



Benutzerhandbuch

Migration-Hub-Strategieempfehlungen



Migration-Hub-Strategieempfehlungen: Benutzerhandbuch

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

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

Table of Contents

Was sind Strategieempfehlungen für den Migration Hub?	1
Sind Sie zum ersten Mal Kunde von Strategy Recommendations?	1
Übersicht	2
Zugehörige Services	2
Einrichtung	4
Melden Sie sich an für ein AWS-Konto	4
Erstellen Sie einen Benutzer mit Administratorzugriff	4
Strategie, Empfehlungen, Benutzer und Rollen	6
Erste Schritte	8
Voraussetzungen	8
Schritt 1: Laden Sie den Collector herunter	10
Schritt 2: Stellen Sie den Collector bereit	11
Stellen Sie den Collector in vCenter bereit	12
Stellen Sie das Collector-AMI bereit	13
Schritt 3: Melden Sie sich beim Collector an	14
Melden Sie sich bei dem in vCenter bereitgestellten Collector an	14
Melden Sie sich bei dem Collector an, der als Amazon EC2 EC2-Instance bereitgestellt wird	15
Schritt 4: Den Collector einrichten	15
AWSKonfigurationen	16
vCenter-Konfigurationen	17
Konfigurationen für Remoteserver	21
Konfigurationen zur Versionskontrolle	23
Bereiten Sie Ihre Remoteserver auf die Datenerfassung vor	24
Überprüfen Sie die Konfiguration für die Datenerfassung	28
Schritt 5: Empfehlungen einholen	30
Empfehlungen	33
Strategieempfehlungen anzeigen	33
Empfehlungen für Anwendungskomponenten	34
Arbeiten mit Anwendungskomponenten	35
Quellcode-Analyse	38
Datenbank-Analyse	38
Binäre Analyse	40
Serverempfehlungen	41

Präferenzen	42
Datenquellen	44
Datenquellen anzeigen	44
Sammler für Anwendungsdaten	45
Vom Sammler gesammelte Daten	45
Den Collector aktualisieren	48
Importieren von Daten	49
Vorlage importieren	50
Daten entfernen	55
Sicherheit	56
Datenschutz	57
Verschlüsselung im Ruhezustand	58
Verschlüsselung während der Übertragung	58
Identity and Access Management	58
Zielgruppe	58
Authentifizierung mit Identitäten	59
Verwalten des Zugriffs mit Richtlinien	63
So funktioniert Migration Hub Strategy Recommendations mit IAM	66
AWS verwaltete Richtlinien	73
Beispiele für identitätsbasierte Richtlinien	80
Fehlerbehebung	84
Verwenden von serviceverknüpften Rollen	88
VPC-Endpunkte (AWS PrivateLink)	90
Compliance-Validierung	92
Arbeiten mit anderen Services	95
AWS CloudTrail	95
Informationen zu Strategieempfehlungen in CloudTrail	95
Grundlagen zu -Protokolldateieinträgen	97
Kontingente	99
Versionshinweise	100
17. November 2023	100
12. Oktober 2023	100
17. April 2023	101
17. März 2023	101
07. November 2022	101
27. September 2022	101

30. Juni 2022	102
18. April 2022	102
25. Februar 2022	102
10. Februar 2022	102
28. Januar 2022	103
14. Januar 2022	103
21. Dezember 2021	103
15. Dezember 2021	103
25. Oktober 2021	104
Dokumentverlauf	105
.....	cviii

Was sind Strategieempfehlungen für den Migration Hub?

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

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

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

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

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

Sind Sie zum ersten Mal Kunde von Strategy Recommendations?

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

- [Überblick über die Strategieempfehlungen](#)

- [Erstellung von Strategieempfehlungen](#)
- [Erste Schritte mit Strategieempfehlungen](#)

Überblick über die Strategieempfehlungen

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

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

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

Zugehörige Services

- [AWS Migration Hub](#)— Sie verwenden die AWS Migration Hub Konsole, um auf die Migration Hub Strategy Recommendations-Konsole zuzugreifen. Außerdem werden Informationen zu den Servern angezeigt, von denen Sie Daten sammeln.
- [AWS Application Discovery Service](#)— Sie verwenden den Application Discovery Service, um Daten über Ihre Server und Anwendungen in der AWS Migration Hub Konsole zu sammeln, bevor Sie Strategy Recommendations verwenden.
- [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 Service migrieren können. AWS
- [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

