aws

Benutzerhandbuch

Migration-Hub-Strategieempfehlungen

Migration-Hub-Strategieempfehlungen: Benutzerhandbuch

Table of Contents

Was sind Strategieempfehlungen für den Migration Hub?

Migration Hub Strategy Recommendations unterstützt Sie bei der Planung von Migrations- und Modernisierungsinitiativen, indem es Empfehlungen für Migrations- und Modernisierungsstrategien für tragfähige Transformationspfade für Ihre Anwendungen bietet.

Strategy Recommendations kann Ihr Serverinventar, Ihre Laufzeitumgebung und Anwendungsbinärdateien für Microsoft IIS- und Java Tomcat- und Jboss-Anwendungen analysieren, um Anti-Pattern-Berichte zu erstellen. Darüber hinaus können Sie Ihren Quellcode so konfigurieren, dass Strategy Recommendations den Quellcode und die Datenbankanalyse all Ihrer Anwendungen durchführen kann. Strategy Recommendations vergleicht diese Analyse mit Ihren Geschäftszielen und den Transformationspräferenzen der Anwendungen und Datenbanken, die Sie uns zur Verfügung gestellt haben, und empfiehlt:

- Die effektivste Migrationsstrategie für jede Ihrer Anwendungen.
- Tools oder Services für Migration und Modernisierung, die Sie verwenden können.
- Anwendungsinkompatibilitäten und Anti-Pattern-Probleme, die für eine bestimmte Option behoben werden müssen.

Strategy Recommendations von Migration Hub empfiehlt Migrations- und Modernisierungsstrategien für Rehosting, Replatforming und Refactoring mit den zugehörigen Bereitstellungszielen, Tools und Programmen. Informationen zu Rehosting, Replatforming und Refactoring finden Sie unter Migrationsbedingungen — 7 Rs im Glossar Prescriptive Guidance. AWS

In den Strategieempfehlungen werden möglicherweise einfache Optionen empfohlen, z. B. ein Rehosting auf Amazon Elastic Compute Cloud (Amazon EC2) mithilfe des AWS Application Migration Service (AWSMGN). Optimiertere Empfehlungen könnten die Umstellung auf Container mithilfe von AWS App2Container oder die Umgestaltung auf Open-Source-Technologien wie .NET Core und PostgreSQL beinhalten.

Sind Sie zum ersten Mal Kunde von Strategy Recommendations?

Wenn Sie Strategy Recommendations zum ersten Mal verwenden, empfehlen wir Ihnen, zunächst die folgenden Abschnitte zu lesen:

- Überblick über die Strategieempfehlungen

- Erstellung von Strategieempfehlungen
- Erste Schritte mit Strategieempfehlungen

Überblick über die Strategieempfehlungen

Sie können die Bewertung für Ihr Server- und Anwendungsportfolio starten, indem Sie die Strategieempfehlungen für Migration Hub von der AWS Migration Hub Konsole aus verwenden. Sie verwenden die Konsole, um eine Bewertung einzurichten und durchzuführen. Nach der Bewertung können Sie in der Konsole die Bewertungsdaten für jeden Server und jede Anwendung sowie das empfohlene Transformationstool anzeigen.

Um Empfehlungen zum Refactoring und eine Liste der Inkompatibilitäten zu erhalten, können Sie Strategy Recommendations verwenden, um den Quellcode und die Datenbanken Ihrer Anwendung zu bewerten.

Sie können die Empfehlungsdaten auch in einer Microsoft Excel-Datei herunterladen.

Zugehörige Services

- AWS Migration Hub— Sie verwenden die AWS Migration Hub Konsole, um auf die Migration Hub Strategy Recommendations-Konsole zuzugreifen. Außerdem werden Informationen zu den Servern angezeigt, von denen Sie Daten sammeln.
- AWS Application Discovery Service— Sie verwenden den Application Discovery Service, um Daten über Ihre Server und Anwendungen in der AWS Migration Hub Konsole zu sammeln, bevor Sie Strategy Recommendations verwenden.
- AWSAnwendungsmigrationsdienst — Der AWS Anwendungsmigrationsdienst ist der primäre Migrationsdienst, der für lift-and-shift Migrationen zu empfohlen wird. AWS
- AWS Database Migration Service— AWS Database Migration Service ist ein Webservice, mit dem Sie Daten aus Ihrer Datenbank, die sich vor Ort, auf einer Amazon Relational Database Service (Amazon RDS) -DB-Instance oder in einer Datenbank auf einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance befindet, in eine Datenbank auf einem Service migrieren können. AWS
- AWSApp2Container — AWS App2Container (A2C) ist ein Befehlszeilentool zur Modernisierung von.NET- und Java-Anwendungen in containerisierte Anwendungen.
- Portierungsassistent für .NET — Wird für die Analyse des .NET-Quellcodes verwendet. Der Portierungsassistent für .NET ist ein Kompatibilitätsscanner, der den manuellen Aufwand

reduziert, der für die Portierung Microsoft Microsoft.NET Framework-Anwendungen auf .NET Core erforderlich ist. Der Portierungsassistent für .NET bewertet den Quellcode der .NET-Anwendung und identifiziert inkompatible APIs und Pakete von Drittanbietern.

- Migrationsprogramm zum Ende des Support für Windows Server — Das End-of-Support-Migrationsprogramm (EMP) für Windows Server umfasst Tools, mit denen Sie Ihre älteren Anwendungen von Windows Server 2003, 2008 und 2008 R2 auf neuere, unterstützte Versionen migrieren können, ohne dass ein Refactoring erforderlich ist. AWS
- AWSSchema Conversion Tool — Sie können das AWS Schema Conversion Tool (AWS SCT) verwenden, um Ihr vorhandenes Datenbankschema von einer Datenbank-Engine in eine andere zu konvertieren.
- Windows Web Application Migration Assistant — Der Windows Web Application Migration Assistant für AWS Elastic Beanstalk ist ein interaktives PowerShell Hilfsprogramm, das ASP.NET- und ASP.NET Core-Anwendungen von lokalen IIS-Windows-Servern zu Elastic Beanstalk migriert.
- Babelfish for Aurora PostgreSQL — Babelfish for Aurora PostgreSQL ist eine neue Funktion für die Amazon Aurora PostgreSQL-kompatible Edition, die es Aurora ermöglicht, Befehle von Anwendungen zu verstehen, die für den Microsoft SQL-Server geschrieben wurden.

Erstellung von Strategieempfehlungen

Bevor Sie die Strategieempfehlungen von Migration Hub zum ersten Mal verwenden, führen Sie die folgenden Aufgaben aus:

Themen

Melden Sie sich 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 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.

Strategie, Empfehlungen, Benutzer und Rollen

Wir empfehlen, dass Sie zwei Rollen für Strategy Recommendations erstellen:

- Um auf die Konsole zuzugreifen, erstellen Sie eine Rolle, der `AWSMigrationHubFullAccess` sowohl die als auch die `AWSMigrationHubStrategyConsoleFullAccess` verwalteten Richtlinien zugeordnet sind.
- Um auf den Anwendungsdatensammler von Strategy Recommendations zuzugreifen, erstellen Sie eine Rolle mit der angehängten `AWSMigrationHubStrategyCollector` verwalteten Richtlinie.

Von IAM verwaltete Richtlinien definieren die Zugriffsebene der Benutzer auf einen Dienst. Die AWS Migration Hub `AWSMigrationHubFullAccess` verwaltete Richtlinie gewährt Zugriff auf die Migration Hub Hub-Konsole. Weitere Informationen finden Sie unter Rollen und Richtlinien für Migration Hub. Informationen zu den `AWSMigrationHubStrategyConsoleFullAccess` und `AWSMigrationHubStrategyCollector` verwalteten Richtlinien finden Sie unterAWS verwaltete Richtlinien für Strategieempfehlungen für den Migration Hub.

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.

Erste Schritte mit Strategieempfehlungen

In diesem Abschnitt wird beschrieben, wie Sie mit den Strategieempfehlungen von Migration Hub beginnen können.

Themen

Voraussetzungen für Strategieempfehlungen

Im Folgenden sind die Voraussetzungen für die Verwendung von Migration Hub Strategy Recommendations aufgeführt.

- Sie müssen über ein oder mehrere AWS Konten verfügen, und Benutzer müssen für diese Konten eingerichtet sein. Weitere Informationen finden Sie unter Erstellung von Strategieempfehlungen.
- Der Anwendungsdatensammlerclient von Strategy Recommendations muss in der Lage sein, Daten remote von Servern zu sammeln. Dazu müssen Sie eine Reihe von Anmeldeinformationen verwenden, die für alle Ihre Windows-Server funktionieren, und eine Reihe von Anmeldeinformationen, die für alle Ihre Linux-Server funktionieren. Die Anmeldeinformationen müssen über Berechtigungen zum Erstellen und Löschen von Verzeichnissen auf Ihren Servern verfügen.
- Die in vCenter bereitgestellte Version des Collectors unterstützt VMware vCenter Server V6.0, V6.5, 6.7 oder 7.0.

  Sie können den Collector auch in einer Amazon EC2 EC2-Instance mithilfe des Collector-AMI bereitstellen.
- Prüfen Sie, ob Ihre Betriebssystemumgebung unterstützt wird:
  - Linux

    - Amazon Linux 2012.03, 2015.03
    - Amazon Linux 2 (Update vom 25. September 2018 und höher)
    - Ubuntu 12.04, 14.04, 16.04, 18.04, 20.04
    - RedHat Enterprise Linux 5.11, 6.10, 7.3, 7.7, 8.1
    - CentOS 5.11, 6.9, 7.3
    - SUSE 11 SP4, 12 SP5
  - Windows
    - Windows Server 2008 R1 SP2, 2008 R2 SP1
    - Windows Server 2012 R1, 2012 R2
    - Windows Server 2016
    - Windows Server 2019
- Für die Quellcode-Analyse müssen Ihr Repository GitHub und Ihr GitHub Enterprise-Repository über ein persönliches Zugriffstoken mit dem Repo-Bereich verfügen, das für den Collector-Client von Strategy Recommendations gemeinsam genutzt werden kann. Weitere Informationen zum Erstellen eines persönlichen Zugriffstokens im Repo-Bereich finden Sie in der Dokumentation unter Erstellen eines persönlichen Zugriffstokens. GitHub

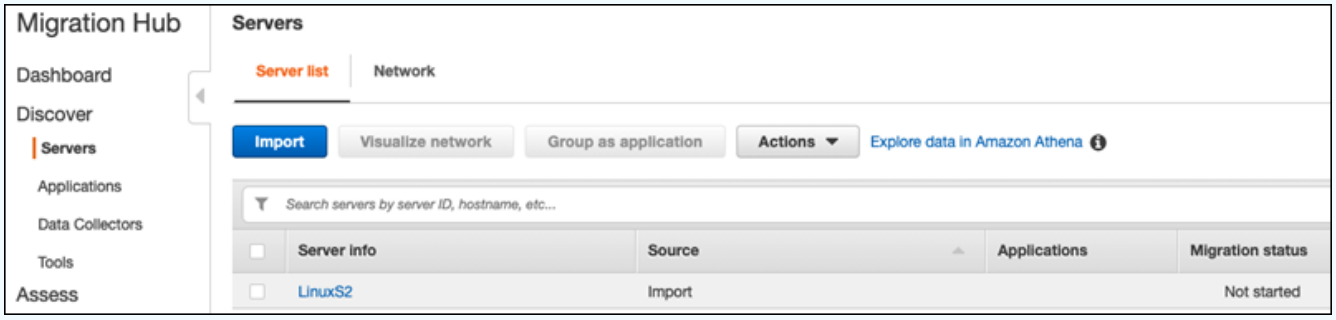
  Um .NET-Repositorys für Empfehlungen von Porting Assistant for .NET zu analysieren, müssen Sie einen Windows-Computer bereitstellen, auf dem das Portierungsbewertungstool von Porting Assistant for .NET installiert ist. Weitere Informationen finden Sie unter Erste Schritte mit Porting Assistant for .NET im Porting Assistant for .NET-Benutzerhandbuch.
- Um Strategieempfehlungen für die Datenbankanalyse zu aktivieren, müssen Sie Anmeldeinformationen unter eingeben AWS Secrets Manager. Weitere Informationen finden Sie unter Datenbankanalyse für Strategy Recommendations.
- Sie müssen die AWS Migration Hub Konsole verwenden AWS Application Discovery Service , um Daten über Ihre Server und Anwendungen zu sammeln, bevor Sie Strategy Recommendations verwenden können. Sie können eine der folgenden Methoden verwenden, um die Daten zu sammeln.
  - Migration Hub-Import — Mit dem Migration Hub Hub-Import können Sie Informationen über Ihre lokalen Server und Anwendungen in Migration Hub importieren. Weitere Informationen finden Sie unter Migration Hub Hub-Import im Application Discovery Service Service-Benutzerhandbuch.
  - AWS Application Discovery Service Agentless Collector — Der Agentless Collector ist eine VMware-Appliance, die Informationen über virtuelle Maschinen (VMs) von VMware sammelt.

Weitere Informationen finden Sie unter Agentless Collector im Application Discovery Service Service-Benutzerhandbuch.

- AWS Application Discovery Agent — Der Discovery Agent ist eine AWS Software, die Sie auf Ihren lokalen Servern und VMs installieren, um Systeminformationen und Details der Netzwerkverbindungen zwischen Systemen zu erfassen. Weitere Informationen finden Sie unter AWS Application Discovery Agent im Application Discovery Service Service-Benutzerhandbuch.

- Datensammler für Strategieempfehlungen — Wenn Ihre Server in VMware vCenter gehostet werden und Sie Zugriff gewähren, kann Strategy Recommendations Ihr Serverinventar automatisch abrufen. Die Strategy Recommendations-Konsole verwendet die gesammelten Informationen, um Sie bei der Bewertung zu unterstützen.

> **Note**
>
> Um zu überprüfen, ob der Migration Hub Hub-Import erfolgreich abgeschlossen wurde, wählen Sie im Navigationsbereich der Migration Hub Hub-Konsole unter Discover die Option Servers aus. Alle importierten Server sollten aufgelistet werden.



Schritt 1: Laden Sie den Strategy Recommendations Collector herunter

Der Anwendungsdatensammler von Migration Hub Strategy Recommendations ist eine virtuelle Appliance, die Sie in Ihrer lokalen VMware-Umgebung installieren können. Der Anwendungsdatensammler von Strategy Recommendations ist auch als Amazon Machine Image (AMI) verfügbar. Wenn Sie die AMI-Version des Collectors zur Bewertung von AWS Anwendungen oder aus einem anderen Grund verwenden möchten, müssen Sie den Collector nicht herunterladen. Sie können diesen Abschnitt überspringen und zu wechselnStellen Sie den Strategy Recommendations-Collector in einer Amazon EC2 EC2-Instance bereit.

In diesem Abschnitt wird beschrieben, wie Sie die Collector Open Virtualization Archive (OVA) -Datei herunterladen, mit der Sie den Collector als virtuelle Maschine (VM) in Ihrer VMware-Umgebung bereitstellen.

Um die Collector-OVA-Datei herunterzuladen

1. Melden Sie sich mit dem AWS Konto, das Sie erstellt habenErstellung von Strategieempfehlungen, bei der Migration Hub Hub-Konsole unter https://console.aws.amazon.com/migrationhub/ an AWS Management Console und öffnen Sie sie.
2. Wählen Sie im Navigationsbereich der Migration Hub Hub-Konsole Strategie aus.
3. Wählen Sie auf der Seite mit den Empfehlungen zur Migration Hub-Strategie die Option Datensammler herunterladen aus.
4. Optional können Sie die Importvorlage herunterladen auswählen, wenn Sie Anwendungsdaten importieren möchten. Weitere Informationen zum Importieren von Daten finden Sie unterDaten in Strategy Recommendations importieren.
5. Klicken Sie auf Empfehlungen abrufen und wählen Sie Zustimmen aus, damit Migration Hub eine serviceverknüpfte Rolle (SLR) in Ihrem Konto erstellen kann. Wenn Sie Strategieempfehlungen zum ersten Mal einrichten, müssen Sie die SLR erstellen. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für Strategieempfehlungen.

Schritt 2: Stellen Sie den Strategy Recommendations Collector bereit

In diesem Abschnitt wird beschrieben, wie Sie den Anwendungsdatensammler für Strategy Recommendations bereitstellen. Ein Anwendungsdatensammelpunkt ist ein Datensammler ohne Agenten, der laufende Anwendungen auf Ihren Servern identifiziert, Quellcodeanalysen durchführt und Ihre Datenbanken analysiert.

Es gibt zwei Möglichkeiten, den Collector bereitzustellen:

- Stellen Sie es als virtuelle Maschine (VM) auf Ihrem VMware vCenter Server bereit. Weitere Informationen finden Sie unter Stellen Sie den Strategy Recommendations Collector in vCenter bereit.
- Wenn Sie AWS Anwendungen haben, die Sie bewerten möchten, können Sie den Strategy Recommendations Collector Amazon Machine Image (AMI) verwenden. Weitere Informationen

finden Sie unter Stellen Sie den Strategy Recommendations-Collector in einer Amazon EC2 EC2-Instance bereit.

Stellen Sie den Strategy Recommendations Collector in vCenter bereit

Der Anwendungsdatensammler von Migration Hub Strategy Recommendations ist eine virtuelle Appliance, die Sie in Ihrer lokalen VMware-Umgebung installieren können. In diesem Abschnitt wird beschrieben, wie Sie die Collector-Datei Open Virtualization Archive (OVA) als virtuelle Maschine (VM) in Ihrer VMware-Umgebung bereitstellen.

Das folgende Verfahren beschreibt, wie Sie den Strategy Recommendations Collector in Ihrer VMware vCenter Server-Umgebung bereitstellen.

So stellen Sie den Collector in vCenter bereit

1. Melden Sie sich bei vCenter als VMware-Administrator an.
2. Stellen Sie die OVA-Datei bereit, die Sie in Schritt 1 heruntergeladen haben. Die OVA-Datei enthält den Collector und eine CLI, die für den Zugriff auf die Strategy Recommendations API verwendet werden können.

   Sie können die OVA-Datei auch über den folgenden Link herunterladen:

   https://application-data-collector-release.s3.us-west-2.amazonaws.com/ova/latest/AWSMHubApplicationDataCollector.ova

Wir empfehlen die folgenden Spezifikationen für die VM.

Strategieempfehlungen, Sammler, VM-Spezifikationen

- RAM — mindestens 8 GB
- CPUs — mindestens 4

> **Note**
>
> Um sicherzustellen, dass Sie die neueste Version des Collectors mit allen neuen Funktionen und Bugfixes verwenden, aktualisieren Sie den Collector, nachdem Sie die Collector-

OVA-Datei bereitgestellt haben. Anweisungen zum Upgrade finden Sie unterDen Strategy Recommendations Collector aktualisieren.

Stellen Sie den Strategy Recommendations-Collector in einer Amazon EC2 EC2-Instance bereit

Wenn Sie AWS Anwendungen haben, die Sie bewerten möchten, können Sie den Anwendungsdatensammler Amazon Machine Image (AMI) für Strategy Recommendations verwenden.

