Administratorberechtigungen. Weitere Informationen hierzu finden Sie unter the section called “Hauptbenutzer ändern”.

> **Note**
>
> Diese Dokumentation bietet einen allgemeinen Überblick über das Learning to Rank-Plugin und hilft Ihnen bei den ersten Schritten. Die vollständige Dokumentation, einschließlich detaillierter Schritte und API-Beschreibungen, finden Sie in der Dokumentation Learning to Rank.

Themen

Erste Schritte mit Learning to Rank

Sie müssen eine Beurteilungsliste bereitstellen, einen Trainingsdatensatz erstellen und das Modell außerhalb von Amazon OpenSearch Service trainieren. Die blau markierten Teile kommen außerhalb von OpenSearch Service vor:



Schritt 1: Initialisieren des Plug-Ins

Um das Learning to Rank-Plugin zu initialisieren, senden Sie die folgende Anfrage an Ihre OpenSearch Service-Domain:

```
PUT _ltr
```

```
{
```

```
  "acknowledged" : true,
  "shards_acknowledged" : true,
  "index" : ".ltrstore"
}
```

Mit diesem Befehl wird ein ausgeblendeter `.ltrstore`-Index erstellt, in dem Metadateninformationen wie Funktions-Sets und Modelle gespeichert werden.

Schritt 2: Erstellen einer Urteilliste

> **Note**
>
> Sie müssen diesen Schritt außerhalb von OpenSearch Service ausführen.

Eine Urteilsliste ist eine Sammlung von Beispielen, von denen ein Machine-Learning-Modell lernt. Ihre Urteilsliste sollte Schlüsselwörter enthalten, die für Sie wichtig sind und eine Reihe von bewerteten Dokumenten für jedes Schlüsselwort.

In diesem Beispiel haben wir eine Urteilsliste für einen Film-Datensatz. Eine Bewertung von 4 weist auf eine perfekte Übereinstimmung hin. Eine Bewertung von 0 gibt die schlechteste Übereinstimmung an.

Bewertung	Stichwort	Dokument-ID	Filmname
4	rambo	7555	Rambo
3	rambo	1370	Rambo III
3	rambo	1369	Rambo: First Blood Teil II
3	rambo	1368	First Blood

Erstellen Sie Ihre Urteilsliste im folgenden Format:

```
4 qid:1 # 7555 Rambo
3 qid:1 # 1370 Rambo III
3 qid:1 # 1369 Rambo: First Blood Part II
```

```
3 qid:1 # 1368 First Blood

where qid:1 represents "rambo"
```

Ein umfassendes Beispiel für eine Urteilliste finden Sie unter Film-Urteile.

Sie können diese Urteilsliste manuell mit Hilfe von menschlichen Kommentatoren erstellen oder sie programmgesteuert aus Analysedaten ableiten.

Schritt 3: Erstellen eines Funktionssets

Eine Funktion ist ein Feld, das der Relevanz eines Dokuments entspricht, z. B. `title`, `overview`, `popularity score` (Anzahl der Ansichten) usw.

Erstellen Sie für jede Funktion einen Funktionssatz mit einer Mustache-Vorlage. Weitere Informationen zu Funktionen finden Sie unter Arbeiten mit Funktionen.

In diesem Beispiel erstellen wir einen `movie_features`-Funktionssatz mit den Feldern `title` und`overview`:

```
POST _ltr/_featureset/movie_features
{
  "featureset" : {
      "name" : "movie_features",
      "features" : [
        {
          "name" : "1",
          "params" : [
            "keywords"
          ],
          "template_language" : "mustache",
          "template" : {
            "match" : {
              "title" : "{{keywords}}"
            }
          }
        },
        {
          "name" : "2",
          "params" : [
            "keywords"
          ],
          "template_language" : "mustache",
```

```
          "template" : {
            "match" : {
              "overview" : "{{keywords}}"
            }
          }
        }
      ]
    }
}
```

Wenn Sie den ursprünglichen `.ltrstore`-Index verwenden, erhalten Sie Ihren Funktionsatz zurück:

```
GET _ltr/_featureset
```

Schritt 4: Protokollieren der Funktionswerte

Die Funktionswerte sind die Relevanzwerte, die von BM-25 für jede Funktion berechnet werden.

Kombinieren Sie den Funktionsatz und die Beurteilungsliste, um die Funktionswerte zu protokollieren. Weitere Informationen zur Protokollierung finden Sie unter Protokollieren von Funktionssätzen.

In diesem Beispiel ruft die `bool`-Abfrage die bewerteten Dokumente mit dem Filter ab und wählt dann den Funktionssatz mit der `sltr`-Abfrage aus. Die `ltr_log`-Abfrage kombiniert die Dokumente und die Funktionen, um die entsprechenden Funktionswerte zu protokollieren:

```
POST tmdb/_search
{
  "_source": {
    "includes": [
      "title",
      "overview"
    ]
  },
  "query": {
    "bool": {
      "filter": [
        {
          "terms": {
            "_id": [
              "7555",
              "1370",
              "1369",
```

```
              "1368"
            ]
          }
        },
        {
          "sltr": {
            "_name": "logged_featureset",
            "featureset": "movie_features",
            "params": {
              "keywords": "rambo"
            }
          }
        }
      ]
    }
  },
  "ext": {
    "ltr_log": {
      "log_specs": {
        "name": "log_entry1",
        "named_query": "logged_featureset"
      }
    }
  }
}
```

Eine Beispielantwort kann wie folgt aussehen:

```
{
  "took" : 7,
  "timed_out" : false,
  "_shards" : {
    "total" : 1,
    "successful" : 1,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : {
      "value" : 4,
      "relation" : "eq"
    },
    "max_score" : 0.0,
```

```
    "hits" : [
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "1368",
        "_score" : 0.0,
        "_source" : {
          "overview" : "When former Green Beret John Rambo is harassed by local law
enforcement and arrested for vagrancy, the Vietnam vet snaps, runs for the hills and
rat-a-tat-tats his way into the action-movie hall of fame. Hounded by a relentless
sheriff, Rambo employs heavy-handed guerilla tactics to shake the cops off his tail.",
          "title" : "First Blood"
        },
        "fields" : {
          "_ltrlog" : [
            {
              "log_entry1" : [
                {
                  "name" : "1"
                },
                {
                  "name" : "2",
                  "value" : 10.558305
                }
              ]
            }
          ]
        },
        "matched_queries" : [
          "logged_featureset"
        ]
      },
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "7555",
        "_score" : 0.0,
        "_source" : {
          "overview" : "When governments fail to act on behalf of captive missionaries,
ex-Green Beret John James Rambo sets aside his peaceful existence along the Salween
River in a war-torn region of Thailand to take action.  Although he's still haunted
by violent memories of his time as a U.S. soldier during the Vietnam War, Rambo can
hardly turn his back on the aid workers who so desperately need his help.",
          "title" : "Rambo"
```

```
        },
        "fields" : {
          "_ltrlog" : [
            {
              "log_entry1" : [
                {
                  "name" : "1",
                  "value" : 11.2569065
                },
                {
                  "name" : "2",
                  "value" : 9.936821
                }
              ]
            }
          ]
        },
        "matched_queries" : [
          "logged_featureset"
        ]
      },
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "1369",
        "_score" : 0.0,
        "_source" : {
          "overview" : "Col. Troutman recruits ex-Green Beret John Rambo for a highly
secret and dangerous mission. Teamed with Co Bao, Rambo goes deep into Vietnam to
rescue POWs. Deserted by his own team, he's left in a hostile jungle to fight for his
life, avenge the death of a woman and bring corrupt officials to justice.",
          "title" : "Rambo: First Blood Part II"
        },
        "fields" : {
          "_ltrlog" : [
            {
              "log_entry1" : [
                {
                  "name" : "1",
                  "value" : 6.334839
                },
                {
                  "name" : "2",
                  "value" : 10.558305
```

```
              }
            ]
          }
        ]
      },
      "matched_queries" : [
        "logged_featureset"
      ]
    },
    {
      "_index" : "tmdb",
      "_type" : "movie",
      "_id" : "1370",
      "_score" : 0.0,
      "_source" : {
        "overview" : "Combat has taken its toll on Rambo, but he's finally begun to
find inner peace in a monastery. When Rambo's friend and mentor Col. Trautman asks for
his help on a top secret mission to Afghanistan, Rambo declines but must reconsider
when Trautman is captured.",
        "title" : "Rambo III"
      },
      "fields" : {
        "_ltrlog" : [
          {
            "log_entry1" : [
              {
                "name" : "1",
                "value" : 9.425955
              },
              {
                "name" : "2",
                "value" : 11.262714
              }
            ]
          }
        ]
      },
      "matched_queries" : [
        "logged_featureset"
      ]
    }
  ]
}
```

```
}
```

Im vorherigen Beispiel hat die erste Funktion keinen Funktionswert, da das Schlüsselwort „rambo“ nicht im Titelfeld des Dokuments mit einer ID 1368 angezeigt wird. Dies ist ein fehlender Funktionswert in den Trainingsdaten.

Schritt 5: Erstellen eines Trainingdatensatzes

> **Note**
>
> Sie müssen diesen Schritt außerhalb von OpenSearch Service ausführen.

Der nächste Schritt besteht darin, die Beurteilungsliste und die Funktionswerte zu kombinieren, um einen Trainingsdatensatz zu erstellen. Wenn Ihre ursprüngliche Urteilsliste wie folgt aussieht:

```
4 qid:1 # 7555 Rambo
3 qid:1 # 1370 Rambo III
3 qid:1 # 1369 Rambo: First Blood Part II
3 qid:1 # 1368 First Blood
```

Konvertieren Sie sie in den abschließenden Trainingsdatensatz, der wie folgt aussieht:

```
4 qid:1 1:12.318474 2:10.573917 # 7555 rambo
3 qid:1 1:10.357875 2:11.950391 # 1370 rambo
3 qid:1 1:7.010513 2:11.220095 # 1369 rambo
3 qid:1 1:0.0 2:11.220095 # 1368 rambo
```

Sie können diesen Schritt manuell ausführen oder ein Programm schreiben, um es zu automatisieren.

Schritt 6: Einen Algorithmus auswählen und das Modell erstellen

> **Note**
>
> Sie müssen diesen Schritt außerhalb des OpenSearch Dienstes ausführen.

Wenn der Trainingsdatensatz vorhanden ist, besteht der nächste Schritt darin, XGBoost- oder Ranklib-Bibliotheken zum Erstellen eines Modells zu verwenden. Mit XGBoost und Ranklib-Bibliotheken können Sie beliebte Modelle wie LambdaMart, Random Forest usw. erstellen.

Anweisungen zur Verwendung von XGBoost und Ranklib zum Erstellen des Modells finden Sie in XGBoost bzw. in der Dokumentation. RankLib Informationen zur Verwendung von Amazon SageMaker zum Erstellen des XGBoost-Modells finden Sie unter XGBoost-Algorithmus.

Schritt 7: Bereitstellen des Modells

Nachdem Sie das Modell erstellt haben, stellen Sie es im Plug-In „Learning to Rank“ bereit. Weitere Informationen zur Bereitstellung eines Modells finden Sie unter Hochladen eines trainierten Modells.

In diesem Beispiel erstellen wir ein `my_ranklib_model`-Modell mit der Ranklib-Bibliothek:

```
POST _ltr/_featureset/movie_features/_createmodel?pretty
{
  "model": {
    "name": "my_ranklib_model",
    "model": {
      "type": "model/ranklib",
      "definition": """## LambdaMART
## No. of trees = 10
## No. of leaves = 10
## No. of threshold candidates = 256
## Learning rate = 0.1
## Stop early = 100

<ensemble>
   <tree id="1" weight="0.1">
      <split>
         <feature>1</feature>
         <threshold>10.357875</threshold>
         <split pos="left">
            <feature>1</feature>
            <threshold>0.0</threshold>
            <split pos="left">
               <output>-2.0</output>
            </split>
            <split pos="right">
               <feature>1</feature>
               <threshold>7.010513</threshold>
               <split pos="left">
                  <output>-2.0</output>
               </split>
               <split pos="right">
                  <output>-2.0</output>
```

```
            </split>
         </split>
      </split>
      <split pos="right">
         <output>2.0</output>
      </split>
   </split>
</tree>
<tree id="2" weight="0.1">
   <split>
      <feature>1</feature>
      <threshold>10.357875</threshold>
      <split pos="left">
         <feature>1</feature>
         <threshold>0.0</threshold>
         <split pos="left">
            <output>-1.67031991481781</output>
         </split>
         <split pos="right">
            <feature>1</feature>
            <threshold>7.010513</threshold>
            <split pos="left">
               <output>-1.67031991481781</output>
            </split>
            <split pos="right">
               <output>-1.6703200340270996</output>
            </split>
         </split>
      </split>
      <split pos="right">
         <output>1.6703201532363892</output>
      </split>
   </split>
</tree>
<tree id="3" weight="0.1">
   <split>
      <feature>2</feature>
      <threshold>10.573917</threshold>
      <split pos="left">
         <output>1.479954481124878</output>
      </split>
      <split pos="right">
         <feature>1</feature>
         <threshold>7.010513</threshold>
```

```
            <split pos="left">
               <feature>1</feature>
               <threshold>0.0</threshold>
               <split pos="left">
                  <output>-1.4799546003341675</output>
               </split>
               <split pos="right">
                  <output>-1.479954481124878</output>
               </split>
            </split>
            <split pos="right">
               <output>-1.479954481124878</output>
            </split>
         </split>
      </split>
   </tree>
   <tree id="4" weight="0.1">
      <split>
         <feature>1</feature>
         <threshold>10.357875</threshold>
         <split pos="left">
            <feature>1</feature>
            <threshold>0.0</threshold>
            <split pos="left">
               <output>-1.3569872379302979</output>
            </split>
            <split pos="right">
               <feature>1</feature>
               <threshold>7.010513</threshold>
               <split pos="left">
                  <output>-1.3569872379302979</output>
               </split>
               <split pos="right">
                  <output>-1.3569872379302979</output>
               </split>
            </split>
         </split>
         <split pos="right">
            <output>1.3569873571395874</output>
         </split>
      </split>
   </tree>
   <tree id="5" weight="0.1">
      <split>
```

```
         <feature>1</feature>
         <threshold>10.357875</threshold>
         <split pos="left">
            <feature>1</feature>
            <threshold>0.0</threshold>
            <split pos="left">
               <output>-1.2721362113952637</output>
            </split>
            <split pos="right">
               <feature>1</feature>
               <threshold>7.010513</threshold>
               <split pos="left">
                  <output>-1.2721363306045532</output>
               </split>
               <split pos="right">
                  <output>-1.2721363306045532</output>
               </split>
            </split>
         </split>
         <split pos="right">
            <output>1.2721362113952637</output>
         </split>
      </split>
   </tree>
   <tree id="6" weight="0.1">
      <split>
         <feature>1</feature>
         <threshold>10.357875</threshold>
         <split pos="left">
            <feature>1</feature>
            <threshold>7.010513</threshold>
            <split pos="left">
               <feature>1</feature>
               <threshold>0.0</threshold>
               <split pos="left">
                  <output>-1.2110036611557007</output>
               </split>
               <split pos="right">
                  <output>-1.2110036611557007</output>
               </split>
            </split>
            <split pos="right">
               <output>-1.2110037803649902</output>
            </split>
```

```
         </split>
         <split pos="right">
            <output>1.2110037803649902</output>
         </split>
      </split>
   </tree>
   <tree id="7" weight="0.1">
      <split>
         <feature>1</feature>
         <threshold>10.357875</threshold>
         <split pos="left">
            <feature>1</feature>
            <threshold>7.010513</threshold>
            <split pos="left">
               <feature>1</feature>
               <threshold>0.0</threshold>
               <split pos="left">
                  <output>-1.165616512298584</output>
               </split>
               <split pos="right">
                  <output>-1.165616512298584</output>
               </split>
            </split>
            <split pos="right">
               <output>-1.165616512298584</output>
            </split>
         </split>
         <split pos="right">
            <output>1.165616512298584</output>
         </split>
      </split>
   </tree>
   <tree id="8" weight="0.1">
      <split>
         <feature>1</feature>
         <threshold>10.357875</threshold>
         <split pos="left">
            <feature>1</feature>
            <threshold>7.010513</threshold>
            <split pos="left">
               <feature>1</feature>
               <threshold>0.0</threshold>
               <split pos="left">
                  <output>-1.131177544593811</output>
```

```
            </split>
            <split pos="right">
               <output>-1.131177544593811</output>
            </split>
         </split>
         <split pos="right">
            <output>-1.131177544593811</output>
         </split>
      </split>
      <split pos="right">
         <output>1.131177544593811</output>
      </split>
   </split>
</tree>
<tree id="9" weight="0.1">
   <split>
      <feature>2</feature>
      <threshold>10.573917</threshold>
      <split pos="left">
         <output>1.1046180725097656</output>
      </split>
      <split pos="right">
         <feature>1</feature>
         <threshold>7.010513</threshold>
         <split pos="left">
            <feature>1</feature>
            <threshold>0.0</threshold>
            <split pos="left">
               <output>-1.1046180725097656</output>
            </split>
            <split pos="right">
               <output>-1.1046180725097656</output>
            </split>
         </split>
         <split pos="right">
            <output>-1.1046180725097656</output>
         </split>
      </split>
   </split>
</tree>
<tree id="10" weight="0.1">
   <split>
      <feature>1</feature>
      <threshold>10.357875</threshold>
```

```
         <split pos="left">
            <feature>1</feature>
            <threshold>7.010513</threshold>
            <split pos="left">
               <feature>1</feature>
               <threshold>0.0</threshold>
               <split pos="left">
                  <output>-1.0838804244995117</output>
               </split>
               <split pos="right">
                  <output>-1.0838804244995117</output>
               </split>
            </split>
            <split pos="right">
               <output>-1.0838804244995117</output>
            </split>
         </split>
         <split pos="right">
            <output>1.0838804244995117</output>
         </split>
      </split>
   </tree>
</ensemble>
"""
    }
  }
}
```

Um das Modell zu sehen, senden Sie die folgende Anfrage:

```
GET _ltr/_model/my_ranklib_model
```

Schritt 8: Suchen mit Learning to Rank

Nach der Bereitstellung des Modells können Sie suchen.

Führen Sie die `sltr`-Abfrage mit den verwendeten Funktionen und dem Namen des Modells aus, das Sie ausführen möchten:

```
POST tmdb/_search
{
  "_source": {
```

```
    "includes": ["title", "overview"]
  },
  "query": {
    "multi_match": {
      "query": "rambo",
      "fields": ["title", "overview"]
    }
  },
  "rescore": {
    "query": {
      "rescore_query": {
        "sltr": {
          "params": {
            "keywords": "rambo"
          },
          "model": "my_ranklib_model"
        }
      }
    }
  }
}
```

Mit „Learning to Ranking“ sehen Sie „Rambo“ als erstes Ergebnis, da wir ihm die höchste Bewertung in der Urteilsliste zugewiesen haben:

```
{
  "took" : 12,
  "timed_out" : false,
  "_shards" : {
    "total" : 1,
    "successful" : 1,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : {
      "value" : 7,
      "relation" : "eq"
    },
    "max_score" : 13.096414,
    "hits" : [
      {
        "_index" : "tmdb",
```

```
        "_type" : "movie",
        "_id" : "7555",
        "_score" : 13.096414,
        "_source" : {
          "overview" : "When governments fail to act on behalf of captive missionaries,
ex-Green Beret John James Rambo sets aside his peaceful existence along the Salween
River in a war-torn region of Thailand to take action.  Although he's still haunted
by violent memories of his time as a U.S. soldier during the Vietnam War, Rambo can
hardly turn his back on the aid workers who so desperately need his help.",
          "title" : "Rambo"
        }
      },
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "1370",
        "_score" : 11.17245,
        "_source" : {
          "overview" : "Combat has taken its toll on Rambo, but he's finally begun to
find inner peace in a monastery. When Rambo's friend and mentor Col. Trautman asks for
his help on a top secret mission to Afghanistan, Rambo declines but must reconsider
when Trautman is captured.",
          "title" : "Rambo III"
        }
      },
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "1368",
        "_score" : 10.442155,
        "_source" : {
          "overview" : "When former Green Beret John Rambo is harassed by local law
enforcement and arrested for vagrancy, the Vietnam vet snaps, runs for the hills and
rat-a-tat-tats his way into the action-movie hall of fame. Hounded by a relentless
sheriff, Rambo employs heavy-handed guerilla tactics to shake the cops off his tail.",
          "title" : "First Blood"
        }
      },
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "1369",
        "_score" : 10.442155,
        "_source" : {
```

```
        "overview" : "Col. Troutman recruits ex-Green Beret John Rambo for a highly
secret and dangerous mission. Teamed with Co Bao, Rambo goes deep into Vietnam to
rescue POWs. Deserted by his own team, he's left in a hostile jungle to fight for his
life, avenge the death of a woman and bring corrupt officials to justice.",
        "title" : "Rambo: First Blood Part II"
      }
    },
    {
      "_index" : "tmdb",
      "_type" : "movie",
      "_id" : "31362",
      "_score" : 7.424202,
      "_source" : {
        "overview" : "It is 1985, and a small, tranquil Florida town is being rocked
by a wave of vicious serial murders and bank robberies. Particularly sickening to the
authorities is the gratuitous use of violence by two “Rambo” like killers who dress
themselves in military garb. Based on actual events taken from FBI files, the movie
depicts the Bureau’s efforts to track down these renegades.",
        "title" : "In the Line of Duty: The F.B.I. Murders"
      }
    },
    {
      "_index" : "tmdb",
      "_type" : "movie",
      "_id" : "13258",
      "_score" : 6.43182,
      "_source" : {
        "overview" : """Will Proudfoot (Bill Milner) is looking for an escape from
his family's stifling home life when he encounters Lee Carter (Will Poulter), the
school bully. Armed with a video camera and a copy of "Rambo: First Blood", Lee plans
to make cinematic history by filming his own action-packed video epic. Together, these
two newfound friends-turned-budding-filmmakers quickly discover that their imaginative
– and sometimes mishap-filled – cinematic adventure has begun to take on a life of its
own!""",
        "title" : "Son of Rambow"
      }
    },
    {
      "_index" : "tmdb",
      "_type" : "movie",
      "_id" : "61410",
      "_score" : 3.9719706,
      "_source" : {
```

```
          "overview" : "It's South Africa 1990. Two major events are about to happen:
 The release of Nelson Mandela and, more importantly, it's Spud Milton's first year
 at an elite boys only private boarding school. John Milton is a boy from an ordinary
 background who wins a scholarship to a private school in Kwazulu-Natal, South Africa.
 Surrounded by boys with nicknames like Gecko, Rambo, Rain Man and Mad Dog, Spud has
 his hands full trying to adapt to his new home. Along the way Spud takes his first
 tentative steps along the path to manhood. (The path it seems could be a rather long
 road). Spud is an only child. He is cursed with parents from well beyond the lunatic
 fringe and a senile granny. His dad is a fervent anti-communist who is paranoid that
 the family domestic worker is running a shebeen from her room at the back of the
 family home. His mom is a free spirit and a teenager's worst nightmare, whether it's
 shopping for Spud's underwear in the local supermarket",
          "title" : "Spud"
        }
      }
    ]
  }
}
```

Wenn Sie suchen, ohne das Learning to Rank-Plugin zu verwenden, OpenSearch werden unterschiedliche Ergebnisse zurückgegeben:

```
POST tmdb/_search
{
  "_source": {
    "includes": ["title", "overview"]
  },
  "query": {
    "multi_match": {
      "query": "Rambo",
      "fields": ["title", "overview"]
    }
  }
}
```

```
{
  "took" : 5,
  "timed_out" : false,
  "_shards" : {
    "total" : 1,
    "successful" : 1,
    "skipped" : 0,
    "failed" : 0
```

```
 },
 "hits" : {
   "total" : {
     "value" : 5,
     "relation" : "eq"
   },
   "max_score" : 11.262714,
   "hits" : [
     {
       "_index" : "tmdb",
       "_type" : "movie",
       "_id" : "1370",
       "_score" : 11.262714,
       "_source" : {
         "overview" : "Combat has taken its toll on Rambo, but he's finally begun to
find inner peace in a monastery. When Rambo's friend and mentor Col. Trautman asks for
his help on a top secret mission to Afghanistan, Rambo declines but must reconsider
when Trautman is captured.",
         "title" : "Rambo III"
       }
     },
     {
       "_index" : "tmdb",
       "_type" : "movie",
       "_id" : "7555",
       "_score" : 11.2569065,
       "_source" : {
         "overview" : "When governments fail to act on behalf of captive missionaries,
ex-Green Beret John James Rambo sets aside his peaceful existence along the Salween
River in a war-torn region of Thailand to take action.  Although he's still haunted
by violent memories of his time as a U.S. soldier during the Vietnam War, Rambo can
hardly turn his back on the aid workers who so desperately need his help.",
         "title" : "Rambo"
       }
     },
     {
       "_index" : "tmdb",
       "_type" : "movie",
       "_id" : "1368",
       "_score" : 10.558305,
       "_source" : {
         "overview" : "When former Green Beret John Rambo is harassed by local law
enforcement and arrested for vagrancy, the Vietnam vet snaps, runs for the hills and
```

```
 rat-a-tat-tats his way into the action-movie hall of fame. Hounded by a relentless
 sheriff, Rambo employs heavy-handed guerilla tactics to shake the cops off his tail.",
          "title" : "First Blood"
        }
      },
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "1369",
        "_score" : 10.558305,
        "_source" : {
          "overview" : "Col. Troutman recruits ex-Green Beret John Rambo for a highly
 secret and dangerous mission. Teamed with Co Bao, Rambo goes deep into Vietnam to
 rescue POWs. Deserted by his own team, he's left in a hostile jungle to fight for his
 life, avenge the death of a woman and bring corrupt officials to justice.",
          "title" : "Rambo: First Blood Part II"
        }
      },
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "13258",
        "_score" : 6.4600153,
        "_source" : {
          "overview" : """Will Proudfoot (Bill Milner) is looking for an escape from
 his family's stifling home life when he encounters Lee Carter (Will Poulter), the
 school bully. Armed with a video camera and a copy of "Rambo: First Blood", Lee plans
 to make cinematic history by filming his own action-packed video epic. Together, these
 two newfound friends-turned-budding-filmmakers quickly discover that their imaginative
 – and sometimes mishap-filled – cinematic adventure has begun to take on a life of its
 own!""",
          "title" : "Son of Rambow"
        }
      }
    ]
  }
}
```

Passen Sie die Beurteilungsliste und die Funktionen an, je nachdem, wie gut das Modell Ihrer Meinung nach funktioniert. Wiederholen Sie anschließend die Schritte 2 bis 8, um die Ranglistenergebnisse im Laufe der Zeit zu verbessern.

Learning-to-Rank-API

Verwenden Sie die Operationen „Learning to Rank“, um programmgesteuert mit Funktionssätzen und Modellen zu arbeiten.

Shop erstellen

Es wird ein ausgeblendeter `.ltrstore`-Index erstellt, in dem Metadateninformationen wie Funktionssätze und Modelle gespeichert werden.

```
PUT _ltr
```

Shop löschen

Löscht den versteckten `.ltrstore`-Index und setzt das Plug-In zurück.

```
DELETE _ltr
```

Erstellen eines Funktionssatzes

Erstellt einen Funktionssatz.

```
POST _ltr/_featureset/<name_of_features>
```

Löschen eines Funktionssatzes

Löscht einen Funktionssatz.

```
DELETE _ltr/_featureset/<name_of_feature_set>
```

Abrufen eines Funktionssatzes

Ruft einen Funktionssatz ab.

```
GET _ltr/_featureset/<name_of_feature_set>
```

Erstellen eines Modells

Erstellt ein Modell.

```
POST _ltr/_featureset/<name_of_feature_set>/_createmodel
```

Löschen eines Modells

Löscht ein Modell.

```
DELETE _ltr/_model/<name_of_model>
```

Abrufen eines Modells

Ruft ein Modell ab.

```
GET _ltr/_model/<name_of_model>
```

Statistiken abrufen

Enthält Informationen darüber, wie sich das Plug-In verhält.

```
GET _ltr/_stats
```

Du kannst auch Filter verwenden, um eine einzelne Statistik abzurufen:

```
GET _ltr/_stats/<stat>
```

Darüber hinaus können Sie die Informationen auf einen einzelnen Knoten im Cluster beschränken:

```
GET _ltr/_stats/<stat>/nodes/<nodeId>

{
  "_nodes" : {
    "total" : 1,
    "successful" : 1,
    "failed" : 0
  },
  "cluster_name" : "873043598401:ltr-77",
  "stores" : {
    ".ltrstore" : {
      "model_count" : 1,
      "featureset_count" : 1,
      "feature_count" : 2,
```

```
      "status" : "green"
    }
  },
  "status" : "green",
  "nodes" : {
    "DjelK-_ZSfyzstO5dhGGQA" : {
      "cache" : {
        "feature" : {
          "eviction_count" : 0,
          "miss_count" : 0,
          "entry_count" : 0,
          "memory_usage_in_bytes" : 0,
          "hit_count" : 0
        },
        "featureset" : {
          "eviction_count" : 2,
          "miss_count" : 2,
          "entry_count" : 0,
          "memory_usage_in_bytes" : 0,
          "hit_count" : 0
        },
        "model" : {
          "eviction_count" : 2,
          "miss_count" : 3,
          "entry_count" : 1,
          "memory_usage_in_bytes" : 3204,
          "hit_count" : 1
        }
      },
      "request_total_count" : 6,
      "request_error_count" : 0
    }
  }
}
```

Die Statistiken werden auf zwei Ebenen, Knoten und Cluster, bereitgestellt, wie in den folgenden Tabellen angegeben:

Statistiken auf Knotenebene

Feldname	Beschreibung
request_total_count	Gesamtzahl der Ranking-Anforderungen.

Feldname	Beschreibung
request_error_count	Gesamtzahl der fehlgeschlagenen Anforderungen.
Cache	Statistiken über alle Caches hinweg (Funktionen, Funktionssätze, Modelle). Ein Cache-Treffer tritt auf, wenn ein Benutzer das Plug-In abfragt und das Modell bereits in den Speicher geladen ist.
cache.eviction_count	Anzahl der Cache-Bereinigungen.
cache.hit_count	Anzahl der Cache-Treffer.
cache.miss_count	Anzahl der Cache-Fehler. Ein Cache-Fehler tritt auf, wenn ein Benutzer das Plug-In abfragt und das Modell noch nicht in den Speicher geladen ist.
cache.entry_count	Anzahl der Einträge im Cache.
cache.memory_usage_in_bytes	Gesamtspeicher, der in Bytes verwendet wird.
cache.cache_capacity_reached	Gibt an, ob das Cache-Limit erreicht ist.

Cluster-Ebenen-Statistiken

Feldname	Beschreibung
stores	Gibt an, wo die Funktionssätze und Modellmetadaten gespeichert werden. (Der Standardwert ist „.ltrstore“. Andernfalls wird „.ltrstore_“ mit einem vom Benutzer angegebenen Namen vorangestellt).
stores.status	Der Indexstatus.
stores.feature_sets	Anzahl der Funktionssätze.

Feldname	Beschreibung
stores.features_count	Anzahl der Funktionen.
stores.model_count	Anzahl der Modelle.
Status	Der Plug-In-Status basierend auf dem Status der Funktionsspeicher-Indizes (rot, gelb oder grün) und des Leistungsschalterstatus (offen oder geschlossen).
cache.cache_capacity_reached	Gibt an, ob das Cache-Limit erreicht ist.

Cache-Statistiken abrufen

Gibt Statistiken über den Cache und die Speichernutzung zurück.

```
GET _ltr/_cachestats

{
    "_nodes": {
        "total": 2,
        "successful": 2,
        "failed": 0
    },
    "cluster_name": "opensearch-cluster",
    "all": {
        "total": {
            "ram": 612,
            "count": 1
        },
        "features": {
            "ram": 0,
            "count": 0
        },
        "featuresets": {
            "ram": 612,
            "count": 1
        },
        "models": {
            "ram": 0,
```

```
            "count": 0
        }
    },
    "stores": {
        ".ltrstore": {
            "total": {
                "ram": 612,
                "count": 1
            },
            "features": {
                "ram": 0,
                "count": 0
            },
            "featuresets": {
                "ram": 612,
                "count": 1
            },
            "models": {
                "ram": 0,
                "count": 0
            }
        }
    },
    "nodes": {
        "ejF6uutERF20wOFNOXB61A": {
            "name": "opensearch1",
            "hostname": "172.18.0.4",
            "stats": {
                "total": {
                    "ram": 612,
                    "count": 1
                },
                "features": {
                    "ram": 0,
                    "count": 0
                },
                "featuresets": {
                    "ram": 612,
                    "count": 1
                },
                "models": {
                    "ram": 0,
                    "count": 0
                }
```

```
            }
        },
        "Z2RZNWRLSveVcz2c6lHf5A": {
            "name": "opensearch2",
            "hostname": "172.18.0.2",
            "stats": {
                ...
            }
        }
    }
}
```

Löschen des Cache

Löscht den Plug-In-Cache. Verwenden Sie diese Option, um das Modell zu aktualisieren.

```
POST _ltr/_clearcache
```

Asynchrone Suche in Amazon Service OpenSearch

Mit der asynchronen Suche nach Amazon OpenSearch Service können Sie eine Suchabfrage stellen, die im Hintergrund ausgeführt wird, den Fortschritt der Anfrage überwachen und Ergebnisse zu einem späteren Zeitpunkt abrufen. Sie können Teilergebnisse abrufen, sobald sie verfügbar sind, bevor die Suche abgeschlossen ist. Nachdem die Suche abgeschlossen ist, speichern Sie die Ergebnisse für einen späteren Abruf und Analyse.

Für die asynchrone Suche ist OpenSearch 1.0 oder höher oder Elasticsearch 7.10 oder höher erforderlich.

Diese Dokumentation bietet einen kurzen Überblick über die asynchrone Suche. Es werden auch die Einschränkungen der Verwendung der asynchronen Suche mit einer verwalteten Amazon OpenSearch Service-Domain anstelle eines OpenSearch Open-Source-Clusters erörtert. Eine vollständige Dokumentation der asynchronen Suche, einschließlich verfügbarer Einstellungen, Berechtigungen und einer vollständigen API-Referenz, finden Sie in der Dokumentation unter Asynchrone Suche. OpenSearch

Beispiele für Suchaufrufe

Um eine asynchrone Suche durchzuführen, senden Sie HTTP-Anforderungen an `_plugins/_asynchronous_search` im folgenden Format:

```
POST opensearch-domain/_plugins/_asynchronous_search
```

> **Note**
>
> Wenn Sie Elasticsearch 7.10 anstelle einer OpenSearch Version verwenden, ersetzen Sie dies `_opendistro` in allen asynchronen Suchanfragen `_plugins` durch.

Sie können die folgenden asynchronen Suchoptionen angeben:

Optionen	Beschreibung	Standardwert	Erforderlich
`wait_for_completion_timeout`	Gibt die Zeitspanne an, in der Sie auf die Ergebnisse warten möchten. Sie können die Ergebnisse sehen, die Sie innerhalb dieser Zeit erhalten, genau wie bei einer normalen Suche. Sie können die verbleibenden Ergebnisse anhand einer ID abfragen. Der Höchstwert beträgt 300 Sekunden.	1 Sekunde	Nein
`keep_on_completion`	Gibt an, ob die Ergebnisse nach Abschluss der Suche im Cluster gespeichert werden sollen. Sie können die gespeicherten Ergebnisse zu einem späteren Zeitpunkt untersuchen.	`false`	Nein
`keep_alive`	Gibt die Zeit an, in der das Ergebnis im Cluster gespeichert wird. `2d` bedeutet beispielsweise, dass die Ergebnisse 48 Stunden lang im Cluster gespeichert werden. Die gespeicherten Suchergebnisse werden nach diesem Zeitraum gelöscht oder wenn die Suche abgebrochen wird. Beachten Sie, dass dies die Abfragelaufzeit einschließt. Wenn die Abfrage dieses Mal überläuft, bricht der Prozess diese Abfrage automatisch ab.	12 Stunden	Nein

Beispielanforderung

```
POST _plugins/_asynchronous_search/?
pretty&size=10&wait_for_completion_timeout=1ms&keep_on_completion=true&request_cache=false
{
  "aggs": {
    "city": {
      "terms": {
        "field": "city",
        "size": 10
      }
    }
  }
}
```

> **Note**
>
> Alle Anforderungsparameter, die für eine Standard-`_search`-Abfrage gelten, werden unterstützt. Wenn Sie Elasticsearch 7.10 anstelle einer OpenSearch Version verwenden, ersetzen Sie es durch. `_plugins` `_opendistro`

Asynchrone Suchberechtigungen

Die asynchrone Suche unterstützt eine abgestimmte Zugriffskontrolle. Ausführliche Informationen zum Mischen und Abgleichen von Berechtigungen für Ihren Anwendungsfall finden Sie unter Sicherheit bei der asynchronen Suche.

Für Domains, bei denen eine abgestimmte Zugriffssteuerung aktiviert ist, benötigen Sie die folgenden Mindestberechtigungen für eine Rolle:

```
# Allows users to use all asynchronous search functionality
asynchronous_search_full_access:
  reserved: true
  cluster_permissions:
    - 'cluster:admin/opensearch/asynchronous-search/*'
  index_permissions:
    - index_patterns:
        - '*'
      allowed_actions:
        - 'indices:data/read/search*'
```

```
# Allows users to read stored asynchronous search results
asynchronous_search_read_access:
  reserved: true
  cluster_permissions:
    - 'cluster:admin/opensearch/asynchronous-search/get'
```

Verwenden Sie für Domains mit deaktivierter Zugriffssteuerung den IAM-Zugriff und den geheimen Schlüssel, um alle Anforderungen zu signieren. Sie können mit der asynchronen Such-ID auf die Ergebnisse zugreifen.

Asynchrone Sucheinstellungen

OpenSearch ermöglicht es Ihnen, alle verfügbaren asynchronen Sucheinstellungen mithilfe der API zu ändern. `_cluster/settings` In OpenSearch Service können Sie nur die folgenden Einstellungen ändern:

- `plugins.asynchronous_search.node_concurrent_running_searches`
- `plugins.asynchronous_search.persist_search_failures`

Cluster-übergreifende Suche

Sie können eine asynchrone Suche über Cluster mit den folgenden geringfügigen Einschränkungen durchführen:

- Sie können eine asynchrone Suche nur in der Quell-Domain ausführen.
- Sie können Netzwerk-Roundtrips als Teil einer clusterübergreifenden Suchabfrage nicht minimieren.

Wenn Sie eine Verbindung zwischen `domain-a -> domain-b` mit dem Verbindungsalias `cluster_b` und `domain-a -> domain-c` mit dem Verbindungsalias `cluster_c` einrichten, suchen Sie `domain-a`, `domain-b` und `domain-c` asynchron, wie folgt:

```
POST https://src-domain.us-east-1.es.amazonaws.com/
local_index,cluster_b:b_index,cluster_c:c_index/_plugins/_asynchronous_search/?
pretty&size=10&wait_for_completion_timeout=500ms&keep_on_completion=true&request_cache=false
{
  "size": 0,
  "_source": {
```

```
    "excludes": []
  },
  "aggs": {
    "2": {
      "terms": {
        "field": "clientip",
        "size": 50,
        "order": {
          "_count": "desc"
        }
      }
    }
  },
  "stored_fields": [
    "*"
  ],
  "script_fields": {},
  "docvalue_fields": [
    "@timestamp"
  ],
  "query": {
    "bool": {
      "must": [
        {
          "query_string": {
            "query": "status:404",
            "analyze_wildcard": true,
            "default_field": "*"
          }
        },
        {
          "range": {
            "@timestamp": {
              "gte": 1483747200000,
              "lte": 1488326400000,
              "format": "epoch_millis"
            }
          }
        }
      ],
      "filter": [],
      "should": [],
      "must_not": []
    }
```

```
  }
}
```

Antwort

```
{
  "id" :
 "Fm9pYzJyVG91U19xb0hIQUJnMHJfRFEAAAAAAAknghQ1OWVBczNZQjVEa2dMYTBXaTdEagAAAAAAAAAB",
  "state" : "RUNNING",
  "start_time_in_millis" : 1609329314796,
  "expiration_time_in_millis" : 1609761314796
}
```

Weitere Informationen finden Sie unter the section called “Cluster-übergreifende Suche”.

UltraWarm

Asynchrone Suchen mit UltraWarm Indizes funktionieren weiterhin. Weitere Informationen finden Sie unter the section called “UltraWarm Speicher”.

> **Note**
>
> Sie können asynchrone Suchstatistiken in überwachen. CloudWatch Eine vollständige Liste der Metriken finden Sie unter the section called “Asynchrone Suchmetriken”.

Point-in-Time-Suche in Amazon OpenSearch Service

Point in Time (PIT) ist ein Suchtyp, mit dem Sie verschiedene Abfragen für einen Datensatz ausführen können, der zeitlich festgelegt ist. Wenn Sie dieselbe Abfrage für denselben Index zu unterschiedlichen Zeitpunkten ausführen, erhalten Sie in der Regel unterschiedliche Ergebnisse, da Dokumente ständig indexiert, aktualisiert und gelöscht werden. Mit PIT können Sie Abfragen anhand eines konstanten Zustands Ihres Datensatzes durchführen.

Der Hauptzweck der PIT-Suche besteht darin, sie mit `search_after` Funktionen zu verbinden. Dies ist die bevorzugte Paginierungsmethode OpenSearch, insbesondere für tiefe Paginierung, da sie mit einem Datensatz arbeitet, der zeitlich eingefroren ist, nicht an eine Abfrage gebunden ist und eine konsistente Paginierung vor- und rückwärts unterstützt. Sie können PIT mit einer Domain verwenden, auf der Version 2.5 ausgeführt wird. OpenSearch

> **Note**
>
> Dieses Thema bietet einen Überblick über PIT und einige Dinge, die bei der Verwendung auf einer verwalteten Amazon OpenSearch Service-Domain und nicht auf einem selbstverwalteten OpenSearch Cluster zu beachten sind. Eine vollständige Dokumentation von PIT, einschließlich einer umfassenden API-Referenz, finden Sie unter Point in Time in der OpenSearch Open-Source-Dokumentation.

Überlegungen

Beachten Sie bei der Konfiguration Ihrer PIT-Suchen Folgendes:

- Wenn Sie ein Upgrade von einer Domain mit OpenSearch Version 2.3 durchführen und eine detaillierte Zugriffskontrolle für PIT-Aktionen benötigen, müssen Sie diese Aktionen und Rollen manuell hinzufügen.
- Es gibt keine Resilienz für PIT. Der Neustart von Knoten, die Kündigung des Knotens, Bereitstellungen in Blau/Grün und OpenSearch Prozessneustarts führen dazu, dass alle PIT-Daten verloren gehen.
- Wenn ein Shard während der Blau/Grün-Bereitstellung verschoben wird, werden nur Live-Datensegmente auf den neuen Knoten übertragen. Shard-Segmente, die sich im Besitz von PIT befinden (sowohl exklusiv als auch diejenigen, die gemeinsam mit aktiven Daten genutzt werden), verbleiben auf dem alten Knoten.
- PIT-Suchen funktionieren derzeit nicht mit asynchroner Suche.

Erstellen Sie eine PIT

Um eine PIT-Abfrage auszuführen, senden Sie HTTP-Anfragen `_search/point_in_time` unter Verwendung des folgenden Formats an:

```
POST opensearch-domain/my-index/_search/point_in_time?keep_alive=time
```

Sie können die folgenden PIT-Optionen angeben:

Optionen	Beschreibung	Standardwert	Erforderlich
`keep_alive`	Die Dauer der Beibehaltung der PIT. Jedes Mal, wenn Sie mit einer Suchanfrage auf eine PIT zugreifen, wird die PIT-Lebensdauer um den Zeitraum verlängert, der dem `keep_alive` Parameter entspricht. Dieser Abfrageparameter ist erforderlich, wenn Sie eine PIT erstellen, bei einer Suchanfrage jedoch optional.		Ja
`preference`	Eine Zeichenfolge, die den Knoten oder den Shard angibt, der für die Suche verwendet wurde.	Zufällig	Nein
`routing`	Eine Zeichenfolge, die angibt, Suchanfragen an einen bestimmten Shard weiterzuleiten.	Das Dokument ist `_id`	Nein
`expand_wildcards`	Eine Zeichenfolge, die den Indextyp angibt, der dem Platzhaltermuster entsprechen kann. Unterstützt kommagetrennte Werte. Gültige Werte: • `all`: Entspricht einem beliebigen Index oder Datenstrom, auch versteckten. • `open`: Ordnet offene, nicht versteckte Indizes oder nicht versteckte Datenströme zu. • `closed`: Ordnet geschlossene, nicht versteckte Indizes oder nicht versteckte Datenströme zu. • `hidden`: Ordnet versteckte Indizes oder Datenströme zu. Muss mit „offen“, „geschlossen“ oder „offen“ und „geschlossen“ kombiniert werden.	`open`	Nein

Optionen	Beschreibung	Standardwert	Erforderlich
	• none: Platzhaltermuster werden nicht akzeptiert.		
allow_partial_pit_creation	Ein boolescher Wert, der angibt, ob eine PIT mit teilweisen Fehlern erstellt werden soll.	true	Nein

Beispielantwort

```
{
    "pit_id":
 "o463QQEPbXktaW5kZXgtMDAwMDAxFnNOWU43ckt3U3IyaFVpbGE1UWEtMncAFjFyeXBsRGJmVFM2RTB6eVg1aVVqQncAA
    "_shards": {
        "total": 1,
        "successful": 1,
        "skipped": 0,
        "failed": 0
    },
    "creation_time": 1658146050064
}
```

Wenn Sie eine PIT erstellen, erhalten Sie in der Antwort eine PIT-ID. Dies ist die ID, die Sie verwenden, um Suchen mit der PIT durchzuführen.

Berechtigungen zu einem bestimmten Zeitpunkt

PIT unterstützt eine differenzierte Zugriffskontrolle. Wenn Sie ein Upgrade auf eine Domain der OpenSearch Version 2.5 durchführen und eine detaillierte Zugriffskontrolle benötigen, müssen Sie manuell Rollen mit den folgenden Berechtigungen erstellen:

```
# Allows users to use all point in time search search functionality
point_in_time_full_access:
  reserved: true
  index_permissions:
    - index_patterns:
        - '*'
      allowed_actions:
        - "indices:data/read/point_in_time/create"
```

```
        - "indices:data/read/point_in_time/delete"
        - "indices:data/read/point_in_time/readall"
        - "indices:data/read/search"
        - "indices:monitor/point_in_time/segments"


# Allows users to use point in time search search functionality for specific index
# All type operations like list all PITs, delete all PITs are not supported in this
 case

point_in_time_index_access:
  reserved: true
  index_permissions:
    - index_patterns:
        - 'my-index-1'
      allowed_actions:
        - "indices:data/read/point_in_time/create"
        - "indices:data/read/point_in_time/delete"
        - "indices:data/read/search"
        - "indices:monitor/point_in_time/segments"
```

Für Domänen mit OpenSearch Version 2.5 und höher können Sie die integrierte `point_in_time_full_access` Rolle verwenden. Weitere Informationen finden Sie in der OpenSearch Dokumentation unter Sicherheitsmodell.

PIT-Einstellungen

OpenSearch ermöglicht es Ihnen, alle verfügbaren PIT-Einstellungen mithilfe der `_cluster/settings` API zu ändern. Im OpenSearch Service können Sie derzeit keine Einstellungen ändern.

Cluster-übergreifende Suche

Sie können PITs erstellen, mit PIT-IDs suchen, PITs auflisten und PITs clusterübergreifend löschen, wobei die folgenden geringfügigen Einschränkungen gelten:

- Sie können nur in der Quelldomäne alle PITs auflisten und alle löschen.
- Sie können Netzwerk-Roundtrips als Teil einer clusterübergreifenden Suchabfrage nicht minimieren.

Weitere Informationen finden Sie unter the section called “Cluster-übergreifende Suche”.

UltraWarm

PIT-Suchen mit UltraWarm Indizes funktionieren weiterhin. Weitere Informationen finden Sie unter the section called “UltraWarm Speicher”.

> **Note**
>
> Sie können die PIT-Suchstatistiken in CloudWatch überwachen. Eine vollständige Liste der Metriken finden Sie unter the section called “Metriken zum aktuellen Zeitpunkt”.

Semantische Suche in Amazon Service OpenSearch

Ab OpenSearch Version 2.9 können Sie die semantische Suche verwenden, um Suchanfragen besser zu verstehen und die Suchrelevanz zu verbessern. Sie können die semantische Suche auf zwei Arten verwenden — mit der neuronalen Suche und mit der Suche nach k-Nearest Neighbor (k-NN).

Mit OpenSearch Service können Sie KI-Konnektoren für AWS-Services und externe Dienste einrichten. Mithilfe der Konsole können Sie auch ein ML-Modell mit einer AWS CloudFormation Vorlage erstellen. Weitere Informationen finden Sie unter the section called “CloudFormation Vorlagen-Integrationen”.

Eine vollständige Dokumentation der semantischen Suche, einschließlich einer step-by-step Anleitung zur Verwendung der semantischen Suche, finden Sie unter Semantische Suche in der Open-Source-Dokumentation. OpenSearch

Gleichzeitige Segmentsuche in Amazon Service OpenSearch

Ab OpenSearch Version 2.13 können Sie die gleichzeitige Segmentsuche verwenden, um während der Abfragephase parallel nach Segmenten zu suchen. Eine vollständige Dokumentation der gleichzeitigen Segmentsuche finden Sie unter Gleichzeitige Segmentsuche in der Open-Source-Dokumentation. OpenSearch Informationen zu CloudWatch Amazon-Metriken im Zusammenhang mit der gleichzeitigen Segmentsuche finden Sie unter Instance-Metriken und UltraWarm Metriken.

Es gibt einige zusätzliche Einschränkungen, die gelten, wenn Sie die aktuelle Segmentsuche mit Amazon OpenSearch Service verwenden:

- Sie können die gleichzeitige Segmentsuche auf Indexebene in OpenSearch Service nicht aktivieren.
- Standardmäßig verwendet OpenSearch Service eine Anzahl von 2 Slices mit dem Mechanismus „Max Slice Count“.

Verwenden von OpenSearch Dashboards mit Amazon Service OpenSearch

OpenSearch Dashboards ist ein Open-Source-Visualisierungstool, mit dem Sie arbeiten können. OpenSearch Amazon OpenSearch Service bietet für jede OpenSearch Service-Domain eine Installation von OpenSearch Dashboards. OpenSearch Dashboards wird auf den Hot-Data-Knoten in der Domain ausgeführt.

In Ihrem Domain-Dashboard in der OpenSearch Servicekonsole finden Sie einen Link zu OpenSearch Dashboards. Für laufende OpenSearch Domains lautet *domain-endpoint*`/_dashboards/` die URL. Für Domains, auf denen Legacy-Elasticsearch ausgeführt wird, lautet *domain-endpoint*`/_plugin/kibana` die URL.

Abfragen, die diese OpenSearch Standard-Dashboards-Installation verwenden, haben ein Timeout von 300 Sekunden.

> **Note**
>
> In dieser Dokumentation werden OpenSearch Dashboards im Kontext von Amazon OpenSearch Service beschrieben, einschließlich verschiedener Verbindungsmöglichkeiten. Eine umfassende Dokumentation, einschließlich eines Leitfadens für die ersten Schritte, einer Anleitung zum Erstellen eines Dashboards, der Verwaltung von Dashboards und der Dashboards Query Language (DQL), finden Sie unter OpenSearch Dashboards in der Open-Source-Dokumentation. OpenSearch

In den folgenden Abschnitten werden einige gängige Anwendungsfälle für Dashboards behandelt: OpenSearch

- the section called “Steuern des Zugriffs auf Dashboards OpenSearch ”
- the section called “Konfiguration von OpenSearch Dashboards für die Verwendung eines WMS-Kartenservers”
- the section called “Einen lokalen Dashboards-Server mit dem Service verbinden OpenSearch ”

Steuern des Zugriffs auf Dashboards OpenSearch

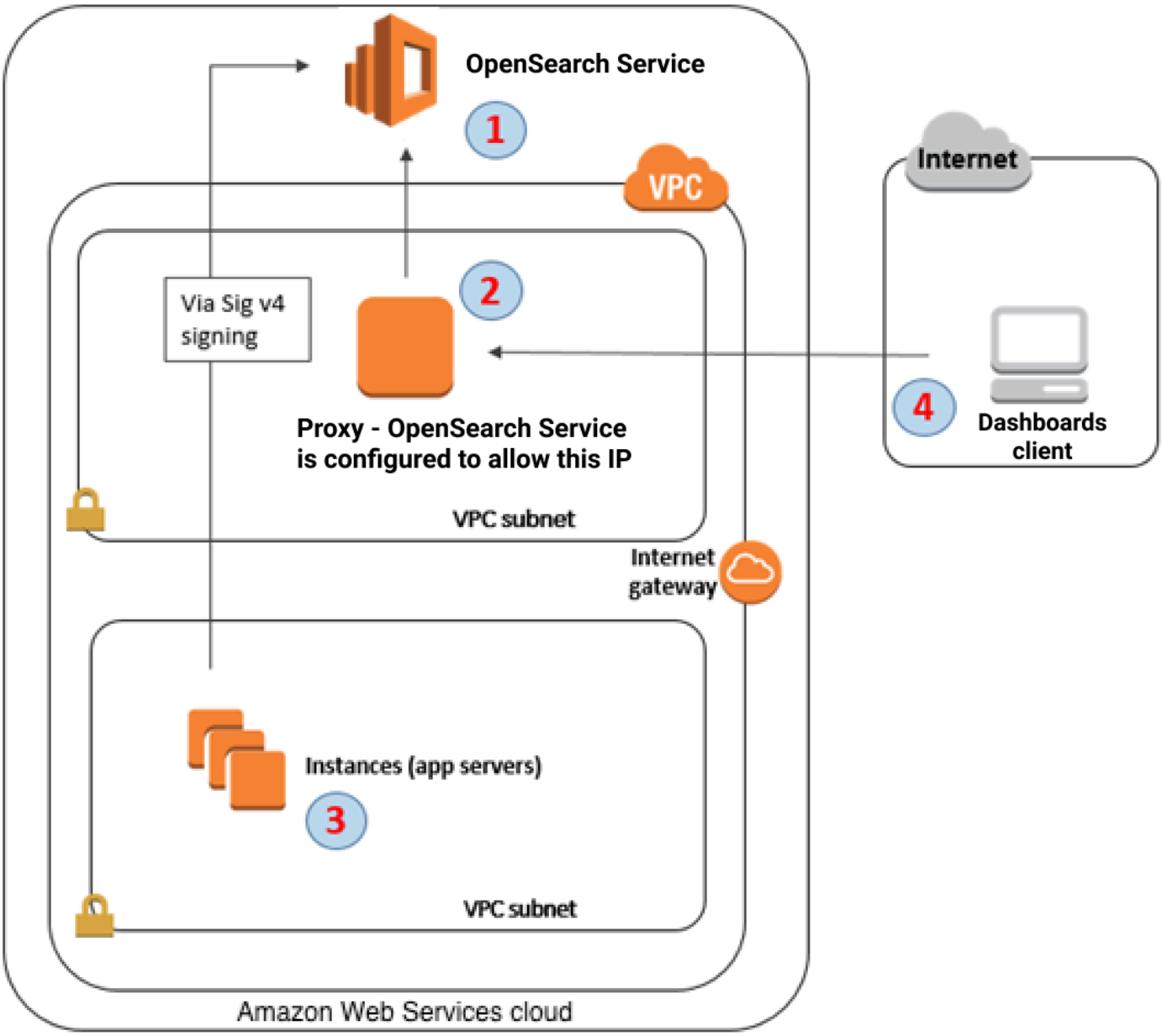
Dashboards unterstützt IAM-Benutzer und -Rollen nicht nativ, aber OpenSearch Service bietet mehrere Lösungen für die Steuerung des Zugriffs auf Dashboards:

- Aktivieren Sie die SAML-Authentifizierung für Dashboards.
- Verwenden Sie eine differenzierte Zugriffskontrolle mit HTTP-Basisauthentifizierung.
- Konfiguration Cognito-Authentifizierung für Dashboards.
- Konfigurieren Sie für öffentliche Zugriff-Domains eine IP-basierte Zugriffsrichtlinie, mit oder ohne Proxy-Server.
- Verwenden Sie für VPC-Zugriff-Domains eine offene Zugriffsrichtlinie mit oder ohne Proxyserver und Sicherheitsgruppen, um den Zugriff zu steuern. Weitere Informationen hierzu finden Sie unter the section called “Zugriffsrichtlinien für VPC-Domänen”.

Verwenden eines Proxys für den Zugriff auf den Service über Dashboards OpenSearch OpenSearch

> **Note**
>
> Dieses Verfahren ist nur anwendbar, wenn Ihre Domain einen öffentlichen Zugriff verwendet und Sie die Cognito-Authentifizierung nicht verwenden möchten. Siehe the section called “Steuern des Zugriffs auf Dashboards OpenSearch ”.

Da es sich bei Dashboards um eine JavaScript Anwendung handelt, stammen Anfragen von der IP-Adresse des Benutzers. Eine IP-basierte Zugriffskontrolle ist möglicherweise wegen der hohen Anzahl von IP-Adressen unpraktisch, die Sie erlaubt haben müssten, um jedem Benutzer Zugriff auf Dashboards zu gewähren. Eine Problemumgehung besteht darin, einen Proxyserver zwischen OpenSearch Dashboards und Service zu platzieren. OpenSearch Anschließend können Sie eine IP-basierte Zugriffsrichtlinie hinzufügen, mit der Anforderungen von nur einer IP-Adresse möglich sind: der Adresse des Proxys. In der folgenden Abbildung ist diese Konfiguration dargestellt.



1. Dies ist Ihre OpenSearch Service-Domain. IAM bietet autorisierten Zugriff auf diese Domain. Eine zusätzliche, IP-basierte Zugriffsrichtlinie bietet Zugriff auf den Proxy-Server.
2. Dies ist der Proxy-Server, der auf einer Amazon-EC2-Instance ausgeführt wird.
3. Andere Anwendungen können den Signaturprozess von Signature Version 4 verwenden, um authentifizierte Anfragen an den OpenSearch Service zu senden.
4. OpenSearch Dashboard-Clients stellen über den Proxy eine Verbindung zu Ihrer OpenSearch Service-Domain her.

Wenn Sie diese Art von Konfiguration aktivieren möchten, benötigen Sie eine ressourcenbasierte Richtlinie, in der Rollen und IP-Adressen angegeben sind. Hier sehen Sie ein Beispiel für eine Richtlinie:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Resource":"arn:aws:es:us-west-2:111111111111:domain/my-domain/*",
         "Principal":{
            "AWS":"arn:aws:iam::111111111111:role/allowedrole1"
         },
         "Action":[
            "es:ESHttpGet"
         ],
         "Effect":"Allow"
      },
      {
         "Effect":"Allow",
         "Principal":{
            "AWS":"*"
         },
         "Action":"es:*",
         "Condition":{
            "IpAddress":{
               "aws:SourceIp":[
                  "203.0.113.0/24",
                  "2001:DB8:1234:5678::/64"
               ]
            }
         },
         "Resource":"arn:aws:es:us-west-2:111111111111:domain/my-domain/*"
      }
   ]
}
```

Wir empfehlen, dass Sie die EC2 Instance, auf der der Proxy-Server ausgeführt wird, mit einer Elastic IP-Adresse konfigurieren. Auf diese Weise können Sie die Instance bei Bedarf ersetzen und weiterhin dieselbe öffentliche IP-Adresse an sie anfügen. Weitere Informationen finden Sie unter Elastic IP Addresses im Amazon EC2 EC2-Benutzerhandbuch.

Wenn Sie einen Proxy-Server und die Cognito-Authentifizierung, verwenden, müssen Sie möglicherweise Einstellungen für Dashboards und Amazon Cognito hinzufügen, um `redirect_mismatch`-Fehler zu vermeiden. Sehen Sie sich das folgende `nginx.conf`-Beispiel an:

```
server {
    listen 443;
    server_name $host;
    rewrite ^/$ https://$host/_plugin/_dashboards redirect;

    ssl_certificate          /etc/nginx/cert.crt;
    ssl_certificate_key      /etc/nginx/cert.key;

    ssl on;
    ssl_session_cache  builtin:1000  shared:SSL:10m;
    ssl_protocols  TLSv1 TLSv1.1 TLSv1.2;
    ssl_ciphers HIGH:!aNULL:!eNULL:!EXPORT:!CAMELLIA:!DES:!MD5:!PSK:!RC4;
    ssl_prefer_server_ciphers on;

    location /_plugin/_dashboards {
        # Forward requests to Dashboards
        proxy_pass https://$dashboards_host/_plugin/_dashboards;

        # Handle redirects to Cognito
        proxy_redirect https://$cognito_host https://$host;

        # Update cookie domain and path
        proxy_cookie_domain $dashboards_host $host;
        proxy_cookie_path / /_plugin/_dashboards/;

        # Response buffer settings
        proxy_buffer_size 128k;
        proxy_buffers 4 256k;
        proxy_busy_buffers_size 256k;
    }

    location ~ \/(log|sign|fav|forgot|change|saml|oauth2) {
        # Forward requests to Cognito
        proxy_pass https://$cognito_host;

        # Handle redirects to Dashboards
        proxy_redirect https://$dashboards_host https://$host;

        # Update cookie domain
```

```
        proxy_cookie_domain $cognito_host $host;
    }
}
```

Konfiguration von OpenSearch Dashboards für die Verwendung eines WMS-Kartenservers

Die Standardinstallation von OpenSearch Dashboards for OpenSearch Service umfasst einen Kartenservice, mit Ausnahme von Domains in den Regionen Indien und China. Der Karten-Service unterstützt bis zu 10 Zoomstufen.

Unabhängig von Ihrer Region können Sie Dashboards so konfigurieren, dass ein anderer Web-Map-Server (WMS)-Server für Koordinatenkartenvisualisierungen verwendet wird. Regionskartenvisualisierungen unterstützen nur den Standardkarten-Service.

So konfigurieren Sie Dashboards für die Verwendung eines WMS-Map-Servers:

1. Öffnen von Dashboards
2. Klicken Sie auf Verwaltung von Stack.
3. Wählen Sie Advanced settings (Erweiterte Einstellungen) aus.
4. Suchen Sie visualization:tileMap:WMSdefaults.
5. Ändern Sie `enabled` zu `true` und `url` zur URL eines gültigen WMS Map-Servers.

   ```
   {
     "enabled": true,
     "url": "wms-server-url",
     "options": {
       "format": "image/png",
       "transparent": true
     }
   }
   ```

6. Wählen Sie Änderungen speichern aus.

Um den neuen Standardwert auf Visualisierungen anzuwenden, müssen Sie möglicherweise Dashboards erneut laden. Wenn Sie Visualisierungen gespeichert haben, wählen Sie Options (Optionen), nachdem Sie die Visualisierung geöffnet haben. Stellen Sie sicher, dass der WMS Map

Server aktiviert ist und die WMS-URL den bevorzugten Map-Server enthält, und wählen Sie dann Apply changes (Änderungen übernehmen) aus.

> **Note**
>
> Map-Services erheben häufig Lizenzgebühren oder schränken die Nutzung ein. Sie sind für all diese Aspekte des Map-Servers verantwortlich, den Sie angeben. Map-Services des U.S. Geological Survey (Geologisches Amt der USA) können zum Testen nützlich sein.

Einen lokalen Dashboards-Server mit dem Service verbinden OpenSearch

Wenn Sie bereits viel Zeit in die Konfiguration Ihrer eigenen OpenSearch Dashboards-Instanz investiert haben, können Sie diese anstelle der von Service bereitgestellten Standard-Dashboards-Instanz (oder zusätzlich zu) verwenden. OpenSearch Das folgende Verfahren funktioniert für Domains, die eine differenzierte Zugriffskontrolle mit einer offenen Zugriffsrichtlinie verwenden.

Um einen lokalen OpenSearch Dashboards-Server mit Service zu verbinden OpenSearch

1. Erstellen Sie in Ihrer OpenSearch Service-Domain einen Benutzer mit den entsprechenden Berechtigungen:
   a. Wechseln Sie in Dashboards zu Sicherheit, Interne Benutzer und wählen Sie Erstellen eines internen Benutzers aus.
   b. Geben Sie einen Benutzernamen und ein Passwort ein und wählen Sie Erstellen aus.
   c. Wechseln Sie zu Rollen und wählen Sie eine Rolle aus.
   d. Wählen Sie Zugeordnete Benutzer aus, und wählen Sie Mapping verwalten aus.
   e. Fügen Sie unter Benutzer Ihren Benutzernamen hinzu und wählen Sie Mapping aus.
2. Laden Sie die entsprechende Version des OpenSearch Sicherheits-Plug-ins herunter und installieren Sie sie auf Ihrer selbstverwalteten Dashboards OSS-Installation.
3. Öffnen Sie die `config/opensearch_dashboards.yml` Datei auf Ihrem lokalen Dashboards-Server und fügen Sie Ihren OpenSearch Service-Endpunkt mit dem zuvor erstellten Benutzernamen und Passwort hinzu:

```
opensearch.hosts: ['https://domain-endpoint']
opensearch.username: 'username'
```

```
opensearch.password: 'password'
```

Verwenden Sie die folgende `opensearch_dashboards.yml`-Beispieldatei:

```
server.host: '0.0.0.0'

opensearch.hosts: ['https://domain-endpoint']

opensearchDashboards.index: ".username"

opensearch.ssl.verificationMode: none # if not using HTTPS

opensearch_security.auth.type: basicauth
opensearch_security.auth.anonymous_auth_enabled: false
opensearch_security.cookie.secure: false # set to true when using HTTPS
opensearch_security.cookie.ttl: 3600000
opensearch_security.session.ttl: 3600000
opensearch_security.session.keepalive: false
opensearch_security.multitenancy.enabled: false
opensearch_security.readonly_mode.roles: ['opensearch_dashboards_read_only']
opensearch_security.auth.unauthenticated_routes: []
opensearch_security.basicauth.login.title: 'Please log in using your username and
 password'

opensearch.username: 'username'
opensearch.password: 'password'
opensearch.requestHeadersWhitelist: [authorization, securitytenant,
 security_tenant]
```

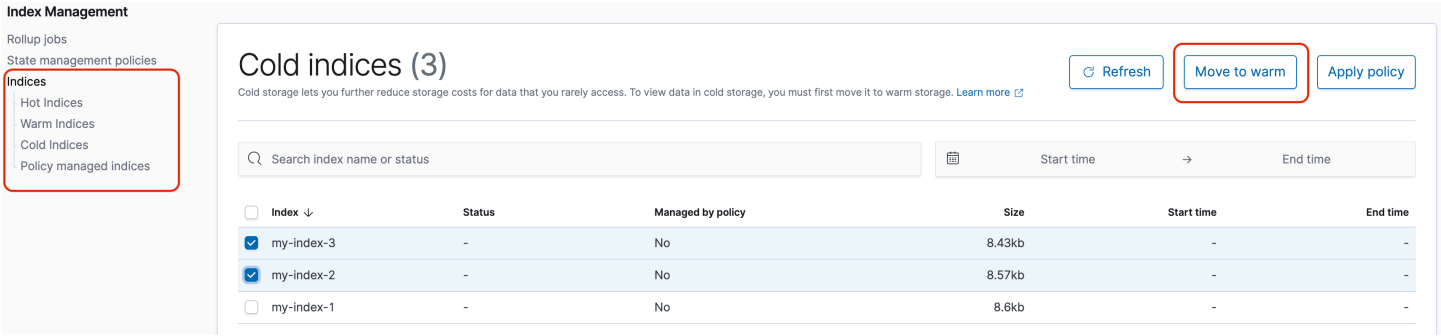
Um Ihre OpenSearch Service-Indizes zu sehen, starten Sie Ihren lokalen Dashboards-Server, gehen Sie zu Dev Tools und führen Sie den folgenden Befehl aus:

```
GET _cat/indices
```

Indizes in Dashboards verwalten OpenSearch

Die OpenSearch Dashboards-Installation auf Ihrer OpenSearch Service-Domain bietet eine nützliche Benutzeroberfläche für die Verwaltung von Indizes in verschiedenen Speicherebenen Ihrer Domain. Wählen Sie im Hauptmenü der Dashboards die Option Indexverwaltung aus, UltraWarmum alle Indizes im Hot- und Cold-Storage sowie Indizes, die durch Index State Management (ISM)

-Richtlinien verwaltet werden, anzuzeigen. Verwenden Sie die Indexverwaltung, um Indizes zwischen Warm- und Cold-Speicher zu verschieben und Migrationen zwischen den drei Ebenen zu überwachen.



Beachten Sie, dass die Indexoptionen „Heiß“, „Warm“ und „Kalter Speicher“ nicht angezeigt werden, es sei denn, Sie haben UltraWarm und/oder Kaltspeicher aktiviert.

Weitere Features

Die Standardinstallation von OpenSearch Dashboards auf jeder OpenSearch Service-Domain bietet einige zusätzliche Funktionen:

- Benutzeroberflächen für die verschiedenen Plugins OpenSearch
- Mandanten
- Berichte

  Verwenden Sie das Menü Berichterstellung, um CSV-Berichte on demand von der Entdecken-Seite und PDF- oder PNG-Berichte von Dashboards oder Visualisierungen zu generieren. CSV-Berichte haben eine Begrenzung von 10.000 Zeilen.
- Gantt-Diagramme
- Notebooks

Verwaltung von Indizes in Amazon Service OpenSearch

Nachdem Sie Daten zu Amazon OpenSearch Service hinzugefügt haben, müssen Sie diese Daten häufig neu indizieren, mit Index-Aliasnamen arbeiten, einen Index in einen kostengünstigeren Speicher verschieben oder ihn ganz löschen. Dieses Kapitel behandelt UltraWarm Speicher, Cold Storage und Index State Management. Informationen zu den OpenSearch Index-APIs finden Sie in der OpenSearch Dokumentation.

Themen

UltraWarm Speicher für Amazon OpenSearch Service

UltraWarm bietet eine kostengünstige Möglichkeit, große Mengen schreibgeschützter Daten auf Amazon OpenSearch Service zu speichern. Standarddatenknoten verwenden „Hot“-Speicher, der in Form von Instance-Speichern oder Amazon EBS-Volumes an jeden Knoten angefügt ist. Hot Storage bietet die schnellstmögliche Leistung für die Indizierung und die Suche nach neuen Daten.

Anstatt angehängten Speicher verwenden UltraWarm Knoten Amazon S3 und eine ausgeklügelte Caching-Lösung, um die Leistung zu verbessern. Bei Indizes, in die Sie nicht aktiv schreiben, seltener Abfragen durchführen und für die Sie nicht dieselbe Leistung benötigen, ergeben sich deutlich UltraWarm niedrigere Kosten pro GiB an Daten. Da warme Indizes schreibgeschützt sind, sofern Sie sie nicht in den Hot-Storage zurückschicken, UltraWarm eignet sie sich am besten für unveränderliche Daten wie Protokolle.

In verhalten OpenSearch sich warme Indizes genauso wie jeder andere Index. Sie können sie mit denselben APIs abfragen oder sie verwenden, um Visualisierungen in Dashboards zu erstellen. OpenSearch

Themen

Voraussetzungen

UltraWarm hat ein paar wichtige Voraussetzungen:

- UltraWarm benötigt OpenSearch Elasticsearch 6.8 oder höher.
- Um einen Warm-Speicher verwenden zu können, müssen Domains über dedizierte Hauptknoten verfügen.
- Bei Verwendung einer Multi-AZ mit Standby-Domain muss die Anzahl der warmen Knoten ein Vielfaches der Anzahl der verwendeten Availability Zones sein.
- Wenn Ihre Domäne einen T2- oder T3-Instance-Typ für Ihre Datenknoten verwendet, können Sie keinen Warm-Speicher verwenden.
- Wenn Ihr Index approximate k-NN (`"index.knn": true`) verwendet, können Sie ihn nicht in einen warmen Speicher verschieben.

- Wenn die Domain eine differenzierte Zugriffskontrolle verwendet, müssen Benutzer der `ultrawarm_manager` Rolle in OpenSearch Dashboards zugeordnet werden, um API-Aufrufe tätigen zu können. UltraWarm

> **Note**
>
> Die `ultrawarm_manager` Rolle ist für einige bereits bestehende Service-Domänen möglicherweise nicht definiert. OpenSearch Wenn die Rolle in Dashboards nicht angezeigt wird, müssen Sie sie manuell erstellen.

So konfigurieren Sie Berechtigungen

Wenn Sie die Funktion in einer bereits vorhandenen OpenSearch Dienstdomäne aktivieren UltraWarm , ist die `ultrawarm_manager` Rolle möglicherweise nicht in der Domäne definiert. Benutzer ohne Administratorrechte müssen dieser Rolle zugeordnet werden, um Warm-Indizes in Domains mithilfe einer fein abgestuften Zugriffskontrolle zu verwalten. Führen Sie die folgenden Schritte aus, um die `ultrawarm_manager`-Rolle manuell zu erstellen:

1. Gehen Sie in OpenSearch Dashboards zu Sicherheit und wählen Sie Berechtigungen aus.
2. Wählen Sie Aktionsgruppe erstellen und konfigurieren Sie die folgenden Gruppen:

Group name (Gruppenname)	Berechtigungen
`ultrawarm_cluster`	• `cluster:admin/ultrawarm/migration/list` • `cluster:monitor/nodes/stats`
`ultrawarm_index_read`	• `indices:admin/ultrawarm/migration/get` • `indices:admin/get`
`ultrawarm_index_write`	• `indices:admin/ultrawarm/migration/warm` • `indices:admin/ultrawarm/migration/hot` • `indices:monitor/stats` • `indices:admin/ultrawarm/migration/cancel`

3. Wählen Sie Rollen und Rolle erstellen.

4. Benennen Sie die Rolle ultrawarm_manager.
5. Wählen Sie für Clusterberechtigungen `ultrawarm_cluster` und `cluster_monitor` aus.
6. Geben Sie für Index * ein.
7. Wählen Sie für Indexberechtigungen `ultrawarm_index_read`, `ultrawarm_index_write` und `indices_monitor` aus.
8. Wählen Sie Erstellen.
9. Nachdem Sie die Rolle erstellt haben, ordnen Sie sie einer beliebigen Benutzer- oder Backend-Rolle zu, die Indizes verwaltet UltraWarm .

UltraWarm Speicheranforderungen und Leistungsaspekte

Wie unter beschriebenthe section called “Berechnung der Speicheranforderungen”, entsteht für Daten im Hot-Storage ein erheblicher Mehraufwand: Replikate, reservierter Linux-Speicherplatz und vom OpenSearch Service reservierter Speicherplatz. Zum Beispiel benötigt ein primärer 20 GiB-Shard mit einem Replica-Shard etwa 58 GiB Hot Storage.

Da Amazon S3 verwendet wird, UltraWarm fällt dieser Overhead nicht an. Bei der Berechnung der UltraWarm Speicheranforderungen berücksichtigen Sie nur die Größe der primären Shards. Durch die Dauerhaftigkeit der Daten in S3 entfällt die Notwendigkeit für Replicas und S3 macht alle Betriebssystem- oder Dienstüberlegungen überflüssig. Derselbe 20 GiB-Shard erfordert 20 GiB Warm-Speicher. Wenn Sie eine `ultrawarm1.large.search`-Instance bereitstellen, können Sie alle 20 TiB des maximalen Speichers für primäre Shards verwenden. Eine Zusammenfassung der Instance-Typen und Informationen zur maximalen Speicherkapazität, die jeder adressieren kann, finden Sie unter the section called “UltraWarm Speicherkontingente”.

Wir empfehlen weiterhin eine maximale Shard-Größe von 50 GiB. UltraWarm Die Anzahl der CPU-Kerne und die Menge an RAM, die jedem UltraWarm Instance-Typ zugewiesen sind, geben Ihnen eine Vorstellung davon, wie viele Shards sie gleichzeitig durchsuchen können. Beachten Sie, dass zwar nur primäre Shards für den UltraWarm Speicherplatz in S3 angerechnet werden, OpenSearch Dashboards und Dashboards `_cat/indices` dennoch die UltraWarm Indexgröße als Summe aller Primär- und Replikat-Shards angeben.

Jede `ultrawarm1.medium.search`-Instance hat beispielsweise zwei CPU-Kerne und kann bis zu 1,5 TiB Speicher auf S3 adressieren. Zwei dieser Instances haben zusammen 3 TiB Speicher, was ungefähr 62 Shards ergibt, wenn jeder Shard 50 GiB groß ist. Wenn eine Anfrage an den Cluster nur vier dieser Shards durchsucht, kann die Leistung hervorragend sein. Wenn die Anfrage

breit gefächert ist und alle 62 durchsucht, können die vier CPU-Kerne Schwierigkeiten haben, den Vorgang auszuführen. Überwachen Sie die `WarmCPUUtilization` und `WarmJVMMemoryPressure` UltraWarm -Metriken, um zu verstehen, wie die Instances mit Ihren Workloads umgehen.

Wenn Sie viel oder häufig suchen, sollten Sie die Indizes im Hot Storage belassen. Wie bei jedem anderen OpenSearch Workload ist der wichtigste Schritt, um festzustellen, ob UltraWarm er Ihren Anforderungen entspricht, die Durchführung repräsentativer Client-Tests anhand eines realistischen Datensatzes.

UltraWarm Preisgestaltung

Bei Hot Storage zahlen Sie für das, was Sie bereitstellen. Einige Instances benötigen ein angefügtes Amazon-EBS-Volume, während andere einen Instance-Speicher enthalten. Unabhängig davon, ob dieser Speicher leer oder voll ist, zahlen Sie den gleichen Preis.

Bei UltraWarm Speicherplatz zahlen Sie für das, was Sie nutzen. Eine `ultrawarm1.large.search`-Instance kann bis zu 20 TiB Speicher auf S3 adressieren, aber wenn Sie nur 1 TiB Daten speichern, werden Ihnen nur 1 TiB Daten in Rechnung gestellt. Wie bei allen anderen Knotentypen zahlen Sie auch für jeden UltraWarm Knoten einen Stundensatz. Weitere Informationen finden Sie unter the section called “Preisgestaltung”.

Aktiviert UltraWarm

Die Konsole ist die einfachste Möglichkeit, eine Domain zu erstellen, die Warm-Speicher verwendet. Wählen Sie beim Erstellen der Domäne die Option UltraWarm Datenknoten aktivieren und geben Sie die gewünschte Anzahl an warmen Knoten an. Derselbe grundlegende Prozess funktioniert auf vorhandenen Domains, sofern sie die Voraussetzungenerfüllen. Auch wenn der Domänenstatus von „In Bearbeitung“ auf „Aktiv“ geändert wurde, kann er UltraWarm möglicherweise mehrere Stunden lang nicht verwendet werden.

Bei Verwendung einer Multi-AZ mit Standby-Domain muss die Anzahl der warmen Knoten ein Vielfaches der Anzahl der verwendeten Availability Zones sein. Weitere Informationen finden Sie unter the section called “Multi-AZ mit Standby”.

Sie können auch die Konfigurations-API AWS CLIoder verwenden UltraWarm, um insbesondere die `WarmType` Optionen `WarmEnabled``WarmCount`, und in `ClusterConfig` zu aktivieren.

> **Note**
>
> Die Domains unterstützen eine maximale Anzahl von Warm-Knoten. Details hierzu finden Sie unter the section called “Kontingente”.

Beispiel für einen CLI-Befehl

Mit dem folgenden AWS CLI Befehl wird eine Domäne mit drei Datenknoten, drei dedizierten Master-Knoten, sechs warmen Knoten und aktivierter detaillierter Zugriffskontrolle erstellt:

```
aws opensearch create-domain \
  --domain-name my-domain \
  --engine-version Opensearch_1.0 \
  --cluster-config
 InstanceCount=3,InstanceType=r6g.large.search,DedicatedMasterEnabled=true,DedicatedMasterType=
 \
  --ebs-options EBSEnabled=true,VolumeType=gp2,VolumeSize=11 \
  --node-to-node-encryption-options Enabled=true \
  --encryption-at-rest-options Enabled=true \
  --domain-endpoint-options EnforceHTTPS=true,TLSSecurityPolicy=Policy-Min-
TLS-1-2-2019-07 \
  --advanced-security-options
 Enabled=true,InternalUserDatabaseEnabled=true,MasterUserOptions='{MasterUserName=master-
user,MasterUserPassword=master-password}' \
  --access-policies '{"Version":"2012-10-17","Statement":
[{"Effect":"Allow","Principal":{"AWS":["123456789012"]},"Action":
["es:*"],"Resource":"arn:aws:es:us-west-1:123456789012:domain/my-domain/*"}]}' \
  --region us-east-1
```

Weitere Informationen finden Sie in der AWS CLI -Befehlsreferenz.

Beispiel für eine Konfigurations-API-Anforderung

Die folgende Anforderung an die Konfigurations-API erstellt eine Domain mit drei Datenknoten, drei dedizierten Hauptknoten und sechs Warm-Knoten mit differenzierter Zugriffskontrolle und einer restriktiven Zugriffsrichtlinie:

```
POST https://es.us-east-2.amazonaws.com/2021-01-01/opensearch/domain
{
  "ClusterConfig": {
    "InstanceCount": 3,
```

```
    "InstanceType": "r6g.large.search",
    "DedicatedMasterEnabled": true,
    "DedicatedMasterType": "r6g.large.search",
    "DedicatedMasterCount": 3,
    "ZoneAwarenessEnabled": true,
    "ZoneAwarenessConfig": {
      "AvailabilityZoneCount": 3
    },
    "WarmEnabled": true,
    "WarmCount": 6,
    "WarmType": "ultrawarm1.medium.search"
  },
  "EBSOptions": {
    "EBSEnabled": true,
    "VolumeType": "gp2",
    "VolumeSize": 11
  },
  "EncryptionAtRestOptions": {
    "Enabled": true
  },
  "NodeToNodeEncryptionOptions": {
    "Enabled": true
  },
  "DomainEndpointOptions": {
    "EnforceHTTPS": true,
    "TLSSecurityPolicy": "Policy-Min-TLS-1-2-2019-07"
  },
   "AdvancedSecurityOptions": {
    "Enabled": true,
    "InternalUserDatabaseEnabled": true,
    "MasterUserOptions": {
      "MasterUserName": "master-user",
      "MasterUserPassword": "master-password"
    }
  },
  "EngineVersion": "Opensearch_1.0",
  "DomainName": "my-domain",
  "AccessPolicies": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect\":\"Allow
\",\"Principal\":{\"AWS\":[\"123456789012\"]},\"Action\":[\"es:*\"],\"Resource\":
\"arn:aws:es:us-east-1:123456789012:domain/my-domain/*\"}]}"
}
```

Ausführliche Informationen finden Sie in der Amazon OpenSearch Service API-Referenz.

Indizes in den Speicher migrieren UltraWarm

Wenn Sie mit dem Schreiben in einen Index fertig sind und nicht mehr die schnellstmögliche Suchleistung benötigen, migrieren Sie ihn von Hot-Modus zu: UltraWarm

```
POST _ultrawarm/migration/my-index/_warm
```

Überprüfen Sie dann den Status der Migration:

```
GET _ultrawarm/migration/my-index/_status

{
  "migration_status": {
    "index": "my-index",
    "state": "RUNNING_SHARD_RELOCATION",
    "migration_type": "HOT_TO_WARM",
    "shard_level_status": {
      "running": 0,
      "total": 5,
      "pending": 3,
      "failed": 0,
      "succeeded": 2
    }
  }
}
```

Die Indexintegrität muss grün sein, um eine Migration durchzuführen. Wenn Sie mehrere Indizes schnell hintereinander migrieren, erhalten Sie eine Zusammenfassung aller Migrationen im Klartext, ähnlich der `_cat`-API:

```
GET _ultrawarm/migration/_status?v

index    migration_type state
my-index HOT_TO_WARM    RUNNING_SHARD_RELOCATION
```

OpenSearch Der Service migriert jeweils einen Index nach dem anderen zu UltraWarm. Sie können bis zu 200 Migrationen in der Warteschlange haben. Jede Anfrage, die das Limit überschreitet, wird abgelehnt. Um die aktuelle Anzahl von Migrationen in der Warteschlange zu überprüfen, überwachen Sie die `HotToWarmMigrationQueueSize`-Metrik. Indizes bleiben während des gesamten Migrationsprozesses verfügbar – keine Ausfallzeiten.

Der Migrationsprozess weist die folgenden Zustände auf:

```
PENDING_INCREMENTAL_SNAPSHOT
RUNNING_INCREMENTAL_SNAPSHOT
FAILED_INCREMENTAL_SNAPSHOT
PENDING_FORCE_MERGE
RUNNING_FORCE_MERGE
FAILED_FORCE_MERGE
PENDING_FULL_SNAPSHOT
RUNNING_FULL_SNAPSHOT
FAILED_FULL_SNAPSHOT
PENDING_SHARD_RELOCATION
RUNNING_SHARD_RELOCATION
FINISHED_SHARD_RELOCATION
```

Wie diese Zustände zeigen, können Migrationen während Snapshots, Shard-Verlagerungen oder erzwungenen Zusammenführungen fehlschlagen. Fehler bei Snapshots oder Shard-Verlagerungen sind in der Regel auf Knotenfehler oder S3-Konnektivitätsprobleme zurückzuführen. Ein Mangel an Speicherplatz ist in der Regel die zugrunde liegende Ursache für Fehler bei erzwungenen Zusammenführungen.

Nach Abschluss der Migration gibt dieselbe `_status`-Anforderung einen Fehler zurück. Wenn Sie den Index zu diesem Zeitpunkt überprüfen, können Sie einige Einstellungen sehen, die für Warm-Indizes eindeutig sind:

```
GET my-index/_settings

{
  "my-index": {
    "settings": {
      "index": {
        "refresh_interval": "-1",
        "auto_expand_replicas": "false",
        "provided_name": "my-index",
        "creation_date": "1599241458998",
        "unassigned": {
          "node_left": {
            "delayed_timeout": "5m"
          }
        },
        "number_of_replicas": "1",
        "uuid": "GswyCdR0RSq0SJYmzsIpiw",
```

```
        "version": {
          "created": "7070099"
        },
        "routing": {
          "allocation": {
            "require": {
              "box_type": "warm"
            }
          }
        },
        "number_of_shards": "5",
        "merge": {
          "policy": {
            "max_merge_at_once_explicit": "50"
          }
        }
      }
    }
  }
}
```

- `number_of_replicas` ist in diesem Fall die Anzahl der passiven Replicas, die keinen Speicherplatz verbrauchen.
- `routing.allocation.require.box_type` gibt an, dass der Index Warm-Knoten anstelle von Standarddatenknoten verwenden soll.
- `merge.policy.max_merge_at_once_explicit` gibt die Anzahl der Segmente an, die während der Migration gleichzeitig zusammengeführt werden sollen.

Indizes im Warmspeicher sind schreibgeschützt, es sei denn, Sie geben sie in den Hotspeicher zurück. Dies ist UltraWarm am besten für unveränderliche Daten wie Protokolle geeignet. Sie können die Indizes abfragen und löschen, aber Sie können keine einzelnen Dokumente hinzufügen, aktualisieren oder löschen. Wenn Sie es versuchen, wird möglicherweise der folgende Fehler angezeigt:

```
{
  "error" : {
    "root_cause" : [
      {
        "type" : "cluster_block_exception",
```

```
        "reason" : "index [indexname] blocked by: [TOO_MANY_REQUESTS/12/disk usage
 exceeded flood-stage watermark, index has read-only-allow-delete block];"
      }
    ],
    "type" : "cluster_block_exception",
    "reason" : "index [indexname] blocked by: [TOO_MANY_REQUESTS/12/disk usage exceeded
 flood-stage watermark, index has read-only-allow-delete block];"
  },
  "status" : 429
}
```

Automatisieren von Migrationen

Wir empfehlen die Verwendung von the section called “Indexstatusmanagement” zur Automatisierung des Migrationsprozesses, nachdem ein Index ein bestimmtes Alter erreicht hat oder andere Bedingungen erfüllt. Sehen Sie sich die Beispielrichtlinie an, die diesen Workflow veranschaulicht.

Migrationsoptimierung

Für Indexmigrationen in den Speicher ist eine erzwungene Zusammenführung erforderlich. UltraWarm Jeder OpenSearch Index besteht aus einer bestimmten Anzahl von Shards, und jeder Shard besteht aus einer bestimmten Anzahl von Lucene-Segmenten. Der Vorgang der erzwungenen Zusammenführung löscht Dokumente, die zum Löschen markiert wurden, und spart Speicherplatz. Führt Indizes standardmäßig zu UltraWarm einem Segment zusammen.

Sie können diesen Wert mit der `index.ultrawarm.migration.force_merge.max_num_segments`-Einstellung auf bis zu 1.000 Segmente ändern. Höhere Werte beschleunigen den Migrationsprozess, erhöhen jedoch die Abfragelatenz für den warmen Index nach Abschluss der Migration. Um die Einstellung zu ändern, stellen Sie die folgende Anfrage:

```
PUT my-index/_settings
{
  "index": {
    "ultrawarm": {
      "migration": {
        "force_merge": {
          "max_num_segments": 1
        }
      }
```

```
    }
  }
}
```

Um zu überprüfen, wie lange diese Phase des Migrationsprozesses dauert, überwachen Sie die `HotToWarmMigrationForceMergeLatency`-Metrik.

Abbrechen von Migrationen

UltraWarm verarbeitet Migrationen sequentiell in einer Warteschlange. Wenn sich eine Migration in der Warteschlange befindet, aber noch nicht gestartet wurde, können Sie sie mit der folgenden Anforderung aus der Warteschlange entfernen:

```
POST _ultrawarm/migration/_cancel/my-index
```

Wenn Ihre Domain eine differenzierte Zugriffskontrolle verwendet, müssen Sie die `indices:admin/ultrawarm/migration/cancel`-Berechtigung haben, um diese Anfrage zu stellen.

Auflisten von Hot- und Warm-Indizes

UltraWarm fügt zwei zusätzliche Optionen hinzu, ähnlich wie`_all`, um die Verwaltung von Hot- und Warm-Indizes zu erleichtern. Für eine Auflistung aller Warm- oder Hot-Indizes, tätigen Sie folgende Anforderungen:

```
GET _warm
GET _hot
```

Sie können diese Optionen in anderen Anforderungen verwenden, die Indizes angeben, zum Beispiel:

```
_cat/indices/_warm
_cluster/state/_all/_hot
```

Warm-Indizes in den Hot Storage zurückbringen

Wenn Sie noch einmal in einen Index schreiben müssen, migrieren Sie ihn zurück in den Hot Storage:

```
POST _ultrawarm/migration/my-index/_hot
```

Sie können bis zu 10 Migrationen vom Warm- zum Hot-Speicher gleichzeitig in der Warteschlange durchführen. OpenSearch Der Service verarbeitet Migrationsanfragen nacheinander in der Reihenfolge, in der sie sich in der Warteschlange befanden. Überwachen Sie die `WarmToHotMigrationQueueSize`-Metrik, um die aktuelle Anzahl zu überprüfen.

Überprüfen Sie nach Abschluss der Migration die Indexeinstellungen, um sicherzustellen, dass sie Ihren Anforderungen entsprechen. Indizes werden mit einem Replikat im Hot Storage wiederhergestellt.

Warme Indizes aus Snapshots wiederherstellen

Fügt zusätzlich zum Standard-Repository für automatisierte Snapshots ein zweites Repository für warme Indizes UltraWarm hinzu. `cs-ultrawarm` Jeder Snapshot in diesem Repository enthält nur einen Index. Wenn Sie einen warmen Index löschen, bleibt sein Snapshot wie jeder andere automatisierte Snapshot 14 Tage lang im `cs-ultrawarm`-Repository.

Wenn Sie einen Snapshot aus `cs-ultrawarm` wiederherstellen, wird er im Warm Storage und nicht im Hot Storage wiederhergestellt. Snapshots in den Repositorys `cs-automated` und `cs-automated-enc` werden im Hot Storage wiederhergestellt.

Um einen UltraWarm Snapshot im Warmspeicher wiederherzustellen

1. Identifizieren Sie den neuesten Snapshot, der den Index enthält, den Sie wiederherstellen möchten:

   ```
   GET _snapshot/cs-ultrawarm/_all?verbose=false

   {
     "snapshots": [{
       "snapshot": "snapshot-name",
       "version": "1.0",
       "indices": [
         "my-index"
       ]
     }]
   }
   ```

> **Note**
>
> Standardmäßig zeigt der `GET _snapshot/<repo>` Vorgang ausführliche Dateninformationen wie Startzeit, Endzeit und Dauer für jeden Snapshot innerhalb eines Repositorys an. Der `GET _snapshot/<repo>` Vorgang ruft Informationen aus den Dateien der einzelnen Snapshots ab, die in einem Repository enthalten sind. Wenn Sie die Startzeit, Endzeit und Dauer nicht benötigen und nur den Namen und die Indexinformationen eines Snapshots benötigen, empfehlen wir, den `verbose=false` Parameter beim Auflisten von Snapshots zu verwenden, um die Verarbeitungszeit zu minimieren und Zeitüberschreitungen zu vermeiden.

2. Wenn der Index bereits vorhanden ist, löschen Sie ihn:

```
DELETE my-index
```

   Wenn Sie den Index nicht löschen möchten, legen Sie ihn in den Hot Storage zurück und indizieren Sie ihn neu.

3. Stellen Sie den Snapshot wieder her:

```
POST _snapshot/cs-ultrawarm/snapshot-name/_restore
```

   UltraWarm ignoriert alle Indexeinstellungen, die Sie in dieser Wiederherstellungsanforderung angeben, aber Sie können Optionen wie `rename_pattern` und angeben. `rename_replacement` Eine Zusammenfassung der Optionen zur Wiederherstellung von OpenSearch Snapshots finden Sie in der OpenSearch Dokumentation.

Manuelle Snapshots von Warm-Indizes

Sie können manuelle Snapshots von Warm-Indizes erstellen, dies wird jedoch nicht empfohlen. Das automatisierte `cs-ultrawarm`-Repository enthält bereits ohne Aufpreis einen Snapshot für jeden warmen Index, der während der Migration erstellt wurde.

Standardmäßig schließt OpenSearch Service keine warmen Indizes in manuelle Snapshots ein. Der folgende Aufruf enthält beispielsweise nur Hot-Indizes:

```
PUT _snapshot/my-repository/my-snapshot
```

Wenn Sie manuelle Snapshots von Warm-Indizes erstellen möchten, müssen mehrere wichtige Überlegungen angestellt werden.

- Sie können Hot- und Warm-Indizes nicht mischen. Die folgende Anfrage schlägt beispielsweise fehl:

  ```
  PUT _snapshot/my-repository/my-snapshot
  {
    "indices": "warm-index-1,hot-index-1",
    "include_global_state": false
  }
  ```

  Wenn sie eine Mischung aus Hot- und Warm-Indizes enthalten, schlagen auch Platzhalter (*)-Anweisungen fehl.

- Sie können nur einen warmen Index pro Snapshot einschließen. Die folgende Anfrage schlägt beispielsweise fehl:

  ```
  PUT _snapshot/my-repository/my-snapshot
  {
    "indices": "warm-index-1,warm-index-2,other-warm-indices-*",
    "include_global_state": false
  }
  ```

  Diese Anfrage ist erfolgreich:

  ```
  PUT _snapshot/my-repository/my-snapshot
  {
    "indices": "warm-index-1",
    "include_global_state": false
  }
  ```

- Manuelle Snapshots werden immer im Hot Storage wiederhergestellt, auch wenn sie ursprünglich einen warmen Index enthielten.

Migration Warm-Indizes in Cold Storage

Wenn Sie Daten haben, die Sie selten abfragen UltraWarm , sollten Sie erwägen, sie in einen Cold Storage zu migrieren. Cold Storage ist für Daten gedacht, auf die Sie nur gelegentlich zugreifen oder die nicht mehr aktiv genutzt werden. Sie können Cold-Indizes weder lesen noch in sie schreiben,

aber Sie können sie kostenlos zurück in den Warm-Speicher migrieren, wann immer Sie sie abfragen müssen. Anweisungen finden Sie unter the section called “Migration von Indizes auf Cold-Speicher”.

Deaktivierung UltraWarm

Die Konsole ist die einfachste Methode zum Deaktivieren UltraWarm. Klicken Sie auf die Domain, wählen Sie Aktionen und Clusterkonfiguration bearbeiten. Deaktivieren Sie die Option UltraWarm Datenknoten aktivieren und wählen Sie Änderungen speichern. Sie können die `WarmEnabled`-Option auch in der AWS CLI und der Konfigurations-API verwenden.

Vor der Deaktivierung UltraWarm müssen Sie entweder alle warmen Indizes löschen oder sie zurück in den Hot-Storage migrieren. Wenn der Warmspeicher leer ist, warten Sie fünf Minuten, bevor Sie versuchen, ihn zu deaktivieren UltraWarm.

Kühlhaus für Amazon OpenSearch Service

Mit Cold Storage können Sie jede Menge selten aufgerufener oder historischer Daten auf Ihrer Amazon OpenSearch Service-Domain speichern und bei Bedarf analysieren, und das zu geringeren Kosten als bei anderen Speicherstufen. Cold-Speicherung ist geeignet, wenn Sie regelmäßige Untersuchungen oder forensische Analysen an Ihren älteren Daten durchführen müssen. Praktische Beispiele für Daten, die für Cold-Speicher geeignet sind, sind selten aufgerufene Protokolle, Daten, die aufbewahrt werden müssen, um Compliance-Anforderungen zu erfüllen, oder Protokolle mit historischem Wert.

Ähnlich wie UltraWarmSpeicher wird Cold Storage von Amazon S3 unterstützt. Wenn Sie kalte Daten abfragen müssen, können Sie sie selektiv an bestehende UltraWarm Knoten anhängen. Sie können die Migration und den Lebenszyklus Ihrer Cold-Daten manuell oder mit Index-Statusmanagement-Verwaltungsrichtlinien verwalten.

Themen

- Automatisierung von Migrationen zum Cold-Speicher
- Abbruch von Migrationen zum Cold-Speicher
- Kalte Indizes auflisten
- Migrieren von Cold-Indizes zum Warm-Speicher
- Wiederherstellen von Cold-Indizes aus Snapshots
- Abbruch von Migrationen von Cold- zu Warm-Speicher
- Cold-Index-Metadaten aktualisieren
- Kalte Indizes löschen
- Deaktivieren von Cold-Speicherung

Voraussetzungen

Cold-Speicherung hat die folgenden Voraussetzungen:

- Für Cold Storage ist Elasticsearch Version 7.9 oder höher erforderlich OpenSearch .
- Um Cold Storage auf einer OpenSearch Service-Domain zu aktivieren, müssen Sie die Aktivierung auch UltraWarm auf derselben Domain durchführen.
- Um einen Cold-Speicher verwenden zu können, müssen Domänen über dedizierte Hauptknoten verfügen.
- Wenn Ihre Domäne einen T2- oder T3-Instance-Typ für Ihre Datenknoten verwendet, können Sie keinen Cold-Speicher verwenden.
- Wenn Ihr Index approximate k-NN (`"index.knn": true`) verwendet, können Sie ihn nicht in einen kühlen Speicher verschieben.
- Wenn die Domain eine differenzierte Zugriffskontrolle verwendet, müssen Benutzer ohne Administratorrechte der `cold_manager` Rolle in OpenSearch Dashboards zugeordnet werden, um Cold-Indizes verwalten zu können.

> **Note**
>
> Die `cold_manager` Rolle ist in einigen bereits vorhandenen Dienstdomänen möglicherweise nicht vorhanden. OpenSearch Wenn die Rolle in Dashboards nicht angezeigt wird, müssen Sie sie manuell erstellen.

So konfigurieren Sie Berechtigungen

Wenn Sie Cold Storage in einer bereits vorhandenen OpenSearch Dienstdomäne aktivieren, ist die `cold_manager` Rolle möglicherweise nicht für die Domäne definiert. Wenn die Domäne eine differenzierte Zugriffskontrolle verwendet, müssen Benutzer ohne Administratorrechte dieser Rolle zugeordnet werden, um Cold-Indizes verwalten zu können. Führen Sie die folgenden Schritte aus, um die `cold_manager`-Rolle manuell zu erstellen:

1. Gehen Sie in OpenSearch Dashboards zu Sicherheit und wählen Sie Berechtigungen aus.
2. Wählen Sie Aktionsgruppe erstellen und konfigurieren Sie die folgenden Gruppen:

Group name (Gruppenname)	Berechtigungen
`cold_cluster`	• `cluster:monitor/nodes/stats` • `cluster:admin/ultrawarm*` • `cluster:admin/cold/*`
`cold_index`	• `indices:monitor/stats` • `indices:data/read/minmax` • `indices:admin/ultrawarm/migration/get` • `indices:admin/ultrawarm/migration/cancel`

3. Wählen Sie Rollen und Rolle erstellen.
4. Benennen Sie die Rolle cold_manager.
5. Wählen Sie für Cluster-Berechtigungen die `cold_cluster`-Gruppe, die Sie erstellt haben.
6. Geben Sie für Index * ein.
7. Wählen Sie für Index-Berechtigungen die `cold_index`-Gruppe, die Sie erstellt haben.
8. Wählen Sie Erstellen.
9. Nachdem Sie die Rolle erstellt haben, ordnen Sie sie einer beliebigen Benutzer- oder Backend-Rolle zu, die kalte Indizes verwaltet.

Cold-Speicheranforderungen und Leistungsüberlegungen

Da Cold Storage Amazon S3 verwendet, entsteht kein Overhead von Hot Storage wie Repliken, reserviertem Linux-Speicherplatz und reserviertem OpenSearch Service-Speicherplatz. Cold-Speicher hat keine spezifischen Instance-Typen, da ihm keine Rechenkapazität zugeordnet ist. Sie können beliebig viele Daten im Cold-Speicher speichern. Überwachen Sie die `ColdStorageSpaceUtilization` Metrik in Amazon CloudWatch , um zu sehen, wie viel Kühlraum Sie verwenden.

Preise für Cold-Speicherung

Ähnlich wie bei der UltraWarm Lagerung zahlen Sie bei Cold Storage nur für die Datenspeicherung. Es fallen keine Rechenkosten für Cold-Daten an und Sie werden nicht in Rechnung gestellt, wenn keine Daten im Cold-Speicher vorhanden sind.

Beim Verschieben von Daten zwischen Cold- und Warm-Speicher fallen keine Transfergebühren an. Während Indizes zwischen Warm- und Cold-Speicher migriert werden, zahlen Sie weiterhin nur für eine Kopie des Indexes. Nach Abschluss der Migration wird der Index entsprechend der Speicherstufe in Rechnung gestellt, auf die er migriert wurde. Weitere Informationen zu den Preisen für Kühlhäuser finden Sie unter Amazon OpenSearch Service-Preise.

Aktivieren von Cold-Speicherung

Die Konsole ist die einfachste Möglichkeit, eine Domäne zu erstellen, die Cold-Speicher verwendet. Wählen Sie beim Erstellen der Domäne Aktivieren von Cold-Speicherung. Derselbe Prozess funktioniert auf vorhandenen Domänen, sofern sie die Voraussetzungen erfüllen. Selbst nachdem der Domänenstatus von Processing (Verarbeitung) zu Active (Aktiv) geändert wurde, steht Cold-Speicher möglicherweise mehrere Stunden lang nicht zur Verfügung.

Sie können auch die AWS CLI oder Konfigurations-API verwenden, um die Cold-Speicherung zu aktivieren.

Beispiel für einen CLI-Befehl

Der folgende AWS CLI Befehl erstellt eine Domain mit drei Datenknoten, drei dedizierten Master-Knoten, aktiviertem Kühlspeicher und aktivierter detaillierter Zugriffskontrolle:

```
aws opensearch create-domain \
  --domain-name my-domain \
  --engine-version Opensearch_1.0 \
```

```
  --cluster-
config ColdStorageOptions={Enabled=true},WarmEnabled=true,WarmCount=4,WarmType=ultrawarm1.mediu
 \
  --ebs-options EBSEnabled=true,VolumeType=gp2,VolumeSize=11 \
  --node-to-node-encryption-options Enabled=true \
  --encryption-at-rest-options Enabled=true \
  --domain-endpoint-options EnforceHTTPS=true,TLSSecurityPolicy=Policy-Min-
TLS-1-2-2019-07 \
  --advanced-security-options
 Enabled=true,InternalUserDatabaseEnabled=true,MasterUserOptions='{MasterUserName=master-
user,MasterUserPassword=master-password}' \
  --region us-east-2
```

Weitere Informationen finden Sie in der AWS CLI -Befehlsreferenz.

Beispiel für eine Konfigurations-API-Anforderung

Die folgende Anfrage an die Konfigurations-API erstellt eine Domäne mit drei Datenknoten, drei dedizierten Hauptknoten, aktiviertem Cold-Speicher und aktivierter feingranularer Zugriffskontrolle:

```
POST https://es.us-east-2.amazonaws.com/2021-01-01/opensearch/domain
{
  "ClusterConfig": {
    "InstanceCount": 3,
    "InstanceType": "r6g.large.search",
    "DedicatedMasterEnabled": true,
    "DedicatedMasterType": "r6g.large.search",
    "DedicatedMasterCount": 3,
    "ZoneAwarenessEnabled": true,
    "ZoneAwarenessConfig": {
      "AvailabilityZoneCount": 3
     },
    "WarmEnabled": true,
    "WarmCount": 4,
    "WarmType": "ultrawarm1.medium.search",
    "ColdStorageOptions": {
       "Enabled": true
     }
  },
  "EBSOptions": {
    "EBSEnabled": true,
    "VolumeType": "gp2",
    "VolumeSize": 11
```

```
  },
  "EncryptionAtRestOptions": {
    "Enabled": true
  },
  "NodeToNodeEncryptionOptions": {
    "Enabled": true
  },
  "DomainEndpointOptions": {
    "EnforceHTTPS": true,
    "TLSSecurityPolicy": "Policy-Min-TLS-1-2-2019-07"
  },
   "AdvancedSecurityOptions": {
    "Enabled": true,
    "InternalUserDatabaseEnabled": true,
    "MasterUserOptions": {
      "MasterUserName": "master-user",
      "MasterUserPassword": "master-password"
    }
  },
  "EngineVersion": "Opensearch_1.0",
  "DomainName": "my-domain"
}
```

Ausführliche Informationen finden Sie in der Amazon OpenSearch Service API-Referenz.

Verwaltung von Cold-Indizes in Dashboards OpenSearch

Sie können heiße, warme und kalte Indizes mit der vorhandenen Dashboard-Oberfläche in Ihrer Service-Domain verwalten. OpenSearch Mit Dashboards können Sie Indizes zwischen Warm- und Cold-Speicher migrieren und den Indexmigrationsstatus überwachen, ohne die CLI oder die Konfigurations-API zu verwenden. Weitere Informationen finden Sie unter Indizes in Dashboards verwalten. OpenSearch

Migration von Indizes auf Cold-Speicher

Wenn Sie Indizes in den Cold-Speicher migrieren, geben Sie einen Zeitbereich für die Daten an, um die Suche zu erleichtern. Sie können ein Zeitstempelfeld basierend auf den Daten in Ihrem Index auswählen, manuell einen Start- und Endzeitstempel angeben oder gar keinen angeben.

Parameter	Unterstützter Wert	Beschreibung
`timestamp_field`	Das Datum/Uhrzeitfeld aus dem Index-Mapping.	Die Minimal- und Maximalwerte des bereitgestellten Feldes werden berechnet und als `start_time` - und `end_time`-Metadaten für den Cold-Index gespeichert.
`start_time` und `end_time`	Eines der folgenden Formate: • strict_date_optional_time. Zum Beispiel `yyyy-MM-dd'T'HH:mm:ss.SSSZ` oder `yyyy-MM-dd` • Epochenzeit in Millisekunden	Die angegebenen Werte werden berechnet und als `start_time` - und `end_time`-Metadaten für den Cold-Index gespeichert.

Wenn Sie keinen Zeitstempel angeben möchten, fügen Sie stattdessen `?ignore=timestamp` zur Anfrage hinzu.

Die folgende Anforderung migriert einen Warm-Index in den Cold-Speicher und stellt Start- und Endzeiten für die Daten in diesem Index bereit:

```
POST _ultrawarm/migration/my-index/_cold
  {
    "start_time": "2020-03-09",
    "end_time": "2020-03-09T23:00:00Z"
  }
```

Überprüfen Sie dann den Status der Migration:

```
GET _ultrawarm/migration/my-index/_status

{
  "migration_status": {
    "index": "my-index",
    "state": "RUNNING_METADATA_RELOCATION",
```

```
    "migration_type": "WARM_TO_COLD"
  }
}
```

OpenSearch Der Service migriert jeweils einen Index in einen Cold Storage. Sie können bis zu 100 Migrationen in der Warteschlange haben. Jede Anfrage, die das Limit überschreitet, wird abgelehnt. Um die aktuelle Anzahl von Migrationen in der Warteschlange zu überprüfen, überwachen Sie die `WarmToColdMigrationQueueSize`-Metrik. Der Migrationsprozess weist die folgenden Zustände auf:

```
ACCEPTED_COLD_MIGRATION - Migration request is accepted and queued.
RUNNING_METADATA_MIGRATION - The migration request was selected for execution and
 metadata is migrating to cold storage.
FAILED_METADATA_MIGRATION - The attempt to add index metadata has failed and all
 retries are exhausted.
PENDING_INDEX_DETACH - Index metadata migration to cold storage is completed. Preparing
 to detach the warm index state from the local cluster.
RUNNING_INDEX_DETACH - Local warm index state from the cluster is being removed. Upon
 success, the migration request will be completed.
FAILED_INDEX_DETACH - The index detach process failed and all retries are exhausted.
```

Automatisierung von Migrationen zum Cold-Speicher

Sie können Index-Stausmanagement verwenden, um den Migrationsprozess zu automatisieren, nachdem ein Index ein bestimmtes Alter erreicht hat oder andere Bedingungen erfüllt. Sehen Sie sich die Beispielrichtlinie an, die zeigt, wie Indizes automatisch von Hot UltraWarm zu Cold Storage migriert werden.

> **Note**
>
> Ein explizites `timestamp_field` ist erforderlich, um Indizes mithilfe einer Index-Statusmanagement-Richtlinie in den Cold-Speicher zu verlagern.

Abbruch von Migrationen zum Cold-Speicher

Wenn eine Migration zum Cold-Speicher in der Warteschlange oder in einem fehlgeschlagenen Zustand ist, können Sie die Migration mit der folgenden Anforderung abbrechen:

```
POST _ultrawarm/migration/_cancel/my-index
```

```
{
  "acknowledged" : true
}
```

Wenn Ihre Domäne differenzierte Zugriffskontrolle verwendet, benötigen Sie die `indices:admin/ultrawarm/migration/cancel`-Berechtigung, um diese Anfrage zu stellen.

Kalte Indizes auflisten

Vor der Abfrage können Sie die Indizes im Cold Storage auflisten, um zu entscheiden, zu welchen Indizes Sie UltraWarm für weitere Analysen migrieren möchten. Die folgende Anfrage listet alle Cold-Indizes, sortiert nach Indexnamen, auf:

```
GET _cold/indices/_search
```

Beispielantwort

```
{
  "pagination_id" : "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY",
  "total_results" : 3,
  "indices" : [
    {
      "index" : "my-index-1",
      "index_cold_uuid" : "hjEoh26mRRCFxRIMdgvLmg",
      "size" : 10339,
      "creation_date" : "2021-06-28T20:23:31.206Z",
      "start_time" : "2020-03-09T00:00Z",
      "end_time" : "2020-03-09T23:00Z"
    },
    {
      "index" : "my-index-2",
      "index_cold_uuid" : "0vIS2n-oROmOWDFmwFIgdw",
      "size" : 6068,
      "creation_date" : "2021-07-15T19:41:18.046Z",
      "start_time" : "2020-03-09T00:00Z",
      "end_time" : "2020-03-09T23:00Z"
    },
    {
      "index" : "my-index-3",
      "index_cold_uuid" : "EaeXOBodTLiDYcivKsXVLQ",
      "size" : 32403,
```

```
      "creation_date" : "2021-07-08T00:12:01.523Z",
      "start_time" : "2020-03-09T00:00Z",
      "end_time" : "2020-03-09T23:00Z"
    }
  ]
}
```

Filtern

Sie können Cold-Indizes basierend auf einem Präfix-basierten Indexmuster und Zeitbereich-Offsets filtern.

Die folgende Anforderung listet Indizes auf, die mit dem Präfixmuster von `event-*` übereinstimmen:

```
GET _cold/indices/_search
 {
   "filters":{
      "index_pattern": "event-*"
   }
 }
```

Beispielantwort

```
{
  "pagination_id" : "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY",
  "total_results" : 1,
  "indices" : [
    {
      "index" : "events-index",
      "index_cold_uuid" : "4eFiab7rRfSvp3slrIsIKA",
      "size" : 32263273,
      "creation_date" : "2021-08-18T18:25:31.845Z",
      "start_time" : "2020-03-09T00:00Z",
      "end_time" : "2020-03-09T23:00Z"
    }
  ]
}
```

Die folgende Anforderung gibt Indizes mit `start_time`- und `end_time`-Metadaten-Feldern zwischen `2019-03-01` und `2020-03-01` zurück:

```
GET _cold/indices/_search
```

```
{
  "filters": {
    "time_range": {
      "start_time": "2019-03-01",
      "end_time": "2020-03-01"
    }
  }
}
```

Beispielantwort

```
{
  "pagination_id" : "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY",
  "total_results" : 1,
  "indices" : [
    {
      "index" : "my-index",
      "index_cold_uuid" : "4eFiab7rRfSvp3slrIsIKA",
      "size" : 32263273,
      "creation_date" : "2021-08-18T18:25:31.845Z",
      "start_time" : "2019-05-09T00:00Z",
      "end_time" : "2019-09-09T23:00Z"
    }
  ]
}
```

Sortieren

Sie können Cold-Indizes nach Metadatenfeldern wie Indexname oder Größe sortieren. Die folgende Abfrage listet alle Indizes nach Größe sortiert in absteigender Reihenfolge auf:

```
GET _cold/indices/_search
 {
 "sort_key": "size:desc"
 }
```

Beispielantwort

```
{
  "pagination_id" : "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY",
  "total_results" : 5,
```

```
  "indices" : [
    {
      "index" : "my-index-6",
      "index_cold_uuid" : "4eFiab7rRfSvp3slrIsIKA",
      "size" : 32263273,
      "creation_date" : "2021-08-18T18:25:31.845Z",
      "start_time" : "2020-03-09T00:00Z",
      "end_time" : "2020-03-09T23:00Z"
    },
    {
      "index" : "my-index-9",
      "index_cold_uuid" : "mbD3ZRVDRI6ONqgEOsJyUA",
      "size" : 57922,
      "creation_date" : "2021-07-07T23:41:35.640Z",
      "start_time" : "2020-03-09T00:00Z",
      "end_time" : "2020-03-09T23:00Z"
    },
    {
      "index" : "my-index-5",
      "index_cold_uuid" : "EaeXOBodTLiDYcivKsXVLQ",
      "size" : 32403,
      "creation_date" : "2021-07-08T00:12:01.523Z",
      "start_time" : "2020-03-09T00:00Z",
      "end_time" : "2020-03-09T23:00Z"
    }
  ]
}
```

Andere gültige Sortierschlüssel sind `start_time:asc/desc`, `end_time:asc/desc` und `index_name:asc/desc`.

Paginierung

Sie können eine Liste mit kalten Indizes paginieren. Konfigurieren Sie die Anzahl der Indizes, die pro Seite zurückgegeben werden sollen, mit dem `page_size`-Parameter (der Standardwert ist 10). Jede `_search`-Anfrage auf Ihre Cold-Indizes gibt eine `pagination_id` zurück, die Sie für nachfolgende Aufrufe verwenden können.

Die folgende Anforderung paginiert die Ergebnisse einer `_search`-Anfrage Ihrer Cold-Indizes und zeigt die nächsten 100 Ergebnisse an:

```
GET _cold/indices/_search?page_size=100
```

```
{
"pagination_id": "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY"
}
```

Migrieren von Cold-Indizes zum Warm-Speicher

Nachdem Sie die Liste der Kaltindizes anhand der Filterkriterien aus dem vorherigen Abschnitt eingegrenzt haben, migrieren Sie sie wieder dorthin, UltraWarm wo Sie die Daten abfragen und zum Erstellen von Visualisierungen verwenden können.

Die folgende Anfrage migriert zwei Cold-Indizes zurück in den Warm-Speicher:

```
POST _cold/migration/_warm
 {
 "indices": "my-index1,my-index2"
 }


{
  "acknowledged" : true
}
```

Um den Status der Migration zu überprüfen und die Migrations-ID abzurufen, senden Sie die folgende Anforderung:

```
GET _cold/migration/_status
```

Beispielantwort

```
{
  "cold_to_warm_migration_status" : [
    {
      "migration_id" : "tyLjXCA-S76zPQbPVHkOKA",
      "indices" : [
        "my-index1,my-index2"
      ],
      "state" : "RUNNING_INDEX_CREATION"
    }
  ]
}
```

Um indexspezifische Migrationsinformationen abzurufen, geben Sie den Indexnamen ein:

```
GET _cold/migration/my-index/_status
```

Anstatt einen Index anzugeben, können Sie die Indizes nach ihrem aktuellen Migrationsstatus auflisten. Gültige Werte sind `_failed`, `_accepted` und `_all`.

Der folgende Befehl ruft den Status aller Indizes in einer einzelnen Migrationsanforderung ab:

```
GET _cold/migration/_status?migration_id=my-migration-id
```

Rufen Sie die Migrations-ID mit der Statusanforderung ab. Für detaillierte Migrationsinformationen fügen Sie `&verbose=true` hinzu.

Sie können Indizes aus dem kalten in den warmen Speicher in Batches von 10 oder weniger migrieren, wobei maximal 100 Indizes gleichzeitig migriert werden können. Jede Anfrage, die das Limit überschreitet, wird abgelehnt. Um die aktuelle Anzahl von Migrationen zu überprüfen, überwachen Sie die `ColdToWarmMigrationQueueSize`-Metrik. Der Migrationsprozess weist die folgenden Zustände auf:

```
ACCEPTED_MIGRATION_REQUEST - Migration request is accepted and queued.
RUNNING_INDEX_CREATION - Migration request is picked up for processing and will create
 warm indexes in the cluster.
PENDING_COLD_METADATA_CLEANUP - Warm index is created and the migration service will
 attempt to clean up cold metadata.
RUNNING_COLD_METADATA_CLEANUP - Cleaning up cold metadata from the indexes migrated to
 warm storage.
FAILED_COLD_METADATA_CLEANUP - Failed to clean up metadata in the cold tier.
FAILED_INDEX_CREATION - Failed to create an index in the warm tier.
```

Wiederherstellen von Cold-Indizes aus Snapshots

Wenn Sie einen gelöschten kalten Index wiederherstellen müssen, können Sie ihn wieder auf die warme Ebene zurücksetzen, indem Sie den Anweisungen unter folgen the section called “Warme Indizes aus Snapshots wiederherstellen” und den Index dann wieder auf die kalte Ebene migrieren. Sie können einen gelöschten Cold-Index nicht direkt wieder auf die Cold-Ebene zurücksetzen. OpenSearch Der Service behält kalte Indizes 14 Tage lang, nachdem sie gelöscht wurden.

Abbruch von Migrationen von Cold- zu Warm-Speicher

Wenn eine Indexmigration von Cold- zu Warm-Speicher in die Warteschlange gestellt wird oder sich in einem fehlgeschlagenen Zustand befindet, können Sie sie mit der folgenden Anforderung abbrechen:

```
POST _cold/migration/my-index/_cancel

{
  "acknowledged" : true
}
```

Um die Migration für einen Batch von Indizes abzubrechen (maximal 10 gleichzeitig), geben Sie die Migrations-ID an:

```
POST _cold/migration/_cancel?migration_id=my-migration-id

{
  "acknowledged" : true
}
```

Rufen Sie die Migrations-ID mit der Statusanforderung ab.

Cold-Index-Metadaten aktualisieren

Sie können die `start_time`- und `end_time`-Felder für einen Cold-Index aktualisieren:

```
PATCH _cold/my-index
 {
 "start_time": "2020-01-01",
 "end_time": "2020-02-01"
 }
```

Sie können nicht die `timestamp_field` eines Indexes im Cold-Speicher aktualiseiren.

> **Note**
>
> OpenSearch Dashboards unterstützt die PATCH-Methode nicht. Verwenden Sie curl, Postman oder eine andere Methode, um Cold-Metadaten zu aktualisieren.

Kalte Indizes löschen

Wenn Sie keine ISM-Richtlinie verwenden, können Sie Cold-Indizes manuell löschen. Die folgende Anforderung löscht einen Cold-Index:

```
DELETE _cold/my-index

{
  "acknowledged" : true
}
```

Deaktivieren von Cold-Speicherung

Die OpenSearch Servicekonsole ist die einfachste Möglichkeit, Cold Storage zu deaktivieren. Wählen Sie die Domäne aus und wählen Sie Aktionen, Clusterkonfiguration bearbeiten und deaktivieren Sie dann Cold-Speicher aktivieren.

Um die AWS CLI oder die Konfigurations-API zu verwenden`ColdStorageOptions`, setzen Sie unter`"Enabled"="false"`.

Bevor Sie den Cold-Speicher deaktivieren, müssen Sie entweder alle Cold-Indizes löschen oder sie wieder in den Warm-Speicher migrieren. Andernfalls schlägt die Deaktivierungsaktion fehl.

OR1-Speicher für Amazon Service OpenSearch

OR1 ist eine Instance-Familie für Amazon OpenSearch Service, die eine kostengünstige Möglichkeit bietet, große Datenmengen zu speichern. Eine Domain mit OR1-Instances verwendet Amazon Elastic Block Store (Amazon EBS) `gp3` oder `io1` Volumes als Primärspeicher, wobei die Daten synchron nach Amazon S3 kopiert werden, sobald sie ankommen. Diese Speicherstruktur bietet einen erhöhten Indexierungsdurchsatz bei hoher Haltbarkeit. Die OR1-Instance-Familie unterstützt auch die automatische Datenwiederherstellung im Falle eines Fehlers. Informationen zu den Optionen für den OR1-Instance-Typ finden Sie unter. the section called “Instance-Typen der aktuellen Generation”

Wenn Sie umfangreiche Workloads für Betriebsanalysen wie Protokollanalysen, Observability oder Sicherheitsanalysen indizieren, können Sie von der verbesserten Leistung und Recheneffizienz von OR1-Instances profitieren. Darüber hinaus verbessert die automatische Datenwiederherstellung, die von OR1-Instances angeboten wird, die allgemeine Zuverlässigkeit Ihrer Domain.

OpenSearch Der Service sendet speicherbezogene OR1-Metriken an Amazon. CloudWatch Eine Liste der verfügbaren Metriken finden Sie unter ???.

OR1-Instances sind auf Abruf oder mit Reserved Instance-Preisen erhältlich, wobei ein Stundensatz für die in Amazon EBS und Amazon S3 bereitgestellten Instances und Speicher gilt.

Themen

Einschränkungen

Beachten Sie die folgenden Einschränkungen, wenn Sie OR1-Instances für Ihre Domain verwenden.

- Auf Ihrer Domain muss OpenSearch Version 2.11 oder höher ausgeführt werden.
- Für Ihre Domain muss die Verschlüsselung im Ruhezustand aktiviert sein. Weitere Informationen finden Sie unter ???.
- Ihre Domain muss eine neue Domain sein. Sie können eine bestehende Domain nicht ändern, um OR1-Instances zu verwenden.
- Wenn Ihre Domain dedizierte Master-Knoten verwendet, müssen diese Graviton-Instances verwenden. Weitere Informationen zu dedizierten Masterknoten finden Sie unter???.
- Die Shard-Größen auf OR1-Instances müssen kleiner als 100 GiB sein. Shards, die größer als 100 GiB sind, können die Wiederherstellungszeiten verlangsamen. Wenn Sie Shards mit mehr als 100 GiB auf OR1-Instances erstellen, blockiert OpenSearch Service Schreibanforderungen an die Domain. Wenn Sie weiterhin Shards mit mehr als 100 GiB verwenden möchten, wenden Sie sich an uns, AWS Supportum eine Erhöhung des Kontingents zu beantragen.
- Das Aktualisierungsintervall für Indizes auf OR1-Instances muss mindestens 10 Sekunden betragen. Das Standard-Aktualisierungsintervall für OR1-Instances beträgt 10 Sekunden.

Wie unterscheidet sich OR1 von Storage UltraWarm

OpenSearch Der Service bietet UltraWarm Instanzen, die so optimiert sind, dass sie die Kosten für das Speichern warmer Daten reduzieren. Sowohl OR1 als auch UltraWarm Instances speichern Daten lokal in Amazon EBS und remote in Amazon S3. OR1 und UltraWarm Instances unterscheiden sich jedoch in mehreren wichtigen Punkten:

- OR1-Instances speichern eine Kopie der Daten sowohl im lokalen als auch im Remotespeicher. UltraWarm Instanzen speichern Daten hauptsächlich im Remotespeicher, um die Speicherkosten zu senken. Je nach Nutzungsverhalten verschieben sie die Daten möglicherweise in den lokalen Speicher.
- OR1-Instances sind aktiv und können Lese- und Schreibvorgänge akzeptieren, wohingegen die Daten auf UltraWarm Instances schreibgeschützt sind, bis Sie sie manuell zurück in den Hot-Storage verschieben.
- UltraWarm stützt sich aus Gründen der Datenbeständigkeit auf Index-Snapshots. OR1-Instances hingegen führen Replikation und Wiederherstellung im Hintergrund durch. Im Falle eines roten Index stellen OR1-Instances automatisch die fehlenden Shards aus dem Remotespeicher in Amazon S3 wieder her. Die Wiederherstellungszeit hängt von der Menge der wiederherzustellenden Daten ab.

Weitere Hinweise zur UltraWarm Speicherung finden Sie unter???.

OR1-Instances verwenden

Sie können OR1-Instances für Ihre Datenknoten auswählen, wenn Sie eine neue Domain mit dem AWS Management Console, dem AWS Command Line Interface (AWS CLI) oder dem AWS SDK erstellen. Anschließend können Sie die Daten mit Ihren vorhandenen Tools indizieren und abfragen.

Konsole

1. Navigieren Sie zur Amazon OpenSearch Service-Konsole unterhttps://console.aws.amazon.com/aos/.
2. Wählen Sie im linken Navigationsbereich die Option Domains aus.
3. Wählen Sie Domain erstellen aus.
4. Geben Sie einen Namen für Ihre Domain zusammen mit Ihren anderen bevorzugten Optionen ein. Wählen Sie unter Instanzfamilie die Option OR1 aus. Wählen Sie Create aus, um mit der Domain-Erstellung zu beginnen.

AWS CLI

1. Navigieren Sie zu Ihrem AWS CLI Terminal. Informationen zur Installation von finden Sie unter Installieren oder Aktualisieren der neuesten Version von AWS CLI. AWS CLI

2. Um OR1-Speicher zu verwenden, müssen Sie bei der Erstellung einer Domain den Wert der spezifischen Größe des OR1-Instance-Typs in das `InstanceType` Feld eingeben. Sie müssen auch die Verschlüsselung im Ruhezustand aktivieren.

   Im folgenden Beispiel wird eine Domäne mit OR1-Instanzen der Größe `2xlarge` erstellt.

```
aws opensearch create-domain \
  --domain-name test-domain \
  --engine-version OpenSearch_2.11 \
  --cluster-config
 "InstanceType=or1.2xlarge.search,InstanceCount=3,DedicatedMasterEnabled=true,DedicatedMast
 \
  --ebs-options "EBSEnabled=true,VolumeType=gp3,VolumeSize=200" \
  --encryption-at-rest-options Enabled=true \
  --advanced-security-options
 "Enabled=true,InternalUserDatabaseEnabled=true,MasterUserOptions={MasterUserName=test-
user,MasterUserPassword=test-password}" \
  --node-to-node-encryption-options Enabled=true \
  --domain-endpoint-options EnforceHTTPS=true \
  --access-policies '{"Version":"2012-10-17","Statement":
[{"Effect":"Allow","Principal":
{"AWS":"*"},"Action":"es:*","Resource":"arn:aws:es:us-east-1:account-
id:domain/test-domain/*"}]}'
```

Verwaltung des Indexstatus in Amazon OpenSearch Service

Mit Index State Management (ISM) in Amazon OpenSearch Service können Sie benutzerdefinierte Verwaltungsrichtlinien definieren, mit denen Routineaufgaben automatisiert und auf Indizes und Indexmuster angewendet werden. Sie müssen keine externen Prozesse mehr einrichten und verwalten, um Ihre Indexvorgänge auszuführen.

Eine Richtlinie umfasst einen Standardzustand und eine Liste der Zustände, die der Index annehmen kann. Für jeden Zustand können Sie eine Liste der Aktionen definieren, die durchgeführt werden sollen, und welche Bedingungen den Zustandswechsel auslösen. Ein typischer Anwendungsfall besteht darin, alte Indizes regelmäßig nach Ablauf eines bestimmten Zeitraums zu löschen. Beispielsweise können Sie eine Richtlinie definieren, die den Index nach 30 Tagen in einen `read_only`-Status verschiebt und ihn dann nach 90 Tagen endgültig löscht.

NNachdem Sie eine Richtlinie an einen Index angefügt haben, erstellt ISM einen Auftrag, der alle 5 bis 8 Minuten (bzw. 30 bis 48 Minuten bei Clustern vor Version 1.3) ausgeführt wird, um

Richtlinienaktionen durchzuführen, Bedingungen zu prüfen und den Index in verschiedene Zustände zu überführen. Die Basiszeit für die Ausführung dieses Auftrags beträgt alle 5 Minuten, außerdem wird ein zufälliger 0–60 %-Jitter hinzugefügt, um sicherzustellen, dass Ihnen nicht ein gleichzeitiger Anstieg der Aktivität von allen Ihren Indizes angezeigt wird. ISM führt keine Aufträge aus, wenn der Clusterstatus rot ist.

ISM erfordert OpenSearch Elasticsearch 6.8 oder höher.

> **Note**
>
> Diese Dokumentation bietet einen kurzen Überblick über ISM und mehrere Beispielrichtlinien. Außerdem wird erklärt, wie sich ISM für Amazon OpenSearch Service-Domains von ISM auf selbstverwalteten OpenSearch Clustern unterscheidet. Eine vollständige Dokumentation von ISM, einschließlich einer umfassenden Parameterreferenz, Beschreibungen der einzelnen Einstellungen und einer API-Referenz, finden Sie in der OpenSearch Dokumentation unter Index State Management.

> **Important**
>
> Sie können keine Indexvorlagen mehr verwenden, um ISM-Richtlinien auf neu erstellte Indizes anzuwenden. Sie können neu erstellte Indizes weiterhin automatisch mit dem ISM-Vorlagenfeld verwalten. Mit diesem Update wird eine grundlegende Änderung eingeführt, die sich auf bestehende CloudFormation Vorlagen auswirkt, die diese Einstellung verwenden.

Erstellen einer ISM-Richtlinie

So beginnen Sie mit Indexstatusmanagement

1. Öffnen Sie die Amazon OpenSearch Service-Konsole unter https://console.aws.amazon.com/aos/home.
2. Wählen Sie die Domain aus, für die Sie eine ISM-Richtlinie erstellen möchten.
3. Navigieren Sie im Dashboard der Domain zur OpenSearch Dashboard-URL und melden Sie sich mit Ihrem Master-Benutzernamen und Passwort an. Die URL weist das folgende Format auf:

   ```
   domain-endpoint/_dashboards/
   ```

4. Öffnen Sie den linken Navigationsbereich in OpenSearch Dashboards und wählen Sie Indexverwaltung und dann Richtlinie erstellen aus.
5. Sie können den visuellen Editor oder JSON-Editor verwenden, um Richtlinien zu erstellen. Wir empfehlen die Verwendung des visuellen Editors, da er eine strukturiertere Methode zur Definition von Richtlinien bietet. Hilfe beim Erstellen von Richtlinien finden Sie unten in den Beispielrichtlinien.
6. Nachdem Sie eine Richtlinie erstellt haben, fügen Sie sie einer oder mehreren Indizes an:

```
POST _plugins/_ism/add/my-index
{
  "policy_id": "my-policy-id"
}
```

> **Note**
>
> Wenn auf Ihrer Domain eine Legacy-Version von Elasticsearch ausgeführt wird, verwenden Sie `_opendistro`anstelle von `_plugins`.

Wählen Sie alternativ den Index in den OpenSearch Dashboards aus und wählen Sie Richtlinie anwenden aus.

Beispielrichtlinien

Die folgenden Beispielrichtlinien veranschaulichen, wie allgemeine ISM-Anwendungsfälle automatisiert werden.

Hot- zu Warm- zu Cold Storage

Diese Beispielrichtlinie verschiebt einen Index vom Hot-Storage in und UltraWarmschließlich in kalter Speicher. Dann löscht es den Index.

Der Index befindet sich zunächst im `hot`-Zustand. Nach zehn Tagen versetzt ISM es in den `warm`-Zustand. 80 Tage später, nachdem der Index 90 Tage alt ist, versetzt ISM den Index in den `cold`-Zustand. Nach einem Jahr sendet der Service eine Benachrichtigung an einen Amazon-Chime-Raum, dass der Index gelöscht wird und löscht ihn dann endgültig.

Beachten Sie, dass Cold-Indizes die `cold_delete`-Operation erfordern, nicht die normale `delete`-Operation. Beachten Sie auch, dass in Ihren Daten ein explizites `timestamp_field` erforderlich ist, um Cold-Indizes mit ISM zu verwalten.

```
{
  "policy": {
    "description": "Demonstrate a hot-warm-cold-delete workflow.",
    "default_state": "hot",
    "schema_version": 1,
    "states": [{
        "name": "hot",
        "actions": [],
        "transitions": [{
          "state_name": "warm",
          "conditions": {
            "min_index_age": "10d"
          }
        }]
      },
      {
        "name": "warm",
        "actions": [{
          "warm_migration": {},
          "retry": {
            "count": 5,
            "delay": "1h"
          }
        }],
        "transitions": [{
          "state_name": "cold",
          "conditions": {
            "min_index_age": "90d"
          }
        }]
      },
      {
        "name": "cold",
        "actions": [{
            "cold_migration": {
              "timestamp_field": "<your timestamp field>"
            }
          }
        ],
```

```
        "transitions": [{
          "state_name": "delete",
          "conditions": {
             "min_index_age": "365d"
          }
        }]
      },
      {
        "name": "delete",
        "actions": [{
          "notification": {
            "destination": {
              "chime": {
                "url": "<URL>"
              }
            },
            "message_template": {
              "source": "The index {{ctx.index}} is being deleted."
            }
          }
        },
        {
          "cold_delete": {}
        }]
      }
    ]
  }
}
```

Reduzieren der Replikatanzahl

Diese Beispielrichtlinie reduziert die Replikatanzahl nach 7 Tagen auf 0, um Speicherplatz zu sparen, und löscht den Index nach 21 Tagen. Bei dieser Richtlinie wird davon ausgegangen, dass Ihr Index nicht kritisch ist und keine Schreibanforderungen mehr empfängt. Wenn keine Replikate vorhanden sind, birgt dies ein gewisses Risiko für Datenverluste.

```
{
  "policy": {
    "description": "Changes replica count and deletes.",
    "schema_version": 1,
    "default_state": "current",
    "states": [{
        "name": "current",
```

```
        "actions": [],
        "transitions": [{
          "state_name": "old",
          "conditions": {
            "min_index_age": "7d"
          }
        }]
      },
      {
        "name": "old",
        "actions": [{
          "replica_count": {
            "number_of_replicas": 0
          }
        }],
        "transitions": [{
          "state_name": "delete",
          "conditions": {
            "min_index_age": "21d"
          }
        }]
      },
      {
        "name": "delete",
        "actions": [{
          "delete": {}
        }],
        "transitions": []
      }
    ]
  }
}
```

Erstellen eines Index-Snapshots

Diese Beispielrichtlinie verwendet die `snapshot`-Operation, um eine Momentaufnahme eines Indexes zu erstellen, sobald er mindestens ein Dokument enthält. `repository` ist der Name des manuellen Snapshot-Repositorys, das Sie in Amazon S3 registriert haben. `snapshot` ist der Name des Snapshots. Informationen zu Snapshot-Voraussetzungen und Schritten zum Registrieren eines Repositorys finden Sie unter the section called “Erstellen von Index-Snapshots”.

```
{
  "policy": {
```

```
    "description": "Takes an index snapshot.",
    "schema_version": 1,
    "default_state": "empty",
    "states": [{
        "name": "empty",
        "actions": [],
        "transitions": [{
          "state_name": "occupied",
          "conditions": {
            "min_doc_count": 1
          }
        }]
      },
      {
        "name": "occupied",
        "actions": [{
          "snapshot": {
            "repository": "<my-repository>",
            "snapshot": "<my-snapshot>"
            }
          }],
          "transitions": []
      }
    ]
  }
}
```

ISM-Vorlagen

Sie können ein `ism_template`-Feld in einer Richtlinie einrichten, sodass beim Erstellen eines Index, der dem Vorlagenmuster entspricht, die Richtlinie automatisch an diesen Index angehängt wird. In diesem Beispiel wird jeder von Ihnen erstellte Index mit einem Namen, der mit „log“ beginnt, automatisch mit der ISM-Richtlinie `my-policy-id` abgeglichen:

```
PUT _plugins/_ism/policies/my-policy-id
{
  "policy": {
    "description": "Example policy.",
    "default_state": "...",
    "states": [...],
    "ism_template": {
      "index_patterns": ["log*"],
      "priority": 100
```

```
    }
  }
}
```

Ein ausführlicheres Beispiel finden Sie unter Beispielrichtlinie mit ISM-Vorlage für automatisches Rollover.

Unterschiede

Im Vergleich OpenSearch zu Elasticsearch weist ISM for Amazon OpenSearch Service mehrere Unterschiede auf.

ISM-Operationen

- OpenSearch Service unterstützt drei einzigartige ISM-Operationen: `warm_migration`cold_migration, und`cold_delete`:
  - Wenn Ihre Domain UltraWarmaktiviert ist, wird der Index durch die `warm_migration` Aktion in den Warmspeicher verschoben.
  - Wenn in Ihrer Domain Cold Storage aktiviert ist, überträgt die `cold_migration`Aktion den Index in den Cold Storage und die `cold_delete`-Aktion löscht den Index aus dem Cold Storage.

  Auch wenn die -Aktion nicht innerhalb des festgelegten Timeout-Zeitraums abgeschlossen wird, wird die Migration zu Warm-Indizes dennoch fortgesetzt. Wenn Sie eine error_notification für eine der oben genannten Aktionen festlegen, werden Sie benachrichtigt, dass die Aktion fehlgeschlagen ist, wenn sie nicht innerhalb des Timeout-Zeitraums abgeschlossen wurde, aber die Benachrichtigung dient nur zu Ihrer eigenen Information. Der eigentliche Vorgang hat kein inhärentes Timeout und wird so lange ausgeführt, bis er schließlich erfolgreich ist oder fehlschlägt.
- Wenn Ihre Domain OpenSearch oder Elasticsearch 7.4 oder höher ausgeführt wird, unterstützt OpenSearch Service ISM `open` und `close` Operations.

- Wenn Ihre Domain OpenSearch oder Elasticsearch 7.7 oder höher ausgeführt wird, unterstützt OpenSearch Service den `snapshot` ISM-Vorgang.

ISM-Vorgänge für Cold Storage

Für Cold-Indizes müssen Sie einen `?type=_cold`-Parameter angeben, wenn Sie die folgenden ISM-APIs verwenden:

- Richtlinie hinzufügen
- Richtlinie entfernen
- Richtlinie aktualisieren
- Wiederholen fehlgeschlagener Index
- Index erklären

Diese APIs für Cold-Indizes weisen die folgenden zusätzlichen Unterschiede auf:

- Platzhalteroperatoren werden nur dann unterstützt, wenn Sie sie am Ende verwenden. Beispiel: `_plugins/_ism/<add, remove, change_policy, retry, explain>/logstash-*` wird unterstützt, `_plugins/_ism/<add, remove, change_policy, retry, explain>/iad-*-prod` jedoch nicht.
- Mehrzeilige Indexnamen und -muster werden nicht unterstützt. Beispiel: `_plugins/_ism/<add, remove, change_policy, retry, explain>/app-logs` wird unterstützt, `_plugins/_ism/<add, remove, change_policy, retry, explain>/app-logs,sample-data` jedoch nicht.

ISM-Einstellungen

OpenSearch und Elasticsearch ermöglicht es Ihnen, alle verfügbaren ISM-Einstellungen mithilfe der `_cluster/settings` API zu ändern. Bei Amazon OpenSearch Service können Sie nur die folgenden ISM-Einstellungen ändern:

- Einstellungen auf Clusterebene:
  - `plugins.index_state_management.enabled`
  - `plugins.index_state_management.history.enabled`
- Einstellungen auf Index-Ebene:
  - `plugins.index_state_management.rollover_alias`

Tutorial: Automatisieren von Indexstatusmanagement-Prozessen

In diesem Tutorial wird erläutert, wie Sie eine ISM-Richtlinie implementieren, die routinemäßige Indexverwaltungsaufgaben automatisiert und sie auf Indizes und Indexmuster anwendet.

Mit Index State Management (ISM) in Amazon OpenSearch Service können Sie wiederkehrende Indexverwaltungsaktivitäten automatisieren, sodass Sie vermeiden können, zusätzliche Tools zur Verwaltung von Index-Lebenszyklen zu verwenden. Sie können eine Richtlinie erstellen, die diese Vorgänge auf der Grundlage von Indexalter, Größe und anderen Bedingungen automatisiert, und das alles innerhalb Ihrer Amazon OpenSearch Service-Domain.

OpenSearch Der Service unterstützt drei Speicherstufen: den Standardstatus „Hot“ für aktives Schreiben und Analysen mit niedriger Latenz, UltraWarm für schreibgeschützte Daten bis zu drei Petabyte und Cold Storage für unbegrenzte Langzeitarchivierung.

Dieses Tutorial stellt einen beispielhaften Anwendungsfall für den Umgang mit Zeitreihendaten in Tagesindizes vor. In diesem Tutorial richten Sie eine Richtlinie ein, die nach 24 Stunden einen automatischen Snapshot jedes angehängten Indexes erstellt. Anschließend migriert er den Index nach zwei Tagen vom standardmäßigen Hot-Status in den UltraWarm Speicher, nach 30 Tagen in den Cold Storage und löscht den Index schließlich nach 60 Tagen.

Voraussetzungen

- Auf Ihrer OpenSearch Service-Domain muss Elasticsearch Version 6.8 oder höher ausgeführt werden.
- Für Ihre Domain muss UltraWarmCold Storage aktiviert sein.
- Sie müssen ein manuelles Snapshot-Repository in Ihrer Domain registrieren.
- Ihre Benutzerrolle benötigt ausreichende Berechtigungen für den Zugriff auf die OpenSearch Servicekonsole. Validieren und konfigurieren Sie den Zugriff auf Ihre Domains, falls erforderlich.

Schritt 1: Konfigurieren der ISM-Richtlinie

Konfigurieren Sie zunächst eine ISM-Richtlinie in OpenSearch Dashboards.

1. Navigieren Sie in Ihrem Domain-Dashboard in der OpenSearch Service-Konsole zur OpenSearch Dashboard-URL und melden Sie sich mit Ihrem Master-Benutzernamen und Passwort an. Die URL weist folgendes Format auf: *`domain-endpoint`*`/_dashboards/`.
2. Wählen Sie in OpenSearch Dashboards die Option Beispieldaten hinzufügen aus und fügen Sie Ihrer Domain einen oder mehrere Beispielindizes hinzu.
3. Öffnen Sie das linke Navigationsfenster und wählen Sie Index Management (Indexverwaltung) und dann Create policy (Richtlinie erstellen).
4. Speichern Sie die Richtlinie unter dem Namen `ism-policy-example`.

5. Ersetzen Sie die Standardrichtlinie durch die folgende Richtlinie:

```
{
  "policy": {
    "description": "Move indexes between storage tiers",
    "default_state": "hot",
    "states": [
      {
        "name": "hot",
        "actions": [],
        "transitions": [
          {
            "state_name": "snapshot",
            "conditions": {
              "min_index_age": "24h"
            }
          }
        ]
      },
      {
        "name": "snapshot",
        "actions": [
          {
            "retry": {
              "count": 5,
              "backoff": "exponential",
              "delay": "30m"
            },
            "snapshot": {
              "repository": "snapshot-repo",
              "snapshot": "ism-snapshot"
            }
          }
        ],
        "transitions": [
          {
            "state_name": "warm",
            "conditions": {
              "min_index_age": "2d"
            }
          }
        ]
      },
```

```
      {
        "name": "warm",
        "actions": [
          {
            "retry": {
              "count": 5,
              "backoff": "exponential",
              "delay": "1h"
            },
            "warm_migration": {}
          }
        ],
        "transitions": [
          {
            "state_name": "cold",
            "conditions": {
              "min_index_age": "30d"
            }
          }
        ]
      },
      {
        "name": "cold",
        "actions": [
          {
            "retry": {
              "count": 5,
              "backoff": "exponential",
              "delay": "1h"
            },
            "cold_migration": {
              "start_time": null,
              "end_time": null,
              "timestamp_field": "@timestamp",
              "ignore": "none"
            }
          }
        ],
        "transitions": [
          {
            "state_name": "delete",
            "conditions": {
              "min_index_age": "60d"
            }
```

```
          }
        ]
      },
      {
        "name": "delete",
        "actions": [
          {
            "cold_delete": {}
          }
        ],
        "transitions": []
      }
    ],
    "ism_template": [
      {
        "index_patterns": [
          "index-*"
        ],
        "priority": 100
      }
    ]
  }
}
```

> **Note**
>
> Das Feld `ism_template` hängt die Richtlinie automatisch an jeden neu erstellten Index an, der einem der angegebenen `index_patterns` entspricht. In diesem Fall alle Indizes, die mit `index-` beginnen. Sie können dieses Feld so ändern, dass es einem Indexformat in Ihrer Umgebung entspricht. Weitere Informationen finden Sie unter ISM-Vorlagen.

6. Im Abschnitt `snapshot` der Richtlinie ersetzen Sie *`snapshot-repo`* durch den Namen des Snapshot-Repositorys, das Sie für Ihre Domain registriert haben. Optional können Sie auch *`ism-snapshot`* ersetzen, was der Name des Snapshots sein wird, wenn er erstellt wird.
7. Wählen Sie Erstellen. Die Richtlinie ist nun auf der Seite State management policies (Statusmanagementrichtlinien) sichtbar.

Schritt 2: Anfügen der Richtlinie an einen oder mehrere Indizes

Nachdem Sie Ihre Richtlinie erstellt haben, fügen Sie sie an einen oder mehrere Indizes in Ihrem Cluster an.

1. Öffnen Sie die Registerkarte Hot indicies (Hot-Indizes) auf und suchen Sie nach `opensearch_dashboards_sample`. Dadurch werden alle Beispielindizes aufgeführt, die Sie in Schritt 1 hinzugefügt haben.
2. Wählen Sie alle Indizes aus und klicken Sie auf Richtlinie anwenden. Wählen Sie dann die Richtlinie aus, die Sie ism-policy-examplegerade erstellt haben.
3. Wählen Sie Apply (Anwenden) aus.

Auf der Seite Policy managed indices (Von der Richtlinie verwaltete Indizes) können Sie die Indizes überwachen, während sie die verschiedenen Zustände durchlaufen.

Zusammenfassung von Indizes in Amazon OpenSearch Service mit Index-Rollups

Mit Index-Rollups in Amazon OpenSearch Service können Sie die Speicherkosten senken, indem Sie alte Daten regelmäßig in zusammengefassten Indizes zusammenfassen.

Sie wählen die Felder aus, die Sie interessieren, und verwenden ein Index-Rollup, um einen neuen Index zu erstellen, in dem nur diese Felder in gröberen Zeitbereichen zusammengefasst sind. Sie können Verlaufsdaten von Monaten oder Jahren zu einem Bruchteil der Kosten mit derselben Abfrageleistung speichern.

Für Index-Rollups ist Elasticsearch 7.9 OpenSearch oder höher erforderlich.

> **Note**
>
> Diese Dokumentation hilft Ihnen bei den ersten Schritten mit der Erstellung eines Index-Rollup-Jobs in Amazon OpenSearch Service. Eine umfassende Dokumentation, einschließlich einer Liste aller verfügbaren Einstellungen und einer vollständigen API-Referenz, finden Sie in der Dokumentation unter Index-Rollups. OpenSearch

Erstellen eines Index-Rollup-Auftrags

Wählen Sie zunächst Indexverwaltung in OpenSearch Dashboards aus. Wählen Sie Rollup-Aufträge und Rollup-Aufträge erstellen aus.

Schritt 1: Indizes einrichten

Richten Sie die Quell- und Zielindizes ein. Der Quellindex ist der, den Sie zusammenrollen möchten. Im Zielindex werden die Index-Rollup-Ergebnisse gespeichert.

Nachdem Sie einen Indizierungs-Rollup-Auftrag erstellt haben, können Sie Ihre Indizierungsauswahl nicht ändern.

Schritt 2: Aggregationen und Metriken definieren

Wählen Sie die Attribute mit den Aggregationen (Bedingungen und Histogramme) und Metriken (Mittelwert, Summe, Max, Min und Wertzahl) aus, die Sie zusammenfassen möchten. Stellen Sie sicher, dass Sie nicht viele stark differenzierte Attribute hinzufügen, da Sie sonst nicht viel Platz sparen.

Schritt 3: Zeitpläne festlegen

Geben Sie einen Zeitplan an, um die Indizes während der Erfassung zusammenzufassen. Standardmäßig ist der Indizierungs-Rollup-Auftrag aktiviert.

Schritt 4: Überprüfen und Erstellen

Überprüfen Sie Ihre Konfiguration und wählen Sie Erstellen aus.

Schritt 5: Den Zielindex suchen

Sie können die Standard-`_search`API verwenden, um den Zielindex zu durchsuchen. Sie können nicht auf die interne Struktur der Daten im Zielindex zugreifen, da das Plug-In die Abfrage automatisch im Hintergrund neu schreibt, um den Zielindex anzupassen. Dadurch wird sichergestellt, dass Sie für den Quell- und Zielindex dieselbe Abfrage verwenden können.

Um den Zielindex abzufragen, legen Sie `size` auf 0 fest:

```
GET target_index/_search
```

```
{
  "size": 0,
  "query": {
    "match_all": {}
  },
  "aggs": {
    "avg_cpu": {
      "avg": {
        "field": "cpu_usage"
      }
    }
  }
}
```

> **Note**
>
> OpenSearch Versionen 2.2 und höher unterstützen die Suche nach mehreren Rollup-Indizes in einer Anfrage. OpenSearch Versionen vor 2.2 und ältere Elasticsearch OSS-Versionen unterstützen nur einen Rollup-Index pro Suche.

Transformation von Indizes in Amazon Service OpenSearch

Während Sie mit Index-Rollup-Jobs die Datengranularität reduzieren können, indem Sie alte Daten zu komprimierten Indizes zusammenfassen, können Sie mit Transformationsjobs eine andere, zusammengefasste Ansicht Ihrer Daten erstellen, die sich auf bestimmte Felder konzentriert, sodass Sie die Daten auf unterschiedliche Weise visualisieren oder analysieren können.

Indextransformationen verfügen über eine OpenSearch Dashboard-Benutzeroberfläche und eine REST-API. Für die Funktion ist OpenSearch Version 1.0 oder höher erforderlich.

> **Note**
>
> Diese Dokumentation bietet einen kurzen Überblick über Indextransformationen, um Ihnen den Einstieg in die Verwendung in einer Amazon OpenSearch Service-Domain zu erleichtern. Eine umfassende Dokumentation und eine REST-API-Referenz finden Sie unter Indextransformationen in der OpenSearch Open-Source-Dokumentation.

Erstellen eines Indextransformationsauftrags

Wenn Sie keine Daten in Ihrem Cluster haben, verwenden Sie die Beispielflugdaten in OpenSearch Dashboards, um Transformationsjobs auszuprobieren. Nachdem Sie die Daten hinzugefügt haben, starten Sie OpenSearch Dashboards. Wählen Sie dann Indexverwaltung, Transformationsaufträge und Transformationsauftrag erstellen.

Schritt 1: Wählen Sie Indizes

Wählen Sie im Abschnitt Indizes den Quell- und Zielindex aus. Sie können entweder einen vorhandenen Zielindex auswählen oder einen neuen erstellen, indem Sie einen Namen dafür eingeben.

Wenn Sie nur eine Teilmenge Ihres Quellindexes transformieren möchten, wählen Sie Datenfilter hinzufügen aus und verwenden Sie die OpenSearch Abfrage DSL, um eine Teilmenge Ihres Quellindex anzugeben.

Schritt 2: Felder auswählen

Nachdem Sie Ihre Indizes ausgewählt haben, wählen Sie die Felder aus, die Sie in Ihrem Transformationsjob verwenden möchten, und wählen Sie aus, ob Gruppierungen oder Aggregationen verwendet werden sollen.

- Sie können Gruppierungen verwenden, um Ihre Daten in separate Buckets in Ihrem transformierten Index zu platzieren. Wenn Sie beispielsweise alle Flughafenziele in den Beispielflugdaten gruppieren möchten, gruppieren Sie das `DestAirportID`-Feld in ein Zielfeld des `DestAirportID_terms`-Felds, und Sie können die gruppierten Flughafen-IDs in Ihrem transformierten Index finden, nachdem der Transformationsauftrag abgeschlossen ist.
- Auf der anderen Seite können Sie mit Aggregationen einfache Berechnungen durchführen. Sie können beispielsweise eine Aggregation in Ihren Transformationsjob einschließen, um ein neues Feld von `sum_of_total_ticket_price` zu definieren, das die Summe aller Flugtickets berechnet. Anschließend können Sie die neuen Daten in Ihrem transformierten Index analysieren.

Schritt 3: Legen Sie einen Zeitplan fest

Transformationsjobs sind standardmäßig aktiviert und werden nach Zeitplänen ausgeführt. Geben Sie für den Ausführungsintervall der Transformation ein Intervall in Minuten, Stunden oder Tagen an.

Schritt 4: Überprüfen und überwachen

Überprüfen Sie Ihre Konfiguration und wählen Sie Erstellen aus. Überwachen Sie dann die Spalte Transformations-Auftragsstatus.

Schritt 5: Den Zielindex suchen

Nach Abschluss des Auftrags können Sie die Standard–`_search`API verwenden, um den Zielindex zu durchsuchen.

Nachdem Sie beispielsweise einen Transformationsjob ausgeführt haben, der die Flugdaten basierend auf dem `DestAirportID`-Feld umwandelt, können Sie die folgende Anforderung ausführen, um alle Felder mit dem Wert `SFO` zurückzugeben:

```
GET target_index/_search
{
  "query": {
    "match": {
      "DestAirportID_terms" : "SFO"
    }
  }
}
```

Clusterübergreifende Replikation für Amazon Service OpenSearch

Mit der clusterübergreifenden Replikation in Amazon OpenSearch Service können Sie Benutzerindizes, Zuordnungen und Metadaten von einer Service-Domain auf eine OpenSearch andere replizieren. Die clusterübergreifende Replikation trägt dazu bei, die Wiederherstellung im Falle eines Ausfalls sicherzustellen, und ermöglicht es Ihnen, Daten über geografisch weit entfernte Rechenzentren hinweg zu replizieren, um die Latenz zu verringern. Sie zahlen die üblichen AWS Datenübertragungsgebühren für die zwischen Domains übertragenen Daten.

Die clusterübergreifende Replikation folgt einem aktiv-passiven Replikationsmodell, bei dem der lokale Index oder der Follower-Index Daten aus dem Remote- oder Leader-Index abruft. Der Leader-Index bezieht sich auf die Datenquelle oder den Index, aus dem Sie Daten replizieren möchten. Der Follower-Index bezieht sich auf das Ziel für die Daten oder den Index, in den Sie Daten replizieren möchten.

Die clusterübergreifende Replikation ist auf Domains verfügbar, auf denen Elasticsearch 7.10 oder 1.1 oder höher ausgeführt wird. OpenSearch

> **Note**
>
> In dieser Dokumentation wird beschrieben, wie Sie die clusterübergreifende Replikation aus Sicht von Amazon OpenSearch Service einrichten. Dazu gehört die Verwendung von AWS Management Console , um clusterübergreifende Verbindungen einzurichten, was auf einem OpenSearch selbstverwalteten Cluster nicht möglich ist. Eine vollständige Dokumentation, einschließlich einer Referenz zu Einstellungen und einer umfassenden API-Referenz, finden Sie in der Dokumentation unter Clusterübergreifende Replikation. OpenSearch

Themen

Einschränkungen

Clusterübergreifende Replikation weist folgende Einschränkungen auf:

- Sie können keine Daten zwischen Amazon OpenSearch Service-Domains und selbstverwalteten Clustern OpenSearch oder Elasticsearch-Clustern replizieren.
- Sie können einen Index nicht von einer Follower-Domain auf eine andere Follower-Domain replizieren. Wenn Sie einen Index auf mehrere Follower-Domains replizieren möchten, können Sie ihn nur von der Single-Leader-Domain aus replizieren.
- Eine Domain kann über eine Kombination aus ein- und ausgehenden Verbindungen mit maximal 20 anderen Domains verbunden werden.

- Wenn Sie anfänglich eine clusterübergreifende Verbindung einrichten, muss sich die Leader-Domain auf derselben oder einer höheren Version als die Follower-Domain befinden.
- Sie können es nicht verwenden, AWS CloudFormation um Domänen zu verbinden.
- Sie können die Cluster-übergreifende Replikation auf M3- oder (T2 und T3) Burstable Instances nicht verwenden.
- Sie können keine Daten zwischen UltraWarm oder kalten Indizes replizieren. Beide Indizes müssen sich im Hot Storage befinden.
- Wenn Sie einen Index aus der Leader-Domain löschen, wird der entsprechende Index in der Follower-Domain nicht automatisch gelöscht.

Voraussetzungen

Bevor Sie die Cluster-übergreifende Replikation einrichten, stellen Sie sicher, dass Ihre Domains die folgenden Anforderungen erfüllen:

- Elasticsearch 7.10 oder 1.1 oder höher OpenSearch
- Differenzierte Zugriffskontrolle aktiviert
- Keine ode-to-node Verschlüsselung aktiviert

Berechtigungsanforderungen

Um die Replikation zu starten, müssen Sie die `es:ESCrossClusterGet`-Berechtigung für die Remote (Leader)-Domain einschließen. Wir empfehlen die folgende IAM-Richtlinie für die Remotedomäne. Mit dieser Richtlinie können Sie auch andere Operationen ausführen, z. B. das Indizieren von Dokumenten und das Durchführen von Standardsuchen:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "*"
        ]
      },
      "Action": [
```

```
        "es:ESHttp*"
      ],
      "Resource": "arn:aws:es:region:account:domain/leader-domain/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "es:ESCrossClusterGet",
      "Resource": "arn:aws:es:region:account:domain/leader-domain"
    }
  ]
}
```

Stellen Sie sicher, dass die `es:ESCrossClusterGet`-Berechtigung auf `/leader-domain` und nicht `/leader-domain/*` angewendet wird.

Damit Nicht-Admin-Benutzer Replikationsaktivitäten ausführen können, müssen sie auch den entsprechenden Berechtigungen zugeordnet werden. Die meisten Berechtigungen entsprechen bestimmten REST-API-Operationen. Mit der Berechtigung `indices:admin/plugins/replication/index/_resume` können Sie beispielsweise die Replikation eines Index fortsetzen. Eine vollständige Liste der Berechtigungen finden Sie in der OpenSearch Dokumentation unter Replikationsberechtigungen.

> **Note**
>
> Die Befehle zum Starten der Replikation und zum Erstellen einer Replikationsregel sind Sonderfälle. Da sie Hintergrundprozesse in den Leader- und Follower-Domänen aufrufen, müssen Sie `follower_cluster_role` in der Anfrage ein `leader_cluster_role` UND übergeben. OpenSearch Der Service verwendet diese Rollen bei allen Backend-Replikationsaufgaben. Informationen zur Zuordnung und Verwendung dieser Rollen finden Sie in der Dokumentation unter Zuordnen der Leader- und Follower-Clusterrollen. OpenSearch

Einrichten einer clusterübergreifenden Verbindung

Um Indizes von einer Domain zu einer anderen zu replizieren, müssen Sie eine clusterübergreifende Verbindung zwischen den Domains einrichten. Der einfachste Weg, Domains zu verbinden, ist über

die Registerkarte Verbindungen des Domain-Dashboards. Sie können auch die Konfigurations-API oder die AWS -CLI verwenden. Da die Cluster-übergreifende Replikation einem „Pull“-Modell folgt, initiieren Sie Verbindungen von der Follower-Domain.

> **Note**
>
> Wenn Sie zuvor zwei Domains verbunden haben, um clusterübergreifende Suchen durchzuführen, können Sie nicht dieselbe Verbindung für die Replikation verwenden. Die Verbindung ist in der Konsole mit `SEARCH_ONLY` gekennzeichnet. Um die Replikation zwischen zwei zuvor verbundenen Domains durchzuführen, müssen Sie die Verbindung löschen und neu erstellen. Wenn Sie dies getan haben, ist die Verbindung sowohl für die clusterübergreifende Suche als auch für die clusterübergreifende Replikation verfügbar.

So richten Sie eine Verbindung ein

1. Wählen Sie in der Amazon OpenSearch Service-Konsole die Follower-Domain aus, wechseln Sie zur Registerkarte Verbindungen und wählen Sie Anfrage aus.
2. Geben Sie unter Verbindungs-Alias einen Namen für die Verbindung ein.
3. Wählen Sie, ob Sie sich mit einer Domain in Ihrer AWS-Konto Region oder mit einem anderen Konto oder einer anderen Region verbinden möchten.

   - Um eine Verbindung zu einer Domain in Ihrer Region AWS-Konto und Ihrer Region herzustellen, wählen Sie die Domain aus und klicken Sie auf Anfrage.
   - Um eine Verbindung zu einer Domain in einer anderen Region AWS-Konto oder Region herzustellen, geben Sie den ARN der Remotedomäne an und wählen Sie Request.

OpenSearch Der Dienst validiert die Verbindungsanfrage. Wenn die Domains nicht kompatibel sind, schlägt die Verbindung fehl. Wenn die Validierung erfolgreich ist, wird sie zur Genehmigung an die Ziel-Domain gesendet. Wenn die ZielDomain die Anforderung genehmigt, können Sie mit der Replikation beginnen.

Die clusterübergreifende Replikation unterstützt die bidirektionale Replikation. Das bedeutet, dass Sie eine ausgehende Verbindung von Domäne A zu Domäne B und eine weitere ausgehende Verbindung von Domäne B zu Domäne A herstellen können. Anschließend können Sie die Replikation so einrichten, dass Domäne A einem Index in Domäne B und Domäne B einem Index in Domäne A folgt.

So starten Sie eine Replikation

Nachdem Sie eine clusterübergreifende Verbindung hergestellt haben, können Sie damit beginnen, Daten zu replizieren. Erstellen Sie zunächst einen Index für die zu replizierende Leader-Domain:

```
PUT leader-01
```

Um diesen Index zu replizieren, senden Sie diesen Befehl an die Follower-Domain:

```
PUT _plugins/_replication/follower-01/_start
{
   "leader_alias": "connection-alias",
   "leader_index": "leader-01",
   "use_roles":{
      "leader_cluster_role": "all_access",
      "follower_cluster_role": "all_access"
   }
}
```

Sie finden den Verbindungsalias auf der Registerkarte Verbindungen in Ihrem Domain-Dashboard.

In diesem Beispiel wird davon ausgegangen, dass ein Administrator die Anfrage ausgibt und der Einfachheit halber `all_access` für `leader_cluster_role` und `follower_cluster_role` verwendet. In Produktionsumgebungen empfehlen wir jedoch, dass Sie Replikationsbenutzer sowohl für den Leader- als auch für den Follower-Index anlegen und diese entsprechend zuweisen. Die Benutzernamen müssen identisch sein. Informationen zu diesen Rollen und deren Zuordnung finden Sie in der Dokumentation unter Zuordnen der Rollen des Leader- und Follower-Clusters. OpenSearch

Replikation bestätigen

Um zu bestätigen, dass die Replikation stattfindet, rufen Sie den Replikationsstatus ab:

```
GET _plugins/_replication/follower-01/_status

{
  "status" : "SYNCING",
  "reason" : "User initiated",
  "leader_alias" : "connection-alias",
  "leader_index" : "leader-01",
  "follower_index" : "follower-01",
```

```
  "syncing_details" : {
    "leader_checkpoint" : -5,
    "follower_checkpoint" : -5,
    "seq_no" : 0
  }
}
```

Die Checkpoint-Werte für Leader und Follower beginnen als negative Ganzzahlen und spiegeln die Anzahl der Shards wider, die Sie haben (-1 für einen Shard, -5 für fünf Shards usw.). Die Werte erhöhen sich bei jeder Änderung, die Sie vornehmen, zu positiven Ganzzahlen. Wenn die Werte identisch sind, bedeutet dies, dass die Indizes vollständig synchronisiert sind. Sie können diese Checkpoint-Werte verwenden, um die Replikationslatenz in Ihren Domains zu messen.

Um die Replikation weiter zu überprüfen, fügen Sie dem Führungslinien-Index ein Dokument hinzu:

```
PUT leader-01/_doc/1
{
   "Doctor Sleep":"Stephen King"
}
```

Und bestätige, dass es im Follower-Index angezeigt wird:

```
GET follower-01/_search

{
    ...
    "max_score" : 1.0,
    "hits" : [
      {
        "_index" : "follower-01",
        "_type" : "_doc",
        "_id" : "1",
        "_score" : 1.0,
        "_source" : {
          "Doctor Sleep" : "Stephen King"
        }
      }
    ]
  }
}
```

Replikation pausieren und Fortsetzen

Sie können die Replikation vorübergehend unterbrechen, wenn Sie Probleme beheben oder die Belastung der Leader-Domain reduzieren müssen. Senden Sie diese Anfrage an die Follower-Domain. Vergewissern Sie sich, einen leeren Anforderungstext einzubeziehen:

```
POST _plugins/_replication/follower-01/_pause
{}
```

Rufen Sie dann den Status ab, um sicherzustellen, dass die Replikation angehalten wurde:

```
GET _plugins/_replication/follower-01/_status

{
  "status" : "PAUSED",
  "reason" : "User initiated",
  "leader_alias" : "connection-alias",
  "leader_index" : "leader-01",
  "follower_index" : "follower-01"
}
```

Wenn Sie mit den Änderungen fertig sind, setzen Sie die Replikation fort. Senden Sie diese Anfrage an die Follower-Domain. Vergewissern Sie sich, einen leeren Anforderungstext einzubeziehen:

```
POST _plugins/_replication/follower-01/_resume
{}
```

Sie können die Replikation nicht fortsetzen, nachdem sie länger als 12 Stunden pausiert wurde. Sie müssen die Replikation beenden, den Follower-Index löschen und die Replikation des Leader neu starten.

Replikation beenden

Wenn Sie die Replikation vollständig einstellen, folgt der Follower-Index dem Leader-Index nicht mehr und wird zu einem Standard-Index. Sie können eine Replikation nicht neu starten, nachdem Sie sie gestoppt haben.

Beenden Sie die Replikation von der Follower-Domain. Vergewissern Sie sich, einen leeren Anforderungstext einzubeziehen:

```
POST _plugins/_replication/follower-01/_stop
{}
```

Automatisches Folgen

Sie können eine Reihe von Replikationsregeln für eine einzelne Führungs-Domain definieren, die automatisch Indizes replizieren, die einem bestimmten Muster entsprechen. Wenn ein Index auf der Leader-Domain einem der Muster entspricht (z. B.`books*`), wird ein entsprechender Follower-Index auf der Follower-Domain erstellt. OpenSearch Service repliziert alle vorhandenen Indizes, die dem Muster entsprechen, sowie neue Indizes, die Sie erstellen. Er repliziert keine Indizes, die bereits in der Follower-Domain vorhanden sind.

Um alle Indizes zu replizieren (mit Ausnahme von vom System erstellten Indizes und derjenigen, die bereits in der Follower-Domain vorhanden sind), verwenden Sie ein Platzhaltermuster (`*`).

