aws

Benutzerhandbuch

Migration-Hub-Strategieempfehlungen

Migration-Hub-Strategieempfehlungen: Benutzerhandbuch

Table of Contents

Was sind Strategieempfehlungen für den Migration Hub?

Migration-Hub-Strategieempfehlungen unterstützen Sie bei der Planung von Migrations- und Modernisierungsinitiativen mithilfe von Empfehlungen für die Migration- und Modernisierungsstrategie für tragfähige Transformationspfade für Ihre Anwendungen.

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 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 (AWS MGN). 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.
- AWS Anwendungsmigrationsdienst — 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 AWS Service migrieren können.
- AWS App2Container — 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 für

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

- End-of-Support Migrationsprogramm 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 AWS, ohne dass Umgestaltungen erforderlich sind.
- AWS Schema 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/die Anmeldung.
2. Folgen Sie den Online-Anweisungen.

   Während der Anmeldung erhalten Sie einen Telefonanruf oder eine Textnachricht und müssen 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. Als bewährte Sicherheitsmethode weisen Sie einem Administratorbenutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Du kannst jederzeit deine aktuellen Kontoaktivitäten einsehen und dein Konto verwalten, indem du zu https://aws.amazon.com/gehst und Mein Konto auswählst.

Erstellen eines Benutzers 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 eines Benutzers 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 Administratorbenutzer im IAM Identity Center Benutzerzugriff.

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

Anmelden als Administratorbenutzer

- 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 Access-Portal.

Weiteren Benutzern Zugriff zuweisen

1. Erstellen Sie im IAM-Identity-Center einen Berechtigungssatz, der den bewährten Vorgehensweisen für die Anwendung von geringsten Berechtigungen folgt.

   Anweisungen hierzu finden Sie unter Berechtigungssatz erstellen im AWS IAM Identity Center Benutzerhandbuch.
2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

   Eine genaue Anleitung finden Sie unter Gruppen hinzufügen im AWS IAM Identity Center Benutzerhandbuch.

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 Anleitung unter Eine Rolle für einen externen Identitätsanbieter (Verbund) erstellen im IAM-Benutzerhandbuch.

- IAM-Benutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Befolgen Sie die Anleitung unter Eine Rolle für einen IAM-Benutzer erstellen 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 EC2 Amazon-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, 12 SP4 SP5
  - Windows
    - Windows Server 2008 R1 SP2, 2008 R2 SP1
    - Windows Server 2012 R1, 2012 R2
    - Windows Server 2016
    - Windows Server 2019
- Für die Quellcodeanalyse müssen Ihr Repository GitHub und Ihr GitHub Enterprise-Repository über ein persönliches Zugriffstoken im Repo-Bereich verfügen, das mit dem Strategy Recommendations Collector-Client 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

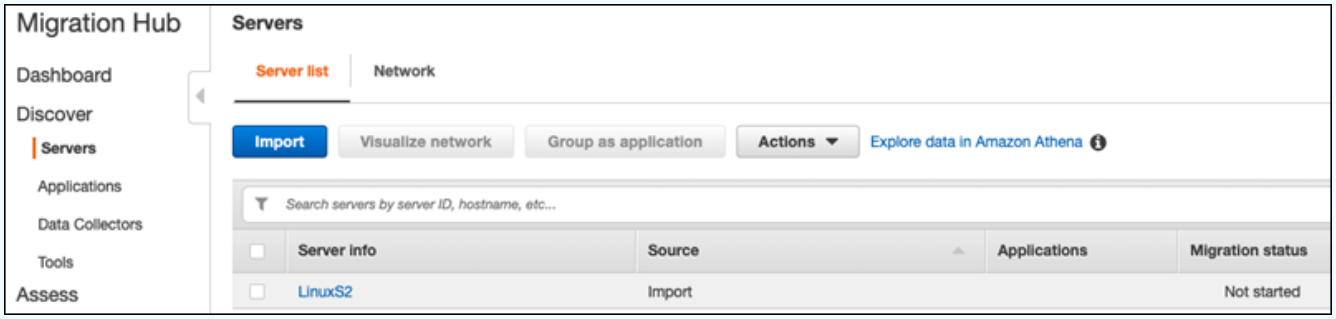
  Um .NET-Repositorys für Empfehlungen von Porting Assistant for .NET zu analysieren, müssen Sie einen Windows-Computer bereitstellen, auf dem das Portierungsbewertungstool von Porting Assistant for .NET installiert ist. Weitere Informationen finden Sie unter Erste Schritte mit Porting Assistant for .NET im Porting Assistant for .NET-Benutzerhandbuch.
- Um Strategieempfehlungen für die Datenbankanalyse zu aktivieren, müssen Sie Anmeldeinformationen 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 VMware virtuelle Maschinen sammelt ()VMs. 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 VMs installieren und die Systeminformationen und Details der Netzwerkverbindungen zwischen Systemen erfasst. 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 EC2 Amazon-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-Konsole an AWS Management Console und öffnen Sie die Migration Hub Hub-Konsole unter https://console.aws.amazon.com/migrationhub/.
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 Anwendungsdatensammler 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) in 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 EC2 Amazon-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 als VMware Administrator bei vCenter 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 EC2 Amazon-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 EC2 Amazon-Instance vom Collector-AMI aus starten.

So stellen Sie die EC2 Collector-Amazon-Instance bereit

1. Öffnen Sie die EC2 Amazon-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 Bilder die Option AMIs.
4. Wählen Sie Öffentliche Bilder aus der Dropdownliste In meinem Besitz 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 EC2 Amazon-Benutzerhandbuch.

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

   Strategieempfehlungen sammeln EC2 Amazon-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 EC2 Amazon-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 als EC2 Amazon-Instance bereitgestellten Collector an

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 WSde3aq1@ ein. Sie müssen das Passwort bei der ersten Anmeldung ändern.

Melden Sie sich bei dem als EC2 Amazon-Instance bereitgestellten Collector an

Um sich beim Strategy Recommendations Collector anzumelden, der als EC2 Amazon-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 EC2 Amazon-Instance vom Collector-AMI aus gestartet haben.

Schritt 4: Den Collector für Strategieempfehlungen einrichten

In diesem Abschnitt wird beschrieben, wie Sie die `collector setup` Befehlszeilenbefehle verwenden, um den Anwendungsdatensammler für Migration Hub Strategy Recommendations zu konfigurieren. Diese Konfigurationen werden lokal gespeichert.