Das folgende Verfahren beschreibt, wie Sie eine Amazon EC2 EC2-Instance vom Collector-AMI aus starten.

So stellen Sie die Collector-Amazon-EC2-Instance bereit

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Auf der Navigationsleiste oben im Bildschirm wird die aktuelle -Region angezeigt (beispielsweise USA Ost (Ohio)). Wählen Sie aus den Regionen, die Strategy Recommendations verwendet, eine Region aus, die Ihren Bedürfnissen entspricht. Eine Liste dieser Regionen finden Sie unter Strategy Recommendations Endpoints in der Allgemeine AWS-Referenz.
3. Wählen Sie im Navigationsbereich unter Images die Option AMIs aus.
4. Wählen Sie in der Drop-down-Liste In meinem Besitz die Option Öffentliche Bilder aus.
5. Wählen Sie die Suchleiste und wählen Sie AMI-Name aus dem Menü aus.
6. Geben Sie den Namen AWSMHubApplicationDataCollector ein.
7. Um sicherzustellen, dass das AMI aus einer sicheren Quelle stammt, stellen Sie sicher, dass der Besitzer des Kontos 703163444405 ist.
8. Um eine Instance von diesem AMI aus zu starten, wählen Sie sie aus und klicken Sie dann auf Launch. Weitere Informationen zum Starten einer Instance mithilfe der Konsole finden Sie unter Launching your Instance from an AMI im Amazon EC2 EC2-Benutzerhandbuch.

   Wir empfehlen die folgenden Spezifikationen für die Amazon EC2 EC2-Instance.

   Strategy Recommendations Collector Amazon EC2 EC2-Instance-Spezifikationen

   - RAM — Mindestens 8 GB
   - CPUs — mindestens 4

Das Strategy Recommendations AMI umfasst den Collector und eine CLI, die für den Zugriff auf die Strategy Recommendations API verwendet werden können.

> **Note**
>
> Um sicherzustellen, dass Sie die neueste Version des Collectors mit allen neuen Funktionen und Bugfixes verwenden, aktualisieren Sie den Collector, nachdem Sie den Strategy Recommendations Collector als Amazon EC2 EC2-Instance bereitgestellt haben. Anweisungen zum Upgrade finden Sie unterDen Strategy Recommendations Collector aktualisieren.

Schritt 3: Melden Sie sich beim Strategy Recommendations Collector an

In diesem Abschnitt wird beschrieben, wie Sie sich beim bereitgestellten Anwendungsdatensammler für Migration Hub Strategy Recommendations anmelden. Wie Sie sich beim Collector anmelden, hängt davon ab, wie Sie ihn bereitgestellt haben.

- Melden Sie sich bei dem Collector an, der in der vCenter-basierten Umgebung bereitgestellt wird
- Melden Sie sich bei dem Collector an, der als Amazon EC2 EC2-Instance bereitgestellt wird

Melden Sie sich bei dem Collector an, der in der vCenter-basierten Umgebung bereitgestellt wird

So melden Sie sich beim Strategy Recommendations Collector an, der in der vCenter-basierten Umgebung bereitgestellt wird

1. Verwenden Sie den folgenden Befehl, um über einen SSH-Client eine Verbindung zum Collector herzustellen.

   ```
   ssh ec2-user@CollectorIPAddress
   ```

2. Wenn Sie zur Eingabe eines Kennworts aufgefordert werden, geben Sie das Standardkennwort aq1 @WSde3 ein. Sie müssen das Passwort ändern, wenn Sie sich zum ersten Mal anmelden.

Melden Sie sich bei dem Collector an, der als Amazon EC2 EC2-Instance bereitgestellt wird

Um sich beim Strategy Recommendations Collector anzumelden, der als Amazon EC2 EC2-Instance bereitgestellt wird

- Verwenden Sie den folgenden Befehl, um über einen SSH-Client eine Verbindung zum Collector herzustellen.

  ```
  ssh -i "Keyname.pem" ec2-user@CollectorIPAddress
  ```

  Keyname.pem ist der private Schlüssel, der generiert wurde, als Sie die Amazon EC2 EC2-Instance vom Collector-AMI aus gestartet haben.

Schritt 4: Den Collector für Strategieempfehlungen einrichten

In diesem Abschnitt wird beschrieben, wie Sie die Befehlszeile verwenden`collector setup`Befehle zur Konfiguration des Anwendungsdatensammlers für Migration Hub Strategy Recommendations. Diese Konfigurationen werden lokal gespeichert.

Bevor Sie verwenden können`collector setup`Bei Befehlen müssen Sie wie folgt eine Bash-Shell-Sitzung im Collector-Docker-Container erstellen`docker exec`Befehl.

```
docker exec -it application-data-collector bash
```

Der`collector setup`Der Befehl führt alle der folgenden Befehle nacheinander aus, Sie können sie jedoch auch einzeln ausführen:

- `collector setup --aws-configurations`— EinrichtenAWSKonfigurationen.
- `collector setup --vcenter-configurations`— Richten Sie vCenter-Konfigurationen ein.

> **Note**
>
> Die Einrichtung der vCenter-Konfiguration ist nur verfügbar, wenn der Collector auf vCenter gehostet wird. Sie können die Einrichtung der vCenter-Konfiguration jedoch mit dem folgenden Befehl erzwingen`collector setup --vcenter-configurations`.

- `collector setup --remote-server-configurations`— Richten Sie Remote-Serverkonfigurationen ein.
- `collector setup --version-control-configurations`— Richten Sie Konfigurationen für die Versionskontrolle ein.

Um alle Collector-Konfigurationen gleichzeitig einzurichten

1. Geben Sie den folgenden Befehl ein.

   ```
   collector setup
   ```

2. Geben Sie die Informationen für einAWSKonfigurationen wie beschrieben unterAufgestelltAWSKonfigurationen.
3. Geben Sie die Informationen für vCenter-Konfigurationen ein, wie unter beschriebenRichten Sie vCenter-Konfigurationen ein.
4. Geben Sie die Informationen für Remoteserverkonfigurationen ein, wie unter beschriebenRichten Sie Remoteserverkonfigurationen ein.
5. Geben Sie die Informationen für Versionskontrollkonfigurationen ein, wie unter beschriebenRichten Sie Konfigurationen für die Versionskontrolle ein.
6. Bereiten Sie Ihre Windows- und Linux-Server für die Erfassung von Collector-Daten vor, indem Sie die Anweisungen unterBereiten Sie Ihre Windows- und Linux-Remote-Server auf die Datenerfassung vor.

AufgestelltAWSKonfigurationen

Zum EinrichtenAWSKonfigurationen, bei Verwendung des`collector setup`Befehl oder`collector setup --aws-configurations`Befehl.

1. Geben Sie einYfür Ja zumHaben Sie IAM-Berechtigungen eingerichtet...Frage. Sie haben diese Berechtigungen eingerichtet, als Sie einen Benutzer für den Zugriff auf den Collector erstellt haben, indem Sie`AWSMigrationHubStrategyCollector`verwaltete Richtlinie gemäß den Schritten unterStrategie, Empfehlungen, Benutzer und Rollen.
2. Geben Sie Ihren Zugangsschlüssel und Ihren geheimen Schlüssel aus demAWSKonto, das den Benutzer hat, den Sie für den Zugriff auf den Collector erstellt haben. Gehen Sie dazu wie folgt vorStrategie, Empfehlungen, Benutzer und Rollen.

3. Geben Sie eine Region ein, zum Beispiel`us-west-2`. Wählen Sie aus den Regionen, die Strategy Recommendations verwendet, eine Region aus, die Ihren Bedürfnissen entspricht. Eine Liste dieser Regionen finden Sie unterEndpunkte der Strategie, Empfehlungenin derAllgemeine AWS-Referenz.
4. EingebenYfür Ja zumMetriken im Zusammenhang mit Collector auf den Migration Hub Strategy Service hochladen?Frage. Informationen zu Metriken helfenAWSbieten Ihnen angemessene Unterstützung.
5. Geben Sie einYfür Ja zumCollector-bezogene Logs auf den Migration Hub Strategy Service hochladen?Frage. Informationen aus Protokollen helfenAWSbieten Ihnen angemessene Unterstützung.

Das folgende Beispiel zeigt, was angezeigt wird, einschließlich Beispieleinträgen fürAWSKonfigurationen.

```
Have you setup IAM permissions in you AWS account as per the user guide? [Y/N]: Y
Choose one of the following options for providing user credentials:
1. Long term AWS credentials
2. Temporary AWS credentials
Enter your options [1-2]: 2
AWS session token:
AWS access key ID [None]:
AWS secret access Key [None]:
AWS region name [us-west-2]:
AWS configurations are saved successfully
Upload collector related metrics to migration hub strategy service? By default
 collector will upload metrics. [Y/N]: Y
Upload collector related logs to migration hub strategy service? By default collector
 will upload logs. [Y/N]: Y
Application data collector configurations are saved successfully
Start registering application data collector
Application data collector is registered successfully.
```

Richten Sie vCenter-Konfigurationen ein

Um vCenter-Konfigurationen einzurichten, verwenden Sie den`collector setup`Befehl oder`collector setup --vcenter-configurations`Befehl:

1. EingebenYfür Ja zumMöchten Sie sich mit VMware vCenter-Anmeldeinformationen authentifizierenFrage, ob Sie sich mit VMware vCenter-Anmeldeinformationen authentifizieren möchten.

   > **Note**
   >
   > Für die Authentifizierung mit VMware vCenter-Anmeldeinformationen müssen die VMware-Tools auf den Zielservern installiert sein.

   Geben Sie denHost-URL, bei der es sich entweder um die vCenter-IP-Adresse oder die URL handeln kann. Geben Sie dann denNutzernameundPasswortfür VMware vCenter.

2. Geben Sie einYfür Ja zumHaben Sie Windows-Computer, die von VMware vCenter verwaltet werdenFrage, ob Sie Windows-Server konfigurieren möchten.

   Geben Sie denNutzernameundPasswortfür Windows.

   > **Note**
   >
   > Wenn Ihr Windows Remote Server zu einer Active Directory-Domäne gehört, müssen Sie den Benutzernamen als eingeben*Domänenname**Nutzername*wenn Sie die CLI verwenden, um Remote-Serverkonfigurationen bereitzustellen. Wenn der Name Ihrer Domain beispielsweise exampledomain lautet und Ihr Benutzername Administrator ist, dann lautet der Benutzername, den Sie in die CLI eingebenBeispieldomäne\Administrator.

3. EingebenYfür Ja zumEinrichtung für Linux mit VMware vCenterFrage, ob Sie Linux-Server konfigurieren möchten.

   Geben Sie denNutzernameundPasswortfür Linux.

4. Geben Sie einYfür Ja zumMöchten Sie Anmeldeinformationen für Server außerhalb von vCenter mithilfe von NTLM für Windows einrichtenundSSH/Cert-basiert für LinuxFragen, wenn Sie Remoteserver-Anmeldeinformationen für Server außerhalb von vCenter einrichten möchten.

5. Für dieMöchten Sie dieselben Windows-Anmeldeinformationen verwenden, die Sie beim vCenter-Setup verwendet habenFrage, geben Sie einYfür ja, wenn die Anmeldeinformationen für die außerhalb von vCenter verwalteten Windows-Maschinen mit den Anmeldeinformationen

übereinstimmen, die bei der Konfiguration der Anmeldeinformationen für vCenter Windows-Maschinen angegeben wurden. Geben Sie andernfalls Folgendes einNfür nein.

Wenn du antwortestYfür ja, es werden die folgenden Fragen gestellt.

a. Geben Sie einYfür Ja zumSind Sie damit einverstanden, dass Collector bei der ersten Interaktion mit Windows-Servern Serverzertifikate in Ihrem Namen akzeptiert und lokal speichert?Frage.

b. Geben Sie ein1für dieGeben Sie Ihre Optionen einFrage, wenn Sie die SSH-Authentifizierung konfigurieren möchten.

   Wenn Sie sich für die SSH-Authentifizierung entscheiden, müssen Sie die generierten Schlüsselanmeldedaten auf Ihre Linux-Server kopieren. Weitere Informationen finden Sie unter Richten Sie die schlüsselbasierte Authentifizierung auf Linux-Servern ein.

Das folgende Beispiel zeigt, was angezeigt wird, einschließlich Beispieleinträgen für die VMware vCenter-Konfigurationen.

```
Your Linux remote server configurations are saved successfully.
collector setup –vcenter-configurations
Start setting up vCenter configurations for remote execution
Note: Authenticating using VMware vCenter credentials requires VMware tools to be
 installed on the target servers
Would you like to authenticate using VMware vCenter credentials? [Y/N]: y

NOTE: Your vSphere user must have Guest Operations privileges enabled.

Host Url for VMware vCenter: domain-name
Username for VMware vCenter: username
Password for VMware vCenter: password
Reenter password for VMware vCenter: password
Successfully stored vCenter credentials...
Do you have Windows machines managed by VMware vCenter? [Y/N]: y

NOTE: For the best experience, we recommend that you create a new Active Directory user
 in the Domain Admins group.

Username for Windows (Domain\User): username
Password for Windows: password
Reenter password for Windows: password
```

```
Successfully stored windows credentials...
You can verify your setup for vCenter windows machines is correct with "collector diag-
check"
Do you have Linux machines managed by VMWare vCenter? [Y/N]: y
Username for Linux: username
Password for Linux: password
Reenter password for Linux: password
Successfully stored linux credentials...
You can verify your setup for vCenter linux machines is correct with "collector diag-
check"
Would you like to setup credentials for servers not managed by vCenter using NTLM for
 windows and SSH/Cert based for Linux? [Y/N]: y
Setting up target server for remote execution:
Would you like to setup credentials for servers not managed by vCenter using NLTM for
 Windows [Y/N]: y
Would you like to use the same Windows credentials used during vCenter setup? [Y/N]: y
Are you okay with collector accepting and locally storing server certificates on your
 behalf during first interaction with windows servers? These certificates will be used
 by collector for secure communication with windows servers [Y/N]: y
Successfully stored windows server credentials...
Please note that all windows server certificates are stored in directory /opt/amazon/
application-data-collector/remote-auth/windows/certs

Please note the IP address of the collector and run the script specified in the user
 documentation on all the windows servers in your inventory
You can verify your setup for remote windows machines is correct with "collector diag-
check"
Would you like to setup credentials for servers not managed by vCenter using SSH/Cert
 based for Linux? [Y/N]: y
Choose one of the following options for remote authentication:
1. SSH based authentication
2. Certificate based authentication
Enter your options [1-2]: 1
Would you like to use the same Linux credentials used during vCenter setup? [Y/N]: y
Generating SSH key on this machine...
Successfully generated SSH key pair

SSH key pair path: /opt/amazon/application-data-collector/remote-auth/linux/keys/
id_rsa_assessment
Please add the public key "id_rsa_assessment.pub" to the "$HOME/.ssh/authorized_keys"
 file in your remote machines.
You can verify your setup for remote linux machines is correct with "collector diag-
check
```

Richten Sie Remoteserverkonfigurationen ein

Um Remoteserverkonfigurationen einzurichten, verwenden Sie den`collector setup`Befehl oder der`collector setup --remote-server-configurations`Befehl:

1. Geben Sie einYfür Ja zumMöchten Sie mithilfe von NLTM für Windows Anmeldeinformationen für Server einrichten, die nicht von vCenter verwaltet werdenFrage, ob Sie Windows-Server konfigurieren möchten.

   Geben Sie denNutzernameundPasswortfür WinRM.

   > **Note**
   >
   > Wenn Ihr Windows Remote Server zu einer Active Directory-Domäne gehört, müssen Sie den Benutzernamen als eingeben*Domänenname**Nutzername*wenn Sie die CLI verwenden, um Remote-Serverkonfigurationen bereitzustellen. Wenn der Name Ihrer Domain beispielsweise exampledomain lautet und Ihr Benutzername Administrator ist, dann lautet der Benutzername, den Sie in die CLI eingebenBeispieldomäne\Administrator.

   EingebenYfür Ja zumSind Sie damit einverstanden, dass Collector bei der ersten Interaktion mit Windows-Servern Serverzertifikate in Ihrem Namen akzeptiert und lokal speichert?Frage. Windows Server-Zertifikate werden im Verzeichnis gespeichert`/opt/amazon/application-data-collector/remote-auth/windows/certs`.

   Sie müssen die generierten Serveranmeldedaten auf Ihre Windows-Server kopieren. Weitere Informationen finden Sie unter Richten Sie die Remoteserverkonfiguration auf Windows-Servern ein.
2. Geben Sie einYfür Ja zumEinrichtung für Linux mit SSH oder CertFrage, ob Sie Linux-Server konfigurieren möchten.
3. Geben Sie ein1für dieGeben Sie Ihre Optionen einFrage, wenn Sie die schlüsselbasierte SSH-Authentifizierung konfigurieren möchten.

   Wenn Sie sich für die SSH-Authentifizierung entscheiden, müssen Sie die generierten Schlüsselanmeldedaten auf Ihre Linux-Server kopieren. Weitere Informationen finden Sie unter Richten Sie die schlüsselbasierte Authentifizierung auf Linux-Servern ein.

4. Geben Sie ein2für dieGeben Sie Ihre Optionen einFrage, wenn Sie die zertifikatsbasierte Authentifizierung konfigurieren möchten.

   Informationen zur Einrichtung der zertifikatsbasierten Authentifizierung finden Sie unterRichten Sie die zertifikatsbasierte Authentifizierung auf Linux-Servern ein.

Das folgende Beispiel zeigt, was angezeigt wurde, einschließlich Beispieleinträgen für die Remoteserverkonfigurationen.

```
Setting up target server for remote execution
Would you like to setup credentials for servers not managed by vCenter using NLTM for
 Windows [Y/N]: y

NOTE: For the best experience, we recommend that you create a new Active Directory user
 in the Domain Admins group.

Username for WinRM (Domain\User): username
Password for WinRM: password
Reenter password for WinRM: password
Are you okay with collector accepting and locally storing server certificates on your
 behalf during first interaction with windows servers? These certificates will be used
 by collector for secure communication with windows servers [Y/N]: Y
Successfully stored windows server credentials...
Please note that all windows server certificates are stored in directory /opt/amazon/
application-data-collector/remote-auth/windows/certs

Please note the IP address of the collector and run the script specified in the user
 documentation on all the windows servers in your inventory
Would you like to setup credentials for servers not managed by vCenter using SSH/Cert
 based for Linux? [Y/N]: Y
Choose one of the following options for remote authentication:
1. SSH based authentication
2. Certificate based authentication
Enter your options [1-2]: 1
User name for remote server: username
Generating SSH key on this machine...
SSH key pair path: /opt/amazon/application-data-collector/remote-auth/linux/keys/
id_rsa_assessment
Please add the public key "id_rsa_assessment.pub" to the "$HOME/.ssh/authorized_keys"
 file in your remote machines.
Your Linux remote server configurations are saved successfully.
```

Richten Sie Konfigurationen für die Versionskontrolle ein

Um Konfigurationen für die Versionskontrolle einzurichten, verwenden Sie`collector setup`Befehl oder der`collector setup --version-control-configurations`Befehl:

1. Geben Sie ein`Y`für Ja zumQuellcode-Analyse einrichten?Frage.
2. Geben Sie ein`1`für dieGeben Sie Ihre Optionen einFrage, ob Sie den Git-Serverendpunkt konfigurieren möchten.