Erstellen einer Replikationsrolle

Erstellen Sie eine Replikationsregel für die Follower-Domain und geben Sie den Namen der clusterübergreifenden Verbindung an:

```
POST _plugins/_replication/_autofollow
{
   "leader_alias" : "connection-alias",
   "name": "rule-name",
   "pattern": "books*",
   "use_roles":{
      "leader_cluster_role": "all_access",
      "follower_cluster_role": "all_access"
   }
}
```

Sie finden den Verbindungsalias auf der Registerkarte Verbindungen in Ihrem Domain-Dashboard.

In diesem Beispiel wird davon ausgegangen, dass ein Administrator die Anfrage stellt, und der Einfachheit halber werden `all_access` als Leader- und Follower-Domain-Rollen verwendet. In Produktionsumgebungen empfehlen wir jedoch, Replikationsbenutzer sowohl auf den Leader- als auch Follower-Indizes zu erstellen und diese entsprechend zuzuweisen. Die Benutzernamen müssen identisch sein. Informationen zu diesen Rollen und deren Zuordnung finden Sie in der Dokumentation unter Zuordnen der Rollen des Leader- und Follower-Clusters. OpenSearch

Um eine Liste vorhandener Replikationsregeln in einer Domain abzurufen, verwenden Sie den API-Vorgang für die automatische Verfolgung von Statistiken.

Um die Regel zu testen, erstellen Sie einen Index, der dem Muster in der Leader-Domain entspricht:

```
PUT books-are-fun
```

Und überprüfen Sie, ob das Replikat in der Follower-Domain angezeigt wird:

```
GET _cat/indices

health status index          uuid                   pri rep docs.count docs.deleted
 store.size pri.store.size
green  open   books-are-fun  ldfHO78xYYdxRMULuiTvSQ     1   1          0            0
     208b           208b
```

Löschen einer Replikationsrolle

Wenn Sie eine Replikationsregel löschen, beendet OpenSearch Service die Replikation neuer Indizes, die dem Muster entsprechen, setzt jedoch die bestehende Replikationsaktivität fort, bis Sie die Replikation dieser Indizes beenden.

Löschen Sie Replikationsregeln aus der Follower-Domain:

```
DELETE _plugins/_replication/_autofollow
{
   "leader_alias" : "connection-alias",
   "name": "rule-name"
}
```

Verbundene Domänen werden aktualisiert

Um die Engine-Version von zwei Domänen zu aktualisieren, die über eine clusterübergreifende Verbindung verfügen, aktualisieren Sie zuerst die Follower-Domain und dann die Leader-Domain. Löschen Sie nicht die Verbindung zwischen ihnen, da sonst die Replikation unterbrochen wird und Sie sie nicht fortsetzen können.

Migration von Amazon OpenSearch Service-Indizes mithilfe der Remote-Neuindizierung

Mit der Remote-Neuindizierung können Sie Indizes von einer Amazon OpenSearch Service-Domain in eine andere kopieren. Sie können Indizes aus beliebigen OpenSearch Service-Domains oder selbstverwalteten OpenSearch Clustern und Elasticsearch-Clustern migrieren.

Eine Remote-Domain und ein Index beziehen sich auf die Quelle der Daten oder die Domain und den Index, aus denen Sie Daten kopieren möchten. Eine lokale Domäne und ein lokaler Index beziehen sich auf das Ziel für die Daten oder auf die Domäne und den Index, in die Sie Daten kopieren möchten.

Für die Remote-Neuindizierung ist OpenSearch 1.0 oder höher oder Elasticsearch 6.7 oder höher für die lokale Domain erforderlich. Bei der Remote-Domain muss es sich um eine niedrigere Version oder dieselbe Hauptversion wie die lokale Domain handeln. Elasticsearch-Versionen gelten als ältere OpenSearch Versionen, was bedeutet, dass Sie Daten aus Elasticsearch-Domänen in Domains neu indizieren können. OpenSearch Innerhalb derselben Hauptversion kann es sich bei der Remote-Domain um eine beliebige Nebenversion handeln. Beispielsweise wird die Remote-Neuindizierung von Elasticsearch 7.10.x auf 7.9 unterstützt, aber OpenSearch 1.0 auf Elasticsearch 7.10.x wird nicht unterstützt.

> **Note**
>
> In dieser Dokumentation wird beschrieben, wie Daten zwischen Amazon OpenSearch Service-Domains neu indexiert werden. Die vollständige Dokumentation für diesen `reindex` Vorgang, einschließlich detaillierter Schritte und unterstützter Optionen, finden Sie im Dokument Reindex in der OpenSearch Dokumentation.

Themen

- Remote-Neuindexierungseinstellungen

Voraussetzungen

Die Remote-Neuindexierung hat die folgenden Anforderungen:

- Auf die Remotedomäne muss von der lokalen Domäne aus zugegriffen werden können. Für eine Remotedomäne, die sich in einer VPC befindet, muss die lokale Domäne Zugriff auf die VPC haben. Dieser Prozess variiert je nach Netzwerkkonfiguration, beinhaltet aber wahrscheinlich eine Verbindung zu einem VPN oder einem verwalteten Netzwerk oder die Verwendung der nativen VPC-Endpunktverbindung. Weitere Informationen hierzu finden Sie unter the section called “VPC-Unterstützung”.
- Die Anfrage muss wie jede andere REST-Anfrage von der Remotedomäne autorisiert werden. Wenn für die Remotedomäne eine differenzierte Zugriffskontrolle aktiviert ist, benötigen Sie die Berechtigung, eine Neuindizierung der Remotedomäne durchzuführen und den Index in der lokalen Domäne zu lesen. Weitere Sicherheitsüberlegungen finden Sie unter the section called “Differenzierte Zugriffskontrolle”.
- Wir empfehlen Ihnen, einen Index mit der gewünschten Einstellung für Ihre lokale Domain zu erstellen, bevor Sie mit der Neuindizierung beginnen.
- Wenn Ihre Domain einen T2- oder T3-Instance-Typ für Ihre Datenknoten verwendet, können Sie die Remote-Neuindizierung nicht verwenden.

Daten zwischen OpenSearch Service-Internetdomänen neu indizieren

Das einfachste Szenario ist, dass sich der Remote-Index in derselben Domäne befindet AWS-Region wie Ihre lokale Domain mit einem öffentlich zugänglichen Endpunkt und Sie signierte IAM-Anmeldeinformationen haben.

Geben Sie in der Remotedomäne den Remote-Index an, von dem aus neu indexiert werden soll, und den lokalen Index, auf den neu indexiert werden soll:

```
POST _reindex
{
  "source": {
    "remote": {
      "host": "https://remote-domain-endpoint:443"
    },
```

```
    "index": "remote_index"
  },
  "dest": {
    "index": "local_index"
  }
}
```

Für eine Validierungsprüfung müssen Sie am Ende des Endpunkts der Remote-Domäne 443 hinzufügen.

Um zu überprüfen, ob der Index in die lokale Domäne kopiert wurde, senden Sie diese Anfrage an die lokale Domäne:

```
GET local_index/_search
```

Wenn sich der Remote-Index in einer anderen Region als Ihrer lokalen Domain befindet, geben Sie den Namen der Region ein, wie in dieser Beispielanforderung:

```
POST _reindex
{
  "source": {
    "remote": {
      "host": "https://remote-domain-endpoint:443",
      "region": "eu-west-1"
    },
    "index": "remote_index"
  },
  "dest": {
    "index": "local_index"
  }
}
```

Bei isolierten Regionen wie AWS GovCloud (US) oder China ist der Endpunkt möglicherweise nicht zugänglich, da Ihr IAM-Benutzer in diesen Regionen nicht erkannt wird.

Wenn die Remote-Domain mit Standardauthentifizierung gesichert ist, geben Sie den Benutzernamen und das Passwort an:

```
POST _reindex
{
  "source": {
    "remote": {
```

```
      "host": "https://remote-domain-endpoint:443",
      "username": "username",
      "password": "password"
    },
    "index": "remote_index"
  },
  "dest": {
    "index": "local_index"
  }
}
```

Daten zwischen OpenSearch Dienstdomänen neu indizieren, wenn sich die Fernbedienung in einer VPC befindet

Jede OpenSearch Service-Domain besteht aus einer eigenen internen Virtual Private Cloud (VPC) - Infrastruktur. Wenn Sie eine neue Domain in einer vorhandenen OpenSearch Service-VPC erstellen, wird für jeden Datenknoten in der VPC eine elastic network interface erstellt.

Da der Remote-Neuindizierungsvorgang von der OpenSearch Remote-Servicedomäne aus und somit innerhalb einer eigenen privaten VPC ausgeführt wird, benötigen Sie eine Möglichkeit, auf die VPC der lokalen Domäne zuzugreifen. Sie können dazu entweder die integrierte VPC-Endpunktverbindungsfunktion verwenden, um eine Verbindung herzustellen AWS PrivateLink, oder indem Sie einen Proxy konfigurieren.

Wenn Ihre lokale Domain OpenSearch Version 1.0 oder höher verwendet, können Sie die Konsole oder die verwenden, AWS CLI um eine AWS PrivateLink Verbindung herzustellen. Eine AWS PrivateLink Verbindung ermöglicht es Ressourcen in der lokalen VPC, sich privat mit Ressourcen in der Remote-VPC innerhalb derselben zu verbinden. AWS-Region

Indizieren Sie Daten erneut mit dem AWS Management Console

Sie können die Remote-Neuindizierung mit der Konsole verwenden, um Indizes zwischen zwei Domänen zu kopieren, die sich eine VPC-Endpunktverbindung teilen.

1. Navigieren Sie zur Amazon OpenSearch Service-Konsole unterhttps://console.aws.amazon.com/aos/.
2. Wählen Sie im linken Navigationsbereich die Option Domains aus.
3. Wählen Sie die lokale Domain oder die Domain aus, in die Sie Daten kopieren möchten. Dadurch wird die Detailseite der Domain geöffnet. Wählen Sie unter den allgemeinen Informationen den Tab Verbindungen aus und klicken Sie auf Anfrage.

4. Wählen Sie auf der Seite Verbindung anfordern die Option VPC-Endpunktverbindung für Ihren Verbindungsmodus aus und geben Sie weitere relevante Details ein. Zu diesen Details gehört die Remote-Domain, also die Domain, von der Sie Daten kopieren möchten. Wählen Sie dann Request (Anfordern) aus.
5. Navigieren Sie zur Detailseite der Remotedomäne, wählen Sie die Registerkarte Verbindungen und suchen Sie die Tabelle Eingehende Verbindungen. Aktivieren Sie das Kontrollkästchen neben dem Namen der Domain, von der Sie gerade die Verbindung erstellt haben (die lokale Domain). Wählen Sie Approve (Genehmigen) aus.
6. Gehen Sie zurück zur lokalen Domain, wählen Sie die Registerkarte Connections (Verbindungen) aus und suchen Sie nach der Tabelle Outbound connections (Ausgehende Verbindungen). Nachdem die Verbindung zwischen den beiden Domains aktiviert wurde, wird in der Spalte Endpoint (Endpunkt) in der Tabelle ein Endpunkt verfügbar. Kopieren Sie den Endpunkt.
7. Öffnen Sie das Dashboard für die lokale Domain und wählen Sie in der linken Navigation Dev Tools aus. Führen Sie die folgende GET-Anfrage aus, um zu bestätigen, dass der Remote-Domänenindex in Ihrer lokalen Domain noch nicht existiert. *remote-domain-index-name*Ersetzen Sie es durch Ihren eigenen Indexnamen.

   ```
   GET remote-domain-index-name/_search
   {
      "query":{
         "match_all":{}
      }
   }
   ```

   In der Ausgabe sollte ein Fehler angezeigt werden, der darauf hinweist, dass der Index nicht gefunden wurde.
8. Erstellen Sie unter Ihrer GET-Anfrage eine POST-Anfrage und verwenden Sie Ihren Endpunkt wie folgt als Remote-Host.

   ```
   POST _reindex
   {
      "source":{
         "remote":{
            "host":"connection-endpoint",
            "username":"username",
            "password":"password"
         },
   ```

```
      "index":"remote-domain-index-name"
   },
   "dest":{
      "index":"local-domain-index-name"
   }
}
```

Führen Sie diese Anfrage aus.

9. Führen Sie die GET-Anfrage erneut aus. Die Ausgabe sollte nun anzeigen, dass der lokale Index existiert. Sie können diesen Index abfragen, um zu überprüfen, ob alle Daten aus dem Remote-Index OpenSearch kopiert wurden.

Indizieren Sie Daten mit OpenSearch Service-API-Vorgängen neu

Sie können die Remote-Neuindizierung mit der API verwenden, um Indizes zwischen zwei Domänen zu kopieren, die sich eine VPC-Endpunktverbindung teilen.

1. Verwenden Sie den CreateOutboundConnectionAPI-Vorgang, um eine neue Verbindung von Ihrer lokalen Domain zu Ihrer Remote-Domain anzufordern.

```
POST https://es.region.amazonaws.com/2021-01-01/opensearch/cc/outboundConnection

{
   "ConnectionAlias": "remote-reindex-example",
   "ConnectionMode": "VPC_ENDPOINT",
   "LocalDomainInfo": {
      "AWSDomainInformation": {
         "DomainName": "local-domain-name",
         "OwnerId": "aws-account-id",
         "Region": "region"
      }
   },
   "RemoteDomainInfo": {
      "AWSDomainInformation": {
         "DomainName": "remote-domain-name",
         "OwnerId": "aws-account-id",
         "Region": "region"
      }
   }
}
```

Sie erhalten `ConnectionId` in der Antwort eine. Speichern Sie diese ID, um sie im nächsten Schritt zu verwenden.

2. Verwenden Sie den AcceptInboundConnectionAPI-Vorgang mit Ihrer Verbindungs-ID, um die Anfrage von der lokalen Domain aus zu genehmigen.

```
PUT https://es.region.amazonaws.com/2021-01-01/opensearch/cc/
inboundConnection/ConnectionId/accept
```

3. Verwenden Sie den DescribeOutboundConnectionsAPI-Vorgang, um den Endpunkt für Ihre Remote-Domain abzurufen.

```
{
    "Connections": [
        {
            "ConnectionAlias": "remote-reindex-example",
            "ConnectionId": "connection-id",
            "ConnectionMode": "VPC_ENDPOINT",
            "ConnectionProperties": {
                "Endpoint": "connection-endpoint"
            },
            ...
        }
    ]
}
```

Speichern Sie den *Verbindungsendpunkt,* der in Schritt 5 verwendet werden soll.

4. Führen Sie die folgende GET-Anfrage aus, um zu bestätigen, dass der Remote-Domänenindex in Ihrer lokalen Domäne noch nicht existiert. *remote-domain-index-name*Ersetzen Sie es durch Ihren eigenen Indexnamen.

```
GET local-domain-endpoint/remote-domain-index-name/_search
{
   "query":{
      "match_all":{}
   }
}
```

In der Ausgabe sollte ein Fehler angezeigt werden, der darauf hinweist, dass der Index nicht gefunden wurde.

5. Erstellen Sie eine POST-Anfrage und verwenden Sie Ihren Endpunkt wie folgt als Remote-Host.

```
POST local-domain-endpoint/_reindex
{
   "source":{
      "remote":{
         "host":"connection-endpoint",
         "username":"username",
         "password":"password"
      },
      "index":"remote-domain-index-name"
   },
   "dest":{
      "index":"local-domain-index-name"
   }
}
```

   Führen Sie diese Anfrage aus.

6. Führen Sie die GET-Anfrage erneut aus. Die Ausgabe sollte nun anzeigen, dass der lokale Index existiert. Sie können diesen Index abfragen, um zu überprüfen, ob alle Daten aus dem Remote-Index OpenSearch kopiert wurden.

Wenn die Remotedomäne in einer VPC gehostet wird und Sie die VPC-Endpunktverbindungsfunktion nicht verwenden möchten, müssen Sie einen Proxy mit einem öffentlich zugänglichen Endpunkt konfigurieren. In diesem Fall benötigt OpenSearch Service einen öffentlichen Endpunkt, da er keinen Datenverkehr an Ihre VPC senden kann.

Wenn Sie eine Domain im VPC-Modus ausführen, werden ein oder mehrere Endpoints in Ihrer VPC platziert. Diese Endpunkte sind jedoch nur für den Datenverkehr vorgesehen, der in die Domain innerhalb der VPC eingeht, und sie lassen keinen Datenverkehr in die VPC selbst zu.

Der Befehl remote reindex wird von der lokalen Domäne aus ausgeführt, sodass der ursprüngliche Datenverkehr diese Endpunkte nicht für den Zugriff auf die Remotedomäne verwenden kann. Aus diesem Grund ist in diesem Anwendungsfall ein Proxy erforderlich. Die Proxy-Domain muss über ein Zertifikat verfügen, das von einer öffentlichen Zertifizierungsstelle (CA) signiert wurde. Selbstsignierte oder private Zertifizierungsstellen-Zertifikate werden nicht unterstützt.

Indizieren Sie Daten zwischen OpenSearch Nicht-Servicedomänen neu

Wenn der Remote-Index außerhalb von OpenSearch Service gehostet wird, z. B. in einer selbstverwalteten EC2-Instanz, setzen Sie den `external` Parameter auf: `true`

```
POST _reindex
{
  "source": {
    "remote": {
      "host": "https://remote-domain-endpoint:443",
      "username": "username",
      "password": "password",
      "external": true
    },
    "index": "remote_index"
  },
  "dest": {
    "index": "local_index"
  }
}
```

In diesem Fall wird nur die Standardauthentifizierung mit einem Benutzernamen und einem Passwort unterstützt. Die Remotedomäne muss über einen öffentlich zugänglichen Endpunkt (auch wenn sie sich in derselben VPC wie die lokale OpenSearch Dienstdomäne befindet) und über ein von einer öffentlichen Zertifizierungsstelle signiertes Zertifikat verfügen. Selbstsignierte oder private, von einer Zertifizierungsstelle signierte Zertifikate werden nicht unterstützt.

Große Datensätze neu indizieren

Die Remote-Neuindizierung sendet eine Scroll-Anfrage mit den folgenden Standardwerten an die Remotedomäne:

- Suchkontext von 5 Minuten
- Socket-Timeout von 30 Sekunden
- Batch-Größe von 1.000

Wir empfehlen, diese Parameter an Ihre Daten anzupassen. Berücksichtigen Sie bei großen Dokumenten eine kleinere Batch-Größe und/oder ein längeres Timeout. Weitere Informationen finden Sie unter Scrollsuche.

```
POST _reindex?pretty=true&scroll=10h&wait_for_completion=false
{
  "source": {
    "remote": {
      "host": "https://remote-domain-endpoint:443",
      "socket_timeout": "60m"
    },
    "size": 100,
    "index": "remote_index"
  },
  "dest": {
    "index": "local_index"
  }
}
```

Wir empfehlen außerdem, dem lokalen Index die folgenden Einstellungen hinzuzufügen, um die Leistung zu verbessern:

```
PUT local_index
{
  "settings": {
    "refresh_interval": -1,
    "number_of_replicas": 0
  }
}
```

Nachdem der Neuindizierungsprozess abgeschlossen ist, können Sie Ihre gewünschte Replikatanzahl festlegen und die Einstellung für das Aktualisierungsintervall entfernen.

Um nur eine Teilmenge der Dokumente, die Sie über eine Abfrage ausgewählt haben, neu zu indizieren, senden Sie diese Anfrage an die lokale Domäne:

```
POST _reindex
{
  "source": {
    "remote": {
      "host": "https://remote-domain-endpoint:443"
    },
    "index": "remote_index",
    "query": {
      "match": {
```

```
        "field_name": "text"
      }
    }
  },
  "dest": {
    "index": "local_index"
  }
}
```

Die Remote-Neuindexierung unterstützt keine Segmentierung, sodass Sie nicht mehrere Scroll-Vorgänge für dieselbe Anforderung parallel ausführen können.

Remote-Neuindexierungseinstellungen

Zusätzlich zu den Standardoptionen für die Neuindizierung unterstützt OpenSearch Service die folgenden Optionen:

Optionen	Zulässige Werte	Beschreibung	Erforderlich
Extern	Boolesch	Wenn es sich bei der Remotedomäne nicht um eine OpenSearch Dienstdomäne handelt oder wenn Sie zwischen zwei VPC-Domänen neu indizieren, geben Sie als an. `true`	Nein
Region	String	Wenn sich die Remotedomäne in einer anderen Region befindet, geben Sie den Namen der Region an.	Nein

Verwaltung von Zeitreihendaten in Amazon OpenSearch Service mit Datenströmen

Ein typischer Workflow zum Verwalten von Zeitreihendaten umfasst mehrere Schritte, z. B. das Erstellen eines Rollover-Indexalias, das Definieren eines Schreibindexes und das Definieren allgemeiner Zuordnungen und Einstellungen für die Backing-Indizes.

Datenströme in Amazon OpenSearch Service helfen dabei, diesen Ersteinrichtungsprozess zu vereinfachen. Datenströme funktionieren sofort für zeitbasierte Daten wie Anwendungsprotokolle, die typischerweise nur Anhänge sind.

Für Datenstreams ist OpenSearch Version 1.0 oder höher erforderlich.

> **Note**
>
> Diese Dokumentation enthält grundlegende Schritte, die Ihnen den Einstieg in Datenstreams in einer Amazon OpenSearch Service-Domain erleichtern sollen. Eine umfassende Dokumentation finden Sie unter Datenströme in der OpenSearch Dokumentation.

Erste Schritte mit Datenströmen

Ein Datenstrom besteht intern aus mehreren Backing-Indizes. Suchanforderungen werden an alle Backing-Indizes weitergeleitet, während Indizierungsanforderungen an den neuesten Schreibindex weitergeleitet werden.

Schritt 1: Erstellen einer Index-Vorlage

Um einen Datenstrom zu erstellen, müssen Sie zunächst eine Indexvorlage erstellen, die einen Satz von Indizes als Datenstrom konfiguriert. Das `data_stream`-Objekt zeigt an, dass es sich um einen Datenstrom und keine reguläre Indexvorlage handelt. Das Indexmuster stimmt mit dem Namen des Datenstroms überein:

```
PUT _index_template/logs-template
{
  "index_patterns": [
    "my-data-stream",
    "logs-*"
```

```
  ],
  "data_stream": {},
  "priority": 100
}
```

In diesem Fall muss jedes aufgenommene Dokument ein `@timestamp`-Feld haben. Sie können auch Ihr eigenes benutzerdefiniertes Zeitstempelfeld als Eigenschaft im `data_stream`-Objekt definieren:

```
PUT _index_template/logs-template
{
  "index_patterns": "my-data-stream",
  "data_stream": {
    "timestamp_field": {
      "name": "request_time"
    }
  }
}
```

Schritt 2: Erstellen eines Datenstroms

Nachdem Sie eine Indexvorlage erstellt haben, können Sie direkt mit der Erfassung von Daten beginnen, ohne einen Datenstrom zu erstellen.

Da wir eine passende Indexvorlage mit einem `data_stream` Objekt haben, OpenSearch wird der Datenstrom automatisch erstellt:

```
POST logs-staging/_doc
{
  "message": "login attempt failed",
  "@timestamp": "2013-03-01T00:00:00"
}
```

Schritt 3: Daten in den Datenstrom aufnehmen

Um Daten in einen Datenstrom aufzunehmen, können Sie die regulären Indizierungs-APIs verwenden. Stellen Sie sicher, dass jedes Dokument, das Sie indizieren, über ein Zeitstempelfeld verfügt. Wenn Sie versuchen, ein Dokument zu übernehmen, das kein Zeitstempelfeld enthält, erhalten Sie einen Fehler.

```
POST logs-redis/_doc
```

```
{
  "message": "login attempt",
  "@timestamp": "2013-03-01T00:00:00"
}
```

Schritt 4: Suchen eines Datenstroms

Sie können einen Datenstrom genauso durchsuchen, wie Sie einen regulären Index oder einen Indexalias durchsuchen. Der Suchvorgang gilt für alle Backing-Indizes (alle Daten, die im Stream vorhanden sind).

```
GET logs-redis/_search
{
  "query": {
    "match": {
      "message": "login"
    }
  }
}
```

Schritt 5: Rollover eines Datenstroms

Sie können eine Indexstatusmanagement (ISM)-Richtlinie einrichten, um den Rollover-Prozess für den Datenstrom zu automatisieren. Die ISM-Richtlinie wird zum Zeitpunkt ihrer Erstellung auf die Backing-Indizes angewendet. Wenn Sie eine Richtlinie einem Datenstrom zuordnen, wirkt sich dies nur auf die zukünftigen Sicherungsindizes dieses Datenstroms aus. Sie müssen auch die `rollover_alias`-Einstellung nicht angeben, da die ISM-Richtlinie diese Informationen aus dem Sicherungsindex ableitet.

> **Note**
>
> Wenn Sie einen Backing-Index in einen Cold Storage migrieren, OpenSearch wird dieser Index aus dem Datenstrom entfernt. Selbst wenn Sie den Index wieder in verschieben UltraWarm, bleibt der Index unabhängig und nicht Teil des ursprünglichen Datenstroms. Nachdem ein Index aus dem Datenstream entfernt wurde, werden bei der Suche nach dem Stream keine Daten aus dem Index zurückgegeben.

> **Warning**
>
> Der Schreibindex für einen Datenstream kann nicht in einen Cold Storage migriert werden. Wenn Sie Daten in Ihrem Datenstrom in einen Cold Storage migrieren möchten, müssen Sie vor der Migration einen Rollover über den Datenstrom durchführen.

Schritt 6: Datenströme in OpenSearch Dashboards verwalten

Um Datenströme von OpenSearch Dashboards aus zu verwalten, öffnen Sie OpenSearch Dashboards, wählen Sie Indexverwaltung, dann Indizes oder Policy-verwaltete Indizes aus.

Schritt 7: Löschen eines Datenstroms

Der Löschvorgang löscht zuerst die Backing-Indizes eines Datenstroms und löscht dann den Datenstrom selbst.

So löschen Sie einen Datenstrom und alle versteckten Backing-Indizes:

```
DELETE _data_stream/name_of_data_stream
```

Überwachen von Daten in Amazon OpenSearch Service

Überwachen Sie Ihre Daten proaktiv in Amazon OpenSearch Service mit Warnungen und Anomalieerkennung. Richten Sie Warnungen ein, um Benachrichtigungen zu erhalten, wenn Ihre Daten bestimmte Schwellenwerte überschreiten. Die Anomalieerkennung verwendet Machine Learning, um Ausreißer in Ihren Streaming-Daten automatisch zu erkennen. Sie können die Anomalieerkennung mit Warnungen verbinden, damit Sie benachrichtigt werden, sobald eine Anomalie erkannt wird.

Themen

Konfiguration von Benachrichtigungen in Amazon OpenSearch Service

Konfigurieren Sie Benachrichtigungen in Amazon OpenSearch Service, um benachrichtigt zu werden, wenn Daten aus einem oder mehreren Indizes bestimmte Bedingungen erfüllen. Sie möchten beispielsweise eine E-Mail erhalten, wenn Ihre Anwendung mehr als fünf HTTP-503-Fehler pro Stunde protokolliert, oder Sie möchten ggf. einen Entwickler benachrichtigen, wenn in den letzten 20 Minuten keine neuen Dokumente indiziert wurden.

Alerting erfordert Elasticsearch 6.2 OpenSearch oder höher.

> **Note**
>
> Diese Dokumentation bietet einen kurzen Überblick über Warnmeldungen und zeigt auf, wie sich Warnmeldungen auf einer Amazon OpenSearch Service-Domain von Warnmeldungen auf einem Open-Source-Cluster unterscheiden. OpenSearch Eine vollständige Dokumentation zu Warnmeldungen, einschließlich einer umfassenden API-Referenz, einer Liste verfügbarer Anforderungsfelder für zusammengesetzte Monitore und Beschreibungen der verfügbaren Auslöser- und Aktionsvariablen, finden Sie in der Dokumentation unter Alerting. OpenSearch

Themen

Warnungsberechtigungen

Warnungen unterstützen die differenzierte Zugriffskontrolle. Einzelheiten zum Kombinieren und Abgleichen von Berechtigungen für Ihren Anwendungsfall finden Sie in der Dokumentation unter Alerting security. OpenSearch

Um in OpenSearch Dashboards auf die Seite „Benachrichtigungen“ zugreifen zu können, müssen Sie mindestens der `alerting_read_access` vordefinierten Rolle zugeordnet sein oder Ihnen müssen entsprechende Berechtigungen erteilt werden. Diese Rolle gewährt Berechtigungen zum Anzeigen von Benachrichtigungen, Zielen und Monitoren, jedoch nicht zum Bestätigen von Warnungen oder zum Ändern von Zielen oder Monitoren.

Erste Schritte mit Warnungen

Um eine Warnung zu erstellen, konfigurieren Sie einen Monitor. Dabei handelt es sich um einen Job, der nach einem definierten Zeitplan ausgeführt wird und OpenSearch Indizes abfragt. Sie konfigurieren auch einen oder mehrere Auslöser, die die Bedingungen definieren, unter denen Ereignisse generiert werden. Abschließend konfigurieren Sie Aktionen, die nach dem Auslösen einer Warnung geschehen.

Erste Schritte mit Warnungen

1. Wählen Sie im Hauptmenü der OpenSearch Dashboards die Option Alerting und dann Monitor erstellen aus.
2. Erstellen Sie eine Überwachung pro Abfrage, pro Bucket, pro Cluster-Metriken oder pro Dokument. Anweisungen finden Sie unter Eine Überwachung erstellen.
3. Erstellen Sie für Triggers (Auslöser) einen oder mehrere Auslöser. Anweisungen finden Sie unter Auslöser erstellen.
4. Legen Sie für Actions (Aktionen) einen Benachrichtigungskanal für die Warnung fest. Wählen Sie zwischen Slack, Amazon Chime, einem benutzerdefinierten Webhook oder Amazon SNS. Wie Sie sich vorstellen können, erfordern Benachrichtigungen eine Verbindung zum

Kanal. Beispielsweise muss deine OpenSearch Service-Domain in der Lage sein, eine Verbindung zum Internet herzustellen, um einen Slack-Channel zu benachrichtigen oder einen benutzerdefinierten Webhook an einen Server eines Drittanbieters zu senden. Der benutzerdefinierte Webhook muss eine öffentliche IP-Adresse haben, damit eine OpenSearch Service-Domain Benachrichtigungen an ihn senden kann.

> **Tip**
>
> Nachdem eine Aktion erfolgreich eine Nachricht gesendet hat, liegt die Zusicherung des Zugriffs auf diese Nachricht (z. B. den Zugriff auf einen Slack-Kanal) in Ihrer Verantwortung. Wenn Ihre Domain sensible Daten enthält, sollten Sie Auslöser ohne Aktionen verwenden und Dashboards regelmäßig auf Warnungen prüfen.

Benachrichtigungen

Alerting ist in Notifications integriert, ein einheitliches System für OpenSearch Benachrichtigungen. Mit Benachrichtigungen können Sie konfigurieren, welchen Kommunikationsservice Sie verwenden möchten, und relevante Statistiken und Informationen zur Fehlerbehebung anzeigen. Eine umfassende Dokumentation finden Sie in der OpenSearch Dokumentation unter Benachrichtigungen.

Auf Ihrer Domain muss OpenSearch Version 2.3 oder höher ausgeführt werden, um Benachrichtigungen verwenden zu können.

> **Note**
>
> OpenSearch Benachrichtigungen sind unabhängig von OpenSearch Dienstbenachrichtigungen, die Einzelheiten zu Service-Software-Updates, Auto-Tune-Verbesserungen und anderen wichtigen Informationen auf Domänenebene enthalten. OpenSearch Benachrichtigungen sind Plugin-spezifisch.

Benachrichtigungskanäle haben ab Version 2.0 die Benachrichtigungsziele ersetzt. OpenSearch Ziele wurden offiziell als veraltet eingestuft und alle Warnmeldungen werden künftig über Kanäle verwaltet.

Wenn Sie Ihre Domains auf Version 2.3 oder höher aktualisieren (da die OpenSearch Serviceunterstützung für 2.x mit 2.3 beginnt), werden Ihre vorhandenen Ziele automatisch auf

Benachrichtigungskanäle migriert. Wenn ein Ziel nicht migriert werden kann, wird es vom Monitor weiterhin verwendet, bis der Monitor zu einem Benachrichtigungskanal migriert wird. Weitere Informationen finden Sie in der Dokumentation unter Fragen zu Zielen. OpenSearch

Um mit Benachrichtigungen zu beginnen, melden Sie sich bei OpenSearch Dashboards an und wählen Sie Benachrichtigungen, Kanäle und Kanal erstellen aus.

Amazon Simple Notification Service (Amazon SNS) ist ein unterstützter Kanaltyp für Benachrichtigungen. Um Benutzer zu authentifizieren, müssen Sie dem Benutzer entweder vollen Zugriff auf Amazon SNS gewähren oder ihn eine IAM-Rolle übernehmen lassen, die Berechtigungen für den Zugriff auf Amazon SNS hat. Anweisungen finden Sie unter Amazon SNS als Kanaltyp.

Unterschiede

Im Vergleich zur Open-Source-Version von OpenSearch weist die Alarmierung in Amazon OpenSearch Service einige bemerkenswerte Unterschiede auf.

Warneinstellungen

OpenSearch Mit Service können Sie die folgenden Alarmeinstellungen ändern:

- `plugins.scheduled_jobs.enabled`
- `plugins.alerting.alert_history_enabled`
- `plugins.alerting.alert_history_max_age`
- `plugins.alerting.alert_history_max_docs`
- `plugins.alerting.alert_history_retention_period`
- `plugins.alerting.alert_history_rollover_period`
- `plugins.alerting.filter_by_backend_roles`

Alle anderen Einstellungen verwenden die Standardwerte, die Sie nicht ändern können.

Um Warnungen zu deaktivieren, senden Sie die folgende Anforderung:

```
PUT _cluster/settings
{
  "persistent" : {
    "plugins.scheduled_jobs.enabled" : false
  }
```

```
}
```

Mit der folgenden Anforderung werden Benachrichtigungen so konfiguriert, dass Verlaufsindizes automatisch nach sieben Tagen und nicht nach den standardmäßigen 30 Tagen gelöscht werden:

```
PUT _cluster/settings
{
  "persistent": {
    "plugins.alerting.alert_history_retention_period": "7d"
  }
}
```

Wenn Sie zuvor Monitore erstellt haben und die Erstellung von Indizes für tägliche Warnmeldungen beenden möchten, löschen Sie alle Indizes für den Warnungsverlauf:

```
DELETE .plugins-alerting-alert-history-*
```

Um die Anzahl der Shards für Verlaufsindizes zu reduzieren, erstellen Sie eine Indexvorlage. Die folgende Anforderung legt Verlaufsindizes für Warnungen auf einen Shard und ein Replikat fest:

```
PUT _index_template/template-name
{
  "index_patterns": [".opendistro-alerting-alert-history-*"],
  "template": {
    "settings": {
      "number_of_shards": 1,
      "number_of_replicas": 1
    }
  }
}
```

Abhängig von Ihrer Toleranz für Datenverlust können Sie sogar die Verwendung von Null-Replikaten in Erwägung ziehen. Weitere Informationen zum Erstellen und Verwalten von Indexvorlagen finden Sie in der OpenSearch Dokumentation unter Indexvorlagen.

Erkennung von Anomalien in Amazon Service OpenSearch

Die Anomalieerkennung in Amazon OpenSearch Service erkennt mithilfe des Random Cut Forest (RCF) -Algorithmus automatisch Anomalien in Ihren OpenSearch Daten nahezu in Echtzeit. RCF ist

ein unüberwachter Algorithmus für Machine Learning, der eine Skizze des eingehenden Datenstroms modelliert. Der Algorithmus berechnet einen `anomaly grade`- und `confidence score`-Wert für jeden eingehenden Datenpunkt. Die Funktion zur Anomalieerkennung verwendet diese Werte, um eine Anomalie von normalen Variationen in Ihren Daten zu unterscheiden.

Sie können das Anomalieerkennungs-Plugin mit dem Alerting-Plugin koppeln, um Sie zu benachrichtigen, sobald eine Anomalie erkannt wird.

Die Erkennung von Anomalien ist für Domains verfügbar, auf denen eine beliebige OpenSearch Version oder Elasticsearch 7.4 oder höher ausgeführt wird. Alle Instance-Typen unterstützen die Anomalieerkennung für `t2.micro` und `t2.small`.

> **Note**
>
> Diese Dokumentation bietet einen kurzen Überblick über die Erkennung von Anomalien im Kontext von Amazon OpenSearch Service. Eine umfassende Dokumentation, einschließlich detaillierter Schritte, einer API-Referenz, einer Referenz aller verfügbaren Einstellungen und Schritten zur Erstellung von Visualisierungen und Dashboards, finden Sie unter Anomalieerkennung in der Open-Source-Dokumentation. OpenSearch

Voraussetzungen

Für die Anomalieerkennung müssen die folgenden Voraussetzungen erfüllt sein:

- Für die Erkennung von Anomalien ist Elasticsearch 7.4 OpenSearch oder höher erforderlich.
- Die Anomalieerkennung unterstützt nur eine detaillierte Zugriffskontrolle auf Elasticsearch-Versionen 7.9 und höher sowie auf allen Versionen von. OpenSearch Vor Elasticsearch 7.9 können nur Admin-Benutzer Detektoren erstellen, anzeigen und verwalten.
- Wenn Ihre Domain eine differenzierte Zugriffskontrolle verwendet, müssen Benutzer ohne Administratorrechte der `anomaly_read_access` Rolle in den OpenSearch Dashboards zugeordnet werden, um Melder anzeigen zu können oder um Detektoren zu erstellen und zu verwalten. `anomaly_full_access`

Erste Schritte mit der Anomalieerkennung

Wählen Sie zunächst die Option Anomalieerkennung in Dashboards aus. OpenSearch

Schritt 1: Erstellen eines Detektors

Ein Detektor ist eine individuelle Anomalieerkennungsaufgabe. Sie können mehrere Detektoren erstellen, und alle Detektoren können gleichzeitig ausgeführt werden, wobei jeder Daten aus verschiedenen Quellen analysiert.

Schritt 2: Hinzufügen von Funktionen zu Ihrem Detektor

Eine Funktion ist das Feld in Ihrem Index, das Sie auf Anomalien überprüfen. Ein Detektor kann Anomalien in einer oder mehreren Funktionen entdecken. Sie müssen für jede Funktion eine der folgenden Aggregationen auswählen: `average()`, `sum()`, `count()`, `min()` oder `max()`.

> **Note**
>
> Die `count()` Aggregationsmethode ist nur in Elasticsearch 7.7 OpenSearch oder höher verfügbar. Verwenden Sie für Elasticsearch 7.4 einen benutzerdefinierten Ausdruck wie den folgenden:
>
> ```
> {
>   "aggregation_name": {
>      "value_count": {
>         "field": "field_name"
>      }
>   }
> }
> ```

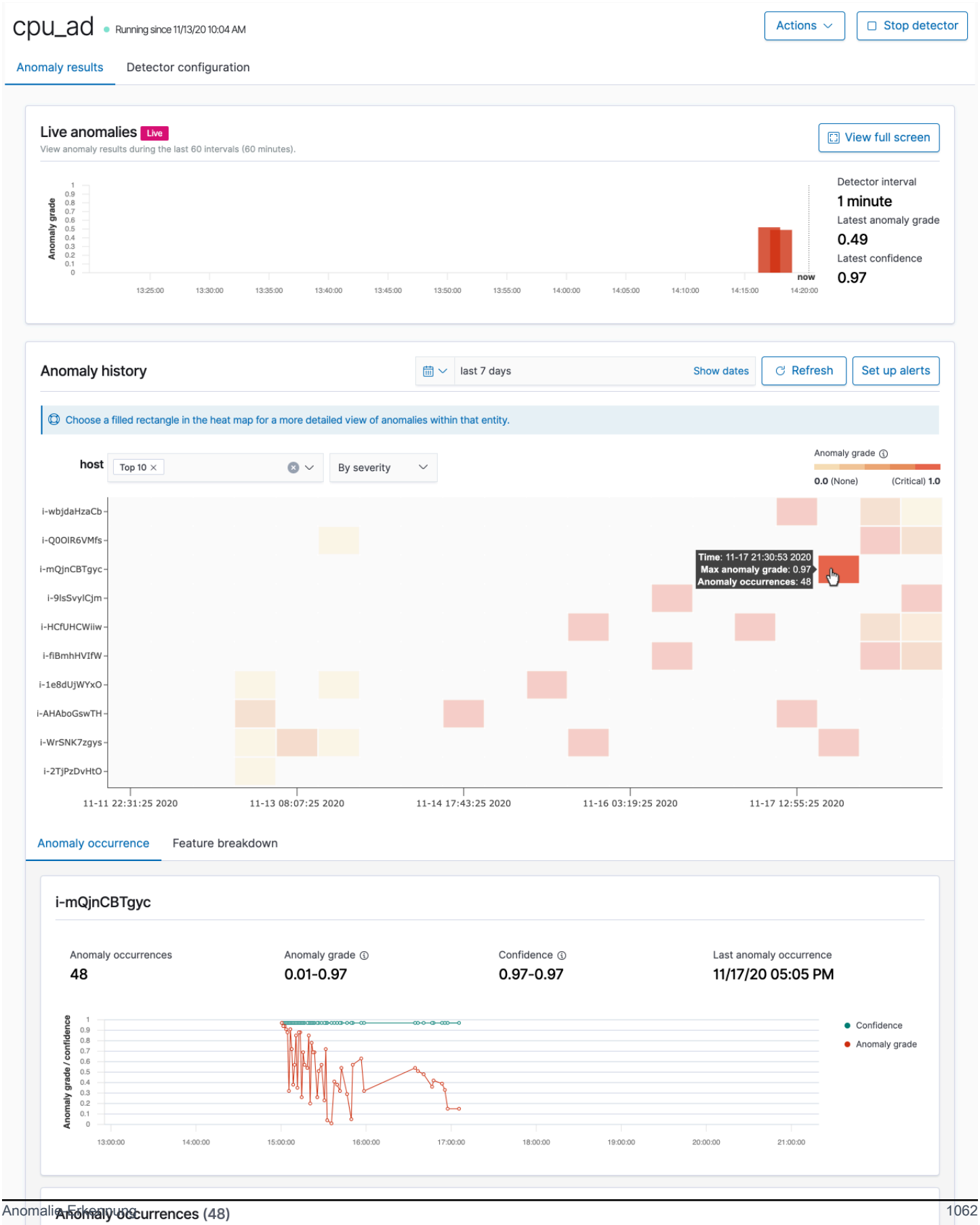
Die Aggregationsmethode legt fest, was eine Anomalie darstellt. Wenn Sie beispielsweise `min()` wählen, konzentriert sich der Detektor darauf, Anomalien basierend auf den Mindestwerten Ihrer Funktion zu finden. Wenn Sie `average()` wählen, findet der Detektor Anomalien basierend auf den Durchschnittswerten Ihrer Funktion. Sie können maximal fünf Funktionen pro Detektor hinzufügen.

Sie können die folgenden optionalen Einstellungen konfigurieren (verfügbar in Elasticsearch 7.7 und höher):

- Kategorie-Feld – Kategorisieren oder schneiden Sie Ihre Daten mit einer Dimension wie IP-Adresse, Produkt-ID, Ländercode usw.
- Größe des Fensters – Legen Sie die Anzahl der Aggregationsintervalle aus Ihrem Datenstrom fest, die in einem Erkennungsfenster berücksichtigt werden sollen.

Nachdem Sie die Funktionen eingerichtet haben, können Sie eine Vorschau von Beispielanomalien anzeigen und ggf. die Funktions-Einstellungen anpassen.

Schritt 3: Beobachten der Ergebnisse



- Live-Anomalien zeigt die Live-Anomalie-Ergebnisse für die letzten 60 Intervalle an. Wenn das Intervall beispielsweise auf 10 eingestellt ist, werden die Ergebnisse der letzten 600 Minuten angezeigt. Dieses Diagramm wird alle 30 Sekunden aktualisiert.
- Anomalieverlauf zeichnet die Anomalieklasse mit dem entsprechenden Konfidenzmaß.
- Funktionsaufschlüsselung – zeichnet die Funktionen basierend auf der Aggregationsmethode. Sie können den Datums-Uhrzeitbereich des Detektors variieren.
- Anomalie-Vorkommnisse – zeigen `Start time`, `End time`, `Data confidence` und `Anomaly grade` für jede erkannte Anomalie an.

  Wenn Sie das Kategoriefeld festlegen, sehen Sie ein zusätzliches Heatmap-Diagramm, das die Ergebnisse für anomale Elemente korreliert. Wählen Sie ein gefülltes Rechteck, um eine detailliertere Ansicht der Anomalie anzuzeigen.

Schritt 4: Einrichten von Warnungen

Um einen Monitor zu erstellen, der Ihnen Benachrichtigungen sendet, wenn Anomalien erkannt werden, wählen Sie Warnungen einrichten. Das Plug-In leitet Sie auf die Seite Monitor hinzufügen weiter, auf der Sie eine Warnung konfigurieren können.

Tutorial: Erkennen hoher CPU-Auslastung mit Anomalieerkennung

Dieses Tutorial zeigt, wie Sie in Amazon OpenSearch Service einen Anomaliedetektor erstellen, um eine hohe CPU-Auslastung zu erkennen. Mithilfe von OpenSearch Dashboards konfigurieren Sie einen Detektor, der die CPU-Auslastung überwacht und eine Warnung generiert, wenn Ihre CPU-Auslastung einen bestimmten Schwellenwert überschreitet.

> **Note**
>
> Diese Schritte gelten für die neueste Version von OpenSearch und können für frühere Versionen leicht abweichen.

Voraussetzungen

- Sie müssen über eine OpenSearch Service-Domain verfügen, auf der Elasticsearch 7.4 oder höher oder eine beliebige OpenSearch Version ausgeführt wird.

- Sie müssen Anwendungsprotokolldateien in Ihren Cluster aufnehmen, die CPU-Auslastungsdaten enthalten.

Schritt 1: Erstellen eines Detektors

Erstellen Sie zunächst einen Detektor, der Anomalien in Ihren CPU-Auslastungsdaten identifiziert.

1. Öffnen Sie das linke Bedienfeldmenü in den OpenSearch Dashboards und wählen Sie „Anomalieerkennung“ und anschließend „Detektor erstellen“.
2. Benennen Sie den Detektor **`high-cpu-usage`**.
3. Wählen Sie für Ihre Datenquelle Ihren Index aus, der Protokolldateien zur CPU-Auslastung enthält, in denen Sie Anomalien identifizieren möchten.
4. Wählen Sie das Feld Timestamp (Zeitstempel) in Ihren Daten aus. Optional können Sie einen Datenfilter hinzufügen. Dieser Datenfilter analysiert nur eine Teilmenge der Datenquelle und reduziert die Menge irrelevanter Daten.
5. Legen Sie den Wert für Detector interval (Detektorintervall) auf 2 Minuten fest. Dieses Intervall definiert die Zeit (in minütlichen Intervallen), die der Detektor benötigt, um die Daten zu sammeln.
6. Fügen Sie unter Window delay (Fensterverzögerung) eine Verzögerung von 1 Minute hinzu. Diese Verzögerung erhöht die Verarbeitungszeit, um sicherzustellen, dass alle Daten innerhalb des Fensters vorhanden sind.
7. Wählen Sie Weiter aus. Wählen Sie im Dashboard zur Erkennung von Anomalien unter dem Namen des Detektors Configure model (Modell konfigurieren).
8. Für Feature name (Feature-Namen) geben Sie **`max_cpu_usage`** ein. Für Feature state (Feature-Zustand) wählen Sie Enable feature (Feature aktivieren) aus.
9. Für Find anomalies based on (Anomalien finden anhand von) wählen Sie Field value (Feldwert).
10. Für Aggregation method (Aggregationsmethode) wählen Sie **`max()`** aus.
11. Für Field (Feld) wählen Sie das Feld in Ihren Daten aus, das auf Anomalien überprüft werden soll. Ein Beispiel wäre `cpu_usage_percentage`.
12. Behalten Sie alle anderen Einstellungen als Standardwerte bei und wählen Sie Next (Weiter) aus.
13. Ignorieren Sie die Einrichtung von Detektoraufträgen und klicken Sie auf Next (Weiter).
14. Wählen Sie im Popup-Fenster aus, wann der Detektor starten soll (automatisch oder manuell) und klicken Sie dann auf Confirm (Bestätigen).

Nachdem der Detektor konfiguriert ist, können Sie nach seiner Initialisierung Echtzeitergebnisse der CPU-Auslastung im Abschnitt Real-time results (Echtzeit-Ergebnisse) Ihres Detektorfensters ansehen. Der Abschnitt Live anomalies (Live-Anomalien) zeigt alle Anomalien an, die bei der Aufnahme von Daten in Echtzeit auftreten.

Schritt 2: Konfigurieren einer Warnung

Nachdem Sie einen Detektor erstellt haben, erstellen Sie eine Überwachung, die eine Warnung auslöst und eine Nachricht an Slack sendet, wenn eine CPU-Auslastung erkannt wird, die die in den Detektoreinstellungen angegebenen Bedingungen erfüllt. Sie erhalten Slack-Benachrichtigungen, wenn Daten aus einem oder mehreren Indizes die Bedingungen erfüllen, die die Warnung auslösen.

1. Öffnen Sie das linke Bedienfeldmenü in den OpenSearch Dashboards und wählen Sie „Alerting“ und anschließend „Monitor erstellen“.
2. Geben Sie einen Namen für die Überwachung an.
3. Für Monitor type (Überwachungstyp) wählen Sie Per-query monitor (Überwachung pro Abfrage) aus. Eine abfragebasierte Überwachung führt eine angegebene Abfrage aus und definiert die Trigger.
4. Wählen Sie für Monitor defining method (Definierende Methode überwachen) Anomaly detector (Anomaliedetektor) aus. Wählen Sie dann den Detektor im Dropdown-Menü Detector (Detektor) aus, den Sie im vorherigen Abschnitt erstellt haben.
5. Wählen Sie für Schedule (Plan) aus, wie oft die Überwachung Daten erfassen soll und wie oft Sie alarmiert werden möchten. Legen Sie für die Zwecke dieses Tutorials die Ausführung alle 7 Minuten fest.
6. Wählen Sie im Bereich Triggers (Auslöser) Add trigger (Auslöser hinzufügen) aus. Für Trigger name (Auslösername) geben Sie **`High CPU usage`** ein. In diesem Tutorial wählen Sie für Severity level (Schweregrad) 1 aus. Das ist der höchste Schweregrad.
7. Für Anomaly grade threshold (Anomalieklassen-Schwellenwert) wählen Sie IS ABOVE (LIEGT ÜBER) aus. Wählen Sie im Menü darunter den anzuwendenden Klassen-Schwellenwert aus. Stellen Sie für dieses Tutorial die Anomaly grade (Anomalieklasse) zu 0.7.
8. Für Anomaly confidence threshold (Anomaliekonfidenz-Schwellenwert) wählen Sie IS ABOVE (LIEGT ÜBER) aus. Geben Sie im Menü darunter dieselbe Zahl wie für die Anomalieklasse an. Stellen Sie für dieses Tutorial den Anomaly confidence threshold (Anomaliekonfidenz-Schwellenwert) 0.7 ein.
9. Im Bereich Actions (Aktionen) wählen Sie Destination (Ziel) aus. Wählen Sie im Feld Name den Namen des Ziels aus. Wählen Sie im Menü Type (Typ) Slack aus. Im Feld Webhook URL

(Webhook-URL) geben seine Webhook-URL ein, an die Alarme gesendet werden sollen. Weitere Informationen finden Sie unter Sending messages using incoming webhooks (Senden von Nachrichten mit eingehenden Webhooks).

10. Wählen Sie Erstellen.

Zugehörige Ressourcen

- the section called “Warnfunktion”

- the section called “Anomalie-Erkennung”
- API zur Anomalieerkennung

Maschinelles Lernen für Amazon OpenSearch Service

ML Commons ist ein OpenSearch Plugin, das eine Reihe gängiger Algorithmen für maschinelles Lernen (ML) durch Transport- und REST-API-Aufrufe bereitstellt. Diese Aufrufe wählen die richtigen Knoten und Ressourcen für jede ML-Anfrage aus und überwachen ML-Aufgaben, um die Verfügbarkeit sicherzustellen. Auf diese Weise können Sie bestehende Open-Source-ML-Algorithmen nutzen und den Aufwand für die Entwicklung neuer ML-Funktionen reduzieren. Weitere Informationen zum Plugin finden Sie in der OpenSearch Dokumentation unter Maschinelles Lernen. In diesem Kapitel wird beschrieben, wie Sie das Plugin mit Amazon OpenSearch Service verwenden.

Themen

Amazon OpenSearch Service ML-Konnektoren für AWS-Services

Wenn Sie Amazon OpenSearch Service Machine Learning (ML) Connectors mit einem anderen verwenden AWS-Service, müssen Sie eine IAM-Rolle einrichten, um Service sicher mit diesem OpenSearch Service zu verbinden. AWS-Services dass Sie einen Connector einrichten können, der Amazon SageMaker und Amazon Bedrock einschließt. In diesem Tutorial erfahren Sie, wie Sie einen Connector von OpenSearch Service zu SageMaker Runtime erstellen. Weitere Informationen zu Konnektoren finden Sie unter Unterstützte Konnektoren.

Themen

Voraussetzungen

Um einen Connector zu erstellen, benötigen Sie einen SageMaker Amazon-Domain-Endpunkt und eine IAM-Rolle, die OpenSearch Servicezugriff gewährt.

Richten Sie eine SageMaker Amazon-Domain ein

Informationen zur Bereitstellung Ihres Machine-Learning-Modells finden Sie unter Bereitstellen eines Modells SageMaker in Amazon im Amazon SageMaker Developer Guide. Notieren Sie sich die Endpunkt-URL für Ihr Modell, die Sie benötigen, um einen AI-Connector zu erstellen.

Erstellen einer IAM-Rolle

Richten Sie eine IAM-Rolle ein, um SageMaker Runtime-Berechtigungen an den Service zu OpenSearch delegieren. Informationen zum Erstellen einer neuen Rolle finden Sie unter Erstellen einer IAM-Rolle (Konsole) im IAM-Benutzerhandbuch. Optional können Sie eine bestehende Rolle verwenden, sofern sie über dieselben Rechte verfügt. Wenn Sie eine neue Rolle erstellen, anstatt eine AWS verwaltete Rolle zu verwenden, ersetzen Sie sie `opensearch-sagemaker-role` in diesem Tutorial durch den Namen Ihrer eigenen Rolle.

1. Fügen Sie Ihrer neuen Rolle die folgende verwaltete IAM-Richtlinie hinzu, damit OpenSearch Service auf Ihren SageMaker Endpunkt zugreifen kann. Informationen zum Anhängen einer Richtlinie an eine Rolle finden Sie unter Hinzufügen von IAM-Identitätsberechtigungen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sagemaker:InvokeEndpointAsync",
                "sagemaker:InvokeEndpoint"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

2. Folgen Sie den Anweisungen unter Vertrauensrichtlinie für Rollen ändern, um die Vertrauensstellung der Rolle zu bearbeiten. Sie müssen OpenSearch Service in der `Principal` Erklärung angeben:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Action": [
                "sts:AssumeRole"
            ],
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "opensearchservice.amazonaws.com"
                ]
            }
        }
    ]
}
```

Wir empfehlen, die Bedingungsschlüssel `aws:SourceAccount` und die `aws:SourceArn` Bedingungsschlüssel zu verwenden, um den Zugriff auf eine bestimmte Domain zu beschränken. Das `SourceAccount` ist die AWS-Konto ID, die dem Besitzer der Domain gehört, und das `SourceArn` ist der ARN der Domain. Sie können der Vertrauensrichtlinie beispielsweise den folgenden Bedingungsblock hinzufügen:

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account-id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:es:region:account-id:domain/domain-name"
    }
}
```

Konfigurieren von Berechtigungen

Um den Connector zu erstellen, benötigen Sie die Erlaubnis, die IAM-Rolle an OpenSearch Service zu übergeben. Sie benötigen außerdem Zugriff auf die Aktion `es:ESHttpPost`. Um diese beiden Berechtigungen zu erteilen, fügen Sie die folgende Richtlinie an die IAM-Rolle an, deren Anmeldeinformationen zum Signieren der Anforderung verwendet werden:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::account-id:role/opensearch-sagemaker-role"
    },
    {
      "Effect": "Allow",
      "Action": "es:ESHttpPost",
      "Resource": "arn:aws:es:region:account-id:domain/domain-name/*"
    }
  ]
}
```

Wenn Ihr Benutzer oder Ihre Rolle nicht `iam:PassRole` berechtigt ist, Ihre Rolle weiterzugeben, kann es sein, dass beim Versuch, ein Repository im nächsten Schritt zu registrieren, ein Autorisierungsfehler auftritt.

Ordnen Sie die ML-Rolle in OpenSearch Dashboards zu (wenn Sie eine differenzierte Zugriffskontrolle verwenden)

Durch eine differenzierte Zugriffskontrolle wird beim Einrichten eines Konnektors ein zusätzlicher Schritt eingeführt. Auch wenn Sie die HTTP-Basisauthentifizierung für alle anderen Zwecke verwenden, müssen Sie die `ml_full_access`-Rolle Ihrer IAM-Rolle mit `iam:PassRole`-Berechtigungen zuordnen, um `opensearch-sagemaker-role` zu übergeben.

1. Navigieren Sie zum OpenSearch Dashboards-Plugin für Ihre OpenSearch Service-Domain. Sie finden den Dashboards-Endpunkt in Ihrem Domain-Dashboard in der OpenSearch Service-Konsole.
2. Wählen Sie im Hauptmenü Sicherheit, Rollen und dann die Rolle ml_full_access aus.
3. Wählen Sie Zugeordnete Benutzer, Mapping verwalten.
4. Fügen Sie unter Backend-Rollen den ARN der Rolle hinzu, die über Berechtigungen zur Weitergabe `opensearch-sagemaker-role` verfügt.

   ```
   arn:aws:iam::account-id:role/role-name
   ```

5. Wählen Sie Zuordnen und bestätigen Sie, dass der Benutzer oder die Rolle unter Zugeordnete Benutzer angezeigt wird.

Erstellen Sie einen OpenSearch Service-Connector

Um einen Connector zu erstellen, senden Sie eine POST Anfrage an den Endpunkt der OpenSearch Service-Domäne. Sie können curl, den Python-Beispielclient, Postman oder eine andere Methode verwenden, um eine signierte Anfrage zu senden. Beachten Sie, dass Sie eine POST Anfrage in der Kibana-Konsole nicht verwenden können. Die Anfrage hat das folgende Format:

```
POST domain-endpoint/_plugins/_ml/connectors/_create
{
   "name": "sagemaker: embedding",
   "description": "Test connector for Sagemaker embedding model",
   "version": 1,
   "protocol": "aws_sigv4",
   "credential": {
      "roleArn": "arn:aws:iam::account-id:role/opensearch-sagemaker-role"
   },
   "parameters": {
      "region": "region",
      "service_name": "sagemaker"
   },
   "actions": [
      {
         "action_type": "predict",
         "method": "POST",
         "headers": {
            "content-type": "application/json"
         },
         "url": "https://runtime.sagemaker.region.amazonaws.com/endpoints/endpoint-id/
invocations",
         "request_body": "{ \"inputs\": { \"question\": \"${parameters.question}\",
 \"context\": \"${parameters.context}\" } }"
      }
   ]
}
```

Wenn sich Ihre Domain in einer Virtual Private Cloud (VPC) befindet, muss Ihr Computer mit der VPC verbunden sein, damit die Anfrage den AI-Connector erfolgreich erstellen kann. Der Zugriff auf eine VPC hängt von der Netzwerkkonfiguration ab, beinhaltet jedoch in der Regel eine Verbindung zu einem VPN- oder Unternehmensnetzwerk. Um zu überprüfen, ob Sie Ihre OpenSearch Service-Domain erreichen können, navigieren Sie `https://your-vpc-`

domain.*region*.es.amazonaws.com in einem Webbrowser zu und stellen Sie sicher, dass Sie die Standard-JSON-Antwort erhalten.

Beispiel für einen Python-Client

Der Python-Client ist einfacher zu automatisieren als eine HTTP-Anfrage und hat eine bessere Wiederverwendbarkeit. Um den AI-Konnektor mit dem Python-Client zu erstellen, speichern Sie den folgenden Beispielcode in einer Python-Datei. Der Client benötigt die `requests-aws4auth`Pakete AWS SDK for Python (Boto3)`requests`, und.

```
import boto3
import requests
from requests_aws4auth import AWS4Auth

host = 'domain-endpoint/'
region = 'region'
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)

# Register repository
path = '_plugins/_ml/connectors/_create'
url = host + path

payload = {
   "name": "sagemaker: embedding",
   "description": "Test connector for Sagemaker embedding model",
   "version": 1,
   "protocol": "aws_sigv4",
   "credential": {
      "roleArn": "arn:aws:iam::account-id:role/opensearch-sagemaker-role"
   },
   "parameters": {
      "region": "region",
      "service_name": "sagemaker"
   },
   "actions": [
      {
         "action_type": "predict",
         "method": "POST",
         "headers": {
            "content-type": "application/json"
```

```
        },
        "url": "https://runtime.sagemaker.region.amazonaws.com/endpoints/endpoint-id/
invocations",
        "request_body": "{ \"inputs\": { \"question\": \"${parameters.question}\",
 \"context\": \"${parameters.context}\" } }"
      }
   ]
}
headers = {"Content-Type": "application/json"}

r = requests.post(url, auth=awsauth, json=payload, headers=headers)
print(r.status_code)
print(r.text)
```

Amazon OpenSearch Service ML-Konnektoren für Plattformen von Drittanbietern

In diesem Tutorial erfahren Sie, wie Sie einen Connector von OpenSearch Service zu Cohere erstellen. Weitere Informationen zu Konnektoren finden Sie unter Unterstützte Konnektoren.

Wenn Sie einen Amazon OpenSearch Service Machine Learning (ML) Connector mit einem externen Remote-Modell verwenden, müssen Sie Ihre spezifischen Autorisierungsdaten in speichern AWS Secrets Manager. Dies kann ein API-Schlüssel oder eine Kombination aus Benutzername und Passwort sein. Das bedeutet, dass Sie auch eine IAM-Rolle erstellen müssen, die es OpenSearch Service Access ermöglicht, aus Secrets Manager zu lesen.

Themen

Voraussetzungen

Um einen Connector für Cohere oder einen externen Anbieter mit OpenSearch Service zu erstellen, benötigen Sie eine IAM-Rolle, die dem OpenSearch Service Zugriff auf den Ort gewährt AWS Secrets Manager, an dem Sie Ihre Anmeldeinformationen speichern. Sie müssen Ihre Anmeldeinformationen auch in Secrets Manager speichern.

Erstellen einer IAM-Rolle

Richten Sie eine IAM-Rolle ein, um Secrets Manager Manager-Berechtigungen an den Service zu OpenSearch delegieren. Sie können auch die vorhandene `SecretManagerReadWrite` Rolle verwenden. Informationen zum Erstellen einer neuen Rolle finden Sie unter Erstellen einer IAM-Rolle (Konsole) im IAM-Benutzerhandbuch. Wenn Sie eine neue Rolle erstellen, anstatt eine AWS verwaltete Rolle zu verwenden, ersetzen Sie sie `opensearch-secretmanager-role` in diesem Tutorial durch den Namen Ihrer eigenen Rolle.

1. Fügen Sie Ihrer neuen Rolle die folgende verwaltete IAM-Richtlinie hinzu, damit OpenSearch Service auf Ihre Secrets Manager Manager-Werte zugreifen kann. Informationen zum Anhängen einer Richtlinie an eine Rolle finden Sie unter Hinzufügen von IAM-Identitätsberechtigungen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

2. Folgen Sie den Anweisungen unter Vertrauensrichtlinie für Rollen ändern, um die Vertrauensstellung der Rolle zu bearbeiten. Sie müssen OpenSearch Service in der `Principal` Erklärung angeben:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sts:AssumeRole"
            ],
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "opensearchservice.amazonaws.com"
```

```
                ]
            }
        }
    ]
}
```

Es wird empfohlen, die Bedingungsschlüssel `aws:SourceAccount` und die `aws:SourceArn` Bedingungsschlüssel zu verwenden, um den Zugriff auf eine bestimmte Domäne zu beschränken. Das `SourceAccount` ist die AWS-Konto ID, die dem Besitzer der Domain gehört, und das `SourceArn` ist der ARN der Domain. Sie können der Vertrauensrichtlinie beispielsweise den folgenden Bedingungsblock hinzufügen:

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account-id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:es:region:account-id:domain/domain-name"
    }
}
```

Konfigurieren von Berechtigungen

Um den Connector zu erstellen, benötigen Sie die Erlaubnis, die IAM-Rolle an OpenSearch Service zu übergeben. Sie benötigen außerdem Zugriff auf die Aktion `es:ESHttpPost`. Um diese beiden Berechtigungen zu erteilen, fügen Sie die folgende Richtlinie an die IAM-Rolle an, deren Anmeldeinformationen zum Signieren der Anforderung verwendet werden:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::account-id:role/opensearch-secretmanager-role"
    },
    {
      "Effect": "Allow",
      "Action": "es:ESHttpPost",
      "Resource": "arn:aws:es:region:account-id:domain/domain-name/*"
```

```
    }
  ]
}
```

Wenn Ihr Benutzer oder Ihre Rolle nicht `iam:PassRole` berechtigt ist, Ihre Rolle weiterzugeben, kann es sein, dass beim Versuch, ein Repository im nächsten Schritt zu registrieren, ein Autorisierungsfehler auftritt.

Richten Sie ein AWS Secrets Manager

Informationen zum Speichern Ihrer Autorisierungsdaten in Secrets Manager finden Sie unter Create an AWS Secrets Manager Secret im AWS Secrets Manager Benutzerhandbuch.

Nachdem Secrets Manager Ihr Schlüssel-Wert-Paar als Geheimnis akzeptiert hat, erhalten Sie einen ARN mit dem Format:. `arn:aws:secretsmanager:us-west-2:123456789012:secret:MySecret-a1b2c3` Notieren Sie sich diesen ARN, wie Sie ihn verwenden, und Ihren Schlüssel, wenn Sie im nächsten Schritt einen Connector erstellen.

Ordnen Sie die ML-Rolle in OpenSearch Dashboards zu (wenn Sie eine differenzierte Zugriffskontrolle verwenden)

Durch eine differenzierte Zugriffskontrolle wird beim Einrichten eines Konnektors ein zusätzlicher Schritt eingeführt. Auch wenn Sie die HTTP-Basisauthentifizierung für alle anderen Zwecke verwenden, müssen Sie die `ml_full_access`-Rolle Ihrer IAM-Rolle mit `iam:PassRole`-Berechtigungen zuordnen, um `opensearch-sagemaker-role` zu übergeben.

1. Navigieren Sie zum OpenSearch Dashboards-Plugin für Ihre OpenSearch Service-Domain. Sie finden den Dashboards-Endpunkt in Ihrem Domain-Dashboard in der OpenSearch Service-Konsole.
2. Wählen Sie im Hauptmenü Sicherheit, Rollen und dann die Rolle ml_full_access aus.
3. Wählen Sie Zugeordnete Benutzer, Mapping verwalten.
4. Fügen Sie unter Backend-Rollen den ARN der Rolle hinzu, die über Berechtigungen zur Weitergabe `opensearch-sagemaker-role` verfügt.

   ```
   arn:aws:iam::account-id:role/role-name
   ```

5. Wählen Sie Zuordnen und bestätigen Sie, dass der Benutzer oder die Rolle unter Zugeordnete Benutzer angezeigt wird.

Erstellen Sie einen OpenSearch Service-Connector

Um einen Connector zu erstellen, senden Sie eine `POST` Anfrage an den Endpunkt der OpenSearch Service-Domäne. Sie können curl, den Python-Beispielclient, Postman oder eine andere Methode verwenden, um eine signierte Anfrage zu senden. Beachten Sie, dass Sie eine `POST` Anfrage in der Kibana-Konsole nicht verwenden können. Die Anfrage hat das folgende Format:

```
POST domain-endpoint/_plugins/_ml/connectors/_create
{
    "name": "Cohere Connector: embedding",
    "description": "The connector to cohere embedding model",
    "version": 1,
    "protocol": "http",
    "credential": {
        "secretArn": "arn:aws:secretsmanager:region:account-id:secret:cohere-key-id",
        "roleArn": "arn:aws:iam::account-id:role/opensearch-secretmanager-role"
    },
    "actions": [
        {
            "action_type": "predict",
            "method": "POST",
            "url": "https://api.cohere.ai/v1/embed",
            "headers": {
                "Authorization": "Bearer ${credential.secretArn.cohere-key-used-in-
secrets-manager}"
            },
            "request_body": "{ \"texts\": ${parameters.texts}, \"truncate\": \"END\" }"
        }
    ]
}
```

Der Anfragetext für diese Anfrage unterscheidet sich in zweierlei Hinsicht von dem einer Open-Source-Connector-Anfrage. Innerhalb des `credential` Felds übergeben Sie den ARN für die IAM-Rolle, die es OpenSearch Service ermöglicht, aus Secrets Manager zu lesen, zusammen mit dem ARN für welches Geheimnis. In `headers` diesem Feld verweisen Sie auf das Geheimnis, indem Sie den geheimen Schlüssel und die Tatsache verwenden, dass es aus einem ARN stammt.

Wenn sich Ihre Domain in einer Virtual Private Cloud (VPC) befindet, muss Ihr Computer mit der VPC verbunden sein, damit die Anfrage den AI-Connector erfolgreich erstellen kann. Der Zugriff auf eine VPC hängt von der Netzwerkkonfiguration ab, beinhaltet jedoch in der Regel eine Verbindung zu einem VPN- oder Unternehmensnetzwerk. Um zu überprüfen, ob Sie

Ihre OpenSearch Service-Domain erreichen können, navigieren Sie `https://your-vpc-domain.region.es.amazonaws.com` in einem Webbrowser zu und stellen Sie sicher, dass Sie die Standard-JSON-Antwort erhalten.

Beispiel für einen Python-Client

Der Python-Client ist einfacher zu automatisieren als eine HTTP-Anfrage und hat eine bessere Wiederverwendbarkeit. Um den AI-Konnektor mit dem Python-Client zu erstellen, speichern Sie den folgenden Beispielcode in einer Python-Datei. Der Client benötigt die `requests-aws4auth`Pakete AWS SDK for Python (Boto3)`requests`, und.

```
import boto3
import requests
from requests_aws4auth import AWS4Auth

host = 'domain-endpoint/'
region = 'region'
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)

path = '_plugins/_ml/connectors/_create'
url = host + path

payload = {
    "name": "Cohere Connector: embedding",
    "description": "The connector to cohere embedding model",
    "version": 1,
    "protocol": "http",
    "credential": {
        "secretArn": "arn:aws:secretsmanager:region:account-id:secret:cohere-key-id",
        "roleArn": "arn:aws:iam::account-id:role/opensearch-secretmanager-role"
    },
    "actions": [
        {
            "action_type": "predict",
            "method": "POST",
            "url": "https://api.cohere.ai/v1/embed",
            "headers": {
                "Authorization": "Bearer ${credential.secretArn.cohere-key-used-in-
secrets-manager}"
            },
```

```
            "request_body": "{ \"texts\": ${parameters.texts}, \"truncate\": \"END\" }"
        }
    ]
}

headers = {"Content-Type": "application/json"}

r = requests.post(url, auth=awsauth, json=payload, headers=headers)
print(r.status_code)
print(r.text)
```

Wird verwendet AWS CloudFormation , um Remote-Inferenz für die semantische Suche einzurichten

Ab OpenSearch Version 2.9 können Sie Remote-Inferenz mit semantischer Suche verwenden, um Ihre eigenen Modelle für maschinelles Lernen (ML) zu hosten. Remote Inference verwendet das ML Commons-Plugin, damit Sie Ihre Modellinferenzen remote auf ML-Diensten wie Amazon BedRock hosten Amazon SageMaker und sie über ML-Konnektoren mit Amazon OpenSearch Service verbinden können.

Um die Einrichtung von Remote-Inferenzen zu vereinfachen, stellt Amazon OpenSearch Service eine AWS CloudFormationVorlage in der Konsole bereit. CloudFormation ist eine AWS-Service , mit der Sie Ressourcen von Drittanbietern modellieren, bereitstellen AWS und verwalten können, indem Sie Infrastruktur als Code behandeln.

Die OpenSearch CloudFormation Vorlage automatisiert den Prozess der Modellbereitstellung für Sie, sodass Sie auf einfache Weise ein Modell in Ihrer OpenSearch Service-Domain erstellen und dann die Modell-ID verwenden können, um Daten aufzunehmen und neuronale Suchabfragen auszuführen.

Wenn Sie neuronale Sparse-Encoder mit OpenSearch Service Version 2.12 und höher verwenden, empfehlen wir, das Tokenizer-Modell lokal zu verwenden, anstatt es remote bereitzustellen. Weitere Informationen finden Sie in der Dokumentation unter Sparse-Kodierungsmodelle. OpenSearch

Themen

- Voraussetzungen
- Amazon SageMaker Vorlagen
- Amazon Bedrock-Vorlagen

Voraussetzungen

Um eine CloudFormation Vorlage mit OpenSearch Service zu verwenden, müssen Sie die folgenden Voraussetzungen erfüllen.

Richten Sie eine OpenSearch Dienstdomäne ein

Bevor Sie eine CloudFormation Vorlage verwenden können, müssen Sie eine Amazon OpenSearch Service-Domain mit Version 2.9 oder höher und aktivierter detaillierter Zugriffskontrolle einrichten. Erstellen Sie eine OpenSearch Service-Backend-Rolle, um dem ML Commons-Plugin die Erlaubnis zu erteilen, Ihren Connector für Sie zu erstellen.

Die CloudFormation Vorlage erstellt für Sie eine Lambda-IAM-Rolle mit dem Standardnamen`LambdaInvokeOpenSearchMLCommonsRole`, den Sie überschreiben können, wenn Sie einen anderen Namen wählen möchten. Nachdem die Vorlage diese IAM-Rolle erstellt hat, müssen Sie der Lambda-Funktion die Erlaubnis erteilen, Ihre OpenSearch Service-Domain aufzurufen. Ordnen Sie dazu die benannte Rolle mit `ml_full_access` den folgenden Schritten Ihrer OpenSearch Service-Backend-Rolle zu:

1. Navigieren Sie zum OpenSearch Dashboards-Plugin für Ihre OpenSearch Service-Domain. Sie finden den Dashboards-Endpunkt in Ihrem Domain-Dashboard in der OpenSearch Service-Konsole.
2. Wählen Sie im Hauptmenü Sicherheit, Rollen und dann die Rolle ml_full_access aus.
3. Wählen Sie Zugeordnete Benutzer, Mapping verwalten.
4. Fügen Sie unter Backend-Rollen den ARN der Lambda-Rolle hinzu, für die eine Berechtigung zum Aufrufen Ihrer Domain erforderlich ist.

   ```
   arn:aws:iam::account-id:role/role-name
   ```

5. Wählen Sie Zuordnen und bestätigen Sie, dass der Benutzer oder die Rolle unter Zugeordnete Benutzer angezeigt wird.

Nachdem Sie die Rolle zugeordnet haben, navigieren Sie zur Sicherheitskonfiguration Ihrer Domain und fügen Sie die Lambda IAM-Rolle zu Ihrer OpenSearch Servicezugriffsrichtlinie hinzu.

Aktivieren Sie die Berechtigungen für Ihr AWS-Konto

Sie AWS-Konto müssen über die Zugriffsberechtigung CloudFormation und Lambda verfügen, zusammen mit dem, was AWS-Service Sie für Ihre Vorlage wählen — entweder SageMaker Runtime oder Amazon. BedRock

Wenn Sie Amazon Bedrock verwenden, müssen Sie auch Ihr Modell registrieren. Informationen zur Registrierung Ihres Modells finden Sie unter Modellzugriff im Amazon Bedrock-Benutzerhandbuch.

Wenn Sie Ihren eigenen Amazon S3 S3-Bucket verwenden, um Modellartefakte bereitzustellen, müssen Sie die CloudFormation IAM-Rolle zu Ihrer S3-Zugriffsrichtlinie hinzufügen. Informationen finden Sie im Abschnitt Hinzufügen und Entfernen von IAM-Identitätsberechtigungen im -IAM-Benutzerhandbuch.

Amazon SageMaker Vorlagen

Die SageMaker CloudFormation Amazon-Vorlagen definieren mehrere AWS Ressourcen, um das neuronale Plugin und die semantische Suche für Sie einzurichten.

Verwenden Sie zunächst die SageMaker Vorlage Integration mit Texteinbettungsmodellen über Amazon, um ein Texteinbettungsmodell in SageMaker Runtime als Server bereitzustellen. Wenn Sie keinen Modellendpunkt angeben, CloudFormation erstellt eine IAM-Rolle, die es SageMaker Runtime ermöglicht, Modellartefakte von Amazon S3 herunterzuladen und auf dem Server bereitzustellen. Wenn Sie einen Endpunkt angeben, CloudFormation erstellt eine IAM-Rolle, die der Lambda-Funktion den Zugriff auf die OpenSearch Dienstdomäne ermöglicht oder, falls die Rolle bereits vorhanden ist, aktualisiert und wiederverwendet. Der Endpunkt dient dem Remote-Modell, das für den ML-Connector mit dem ML Commons-Plugin verwendet wird.

Verwenden Sie als Nächstes die Vorlage Integration with Sparse Encoders through Amazon Sagemaker, um eine Lambda-Funktion zu erstellen, mit der Ihre Domain Remote Inference Connectors einrichtet. Nachdem der Konnektor in OpenSearch Service erstellt wurde, kann die Remote-Inferenz mithilfe des Remote-Modells in Runtime eine semantische Suche ausführen. SageMaker Die Vorlage gibt Ihnen die Modell-ID in Ihrer Domain zurück, sodass Sie mit der Suche beginnen können.

Um die SageMaker CloudFormation Amazon-Vorlagen zu verwenden

1. Öffnen Sie die Amazon OpenSearch Service-Konsole unter https://console.aws.amazon.com/aos/home.
2. Wählen Sie in der linken Navigationsleiste Integrationen aus.

3. Wählen Sie unter jeder SageMaker Amazon-Vorlage die Optionen Domain konfigurieren, Public Domain konfigurieren aus.
4. Folgen Sie der Aufforderung in der CloudFormation Konsole, um Ihren Stack bereitzustellen und ein Modell einzurichten.

> **Note**
>
> OpenSearch Der Service bietet auch eine separate Vorlage für die Konfiguration der VPC-Domäne. Wenn Sie diese Vorlage verwenden, müssen Sie die VPC-ID für die Lambda-Funktion angeben.

Amazon Bedrock-Vorlagen

Ähnlich wie die SageMaker CloudFormation Amazon-Vorlagen stellt die Amazon CloudFormation Bedrock-Vorlage die AWS Ressourcen bereit, die zum Erstellen von Verbindungen zwischen OpenSearch Service und Amazon Bedrock erforderlich sind.

Zunächst erstellt die Vorlage eine IAM-Rolle, die es der future Lambda-Funktion ermöglicht, auf Ihre OpenSearch Service-Domain zuzugreifen. Die Vorlage erstellt dann die Lambda-Funktion, bei der die Domain mithilfe des ML Commons-Plugins einen Konnektor erstellt. Nachdem OpenSearch Service den Connector erstellt hat, ist die Einrichtung der Remote-Inferenz abgeschlossen und Sie können semantische Suchen mithilfe der Amazon Bedrock API-Operationen ausführen.

Beachten Sie, dass Sie kein Modell für SageMaker Runtime bereitstellen müssen, da Amazon Bedrock seine eigenen ML-Modelle hostet. Stattdessen verwendet die Vorlage einen vordefinierten Endpunkt für Amazon Bedrock und überspringt die Schritte zur Endpunktbereitstellung.

Um die Amazon CloudFormation Bedrock-Vorlage zu verwenden

1. Öffnen Sie die Amazon OpenSearch Service-Konsole unter https://console.aws.amazon.com/aos/home.
2. Wählen Sie in der linken Navigationsleiste Integrationen aus.
3. Wählen Sie unter Integrate with Amazon Titan Text Embeddings model through Amazon Bedrock die Optionen Domain konfigurieren, Public domain konfigurieren aus.
4. Folgen Sie der Aufforderung, um Ihr Modell einzurichten.

> **Note**
>
> OpenSearch Der Service bietet auch eine separate Vorlage für die Konfiguration der VPC-Domäne. Wenn Sie diese Vorlage verwenden, müssen Sie die VPC-ID für die Lambda-Funktion angeben.

Darüber hinaus bietet OpenSearch Service die folgenden Amazon Bedrock-Vorlagen für die Verbindung mit dem Cohere-Modell und dem multimodalen Einbettungsmodell von Amazon Titan:

- `Integration with Cohere Embed through Amazon Bedrock`
- `Integrate with Amazon Bedrock Titan Multi-modal`

ML Commons-Einstellungen werden nicht unterstützt

Amazon OpenSearch Service unterstützt die Verwendung der folgenden ML Commons-Einstellungen nicht:

- `plugins.ml_commons.allow_registering_model_via_url`
- `plugins.ml_commons.allow_registering_model_via_local_file`

Weitere Informationen zu den ML Commons-Einstellungen finden Sie unter ML Commons-Cluster-Einstellungen.

OpenSearch Vorlagen für das Service Flow-Framework

Mit den Amazon OpenSearch Service Flow Framework-Vorlagen können Sie komplexe Aufgaben zur Einrichtung und Vorverarbeitung von OpenSearch Services automatisieren, indem sie Vorlagen für gängige Anwendungsfälle bereitstellen. Sie können beispielsweise Flow-Framework-Vorlagen verwenden, um Einrichtungsaufgaben für maschinelles Lernen zu automatisieren. Die Amazon OpenSearch Service Flow Framework-Vorlagen bieten eine kompakte Beschreibung des Einrichtungsprozesses in einem JSON- oder YAML-Dokument. Diese Vorlagen beschreiben automatisierte Workflow-Konfigurationen für Konversationschats oder die Generierung von Abfragen, KI-Konnektoren, Tools, Agenten und andere Komponenten, die den OpenSearch Service für die Backend-Nutzung für generative Modelle vorbereiten.

Die Vorlagen für das Amazon OpenSearch Service Flow Framework können an Ihre spezifischen Bedürfnisse angepasst werden. Ein Beispiel für eine benutzerdefinierte Flow-Framework-Vorlage finden Sie unter Flow-Framework. Vom OpenSearch Service bereitgestellte Vorlagen finden Sie unter Workflow-Vorlagen. Eine umfassende Dokumentation, einschließlich detaillierter Schritte, einer API-Referenz und einer Referenz aller verfügbaren Einstellungen, finden Sie in der Open-Source-Dokumentation unter Automatisieren der Konfiguration. OpenSearch

ML-Konnektoren im OpenSearch Service erstellen

Mit Amazon OpenSearch Service Flow Framework-Vorlagen können Sie ML-Konnektoren konfigurieren und installieren, indem Sie die in ml-commons angebotene Create Connector-API verwenden. Sie können ML-Konnektoren verwenden, um OpenSearch Service mit anderen AWS Diensten oder Plattformen von Drittanbietern zu verbinden. Weitere Informationen dazu finden Sie unter Connectors für ML-Plattformen von Drittanbietern erstellen. Die Amazon OpenSearch Service Flow Framework-API ermöglicht Ihnen die Automatisierung von Aufgaben zur Einrichtung und Vorverarbeitung von OpenSearch Services und kann zur Erstellung von ML-Konnektoren verwendet werden.

Bevor Sie einen Connector in OpenSearch Service erstellen können, müssen Sie Folgendes tun:

- Erstellen Sie eine SageMaker Amazon-Domain.
- Erstellen Sie eine IAM-Rolle.
- Konfigurieren Sie die Pass-Rollen-Berechtigung.
- Ordnen Sie die Flow-Framework- und ML-Commons-Rollen in OpenSearch Dashboards zu.

Weitere Informationen zur Einrichtung von ML-Konnektoren für AWS Services finden Sie unter Amazon OpenSearch Service ML-Konnektoren für AWS Services. Weitere Informationen zur Verwendung von OpenSearch Service ML-Konnektoren mit Plattformen von Drittanbietern finden Sie unter Amazon OpenSearch Service ML-Konnektoren für Drittanbieterplattformen.