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

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

Erstellung von Strategieempfehlungen

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

Themen

- [Melden Sie sich an für ein AWS-Konto](#)
- [Erstellen Sie einen Benutzer mit Administratorzugriff](#)
- [Strategie, Empfehlungen, Benutzer und Rollen](#)

Melden Sie sich an für ein AWS-Konto

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

Um sich für eine anzumelden AWS-Konto

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

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

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

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

Erstellen Sie einen Benutzer mit Administratorzugriff

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

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich [AWS Management Console](#) als Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter [Anmelden als Root-Benutzer](#) im AWS-Anmeldung Benutzerhandbuch zu.

2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

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

Erstellen Sie einen Benutzer mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

Anweisungen finden Sie unter [Aktivieren AWS IAM Identity Center](#) im AWS IAM Identity Center Benutzerhandbuch.

2. Gewähren Sie einem Benutzer in IAM Identity Center Administratorzugriff.

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

Melden Sie sich als Benutzer mit Administratorzugriff an

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

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

Weisen Sie weiteren Benutzern Zugriff zu

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

Anweisungen finden Sie im Benutzerhandbuch unter [Einen Berechtigungssatz erstellen](#).AWS IAM Identity Center

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

Anweisungen finden [Sie im AWS IAM Identity Center Benutzerhandbuch unter Gruppen hinzufügen](#).

Strategie, Empfehlungen, Benutzer und Rollen

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

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

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

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

- Benutzer und Gruppen in AWS IAM Identity Center:

Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter [Erstellen eines Berechtigungssatzes](#) im AWS IAM Identity Center -Benutzerhandbuch.

- Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anweisungen unter [Erstellen einer Rolle für einen externen Identitätsanbieter \(Verbund\)](#) im IAM-Benutzerhandbuch.

- IAM-Benutzer:

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

Erste Schritte mit Strategieempfehlungen

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

Themen

- [Voraussetzungen für Strategieempfehlungen](#)
- [Schritt 1: Laden Sie den Strategy Recommendations Collector herunter](#)
- [Schritt 2: Stellen Sie den Strategy Recommendations Collector bereit](#)
- [Schritt 3: Melden Sie sich beim Strategy Recommendations Collector an](#)
- [Schritt 4: Den Collector für Strategieempfehlungen einrichten](#)
- [Schritt 5: Verwenden Sie Strategieempfehlungen in der Migration Hub Hub-Konsole, um Empfehlungen zu erhalten](#)

Voraussetzungen für Strategieempfehlungen

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

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

Sie können den Collector auch in einer Amazon EC2 EC2-Instance mithilfe des Collector-AMI bereitstellen.

- Prüfen Sie, ob Ihre Betriebssystemumgebung unterstützt wird:
 - Linux

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

Um .NET-Repositoryys für Empfehlungen von Porting Assistant for .NET zu analysieren, müssen Sie einen Windows-Computer bereitstellen, auf dem das Portierungsbewertungstool von Porting Assistant for .NET installiert ist. Weitere Informationen finden Sie unter [Erste Schritte mit Porting Assistant for .NET](#) im Porting Assistant for .NET-Benutzerhandbuch.