   Geben Sie ein`github.com`für dieGIT-Serverendpunkt:.
3. Eingeben`2`für dieGeben Sie Ihre Optionen einFrage, wenn Sie eine konfigurieren möchten GitHubUnternehmensserver.

   Geben Sie den Unternehmensendpunkt ohne https://wie folgt ein:GIT-Serverendpunkt: *`git-enterprise-endpoint`*
4. Gib dein Git ein*`Nutzername`*und persönlicher Zugang*`Zeichen`*.
5. Eingeben`Y`für Ja zumHaben Sie irgendwelche Csharp-Repositorys, die auf einem Windows-Computer analysiert werden sollten?Frage, wenn Sie C#-Code analysieren möchten.

   > **Note**
   >
   > Um .NET-Repositorys anhand der Empfehlungen von Porting Assistant for .NET zu analysieren, müssen Sie einen Windows-Computer bereitstellen, auf dem das Portierungsbewertungstool Porting Assistant for .NET installiert ist. Weitere Informationen finden Sie unterErste Schritte mit Porting Assistant for .NETin derPorting Assistant for .NET-Benutzerhandbuch.
6. Für dieMöchten Sie vorhandene Windows-Anmeldeinformationen auf diesem Computer wiederverwenden?Frage. Geben Sie ein`Y`für ja, wenn der Windows-Computer für die C#-Quellcodeanalyse dieselben Anmeldeinformationen verwendet wie die Anmeldeinformationen, die zuvor im Rahmen der Einrichtung angegeben wurden`--remote-server-configurations`oder`--vcenter-configurations`.

   Eingeben`N`für nein, wenn Sie neue Anmeldeinformationen eingeben möchten.
7. Zu verwendenVMware vCenter Windows-MaschineAnmeldeinformationen, geben Sie ein`1`zumWählen Sie eine der folgenden Optionen für Windows-Anmeldeinformationen.
8. Geben Sie die IP-Adresse für den Windows-Computer ein.

Das folgende Beispiel zeigt, was angezeigt wird, einschließlich Beispieleinträgen für die Versionskontrollkonfigurationen.

```
Set up for source code analysis [Y/N]: y
Choose one of the following options for version control type:
1. GIT
2. GIT Enterprise
3. Azure DevOps - Git
Enter your options [1-3]: 3
Your server endpoint: dev.azure.com (http://dev.azure.com/)
Your DevOps Organization name: <Your organization name>
Personal access token [None]:
Your version control credentials are saved successfully.
Do you have any csharp repositories that should be analyzed on a windows machine? [Y/
N]: y
Would you like to reuse existing windows credentials on this machine? [Y/N]: y
Choose one of the following options for windows credentials:
1. VMWare vCenter Windows Machine
2. Standard Windows Machine
Enter your options [1-2]:
1
Windows machine IP Address: <Your windows machine IP address>
Using VMWare vCenter Windows Machine credentials
Successfully stored windows server credentials...
```

Bereiten Sie Ihre Windows- und Linux-Remote-Server auf die Datenerfassung vor

> **Note**
>
> Dieser Schritt ist nicht erforderlich, wenn Sie den Datensammelpunkt für Strategy Recommendations-Anwendungen mithilfe von vCenter-Anmeldeinformationen einrichten.

Wenn Sie nach der Einrichtung Ihrer Remoteserverkonfigurationen den`collector setup` commandoder das`collector setup --remote-server-configurations`Befehl, müssen Sie Ihre Remoteserver so vorbereiten, dass der Datensammler der Strategy Recommendations-Anwendungen Daten von ihnen sammeln kann.

> **Note**
>
> Sie müssen sicherstellen, dass die Server über ihre private IP-Adresse erreichbar sind. Weitere Anweisungen zur Einrichtung der Umgebung über eine Virtual Private Cloud (VPC) finden Sie unterAWSInformationen zur Ausführung aus der Ferne finden Sie imAmazon Virtual Private Cloud-Benutzerhandbuch.

Informationen zur Vorbereitung Ihrer Linux-Remote-Server finden Sie unterBereiten Sie Linux-Remote-Server vor.

Informationen zur Vorbereitung Ihrer Windows-Remoteserver finden Sie unterRichten Sie die Remoteserverkonfiguration auf Windows-Servern ein.

Bereiten Sie Linux-Remote-Server vor

Richten Sie die schlüsselbasierte Authentifizierung auf Linux-Servern ein

Wenn Sie sich bei der Konfiguration von Remoteserverkonfigurationen dafür entscheiden, die schlüsselbasierte SSH-Authentifizierung für Linux einzurichten, müssen Sie die folgenden Schritte ausführen, um die schlüsselbasierte Authentifizierung auf Ihren Servern einzurichten, sodass Daten vom Datensammler für Strategy Recommendations-Apps gesammelt werden können.

So richten Sie die schlüsselbasierte Authentifizierung auf Ihren Linux-Servern ein

1. Kopieren Sie den mit dem Namen generierten öffentlichen Schlüsselid_rsa_assessment.pubaus dem folgenden Ordner im Container:

   /opt/amazon/application-data-collector/remote-auth/linux/keys.
2. Hängen Sie den kopierten öffentlichen Schlüssel an`$HOME/.ssh/authorized_keys`Datei für alle Remote-Computer. Wenn keine Datei verfügbar ist, erstellen Sie sie mit dem`touch`oder`vim`Befehl.
3. Stellen Sie sicher, dass der Home-Ordner auf dem Remoteserver über eine Berechtigungsstufe verfügt`755`oder weniger. Wenn es`777`, es wird nicht funktionieren. Du kannst das benutzen`chmod`Befehl zum Einschränken von Berechtigungen.

Richten Sie die zertifikatsbasierte Authentifizierung auf Linux-Servern ein

Wenn Sie bei der Konfiguration von Remoteserverkonfigurationen die zertifikatsbasierte Authentifizierung für Linux einrichten möchten, müssen Sie die folgenden Schritte ausführen, damit Daten vom Anwendungsdatensammler von Strategy Recommendations erfasst werden können.

Wir empfehlen diese Option, wenn Sie bereits eine Zertifizierungsstelle (CA) für Ihre Anwendungsserver eingerichtet haben.

Um die zertifikatsbasierte Authentifizierung auf Ihren Linux-Servern einzurichten

1. Kopieren Sie den Benutzernamen, der mit all Ihren Remoteservern funktioniert.
2. Kopieren Sie den öffentlichen Schlüssel des Collectors in die CA.

   Der öffentliche Schlüssel für den Collector befindet sich im folgenden Verzeichnis:

   /opt/amazon/application-data-collector/remote-auth/linux/keys/id_rsa_assessment.pub

   Dieser öffentliche Schlüssel muss Ihrer CA hinzugefügt werden, um das Zertifikat zu generieren.
3. Kopieren Sie das im vorherigen Schritt generierte Zertifikat an den folgenden Speicherort im Collector:

   /opt/amazon/application-data-collector/remote-auth/linux/keys

   Der Name des Zertifikats mussid_rsa_assessment-cert.pub.
4. Geben Sie während des Einrichtungsschritts den Namen der Zertifikatsdatei an.

Richten Sie die Remoteserverkonfiguration auf Windows-Servern ein

Wenn Sie sich bei der Konfiguration von Remoteserverkonfigurationen im Collector-Setup dafür entscheiden, Windows einzurichten, müssen Sie die folgenden Schritte ausführen, damit Daten im Rahmen von Strategy Recommendations gesammelt werden können.

> Um mehr über das zu erfahren PowerShell Lesen Sie diesen Hinweis für das Skript, das auf dem Remoteserver ausgeführt wird.
>
> Das Skript ermöglicht PowerShell remote und deaktiviert alle Authentifizierungsmethoden außer Negotiate. Dies wird für Windows NT LAN Manager (NTLM) verwendet und legt den“AllowUnencrypted"Das WSMan-Protokoll wird auf false gesetzt, um sicherzustellen, dass

der neu erstellte Listener nur verschlüsselten Datenverkehr akzeptiert. Unter Verwendung des von Microsoft bereitgestellten Skripts`New-SelfSignedCertificateEx.ps1`, erstellt es ein selbstsigniertes Zertifikat.
Jede WSMan-Instanz, die über einen HTTP-Listener verfügt, wird zusammen mit den vorhandenen HTTPS-Listenern entfernt. Anschließend wird ein neuer HTTPS-Listener erstellt. Außerdem wird eine Firewallregel für eingehenden Datenverkehr für TCP-Port 5986 erstellt. Im letzten Schritt wird der WinRM-Dienst neu gestartet.

So richten Sie die Datenerfassung über eine Remoteverbindung auf Ihren Windows 2008-Servern ein

1. Verwenden Sie den folgenden Befehl, um die Version von zu überprüfen PowerShell auf Ihrem Server installiert.

   ```
   $PSVersionTable
   ```

2. Wenn der PowerShell Version ist nicht 5.1, laden Sie WMF 5.1 herunter und installieren Sie es, indem Sie den Anweisungen unter folgenInstallieren und konfigurieren Sie WMF 5.1in der Microsoft-Dokumentation.
3. Verwenden Sie den folgenden Befehl in einem neuen PowerShell Fenster, um sicherzustellen, dass PowerShell 5.1 ist installiert.

   ```
   $PSVersionTable
   ```

4. Folgen Sie den nächsten Schritten, in denen beschrieben wird, wie Sie die Datenerfassung über eine Remoteverbindung unter Windows 2012 und höher einrichten.

So richten Sie die Datenerfassung über eine Remoteverbindung auf Ihren Windows 2012- und neueren Servern ein

1. Laden Sie das Setup-Skript von der folgenden URL herunter:

   https://application-data-collector-release. s3.us-west-2.amazonaws.com /scripts/WinRMSetup.ps1
2. Laden Sie das herunter`New-SelfSignedCertificateEx.ps1`von der folgenden URL und fügen Sie das Skript in denselben Ordner ein, in den Sie es heruntergeladen haben`WinRMSetup.ps1`:

https://github.com/Azure/azure-libraries-for-net/blob/master/samples/asset/new-SelfSignedCertificateEx.ps1

3. Um das Setup abzuschließen, führen Sie den heruntergeladenen PowerShell Skript auf allen Anwendungsservern.

```
.\WinRMSetup.ps1
```

> **Note**
>
> Wenn Windows Remote Management (WinRM) auf dem Windows-Remoteserver nicht richtig eingerichtet ist, schlägt der Versuch, Daten von diesem Server zu sammeln, fehl. In diesem Fall müssen Sie das Zertifikat, das diesem Server entspricht, vom folgenden Speicherort auf dem Container löschen: /opt/amazon/application-data-collector/remote-auth/windows/certs/***ads-server-id***.cer Warten Sie nach dem Löschen des Zertifikats, bis der Datenerfassungsvorgang erneut versucht wird.

Stellen Sie sicher, dass Ihr Collector und Ihre Server für die Datenerfassung eingerichtet sind

Stellen Sie mithilfe des folgenden Befehls sicher, dass Ihr Collector und Ihre Server korrekt für die Datenerfassung eingerichtet sind.

```
collector diag-check
```

Dieser Befehl führt eine Reihe von Diagnoseprüfungen für Ihre Serverkonfigurationen durch und liefert Informationen zu fehlgeschlagenen Prüfungen.

Wenn Sie den Befehl in verwenden-aModus, Sie erhalten die Ausgabe in einemDiagnosticCheckResult.txtDatei, nachdem die Prüfungen abgeschlossen sind.

```
collector diag-check -a
```

Sie können eine Diagnoseprüfung für die Serverkonfigurationen eines einzelnen Servers mit der IP-Adresse dieses Servers durchführen.

Die folgenden Beispiele zeigen das Ergebnis einer erfolgreichen Installation.

Linux-Server

```
            Provide your test server IP address: IP address
-------------------------------------------------------------
Start checking connectivity & credentials...
Connectivity and Credential Checks succeeded
-------------------------------------------------------------
Start checking permissions...
Permission Check succeeded
-------------------------------------------------------------
Start checking OS version...
OS version check succeeded
-------------------------------------------------------------
Start checking Linux Bash installation...
Linux Bash installation check succeeded
-------------------------------------------------------------
All diagnostic checks complete successfully.
This server is correctly set up and ready for data collection.
```

Windows-Server

```
            Windows PowerShell Version Check succeeded
Provide your test server IP address: IP address
-------------------------------------------------------------
Start checking connectivity & credentials...
Connectivity and Credential Checks succeeded
-------------------------------------------------------------
Start checking permissions...
Permission Check succeeded
-------------------------------------------------------------
Start checking OS version...
OS version check succeeded
-------------------------------------------------------------
Start checking Windows architecture type...
Windows Architecture Type Check succeeded
-------------------------------------------------------------
All diagnostic checks complete successfully.
This server is correctly set up and ready for data collection.
```

Das folgende Beispiel zeigt eine Fehlermeldung, die angezeigt wird, wenn Ihre Anmeldeinformationen für den Remoteserver falsch sind.

```
Unable to authenticate the server credentials with IP address ${IPAddress}.
Ensure that your credentials are accurate and the server is configured correctly.
Use the following command to reset incorrect credentials.
collector setup –remote-server-configurations
```

Schritt 5: Verwenden Sie Strategieempfehlungen in der Migration Hub Hub-Konsole, um Empfehlungen zu erhalten

In diesem Abschnitt wird beschrieben, wie Sie Strategieempfehlungen in der Migration Hub Hub-Konsole verwenden, um Migrationsempfehlungen zum ersten Mal abzurufen.

So erhalten Sie Empfehlungen

1. Melden Sie sich mit dem AWS Konto, das Sie erstellt habenErstellung von Strategieempfehlungen, bei der Migration Hub Hub-Konsole unter https://console.aws.amazon.com/migrationhub/ an AWS Management Console und öffnen Sie sie.
2. Wählen Sie im Navigationsbereich der Migration Hub Hub-Konsole Strategie aus.
3. Wählen Sie auf der Seite Strategie-Empfehlungen für den Migration Hub die Option Empfehlungen abrufen aus.
4. Wählen Sie Zustimmen, wenn Sie damit einverstanden sind, dass Migration Hub eine serviceverknüpfte Rolle (SLR) in Ihrem Konto erstellt. Weitere Informationen zur Spiegelreflexkamera finden Sie unter. Verwenden von serviceverknüpften Rollen für Strategieempfehlungen
5. Datenquellen konfigurieren

    a. Auf der Seite Datenquellen konfigurieren müssen Sie die Quelle Ihrer zu analysierenden Server aus den folgenden Optionen auswählen:

        i. Strategy Recommendations-Anwendungsdatensammler — Sie können den Strategy Recommendations-Sammler verwenden, um automatisch Informationen über in

VMware vCenter gehostete VMs abzurufen. Wenn Sie diese Option verwenden, müssen Sie keine zusätzlichen Einstellungen vornehmen.

ii. Manueller Import — Wenn Sie Daten über Ihre Server und Anwendungen unabhängig voneinander importieren möchten, können Sie die Importvorlage Strategy Recommendations verwenden. Die Importvorlage ist eine JSON-Datei, in die Sie die verfügbaren Informationen für Ihre VMs eingeben können.

iii. Application Discovery Service — Sie können den Application Discovery Service verwenden, um Informationen über Ihre lokalen Anwendungen und Server zu sammeln. In der Migration Hub Hub-Konsole können Sie im Abschnitt Tools unter Discovery-Tools aus mehreren Optionen wählen. Sie können beispielsweise Application Discovery Service Agentless Collector, AWSDiscovery Agent oder Import (für CSV-Dateien) wählen.

b. In der Tabelle Server werden alle verfügbaren Server auf der Grundlage Ihrer Auswahl im Abschnitt Datenquelle aufgeführt.

c. Unter Registrierte Anwendungsdatensammelpunkte werden die Anwendungsdatensammelpunkte aufgeführt, die Sie eingerichtet haben. Wenn Sie keine Datensammelpunkte eingerichtet haben, können Sie den Datensammelpunkt herunterladen und dann bereitstellen. Weitere Informationen finden Sie unter Schritt 1: Laden Sie den Strategy Recommendations Collector herunter und Schritt 2: Stellen Sie den Strategy Recommendations Collector bereit.

> **Note**
>
> Um Strategieempfehlungen zu erhalten, müssen Sie mindestens einen Anwendungsdatensammelpunkt einrichten oder einen Anwendungsdatenimport durchführen. Wenn Sie Ihre Daten auf Anwendungsebene hinzufügen möchten, ohne einen Collector einzurichten, können Sie die Vorlage für den Import von Anwendungsdaten verwenden. Sie können später weitere Datenquellen hinzufügen.

d. Wenn Sie Manueller Import ausgewählt haben, wählen Sie unter Importdetails die Option Neuen Import hinzufügen aus.

e. Geben Sie unter Importname einen Namen für Ihren Import ein.

f. Geben Sie für S3-Bucket-URI den S3-Bucket-URI ein, in den Ihre Import-JSON-Datei hochgeladen werden soll.

> **Important**
>
> Der S3-Bucket-Name muss mit dem Präfix beginnen**`migrationhub-strategy`**.

g. Wählen Sie Weiter.

6. Geben Sie die Einstellungen an

   a. Richten Sie auf der Seite „Einstellungen angeben“ Ihre Geschäftsziele und Migrationspräferenzen ein. Strategy Recommendations empfiehlt die optimale Strategie für die Migration und Modernisierung Ihrer Anwendungen und Datenbanken auf der Grundlage der von Ihnen angegebenen Einstellungen. Sie können diese Einstellungen zu einem späteren Zeitpunkt ändern.

   b. Wählen Sie Weiter.

7. Überprüfen und abschicken.

   a. Überprüfen Sie Ihre konfigurierten Datenquellen und Migrationseinstellungen.

   b. Wenn alles korrekt aussieht, wählen Sie Datenanalyse starten. Dadurch werden Ihr Serverinventar und Ihre Laufzeitumgebung sowie die Anwendungsbinärdateien für Ihre Microsoft IIS- und Java-Anwendungen analysiert.

> **Note**
>
> Der Status der binären Analyse wird nicht in der Konsole angezeigt. Nach Abschluss der Analyse wird entweder ein Link zum Anti-Pattern-Bericht oder eine Meldung angezeigt, dass die Analyse nicht erfolgreich war.

Strategie, Empfehlungen, Empfehlungen

In diesem Abschnitt wird beschrieben, wie Sie Strategieempfehlungen zur Migration und Modernisierung für Server und Anwendungen in Ihrem Migrationsportfolio einsehen können.

Themen

Strategieempfehlungen finden Sie unter Strategieempfehlungen

In diesem Abschnitt wird beschrieben, wie Sie Strategieempfehlungen in der AWS Migration Hub Konsole verwenden, um Empfehlungen zur Migrationsstrategie anzuzeigen.