Einen Connector über einen Flow-Framework-Service erstellen

Um eine Flow-Framework-Vorlage mit Connector zu erstellen, müssen Sie eine `POST` Anfrage an Ihren OpenSearch Service-Domain-Endpunkt senden. Sie können cURL, einen Python-Beispielclient, Postman oder eine andere Methode verwenden, um eine signierte Anfrage zu senden. Die `POST` Anfrage hat das folgende Format:

```
POST /_plugins/_flow_framework/workflow
```

```
{
  "name": "Deploy Claude Model",
  "description": "Deploy a model using a connector to Claude",
  "use_case": "PROVISION",
  "version": {
    "template": "1.0.0",
    "compatibility": [
      "2.12.0",
      "3.0.0"
    ]
  },
  "workflows": {
    "provision": {
      "nodes": [
        {
          "id": "create_claude_connector",
          "type": "create_connector",
          "user_inputs": {
            "name": "Claude Instant Runtime Connector",
            "version": "1",
            "protocol": "aws_sigv4",
            "description": "The connector to BedRock service for Claude model",
            "actions": [
              {
                "headers": {
                  "x-amz-content-sha256": "required",
                  "content-type": "application/json"
                },
                "method": "POST",
                "request_body": "{ \"prompt\":\"${parameters.prompt}\",
 \"max_tokens_to_sample\":${parameters.max_tokens_to_sample},
 \"temperature\":${parameters.temperature},  \"anthropic_version\":
\"${parameters.anthropic_version}\" }",
                "action_type": "predict",
                "url": "https://bedrock-runtime.us-west-2.amazonaws.com/model/
anthropic.claude-instant-v1/invoke"
              }
            ],
            "credential": {
                "roleArn": "arn:aws:iam::account-id:role/opensearch-secretmanager-
role"
             },
            "parameters": {
              "endpoint": "bedrock-runtime.us-west-2.amazonaws.com",
```

```
              "content_type": "application/json",
              "auth": "Sig_V4",
              "max_tokens_to_sample": "8000",
              "service_name": "bedrock",
              "temperature": "0.0001",
              "response_filter": "$.completion",
              "region": "us-west-2",
              "anthropic_version": "bedrock-2023-05-31"
            }
          }
        }
      ]
    }
  }
}
```

Wenn sich Ihre Domain in einer Virtual Private Cloud (Amazon VPC) befindet, müssen Sie mit der Amazon VPC verbunden sein, damit die Anfrage den AI-Connector erfolgreich erstellen kann. Der Zugriff auf eine Amazon VPC hängt von der Netzwerkkonfiguration ab, beinhaltet jedoch in der Regel eine Verbindung zu einem VPN- oder Unternehmensnetzwerk. Um zu überprüfen, ob Sie Ihre OpenSearch Service-Domain erreichen können, navigieren Sie `https://your-vpc-domain.region.es.amazonaws.com` in einem Webbrowser zu und stellen Sie sicher, dass Sie die Standard-JSON-Antwort erhalten.

Beispiel für einen Python-Client

Der Python-Client ist einfacher zu automatisieren als eine HTTP Anfrage und hat eine bessere Wiederverwendbarkeit. Um den AI-Konnektor mit dem Python-Client zu erstellen, speichern Sie den folgenden Beispielcode in einer Python-Datei. Der Client benötigt das AWS SDK for Python (Boto3), die Pakete requests:Http for Humans und requests-aws4auth 1.2.3.

```
import boto3
import requests
from requests_aws4auth import AWS4Auth

host = 'domain-endpoint/'
region = 'region'
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)
```

```
path = '_plugins/_flow_framework/workflow'
url = host + path

payload = {
  "name": "Deploy Claude Model",
  "description": "Deploy a model using a connector to Claude",
  "use_case": "PROVISION",
  "version": {
    "template": "1.0.0",
    "compatibility": [
      "2.12.0",
      "3.0.0"
    ]
  },
  "workflows": {
    "provision": {
      "nodes": [
        {
          "id": "create_claude_connector",
          "type": "create_connector",
          "user_inputs": {
            "name": "Claude Instant Runtime Connector",
            "version": "1",
            "protocol": "aws_sigv4",
            "description": "The connector to BedRock service for Claude model",
            "actions": [
              {
                "headers": {
                  "x-amz-content-sha256": "required",
                  "content-type": "application/json"
                },
                "method": "POST",
                "request_body": "{ \"prompt\":\"${parameters.prompt}\",
 \"max_tokens_to_sample\":${parameters.max_tokens_to_sample},
 \"temperature\":${parameters.temperature},  \"anthropic_version\":
\"${parameters.anthropic_version}\" }",
                "action_type": "predict",
                "url": "https://bedrock-runtime.us-west-2.amazonaws.com/model/
anthropic.claude-instant-v1/invoke"
              }
            ],
            "credential": {
                "roleArn": "arn:aws:iam::account-id:role/opensearch-secretmanager-
role"
```

```
            },
            "parameters": {
              "endpoint": "bedrock-runtime.us-west-2.amazonaws.com",
              "content_type": "application/json",
              "auth": "Sig_V4",
              "max_tokens_to_sample": "8000",
              "service_name": "bedrock",
              "temperature": "0.0001",
              "response_filter": "$.completion",
              "region": "us-west-2",
              "anthropic_version": "bedrock-2023-05-31"
            }
          }
        }
      ]
    }
  }
}

headers = {"Content-Type": "application/json"}

r = requests.post(url, auth=awsauth, json=payload, headers=headers)
print(r.status_code)
print(r.text)
```

Vordefinierte Workflow-Vorlagen

Amazon OpenSearch Service bietet mehrere Workflow-Vorlagen für einige gängige Anwendungsfälle des maschinellen Lernens (ML). Die Verwendung einer Vorlage vereinfacht komplexe Setups und bietet viele Standardwerte für Anwendungsfälle wie semantische Suche oder Konversationssuche. Sie können eine Workflow-Vorlage angeben, wenn Sie die Create Workflow API aufrufen.

- Um eine vom OpenSearch Service bereitgestellte Workflow-Vorlage zu verwenden, geben Sie den Anwendungsfall der Vorlage als `use_case` Abfrageparameter an.
- Um eine benutzerdefinierte Workflow-Vorlage zu verwenden, geben Sie die vollständige Vorlage im Anfragetext an. Ein Beispiel für eine benutzerdefinierte Vorlage finden Sie in einer JSON-Beispielvorlage oder einer YAML-Beispielvorlage.

Anwendungsfälle für Vorlagen

Diese Tabelle bietet einen Überblick über die verschiedenen verfügbaren Vorlagen, eine Beschreibung der Vorlagen und die erforderlichen Parameter.

Anwendungsfall für Vorlagen	Beschreibung	Erforderliche Parameter
`bedrock_titan_embedding_model_deploy`	Erstellt ein Amazon Bedrock-Einbettungsmodell und stellt es bereit (standardmäßig `titan-embed-text-v1`	`create_connector.credential.roleArn`
`bedrock_titan_embedding_model_deploy`	Erstellt und implementiert ein multimodales Einbettungsmodell von Amazon Bedrock (standardmäßig `titan-embed-text-v1`	`create_connector.credential.roleArn`
`cohere_embedding_model_deploy`	Erstellt ein Cohere-Einbettungsmodell und stellt es bereit (standardmäßig 3.0). embed-english-v	`create_connector.credential.roleArn` , `create_connector.credential.secretArn`
`cohere_chat_model_deploy`	Erstellt ein Cohere-Chat-Modell und stellt es bereit (standardmäßig Cohere Command).	`create_connector.credential.roleArn` , `create_connector.credential.secretArn`
`open_ai_embedding_model_deploy`	Erzeugt und implementiert ein OpenAI-Einbettungsmodell (standardmäßig -002). text-embedding-ada	`create_connector.credential.roleArn` , `create_connector.credential.secretArn`
`openai_chat_model_deploy`	Erzeugt und implementiert ein OpenAI-Chat-Modell (standardmäßig gpt-3.5-Turbo).	`create_connector.credential.roleArn` , `create_connector.credential.secretArn`

Anwendungsfall für Vorlagen	Beschreibung	Erforderliche Parameter
`semantic_search_with_cohere_embedding`	Konfiguriert die semantische Suche und stellt ein Cohere-Einbettungsmodell bereit. Sie müssen den API-Schlüssel für das Cohere-Modell angeben.	`create_connector.credential.roleArn`, `create_connector.credential.secretArn`
`semantic_search_with_cohere_embedding_query_enricher`	Konfiguriert die semantische Suche und stellt ein Cohere-Einbettungsmodell bereit. Fügt einen query_enricher-Suchprozessor hinzu, der eine Standardmodell-ID für neuronale Abfragen festlegt. Sie müssen den API-Schlüssel für das Cohere-Modell angeben.	`create_connector.credential.roleArn`, `create_connector.credential.secretArn`
`multimodal_search_with_bedrock_titan`	Stellt ein multimodales Amazon Bedrock-Modell bereit und konfiguriert eine Aufnahme-Pipeline mit einem text_image_embedding-Prozessor und einem k-NN-Index für die multimodale Suche. Sie müssen Ihre Anmeldeinformationen angeben. AWS	`create_connector.credential.roleArn`

> **Note**
>
> Für alle Vorlagen, die einen geheimen ARN benötigen, wird das Geheimnis standardmäßig mit dem Schlüsselnamen „key“ im AWS Secrets Manager gespeichert.

Standardvorlagen mit vortrainierten Modellen

Amazon OpenSearch Service bietet zwei zusätzliche Standard-Workflow-Vorlagen, die im OpenSearch Open-Source-Service nicht verfügbar sind.

Anwendungsfall für Vorlagen	Beschreibung
`semantic_search_with_local_model`	Konfiguriert die semantische Suche und stellt ein vortrainiertes Modell bereit (). `msmarco-distilbert-base-tas-b` Fügt einen `neural_query_enricher` Suchprozessor hinzu, der eine Standardmodell-ID für neuronale Abfragen festlegt und einen verknüpften k-NN-Index namens " erstellt. my-nlp-index
`hybrid_search_with_local_model`	Konfiguriert die Hybridsuche und stellt ein vortrainiertes Modell bereit (). `msmarco-distilbert-base-tas-b` Fügt einen `neural_query_enricher` Suchprozessor hinzu, der eine Standardmodell-ID für neuronale Abfragen festlegt und einen verknüpften k-NN-Index namens " erstellt. my-nlp-index

Konfigurieren von Berechtigungen

Wenn Sie eine neue Domäne mit Version 2.13 oder höher erstellen, sind die Berechtigungen bereits vorhanden. Wenn Sie Flow Framework auf einer bereits vorhandenen OpenSearch Service-Domain mit Version 2.11 oder früher aktivieren, die Sie dann auf Version 2.13 oder höher aktualisieren, müssen Sie die Rolle definieren. `flow_framework_manager` Benutzer ohne Administratorrechte müssen dieser Rolle zugeordnet werden, um Warm-Indizes in Domains mithilfe einer fein abgestuften Zugriffskontrolle zu verwalten. Führen Sie die folgenden Schritte aus, um die `flow_framework_manager`-Rolle manuell zu erstellen:

1. Gehen Sie in OpenSearch Dashboards zu Sicherheit und wählen Sie Berechtigungen aus.
2. Wählen Sie Aktionsgruppe erstellen und konfigurieren Sie die folgenden Gruppen:

Group name (Gruppenname)	Berechtigungen
`flow_framework_full_access`	• `cluster:admin/opensearch/flow_framework/*` • `cluster_monitor`
`flow_framework_read_accesss`	• `cluster:admin/opensearch/flow_framework/workflow/get` • `cluster:admin/opensearch/flow_framework/workflow/search` • `cluster:admin/opensearch/flow_framework/workflow_state/get` • `cluster:admin/opensearch/flow_framework/workflow_state/search`

3. Wählen Sie Rollen und Rolle erstellen.
4. Nennen Sie die Rolle flow_framework_manager.
5. Wählen Sie für Clusterberechtigungen `flow_framework_full_access` und `flow_framework_read_access` aus.
6. Geben Sie für Index * ein.
7. Wählen Sie für Indexberechtigungen `indices:admin/aliases/get`, `indices:admin/mappings/get` und `indices_monitor` aus.
8. Wählen Sie Erstellen.
9. Nachdem Sie die Rolle erstellt haben, ordnen Sie sie einer beliebigen Benutzer- oder Backend-Rolle zu, die die Flow-Framework-Indizes verwaltet.

Sicherheitsanalysen für Amazon OpenSearch Service

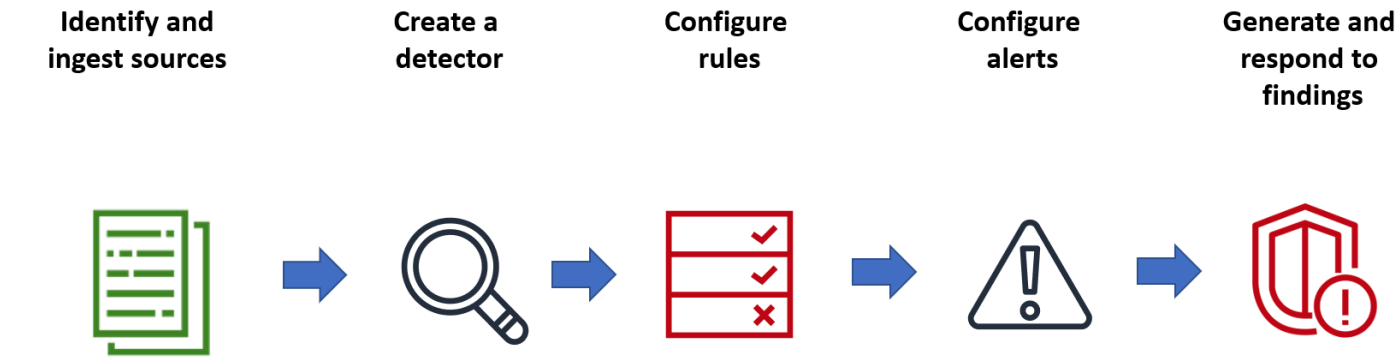
Security Analytics ist eine OpenSearch Lösung, die Einblick in die Infrastruktur Ihres Unternehmens bietet, ungewöhnliche Aktivitäten überwacht, potenzielle Sicherheitsbedrohungen in Echtzeit erkennt und Warnmeldungen an vorkonfigurierte Ziele auslöst. Sie können anhand Ihrer Sicherheitsereignisprotokolle nach böswilligen Aktivitäten Ausschau halten, indem Sie die Sicherheitsregeln kontinuierlich auswerten und die automatisch generierten Sicherheitsergebnisse überprüfen. Darüber hinaus kann Security Analytics automatische Warnmeldungen generieren und diese an einen bestimmten Benachrichtigungskanal wie Slack oder E-Mail senden.

Sie können das Security Analytics-Plugin verwenden, um häufig auftretende Bedrohungen zu erkennen out-of-the-box und wichtige Sicherheitsinformationen aus Ihren vorhandenen Sicherheitsereignisprotokollen wie Firewallprotokollen, Windows-Protokollen und Authentifizierungsprotokollen zu gewinnen. Um Security Analytics verwenden zu können, muss auf Ihrer Domain OpenSearch Version 2.5 oder höher ausgeführt werden.

> **Note**
>
> Diese Dokumentation bietet einen kurzen Überblick über Security Analytics for Amazon OpenSearch Service. Es definiert die wichtigsten Konzepte und enthält Schritte zur Konfiguration von Berechtigungen. Eine umfassende Dokumentation, einschließlich eines Einrichtungsleitfadens, einer API-Referenz und einer Referenz aller verfügbaren Einstellungen, finden Sie in der OpenSearch Dokumentation unter Security Analytics.

Komponenten und Konzepte der Sicherheitsanalyse

Eine Reihe von Tools und Funktionen bilden die Grundlage für den Betrieb von Security Analytics. Zu den Hauptkomponenten, aus denen das Plugin besteht, gehören Detektoren, Protokolltypen, Regeln, Ergebnisse und Warnungen.



Typen von Protokollen

OpenSearch unterstützt mehrere Arten von Protokollen und bietet out-of-the-box Zuordnungen für jeden Typ. Sie geben den Protokolltyp an und konfigurieren ein Zeitintervall, wenn Sie einen Detektor erstellen. Von dort aus aktiviert Security Analytics automatisch einen entsprechenden Regelsatz, der in diesem Intervall ausgeführt wird.

Detektoren

Detektoren identifizieren eine Reihe von Cybersicherheitsbedrohungen für einen Protokolltyp in Ihren Datenindizes. Sie konfigurieren Ihren Detektor so, dass er sowohl benutzerdefinierte Regeln als auch vorgefertigte Sigma-Regeln verwendet, die Ereignisse im System auswerten. Der Detektor generiert dann Sicherheitsergebnisse aus diesen Ereignissen. Weitere Informationen zu Meldern finden Sie in der OpenSearch Dokumentation unter Melder erstellen.

Regeln

Regeln zur Bedrohungserkennung definieren die Bedingungen, die Melder auf aufgenommene Protokolldaten anwenden, um ein Sicherheitsereignis zu identifizieren. Security Analytics unterstützt das Importieren, Erstellen und Anpassen von Regeln, um Ihre Anforderungen zu erfüllen, und bietet außerdem vorkonfigurierte Open-Source-Sigma-Regeln, mit denen Sie häufig auftretende Bedrohungen anhand Ihrer Protokolle erkennen können. Security Analytics ordnet viele Regeln einer ständig wachsenden Wissensbasis über gegnerische Taktiken und Techniken zu, die von der MITRE ATT&CK-Organisation verwaltet werden. Sie können sowohl OpenSearch Dashboards als auch APIs verwenden, um Regeln zu erstellen und zu verwenden. Weitere Informationen zu Regeln finden Sie in der OpenSearch Dokumentation unter Arbeiten mit Regeln.

Funde

Wenn ein Detektor eine Regel mit einem Protokollereignis abgleicht, generiert er einen Befund. Jedes Ergebnis umfasst eine eindeutige Kombination aus ausgewählten Regeln, einem Protokolltyp und einem Regelschweregrad. Die Ergebnisse deuten nicht unbedingt auf unmittelbare Bedrohungen innerhalb des Systems hin, aber sie isolieren immer ein interessierendes Ereignis. Weitere Informationen zu den Ergebnissen finden Sie in der OpenSearch Dokumentation unter Arbeiten mit Ergebnissen.

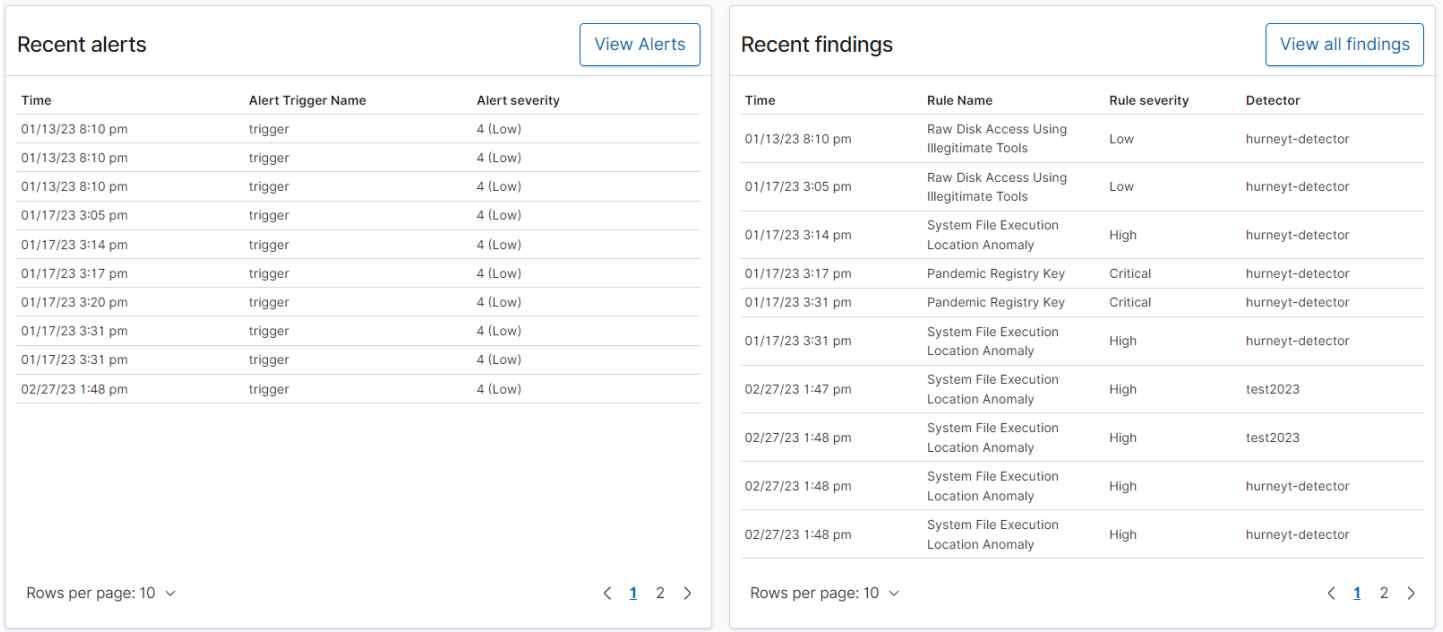
Benachrichtigungen

Wenn Sie einen Detektor erstellen, können Sie eine oder mehrere Bedingungen angeben, die eine Warnung auslösen. Eine Warnung ist eine Benachrichtigung, die an einen bevorzugten Kanal wie Slack oder E-Mail gesendet wird. Sie legen fest, dass die Warnung ausgelöst wird, wenn der Detektor einer oder mehreren Regeln entspricht, und können die Benachrichtigungsnachricht anpassen. Weitere Informationen zu Warnmeldungen finden Sie in der OpenSearch Dokumentation unter Arbeiten mit Warnmeldungen.

Erfahren Sie mehr über Sicherheitsanalysen

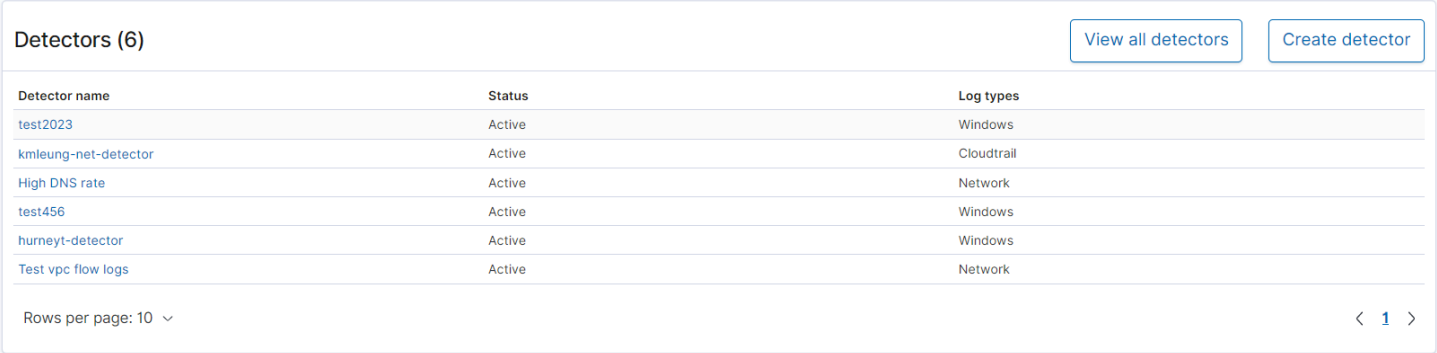
Sie können OpenSearch Dashboards verwenden, um Ihr Security Analytics-Plugin zu visualisieren und Einblicke in dieses zu erhalten. Die Übersichtsansicht enthält Informationen wie Ergebnisse und Anzahl der Alarme, aktuelle Ergebnisse und Warnungen, Regeln für häufige Erkennungen und eine Liste Ihrer Melder. Sie können eine Übersichtsansicht sehen, die aus mehreren Visualisierungen besteht. Das folgende Diagramm zeigt beispielsweise den Trend der Ergebnisse und Warnmeldungen für verschiedene Protokolltypen über einen bestimmten Zeitraum.

Weiter unten auf der Seite können Sie Ihre neuesten Ergebnisse und Warnungen überprüfen.



Darüber hinaus können Sie eine Verteilung der am häufigsten ausgelösten Regeln auf alle aktiven Melder sehen. Dies kann Ihnen helfen, verschiedene Arten bösartiger Aktivitäten in verschiedenen Protokolltypen zu erkennen und zu untersuchen.

Schließlich können Sie den Status der konfigurierten Melder einsehen. Von diesem Bereich aus können Sie auch zum Workflow zum Erstellen von Meldern navigieren.



Um Ihr Security Analytics-Setup zu konfigurieren, erstellen Sie Regeln auf der Seite „Regeln“ und verwenden Sie diese Regeln, um Melder auf der Seite „Detektoren“ zu schreiben. Für eine genauere Ansicht Ihrer Security Analytics-Ergebnisse können Sie die Seiten Ergebnisse und Warnungen verwenden.

Konfigurieren von Berechtigungen

Wenn Sie Security Analytics für eine bereits bestehende OpenSearch Dienstdomäne aktivieren, ist die `security_analytics_manager` Rolle möglicherweise nicht für die Domäne definiert. Benutzer ohne Administratorrechte müssen dieser Rolle zugeordnet werden, um Warm-Indizes in Domains mithilfe einer fein abgestuften Zugriffskontrolle zu verwalten. Führen Sie die folgenden Schritte aus, um die `security_analytics_manager`-Rolle manuell zu erstellen:

1. Gehen Sie in OpenSearch Dashboards zu Sicherheit und wählen Sie Berechtigungen aus.
2. Wählen Sie Aktionsgruppe erstellen und konfigurieren Sie die folgenden Gruppen:

Group name (Gruppenname)	Berechtigungen
security_analytics_full_access	• cluster:admin/opensearch/securityanalytics/alerts/* • cluster:admin/opensearch/securityanalytics/detector/* • cluster:admin/opensearch/securityanalytics/findings/* • cluster:admin/opensearch/securityanalytics/mapping/* • cluster:admin/opensearch/securityanalytics/rule/*
security_analytics_read_access	• cluster:admin/opensearch/securityanalytics/alerts/get • cluster:admin/opensearch/securityanalytics/detector/get • cluster:admin/opensearch/securityanalytics/detector/search • cluster:admin/opensearch/securityanalytics/findings/get • cluster:admin/opensearch/securityanalytics/mapping/get • cluster:admin/opensearch/securityanalytics/mapping/view/get • cluster:admin/opensearch/securityanalytics/rule/get • cluster:admin/opensearch/securityanalytics/rule/search

3. Wählen Sie Rollen und Rolle erstellen.
4. Nennen Sie die Rolle security_analytics_manager.

5. Wählen Sie für Clusterberechtigungen `security_analytics_full_access` und `security_analytics_read_access` aus.
6. Geben Sie für Index * ein.
7. Wählen Sie für Indexberechtigungen die Option und aus. `indices:admin/mapping/put` `indices:admin/mappings/get`
8. Wählen Sie Erstellen.
9. Nachdem Sie die Rolle erstellt haben, ordnen Sie sie einer beliebigen Benutzer- oder Back-End-Rolle zu, die Security Analytics-Indizes verwaltet.

Fehlerbehebung

Kein solcher Indexfehler

Wenn Sie keine Melder haben und das Security Analytics-Dashboard öffnen, sehen Sie möglicherweise unten rechts eine Benachrichtigung mit der Aufschrift`[index_not_found_exception] no such index [.opensearch-sap-detectors-config]`. Sie können diese Benachrichtigung ignorieren. Sie verschwindet innerhalb weniger Sekunden und erscheint nicht mehr, sobald Sie einen Detektor erstellt haben.

Beobachtbarkeit in Amazon Service OpenSearch

Die Standardinstallation von OpenSearch Dashboards for Amazon OpenSearch Service umfasst das Observability-Plugin, mit dem Sie datengesteuerte Ereignisse mithilfe der Piped Processing Language (PPL) visualisieren können, um darin gespeicherte Daten zu untersuchen, zu entdecken und abzufragen. OpenSearch Das Plugin benötigt 1.2 oder höher. OpenSearch

Das Beobachtbarkeits-Plug-In bietet ein einheitliche Erlebnis zum Erfassen und Überwachen von Metriken, Protokollen und Traces aus gängigen Datenquellen. Die Datenerfassung und -überwachung an einem Ort ermöglicht die vollständige end-to-end Überwachung Ihrer gesamten Infrastruktur.

> **Note**
>
> Diese Dokumentation bietet einen kurzen Überblick über Observability in Service. OpenSearch Eine umfassende Dokumentation des Observability-Plug-ins, einschließlich der Berechtigungen, finden Sie unter Observability.

Jeder Prozess zur Untersuchung von Daten ist anders. Wenn Sie mit der Erkundung von Daten und der Erstellung von Visualisierungen noch nicht vertraut sind, empfehlen wir Ihnen, einen Workflow wie den folgenden auszuprobieren.

Erkunden Ihrer Daten mit Ereignisanalytik

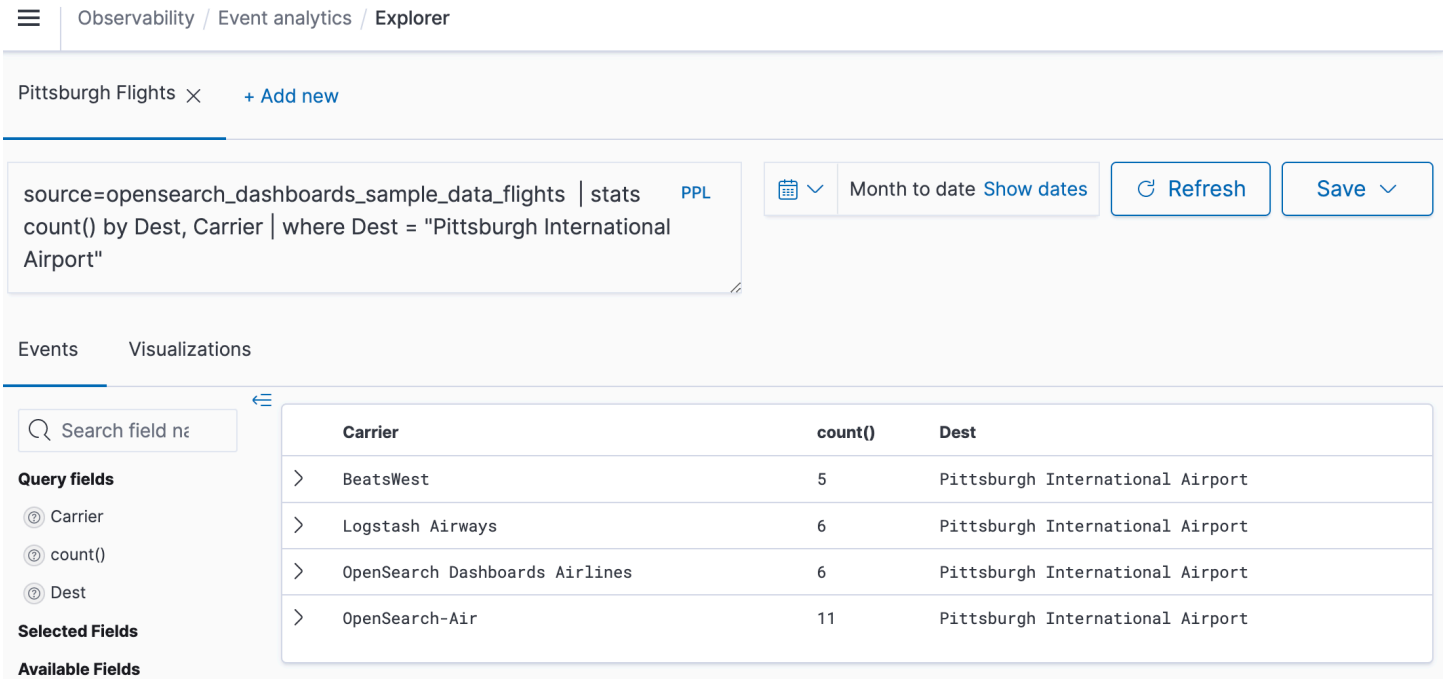
Nehmen wir zunächst an, Sie sammeln Flugdaten in Ihrer OpenSearch Service-Domain und möchten herausfinden, bei welcher Fluggesellschaft im letzten Monat die meisten Flüge am Pittsburgh International Airport angekommen sind. Sie schreiben die folgende PPL-Abfrage:

```
source=opensearch_dashboards_sample_data_flights |
    stats count() by Dest, Carrier |
    where Dest = "Pittsburgh International Airport"
```

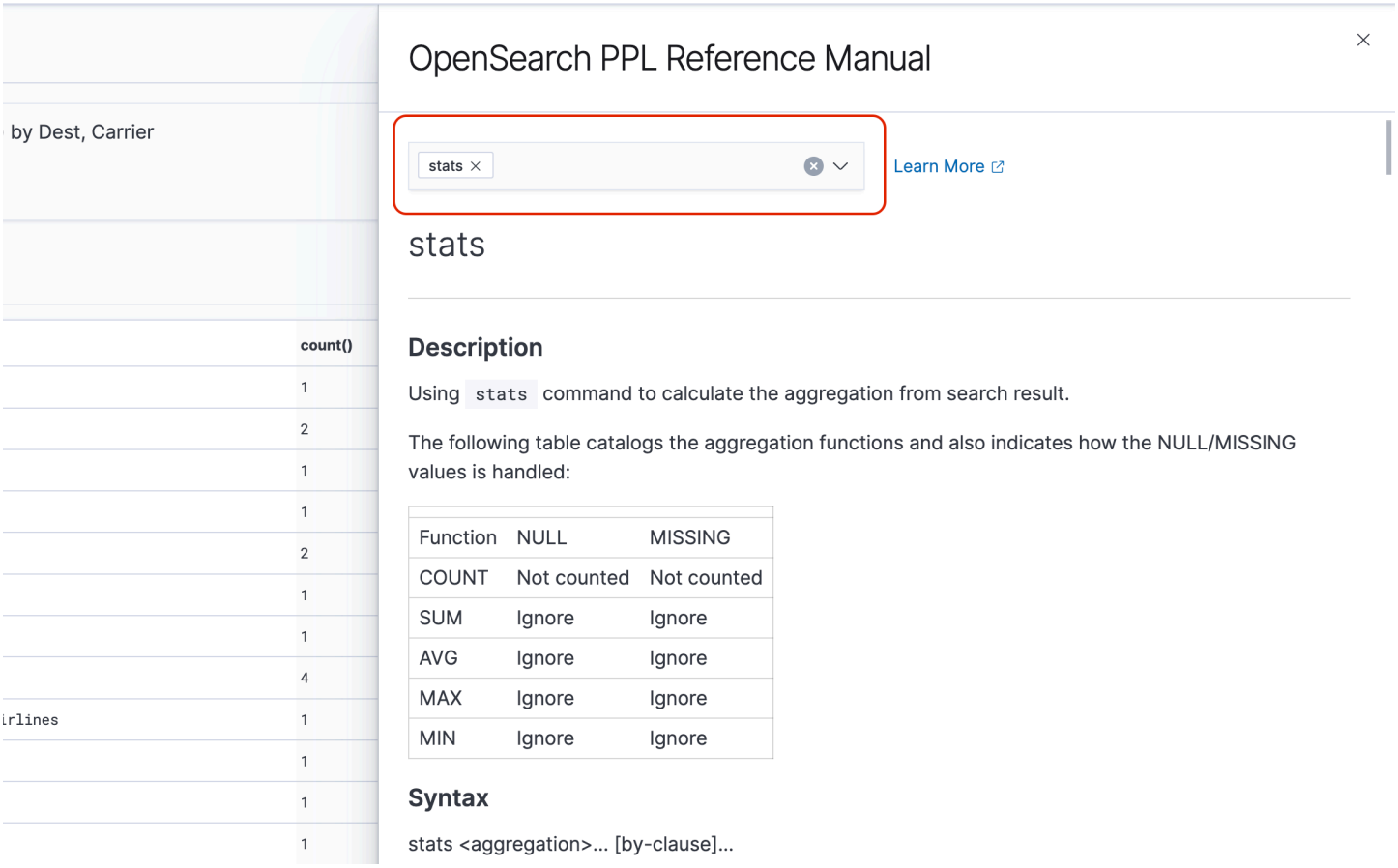
Diese Abfrage ruft Daten aus dem Index namens `opensearch_dashboards_sample_data_flights` ab. Sie nutzt dann den Befehl `stats`, um eine Gesamtzahl der Flüge zu erhalten und sie nach Zielflughafen und Fluggesellschaft zu

gruppieren. Schließlich benutzt sie die `where`-Klausel, um die Ergebnisse für Flüge zu filtern, die am Pittsburgh International Airport ankommen.

So sehen die Daten aus, wenn sie für den vergangenen Monat angezeigt werden:



Sie können die Schaltfläche PPL im Abfrage-Editor auswählen, um Nutzungsinformationen und Beispiele für jeden PPL-Befehl abzurufen:



Sehen wir uns ein komplexeres Beispiel an, das Informationen über Flugverspätungen abfragt:

```
source=opensearch_dashboards_sample_data_flights |
    where FlightDelayMin > 0 |
    stats sum(FlightDelayMin) as minimum_delay, count() as total_delayed by Carrier,
 Dest |
    eval avg_delay=minimum_delay / total_delayed |
    sort - avg_delay
```

Jeder Befehl in der Abfrage wirkt sich auf die endgültige Ausgabe aus:

- `source=opensearch_dashboards_sample_data_flights` ruft Daten aus demselben Index wie im vorherigen Beispiel ab.
- `where FlightDelayMin > 0` filtert die Daten nach Flügen, die verspätet waren.
- `stats sum(FlightDelayMin) as minimum_delay, count() as total_delayed by Carrier` ruft für jede Fluggesellschaft die gesamte minimale Verspätungszeit und die Gesamtzahl der verspäteten Flüge ab.

- `eval avg_delay=minimum_delay / total_delayed` berechnet die durchschnittliche Verspätungszeit für jede Fluggesellschaft durch Dividieren der minimalen Verspätungszeit durch die Gesamtzahl der verspäteten Flüge.
- `sort - avg_delay` sortiert die Ergebnisse nach durchschnittlicher Verzögerung in absteigender Reihenfolge.

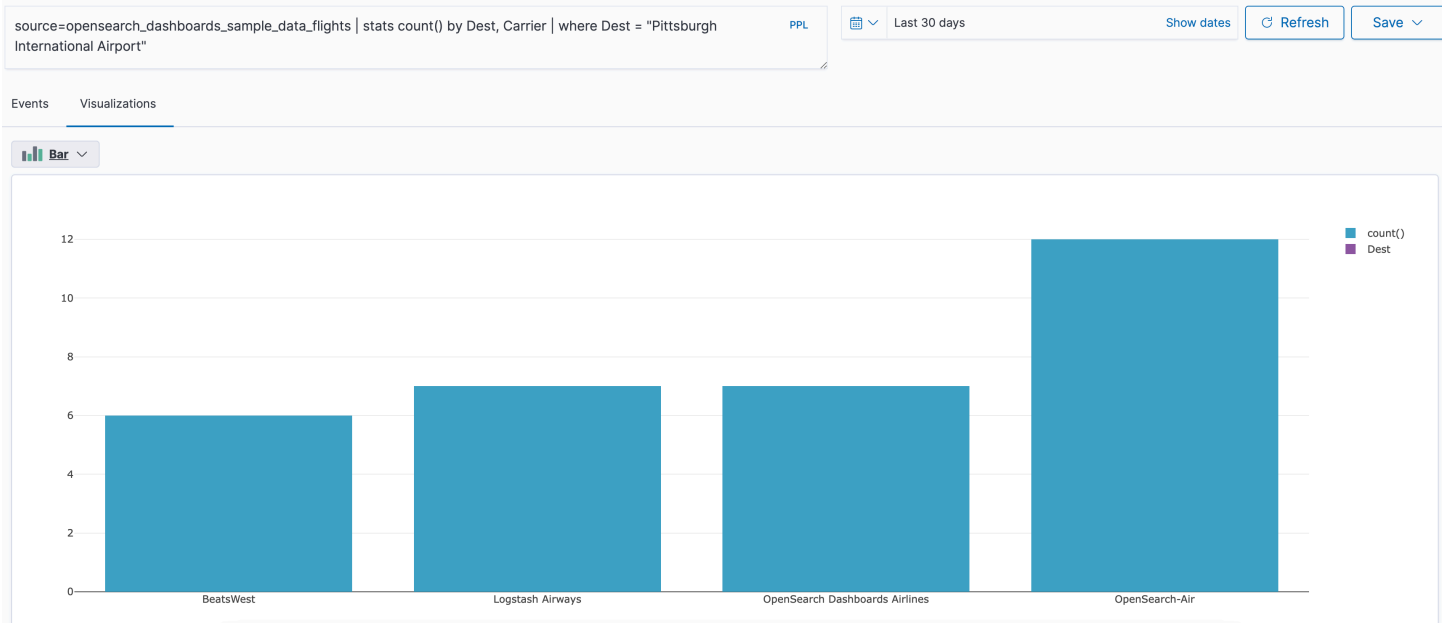
Mit dieser Abfrage können Sie feststellen, dass OpenSearch Dashboards Airlines im Durchschnitt weniger Verspätungen aufweist.

	avg_delay	Carrier	minimum_delay	total_delayed
>	212	Logstash Airways	4470	21
>	184	OpenSearch-Air	4245	23
>	155	BeatsWest	2025	13
>	153	OpenSearch Dashboards Airlines	4305	28

Weitere Beispiele für PPL-Abfragen finden Sie unter Abfragen und Visualisierungen auf der SeiteEreignisanalytik.

Erstellen von Visualisierungen

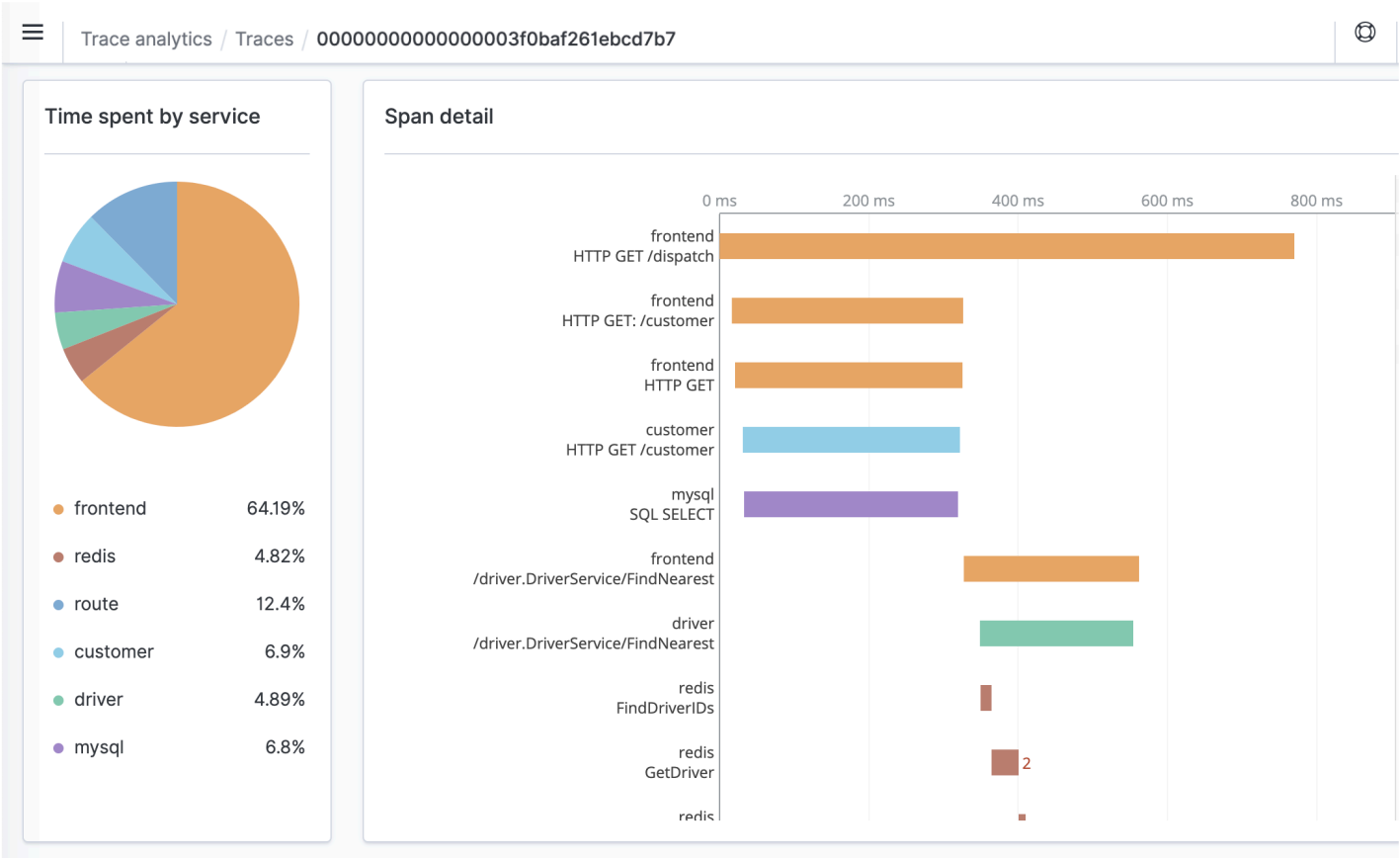
Sobald Sie die Daten, an denen Sie interessiert sind, korrekt abgefragt haben, können Sie diese Abfragen als Visualisierungen speichern:



Fügen Sie diese Visualisierungen dann Operative Bereiche hinzu, um verschiedene Daten zu vergleichen. Nutzen Sie Notebooks, um verschiedene Visualisierungen und Codeblöcke zu kombinieren, die Sie mit Teammitgliedern teilen können.

Detaillierter Einblick in Trace Analytics

Trace Analytics bietet eine Möglichkeit, den Fluss von Ereignissen in Ihren OpenSearch Daten zu visualisieren, um Leistungsprobleme in verteilten Anwendungen zu identifizieren und zu beheben.



Trace Analytics für Amazon OpenSearch Service

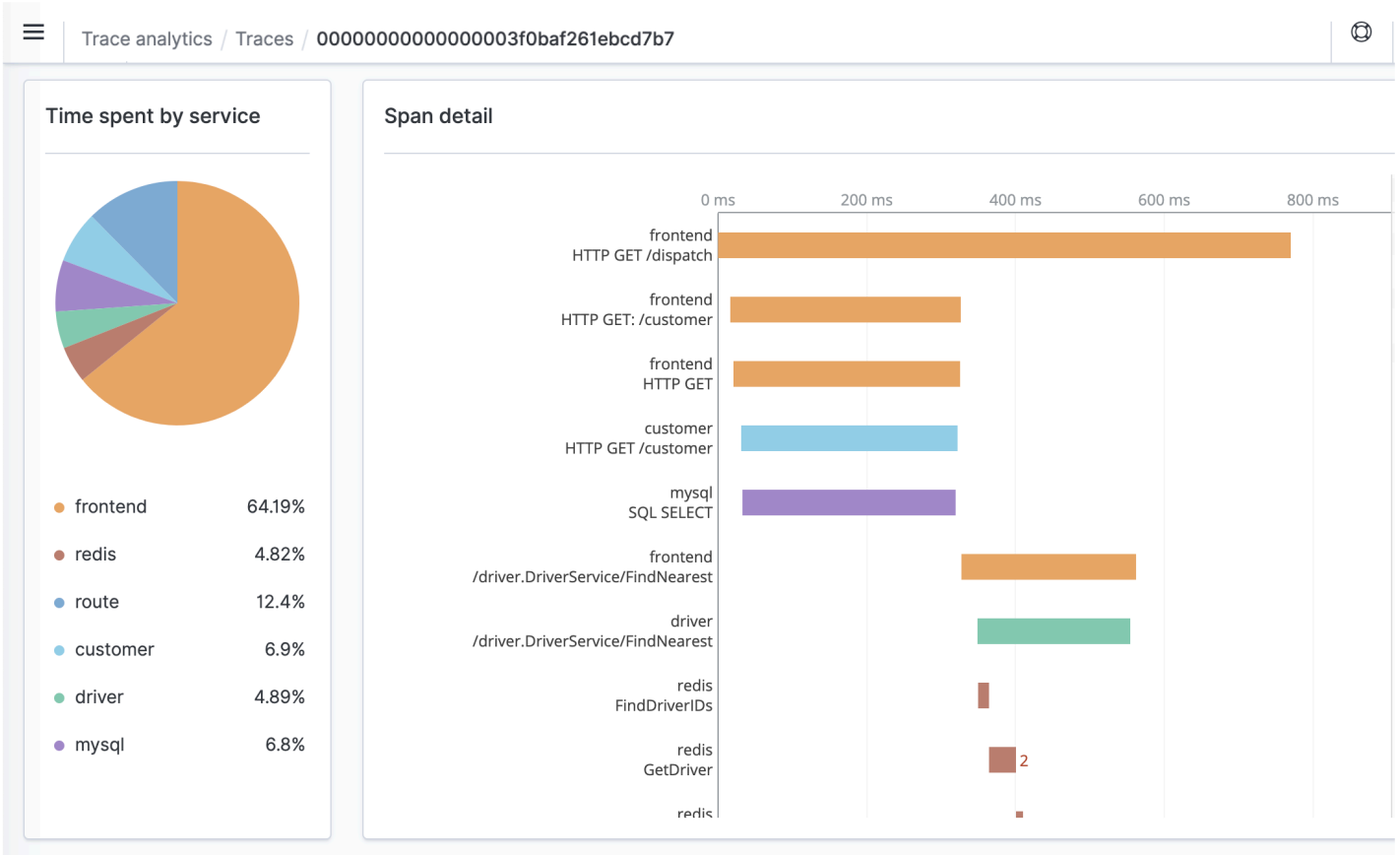
Sie können Trace Analytics verwenden, das Teil des OpenSearch Observability-Plug-ins ist, um Trace-Daten aus verteilten Anwendungen zu analysieren. Trace Analytics erfordert OpenSearch Elasticsearch 7.9 oder höher.

In einer verteilten Anwendung kann ein einzelner Vorgang, z. B. das Klicken eines Benutzers auf eine Schaltfläche, eine erweiterte Reihe von Ereignissen auslösen. Das Anwendungs-Front-End kann beispielsweise einen Backend-Dienst aufrufen, der einen anderen Dienst aufruft, der eine Datenbank

abfragt, die Abfrage verarbeitet und ein Ergebnis zurückgibt. Dann sendet der erste Backend-Dienst eine Bestätigung an das Front-End, das die Benutzeroberfläche aktualisiert.

Sie können Spurenanalytik verwenden, um diesen Ereignisfluss zu visualisieren und Leistungsprobleme zu identifizieren.

> **Note**
>
> Diese Dokumentation bietet einen kurzen Überblick über Trace Analytics. Eine umfassende Dokumentation finden Sie unter Trace Analytics in der OpenSearch Open-Source-Dokumentation.



Voraussetzungen

Für Trace Analytics müssen Sie Ihrer Anwendung Instrumente hinzufügen und Trace-Daten mithilfe einer OpenTelemetry unterstützten Bibliothek wie Jaeger oder Zipkin generieren. Dieser Schritt erfolgt vollständig außerhalb von Service. OpenSearch Die OpenTelemetry Dokumentation zur AWS

Distribution enthält Beispielanwendungen für viele Programmiersprachen, die Ihnen den Einstieg erleichtern können, darunter Java, Python, Go und JavaScript.

Nachdem Sie Ihrer Anwendung Instrumentierung hinzugefügt haben, empfängt der OpenTelemetryCollector Daten von der Anwendung und formatiert sie in OpenTelemetry Daten. Die Liste der Empfänger finden Sie unter GitHub. AWS Distro for OpenTelemetry enthält einen Empfänger für. AWS X-Ray

Schließlich können Sie diese OpenTelemetry Daten für OpenSearch Einnahme durch Amazon die Verwendung mit OpenSearch formatieren.

OpenTelemetry Collector-Beispielkonfiguration

Um den OpenTelemetry Collector mit zu verwenden OpenSearch Einnahme durch Amazon, probieren Sie die folgende Beispielkonfiguration aus:

```
extensions:
  sigv4auth:
    region: "us-east-1"
    service: "osis"

receivers:
  jaeger:
    protocols:
      grpc:

exporters:
  otlphttp:
    traces_endpoint: "https://pipeline-endpoint.us-east-1.osis.amazonaws.com/
opentelemetry.proto.collector.trace.v1.TraceService/Export"
    auth:
      authenticator: sigv4auth
    compression: none

service:
  extensions: [sigv4auth]
  pipelines:
    traces:
      receivers: [jaeger]
      exporters: [otlphttp]
```

OpenSearch Beispielkonfiguration für die Aufnahme

Um Trace-Daten an eine OpenSearch Service-Domain zu senden, probieren Sie die folgende Beispielkonfiguration für die OpenSearch Ingestion-Pipeline aus. Anweisungen zum Erstellen einer Pipeline finden Sie unter. the section called “Pipelines erstellen”

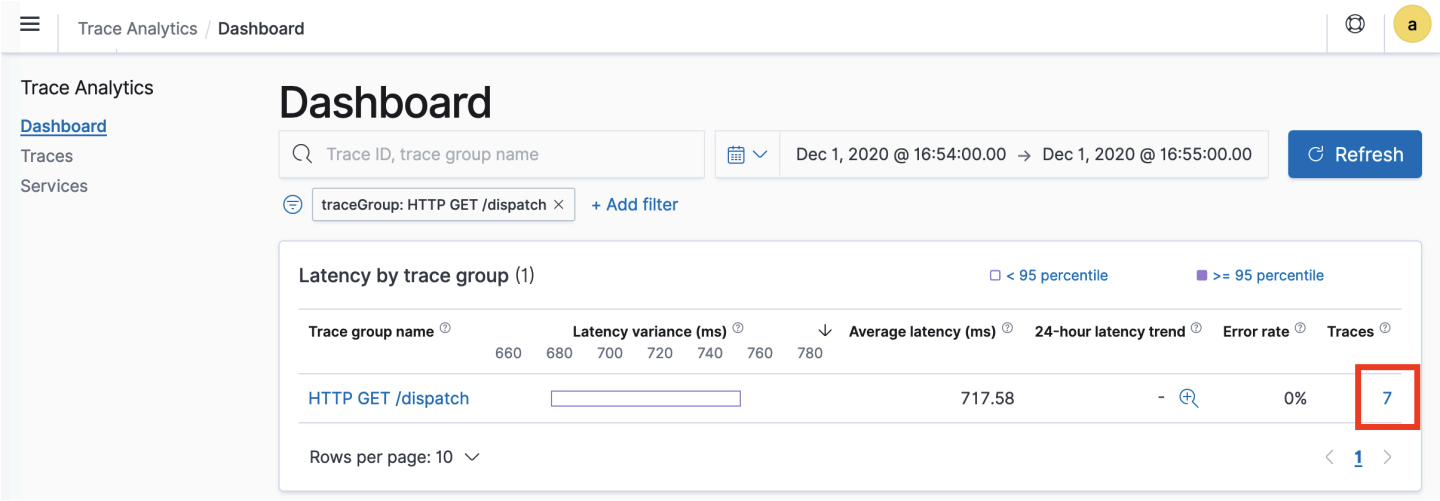
```
version: "2"
otel-trace-pipeline:
  source:
    otel_trace_source:
      "/${pipelineName}/ingest"
  processor:
    - trace_peer_forwarder:
  sink:
    - pipeline:
        name: "trace_pipeline"
    - pipeline:
        name: "service_map_pipeline"
trace-pipeline:
  source:
    pipeline:
      name: "otel-trace-pipeline"
  processor:
    - otel_traces:
  sink:
    - opensearch:
        hosts: ["https://domain-endpoint"]
        index_type: trace-analytics-raw
        aws:
          # IAM role that OpenSearch Ingestion assumes to access the domain sink
          sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
          region: "us-east-1"

service-map-pipeline:
  source:
    pipeline:
      name: "otel-trace-pipeline"
  processor:
    - service_map:
  sink:
    - opensearch:
        hosts: ["https://domain-endpoint"]
        index_type: trace-analytics-service-map
```

```
    aws:
      # IAM role that the pipeline assumes to access the domain sink
      sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
      region: "us-east-1"
```

Die Pipeline-Rolle, die Sie in der `sts_role_arn` Option angeben, muss über Schreibberechtigungen für die Senke verfügen. Anweisungen zum Konfigurieren von Berechtigungen für die Pipeline-Rolle finden Sie unterthe section called “Rollen und Benutzer einrichten”.

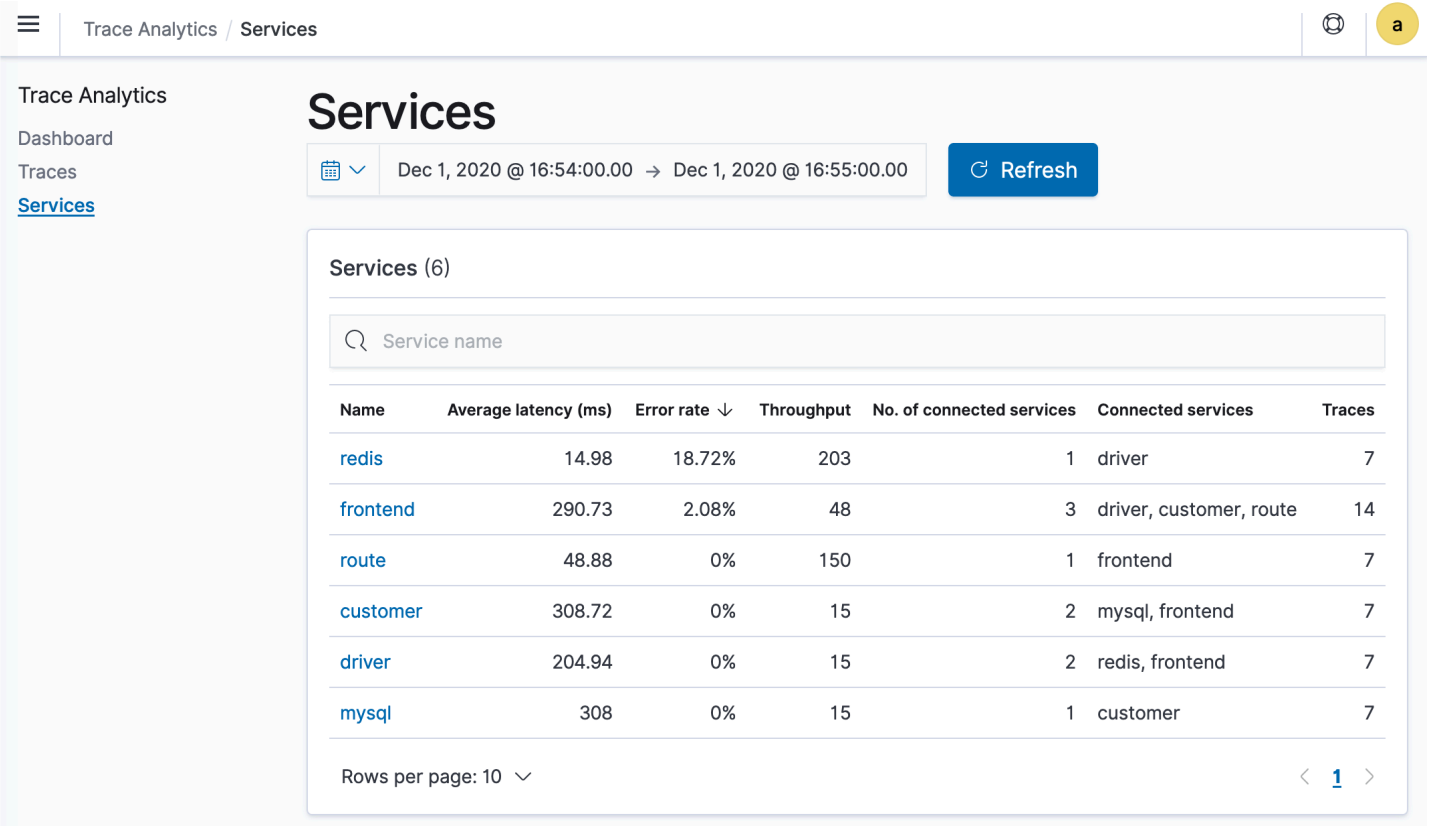
Spurendaten untersuchen

Die Dashboard-Ansicht gruppiert Spuren nach HTTP-Methode und -Pfad, sodass Sie die durchschnittliche Latenz, Fehlerrate und Trends im Zusammenhang mit einem bestimmten Vorgang sehen können. Versuchen Sie für eine fokussiertere Ansicht, nach Spurengruppennamen zu filtern.



Um einen Drilldown zu den Spuren durchzuführen, die eine Spuren-Gruppe bilden, wählen Sie die Anzahl der Spuren in der rechten Spalte. Wählen Sie dann eine einzelne Spur für eine detaillierte Zusammenfassung aus.

Die Ansicht Services listet alle Dienste in der Anwendung sowie eine interaktive Karte auf, die zeigt, wie die verschiedenen Dienste miteinander verbunden sind. Im Gegensatz zum Dashboard (das hilft, Probleme nach Betrieb zu identifizieren), hilft Ihnen die Service Map, Probleme nach Service zu identifizieren. Versuchen Sie, nach Fehlerrate oder Latenz zu sortieren, um ein Gefühl für potenzielle Problembereiche Ihrer Anwendung zu erhalten.



Abfragen von Amazon OpenSearch Service-Daten mit Piped Processing Language

Piped Processing Language (PPL) ist eine Abfragesprache, mit der Sie die pipe (|) -Syntax verwenden können, um in Amazon OpenSearch Service gespeicherte Daten abzufragen. PPL benötigt entweder Elasticsearch OpenSearch 7.9 oder höher.

> **Note**
>
> Diese Dokumentation bietet einen kurzen Überblick über PPL für Amazon OpenSearch Service. Ausführliche Schritte und eine vollständige Befehlsreferenz finden Sie unter PPL in der OpenSearch Open-Source-Dokumentation.

Die PPL-Syntax besteht aus Befehlen, die durch ein Pipe-Zeichen (|) begrenzt sind, wobei Daten von links nach rechts durch jede Pipeline fließen. Die PPL-Syntax, um die Anzahl der Hosts mit HTTP 403- oder 503-Fehlern zu ermitteln, sie pro Host zu aggregieren und sie in der Reihenfolge der Auswirkungen zu sortieren, lautet beispielsweise wie folgt:

```
source = dashboards_sample_data_logs | where response='403' or response='503' | stats
 count(request) as request_count by host, response | sort -request_count
```

Wählen Sie zunächst in OpenSearch Dashboards Query Workbench und anschließend PPL aus. Verwenden Sie die `bulk`-Operation, um einige Beispieldaten zu indizieren:

```
PUT accounts/_bulk?refresh
{"index":{"_id":"1"}}
{"account_number":1,"balance":39225,"firstname":"Amber","lastname":"Duke","age":32,"gender":"M"
 Holmes
 Lane","employer":"Pyrami","email":"amberduke@pyrami.com","city":"Brogan","state":"IL"}
{"index":{"_id":"6"}}
{"account_number":6,"balance":5686,"firstname":"Hattie","lastname":"Bond","age":36,"gender":"M"
 Bristol
 Street","employer":"Netagy","email":"hattiebond@netagy.com","city":"Dante","state":"TN"}
{"index":{"_id":"13"}}
{"account_number":13,"balance":32838,"firstname":"Nanette","lastname":"Bates","age":28,"gender"
 Mady Street","employer":"Quility","city":"Nogal","state":"VA"}
{"index":{"_id":"18"}}
{"account_number":18,"balance":4180,"firstname":"Dale","lastname":"Adams","age":33,"gender":"M"
 Hutchinson Court","email":"daleadams@boink.com","city":"Orick","state":"MD"}
```

Im folgenden Beispiel wird Folgendes zurückgegeben: `firstname`- und `lastname`-Felder für Dokumente in einem Kontenindex mit `age` größer als 18:

```
search source=accounts | where age > 18 | fields firstname, lastname
```

Beispielantwort

id	FirstName	LastName
0	Amber	Duke
1	Hattie	Bond
2	Nanette	Bates
3	Dale	Adams

Sie können einen kompletten Satz schreibgeschützter Befehle wie `search`, `where`, `fields`, `rename`, `dedup`, `stats`, `sort`, `eval`, `head`, `top` und `rare` verwenden. Das PPL-Plug-In unterstützt alle SQL-Funktionen, einschließlich mathematischer, trigonometrischer, Datum-Zeit-, Zeichenfolgen-, aggregierter und fortgeschrittener Operatoren und Ausdrücke. Weitere Informationen finden Sie im OpenSearch PPL-Referenzhandbuch.

Bewährte Betriebspraktiken für Amazon OpenSearch Service

Dieses Kapitel enthält bewährte Methoden für den Betrieb von Amazon OpenSearch Service-Domains und enthält allgemeine Richtlinien, die für viele Anwendungsfälle gelten. Jede Workload ist einzigartig und weist einzigartige Merkmale auf, sodass keine generische Empfehlung für jeden Anwendungsfall genau richtig ist. Die wichtigste bewährte Methode besteht darin, Ihre Domains in einem kontinuierlichen Zyklus bereitzustellen, zu testen und anzupassen, um die optimale Konfiguration, Stabilität und Kosten für Ihre Workload zu ermitteln.

Themen

Überwachen und Warnen

Die folgenden bewährten Methoden gelten für die Überwachung Ihrer OpenSearch Service-Domains.

CloudWatch Alarme konfigurieren

OpenSearch Der Service sendet Leistungskennzahlen an Amazon CloudWatch. Überprüfen Sie regelmäßig Ihre Cluster- und Instance-Metriken und konfigurieren Sie empfohlene CloudWatch Alarme auf der Grundlage Ihrer Workload-Leistung.

Aktivieren der Protokollveröffentlichung

OpenSearch Der Service macht OpenSearch Fehlerprotokolle, Suchprotokolle, Indexierungsprotokolle und Auditprotokolle in Amazon CloudWatch Logs verfügbar. Protokolle für langsame Suchen, Protokolle für langsame Indizierung und Fehlerprotokolle sind für die Problembehandlung bei Leistungs- und Stabilitätsproblemen nützlich. Überwachungsprotokolle, die nur verfügbar sind, wenn Sie eine differenzierte Zugriffskontrolle aktivieren, verfolgen die Benutzeraktivität. Weitere Informationen finden Sie in der Dokumentation unter Logs. OpenSearch

Protokolle für langsame Suchen, Protokolle für langsame Indizierung sind ein wichtiges Tool, um die Leistung Ihrer Such- und Indizierungsvorgänge zu verstehen und Fehler zu beheben. Aktivieren Sie die Bereitstellung von Protokollen für langsame Suchen und Indizes für alle ProduktionsDomains. Sie müssen auch Schwellenwerte für die Protokollierung konfigurieren — andernfalls werden die Protokolle CloudWatch nicht erfasst.

Shard-Strategie

Shards verteilen Ihre Arbeitslast auf die Datenknoten in Ihrer OpenSearch Service-Domain. Richtig konfigurierte Indizes können dazu beitragen, die Gesamtleistung der Domain zu steigern.

Wenn Sie Daten an OpenSearch Service senden, senden Sie diese Daten an einen Index. Ein Index ist vergleichbar mit einer Datenbanktabelle, mit Dokumenten als Zeilen und Feldern als Spalten. Wenn Sie den Index erstellen, geben Sie an, OpenSearch wie viele primäre Shards Sie erstellen möchten. Die primären Shards sind unabhängige Partitionen des gesamten Datensatzes. OpenSearch Der Service verteilt Ihre Daten automatisch auf die primären Shards in einem Index. Sie können auch Replikate des Index konfigurieren. Jedes Replikat umfasst einen vollständigen Satz von Kopien der primären Shards für diesen Index.

OpenSearch Der Service ordnet die Shards für jeden Index den Datenknoten in Ihrem Cluster zu. Er stellt sicher, dass sich die Primär- und Replikat-Shards für den Index auf unterschiedlichen Datenknoten befinden. Das erste Replikat stellt sicher, dass Sie zwei Kopien der Daten im Index haben. Sie sollten immer mindestens ein Replikat verwenden. Zusätzliche Replikate bieten zusätzliche Redundanz und Lesekapazität.

OpenSearch sendet Indexierungsanfragen an alle Datenknoten, die Shards enthalten, die zum Index gehören. Indizierungsanforderungen werden zuerst an Datenknoten gesendet, die primäre Shards enthalten, und dann an Datenknoten, die Replikat-Shards enthalten. Suchanfragen werden vom Koordinationsknoten entweder an einen primären oder einen Replikat-Shard für alle zum Index gehörenden Shards weitergeleitet.

Bei einem Index mit fünf primären Shards und einem Replikat berührt beispielsweise jede Indizierungsanforderung 10 Shards. Im Gegensatz dazu werden Suchanfragen an n Shards gesendet, wobei n die Anzahl der primären Shards ist. Bei einem Index mit fünf primären Shards und einem Replikat berührt jede Suchanfrage fünf Shards (primär oder Replikat) aus diesem Index.

Ermitteln der Anzahl der Shards und Datenknoten

Verwenden Sie die folgenden bewährten Methoden, um die Anzahl der Shards und Datenknoten für Ihre Domain zu bestimmen.

Shard-Größe – Die Größe der Daten auf der Festplatte ist ein direktes Ergebnis der Größe Ihrer Quelldaten und ändert sich, wenn Sie mehr Daten indizieren. Das source-to-index Verhältnis kann stark variieren, von 1:10 bis 10:1 oder mehr, aber normalerweise liegt es bei etwa 1:1,10. Sie können dieses Verhältnis verwenden, um die Indexgröße auf der Festplatte vorherzusagen. Sie können auch einige Daten indizieren und die tatsächlichen Indexgrößen abrufen, um das Verhältnis für Ihre Workload zu bestimmen. Sobald Sie eine voraussichtliche Indexgröße haben, legen Sie eine Shard-Anzahl fest, sodass jeder Shard zwischen 10 und 30 GiB (für Such-Workloads) oder zwischen 30 und 50 GiB (für Protokoll-Workloads) liegt. 50 GiB sollten das Maximum sein; planen Sie auf jeden Fall einen Zuwachs ein.

Shard-Anzahl – Die Verteilung von Shards auf Datenknoten hat einen großen Einfluss auf die Leistung einer Domain. Wenn Sie Indizes mit mehreren Shards haben, versuchen Sie, die Anzahl der Shards auf ein gerades Vielfaches der Anzahl der Datenknoten einzustellen. Dies sorgt dafür, dass Shards gleichmäßig über Datenknoten verteilt sind, und verhindert heiße Knoten. Wenn Sie beispielsweise 12 primäre Shards haben, sollte Ihre Datenknotenanzahl 2, 3, 4, 6 oder 12 betragen. Die Shard-Anzahl ist jedoch zweitrangig gegenüber der Shard-Größe; Wenn Sie über 5 GiB an Daten verfügen, sollten Sie dennoch einen einzelnen Shard verwenden.

Shards pro Datenknoten – Die Gesamtzahl der Shards, die ein Knoten verarbeiten kann, ist proportional zum Java Virtual Machine (JVM)-Speicher des Knotens. Streben Sie 25 Shards oder weniger pro GiB Heap-Speicher an. Beispielsweise sollte ein Knoten mit 32 GiB Heap-Speicher nicht mehr als 800 Shards verarbeiten. Obwohl die Shard-Verteilung basierend auf Ihren Workload-Mustern variieren kann, gibt es ein Limit von 1 000 Shards pro Knoten. Die cat/allocation-API bietet einen schnellen Überblick über die Anzahl der Shards und den gesamten Shard-Speicher über Datenknoten hinweg.

Shard-zu-CPU-Verhältnis – Wenn ein Shard an einer Indexierungs- oder Suchanforderung beteiligt ist, verwendet es eine vCPU, um die Anforderung zu verarbeiten. Verwenden Sie als bewährte Methode einen anfänglichen Skalierungspunkt von 1,5 vCPU pro Shard. Wenn Ihr Instance-Typ

8 vCPUs hat, legen Sie die Anzahl Ihrer Datenknoten so fest, dass jeder Knoten nicht mehr als sechs Shards hat. Beachten Sie, dass dies eine Annäherung ist. Testen Sie unbedingt Ihren Workload und skalieren Sie Ihren Cluster entsprechend.

Empfehlungen zu Speichervolumen, Shard-Größe und Instance-Typ finden Sie in den folgenden Ressourcen:

- the section called “Größenanpassung von Domains”
- the section called “Petabyte-Größe”

Vermeiden von Speicherversatz

Speicherversatz tritt auf, wenn ein oder mehrere Knoten innerhalb eines Clusters einen höheren Anteil an Speicher für einen oder mehrere Indizes halten als die anderen. Anzeichen für Speicherversatz sind ungleichmäßige CPU-Auslastung, intermittierende und ungleichmäßige Latenzzeiten und ungleichmäßige Warteschlangen auf den Datenknoten. Um festzustellen, ob Sie Probleme mit dem Versatz haben, lesen Sie die folgenden Abschnitte zur Fehlerbehebung:

- the section called “Knoten-Shard und Speicherversatz”
- the section called “Index-Shard und Speicherversatz”

Stabilität

Die folgenden bewährten Methoden gelten für die Aufrechterhaltung einer stabilen und fehlerfreien Service-Domain. OpenSearch

Bleiben Sie auf dem Laufenden mit OpenSearch

Service-Software-Updates

OpenSearch Service veröffentlicht regelmäßig Softwareupdates, die Funktionen hinzufügen oder Ihre Domains auf andere Weise verbessern. Updates ändern weder die Version noch die OpenSearch Version der Elasticsearch-Engine. Wir empfehlen, dass Sie einen wiederkehrenden Zeitpunkt für die Ausführung des DescribeDomainAPI-Vorgangs einplanen und gegebenenfalls ein Service-Software-Update einleiten. `UpdateStatus` `ELIGIBLE` Wenn Sie Ihre Domain nicht innerhalb eines bestimmten Zeitraums (in der Regel zwei Wochen) aktualisieren, führt der OpenSearch Service das Update automatisch durch.

OpenSearch Versions-Upgrades

OpenSearch Der Service bietet regelmäßig Unterstützung für von der Community verwaltete Versionen von. OpenSearch Führen Sie immer ein Upgrade auf die neuesten OpenSearch Versionen durch, wenn diese verfügbar sind.

OpenSearch Der Service aktualisiert gleichzeitig OpenSearch sowohl OpenSearch Dashboards als auch Dashboards (oder Elasticsearch und Kibana, wenn auf Ihrer Domain eine ältere Engine läuft). Wenn der Cluster über dedizierte Master-Knoten verfügt, werden Upgrades ohne Ausfallzeiten abgeschlossen. Andernfalls reagiert der Cluster nach dem Upgrade möglicherweise einige Sekunden lang nicht, während er einen Master-Knoten auswählt. OpenSearch Dashboards sind möglicherweise während eines Teils oder des gesamten Upgrades nicht verfügbar.

Es gibt zwei Möglichkeiten, eine Domain zu aktualisieren:

- Direktes Upgrade – Diese Option ist einfacher, da Sie denselben Cluster beibehalten.
- Snapshot-/Wiederherstellungs-Upgrade – Diese Option ist gut geeignet zum Testen neuer Versionen auf einem neuen Cluster oder zum Migrieren zwischen Clustern.

Unabhängig davon, welchen Upgradeprozess Sie verwenden, empfehlen wir, eine Domain zu verwalten, die ausschließlich zu Entwicklungs- und Testzwecken dient, und sie auf die neue Version zu aktualisieren, bevor Sie Ihre Produktion-Domain aktualisieren. Wählen Sie Development and testing (Entwicklung und Prüfung) als Bereitstellungstyp aus, wenn Sie die Test-Domain erstellen. Stellen Sie sicher, dass Sie alle Clients unmittelbar nach dem Domain-Upgrade auf kompatible Versionen aktualisieren.

Verbessern Sie die Snapshot-

Um zu verhindern, dass Ihr Snapshot bei der Verarbeitung hängen bleibt, sollte der Instance-Typ für den dedizierten Master-Knoten mit der Anzahl der Shards übereinstimmen. Weitere Informationen finden Sie unter the section called “Auswählen von Instance-Typen für dedizierte Hauptknoten”. Darüber hinaus sollte jeder Knoten nicht mehr als die empfohlenen 25 Shards pro GiB Java-Heap-Speicher haben. Weitere Informationen finden Sie unter the section called “Auswahl der Anzahl der Shards”.

Dedizierte Hauptknoten aktivieren

Dedizierte Hauptknoten erhöhen die Cluster-Stabilität. Ein dedizierter Hauptknoten führt Cluster-Verwaltungsaufgaben aus, enthält jedoch keine Indexdaten und antwortet nicht auf Client-

Anforderungen. Diese Auslagerung von Cluster-Verwaltungsaufgaben erhöht die Stabilität Ihrer Domain und ermöglicht es, einige Konfigurationsänderungen ohne Ausfallzeiten durchzuführen.

Aktivieren und verwenden Sie drei dedizierte Hauptknoten für optimale Domain-Stabilität in drei Availability Zones. Bei der Bereitstellung mit Multi-AZ mit Standby werden drei dedizierte Master-Knoten für Sie konfiguriert. Empfehlungen zu Instance-Typen finden Sie unter the section called “Auswählen von Instance-Typen für dedizierte Hauptknoten”.

Bereitstellen über mehrere Availability Zones hinweg

Um Datenverlust zu vermeiden und die Ausfallzeit des Clusters im Falle einer Unterbrechung des Service zu minimieren, können Sie die Knoten auf zwei oder drei Availability Zones im selben AWS-Region verteilen. Eine bewährte Methode ist die Verwendung von Multi-AZ mit Standby, bei der drei Availability Zones konfiguriert werden, wobei zwei Zonen aktiv sind und eine als Standby-Zone fungiert, und mit zwei Replikat-Shards pro Index. Diese Konfiguration ermöglicht es OpenSearch Service, Replikat-Shards an andere AZs als die entsprechenden primären Shards zu verteilen. Für die Cluster-Kommunikation zwischen Availability Zones fallen keine Availability-Zone-übergreifenden Datenübertragungsgebühren an.

Availability Zones sind isolierte Standorte innerhalb jeder -Region. Bei einer Konfiguration mit zwei Availability Zones bedeutet der Verlust einer Availability Zone, dass Sie die Hälfte der gesamten Domain-Kapazität verlieren. Durch die Umstellung auf drei Availability Zones werden die Auswirkungen des Verlusts einer einzelnen Availability Zone weiter reduziert.

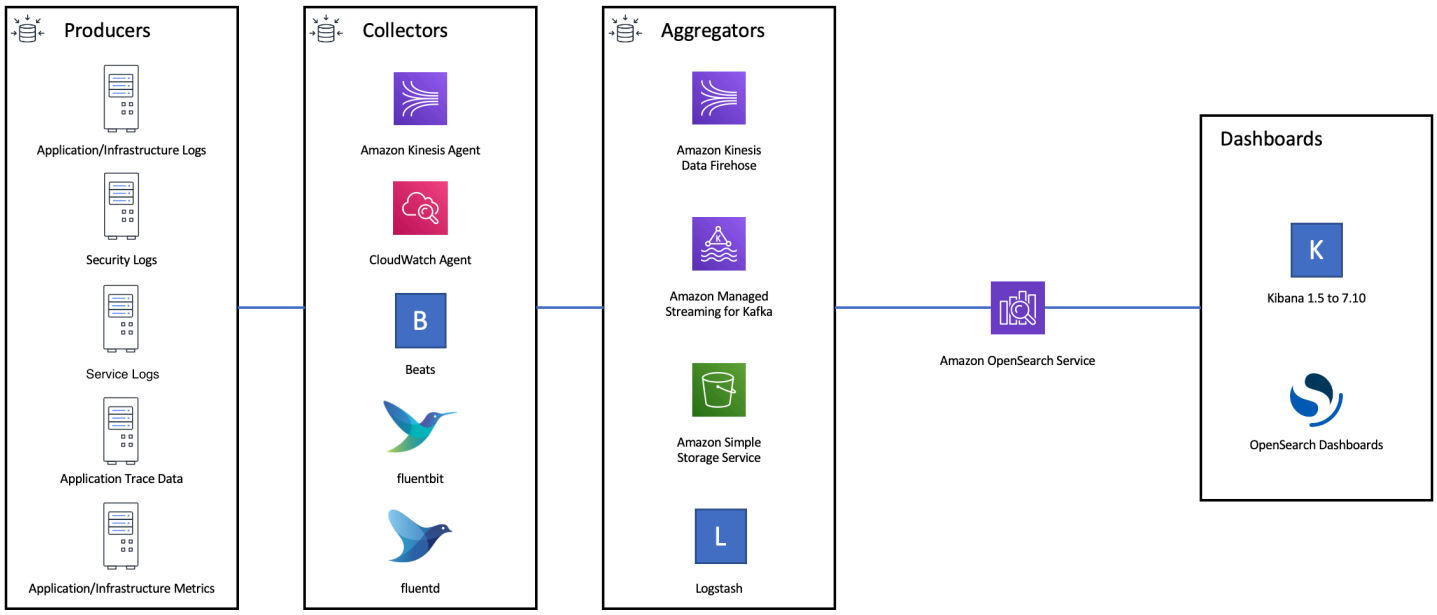
Steuern von Erfassungsablauf und Pufferung

Wir empfehlen, die Gesamtzahl der Anforderungen mithilfe des API-Vorgangs _bulk zu begrenzen. Es ist effizienter, eine `_bulk`-Anforderung zu senden, die 5 000 Dokumente enthält, als 5 000 Anforderungen zu senden, die jeweils ein Dokument enthalten.

Für eine optimale Betriebsstabilität ist es manchmal erforderlich, den Upstream-Ablauf von Indizierungsanforderungen zu begrenzen oder sogar anzuhalten. Die Begrenzung der Rate von Indexanforderungen ist ein wichtiger Mechanismus für den Umgang mit unerwarteten oder gelegentlichen Spitzen bei Anfragen, die andernfalls den Cluster überfordern könnten. Erwägen Sie, einen Mechanismus zur Ablaufkontrolle in Ihre Upstream-Architektur einzubauen.

Das folgende Diagramm zeigt mehrere Komponentenoptionen für eine Protokollerfassungsarchitektur. Konfigurieren Sie die Aggregationsebene so, dass ausreichend Platz

zum Puffern eingehender Daten für plötzliche Datenverkehrsspitzen und kurze Domain-Wartung vorhanden ist.



Erstellen von Zuordnungen für Such-Workloads

Erstellen Sie für Such-Workloads Zuordnungen, die definieren, wie Dokumente und ihre Felder OpenSearch gespeichert und indexiert werden. Setzen Sie `dynamic` auf `strict`, um ein versehentliches Hinzufügen neuer Felder zu verhindern:

```
PUT my-index
{
  "mappings": {
    "dynamic": "strict",
    "properties": {
      "title": { "type" : "text" },
      "author": { "type" : "integer" },
      "year": { "type" : "text" }
    }
  }
}
```

Verwenden von Indexvorlagen

Mithilfe einer Indexvorlage können Sie festlegen, wie ein Index konfiguriert wird, wenn er erstellt wird. OpenSearch Konfigurieren Sie Indexvorlagen, bevor Sie Indizes erstellen. Wenn Sie dann einen Index erstellen, erbt dieser die Einstellungen und Zuordnungen von der Vorlage. Sie können mehrere

Vorlage auf einen einzelnen Index anwenden, d. h. Sie können Einstellungen in einer Vorlage und Zuordnungen in einer anderen angeben. Diese Strategie ermöglicht eine Vorlage für allgemeine Einstellungen über mehrere Indizes hinweg und separate Vorlagen für spezifischere Einstellungen und Zuordnungen.

Die folgenden Einstellungen sind hilfreich bei der Konfiguration in Vorlagen:

- Anzahl der Primär- und Replikat-Shards
- Aktualisierungsintervall (wie oft der Index aktualisiert werden soll, damit die letzten Änderungen für die Suche verfügbar sind)
- Dynamische Zuordnungssteuerung
- Explizite Feldzuordnungen

Die folgende Beispielvorlage enthält jede dieser Einstellungen:

```
{
   "index_patterns":[
      "index-*"
   ],
   "order": 0,
   "settings": {
      "index": {
         "number_of_shards": 3,
         "number_of_replicas": 1,
         "refresh_interval": "60s"
      }
   },
   "mappings": {
      "dynamic": false,
      "properties": {
         "field_name1": {
            "type": "keyword"
         }
      }
   }
}
```

Auch wenn sie sich selten ändern, OpenSearch ist es einfacher, Einstellungen und Zuordnungen zentral zu definieren, als mehrere Upstream-Clients zu aktualisieren.