Bevor Sie `collector setup` Befehle verwenden können, müssen Sie mit dem folgenden `docker exec` Befehl eine Bash-Shell-Sitzung im Collector-Docker-Container erstellen.

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

`collector setup`Mit dem Befehl werden alle folgenden Befehle nacheinander ausgeführt, Sie können sie jedoch auch einzeln ausführen:

- `collector setup --aws-configurations`— Richten Sie AWS Konfigurationen ein.
- `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 jedoch die Einrichtung der vCenter-Konfiguration mithilfe des Befehls `collector setup --vcenter-configurations` erzwingen.

- `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 AWS Konfigurationen ein, wie unter beschriebenRichten Sie AWS Konfigurationen ein.
3. Geben Sie die Informationen für vCenter-Konfigurationen ein, wie unter beschriebenvCenter-Konfigurationen einrichten.
4. Geben Sie die Informationen für Remoteserverkonfigurationen ein, wie unter beschriebenRichten Sie Remote-Serverkonfigurationen 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 unter befolgenBereiten Sie Ihre Windows- und Linux-Remote-Server auf die Datenerfassung vor.

Richten Sie AWS Konfigurationen ein

Um AWS Konfigurationen einzurichten, wenn Sie den `collector setup` Befehl oder den `collector setup --aws-configurations` Befehl verwenden.

1. Geben Sie Y für Ja in das Feld Haben Sie IAM-Berechtigungen eingerichtet... ein Frage. Sie haben diese Berechtigungen eingerichtet, als Sie mithilfe der `AWSMigrationHubStrategyCollector` verwalteten Richtlinie einen Benutzer für den Zugriff auf den Collector erstellt haben. Gehen Sie dabei wie unter beschrieben vorStrategie, Empfehlungen, Benutzer und Rollen.
2. Geben Sie Ihren Zugriffsschlüssel und den geheimen Schlüssel aus dem AWS Konto ein, das den Benutzer hat, den Sie für den Zugriff auf den Collector erstellt haben. Gehen Sie dazu wie unter beschrieben 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 unter Strategy Recommendations Endpoints in der Allgemeine AWS-Referenz.
4. Geben Sie J für Ja ein, um den Strategiedienst Upload Collector-bezogene Metriken zum Migration Hub zu erhalten? Frage. Metrikinformationen helfen AWS Ihnen dabei, angemessene Unterstützung zu bieten.
5. Geben Sie Y für Ja ein, um den Strategiedienst Collector-bezogene Logs auf Migration Hub hochladen? Frage. Informationen aus Protokollen helfen AWS Ihnen dabei, angemessene Unterstützung zu bieten.

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

```
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.
```

vCenter-Konfigurationen einrichten

So richten Sie vCenter-Konfigurationen ein, wenn Sie den `collector setup` Befehl oder den `collector setup --vcenter-configurations` Befehl verwenden:

1. Geben Sie Y für Ja in die Frage Möchten Sie sich mit VMware vCenter-Anmeldeinformationen authentifizieren ein, wenn Sie sich mit vCenter-Anmeldeinformationen VMware authentifizieren möchten.

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

   Geben Sie die Host-URL ein, bei der es sich entweder um die vCenter-IP-Adresse oder die URL handeln kann. Geben Sie dann den Benutzernamen und das Passwort für VMware vCenter ein.
2. Geben Sie Y für Ja für die Frage Haben Sie Windows-Maschinen, die von VMware vCenter verwaltet werden, ein, wenn Sie Windows-Server konfigurieren möchten.

   Geben Sie den Benutzernamen und das Passwort für Windows ein.

   > **Note**
   >
   > Wenn Ihr Windows Remote Server zu einer Active Directory-Domäne gehört, müssen Sie den Benutzernamen als*`domain-name`*\ eingeben, *`username`* wenn Sie die CLI verwenden, um Remoteserverkonfigurationen bereitzustellen. Wenn der Name Ihrer Domain beispielsweise exampledomain und Ihr Benutzername Administrator ist, dann ist der Benutzername, den Sie in der CLI eingeben, exampledomain\ Administrator.
3. Geben Sie Y für Ja zur Frage Setup für Linux mit VMware vCenter ein, wenn Sie Linux-Server konfigurieren möchten.

   Geben Sie den Benutzernamen und das Passwort für Linux ein.
4. Geben Sie Y für Ja ein für die Fragen Möchten Sie Anmeldeinformationen für Server außerhalb von vCenter einrichten, die NTLM für Windows und SSH/Cert-basiert für Linux verwenden, wenn Sie Remoteserver-Anmeldeinformationen für Server außerhalb von vCenter einrichten möchten.
5. Geben Sie für die Frage Möchten Sie dieselben Windows-Anmeldeinformationen verwenden, die bei der Einrichtung von vCenter verwendet wurden, Y für Ja ein, 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 N für Nein ein.

Wenn Sie Y mit Ja beantworten, werden die folgenden Fragen gestellt.

a. Geben Sie Y für Ja ein, wenn Collector bei der ersten Interaktion mit Windows-Servern Serverzertifikate akzeptiert und lokal in Ihrem Namen speichert? Frage.

b. Geben Sie 1 für die Frage Geben Sie Ihre Optionen ein, 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 Remote-Serverkonfigurationen ein

So richten Sie Remoteserverkonfigurationen ein, wenn Sie den `collector setup` Befehl oder den `collector setup --remote-server-configurations` Befehl verwenden:

1. Geben Sie Y für Ja in die Frage Möchten Sie Anmeldeinformationen für Server einrichten, die nicht von vCenter mithilfe von NLTM für Windows verwaltet werden, ein, wenn Sie Windows-Server konfigurieren möchten.

   Geben Sie den Benutzernamen und das Passwort für WinRM ein.

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

   Geben Sie Y für Ja ein, wenn Collector bei der ersten Interaktion mit Windows-Servern Serverzertifikate akzeptiert und lokal in Ihrem Namen 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 Y für Ja zur Frage Setup für Linux mit SSH oder Zertifikat ein, wenn Sie Linux-Server konfigurieren möchten.
3. Geben Sie 1 für die Frage Geben Sie Ihre Optionen ein, 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 2 für die Frage Geben Sie Ihre Optionen ein, wenn Sie die zertifikatsbasierte Authentifizierung konfigurieren möchten.

   Informationen zur Einrichtung der zertifikatsbasierten Authentifizierung finden Sie unter. Richten 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

So richten Sie Konfigurationen für die Versionskontrolle ein, wenn Sie den `collector setup` Befehl oder den `collector setup --version-control-configurations` Befehl verwenden:

1. Geben Sie Y für Ja ein, um Quellcodeanalyse einrichten? Frage.

2. Geben Sie 1 für die Frage Geben Sie Ihre Optionen ein, wenn Sie den Git-Serverendpunkt konfigurieren möchten.

   Geben Sie github.com für den GIT-Serverendpunkt ein:.