Um Strategieempfehlungen einzusehen

1. Melden Sie sich mit dem AWS Konto, das Sie erstellt habenErstellung von Strategieempfehlungen, bei der Migration Hub Hub-Konsole unter https://console.aws.amazon.com/migrationhub/ an AWS Management Console und öffnen Sie sie.
2. Wählen Sie im Navigationsbereich der Migration Hub Hub-Konsole Strategie und dann Empfehlungen aus.
3. Auf der Seite „Empfehlungen“ können Sie zusammenfassende Empfehlungen Ihres Portfolios sowie detaillierte Empfehlungen zur Migrationsstrategie „R“ einsehen und exportieren. Sie können sich auch Tools und Ziele für Migration und Modernisierung sowie Anti-Pattern für Ihre Server und Anwendungskomponenten ansehen.

   Bei Anti-Pattern handelt es sich um eine Liste bekannter Probleme in Ihrem Portfolio, die nach Schweregrad kategorisiert sind. Anti-Pattern mit hohem Schweregrad stehen für Inkompatibilitäten, die behoben werden müssen, Anti-Pattern-Angriffe mit mittlerem Schweregrad für Warnungen und Anti-Pattern-Angriffe mit niedrigem Schweregrad für Informationsprobleme. Informationen zur „R“ -Strategie finden Sie unter Migrationsbegriffe — 7 Rs im Glossar AWS Prescriptive Guidance.

- Wenn in Ihrem Rechenzentrum eine Änderung eintritt oder wenn Sie Ihre Einstellungen aktualisieren, empfehlen wir Ihnen, Ihre Daten erneut zu analysieren. Um Ihre Daten erneut zu analysieren und neue Empfehlungen zu erhalten, wählen Sie Daten erneut analysieren.

  Bis zum Abschluss der erneuten Analyse können die Ergebnisse Ihrer Empfehlungsdaten eine Mischung aus früheren Daten und neuen Daten sein.

  Um eine Berichtsdatei mit den Empfehlungen herunterzuladen, wählen Sie Empfehlungen exportieren.

4. Auf der Registerkarte Anwendungskomponenten können Sie die Empfehlungen für Anwendungskomponenten in Ihrem Migrationsportfolio einsehen. Weitere Informationen finden Sie unter Strategieempfehlungen, Empfehlungen für Anwendungskomponenten.
5. Auf der Registerkarte Server können Sie die Empfehlungen für die Server in Ihrem Migrationsportfolio einsehen. Weitere Informationen finden Sie unter Strategieempfehlungen, Serverempfehlungen.
6. Auf der Registerkarte Einstellungen können Sie die Einstellungen bearbeiten, die Sie unter angegeben habenSchritt 5: Empfehlungen einholen. Informationen zur Bearbeitung Ihrer Einstellungen finden Sie unterEinstellungen für Strategie und Empfehlungen.

Strategieempfehlungen, Empfehlungen für Anwendungskomponenten

In diesem Abschnitt wird beschrieben, wie Sie Strategieempfehlungen in der Migration Hub Hub-Konsole verwenden, um Empfehlungen zur Migrationsstrategie für Anwendungskomponenten anzuzeigen und zu analysieren.

Themen

- Arbeiten mit Anwendungskomponenten in Strategieempfehlungen
- Strategieempfehlungen, Quellcode-Analyse
- Datenbankanalyse für Strategy Recommendations
- Strategieempfehlungen, binäre Analyse.

Arbeiten mit Anwendungskomponenten in Strategieempfehlungen

In diesem Abschnitt wird beschrieben, wie Sie die Strategieempfehlungen für Migration Hub in der Migration Hub Hub-Konsole verwenden, um Empfehlungen für Migrations- und Modernisierungsstrategien anzuzeigen und zu konfigurieren.

Themen

Empfehlungen für Anwendungskomponenten anzeigen

In diesem Abschnitt wird beschrieben, wie Sie Strategieempfehlungen in der Migration Hub Hub-Konsole verwenden, um Empfehlungen zur Migrationsstrategie für Anwendungskomponenten anzuzeigen.

Um Einzelheiten zu den Empfehlungen für Anwendungskomponenten anzuzeigen

1. Melden Sie sich mit dem AWS Konto, das Sie erstellt habenErstellung von Strategieempfehlungen, bei der Migration Hub Hub-Konsole unter https://console.aws.amazon.com/migrationhub/ an AWS Management Console und öffnen Sie sie.
2. Wählen Sie im Navigationsbereich der Migration Hub Hub-Konsole Strategie und dann Empfehlungen aus.
3. Wählen Sie auf der Seite mit den Empfehlungen die Registerkarte Anwendungskomponenten aus.

    a. Unter Zusammenfassung der Anwendungskomponenten finden Sie einen Überblick über die verschiedenen Arten von Anwendungskomponenten, die Sie in Ihrem Serverportfolio ausführen.

    b. Unter Anwendungskomponenten finden Sie Komponentennamen, Komponententyp und Empfehlungen zur Migrationsstrategie „R“. Sie können sich auch das Migrationsziel und die Tools für Migration und Modernisierung ansehen, die Sie für verschiedene Anwendungskomponenten verwenden können, die in Ihrem Serverportfolio ausgeführt werden. Informationen zur „R“ -Strategie finden Sie unter Migrationsbegriffe — 7 Rs im Glossar AWS Prescriptive Guidance.

4. Um die Details für eine Anwendungskomponente anzuzeigen, wählen Sie eine Anwendungskomponente aus und klicken Sie dann auf Details anzeigen.
5. Auf der Detailseite der Anwendungskomponente (die Seite mit dem Namen der Komponente als Überschrift) unter Empfehlungsübersicht können Sie die Empfehlungen für die Anwendungskomponente einsehen. Sie können sich auch identifizierte Anti-Pattern ansehen. Bei Anti-Pattern handelt es sich um eine Liste bekannter Probleme in Ihrem Portfolio, die nach Schweregrad kategorisiert sind.
6. Wählen Sie die Registerkarte Strategieoptionen, um die Migrationsempfehlung für die Anwendungskomponente anzuzeigen. Sie können die empfohlene Strategie außer Kraft setzen, indem Sie eine andere Strategie auswählen und dann Als bevorzugt festlegen klicken.
7. Je nachdem, welche Art von Anwendungskomponente Sie betrachten, gibt es eine Registerkarte „Quellkonfiguration“ oder „Datenbankkonfiguration“. Hinweise zur Quellkonfiguration finden Sie unterKonfigurieren Sie die Quellcodeanalyse für eine Anwendungskomponente. Hinweise zur Datenbankkonfiguration finden Sie unterKonfigurieren Sie die Datenbankanalyse für eine Anwendungskomponente.

Konfigurieren Sie die Quellcodeanalyse für eine Anwendungskomponente

In diesem Abschnitt wird beschrieben, wie Sie Strategieempfehlungen in der Migration Hub Hub-Konsole verwenden, um die Quellcodeanalyse für eine Anwendungskomponente zu konfigurieren.

So konfigurieren Sie die Quellcodeanalyse für eine Anwendungskomponente

1. Wählen Sie im Navigationsbereich der Migration Hub Hub-Konsole Strategie und dann Empfehlungen aus.
2. Wählen Sie auf der Seite mit den Empfehlungen die Registerkarte Anwendungskomponenten aus.
3. Wählen Sie aus der Liste der Komponenten unter Anwendungskomponenten eine Anwendungskomponente mit dem Komponententyp Java, Dotnetframework oder IIS aus, und klicken Sie dann auf Details anzeigen.
4. Wählen Sie auf der Detailseite der Anwendungskomponente (die Seite mit dem Namen der Komponente als Überschrift) die Registerkarte Quellcode-Konfiguration aus.
5. Wählen Sie unter Details zur Quellcode-Konfiguration die Option Quellcode analysieren aus.
6. Geben Sie auf der Seite Quellcode analysieren den Repository-Namen, den Branch-Namen und den Projektnamen (falls zutreffend) an, in dem der Quellcode für die Anwendungskomponente

gespeichert ist. Wählen Sie die Art der GitHub Quellcode-Versionskontrolle aus, die Sie verwenden möchten, und wählen Sie dann Analysieren.

Nach Abschluss der Analyse können Sie die aktualisierten Empfehlungen auf der Detailseite der Anwendungskomponenten einsehen.

Weitere Informationen zur Quellcodeanalyse finden Sie unterStrategieempfehlungen, Quellcode-Analyse.

Konfigurieren Sie die Datenbankanalyse für eine Anwendungskomponente

In diesem Abschnitt wird beschrieben, wie Sie Strategieempfehlungen in der Migration Hub Hub-Konsole verwenden, um die Datenbankanalyse für eine Anwendungskomponente zu konfigurieren.

So konfigurieren Sie die Datenbankanalyse für eine Anwendungskomponente

1. Wählen Sie im Navigationsbereich der Migration Hub Hub-Konsole Strategie und dann Empfehlungen aus.
2. Wählen Sie auf der Seite mit den Empfehlungen die Registerkarte Anwendungskomponenten aus.
3. Wählen Sie aus der Liste der Komponenten unter Anwendungskomponenten eine Anwendungskomponente mit dem Komponententyp SQLServer aus und klicken Sie dann auf Details anzeigen.
4. Wählen Sie auf der Detailseite der Anwendungskomponente (die Seite mit dem Namen der Komponente als Überschrift) die Registerkarte Datenbankkonfiguration aus.
5. Wählen Sie unter Datenbankkonfigurationsdetails die Option Datenbankdetails analysieren aus.
6. Wählen Sie aus dem Dropdownmenü, das Sie in AWS Secrets Manager erstellt haben, einen geheimen Namen für Datenbankanmeldedaten aus, und wählen Sie dann Analysieren aus.

   Nach Abschluss der Analyse können Sie die aktualisierten Empfehlungen auf der Detailseite der Anwendungskomponenten einsehen.

Weitere Hinweise zur Datenbankanalyse und zur Einrichtung eines geheimen Namens finden Sie unterDatenbankanalyse für Strategy Recommendations.

Strategieempfehlungen, Quellcode-Analyse

Migration Hub Strategy Recommendations identifiziert automatisch die Anwendungen in Ihrem Portfolio und erstellt Anwendungskomponenten für sie. Wenn Ihr Portfolio beispielsweise eine Java-Anwendung enthält, wird diese als Anwendungskomponente mit dem Komponententyp Java identifiziert.

Strategy Recommendations analysiert den Quellcode für die Anwendungskomponenten, sofern Sie ihn entsprechend konfigurieren. Hinweise zur Konfiguration einer Anwendungskomponente für die Quellcodeanalyse finden Sie unterKonfigurieren Sie die Quellcodeanalyse für eine Anwendungskomponente.

Strategy Recommendations führt eine Quellcodeanalyse für die Programmiersprachen Java und C# durch.

Informationen zu den Voraussetzungen für die Verwendung der Quellcodeanalyse von Strategy Recommendations finden Sie unterVoraussetzungen für Strategieempfehlungen.

Datenbankanalyse für Strategy Recommendations

Strategy Recommendations identifiziert automatisch die Datenbankserver in Ihrem Portfolio und erstellt Anwendungskomponenten für sie. Wenn Ihr Portfolio beispielsweise eine SQL Server-Datenbank enthält, wird diese als Anwendungskomponente sqlservr.exe identifiziert.

Strategy Recommendations analysiert einzelne Datenbanken in der identifizierten SQL Server-Anwendungskomponente sqlservr.exe mit dem AWS Schema Conversion Tool. Strategy Recommendations identifiziert auch Inkompatibilitäten bei der Migration der Datenbanken zu AWS Datenbanken wie Amazon Aurora MySQL-Compatible Edition, Amazon Aurora PostgreSQL-Compatible Edition, Amazon RDS for MySQL und Amazon RDS for PostgreSQL.

Derzeit ist die Datenbankanalyse von Strategy Recommendations nur für SQL Server verfügbar.

Um Strategy Recommendations für die Analyse Ihrer Datenbanken zu konfigurieren, müssen Sie Anmeldeinformationen für den Datensammelpunkt der Strategy Recommendations-Anwendung angeben, um eine Verbindung zu Ihren Datenbanken herzustellen. Erstellen Sie dazu ein Geheimnis in AWS Secrets Manager in Ihrem AWS Konto.

Informationen zu den Berechtigungen und Privilegien der von Ihnen angegebenen Anmeldeinformationen finden Sie unterErforderliche Rechte für Anmeldeinformationen für AWS das Schema Conversion Tool. Informationen zum Erstellen eines Geheimnisses

mit den Anmeldeinformationen finden Sie unterEin Geheimnis in Secrets Manager für Datenbankanmeldedaten erstellen.

Nachdem Sie die Anmeldeinformationen und den geheimen Schlüssel eingerichtet haben, können Sie die Analyse des AWS Schema Conversion Tool auf dem Datenbankserver konfigurieren. Weitere Informationen finden Sie unter Konfigurieren Sie die Datenbankanalyse für eine Anwendungskomponente.

Nachdem Sie die Datenbankanalyse für die Anwendungskomponente konfiguriert haben, wird eine Inventarisierungsaufgabe für das AWS Schema Conversion Tool geplant. Nach Abschluss dieser Aufgabe werden Sie sehen, wie die neuen Anwendungskomponenten für jede einzelne Datenbank auf diesem Datenbankserver erstellt werden. Wenn Ihr SQL Server beispielsweise zwei Datenbanken hat (exampledbs1 und exampledbs2), wird für jede der Datenbanken eine Anwendungskomponente mit den Namen exampledbs1 und exampledbs2 erstellt.

Wenn Sie bei der Migration jeder identifizierten Datenbank zu Datenbanken Anti-Pattern feststellen möchten, richten Sie die Analyse für jede Datenbank ein. Gehen Sie dabei wie unter beschrieben vor. AWS Konfigurieren Sie die Datenbankanalyse für eine Anwendungskomponente

Erforderliche Rechte für Anmeldeinformationen für AWS das Schema Conversion Tool

Die Anmeldeinformationen, die Sie AWS Secrets Manager zur Verfügung stellen, benötigen nur `VIEW SERVER STATE` und `VIEW ANY DEFINITION` Rechte. Optional können Sie mithilfe des Skripts, das unter https://gitlab.aws.dev/dmaf-pub/dmaf/-/blob/master/create_mssql_ro_user.sql verfügbar ist, ein neues Login erstellen.

Sie können bei der Erstellung des SQL Server-Anmeldenamens einen beliebigen Anmeldenamen und ein beliebiges Kennwort angeben.

Ein Geheimnis in Secrets Manager für Datenbankanmeldedaten erstellen

Wenn die Anmeldeinformationen bereit sind, damit der Strategy Recommendations-Anwendungsdatensammelpunkt eine Verbindung zu einer Datenbank herstellen kann, erstellen Sie in AWS Secrets Manager einen geheimen Schlüssel in Ihrem AWS Konto, wie im folgenden Verfahren beschrieben.

Um ein Geheimnis mit AWS Secrets Manager in Ihrem AWS Konto zu erstellen

1. Melden Sie sich mit dem AWS Konto, das Sie erstellt habenErstellung von Strategieempfehlungen, bei der AWS Secrets Manager Manager-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/secretsmanager/.

2. Wählen Sie Store a new secret (Ein neues Secret speichern).
3. Wählen Sie den Geheimtyp als Andere Art von Geheimnissen aus.
4. Geben Sie unter Schlüssel/Wert-Paare die folgenden Informationen ein.

   Nutzername – dein Nutzername

   Wählen Sie dann + Zeile hinzufügen und geben Sie die folgenden Informationen ein.

   Passwort - *dein* Passwort
5. Wählen Sie Weiter aus.
6. Geben Sie Secret Name als eine beliebige Zeichenfolge mit dem Präfix migrationhub-strategy - ein. Zum Beispiel migrationhub-strategy-one.

   > **Note**
   >
   > Bewahren Sie Ihren geheimen Namen zur späteren Verwendung an einem sicheren Ort auf.
7. Wählen Sie Weiter und dann erneut Weiter.
8. Wählen Sie Store (Speichern) aus.

Sie können den geheimen Schlüssel, den Sie für Datenbankanmeldedaten erstellt haben, verwenden, wenn Sie die Datenbankanalyse in den Strategieempfehlungen einrichten.

Strategieempfehlungen, binäre Analyse.

Migration Hub Strategy Recommendations identifiziert automatisch die Anwendungen in Ihrem Portfolio und die zugehörigen Anwendungskomponenten. Wenn Ihr Portfolio beispielsweise eine Java-Anwendung enthält, identifiziert Strategy Recommendations sie als Anwendungskomponente mit dem Komponententyp Java. Strategy Recommendations kann Binäranalysen durchführen, ohne dass Sie den Zugriff auf den Quellcode konfigurieren müssen, indem sie die IIS-Anwendungs-DLLs unter Windows oder die Anwendungs-JAR-Dateien unter Linux überprüfen und Anti-Pattern-Berichte oder Inkompatibilitätsberichte bereitstellen. Ein Anti-Pattern-Bericht ist eine nach Schweregrad kategorisierte Liste bekannter Probleme, die Strategy Recommendations in Ihrem Portfolio entdeckt. Ein Inkompatibilitätsbericht enthält eine Teilmenge der Anti-Pattern, nämlich API-Kompatibilität, Nuget Package und Porting Action.

Strategy Recommendations führt Analysen für Windows IIS- und Java Tomcat- und Jboss-Anwendungen durch. Wenn Sie über eine IIS-Anwendung verfügen, generiert Strategy Recommendations standardmäßig einen Inkompatibilitätsbericht. Sie müssen den Quellcodezugriff konfigurieren, um den vollständigen Anti-Pattern-Bericht zu erhalten. Wenn Sie über eine Java-Anwendung verfügen, generiert Strategy Recommendations standardmäßig den vollständigen Anti-Pattern-Bericht.

Der inkompatible Bericht oder der Anti-Pattern-Bericht wird nach Abschluss der Analyse angezeigt. Wenn die Analyse nicht erfolgreich ist, können Sie versuchen, eine Quellcodeanalyse durchzuführen, indem Sie den Zugriff auf den Quellcode gewähren, wie unter beschriebenRichten Sie Konfigurationen für die Versionskontrolle ein.

Strategieempfehlungen, Serverempfehlungen

In diesem Abschnitt wird beschrieben, wie Sie die Strategieempfehlungen für Migration Hub in der Migration Hub Hub-Konsole verwenden, um Empfehlungen zur Migrationsstrategie für die Server in Ihrem Migrationsportfolio anzuzeigen.