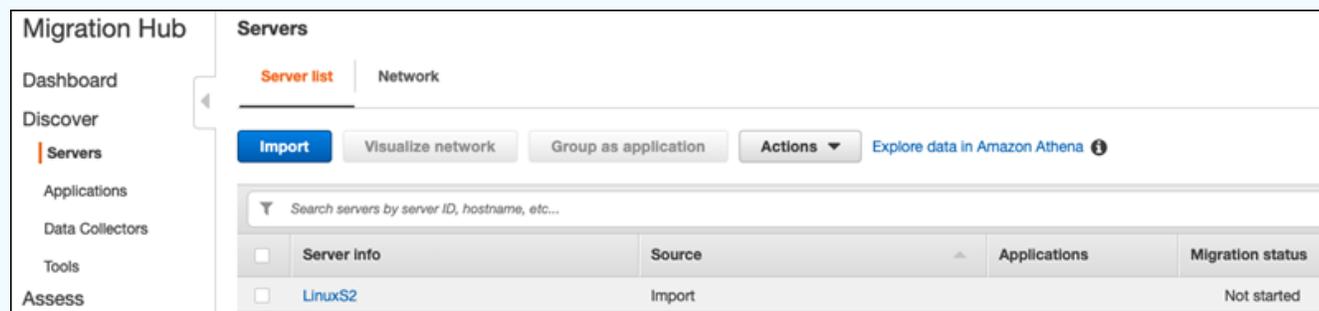
- Um Strategieempfehlungen für die Datenbankanalyse zu aktivieren, müssen Sie Anmeldeinformationen unter eingeben AWS Secrets Manager. Weitere Informationen finden Sie unter [Datenbankanalyse für Strategy Recommendations](#).
- Sie müssen die AWS Migration Hub Konsole verwenden AWS Application Discovery Service , um Daten über Ihre Server und Anwendungen zu sammeln, bevor Sie Strategy Recommendations verwenden können. Sie können eine der folgenden Methoden verwenden, um die Daten zu sammeln.
 - Migration Hub-Import — Mit dem Migration Hub Hub-Import können Sie Informationen über Ihre lokalen Server und Anwendungen in Migration Hub importieren. Weitere Informationen finden Sie unter [Migration Hub Hub-Import](#) im Application Discovery Service Service-Benutzerhandbuch.
 - AWS Application Discovery Service Agentless Collector — Der Agentless Collector ist eine VMware-Appliance, die Informationen über virtuelle Maschinen (VMs) von VMware sammelt.

Weitere Informationen finden Sie unter [Agentless Collector](#) im Application Discovery Service Service-Benutzerhandbuch.

- **AWS Application Discovery Agent** — Der Discovery Agent ist eine AWS Software, die Sie auf Ihren lokalen Servern und VMs installieren, um Systeminformationen und Details der Netzwerkverbindungen zwischen Systemen zu erfassen. Weitere Informationen finden Sie unter [AWS Application Discovery Agent](#) im Application Discovery Service Service-Benutzerhandbuch.
- **Datensammler für Strategieempfehlungen** — Wenn Ihre Server in VMware vCenter gehostet werden und Sie Zugriff gewähren, kann Strategy Recommendations Ihr Serverinventar automatisch abrufen. Die Strategy Recommendations-Konsole verwendet die gesammelten Informationen, um Sie bei der Bewertung zu unterstützen.

Note

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



Schritt 1: Laden Sie den Strategy Recommendations Collector herunter

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

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

Um die Collector-OVA-Datei herunterzuladen

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

Schritt 2: Stellen Sie den Strategy Recommendations Collector bereit

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

Es gibt zwei Möglichkeiten, den Collector bereitzustellen:

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

finden Sie unter [Stellen Sie den Strategy Recommendations-Collector in einer Amazon EC2 EC2-Instance bereit](#).

Stellen Sie den Strategy Recommendations Collector in vCenter bereit

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

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

So stellen Sie den Collector in vCenter bereit

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

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

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

Wir empfehlen die folgenden Spezifikationen für die VM.

Strategieempfehlungen, Sammler, VM-Spezifikationen

- RAM — mindestens 8 GB
- CPUs — mindestens 4

Note

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

OVA-Datei bereitgestellt haben. Anweisungen zum Upgrade finden Sie unter [Den Strategy Recommendations Collector aktualisieren](#).

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

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

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

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

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

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

Strategy Recommendations Collector Amazon EC2 EC2-Instance-Spezifikationen

- RAM — Mindestens 8 GB
- CPUs — mindestens 4

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

Note

Um sicherzustellen, dass Sie die neueste Version des Collectors mit allen neuen Funktionen und Bugfixes verwenden, aktualisieren Sie den Collector, nachdem Sie den Strategy Recommendations Collector als Amazon EC2 EC2-Instance bereitgestellt haben. Anweisungen zum Upgrade finden Sie unter [Den Strategy Recommendations Collector aktualisieren](#).