3. Geben Sie 2 für die Frage Geben Sie Ihre Optionen ein, wenn Sie einen GitHub Enterprise Server konfigurieren möchten.

   Geben Sie den Unternehmensendpunkt ohne https://wie folgt ein: GIT-Serverendpunkt: *git-enterprise-endpoint*

4. Gib deinen Git *username* und deinen persönlichen Zugang ein*token*.

5. Geben Sie Y für Ja ein, um zu Haben Sie irgendwelche Csharp-Repositorys, die auf einem Windows-Computer analysiert werden sollten? Frage, wenn Sie C#-Code analysieren möchten.

   > **Note**
   >
   > Um .NET-Repositorys für 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 unter Erste Schritte mit Porting Assistant for .NET im Porting Assistant for .NET-Benutzerhandbuch.

6. Für das Möchten Sie vorhandene Windows-Anmeldeinformationen auf diesem Computer wiederverwenden? Frage. Geben Sie Y für Ja ein, wenn der Windows-Computer für die C#-Quellcodeanalyse dieselben Anmeldeinformationen verwendet wie die Anmeldeinformationen, die Sie zuvor bei der Einrichtung von `--remote-server-configurations` oder `--vcenter-configurations` angegeben haben.

   Geben Sie N für nein ein, wenn Sie neue Anmeldeinformationen eingeben möchten.

7. Um VMWare vCenter Windows Machine-Anmeldeinformationen zu verwenden, geben Sie 1 für Wählen Sie eine der folgenden Optionen für Windows-Anmeldeinformationen ein.

8. Geben Sie die IP-Adresse für die Windows-Maschine 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 Anwendungsdatensammler von Strategy Recommendations mithilfe von vCenter-Anmeldeinformationen einrichten.

Wenn Sie nach der Einrichtung Ihrer Remoteserverkonfigurationen den `collector setup --remote-server-configurations` Befehl `collector setup command` oder verwenden, müssen Sie Ihre Remoteserver so vorbereiten, dass der Strategy Recommendations-Anwendungsdatensammler 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) AWS für den Fernbetrieb finden Sie im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch.

Informationen zur Vorbereitung Ihrer Remote-Linux-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 Datenerfassungsprogramm 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 id_rsa_assessment.pub generierten öffentlichen Schlüssel aus dem folgenden Ordner im Container:

   /opt/amazon/application-data-collector/remote-auth/linux/keys.
2. Hängen Sie den kopierten öffentlichen Schlüssel an die Datei für alle Remote-Computer an. `$HOME/.ssh/authorized_keys` Wenn keine Datei verfügbar ist, erstellen Sie sie mit dem `vim` Befehl `touch` oder.
3. Vergewissern Sie sich, dass der Basisordner auf dem Remoteserver über eine `755` oder weniger Zugriffsrechte verfügt. Wenn ja`777`, funktioniert es nicht. Sie können den `chmod` Befehl verwenden, um Berechtigungen einzuschränken.

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 muss id_rsa_assessment-cert.pub lauten.
4. Geben Sie beim Einrichtungsschritt 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 der Strategieempfehlungen gesammelt werden können.

Weitere Informationen zu dem PowerShell Skript, das auf dem Remoteserver ausgeführt wird, finden Sie in diesem Hinweis.

Das Skript aktiviert PowerShell Remote und deaktiviert alle Authentifizierungsmethoden außer Negotiate. Dies wird für Windows NT LAN Manager (NTLM) verwendet und setzt das WSMan Protokoll "AllowUnencrypted" auf False, um sicherzustellen, dass der neu erstellte Listener nur verschlüsselten Datenverkehr akzeptiert. Mithilfe des von Microsoft bereitgestellten Skripts `New-SelfSignedCertificateEx.ps1` wird ein selbstsigniertes Zertifikat erstellt.
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 auf Ihrem Server PowerShell installierte Version von zu überprüfen.

   ```
   $PSVersionTable
   ```

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

   ```
   $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 `New-SelfSignedCertificateEx.ps1` von der folgenden URL herunter und fügen Sie das Skript in denselben Ordner ein, in dem 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 das heruntergeladene PowerShell Skript auf allen Anwendungsservern aus.

```
.\WinRMSetup.ps1
```

> **Note**
>
> Wenn Windows Remote Management (WinRM) auf dem Windows-Remoteserver nicht ordnungsgemäß 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 im `-a` Modus verwenden, erhalten Sie die Ausgabe nach Abschluss der Prüfungen in einer DiagnosticCheckResultTXT-Datei.

```
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-Konsole an AWS Management Console und öffnen Sie die Migration Hub Hub-Konsole unter https://console.aws.amazon.com/migrationhub/.
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 VMs gehostete Objekte 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 eingeben können VMs.

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, AWS Discovery 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 erhalten 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-Konsole an AWS Management Console und öffnen Sie die Migration Hub Hub-Konsole unter https://console.aws.amazon.com/migrationhub/.
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 Strategische Empfehlungen, 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.

Strategische Empfehlungen, 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-Konsole an AWS Management Console und öffnen Sie die Migration Hub Hub-Konsole unter https://console.aws.amazon.com/migrationhub/.
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 Strategieempfehlungen für die Migration „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 Zusammenfassung der Empfehlungen können Sie sich die Empfehlungen für die Anwendungskomponente ansehen. 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 Komponententyp aus SQLServerund 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.
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 mithilfe des AWS Schemakonvertierungstools. 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 über zwei Datenbanken (exampledbs1 und exampledbs2) verfügt, 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.

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 Secrets Manager-Konsole an AWS Management Console und

öffnen Sie die AWS Secrets Manager Manager-Konsole 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 - *your-username*

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

   Passwort - *your-password*
5. Wählen Sie Weiter aus.
6. Geben Sie Secret Name als eine beliebige Zeichenfolge mit dem Präfix migrationhub-strategy - ein. 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-Anwendung unter Windows oder die JAR-Dateien der Anwendung DLLs 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-Konsole an AWS Management Console und öffnen Sie die Migration Hub Hub-Konsole unter https://console.aws.amazon.com/migrationhub/.
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, die auf den Empfehlungen basieren, einsehen. 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-Konsole an AWS Management Console und öffnen Sie die Migration Hub Hub-Konsole unter https://console.aws.amazon.com/migrationhub/.
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-Konsole an AWS Management Console und öffnen Sie die Migration Hub Hub-Konsole unter https://console.aws.amazon.com/migrationhub/.
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

Daten, die vom Kollektor für Strategieempfehlungen gesammelt wurden

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 von mehreren OSs
Firmware-Typ	BIOS, UEFI

Datenfeld	Beschreibung
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 MSdtsservr .exe, .exe usw.
Anwendungstyp	IIS JBoss, Tomcat usw.