Indizes mit Indexstatusmanagement verwalten

Wenn Sie Protokolle oder Zeitreihendaten verwalten, empfehlen wir die Verwendung von Indexstatusmanagement (ISM). Mit ISM können Sie regelmäßige Aufgaben zur Verwaltung des Indexlebenszyklus automatisieren. Mit ISM können Sie Richtlinien erstellen, die Index-Alias-Rollover aufrufen, Index-Snapshots erstellen, Indizes zwischen Speicherebenen verschieben und alte Indizes löschen. Sie können den ISM-Rollover-Vorgang sogar als alternative Strategie für die Verwaltung des Datenlebenszyklus verwenden, um Shard-Versatz zu vermeiden.

Richten Sie zuerst eine ISM-Richtlinie ein. Ein Beispiel finden Sie unter the section called “Beispielrichtlinien”. Fügen Sie dann die Richtlinie einem oder mehreren Indizes zu. Wenn Sie ein ISM-Vorlagenfeld in die Richtlinie aufnehmen, wendet der OpenSearch Service die Richtlinie automatisch auf jeden Index an, der dem angegebenen Muster entspricht.

Entferne nicht verwendete Indizes

Überprüfen Sie regelmäßig die Indizes in Ihrem Cluster und identifizieren Sie alle, die nicht verwendet werden. Erstellen Sie einen Snapshot dieser Indizes, damit sie in S3 gespeichert werden, und löschen Sie sie dann. Wenn Sie nicht verwendete Indizes entfernen, reduzieren Sie die Anzahl der Shards und ermöglichen knotenübergreifend eine ausgewogenere Speicherverteilung und Ressourcenauslastung. Selbst im Leerlauf verbrauchen Indizes während der internen Indexwartung einige Ressourcen.

Anstatt ungenutzte Indizes manuell zu löschen, können Sie ISM verwenden, um automatisch einen Snapshot zu erstellen und Indizes nach einem bestimmten Zeitraum zu löschen.

Verwenden mehrerer Domains für hohe Verfügbarkeit

Um eine hohe Verfügbarkeit von über 99,9 % Betriebszeit in mehreren Regionen zu erreichen, sollten Sie die Verwendung von zwei Domains in Erwägung ziehen. Für kleine oder sich langsam ändernde Datensätze können Sie clusterübergreifende Replikation einrichten, um ein Aktiv-Passiv-Modell aufrechtzuerhalten. In diesem Modell wird nur in die Leader-Domain geschrieben, aber aus jeder Domain kann gelesen werden. Konfigurieren Sie für größere Datensätze und sich schnell ändernde Daten die duale Bereitstellung in Ihrer Aufnahmepipeline, sodass alle Daten in einem Aktiv-Aktiv-Modell unabhängig voneinander in beide Domains geschrieben werden.

Entwickeln Sie Ihre Upstream- und Downstream-Anwendungen unter Berücksichtigung von Failover. Stellen Sie sicher, dass Sie den Failover-Prozess zusammen mit anderen Notfallwiederherstellungsprozessen testen.

Leistung

Die folgenden bewährten Methoden gelten für die Abstimmung Ihrer Domains für eine optimale Leistung.

Größe und Komprimierung von Massenanfragen optimieren

Die Massengröße hängt von Ihren Daten, Ihrer Analyse und Ihrer Clusterkonfiguration ab, aber ein guter Ausgangspunkt sind 3–5 MiB pro Massenanforderung.

Senden Sie Anfragen und empfangen Sie Antworten von Ihren OpenSearch Domains, indem Sie die Gzip-Komprimierung verwenden, um die Nutzlast von Anfragen und Antworten zu reduzieren. Sie können die Gzip-Komprimierung mit dem OpenSearch Python-Client verwenden oder indem Sie die folgenden Header von der Clientseite aus einbeziehen:

- `'Accept-Encoding': 'gzip'`
- `'Content-Encoding': 'gzip'`

Zum Optimieren der Größe Ihrer Massenanforderungen beginnen Sie mit einer Massenanfragengröße von 3 MiB. Erhöhen Sie dann langsam die Anforderungsgröße, bis sich die Indizierungsleistung nicht mehr verbessert.

> **Note**
>
> Um die gzip-Komprimierung auf Domains zu aktivieren, auf denen Elasticsearch Version 6.x ausgeführt wird, müssen Sie `http_compression.enabled` auf Cluster-Ebene festlegen. Diese Einstellung ist standardmäßig in Elasticsearch-Versionen 7.x und allen Versionen von wahr. OpenSearch

Größe der Antworten auf Massenanfragen reduzieren

Um die Größe der OpenSearch Antworten zu reduzieren, schließen Sie unnötige Felder mit dem `filter_path` Parameter aus. Achten Sie darauf, keine Felder herauszufiltern, die zur Identifizierung oder Wiederholung fehlgeschlagener Anforderungen erforderlich sind. Weitere Informationen und Beispiele finden Sie unter the section called “Reduzierung der Antwortgröße”.

Aktualisierungsintervalle optimieren

OpenSearch Indizes weisen letztendlich Lesekonsistenz auf. Ein Aktualisierungsvorgang macht alle Aktualisierungen, die an einem Index durchgeführt werden, für die Suche verfügbar. Das standardmäßige Aktualisierungsintervall beträgt eine Sekunde, was bedeutet, dass OpenSearch jede Sekunde eine Aktualisierung durchgeführt wird, während in einen Index geschrieben wird.

Je seltener Sie einen Index aktualisieren (höheres Aktualisierungsintervall), desto besser ist die Indizierungsleistung insgesamt. Der Nachteil der Verlängerung des Aktualisierungsintervalls besteht darin, dass es eine längere Verzögerung zwischen einer Indexaktualisierung und dem Zeitpunkt gibt, zu dem die neuen Daten für die Suche verfügbar sind. Stellen Sie Ihr Aktualisierungsintervall so hoch wie möglich ein, um die Gesamtleistung zu verbessern.

Wir empfehlen, den `refresh_interval`-Parameter für alle Ihre Indizes auf 30 Sekunden oder mehr einzustellen.

Automatische Optimierung aktivieren

Auto-Tune verwendet Leistungs- und Nutzungsmetriken aus Ihrem OpenSearch Cluster, um Änderungen an den Warteschlangengrößen, Cachegrößen und den Einstellungen der Java Virtual Machine (JVM) auf Ihren Knoten vorzuschlagen. Diese optionalen Änderungen verbessern die Clustergeschwindigkeit und -stabilität. Sie können jederzeit zu den standardmäßigen OpenSearch Serviceeinstellungen zurückkehren. Automatische Optimierung ist bei neuen Domains standardmäßig aktiviert, es sei denn, Sie deaktivieren sie ausdrücklich.

Wir empfehlen, die automatische Optimierung für alle Domains zu aktivieren und entweder ein wiederkehrendes Wartungsfenster festzulegen oder die Empfehlungen regelmäßig zu überprüfen.

Sicherheit

Die folgenden bewährten Methoden gelten für die Sicherung Ihrer Domains.

Differenzierte Zugriffskontrolle aktivieren

Mit einer detaillierten Zugriffskontrolle können Sie steuern, wer auf bestimmte Daten innerhalb einer OpenSearch Dienstdomäne zugreifen kann. Im Vergleich zur allgemeinen Zugriffskontrolle gibt die differenzierte Zugriffssteuerung jedem Cluster, Index, Dokument und Feld eine eigene festgelegte Zugriffsrichtlinie. Zugriffskriterien können auf einer Reihe von Faktoren basieren, einschließlich der Rolle der Person, die den Zugriff anfordert, und der Aktion, die sie mit den Daten

durchführen möchte. Beispielsweise können Sie einem Benutzer Zugriff zum Schreiben in einen Index gewähren, während ein anderer nur Zugriff zum Lesen der Daten im Index erhält, ohne Änderungen vorzunehmen.

Durch die differenzierte Zugriffskontrolle können Daten mit unterschiedlichen Zugriffsanforderungen auf demselben Speicherplatz vorhanden sein, ohne dass Sicherheits- oder Compliance-Probleme auftreten.

Wir empfehlen, eine differenzierte Zugriffssteuerung für Ihre Domains zu aktivieren.

Bereitstellen von Domains innerhalb einer VPC

Wenn Sie Ihre OpenSearch Service-Domain in einer Virtual Private Cloud (VPC) platzieren, können Sie eine sichere Kommunikation zwischen dem OpenSearch Service und anderen Diensten innerhalb der VPC ermöglichen — ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains, die öffentliche Endpunkte nutzen, über eine zusätzliche Sicherheitsebene.

Wir empfehlen, dass Sie Ihre Domains innerhalb einer VPC erstellen.

Anwenden einer restriktiven Zugriffsrichtlinie

Selbst wenn Ihre Domain innerhalb einer VPC bereitgestellt wird, ist das Implementieren der Sicherheit in mehreren Schichten eine bewährte Methode. Stellen Sie sicher, dass Sie die Konfiguration Ihrer aktuellen Zugriffsrichtlinien überprüfen.

Wenden Sie eine restriktive, ressourcenbasierte Zugriffsrichtlinie auf Ihre Domains an und folgen Sie dem Prinzip der geringsten Rechte, wenn Sie Zugriff auf die Konfigurations-API und die OpenSearch API-Operationen gewähren. Vermeiden Sie in der Regel die Verwendung des anonymen Benutzerprinzipals `"Principal": {"AWS": "*" }` in Ihren Zugriffsrichtlinien.

In einigen Situationen ist es jedoch akzeptabel, eine offene Zugriffsrichtlinie zu verwenden, z. B. wenn Sie eine differenzierte Zugriffssteuerung aktivieren. Eine offene Zugriffsrichtlinie kann Ihnen den Zugriff auf die Domain in Fällen ermöglichen, in denen das Signieren von Anforderungen schwierig oder unmöglich ist, z. B. von bestimmten Clients und Tools.

Verschlüsselung im Ruhezustand aktivieren

OpenSearch Service-Domains bieten Verschlüsselung von Daten im Ruhezustand, um unbefugten Zugriff auf Ihre Daten zu verhindern. Encryption at Rest verwendet AWS Key Management Service

(AWS KMS) zum Speichern und Verwalten Ihrer Verschlüsselungsschlüssel und den Advanced Encryption Standard-Algorithmus mit 256-Bit-Schlüsseln (AES-256) zur Verschlüsselung.

Wenn Ihre Domain sensible Daten speichert, aktivieren Sie die Verschlüsselung der Daten im Ruhezustand.

Aktivieren Sie die Verschlüsselung node-to-node

Die ode-to-node N-Verschlüsselung bietet zusätzlich zu den Standardsicherheitsfunktionen des OpenSearch Dienstes eine zusätzliche Sicherheitsebene. Sie implementiert Transport Layer Security (TLS) für die gesamte Kommunikation zwischen den Knoten, die innerhalb OpenSearch des Systems bereitgestellt werden. Keine ode-to-node Verschlüsselung: Alle Daten, die über HTTPS an Ihre OpenSearch Service-Domain gesendet werden, bleiben während der Übertragung verschlüsselt, während sie zwischen den Knoten verteilt und repliziert werden.

Wenn Ihre Domain vertrauliche Daten speichert, aktivieren Sie die node-to-node Verschlüsselung.

Überwachen Sie mit AWS Security Hub

Überwachen Sie Ihre Nutzung des OpenSearch Dienstes in Bezug auf bewährte Sicherheitsverfahren mithilfe von AWS Security Hub. Security Hub verwendet Sicherheitskontrollen für die Bewertung von Ressourcenkonfigurationen und Sicherheitsstandards, um Sie bei der Einhaltung verschiedener Compliance-Frameworks zu unterstützen. Weitere Informationen zur Verwendung von Security Hub zur Evaluierung von OpenSearch Serviceressourcen finden Sie unter Amazon OpenSearch Service Steuerelemente im AWS Security Hub Benutzerhandbuch.

Kostenoptimierung

Die folgenden bewährten Methoden gelten für die Optimierung und Einsparung Ihrer OpenSearch Servicekosten.

Instance-Typen der neuesten Generation verwenden

OpenSearch Der Service führt ständig neue Amazon EC2 EC2-Instance-Typen ein, die eine bessere Leistung zu geringeren Kosten bieten. Wir empfehlen, immer die Instances der neuesten Generation zu verwenden.

Vermeiden Sie es, T2 oder `t3.small`-Instances für Produktion-Domains zu verwenden, da diese bei anhaltender hoher Last instabil werden können. `r6g.large`-Instances sind eine Option für kleine Produktion-Workloads (sowohl als Datenknoten als auch als dedizierte Hauptknoten).

Verwenden Sie die neuesten Amazon-EBS-gp3-Volumes

OpenSearch Datenknoten benötigen Speicher mit geringer Latenz und hohem Durchsatz, um eine schnelle Indizierung und Abfrage zu ermöglichen. Durch die Verwendung von Amazon-EBS-gp3-Volumes erhalten Sie eine höhere Basisleistung (IOPS und Durchsatz) zu 9,6 % niedrigeren Kosten als mit dem zuvor angebotenen Amazon-EBS-gp2-Volume-Typ. Mit gp3 können Sie unabhängig von der Volume-Größe zusätzliche IOPS und Durchsätze bereitstellen. Diese Volumes sind auch stabiler als Volumes der vorherigen Generation, da sie keine Burst-Gutschriften verwenden. Der GP3-Volumetyp verdoppelt außerdem die per-data-node Volumengrößenbeschränkungen des GP2-Volumetyps. Mit diesen größeren Volumina können Sie die Kosten für passive Daten senken, indem Sie die Speichermenge pro Datenknoten erhöhen.

Verwendung UltraWarm und Cold Storage für Zeitreihen-Protokolldaten

Wenn Sie sie OpenSearch für Protokollanalysen verwenden, verschieben Sie Ihre Daten in einen UltraWarm Kühlraum, um die Kosten zu senken. Verwenden Sie Indexstatusmanagement (ISM), um Daten zwischen Speicherebenen zu migrieren und die Datenaufbewahrung zu verwalten.

UltraWarmbietet eine kostengünstige Möglichkeit, große Mengen schreibgeschützter Daten im OpenSearch Service zu speichern. UltraWarm verwendet Amazon S3 für die Speicherung, was bedeutet, dass die Daten unveränderlich sind und nur eine Kopie benötigt wird. Sie zahlen nur für den Speicherplatz, der der Größe der primären Shards in Ihren Indizes entspricht. Die Latenzen für UltraWarm Abfragen steigen mit der Menge an S3-Daten, die für die Bearbeitung der Abfrage benötigt werden. Nachdem die Daten auf den Knoten zwischengespeichert wurden, verhalten sich Abfragen an UltraWarm Indizes ähnlich wie Abfragen an Hot-Indizes.

Cold Storage wird auch von S3 unterstützt. Wenn Sie kalte Daten abfragen müssen, können Sie sie selektiv an vorhandene Knoten anhängen. UltraWarm Für kalte Daten fallen dieselben verwalteten Speicherkosten an wie UltraWarm, aber Objekte im Cold Storage verbrauchen keine UltraWarm Knotenressourcen. Daher bietet Cold Storage eine beträchtliche Menge an Speicherkapazität, ohne die Größe oder Anzahl der UltraWarm Knoten zu beeinflussen.

UltraWarm wird kostengünstig, wenn Sie etwa 2,5 TiB an Daten aus dem Hot-Storage migrieren müssen. Überwachen Sie Ihre Füllrate und planen Sie, Indizes zu verschieben, UltraWarm bevor Sie dieses Datenvolumen erreichen.

Empfehlungen für Reserved Instances überprüfen

Ziehen Sie den Kauf von Reserved Instances (RIs) in Erwägung, nachdem Sie eine gute Ausgangsbasis für Ihre Leistung und Ihren Rechenaufwand haben. Rabatte beginnen bei etwa 30 % für 1-Jahres-Reservierungen ohne Vorauszahlung und können bis zu 50 % für alle 3-Jahres-Verpflichtungen im Voraus erhöhen.

Nachdem Sie mindestens 14 Tage lang einen stabilen Betrieb beobachtet haben, überprüfen Sie die Empfehlungen für Reserved Instances in Cost Explorer. In der Überschrift Amazon OpenSearch Service werden spezifische Kaufempfehlungen von RI und prognostizierte Einsparungen angezeigt.

Dimensionierung von Amazon OpenSearch Service-Domains

Es gibt keine perfekte Methode zur Dimensionierung von Amazon OpenSearch Service-Domains. Wenn Sie jedoch mit einem Verständnis Ihrer Speicheranforderungen, des Services und OpenSearch selbst beginnen, können Sie eine fundierte erste Schätzung Ihres Hardwarebedarfs vornehmen. Diese Schätzung kann als Ausgangspunkt für den wichtigsten Aspekt der Dimensionierung von Domains dienen: Tests mit repräsentativen Workloads und Überwachung ihrer Leistung.

Themen

- Berechnung der Speicheranforderungen
- Auswahl der Anzahl der Shards
- Auswählen von Instance-Typen und Tests

Berechnung der Speicheranforderungen

Die meisten OpenSearch Workloads lassen sich in eine von zwei großen Kategorien einteilen:

- Langlebiger Index: Sie schreiben Code, der Daten in einem oder mehreren Indizes verarbeitet und diese OpenSearch Indizes dann regelmäßig aktualisiert, wenn sich die Quelldaten ändern. Einige allgemeine Beispiele sind Suchen auf Websites, in Dokumenten und für e-Commerce-Zwecke.
- Rolling-Indizes: Daten fließen kontinuierlich in einen Satz temporärer Indizes mit einem Indizierungszeitraum und einem Aufbewahrungsfenster (z. B. einen Satz täglicher Indizes, der zwei Wochen lang aufbewahrt wird). Einige allgemeine Beispiele sind Protokollanalyse, Zeitreihenverarbeitung und Clickstream-Analyse.

Für langlebige Index-Workloads können Sie die Quelldaten auf dem Datenträger untersuchen und einfach bestimmen, wie viel Speicherplatz dafür benötigt wird. Wenn die Daten aus mehreren Quellen stammen, addieren Sie diese Quellen einfach.

Für Rolling-Indizes können Sie die während eines repräsentativen Zeitraums generierten Datenmenge mit dem Aufbewahrungszeitraum multiplizieren. Wenn Sie beispielsweise 200 MiB Protokolldaten pro Stunde generieren, sind das 4,7 GiB pro Tag, also 66 GiB Daten zu jedem Zeitpunkt, wenn Sie einen Aufbewahrungszeitraum von zwei Wochen verwenden.

Die Größe Ihrer Datenquelle ist jedoch nur ein Aspekt Ihrer Speicheranforderungen. Außerdem müssen Sie Folgendes berücksichtigen:

- Anzahl der Replikate: Jedes Replikat ist eine vollständige Kopie eines Index und benötigt den gleichen Speicherplatz. Standardmäßig hat jeder OpenSearch Index ein Replikat. Wir empfehlen, mindestens eines zu verwenden, um sich gegen Datenverlust zu schützen. Replikate können auch die Suchleistung verbessern. Wenn Sie einen hohen Workload haben, können Sie in Betracht ziehen, mehrere zu erstellen. Verwenden Sie `PUT /my-index/_settings`, um die `number_of_replicas`-Einstellung für Ihren Index zu aktualisieren.
- OpenSearch Indizierungsaufwand: Die Größe eines Indexes auf der Festplatte variiert. Die Gesamtgröße der Quelldaten plus Index beträgt oft 110 % der Quelle, wobei der Index bis zu 10 % der Quelldaten ausmacht. Nachdem Sie Ihre Daten indiziert haben, können Sie die `_cat/indices?v`-API und den `pri.store.size`-Wert verwenden, um den genauen Zusatzaufwand zu berechnen. `_cat/allocation?v` bietet auch eine nützliche Zusammenfassung.
- Für das Betriebssystem reservierter Speicherplatz: Standardmäßig reserviert Linux 5 % des Dateisystems für den `root`-Benutzer für kritische Prozesse, zur Systemwiederherstellung und zum Schutz vor Problemen mit der Festplattenfragmentierung.
- OpenSearch Serviceaufwand: Der OpenSearch Service reserviert 20% des Speicherplatzes jeder Instanz (bis zu 20 GiB) für Segmentzusammenführungen, Protokolle und andere interne Operationen.

  Aufgrund dieses Höchstwerts von 20 GiB kann die Gesamtmenge an reserviertem Speicherplatz stark variieren und hängt von der Anzahl der Instances in Ihrer Domain ab. Beispiel: Eine Domain kann drei `m6g.xlarge.search`-Instances haben, mit jeweils 500 GiB Speicherplatz, also insgesamt 1,46 TiB. In diesem Fall beträgt der gesamte reservierte Speicherplatz nur 60 GiB. Eine andere Domain kann 10 `m3.medium.search`-Instances haben, mit jeweils 100 GiB Speicherplatz, also insgesamt 0,98 TiB. Hier beträgt der gesamte reservierte Speicherplatz 200 GiB, auch wenn die erste Domain 50 % größer ist.

In der folgenden Formel wenden wir eine „Worst-Case“-Schätzung für den Zusatzaufwand an. Diese Schätzung beinhaltet zusätzlichen freien Speicherplatz, um die Auswirkungen von Knotenausfällen und Ausfällen der Availability Zone zu minimieren.

Wenn Sie insgesamt jederzeit 66 GiB Quelldaten haben und ein Replikat verwenden wollen, liegt Ihr minimaler Speicherbedarf nahe 66 * 2 * 1,1/0,95/0,8 = 191 GiB. Sie können diese Berechnung wie folgt verallgemeinern:

Quelldaten * (1 + Anzahl von Replikaten) * (1 + Indexierungsaufwand)/(1 — reservierter Linux-Speicherplatz)/(1 — OpenSearch Serviceaufwand) = Mindestspeicherbedarf

Sie können diese vereinfachte Version verwenden:

Quelldaten * (1 + Anzahl der Replikate) * 1,45 = Mindestspeicheranforderung

Unzureichender Speicherplatz ist eine der häufigsten Ursachen für Clusterinstabilität. Sie sollten also die Zahlen überprüfen, wenn Sie Instance-Typen, Instance-Anzahlen und Speicher-Volumes auswählen.

Es gibt weitere Überlegungen zum Speicher.

- Wenn Ihre Mindestspeicheranforderungen 1 PB überschreiten, lesen Sie nach unter the section called “Petabyte-Größe”.
- Wenn Sie Rolling-Indizes haben und eine Hot-Warm-Architektur verwenden wollen, lesen Sie the section called “UltraWarm Speicher”.

Auswahl der Anzahl der Shards

Nachdem Sie die Speicheranforderungen kennen, können Sie über Ihre Indizierungsstrategie nachdenken. Standardmäßig ist in OpenSearch Service jeder Index in fünf primäre Shards und ein Replikat (insgesamt 10 Shards) unterteilt. Dieses Verhalten unterscheidet sich von Open Source OpenSearch, bei dem standardmäßig ein primärer Shard und ein Replikat-Shard verwendet werden. Da Sie die Anzahl der primären Shards für einen vorhandenen Index nicht leicht ändern können, sollten Sie die Anzahl der Shards festlegen, bevor Sie Ihr erstes Dokument indizieren.

Das übergeordnete Ziel bei der Auswahl der Shard-Anzahl ist es, einen Index gleichmäßig über alle Knoten im Cluster zu verteilen. Diese Shards sollten jedoch nicht zu groß oder zu zahlreich sein. Als allgemeine Richtlinie gilt, dass die Shard-Größe bei Workloads, bei denen die Suchlatenz ein

wichtiges Leistungsziel ist, zwischen 10 und 30 GiB und bei schreibintensiven Workloads wie der Protokollanalyse zwischen 30 und 50 GiB liegen sollte.

Große Shards können die Wiederherstellung OpenSearch nach einem Ausfall erschweren. Da jedoch jede Shard eine gewisse Menge an CPU und Arbeitsspeicher beansprucht, können zu viele kleine Shards zu Leistungseinbußen und Speicherproblemen führen. Mit anderen Worten, Shards sollten klein genug sein, dass die zugrunde liegende OpenSearch Service-Instanz sie verarbeiten kann, aber nicht so klein, dass sie die Hardware unnötig belasten.

Angenommen, Sie haben 66 GiB Daten. Sie gehen nicht davon aus, dass diese Anzahl mit der Zeit zunimmt, und Sie möchten Ihre Shards mit je 30 GiB beibehalten. Die Anzahl der Shards sollte deshalb ca. 66 * 1,1/30 = 3 betragen. Sie können diese Berechnung wie folgt verallgemeinern:

(Datenquelle + Wachstumspotenzial) * (1 + Indizierungsaufwand)/Gewünschte Shard-Größe = Ungefähre Anzahl der primären Shards

Diese Gleichung hilft Daten-Wachstum im Laufe der Zeit auszugleichen. Wenn Sie davon ausgehen, dass sich dieselben 66 GiB Daten innerhalb des nächsten Jahres vervierfachen, ist die ungefähre Anzahl der Shards (66 + 198) * 1,1 / 30 = 10. Beachten Sie jedoch, dass Sie diese zusätzlichen 198 GiB Daten noch nicht haben. Stellen Sie sicher, dass diese Vorbereitung für die Zukunft nicht unnötig kleine Shards erzeugt, die aktuell sehr große Mengen an CPU-Leistung und Speicher verbrauchen. In diesem Fall sind 66 * 1,1/10 Shards = 7,26 GiB pro Shard, was zusätzliche Ressourcen verbraucht und unterhalb des empfohlenen Größenbereichs liegt. Sie könnten eher den middle-of-the-road Ansatz von sechs Shards in Betracht ziehen, sodass Sie heute 12-GiB-Shards und in future 48-GiB-Shards haben werden. Auch hier könnten Sie bevorzugen, mit drei Shards zu beginnen und Ihre Daten neu zu indizieren, wenn die Shards über 50 GiB zunehmen.

Ein weitaus weniger häufiges Problem ist die Begrenzung der Shard-Anzahl pro Knoten. Wenn Sie Ihre Shards entsprechend dimensionieren, geht Ihnen in der Regel schon lange vor Erreichen dieser Grenze der Datenträger-Speicherplatz aus. Beispielsweise verfügt eine `m6g.large.search`-Instance über eine maximale Datenträgergröße von 512 GiB. Wenn Sie unter 80 % der Datenträgernutzung bleiben und die Größe Ihrer Shards bei 20 GiB liegt, können ungefähr 20 Shards untergebracht werden. Elasticsearch 7. x und höher sowie alle Versionen von OpenSearch haben ein Limit von 1.000 Shards pro Knoten. Um die maximalen Shards pro Knoten anzupassen, konfigurieren Sie die `cluster.max_shards_per_node`-Einstellung. Ein Beispiel finden Sie unter Cluster-Einstellungen.

Durch eine angemessene Dimensionierung der Shards bleiben Sie fast immer unter dieser Grenze, Sie können jedoch auch die Anzahl der Shards pro GiB des Java-Heaps prüfen. Auf einem

vorgegebenen Knoten sollten Sie nicht mehr als 25 Shards pro GB des Java-Heaps haben. Eine `m5.large.search`-Instance verfügt bspw. über einen 4-GiB-Heap, sodass jeder Knoten nicht mehr als 100 Shards haben sollte. Bei dieser Anzahl an Shards ist jeder Shard etwa 5 GiB groß, was weit unter unserer Empfehlung liegt.

Auswählen von Instance-Typen und Tests

Nachdem Sie Ihre Speicheranforderungen berechnet und die Anzahl der benötigten Shards ausgewählt haben, können Sie Hardware-Entscheidungen treffen. Hardware-Anforderungen variieren je nach Workload erheblich. Wir können jedoch einige grundlegende Empfehlungen bieten.

Im Allgemeinen entsprechen die Speicherlimits für jeden Instance-Typ der CPU-Leistung und dem Speicher, die Sie gegebenenfalls für geringe Workloads benötigen. Angenommen, eine `m6g.large.search`-Instance hat eine maximale EBS-Volume-Größe von 512 GiB, 2 vCPU-Prozessorkerne und 8 GiB Arbeitsspeicher. Wenn Ihr Cluster viele Shards hat, aufwändige Aggregationen ausführt, Dokumente häufig aktualisiert oder eine große Anzahl von Abfragen verarbeitet, sind diese Ressourcen möglicherweise für Ihre Anforderungen nicht ausreichend. Wenn Ihr Cluster in eine dieser Kategorien fällt, versuchen Sie es zunächst mit einer Konfiguration von eher 2 vCPU-Prozessorkernen und 8 GiB Arbeitsspeicher für je 100 GiB Ihrer Speicheranforderung.

> **Tip**
>
> Eine Zusammenfassung der Hardwareressourcen, die jedem Instance-Typ zugewiesen sind, finden Sie unter Amazon OpenSearch Service-Preise.

Dennoch sind auch diese Ressourcen möglicherweise nicht ausreichend. Einige OpenSearch Benutzer berichten, dass sie ein Vielfaches dieser Ressourcen benötigen, um ihre Anforderungen zu erfüllen. Um die richtige Hardware für Ihre Workloads zu finden, müssen Sie eine fundierte erste Einschätzung vornehmen, mit repräsentativen Workloads testen, anpassen und erneut testen.

Schritt 1: Machen Sie einen ersten Schätzwert

Zu Beginn empfehlen wir mindestens drei Knoten, um mögliche OpenSearch Probleme zu vermeiden, wie z. B. einen Split-Brain-Status (wenn ein Kommunikationsausfall dazu führt, dass ein Cluster zwei Master-Knoten hat). Wenn Sie drei dedizierte Hauptknoten haben, empfehlen wir immer noch mindestens zwei Datenknoten für die Replikation.

Schritt 2: Berechnen Sie den Speicherbedarf pro Knoten

Wenn Sie eine Speicheranforderung von 184 GiB haben und die empfohlene Mindestanzahl von drei Knoten, verwenden Sie die Gleichung 184/3 = 61 GiB, um den Speicherplatz zu ermitteln, die jeder Knoten benötigt. In diesem Beispiel könnten Sie drei `m6g.large.search`-Instances auswählen, die jeweils ein EBS-Speicher-Volume mit 90 GiB verwenden, sodass Sie über eine Sicherheitsreserve verfügen und Wachstum im Laufe der Zeit unterstützen können. Diese Konfiguration bietet 6 vCPU-Kerne und 24 GiB Arbeitsspeicher, sodass sie für leichtere Workloads geeignet ist.

Als größer ausgelegtes Beispiel nehmen Sie etwa eine Speicheranforderung von 14 TiB (14.336 GiB) Speicher und einen hohen Workload an. In diesem Fall können Sie damit beginnen, Tests mit 2 * 144 = 288 vCPU-Prozessorkernen und 8 * 144 = 1152 GiB Arbeitsspeicher zu beginnen. Diese Zahlen funktionieren für etwa 18 `i3.4xlarge.search`-Instances. Wenn Sie keinen schnellen, lokalen Speicher benötigen, können Sie auch 18 `r6g.4xlarge.search`-Instances mit jeweils einem EBS-Speicher-Volume mit 1 TiB testen.

Informationen zu Clustern mit Hunderten von Terabytes an Daten finden Sie unter the section called “Petabyte-Größe”.

Schritt 3: Führen Sie repräsentative Tests durch

Nach der Konfiguration des Clusters können Sie Ihre Indizes anhand der zuvor berechneten Anzahl von Shards hinzufügen, einige repräsentative Client-Tests anhand eines realistischen Datensatzes durchführen und CloudWatch Metriken überwachen, um zu sehen, wie der Cluster mit der Arbeitslast umgeht.

Schritt 4: Erfolg oder Iterieren

Wenn die Leistung Ihren Anforderungen entspricht, die Tests erfolgreich sind und die CloudWatch Metriken normal sind, ist der Cluster einsatzbereit. Denken Sie daran, CloudWatch Alarme einzurichten, um eine ungesunde Ressourcennutzung zu erkennen.

Wenn die Leistung nicht akzeptabel ist, Tests fehlschlagen oder `CPUUtilization` oder `JVMMemoryPressure` hoch sind, müssen Sie möglicherweise einen anderen Instance-Typ wählen (oder Instances hinzufügen) und die Tests fortsetzen. Wenn Sie Instances hinzufügen, OpenSearch wird die Verteilung der Shards im Cluster automatisch ausgeglichen.

Da es einfacher ist, die überschüssige Kapazität in einem überlasteten Cluster als das Defizit in einem zu wenig ausgelasteten Cluster zu messen, empfehlen wir, mit einem Cluster zu beginnen, der

größer ist als der, den Sie wahrscheinlich benötigen werden. Testen und skalieren Sie anschließend abwärts zu einem effizienten Cluster, der über die zusätzlichen Ressourcen verfügt, um einen stabilen Betrieb in Zeiten erhöhter Aktivität sicherzustellen.

Produktions-Cluster oder Cluster mit komplexen Zuständen profitieren von dedizierten Hauptknoten, die die Leistung und Cluster-Zuverlässigkeit verbessern.

Petabyte-Größe in Amazon OpenSearch Service

Amazon OpenSearch -Service-Domains bieten einen angefügten Speicher von bis zu 3 PB. Sie können eine Domäne mit 200 `i3.16xlarge.search` Instance-Typen mit jeweils 15 TB Speicher konfigurieren. Aufgrund des großen Unterschieds bei der Skalierung unterscheiden sich die Empfehlungen für Domänen dieser Größe von unseren allgemeinen Empfehlungen. In diesem Abschnitt werden Überlegungen bei der Erstellung von Domänen, Kosten, Speicher und Shard-Größe dargelegt.

Während dieser Abschnitts häufig auf die `i3.16xlarge.search` Instance-Typen verweist, können Sie verschiedene andere Instance-Typen verwenden, um 1 PB Gesamt-Domänenspeicher zu erreichen.

Domänen erstellen

Domains dieser Größe überschreiten das Standardlimit von 80 Instances pro Domain. Um eine Erhöhung der Serviceobergrenze von bis zu 200 Instances pro Domäne anzufordern, erstellen Sie einen Fall im AWS -Support-Center.

Preisgestaltung

Bevor Sie eine Domain dieser Größe erstellen, überprüfen Sie die Seite Amazon OpenSearch Service – Preise, um sicherzustellen, dass die damit verbundenen Kosten Ihren Erwartungen entsprechen. Überprüfen Sie the section called “UltraWarm Speicher” darauf, ob eine Hot-Warm-Architektur zu Ihrem Anwendungsfall passt.

Speicher

Die `i3`-Instance-Typen sind dafür konzipiert, um schnellen, lokalen nicht-flüchtigen Express (NVMe)-Speicher bereitzustellen. Da dieser lokale Speicher im Vergleich zu Amazon Elastic Block Store in der Regel Leistungsvorteile bietet, sind EBS-Volumes keine Option, wenn Sie diese Instance-Typen in OpenSearch Service auswählen. Wenn Sie lieber EBS-Speicher, verwenden Sie einen anderen Instance-Typ, z. B. `r6.12xlarge.search`.

Shard-Größe und -Anzahl

Eine gängige OpenSearch Richtlinie besteht darin, 50 GB pro Shard nicht zu überschreiten. Aufgrund der Anzahl der Shards, die für große Domänen und die verfügbaren Ressourcen für `i3.16xlarge.search`-Instances erforderlich sind, empfehlen wir eine Shard-Größe von 100 GB.

Wenn Sie beispielsweise 450 TB Quelldaten haben und ein Replikat verwenden wollen, liegt Ihr minimaler Speicherbedarf nahe 450 TB * 2 * 1,1/0,95 = 1,04 PB. Eine Erklärung dieser Berechnung finden Sie unter the section called “Berechnung der Speicheranforderungen”. Obwohl 1.04 PB / 15 TB = 70 Instances ergibt, sollten Sie 90 oder mehr `i3.16xlarge.search` Instances wählen, damit Sie eine Sicherheitsreserve, einen Deal mit Knotenfehlern haben und Abweichungen in der Datenmenge im Laufe der Zeit berücksichtigt werden. Von jeder Instance werden weitere 20 GiB zu den Mindestspeicheranforderungen hinzugefügt, aber bei Datenträgern dieser Größe sind 20 GiB nahezu vernachlässigbar.

Die Kontrolle der Anzahl der Shards ist schwierig. - OpenSearch Benutzer rotieren Indizes häufig täglich und behalten Daten ein oder zwei Wochen lang bei. In diesem Fall finden Sie es möglicherweise nützlich, zwischen "aktiven" und "inaktiven" Shards zu unterscheiden. Aktive Shards werden aktiv gelesen oder geschrieben. Inaktive Shards können einige Leseanforderungen bedienen, sind aber größtenteils im Leerlauf. Im Allgemeinen gilt, die Anzahl der aktiven Shards unten ein paar Tausend zu halten. Wenn sich die Anzahl der aktiven Shards 10.000 nähert, ist dies mit erheblichen Leistungs- und Stabilitätsrisiken verbunden.

Zum Berechnen der Anzahl der primären Shards verwenden Sie die folgende Formel: 450.000 GB * 1,1/100 GB pro Shard = 4,950 Shards. Eine Verdoppelung dieser Anzahl zur Berücksichtigung von Replikaten ergibt 9.900 Shards. Wenn alle Shards aktiv sind, stellt dies ein großes Problem dar. Wenn Sie jedoch die Indizes rotieren und nur 1/7 oder 1/14 der Shards an einem bestimmten Tag aktiv sind (1 414 bzw. 707 Shards), kann der Cluster gut funktionieren. Wie immer besteht der wichtigste Schritt bei der Dimensionierung und Konfiguration Ihrer Domäne darin, repräsentative Client-Tests unter Verwendung einer realistischen Datenmenge auszuführen.

Dedizierte Masterknoten in Amazon OpenSearch Service

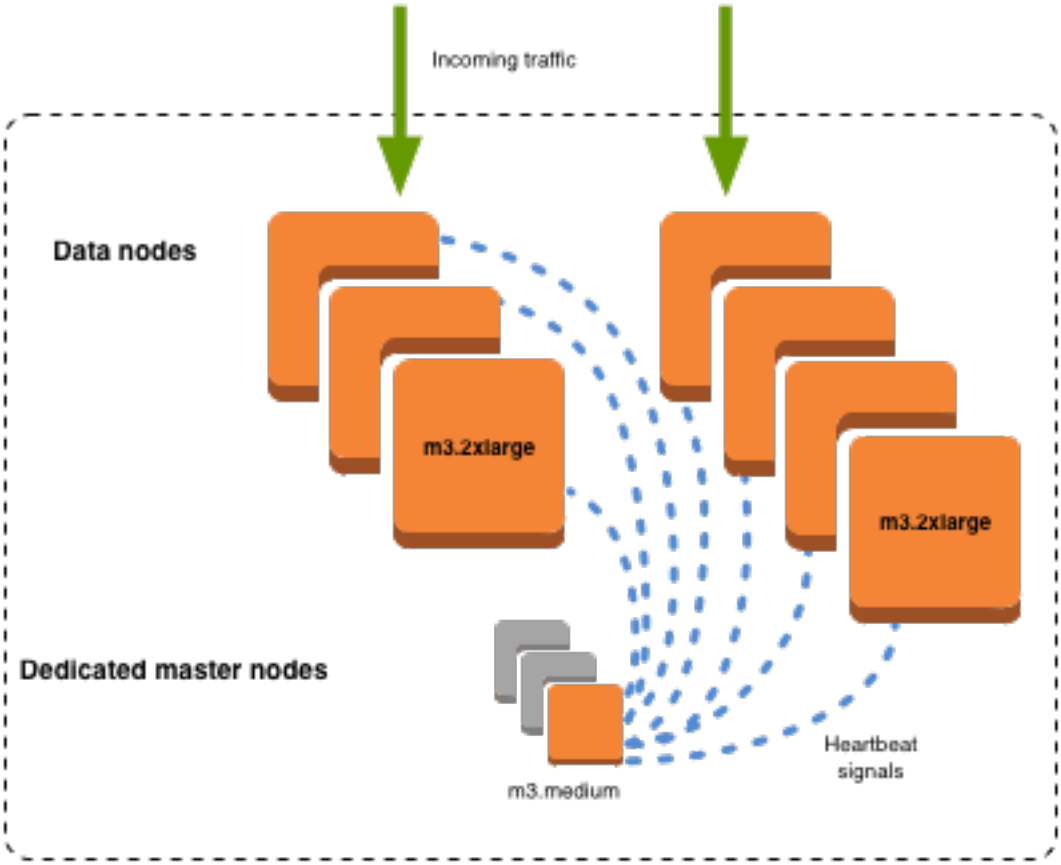
Amazon OpenSearch Service verwendet dedizierte Master-Knoten, um die Cluster-Stabilität zu erhöhen. Ein dedizierter Hauptknoten führt Cluster-Verwaltungsaufgaben aus, jedoch keine Daten hält oder auf Daten-Upload-Anforderungen reagiert. Diese Auslagerung von Cluster-

Verwaltungsaufgaben erhöht die Stabilität Ihrer Domain. Wie bei allen anderen Knotentypen zahlen Sie einen Stundensatz für jeden dedizierten Hauptknoten.

Dedizierte Hauptknoten führten die folgenden Cluster-Verwaltungsaufgaben aus:

- Nachverfolgung aller Knoten im Cluster
- Nachverfolgung der Indexanzahl im Cluster
- Nachverfolgung der Anzahl der Shards, die zu jedem Index gehören
- Pflege der Routing-Informationen für Knoten im Cluster
- Aktualisierung des Cluster-Status nach Statusänderungen, z. B. dem Erstellen eines Index und dem Hinzufügen oder Entfernen von Knoten im Cluster
- Replikation von Änderungen am Cluster-Status über alle Knoten im Cluster hinweg
- Überwachung der Integrität aller Cluster-Knoten, indem Funktionsmeldungen gesendet werden, also periodische Signale, die die Verfügbarkeit der Datenknoten im Cluster überwachen

Die folgende Abbildung zeigt eine OpenSearch Service-Domain mit 10 Instanzen. Sieben der Instances sind Datenknoten und drei sind dedizierte Hauptknoten. Nur einer der dedizierten Hauptknoten ist aktiv. Die beiden grauen dedizierte Hauptknoten sind als Sicherung vorgesehen, falls der aktive dedizierte Hauptknoten ausfällt. Alle Daten-Upload-Anforderungen werden von den sieben Datenknoten bedient und alle Cluster-Verwaltungsaufgaben werden vom aktiven dedizierten Hauptknoten übernommen.



Anzahl der dedizierten Hauptknoten auswählen

Wir empfehlen, Multi-AZ mit Standby zu verwenden, wodurch jeder OpenSearch Produktions-Servicedomäne drei dedizierte Masterknoten hinzugefügt werden. Wenn Sie mit Multi-AZ ohne Standby oder Single-AZ bereitstellen, empfehlen wir dennoch drei dedizierte Masterknoten. Wählen Sie niemals eine gerade Anzahl an dedizierten Hauptknoten. Berücksichtigen Sie bei der Auswahl der Anzahl dedizierter Hauptknoten Folgendes:

- Ein dedizierter Master-Knoten ist vom OpenSearch Service ausdrücklich verboten, da Sie für den Fall eines Fehlers kein Backup haben. Sie erhalten eine Validierungsausnahme, wenn Sie versuchen, eine Domain mit nur einem dedizierten Hauptknoten zu erstellen.
- Wenn Sie zwei dedizierte Hauptknoten haben, verfügt Ihr Cluster nicht über das erforderliche Knoten-Quorum für die Wahl eines neuen Hauptknotens bei einem Ausfall.

  Ein Quorum ist die Anzahl der dedizierten Hauptknoten / 2 + 1 (abgerundet auf die nächste ganze Zahl). In diesem Fall: 2/2 + 1 = 2. Da ein dedizierter Hauptknoten ausgefallen ist und nur

ein Backup vorhanden ist, verfügt der Cluster nicht über ein Quorum und kann keinen neuen Hauptknoten wählen.

- Drei dedizierte Hauptknoten, die empfohlene Anzahl, bieten zwei Backup-Knoten für den Fall eines Hauptknotenausfalls, und das erforderliche Quorum (2) für die Wahl eines neuen Hauptknotens.
- Vier dedizierte Hauptknoten bieten gegenüber dreien keine Vorteile und können Probleme verursachen, wenn Sie mehrere Availability Zones verwenden.
  - Wenn ein Hauptknoten ausfällt, haben Sie das Quorum (3), um einen neuen Hauptknoten zu wählen. Wenn zwei Knoten ausfallen, verlieren Sie dieses Quorum, genau wie bei drei dedizierten Hauptknoten.
  - In einer Konfiguration mit drei Availability Zonen verfügen zwei AZs über einen dedizierten Hauptknoten und eine AZ über zwei. Wenn diese AZ eine Störung hat, haben die verbleibenden beiden AZs nicht das erforderliche Quorum (3), um einen neuen Hauptknoten zu wählen.
- Fünf dedizierte Hauptknoten funktionieren ebenso wie drei und ermöglichen Ihnen, zwei Knoten zu verlieren und ein Quorum zu behalten. Da jedoch nur ein dedizierter Hauptknoten zu einem bestimmten Zeitpunkt aktiv ist, bedeutet diese Konfiguration, dass vier Leerlaufknoten bezahlt werden müssen. Nach Ansicht vieler Kunden ist ein derartiger Failover-Schutz übertrieben.

Wenn ein Cluster über eine gerade Anzahl von Knoten verfügt, die als Master in Frage kommen, OpenSearch und Elasticsearch-Versionen 7. x und später ignorieren einen Knoten, sodass die Abstimmungskonfiguration immer eine ungerade Zahl ist. In diesem Fall sind vier dedizierte Hauptknoten im Wesentlichen mit drei (und zwei mit einem) äquivalent.

> **Note**
>
> Wenn Ihr Cluster nicht über das erforderliche Quorum für die Wahl eines neuen Hauptknotens verfügt, schlagen Schreib- und Leseanforderungen an den Cluster fehl. Dieses Verhalten unterscheidet sich von der OpenSearch Standardeinstellung.

Auswählen von Instance-Typen für dedizierte Hauptknoten

Obwohl dedizierte Master-Knoten keine Such- und Abfrageanfragen verarbeiten, korreliert ihre Größe stark mit der Instanzgröße und der Anzahl der Instances, Indizes und Shards, die sie verwalten können. Für Produktionscluster empfehlen wir mindestens die folgenden Instance-Typen für dedizierte Master-Knoten.

Diese Empfehlungen basieren auf typischen Workloads und können je nach Ihren Anforderungen variieren. Cluster mit vielen Shards oder Feldzuordnungen profitieren von größeren Instance-Typen. Überwachen Sie die Metriken dedizierter Hauptknoten, um zu sehen, ob Sie einen größeren Instance-Typ verwenden müssen.

Instance-Anzahl	Hauptknoten-RAM-Größe	Maximal unterstützte Shard-Anzahl	Empfohlenes Minimum für den dedizierten Hauptknoten-Instance-Typ
1–10	8 GiB	10 K	`m5.large.search` oder `m6g.large.search`
11–30	16 GiB	30 K	`c5.2xlarge.search` oder `c6g.2xlarge.search`
31–75	32 GiB	40 000	`r5.xlarge.search` oder `r6g.xlarge.search`
76 – 125	64 GiB	75 K	`r5.2xlarge.search` oder `r6g.2xlarge.search`
126 – 200	128 GiB	75 K	`r5.4xlarge.search` oder `r6g.4xlarge.search`

- Weitere Informationen darüber, wie bestimmte Konfigurationsänderungen sich auf einen dedizierten Hauptknoten auswirken können, finden Sie unter the section called “Konfigurationsänderungen”.

- Weitere Informationen zu den Grenzwerten für die Anzahl der Instanzen finden Sie unter Kontingente für OpenSearch Dienstdomänen und Instanzen.
- Weitere Informationen zu bestimmten Instance-Typen, einschließlich vCPU, Arbeitsspeicher und Preisen, finden Sie unter Amazon OpenSearch Service-Preise.

Empfohlene CloudWatch Alarme für Amazon OpenSearch Service

CloudWatch Alarme führen eine Aktion aus, wenn eine CloudWatch Metrik für einen bestimmten Zeitraum einen bestimmten Wert überschreitet. Möglicherweise möchten Sie Ihnen eine E-Mail AWS senden, wenn Ihr Cluster-Integritätsstatus `red` länger als eine Minute andauert. Dieser Abschnitt enthält einige empfohlene Alarme für Amazon OpenSearch Service und wie Sie darauf reagieren können.

Sie können diese Alarme automatisch einrichten mit AWS CloudFormation. Einen Beispielstapel finden Sie im entsprechenden GitHubRepository.

> **Note**
>
> Wenn Sie den CloudFormation Stack bereitstellen, sind die `KMSKeyInaccessible` Alarme `KMSKeyError` und in einem bestimmten `Insufficient Data` Zustand vorhanden, da diese Metriken nur angezeigt werden, wenn bei einer Domain ein Problem mit ihrem Verschlüsselungsschlüssel auftritt.

Weitere Informationen zur Konfiguration von Alarmen finden Sie unter CloudWatchAmazon-Alarme erstellen im CloudWatch Amazon-Benutzerhandbuch.

Alarm	Problem
`ClusterStatus.red` Maximum ist >= 1 für 1 Minute, 1 Mal hintereinander	Mindestens ein primärer Shard und dessen Replikate sind keinem Knoten zugewiesen. Siehe the section called “Roter Cluster-Status”.
`ClusterStatus.yellow` Maximum ist >= 1	Mindestens ein Replikat-Shard ist nicht einem Knoten zugewiesen. Siehe the section called “Gelber Cluster-Status”.

Alarm	Problem
für 1 Minute, 5 Mal hintereinander	
`FreeStorageSpace` Minimum ist <= 20480 für 1 Minute, 1 Mal hintereinander	Ein Knoten in Ihrem Cluster hat nur noch 20 GiB freien Speicherplatz. Siehe the section called “Zu wenig verfügbarer Speicherplatz”. Dieser Wert wird in MiB angegeben, statt 20480 empfehlen wir deshalb eine Einstellung auf 25 % Ihres Speicherplatzes pro Knoten.
`ClusterIndexWritesBlocked` ist >= 1 für 5 Minuten, 1 Mal hintereinander	Ihr Cluster blockiert Schreibanforderungen. Siehe the section called “ClusterBlockException”.
`Nodes` Minimum ist < x für 1 Tag, 1 Mal hintereinander	x ist die Anzahl der Knoten in Ihrem Cluster. Dieser Alarm gibt an, dass mindestens ein Knoten in Ihrem Cluster für einen Tag nicht erreichbar war. Siehe the section called “Fehlgeschlagene Cluster-Knoten”.

`AutomatedSnapshotFailure` Maximum ist >= 1 für 1 Minute, 1 Mal hintereinander	Ein automatisierter Snapshot ist fehlgeschlagen. Dieser Fehler ist häufig das Ergebnis eines roten Cluster-Integritätsstatus. Siehe the section called “Roter Cluster-Status”.
	
	Für eine Zusammenfassung aller automatischen Snapshots und einige Informationen zu Ausfällen können Sie auch einen der folgenden Schritte ausprobieren:
	
	`GET domain_endpoint /_snapshot/cs-automated/_all`
	`GET domain_endpoint /_snapshot/cs-automated-enc/_all`

`CPUUtilization` oder `WarmCPUUtilization` Maximum ist >= 80 % für 15 Minuten, 3 Mal hintereinander	Eine 100%ige CPU-Auslastung kann manchmal auftreten, aber eine anhaltend hohe Auslastung ist problematisch. Ziehen Sie die Verwendung von größeren Instance-Typen oder das Hinzufügen von Instances in Betracht.

Alarm	Problem
`JVMMemory Pressure` Maximum ist >= 95 % für 1 Minute, 3 Mal hintereinander	Der Cluster könnte Fehler aufgrund von unzureichendem Speicherp latz erhalten, wenn die Nutzung zunimmt. Erwägen Sie eine vertikale Skalierung. OpenSearch Der Dienst verwendet die Hälfte des RAM einer Instanz für den Java-Heap, bis zu einer Heap-Größe von 32 GiB. Sie können Instances bis zu 64 GiB RAM vertikal skalieren. Dann können Sie eine horizontale Skalierung durchführen, indem Sie Instances hinzufügen.
`OldGenJVM MemoryPressure` Maximum ist >= 80 % für 1 Minute, 3 Mal hintereinander	
`MasterCPU Utilization` Maximum ist >= 50 % für 15 Minuten, 3 Mal hintereinander	Ziehen Sie die Verwendung von größeren Instance-Typen für Ihre dedizierten Hauptknoten in Betracht. Aufgrund ihrer Rolle für die Cluster-Stabilität und Blau/Grün-Bereitstellungen sollten dedizierte Hauptknoten eine geringere CPU-Nutzung als Datenknoten haben.
`MasterJVM MemoryPressure` Maximum ist >= 95 % für 1 Minute, 3 Mal hintereinander	
`MasterOld GenJVMMem oryPressure` Maximum ist >= 80 % für 1 Minute, 3 Mal hintereinander	
`KMSKeyError` ist >= 1 für 1 Minute, 1 Mal hintereinander	Der AWS KMS Verschlüsselungsschlüssel, der zum Verschlüsseln ruhender Daten in Ihrer Domain verwendet wird, ist deaktiviert. Reaktivie ren Sie es, um den normalen Betrieb wiederherzustellen. Weitere Informationen finden Sie unter the section called “Verschlüsselung im Ruhezustand”.

Alarm	Problem
`KMSKeyInaccessible` ist >= 1 für 1 Minute, 1 Mal hintereinander	Der AWS KMS Verschlüsselungsschlüssel, der zum Verschlüsseln von gespeicherten Daten in Ihrer Domain verwendet wird, wurde gelöscht oder der Service wurde nicht mehr gewährt. OpenSearch Für Domains, die sich in diesem Zustand befinden, ist die Wiederherstellung nicht möglich. Wenn Sie jedoch über einen manuellen Snapshot verfügen, können Sie diesen für die Migration zu einer neuen Domain verwenden . Weitere Informationen hierzu finden Sie unter the section called “Verschlüsselung im Ruhezustand”.
`shards.active` ist >= 30000 für 1 Minute, 1 Mal hintereinander	Die Gesamtzahl der aktiven primären und Replikat-Shards ist größer als 30.000. Möglicherweise rotieren Sie Ihre Indizes zu häufig. Erwägen Sie, ISM zu verwenden, um Indizes zu entfernen, sobald sie ein bestimmtes Alter erreichen.
5*xx* Alarme >= 10 % von `OpenSearchRequests` .	Ein oder mehrere Datenknoten sind möglicherweise überlastet oder Anfragen können innerhalb des Zeitraums im Leerlauf nicht abgeschlossen werden. Erwägen Sie, zu größeren Instance-Typen zu wechseln oder dem Cluster weitere Knoten hinzuzufügen. Bestätigen Sie Bewährte Methoden für Shard- und Cluster-Architektur.
`MasterReachableFromNode` Der Höchstwert ist < 1 für 5 Minuten, 1 Mal hintereinander	Dieser Alarm zeigt an, dass der Hauptknoten angehalten wurde oder nicht erreichbar ist. Diese Ausfälle sind in der Regel auf ein Problem mit der Netzwerkkonnektivität oder auf ein AWS Abhängigkeitsproblem zurückzuführen.
`ThreadpoolWriteQueue` Durchschnitt ist >= 100 für 1 Minute, 1 Mal hintereinander	Der Cluster erlebt eine hohe Indexierungs-Parallelität. Überprüfen und steuern Sie Indexierungsanforderungen oder erhöhen Sie die Clusterressourcen.

Alarm	Problem
`Threadpool SearchQueue` Durchschnitt ist >= 500 für 1 Minute, 1 Mal hintereinander	Der Cluster erlebt eine hohe Suchparallelität. Überlegen Sie, Ihren Cluster zu skalieren. Sie können auch die Größe der Suchwarteschlange erhöhen, aber eine übermäßige Erhöhung kann zu Fehlern außerhalb des Speichers führen.
`Threadpool SearchQueue` Maximum ist >= 5000 für 1 Minute, 1 Mal hintereinander	
Die Erhöhung der `Threadpool SearchRejected` SUMME beträgt >=1 {mathematischer Ausdruck DIFF ()} für 1 Minute, 1 Mal hintereinander	Diese Alarme benachrichtigen Sie über Domain-Probleme, die sich auf Leistung und Stabilität auswirken können.
Die Erhöhung von `Threadpool WriteRejected` SUM beträgt >=1 {mathematischer Ausdruck DIFF ()} für 1 Minute, 1 Mal hintereinander	

> **Note**
>
> Wenn Sie nur Metriken anzeigen möchten, siehe the section called “Überwachen von Cluster-Metriken”.

Andere Alarme, die Sie in Betracht ziehen könnten

Erwägen Sie, je nachdem, welche OpenSearch Servicefunktionen Sie regelmäßig nutzen, die folgenden Alarme zu konfigurieren.

Alarm	Problem
`WarmFreeStorageSpace` ist >= 10%	Sie haben 10% Ihres gesamten freien Warmspeichers erreicht. `WarmFreeStorageSpace` misst die Summe Ihres freien warmen Speicherplatzes in MiB. UltraWarm verwendet Amazon S3 anstelle von angeschlossenen Festplatten.
`HotToWarmMigrationQueueSize` ist >= 20 für 1 Minute, 3 Mal hintereinander	Eine große Anzahl von Indizes wird gleichzeitig vom Hot-in den Speicherbereich verschoben. UltraWarm Überlegen Sie, Ihren Cluster zu skalieren.
`HotToWarmMigrationSuccessLatency` ist >= 1 Tag, 1 Mal hintereinander	Konfigurieren Sie diesen Alarm so, dass Sie benachrichtigt werden, wenn die `HotToWarmMigrationSuccessCount` -x-Latenz mehr als 24 Stunden beträgt, wenn Sie versuchen, tägliche Indizes zu rollen.
`WarmJVMMemoryPressure` Maximum ist >= 95 % für 1 Minute, 3 Mal hintereinander	Der Cluster könnte Fehler aufgrund von unzureichendem Speicherplatz erhalten, wenn die Nutzung zunimmt. Erwägen Sie eine vertikale Skalierung. OpenSearch Der Dienst verwendet die Hälfte des RAM einer Instanz für den Java-Heap, bis zu einer Heap-Größe von 32 GiB. Sie können Instances bis zu 64 GiB RAM vertikal skalieren. Dann können Sie eine horizontale Skalierung durchführen, indem Sie Instances hinzufügen.
`WarmOldGenJVMMemoryPressure` Maximum ist >= 80 % für 1 Minute, 3 Mal hintereinander	

Alarm	Problem
`WarmToColdMigrationQueueSize` ist >= 20 für 1 Minute, 3 Mal hintereinander	Eine große Anzahl von Indizes wird gleichzeitig vom UltraWarm Cold Storage in den Cold Storage verschoben. Überlegen Sie, Ihren Cluster zu skalieren.
`HotToWarmMigrationFailureCount` ist >= 1 für 1 Minute, 1 Mal hintereinander	Migrationen können während Snapshots, Shard-Verlagerungen oder erzwungenen Zusammenführungen fehlschlagen. Fehler bei Snapshots oder Shard-Verlagerungen sind in der Regel auf Knotenfehler oder S3-Konnektivitätsprobleme zurückzuführen. Ein Mangel an Speicherplatz ist in der Regel die zugrunde liegende Ursache für Fehler bei erzwungenen Zusammenführungen.
`WarmToColdMigrationFailureCount` ist >= 1 für 1 Minute, 1 Mal hintereinander	Migrationen schlagen normalerweise fehl, wenn Versuche, Indexmeta daten auf Cold Storage zu migrieren, fehlschlagen. Fehler können auch auftreten, wenn der Warm-Indexcluster-Status entfernt wird.
`WarmToColdMigrationLatency` ist >= 1 Tag, 1 Mal hintereinander	Konfigurieren Sie diesen Alarm so, dass Sie benachrichtigt werden, wenn die `WarmToColdMigrationSuccessCount` -x-Latenz mehr als 24 Stunden beträgt, wenn Sie versuchen, tägliche Indizes zu rollen.
`AlertingDegraded` ist >= 1 für 1 Minute, 1 Mal hintereinander	Entweder ist der Warnungsindex rot, oder ein oder mehrere Knoten sind nicht im Zeitplan.
`ADPluginUnhealthy` ist >= 1 für 1 Minute, 1 Mal hintereinander	Das Plug-In zur Anomalieerkennung funktioniert nicht ordnungsgemäß, entweder aufgrund hoher Fehlerraten oder weil einer der verwendeten Indizes rot ist.

Alarm	Problem
`AsynchronousSearchFailureRate` ist >= 1 für 1 Minute, 1 Mal hintereinander	Mindestens eine asynchrone Suche ist in letzter Minute fehlgeschlagen, was wahrscheinlich bedeutet, dass der Koordinatorknoten fehlgeschlagen ist. Der Lebenszyklus einer asynchronen Suchanfrage wird ausschließlich auf dem Koordinatorknoten verwaltet. Wenn der Koordinator ausfällt, schlägt die Anforderung fehl.
`AsynchronousSearchStoreHealth` ist >= 1 für 1 Minute, 1 Mal hintereinander	Der Zustand des asynchronen Reaktionsspeichers für die asynchrone Suche im anhaltenden Index ist rot. Möglicherweise speichern Sie große asynchrone Antworten, die einen Cluster destabilisieren können. Versuchen Sie, Ihre asynchronen Suchantworten auf 10 MB oder weniger zu beschränken.
`SQLUnhealthy` ist >= 1 für 1 Minute, 3 Mal hintereinander	Das SQL-Plug-In gibt 5 Xx-Antwortcodes zurück oder übergibt eine ungültige DSL-Abfrage an. OpenSearch Beheben Sie Probleme mit den Anforderungen, die Ihre Clients an das Plug-in stellen.
`LTRStatus.red` ist >= 1 für 1 Minute, 1 Mal hintereinander	Mindestens einer der Indizes, die zum Ausführen des Plug-ins „Learning to Rank“ erforderlich sind, ist nicht funktionsfähig, da primäre Shards fehlen.

Allgemeine Referenz für Amazon OpenSearch Service

Amazon OpenSearch Service unterstützt eine Vielzahl von Instances, Vorgängen, Plugins und anderen Ressourcen.

Themen

Unterstützte Instance-Typen in Amazon OpenSearch Service

Amazon OpenSearch Service unterstützt die folgenden Instance-Typen. Nicht alle Regionen unterstützen alle Instance-Typen. Einzelheiten zur Verfügbarkeit finden Sie unter Amazon OpenSearch Service-Preise.

Weitere Informationen darüber, welcher Instance-Typ für Ihren Anwendungsfall am besten geeignet ist, finden Sie unter the section called “Größenanpassung von Domains”, the section called “EBS-Volume-Größenkontigente” und the section called “Netzwerk-Kontingente”.

Instance-Typen der aktuellen Generation

Für eine optimale Leistung empfehlen wir, die folgenden Instance-Typen zu verwenden, wenn Sie neue OpenSearch Service-Domains erstellen.

Instance-Typ	Instances	Einschränkungen
ODER 1	`or1.medium.search`	• Die OR1-Instance-Typen erfordern OpenSearch 2.11 oder höher. • OR1-Instances sind nur mit Master-Knoten anderer Graviton-Instance-Typen (C6g, M6g, R6g) kompatibel.

Instance-Typ	Instances	Einschränkungen
	or1.large.search or1.xlarge.search or1.2xlarge.search or1.4xlarge.search or1.8xlarge.search or1.12xlarge.search or1.16xlarge.search	

Instance-Typ	Instances	Einschränkungen

Im4gn	`im4gn.large.search`
	`im4gn.xlarge.search`
	`im4gn.2xlarge.search`
	`im4gn.4xlarge.search`
	`im4gn.8xlarge.search`
	`im4gn.16xlarge.search`
		• Die iM4GN-Instance-Typen erfordern Elasticsearch 7.9 oder höher oder eine beliebige Version von und unterstützen keine EBS-Speichervolumes. OpenSearch
		• iM4GN-Instances sind nur mit anderen Graviton-Instance-Typen (C6g, M6g, R6g, R6gd) kompatibel. Graviton- und Nicht-Graviton-Instances können nicht in demselben Cluster kombiniert werden.

Instance-Typ	Instances	Einschränkungen

C5	`c5.large.search`
	`c5.xlarge.search`
	`c5.2xlarge.search`
	`c5.4xlarge.search`
	`c5.9xlarge.search`
	`c5.18xlarge.search`
		Die C5-Instance-Typen erfordern Elasticsearch 5.1 oder höher oder eine beliebige Version von. OpenSearch

Instance-Typ	Instances	Einschränkungen

C6g	`c6g.large.search`
	`c6g.xlarge.search`
	`c6g.2xlarge.search`
	`c6g.4xlarge.search`
	`c6g.8xlarge.search`
	`c6g.12xlarge.search`
		• Die C6g-Instanztypen erfordern Elasticsearch 7.9 oder höher oder eine beliebige Version von. OpenSearch
		• C6g-Instances sind nur mit anderen Graviton-Instance-Typen (iM4GN, M6G, R6g, R6gd) kompatibel. Graviton- und Nicht-Graviton-Instances können nicht in demselben Cluster kombiniert werden.

Instance-Typ	Instances	Einschränkungen

I3	`i3.large.search`
	`i3.xlarge.search`
	`i3.2xlarge.search`
	`i3.4xlarge.search`
	`i3.8xlarge.search`
	`i3.16xlarge.search`
		Die I3-Instance-Typen erfordern Elasticsearch 5.1 oder höher oder eine beliebige Version von und unterstützen keine EBS-Speic hervolumes. OpenSearch

M5	`m5.large.search`
	`m5.xlarge.search`
	`m5.2xlarge.search`
	`m5.4xlarge.search`
	`m5.12xlarge.search`
		Die M5-Instance-Typen erfordern Elasticsearch 5.1 oder höher oder eine beliebige Version von. OpenSearch

Instance-Typ	Instances	Einschränkungen

M6g	`m6g.large.search`
	`m6g.xlarge.search`
	`m6g.2xlarge.search`
	`m6g.4xlarge.search`
	`m6g.8xlarge.search`
	`m6g.12xlarge.search`
		• Die M6g-Instanztypen erfordern Elasticsearch 7.9 oder höher oder eine beliebige Version von. OpenSearch
		• M6g-Instances sind nur mit anderen Graviton-Instance-Typen (iM4GN, C6g, R6g, R6gd) kompatibel. Graviton- und Nicht-Graviton-Instances können nicht in demselben Cluster kombiniert werden.

Instance-Typ	Instances	Einschränkungen

R5	`r5.large.search`
	`r5.xlarge.search`
	`r5.2xlarge.search`
	`r5.4xlarge.search`
	`r5.12xlarge.search`
		Die R5-Instance-Typen erfordern Elasticsearch 5.1 oder höher oder eine beliebige Version von. OpenSearch

Instance-Typ	Instances	Einschränkungen

R6g	`r6g.large.search`
	`r6g.xlarge.search`
	`r6g.2xlarge.search`
	`r6g.4xlarge.search`
	`r6g.8xlarge.search`
	`r6g.12xlarge.search`
		• Die R6g-Instanztypen erfordern Elasticsearch 7.9 oder höher oder eine beliebige Version von. OpenSearch
		• R6g-Instances sind nur mit anderen Graviton-Instance-Typen (iM4GN, C6G, M6g, R6gd) kompatibel. Graviton- und Nicht-Graviton-Instances können nicht in demselben Cluster kombiniert werden.

Instance-Typ	Instances	Einschränkungen

R6gd	`r6gd.large.search`
	`r6gd.xlarge.search`
	`r6gd.2xlarge.search`
	`r6gd.4xlarge.search`
	`r6gd.8xlarge.search`
	`r6gd.12xlarge.search`
	`r6gd.16xlarge.search`
		• Die R6gd-Instance-Typen erfordern Elasticsearch 7.9 oder höher oder eine beliebige Version von und unterstützen keine EBS-Speichervolumes. OpenSearch
		• R6gd-Instances sind nur mit anderen Graviton-Instance-Typen (iM4gn, C6g, M6g, R6g) kompatibel. Graviton- und Nicht-Graviton-Instances können nicht in demselben Cluster kombiniert werden.

Instance-Typ	Instances	Einschränkungen
T3	`t3.small.search` `t3.medium.search`	• Die T3-Instance-Typen erfordern Elasticsearch 5.6 oder höher oder eine beliebige Version von. OpenSearch • Sie können T3-Instance-Typen nur verwenden, wenn Ihre Domain ohne Standby bereitgestellt wird. Weitere Informationen finden Sie unter the section called “Multi-AZ ohne Standby”. • Sie können T3-Instance-Typen nur verwenden, wenn die Anzahl der Instanzen für Ihre Domain 10 oder weniger beträgt. • Die T3-Instance-Typen unterstützen weder UltraWarm Storage, Cold Storage noch Auto-Tune.

Instance-Typen der vorherigen Generation

OpenSearch Der Service bietet Instance-Typen der vorherigen Generation für Benutzer, die ihre Anwendungen entsprechend optimiert haben und noch kein Upgrade durchgeführt haben. Wir raten dazu, Instance-Typen der aktuellen Generation zu verwenden, um von der besten Leistung zu profitieren, die folgenden Instance-Typen der vorherigen Generation werden aber weiterhin unterstützt.

Instance-Typ	Instances	Einschränkungen

C4	`c4.large.search`
	`c4.xlarge.search`
	`c4.2xlarge.search`
	`c4.4xlarge.search`	

Instance-Typ	Instances	Einschränkungen
	c4.8xlarge.search	
I2	i2.xlarge.search i2.2xlarge.search	
M3	m3.medium.search m3.large.search m3.xlarge.search m3.2xlarge.search	• Die M3-Instance-Typen unterstützen keine Verschlüsselung von Daten im Ruhezustand, differenzierte Zugriffskontrolle oder Cluster-übergreifende Suche. • Für die M3-Instance-Typen gelten je nach OpenSearch Version zusätzliche Einschränkungen. Weitere Informationen hierzu finden Sie unter the section called “Ungültiger M3-Instance-Typ”.
M4	m4.large.search m4.xlarge.search m4.2xlarge.search m4.4xlarge.search m4.10xlarge.search	

Instance-Typ	Instances	Einschränkungen
R3	r3.large.search r3.xlarge.search r3.2xlarge.search r3.4xlarge.search r3.8xlarge.search	Die R3-Instance-Typen unterstützen keine Verschlüsselung von Daten im Ruhezustand oder differenzierte Zugriffskontrolle.
R4	r4.large.search r4.xlarge.search r4.2xlarge.search r4.4xlarge.search r4.8xlarge.search r4.16xlarge.search	

Instance-Typ	Instances	Einschränkungen

T2	`t2.micro.search`
	`t2.small.search`
	`t2.medium.search`
		• Sie können die T2-Instance-Typen nur dann verwenden, wenn die Anzahl der Instances für Ihre Domain zehn oder weniger beträgt.
		• Der Instance-Typ `t2.micro.search` unterstützt nur Elasticsearch 1.5 und 2.3.
		• Die T2-Instance-Typen unterstützen keine Verschlüsselung von Daten im Ruhezustand, detaillierte Zugriffskontrolle, UltraWarm Speicherung, Cold Storage, clusterübergreifende Suche oder Auto-Tune.

> **Tip**
>
> Wir empfehlen oft verschiedene Instance-Typen für dedizierte Hauptknoten und Datenknoten.

Funktionen nach Engine-Version in Amazon OpenSearch Service

Für viele OpenSearch Servicefunktionen ist eine OpenSearch Mindestversion oder eine ältere Elasticsearch OSS-Version erforderlich. Wenn Sie die Mindestversion für eine Funktion erfüllen, die Funktion jedoch in Ihrer Domain nicht verfügbar ist, aktualisieren Sie die Service-Software.

Funktion	Erforderliche Mindestversion OpenSearch	Erforderliche Mindestversion von Elasticsearch
VPC-Unterstützung	1,0	1,0
HTTPS für den gesamten Datenverkehr zur		

Funktion	Erforderliche Mindestversion OpenSearch	Erforderliche Mindestversion von Elasticsearch
Domain erforderlich		
Multi-AZ-Unterstützung		
Dedizierte Hauptknoten		
Benutzerdefinierte Pakete		
Benutzerdefinierte Endpunkte		
Veröffentlichen von Slow-Protokollen		
Veröffentlichen von Fehler-Protokollen	1,0	5.1
Verschlüsselung gespeicherter Daten		

Funktion	Erforderliche Mindestversion OpenSearch	Erforderliche Mindestversion von Elasticsearch
Cognito-Authentifizierung für Dashboards OpenSearch		
Direkte Upgrades		
Kuratoren-Unterstützung	Nicht enthalten	5.1
Stündliche automatische Snapshots	1,0	5.3
Keine Verschlüsselung ode-to-node	1,0	6.0
Java-Unterstützung für High-Level-REST-Clients		
HTTP-Anfragen und Antwort-Komprimierung		

Funktion	Erforderliche Mindestversion OpenSearch	Erforderliche Mindestversion von Elasticsearch
Warnfunktion	1,0	6.2
SQL	1,0	6,5
Cluster-übergreifende Suche	1,0	6.7
Differenzierte Zugriffskontrolle		
SAML-Authentifizierung für Dashboards OpenSearch		
Automatische Optimierung		
Remote-Neuindexierung		
UltraWarm	1,0	6.8
Indexstatusmanagement		

Funktion	Erforderliche Mindestversion OpenSearch	Erforderliche Mindestversion von Elasticsearch
k-NN nach euklidischer Entfernung	1,0	7.1
Anomaliee rkennung	1,0	7.4
k-NN nach Kosinus-Ä hnlichkeit	1,0	7.7
Learning to Rank		
Piped Processing Language	1,0	7.9
OpenSearc h Dashboard s, Berichte		
OpenSearc h Dashboard s Trace Analytics		
ARM-basie rte Graviton-Instances		
Cold Storage		

Funktion	Erforderliche Mindestversion OpenSearch	Erforderliche Mindestversion von Elasticsearch
Hamming-Distanz, L1-Norm-Distanz und Painless-Scripting für k-NN	1,0	7.10
Asynchrone Suche		
Indextransformationen	1,0	Nicht enthalten
Cluster-übergreifende Replikation	1.1	7,10
ML Commons	1.3	Nicht enthalten
Benachrichtigungen	2.3	Nicht enthalten
Suche zu einem bestimmten Zeitpunkt	2.5	Nicht enthalten
Pipelines durchsuchen	2.9	Nicht enthalten

Funktion	Erforderliche Mindestversion OpenSearch	Erforderliche Mindestversion von Elasticsearch
Konnektoren für maschinelles Lernen	2.9	Nicht enthalten
Multimodale semantische Suche	2.11	Nicht enthalten
Direkte Abfrage von Datenquellen für Amazon S3	2.11	Nicht enthalten

Weitere Informationen zu Plug-ins, die einige dieser Funktionen und zusätzliche Funktionalität ermöglichen, finden Sie unter the section called “Plug-ins nach Engine-Version”. Informationen zur OpenSearch API für jede Version finden Sie unter. the section called “Unterstützte Vorgänge”

Plugins nach Engine-Version in Amazon OpenSearch Service

Amazon OpenSearch Service-Domains werden mit Plug-ins aus der OpenSearch Community vorkonfiguriert geliefert. Der Service stellt Plugins automatisch für Sie bereit und verwaltet sie. Je nachdem, welche Version OpenSearch oder welches Legacy-Elasticsearch-Betriebssystem Sie für Ihre Domain auswählen, werden jedoch unterschiedliche Plugins bereitgestellt.

In der folgenden Tabelle sind die Plugins nach OpenSearch Version sowie die kompatiblen Versionen der Legacy-Elasticsearch-Betriebssysteme aufgeführt. Sie enthält nur Plugins, mit denen Sie möglicherweise interagieren — sie ist nicht umfassend. OpenSearch Service verwendet zusätzliche Plug-ins, um die Kernfunktionen des Dienstes zu aktivieren, z. B. das S3 Repository-Plugin für Snapshots und das OpenSearchPerformance Analyzer-Plugin für Optimierung und Überwachung. Für eine vollständige Liste aller Plug-Ins, die auf Ihrer Domain ausgeführt werden, stellen Sie folgende Anfrage:

```
GET _cat/plugins?v
```

Plug-In	Erforderliche Mindestversion OpenSearch	Mindestens erforderliche Elasticsearch-Version
ICU Analysis	1,0	In allen Domains enthalten
Japanese (kuromoji) Analysis		
Phonetic Analysis	1,0	2.3
Seunjeon Korean Analysis	1,0	5.1
Smart Chinese Analysis		
Stempel Polish Analysis		
Ingest Attachment Processor		
Ingest User Agent Processor		
Mapper Murmur3		

Plug-In	Erforderliche Mindestversion OpenSearch	Mindestens erforderliche Elasticsearch-Version
Mapper Size	1,0	5.3
Ukrainische Analyse		
OpenSearch Warnung	1,0	6.2
OpenSearch SQL	1,0	6,5
OpenSearch Sicherheit	1,0	6.7
OpenSearch Indexstatusmanagement	1,0	6.8
OpenSearch k-NN	1,0	7.1
OpenSearch Erkennung von Anomalien	1,0	7.4
IK-Analyse (Chinesisch)	1,0	7.7
Vietnamesische Analyse		

Plug-In	Erforderliche Mindestversion OpenSearch	Mindestens erforderliche Elasticsearch-Version
Thai Analyse		
Learning to Rank		
OpenSearch asynchrone Suche	1,0	7.10
OpenSearch Clusterübergreifende Replikation	1.1	7.10
OpenSearch Beobachtbarkeit	1.2	Nicht unterstützt
Nori-Analyse	1.3	Nicht unterstützt
Pinyin-Analyse	1.3	Nicht unterstützt
STConvert	1.3	Nicht unterstützt
Sudachi-Analyse	1.3	Nicht unterstützt
ML Commons	1.3	Nicht unterstützt

Plug-In	Erforderliche Mindestversion OpenSearch	Mindestens erforderliche Elasticsearch-Version
OpenSearch Benachrichtigungen	2.3	Nicht unterstützt
Sicherheitsanalysen	2.5	Nicht unterstützt
Neuronale Suche	2.9	Nicht unterstützt
Amazon Personalize Search Ranking	2.9	Nicht unterstützt
Hebräische Analyse	2.11	Nicht unterstützt
HanP	2.11	Nicht unterstützt

Optionale Plug-ins

Zusätzlich zu den vorinstallierten Standard-Plugins unterstützt Amazon OpenSearch Service mehrere optionale Sprachanalyse-Plugins. Sie können das AWS Management Console und verwenden AWS CLI , um ein Plugin einer Domain zuzuordnen, ein Plugin von einer Domain zu trennen und alle Plugins aufzulisten. Ein optionales Plugin-Paket ist mit einer bestimmten OpenSearch Version kompatibel und kann nur Domains mit dieser Version zugeordnet werden.

Beachten Sie, dass beim Sudachi-Plugin, wenn Sie eine Wörterbuchdatei neu zuordnen, dies nicht sofort der Domain entspricht. Das Wörterbuch wird aktualisiert, wenn die nächste blaue/grüne Bereitstellung im Rahmen einer Konfigurationsänderung oder eines anderen Updates auf der Domain ausgeführt wird. Alternativ können Sie ein neues Paket mit den aktualisierten Daten erstellen, mit diesem neuen Paket einen neuen Index erstellen, den vorhandenen Index erneut mit dem neuen Index indizieren und dann den alten Index löschen. Wenn Sie den Ansatz der Neuindizierung bevorzugen, verwenden Sie einen Indexalias, damit Ihr Datenverkehr nicht unterbrochen wird.

Optionale Plugins verwenden den `ZIP-PLUGIN` Pakettyp. Weitere Hinweise zu optionalen Plug-ins finden Sie unterthe section called “Benutzerdefinierte Pakete”.

Unterstützte Vorgänge in Amazon OpenSearch Service

OpenSearch Der Service unterstützt viele Versionen OpenSearch und ältere Versionen von Elasticsearch OSS. In den folgenden Abschnitten werden die Operationen beschrieben, die OpenSearch Service für jede Version unterstützt.

Themen

- Elasticsearch Version 6.3
- Elasticsearch Version 6.2
- Elasticsearch Version 6.0
- Elasticsearch Version 5.6
- Elasticsearch Version 5.5
- Elasticsearch Version 5.3
- Elasticsearch Version 5.1
- Elasticsearch Version 2.3
- Elasticsearch Version 1.5

Erwähnenswerte API-Unterschiede

Einstellungen und Statistiken

OpenSearch Der Service akzeptiert nur PUT-Anfragen an die `_cluster/settings` API, die das „flache“ Einstellungsformular verwenden. Es lehnt Anforderungen ab, die die ausgeschriebene Form der Einstellungen verwenden.

```
// Accepted
PUT _cluster/settings
{
  "persistent" : {
    "action.auto_create_index" : false
  }
}

// Rejected
PUT _cluster/settings
{
  "persistent": {
    "action": {
      "auto_create_index": false
    }
  }
}
```

Der High-Level-Java-REST-Client verwendet die ausgeschriebene Form. Wenn Sie also Einstellungsanforderungen senden müssen, verwenden Sie den Low-Level-Client.

Vor Elasticsearch 5.3 unterstützte die `_cluster/settings` API auf OpenSearch Service-Domains nur die PUT HTTP-Methode, nicht die GET Methode. OpenSearch und spätere Versionen von Elasticsearch unterstützen die GET Methode, wie im folgenden Beispiel gezeigt:

```
GET https://domain-name.region.es.amazonaws.com/_cluster/settings?pretty
```

Hier ist ein Rückgabebeispiel:

```
{
  "persistent": {
    "cluster": {
      "routing": {
        "allocation": {
          "cluster_concurrent_rebalance": "2",
          "node_concurrent_recoveries": "2",
          "disk": {
            "watermark": {
              "low": "1.35gb",
              "flood_stage": "0.45gb",
              "high": "0.9gb"
            }
          },
          "node_initial_primarirecoveries": "4"
        }
      }
    },
    "indices": {
      "recovery": {
        "max_bytper_sec": "40mb"
      }
    }
  }
}
```

Wenn Sie die Antworten eines OpenSearch Open-Source-Clusters und eines OpenSearch Dienstes für bestimmte Einstellungs- und Statistik-APIs vergleichen, stellen Sie möglicherweise fest, dass Felder fehlen. OpenSearch Der Dienst unkennzeichnet bestimmte Informationen, die interne Daten des Dienstes offenlegen, z. B. den Datenpfad des Dateisystems von `_nodes/stats` oder den Namen und die Version des Betriebssystems. `_nodes`

Shrink

Die `_shrink`-API kann dazu führen, dass Upgrades, Konfigurationsänderungen und Domain-Löschvorgänge fehlschlagen. Wir empfehlen Ihnen nicht, sie auf Domains zu verwenden, die mit Elasticsearch Version 5.3 oder 5.1 ausführt werden. Diese Versionen beinhalten einen Fehler, der dazu führen kann, dass Snapshot-Wiederherstellungen von geschrumpften Indizes fehlschlagen.

Wenn Sie die `_shrink` API auf anderen Elasticsearch oder anderen OpenSearch Versionen verwenden, stellen Sie die folgende Anfrage, bevor Sie den Verkleinerungsvorgang starten:

```
PUT https://domain-name.region.es.amazonaws.com/source-index/_settings
{
  "settings": {
    "index.routing.allocation.require._name": "name-of-the-node-to-shrink-to",
    "index.blocks.read_only": true
  }
}
```

Nach dem Abschließen der Shrink-Operation senden Sie dann folgende Anforderungen:

```
PUT https://domain-name.region.es.amazonaws.com/source-index/_settings
{
  "settings": {
    "index.routing.allocation.require._name": null,
    "index.blocks.read_only": false
  }
}

PUT https://domain-name.region.es.amazonaws.com/shrunken-index/_settings
{
  "settings": {
    "index.routing.allocation.require._name": null,
    "index.blocks.read_only": false
  }
}
```

OpenSearch Version 2.13

Für OpenSearch 2.13 unterstützt OpenSearch Service die folgenden Operationen. Informationen zu den meisten Vorgängen finden Sie in der OpenSearchREST-API-Referenz oder in der API-Referenz für das jeweilige Plugin.