Um Empfehlungen für Server anzuzeigen

1. Melden Sie sich mit dem AWS Konto, das Sie erstellt habenErstellung von Strategieempfehlungen, bei der Migration Hub Hub-Konsole unter https://console.aws.amazon.com/migrationhub/ an AWS Management Console und öffnen Sie sie.
2. Wählen Sie im Navigationsbereich der Migration Hub Hub-Konsole Strategie und dann Empfehlungen aus.
3. Wählen Sie auf der Seite mit den Empfehlungen die Registerkarte Server aus.
    a. Unter Serverübersicht finden Sie eine Übersicht über die verschiedenen Servertypen, die Sie in Ihrem Portfolio betreiben.
    b. Unter Server finden Sie Server- und Betriebssystemdetails sowie Empfehlungen zur Migrationsstrategie „R“. Sie können auch das Migrationsziel und die Anzahl der auf Ihren Servern identifizierten Anti-Pattern einsehen, die auf den Empfehlungen basieren. Informationen zur „R“ -Strategie finden Sie unter Migrationsbegriffe — 7 Rs im Glossar AWS Prescriptive Guidance.
4. Um ausführliche Empfehlungsdetails für einen Server anzuzeigen, wählen Sie den Server aus der Liste aus und klicken Sie dann auf Details anzeigen. Sie können die für den Server

gesammelten Metadaten zusammen mit ausführlichen Analysen und Empfehlungen anzeigen, die auf den Anwendungskomponenten basieren, die auf dem Server ausgeführt werden.

5. Auf der Seite mit den Serverdetails (der Seite mit dem Servernamen als Überschrift) finden Sie unter Zusammenfassung der Empfehlungen einen Überblick über die Strategieempfehlungen für den Server. Sie können sich auch identifizierte Anti-Pattern ansehen. Bei Anti-Pattern handelt es sich um eine Liste bekannter Probleme in Ihrem Portfolio, die nach Schweregrad kategorisiert sind.
6. Wählen Sie die Registerkarte Strategieoptionen, um die Migrationsempfehlung für den Server anzuzeigen. Sie können die empfohlene Strategie außer Kraft setzen, indem Sie eine andere Strategie auswählen und dann Als bevorzugt festlegen auswählen.
7. Wählen Sie die Registerkarte Anwendungskomponenten, um die Liste der Anwendungskomponenten anzuzeigen, die dem Server zugeordnet sind.
8. Um Details zur Anwendungskomponente anzuzeigen, wählen Sie die Komponente aus der Liste aus und klicken Sie dann auf Details anzeigen. Weitere Informationen zu Anwendungskomponenten finden Sie unterArbeiten mit Anwendungskomponenten.

Einstellungen für Strategie und Empfehlungen

In diesem Abschnitt wird beschrieben, wie Sie die Einstellungen für die Migration Hub-Strategieempfehlungen in der Migration Hub Hub-Konsole anzeigen und bearbeiten.

Sie wählen Ihre Empfehlungseinstellungen, wenn Sie Strategieempfehlungen zum ersten Mal einrichten, wie unter beschriebenSchritt 5: Empfehlungen einholen. Sie können diese Einstellungen bearbeiten.

Um die Einstellungen für Empfehlungen zu bearbeiten

1. Melden Sie sich mit dem AWS Konto, das Sie erstellt habenErstellung von Strategieempfehlungen, bei der Migration Hub Hub-Konsole unter https://console.aws.amazon.com/migrationhub/ an AWS Management Console und öffnen Sie sie.
2. Wählen Sie im Navigationsbereich der Migration Hub Hub-Konsole Strategie und dann Empfehlungen aus.
3. Wählen Sie auf der Seite mit den Empfehlungen die Registerkarte Einstellungen aus.
4. Unter Priorisierte Geschäftsziele können Sie die Geschäftsziele per Drag-and-Drop verschieben, um sie neu anzuordnen.

5. Wählen Sie die gewünschten Anwendungseinstellungen und Datenbankeinstellungen aus, und klicken Sie dann auf Änderungen speichern.

Wenn Sie Ihre Einstellungen ändern, wird ein Banner angezeigt, das Sie daran erinnert, Daten erneut analysieren auszuwählen.

Datenquellen für Strategieempfehlungen

In diesem Abschnitt werden die Datenquellen beschrieben, die Strategy Recommendations verwendet.

Themen

Datenquellen für Strategy Recommendations anzeigen

In diesem Abschnitt wird beschrieben, wie Sie die Datenquellen für Strategieempfehlungen in der anzeigen AWS Management Console.

Um Datenquellen anzuzeigen

1. Melden Sie sich mit dem AWS Konto, das Sie erstellt habenErstellung von Strategieempfehlungen, bei der Migration Hub Hub-Konsole unter https://console.aws.amazon.com/migrationhub/ an AWS Management Console und öffnen Sie sie.
2. Wählen Sie im Navigationsbereich der Migration Hub Hub-Konsole Strategie und dann Datenquellen aus.
3. Auf der Registerkarte Collectors können Sie die Datensammelpunkte der Strategy Recommendations-Anwendung anzeigen, die Sie eingerichtet haben. Weitere Informationen zum Collector finden Sie unterStrategie, Empfehlungen, Anwendungsdatensammler..
4. Auf der Registerkarte Importe können Sie Daten importieren und Ihre Datenimporte anzeigen. Weitere Informationen finden Sie unter Daten in Strategy Recommendations importieren.
5. Auf der Registerkarte Tools können Sie die Datenvorlage für den Collector und die Anwendung herunterladen.

Strategie, Empfehlungen, Anwendungsdatensammler.

In diesem Abschnitt wird beschrieben, wie Sie den Anwendungsdatensammler von Strategy Recommendations verwenden.

Informationen zum Herunterladen und Einrichten eines Anwendungsdatensammelpunkts finden Sie unterSchritt 1: Laden Sie den Strategy Recommendations Collector herunter.

Themen

Vom Kollektor für Strategieempfehlungen gesammelte Daten

In diesem Abschnitt wird die Art der Daten beschrieben, die der Anwendungsdatensammler für Migration Hub Strategy Recommendations sammelt. Ein Anwendungsdatensammler ist ein Datensammler ohne Agenten, der laufende Anwendungen auf Ihren Servern identifiziert, Quellcodeanalysen durchführt und Ihre Datenbanken analysiert.

Datenfeld	Beschreibung
Typ des Betriebssystems	Windows oder Linux
Betriebssystemversion	Die spezifische Version des Betriebssystems. Zum Beispiel Windows Server 2003, RHEL 5.2.
Betriebssystem-Architektur	32-Bit- oder 64-Bit-Betriebssystem
Ist Server-VM	Der Server ist eine VM oder eine physische Maschine.
Virtualisierungssoftware	Zum Beispiel vCenter, Hyper-V.
Ort	Zum Beispiel die Amazon Elastic Compute Cloud-Konsole (Amazon EC2) oder lokal.
Ist DualBoot	Ermöglicht das Booten mehrerer Betriebss ysteme

Datenfeld	Beschreibung
Firmware-Typ	BIOS, UEFI
Bootloader	GRUB, GRUB 2
Typ der Partitionstabelle	MBR, GPT
CPU-Geschwindigkeit	CPU-Geschwindigkeit in GHz. Zum Beispiel 2,4 GHz.
Windows OS data	
Windows-Ausgabe	Standard, Rechenzentrum, Unternehmen
.NET-Framework-Version	Die installierte Version des.NET-Frameworks.
.NET Core-Version	Die installierte Version von.NET Core.
Linux data	
Linux-Betriebssystemverteilung	RHEL, CentOS, SUSE und so weiter.
Kernel-Version	Ausgabe von uname -r, z. B. `4.9.217-0.1.ac.205.84.332.metal1.x86_64`
For each disk volume	
Dateisystemtyp	FAT32, NTFS, ReFS, ext4, jfs und so weiter.
Größe des Festplattenvolumens	Gesamtgröße der Festplatte
Freier Speicherplatz auf der Festplatte	Freier Festplattenspeicher
Image-Format für virtuelle Festplatten	vmdk, vhd, vhdx
Festplattentyp (Windows)	Einfach, dynamisch
Application level data	
Anwendungsname	Der Name des laufenden Prozesses. Zum Beispiel SQLServr.exe, MSdtsservr.exe usw.

Datenfeld	Beschreibung
Anwendungstyp	IIS, JBoss, Tomcat usw.
Programmiersprache und Version	C#, Java
JDK-Version	Die Version des installierten JDK.
Ist der Quellcode verfügbar	Wenn Sie ein Quellcode-Repository bereitstellen, bedeutet dies, dass der Quellcode verfügbar ist.
Bitgröße der Anwendung	16-Bit, 32-Bit, 64-Bit
Windows	
.NET-Framework-Version, die von der App verwendet wird	Die Version der.NET-Framework-DLL, die zur Laufzeit für die Anwendung geladen wird.
.NET Core-Version	Die.NET-Core-DLL-Version, die zur Laufzeit der Anwendung geladen wird.
Verwendet das WPF-Framework?	Ermittelt, ob es sich bei der .NET-basierten Anwendung um eine Art WPF-App handelt oder nicht.
Verwendet das WCF-Framework?	Ermittelt, ob es sich bei der .NET-basierten Anwendung um eine Art WCF-App handelt oder nicht.
ASP.NET-Version	Die Version von ASP.NET.
IIS-Version	Die Version des IIS-Servers, der auf dem Windows-Computer installiert ist.
Bitgröße der Betriebssystemtreiber der Anwendung	32-Bit, 64-Bit

Datenfeld	Beschreibung
Verwendung der Windows-Registrierung	Fragt die Registrierungsschlüssel des Computers ab, um Informationen wie Datenbankversion, Java-Version, .NET-Version usw. zu finden.
Alle von der Anwendung verwendeten DLLs	Ruft die Liste aller DLLs ab, die zur Laufzeit von einem Windows-Prozess geladen wurden.
PowerShell Version	Überprüft die auf dem Computer installierte PowerShell Version, die 5.1 oder höher sein sollte.
Linux	
Typ des Anwendungs-Frameworks	Tomcat, Spring Boot, JBoss, WebLogic WebSphere
Version des Anwendungs-Frameworks	Die Version des Anwendungsframeworks.
Database	
Datenbanktyp	MS SQL, Oracle, MySQL und so weiter.
Datenbankversion	Die Version der Datenbank.

Entfernen Sie Ihre Daten aus den Strategieempfehlungen

Um all Ihre Daten aus den Strategieempfehlungen entfernen zu lassen, wenden Sie sich an uns AWS Supportund fordern Sie die vollständige Löschung der Daten an.

Den Strategy Recommendations Collector aktualisieren

Der Anwendungsdatensammler für Migration Hub Strategy Recommendations wird automatisch aktualisiert. Sie können das folgende Verfahren verwenden, um den Collector bei Bedarf manuell zu aktualisieren.

Um den Strategy Recommendations Collector zu aktualisieren

1. Verwenden Sie den folgenden Befehl, um mithilfe eines SSH-Clients eine Verbindung zur Collector-VM herzustellen.

```
ssh ec2-user@CollectorIPAddress
```

2. Wechseln Sie in das Upgrade-Verzeichnis in der Collector-VM, wie im folgenden Beispiel gezeigt.

```
cd  /home/ec2-user/collector/upgrades
```

3. Verwenden Sie den folgenden Befehl, um das Upgrade-Skript auszuführen.

```
bash application-data-collector-upgrade
```

Daten in Strategy Recommendations importieren

Als Alternative zur Verwendung des Anwendungsdatensammlers können Sie Informationen zu den Anwendungen und Servern importieren, für die Sie Empfehlungen zur Migration und Modernisierung wünschen.

Wenn Sie Daten importieren, sind die Empfehlungen nicht so ausführlich wie bei der Verwendung des Datensammelpunkts. Beispielsweise können Sie die Quellcodeanalyse nicht für importierte Daten verwenden.

In diesem Abschnitt wird beschrieben, wie Sie die Vorlage für den Anwendungsimport verwenden, um Daten in Strategy Recommendations in der Migration Hub Hub-Konsole zu importieren.

Um Daten zu importieren

1. Melden Sie sich mit dem AWS Konto, das Sie erstellt habenErstellung von Strategieempfehlungen, bei der Migration Hub Hub-Konsole unter https://console.aws.amazon.com/migrationhub/ an AWS Management Console und öffnen Sie sie.
2. Wählen Sie im Navigationsbereich der Migration Hub Hub-Konsole Strategie und dann Datenquellen aus.
3. Wählen Sie die Registerkarte Importe.

4. Wählen Sie Importvorlage herunterladen, um die Importvorlage für die Anwendung herunterzuladen.
5. Füllen Sie die Vorlage aus und laden Sie sie in einen Amazon S3 S3-Bucket hoch. Stellen Sie sicher, dass der Name des Buckets mit dem Präfix beginnt`migrationhub-strategy`.
6. Kehren Sie zur Registerkarte Importe zurück und wählen Sie dann Import.
7. Geben Sie einen Namen für Ihren Import ein, geben Sie die Amazon S3 S3-Objekt-URI für Ihre ausgefüllte Datenvorlage ein und wählen Sie dann Import starten.

Die Importvorlage für Strategieempfehlungen

Die Importvorlage, die Sie herunterladen, ist eine `.json` Datei, wie im folgenden Beispiel gezeigt.

```
{
    "ImportFormatVersion": 1,
    "Resources": [
        {
            "ResourceType": "SERVER",
            "ResourceName": "",
            "ResourceId": "",
            "IpAddress": "",
            "OSDistribution": "",
            "OSType": "",
            "HostName": "",
            "OSVersion": "",
            "CPUArchitecture": ""
        },
        {
            "ResourceType": "PROCESS",
            "ResourceName": "",
            "ResourceId": "",
            "ApplicationType": "",
            "DotNetFrameworkVersion": "",
            "ApplicationVersion": "",
            "DotNetCoreVersion": "",
            "JdkVersion": "",
            "ProgrammingLanguage": "",
            "DatabaseType": "",
            "DatabaseVersion": "",
            "DatabaseEdition": "",
            "AssociatedServerIds": []
        }
```

```
    ]
}
```

Um Ihnen das Ausfüllen der Importvorlage zu erleichtern, sind die gültigen Werte für die Datenfelder in den folgenden Tabellen aufgeführt.

Die erforderlichen Felder für Server sind in der folgenden Tabelle aufgeführt.

Name	Beschreibung	Typ	Erforderlich	Zulässige Werte
ResourceId	Eine eindeutige ID für die Ressource	String	Ja	Beliebige eindeutige Zeichenfolge
ResourceName	Der Name der Ressource	String	Ja	Jede Zeichenfolge
ResourceType	Der Typ der zu importierenden Ressource	String	Ja	„Server“, „Prozess“
Betriebssystem-Verteilung	Windows, Windows Server, Ubuntu	String	Ja	Windows: „Windows-PC“, „Windows-Server“ Linux: „Ubuntu“, „RHEL“, „Amazon Linux“, „DEBIAN“, „SLES“, „CENT_OS“, „ORACLE_LINUX“, „FEDORA“, „KALI“
OSType	Die Art des Betriebssystems	String	Ja	„Windows“, „Linux“
Betriebssystemversion	Die Kernel-Version	String	Ja	Sehen Sie sich die HTML-Version der Dokumentation an.

Name	Beschreibung	Typ	Erforderlich	Zulässige Werte
CPU-Architektur	Die CPU-Architektur	String	Nein	„32 Bit“, „64 Bit“
IpAddress	Die IP-Adresse des Servers	Array	Nein	Im Format xxx.xxx.xxx.xxx
MacAddresses	Die mit dem Server verknüpften Mac-Adressen	Array	Nein	Im Format xx:xx:xx:xx:xx:xx
Hostname	Der Name des Hosts	String	Nein	Jede Zeichenfolge

Die erforderlichen Felder für Prozesse sind in der folgenden Tabelle aufgeführt.

Name	Beschreibung	Typ	Erforderlich	Zulässige Werte
ResourceId	Eine eindeutige ID für die Ressource	String	Ja	Beliebige eindeutige Zeichenfolge
ResourceName	Der Name der Ressource	String	Ja	Jede Zeichenfolge
ResourceType	Der Typ der zu importierenden Ressource	String	Ja	„Server“, „Prozess“
AssociatedServerIDs	Eine Liste von Server-IDs, auf denen	String	Ja	Der ResourceId "ResourceType„: „SERVER“, den Sie definiert haben.

Name	Beschreibung	Typ	Erforderlich	Zulässige Werte
	der Prozess läuft.			
ApplicationType	Die Art der Anwendung	String	Ja	„Tomcat“, „JBoss“, „Spring“, „IIS“, „Mongo DB“, „DB2", „Maria DB“, „MySQL“, „Oracle“, „SQLServer“, „Sybase“, „PostgreSQLServer“, „Cassandra“, „IBM WebSphere“, „Oracle“, „Java Generic“ WebLogic
ApplicationVersion	Die Version der Anwendung	String	Ja	„IIS 1.0", „IIS 2.0", „IIS 3.0", „IIS 4.0", „IIS 5.0", „IIS 5.1", „IIS 6.0", „IIS 7.0", „IIS 7.5", „IIS 8.0", „IIS 8.5", „IIS 10.0"
ProgrammingLanguage	Die Programmiersprache für die Anwendung	String	Nein	„Java“, „CSharp“

Name	Beschreibung	Typ	Erforderlich	Zulässige Werte
DotNetFrameworkVersion	Die Version von.NET Framework, falls die Anwendung auf .NET Framework basiert	String	Nein	„DotnetFramework 1,0"," DotnetFramework 1,0 SP1", "DotnetFramework 1,0 SP2"," 1,0 SP3", "DotnetFramework DotnetFramework 1,1"," DotnetFramework 1,1 SP1", "2,0"," 2,0 SP1", DotnetFramework "DotnetFramework 2,0 SP2"," 3,0", "DotnetFramework 3,0 SP1"," DotnetFramework 3,0 SP2", "DotnetFramework DotnetFramework 3,5"," DotnetFramework 3,5 SP1", "DotnetFramework4,5"," 4,5", "4,5"," DotnetFramework 4,5", DotnetFramework "DotnetFramework4,5,2"," 4,6", "DotnetFramework 4,6"," DotnetFramework 4,6,1" 2", "4,7"," DotnetFramework 4,7,1", "DotnetFramework 4,7,2"," 4,8“ DotnetFramework DotnetFramework DotnetFramework DotnetFramework
DotNetCoreVersion	Die Version von.NET Core, falls die Anwendung auf .NET Core basiert	String	Nein	„.NET Core 1.0", „.NET Core 1.1", „.NET Core 2.0", „.NET Core 2.1", „.NET Core 2.2", „.NET Core 3.0", „.NET Core 3.1“

Name	Beschreibung	Typ	Erforderlich	Zulässige Werte
JdkVersion	Die Version des JDK, falls die Anwendung das JDK verwendet	String	Nein	„JDK1.0", „JDK2.0", „JDK3.0", ..., „JDK11.0"
DatabaseType	Der Typ Datenbank	String	Nein	„SQLServer“, „Oracle“, „Sybase“, „Mongo DB“, „Maria DB“, „Apache Cassandra “, „MySQL“, „IBM DB2", „PostgreSQLServer“
DatabaseEdition	Die Edition der Datenbank	String	Nein	
DatabaseVersion	Die Version der Datenbank	String	Nein	Weitere Informationen finden Sie in der HTML-Version der Dokumentation.

Ihre Daten aus den Strategieempfehlungen entfernen

Um all Ihre Daten aus den Strategieempfehlungen von Migration Hub entfernen zu lassen, wenden Sie sich an AWS Support.