Datenfeld	Beschreibung
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
Verwendung der Windows-Registrierung	Fragt die Registrierungsschlüssel des Computers ab, um Informationen wie Datenbankversion, Java-Version, .NET-Version usw. zu finden.

Datenfeld	Beschreibung
Alle DLLs werden von der Anwendung verwendet	Ruft die Liste aller zur Laufzeit von einem Windows-Prozess DLLs geladenen Dateien ab.
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.

```
sudo 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 Migrations- und Modernisierungsempfehlungen 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-Konsole an AWS Management Console und öffnen Sie die Migration Hub Hub-Konsole unter https://console.aws.amazon.com/migrationhub/.
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“
OSDistribution	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“
OSVersion	Die Kernel-Version	String	Ja	Sehen Sie sich die HTML-Version der Dokumentation an.
CPUArchitecture	Die CPU-Architektur	String	Nein	„32 Bit“, „64 Bit“
IpAddress	Die IP-Adresse des Servers	Array	Nein	Im Format xxx.xxx.xxx.xxx

Name	Beschreibung	Typ	Erforderlich	Zulässige Werte
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 der Server, IDs auf denen der Prozess läuft.	String	Ja	Der ResourceId "Resource Type„: „SERVER“, den Sie definiert haben.
ApplicationType	Die Art der Anwendung	String	Ja	„Tomcat“, "JBoss„, „Spring“, „IIS“, „Mongo DB“, ", DB2 „Maria DB“, „MySQL“,

Name	Beschreibung	Typ	Erforderlich	Zulässige Werte
				„Oracle“, "„, SQLServer „Sybase“, „Postgre“, „Cassandra“, SQLServer „IBM“, „Oracle WebLogic“, WebSphere „Java Generic“
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"," 1,0 „," DotnetFramework 1,0 SP1 „," DotnetFramework 1,0 SP2 „," DotnetFramework 1,1", "DotnetFramework DotnetFramework 1,1 SP3 „," 2,0", "2,0 SP1 „," DotnetFramework 2,0 „," 3,0", "DotnetFramework 3,0 SP1 „," DotnetFramework DotnetFramework 3,0 SP2 „," 3,5", "DotnetFramework 3,5"," DotnetFramework 4,5", "4,5"," DotnetFramework 4,5", "4,5,1"," DotnetFramework DotnetFramework 4,5,2", "DotnetFramework 4,6",DotnetFramework " 4,6,1", "DotnetFramework DotnetFramework DotnetFramework 4,6,2"," 4,7", "4,7“, "4,7“, "4,7“, "4,7“, "DotnetFramework 4,7“, "4,6" DotnetFramework 7,1", "4,7,2", SP1 SP2 SP1 DotnetFramework DotnetFramework "DotnetFramework 4,8"
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"," .0", "JDK2.0",...," JDK3 .0" JDK11
DatabaseType	Der Typ Datenbank	String	Nein	„, SQLServer „Oracle“, „Sybase“, „Mongo DB“, „Maria DB“, „Apache Cassandra “, „MySQL“, „IBM“, DB2 „Postgre“ SQLServer
DatabaseEdition	Die Ausgabe 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

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame AWS Verantwortung von Ihnen und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud selbst und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, auf der AWS Dienste in der ausgeführt AWS Cloud werden. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Externe Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWS . Weitere Informationen zu den Compliance-Programmen, die für die Strategieempfehlungen von Migration Hub gelten, finden Sie unter AWS Services im Umfang nach Compliance-Programm AWS .
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Dienst, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung von Strategieempfehlungen anwenden können. In den folgenden Themen erfahren Sie, wie Sie Strategieempfehlungen konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu 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, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der die gesamte Infrastruktur läuft AWS

Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS -Modell der geteilten Verantwortung und in der DSGVO im AWS -Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Verwenden Sie SSL/TLS, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrail Benutzerhandbuch.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-3.

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 Konsole, API oder arbeiten. AWS CLI AWS SDKs 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.

Strategieempfehlungen für Identitäts- und Zugriffsmanagement für Migration Hub

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu AWS kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Ressourcen von Strategy Recommendations zu nutzen. IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

Zielgruppe

Die Art und Weise, wie Sie AWS Identity and Access Management (IAM) verwenden, hängt davon ab, welche Arbeit Sie im Rahmen von Strategy Recommendations ausführen.

Dienstbenutzer — Wenn Sie den Strategy Recommendations-Service für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die erforderlichen Anmeldeinformationen und Berechtigungen zur Verfügung. Wenn Sie für Ihre Arbeit mehr Funktionen von Strategy Recommendations verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Funktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anfordern müssen. Wenn Sie in Strategy Recommendations nicht auf eine Funktion zugreifen können, finden Sie weitere Informationen unterFehlerbehebung bei der Migration Hub-Strategie, Empfehlungen, Identität und Zugriff.

Serviceadministrator — Wenn Sie in Ihrem Unternehmen für die Ressourcen zu Strategy Recommendations zuständig sind, haben Sie wahrscheinlich vollen Zugriff auf Strategy Recommendations. Es ist Ihre Aufgabe, zu bestimmen, auf welche Funktionen und Ressourcen von Strategy Recommendations Ihre Servicebenutzer zugreifen sollen. Anschließend müssen Sie Anforderungen an Ihren IAM-Administrator senden, um die Berechtigungen der Servicebenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen darüber, wie Ihr Unternehmen IAM mit Strategieempfehlungen nutzen kann, finden Sie unterSo funktioniert Migration Hub Strategy Recommendations mit IAM.

IAM-Administrator — Wenn Sie ein IAM-Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien schreiben können, um den Zugriff auf Strategieempfehlungen zu verwalten. Beispiele für identitätsbasierte Richtlinien von Strategy Recommendations, die Sie in IAM verwenden können, finden Sie unter. Identitätsbasierte Politikbeispiele für Strategieempfehlungen Migration Hub Migrationszentren

Authentifizierung mit Identitäten

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

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) -Benutzer, die Single Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie über den Verbund darauf zugreifen AWS , übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert darauf zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, um Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch zu signieren. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode für die Selbstsignierung von Anforderungen finden Sie unter AWS Signature Version 4 für API-Anforderungen im IAM-Benutzerhandbuch.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen bereitstellen. AWS Empfiehlt beispielsweise, die 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 AWS Multi-Faktor-Authentifizierung (MFA) in IAM im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, 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. Verwenden Sie diese nur, 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

Als bewährte Methode sollten menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen den Verbund mit einem Identitätsanbieter verwenden.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter AWS Directory Service, dem Identity Center-Verzeichnis oder einem beliebigen Benutzer, der mithilfe AWS-Services von Anmeldeinformationen zugreift, die über eine

Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf 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 Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten 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 innerhalb Ihres Unternehmens AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. 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 eine Gruppe benennen IAMAdminsund dieser Gruppe Berechtigungen zur Verwaltung 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 Anwendungsfälle für IAM-Benutzer im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität innerhalb von Ihnen AWS-Konto , die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, jedoch nicht mit einer bestimmten Person verknüpft. Um vorübergehend eine IAM-Rolle in der zu übernehmen AWS Management Console, können Sie von einer Benutzer- zu einer IAM-Rolle (Konsole) 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 Methoden für die Übernahme einer Rolle 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 (Verbund) 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 Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise in einem Service einen Anruf tätigen, ist es üblich, dass dieser Service Anwendungen in Amazon ausführt EC2 oder Objekte in Amazon S3 speichert. 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 auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. 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.
- Dienstbezogene Rolle — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

- Auf Amazon ausgeführte Anwendungen EC2 — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2 Instance ausgeführt werden und AWS API-Anfragen stellen AWS CLI . Dies ist dem Speichern von Zugriffsschlüsseln innerhalb der EC2 Instance vorzuziehen. Um einer EC2 Instanz eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instanzprofil, das an die Instanz angehängt ist. Ein Instanzprofil enthält die Rolle und ermöglicht Programmen, die auf der EC2 Instanz ausgeführt werden, temporäre Anmeldeinformationen abzurufen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Verwenden einer IAM-Rolle, um Berechtigungen für Anwendungen zu gewähren, die auf EC2 Amazon-Instances ausgeführt werden.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Die Berechtigungen in den Richtlinien legen fest, ob eine Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden 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 mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

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 von der AWS Management Console AWS CLI, der oder der 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 Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten 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 System zuordnen können AWS-Konto. Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer Inline-Richtlinie wählen, finden Sie unter Auswählen 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. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

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

Zugriffskontrolllisten () ACLs

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Dienste, die Unterstützung ACLs bieten. AWS WAF Weitere Informationen finden Sie unter Übersicht über ACLs die Zugriffskontrollliste (ACL) im Amazon Simple Storage Service Developer Guide.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete 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.
- Dienststeuerungsrichtlinien (SCPs) — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie alle Funktionen in einer Organisation aktivieren, können Sie Richtlinien zur Servicesteuerung (SCPs) auf einige oder alle Ihre Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Root-Benutzer des AWS-Kontos Entitäten. Weitere Informationen zu Organizations und SCPs finden Sie unter Richtlinien zur Servicesteuerung im AWS Organizations Benutzerhandbuch.

- Ressourcenkontrollrichtlinien (RCPs) — RCPs sind JSON-Richtlinien, mit denen Sie die maximal verfügbaren Berechtigungen für Ressourcen in Ihren Konten festlegen können, ohne die IAM-Richtlinien aktualisieren zu müssen, die jeder Ressource zugeordnet sind, deren Eigentümer Sie sind. Das RCP schränkt die Berechtigungen für Ressourcen in Mitgliedskonten ein und kann sich auf die effektiven Berechtigungen für Identitäten auswirken, einschließlich der Root-Benutzer des AWS-Kontos, unabhängig davon, ob sie zu Ihrer Organisation gehören. Weitere Informationen zu Organizations RCPs, einschließlich einer Liste AWS-Services dieser Support-Leistungen RCPs, finden Sie unter Resource Control Policies (RCPs) 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 darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter Bewertungslogik für Richtlinien.

So funktioniert Migration Hub Strategy Recommendations mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf Strategy Recommendations zu verwalten, sollten Sie sich darüber informieren, welche IAM-Funktionen zusammen mit Strategy Recommendations zur Verfügung stehen.

IAM-Funktionen, die Sie mit den Strategieempfehlungen von Migration Hub verwenden können

IAM-Feature	Unterstützung bei Strategieempfehlungen
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein

IAM-Feature	Unterstützung bei Strategieempfehlungen
Richtlinienaktionen	Ja
Richtlinienressourcen	Nein
Bedingungsschlüssel für die Richtlinie	Nein
ACLs	Nein
ABAC (Tags in Richtlinien)	Nein
Temporäre Anmeldeinformationen	Ja
Prinzipalberechtigungen	Ja
Servicerollen	Nein
Serviceverknüpfte Rollen	Ja

Einen allgemeinen Überblick darüber, wie Strategieempfehlungen und andere AWS Dienste mit den meisten IAM-Funktionen funktionieren, finden Sie im IAM-Benutzerhandbuch unter AWS Dienste, die mit IAM funktionieren.

Identitätsbasierte Richtlinien für Strategieempfehlungen

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 Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten 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.

Identitätsbasierte Politikbeispiele für Strategieempfehlungen

Beispiele für identitätsbasierte Strategien mit Strategieempfehlungen finden Sie unter. Identitätsbasierte Politikbeispiele für Strategieempfehlungen Migration Hub Migrationszentren

Ressourcenbasierte Richtlinien im Rahmen der Strategieempfehlungen

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. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. 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 unterscheiden AWS-Konten, muss ein IAM-Administrator des vertrauenswürdigen Kontos auch der Prinzipalentität (Benutzer oder Rolle) die Berechtigung zum 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 Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Politische Maßnahmen für Strategieempfehlungen

Unterstützt Richtlinienaktionen: Ja

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

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Eine Liste der Aktionen mit Strategieempfehlungen finden Sie unter Durch die Strategieempfehlungen von Migration Hub definierte Aktionen in der Serviceautorisierungsreferenz.

Bei Richtlinienaktionen in den Strategieempfehlungen wird vor der Aktion das folgende Präfix verwendet:

```
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 Strategien in Strategieempfehlungen finden Sie unter. Identitätsbasierte Politikbeispiele für Strategieempfehlungen Migration Hub Migrationszentren

Politische Ressourcen für Strategieempfehlungen

Unterstützt politische Ressourcen: Nein

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und 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 und ihrer ARNs Ressourcen für Strategieempfehlungen finden Sie unter Durch die Strategieempfehlungen von Migration Hub definierte Ressourcen in der Service Authorization Reference. Informationen darüber, mit welchen Aktionen Sie den ARN jeder Ressource angeben können, finden Sie unter In den Strategieempfehlungen des Migration Hub definierte Aktionen.