- Alle Operationen im Index-Pfad (bspw. */index-name* /_forcemerge , */index-name* /update/*id* und */index-name* /_close)
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (außer /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings für mehrere Eigenschaften[4]:
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - cluster.max_shards_per_node
  - cluster.search.request.slowlog.level
- /_delete_by_query [1]
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_ltr
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_plugins/_asynchronous_search
- /_plugins/_alerting
- /_plugins/_anomaly_detection
- /_plugins/_ism
- /_plugins/_ml
- /_plugins/_notifications
- /_plugins/_ppl
- /_plugins/_security
- /_plugins/_security_analytics
- /_plugins/_sm
- /_plugins/_sql
- /_percolate
- /_rank_eval
- /_refresh
- /_reindex [1]
- /_render
- /_resolve/index
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search/pipeline
- /_search/point_in_time
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

  - `cluster.search.request.slowlog.threshold.warn`
  - `cluster.search.request.slowlog.threshold.info`
  - `cluster.search.request.slowlog.threshold.debug`
  - `cluster.search.request.slowlog.threshold.trace`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_dashboards`

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Anforderungstext und nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Verweist auf die `PUT`-Methode. Weitere Information zur `GET`-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen OpenSearch Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.

OpenSearch Version 2.11

Für OpenSearch 2.11 unterstützt OpenSearch Service die folgenden Operationen. Informationen zu den meisten Vorgängen finden Sie in der OpenSearchREST-API-Referenz oder in der API-Referenz für das jeweilige Plugin.

- Alle Operationen im Index-Pfad (bspw. */index-name* / _forcemerge , */index-name* /update/*id* und */index-name* /_close)
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (außer /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings für mehrere Eigenschaften[4]:
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
- /_delete_by_query [1]
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_ltr
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_plugins/_asynchronous_search
- /_plugins/_alerting
- /_plugins/_anomaly_detection
- /_plugins/_ism
- /_plugins/_ml
- /_plugins/_notifications
- /_plugins/_ppl
- /_plugins/_security
- /_refresh
- /_reindex [1]
- /_render
- /_resolve/index
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search/pipeline
- /_search/point_in_time
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

- indices.breaker.total.limit
- cluster.max_shards_per_node
- /_cluster/state
- /_cluster/stats
- /_count
- /_dashboards
- /_plugins/_security_analytics
- /_plugins/_sm
- /_plugins/_sql
- /_percolate
- /_rank_eval

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des /_tasks-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für /_search/scroll mit einem Nachrichtentext müssen "Content-Length" im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in scroll_id Werten zu vermeiden, verwenden Sie den Anforderungstext und nicht die Abfragezeichenfolge, um scroll_id Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Verweist auf die PUT-Methode. Weitere Information zur GET-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen OpenSearch Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.

OpenSearch Version 2.9

Für OpenSearch 2.9 unterstützt OpenSearch Service die folgenden Operationen. Informationen zu den meisten Vorgängen finden Sie in der OpenSearchREST-API-Referenz oder in der API-Referenz für das jeweilige Plugin.

- Alle Operationen im Index-Pfad (bspw. /*index-name* /
- /_delete_by_query [1]
- /_explain
- /_refresh
- /_reindex [1]

_forcemerge , */index-name* /update/*id* und */index-name* /_close)

- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (außer /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings für mehrere Eigenschaften[4]:
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - cluster.max_shards_per_node
- /_cluster/state
- /_cluster/stats
- /_count
- /_dashboards
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_ltr
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_plugins/_asynchronous_search
- /_plugins/_alerting
- /_plugins/_anomaly_detection
- /_plugins/_ism
- /_plugins/_ml
- /_plugins/_notifications
- /_plugins/_ppl
- /_plugins/_security
- /_plugins/_security_analytics
- /_plugins/_sm
- /_plugins/_sql
- /_percolate
- /_rank_eval
- /_render
- /_resolve/index
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search/pipeline
- /_search/point_in_time
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Anforderungstext und nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Verweist auf die PUT-Methode. Weitere Information zur GET-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen OpenSearch Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.

OpenSearch Version 2.7

Für OpenSearch 2.7 unterstützt OpenSearch Service die folgenden Operationen. Informationen zu den meisten Vorgängen finden Sie in der OpenSearchREST-API-Referenz oder in der API-Referenz für das jeweilige Plugin.

- Alle Operationen im Index-Pfad (bspw. */index-name* `/_forcemerge` , */index-name* `/update/`*id* und */index-name* `/_close`)
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (außer `/_cat/nodeattrs`)
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_ltr`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_resolve/index`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search/point_in_time`
- `/_search profile`
- `/_shard_stores`

- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` für mehrere Eigenschaften[4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
  - `cluster.max_shards_per_node`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_dashboards`
- `/_nodes`
- `/_plugins/_asynchronous_search`
- `/_plugins/_alerting`
- `/_plugins/_anomaly_detection`
- `/_plugins/_ism`
- `/_plugins/_ml`
- `/_plugins/_notifications`
- `/_plugins/_ppl`
- `/_plugins/_security`
- `/_plugins/_security_analytics`
- `/_plugins/_sm`
- `/_plugins/_sql`
- `/_percolate`
- `/_rank_eval`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Anforderungstext und nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.

4. Verweist auf die PUT-Methode. Weitere Information zur GET-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen OpenSearch Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.

OpenSearch Version 2.5

Für OpenSearch 2.5 unterstützt OpenSearch Service die folgenden Operationen. Informationen zu den meisten Vorgängen finden Sie in der OpenSearchREST-API-Referenz oder in der API-Referenz für das jeweilige Plugin.

- Alle Operationen im Index-Pfad (bspw. */index-name* /_forcemerge , */index-name* /update/*id* und */index-name* /_close)
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (außer /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings für mehrere Eigenschaften[4]:
  - action.auto_create_index
- /_delete_by_query [1]
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_ltr
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_plugins/_asynchronous_search
- /_plugins/_alerting
- /_plugins/_anomaly_detection
- /_plugins/_ism
- /_plugins/_ml
- /_refresh
- /_reindex [1]
- /_render
- /_resolve/index
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search/point_in_time
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

- `action.search.shard_count.limit`
- `indices.breaker.fielddata.limit`
- `indices.breaker.request.limit`
- `indices.breaker.total.limit`
- `cluster.max_shards_per_node`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_dashboards`
- `/_plugins/_notifications`
- `/_plugins/_ppl`
- `/_plugins/_security`
- `/_plugins/_security_analytics`
- `/_plugins/_sm`
- `/_plugins/_sql`
- `/_percolate`
- `/_rank_eval`

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Anforderungstext und nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Verweist auf die `PUT`-Methode. Weitere Information zur `GET`-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen OpenSearch Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.

OpenSearch Version 2.3

Für OpenSearch 2.3 unterstützt OpenSearch Service die folgenden Operationen. Informationen zu den meisten Vorgängen finden Sie in der OpenSearchREST-API-Referenz oder in der API-Referenz für das jeweilige Plugin.

- Alle Operationen im Index-Pfad (bspw. */index-name* / _forcemerge , */index-name* /update/*id* und */index-name* /_close)
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (außer /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings für mehrere Eigenschaften[4]:
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
- /_delete_by_query [1]
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_ltr
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_plugins/_asynchronous_search
- /_plugins/_alerting
- /_plugins/_anomaly_detection
- /_plugins/_ism
- /_plugins/_ml
- _plugins/_notifications
- /_plugins/_ppl
- /_plugins/_security
- /_plugins/_sql
- /_refresh
- /_reindex [1]
- /_render
- /_resolve/index
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

- indices.breaker.total.limit
- cluster.max_shards_per_node
- /_cluster/state
- /_cluster/stats
- /_count
- /_dashboards
- /_percolate
- /_rank_eval

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des /_tasks-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für /_search/scroll mit einem Nachrichtentext müssen "Content-Length" im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in scroll_id Werten zu vermeiden, verwenden Sie den Anforderungstext und nicht die Abfragezeichenfolge, um scroll_id Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Verweist auf die PUT-Methode. Weitere Information zur GET-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen OpenSearch Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.

OpenSearch Version 1.3

Für OpenSearch 1.3 unterstützt OpenSearch Service die folgenden Operationen. Informationen zu den meisten Vorgängen finden Sie in der OpenSearchREST-API-Referenz oder in der API-Referenz für das jeweilige Plugin.

- Alle Operationen im Index-Pfad (bspw. /*index-name* /
- /_delete_by_query [1]
- /_explain
- /_refresh
- /_reindex [1]

_forcemerge , */index-name* /update/*id* und */index-name* /_close)

- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (außer /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings für mehrere Eigenschaften[4]:
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - cluster.max_shards_per_node
- /_cluster/state
- /_cluster/stats
- /_count
- /_dashboards
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_ltr
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_plugins/_asynchronous_search
- /_plugins/_alerting
- /_plugins/_anomaly_detection
- /_plugins/_ism
- /_plugins/_ml
- /_plugins/_ppl
- /_plugins/_security
- /_plugins/_sql
- /_percolate
- /_rank_eval
- /_render
- /_resolve/index
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Anforderungstext und nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Verweist auf die PUT-Methode. Weitere Information zur GET-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen OpenSearch Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.

OpenSearch Version 1.2

Für OpenSearch 1.2 unterstützt OpenSearch Service die folgenden Operationen. Informationen zu den meisten Vorgängen finden Sie in der OpenSearchREST-API-Referenz oder in der API-Referenz für das jeweilige Plugin.

- Alle Operationen im Index-Pfad (bspw. */index-name* / `_forcemerge` , */index-name* /update/*id* und */index-name* `/_close`)
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (außer `/_cat/nodeattrs`)
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_ltr`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_resolve/index`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`

- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` für mehrere Eigenschaften[4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
  - `cluster.max_shards_per_node`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_dashboards`
- `/_nodes`
- `/_plugins/_asynchronous_search`
- `/_plugins/_alerting`
- `/_plugins/_anomaly_detection`
- `/_plugins/_ism`
- `/_plugins/_ppl`
- `/_plugins/_security`
- `/_plugins/_sql`
- `/_percolate`
- `/_rank_eval`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Anforderungstext und nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.

4. Verweist auf die PUT-Methode. Weitere Information zur GET-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen OpenSearch Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.

OpenSearch Version 1.1

Für OpenSearch 1.1 unterstützt OpenSearch Service die folgenden Operationen. Informationen zu den meisten Vorgängen finden Sie in der OpenSearchREST-API-Referenz oder in der API-Referenz für das jeweilige Plugin.

- Alle Operationen im Index-Pfad (bspw. */index-name /_forcemerge* , */index-name /update/id* und */index-name /_close*)
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (außer /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings für mehrere Eigenschaften[4]:
  - action.auto_create_index
- /_delete_by_query [1]
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_ltr
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_plugins/_asynchronous_search
- /_plugins/_alerting
- /_plugins/_anomaly_detection
- /_plugins/_ism
- /_plugins/_ppl
- /_refresh
- /_reindex [1]
- /_render
- /_resolve/index
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - cluster.max_shards_per_node
- /_cluster/state
- /_cluster/stats
- /_count
- /_dashboards
- /_plugins/_security
- /_plugins/_sql
- /_plugins/_transforms
- /_percolate
- /_rank_eval

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des /_tasks-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für /_search/scroll mit einem Nachrichtentext müssen "Content-Length" im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in scroll_id Werten zu vermeiden, verwenden Sie den Anforderungstext und nicht die Abfragezeichenfolge, um scroll_id Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Verweist auf die PUT-Methode. Weitere Information zur GET-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen OpenSearch Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.

OpenSearch Version 1.0

Für OpenSearch 1.0 unterstützt OpenSearch Service die folgenden Operationen. Informationen zu den meisten Vorgängen finden Sie in der OpenSearchREST-API-Referenz oder in der API-Referenz für das jeweilige Plugin.

- Alle Operationen im Index-Pfad (bspw. */index-name* / _forcemerge , */index-name* /update/*id* und */index-name* /_close)
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (außer /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings für mehrere Eigenschaften[4]:
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
- /_delete_by_query [1]
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_ltr
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_plugins/_asynchronous_search
- /_plugins/_alerting
- /_plugins/_anomaly_detection
- /_plugins/_ism
- /_plugins/_ppl
- /_plugins/_security
- /_plugins/_sql
- /_plugins/_transforms
- /_percolate
- /_refresh
- /_reindex [1]
- /_render
- /_resolve/index
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

- `indices.breaker.total.limit`
- `cluster.max_shards_per_node`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_dashboards`
- `/_rank_eval`

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Anforderungstext und nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Verweist auf die `PUT`-Methode. Weitere Information zur `GET`-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen OpenSearch Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.

Elasticsearch Version 7.10

Für Elasticsearch 7.10 unterstützt OpenSearch Service die folgenden Operationen.

- Alle Operationen im Index-Pfad (bspw. */index-name* / `_forcemerge` , */index-nam*
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_resolve/index`

e /update/*id* und /*index-name* /_close)
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (außer /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings für mehrere Eigenschaften[4]:
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - cluster.max_shards_per_node
- /_cluster/state
- /_cluster/stats
- /_count
- /_flush
- /_index_template [6]
- /_ingest/pipeline
- /_index_template
- /_ltr
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_opendistro/_alerting
- /_opendistro/_asynchronous_search
- /_opendistro/_anomaly_detection
- /_opendistro/_ism
- /_opendistro/_ppl
- /_opendistro/_security
- /_opendistro/_sql
- /_percolate
- /_plugin/kibana
- /_plugins/_replication
- /_rank_eval
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template [6]
- /_update_by_query [1]
- /_validate

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Hauptteil der Anfrage, nicht die Abfragezeichenfolge, um `scroll_id` Werte an Service zu OpenSearch übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Verweist auf die PUT-Methode. Weitere Information zur GET-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen Elasticsearch-Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.
6. Legacy-Indexvorlagen (`_template`) wurden durch zusammensetzbare Vorlagen (`_index_template`), beginnend mit Elasticsearch 7.8, ersetzt. Zusammensetzbare Vorlagen haben Vorrang vor Legacy-Vorlagen. Wenn keine zusammensetzbare Vorlage mit einem bestimmten Index übereinstimmt, kann eine Legacy-Vorlage weiterhin übereinstimmen und angewendet werden. Der `_template` Vorgang funktioniert immer noch auf OpenSearch und späteren Versionen von Elasticsearch OSS, aber GET-Aufrufe an die beiden Vorlagentypen liefern unterschiedliche Ergebnisse.

Elasticsearch Version 7.9

Für Elasticsearch 7.9 unterstützt OpenSearch Service die folgenden Operationen.

- Alle Operationen im Index-Pfad (bspw. */index-name* / `_forcemerge` , */index-name* `/update/`*id* und */index-name* `/_close`)
- `/_alias`
- `/_aliases`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_index_template` [6]
- `/_ingest/pipeline`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_resolve/index`
- `/_rollover`
- `/_scripts` [3]
- `/_search` [2]

- /_all
- /_analyze
- /_bulk
- /_cat (außer /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings für mehrere Eigenschaften[4]:
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - cluster.max_shards_per_node
- /_cluster/state
- /_cluster/stats
- /_count
- /_ltr
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_opendistro/_alerting
- /_opendistro/_anomaly_detection
- /_opendistro/_ism
- /_opendistro/_ppl
- /_opendistro/_security
- /_opendistro/_sql
- /_percolate
- /_plugin/kibana
- /_rank_eval
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template [6]
- /_update_by_query [1]
- /_validate

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des /_tasks-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für /_search/scroll mit einem Nachrichtentext müssen "Content-Length" im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig

hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Hauptteil der Anfrage, nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.

3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Verweist auf die PUT-Methode. Weitere Information zur GET-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen OpenSearch Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.
6. Legacy-Indexvorlagen (`_template`) wurden durch zusammensetzbare Vorlagen (`_index_template`), beginnend mit Elasticsearch 7.8, ersetzt. Zusammensetzbare Vorlagen haben Vorrang vor Legacy-Vorlagen. Wenn keine zusammensetzbare Vorlage mit einem bestimmten Index übereinstimmt, kann eine Legacy-Vorlage weiterhin übereinstimmen und angewendet werden. Der `_template` Vorgang funktioniert immer noch auf OpenSearch und späteren Versionen von Elasticsearch OSS, aber GET-Aufrufe an die beiden Vorlagentypen liefern unterschiedliche Ergebnisse.

Elasticsearch Version 7.8

Für Elasticsearch 7.8 unterstützt OpenSearch Service die folgenden Operationen.

- Alle Operationen im Index-Pfad (bspw. */index-name* / `_forcemerge` , */index-name* /update/*id* und */index-name* /`_close`)
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (außer `/_cat/nodeattrs`)
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_index_template` [6]
- `/_ingest/pipeline`
- `/_ltr`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`

- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` für mehrere Eigenschaften[4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
  - `cluster.max_shards_per_node`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_opendistro/_alerting`
- `/_opendistro/_anomaly_detection`
- `/_opendistro/_ism`
- `/_opendistro/_security`
- `/_opendistro/_sql`
- `/_percolate`
- `/_plugin/kibana`
- `/_rank_eval`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template` [6]
- `/_update_by_query` [1]
- `/_validate`

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Hauptteil der Anfrage, nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Verweist auf die `PUT`-Methode. Weitere Information zur `GET`-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen Elasticsearch-Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.

5. Siehe the section called “Shrink”.
6. Legacy-Indexvorlagen (`_template`) wurden durch zusammensetzbare Vorlagen (`_index_template`), beginnend mit Elasticsearch 7.8, ersetzt. Zusammensetzbare Vorlagen haben Vorrang vor Legacy-Vorlagen. Wenn keine zusammensetzbare Vorlage mit einem bestimmten Index übereinstimmt, kann eine Legacy-Vorlage weiterhin übereinstimmen und angewendet werden. Der `_template` Vorgang funktioniert immer noch auf OpenSearch und späteren Versionen von Elasticsearch OSS, aber GET-Aufrufe an die beiden Vorlagentypen liefern unterschiedliche Ergebnisse.

Elasticsearch Version 7.7

Für Elasticsearch 7.7 unterstützt OpenSearch Service die folgenden Operationen.

- Alle Operationen im Index-Pfad (bspw. */index-name* / `_forcemerge` , */index-name* /`update/`*id* und */index-name* `/_close`)
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (außer `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` für mehrere Eigenschaften[4]:
  - `action.auto_create_index`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_ltr`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_opendistro/_alerting`
- `/_opendistro/_anomaly_detection`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

- `action.search.shard_count.limit`
- `indices.breaker.fielddata.limit`
- `indices.breaker.request.limit`
- `indices.breaker.total.limit`
- `cluster.max_shards_per_node`

- `/_opendistro/_ism`
- `/_opendistro/_security`
- `/_opendistro/_sql`
- `/_percolate`
- `/_plugin/kibana`
- `/_rank_eval`

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Hauptteil der Anfrage, nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Verweist auf die PUT-Methode. Weitere Information zur GET-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen Elasticsearch-Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.

Elasticsearch Version 7.4

Für Elasticsearch 7.4 unterstützt OpenSearch Service die folgenden Operationen.

- Alle Operationen im Index-Pfad (bspw. */index-name /*

- `/_cluster/state`
- `/_cluster/stats`

- `/_refresh`
- `/_reindex` [1]

_forcemerge , */index-name* /update/*id* und */index-name* /_close)
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (außer /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings für mehrere Eigenschaften[4]:
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - cluster.max_shards_per_node
- /_count
- /_delete_by_query [1]
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_opendistro/_alerting
- /_opendistro/_anomaly_detection
- /_opendistro/_ism
- /_opendistro/_security
- /_opendistro/_sql
- /_percolate
- /_plugin/kibana
- /_rank_eval
- /_render
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des /_tasks-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.

2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Hauptteil der Anfrage, nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Verweist auf die PUT-Methode. Weitere Information zur GET-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen Elasticsearch-Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.

Elasticsearch Version 7.1

Für Elasticsearch 7.1 unterstützt OpenSearch Service die folgenden Operationen.

- Alle Operationen im Index-Pfad (bspw. */index-name /_forcemerge* und */index-name /update/id*) außer */index-name /_close*
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (außer `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_opendistro/_alerting`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`

- `/_cluster/settings` für mehrere Eigenschaften[4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
  - `cluster.max_shards_per_node`
- `/_opendistro/_ism`
- `/_opendistro/_security`
- `/_opendistro/_sql`
- `/_percolate`
- `/_plugin/kibana`
- `/_rank_eval`
- `/_update_by_query` [1]
- `/_validate`

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Hauptteil der Anfrage, nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Verweist auf die `PUT`-Methode. Weitere Information zur `GET`-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen Elasticsearch-Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.

Elasticsearch Version 6.8

Für Elasticsearch 6.8 unterstützt OpenSearch Service die folgenden Operationen.

- Alle Operationen im Index-Pfad (bspw. */index-name* / _forcemerge und */index-name* /update/*id*) außer */index-name* /_close
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (außer /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings für mehrere Eigenschaften[4]:
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
- /_cluster/state
- /_cluster/stats
- /_count
- /_delete_by_query [1]
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_opendistro/_alerting
- /_opendistro/_ism
- /_opendistro/_security
- /_opendistro/_sql
- /_percolate
- /_plugin/kibana
- /_rank_eval
- /_refresh
- /_reindex [1]
- /_render
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

- `cluster.max_shards_per_node`
- `cluster.blocks.read_only`

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Hauptteil der Anfrage, nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Verweist auf die PUT-Methode. Weitere Information zur GET-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen Elasticsearch-Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.

Elasticsearch Version 6.7

Für Elasticsearch 6.7 unterstützt OpenSearch Service die folgenden Operationen.

- Alle Operationen im Index-Pfad (bspw. */index-name* `/_forcemerge` und */index-name* `/update/`*id*) außer */index-name* `/_close`
- `/_alias`
- `/_aliases`
- `/_all`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`

- `/_analyze`
- `/_bulk`
- `/_cat` (außer `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` für mehrere Eigenschaften[4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
  - `cluster.max_shards_per_node`
- `/_ingest/pipeline`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_opendistro/_alerting`
- `/_opendistro/_security`
- `/_opendistro/_sql`
- `/_percolate`
- `/_plugin/kibana`
- `/_rank_eval`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Hauptteil der Anfrage, nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.

4. Verweist auf die PUT-Methode. Weitere Information zur GET-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen Elasticsearch-Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.

Elasticsearch Version 6.5

Für Elasticsearch 6.5 unterstützt OpenSearch Service die folgenden Operationen.

- Alle Operationen im Index-Pfad (bspw. `/index-name /_forcemerge` und `/index-name /update/id`) außer `/index-name /_close`
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (außer `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` für mehrere Eigenschaften[4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_opendistro/_alerting`
- `/_opendistro/_sql`
- `/_percolate`
- `/_plugin/kibana`
- `/_rank_eval`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

- `indices.breaker.fielddata.limit`
- `indices.breaker.request.limit`
- `indices.breaker.total.limit`

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Hauptteil der Anfrage, nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Verweist auf die `PUT`-Methode. Weitere Information zur `GET`-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen Elasticsearch-Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.

Elasticsearch Version 6.4

Für Elasticsearch 6.4 unterstützt OpenSearch Service die folgenden Operationen.

- Alle Operationen im Index-Pfad (bspw. */index-name* `/_forcemerge` und */index-name* `/update/`*id*) außer */index-name* `/_close`
- `/_alias`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_rollover`
- `/_scripts` [3]
- `/_search` [2]

- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (außer `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` für mehrere Eigenschaften[4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_opendistro/_alerting`
- `/_percolate`
- `/_plugin/kibana`
- `/_rank_eval`
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Hauptteil der Anfrage, nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.

4. Verweist auf die PUT-Methode. Weitere Information zur GET-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen Elasticsearch-Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.

Elasticsearch Version 6.3

Für Elasticsearch 6.3 unterstützt OpenSearch Service die folgenden Operationen.

- Alle Operationen im Index-Pfad (bspw. */index-name /_forcemerge* und */index-name /update/id*) außer */index-name /_close*
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (außer /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings für mehrere Eigenschaften[4]:
  - action.auto_create_index
  - action.search.shard_count.limit
- /_cluster/state
- /_cluster/stats
- /_count
- /_delete_by_query [1]
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_opendistro/_alerting
- /_percolate
- /_plugin/kibana
- /_rank_eval
- /_refresh
- /_reindex [1]
- /_render
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

- `indices.breaker.fielddata.limit`
- `indices.breaker.request.limit`
- `indices.breaker.total.limit`

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Hauptteil der Anfrage, nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Verweist auf die `PUT`-Methode. Weitere Information zur `GET`-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen Elasticsearch-Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.

Elasticsearch Version 6.2

Für Elasticsearch 6.2 unterstützt OpenSearch Service die folgenden Operationen.

- Alle Operationen im Index-Pfad (bspw. */index-name* `/_forcemerge` und */index-name* `/update/`*id*) außer */index-name* `/_close`
- `/_alias`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_rollover`
- `/_scripts` [3]
- `/_search` [2]

- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (außer `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` für mehrere Eigenschaften[4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_opendistro/_alerting`
- `/_percolate`
- `/_plugin/kibana`
- `/_rank_eval`
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Hauptteil der Anfrage, nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.

4. Verweist auf die PUT-Methode. Weitere Information zur GET-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen Elasticsearch-Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.

Elasticsearch Version 6.0

Für Elasticsearch 6.0 unterstützt OpenSearch Service die folgenden Operationen.

- Alle Operationen im Index-Pfad (bspw. */index-name /_forcemerge* und */index-name /update/id*) außer */index-name /_close*
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (außer /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings für mehrere Eigenschaften[4]:
  - action.auto_create_index
  - action.search.shard_count.limit
- /_cluster/state
- /_cluster/stats
- /_count
- /_delete_by_query [1]
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_percolate
- /_plugin/kibana
- /_refresh
- /_reindex [1]
- /_render
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

- `indices.breaker.fielddata.limit`
- `indices.breaker.request.limit`
- `indices.breaker.total.limit`

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Hauptteil der Anfrage, nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Verweist auf die `PUT`-Methode. Weitere Information zur `GET`-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen Elasticsearch-Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.

Elasticsearch Version 5.6

Für Elasticsearch 5.6 unterstützt OpenSearch Service die folgenden Operationen.

- Alle Operationen im Index-Pfad (bspw. */index-name* `/_forcemerge` und */index-name* `/update/`*id*) außer */index-name* `/_close`
- `/_alias`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_render`
- `/_rollover`
- `/_scripts` [3]
- `/_search` [2]
- `/_search profile`
- `/_shard_stores`

- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (außer /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings für mehrere Eigenschaften[4]:
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_percolate
- /_plugin/kibana
- /_refresh
- /_reindex [1]
- /_shrink[5]
- /_snapshot
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des /_tasks-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für /_search/scroll mit einem Nachrichtentext müssen "Content-Length" im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in scroll_id Werten zu vermeiden, verwenden Sie den Hauptteil der Anfrage, nicht die Abfragezeichenfolge, um scroll_id Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.

4. Verweist auf die PUT-Methode. Weitere Information zur GET-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen Elasticsearch-Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.

Elasticsearch Version 5.5

Für Elasticsearch 5.5 unterstützt OpenSearch Service die folgenden Operationen.

- Alle Operationen im Index-Pfad (bspw. */index-name* /_forcemerge und */index-name* /update/*id*) außer */index-name* /_close
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (außer /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings für mehrere Eigenschaften[4]:
  - action.auto_create_index
  - action.search.shard_count.limit
- /_cluster/state
- /_cluster/stats
- /_count
- /_delete_by_query [1]
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_percolate
- /_plugin/kibana
- /_refresh
- /_reindex [1]
- /_render
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

- `indices.breaker.fielddata.limit`
- `indices.breaker.request.limit`
- `indices.breaker.total.limit`

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Hauptteil der Anfrage, nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.
3. Überlegungen zur Verwendung von Skripts finden Sie unter the section called “Andere unterstützte Ressourcen”.
4. Verweist auf die `PUT`-Methode. Weitere Information zur `GET`-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen Elasticsearch-Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.
5. Siehe the section called “Shrink”.

Elasticsearch Version 5.3

Für Elasticsearch 5.3 unterstützt OpenSearch Service die folgenden Operationen.

- Alle Operationen im Index-Pfad (bspw. */index-name* `/_forcemerge` und */index-name* `/update/`*id*) außer */index-name* `/_close`
- `/_alias`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_render`
- `/_rollover`
- `/_search` [2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink` [4]

- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (außer /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings für mehrere Eigenschaften [3]:
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_percolate
- /_plugin/kibana
- /_refresh
- /_reindex [1]
- /_snapshot
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des /_tasks-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für /_search/scroll mit einem Nachrichtentext müssen "Content-Length" im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in scroll_id Werten zu vermeiden, verwenden Sie den Hauptteil der Anfrage, nicht die Abfragezeichenfolge, um scroll_id Werte an OpenSearch Service zu übergeben.
3. Verweist auf die PUT-Methode. Weitere Information zur GET-Methode finden Sie unter the section called “Erwähnenswerte API-Unterschiede”. Diese Liste bezieht sich nur auf die generischen

Elasticsearch-Operationen, die OpenSearch Service unterstützt, und enthält keine Plugin-spezifischen unterstützten Operationen zur Erkennung von Anomalien, ISM usw.

4. Siehe the section called “Shrink”.

Elasticsearch Version 5.1

Für Elasticsearch 5.1 unterstützt OpenSearch Service die folgenden Operationen.

- Alle Operationen im Index-Pfad (bspw. */index-name /_forcemerge* und */index-name /update/id*) außer */index-name /_close*
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (außer `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` für mehrere Eigenschaften (nur PUT):
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_percolate`
- `/_plugin/kibana`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_rollover`
- `/_search` [2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink` [3]
- `/_snapshot`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

- `indices.breaker.request.limit`
- `indices.breaker.total.limit`

1. Cluster-Konfigurationsänderungen können diese Vorgänge unterbrechen, bevor sie abgeschlossen sind. Wir empfehlen die Verwendung des `/_tasks`-Vorgangs zusammen mit diesen Vorgängen, um zu überprüfen, dass die Anforderungen erfolgreich abgeschlossen wurden.
2. DELETE-Anforderungen für `/_search/scroll` mit einem Nachrichtentext müssen `"Content-Length"` im HTTP-Header angeben. Die meisten Clients fügen diesen Header standardmäßig hinzu. Um Probleme mit = Zeichen in `scroll_id` Werten zu vermeiden, verwenden Sie den Hauptteil der Anfrage, nicht die Abfragezeichenfolge, um `scroll_id` Werte an OpenSearch Service zu übergeben.
3. Siehe the section called “Shrink”.

Elasticsearch Version 2.3

Für Elasticsearch 2.3 unterstützt OpenSearch Service die folgenden Operationen.

- Alle Operationen im Index-Pfad (bspw. `/index-name /_forcemerge` und `/index-name /_recovery`) außer `/index-name /_close`
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cache/clear` (nur Index)
- `/_cat` (außer `/_cat/nodeattrs`)
- `/_cluster/health`
- `/_cluster/settings` für mehrere Eigenschaften (nur PUT):
- `/_cluster/stats`
- `/_count`
- `/_flush`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_nodes`
- `/_percolate`
- `/_plugin/kibana`
- `/_refresh`
- `/_render`
- `/_search`
- `/_snapshot`

- `indices.breaker.fielddata.limit`
- `indices.breaker.request.limit`
- `indices.breaker.total.limit`
- `threadpool.get.queue_size`
- `threadpool.bulk.queue_size`
- `threadpool.index.queue_size`
- `threadpool.percolate.queue_size`
- `threadpool.search.queue_size`
- `threadpool.suggest.queue_size`

- `/_stats`
- `/_status`
- `/_template`

Elasticsearch Version 1.5

Für Elasticsearch 1.5 unterstützt OpenSearch Service die folgenden Operationen.

- Alle Operationen im Index-Pfad, bspw. */index-name* `/_optimize` und */index-name* `/_warmer`, außer */index-name* `/_close`
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat`
- `/_cluster/health`
- `/_cluster/settings` für mehrere Eigenschaften (nur PUT):
  - `indices.breaker.fielddata.limit`

- `/_cluster/stats`
- `/_count`
- `/_flush`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_nodes`
- `/_percolate`
- `/_plugin/kibana`
- `/_plugin/kibana3`
- `/_plugin/migration`
- `/_refresh`
- `/_search`
- `/_snapshot`
- `/_stats`

- indices.breaker.request.limit
- indices.breaker.total.limit
- threadpool.get.queue_size
- threadpool.bulk.queue_size
- threadpool.index.queue_size
- threadpool.percolate.queue_size
- threadpool.search.queue_size
- threadpool.suggest.queue_size
- /_status
- /_template

Amazon OpenSearch Service-Kontingente

Ihr AWS Konto verfügt über Standardkontingente, die früher als Limits bezeichnet wurden, für jeden AWS Service. Wenn nicht anders angegeben, gilt jedes Kontingent spezifisch für eine Region.

Die Kontingente für OpenSearch Service-Domains und -Instances, Amazon OpenSearch Serverless und Amazon OpenSearch Ingestion finden Sie unter Amazon OpenSearch Service-Kontingente in der. Allgemeine AWS-Referenz

Um die Kontingente für OpenSearch Service in der anzuzeigen AWS Management Console, öffnen Sie die Konsole Service Quotas. Wählen Sie im Navigationsbereich AWS Services und dann Amazon OpenSearch Service aus. Informationen zur Erhöhung eines Kontingents finden Sie unter Anfordern einer Kontingenterhöhung im Service-Quotas-Benutzerhandbuch.

Themen

- UltraWarm Speicherkontingente
- EBS-Volume-Größenkontigente
- Netzwerk-Kontingente
- Kontingente für die Größe von Shards
- Java-Prozess-Kontingente
- Domain-Richtlinien-Kontingente

UltraWarm Speicherkontingente

In der folgenden Tabelle sind die UltraWarm Instanztypen und die maximale Speichermenge aufgeführt, die jeder Typ verwenden kann. Weitere Informationen zu finden UltraWarm Sie unterthe section called “UltraWarm Speicher”.

Instance-Typ	Maximaler Speicher
`ultrawarm1.medium.search`	1,5 TiB
`ultrawarm1.large.search`	20 TiB

EBS-Volume-Größenkontigente

Die folgende Tabelle zeigt die Mindest- und Höchstgrößen für EBS-Volumes für jeden Instance-Typ, den OpenSearch Service unterstützt. Informationen darüber, welche Instance-Typen Instance-Speicher und zusätzliche Hardwaredetails beinhalten, finden Sie unter Amazon OpenSearch Service-Preise.

- Wenn Sie beim Erstellen Ihrer Domain unter EBS-Volume-Typ Magnetspeicher auswählen, beträgt die maximale Volume-Größe 100 GiB für alle Instance-Typen außer `t2.small` und `t2.medium` und alle Graviton-Instances (M6g, C6g, R6g und R6gd), die magnetischen Speicher nicht unterstützen. Wählen Sie für die maximalen Größen in der folgenden Tabelle eine der SSD-Optionen aus.
- Einige Instance-Typen älterer Generation umfassen Instance-Speicher, unterstützen aber auch EBS-Speicher. Wenn Sie EBS-Speicher für einen dieser Instance-Typen wählen, gelten die Speicher-Volumes nicht additiv. Sie können entweder ein EBS-Volume oder Instance-Speicher verwenden, nicht aber beides.

Instance-Typ	EBS-Mindestgröße	Maximale EBS-Größe (gp2)	Maximale EBS-Größe (gp3)
`t2.micro.search`	10 GiB	35 GiB	N/A
`t2.small.search`	10 GiB	35 GiB	N/A

Instance-Typ	EBS-Mindestgröße	Maximale EBS-Größe (gp2)	Maximale EBS-Größe (gp3)
t2.medium.search	10 GiB	35 GiB	N/A
t3.small.search	10 GiB	100 GiB	100 GiB
t3.medium.search	10 GiB	200 GiB	200 GiB
m3.medium.search	10 GiB	100 GiB	N/A
m3.large.search	10 GiB	512 GiB	N/A
m3.xlarge.search	10 GiB	512 GiB	N/A
m3.2xlarge.search	10 GiB	512 GiB	N/A
m4.large.search	10 GiB	512 GiB	N/A
m4.xlarge.search	10 GiB	1 TiB	N/A
m4.2xlarge.search	10 GiB	1,5 TiB	N/A
m4.4xlarge.search	10 GiB	1,5 TiB	N/A
m4.10xlarge.search	10 GiB	1,5 TiB	N/A
m5.large.search	10 GiB	512 GiB	1 TiB
m5.xlarge.search	10 GiB	1 TiB	2 TiB
m5.2xlarge.search	10 GiB	1,5 TiB	3 TiB
m5.4xlarge.search	10 GiB	3 TiB	6 TiB
m5.12xlarge.search	10 GiB	9 TiB	18 TiB
m6g.large.search	10 GiB	512 GiB	1 TiB
m6g.xlarge.search	10 GiB	1 TiB	2 TiB

Instance-Typ	EBS-Mindestgröße	Maximale EBS-Größe (gp2)	Maximale EBS-Größe (gp3)
m6g.2xlarge.search	10 GiB	1,5 TiB	3 TiB
m6g.4xlarge.search	10 GiB	3 TiB	6 TiB
m6g.8xlarge.search	10 GiB	6 TiB	12 TiB
m6g.12xlarge.search	10 GiB	9 TiB	18 TiB
c4.large.search	10 GiB	100 GiB	N/A
c4.xlarge.search	10 GiB	512 GiB	N/A
c4.2xlarge.search	10 GiB	1 TiB	N/A
c4.4xlarge.search	10 GiB	1,5 TiB	N/A
c4.8xlarge.search	10 GiB	1,5 TiB	N/A
c5.large.search	10 GiB	256 GiB	256 GiB
c5.xlarge.search	10 GiB	512 GiB	512 GiB
c5.2xlarge.search	10 GiB	1 TiB	1 TiB
c5.4xlarge.search	10 GiB	1,5 TiB	1,5 TiB
c5.9xlarge.search	10 GiB	3,5 TiB	3,5 TiB
c5.18xlarge.search	10 GiB	7 TiB	7 TiB
c6g.large.search	10 GiB	256 GiB	256 GiB
c6g.xlarge.search	10 GiB	512 GiB	512 GiB
c6g.2xlarge.search	10 GiB	1 TiB	1 TiB
c6g.4xlarge.search	10 GiB	1,5 TiB	1,5 TiB

Instance-Typ	EBS-Mindestgröße	Maximale EBS-Größe (gp2)	Maximale EBS-Größe (gp3)
c6g.8xlarge.search	10 GiB	3 TiB	3 TiB
c6g.12xlarge.search	10 GiB	4.5 TiB	4.5 TiB
r3.large.search	10 GiB	512 GiB	N/A
r3.xlarge.search	10 GiB	512 GiB	N/A
r3.2xlarge.search	10 GiB	512 GiB	N/A
r3.4xlarge.search	10 GiB	512 GiB	N/A
r3.8xlarge.search	10 GiB	512 GiB	N/A
r4.large.search	10 GiB	1 TiB	N/A
r4.xlarge.search	10 GiB	1,5 TiB	N/A
r4.2xlarge.search	10 GiB	1,5 TiB	N/A
r4.4xlarge.search	10 GiB	1,5 TiB	N/A
r4.8xlarge.search	10 GiB	1,5 TiB	N/A
r4.16xlarge.search	10 GiB	1,5 TiB	N/A
r5.large.search	10 GiB	1 TiB	2 TiB
r5.xlarge.search	10 GiB	1,5 TiB	3 TiB
r5.2xlarge.search	10 GiB	3 TiB	6 TiB
r5.4xlarge.search	10 GiB	6 TiB	12 TiB
r5.12xlarge.search	10 GiB	12 TiB	24 TiB
r6g.large.search	10 GiB	1 TiB	2 TiB

Instance-Typ	EBS-Mindestgröße	Maximale EBS-Größe (gp2)	Maximale EBS-Größe (gp3)
r6g.xlarge.search	10 GiB	1,5 TiB	3 TiB
r6g.2xlarge.search	10 GiB	3 TiB	6 TiB
r6g.4xlarge.search	10 GiB	6 TiB	12 TiB
r6g.8xlarge.search	10 GiB	8 TiB	16 TiB
r6g.12xlarge.search	10 GiB	12 TiB	24 TiB
r6gd.large.search	N/A	–	–
r6gd.xlarge.search	–	–	–
r6gd.2xlarge.search	–	–	–
r6gd.4xlarge.search	–	–	–
r6gd.8xlarge.search	–	–	–
r6gd.12xlarge.search	–	–	–
r6gd.16xlarge.search	–	–	N/A
i2.xlarge.search	10 GiB	512 GiB	N/A
i2.2xlarge.search	10 GiB	512 GiB	N/A
i3.large.search	–	–	–
i3.xlarge.search	–	–	–
i3.2xlarge.search	–	–	–
i3.4xlarge.search	–	–	–
i3.8xlarge.search	–	–	–

Instance-Typ	EBS-Mindestgröße	Maximale EBS-Größe (gp2)	Maximale EBS-Größe (gp3)
i3.16xlarge.search	–	–	N/A
or1.medium.search	20 GiB	N/A	768 GiB
or1.large.search	20 GiB	N/A	1532 GiB
or1.xlarge.search	20 GiB	N/A	3 TiB
or1.2xlarge.search	20 GiB	N/A	6 TiB
or1.4xlarge.search	20 GiB	N/A	12 TiB
or1.8xlarge.search	20 GiB	N/A	16 TiB
or1.12xlarge.search	20 GiB	N/A	24 TiB
or1.16xlarge.search	20 GiB	N/A	36 TiB
im4gn.large.search	N/A	–	–
im4gn.xlarge.search	–	–	–
im4gn.2xlarge.search	–	–	–
im4gn.4xlarge.search	–	–	–
im4gn.8xlarge.search	–	–	–
im4gn.16xlarge.search	–	–	N/A

Netzwerk-Kontingente

Die folgende Tabelle zeigt die maximale Größe von HTTP-Anforderungsnutzlasten.

Instance-Typ	Maximale Größe von HTTP-Anforderungsnutzlasten
t2.micro.search	10 MiB
t2.small.search	10 MiB
t2.medium.search	10 MiB
t3.small.search	10 MiB
t3.medium.search	10 MiB
m3.medium.search	10 MiB
m3.large.search	10 MiB
m3.xlarge.search	100 MiB
m3.2xlarge.search	100 MiB
m4.large.search	10 MiB
m4.xlarge.search	100 MiB
m4.2xlarge.search	100 MiB
m4.4xlarge.search	100 MiB
m4.10xlarge.search	100 MiB
m5.large.search	10 MiB
m5.xlarge.search	100 MiB
m5.2xlarge.search	100 MiB
m5.4xlarge.search	100 MiB
m5.12xlarge.search	100 MiB

Instance-Typ	Maximale Größe von HTTP-Anforderungsnutzlasten
m6g.large.search	10 MiB
m6g.xlarge.search	100 MiB
m6g.2xlarge.search	100 MiB
m6g.4xlarge.search	100 MiB
m6g.8xlarge.search	100 MiB
m6g.12xlarge.search	100 MiB
c4.large.search	10 MiB
c4.xlarge.search	100 MiB
c4.2xlarge.search	100 MiB
c4.4xlarge.search	100 MiB
c4.8xlarge.search	100 MiB
c5.large.search	10 MiB
c5.xlarge.search	100 MiB
c5.2xlarge.search	100 MiB
c5.4xlarge.search	100 MiB
c5.9xlarge.search	100 MiB
c5.18xlarge.search	100 MiB

Instance-Typ	Maximale Größe von HTTP-Anforderungsnutzlasten
c6g.large.search	10 MiB
c6g.xlarge.search	100 MiB
c6g.2xlarge.search	100 MiB
c6g.4xlarge.search	100 MiB
c6g.8xlarge.search	100 MiB
c6g.12xlarge.search	100 MiB
r3.large.search	10 MiB
r3.xlarge.search	100 MiB
r3.2xlarge.search	100 MiB
r3.4xlarge.search	100 MiB
r3.8xlarge.search	100 MiB
r4.large.search	100 MiB
r4.xlarge.search	100 MiB
r4.2xlarge.search	100 MiB
r4.4xlarge.search	100 MiB
r4.8xlarge.search	100 MiB
r4.16xlarge.search	100 MiB

Instance-Typ	Maximale Größe von HTTP-Anforderungsnutzlasten
r5.large.search	100 MiB
r5.xlarge.search	100 MiB
r5.2xlarge.search	100 MiB
r5.4xlarge.search	100 MiB
r5.12xlarge.search	100 MiB
r6g.large.search	100 MiB
r6g.xlarge.search	100 MiB
r6g.2xlarge.search	100 MiB
r6g.4xlarge.search	100 MiB
r6g.8xlarge.search	100 MiB
r6g.12xlarge.search	100 MiB
r6gd.large.search	100 MiB
r6gd.xlarge.search	100 MiB
r6gd.2xlarge.search	100 MiB
r6gd.4xlarge.search	100 MiB

Instance-Typ	Maximale Größe von HTTP-Anforderungsnutzlasten
r6gd.8xlarge.search	100 MiB
r6gd.12xlarge.search	100 MiB
r6gd.16xlarge.search	100 MiB
i2.xlarge.search	100 MiB
i2.2xlarge.search	100 MiB
i3.large.search	100 MiB
i3.xlarge.search	100 MiB
i3.2xlarge.search	100 MiB
i3.4xlarge.search	100 MiB
i3.8xlarge.search	100 MiB
i3.16xlarge.search	100 MiB
or1.medium.search	10 MiB
or1.large.search	100 MiB
or1.xlarge.search	100 MiB
or1.2xlarge.search	100 MiB
or1.4xlarge.search	100 MiB

Instance-Typ	Maximale Größe von HTTP-Anforderungsnutzlasten
or1.8xlarge.search	100 MiB
or1.12xlarge.search	100 MiB
or1.16xlarge.search	100 MiB
im4gn.large.search	100 MiB
im4gn.xlarge.search	100 MiB
im4gn.2xlarge.search	100 MiB
im4gn.4xlarge.search	100 MiB
im4gn.8xlarge.search	100 MiB
im4gn.16xlarge.search	100 MiB

Kontingente für die Größe von Shards

Im folgenden Abschnitt sind die maximalen Shard-Größen für verschiedene Instance-Familien aufgeführt.

Instance-Typ	Multi-AZ ohne Standby	Multi-AZ mit Standby
R5, C5, M5	N/A	65 GiB

Instance-Typ	Multi-AZ ohne Standby	Multi-AZ mit Standby
I3	N/A	65 GiB
R6 g, C6 g, M6 g, R6 Gd	N/A	65 GiB
ODER 1	100 GiB	65 GiB
Im4gn	N/A	65 GiB

Um eine Erhöhung des Kontingents zu beantragen, wenden Sie sich an den AWS Support.

Java-Prozess-Kontingente

OpenSearch Der Service begrenzt Java-Prozesse auf eine Heap-Größe von 32 GiB. Fortgeschrittene Benutzer können den Prozentanteil des Heap für Felddaten angeben. Weitere Informationen finden Sie unter the section called “Erweiterte Clustereinstellungen” und the section called “JVM OutOfMemoryError”.

Domain-Richtlinien-Kontingente

OpenSearch Der Service begrenzt die Zugriffsrichtlinien für Domains auf 100 KiB.

Reserved Instances in Amazon OpenSearch Service

Reserved Instances (RIs) in Amazon OpenSearch Service bieten verglichen mit Standard-On-Demand-Instances beträchtliche Rabatte. Die Instances selbst sind identisch. RIs sind nur ein Fakturierungsrabatt, der auf On-Demand-Instances in Ihrem Konto angewendet wird. Für Anwendungen mit langer Lebensdauer und vorhersehbarer Nutzung können RIs im Laufe der Zeit für erhebliche Einsparungen sorgen.

OpenSearch Service RIs erfordern eine Laufzeit von einem Jahr oder drei Jahren und verfügen über drei Zahlungsoptionen, die sich auf den Rabatt auswirken:

- No Upfront - Sie leisten keine Zahlung im Voraus. Sie zahlen einen ermäßigten Stundensatz für jede Stunde während der Laufzeit.
- Partial Upfront - Sie zahlen einen Teil der Kosten im Voraus und zahlen einen ermäßigten Stundensatz für jede Stunde während der Laufzeit.

- All Upfront - Sie zahlen den gesamten Betrag im Voraus. Sie zahlen keinen Stundensatz für die Laufzeit.

Im Allgemeinen bedeutet eine größere Vorauszahlung einen größeren Rabatt. Reserved Instances können nicht storniert werden. Wenn Sie sie reservieren, verpflichten Sie sich, für die gesamte Laufzeit zu zahlen. Außerdem sind Vorauszahlungen nicht rückerstattungsfähig.

RIs sind nicht flexibel, sie gelten nur für den genauen Instance-Typ, den Sie reservieren. Eine Reservierung für acht `c5.2xlarge.search`-Instances gilt beispielsweise nicht für sechzehn `c5.xlarge.search`-Instanzen oder vier `c5.4xlarge.search`-Instanzen. Details zur Verfügbarkeit finden Sie unter Amazon OpenSearch Service-Preise und FAQ.

Themen

Erwerben von Reserved Instances (Konsole)

Mithilfe der Konsole können Sie Ihre vorhandenen Reserved Instances anzeigen und neue erwerben.

So erwerben Sie eine Reservierung

1. Rufen Sie die Webseite https://aws.amazon.com auf und klicken Sie dann auf Sign In to the Console (Bei der Konsole anmelden).
2. Unter Analytik wählen sie Amazon OpenSearch Service aus.
3. Wählen Sie im Navigationsbereich Reserved Instance Leases aus.

   Auf dieser Seite erhalten Sie einen Überblick über Ihre vorhandenen Reservierungen. Sie können zahlreiche vorhandene Reservierungen filtern, um eine bestimmte Reservierung leichter identifizieren und anzuzeigen zu können.

> **Tip**
>
> Wenn der Link Reserved Instance Leases nicht angezeigt wird, erstellen Sie eine Domäne in der AWS-Region.

4. Wählen Sie Reserved Instances bestellen aus.
5. Geben Sie einen eindeutigen und aussagekräftigen Namen ein.
6. Wählen Sie einen Instance-Typ und die Anzahl der Instances aus. Anleitungen finden Sie unter the section called “Größenanpassung von Domains”.
7. Wählen Sie eine Laufzeit und eine Zahlungsoption aus. Überprüfen Sie die Zahlungsinformationen sorgfältig.
8. Wählen Sie Next (Weiter).
9. Überprüfen Sie die Kaufübersicht sorgfältig. Erworbene Reserved Instances sind nicht erstattungsfähig.
10. Klicken Sie auf Bestellung.

Erwerben von Reserved Instances (AWS-CLI)

Die AWS CLI verfügt über Befehle zum Anzeigen von Angeboten, zum Erwerben einer Reservierung und zum Anzeigen Ihrer Reservierungen. Das folgende Beispiel und das Antwortbeispiel zeigen die Angebote für eine bestimmte AWS-Region:

```
aws opensearch describe-reserved-instance-offerings --region us-east-1
{
  "ReservedInstanceOfferings": [
    {
      "FixedPrice": x,
      "ReservedInstanceOfferingId": "1a2a3a4a5-1a2a-3a4a-5a6a-1a2a3a4a5a6a",
      "RecurringCharges": [
        {
          "RecurringChargeAmount": y,
          "RecurringChargeFrequency": "Hourly"
        }
      ],
      "UsagePrice": 0.0,
      "PaymentOption": "PARTIAL_UPFRONT",
      "Duration": 31536000,
```

```
      "InstanceType": "m4.2xlarge.search",
      "CurrencyCode": "USD"
    }
  ]
}
```

Eine Beschreibung der einzelnen Rückgabewerte finden Sie in der folgenden Tabelle.

Feld	Beschreibung
`FixedPrice`	Die Vorauszahlungskosten der Reservierung.
`ReservedInstanceOfferingId`	Die Angebots-ID. Notieren Sie diesen Wert, wenn Sie das Angebot reservieren möchten.
`RecurringCharges`	Der Stundensatz für die Reservierung.
`UsagePrice`	Ein Legacy-Feld. Für OpenSearch Service ist dieser Wert immer 0.
`PaymentOption`	„No Upfront“ (Keine Vorauszahlung), „Partial Upfront“ (Teilweise Vorauszahlung) oder „All Upfront“ (Komplette Vorauszahlung).
`Duration`	Laufzeitlänge in Sekunden: • 31536000 Sekunden entsprechen einem Jahr. • 94608000 Sekunden entsprechen drei Jahren.
`InstanceType`	Der Instance-Typ für die Reservierung. Informationen über die Hardware-Ressourcen, die jedem Instance-Typ zugeordnet sind, finden Sie unter Amazon Opensearch Service – Preise.
`CurrencyCode`	Die Währung für `FixedPrice` und `RecurringChargeAmount`.

In diesem nächsten Beispiel wird eine Reservierung erworben:

```
aws opensearch purchase-reserved-instance-offering --reserved-instance-offering-
id 1a2a3a4a5-1a2a-3a4a-5a6a-1a2a3a4a5a6a --reservation-name my-reservation --instance-
count 3 --region us-east-1
{
  "ReservationName": "my-reservation",
  "ReservedInstanceId": "9a8a7a6a-5a4a-3a2a-1a0a-9a8a7a6a5a4a"
}
```

Schließlich können Sie entsprechend dem folgenden Beispiel Ihre Reservierungen für einen bestimmten Zeitraum auflisten:

```
aws opensearch describe-reserved-instances --region us-east-1
{
  "ReservedInstances": [
    {
      "FixedPrice": x,
      "ReservedInstanceOfferingId": "1a2a3a4a5-1a2a-3a4a-5a6a-1a2a3a4a5a6a",
      "ReservationName": "my-reservation",
      "PaymentOption": "PARTIAL_UPFRONT",
      "UsagePrice": 0.0,
      "ReservedInstanceId": "9a8a7a6a-5a4a-3a2a-1a0a-9a8a7a6a5a4a",
      "RecurringCharges": [
        {
          "RecurringChargeAmount": y,
          "RecurringChargeFrequency": "Hourly"
        }
      ],
      "State": "payment-pending",
      "StartTime": 1522872571.229,
      "InstanceCount": 3,
      "Duration": 31536000,
      "InstanceType": "m4.2xlarge.search",
      "CurrencyCode": "USD"
    }
  ]
}
```

> **Note**
>
> `StartTime` ist die Zeit seit Unix-Epoche. Dies ist die Anzahl der Sekunden, die seit Mitternacht UTC am 1. Januar 1970 verstrichen sind. Beispielsweise entspricht 1522872571 in der Zeit seit Unix-Epoche 20:09:31 UTC am 4. April 2018. Sie können Online-Konverter verwenden.

Weitere Informationen über die in den vorherigen Beispielen verwendeten Befehle finden Sie in der AWS CLI-Befehlsreferenz.

Erwerben von Reserved Instances (AWS-SDKs)

Die AWS-SDKs (außer den Android- und iOS-SDKs) unterstützen alle Vorgänge, die in der API-Referenz für Amazon OpenSearch Service definiert sind, einschließlich der folgenden:

- `DescribeReservedInstanceOfferings`
- `PurchaseReservedInstanceOffering`
- `DescribeReservedInstances`

Dieses Beispielskript verwendet den Low-Level-Python-Client OpenSearchService von AWS SDK for Python (Boto3), um reservierte Instances zu kaufen. Sie müssen einen Wert für `instance_type` angeben.

```
import boto3
from botocore.config import Config

# Build the client using the default credential configuration.
# You can use the CLI and run 'aws configure' to set access key, secret
# key, and default region.

my_config = Config(
    # Optionally lets you specify a region other than your default.
    region_name='us-east-1'
)

client = boto3.client('opensearch', config=my_config)

instance_type = '' # e.g. m4.2xlarge.search
```

```
def describe_RI_offerings(client):
    """Gets the Reserved Instance offerings for this account"""

    response = client.describe_reserved_instance_offerings()
    offerings = (response['ReservedInstanceOfferings'])
    return offerings


def check_instance(offering):
    """Returns True if instance type is the one you specified above"""

    if offering['InstanceType'] == instance_type:
        return True

    return False


def get_instance_id():
    """Iterates through the available offerings to find the ID of the one you
 specified"""

    instance_type_iterator = filter(
        check_instance, describe_RI_offerings(client))
    offering = list(instance_type_iterator)
    id = offering[0]['ReservedInstanceOfferingId']
    return id


def purchase_RI_offering(client):
    """Purchase Reserved Instances"""

    response = client.purchase_reserved_instance_offering(
        ReservedInstanceOfferingId = get_instance_id(),
        ReservationName = 'my-reservation',
        InstanceCount = 1
    )
    print('Purchased reserved instance offering of type ' + instance_type)
    print(response)


def main():
    """Purchase Reserved Instances"""
```

```
    purchase_RI_offering(client)
```

Weitere Informationen über die Installation und Verwendung der AWS-SDKs finden Sie unter AWS-Software-Entwicklungs-Kits.

Untersuchen der Kosten

Cost Explorer ist ein kostenloses Tool, mit dem Sie Daten zu Ihren Ausgaben für die letzten 13 Monate anzeigen können. Durch die Analyse dieser Daten können Sie Trends aufdecken und erkennen, ob RIs für Ihren Anwendungsfall geeignet wären. Wenn Sie bereits über RIs verfügen, können Sie durch Gruppieren nach Kaufoption und durch Anzeigen amortisierter Kosten diese Ausgaben mit den Ausgaben für On-Demand-Instances vergleichen. Sie können auch Nutzungsbudgets festlegen, um sicherzustellen, dass Sie alle Vorteile Ihrer Reservierungen nutzen. Weitere Informationen finden Sie unter Analysieren von Kosten mit Cost Explorer im AWS Billing-Benutzerhandbuch.

Andere unterstützte Ressourcen in Amazon OpenSearch Service

In diesem Thema werden zusätzliche Ressourcen beschrieben, die Amazon OpenSearch Service unterstützt.

bootstrap.memory_lock

OpenSearch Service aktiviert `bootstrap.memory_lock` in `opensearch.yml`, wodurch der JVM-Speicher gesperrt wird und verhindert wird, dass das Betriebssystem ihn auf die Festplatte auslagert. Dies gilt für alle unterstützten Instance-Typen außer den Folgenden:

- `t2.micro.search`
- `t2.small.search`
- `t2.medium.search`
- `t3.small.search`
- `t3.medium.search`

Scripting-Modul

OpenSearch Der Service unterstützt Scripting für Elasticsearch 5. Domänen x und höher. Er unterstützt kein Scripting für 1.5 oder 2.3.

Unterstützte Scripting-Optionen umfassen die Folgenden:

- Painless
- Lucene Expressions
- Mustache

Für Elasticsearch-Domains ab Version 5.5 sowie für alle OpenSearch Domains unterstützt OpenSearch Service gespeicherte Skripts, die den `_scripts` Endpunkt verwenden. Elasticsearch 5.3- und 5.1-Domains unterstützen nur Inline-Skripts.

TLS-Transport

OpenSearch Der Service unterstützt HTTP auf Port 80 und HTTPS auf Port 443, unterstützt jedoch keinen TLS-Transport.

Tutorials für Amazon OpenSearch Service

Dieses Kapitel enthält mehrere Start-bis-Ende-Tutorials für die Arbeit mit Amazon OpenSearch Service, einschließlich der Migration zum Service, der Erstellung einer einfachen Suchanwendung und der Erstellung einer Visualisierung in OpenSearch Dashboards.

Themen

Tutorial: Dokumente in Amazon OpenSearch Service erstellen und danach suchen

In diesem Tutorial erfahren Sie, wie Sie ein Dokument in Amazon OpenSearch Service erstellen und danach suchen. Sie fügen einem Index Daten in Form eines JSON-Dokuments hinzu. OpenSearch Der Dienst erstellt einen Index rund um das erste Dokument, das Sie hinzufügen.

In diesem Tutorial wird erläutert, wie Sie HTTP-Anforderungen zum Erstellen von Dokumenten stellen, automatisch eine ID für ein Dokument generieren und grundlegende und erweiterte Suchvorgänge für Ihre Dokumente durchführen.

> **Note**
>
> Dieses Tutorial verwendet eine Domain mit offenem Zugriff. Für ein Höchstmaß an Sicherheit empfehlen wir, Ihre Domain in eine Virtual Private Cloud (VPC) zu legen.

Voraussetzungen

Für dieses Tutorial müssen die folgenden Voraussetzungen erfüllt sein:

- Sie benötigen ein AWS-Konto.

- Sie müssen über eine aktive OpenSearch Dienstdomäne verfügen.

Hinzufügen eines Dokuments zu einem Index

Um ein Dokument zu einem Index hinzuzufügen, können Sie ein beliebiges HTTP-Tool wie Postman, cURL oder die OpenSearch Dashboards-Konsole verwenden. Bei diesen Beispielen wird davon ausgegangen, dass Sie die Entwicklerkonsole in Dashboards verwenden. OpenSearch Wenn Sie ein anderes Tool verwenden, passen Sie es entsprechend an, indem Sie bei Bedarf die vollständige URL und Anmeldeinformationen angeben.

Fügen Sie ein Dokument wie folgt einem Index hinzu

1. Navigieren Sie zur OpenSearch Dashboard-URL für Ihre Domain. Sie finden die URL im Dashboard der Domain in der OpenSearch Servicekonsole. Die URL weist das folgende Format auf:

   ```
   domain-endpoint/_dashboards/
   ```

2. Melden Sie sich mit Ihrem primären Benutzernamen und Passwort an.
3. Öffnen Sie den linken Navigationsbereich und wählen Sie Dev Tools (Entwickler-Tools) aus.
4. Das HTTP-Verb zum Erstellen einer neuen Ressource ist PUT, das Sie zum Erstellen eines neuen Dokuments und Indexes verwenden. Geben Sie in der Konsole den folgenden Befehl ein:

   ```
   PUT fruit/_doc/1
   {
     "name":"strawberry",
     "color":"red"
   }
   ```

   Die PUT-Anforderung erstellt einen Index namens fruit und erstellt ein einzelnes Dokument gemäß des Indexes mit der ID 1. Sie erzeugt folgende Antwort:

   ```
   {
     "_index" : "fruit",
     "_type" : "_doc",
     "_id" : "1",
     "_version" : 1,
     "result" : "created",
     "_shards" : {
   ```

```
    "total" : 2,
    "successful" : 2,
    "failed" : 0
  },
  "_seq_no" : 0,
  "_primary_term" : 1
}
```

Erstellen automatisch generierter IDs

OpenSearch Der Service kann automatisch eine ID für Ihre Dokumente generieren. Der Befehl zum Generieren von IDs verwendet eine POST-Anforderung anstelle einer PUT-Anforderung und erfordert keine Dokument-ID (im Vergleich zur vorherigen Anforderung).

Geben Sie die folgende Anforderung in der Entwicklerkonsole ein:

```
POST veggies/_doc
{
  "name":"beet",
  "color":"red",
  "classification":"root"
}
```

Diese Anfrage erstellt einen Index mit dem Namen veggies und fügt das Dokument dem Index hinzu. Sie erzeugt folgende Antwort:

```
{
  "_index" : "veggies",
  "_type" : "_doc",
  "_id" : "3WgyS4IB5DLqbRIvLxtF",
  "_version" : 1,
  "result" : "created",
  "_shards" : {
    "total" : 2,
    "successful" : 2,
    "failed" : 0
  },
  "_seq_no" : 0,
  "_primary_term" : 1
}
```

Beachten Sie das zusätzliche Feld `_id` in der Antwort, das anzeigt, dass automatisch eine ID erstellt wurde.

> **Note**
>
> Nach `_doc` geben Sie nichts mehr in der URL an, wo normalerweise die ID steht. Da Sie ein Dokument mit einer generierten ID erstellen, geben Sie noch keine an. Diese ist für Updates reserviert.

Aktualisieren eines Dokuments mit einem POST-Befehl

Um ein Dokument zu aktualisieren, verwenden Sie einen HTTP-`POST`-Befehl mit der ID-Nummer.

Erstellen Sie zunächst ein Dokument mit der ID `42`:

```
POST fruits/_doc/42
{
  "name":"banana",
  "color":"yellow"
}
```

Verwenden Sie dann diese ID, um das Dokument zu aktualisieren:

```
POST fruits/_doc/42
{
  "name":"banana",
  "color":"yellow",
  "classification":"berries"
}
```

Dieser Befehl aktualisiert das Dokument mit dem neuen Feld `classification`. Sie erzeugt folgende Antwort:

```
{
  "_index" : "fruits",
  "_type" : "_doc",
  "_id" : "42",
  "_version" : 2,
  "result" : "updated",
```

```
  "_shards" : {
    "total" : 2,
    "successful" : 2,
    "failed" : 0
  },
  "_seq_no" : 1,
  "_primary_term" : 1
}
```

> **Note**
>
> Wenn Sie versuchen, ein Dokument zu aktualisieren, das nicht existiert, erstellt OpenSearch Service das Dokument.

Ausführen von Massenaktionen

Sie können die API-Operation `POST _bulk` zum Ausführen mehrerer Aktionen für einen oder mehrere Indizes in einer Anforderung verwenden. Befehle für Massenaktionen haben folgendes Format:

```
POST /_bulk
<action_meta>\n
<action_data>\n
<action_meta>\n
<action_data>\n
```

Jede Aktion erfordert zwei JSON-Zeilen. Zuerst geben Sie die Beschreibung der Aktion oder Metadaten an. In der nächsten Zeile geben Sie die Daten ein. Jeder Teil wird durch einen Zeilenumbruch (\n) getrennt. Eine Aktionsbeschreibung für eine Einfügung kann wie folgt aussehen:

```
{ "create" : { "_index" : "veggies", "_type" : "_doc", "_id" : "7" } }
```

Und die nächste Zeile mit den Daten könnte folgendermaßen aussehen:

```
{ "name":"kale", "color":"green", "classification":"leafy-green" }
```

Zusammengenommen stellen die Metadaten und die Daten eine einzelne Aktion in einem Massenvorgang dar. Sie können wie folgt viele Operationen in einer Anfrage ausführen:

```
POST /_bulk
{ "create" : { "_index" : "veggies", "_id" : "35" } }
{ "name":"kale", "color":"green", "classification":"leafy-green" }
{ "create" : { "_index" : "veggies", "_id" : "36" } }
{ "name":"spinach", "color":"green", "classification":"leafy-green" }
{ "create" : { "_index" : "veggies", "_id" : "37" } }
{ "name":"arugula", "color":"green", "classification":"leafy-green" }
{ "create" : { "_index" : "veggies", "_id" : "38" } }
{ "name":"endive", "color":"green", "classification":"leafy-green" }
{ "create" : { "_index" : "veggies", "_id" : "39" } }
{ "name":"lettuce", "color":"green", "classification":"leafy-green" }
{ "delete" : { "_index" : "vegetables", "_id" : "1" } }
```

Beachten Sie, dass die letzte Aktion vom Typ `delete` ist. Es gibt keine Daten nach der `delete`-Aktion.

Suchen nach Dokumenten

Jetzt, da Daten in Ihrem Cluster vorhanden sind, können Sie danach suchen. Sie können beispielsweise nach allen Wurzelgemüsen suchen oder eine Anzahl aller Blattgemüse ermitteln oder die Anzahl der pro Stunde protokollierten Fehler ermitteln.

Einfache Suchen

Eine einfache Suche sieht etwa folgendermaßen aus:

```
GET veggies/_search?q=name:l*
```

Die Anfrage erzeugt eine JSON-Antwort, die das Dokument zu Salaten enthält.

Erweiterte Suchen

Sie können erweiterte Suchvorgänge durchführen, indem Sie die Abfrageoptionen als JSON im Anfragetext angeben:

```
GET veggies/_search
{
  "query": {
    "term": {
      "name": "lettuce"
```

```
    }
  }
}
```

Dieses Beispiel erzeugt auch eine JSON-Antwort mit dem Dokument zu Salaten.

Sortieren

Sie können mehrere dieser Art von Abfragen mithilfe der Sortierung ausführen. Zuerst müssen Sie den Index neu erstellen, da bei der automatischen Feldzuordnung Typen ausgewählt wurden, die standardmäßig nicht sortiert werden können. Senden Sie die folgenden Anfragen, um den Index zu löschen und neu zu erstellen:

```
DELETE /veggies

PUT /veggies
{
   "mappings":{
      "properties":{
         "name":{
            "type":"keyword"
         },
         "color":{
            "type":"keyword"
         },
         "classification":{
            "type":"keyword"
         }
      }
   }
}
```

Füllen Sie dann den Index erneut mit Daten:

```
POST /_bulk
{ "create" : { "_index" : "veggies", "_id" : "7"  } }
{ "name":"kale", "color":"green", "classification":"leafy-green" }
{ "create" : { "_index" : "veggies", "_id" : "8" } }
{ "name":"spinach", "color":"green", "classification":"leafy-green" }
{ "create" : { "_index" : "veggies", "_id" : "9" } }
{ "name":"arugula", "color":"green", "classification":"leafy-green" }
{ "create" : { "_index" : "veggies", "_id" : "10" } }
```

```
{ "name":"endive", "color":"green", "classification":"leafy-green" }
{ "create" : { "_index" : "veggies", "_id" : "11" } }
{ "name":"lettuce", "color":"green", "classification":"leafy-green" }
```

Jetzt können Sie mit einer Sortierung suchen. Diese Anforderung fügt eine aufsteigende Sortierung nach der Klassifizierung hinzu:

```
GET veggies/_search
{
  "query" : {
    "term": { "color": "green" }
  },
  "sort" : [
      "classification"
  ]
}
```

Zugehörige Ressourcen

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Erste Schritte
- Indizierung von Daten
- Suchen von Daten

Tutorial: Migration zu AmazonOpenSearchBedienung

Index-Snapshots sind eine beliebte Methode, um von einem selbstverwalteten System zu migrierenOpenSearchoder veralteter Elasticsearch-Cluster zu AmazonOpenSearchBedienung. Im Großen und Ganzen besteht der Prozess aus den folgenden Schritten:

1. Erstellen Sie einen Snapshot des vorhandenen Clusters, und laden Sie den Snapshot in einen Amazon S3-Bucket hoch.
2. Erstelle eineOpenSearchDienstdomäne.
3. GebenOpenSearchDienstberechtigungen für den Zugriff auf den Bucket und stellen Sie sicher, dass Sie über die Berechtigungen zum Arbeiten mit Snapshots verfügen.
4. Stellen Sie den Snapshot auf dem wieder herOpenSearchDienstdomäne.

Dieser Walkthrough enthält detailliertere Schritte und gegebenenfalls alternative Optionen.

Snapshot erstellen und hochladen

Obwohl Sie das repository-s3-Plug-In verwenden können, um Snapshots direkt in S3 zu erstellen, müssen Sie das Plugin auf jedem Knoten installieren, `opensearch.yml` (oder `elasticsearch.yml` bei Verwendung eines Elasticsearch-Clusters) optimieren, jeden Knoten neu starten, Ihre AWS-Anmeldeinformationen hinzufügen und schließlich den Snapshot erstellen. Das Plugin ist eine großartige Option für den laufenden Einsatz oder für die Migration größerer Cluster.

Bei kleineren Clustern besteht ein einmaliger Ansatz darin, einen freigegebenen Dateisystem-Snapshot zu erstellen und dann die AWS CLI zum Hochladen in S3 zu verwenden. Wenn Sie bereits einen Snapshot haben, fahren Sie mit Schritt 4 fort.

So erstellen Sie einen Snapshot und laden ihn auf Amazon S3 hoch

1. Fügen Sie die `path.repo`-Einstellung zu `opensearch.yml` (oder `Elasticsearch.yml`) auf allen Knoten hinzu, und starten Sie dann jeden Knoten neu.

   ```
   path.repo: ["/my/shared/directory/snapshots"]
   ```

2. Sie müssen ein Snapshot-Repository registrieren, bevor Sie einen Schnappschuss erstellen können. Ein Repository ist nur ein Speicherort: ein freigegebenes Dateisystem, Amazon S3, Hadoop Distributed File System (HDFS) usw. In diesem Fall verwenden wir ein freigegebenes Dateisystem („fs“):

   ```
   PUT _snapshot/my-snapshot-repo-name
   {
     "type": "fs",
     "settings": {
       "location": "/my/shared/directory/snapshots"
     }
   }
   ```

3. Erstellen Sie den Snapshot:

   ```
   PUT _snapshot/my-snapshot-repo-name/my-snapshot-name
   {
     "indices": "migration-index1,migration-index2,other-indices-*",
     "include_global_state": false
   }
   ```

4. Installieren Sie die AWS CLI, und führen Sie `aws configure` aus, um Ihre Anmeldeinformationen hinzuzufügen.
5. Navigieren Sie zum Snapshot-Verzeichnis. Führen Sie dann die folgenden Befehle aus, um einen neuen S3-Bucket zu erstellen, und laden Sie den Inhalt des Snapshot-Verzeichnisses in diesen Bucket hoch:

   ```
   aws s3 mb s3://bucket-name --region us-west-2
   aws s3 sync . s3://bucket-name --sse AES256
   ```

   Abhängig von der Größe des Snapshots und der Geschwindigkeit Ihrer Internetverbindung kann dieser Vorgang eine Weile dauern.

Domain erstellen

Obwohl sich eine Domain am einfachsten mit der Konsole erstellen lässt, haben Sie in diesem Fall bereits das Terminal geöffnet und die AWS CLI installiert. Ändern Sie den folgenden Befehl, um eine Domain zu erstellen, die Ihren Anforderungen entspricht:

```
aws opensearch create-domain \
  --domain-name migration-domain \
  --engine-version OpenSearch_1.0 \
  --cluster-config InstanceType=c5.large.search,InstanceCount=2 \
  --ebs-options EBSEnabled=true,VolumeType=gp2,VolumeSize=100 \
  --node-to-node-encryption-options Enabled=true \
  --encryption-at-rest-options Enabled=true \
  --domain-endpoint-options EnforceHTTPS=true,TLSSecurityPolicy=Policy-Min-
TLS-1-2-2019-07 \
  --advanced-security-options
 Enabled=true,InternalUserDatabaseEnabled=true,MasterUserOptions='{MasterUserName=master-
user,MasterUserPassword=master-user-password}' \
  --access-policies '{"Version":"2012-10-17","Statement":
[{"Effect":"Allow","Principal":{"AWS":["*"]},"Action":
["es:ESHttp*"],"Resource":"arn:aws:es:us-west-2:123456789012:domain/migration-domain/
*"}]}' \
  --region us-west-2
```

Mit dem Befehl wird eine für das Internet zugängliche Domain mit zwei Datenknoten erstellt, die jeweils 100 GiB Speicher aufweisen. Er ermöglicht auch eine differenzierte Zugriffskontrolle mit HTTP-Standardauthentifizierung und allen Verschlüsselungseinstellungen. Benutze

dieOpenSearchServicekonsole, wenn Sie eine erweiterte Sicherheitskonfiguration benötigen, z. B. eine VPC.

Bevor Sie den Befehl ausführen, ändern Sie den Domain-Namen, die Anmeldeinformationen des Master-Benutzers und die Kontonummer. Geben Sie dasselbe anAWS-Regionden Sie für den S3-Bucket verwendet haben und einOpenSearch/Elasticsearch-Version, die mit Ihrem Snapshot kompatibel ist.

> **Important**
>
> Snapshots sind nur vorwärtskompatibel und auch nur mit einer Hauptversion. Sie können beispielsweise keinen Snapshot aus einem wiederherstellenOpenSearch1.xCluster auf einem Elasticsearch 7.xCluster, nur einOpenSearch1.xoder 2.xCluster. Kleinere Versionen sind ebenfalls von Bedeutung. Sie können einen Snapshot nicht aus einem selbstverwalteten 5.3.3-Cluster auf einem 5.3.2-Cluster wiederherstellenOpenSearchDienstdomäne. Wir empfehlen, die neueste Version von zu wählenOpenSearchoder Elasticsearch, das Ihr Snapshot unterstützt. Eine Tabelle mit kompatiblen Versionen finden Sie unter the section called “Verwenden eines Snapshots zum Migrieren von Daten”.

Erteilen Sie Berechtigungen für den Zugriff auf den S3-Bucket

In der AWS Identity and Access Management (IAM)-Konsole erstellen Sie eine Rolle mit den folgenden Berechtigungen und der folgenden Vertrauensstellung. Wählen Sie beim Erstellen der Rolle S3 als AWS-Service aus. Nennen Sie die Rolle `OpenSearchSnapshotRole`, damit sie leicht zu finden ist.

Berechtigungen

```
{
  "Version": "2012-10-17",
  "Statement": [{
      "Action": [
        "s3:ListBucket"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::bucket-name"
      ]
    },
```

```
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::bucket-name/*"
      ]
    }
  ]
}
```

Vertrauensstellung

```
{
  "Version": "2012-10-17",
  "Statement": [{
      "Effect": "Allow",
      "Principal": {
        "Service": "es.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Geben Sie dann Ihrer persönlichen IAM-Rolle die Berechtigungen, `OpenSearchSnapshotRole` zu übernehmen. Erstellen Sie die folgende Richtlinie und fügen Sie sie Ihrer Identität hinzu:

Berechtigungen

```
{
  "Version": "2012-10-17",
  "Statement": [{
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::123456789012:role/OpenSearchSnapshotRole"
    }
  ]
}
```

Ordnen Sie die Snapshot-Rolle in zuOpenSearchDashboards (wenn Sie eine differenzierte Zugriffskontrolle verwenden)

Wenn Sie distanzierte Zugriffskontrolle aktiviert haben, selbst wenn Sie HTTP-Basisauthentifizierung für alle anderen Zwecke verwenden, müssen Sie die`manage_snapshots`-Rolle zu Ihrer IAM-Rolle verwenden, damit Sie mit Snapshots arbeiten können.

Um Ihrer Identität Berechtigungen für die Arbeit mit Snapshots zu erteilen

1. Melden Sie sich bei Dashboards mit den Master-Benutzeranmeldeinformationen an, die Sie bei der Erstellung desOpenSearchDienstdomäne. Sie finden die Dashboard-URL imOpenSearchServicekonsole. Er hat die Form `https://`*`domain-endpoint`*`/_dashboards/`.
2. Wählen Sie im Hauptmenü Sicherheit, Rollen, und wählen Sie die Rolle manage_snapshots.
3. Wählen Sie Zugeordnete Benutzer, Mapping verwalten.
4. Fügen Sie den Domain-ARN Ihrer persönlichen IAM-Rolle in das entsprechende Feld ein. Der ARN nimmt eines der folgenden Formate an:

   ```
   arn:aws:iam::123456789123:user/user-name
   ```

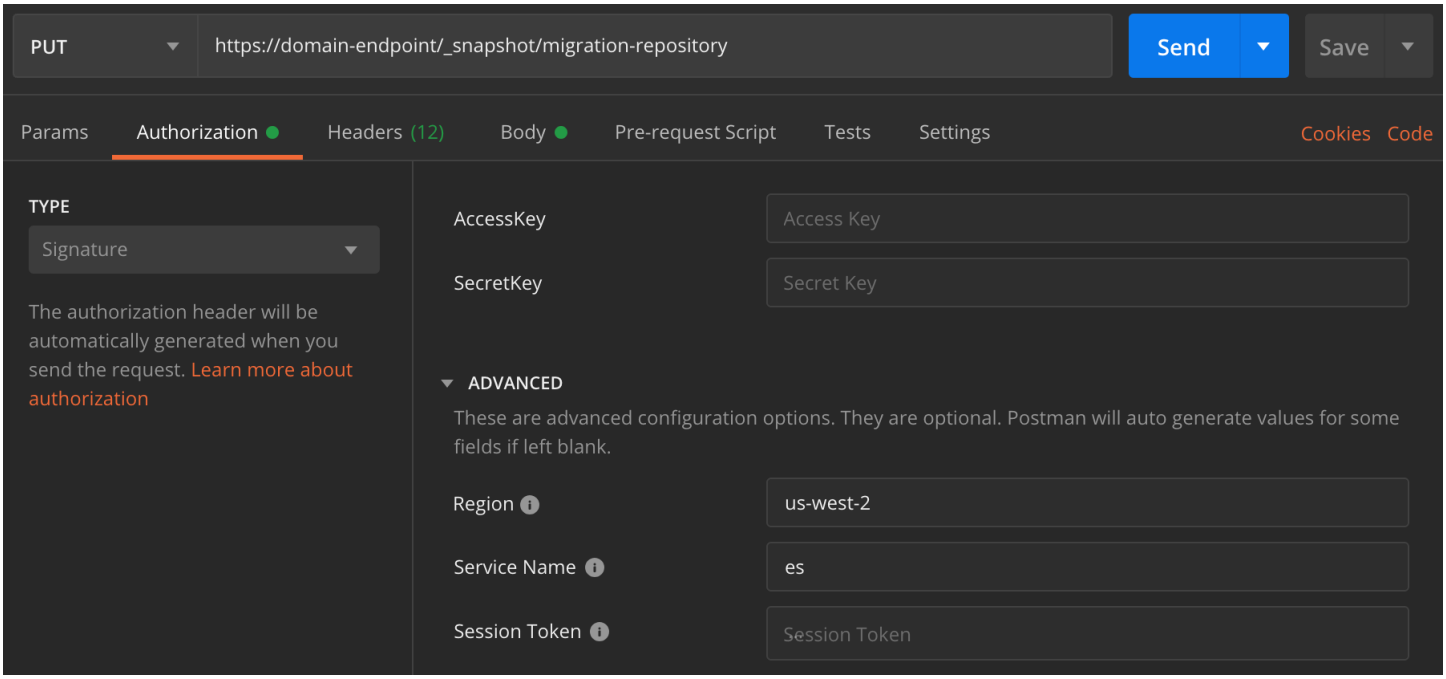
   ```
   arn:aws:iam::123456789123:role/role-name
   ```

5. Wählen Sie Map (Zuordnen) aus und bestätigen Sie, dass die Rolle unter Mapped users (Zugeordnete Benutzer) angezeigt wird.

Stellen Sie den Snapshot wieder her

Zu diesem Zeitpunkt haben Sie zwei Möglichkeiten, auf IhreOpenSearchServicedomäne: HTTP-Basisauthentifizierung mit Ihren Master-Benutzeranmeldeinformationen oderAWSAuthentifizierung mit Ihren IAM-Anmeldeinformationen. Da Snapshots Amazon S3 verwenden, das kein Konzept für den Master-Benutzer hat, müssen Sie Ihre IAM-Anmeldeinformationen verwenden, um das Snapshot-Repository bei IhremOpenSearchDienstdomäne.

Die meisten Programmiersprachen haben Bibliotheken, die beim Signieren von Anfragen helfen, aber der einfachere Ansatz besteht darin, ein Tool wiePostboteund geben Sie Ihre IAM-Anmeldedaten in dasAutorisierungAbschnitt.



So stellen Sie den Snapshot wieder her

1. Unabhängig davon, wie Sie Ihre Anfragen signieren, besteht der erste Schritt darin, das Repository zu registrieren:

```
PUT _snapshot/my-snapshot-repo-name
{
  "type": "s3",
  "settings": {
    "bucket": "bucket-name",
    "region": "us-west-2",
    "role_arn": "arn:aws:iam::123456789012:role/OpenSearchSnapshotRole"
  }
}
```

2. Führen Sie dann die Snapshots im Repository auf, und suchen Sie die Snapshots, die Sie wiederherstellen möchten. An diesem Punkt können Sie Postman weiter verwenden oder zu einem Werkzeug wie curl wechseln.

   Kurzschrift

   ```
   GET _snapshot/my-snapshot-repo-name/_all
   ```

   curl

```
curl -XGET -u 'master-user:master-user-password' https://domain-endpoint/
_snapshot/my-snapshot-repo-name/_all
```

3. Stellen Sie den Snapshot wieder her.

   Kurzschrift

   ```
   POST _snapshot/my-snapshot-repo-name/my-snapshot-name/_restore
   {
     "indices": "migration-index1,migration-index2,other-indices-*",
     "include_global_state": false
   }
   ```

   curl

   ```
   curl -XPOST -u 'master-user:master-user-password' https://domain-endpoint/
   _snapshot/my-snapshot-repo-name/my-snapshot-name/_restore \
     -H 'Content-Type: application/json' \
     -d '{"indices":"migration-index1,migration-index2,other-indices-
   *","include_global_state":false}'
   ```

4. Überprüfen Sie abschließend, ob Ihre Indizes wie erwartet wiederhergestellt wurden.

   Kurzschrift

   ```
   GET _cat/indices?v
   ```

   curl

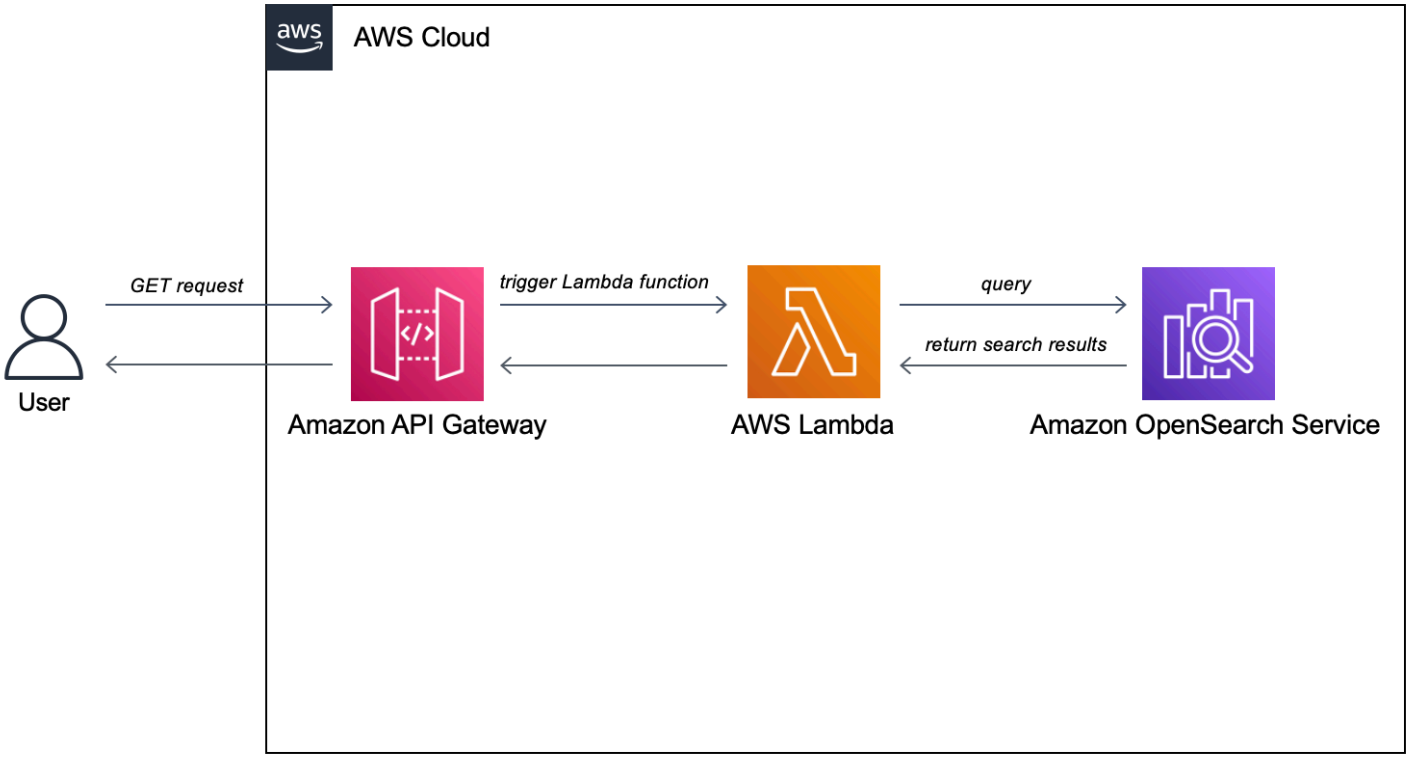
   ```
   curl -XGET -u 'master-user:master-user-password' https://domain-endpoint/_cat/
   indices?v
   ```

Zu diesem Zeitpunkt ist die Migration abgeschlossen. Sie könnten Ihre Kunden so konfigurieren, dass sie das neue verwendenOpenSearchServiceendpunkt,Größe der Domain ändernum Ihrem Workload gerecht zu werden, überprüfen Sie die Shard-Anzahl für Ihre Indizes und wechseln Sie zu einemIAM-Masterbenutzer, oder beginnen Sie mit der Erstellung von Visualisierungen inOpenSearchArmaturenbretter.

Tutorial: Eine Suchanwendung mit Amazon OpenSearch Service erstellen

Eine gängige Methode, um eine Suchanwendung mit Amazon OpenSearch Service zu erstellen, besteht darin, Webformulare zu verwenden, um Benutzeranfragen an einen Server zu senden. Anschließend können Sie den Server autorisieren, die OpenSearch APIs direkt aufzurufen und den Server Anfragen an den OpenSearch Service senden lassen. Wenn Sie clientseitigen Code schreiben möchten, der nicht auf einen Server angewiesen ist, sollten Sie jedoch die Sicherheits- und Leistungsrisiken ausgleichen. Es wird nicht empfohlen, unsignierten, öffentlichen Zugriff auf die OpenSearch APIs zuzulassen. Die Benutzer können auf ungesicherte Endpunkte zugreifen oder die Cluster-Leistung durch übermäßig umfangreiche Abfragen (oder zu viele Abfragen) beeinflussen.

In diesem Kapitel wird eine Lösung vorgestellt: Verwenden Sie Amazon API Gateway, um Benutzer auf eine Teilmenge der OpenSearch APIs zu beschränken und Anfragen von API Gateway AWS Lambda to OpenSearch Service zu signieren.



> **Note**
>
> Es gilt die standardmäßige API-Gateway- und Lamda-Preisgestaltung, aber innerhalb der begrenzten Nutzung dieses Tutorials sollten die Kosten vernachlässigbar sein.

Voraussetzungen

Voraussetzung für dieses Tutorial ist eine OpenSearch Service-Domain. Wenn Sie noch keine haben, folgen Sie den Schritten unter Erstellen einer OpenSearch Dienstdomäne, um eine zu erstellen.

Schritt 1: Indizieren von Beispieldaten

Laden Sie sample-movies.zip herunter, dekomprimieren Sie sie und verwenden Sie die _bulk-API-Operation zum Hinzufügen der 5 000 Dokumente in den `movies`-Index:

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/_bulk
{ "index": { "_index": "movies", "_id": "tt1979320" } }
{"directors":["Ron
 Howard"],"release_date":"2013-09-02T00:00:00Z","rating":8.3,"genres":
["Action","Biography","Drama","Sport"],"image_url":"http://ia.media-imdb.com/images/
M/MV5BMTQyMDE0MTY0OV5BMl5BanBnXkFtZTcwMjI2OTI0OQ@@._V1_SX400_.jpg","plot":"A re-
creation of the merciless 1970s rivalry between Formula One rivals James Hunt and
 Niki Lauda.","title":"Rush","rank":2,"running_time_secs":7380,"actors":["Daniel
 Brühl","Chris Hemsworth","Olivia Wilde"],"year":2013,"id":"tt1979320","type":"add"}
{ "index": { "_index": "movies", "_id": "tt1951264" } }
{"directors":["Francis Lawrence"],"release_date":"2013-11-11T00:00:00Z","genres":
["Action","Adventure","Sci-Fi","Thriller"],"image_url":"http://ia.media-imdb.com/
images/M/
MV5BMTAyMjQ3OTAxMzNeQTJeQWpwZ15BbWU4MDU0NzA1MzAx._V1_SX400_.jpg","plot":"Katniss
 Everdeen and Peeta Mellark become targets of the Capitol after
 their victory in the 74th Hunger Games sparks a rebellion in
 the Districts of Panem.","title":"The Hunger Games: Catching
 Fire","rank":4,"running_time_secs":8760,"actors":["Jennifer Lawrence","Josh
 Hutcherson","Liam Hemsworth"],"year":2013,"id":"tt1951264","type":"add"}
...
```

Beachten Sie, dass es sich bei dem obigen Befehl um einen Beispielbefehl mit einer kleinen Teilmenge der verfügbaren Daten handelt. Um den `_bulk` Vorgang auszuführen, müssen Sie den gesamten Inhalt der `sample-movies` Datei kopieren und einfügen. Weitere Anweisungen finden Sie unterthe section called “Option 2: Hochladen mehrerer Dokumente”.