Strategieempfehlungen für Sicherheit im Migration Hub

Die Sicherheit in der Cloud hat für AWS höchste Priorität. Als AWS-Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die eingerichtet wurden, um die Anforderungen der anspruchsvollsten Organisationen in puncto Sicherheit zu erfüllen.

Sicherheit ist eine übergreifende Verantwortlichkeit zwischen AWS und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud selbst und als 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. Weitere Informationen zu den Compliance-Programmen, die für die Strategieempfehlungen von Migration Hub gelten, finden Sie unter AWSServices im Umfang nach Compliance-Programm AWS .
- Sicherheit in der Cloud – Ihr Verantwortungsumfang wird durch den AWS-Dienst 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.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung von Strategieempfehlungen anwenden können. In den folgenden Themen erfahren Sie, wie Sie Strategieempfehlungen so konfigurieren, dass sie Ihre Sicherheits- und Compliance-Ziele erreichen. Außerdem erfahren Sie, wie Sie andere AWS Dienste nutzen können, die Sie bei der Überwachung und Sicherung Ihrer Ressourcen für Strategieempfehlungen unterstützen.

Themen

Datenschutz in den Strategieempfehlungen des Migration Hub

Das Modell der AWS gemeinsamen Verantwortung gilt für den Datenschutz in den Strategieempfehlungen des Migration Hub. Wie in diesem Modell beschrieben, ist AWS für den Schutz der globalen Infrastruktur verantwortlich, in der die gesamte AWS Cloud ausgeführt wird. 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, AWS-Konto-Anmeldeinformationen zu schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einzurichten. 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 für die Kommunikation mit AWS-Ressourcen. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit AWS CloudTrail ein.
- Verwenden Sie AWS-Verschlüsselungslösungen zusammen mit allen Standardsicherheitskontrollen in 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 auf AWS über eine Befehlszeilenschnittstelle oder über 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 Strategy Recommendations oder auf andere Weise AWS-Services über die KonsoleAWS CLI, API oder AWS SDKs arbeiten. 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 im Ruhezustand

Alle in der Datenbank von Strategy Recommendations gespeicherten Daten sind verschlüsselt.

Verschlüsselung während der Übertragung

Strategy Recommendations Die Netzwerkkommunikation unterstützt die TLS 1.2-Verschlüsselung zwischen allen Komponenten und Clients.

Identity and Access Management für Migration Hub Strategy Recommendations

AWS Identity and Access Management (IAM) ist ein AWS-Service , mit dem ein Administrator den Zugriff auf - AWS Ressourcen sicher steuern kann. IAM-Administratoren steuern, wer authentifiziert (angemeldet) und autorisiert (im Besitz von Berechtigungen) ist, Strategy Recommendations-Ressourcen zu nutzen. IAM ist ein AWS-Service , den Sie ohne zusätzliche Kosten verwenden können.

Themen

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, unterscheidet sich je nach Ihrer Arbeit in Strategy Recommendations.

Service-Benutzer – Wenn Sie den Service Strategy Recommendations zur Ausführung von Aufgaben verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen bereit, die Sie benötigen. Wenn Sie für Ihre Arbeit weitere Funktionen von Strategy Recommendations verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Fuktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Wenn Sie nicht auf ein Feature in Strategy Recommendations zugreifen können, finden Sie weitere Informationen unter Fehlerbehebung bei Identität und Zugriff auf Migration Hub Strategy Recommendations.

Service-Administrator – Wenn Sie in Ihrem Unternehmen für die Ressourcen für Strategieempfehlungen verantwortlich sind, haben Sie wahrscheinlich vollständigen Zugriff auf Strategieempfehlungen. Es ist Ihre Aufgabe, zu bestimmen, auf welche Funktionen und Ressourcen von Strategy Recommendations Ihre Service-Benutzer zugreifen sollen. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Servicenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen dazu, wie Ihr Unternehmen IAM mit Strategieempfehlungen verwenden kann, finden Sie unter So funktionieren Migration Hub Strategy Recommendations mit IAM.

IAM-Administrator – Wenn Sie als IAM-Administrator fungieren, sollten Sie Einzelheiten dazu kennen, wie Sie Richtlinien zur Verwaltung des Zugriffs auf Strategy Recommendations verfassen können. Beispiele für identitätsbasierte Richtlinien für Strategieempfehlungen, die Sie in IAM verwenden können, finden Sie unter Beispiele für identitätsbasierte Richtlinien für Migration Hub Strategy Recommendations.

Authentifizierung mit Identitäten

Die Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten bei anmelden. Sie müssen als Root-Benutzer des AWS-Kontos, als IAM-Benutzer oder durch Übernahme einer IAM-Rolle authentifiziert (bei angemeldet AWS) sein.

Sie können sich bei AWS als Verbundidentität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt werden. AWS IAM Identity Center (IAM Identity Center)-Benutzer, die Single-Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für Verbundidentitäten. Wenn Sie

sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie AWS über einen Verbund auf zugreifen, übernehmen Sie indirekt eine Rolle.

Je nachdem, um welchen Benutzertyp es sich handelt, können Sie sich bei der AWS Management Console oder im - AWS Zugriffsportal anmelden. Weitere Informationen zur Anmeldung bei AWS finden Sie unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung - Benutzerhandbuch.

Wenn Sie AWS programmgesteuert auf zugreifen, AWS stellt ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (Command Line Interface, CLI) bereit, um Ihre Anforderungen mithilfe Ihrer Anmeldeinformationen kryptografisch zu signieren. Wenn Sie keine AWS Tools verwenden, müssen Sie Anforderungen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode zum eigenständigen Signieren von Anforderungen finden Sie unter Signieren von AWS API-Anforderungen im IAM-Benutzerhandbuch.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. empfiehlt beispielsweise, AWS Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center - Benutzerhandbuch und Verwenden der Multi-Faktor-Authentifizierung (MFA) in AWS im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie ein erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services und Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet und Sie melden sich mit der E-Mail-Adresse und dem Passwort an, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Verbundidentität

Fordern Sie als bewährte Methode menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, auf, den Verbund mit einem Identitätsanbieter zu verwenden, um AWS-Services mithilfe temporärer Anmeldeinformationen auf zuzugreifen.

Eine Verbundidentität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, ein Web-Identitätsanbieter, die AWS Directory Service, das Identity-Center-Verzeichnis oder jeder Benutzer, der mit AWS-Services Anmeldeinformationen auf zugreift, die über eine Identitätsquelle bereitgestellt werden. Wenn Verbundidentitäten auf zugreifen AWS-Konten, übernehmen sie Rollen und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen in IAM Identity Center erstellen oder eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und synchronisieren, um sie für alle Ihre AWS-Konten und Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center -Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität in Ihrem AWS-Konto mit bestimmten Berechtigungen für eine einzelne Person oder Anwendung. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Eine IAM-Gruppe ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Erstellen eines IAM-Benutzers (anstatt einer Rolle) im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität in Ihrem AWS-Konto mit bestimmten Berechtigungen. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der übernehmen, AWS Management Console indem Sie die Rollen

wechseln. Sie können eine Rolle übernehmen, indem Sie eine AWS CLI - oder AWS -API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter Verwenden von IAM-Rollen im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- Verbundbenutzerzugriff: Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center -Benutzerhandbuch.
- Temporäre IAM-Benutzerberechtigungen: Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können AWS-Services Sie jedoch eine Richtlinie direkt an eine Ressource anfügen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff – Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon EC2 aus oder speichert Objekte in Amazon S3. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Forward Access Sessions (FAS) – Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen in auszuführen AWS, gelten Sie als Prinzipal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anforderung AWS-Service , Anfragen an nachgelagerte Services zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Service eine Anfrage erhält, die Interaktionen mit anderen AWS-

Services oder -Ressourcen erfordert. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

- Servicerolle: Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.
- Serviceverknüpfte Rolle – Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einem verknüpft ist AWS-Service. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem angezeigt AWS-Konto und gehören dem Service. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

- Anwendungen, die auf Amazon EC2 ausgeführt werden – Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und - AWS CLI oder AWS -API-Anforderungen stellen. Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2-Instance eine - AWS Rolle zuzuweisen und sie für alle ihre Anwendungen verfügbar zu machen, erstellen Sie ein Instance-Profil, das an die Instance angehängt ist. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon EC2-Instances ausgeführt werden im IAM-Benutzerhandbuch.

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter Erstellen einer IAM-Rolle (anstatt eines Benutzers) im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie steuern den Zugriff in , AWS indem Sie Richtlinien erstellen und sie an AWS Identitäten oder Ressourcen anfügen. Eine Richtlinie ist ein Objekt in , AWS das, wenn es einer Identität oder Ressource zugeordnet wird, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anforderung stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden in AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Administratoren können AWS JSON-Richtlinien verwenden, um anzugeben, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. 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.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen über die AWS Management Console, die AWS CLI oder die AWS -API abrufen.

Identitätsbasierte Richtlinien

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.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem anfügen können AWS-Konto. Verwaltete Richtlinien umfassen - AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer eingebundenen Richtlinie wählen, finden Sie unter Auswahl zwischen verwalteten und eingebundenen Richtlinien im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen

in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Prinzipale können Konten, Benutzer, Rollen, Verbundbenutzer oder umfassen AWS-Services.

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Zugriffssteuerungslisten (ACLs)

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Services AWS WAF, die ACLs unterstützen. Weitere Informationen zu ACLs finden Sie unter Zugriffssteuerungsliste (ACL) – Übersicht (Access Control List) im Amazon-Simple-Storage-Service-Entwicklerhandbuch.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger häufig verwendete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Berechtigungsgrenzen:Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.
- Service-Kontrollrichtlinien (SCPs)– SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in angeben AWS Organizations. AWS Organizations ist ein Service zum Gruppieren und zentralen Verwalten mehrerer AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. Die SCP beschränkt Berechtigungen für Entitäten in Mitgliedskonten, einschließlich jeder Root-Benutzer des AWS-Kontos. Weitere Informationen zu Organizations und SCPs finden Sie unter Funktionsweise von SCPs im AWS Organizations -Benutzerhandbuch.

- Sitzungsrichtlinien:Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen dazu, wie AWS bestimmt, ob eine Anforderung zugelassen werden soll, wenn mehrere Richtlinientypen beteiligt sind, finden Sie unter Logik zur Richtlinienbewertung im IAM-Benutzerhandbuch.

So funktionieren Migration Hub Strategy Recommendations mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf Strategy Recommendations zu verwalten, erfahren Sie, welche IAM-Features Sie mit Strategy Recommendations verwenden können.

IAM-Features, die Sie mit Migration Hub Strategy Recommendations verwenden können

IAM-Feature	Unterstützung für Strategieempfehlungen
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Nein
Bedingungsschlüssel für die Richtlinie	Nein
ACLs	Nein
ABAC (Tags in Richtlinien)	Nein
Temporäre Anmeldeinformationen	Ja

IAM-Feature	Unterstützung für Strategieempfehlungen
Hauptberechtigungen	Ja
Servicerollen	Nein
Serviceverknüpfte Rollen	Ja

Einen Überblick über das Zusammenwirken von Strategy Recommendations und anderen - AWS Services mit den meisten IAM-Funktionen finden Sie unter -AWS Services, die mit IAM funktionieren im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien für Strategy Recommendations

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 Strategy Recommendations

Beispiele für identitätsbasierte Richtlinien für Strategieempfehlungen finden Sie unter Beispiele für identitätsbasierte Richtlinien für Migration Hub Strategy Recommendations.

Ressourcenbasierte Richtlinien in Strategy Recommendations

Unterstützt ressourcenbasierte Richtlinien	Nein

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Prinzipale können Konten, Benutzer, Rollen, Verbundbenutzer oder umfassen AWS-Services.

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource in unterschiedlichen befinden AWS-Konten, muss ein IAM-Administrator im vertrauenswürdigen Konto auch der Prinzipal-Entität (Benutzer oder Rolle) die Berechtigung für den Zugriff auf die Ressource erteilen. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie unter Wie sich IAM-Rollen von ressourcenbasierten Richtlinien unterscheiden im IAM-Benutzerhandbuch.

Richtlinienaktionen für Strategieempfehlungen

Unterstützt Richtlinienaktionen	Ja

Administratoren können AWS JSON-Richtlinien verwenden, um anzugeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben in der Regel 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 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.

Eine Liste der Aktionen für Strategieempfehlungen finden Sie unter Von Migration Hub Strategy Recommendations definierte Aktionen in der Service-Autorisierungs-Referenz.

Richtlinienaktionen in Strategy Recommendations verwenden das folgende Präfix vor der Aktion:

```
migrationhub-strategy
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [
      "migrationhub-strategy:action1",
      "migrationhub-strategy:action2"
         ]
```

Beispiele für identitätsbasierte Richtlinien für Strategieempfehlungen finden Sie unter Beispiele für identitätsbasierte Richtlinien für Migration Hub Strategy Recommendations.