Beispiele für identitätsbasierte Richtlinien mit Strategieempfehlungen finden Sie unter. Identitätsbasierte Politikbeispiele für Strategieempfehlungen Migration Hub Migrationszentren

Schlüssel zu den politischen Bedingungen für Strategieempfehlungen

Unterstützt dienstspezifische Richtlinien-Bedingungsschlüssel: Nein

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, 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 dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Eine Liste der Bedingungsschlüssel für Strategy Recommendations finden Sie unter Condition Keys for Migration Hub Strategy Recommendations in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter In den Strategieempfehlungen des Migration Hub definierte Aktionen.

Beispiele für identitätsbasierte Richtlinien mit Strategieempfehlungen finden Sie unter. Identitätsbasierte Politikbeispiele für Strategieempfehlungen Migration Hub Migrationszentren

Zugriffskontrolllisten (ACLs) in den Strategieempfehlungen

Unterstützt ACLs: Nein

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten 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 AWS werden diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter Definieren von Berechtigungen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Temporäre Anmeldeinformationen mit Strategieempfehlungen verwenden

Unterstützt temporäre Anmeldeinformationen: Ja

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

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Passwort anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter Wechseln von einer Benutzerrolle zu einer IAM-Rolle (Konsole) im IAM-Benutzerhandbuch.

Mithilfe der AWS API AWS CLI oder können Sie temporäre Anmeldeinformationen manuell erstellen. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

Serviceübergreifende Prinzipalberechtigungen für Strategieempfehlungen

Unterstützt Forward Access Sessions (FAS): Ja

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren

Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. 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 Strategieempfehlungen

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**
>
> Durch das Ändern der Berechtigungen für eine Servicerolle kann die Funktionalität von Strategy Recommendations beeinträchtigt werden. Bearbeiten Sie Servicerollen nur, wenn Strategy Recommendations eine Anleitung dazu enthält.

Servicebezogene Rollen für Strategy Recommendations

Unterstützt dienstbezogene Rollen: Ja

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

Einzelheiten zum Erstellen oder Verwalten von dienstbezogenen Rollen mit Strategy Recommendations 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: AWSMigration HubStrategyConsoleFullAccess

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 unter AWSMigrationHubStrategyConsoleFullAccessim Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: AWSMigration HubStrategyCollector

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 Bearbeitung von 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.

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

Strategische Empfehlungen 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`PutLogData` , `StartPortingCompatibilityAssessment` `GetPortingCompatibilityAssessment` , `StartPortingRecommendationAssessment` und `GetPortingRecommendationAssessment` Anwendungstransformation, damit der Anwendungstransformationsdienst Protokolle und Metriken an den Dienst senden kann.	1. April 2024

Änderung	Beschreibung	Datum
	Die `ListBucket` und `GetBucketLocation` wurden für Amazon Simple Storage Service (Amazon S3) hinzugefügt, um Protokoll- und Metrik-Uploads zu unterstützen. Die beiden `PutLogData` `PutMetricData` wurden auch hinzugefügt, damit der Strategy Recommendations-Collector Logs und Metriken an den Endpunkt des Services senden kann.	
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 Anwendungstransformation. Dieses Update fügt auch Bedingungen hinzu, um sicherzustellen, `aws:ResourceAccount` dass die der Genehmigung `aws:PrincipalAccount` zur Nutzung des enthaltenen Amazon Simple Storage Service und der entsprechenden AWS Secrets Manager Aktionen entsprechen.	5. Februar 2024

Änderung	Beschreibung	Datum
AWSMigrationHubStrategyCollector – Aktualisierung auf eine bestehende Richtlinie	Diese Richtlinie wurde mit den folgenden Amazon S3 APIs —`CreateBucket` ,`PutEncryptionConfiguration` ,`PutBucketPublicAccessBlock` , `PutBucketPolicy` `PutBucketVersioning` , und aktualisiertPutLifecycleConfiguration .	15. September 2023
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 um drei AWS Application Discovery Service APIs — `DescribeConfigurations` `DescribeTags` , und aktualisiertListConfigurations .	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

Änderung	Beschreibung	Datum
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
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 verfügbar gemacht	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

Änderung	Beschreibung	Datum
Strategy Recommendations begann, Änderungen nachzuverfolgen	Strategy Recommendations begann, Änderungen an den AWS verwalteten Richtlinien nachzuverfolgen.	25. Oktober 2021

Identitätsbasierte Politikbeispiele für Strategieempfehlungen Migration Hub Migrationszentren

Standardmäßig sind Benutzer und Rollen nicht berechtigt, Ressourcen für Strategy Recommendations 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 (Konsole) im IAM-Benutzerhandbuch.

Einzelheiten zu den in Strategy Recommendations definierten Aktionen und Ressourcentypen, einschließlich des Formats ARNs für die einzelnen Ressourcentypen, finden Sie unter Strategy Recommendations Actions, Resources and Condition Keys for Migration Hub Strategy Recommendations in der Service Authorization Reference.

Themen

- Bewährte Methoden für Richtlinien
- Verwenden der Strategy Recommendations-Konsole
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer
- Zugreifen auf einen Amazon-S3-Bucket

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand Ressourcen für Strategy Recommendations in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr

verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um Ihren Benutzern und Workloads zunächst Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien oder AWS -verwaltete Richtlinien für Auftrags-Funktionen im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung mit IAM Access Analyzer im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren

Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Sicherer API-Zugriff mit MFA 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 Strategy Recommendations-Konsole

Um auf die Migration Hub Strategy Recommendations-Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, die Ressourcen für Strategy Recommendations in Ihrem aufzulisten und Details zu diesen Ressourcen 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.