Schritt 3: Melden Sie sich beim Strategy Recommendations Collector an

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

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

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

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

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

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

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

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

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

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

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

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

Schritt 4: Den Collector für Strategieempfehlungen einrichten

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

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

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

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

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

Note

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

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

Um alle Collector-Konfigurationen gleichzeitig einzurichten

1. Geben Sie den folgenden Befehl ein.

```
collector setup
```

2. Geben Sie die Informationen für einAWSKonfigurationen wie beschrieben unter [AufgestelltAWSKonfigurationen](#).
3. Geben Sie die Informationen für vCenter-Konfigurationen ein, wie unter beschrieben [Richten Sie vCenter-Konfigurationen ein](#).
4. Geben Sie die Informationen für Remoteserverkonfigurationen ein, wie unter beschrieben [Richten Sie Remoteserverkonfigurationen ein](#).
5. Geben Sie die Informationen für Versionskontrollkonfigurationen ein, wie unter beschrieben [Richten 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 [Bereiten Sie Ihre Windows- und Linux-Remote-Server auf die Datenerfassung vor](#).

AufgestelltAWSKonfigurationen

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

1. Geben Sie ein `Y` für Ja zum Haben Sie IAM-Berechtigungen eingerichtet...Frage. Sie haben diese Berechtigungen eingerichtet, als Sie einen Benutzer für den Zugriff auf den Collector erstellt haben, indem Sie `AWSMigrationHubStrategyCollector` verwaltete Richtlinie gemäß den Schritten unter [Strategie, Empfehlungen, Benutzer und Rollen](#).
2. Geben Sie Ihren Zugangsschlüssel und Ihren geheimen Schlüssel aus demAWSKonto, das den Benutzer hat, den Sie für den Zugriff auf den Collector erstellt haben. Gehen Sie dazu wie folgt vor [Strategie, 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 [Endpunkte der Strategie, Empfehlungen](#) in der Allgemeinen AWS-Referenz.
4. Eingeben Sie Ja zu den Metriken im Zusammenhang mit Collector auf den Migration Hub Strategy Service hochladen? Frage. Informationen zu Metriken helfen AWS, Ihnen angemessene Unterstützung zu bieten.
5. Geben Sie Ja zu den Collector-bezogenen Logs auf den Migration Hub Strategy Service hochladen? Frage. Informationen aus Protokollen helfen AWS, Ihnen angemessene Unterstützung zu bieten.

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

Richten Sie vCenter-Konfigurationen ein

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

1. Geben Sie für Ja zum Möchten Sie sich mit VMware vCenter-Anmeldeinformationen authentifizieren Frage, ob Sie sich mit VMware vCenter-Anmeldeinformationen authentifizieren möchten.

 Note

Für die Authentifizierung mit VMware vCenter-Anmeldeinformationen müssen die VMware-Tools auf den Zielsevern installiert sein.

Geben Sie den Host-URL, bei der es sich entweder um die vCenter-IP-Adresse oder die URL handeln kann. Geben Sie dann den Nutzernamen und Passwort für VMware vCenter.

2. Geben Sie für Ja zum Haben Sie Windows-Computer, die von VMware vCenter verwaltet werden Frage, ob Sie Windows-Server konfigurieren möchten.

Geben Sie den Nutzernamen und Passwort für Windows.

 Note

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

3. Geben Sie für Ja zum Einrichtung für Linux mit VMware vCenter Frage, ob Sie Linux-Server konfigurieren möchten.

Geben Sie den Nutzernamen und Passwort für Linux.

4. Geben Sie für Ja zum Möchten Sie Anmeldeinformationen für Server außerhalb von vCenter mithilfe von NTLM für Windows einrichten und SSH/Cert-basiert für Linux Fragen, wenn Sie Remote-Server-Anmeldeinformationen für Server außerhalb von vCenter einrichten möchten.
5. Für die Möchten Sie dieselben Windows-Anmeldeinformationen verwenden, die Sie beim vCenter-Setup verwendet haben Frage, geben Sie für ja, wenn die Anmeldeinformationen für die außerhalb von vCenter verwalteten Windows-Maschinen mit den Anmeldeinformationen

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

Wenn du antwortest für ja, es werden die folgenden Fragen gestellt.

- a. Geben Sie ein für Ja zum Sind Sie damit einverstanden, dass Collector bei der ersten Interaktion mit Windows-Servern Serverzertifikate in Ihrem Namen akzeptiert und lokal speichert? Frage.
- b. Geben Sie ein für die Geben Sie Ihre Optionen ein Frage, wenn Sie die SSH-Authentifizierung konfigurieren möchten.

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

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

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

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

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

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

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

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

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

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

Richten Sie Remoteserverkonfigurationen ein

Um Remoteserverkonfigurationen einzurichten, verwenden Sie `dencollector setup` Befehl oder `dercollector setup --remote-server-configurations` Befehl:

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

Geben Sie den `Nutzername` und `Passwort` für WinRM.