Richtlinienressourcen für Strategy Recommendations

Unterstützt Richtlinienressourcen	Nein

Administratoren können AWS JSON-Richtlinien verwenden, um anzugeben, wer Zugriff auf was 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": "*"
```

Eine Liste der Ressourcentypen von Strategy Recommendations und ihrer ARNs finden Sie unter Von Migration Hub Strategy Recommendations definierte Ressourcen in der Service Authorization Reference . Informationen zu den Aktionen, mit denen Sie den ARN einzelner Ressourcen angeben können, finden Sie unter Von Migration Hub Strategy Recommendations definierte Aktionen.

Beispiele für identitätsbasierte Richtlinien für Strategieempfehlungen finden Sie unter Beispiele für identitätsbasierte Richtlinien für Migration Hub Strategy Recommendations.

Richtlinienbedingungsschlüssel für Strategy Recommendations

Unterstützt servicespezifische Richtlinienbedingungsschlüssel	Nein

Administratoren können AWS JSON-Richtlinien verwenden, um anzugeben, wer Zugriff auf was 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 servicespezifische Bedingungsschlüssel. Informationen zum Anzeigen aller AWS globalen Bedingungsschlüssel finden Sie unter AWS Globale Bedingungskontextschlüssel im IAM-Benutzerhandbuch.

Eine Liste der Bedingungsschlüssel für Strategieempfehlungen finden Sie unter Bedingungsschlüssel für Migration Hub Strategy Recommendations in der Service-Autorisierungs-Referenz. Informationen dazu, mit welchen Aktionen und Ressourcen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von Migration Hub Strategy Recommendations definierte Aktionen.

Beispiele für identitätsbasierte Richtlinien für Strategieempfehlungen finden Sie unter Beispiele für identitätsbasierte Richtlinien für Migration Hub Strategy Recommendations.

Zugriffssteuerungslisten (ACLs) in Strategy Recommendations

Unterstützt ACLs	Nein

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Attributbasierte Zugriffskontrolle (ABAC) mit Strategieempfehlungen

Unterstützt ABAC (Tags in Richtlinien)	Nein

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 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 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.

Verwenden temporärer Anmeldeinformationen mit Strategieempfehlungen

Unterstützt temporäre Anmeldeinformationen	Ja

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich der , die mit temporären Anmeldeinformationen AWS-Services funktionieren, finden Sie unter AWS-Services , die mit IAM funktionieren im IAM-Benutzerhandbuch.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich AWS Management Console mit einer anderen Methode als einem Benutzernamen und einem Passwort bei der anmelden. Wenn Sie beispielsweise AWS über den SSO-Link (Single Sign-On) Ihres Unternehmens auf 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 temporäre Anmeldeinformationen manuell mit der AWS CLI oder der AWS API erstellen. Sie können diese temporären Anmeldeinformationen dann verwenden, um auf zuzugreifen AWS. AWS empfohlen, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

Serviceübergreifende Prinzipalberechtigungen für Strategy Recommendations

Unterstützt Forward Access Sessions (FAS)	Ja

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen in auszuführen AWS, gelten Sie als Prinzipal. Bei einigen Services könnte es Aktionen geben, die dann eine andere

Aktion in einem anderen Service auslösen. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anforderung AWS-Service , Anforderungen an nachgelagerte Services zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Service eine Anfrage erhält, die Interaktionen mit anderen AWS-Services oder -Ressourcen erfordert. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für Strategy Recommendations

Unterstützt Servicerollen	Nein

Eine Servicerolle ist eine IAM-Rolle, die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

> **Warning**
>
> Das Ändern der Berechtigungen für eine Servicerolle könnte die Funktionalität von Strategy Recommendations beeinträchtigen. Bearbeiten Sie Servicerollen nur, wenn Strategy Recommendations dazu Anleitungen gibt.

Serviceverknüpfte Rollen für Strategy Recommendations

Unterstützt serviceverknüpfte Rollen	Ja

Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einem verknüpft ist AWS-Service. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem angezeigt AWS-Konto und gehören dem Service. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Weitere Informationen zum Erstellen oder Verwalten von serviceverknüpften Rollen für Strategieempfehlungen finden Sie unter Verwenden von serviceverknüpften Rollen für Strategieempfehlungen.

AWS verwaltete Richtlinien für Strategieempfehlungen für den Migration Hub

Um Benutzern, Gruppen und Rollen Berechtigungen hinzuzufügen, ist es einfacher, AWS verwaltete Richtlinien zu verwenden, als Richtlinien selbst zu schreiben. Es erfordert Zeit und Fachwissen, um von Kunden verwaltete IAM-Richtlinien zu erstellen, die Ihrem Team nur die benötigten Berechtigungen bieten. Um schnell loszulegen, können Sie unsere AWS verwalteten Richtlinien verwenden. Diese Richtlinien decken allgemeine Anwendungsfälle ab und sind in Ihrem AWS-Konto verfügbar. Weitere Informationen zu AWS verwalteten Richtlinien finden Sie im IAM-Benutzerhandbuch unter AWS Verwaltete Richtlinien.

AWS Dienste verwalten und aktualisieren AWS verwaltete Richtlinien. Sie können die Berechtigungen in AWS verwalteten Richtlinien nicht ändern. Dienste fügen einer AWS verwalteten Richtlinie gelegentlich zusätzliche Berechtigungen hinzu, um neue Funktionen zu unterstützen. Diese Art von Update betrifft alle Identitäten (Benutzer, Gruppen und Rollen), an welche die Richtlinie angehängt ist. Es ist sehr wahrscheinlich, dass Dienste eine AWS verwaltete Richtlinie aktualisieren, wenn eine neue Funktion eingeführt wird oder wenn neue Operationen verfügbar werden. Dienste entfernen keine Berechtigungen aus einer AWS verwalteten Richtlinie, sodass durch Richtlinienaktualisierungen Ihre bestehenden Berechtigungen nicht beeinträchtigt werden.

AWS Unterstützt außerdem verwaltete Richtlinien für Jobfunktionen, die sich über mehrere Dienste erstrecken. Die ReadOnlyAccess AWS verwaltete Richtlinie bietet beispielsweise schreibgeschützten Zugriff auf alle AWS Dienste und Ressourcen. Wenn ein Dienst eine neue Funktion startet, werden nur Leseberechtigungen für neue Operationen und Ressourcen AWS hinzugefügt. Eine Liste und Beschreibungen der Richtlinien für Auftragsfunktionen finden Sie in Verwaltete AWS -Richtlinien für Auftragsfunktionen im IAM-Leitfaden.

AWS verwaltete Richtlinie: AWSMigrationHubStrategyConsoleFullAccess

Sie können die `AWSMigrationHubStrategyConsoleFullAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Die `AWSMigrationHubStrategyConsoleFullAccess` Richtlinie gewährt einem Benutzer vollen Zugriff auf den Strategy Recommendations-Service über die AWS Management Console.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `discovery`— Gewährt dem Benutzer Zugriff auf den Abruf einer Discovery-Zusammenfassung im Application Discovery Service.
- `iam`— Ermöglicht die Erstellung einer dienstbezogenen Rolle für den Benutzer. Dies ist eine Voraussetzung für die Verwendung von Strategy Recommendations.
- `migrationhub-strategy`— Gewährt dem Benutzer vollen Zugriff auf Strategy Recommendations.
- `s3`— Ermöglicht dem Benutzer, die von Strategy Recommendations verwendeten S3-Buckets zu erstellen und aus ihnen zu lesen.
- `secretsmanager`— Ermöglicht dem Benutzer, den Zugriff auf geheime Daten im Secrets Manager aufzulisten.

Die Berechtigungen für diese Richtlinie finden Sie AWSMigrationHubStrategyConsoleFullAccessim Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: AWSMigrationHubStrategyCollector

Sie können die `AWSMigrationHubStrategyCollector`-Richtlinie an Ihre IAM-Identitäten anfügen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `application-transformation`— Erteilt Berechtigungen zum Hochladen von Protokoll- und Metrikdaten für Operationen zur Anwendungstransformation und zur Arbeit mit Portierungskompatibilitätsbewertungen und Empfehlungen.
- `execute-api`— Ermöglicht dem Benutzer den Zugriff auf Amazon API Gateway, um Protokolle und Metriken hochzuladen AWS.
- `migrationhub-strategy`— Gewährt dem Benutzer Zugriff zum Registrieren von Nachrichten, Senden von Nachrichten, Hochladen von Protokolldaten und Hochladen von Metrikdaten in Strategy Recommendations.

- `s3`— Gewährt dem Benutzer Zugriff auf Listenbereiche und deren Standorte. Benutzern wird außerdem Zugriff auf die von Strategy Recommendations verwendeten S3-Buckets gewährt, sie können Objekte abrufen, Objekte hinzufügen, deren Zugriffskontrollliste (ACL) zurückgeben, sie erstellen, darauf zugreifen, die Verschlüsselung für konfigurieren, die `PublicAccessBlock` Konfiguration ändern, den Versionsstatus für festlegen und eine Lebenszykluskonfiguration für die von Strategy Recommendations verwendeten S3-Buckets erstellen oder ersetzen.
- `secretsmanager`— Ermöglicht dem Benutzer den Zugriff auf Geheimnisse im Secrets Manager, die von Strategy Recommendations verwendet werden.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie AWSMigrationHubStrategyCollectorim Referenzhandbuch für AWS verwaltete Richtlinien.

Strategieempfehlungen und Aktualisierungen AWS verwalteter Richtlinien

Hier finden Sie Informationen zu Aktualisierungen der AWS verwalteten Richtlinien für Strategy Recommendations, seit dieser Service begonnen hat, diese Änderungen nachzuverfolgen. Wenn Sie automatische Benachrichtigungen über Änderungen an dieser Seite erhalten möchten, abonnieren Sie den RSS-Feed auf der Seite mit dem Verlauf des Strategieempfehlungsdokuments.

Änderung	Beschreibung	Datum
AWSMigrationHubStrategyCollector – Aktualisierung auf eine bestehende Richtlinie	Diese Richtlinie wurde aktualisiert und umfasst nun die Aktionen`PutLogDat a` , `StartPort ingCompatibilityAs sessment` `GetPortin gCompatibilityAsse ssment` , `StartPort ingRecommendationA ssessment` und `GetPortingRecommen dationAssessment` Anwendungstransformation,	1. April 2024

Änderung	Beschreibung	Datum
	damit der Anwendung stransformationsdienst Protokolle und Metriken an den Dienst senden kann. Die `ListBucket` und `GetBucketLocation` wurden für Amazon Simple Storage Service (Amazon S3) hinzugefügt, um Protokoll- und Metrik-Uploads zu unterstüt zen. Die beiden `PutLogDat a` `PutMetricData` wurden auch hinzugefügt, damit der Strategy Recommendations-Collector Logs und Metriken an den Endpunkt des Services senden kann.	

Änderung	Beschreibung	Datum
AWSMigrationHubStrategyCollector – Aktualisierung auf eine bestehende Richtlinie	Diese Richtlinie wurde mit den `PutLogData` Aktionen `PutMetricData` und aktualisiert. Diese Aktionen ermöglichen das Hochladen von Protokoll- und Metrikdaten für Vorgänge zur Anwendung stransformation. Dieses Update fügt auch Bedingung en hinzu, um sicherzustellen, `aws:ResourceAccount` dass die der Genehmigung `aws:PrincipalAccount` zur Nutzung des enthalten en Amazon Simple Storage Service und der entsprech enden AWS Secrets Manager Aktionen entsprechen.	5. Februar 2024
AWSMigrationHubStrategyCollector – Aktualisierung auf eine bestehende Richtlinie	Diese Richtlinie wurde mit den folgenden Amazon S3 S3-APIs aktualisiert — `CreateBucket PutEncryp tionConfi guration ,PutBucket PublicAcc essBlock ,PutBucket Policy ,PutBucket Versioning , undPutLifecycleConfig uration .`	15. September 2023

Änderung	Beschreibung	Datum
AWSMigrationHubStrategyCollector – Aktualisierung auf eine bestehende Richtlinie	Diese Aktualisierung der Richtlinie gewährt Berechtigungen, die die Analyse des Quellcodes ermöglichen.	08. März 2023
AWSMigrationHubStrategyConsoleFullAccess – Aktualisierung auf eine bestehende Richtlinie	Diese Richtlinie wurde mit drei AWS Application Discovery Service APIs aktualisiert — `DescribeConfigurations DescribeTags` , und`ListConfigurations` .	10. November 2022
AWSMigrationHubStrategyCollector – Aktualisierung auf eine bestehende Richtlinie	Diese Richtlinie wird mit der `UpdateCollectorConfiguration` Aktion aktualisiert. Diese Aktion speichert die Konfiguration Ihres Collectors für einen einfachen Abruf.	07. September 2022
AWSMigrationHubStrategyConsoleFullAccess— Neue Richtlinie wird beim Start veröffentlicht	`AWSMigrationHubStrategyConsoleFullAccess` gewährt einem Benutzer vollen Zugriff auf den Strategy Recommendations-Service über die AWS Management Console.	25. Oktober 2021

Änderung	Beschreibung	Datum
AWSMigrationHubStrategyCollector— Neue Richtlinie wird beim Start verfügbar gemacht	`AWSMigrationHubStrategyCollector` gewährt einem Benutzer Zugriff auf den Strategy Recommendations-Service und Lese-/Schreibzugriff auf die S3-Buckets, die sich auf den Dienst beziehen. Es gewährt auch Amazon API Gateway Gateway-Zugriff zum Hochladen von Protokollen und Metriken sowie AWS Secrets Manager Manager-Zugriff zum Abrufen von Anmeldeinformationen. AWS	25. Oktober 2021
AWSMigrationHubStrategyServiceRolePolicy— Neue Richtlinie wird beim Start zur Verfügung gestellt	Die `AWSMigrationHubStrategyServiceRolePolicy` servicebezogene Rollenrichtlinie bietet Zugriff auf AWS Migration Hub und AWS Application Discovery Service. Diese Richtlinie gewährt auch Berechtigungen zum Speichern von Berichten in Amazon Simple Storage Service (Amazon S3).	25. Oktober 2021
Strategy Recommendations begann, Änderungen nachzuverfolgen	Strategy Recommendations begann, Änderungen an den AWS verwalteten Richtlinien nachzuverfolgen.	25. Oktober 2021

Beispiele für identitätsbasierte Richtlinien für Migration Hub Strategy Recommendations

Benutzer und Rollen haben standardmäßig nicht die Berechtigung, Ressourcen für Strategieempfehlungen zu erstellen oder zu ändern. 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 Aktionen und Ressourcentypen, die durch Strategieempfehlungen definiert werden, einschließlich des Formats der ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Migration Hub Strategy Recommendations in der Service Authorization Reference.

Themen

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand Strategy Recommendations-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 verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen – Um Ihren Benutzern und Workloads Berechtigungen zu erteilen, verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele häufige Anwendungsfälle 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 für Ihre Anwendungsfälle spezifisch 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 Service-Aktionen zu gewähren, wenn sie über eine bestimmte verwendet werden AWS-Service, z. B. AWS CloudFormation. 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 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.

Verwenden der Konsole für Strategieempfehlungen

Um auf die Migration Hub Strategy Recommendations-Konsole zugreifen zu können, müssen Sie über einen Mindestsatz von Berechtigungen verfügen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den Ressourcen für Strategieempfehlungen in Ihrem aufzulisten und anzuzeigen AWS-Konto. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Für Benutzer, die nur Aufrufe an die AWS CLI oder die AWS API durchführen, müssen Sie keine Mindestberechtigungen für die Konsole erteilen. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die die Benutzer ausführen möchten.

Um sicherzustellen, dass Benutzer und Rollen weiterhin die Konsole für Strategieempfehlungen verwenden können, fügen Sie den Entitäten auch die Strategieempfehlungen `ConsoleAccess` oder die `ReadOnly` AWS verwaltete Richtlinie hinzu. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie enthält Berechtigungen zum Ausführen dieser Aktion auf der -Konsole oder programmgesteuert mithilfe der - AWS CLI oder AWS -API.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
```

```
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Zugreifen auf einen Amazon-S3-Bucket

In diesem Beispiel möchten Sie einem IAM-Benutzer in Ihrem AWS-Konto Zugriff auf einen Ihrer Amazon S3-Buckets gewähren, `examplebucket`. Sie möchten dem Benutzer außerdem Berechtigungen zum Hinzufügen, Aktualisieren und Löschen von Objekten gewähren.

Zusätzlich zum Erteilen der Berechtigungen `s3:PutObject`, `s3:GetObject` und `s3:DeleteObject` für den Benutzer, gewährt die Richtlinie die Berechtigungen `s3:ListAllMyBuckets`, `s3:GetBucketLocation` und `s3:ListBucket`. Dies sind die zusätzlichen Berechtigungen, die von der Konsole benötigt werden. Außerdem sind die Aktionen `s3:PutObjectAcl` und `s3:GetObjectAcl` erforderlich, um Objekte in der Konsole kopieren, ausschneiden und einfügen zu können. Eine Beispielanleitung, die Benutzern Berechtigungen erteilt und sie mithilfe der Konsole testet, finden Sie unter Eine Beispielanleitung: Verwenden von Benutzerrichtlinien zur Steuerung des Zugriffs auf Ihren Bucket.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"ListBucketsInConsole",
         "Effect":"Allow",
         "Action":[
            "s3:ListAllMyBuckets"
         ],
         "Resource":"arn:aws:s3:::*"
```

```
      },
      {
         "Sid":"ViewSpecificBucketInfo",
         "Effect":"Allow",
         "Action":[
            "s3:ListBucket",
            "s3:GetBucketLocation"
         ],
         "Resource":"arn:aws:s3:::examplebucket"
      },
      {
         "Sid":"ManageBucketContents",
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
            "s3:PutObjectAcl",
            "s3:GetObject",
            "s3:GetObjectAcl",
            "s3:DeleteObject"
         ],
         "Resource":"arn:aws:s3:::examplebucket/*"
      }
   ]
}
```

Fehlerbehebung bei Identität und Zugriff auf Migration Hub Strategy Recommendations

Verwenden Sie die folgenden Informationen, um häufige Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit Strategy Recommendations und IAM auftreten können.

Themen

- Ich bin nicht autorisiert, eine Aktion in Strategy Recommendations auszuführen
- Ich bin nicht autorisiert, iam durchzuführen:PassRole
- Ich möchte meine Zugriffsschlüssel anzeigen
- Ich bin Administrator und möchte anderen Zugriff auf Strategy Recommendations gewähren
- Ich möchte Personen außerhalb meines AWS-Konto Zugriff auf meine Ressourcen für Strategieempfehlungen gewähren

Ich bin nicht autorisiert, eine Aktion in Strategy Recommendations auszuführen

Wenn die Ihnen AWS Management Console mitteilt, dass Sie nicht zur Ausführung einer Aktion autorisiert sind, müssen Sie sich an Ihren Administrator wenden, um Unterstützung zu erhalten. Ihr Administrator ist die Person, die Ihnen Ihren Benutzernamen und Ihr Passwort bereitgestellt hat.

Der folgende Beispielfehler tritt auf, wenn der `mateojackson` IAM-Benutzer versucht, die Konsole zum Anzeigen von Details zu einer fiktiven *`my-example-widget`*-Ressource zu verwenden, jedoch nicht über `migrationhub-strategy:`*`GetWidget`*-Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 migrationhub-strategy:GetWidget on resource: my-example-widget
```

In diesem Fall bittet Mateo seinen Administrator um die Aktualisierung seiner Richtlinien, um unter Verwendung der Aktion *`my-example-widget`* auf die Ressource `migrationhub-strategy:`*`GetWidget`* zugreifen zu können.

Ich bin nicht autorisiert, iam durchzuführen:PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zur Ausführung der `iam:PassRole` Aktion autorisiert sind, müssen Ihre Richtlinien aktualisiert werden, um eine Rolle an Strategy Recommendations übergeben zu können.

Einige AWS-Services ermöglichen es Ihnen, eine vorhandene Rolle an diesen Service zu übergeben, anstatt eine neue Servicerolle oder serviceverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in Strategy Recommendations auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen odzur Verfügung gestellt.

Ich möchte meine Zugriffsschlüssel anzeigen

Nachdem Sie Ihre IAM-Benutzerzugriffsschlüssel erstellt haben, können Sie Ihre Zugriffsschlüssel-ID jederzeit anzeigen. Sie können Ihren geheimen Zugriffsschlüssel jedoch nicht erneut anzeigen. Wenn Sie den geheimen Zugriffsschlüssel verlieren, müssen Sie ein neues Zugriffsschlüsselpaar erstellen.

Zugriffsschlüssel bestehen aus zwei Teilen: einer Zugriffsschlüssel-ID (z. B. `AKIAIOSFODNN7EXAMPLE`) und einem geheimen Zugriffsschlüssel (z. B. `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`). Ähnlich wie bei Benutzernamen und Passwörtern müssen Sie die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel zusammen verwenden, um Ihre Anforderungen zu authentifizieren. Verwalten Sie Ihre Zugriffsschlüssel so sicher wie Ihren Benutzernamen und Ihr Passwort.

> **Important**
>
> Geben Sie Ihre Zugriffsschlüssel nicht an Dritte weiter, auch nicht für die Suche nach Ihrer kanonischen Benutzer-ID. Auf diese Weise können Sie jemandem permanenten Zugriff auf Ihr gewähren AWS-Konto.

Während der Erstellung eines Zugriffsschlüsselpaars werden Sie aufgefordert, die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel an einem sicheren Speicherort zu speichern. Der geheime Zugriffsschlüssel ist nur zu dem Zeitpunkt verfügbar, an dem Sie ihn erstellen. Wenn Sie Ihren geheimen Zugriffsschlüssel verlieren, müssen Sie Ihrem IAM-Benutzer neue Zugriffsschlüssel hinzufügen. Sie können maximal zwei Zugriffsschlüssel besitzen. Wenn Sie bereits zwei Zugriffschlüssel besitzen, müssen Sie ein Schlüsselpaar löschen, bevor Sie ein neues erstellen. Anweisungen hierfür finden Sie unter Verwalten von Zugriffsschlüsseln im IAM-Benutzerhandbuch.

Ich bin Administrator und möchte anderen Zugriff auf Strategy Recommendations gewähren

Um anderen Personen oder einer Anwendung Zugriff auf Strategy Recommendations zu gewähren, müssen Sie eine IAM-Entität (Benutzer oder Rolle) für die Person oder Anwendung erstellen, die Zugriff benötigt. Sie werden die Anmeldeinformationen für diese Einrichtung verwenden, um auf AWS zuzugreifen. Anschließend müssen Sie der Entität eine Richtlinie anfügen, die dieser die richtigen Berechtigungen in Strategy Recommendations gewährt.

Informationen zum Einstieg finden Sie unter Erstellen Ihrer ersten delegierten IAM-Benutzer und -Gruppen im IAM-Benutzerhandbuch.

Ich möchte Personen außerhalb meines AWS-Konto Zugriff auf meine Ressourcen für Strategieempfehlungen gewähren

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Im Fall von Services, die ressourcenbasierte Richtlinien oder Zugriffssteuerungslisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen dazu, ob Strategy Recommendations diese Funktionen unterstützt, finden Sie unter So funktionieren Migration Hub Strategy Recommendations mit IAM.
- Informationen zum Gewähren des Zugriffs auf Ihre AWS-Konten -Ressourcen in Ihrem Besitz finden Sie unter Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen AWS-Konto , das Sie besitzen im IAM-Benutzerhandbuch.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre -Ressourcen gewähren AWS-Konten, finden Sie unter Gewähren von Zugriff auf im AWS-Konten Besitz von Dritten im IAM-Benutzerhandbuch.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.

Verwenden von serviceverknüpften Rollen für Strategieempfehlungen

Migration Hub Strategy Recommendations verwendet AWS Identity and Access Management (IAM) serviceverknüpfte Rollen. Eine serviceverknüpfte Rolle ist eine einzigartige Art von IAM-Rolle, die direkt mit Strategy Recommendations verknüpft ist. Serviceverknüpfte Rollen werden von Strategy Recommendations vordefiniert und schließen alle Berechtigungen ein, die der Service zum Aufrufen anderer - AWS Services in Ihrem Namen erfordert.

Eine serviceverknüpfte Rolle vereinfacht die Einrichtung von Strategy Recommendations, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Strategy Recommendations definiert die Berechtigungen seiner serviceverknüpften Rollen. Sofern keine andere Konfiguration festgelegt wurde, können nur Strategy Recommendations die Rollen übernehmen. Die definierten

Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Informationen zu anderen Services, die serviceverknüpfte Rollen unterstützen, finden Sie unter AWS Services, die mit IAM funktionieren. Suchen Sie nach den Services, für die Ja in der Spalte Serviceverknüpfte Rolle angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Berechtigungen von serviceverknüpften Rollen für Strategy Recommendations

Strategy Recommendations verwendet die serviceverknüpfte Rolle namens AWSServiceRoleForMigrationHubStrategy und ordnet sie der AWSMigrationHubStrategyServiceRolePolicy IAM-Richtlinie zu – Bietet Zugriff auf AWS Migration Hub und AWS Application Discovery Service. Diese Richtlinie gewährt auch Berechtigungen zum Speichern von Berichten in Amazon Simple Storage Service (Amazon S3).

Die serviceverknüpfte Rolle AWSServiceRoleForMigrationHubStrategy vertraut darauf, dass die folgenden Services die Rolle annehmen:

- `migrationhub-strategy.amazonaws.com`

Die Rollenberechtigungsrichtlinie ermöglicht es Strategy Recommendations, die folgenden Aktionen durchzuführen.

AWS Application Discovery Service -Aktionen