Sie können auch den folgenden curl-Befehl verwenden, um dasselbe Ergebnis zu erzielen:

```
curl -XPOST -u 'master-user:master-user-password' 'domain-endpoint/_bulk' --data-binary
 @bulk_movies.json -H 'Content-Type: application/json'
```

Schritt 2: Lambda-Funktion erstellen und bereitstellen

Bevor Sie Ihre API in API Gateway erstellen, erstellen Sie die Lambda-Funktion, an die Anfragen weitergeleitet werden.

So erstellen Sie die Lambda-Funktion:

In dieser Lösung leitet API Gateway Anfragen an eine Lambda-Funktion weiter, die OpenSearch Service abfragt und Ergebnisse zurückgibt. Da diese Beispielfunktion externe Bibliotheken verwendet, müssen Sie ein Bereitstellungspaket erstellen und es auf Lambda hochladen.

Erstellen des Bereitstellungspakets

1. Öffnen Sie eine Eingabeaufforderung und erstellen Sie ein `my-opensearch-function`-Projektverzeichnis. Zum Beispiel unter macOS:

   ```
   mkdir my-opensearch-function
   ```

2. Navigieren Sie zum `my-sourcecode-function`-Projektverzeichnis.

   ```
   cd my-opensearch-function
   ```

3. Kopieren Sie den Inhalt des folgenden Python-Beispielcodes und speichern Sie ihn in einer neuen Datei mit dem Namen`opensearch-lambda.py`. Fügen Sie der Datei Ihre Region und Ihren Host-Endpunkt hinzu.

   ```
   import boto3
   import json
   import requests
   from requests_aws4auth import AWS4Auth

   region = '' # For example, us-west-1
   service = 'es'
   credentials = boto3.Session().get_credentials()
   awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
    session_token=credentials.token)
   ```

```
host = '' # The OpenSearch domain endpoint with https:// and without a trailing
 slash
index = 'movies'
url = host + '/' + index + '/_search'

# Lambda execution starts here
def lambda_handler(event, context):

    # Put the user query into the query DSL for more accurate search results.
    # Note that certain fields are boosted (^).
    query = {
        "size": 25,
        "query": {
            "multi_match": {
                "query": event['queryStringParameters']['q'],
                "fields": ["title^4", "plot^2", "actors", "directors"]
            }
        }
    }

    # Elasticsearch 6.x requires an explicit Content-Type header
    headers = { "Content-Type": "application/json" }

    # Make the signed HTTP request
    r = requests.get(url, auth=awsauth, headers=headers, data=json.dumps(query))

    # Create the response and add some extra content to support CORS
    response = {
        "statusCode": 200,
        "headers": {
            "Access-Control-Allow-Origin": '*'
        },
        "isBase64Encoded": False
    }

    # Add the search results to the response
    response['body'] = r.text
    return response
```

4. Installieren Sie die externen Bibliotheken in einem neuen `package` Verzeichnis.

```
pip3 install --target ./package boto3
pip3 install --target ./package requests
```

```
pip3 install --target ./package requests_aws4auth
```

5. Erstellen Sie ein Bereitstellungspaket, an dessen Stamm die installierte Bibliothek angefügt ist. Der folgende Befehl generiert eine `my-deployment-package.zip` Datei in Ihrem Projektverzeichnis.

```
cd package
zip -r ../my-deployment-package.zip .
```

6. Fügen Sie die `opensearch-lambda.py`-Datei dem Stamm der ZIP-Datei hinzu.

```
cd ..
zip my-deployment-package.zip opensearch-lambda.py
```

Weitere Informationen zum Erstellen von Lambda-Funktionen und Bereitstellungspaketen finden Sie unter Bereitstellen von Python-Lambda-Funktionen mit ZIP-Dateiarchiven imAWS Lambda-Entwicklerhandbuch und the section called “Erstellen des Lambda-Bereitstellungspakets” in diesem Leitfaden.

So erstellen Sie Ihre Funktion mit der Lambda-Konsole

1. Navigieren Sie zur Lambda-Konsole unter https://console.aws.amazon.com/lambda/home. Wählen Sie im linken Navigationsbereich Funktionen aus.
2. Wählen Sie Funktion erstellen aus.
3. Konfigurieren Sie die folgenden Felder:

   - Funktionsname: opensearch-function
   - Laufzeit: Python 3.9
   - Architektur: x86_64

   Behalten Sie alle anderen Standardoptionen bei und wählen Sie Funktion erstellen.
4. Wählen Sie auf der Seite mit der Funktionsübersicht im Abschnitt „Codequelle“ die Dropdownliste „Von hochladen“ und wählen Sie „.zip-Datei“ aus. Suchen Sie die **`my-deployment-package.zip`** Datei, die Sie erstellt haben, und wählen Sie Speichern aus.
5. Der Handler ist die Methode in Ihrem Funktions-Code, die Ereignisse verarbeitet. Wählen Sie unter Runtime-Einstellungen die Option Bearbeiten und ändern Sie den Namen des Handlers entsprechend dem Namen der Datei in Ihrem Bereitstellungspaket, in der sich die Lambda-

Funktion befindet. Da Ihre Datei benannt istopensearch-lambda.py, benennen Sie den Handler in umopensearch-lambda.lambda_handler. Weitere Informationen finden Sie unter Lambda-Funktions-Handler in Python.

Schritt 3: Erstellen Sie die API in API Gateway

Mit API Gateway können Sie eine eingeschränktere API erstellen und den Prozess der Interaktion mit der OpenSearch _search API vereinfachen. Mit API Gateway können Sie Sicherheitsfunktionen wie die Amazon-Cognito-Authentifizierung und die Anforderungsdrosselung aktivieren. Führen Sie die folgenden Schritte aus, um eine API zu erstellen und bereitzustellen:

Erstellen und Konfigurieren Sie die API

So erstellen Sie Ihre API über die API-Gateway-Konsole

1. Navigieren Sie zur API Gateway Gateway-Konsole unter https://console.aws.amazon.com/apigateway/home. Wählen Sie im linken Navigationsbereich APIs aus.
2. Suchen Sie die REST-API (nicht privat) und wählen Sie Build aus.
3. Suchen Sie auf der folgenden Seite nach dem Abschnitt Neue API erstellen und stellen Sie sicher, dass Neue API ausgewählt ist.
4. Konfigurieren Sie die folgenden Felder:
   - API-Name: opensearch-api
   - Beschreibung: Öffentliche API für die Suche nach einer Amazon OpenSearch Service-Domain
   - Endpunkttyp: Regional
5. Wählen Sie Create API (API erstellen) aus.
6. Wählen Sie Aktionen und Methode erstellen aus.
7. Wählen Sie im Dropdown-Menü GET aus und klicken Sie zur Bestätigung auf das Häkchen.
8. Konfigurieren Sie die folgenden Einstellungen und wählen Sie dann Speichern:

Einstellung	Wert
Integrationstyp	Lambda-Funktion
Lambda-Proxy-Integration verwenden	Ja

Einstellung	Wert
Lambda-Region	*us-west-1*
Lambda-Funktion	opensearch-lambda
Standardzeitüberschreitung verwenden	Ja

Konfigurieren Sie die Methodenanforderung

Klicken Sie auf Methodenanforderung und konfigurieren Sie die folgenden Einstellungen:

Einstellung	Wert
Autorisierung	NONE
Anforderungs-Validator	Abfragezeichenfolgeparameter und Header validieren
API-Schlüssel erforderlich	false

Wählen Sie unter URL-Abfragezeichenfolge-Parameter die Option Abfragezeichenfolge hinzufügen aus und konfigurieren Sie den folgenden Parameter:

Einstellung	Wert
Name	q
Erforderlich	Ja

Stellen Sie die API bereit und Konfigurieren Sie eine Stufe

Mit der API Gateway-Konsole können Sie eine API bereitstellen, indem Sie eine Bereitstellung erstellen und sie mit einer neuen oder bestehenden Stufe verknüpfen.

1. Wählen Sie Aktionen und Bereitstellen der API aus.

2. Für Bereitstellungsstufe, wählen Sie Neue Stufe und nennen Sie die Stufe `opensearch-api-test`.
3. Wählen Sie Bereitstellen aus.
4. Konfigurieren Sie die folgenden Einstellungen im Stufen-Editor und wählen Sie dann Änderungen speichern:

Einstellung	Wert
Drosselung aktivieren	Ja
Rate (Tarif)	1000
Burst	500

Diese Einstellungen konfigurieren eine API, die nur über eine Methode verfügt: eine `GET`-Anforderung an den Endpunkt-Root (`https://`*`some-id`*`.execute-api.`*`us-west-1`*`.amazonaws.com/search-es-api-test`). Die Anforderung erfordert einen einzelnen Parameter (`q`), die Abfragezeichenfolge, nach der gesucht werden soll. Beim Aufruf übergibt die Methode die Anforderung an Lambda, die die `opensearch-lambda`-Funktion ausführt. Weitere Informationen finden Sie unter Erstellen einer API in Amazon API Gateway und Bereitstellen einer REST API in Amazon API Gateway.

Schritt 4: (Optional) Ändern der Domain-Zugriffsrichtlinie

Ihre OpenSearch Service-Domain muss es der Lambda-Funktion ermöglichen, `GET` Anfragen an den `movies` Index zu stellen. Wenn Ihre Domain eine offene Zugriffsrichtlinie hat, bei der eine abgestufte Zugriffssteuerung aktiviert ist, können Sie sie so wie sie ist belassen:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "es:*",
      "Resource": "arn:aws:es:us-west-1:123456789012:domain/domain-name/*"
```

```
    }
  ]
}
```

Alternativ können Sie Ihre Domain-Zugriffsrichtlinie detaillierter gestalten. Beispielsweise gewährt die folgende Richtlinie `opensearch-lambda-role` (erstellt durch Lambda) Schreibzugriff auf den `movies`-Index. Um den genauen Namen der Rolle zu erhalten, die Lambda automatisch erstellt, rufen Sie die AWS Identity and Access Management (IAM)-Konsole auf, wählen Sie Rollen aus und suchen Sie nach „lambda“.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:role/service-role/opensearch-lambda-
role-1abcdefg"
      },
      "Action": "es:ESHttpGet",
      "Resource": "arn:aws:es:us-west-1:123456789012:domain/domain-name/movies/_search"
    }
  ]
}
```

> **Important**
>
> Wenn Sie eine detaillierte Zugriffskontrolle für die Domain aktiviert haben, müssen Sie die Rolle auch einem Benutzer in OpenSearch Dashboards zuordnen, da andernfalls Berechtigungsfehler angezeigt werden.

Weitere Informationen zu Zugriffsrichtlinien finden Sie unter the section called “Konfigurieren von Zugriffsrichtlinien”.

Zuordnen der Lambda-Rolle (bei Verwendung einer differenzierten Zugriffskontrolle)

Die differenzierte Zugriffskontrolle führt einen zusätzlichen Schritt ein, bevor Sie die Anwendung testen können. Auch wenn Sie die HTTP-Standardauthentifizierung für alle anderen Zwecke

verwenden, müssen Sie die Lambda-Rolle einem Benutzer zuordnen, andernfalls werden Berechtigungsfehler angezeigt.

1. Navigieren Sie zur OpenSearch Dashboard-URL für die Domain.
2. Wählen Sie im Hauptmenü Sicherheit, Rollen und dann den Link zu der Rolle aus`all_access`, der Sie die Lambda-Rolle zuordnen müssen.
3. Wählen Sie Zugeordnete Benutzer, Mapping verwalten.
4. Fügen Sie unter Backend roles (Backend-Rollen) den Amazon-Ressourcennamen (ARN) der Lambda-Rolle hinzu. Der ARN sollte die Form von habe`arn:aws:iam::`*`123456789123`*`:role/service-role/`*`opensearch-lambda-role-1abcdefg`*.
5. Wählen Sie Zuordnen und bestätigen Sie, dass der Benutzer oder die Rolle unter Zugeordnete Benutzer angezeigt wird.

Schritt 5: Testen der Webanwendung

So testen Sie die Webanwendung

1. Laden Sie sample-site.zip herunter, dekomprimieren Sie sie und öffnen Sie `scripts/search.js` in Ihrem bevorzugten Texteditor.
2. Aktualisieren Sie die `apigatewayendpoint` Variable so, dass sie auf Ihren API-Gateway-Endpunkt zeigt, und fügen Sie am Ende des angegebenen Pfads einen Backslash hinzu. Sie können den Endpunkt schnell im API Gateway finden, indem Sie Phasen und den Namen der API auswählen. Die `apigatewayendpoint` Variable sollte die Form von/haben. `https://`*`some-id`*`.execute-api.`*`us-west-1`*`.amazonaws.com/opensearch-api-test`
3. Öffnen Sie `index.html` und versuchen Sie, nach thor, house und einigen anderen Begriffen zu suchen.

Movie Search

thor

Found 7 results.

Thor

2011 — The powerful but arrogant god Thor is cast out of Asgard to live amongst humans in Midgard (Earth), where he soon becomes one of their finest defenders.

Thor: The Dark World

2013 — Faced with an enemy that even Odin and Asgard cannot withstand, Thor must embark on his most perilous and personal journey yet, one that will reunite him with Jane Foster and force him to sacrifice everything to save us all.

Vikingdom

2013 — A forgotten king, Eirick, is tasked with the impossible odds to defeat Thor, the God of Thunder.

Beheben von CORS-Fehlern

Auch wenn die Lambda-Funktion Inhalte in die Antwort einschließt, um CORS zu unterstützen, kann der folgende Fehler auftreten:

```
Access to XMLHttpRequest at '<api-gateway-endpoint>' from origin 'null' has been
 blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present in the
 requested resource.
```

Versuchen Sie in diesem Fall Folgendes:

1. Aktivieren Sie CORS in der GET-Ressource. Unter Advanced legen Sie Access-Control-Allow-Credentials auf `'true'` fest.
2. Stellen Sie Ihre API erneut in API Gateway (Aktionen,API bereitstellen) bereit.
3. Löschen Sie Ihren Lambda-Funktionsauslöser und fügen Sie ihn erneut hinzu. Fügen Sie sie hinzu, fügen Sie sie erneut hinzu, wählen Sie Auslöser hinzufügen und erstellen Sie den HTTP-Endpunkt, der Ihre Funktion aufruft. Der Auslöser muss die folgende Konfiguration haben:

Auslöser	API	Bereitstellungsstufe	Sicherheit
API Gateway	opensearch-api	opensearch-api-test	Öffnen

Nächste Schritte

Dieses Kapitel ist nur ein Ausgangspunkt zur Demonstration eines Konzepts. Sie sollten die folgenden Änderungen in Erwägung ziehen:

- Fügen Sie der OpenSearch Service-Domain Ihre eigenen Daten hinzu.
- Fügen Sie Methoden Ihrer API hinzu.
- Ändern Sie in der Lambda-Funktion die Suchanfrage oder steigern Sie andere Felder.
- Gestalten Sie die Ergebnisse unterschiedlich oder ändern Sie `search.js`, um dem Benutzer verschiedene Felder anzuzeigen.

Tutorial: Visualisierung von Kunden-Support-Aufrufen mit OpenSearch Service und Dashboards OpenSearch

Dieses Kapitel enthält eine vollständige Schritt-für-Schritt-Anleitung für folgendes Szenario: In einem Unternehmen geht eine bestimmte Anzahl an Anrufen beim Kundensupport ein. Diese sollen analysiert werden. Wie lauteten die Themen der einzelnen Anrufe? Wie viele Gespräche waren positiv? Wie viele Gespräche waren negativ? Wie können Vorgesetzte nach den Transkripten der Anrufe suchen oder diese überprüfen?

Zu einem manuellen Workflow könnte das Anhören von Aufzeichnungen, das Notieren des Themas des Anrufs und die Feststellung, ob die Interaktion mit dem Kunden positiv war, gehören.

Dieser Prozess wäre aber sehr arbeitsaufwendig. Wenn man von einer durchschnittlichen Anrufdauer von 10 Minuten ausgeht, können Mitarbeiter 48 Anrufe pro Tag entgegennehmen. Ohne menschliche Voreingenommenheit wären die Daten, die generiert werden würden, sehr zuverlässig, die Menge der Daten aber minimal: Sie würden nur Aufschluss über das Thema des Anrufs und darüber geben, ob ein Kunde zufrieden war oder nicht. Weitere Daten, beispielsweise ein vollständiges Transkript, würde enorm viel Zeit in Anspruch nehmen.

Mit Amazon S3, Amazon Transcribe, Amazon Comprehend und Amazon OpenSearch Service können Sie einen ähnlichen Prozess mit sehr wenig Code automatisieren und erhalten viel mehr Daten. Sie könnten beispielsweise ein vollständiges Transkript des Anrufs bekommen sowie Schlüsselwörter und eine Angabe zur allgemeinen "Stimmung" des Anrufs (positiv, negativ, neutral oder gemischt). Anschließend können Sie mit OpenSearch Hilfe von OpenSearch Dashboards Daten suchen und visualisieren.

Sie können diese Anleitung unverändert nutzen. Die Idee dahinter ist jedoch, eine Idee davon zu bekommen, wie Sie Ihre JSON-Dokumente anreichern können, ehe Sie diese in OpenSearch Service indizieren.

Geschätzte Kosten

Im Allgemeinen sollte die Durchführung der Schritte in dieser Anleitung weniger als 2 USD kosten. Es werden folgende Ressourcen verwendet:

- S3-Bucket mit weniger als 100 MB übertragenen und gespeicherten Daten

  Weitere Informationen finden Sie unter Amazon S3 – Preise.

- OpenSearchService-Domain mit einer `t2.medium` Instance und 10 GiB EBS-Speicher für mehrere Stunden

  Weitere Informationen finden Sie unter OpenSearchAmazon-Preise.
- Mehrere Aufrufe von Amazon Transcribe

  Weitere Informationen finden Sie unter Amazon Transcribe – Preise.
- Mehrere natürliche Sprachverarbeitungsaufrufe an Amazon Comprehend

  Weitere Informationen finden Sie unter Amazon Comprehend – Preise.

Themen

Schritt 1: Konfigurieren der Voraussetzungen

Zum Fortfahren benötigen Sie die folgenden Ressourcen.

Voraussetzung	Beschreibung
Amazon-S3-Bucket	Weitere Informationen erhalten Sie unter Erstellen eines Buckets im Benutzerhandbuch für Amazon Simple Storage Service.
OpenSearchDienstdomäne	Das Ziel für die Daten. Weitere Informationen finden Sie unter Erstellen von OpenSearch Servicedomänen.

Wenn Sie noch nicht über diese Ressourcen verfügen, können Sie diese mit den folgenden AWS CLI-Befehlen erstellen:

```
aws s3 mb s3://my-transcribe-test --region us-west-2
```

```
aws opensearch create-domain --domain-name my-transcribe-test --engine-version
 OpenSearch_1.0 --cluster-config  InstanceType=t2.medium.search,InstanceCount=1
 --ebs-options EBSEnabled=true,VolumeType=standard,VolumeSize=10 --access-
policies '{"Version":"2012-10-17","Statement":[{"Effect":"Allow","Principal":
{"AWS":"arn:aws:iam::123456789012:root"},"Action":"es:*","Resource":"arn:aws:es:us-
west-2:123456789012:domain/my-transcribe-test/*"}]}' --region us-west-2
```

> **Note**
>
> Diese Befehle verwenden die `us-west-2`-Region. Sie können jedoch jede Region nutzen, die von Amazon Comprehend unterstützt wird. Weitere Informationen finden Sie in unter Allgemeine AWS-Referenz.

Schritt 2: Kopieren des Beispiel-Codes

1. Kopieren Sie den folgenden Python-3-Beispiel-Code in eine neue Datei namens `call-center.py`:

```
import boto3
import datetime
import json
import requests
from requests_aws4auth import AWS4Auth
import time
import urllib.request

# Variables to update
audio_file_name = '' # For example, 000001.mp3
bucket_name = '' # For example, my-transcribe-test
domain = '' # For example, https://search-my-transcribe-test-12345.us-
west-2.es.amazonaws.com
index = 'support-calls'
type = '_doc'
region = 'us-west-2'

# Upload audio file to S3.
s3_client = boto3.client('s3')

audio_file = open(audio_file_name, 'rb')
```

```
print('Uploading ' + audio_file_name + '...')
response = s3_client.put_object(
    Body=audio_file,
    Bucket=bucket_name,
    Key=audio_file_name
)

# # Build the URL to the audio file on S3.
# # Only for the us-east-1 region.
# mp3_uri = 'https://' + bucket_name + '.s3.amazonaws.com/' + audio_file_name

# Get the necessary details and build the URL to the audio file on S3.
# For all other regions.
response = s3_client.get_bucket_location(
    Bucket=bucket_name
)
bucket_region = response['LocationConstraint']
mp3_uri = 'https://' + bucket_name + '.s3-' + bucket_region + '.amazonaws.com/' +
 audio_file_name

# Start transcription job.
transcribe_client = boto3.client('transcribe')

print('Starting transcription job...')
response = transcribe_client.start_transcription_job(
    TranscriptionJobName=audio_file_name,
    LanguageCode='en-US',
    MediaFormat='mp3',
    Media={
        'MediaFileUri': mp3_uri
    },
    Settings={
        'ShowSpeakerLabels': True,
        'MaxSpeakerLabels': 2 # assumes two people on a phone call
    }
)

# Wait for the transcription job to finish.
print('Waiting for job to complete...')
while True:
    response =
 transcribe_client.get_transcription_job(TranscriptionJobName=audio_file_name)
    if response['TranscriptionJob']['TranscriptionJobStatus'] in ['COMPLETED',
 'FAILED']:
```

```
        break
    else:
        print('Still waiting...')
    time.sleep(10)

transcript_uri = response['TranscriptionJob']['Transcript']['TranscriptFileUri']

# Open the JSON file, read it, and get the transcript.
response = urllib.request.urlopen(transcript_uri)
raw_json = response.read()
loaded_json = json.loads(raw_json)
transcript = loaded_json['results']['transcripts'][0]['transcript']

# Send transcript to Comprehend for key phrases and sentiment.
comprehend_client = boto3.client('comprehend')

# If necessary, trim the transcript.
# If the transcript is more than 5 KB, the Comprehend calls fail.
if len(transcript) > 5000:
    trimmed_transcript = transcript[:5000]
else:
    trimmed_transcript = transcript

print('Detecting key phrases...')
response = comprehend_client.detect_key_phrases(
    Text=trimmed_transcript,
    LanguageCode='en'
)

keywords = []
for keyword in response['KeyPhrases']:
    keywords.append(keyword['Text'])

print('Detecting sentiment...')
response = comprehend_client.detect_sentiment(
    Text=trimmed_transcript,
    LanguageCode='en'
)

sentiment = response['Sentiment']

# Build the Amazon OpenSearch Service URL.
id = audio_file_name.strip('.mp3')
url = domain + '/' + index + '/' + type + '/' + id
```

```
# Create the JSON document.
json_document = {'transcript': transcript, 'keywords': keywords, 'sentiment':
 sentiment, 'timestamp': datetime.datetime.now().isoformat()}

# Provide all details necessary to sign the indexing request.
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region,
 'opensearchservice', session_token=credentials.token)

# Index the document.
print('Indexing document...')
response = requests.put(url, auth=awsauth, json=json_document, headers=headers)

print(response)
print(response.json())
```

2. Aktualisieren Sie die ersten sechs Variablen.
3. Installieren Sie die erforderlichen Pakete mit den folgenden Befehlen:

```
pip install boto3
pip install requests
pip install requests_aws4auth
```

4. Platzieren Sie Ihre MP3-Datei im selben Verzeichnis wie `call-center.py` und führen Sie das Skript aus. Hier ein Beispiel für eine Ausgabe:

```
$ python call-center.py
Uploading 000001.mp3...
Starting transcription job...
Waiting for job to complete...
Still waiting...
Still waiting...
Still waiting...
Still waiting...
Still waiting...
Still waiting...
Still waiting...
Detecting key phrases...
Detecting sentiment...
Indexing document...
<Response [201]>
```

```
{u'_type': u'call', u'_seq_no': 0, u'_shards': {u'successful': 1, u'failed': 0,
 u'total': 2}, u'_index': u'support-calls4', u'_version': 1, u'_primary_term': 1,
 u'result': u'created', u'_id': u'000001'}
```

`call-center.py` führt eine Reihe von Operationen durch:

1. Das Skript lädt eine Audio-Datei (in diesem Fall eine MP3, Amazon Transcribe unterstützt aber viele Formate) in Ihren S3-Bucket hoch.
2. Es sendet die URL der Audio-Datei an Amazon Transcribe und wartet, bis der Transkriptionsauftrag abgeschlossen ist.

   Die Zeit bis zum Abschließen des Transkriptionsauftrags hängt von der Länge der Audiodatei ab. Gehen Sie aber von Minuten und nicht Sekunden aus.

   > **Tip**
   >
   > Zur Verbesserung der Qualität der Transkription können Sie ein benutzerdefiniertes Vokabular für Amazon Transcribe konfigurieren.

3. Nach Abschluss des Transkriptionsauftrag extrahiert das Skript das Transkript, kürzt es auf 5.000 Zeichen und sendet es zwecks Schlüsselwort- und Stimmungsanalyse an Amazon Comprehend.
4. Abschließend fügt das Skript das vollständige Transkript, die Schlüsselwörter, die Stimmungsdaten und den aktuellen Zeitstempel zu einem JSON-Dokument hinzu und indiziert es in OpenSearch Service.

> **Tip**
>
> LibriVoxhat gemeinfreie Hörbücher, die Sie zum Testen verwenden können.

(Optional) Schritt 3: Indizieren von Beispieldaten

Wenn Sie keine Aufrufaufzeichnungen zur Hand haben – und wer hat das schon? – können Sie die Beispieldokumente in der Datei sample-calls.zip indizieren, die mit dem vergleichbar sind, was `call-center.py` produziert.

1. Erstellen Sie eine Datei namens `bulk-helper.py`:

```
import boto3
from opensearchpy import OpenSearch, RequestsHttpConnection
import json
from requests_aws4auth import AWS4Auth

host = '' # For example, my-test-domain.us-west-2.es.amazonaws.com
region = '' # For example, us-west-2
service = 'es'

bulk_file = open('sample-calls.bulk', 'r').read()

credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)

search = OpenSearch(
    hosts = [{'host': host, 'port': 443}],
    http_auth = awsauth,
    use_ssl = True,
    verify_certs = True,
    connection_class = RequestsHttpConnection
)

response = search.bulk(bulk_file)
print(json.dumps(response, indent=2, sort_keys=True))
```

2. Aktualisieren Sie die ersten zwei Variablen für `host` und `region`.
3. Installieren Sie das erforderlich Paket mit folgendem Befehl:

```
pip install opensearch-py
```

4. Laden Sie die Datei sample-calls.zip herunter und entpacken Sie sie.
5. Speichern Sie `sample-calls.bulk` in demselben Verzeichnis wie `bulk-helper.py` und führen Sie das Helferobjekt aus. Hier ein Beispiel für eine Ausgabe:

```
$ python bulk-helper.py
{
  "errors": false,
  "items": [
    {
      "index": {
```

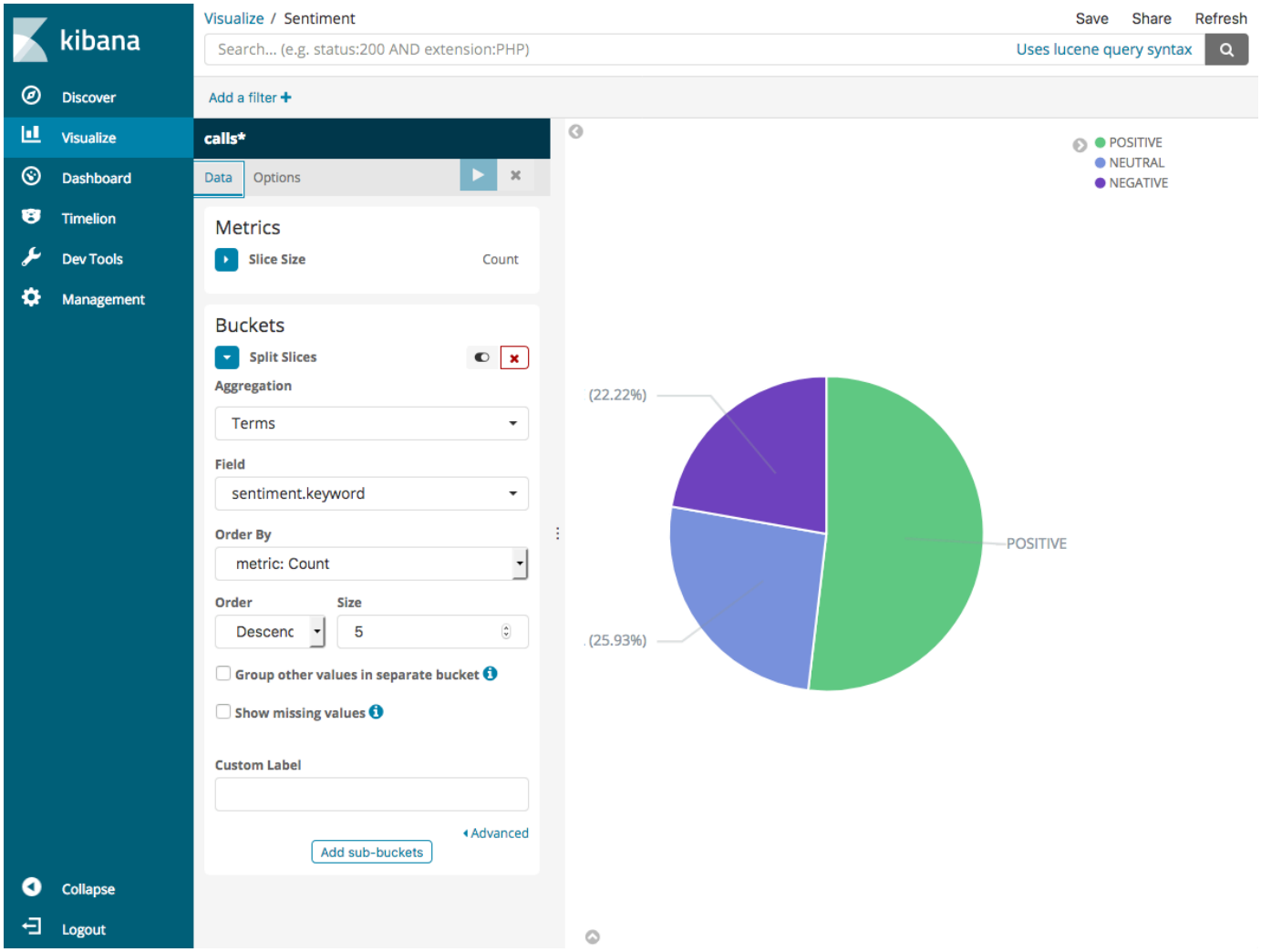
```
        "_id": "1",
        "_index": "support-calls",
        "_primary_term": 1,
        "_seq_no": 42,
        "_shards": {
          "failed": 0,
          "successful": 1,
          "total": 2
        },
        "_type": "_doc",
        "_version": 9,
        "result": "updated",
        "status": 200
      }
    },
    ...
  ],
  "took": 27
}
```

Schritt 4: Analysieren und Visualisieren Sie Ihre Daten

Nachdem Sie nun über einige Daten in OpenSearch Service verfügen, können Sie diese mit OpenSearch Dashboards visuell darstellen.

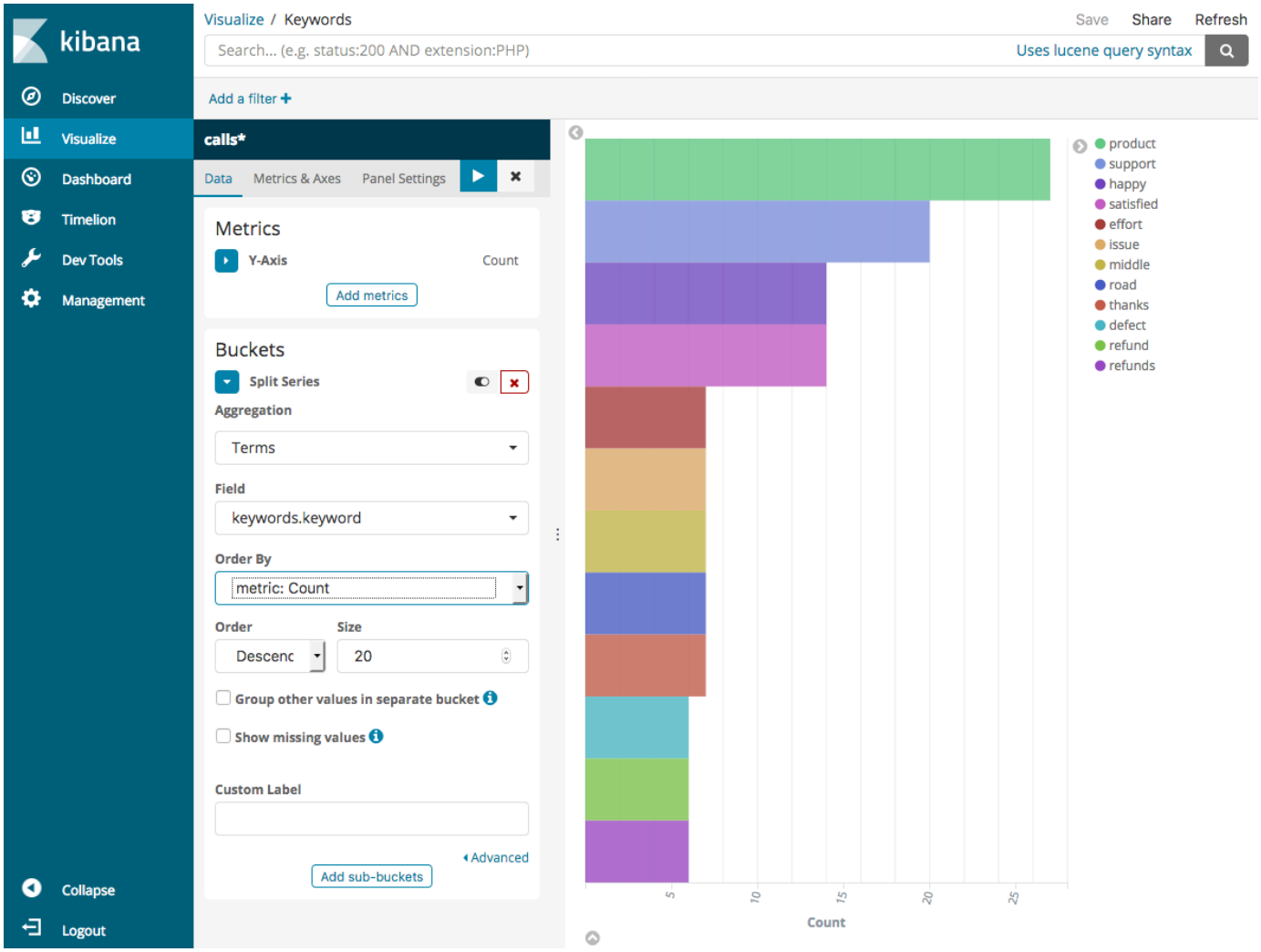
1. Navigieren Sie zu `https://search-`*`domain`*`.`*`region`*`.es.amazonaws.com/_dashboards`.
2. Bevor Sie OpenSearch Dashboards verwenden können, benötigen Sie ein Index-Muster. Dashboards verwendet Index-Muster, um ihre Analyse auf einen oder mehrere Indizes einzugrenzen. Um den `support-calls`-Index abzugleichen, den `call-center.py` erstellt hat, gehen Sie zu Stack Management, Index Patterns, und definieren Sie ein Indexmuster von `support*`, und wählen Sie dann Nächster Schritt.
3. Wählen Sie für Time Filter field name (Feldname für Zeitfilter) die Option timestamp (Zeitstempel) aus.
4. Sie können nun mit dem Generieren von Visualisierungen beginnen. Wählen Sie Visualize (Visualisieren) aus und fügen Sie eine neue Visualisierung hinzu.
5. Wählen Sie das Kreisdiagramm und das `support*`-Index-Muster aus.
6. Die Standardvisualisierung ist eine eher grundlegende. Eine detaillierte Visualisierung erhalten Sie, wenn Sie Split Slices (Slices aufteilen) auswählen.

Wählen Sie unter Aggregation den Eintrag Terms (Bedingungen) aus. Wählen Sie für Field (Feld) sentiment.keyword aus. Klicken Sie dann auf Apply changes (Änderungen übernehmen) und Save (Speichern).

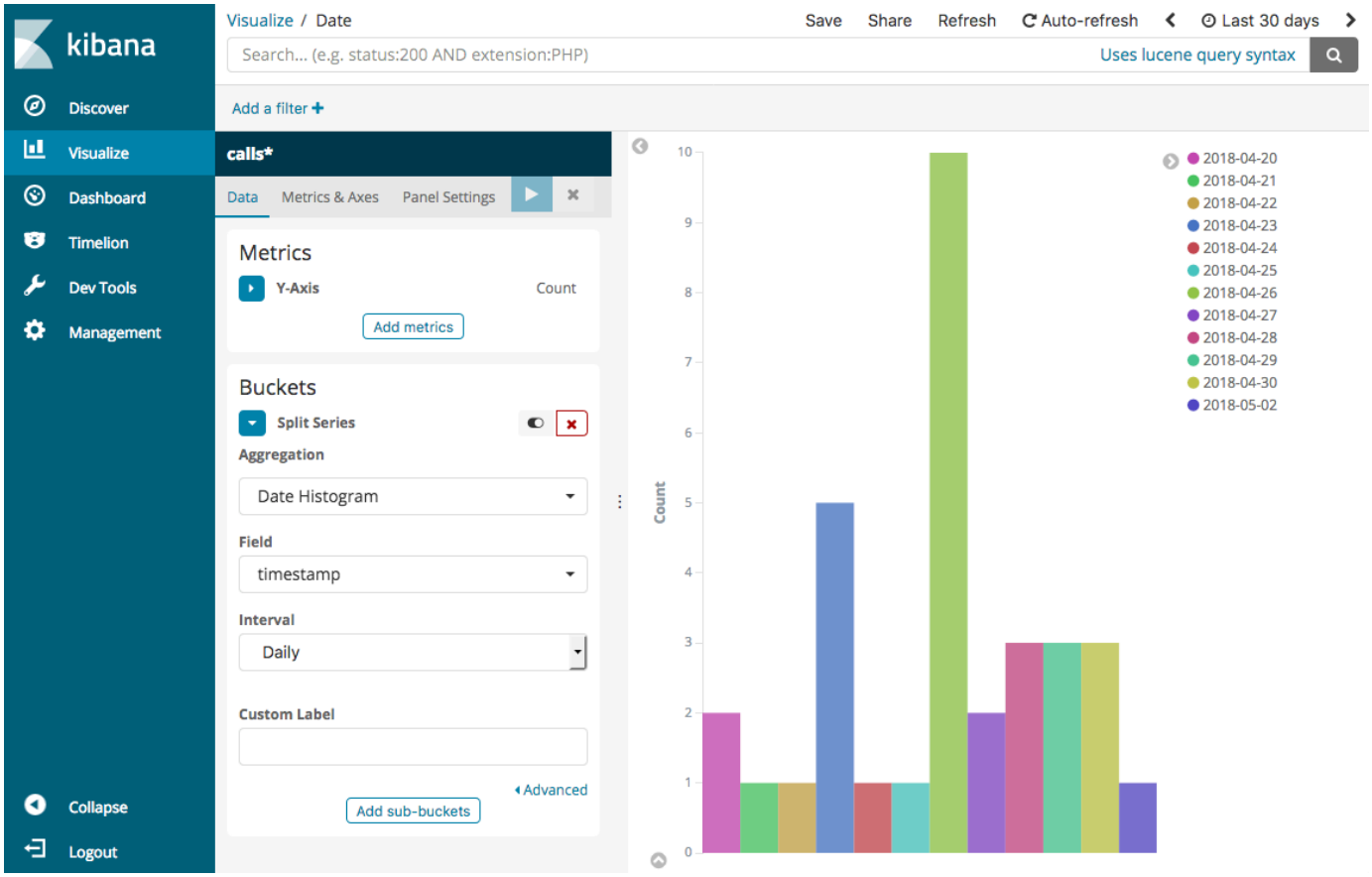


7. Kehren Sie zur Seite Visualize (Visualisieren) zurück und fügen Sie eine weitere Visualisierung hinzu. Wählen Sie dieses Mal das horizontale Balkendiagramm aus.
8. Wählen Sie Split Series (Serie aufteilen) aus.

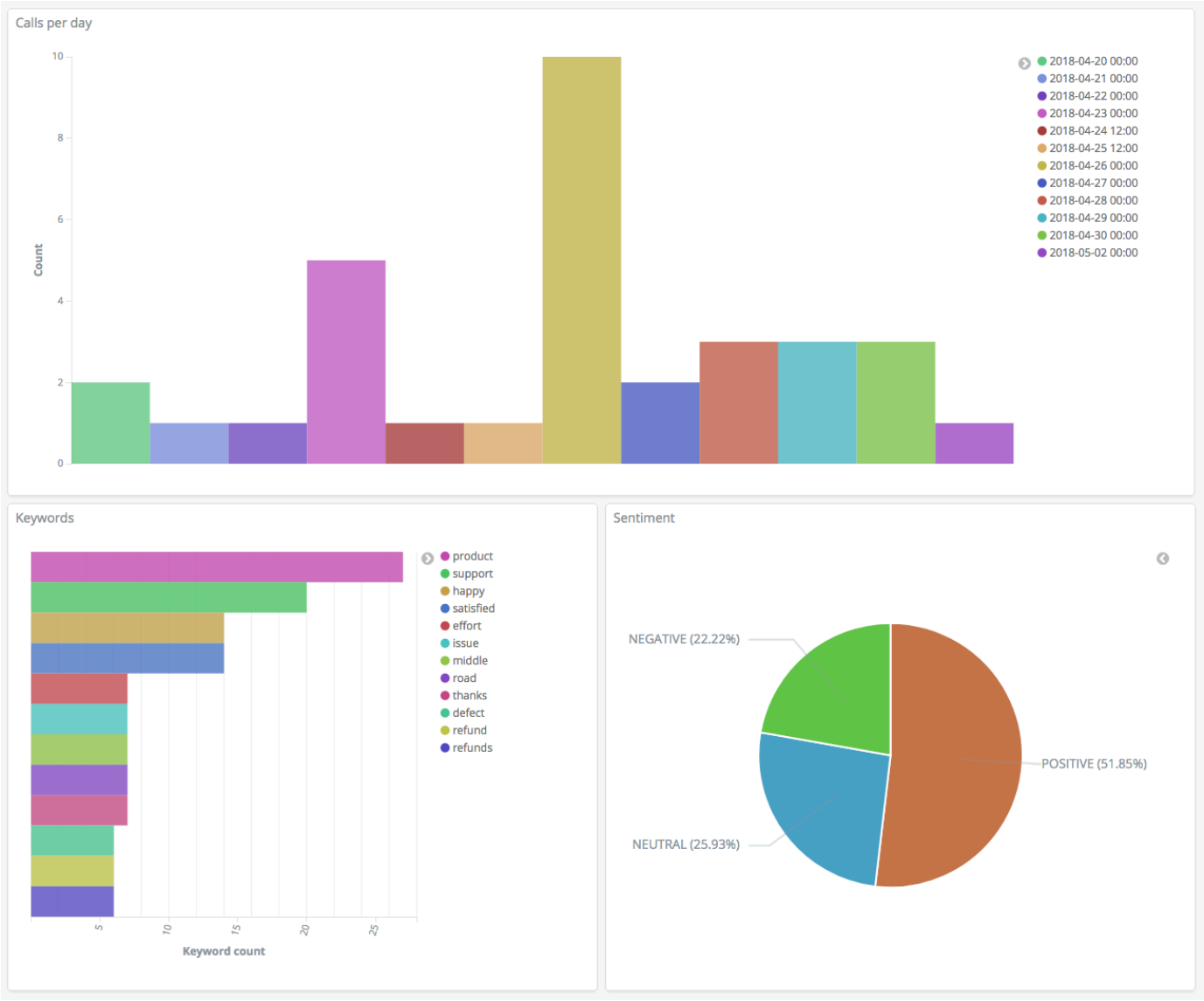
   Wählen Sie unter Aggregation den Eintrag Terms (Bedingungen) aus. Wählen Sie für Field (Feld) keywords.keyword aus und ändern Sie Size (Größe) in 20. Klicken Sie dann auf Apply changes (Änderungen übernehmen) und Save (Speichern).



9. Kehren Sie zur Seite Visualize (Visualisieren) zurück und fügen Sie eine letzte Visualisierung, ein vertikales Balkendiagramm, hinzu.
10. Wählen Sie Split Series (Serie aufteilen) aus. Wählen Sie für Aggregation (Aggregation) Date Histogram (Datumshistogramm) aus. Wählen Sie für Field (Feld) timestamp aus und ändern Sie das Interval (Intervall) in Daily (Täglich).
11. Wählen Sie Metrics & Axes (Metriken & Achsen) aus und ändern Sie den Mode (Modus) in normal.
12. Klicken Sie auf Apply changes (Änderungen übernehmen) und Save (Speichern).



13. Nachdem Sie nun drei Visualisierungen haben, können Sie diese zu einer Dashboard-Visualisierung hinzufügen. Klicken Sie auf Dashboard, erstellen Sie ein Dashboard und fügen Sie Ihre Visualisierungen hinzu.



Schritt 5: Bereinigen Sie Ressourcen und nächste Schritte

Um unnötige Kosten zu vermeiden, löschen Sie den S3-Bucket und die OpenSearch Service-Domäne. Weitere Informationen finden Sie unter Löschen eines Buckets im Amazon Simple Storage Service-Benutzerhandbuch und Löschen einer OpenSearch Service-Domain in diesem Handbuch.

Transkripte erfordern weniger Speicherplatz als MP3-Dateien. Sie können die Einstellungen für Ihr MP3-Aufbewahrungsfenster ändern – beispielsweise können Sie die dreimonatige Aufbewahrungsdauer für Anrufaufzeichnungen auf einen Monat verkürzen – Transkripte jahrelang aufbewahren und immer noch Speicherkosten sparen.

Sie können auch den Transkriptionsprozess mit AWS Step Functions und Lambda automatisieren, weitere Metadaten vor der Indizierung hinzufügen oder komplexere Visualisierungen generieren, um Ihrem Anwendungsfall gerecht zu werden.

Umbenennung von Amazon OpenSearch Service – Zusammenfassung der Änderungen

Am 8. September 2021 wurde unsere Such- und Analyse-Suite in Amazon OpenSearch Service umbenannt. OpenSearch Service unterstützt OpenSearch und auch Legacy-System-Elasticsearch-OSS. In den folgenden Abschnitten werden die verschiedenen Teile des Services beschrieben, die sich mit der Umbenennung geändert haben und welche Maßnahmen Sie ergreifen müssen, um sicherzustellen, dass Ihre Domänen weiterhin ordnungsgemäß funktionieren.

Einige dieser Änderungen gelten nur, wenn Sie Ihre Domänen von Elasticsearch auf OpenSearch aktualisieren. In anderen Fällen, z. B. in der Fakturierung- und Kostenmanagement-Konsole, ändert sich die Benutzererfahrung sofort.

Beachten Sie, dass diese Liste nicht vollumfänglich ist. Auch andere Teile des Produkts haben sich geändert, aber diese Updates sind am relevantesten.

Themen

Neue API-Version

Die neue Version der OpenSearch Service-Konfigurations-API (2021-01-01) funktioniert sowohl mit OpenSearch als auch mit Legacy-System-Elasticsearch OSS. 21 API-Operationen wurden durch

prägnantere und Engine-agnostische Namen ersetzt (z. B. `CreateElasticsearchDomain`geändert in `CreateDomain`), aber OpenSearch Service unterstützt weiterhin beide API-Versionen.

Wir empfehlen, dass Sie zukünftig die neuen API-Operationen verwenden, um Domänen zu erstellen und zu verwalten. Beachten Sie, dass Sie bei Verwendung der neuen API-Operationen zum Erstellen einer Domäne den `EngineVersion`-Parameter im Format `Elasticsearch_X.Y` oder `OpenSearch_X.Y` und nicht nur die Versionsnummer angeben müssen. Wenn Sie keine Version angeben, wird standardmäßig die neueste Version von OpenSearch verwendet.

Aktualisieren Sie AWS CLI auf Version 1.20.40 oder höher, um `aws opensearch ...` zum Erstellen und Verwalten Ihrer Domänen zu verwenden. Informationen zum neuen CLI-Format finden Sie in der OpenSearch CLI-Referenz.

Umbenannte Instance-Typen

Instance-Typen in Amazon OpenSearch Service haben jetzt das Format `<type>.<size>.search` – zum Beispiel `m6g.large.`*`search`* statt `m6g.large.`*`elasticsearch`*. Sie müssen selbst keine Aktion durchführen. Vorhandene Domänen werden automatisch auf die neuen Instance-Typen innerhalb der API und in der Fakturierungs- und Kostenmanagementkonsole verweisen.

Falls Sie über Reserved Instances (RIs) verfügen, wird Ihr Vertrag von der Änderung nicht beeinflusst. Die alte Konfigurations-API-Version ist weiterhin kompatibel mit dem alten Benennungsformat, aber wenn Sie die neue API-Version verwenden möchten, müssen Sie das neue Format verwenden.

Änderungen der Zugriffsrichtlinie

In den folgenden Abschnitten wird beschrieben, welche Aktionen Sie ergreifen müssen, um Ihre Zugriffsrichtlinien zu aktualisieren.

IAM-Richtlinien

Wir empfehlen, dass Sie Ihre IAM-Richtlinien, um die umbenannten API-Vorgänge zu verwenden. OpenSearch Service wird jedoch weiterhin bestehende Richtlinien respektieren, indem es intern die alten API-Berechtigungen repliziert. Wenn Sie beispielsweise derzeit über die Berechtigung zum Ausführen des `CreateElasticsearchDomain`-Vorgangs verfügen, können Sie jetzt sowohl `CreateElasticsearchDomain` (alte API-Operation) als auch `CreateDomain` (neue API-Operation) aufrufen. Dasselbe gilt für explizite Zugriffsverweigerungen. Eine Liste der aktualisierten API-Operationen finden Sie in der Richtlinienelementverweis.

SCP-Richtlinien

Service Control Policies (SCPs) führen im Vergleich zu Standard-IAM eine zusätzliche Komplexitätsebene ein. Um zu verhindern, dass Ihre SCP-Richtlinien verletzt werden, müssen Sie jeder Ihrer SCP-Richtlinien sowohl die alten als auch die neuen API-Operationen hinzufügen. Wenn ein Benutzer beispielsweise derzeit über Berechtigungen zum Zulassen von `CreateElasticsearchDomain` verfügt, müssen Sie ihm auch Berechtigungen zum Zulassen von `CreateDomain` erteilen, damit er weiterhin Domänen erstellen kann. Dasselbe gilt für explizite Zugriffsverweigerungen.

Zum Beispiel:

```
"Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "es:CreateElasticsearchDomain",
        "es:CreateDomain"
         ...
      ],
    },
      "Effect": "Deny",
      "Action:" [
        "es:DeleteElasticsearchDomain",
        "es:DeleteDomain"
         ...
```

Neue Ressourcentypen

OpenSearch Service führt die folgenden neuen Ressourcentypen ein:

Ressource	Beschreibung
`AWS::OpenSearchService::Domain`	Repräsentiert eine Amazon OpenSearch Service-Domäne. Diese Ressource existiert auf Service-Ebene und ist nicht spezifisch für die Software, die in der Domäne ausgeführt wird. Sie gilt für Dienste wie AWS CloudFormation- und AWS-Ressourcengruppen, in denen Sie

Ressource	Beschreibung
	Ressourcen für den Dienst als Ganzes erstellen und verwalten. Anweisungen zum Upgrade von Domänen, die in CloudFormation von Elasticsearch auf OpenSearch definiert sind, finden Sie unter Anmerkungen im CloudFormation-Benutzerhandbuch.
`AWS::OpenSearch::Domain`	Repräsentiert OpenSearch/ElasticSearch-Software, die auf einer Domäne ausgeführt wird. Diese Ressource gilt für Services wie AWS CloudTrail und AWS Config, die auf die Software verweisen, die auf der Domäne ausgeführt wird, und nicht auf OpenSearch Service als Ganzes. Diese Dienste enthalten jetzt separate Ressourcentypen für Domänen, auf denen Elasticsearch (`AWS::Elasticsearch::Domain`) ausgeführt wird, und Domänen, auf denen OpenSearch (`AWS::OpenSearch::Domain`) ausgeführt wird.

> **Note**
>
> In AWS Config sehen Sie Ihre Daten weiterhin unter der vorhandenen `AWS::Elasticsearch::Domain`-Ressourcentyp für mehrere Wochen, auch wenn Sie eine oder mehrere Domänen auf OpenSearch upgraden.

Kibana wurde in OpenSearch Dashboards umbenannt

OpenSearch Dashboards, die AWS-Alternative zu Kibana, ist ein Open-Source-Visualisierungs-Tool, das für OpenSearch entwickelt wurde. Nachdem Sie eine Domäne von Elasticsearch auf OpenSearch aktualisiert haben, ändert sich der `/_plugin/kibana`-Endpunkt in `/_dashboards`.

Der OpenSearch-Dienst leitet alle Anfragen an den neuen Endpunkt um. Wenn Sie jedoch den Kibana-Endpunkt in einer Ihrer IAM-Richtlinien verwenden, aktualisieren Sie diese Richtlinien, um auch den neuen `/_dashboards`-Endpunkt einzuschließen.

Wenn Sie the section called “SAML-Authentifizierung für Dashboards OpenSearch ” verwenden, müssen Sie vor dem Upgrade Ihrer Domäne auf OpenSearch alle in Ihrem Identitätsanbieter (IdP) konfigurierten Kibana-URLs von `/_plugin/kibana` auf `/_dashboards` ändern. Die häufigsten URLs sind Assertion Consumer Service (ACS)-URLs und Empfänger-URLs.

Die `kibana_read_only`-Standardrolle für OpenSearch Dashboards wurde umbenannt in `opensearch_dashboards_read_only`, und die `kibana_user`-Rolle wurde umbenannt in`opensearch_dashboards_user`. Die Änderung gilt für alle neu erstellten OpenSearch 1.x-Domänen mit Service-Software R20211203 oder höher. Wenn Sie eine bereits vorhandene Domäne auf die Service-Software R20211203 aktualisieren, bleiben die Rollennamen gleich.

Umbenannte CloudWatch-Metriken

Für Domänen, die OpenSearch ausführen, ändern sich mehrere CloudWatch-Metriken. Wenn Sie eine Domäne auf OpenSearch aktualisieren, ändern sich die Metriken automatisch und Ihre aktuellen CloudWatch-Alarme werden unterbrochen. Bevor Sie Ihren Cluster von einer Elasticsearch-Version auf eine OpenSearch-Version aktualisieren, müssen Sie Ihre CloudWatch-Alarme aktualisieren, um die neuen Metriken zu verwenden.

Die folgenden Metriken haben sich verändert:

Ursprünglicher Metrikname	Neuer Name
`KibanaHealthyNodes`	`OpenSearchDashboardsHealthyNodes`
`KibanaConcurrentConnections`	`OpenSearchDashboardsConcurrentConnections`
`KibanaHeapTotal`	`OpenSearchDashboardsHeapTotal`
`KibanaHeapUsed`	`OpenSearchDashboardsHeapUsed`
`KibanaHeapUtilization`	`OpenSearchDashboardsHeapUtilization`

Ursprünglicher Metrikname	Neuer Name
KibanaOS1MinuteLoad	OpenSearchDashboardsOS1MinuteLoad
KibanaRequestTotal	OpenSearchDashboardsRequestTotal
KibanaResponseTimesMaxInMillis	OpenSearchDashboardsResponseTimesMaxInMillis
ESReportingFailedRequestSysErrCount	KibanaReportingFailedRequestSysErrCount
ESReportingRequestCount	KibanaReportingRequestCount
ESReportingFailedRequestUserErrCount	KibanaReportingFailedRequestUserErrCount
ESReportingSuccessCount	KibanaReportingSuccessCount
ElasticsearchRequests	OpenSearchRequests

Eine vollständige Liste der Metriken, die OpenSearch Service an Amazon CloudWatch sendet, finden Sie unter the section called “Überwachen von Cluster-Metriken”.

Änderungen Fakturierung und Kostenmanagement

Historische Daten in der Rechnungsstellungs- und Kostenmanagement-Konsole und in den Kosten- und Nutzungsberichten werden weiterhin den alten Service-Namen verwenden. Daher benötigen Sie bei der Suche nach Daten Filter sowohl für Amazon OpenSearch Service als auch für den alten Elasticsearch-Namen. Wenn Sie über gespeicherte Berichte verfügen, aktualisieren Sie die Filter, um sicherzustellen, dass sie auch den OpenSearch Service enthalten. Möglicherweise erhalten Sie zunächst eine Warnung, wenn Ihre Nutzung für Elasticsearch abnimmt und für OpenSearch zunimmt, diese verschwindet jedoch innerhalb weniger Tage.

Zusätzlich zum Service-Namen ändern sich die folgenden Felder für alle Berichte, Rechnungen und Preislisten-API-Vorgänge:

Feld	Altes Format	Neues Format
Instance-Typ	`m5.large.elasticsearch`	`m5.large.search`
Produktfamilie	Elasticsearch-Instance Elasticsearch-Volume	Amazon-OpenSearch-Service-Instance Amazon-OpenSearch-Service-Volume
Preisbeschreibung	5,098$ pro c5.18xlarge.elasticsearch-Instance-Stunde (oder Teilstunde) - EU	5,098$ pro c5.18xlarge.search-Instance-Stunde (oder Teilstunde) - EU
Instance-Familie	`ultrawarm.elasticsearch`	`ultrawarm.search`

Neues Ereignisformat

Das Format der Ereignisse, die OpenSearch Service an Amazon EventBridge und Amazon CloudWatch sendet, hat sich geändert, insbesondere das Feld `detail-type`. Das Quellfeld (`aws.es`) bleibt gleich. Das vollständige Format für jeden Ereignistyp finden Sie unter the section called “Überwachung von Ereignissen”. Wenn Sie über vorhandene Ereignisregeln verfügen, die vom alten Format abhängen, stellen Sie sicher, dass sie dem neuen Format entsprechen.

Was bleibt gleich?

Die folgenden Funktionen und Funktionalitäten, unter anderem nicht aufgeführt, bleiben gleich:

- Dienstauftraggeber (`es.amazonaws.com`)
- Anbieter-Code
- Domänen-ARNs
- Domänen-Endpunkte

Erste Schritte: Aktualisieren Sie Ihre Domänen auf OpenSearch 1.x

OpenSearch 1.x unterstützt Upgrades von Elasticsearch Version 6.8 und 7.x aus. Anweisungen zum Upgrade Ihrer Domäne finden Sie unter the section called “Starten eines Upgrades (Konsole)”. Wenn Sie die AWS CLI oder Konfigurations-API zum Aktualisieren Ihrer Domäne verwenden, müssen Sie die `TargetVersion` als `OpenSearch_1.x` angeben.

OpenSearch 1.x führt eine zusätzliche Domäneneinstellung namens Kompatibilitätsmodus aktivieren ein. Da bestimmte Elasticsearch OSS-Clients und Plug-ins die Clusterversion vor der Verbindung überprüfen, setzt der Kompatibilitätsmodus OpenSearch so ein, dass er dessen Version als 7.10 meldet, damit diese Clients weiterhin funktionieren.

Sie können den Kompatibilitätsmodus aktivieren, wenn Sie OpenSearch-Domänen zum ersten Mal erstellen oder wenn Sie von einer Elasticsearch-Version auf OpenSearch aktualisieren. Wenn er nicht gesetzt ist, wird der Parameter standardmäßig auf `false` gesetzt, wenn Sie eine Domäne erstellen, und auf `true` wenn Sie eine Domäne aktualisieren.

Um den Kompatibilitätsmodus mit der Konfigurations-API zu aktivieren, setzen Sie `override_main_response_version` auf `true`:

```
POST https://es.us-east-1.amazonaws.com/2021-01-01/opensearch/upgradeDomain
{
  "DomainName": "domain-name",
  "TargetVersion": "OpenSearch_1.0",
  "AdvancedOptions": {
    "override_main_response_version": "true"
   }
}
```

Um den Kompatibilitätsmodus für vorhandene OpenSearch-Domänen zu aktivieren oder zu deaktivieren, müssen Sie die OpenSearch API-Operation _cluster/settings verwenden:

```
PUT /_cluster/settings
{
  "persistent" : {
    "compatibility.override_main_response_version" : true
  }
}
```

Problembehebung bei Amazon OpenSearch Service

In diesem Thema wird beschrieben, wie Sie häufig auftretende Probleme mit Amazon OpenSearch Service identifizieren und lösen können. Lesen Sie die Informationen in diesem Abschnitt, bevor Sie sich an den AWS -Support wenden.

Ich kann nicht auf OpenSearch Dashboards zugreifen

Der OpenSearch Dashboards-Endpunkt unterstützt keine signierten Anfragen. Wenn durch die Zugriffskontrollrichtlinie Ihrer Domain nur Zugriff auf bestimmte IAM-Rollen gewährt wird und Sie Amazon-Cognito-Authentifizierung nicht konfiguriert haben, erhalten Sie möglicherweise folgende Fehlermeldung, wenn Sie versuchen, auf Dashboards zuzugreifen:

```
"User: anonymous is not authorized to perform: es:ESHttpGet"
```

Wenn Ihre OpenSearch Service-Domain VPC-Zugriff verwendet, erhalten Sie diesen Fehler möglicherweise nicht, aber es kann zu einem Timeout bei der Anfrage kommen. Informationen zur Behebung dieses Problems und zu den verschiedenen verfügbaren Konfigurationsoptionen finden Sie unter the section called “Steuern des Zugriffs auf Dashboards OpenSearch ” the section called “Zugriffsrichtlinien für VPC-Domänen” und the section called “Identitäts- und Zugriffsverwaltung”.

Zugriff auf VPC-Domain nicht möglich

Siehe the section called “Zugriffsrichtlinien für VPC-Domänen” und the section called “Testen von VPC-Domänen”.

Cluster im schreibgeschützten Zustand

Im Vergleich zu früheren Elasticsearch-Versionen OpenSearch und Elasticsearch 7. x verwendet ein anderes System für die Cluster-Koordination. Wenn der Cluster in diesem neuen System das Quorum verliert, ist der Cluster erst verfügbar, wenn Sie Maßnahmen ergreifen. Der Verlust des Quorums kann zwei Formen annehmen:

- Wenn Ihr Cluster dedizierte Hauptknoten verwendet, tritt ein Quorum-Verlust auf, wenn die Hälfte oder mehr nicht verfügbar sind.

- Wenn Ihr Cluster keine dedizierten Hauptknoten verwendet, tritt ein Quorum-Verlust auf, wenn die Hälfte oder mehr Ihrer Datenknoten nicht verfügbar sind.

Wenn ein Quorumverlust auftritt und Ihr Cluster mehr als einen Knoten hat, stellt der OpenSearch Dienst das Quorum wieder her und versetzt den Cluster in einen schreibgeschützten Zustand. Sie haben hierfür zwei Möglichkeiten:

- Entfernen Sie den schreibgeschützten Status und verwenden Sie den Cluster wie er ist.
- Stellen Sie den Cluster oder einzelne Indizes aus einem Snapshot wieder her.

Wenn Sie den Cluster vorziehen, wie er ist, überprüfen Sie mit der folgenden Anforderung, ob der Cluster-Zustand grün ist:

```
GET _cat/health?v
```

Wenn der Cluster-Zustand rot ist, empfehlen wir, den Cluster aus einem Snapshot wiederherzustellen. Informationen zur Fehlerbehebung finden Sie auch unter the section called “Roter Cluster-Status”. Wenn der Cluster-Zustand grün ist, überprüfen Sie mit der folgenden Anforderung, ob alle erwarteten Indizes vorhanden sind:

```
GET _cat/indices?v
```

Führen Sie dann einige Suchanfragen aus, um zu überprüfen, ob die erwarteten Daten vorhanden sind. Wenn dies der Fall ist, können Sie den schreibgeschützten Status mithilfe der folgenden Anforderung entfernen:

```
PUT _cluster/settings
{
  "persistent": {
    "cluster.blocks.read_only": false
  }
}
```

Wenn ein Quorumverlust auftritt und Ihr Cluster nur aus einem Knoten besteht, ersetzt OpenSearch Service den Knoten und versetzt den Cluster nicht in einen schreibgeschützten Zustand. Andernfalls sind Ihre Optionen gleich: Verwenden Sie den Cluster unverändert oder stellen Sie ihn aus einem Snapshot wieder her.

In beiden Situationen sendet OpenSearch Service zwei Ereignisse an Ihren. AWS Health Dashboard Das erste informiert Sie über den Verlust des Quorums. Das zweite Ereignis tritt ein, nachdem OpenSearch Service das Quorum erfolgreich wiederhergestellt hat. Weitere Informationen zur Verwendung von finden Sie im AWS Health Benutzerhandbuch. AWS Health Dashboard

Roter Cluster-Status

Ein roter Clusterstatus bedeutet, dass mindestens ein primärer Shard und seine Replikate keinem Knoten zugewiesen sind. OpenSearch Der Dienst versucht weiterhin, automatische Snapshots aller Indizes unabhängig von ihrem Status zu erstellen, aber die Snapshots schlagen fehl, solange der rote Clusterstatus bestehen bleibt.

Die häufigsten Ursachen für einen roten Clusterstatus sind ausgefallene Clusterknoten und OpenSearch Prozessabstürze aufgrund einer kontinuierlich hohen Verarbeitungslast.

> **Note**
>
> OpenSearch Der Service speichert automatische Snapshots unabhängig vom Clusterstatus 14 Tage lang. Wenn der rote Cluster-Status länger als zwei Wochen anhält, wird daher der letzte fehlerfreie automatisierte Snapshot gelöscht und Sie könnten die Daten Ihres Clusters dauerhaft verlieren. Wenn Ihre OpenSearch Service-Domain den Cluster-Status Rot annimmt, kontaktieren Sie AWS Support möglicherweise, um zu fragen, ob Sie das Problem selbst lösen möchten oder ob Sie möchten, dass Ihnen das Support-Team weiterhilft. Sie können einen CloudWatch Alarm einrichten, der Sie benachrichtigt, wenn ein roter Clusterstatus eintritt.

Letztlich führen rote Shards zu roten Clustern; und rote Indizes verursachen rote Shards. Um die Indizes zu identifizieren, die den roten Clusterstatus verursachen, OpenSearch gibt es einige hilfreiche APIs.

- `GET /_cluster/allocation/explain` wählt den ersten nicht zugewiesenen Shard aus und erklärt, warum er keinem Knoten zugeordnet werden kann:

```
{
    "index": "test4",
    "shard": 0,
    "primary": true,
```

```
    "current_state": "unassigned",
    "can_allocate": "no",
    "allocate_explanation": "cannot allocate because allocation is not permitted to
 any of the nodes"
}
```

- `GET /_cat/indices?v` zeigt den Zustand, die Anzahl der Dokumente und die Festplattennutzung für jeden Index an:

```
health status index            uuid                   pri rep docs.count docs.deleted
 store.size pri.store.size
green  open   test1            30h1EiMvS5uAFr2t5CEVoQ   5   0        820            0
       14mb           14mb
green  open   test2            sdIxs_WDT56afFGu5KPbFQ   1   0          0            0
       233b           233b
green  open   test3            GGRZp_TBRZuSaZpAGk2pmw   1   1          2            0
     14.7kb          7.3kb
red    open   test4            BJxfAErbTtu5HBjIXJV_7A   1   0
green  open   test5            _8C6MIXOSxCqVYicH3jsEA   1   0          7            0
     24.3kb         24.3kb
```

Das Löschen von roten Indizes ist die schnellste Möglichkeit, einen roten Cluster-Status zu beheben. Abhängig vom Grund für den roten Cluster-Status können Sie dann Ihre OpenSearch Service-Domain skalieren, um größere Instance-Typen, mehr Instances oder mehr EBS-basierten Speicher zu verwenden, und versuchen, die problematischen Indizes neu zu erstellen.

Sollte ein fehlerhafter Index nicht löschbar sein, können Sie einen Snapshot wiederherstellen, Dokumente aus dem Index löschen, die Indexeinstellungen ändern, die Anzahl der Replikate verringern oder andere Indizes löschen, um Speicherplatz freizusetzen. Der wichtige Schritt besteht darin, den roten Clusterstatus zu beheben, bevor Sie Ihre Service-Domain neu konfigurieren. OpenSearch Falls eine Domain mit rotem Cluster-Status neu konfiguriert wird, kann sich das Problem verschlimmern und dazu führen, dass die Domain im Konfigurationsstatus Processing (Verarbeitung) verharrt, bis der rote Status behoben ist.

Automatische Behebung von roten Clustern

Wenn der Status Ihres Clusters länger als eine Stunde ununterbrochen rot ist, versucht OpenSearch Service, das Problem automatisch zu beheben, indem nicht zugewiesene Shards umgeleitet oder Daten aus früheren Snapshots wiederhergestellt werden.

Wenn ein oder mehrere rote Indizes nicht repariert werden können und der Clusterstatus insgesamt 14 Tage lang rot bleibt, ergreift OpenSearch Service nur dann weitere Maßnahmen, wenn der Cluster mindestens eines der folgenden Kriterien erfüllt:

- Hat nur eine Availability Zone
- Hat keine dedizierten Hauptknoten
- Enthält Burstable-Instance-Typen (T2 oder T3)

Wenn Ihr Cluster eines dieser Kriterien erfüllt, sendet Ihnen OpenSearch Service in den nächsten 7 Tagen täglich Benachrichtigungen, in denen erklärt wird, dass alle nicht zugewiesenen Shards gelöscht werden, wenn Sie diese Indizes nicht korrigieren. Wenn Ihr Clusterstatus nach 21 Tagen immer noch rot ist, löscht OpenSearch Service die nicht zugewiesenen Shards (Speicher und Rechenleistung) in allen roten Indizes. Für jedes dieser Ereignisse erhalten Sie im Benachrichtigungsbereich der OpenSearch Servicekonsole Benachrichtigungen. Weitere Informationen finden Sie unter the section called “Ereignisse zum Cluster-Zustand”.

Wiederherstellung nach einem kontinuierlich starken Workload

Um zu ermitteln, ob ein roter Cluster-Status durch einen kontinuierlich starken Workload auf einem Datenknoten verursacht wird, überwachen Sie die folgenden Cluster-Metriken.

Relevante Metrik	Beschreibung	Wiederherstellung
JVM MemoryPressure	Gibt den Prozentsatz des Java-Heap an, der für alle Datenknoten in einem Cluster verwendet wird. Zeigen Sie die Statistik Maximum für diese Metrik an und achten Sie auf eine immer kleiner werdende Verringerung der Speicherbelastung, während der Java Garbage Collector keine ausreichende Arbeitsspeichermenge mehr zurückgewinnt. Dieses Muster wird wahrscheinlich durch komplexe Abfragen oder große Datenfelder verursacht.	Legen Sie Arbeitsspeicher-Leistungsschutzschalter für die JVM fest. Weitere Informationen finden Sie unter the section called “JVM OutOfMemoryError”. Wenn das Problem weiterhin besteht, löschen Sie unnötige Indizes, reduzieren Sie die Anzahl oder Komplexität der Anforderungen an die Domain, fügen Sie Instances hinzu oder

Relevante Metrik	Beschreibung	Wiederherstellung
	x86-Instance-Typen verwenden den Garbage Collector „Concurrent Mark Sweep (CMS)“, der zusammen mit Anwendungs-Threads ausgeführt wird, um Pausen kurz zu halten. Wenn CMS während seiner normalen Sammelvorgänge nicht ausreichend Arbeitsspeicher zurückgewinnen kann, löst es eine vollständige Garbage Collection aus, was zu langen Anwendungspausen und Auswirkungen auf die Clusterstabilität führen kann. ARM-basierte Graviton-Instance-Typen verwenden den Garbage-First (G1) Garbage Collector, der CMS ähnlich ist, jedoch zusätzliche kurze Pausen und Heap-Defragmentierung verwendet, um die Notwendigkeit vollständiger Garbage Collections weiter zu reduzieren. In beiden Fällen OpenSearch stürzt der Speicherverbrauch mit einem Speichermangel ab, wenn der Speicherverbrauch über das hinausgeht, was der Garbage-Collector bei vollständigen Garbage-Collections zurückgewinnen kann. Bei allen Instance-Typen gilt als Faustregel, die Nutzung unter 80 % zu halten. Die `_nodes/stats/jvm` -API bietet eine hilfreiche Übersicht über	verwenden Sie größere Instance-Typen.

Relevante Metrik	Beschreibung	Wiederherstellung
	die JVM-Statistiken, Speicherpoolnutzung und Garbage Collection-Informationen: `GET domain-endpoint /_nodes/stats/jvm?pretty`	
CPUUtilization	Gibt den Prozentsatz der CPU-Ressourcen an, die für Datenknoten in einem Cluster verwendet werden. Sehen Sie sich die Statistik Maximum für diese Metrik an und suchen Sie nach einem kontinuierlichen Muster für starke Nutzung.	Fügen Sie Datenknoten hinzu oder erhöhen Sie die Größe der Instance-Typen vorhandener Datenknoten.
Knoten	Gibt die Anzahl der Knoten in einem Cluster an. Sehen Sie sich die Statistik Maximum für diese Metrik an. Dieser Wert schwankt, wenn der Service eine neue Flotte an Instances für einen Cluster bereitstellt.	Fügen Sie Datenknoten hinzu.

Gelber Cluster-Status

Ein gelber Cluster-Status bedeutet, dass die primären Shards für alle Indizes zu Knoten in einem Cluster zugewiesen sind, die Replikat-Shards für mindestens einen Index jedoch nicht. Cluster mit einem Knoten werden immer mit einem gelben Clusterstatus initialisiert, da es keinen anderen Knoten gibt, dem der OpenSearch Dienst ein Replikat zuweisen kann. Erhöhen Sie die Knotenanzahl, um einen grünen Cluster-Status zu erreichen. Weitere Informationen finden Sie unter the section called “Größenanpassung von Domains”.

Cluster mit mehreren Knoten können nach dem Erstellen eines neuen Index oder nach einem Knotenausfall kurzzeitig einen gelben Clusterstatus aufweisen. Dieser Status löst sich von selbst auf, wenn Daten im gesamten Cluster OpenSearch repliziert werden. Ein Mangel an Festplattenspeicher

kann auch zu einem gelben Cluster-Status führen; Der Cluster kann Replikat-Shards nur verteilen, wenn die Knoten über ausreichend Speicherplatz verfügen, um sie aufzunehmen.

ClusterBlockException

Unter Umständen erhalten Sie aus folgenden Gründen den Fehler `ClusterBlockException`.

Zu wenig verfügbarer Speicherplatz

Wenn ein oder mehrere Knoten in Ihrem Cluster über Speicherplatz verfügen, der unter dem Mindestwert von 1) 20% des verfügbaren Speicherplatzes oder 2) 20 GiB Speicherplatz liegt, können grundlegende Schreibvorgänge wie das Hinzufügen von Dokumenten und das Erstellen von Indizes fehlschlagen. the section called “Berechnung der Speicheranforderungen”bietet eine Zusammenfassung darüber, wie OpenSearch Service Festplattenspeicher verwendet.

Um Probleme zu vermeiden, sollten Sie die `FreeStorageSpace` Metrik in der OpenSearch Servicekonsole überwachen und CloudWatch Alarme einrichten, die ausgelöst werden, wenn `FreeStorageSpace` ein bestimmter Schwellenwert unterschritten wird. `GET /_cat/allocation?v`bietet außerdem eine nützliche Zusammenfassung der Shard-Zuweisung und der Festplattennutzung. Um Probleme im Zusammenhang mit fehlendem Speicherplatz zu beheben, skalieren Sie Ihre OpenSearch Service-Domain so, dass sie größere Instance-Typen, mehr Instanzen oder mehr EBS-basierten Speicher verwendet.

Hoher JVM-Speicherdruck

Wenn die MemoryPressureJVM-Metrik 30 Minuten lang 92% überschreitet, löst der OpenSearch Service einen Schutzmechanismus aus und blockiert alle Schreibvorgänge, um zu verhindern, dass der Cluster den roten Status erreicht. Wenn der Schutz aktiviert ist, schlagen Schreibvorgänge mit einem `ClusterBlockException`-Fehler fehl, es können keine neuen Indizes erstellt werden und der Fehler `IndexCreateBlockException` wird ausgegeben.

Wenn die MemoryPressureJVM-Metrik fünf Minuten lang auf 88% oder weniger zurückgeht, ist der Schutz deaktiviert und Schreibvorgänge in den Cluster werden entsperrt.

Ein hoher JVM-Speicherdruck kann durch Spitzen in der Anzahl der Anfragen an den Cluster, unausgewogene Shard-Zuweisungen über Knoten hinweg, zu viele Shards in einem Cluster, Felddaten- oder Indexzuordnungsexplosionen oder Instance-Typen, die eingehende Lasten nicht bewältigen können, verursacht werden. Er kann außerdem auch durch die Verwendung von Aggregationen, Platzhaltern oder großen Zeitbereichen in Abfragen verursacht werden.