Note

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

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

Sie müssen die generierten Serveranmeldedaten auf Ihre Windows-Server kopieren. Weitere Informationen finden Sie unter [Richten Sie die Remoteserverkonfiguration auf Windows-Servern ein](#).

2. Geben Sie ein `Y` für Ja zum `Einrichtung für Linux mit SSH oder Cert` Frage, ob Sie Linux-Server konfigurieren möchten.
3. Geben Sie ein `1` für die `Geben Sie Ihre Optionen ein` Frage, 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 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

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

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

Geben Sie ein `github.com` für die GIT-Serverendpunkt:.

3. Eingeben `2` für die Geben Sie Ihre Optionen ein Frage, wenn Sie eine konfigurieren möchten GitHub Unternehmensserver.

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

4. Gib dein Git ein *Nutzername* und persönlicher Zugang *Zeichen*.
5. Eingeben `Y` für Ja zum Haben Sie irgendwelche Csharp-Repositorys, die auf einem Windows-Computer analysiert werden sollten? Frage, wenn Sie C#-Code analysieren möchten.

Note

Um .NET-Repositorys anhand der Empfehlungen von Porting Assistant for .NET zu analysieren, müssen Sie einen Windows-Computer bereitstellen, auf dem das Portierungsbewertungstool Porting Assistant for .NET installiert ist. Weitere Informationen finden Sie unter [Erste Schritte mit Porting Assistant for .NET](#) in der Porting Assistant for .NET-Benutzerhandbuch.

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

Eingeben `N` für nein, wenn Sie neue Anmeldeinformationen eingeben möchten.

7. Zu verwenden VMware vCenter Windows-Maschine Anmeldeinformationen, geben Sie ein `1` zum Wählen Sie eine der folgenden Optionen für Windows-Anmeldeinformationen.
8. Geben Sie die IP-Adresse für den Windows-Computer ein.

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

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

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

Note

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

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

Note

Sie müssen sicherstellen, dass die Server über ihre private IP-Adresse erreichbar sind. Weitere Anweisungen zur Einrichtung der Umgebung über eine Virtual Private Cloud (VPC) finden Sie unter [AWS-Informationen zur Ausführung aus der Ferne](#) finden Sie im [Amazon Virtual Private Cloud-Benutzerhandbuch](#).

Informationen zur Vorbereitung Ihrer Linux-Remote-Server finden Sie unter [Bereiten Sie Linux-Remote-Server vor](#).

Informationen zur Vorbereitung Ihrer Windows-Remoteserver finden Sie unter [Richten Sie die Remoteserverkonfiguration auf Windows-Servern ein](#).

Bereiten Sie Linux-Remote-Server vor

Richten Sie die schlüsselbasierte Authentifizierung auf Linux-Servern ein

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

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

1. Kopieren Sie den mit dem Namen generierten öffentlichen Schlüssel `id_rsa_assessment.pub` aus dem folgenden Ordner im Container:

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

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

Richten Sie die zertifikatsbasierte Authentifizierung auf Linux-Servern ein

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

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

Um die zertifikatsbasierte Authentifizierung auf Ihren Linux-Servern einzurichten

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

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

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

Dieser öffentliche Schlüssel muss Ihrer CA hinzugefügt werden, um das Zertifikat zu generieren.

3. Kopieren Sie das im vorherigen Schritt generierte Zertifikat an den folgenden Speicherort im Collector:

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

Der Name des Zertifikats muss `id_rsa_assessment-cert.pub` sein.

4. Geben Sie während des Einrichtungsschritts den Namen der Zertifikatsdatei an.

Richten Sie die Remoteserverkonfiguration auf Windows-Servern ein

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

 Um mehr über das zu erfahren PowerShell Lesen Sie diesen Hinweis für das Skript, das auf dem Remoteserver ausgeführt wird.

Das Skript ermöglicht PowerShell remote und deaktiviert alle Authentifizierungsmethoden außer Negotiate. Dies wird für Windows NT LAN Manager (NTLM) verwendet und legt den "AllowUnencrypted" Das WSMAN-Protokoll wird auf false gesetzt, um sicherzustellen, dass

der neu erstellte Listener nur verschlüsselten Datenverkehr akzeptiert. Unter Verwendung des von Microsoft bereitgestellten Skripts `New-SelfSignedCertificateEx.ps1`, erstellt es ein selbstsigniertes Zertifikat.