Sie müssen Benutzern, die nur die API AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. 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 die Strategy Recommendations-Konsole weiterhin 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 umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der API AWS CLI oder AWS .

```
{
    "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 AWS-Konto Zugriff auf einen Ihrer Amazon S3 S3-Buckets gewähren. `amzn-s3-demo-bucket` 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. Ein Beispiel für eine exemplarische Vorgehensweise, bei der Benutzern Berechtigungen erteilt und diese mithilfe der Konsole getestet werden, finden Sie unter Eine exemplarische Vorgehensweise: 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:::amzn-s3-demo-bucket"
      },
      {
         "Sid":"ManageBucketContents",
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
            "s3:PutObjectAcl",
            "s3:GetObject",
            "s3:GetObjectAcl",
            "s3:DeleteObject"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket/*"
      }
   ]
}
```

Fehlerbehebung bei der Migration Hub-Strategie, Empfehlungen, Identität und Zugriff

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

Themen

Ich bin nicht berechtigt, eine Aktion in Strategy Recommendations durchzuführen

Wenn Ihnen AWS Management Console mitgeteilt wird, dass Sie nicht berechtigt sind, eine Aktion durchzuführen, 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 berechtigt, iam auszuführen: PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zur Durchführung der `iam:PassRole` Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie Strategy Recommendations eine Rolle zuweisen können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte 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 „Strategy Recommendations“ `marymajor` versucht, mithilfe der Konsole eine Aktion 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 dauerhaften Zugriff auf Ihre 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 den Zugriff auf Strategieempfehlungen ermöglichen

Um anderen den Zugriff auf Strategieempfehlungen zu ermöglichen, müssen Sie den Personen oder Anwendungen, die Zugriff benötigen, die entsprechenden Berechtigungen erteilen. Wenn Sie Personen und Anwendungen verwalten, weisen Sie Benutzern oder Gruppen Berechtigungssätze zu, um deren Zugriffsebene zu definieren. AWS IAM Identity Center Mit Berechtigungssätzen werden automatisch IAM-Richtlinien erstellt und den IAM-Rollen zugewiesen, die der Person oder Anwendung zugeordnet sind. Weitere Informationen finden Sie im AWS IAM Identity Center Benutzerhandbuch unter Berechtigungssätze.

Wenn Sie IAM Identity Center nicht verwenden, müssen Sie IAM-Entitäten (Benutzer oder Rollen) für die Personen oder Anwendungen erstellen, die Zugriff benötigen. Anschließend müssen Sie der Entität eine Richtlinie hinzufügen, die ihr in den Strategieempfehlungen die richtigen Berechtigungen gewährt. Nachdem die Berechtigungen erteilt wurden, geben Sie die Anmeldeinformationen an den Benutzer oder Anwendungsentwickler weiter. Sie werden diese Anmeldeinformationen für den Zugriff verwenden AWS. Weitere Informationen zum Erstellen von IAM-Benutzern, -Gruppen, -Richtlinien und -Berechtigungen finden Sie im IAM-Benutzerhandbuch unter IAM-Identitäten sowie Richtlinien und Berechtigungen in IAM.

Ich möchte Personen außerhalb von mir den Zugriff auf meine AWS-Konto Ressourcen für Strategieempfehlungen ermöglichen

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. Für Dienste, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (ACLs) unterstützen, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob Strategy Recommendations diese Funktionen unterstützt, finden Sie unter. So funktioniert Migration Hub Strategy Recommendations mit IAM
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte.

- 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 Kontoübergreifender Ressourcenzugriff in IAM 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. Servicebezogene Rollen sind in Strategy Recommendations vordefiniert und beinhalten alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

Eine dienstbezogene Rolle erleichtert die Einrichtung von Strategy Recommendations, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Strategy Recommendations definiert die Berechtigungen seiner dienstbezogenen Rollen. Sofern nicht anders definiert, können nur Strategy Recommendations diese Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Informationen zu anderen Diensten, die dienstverknüpfte Rollen unterstützen, finden Sie unter AWS Dienste, die mit IAM funktionieren. Suchen Sie dort in der Spalte „Dienstverknüpfte Rolle“ nach den Diensten, für die „Ja“ steht. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Berechtigungen für dienstbezogene Rollen für Strategieempfehlungen

Strategy Recommendations verwendet die benannte dienstbezogene Rolle AWSServiceRoleForMigrationHubStrategyund ordnet sie der AWSMigrationHubStrategyServiceRolePolicyIAM-Richtlinie zu — Ermöglicht Zugriff auf und. AWS Migration Hub 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 Richtlinie für Rollenberechtigungen ermöglicht 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
```

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

Den Aktualisierungsverlauf dieser Richtlinie finden Sie unterStrategische Empfehlungen 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.

Eine dienstbezogene Rolle für Strategy Recommendations erstellen

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie damit einverstanden sind, Migration Hub die Erstellung einer serviceverknüpften Rolle (SLR) in Ihrem Konto im zu gestatten 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, dass Migration Hub eine serviceverknüpfte Rolle (SLR) in Ihrem Konto erstellt, erstellt Strategy Recommendations die serviceverknüpfte Rolle erneut für Sie.

Bearbeitung einer dienstbezogenen Rolle für Strategy Recommendations

Mit Strategy Recommendations können Sie die AWSServiceRoleForMigrationHubStrategydienstbezogene Rolle nicht 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 Strategy Recommendations-Konsole, 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 AWSServiceRoleForMigrationHubStrategyserviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Leitfaden.

Wenn Sie Ressourcen für Strategy Recommendations löschen, die vom AWSServiceRoleForMigrationHubStrategySLR verwendet werden, können keine laufenden Bewertungen (Aufgaben zur Generierung von Empfehlungen) ausgeführt werden. Es können auch keine Hintergrundbewertungen ausgeführt werden. Wenn Tests ausgeführt werden, schlägt das Löschen der Spiegelreflexkamera in der IAM-Konsole fehl. Schlägt das Löschen der Spiegelreflexkamera fehl, können Sie den Löschvorgang wiederholen, nachdem alle Hintergrundaufgaben abgeschlossen sind. Sie müssen keine erstellten Ressourcen bereinigen, bevor Sie die Spiegelreflexkamera löschen.

Unterstützte Rollen im Zusammenhang mit dem Dienst „Strategy Recommendations“

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

Strategieempfehlungen für Migration Hub und VPC-Endpunkte für Schnittstellen ()AWS PrivateLink

Sie können eine private Verbindung zwischen Ihrer VPC und den Strategieempfehlungen für Migration Hub herstellen, indem Sie einen VPC-Schnittstellen-Endpunkt erstellen. Schnittstellenendpunkte werden von unterstütz AWS PrivateLink. Mit AWS PrivateLink können Sie privat auf die API-Operationen von Strategy Recommendations zugreifen, ohne ein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder AWS Direct Connect eine Verbindung zu benötigen. Instances in Ihrer VPC benötigen keine öffentlichen IP-Adressen, um mit den API-Vorgängen von Strategy Recommendations zu kommunizieren. Der Datenverkehr zwischen Ihrer VPC und Strategy Recommendations verbleibt im Amazon-Netzwerk.

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

Weitere Informationen finden Sie unter Schnittstellen-VPC-Endpunkte (AWS PrivateLink) im Amazon-VPC-Benutzerhandbuch.

Überlegungen zu Strategieempfehlungen VPC-Endpoints

Bevor Sie einen Schnittstellen-VPC-Endpunkt für Strategieempfehlungen einrichten, stellen Sie sicher, dass Sie die Eigenschaften und Einschränkungen und AWS PrivateLink Kontingente der Schnittstellen-Endpunkte im Amazon VPC-Benutzerhandbuch lesen.

Strategy Recommendations unterstützt Aufrufe aller API-Aktionen von Ihrer VPC aus. Um alle Strategieempfehlungen verwenden zu können, müssen Sie einen VPC-Endpunkt erstellen.

Erstellen eines VPC-Schnittstellen-Endpunkts für Strategieempfehlungen

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

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

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

Wenn Sie privates DNS für den Endpunkt verwenden, können Sie API-Anfragen an Strategy Recommendations stellen, indem Sie den Standard-DNS-Namen für die Region verwenden.

Sie können beispielsweise den Namen verwenden`migrationhub-strategy.us-east-1.amazonaws.com`.

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

Erstellung einer VPC-Endpunktrichtlinie für Strategieempfehlungen

Sie können Ihrem VPC-Endpunkt eine Endpunktrichtlinie hinzufügen, die 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, auf denen 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 Maßnahmen mit Strategieempfehlungen

Im Folgenden finden Sie ein Beispiel für eine Endpunktrichtlinie für Strategieempfehlungen. Wenn diese Richtlinie an einen Endpunkt angehängt ist, gewährt sie allen Prinzipalen auf allen Ressourcen Zugriff auf die aufgelisteten Strategieempfehlungsaktionen.