```
discovery:ListConfigurations

discovery:DescribeConfigurations
```

AWS Migration Hub -Aktionen

```
mgh:GetHomeRegion
```

Amazon-S3-Aktionen

```
s3:GetBucketAcl

s3:GetBucketLocation

s3:GetObject
```

```
s3:ListAllMyBuckets

s3:ListBucket

s3:PutObject

s3:PutObjectAcl
```

Informationen zum Anzeigen der Berechtigungen für diese Richtlinie finden Sie unter AWSMigrationHubStrategyServiceRolePolicy im AWS Referenzhandbuch zu verwalteten Richtlinien.

Den Aktualisierungsverlauf dieser Richtlinie finden Sie unter Strategieempfehlungen und Aktualisierungen AWS verwalteter Richtlinien.

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 Rollenberechtigungen im IAM-Benutzerhandbuch.

Erstellen einer serviceverknüpften Rolle für Strategy Recommendations

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie damit einverstanden sind, Migration Hub zu erlauben, eine serviceverknüpfte Rolle (SLR) in Ihrem Konto in der zu erstellen AWS Management Console, erstellt Strategy Recommendations die serviceverknüpfte 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 damit einverstanden sind, Migration Hub zu erlauben, eine serviceverknüpfte Rolle (SLR) in Ihrem Konto zu erstellen, erstellt Strategy Recommendations die serviceverknüpfte Rolle erneut für Sie.

Bearbeiten einer serviceverknüpften Rolle für Strategieempfehlungen

Strategy Recommendations erlaubt es Ihnen nicht, die AWSServiceRoleForMigrationHubStrategy serviceverknüpfte Rolle zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können die Beschreibung der Rolle jedoch mithilfe der Konsole für Strategieempfehlungen, der CLI oder der API bearbeiten.

Löschen einer serviceverknüpften Rolle für Strategy Recommendations

So löschen Sie die serviceverknüpfte Rolle mit IAM

Verwenden Sie die IAM-Konsole, die oder die - AWS API AWS CLI, um die AWSServiceRoleForMigrationHubStrategy serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Leitfaden.

Beim Löschen von Strategy Recommendations-Ressourcen, die von der AWSServiceRoleForMigrationHubStrategy SLR verwendet werden, können Sie keine laufenden Bewertungen (Aufgaben zum Generieren von Empfehlungen) haben. Es können auch keine Hintergrundbewertungen durchgeführt werden. Wenn Bewertungen ausgeführt werden, schlägt das Löschen der SLR in der IAM-Konsole fehl. Wenn der SLR-Löschvorgang fehlschlägt, können Sie den Löschvorgang wiederholen, nachdem alle Hintergrundaufgaben abgeschlossen sind. Sie müssen keine erstellten Ressourcen bereinigen, bevor Sie die SLR löschen.

Unterstützte Regionen für serviceverknüpfte Rollen mit Strategy Recommendations

Strategy Recommendations unterstützt die Verwendung von serviceverknüpften Rollen in allen Regionen, in denen der Service verfügbar ist. Weitere Informationen finden Sie unter AWS Regionen und Endpunkte.

Migrations-Hub-Strategieempfehlungen und Schnittstellen-VPC-Endpunkte (AWS PrivateLink)

Sie können eine private Verbindung zwischen Ihrer VPC und Migration Hub Hub-Strategieempfehlungen herstellen, indem Sie einenSchnittstellen-VPC-Endpunktaus. Schnittstellenendpunkte werden von unterstütz AWS PrivateLink. mitAWS PrivateLinkSie können privat auf Strategy Recommendations-API-Operationen ohne Internet-Gateway, NAT-Gerät, VPN-Verbindung oderAWS Direct Connect-Verbindung. Die Instances in Ihrer VPC benötigen für die Kommunikation mit Strategy Recommendations-API-Operationen keine öffentlichen IP-Adressen. Der Datenverkehr zwischen Ihrer VPC und Strategy Recommendations bleibt im Amazon-Netzwerk.

Jeder Schnittstellenendpunkt wird durch eine oder mehrere Elastic Network-Schnittstellen in Ihren Subnetzen dargestellt.

Weitere Informationen finden Sie unterSchnittstellen-VPC-Endpunkte (AWS PrivateLink)imAmazon VPC User Guideaus.

Überlegungen zu Strategieempfehlungen VPC-Endpunkte

Bevor Sie einen Schnittstellen-VPC-Endpunkt für Strategieempfehlungen einrichten, stellen Sie sicher, dass Sie die Überprüfung einsehenEigenschaften und Beschränkungen von SchnittstellenendpunktenundAWS PrivateLinkQuotenimAmazon VPC User Guideaus.

Strategieempfehlungen unterstützen Aufrufe all seiner API-Aktionen aus der VPC. Um alle Strategieempfehlungen verwenden zu können, müssen Sie einen VPC-Endpunkt erstellen.

Erstellen eines Schnittstellen-VPC-Endpunkts für Strategieempfehlungen

Sie können einen VPC-Endpunkt für Strategieempfehlungen mithilfe der Amazon-VPC-Konsole oder derAWS Command Line Interface(AWS CLI) enthalten. Weitere Informationen finden Sie unter Erstellung eines Schnittstellenendpunkts im Benutzerhandbuch für Amazon VPC.

Erstellen Sie einen VPC-Endpunkt für Strategieempfehlungen mit dem folgenden Servicenamen:

- `com.amazonaws.region.migrationhub-strategy`

Wenn Sie einen privaten DNS für den Endpunkt verwenden, können Sie mit seinem standardmäßigen DNS-Namen für die -Region API-Anforderungen an senden. Sie können beispielsweise den Namen verwenden`migrationhub-strategy.us-east-1.amazonaws.com`aus.

Weitere Informationen finden Sie unter Zugriff auf einen Service über einen Schnittstellenendpunkt im Benutzerhandbuch für Amazon VPC.

Erstellen einer VPC-Endpunktrichtlinie für Strategieempfehlungen

Sie können eine Endpunktrichtlinie an Ihren VPC-Endpunkt anhängen, der den Zugriff auf Strategieempfehlungen steuert. Die Richtlinie gibt die folgenden Informationen an:

- Prinzipal, der die Aktionen ausführen kann
- Aktionen, die ausgeführt werden können
- Die Ressourcen, für die diese Aktionen ausgeführt werden können.

Weitere Informationen finden Sie unter Steuerung des Zugriffs auf Services mit VPC-Endpunkten im Amazon-VPC-Benutzerhandbuch.

Beispiel: VPC-Endpunktrichtlinie für Strategieempfehlungsmaßnahmen

Im Folgenden finden Sie ein Beispiel für eine Endpunktrichtlinie für Strategieempfehlungen. Wenn diese Richtlinie an einen Endpunkt angefügt wird, gewährt sie Zugriff auf die aufgelisteten Strategieempfehlungsaktionen für alle Prinzipale auf allen Ressourcen.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "migrationhub-strategy:ListContacts",
         ],
         "Resource":"*"
      }
   ]
}
```

Konformitätsprüfung der Strategieempfehlungen für den Migration Hub

Informationen darüber, ob AWS-Service ein AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter 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.

Arbeiten mit anderen Services

In diesem Abschnitt werden andere beschriebenAWSDienste, die mit Migration Hub Hub-Strategieempfehlungen interagieren.

Themen

- Protokollierung von -API-Aufrufen mitAWS CloudTrail

Protokollierung von -API-Aufrufen mitAWS CloudTrail

Migration Hub Hub-Strategieempfehlungen sind integriert mitAWS CloudTrail, ein Service, der die Aktionen eines Benutzers, einer Rolle oder einesAWSService in Strategieempfehlungen. CloudTrail erfasst alle API-Aufrufe für Strategieempfehlungen als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der Strategy Recommendations-Konsole und Code-Aufrufe der -API-Operationen.

Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail-Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für Strategieempfehlungen. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse in der CloudTrail-Konsole trotzdem im Ereignisverlauf anzeigen. Anhand der von CloudTrail erfassten Informationen können Sie feststellen, welche Anforderung an Strategieempfehlungen gesendet wurde, die IP-Adresse, von der die Anfrage gestellt wurde, den Absenden und den Zeitpunkt der Anforderung sowie weitere Details.

Weitere Informationen zu CloudTrail finden Sie im AWS CloudTrail-Benutzerhandbuch.

Informationen zu Strategieempfehlungen in CloudTrail

CloudTrail ist auf IhremAWS-Kontowenn Sie das -Konto anlegen. Die in Strategieempfehlungen auftretenden Aktivitäten werden als CloudTrail-Ereignis zusammen mit anderen aufgezeichnetAWSService-Ereignisse inEreignisverlauf deraus. Sie können aktuelle Ereignisse in IhremAWS-Kontoaus. Weitere Informationen finden Sie unterAnzeigen von Ereignissen mit CloudTrail Ereignisverlaufaus.

Zur kontinuierlichen Aufzeichnung von Ereignissen in IhremAWS-KontoErstellen Sie einen Trail, einschließlich Ereignissen für Strategieempfehlungen. Ein Trail ermöglicht es CloudTrail, Protokolldateien in einem Amazon-S3-Bucket bereitzustellen. Wenn Sie einen Pfad in der Konsole anlegen, gilt dieser standardmäßig für alleAWS-Regionenaus. Der Trail protokolliert Ereignisse aus

allen Regionen in der AWS-Partition und stellt die Protokolldateien in dem Amazon-S3-Bucket bereit, den Sie angeben. 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 von mehreren Konten.

Strategieempfehlungen unterstützen die Protokollierung der folgenden Aktionen als Ereignisse in CloudTrail-Protokolldateien:

- getApplicationComponentStrategies
- getApplicationComponentDetails
- getAssesment
- GetImportFileTask
- getPortfoliopReferences
- getPortfolioSummary
- getServerDetails
- GetServerStrategies
- listApplicationComponents
- ListCollectors
- ListImportFileTask
- ListServers
- PutPortfoliopReferences
- StartAssess
- StarTimportFileTask
- StoppBewertung
- updateApplicationComponetConfig
- updateServerConfig

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-Element userIdentity.

Grundlagen zu -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 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 Stack-Trace der öffentlichen API-Aufrufe und erscheinen daher in keiner bestimmten Reihenfolge.

Das folgende Beispiel zeigt einen CloudTrail-Protokolleintrag, der diegetServerDetailsAktion

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "777777777777",
        "arn": "arn:aws:sts::111122223333:assumed-role/myUserName/...",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "777777777777",
                "arn": "arn:aws:iam::111122223333:role/myUserName",
                "accountId": "111122223333",
                "userName": "myUserName"
            },
            "webIdFederationData": {},
```

```
            "attributes": {
                "creationDate": "2021-09-20T01:07:16Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2021-09-20T01:07:43Z",
    "eventSource": "migrationhub-strategy.amazonaws.com",
    "eventName": "GetServerDetails",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "",
    "userAgent": "",
    "requestParameters": {
        "serverId": "ads-server-006"
    },
    "responseElements": null,
    "requestID": "07D681279BD94AED",
    "eventID": "cdc4b7ed-e171-4cef-975a-ad829d4123e8",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Kontingente für Migrations-Hub-Strategieempfehlungen

Das AWS-Konto verfügt über Standardkontingente (früher als Limits bezeichnet) für jeden AWS-Service. Wenn nicht anders angegeben, gilt jedes Kontingent spezifisch für eine Region. Sie können Erhöhungen für einige Kontingente beantragen und andere Kontingente können nicht erhöht werden.

Eine Liste der Kontingente für Migration Hub Hub-Strategieempfehlungen finden Sie unterStrategieempfehlungen Servicekontingenteaus.

Sie können die Kontingente für Strategieempfehlungen auch anzeigen, indem Sie dieKonsole Service Quotas Servicekontingenteaus. Wählen Sie im NavigationsbereichAWSDienstleistungenund SelectMigration Hub Hub-Strategie-Empfehlungenaus.

Informationen zur Erhöhung eines Kontingents finden Sie unter Anfordern einer Kontingenterhöhung im Benutzerhandbuch zu Service Quotas. Wenn das Kontingent unter Service Quotas noch nicht in verfügbar ist, verwenden Sie das Formular zur Erhöhung des Service-Limits.

Versionshinweise

Themen

17. November 2023

Neue Features

- Sammler v1.1.47
- Support für.NET 8-Anwendungen.

12. Oktober 2023

Neue Features

- Collector v1.1.45
- Support für Multi-Datenquellen.

17. April 2023

Neue Features

- Collector v1.1.22
- Verbesserungen am Upgrade-Skript. Dies erfordert die neueste Version von Collector.

17. März 2023

Neues Feature

Es wurde eine binäre Analyse hinzugefügt, die die Erkennung von Anti-Pattern und Inkompatibilitäten ohne Quellcode ermöglicht.

07. November 2022

Neues Feature

- Anwendungsfilterung für Anwendungen
- Serverfilterung nach AWS Application Discovery Service Tags

27. September 2022

Neues Feature

- Collector v1.1.12
  - SCT Ausführung 667
  - EmpAnalyzer 2.2.0.368
- `diag check`Befehle für Server Insights hinzugefügt.
- Unterstützung für potenzielle Empfehlungen hinzugefügt.
- Verbesserte Benutzeroberfläche zur Überprüfung der Konfiguration und des Bewertungsstatus.

Fehlerkorrekturen

- Portierung des Assistenzübersetzers und andere Korrekturen.

30. Juni 2022

Neues Feature

- Collector v1.1.11
  - VMware-API-Unterstützung hinzugefügt.
  - A2C hat beim Herunterladen der Binärdatei Änderungen angefordert, um den Benutzer-Header hinzuzufügen.
  - Linux-Home-Pfad, Standard-Shell und Remote-Terminierung aller Shells hinzugefügt.
- Öffentliche Binärdatei A2C v1.17
  - Unterstützung für Azure DevOps als Ziel für die Pipeline-Bereitstellung wurde hinzugefügt.

18. April 2022

Neues Feature

- Collector v1.1.7
- Es wurde die Möglichkeit hinzugefügt, A2C-Binärdateien dynamisch von der öffentlichen URL herunterzuladen.

Fehlerkorrekturen

- A2C v1.1.5

25. Februar 2022

Fehlerkorrekturen

- SCT v5.6.9
- A2C v1.1.2
- Kollektor v1.1.4

10. Februar 2022

Fehlerkorrekturen

- SCT v5.6.8
- A2C v1.1.1
  - Es wurde eine Prüfung für den tar Befehl unter Linux hinzugefügt.
  - Das Problem beim Überprüfen von Anwendungsbildern in Amazon ECR wurde behoben.
  - Das Problem, bei dem der Container zur Vorvalidierung entfernt werden musste, wurde behoben.
- Collector v1.1.3
  - Der 4xx-Fehler für einen Remote-32-Bit-Computer wurde behoben.
  - Die A2C-Fehlercodes wurden aktualisiert.
  - Die IP-Adresse wurde `C#` für die Quellcode-Analyse des Remote-Computers validiert.

28. Januar 2022

Neues Feature

- Collector v1.1.2
- Unterstützung für Azure DevOps Git Repositorys für die Quellcodeanalyse hinzugefügt.

14. Januar 2022

Neues Feature

- Collector v1.1.1
- Babelfish-Empfehlungen für SQL-Datenbanken hinzugefügt.

21. Dezember 2021

Das Problem wurde behoben

- Collector v1.1.0
- Die Datenbankanalyse wurde wiederhergestellt.

15. Dezember 2021

Bekanntes Problem

- Collector v1.0.4
- Die Datenbankanalyse wird derzeit nicht unterstützt (CVE-2021-44228).

25. Oktober 2021

Neues Feature

- Collector v1.0.0
- Erste Veröffentlichung des Benutzerleitfadens mit den Strategieempfehlungen für den Migration Hub.

Dokument- und Versionshistorie

In der folgenden Tabelle werden die Dokumentationsversionen für Strategieempfehlungen beschrieben. Weitere Informationen finden Sie unter Versionshinweise.

Änderung	Beschreibung	Date (Datum)
AWS verwaltete Richtlinienaktualisierungen — Aktualisierung auf AWSMigrationHubStrategyCollector	Die AWSMigrationHubStrategyCollectorRichtlinie wurde aktualisiert und umfasst nun neue `s3application-transformation` , und `migrationhub-strategy` Aktionen.	1. April 2024
AWS verwaltete Richtlinienaktualisierungen — Aktualisierung auf AWSMigrationHubStrategyCollector	Die AWSMigrationHubStrategyCollectorRichtlinie wurde aktualisiert und umfasst nun neue `application-transformation` Aktionen. Dieses Update fügt auch Bedingungen hinzu, um verschiedene Aktionen einzuschränken, wobei diese Bedingungen den entsprechen `aws:ResourceAccount` müssen`aws:PrincipalAccount` .	5. Februar 2024
Neues Feature	Strategy Recommendations Application Data Collector Client v1.1.47 ist mit Unterstützung für.NET 8-Anwendungen verfügbar.	17. November 2023
Neues Feature	Der Application Data Collector Client v1.1.45 von Strategy	12. Oktober 2023

	Recommendations ist mit Unterstützung für mehrere Datenquellen verfügbar.	
AWS verwaltete Richtlini enaktualisierungen — Update auf AWSMigrationHubStr ategyCollector	Die AWSMigrationHubStr ategyCollectorRichtlinie wurde aktualisiert, um neue Amazon S3 S3-APIs aufzunehmen.	15. September 2023
AWS verwaltete Richtlini enaktualisierungen — Aktualisierung auf AWSMigrat ionHubStrategyCollector	Die AWSMigrationHubStr ategyCollectorRichtlinie wurde aktualisiert und enthält nun neue Analysatoren für den Quellcode.	08. März 2023
Aktualisierungen der bewährten Methoden für IAM	Weitere Informationen finden Sie unter Bewährte IAM-Metho den.	25. Februar 2023
AWS verwaltete Richtlini enaktualisierungen — Aktualisi erung einer bestehenden Richtlinie	Mit den Strategieempfehlun gen von Migration Hub wurden drei AWS Applicati on Discovery Service APIs zu einer bestehenden Richtlinie hinzugefügt.	10. November 2022
Sicherheits-Updates	Stellen Sie eine private Verbindung mit dem VPC-Endpunkt der Schnittstelle her.	07. März 2022
Neues Feature	Unterstützung für Azure DevOps Git Repositorys für die Quellcodeanalyse hinzugefügt.	28. Januar 2022
Neues Feature	Babelfish-Empfehlungen für SQL-Datenbanken hinzugefü gt.	14. Januar 2022

Erstversion	Erste Veröffentlichung des Benutzerleitfadens mit den Strategieempfehlungen für den Migration Hub.	25. Oktober 2021

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.