Jede WSMAN-Instanz, die über einen HTTP-Listener verfügt, wird zusammen mit den vorhandenen HTTPS-Listnern entfernt. Anschließend wird ein neuer HTTPS-Listener erstellt. Außerdem wird eine Firewallregel für eingehenden Datenverkehr für TCP-Port 5986 erstellt. Im letzten Schritt wird der WinRM-Dienst neu gestartet.

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

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

```
$PSVersionTable
```

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

```
$PSVersionTable
```

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

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

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

<https://application-data-collector-release.s3.us-west-2.amazonaws.com/scripts/WinRMSetup.ps1>

2. Laden Sie das herunter `New-SelfSignedCertificateEx.ps1` von der folgenden URL und fügen Sie das Skript in denselben Ordner ein, in den Sie es heruntergeladen haben `WinRMSetup.ps1`:

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

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

```
.\WinRMSetup.ps1
```

Note

Wenn Windows Remote Management (WinRM) auf dem Windows-Remoteserver nicht richtig eingerichtet ist, schlägt der Versuch, Daten von diesem Server zu sammeln, fehl. In diesem Fall müssen Sie das Zertifikat, das diesem Server entspricht, vom folgenden Speicherort auf dem Container löschen:

```
/opt/amazon/application-data-collector/remote-auth/windows/certs/ads-server-id.cer
```

Warten Sie nach dem Löschen des Zertifikats, bis der Datenerfassungsvorgang erneut versucht wird.

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

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

```
collector diag-check
```

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

Wenn Sie den Befehl in verwenden -a Modus, Sie erhalten die Ausgabe in einem `DiagnosticCheckResult.txt` Datei, nachdem die Prüfungen abgeschlossen sind.

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

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

Die folgenden Beispiele zeigen das Ergebnis einer erfolgreichen Installation.

Linux-Server

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

Windows-Server

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

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

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

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

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

So erhalten Sie Empfehlungen

1. Melden Sie sich mit dem AWS Konto, das Sie erstellt haben [Erstellung von Strategieempfehlungen](#), bei der Migration Hub Hub-Konsole unter <https://console.aws.amazon.com/migrationhub/> an AWS Management Console und öffnen Sie sie.
2. Wählen Sie im Navigationsbereich der Migration Hub Hub-Konsole Strategie aus.
3. Wählen Sie auf der Seite Strategie-Empfehlungen für den Migration Hub die Option Empfehlungen abrufen aus.
4. Wählen Sie Zustimmung, wenn Sie damit einverstanden sind, dass Migration Hub eine serviceverknüpfte Rolle (SLR) in Ihrem Konto erstellt. Weitere Informationen zur Spiegelreflexkamera finden Sie unter [Verwenden von serviceverknüpften Rollen für Strategieempfehlungen](#)
5. Datenquellen konfigurieren
 - a. Auf der Seite Datenquellen konfigurieren müssen Sie die Quelle Ihrer zu analysierenden Server aus den folgenden Optionen auswählen:
 - i. Strategy Recommendations-Anwendungsdatensammler — Sie können den Strategy Recommendations-Sammler verwenden, um automatisch Informationen über in

- VMware vCenter gehostete VMs abzurufen. Wenn Sie diese Option verwenden, müssen Sie keine zusätzlichen Einstellungen vornehmen.
- ii. **Manueller Import** — Wenn Sie Daten über Ihre Server und Anwendungen unabhängig voneinander importieren möchten, können Sie die Importvorlage *Strategy Recommendations* verwenden. Die Importvorlage ist eine JSON-Datei, in die Sie die verfügbaren Informationen für Ihre VMs eingeben können.
 - iii. **Application Discovery Service** — Sie können den *Application Discovery Service* verwenden, um Informationen über Ihre lokalen Anwendungen und Server zu sammeln. In der Migration Hub Hub-Konsole können Sie im Abschnitt *Tools* unter *Discovery-Tools* aus mehreren Optionen wählen. Sie können beispielsweise *Application Discovery Service Agentless Collector*, *AWSDiscovery Agent* oder *Import* (für CSV-Dateien) wählen.
- b. In der Tabelle *Server* werden alle verfügbaren Server auf der Grundlage Ihrer Auswahl im Abschnitt *Datenquelle* aufgeführt.
 - c. Unter *Registrierte Anwendungsdatensammelpunkte* werden die Anwendungsdatensammelpunkte aufgeführt, die Sie eingerichtet haben. Wenn Sie keine Datensammelpunkte eingerichtet haben, können Sie den Datensammelpunkt herunterladen und dann bereitstellen. Weitere Informationen finden Sie unter [Schritt 1: Laden Sie den Strategy Recommendations Collector herunter](#) und [Schritt 2: Stellen Sie den Strategy Recommendations Collector bereit](#).
-  **Note**