Um den Datenverkehr zum Cluster zu reduzieren und Probleme mit hohem JVM-Speicherdruck zu beheben, versuchen Sie eine oder mehrere der folgenden Möglichkeiten:

- Skalieren Sie die Domain so, dass die maximale Heap-Größe pro Knoten 32 GB beträgt.
- Reduzieren Sie die Anzahl der Shards, indem Sie alte oder nicht verwendete Indizes löschen.
- Leeren Sie den Datencache mit dem API-Vorgang `POST index-name/_cache/clear?fielddata=true`. Beachten Sie, dass das Löschen des Caches laufende Abfragen beeinträchtigen kann.

Um künftig einen hohen JVM-Speicherbedarf zu vermeiden, sollten Sie sich allgemein an die folgenden bewährten Methoden halten:

- Vermeiden Sie das Aggregieren in Textfeldern oder ändern Sie den Zuordnungstyp für Ihre Indizes in `keyword`.
- Optimieren Sie Such- und Indizierungsanforderungen durch die Auswahl der richtigen Anzahl von Shards.
- Richten Sie Index State Management (ISM)-Richtlinien ein, um nicht verwendete Indizes regelmäßig zu entfernen.

Fehler bei der Migration zu Multi-AZ mit Standby

Die folgenden Probleme können auftreten, wenn Sie eine bestehende Domain zu Multi-AZ mit Standby migrieren.

Erstellen eines Indexes, einer Indexvorlage oder einer ISM-Richtlinie während der Migration von Domänen ohne Standby zu Domänen mit Standby

Wenn Sie bei der Migration einer Domain von Multi-AZ ohne Standby zu mit Standby einen Index erstellen und die Indexvorlage oder ISM-Richtlinie nicht den empfohlenen Richtlinien für das Kopieren von Daten entspricht, kann dies zu Dateninkonsistenzen führen und die Migration kann fehlschlagen. Um diese Situation zu vermeiden, erstellen Sie den neuen Index mit einer Anzahl von Datenkopien (einschließlich primärer Knoten und Replikate), die ein Vielfaches von drei ist. Sie können den Migrationsfortschritt mithilfe der API überprüfen. `DescribeDomainChangeProgress` Wenn Sie auf einen Fehler bei der Anzahl der Replikate stoßen, beheben Sie den Fehler und wenden Sie sich dann an den AWS Support, um die Migration erneut zu versuchen.

Falsche Anzahl von Datenkopien

Wenn Sie nicht über die richtige Anzahl von Datenkopien in Ihrer Domain verfügen, schlägt die Migration zu Multi-AZ mit Standby fehl.

JVM OutOfMemoryError

Ein JVM-`OutOfMemoryError` bedeutet in der Regel, dass einer der folgenden JVM-Leistungsschutzschalter erreicht wurde.

Leistungsschutzschalter	Beschreibung	Eigenschaft der Cluster-Einstellung
Übergeordneter Schalter	Gesamter JVM-Heap-Arbeitsspeicher in Prozent, der für alle Leitungss chutzschalter zulässig ist. Der Standardwert ist 95 %.	`indices.breaker.total.limit`
Felddaten-Schutzschalter	Prozentsatz des JVM-Heap-Arbeitsspeichers, der für das Laden eines einzelnen Datenfelds in den Arbeitsspeicher zulässig ist. Der Standardwert lautet 40%. Wenn Sie Daten mit großen Feldern hochladen, müssen Sie dieses Limit möglicher weise erhöhen.	`indices.breaker.fielddata.limit`
Anforderungs-Schutzschalter	Prozentsatz des JVM-Heap-Arbeitsspeichers, der zulässig ist für Datenstrukturen, die zur Antwort auf eine Serviceanforderung verwendet werden. Der	`indices.breaker.request.limit`

Leistungsschutzschalter	Beschreibung	Eigenschaft der Cluster-Einstellung
	Standardwert lautet 60%. Wenn Ihre Servicean fragen die Berechnung von Aggregationen beinhalten, müssen Sie dieses Limit möglicherweise erhöhen.	

Fehlgeschlagene Cluster-Knoten

Bei Amazon-EC2-Instances kann es zu unerwarteten Beendigungen und Neustarts kommen. In der Regel startet OpenSearch Service die Knoten für Sie neu. Es ist jedoch möglich, dass ein oder mehrere Knoten in einem OpenSearch Cluster weiterhin ausgefallen sind.

Um nach diesem Zustand zu suchen, öffnen Sie Ihr Domain-Dashboard in der OpenSearch Servicekonsole. Wählen Sie die Registerkarte Clusterzustand und anschließend die Gesamte Knoten-Metrik aus. Überprüfen Sie, ob die gemeldete Anzahl an Knoten geringer ist als die Anzahl, die Sie für Ihren Cluster konfiguriert haben. Wenn die Metrik zeigt, dass ein oder mehrere Knoten länger als einen Tag ausgefallen sind, wenden Sie sich bitte an den AWS -Support.

Sie können auch einen CloudWatch Alarm einrichten, der Sie benachrichtigt, wenn dieses Problem auftritt.

> **Note**
>
> Die Knoten-Metrik ist während Änderungen an Ihrer Cluster-Konfiguration und routinemäßigen Wartungen des Services nicht genau. Dieses Verhalten wird erwartet. Die Metrik wird die richtige Anzahl an Cluster-Knoten in Kürze angeben. Weitere Informationen hierzu finden Sie unter the section called “Konfigurationsänderungen”.

Um Ihre Cluster vor unerwarteten Knotenabbrüchen und Neustarts zu schützen, erstellen Sie mindestens ein Replikat für jeden Index in Ihrer OpenSearch Service-Domain.

Maximales Shard-Limit überschritten

OpenSearch sowie 7. x-Versionen von Elasticsearch haben eine Standardeinstellung von nicht mehr als 1.000 Shards pro Knoten. OpenSearch/Elasticsearch gibt einen Fehler aus, wenn eine Anfrage, z. B. die Erstellung eines neuen Indexes, dazu führen würde, dass Sie dieses Limit überschreiten. Wenn dieser Fehler auftritt, haben Sie mehrere Möglichkeiten:

- Fügen Sie dem Cluster weitere Datenknoten hinzu.
- Erhöhen Sie die `_cluster/settings/cluster.max_shards_per_node`-Einstellung.
- Verwenden Sie die _shrink-API, um die Anzahl der Shards auf dem Knoten zu reduzieren.

Domain bleibt im Bearbeitungsstatus hängen

Ihre OpenSearch Service-Domain wechselt in den Status „In Bearbeitung“, wenn sie sich mitten in einer Konfigurationsänderung befindet. Wenn Sie eine Konfigurationsänderung einleiten, ändert sich der Domänenstatus in „In Bearbeitung“, während OpenSearch Service eine neue Umgebung erstellt. In der neuen Umgebung startet der OpenSearch Service einen neuen Satz geeigneter Knoten (z. B. Data, Master oder UltraWarm). Nachdem die Migration abgeschlossen ist, werden die älteren Knoten beendet.

Der Cluster kann im Status „Verarbeitung“ hängen bleiben, wenn eine der folgenden Situationen eintritt:

- Ein neuer Satz von Datenknoten kann nicht gestartet werden.

- Die Shard-Migration auf den neuen Satz von Datenknoten ist nicht erfolgreich.
- Die Validierungsprüfung ist mit Fehlern fehlgeschlagen.

Detaillierte Lösungsschritte für jede dieser Situationen finden Sie unter Warum befindet sich meine Amazon OpenSearch Service-Domain im Status „In Bearbeitung“? .

Niedrige EBS-Burst-Balance

OpenSearch Der Service sendet Ihnen eine Konsolenbenachrichtigung, wenn der EBS-Burst-Saldo auf einem Ihrer General Purpose (SSD) -Volumes unter 70% liegt, und eine Folgebenachrichtigung, wenn der Saldo unter 20% fällt. Um dieses Problem zu beheben, können Sie entweder Ihren

Cluster hochskalieren oder die Lese- und Schreib-IOPS reduzieren, sodass die Burst-Balance gutgeschrieben werden kann. Das Burst-Balance bleibt für Domains mit GP3-Volume-Typen und Domains mit GP2-Volumes mit einer Volume-Größe von über 1.000 GiB bei 0. Weitere Informationen finden Sie unter universelle SSD-Volumes (gp2). Sie können den EBS-Burst-Saldo anhand der `BurstBalance` CloudWatch Metrik überwachen.

Prüfungsprotokolle können nicht aktiviert werden

Wenn Sie versuchen, die Veröffentlichung von Audit-Protokollen über die OpenSearch Service-Konsole zu aktivieren, tritt möglicherweise der folgende Fehler auf:

Die für die Protokollgruppe CloudWatch Logs angegebene Ressourcenzugriffsrichtlinie gewährt Amazon OpenSearch Service nicht genügend Berechtigungen, um einen Protokollstream zu erstellen. Überprüfen Sie die Ressourcenzugriffsrichtlinie.

Wenn dieser Fehler auftritt, überprüfen Sie, ob das `resource`-Element Ihrer Richtlinie den richtigen Protokollgruppen-ARN enthält. Führen Sie in diesem Fall die folgenden Schritte aus:

1. Warten Sie einige Minuten.
2. Aktualisieren Sie die Seite in Ihrem Webbrowser.
3. Wählen Sie Vorhandene Gruppe auswählen.
4. Wählen Sie für Vorhandene Protokollgruppe die Protokollgruppe aus, die Sie erstellt haben, bevor Sie die Fehlermeldung erhalten.
5. Wählen Sie im Abschnitt Zugriffsrichtlinie die Option Vorhandene Richtlinie auswählen aus.
6. Wählen Sie für Vorhandene Richtlinie die Richtlinie aus, die Sie erstellt haben, bevor Sie die Fehlermeldung erhalten.
7. Wählen Sie Enable (Aktivieren) aus.

Wenn der Fehler nach mehrmaligem Wiederholen des Vorgangs weiterhin besteht, wenden Sie sich an den AWS -Support.

Schließen des Indexes nicht möglich

OpenSearch Der Service unterstützt die `_close`API nur für OpenSearch Elasticsearch-Versionen 7.4 und höher. Wenn Sie eine ältere Version verwenden und einen Index aus einem Snapshot

wiederherstellen, können Sie den vorhandenen Index löschen (vor oder nach der erneuten Indizierung).

Prüfungen für Client-Lizenz

Die Standarddistributionen von Logstash und Beats beinhalten eine Prüfung der eigenen Lizenz und können keine Verbindung zur Open-Source-Version von herstellen. OpenSearch Stellen Sie sicher, dass Sie die Apache 2.0 (OSS) -Distributionen dieser Clients mit Service verwenden. OpenSearch

Drosselung anfordern

Wenn Sie dauerhafte `403 Request throttled due to too many requests`- oder `429 Too Many Requests`-Fehler erhalten, sollten Sie eine vertikale Skalierung in Betracht ziehen. Amazon OpenSearch Service drosselt Anfragen, wenn die Nutzlast dazu führen würde, dass die Speichernutzung die maximale Größe des Java-Heaps überschreitet.

SSH im Knoten nicht möglich

Sie können SSH nicht verwenden, um auf einen der Knoten in Ihrem OpenSearch Cluster zuzugreifen, und Sie können Änderungen nicht direkt vornehmen. `opensearch.yml` Verwenden Sie stattdessen die Konsole oder die SDKs AWS CLI, um Ihre Domain zu konfigurieren. Mithilfe der OpenSearch REST-APIs können Sie auch einige Einstellungen auf Clusterebene angeben. Weitere Informationen finden Sie in der Amazon OpenSearch Service API-Referenz undthe section called “Unterstützte Vorgänge”.

Wenn Sie mehr Einblick in die Leistung des Clusters benötigen, können Sie Fehlerprotokolle und langsame Protokolle unter veröffentlichen CloudWatch.

Snapshot-Fehler „Nicht gültig für die Speicherklasse des Objekts“

OpenSearch Service-Snapshots unterstützen die Speicherklasse S3 Glacier nicht. Dieser Fehler kann auftreten, wenn Sie versuchen, Snapshots aufzulisten, wenn Ihr S3-Bucket eine Lebenszyklusregel enthält, die einen Übergang der Objekte in die Speicherklasse S3 Glacier bewirkt.

Wenn Sie einen Snapshot aus einem Bucket wiederherstellen müssen, stellen Sie die Objekte aus S3 Glacier wieder her, kopieren Sie die Objekte in einen neuen Bucket und registrieren Sie den neuen Bucket als Snapshot-Repository.

Ungültiger Host-Header

OpenSearch Der Service erfordert, dass die Clients dies `Host` in den Anforderungsheadern angeben. Ein gültiger `Host`-Wert ist der Domain-Endpunkt ohne `https://`, z. B.:

```
Host: search-my-sample-domain-ih2lhn2ew2scurji.us-west-2.es.amazonaws.com
```

Wenn Sie bei einer Anfrage eine `Invalid Host Header` Fehlermeldung erhalten, überprüfen Sie, ob Ihr Client oder Proxy den OpenSearch Service-Domänenendpunkt (und nicht beispielsweise seine IP-Adresse) im `Host` Header enthält.

Ungültiger M3-Instance-Typ

OpenSearch Der Service unterstützt das Hinzufügen oder Ändern von M3-Instances zu bestehenden Domains, auf denen die Elasticsearch-Versionen 6.7 und höher ausgeführt OpenSearch werden, nicht. Sie können weiterhin M3-Instances mit Elasticsearch 6.5 und früher verwenden.

Es wird empfohlen, einen neueren Instance-Typ auszuwählen. Für Domains, die auf Elasticsearch 6.7 oder höher laufen OpenSearch , gelten die folgenden Einschränkungen:

- Wenn Ihre vorhandene Domain keine M3-Instances verwendet, können Sie nicht mehr zu diesen wechseln.
- Wenn Sie eine vorhandene Domain von einem M3-Instance-Typ in einen anderen Instance-Typ ändern, können Sie nicht zurückwechseln.

Hot Queries funktionieren nach der Aktivierung nicht mehr UltraWarm

Wenn Sie die Option für eine Domäne aktivieren und die `search.max_buckets` Einstellung nicht bereits außer Kraft gesetzt wurde, legt OpenSearch Service den Wert automatisch UltraWarm auf fest, um `10000` zu verhindern, dass speicherintensive Abfragen warme Knoten überlasten. Wenn Ihre Hot-Abfragen mehr als 10.000 Buckets verwenden, funktionieren sie möglicherweise nicht mehr, wenn Sie sie aktivieren. UltraWarm

Da Sie diese Einstellung aufgrund des verwalteten Charakters von Amazon OpenSearch Service nicht ändern können, müssen Sie einen Support-Fall eröffnen, um das Limit zu erhöhen. Limiterhöhungen erfordern kein Premium-Support-Abonnement.

Nach einem Upgrade ist kein Downgrade möglich

Direkte Upgrades können nicht mehr rückgängig gemacht werden. Wenn Sie sich jedoch an den AWS Support wenden, können die Mitarbeiter Ihnen helfen, den automatischen Pre-Upgrade-Snapshot auf einer neuen Domain wiederherzustellen. Wenn Sie beispielsweise eine Domain von Elasticsearch 5.6 auf 6.4 aktualisieren, kann der AWS Support Ihnen helfen, den Snapshot vor dem Upgrade auf einer neuen Elasticsearch 5.6-Domain wiederherzustellen. Wenn Sie einen manuellen Snapshot der ursprünglichen Domain erstellen würden, könnten Sie diesen Schritt selbst ausführen.

Erforderliche Zusammenfassung der Domains für alle AWS-Regionen

Das folgende Skript verwendet den Amazon EC2 AWS CLI EC2-Befehl describe-regions, um eine Liste aller Regionen zu erstellen, in denen der OpenSearch Service verfügbar sein könnte. Dann ruft es list-domain-namesfür jede Region auf:

```
for region in `aws ec2 describe-regions --output text | cut -f4`
do
    echo "\nListing domains in region '$region':"
    aws opensearch list-domain-names --region $region --query 'DomainNames'
done
```

Sie erhalten die folgende Ausgabe für jede Region:

```
Listing domains in region:'us-west-2'...
[
  {
    "DomainName": "sample-domain"
  }
]
```

Regionen, in denen der OpenSearch Dienst nicht verfügbar ist, geben „Es konnte keine Verbindung zur Endpunkt-URL hergestellt werden“ zurück.

Browserfehler bei der Verwendung von OpenSearch Dashboards

Ihr Browser verpackt Dienstfehlermeldungen in HTTP-Antwortobjekten, wenn Sie Dashboards verwenden, um Daten in Ihrer OpenSearch Service-Domain anzuzeigen. Sie können die gängigen

Entwickler-Tools in Web-Browsern, wie den Entwicklermodus in Chrome, verwenden, um die zugrundeliegenden Servicefehler anzuzeigen und Ihre Debugging-Bemühungen zu unterstützen.

So zeigen Sie Servicefehler in Chrome an

1. Wählen Sie im Menü Anzeigen, Entwickler, Entwickler-Tools aus.
2. Wählen Sie die Registerkarte Network (Netzwerk) aus.
3. Wählen Sie in der Spalte Status eine beliebige HTTP-Sitzung mit dem Status 500 aus.

So zeigen Sie Servicefehler in Firefox an

1. Wählen Sie im Menü Tools, Web Developer (Web-Entwickler), Network (Netzwerk) aus.
2. Wählen Sie eine HTTP-Sitzung mit dem Status 500.
3. Wählen Sie die Registerkarte Response (Antwort) aus, um die Serviceantwort anzuzeigen.

Knoten-Shard und Speicherversatz

Knoten-Shard-Versatz liegt vor, wenn ein oder mehrere Knoten innerhalb eines Clusters deutlich mehr Shards als die anderen Knoten haben. Knoten-Speicherversatz liegt vor, wenn ein oder mehrere Knoten innerhalb eines Clusters deutlich mehr Speicher (`disk.indices`) haben als die anderen Knoten. Während diese beiden Bedingungen vorübergehend auftreten können, z. B. wenn eine Domain einen Knoten ersetzt hat und ihm immer noch Shards zuweist, sollten Sie sie beheben, wenn sie bestehen bleiben.

Um beide Arten von Versatz zu erkennen, führen Sie den API-Vorgang _cat/allocation aus und vergleichen Sie die Einträge `shards` und `disk.indices` in der Antwort:

```
shards    | disk.indices  | disk.used  | disk.avail   | disk.total   | disk.percent |
host     | ip       | node
   264    |      465.3mb  |   229.9mb  |      1.4tb   |      1.5tb   |            0 |
 x.x.x.x  | x.x.x.x  | node1
   115    |        7.9mb  |    83.7mb  |     49.1gb   |     49.2gb   |            0 |
x.x.x.x  | x.x.x.x  | node2
   264    |      465.3mb  |   235.3mb  |      1.4tb   |      1.5tb   |            0 |
 x.x.x.x  | x.x.x.x  | node3
   116    |        7.9mb  |    82.8mb  |     49.1gb   |     49.2gb   |            0 |
x.x.x.x  | x.x.x.x  | node4
```

```
    115    |        8.4mb  |      85mb  |     49.1gb   |     49.2gb   |           0 |
 x.x.x.x  | x.x.x.x  | node5
```

Während ein gewisser Speicherversatz normal ist, ist alles über 10 % des Durchschnitts signifikant. Wenn die Shard-Verteilung verzerrt ist, kann die Nutzung der CPU-, Netzwerk- und Festplattenbandbreite ebenfalls verzerrt werden. Da mehr Daten im Allgemeinen mehr Indizierungs- und Suchvorgänge bedeuten, sind die schwersten Knoten in der Regel auch die Knoten mit der höchsten Ressourcenbelastung, während die leichteren Knoten eine nicht ausgelastete Kapazität darstellen.

Abhilfe: Verwenden Sie Shard-Zählungen, die ein Vielfaches der Datenknotenanzahl sind, um sicherzustellen, dass jeder Index gleichmäßig über die Datenknoten verteilt wird.

Index-Shard und Speicherversatz

Index-Shard-Versatz liegt vor, wenn ein oder mehrere Knoten mehr Shards eines Index enthalten als die anderen Knoten. Index-Speicher-Versatz liegt vor, wenn ein oder mehrere Knoten eine unverhältnismäßig große Menge des Gesamtspeichers eines Index halten.

Indexversatz ist schwieriger zu erkennen als Knoten-Versatz, da er eine gewisse Manipulation der _cat/shards-API-Ausgabe erfordert. Untersuchen Sie den Indexversatz, wenn es Anzeichen für einen Versatz in den Cluster- oder Knotenmetriken gibt. Im Folgenden finden Sie häufige Anzeichen für Indexversatz:

- HTTP-429-Fehler, die auf einer Teilmenge von Datenknoten auftreten
- Ungleiche Index- oder Suchoperationen-Warteschlangen auf den Datenknoten
- Ungleichmäßige JVM-Heap- und/oder CPU-Auslastung auf den Datenknoten

Abhilfe: Verwenden Sie Shard-Zählungen, die ein Vielfaches der Datenknotenanzahl sind, um sicherzustellen, dass jeder Index gleichmäßig über die Datenknoten verteilt wird. Wenn Sie immer noch eine Verzerrung des Indexspeichers oder des Shards sehen, müssen Sie möglicherweise eine Shard-Neuzuweisung erzwingen, die bei jeder Bereitstellung Ihrer Service-Domain in Blau/Grün erfolgt. OpenSearch

Unautorisierte Operation nach dem Auswählen des VPC-Zugriffs

Wenn Sie mit der OpenSearch Service-Konsole eine neue Domain erstellen, haben Sie die Möglichkeit, VPC oder Public Access auszuwählen. Wenn Sie VPC-Zugriff wählen, fragt der

OpenSearch Service nach VPC-Informationen ab und schlägt fehl, wenn Sie nicht über die entsprechenden Berechtigungen verfügen:

```
You are not authorized to perform this operation. (Service: AmazonEC2; Status Code:
 403; Error Code: UnauthorizedOperation
```

Damit diese Abfrage durchgeführt werden kann, benötigen Sie Zugriff auf die Operationen `ec2:DescribeVpcs`, `ec2:DescribeSubnets` und `ec2:DescribeSecurityGroups`. Diese Voraussetzung gilt nur für die Konsole. Wenn Sie die AWS CLI verwenden, um eine Domain mit einem VPC-Endpunkt zu erstellen und zu konfigurieren, benötigen Sie keinen Zugriff auf diese Operationen.

Hängenbleiben im Status "Loading" nach dem Erstellen von VPC-Domains

Es kann vorkommen, dass der Configuration state (Konfigurationsstatus) einer neu erstellten Domain mit VPC-Zugriff dauerhaft Loading bleibt. Wenn dieses Problem auftritt, haben Sie wahrscheinlich AWS Security Token Service (AWS STS) für Ihre Region deaktiviert.

Um VPC-Endpoints zu Ihrer VPC hinzuzufügen, muss OpenSearch Service die Rolle übernehmen. `AWSServiceRoleForAmazonOpenSearchService` Daher AWS STS muss aktiviert sein, um neue Domänen zu erstellen, die VPC-Zugriff in einer bestimmten Region verwenden. Weitere Informationen zur Aktivierung und Deaktivierung AWS STS finden Sie im IAM-Benutzerhandbuch.

Abgelehnte Anfragen an die API OpenSearch

Mit der Einführung der tagbasierten Zugriffskontrolle für die OpenSearch API treten möglicherweise Fehler auf, bei denen der Zugriff verweigert wurde. Dies kann daran liegen, dass eine oder mehrere Ihrer Zugriffsrichtlinien `Deny`enthalten, der den Zustand `ResourceTag` verwendet, und diese Bedingungen jetzt eingehalten werden.

Beispielsweise die folgende Richtlinie zum Verweigern des Zugriffs auf die Aktion `CreateDomain` der Konfigurations-API, wenn die Domain das Tag `environment=production` hatte. Obwohl die Aktionsliste auch `ESHttpPut` enthält, traf die Verweigerungserklärung nicht für diese oder andere `ESHttp*`-Aktionen zu.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [{
    "Action": [
      "es:CreateDomain",
      "es:ESHttpPut"
    ],
    "Effect": "Deny",
    "Resource": "*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:ResourceTag/environment": [
          "production"
        ]
      }
    }
  }]
}
```

Mit der zusätzlichen Unterstützung von Tags für OpenSearch HTTP-Methoden führt eine identitätsbasierte IAM-Richtlinie wie die oben beschriebene dazu, dass dem verbundenen Benutzer der Zugriff auf die Aktion verweigert wird. `ESHttpPut` Zuvor hätte der angehängte Benutzer in Ermangelung einer Tag-Validierung weiterhin PUT-Anfragen senden können.

Wenn Sie nach dem Aktualisieren Ihrer Domains auf die Service-Software R20220323 oder höher Fehler beim Zugriff feststellen, überprüfen Sie Ihre identitätsbasierten Zugriffsrichtlinien, um festzustellen, ob dies der Fall ist, und aktualisieren Sie sie gegebenenfalls, um den Zugriff zu ermöglichen.

Verbindung von Alpine Linux kann nicht hergestellt werden

Alpine Linux begrenzt die DNS-Antwortgröße auf 512 Byte. Wenn Sie versuchen, von Alpine Linux Version 3.18.0 oder niedriger aus eine Verbindung zu Ihrer OpenSearch Service-Domain herzustellen, kann die DNS-Auflösung fehlschlagen, wenn sich die Domain in einer VPC befindet und mehr als 20 Knoten hat. Wenn Sie eine Alpine Linux-Version verwenden, die höher als 3.18.0 ist, sollten Sie in der Lage sein, mehr als 20 Hosts aufzulösen. Weitere Informationen finden Sie in den Versionshinweisen zu Alpine Linux 3.18.0.

Wenn sich Ihre Domain in einer VPC befindet, empfehlen wir, andere Linux-Distributionen wie Debian, Ubuntu, CentOS, Red Hat Enterprise Linux oder Amazon Linux 2 zu verwenden, um eine Verbindung herzustellen.

Zu viele Anfragen für Search Backpressure

Bei der CPU-basierten Zugangskontrolle handelt es sich um einen Gatekeeping-Mechanismus, der die Anzahl der Anfragen an einen Knoten auf der Grundlage seiner aktuellen Kapazität proaktiv begrenzt, sowohl bei organischem Anstieg als auch bei Verkehrsspitzen. Übermäßige Anfragen geben bei Ablehnung den HTTP-Statuscode 429 „Zu viele Anfragen“ zurück. Dieser Fehler weist entweder auf unzureichende Clusterressourcen, ressourcenintensive Suchanfragen oder einen unbeabsichtigten Anstieg der Arbeitslast hin.

Der Such-Backpressure liefert den Grund für die Ablehnung, was bei der Feinabstimmung ressourcenintensiver Suchanfragen helfen kann. Bei Datenverkehrsspitzen empfehlen wir clientseitige Wiederholungen mit exponentiellem Backoff und Jitter.

Zertifikatsfehler bei der Verwendung von SDKs

Da AWS SDKs die CA-Zertifikate Ihres Computers verwenden, können Änderungen an den Zertifikaten auf den AWS Servern zu Verbindungsfehlern führen, wenn Sie versuchen, ein SDK zu verwenden. Fehlermeldungen variieren, enthalten aber in der Regel den folgenden Text:

```
Failed to query OpenSearch
...
SSL3_GET_SERVER_CERTIFICATE:certificate verify failed
```

Sie können diese Fehler verhindern, indem Sie die CA-Zertifikate und das Betriebssystem up-to-date Ihres Computers beibehalten. Wenn dieses Problem in einer Unternehmensumgebung auftritt und Sie Ihren eigenen Computer nicht selbst verwalten, müssen Sie möglicherweise einen Administrator bitten, bei der Aktualisierung zu helfen.

Die folgende Liste zeigt die Mindestanforderungen an Betriebssystem- und Java-Versionen:

- Microsoft Windows-Versionen mit installierten Updates von Januar 2005 oder später enthalten mindestens eine der erforderlichen Zertifizierungsstellen in ihrer Trust-Liste.
- Mac OS X 10.4 mit Java für Mac OS X 10.4 Release 5 (Februar 2007), Mac OS X 10.5 (Oktober 2007) und spätere Versionen enthalten mindestens eine der erforderlichen Zertifizierungsstellen in ihrer Trust-Liste.
- Red Hat Enterprise Linux 5 (März 2007), 6 und 7 und CentOS 5, 6, und 7 enthalten alle mindestens eine der erforderlichen Zertifizierungsstellen in ihrer standardmäßigen CA-Trust-Liste.

- Java 1.4.2_12 (Mai 2006), 5 Update 2 (März 2005) und alle späteren Versionen, einschließlich Java 6 (Dezember 2006), 7 und 8, enthalten mindestens eine der erforderlichen Zertifizierungsstellen in ihrer standardmäßigen CA-Trust-Liste.

Die drei Zertifizierungsstellen sind:

- Amazon Root CA 1
- Starfield Services Root Certificate Authority – G2
- Starfield Class 2 Certification Authority

Stammzertifikate der ersten beiden Behörden sind bei Amazon Trust Services erhältlich, aber up-to-date es ist einfacher, Ihren Computer zu behalten. Weitere Informationen zu von ACM bereitgestellten Zertifikaten finden Sie unter AWS Certificate Manager – Häufig gestellte Fragen.

> **Note**
>
> Derzeit verwenden OpenSearch Dienstdomänen in der Region US-East-1 Zertifikate von einer anderen Behörde. Wir planen die Aktualisierung der Region zur Verwendung dieser neuen Zertifikatsstellen in naher Zukunft.

Dokumentenverlauf für Amazon OpenSearch Service

In diesem Thema werden wichtige Änderungen an Amazon OpenSearch Service beschrieben. Service-Software-Updates bieten zusätzlich Unterstützung für neue Funktionen, Sicherheits-Patches, Fehlerbehebungen und andere Verbesserungen. Um neue Funktionen zu verwenden, müssen Sie möglicherweise die Service-Software in Ihrer Domain aktualisieren. Weitere Informationen finden Sie unter the section called “Service-Software-Updates”.

Servicefunktionen werden schrittweise dort eingeführt, AWS-Regionen wo ein Service verfügbar ist. Wir aktualisieren diese Dokumentation nur für die erste Version. Wir stellen keine Informationen über die Verfügbarkeit von Regionen zur Verfügung und kündigen auch keine späteren Rollouts von Regionen an. Informationen zur regionalen Verfügbarkeit von Servicefunktionen und zum Abonnieren von Benachrichtigungen über Updates finden Sie unter Was gibt's Neues bei AWS?

Relevante Daten zu diesem Verlauf:

- Aktuelle Produktversion:2021-01-01
- Letzte Produktveröffentlichung — 12. Juni 2024
- Letzte Aktualisierung der Dokumentation — 12. Juni 2024

Um Benachrichtigungen über Updates zu erhalten, können Sie den RSS-Feed abonnieren.

> **Note**
>
> Patch-Versionen: Bei Service-Softwareversionen, die mit „-P“ und einer Zahl wie R20211203-P4 enden, handelt es sich um Patch-Versionen. Patches werden vermutlich Leistungsverbesserungen, kleinere Bugfixes und Behebungen von Sicherheitslücken oder Verbesserungen der Sicherheitslage beinhalten. Da Patches keine neuen Funktionen oder bahnbrechenden Änderungen enthalten, haben sie in der Regel keine direkten Auswirkungen auf die Benutzer oder die Dokumentation, weshalb die Einzelheiten der einzelnen Patches nicht in diesem Dokumentverlauf enthalten sind.

Änderung	Beschreibung	Datum
Neue serviceverknüpfte Rolle	Amazon OpenSearch Service fügt eine	12. Juni 2024

	servicebezogene Rolle namens hinzu`AWSServiceRoleForOpensearchIngestionSelfManagedVpce` , die es Amazon OpenSearch Ingestion ermöglicht, Metrikdaten an Amazon CloudWatch für Pipelines mit selbstverwalteten VPC-Endpunkten zu senden.	
Amazon OpenSearch Service Zero-ETL-Integration mit Amazon S3	Amazon OpenSearch Service unterstützt jetzt direkte Abfragen zur Abfrage von Daten in Amazon S3.	22. Mai 2024
OpenSearch 2.13-Unterstützung	Amazon OpenSearch Service unterstützt jetzt OpenSearch Version 2.13. Diese Version enthält alle Funktionen, die Teil der Versionen 2.12 und 2.13 waren. Weitere Informationen finden Sie in den Versionshinweisen zu 2.12 und 2.13.	21. Mai 2024
Amazon OpenSearch Ingestion-Unterstützung für Data Prepper Version 2.7	Amazon OpenSearch Ingestion fügt Unterstützung für Data Prepper Version 2.7 hinzu. Weitere Informationen finden Sie in den Versionshinweisen zu 2.7.	4. April 2024

AWS-Service privater Zugang für OpenSearch serverlose Sammlungen	Sie können jetzt im Rahmen einer Netzwerkzugriffsrichtlinie bestimmten AWS-Services Zugriff auf Ihre OpenSearch serverlosen Sammlungen gewähren, z. B. Amazon Bedrock.	28. März 2024
Direkte EBS-Updates	Sie können jetzt einige EBS-Änderungen an Ihren Domains vornehmen, ohne dass eine blaue/grüne Bereitstellung in Amazon OpenSearch Service erfolgt.	14. Februar 2024
Sichtbarkeit von Konfigurationsänderungen	Sie können jetzt Änderungen an der Domain-Konfiguration in der Amazon OpenSearch Service-Konsole und mithilfe der Konfigurations-API verfolgen.	6. Februar 2024

Allgemeine Verfügbarkeit von Sammlungen zur Vektorsuche	Sammlungen von Amazon OpenSearch Serverless Vector Search sind jetzt allgemein verfügbar. In der Vorschauphase wurden die folgenden bemerkenswerten Verbesserungen vorgenommen: • Vektorsuchsammlungen unterstützen jetzt Workloads mit Milliarden von Vektoren mit jeweils bis zu 128 Dimensionen. • OpenSearch Dashboards unterstützen jetzt Vektorsuchsammlungen.	29. November 2023
OR1-Instanzen	Amazon OpenSearch Service unterstützt jetzt OR1-Instance-Typen.	29. November 2023
Direkte Abfragen mit Amazon S3 (Vorschauversion)	Direkte Abfragen bieten eine vollständig verwaltete Lösung, um Transaktionsdaten innerhalb von Sekunden nach dem Schreiben in einen Amazon S3-Bucket in Amazon OpenSearch Service verfügbar zu machen.	29. November 2023

Kapazität von 10 TiB für Zeitreihenerfassungen	Amazon OpenSearch Serverless bietet Unterstützung für bis zu 10 TiB Indexdaten für Zeitreihenerfassungen. Diese Version unterstützt außerdem eine maximal zulässige Kapazität von 200 OCUs für alle Arten von Sammlungen und die Möglichkeit, Standby-Replikate zu deaktivieren, wenn Sie eine Sammlung erstellen.	29. November 2023
OpenSearch 2.11-Unterstützung	Amazon OpenSearch Service unterstützt jetzt OpenSearch Version 2.11. Diese Version enthält alle Funktionen, die Teil der Versionen 2.10 und 2.11 waren. Weitere Informationen finden Sie in den Versionshinweisen zu 2.10 und 2.11.	17. November 2023
Amazon OpenSearch Ingestion-Unterstützung für Data Prepper Version 2.6	Amazon OpenSearch Ingestion fügt Unterstützung für Data Prepper Version 2.6 hinzu. Weitere Informationen finden Sie in den Versionshinweisen zu 2.6. Darüber hinaus können Sie Amazon DynamoDB als Pipeline-Quelle angeben. Weitere Informationen finden Sie unter Verwenden einer OpenSearch Ingestion-Pipeline mit Amazon DynamoDB.	17. November 2023

Amazon OpenSearch Ingestion-Unterstützung für Data Prepper Version 2.5	Amazon OpenSearch Ingestion fügt Unterstützung für Data Prepper Version 2.5 hinzu. Weitere Informationen finden Sie in den Versionsh inweisen zu 2.5. Darüber hinaus können Sie jetzt eine OpenSearch Dienstdom äne oder eine OpenSearc h Serverless-Sammlung als Pipeline-Quelle angeben. Weitere Informationen finden Sie im OpenSearch Quell-Plu g-In in der Data Prepper-D okumentation.	17. November 2023
CloudFormation Vorlage für Ferninferenz	Um die Einrichtung von Remote-Inferenzen für die semantische Suche zu vereinfachen, stellt Amazon OpenSearch Service in der Konsole eine AWS CloudForm ation Vorlage bereit, die den Prozess der Modellbereitstellu ng für Sie automatisiert.	7. November 2023

Aktualisierung der Richtlinie für dienstbezogene Rollen	Fügt die Berechtigungen hinzu, die für die Richtlinie für dienstbezogene Rollen zum Zuweisen und Aufheben der `AmazonOpenSearchServiceRolePolicy` Zuweisung von IPv6-Adressen erforderlich sind. Die veraltete Elasticsearch-Richtlinie `AmazonElasticsearchServiceRolePolicy` wurde ebenfalls aktualisiert, um die Abwärtskompatibilität zu gewährleisten.	26. Oktober 2023
Lebenszyklusrichtlinien für Amazon OpenSearch Serverless	Amazon OpenSearch Serverless führt Richtlinien für den Indexlebenszyklus ein, um die Verwaltung der Aufbewahrung und Löschung von Daten zu optimieren. Sie können jetzt APIs oder eine Konfigurationsoberfläche in der Konsole verwenden, um Datenaufbewahrungsrichtlinien für Zeitreihenerfassungen festzulegen, sodass Sie keine täglichen Indizes oder Skripts zum Löschen alter Daten erstellen müssen.	25. Oktober 2023

Unterstützung für iM4GN-Instanzen	Amazon OpenSearch Service unterstützt jetzt IM4GN-Instance-Typen. IM4GN-Instances sind für Workloads optimiert, die große Datensätze verwalten und eine hohe Speicherdichte pro vCPU benötigen.	20. Oktober 2023
Administrative Optionen	Amazon OpenSearch Service bietet jetzt mehrere Verwaltungsoptionen, mit denen Sie detailliert steuern können, ob Sie Probleme mit Ihrer Domain beheben müssen. Zu diesen Optionen gehören die Möglichkeit, den OpenSearch Prozess auf einem Datenknoten neu zu starten, und die Möglichkeit, einen Datenknoten neu zu starten.	17. Oktober 2023
Optionale Plug-ins	Amazon OpenSearch Service bietet Unterstützung für vier neue Sprachanalyse-Plugins: Nori (Koreanisch), Sudachi (Japanisch), Pinyin (Chinesisch) und StConvert Analysis (Chinesisch) sowie das Amazon Personalize Search Ranking-Plugin.	16. Oktober 2023

OpenSearch 2.9-Unterstützung	Amazon OpenSearch Service unterstützt jetzt OpenSearch Version 2.9. Diese Version enthält alle Funktionen, die Teil der Versionen 2.8 und 2.9 waren. Weitere Informationen finden Sie in den Versionshinweisen zu 2.8 und 2.9.	2. Oktober 2023
ML-Steckverbinder	Amazon OpenSearch Service bietet Unterstützung für Machine-Learning-Konnektoren (ML). Konnektoren erleichtern den Zugriff auf ML-Modelle AWS-Services, die auf anderen Plattformen oder auf Plattformen für maschinelles Lernen (ML) von Drittanbietern gehostet werden.	6. September 2023
Amazon OpenSearch Ingestion bietet Unterstützung für Data Prepper Version 2.4	Amazon OpenSearch Ingestion fügt Unterstützung für Data Prepper Version 2.4 hinzu. Weitere Informationen finden Sie in den Versionshinweisen zu 2.4. Darüber hinaus können Sie jetzt Amazon Managed Streaming for Apache Kafka (Amazon MSK) als Pipeline-Quelle angeben.	31. August 2023

Kapazität von 6 TiB für Zeitreihenerfassungen	Amazon OpenSearch Serverless bietet Unterstützung für bis zu 6 TiB Indexdaten für Zeitreihenerfassungen. Diese Version unterstützt außerdem eine maximal zulässige Kapazität von 100 OCUs sowohl für die Suche als auch für die Erfassung von Zeitreihen.	15. August 2023
Sammlungen mit Vektorsuche	Amazon OpenSearch Serverless bietet die Option, eine Vektorsuchsammlung zu erstellen, in der Sie Vektoreinbettungen speichern können, um Ähnlichkeits- und semantische Suchen zu ermöglichen.	26. Juli 2023
OpenSearch 2.7 Unterstützung	Amazon OpenSearch Service unterstützt jetzt OpenSearch Version 2.7. Diese Version enthält alle Funktionen, die Teil der Versionen 2.6 und 2.7 waren. Weitere Informationen finden Sie in den Versionshinweisen zu 2.6 und 2.7.	10. Juli 2023

Unterstützung für Data Prepper 2.3	Amazon OpenSearch Ingestion fügt Unterstützung für Data Prepper Version 2.3 hinzu. Weitere Informationen finden Sie in den Versionsh inweisen zu 2.3. Darüber hinaus können Sie jetzt Amazon Security Lake als Pipeline-Quelle angeben.	26. Juni 2023
Multi-AZ mit Standby	Amazon OpenSearch Service bietet die Option, eine Domain in drei Availability Zones (AZs) bereitzustellen, wobei jede AZ eine vollständige Kopie der Daten enthält und Knoten in einer dieser AZs als Standby fungieren. Die Bereitste llungsoption Multi-AZ mit Standby bietet eine Verfügbar keit von 99,99% und eine gleichbleibende Leistung im Falle eines Infrastrukturausfa lls.	3. Mai 2023
Neue serviceverknüpfte Rolle	Amazon OpenSearc h Service fügt eine serviceverknüpfte Rolle namens hinzu`AWSServic eRoleForAmazonOpen SearchIngestionSer vice` , die es Amazon OpenSearch Ingestion ermöglicht, Metrikdaten an zu senden. Amazon CloudWatch	26. April 2023

OpenSearch Einnahme durch Amazon	Amazon OpenSearch Ingestion ist ein vollständig verwalteter Datensammler, der Protokoll- und Ablaufverfolgungsdaten in Echtzeit für OpenSearch Service-Domains und OpenSearch serverlose Sammlungen bereitstellt. OpenSearch Durch die Aufnahme müssen Sie keine Drittanbieterlösungen wie Logstash oder Jaeger verwenden, um Daten in Ihre Domains und Sammlungen aufzunehmen.	26. April 2023
OpenSearch 2.5 Unterstützung	Amazon OpenSearch Service unterstützt jetzt OpenSearch Version 2.5. Diese Version enthält alle Funktionen, die Teil der Versionen 2.4 und 2.5 waren. Weitere Informationen finden Sie in den Versionshinweisen zu 2.4 und 2.5.	13. März 2023

Wartungsfenster außerhalb der Spitzenzeiten	Amazon OpenSearch Service fügt Zeitfenster außerhalb der Spitzenzeiten hinzu, d. h. tägliche 10-Stunden-Zeitblöcke mit geringem Datenverkehr, in denen Service-Software-Updates und Auto-Tune-Optimierungen geplant werden können, für die eine blaue/grüne Bereitstellung erforderlich ist. Updates außerhalb der Spitzenzeiten tragen dazu bei, die Belastung der dedizierten Master-Knoten eines Clusters in Zeiten mit höherem Datenverkehr zu minimieren. Für neue Domains, die nach dem 16. Februar erstellt wurden, wird das Zeitfenster außerhalb der Spitzenzeiten automatisch für die Zeit zwischen 22:00 Uhr und 8:00 Uhr Ortszeit konfiguriert. Für bestehende Domains müssen Sie das Fenster explizit aktivieren.	16. Februar 2023

Konfiguration der SAML-Authentifizierung bei der Domainerstellung	Amazon OpenSearch Service unterstützt jetzt die Konfiguration der SAML-Authentifizierung bei der Domainerstellung. Bisher mussten Sie SAML-Optionen konfigurieren, nachdem die Domain bereits erstellt wurde.	1. Februar 2023
Remote-Neuindizierung für VPC-Domains	Amazon OpenSearch Service fügt die Option für eine VPC-Endpunktverbindung zwischen zwei Domains hinzu. Sie können jetzt Remote-Neuindizierung verwenden, um Indizes ohne Reverse-Proxy von einer VPC-Domain in eine andere zu kopieren. Ihre VPC-Domain muss die Service-Software R20221114 oder höher ausführen, um diese Funktion nutzen zu können.	31. Januar 2023

Allgemeine Verfügbarkeit von Amazon OpenSearch Serverless	Amazon OpenSearch Serverless ist jetzt allgemein verfügbar. In der Vorschaup hase wurden die folgenden bemerkenswerten Verbesser ungen vorgenommen: • Die Kapazität kann jetzt auf die minimal konfiguri erten OCUs herunters kaliert werden, wenn der Datenverkehr auf dem Sammlungsendpunkt abnimmt. • Die maximal zulässige Anzahl an OCUs sowohl für die Indizierung als auch für die Suche wurde von 20 auf 50 erhöht. Jede OCU enthält ausreichend flüchtige n Hot-Speicher für 120 GiB Indexdaten. • Sie können jetzt Datenzugr iffseinstellungen beim Erstellen von Sammlungen konfigurieren, anstatt sie in einem separaten Workflow konfigurieren zu müssen.	25. Januar 2023

Asynchroner Testlauf	Amazon OpenSearch Service unterstützt jetzt den asynchron en Testlauf, mit dem Sie vor einer Konfigurationsände rung eine Validierungsprüfun g durchführen können. Außerdem werden Sie benachrichtigt, wenn Ihre Änderungen zu einer blauen/gr ünen Bereitstellung führen.	19. Januar 2023
Neue serviceverknüpfte Rolle	Amazon OpenSearc h Service fügt eine serviceverknüpfte Rolle namens hinzu`AWSServic eRoleForAmazonOpen SearchServerless` , die es OpenSearch Serverless ermöglicht, Metrikdaten an zu senden. Amazon CloudWatch	29. November 2022
Vorversion von Amazon OpenSearch Serverless	Amazon OpenSearch Serverless ist eine serverlos e On-Demand-Konfigur ation mit auto Skalierung für Amazon OpenSearch Service. Serverless beseitigt die betriebliche Komplexität der Bereitstellung, Konfigura tion und Optimierung Ihrer Cluster. OpenSearch	29. November 2022

OpenSearch 2.3 Unterstützung	Amazon OpenSearch Service unterstützt jetzt OpenSearch Version 2.3. Diese Version enthält alle Funktionen, die Teil der Versionen 2.0, 2.1 und 2.2 waren. Weitere Informationen finden Sie in den Versionshinweisen zu 2.0, 2.1, 2.2 und 2.3. Version 2.3 enthält eine grundlegende Änderung. Weitere Informationen finden Sie unter Unterstützte Upgrade-Pfade.	15. November 2022
Unterstützung für Benachrichtigungs-Plugins	Amazon OpenSearch Service unterstützt jetzt das Notifications-Plugin, das einen zentralen Ort für all Ihre Benachrichtigungen von OpenSearch Plugins bietet. Ab Version 2.0 wurden Warnziele als veraltet eingestuft und durch Benachrichtigungs-Kanäle ersetzt.	15. November 2022

Unterstützung für Kibana 7.1.1	Amazon OpenSearch Service-Domains, auf denen Elasticsearch 7.1 ausgeführt wird, unterstützen jetzt die neueste Patch-Version für Kibana 7.1.1, die Bugfixes hinzufügt und die Sicherheit verbessert. Wenn Sie Ihre 7.1-Domains auf die Service-Software R20221114 aktualisieren, aktualisiert OpenSearch Service sie automatisch auf diese Patch-Version.	15. November 2022
Unterstützung für Kibana 6.8.13	Amazon OpenSearch Service-Domains, auf denen Elasticsearch 6.8 ausgeführt wird, unterstützen jetzt die neueste Patch-Version für Kibana 6.8.13, die Bugfixes hinzufügt und die Sicherheit verbessert. Wenn Sie Ihre 6.8-Domains auf die Service-Software R20221114 aktualisieren, aktualisiert OpenSearch Service sie automatisch auf diese Patch-Version.	15. November 2022

Unterstützung für Kibana 6.3.2	Amazon OpenSearch Service-Domains, auf denen Elasticsearch 6.3 ausgeführt wird, unterstützen jetzt die neueste Patch-Version für Kibana 6.3.2, die Bugfixes hinzufügt und die Sicherheit verbessert. Wenn Sie Ihre 6.3-Domains auf die Service-Software R20221114 aktualisieren, aktualisiert OpenSearch Service sie automatisch auf diese Patch-Version.	15. November 2022

AWS PrivateLink	Mit von Amazon OpenSearch Service verwalteten VPC-Endpunkten können Sie eine direkte Verbindung zu OpenSearch Service-VPC-Domains herstellen, indem Sie einen VPC-Schnittstellen-Endpunkt verwenden, anstatt eine Verbindung über das Internet herzustellen. Auf einen OpenSearch vom Service verwalteten VPC-Endpunkt kann nur innerhalb der VPC zugegriffen werden, in der der Endpunkt bereitgestellt wird, oder von allen VPCs, die mit der VPC verbunden sind, auf der der Endpunkt bereitgestellt wird, wie es die Routing-Tabellen und Sicherheitsgruppen zulassen. Ihre VPC-Domain muss die Service-Software R20220928 oder höher ausführen, um eine Verbindung zu einem Schnittstellen-VPC-Endpunkt herzustellen.	7. November 2022

Fehlerbehebungen und Leistungsverbesserungen	Die Servicesoftware R20220928 enthält Fehlerbehebungen und Leistungsverbesserungen, einschließlich verbesserter SAML-Protokollierung. Das Update ändert auch den Standardmandanten auf `Global` statt auf `Private`.	3. Oktober 2022
Verbesserte API-Referenz	Amazon OpenSearch Service bietet eine verbesserte, umfassende Konfigurations-API-Referenz. Die neuen Referenzen enthalten alle verfügbaren Aktionen und Datentypen, Beispiele für Anforderungs- und Antwortsyntax sowie Links zu den entsprechenden SDK-Verweisen für alle unterstützten Sprachen.	13. September 2022
Blau/Grün-Validierung	Amazon OpenSearch Service führt jetzt vor Blau/Grün-Bereitstellungen eine Validierungsprüfung durch und zeigt Validierungsfehler an, wenn Ihre Domain nicht für ein Update in Frage kommt.	16. August 2022
OpenSearch 1.3 Unterstützung	Amazon OpenSearch Service unterstützt jetzt OpenSearch Version 1.3. Weitere Informationen finden Sie unter 1.3 Versionshinweise.	27. Juli 2022

Unterstützung für ML-Commons-Plug-Ins	Amazon OpenSearch Service bietet Unterstützung für das ML Commons-Plugin, das über Transport- und REST-API-Aufrufe eine Reihe gängiger Algorithmen für maschinelles Lernen bereitstellt. Sie können auch über PPL-Befehle mit dem ML-Commons-Plug-In interagieren.	27. Juli 2022
Unterstützung für gp3-Volumes	Amazon OpenSearch Service bietet Unterstützung für den Volumetyp gp3 EBS General Purpose SSD. Sie können zusätzliche bereitgestellte IOPS und Durchsatz angeben, wenn Sie die Domain erstellen oder ändern.	26. Juli 2022
Verbesserte Dokumentation bewährter Methoden	Die Amazon OpenSearch Service-Dokumentation enthält verbesserte betriebliche Best Practices und allgemeine Empfehlungen für die Erstellung und den Betrieb von OpenSearch Service-Domains.	6. Juli 2022
Integration mit Service Quotas	In der Service Quotas-Konsole können Sie jetzt Kontingente für Amazon OpenSearch Service Quotas einsehen und Kontingenterhöhungen beantragen.	29. Juni 2022

Tag-basierte Zugriffskontrolle für die API OpenSearch	Sie können jetzt Tags verwenden, um den Zugriff auf die OpenSearch APIs zu kontrollieren. Bisher konnten Sie nur Tags verwenden, um den Zugriff auf die Konfigura tions-API zu steuern.	16. Juni 2022
Cluster-übergreifende Suche in mehreren Regionen	Die clusterübergreifende Suche wird jetzt unterstützt, AWS-Regionen solange auf beiden Domains Elasticsearch Version 7.10 oder höher oder eine beliebige Version von ausgeführt wird. OpenSearch	14. Juni 2022
Support für Single Kibana 5.6	Amazon OpenSearch Service fügt Unterstützung für einzelne Kibana 5.6.16 hinzu. Mit SingleKibana 5.6.16 können Sie Kibana 5.6 als Front-End verwenden, während Sie eine Verbindung mit Elasticse arch in den Versionen 5.1, 5.3, 5.5 und 5.6 herstellen. Sie müssen über Serviceso ftware R20220323 oder neuer verfügen, um Single Kibana 5.6 verwenden zu können.	4. April 2022

R20220323-P1	Amazon OpenSearch Service hat kürzlich das Service-Software-Update R20220323 veröffentlicht, aber das Update wurde anschließend aufgrund eines Problems rückgängig gemacht. Wir empfehlen Ihnen, Ihre Domains auf Patch-Release R20220323-P1 oder höher zu aktualisieren, wodurch das Problem behoben wird.	4. April 2022
OpenSearch 1.2 Unterstützung	Amazon OpenSearch Service unterstützt jetzt OpenSearch Version 1.2. Weitere Informationen finden Sie unter 1.2 Versionshinweise.	4. April 2022
Beobachtbarkeit	Die Standardinstallation von OpenSearch Dashboards for Amazon OpenSearch Service umfasst das Observability-Plugin, mit dem Sie datengesteuerte Ereignisse mithilfe der Piped Processing Language (PPL) visualisieren können, um Ihre Daten zu untersuchen und abzufragen. Das Plugin erfordert OpenSearch 1.2 oder höher und die Servicesoftware R20220323 oder höher.	4. April 2022

Support für Kibana 7.7.1	Amazon OpenSearch Service-Domains, auf denen Elasticsearch 7.7 ausgeführt wird, unterstützen jetzt die neueste Patch-Version für Kibana 7.7, die Bugfixes hinzufügt und die Sicherheit verbessert. Wenn Sie Ihre 7.7-Domains auf die Service-Software R20220323 oder höher aktualisieren, aktualisiert OpenSearch Service sie automatisch auf diese Patch-Version.	4. April 2022
Änderungen der JVM-Speicherdruckmetrik	Amazon OpenSearch Service hat die Logik für die `JVMMemoryPressure` CloudWatch Metriken geändert, um die Speichernutzung genauer widerzuspiegeln. Zuvor betrachteten die Metriken nur den Speicherpool der alten Generation von JVM-Heap. Nach dieser Änderung berücksichtigt die Metrik auch den Speicherpool der jungen Generation. Nachdem Sie Ihre Domain auf Servicesoftware R20220323 aktualisiert haben, sehen Sie möglicherweise einen Anstieg der `JVMMemoryPressure` -, `MasterJVMMemoryPressure` - und/oder `WarmJVMMemoryPressure` -Metriken.	4. April 2022

Benutzerdefinierte Wörterbücher mit dem IK-Analyse-Plug-in (Chinesisch)	Amazon OpenSearch Service unterstützt jetzt die Verwendung benutzerdefinierter Wörterbücher mit dem Analyse-Plugin IK (Chinese).	4. April 2022
Cluster-übergreifende Replikation auf bestehenden Domain	Amazon OpenSearch Service hat die Einschränkung aufgehoben, dass Sie die clusterübergreifende Suche und clusterübergreifende Replikation nur für Domains implementieren können, die am oder nach dem 3. Juni 2020 erstellt wurden. Sie können diese Funktionen jetzt für alle Domains aktivieren, unabhängig davon, wann sie erstellt wurden. Beide Domain müssen über Serviceoftware R20220323 oder höher ausgeführt werden.	4. April 2022
Einblick in Blau/Grün-Bereitstellungen	Amazon OpenSearch Service bietet jetzt mehr Einblick in den Fortschritt der Blau/Grün-Implementierungen. Sie können diese Details in der Konsole oder mithilfe der Konfigurations-API überwachen.	27. Januar 2022

Differenzierte Zugriffskontrolle für vorhandene Domains	Sie können nun die differenzierte Zugriffskontrolle für vorhandene Domains aktivieren. Sie können einen temporären Migrationszeitraum für offene/IP-basierte Zugriffsrichtlinien aktivieren, damit Benutzer weiterhin auf Ihre Domain zugreifen können, während Sie Rollen erstellen und zuordnen. Für die Aktivierung einer differenzierten Zugriffskontrolle für vorhandene Domains ist Service-Software R20211203 oder höher erforderlich.	6. Januar 2022
Die Rollen der Dashboards wurden umbenannt OpenSearch	Mit der Service-Software R20211203 wurde die Rolle `kibana_user` in `opensearch_dashboards_user` , und `kibana_read_only` in `opensearch_dashboards_read_only` umbenannt. Diese Änderung gilt für alle neu erstellten 1. OpenSearch X-Domänen. Für bestehende OpenSearch Domänen, die Sie auf die Servicesoftware R20211203 aktualisieren, bleiben die Rollen unverändert.	4. Januar 2022

OpenSearch 1.1 Unterstützung	Amazon OpenSearch Service unterstützt jetzt OpenSearch Version 1.1. Weitere Informationen finden Sie unter 1.1 Versionshinweise.	4. Januar 2022
Visueller Editor ISM	Die Standardinstallation von OpenSearch Dashboards for Amazon OpenSearch Service unterstützt jetzt den visuellen Editor für ISM-Richtlinien. Für diese Funktion ist OpenSearch 1.1 oder höher erforderlich.	4. Januar 2022
Update zur Vermeidung des Problems des verwirrten Stellvertreters (dienstübergreifend)	Amazon OpenSearch Service unterstützt die Verwendung der Kontextschlüssel `aws:SourceArn` und der `aws:SourceAccount` globalen Bedingungsschlüssel in IAM-Ressourcenrichtlinien, um das Problem des verwirrten Stellvertreters zu vermeiden. Sie müssen über Service-Software R20211203 oder höher verfügen, um diese Bedingungsschlüssel verwenden zu können.	4. Januar 2022

Log4j-Patch	Die Service-Software R20211203-P2 aktualisiert die im Service verwendete Version von Log4j, wie in den Hinweisen in CVE-2021-44228 und OpenSearch CVE-2021-45046 empfohlen. Der Patch gilt für Domains, auf denen OpenSearch alle Versionen von Elasticsearch ausgeführt werden. OpenSearch Der Service wird weiterhin verschiedene Log4j-Versionen intern aktualisieren, und diese werden nicht unbedingt auf die neueste Version von Log4j beschränkt sein. Die Log4j-Version auf Ihrer Domain hängt von der Softwareversion ab, die auf der Domain ausgeführt wird. Unabhängig von der Log4j-Version enthalten Ihre Domains jedoch das Log4j-Update, das zur Behebung von CVE-2021-44228 und CVE-2021-45046 erforderlich ist, sofern Sie R20211203-P2 oder höher ausführen.	15. Dezember 2021

Cluster-übergreifende Replikation	Mit der clusterübergreifenden Replikation können Sie Indizes, Mappings und Metadaten von einer Service-Domain in eine andere replizieren. OpenSearch Für die clusterübergreifende Replikation ist eine Domain erforderlich, auf der Elasticsearch 7.10 oder 1.1 oder höher ausgeführt wird. OpenSearch	5. Oktober 2021
Neue verwaltete Richtlinien AWS	Die Einführung von Amazon OpenSearch Service beinhaltet neue AWS verwaltete Richtlinien und die Abschaffung alter Richtlinien.	8. September 2021
Support für Kibana 6.4.3	Amazon OpenSearch Service-Domains, auf denen die Legacy-Elasticsearch-Version 6.4 ausgeführt wird, unterstützen jetzt die neueste Patch-Version für Kibana 6.4, die Bugfixes hinzufügt und die Sicherheit verbessert. OpenSearch Der Service aktualisiert Domains automatisch auf diese Patch-Version.	8. September 2021

Datenströme	Amazon OpenSearch Service bietet Unterstützung für Datenstreams, wodurch die Verwaltung von Zeitreihe ndaten vereinfacht wird. Ihre Domain muss OpenSearc h 1.0 oder höher laufen, um Datenstreams verwenden zu können.	8. September 2021
OpenSearch Amazon-Dienst	AWS benennt Amazon OpenSearch Service um, um das alte Branding „Elastics earch“ zu entfernen. Amazon OpenSearch Service unterstüt zt OpenSearch und veraltete s Elasticsearch OSS. Wenn Sie einen Cluster erstellen, haben Sie die Wahl, welche Suchmaschine Sie verwenden möchten. OpenSearch Der Service bietet umfassende Kompatibilität mit Elasticse arch OSS 7.10, der endgültig en Open-Source-Version der Software.	8. September 2021

Cold Storage	Der Cold Storage ist eine neue Speicherebene für selten aufgerufene oder historische Daten. Cold-Indizes belegen nur S3-Speicher und haben keine angefügte Rechenlei stung. Für den Cold Storage ist eine Domain erforderlich, auf der Elasticsearch 7.9 oder neuer ausgeführt wird, und die Servicesoftware R20210426 oder neuer ausgeführt wird.	13. Mai 2021
ARM-basierte Graviton-Instances	Amazon OpenSearch Service unterstützt jetzt ARM-basie rte Graviton-Instance-Typen (M6G, C6G, R6G und R6GD). Graviton-Instance-Typen sind auf neuen und vorhanden en Domains verfügbar, auf denen Elasticsearch 7.9 oder neuer ausgeführt wird und die Servicesoftware R20210331 oder neuer ausgeführt wird.	4. Mai 2021

ISM-Vorlagen	Amazon OpenSearch Service bietet Unterstützung für ISM-Vorlagen, mit denen Sie automatisch eine ISM-Richtlinie an einen Index anhängen können, wenn der Index einem in der Richtlinie definierten Muster entsprich t. ISM-Vorlagen erfordern Servicesoftware R20210426 oder neuer. Dieses Update veraltert auch die `policy_id` -Einstellung, d. h. Sie können keine Indexvorlagen mehr verwenden, um ISM-Richt linien auf neu erstellte Indizes anzuwenden. Das Update führt eine grundlegende Änderung für bestehende CloudFormation Vorlagen ein, die diese Einstellung verwenden.	27. April 2021
Support für Elasticsearch 7.10	Amazon OpenSearch Service unterstützt jetzt Elasticse arch Version 7.10. Weitere Informationen finden Sie unter 7.10 Versionshinweise.	21. April 2021

Asynchrone Suche	Amazon OpenSearch Service unterstützt jetzt die asynchrone Suche, sodass Sie Suchanfragen im Hintergrund ausführen können. Für die asynchrone Suche ist eine Domain erforderlich, auf der Elasticsearch 7.10 oder neuer ausgeführt wird, und die Servicesoftware R20210331 oder neuer ausgeführt wird.	21. April 2021
Tag-basierte Zugriffskontrolle für die Konfigurations-API	Sie können jetzt AWS Tags verwenden, um den Zugriff auf die Amazon ES-Konfigurations-API zu steuern.	2. März 2021
Automatische Optimierung	Amazon OpenSearch Service fügt Auto-Tune hinzu, das Leistungs- und Nutzungsmetriken aus Ihrem Cluster verwendet, um Änderungen an den JVM-Einstellungen auf Ihren Knoten vorzuschlagen. Für die automatische Optimierung ist eine Domain erforderlich, auf der Elasticsearch 6.7 oder neuer ausgeführt wird, und die Servicesoftware R20201117 oder neuer ausgeführt wird.	24. Februar 2021

Trace Analytics	Die Standardinstallation von Kibana for Amazon OpenSearch Service umfasst jetzt das Trace-Analytics-Plugin, mit dem Sie Trace-Daten aus Ihren verteilten Anwendungen überwachen können. Für das Plug-in ist eine Domain erforderlich, auf der Elasticsearch 7.9 oder neuer ausgeführt wird, und die Servicesoftware R20210201 oder neuer ausgeführt wird.	17. Februar 2021
Shard-Metriken	Amazon OpenSearch Service fügt die folgenden CloudWatch Metriken für die Verfolgung des Shard-Status hinzu:`Shards.active` ,`Shards.unassigned` , `Shards.delayedUnassigned` `Shards.activePrimary` ,`Shards.initializing` ,`Shards.relocating` . Die Metriken sind auf Domains mit Service-Software R20210201 oder höher verfügbar.	17. Februar 2021

Kibana-Berichte	Die Standardinstallation von Kibana for Amazon OpenSearch Service unterstützt jetzt On-Demand-Berichte für die Seiten Discover, Visualize und Dashboard. Für diese Funktion ist eine Domain erforderlich, auf der Elasticsearch 7.9 oder neuer und die Servicesoftware R20210201 oder neuer ausgeführt wird.	17. Februar 2021
Support für Kibana 5.6.16	Amazon OpenSearch Service-Domains, auf denen Elasticsearch 5.6 ausgeführt wird, unterstützen jetzt die neueste Patch-Version für Kibana 5.6, die Bugfixes hinzufügt und die Sicherheit verbessert. Amazon ES aktualisiert Domains automatisch auf diese Patch-Version.	17. Februar 2021
Verschlüsselung für vorhandene Domains	Amazon OpenSearch Service unterstützt jetzt die Aktivierung der Verschlüsselung ruhender Daten und der node-to-node Verschlüsselung für bestehende Domains, auf denen Elasticsearch 6.7 oder höher ausgeführt wird. Nachdem Sie diese Einstellungen aktiviert haben, können Sie sie nicht mehr deaktivieren.	27. Januar 2021

Remote-Neuindexierung	Amazon OpenSearch Service unterstützt jetzt die Remote-Neuindizierung, sodass Sie Indizes von Remote-Domains migrieren können. Diese Funktion erfordert Service-Software R20201117 oder neuer.	24. November 2020
Piped Processing Language	Amazon OpenSearch Service unterstützt jetzt Piped Processing Language (PPL), eine Abfragesprache, mit der Sie die Pipe-Syntax (|) verwenden können, um in Elasticsearch gespeicherte Daten abzufragen. Diese Funktion erfordert Service-Software R20201117 oder neuer. Weitere Informationen hierzu finden Sie unter .	24. November 2020
Kibana-Notebooks	Amazon OpenSearch Service bietet Unterstützung für Kibana-Notizbücher, sodass Sie Live-Visualisierungen und erläuternden Text in einer einzigen Oberfläche kombinieren können. Diese Funktion erfordert Service-Software R20201117 oder neuer.	24. November 2020

Gantt-Diagramme	Die Standardinstallation von Kibana for Amazon OpenSearch Service unterstützt jetzt einen neuen Visualisierungstyp, Gantt-Diagramme. Diese Funktion erfordert Service-Software R20201117 oder neuer.	24. November 2020
Support für Elasticsearch 7.9	Amazon OpenSearch Service unterstützt jetzt Elasticsearch Version 7.9. Weitere Informationen finden Sie unter 7.9 Versionshinweise.	24. November 2020
Aktualisierungen für Anomalieerkennung	Die Anomalieerkennung für Amazon OpenSearch Service bietet Unterstützung für hohe Kardinalität, sodass Sie Anomalien anhand von Dimensionen wie IP-Adresse, Produkt-ID, Ländercode usw. kategorisieren können. Diese Funktion erfordert Service-Software R20201117 oder neuer.	24. November 2020

Aktualisierungen für dynamisches Wörterbuch	Mit Amazon OpenSearch Service können Sie jetzt Ihre Suchanalyseprogramme aktualisieren, ohne sie erneut indizieren zu müssen. Sie können die Wörterbuchdateien für einige oder alle Ihrer Domains aktualisieren, und Amazon ES verfolgt Paketversionen im Laufe der Zeit, sodass Sie einen Überblick darüber haben, was sich wann geändert hat. Diese Funktion erfordert Service-Software R20201019 oder neuer.	17. November 2020
Benutzerdefinierte Endpunkte	Amazon OpenSearch Service unterstützt jetzt benutzerdefinierte Endpunkte, mit denen Sie Ihrer Amazon ES-Domain eine neue URL zuweisen können. Wenn Sie je Domain austauschen, können Sie die gleiche URL pflegen. Diese Funktion erfordert Service-Software R20201019 oder neuer.	5. November 2020

Neue Sprach-Plug-ins	Amazon OpenSearch Service unterstützt jetzt die Plug-ins IK (Chinese) Analysis, Vietnamese Analysis und Thai Analysis auf Domains, auf denen Elasticsearch 7.7 oder höher mit der Service-Software R20201019 oder höher ausgeführt wird.	28. Oktober 2020
Support für Elasticsearch 7.8	Amazon OpenSearch Service unterstützt jetzt Elasticsearch Version 7.8. Weitere Informationen finden Sie unter 7.8 Versionshinweise.	28. Oktober 2020
SAML-Authentifizierung für Kibana	Amazon OpenSearch Service unterstützt jetzt die SAML-Authentifizierung für Kibana, sodass Sie externe Identitätsanbieter verwenden können, um sich bei Kibana anzumelden, eine detaillierte Zugriffskontrolle zu verwalten, Ihre Daten zu durchsuchen und Visualisierungen zu erstellen. Diese Funktion erfordert Service-Software R20201019 oder neuer.	27. Oktober 2020
T3-Instances	Amazon OpenSearch Service unterstützt jetzt die `t3.medium` Instance-Typen `t3.small` und.	23. September 2020

Prüfungsprotokolle	Amazon OpenSearch Service unterstützt jetzt Prüfprotokolle für Ihre Daten, mit denen Sie fehlgeschlagene Anmeldeversuche, Benutzerzugriffe auf Indizes, Dokumente und Felder und vieles mehr verfolgen können. Diese Funktion erfordert Service-Software R20200910 oder neuer.	16. September 2020
UltraWarm Aktualisierungen	UltraWarm for Amazon OpenSearch Service fügt neue Metriken, neue Einstellungen, eine größere Migrationswarteschlange und eine Stornierungs-API hinzu. Für diese Updates ist Serviceoftware R20200910 oder neuer erforderlich. Weitere Informationen finden Sie unter .	14. September 2020
Learning to Rank	Amazon OpenSearch Service unterstützt jetzt das Open-Source-Plugin Learning to Rank, mit dem Sie Technologien für maschinelles Lernen verwenden können, um die Suchrelevanz zu verbessern. Diese Funktion erfordert Service-Software R20200721 oder neuer.	27. Juli 2020

k-NN-Kosinus-Ähnlichkeit	Mit k-Nearest Neighbor (k-NN) können Sie nun zusätzlich zur euklidischen Entfernung nach „nächsten Nachbarn“ nach Kosinusähnlichkeit suchen. Diese Funktion erfordert Service-Software R20200721 oder neuer.	23. Juli 2020
gzip-Komprimierung	Amazon OpenSearch Service unterstützt jetzt die GZIP-Komprimierung für die meisten HTTP-Anfragen und -Antworten, wodurch die Latenz reduziert und Bandbreite gespart werden kann. Diese Funktion erfordert Service-Software R20200721 oder neuer.	23. Juli 2020
Support für Elasticsearch 7.7	Amazon OpenSearch Service unterstützt jetzt Elasticsearch Version 7.7. Weitere Informationen finden Sie unter 7.7 Versionshinweise.	23. Juli 2020
Kibana-Karten-Service	Die Standardinstallation von Kibana für Amazon OpenSearch Service umfasst jetzt einen WMS-Kartenserver, mit Ausnahme von Domains in den Regionen Indien und China.	18. Juni 2020

SQL-Verbesserungen	Die SQL-Unterstützung für Amazon OpenSearch Service unterstützt jetzt viele neue Operationen, eine spezielle Kibana-Benutzeroberfläche für die Datenexploration und eine interaktive CLI. Weitere Informationen finden Sie unter .	3. Juni 2020
Cluster-übergreifende Suche	Mit Amazon OpenSearch Service können Sie clusterüb ergreifende Abfragen und Aggregationen für mehrere verbundene Domains durchführen.	3. Juni 2020
Anomalieerkennung	Mit Amazon OpenSearch Service können Sie Anomalien fast in Echtzeit automatisch erkennen.	3. Juni 2020
UltraWarm	UltraWarm Der Speicherp latz für Amazon OpenSearc h Service hat die öffentliche Vorschauversion verlassen und ist jetzt allgemein verfügbar. Die Funktion unterstützt jetzt eine größere Auswahl an Versionen und AWS-Regionen. Weitere Informationen finden Sie unter .	5. Mai 2020

Benutzerdefinierte Wörterbücher	Mit Amazon OpenSearch Service können Sie benutzerdefinierte Wörterbuchdateien zur Verwendung mit Ihrem Cluster hochladen. Diese Dateien verbessern Ihre Suchergebnisse, indem sie Elasticsearch anweisen, bestimmte hochfrequente Wörter zu ignorieren oder Begriffe als gleichwertig zu behandeln.	21. April 2020
Support für Elasticsearch 7.4	Amazon OpenSearch Service unterstützt jetzt Elasticsearch Version 7.4. Weitere Informationen finden Sie unter unterstützte Versionen.	12. März 2020
k-NN	Amazon OpenSearch Service bietet Unterstützung für die Suche nach k-Nearest Neighbor (k-NN). k-NN benötigt die Servicesoftware R20200302 oder höher.	3. März 2020
Indexstatusmanagement	Amazon OpenSearch Service fügt Index State Management (ISM) hinzu, mit dem Sie Routineaufgaben automatisieren können, z. B. das Löschen von Indizes, wenn sie ein bestimmtes Alter erreicht haben. Diese Funktion erfordert Service-Software R20200302 oder neuer.	3. März 2020

Support für Elasticsearch 5.6.16	Amazon OpenSearch Service unterstützt jetzt die neueste Patch-Version für Version 5.6, die Bugfixes hinzufügt und die Sicherheit verbessert. Amazon ES aktualisiert vorhandene 5.6-Domains automatisch auf diese Version. Beachten Sie, dass die Versionsnummer dieser Elasticsearch-Version fälschlicherweise als 5.6.17 angegeben wird..	2. März 2020
Differenzierte Zugriffskontrolle	Amazon OpenSearch Service unterstützt jetzt eine differenz ierte Zugriffskontrolle, die Sicherheit auf Index-, Dokument- und Feldebene , Kibana-Mehrmandant enfähigkeit und optionale HTTP-Basisauthentifizierung für Ihren Cluster bietet.	11. Februar 2020
UltraWarm Speicher (Vorschau)	Amazon OpenSearch Service fügt UltraWarm eine neue Warm-Speicherstufe hinzu, die Amazon S3 und eine ausgeklügelte Caching-Lösung zur Leistungsverbesserung verwendet. Für Indizes, in die Sie nicht aktiv schreiben und die Sie seltener abfragen, bietet UltraWarm Speicher deutlich niedrigere Kosten pro GiB.	3. Dezember 2019

Verschlüsselungsfunktionen für Regionen in China	Verschlüsselung ruhender Daten und node-to-node Verschlüsselung sind jetzt in den Regionen `cn-north-1` China (Peking) und `cn-northwest-1` China (Ningxia) verfügbar.	20. November 2019
Erzwingung von HTTPS	Sie können jetzt erzwingen, dass der gesamte Datenverkehr zu Ihren Amazon ES-Domains über HTTPS eingeht. Aktivieren Sie beim Konfigurieren Ihrer Domain das Kontrollkästchen Require HTTPS (Erzwingung von HTTPS). Diese Funktion erfordert Service-Software R20190808 oder neuer.	3. Oktober 2019
Support für Elasticsearch 7.1 und 6.8	Amazon OpenSearch Service unterstützt jetzt Elasticsearch in den Versionen 7.1 und 6.8. Weitere Informationen finden Sie unter unterstützte Versionen.	13. August 2019
Stündliche Snapshots	Statt täglicher Snapshots erstellt Amazon OpenSearch Service jetzt stündlich Schnappschüsse von Domains, auf denen Elasticsearch 5.3 und höher ausgeführt wird, sodass Sie häufiger Backups haben, aus denen Sie Ihre Daten wiederherstellen können.	8. Juli 2019

Support für Elasticsearch 6.7	Amazon OpenSearch Service unterstützt jetzt Elasticsearch Version 6.7. Weitere Informationen finden Sie unter unterstützte Versionen.	29. Mai 2019
SQL-Unterstützung	Mit Amazon OpenSearch Service können Sie Ihre Daten jetzt mit SQL abfragen. SQL-Unterstützung erfordert Service-Software R20190418 oder neuer.	15. Mai 2019
5-Serie-Instance-Typen	Amazon OpenSearch Service unterstützt jetzt die Instance-Typen M5, C5 und R5. Im Vergleich zu Instance-Typen der vorigen Generation bieten diese neuen Typen eine bessere Leistung zu niedrigeren Kosten. Weitere Informationen finden Sie unter Limits.	24. April 2019
Support für Elasticsearch 6.5	Amazon OpenSearch Service unterstützt jetzt Elasticsearch Version 6.5.	8. April 2019
Warnfunktion	Alerting for Amazon OpenSearch Service benachrichtigt Sie, wenn Daten aus einem oder mehreren Amazon ES-Indizes bestimmte Bedingungen erfüllen. Die Warnfunktion erfordert Service-Software R20190221 oder neuer.	25. März 2019

Support für drei Availability Zones	Amazon OpenSearch Service unterstützt jetzt drei Availability Zones in vielen Regionen. Diese Version enthält auch eine optimierte Konsolenumgebung. Dieses Multi-AZ erfordert Service-Software R20181023 oder neuer.	7. Februar 2019
Support für Elasticsearch 6.4	Amazon OpenSearch Service unterstützt jetzt Elasticsearch Version 6.4.	23. Januar 2019
200-Knoten-Cluster	Mit Amazon ES können Sie nun Cluster mit bis zu 200 Datenknoten für insgesamt 3 PB Speicher erstellen.	22. Januar 2019
Service-Software-Updates	Mit Amazon ES können Sie die Service-Software für Ihre Domain jetzt manuell aktualisieren, um neue Funktionen schneller zu nutzen oder um ein Update zu einem Zeitpunkt mit geringem Datenverkehr durchzuführen. Weitere Informationen hierzu finden Sie unter .	20. November 2018
Neue Metriken CloudWatch	Amazon ES bietet jetzt Metriken auf Knotenebene und neue Registerkarten für Cluster-Zustand und Instance-Zustand in der Amazon ES-Konsole.	20. November 2018

Support für China (Peking)	Amazon OpenSearch Service ist jetzt in der Region cn-north-1 verfügbar, wo es die Instance-Typen M4, C4 und R4 unterstützt.	17. Oktober 2018
Keine Verschlüsselung ode-to-node	Amazon OpenSearch Service unterstützt jetzt node-to-node Verschlüsselung, wodurch Ihre Daten verschlüsselt bleiben, während Amazon ES sie in Ihrem Cluster verteilt.	18. September 2018
In-Situ-Versions-Upgrades	Amazon OpenSearch Service unterstützt jetzt direkte Versionsupgrades.	14. August 2018
Support für Elasticsearch 6.3 und 5.6	Amazon OpenSearch Service unterstützt jetzt Elasticsearch in den Versionen 6.3 und 5.6.	14. August 2018
Fehlerprotokolle	Mit Amazon ES können Sie jetzt Elasticsearch-Fehlerprotokolle auf Amazon CloudWatch veröffentlichen.	31. Juli 2018
Reserved Instances in China (Ningxia)	Amazon ES unterstützt jetzt Reserved Instances in der Region China (Ningxia).	29. Mai 2018
Reserved Instances	Amazon ES bietet jetzt Unterstützung für Reserved Instances.	7. Mai 2018

Frühere Aktualisierungen

In der folgenden Tabelle werden die wichtigen Änderungen an Amazon ES vor Mai 2018 beschrieben.

Änderung	Beschreibung	Datum
Amazon Cognito-Authentifizierung für Kibana	Amazon ES bietet nun Schutz für die Anmeldeseite für Kibana. Weitere Informationen hierzu finden Sie unter the section called “Amazon Cognito Cognito-Authentifizierung für Dashboards OpenSearch ”.	2. April 2018
Support für Elasticsearch 6.2	Amazon OpenSearch Service unterstützt jetzt Elasticsearch Version 6.2.	14. März 2018
Koreanisches Analyse-Plug-in	Amazon ES unterstützt nun eine speicheroptimierte Version von Seunjeon, dem koreanischen Analyse-Plug-in.	13. März 2018
Sofortige Updates der Zugriffskontrolle	Änderungen an den Zugriffskontrollrichtlinien auf Amazon ES-Domains werden nun unverzüglich übernommen.	7. März 2018
Petabyte-Größe	Amazon ES unterstützt jetzt I3-Instance-Typen und einen Gesamt-Domain-Speicher von bis zu 1,5 PB. Weitere Informationen hierzu finden Sie unter the section called “Petabyte-Größe”.	19. Dezember 2017
Verschlüsselung gespeicherter Daten	Amazon ES unterstützt nun die Verschlüsselung von Data-at-Rest. Weitere Informationen hierzu finden Sie unter the section called “Verschlüsselung im Ruhezustand”.	7. Dezember 2017
Support für Elasticsearch 6.0	Amazon ES unterstützt jetzt Elasticsearch Version 6.0. Überlegungen und Anweisungen für Migrationen finden Sie unter the section called “Aktualisieren von Domains”.	6. Dezember 2017
VPC-Unterstützung	Amazon ES ermöglicht jetzt das Launchen von Domains in einer Amazon Virtual Private Cloud. Die VPC-Unterstützung bietet zusätzliche Sicherheit und vereinfacht die Kommunikation zwischen Amazon ES und anderen	17. Oktober 2017

Änderung	Beschreibung	Datum
	Services in einer VPC. Weitere Informationen hierzu finden Sie unter the section called “VPC-Unterstützung”.	
Veröffentlichen von Slow-Protokollen	Amazon ES unterstützt jetzt die Veröffentlichung von langsamen Protokollen in CloudWatch Logs. Weitere Informationen hierzu finden Sie unter the section called “Überwachen von Protokollen”.	16. Oktober 2017
Support für Elasticsearch 5.5	Amazon ES unterstützt jetzt Elasticsearch Version 5.5. Sie können jetzt automatische Snapshots wiederherstellen, ohne mit AWS Support Kontakt aufzunehmen und Skripts mithilfe der `_scripts`-API speichern.	7. September 2017
Support für Elasticsearch 5.3	Amazon ES unterstützt jetzt Elasticsearch Version 5.3.	1. Juni 2017
Mehr Instances und EBS-Kapazität pro Cluster	Amazon ES bietet jetzt Unterstützung für bis zu 100 Knoten und 150 TB EBS-Kapazität pro Cluster.	5. April 2017
Unterstützung für Kanada (Zentral) und EU (London)	Amazon ES bietet Unterstützung für die folgenden Regionen: Kanada (Zentral), ca-central-1, und EU (London), eu-west-2.	20. März 2017
Mehr Instances und größere EBS-Volumes	Amazon ES bietet Unterstützung für mehr Instances und größere EBS-Volumes.	21. Februar 2017
Support für Elasticsearch 5.1	Amazon ES unterstützt jetzt Elasticsearch Version 5.1.	30. Januar 2017
Unterstützung für das Phonetic Analysis Plug-in	Amazon ES bietet nun Integration in das Phonetic Analysis-Plug-in, das das Ausführen von "tonähnlichen" Abfragen für Ihre Daten ermöglicht.	22. Dezember 2016

Änderung	Beschreibung	Datum
Unterstützung für USA Ost (Ohio)	Amazon ES bietet Unterstützung für die folgende Region: USA Ost (Ohio), us-east-2.	17. Oktober 2016
Neue Leistungs metrik	Amazon ES verfügt über eine neue Leistungsmetrik, `ClusterUsedSpace` .	29. Juli 2016
Support für Elasticsearch 2.3	Amazon ES unterstützt jetzt Elasticsearch Version 2.3.	27. Juli 2016
Unterstützung für Asien-Pazifik (Mumbai)	Amazon ES bietet Unterstützung für die folgenden Regionen: Asien-Pazifik (Mumbai), ap-south-1.	27. Juni 2016
Mehr Instances pro Cluster	In Amazon ES wurde die maximale Anzahl von Instances (Anzahl der Instances) pro Cluster von 10 auf 20 erhöht.	18. Mai 2016
Unterstützung für Asien-Pazifik (Seoul)	Amazon ES bietet Unterstützung für die folgenden Regionen: Asien-Pazifik (Seoul), ap-northeast-2.	28. Januar 2016
Amazon ES	Erstversion.	1. Oktober 2015

AWS-Glossar

Die neueste AWS-Terminologie finden Sie im AWS-Glossar in der AWS-Glossar-Referenz.

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.