```
{
   "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:

- Compliance und Governance im Bereich Sicherheit – In diesen Anleitungen für die Lösungsimplementierung werden Überlegungen zur Architektur behandelt. Außerdem werden Schritte für die Bereitstellung von Sicherheits- und Compliance-Features beschrieben.
- Referenz für berechtigte HIPAA-Services – Listet berechtigte HIPAA-Services auf. Nicht alle AWS-Services sind HIPAA-fähig.
- AWS Compliance-Ressourcen — Diese Sammlung von Arbeitsmappen und Leitfäden gilt möglicherweise für Ihre Branche und Ihren Standort.
- AWS Leitfäden zur Einhaltung von Vorschriften für Kunden — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.
- Evaluierung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub— Dies AWS-Service bietet einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu

überprüfen. Die Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerelementreferenz.

- 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 AWS Dienste beschrieben, die mit den Strategieempfehlungen von Migration Hub interagieren.

Themen

API-Aufrufe für Strategieempfehlungen protokollieren mit AWS CloudTrail

Migration Hub Strategy Recommendations ist in einen Service integriert AWS CloudTrail, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem AWS Dienst durchgeführten Aktionen in Strategy Recommendations bereitstellt. CloudTrail erfasst API-Aufrufe für Strategieempfehlungen als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der Strategy Recommendations-Konsole und Codeaufrufen für die Strategy Recommendations-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 trotzdem in der CloudTrail Konsole im Ereignisverlauf anzeigen. Anhand der von CloudTrail gesammelten Informationen können Sie die Anfrage an Strategy Recommendations, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln.

Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrail Benutzerhandbuch.

Informationen zu Strategieempfehlungen finden Sie unter CloudTrail

CloudTrail ist auf Ihrem aktiviert AWS-Konto , wenn Sie das Konto erstellen. Wenn in Strategy Recommendations eine Aktivität auftritt, wird diese Aktivität zusammen mit anderen CloudTrail AWS Serviceereignissen in der Ereignishistorie als Ereignis aufgezeichnet. Sie können in Ihrem AWS-Konto die neusten Ereignisse anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter Ereignisse mit dem CloudTrail Ereignisverlauf anzeigen.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem System AWS-Konto, einschließlich der Ereignisse für Strategieempfehlungen, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail

die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

- Übersicht zum Erstellen eines Trails
- CloudTrail unterstützte Dienste und Integrationen
- Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

Strategy Recommendations unterstützt die Protokollierung der folgenden Aktionen als Ereignisse in CloudTrail Protokolldateien:

- GetApplicationComponentStrategies
- GetApplicationComponentDetails
- GetAssesment
- GetImportFileTask
- GetPortfolioPreferences
- GetPortfolioSummary
- GetServerDetails
- GetServerStrategies
- ListApplicationComponents
- ListCollectors
- ListImportFileTask
- ListServers
- PutPortfolioPreferences
- StartAssessment
- StartImportFileTask
- StopAssessment
- UpdateApplicationComponetConfig

- UpdateServerConfig

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root- oder AWS Identity and Access Management (IAM-) Benutzeranmeldedaten gestellt wurde
- Ob die Anfrage mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen föderierten Benutzer ausgeführt wurde
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

Grundlegendes zu den Einträgen in der Protokolldatei von Strateg

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die GetServerDetailsAktion demonstriert.

```
{
    "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"
}
```

Quoten für Strategieempfehlungen für den Migration Hub

Ihr AWS Konto verfügt über Standardkontingente, die früher als Limits bezeichnet wurden, für jeden AWS Dienst. 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 Strategieempfehlungen für Migration Hub finden Sie unter Servicekontingente für Strategy Recommendations.

Sie können die Kontingente für Strategieempfehlungen auch anzeigen, indem Sie die Konsole Service Quotas öffnen. Wählen Sie im Navigationsbereich AWS Dienste und dann Migration Hub Strategy Recommendations aus.

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-Version 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 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

Problem gelöst

- 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 um neue `application-transformation` Aktionen aktualisiert. 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 Recommendations ist mit	12. Oktober 2023

	Unterstützung für mehrere Datenquellen verfügbar.	
AWS verwaltete Richtlini enaktualisierungen — Update auf AWSMigration HubStrate gyCollector	Die AWSMigrationHubStr ategyCollectorRichtlinie wurde aktualisiert, um das neue Amazon S3 aufzunehmen APIs.	15. September 2023
AWS verwaltete Richtlini enaktualisierungen — Aktualisi erung auf AWSMigration HubStrategyCollector	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 für den Migration Hub AWS Application Discovery Service APIs wurden drei 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.