Um Strategieempfehlungen zu erhalten, müssen Sie mindestens einen Anwendungsdatensammelpunkt einrichten oder einen Anwendungsdatenimport durchführen. Wenn Sie Ihre Daten auf Anwendungsebene hinzufügen möchten, ohne einen Collector einzurichten, können Sie die Vorlage für den Import von Anwendungsdaten verwenden. Sie können später weitere Datenquellen hinzufügen.
- d. Wenn Sie *Manueller Import* ausgewählt haben, wählen Sie unter *Importdetails* die Option *Neuen Import hinzufügen* aus.
 - e. Geben Sie unter *Importname* einen Namen für Ihren Import ein.
 - f. Geben Sie für *S3-Bucket-URI* den S3-Bucket-URI ein, in den Ihre Import-JSON-Datei hochgeladen werden soll.

 **Important**

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

- g. Wählen Sie Weiter.
6. Geben Sie die Einstellungen an
 - a. Richten Sie auf der Seite „Einstellungen angeben“ Ihre Geschäftsziele und Migrationspräferenzen ein. Strategy Recommendations empfiehlt die optimale Strategie für die Migration und Modernisierung Ihrer Anwendungen und Datenbanken auf der Grundlage der von Ihnen angegebenen Einstellungen. Sie können diese Einstellungen zu einem späteren Zeitpunkt ändern.
 - b. Wählen Sie Weiter.
 7. Überprüfen und abschicken.
 - a. Überprüfen Sie Ihre konfigurierten Datenquellen und Migrationseinstellungen.
 - b. Wenn alles korrekt aussieht, wählen Sie Datenanalyse starten. Dadurch werden Ihr Serverinventar und Ihre Laufzeitumgebung sowie die Anwendungsbinärdateien für Ihre Microsoft IIS- und Java-Anwendungen analysiert.

 **Note**

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

Strategie, Empfehlungen, Empfehlungen.

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

Themen

- [Strategieempfehlungen finden Sie unter Strategieempfehlungen](#)
- [Strategieempfehlungen, Empfehlungen für Anwendungskomponenten](#)
- [Strategieempfehlungen, Serverempfehlungen](#)
- [Einstellungen für Strategie und Empfehlungen](#)

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 haben [Erstellung 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 [Strategieempfehlungen, Empfehlungen für Anwendungskomponenten](#).
5. Auf der Registerkarte Server können Sie die Empfehlungen für die Server in Ihrem Migrationsportfolio einsehen. Weitere Informationen finden Sie unter [Strategieempfehlungen, Serverempfehlungen](#).
6. Auf der Registerkarte Einstellungen können Sie die Einstellungen bearbeiten, die Sie unter angegeben haben [Schritt 5: Empfehlungen einholen](#). Informationen zur Bearbeitung Ihrer Einstellungen finden Sie unter [Einstellungen für Strategie und Empfehlungen](#).

Strategieempfehlungen, Empfehlungen für Anwendungskomponenten

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

Themen

- [Arbeiten mit Anwendungskomponenten in Strategieempfehlungen](#)
- [Strategieempfehlungen, Quellcode-Analyse](#)
- [Datenbankanalyse für Strategy Recommendations](#)
- [Strategieempfehlungen, binäre Analyse](#)

Arbeiten mit Anwendungskomponenten in Strategieempfehlungen

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

Themen

- [Empfehlungen für Anwendungskomponenten anzeigen](#)
- [Konfigurieren Sie die Quellcodeanalyse für eine Anwendungskomponente](#)
- [Konfigurieren Sie die Datenbankanalyse für eine Anwendungskomponente](#)

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 Empfehlungen für Anwendungskomponenten anzuzeigen

1. Melden Sie sich mit dem AWS Konto, das Sie erstellt haben [Erstellung 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 Empfehlungsübersicht können Sie die Empfehlungen für die Anwendungskomponente einsehen. Sie können sich auch identifizierte Anti-Pattern ansehen. Bei Anti-Pattern handelt es sich um eine Liste bekannter Probleme in Ihrem Portfolio, die nach Schweregrad kategorisiert sind.
6. Wählen Sie die Registerkarte Strategieoptionen, um die Migrationsempfehlung für die Anwendungskomponente anzuzeigen. Sie können die empfohlene Strategie außer Kraft setzen, indem Sie eine andere Strategie auswählen und dann Als bevorzugt festlegen klicken.
7. Je nachdem, welche Art von Anwendungskomponente Sie betrachten, gibt es eine Registerkarte „Quellkonfiguration“ oder „Datenbankkonfiguration“. Hinweise zur Quellkonfiguration finden Sie unter [Konfigurieren Sie die Quellcodeanalyse für eine Anwendungskomponente](#). Hinweise zur Datenbankkonfiguration finden Sie unter [Konfigurieren 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 aus IIS, und klicken Sie dann auf Details anzeigen.
4. Wählen Sie auf der Detailseite der Anwendungskomponente (der 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 unter [Strategieempfehlungen, 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 SQLServer und klicken Sie dann auf Details anzeigen.
4. Wählen Sie auf der Detailseite der Anwendungskomponente (die Seite mit dem Namen der Komponente als Überschrift) die Registerkarte Datenbankkonfiguration.
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 unter [Datenbankanalyse 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 unter [Konfigurieren 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 unter [Voraussetzungen 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 Serverdatenbank enthält, wird diese als Anwendungskomponente sqlservr.exe identifiziert.

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

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

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 unter [Erforderliche Rechte für Anmeldeinformationen für AWS das Schema Conversion Tool](#). Informationen zum Erstellen eines Geheimnisses

mit den Anmeldeinformationen finden Sie unter [Ein 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 (examplepbs1 und examplepbs2) verfügt, wird für jede der Datenbanken eine Anwendungskomponente mit den Namen examplepbs1 und examplepbs2 erstellt.

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

Erforderliche Rechte für Anmeldeinformationen für AWS das Schema Conversion Tool

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

Sie können bei der Erstellung der SQL Serveranmeldung einen beliebigen Anmeldenamen und ein beliebiges Passwort 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 an [Erstellung von Strategieempfehlungen](#), das Sie erstellt haben, 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.
6. Geben Sie Secret Name als eine beliebige Zeichenfolge mit dem Präfix migrationhub-strategy - ein. Zum Beispiel. migrationhub-strategy-one

 Note

Bewahren Sie Ihren geheimen Namen zur späteren Verwendung an einem sicheren Ort auf.

7. Wählen Sie Weiter und dann erneut Weiter.
8. Wählen Sie Store (Speichern) aus.

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

Strategieempfehlungen, binäre Analyse

Migration Hub Strategy Recommendations identifiziert automatisch die Anwendungen in Ihrem Portfolio und die zugehörigen Anwendungskomponenten. Wenn Ihr Portfolio beispielsweise eine Java-Anwendung enthält, identifiziert Strategy Recommendations sie als Anwendungskomponente mit dem Komponententyp Java. Strategy Recommendations kann Binäranalysen durchführen, ohne dass Sie den Zugriff DLLs auf den Quellcode konfigurieren müssen, indem sie die Anwendung unter Windows oder die IIS JAR Anwendungsdateien 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 Zugriff auf den Quellcode gewähren, wie unter beschrieben [Richten 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 haben [Erstellung 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 einsehen, die auf den Empfehlungen basieren. Informationen zur „R“-Strategie finden Sie unter [Migrationsbegriffe — 7 Rs im Glossar AWS Prescriptive Guidance](#).
4. Um ausführliche Empfehlungsdetails für einen Server anzuzeigen, wählen Sie den Server aus der Liste aus und klicken Sie dann auf Details anzeigen. Sie können die für den Server

- gesammelten Metadaten zusammen mit ausführlichen Analysen und Empfehlungen anzeigen, die auf den Anwendungskomponenten basieren, die auf dem Server ausgeführt werden.
5. Auf der Seite mit den Serverdetails (der Seite mit dem Servernamen als Überschrift) finden Sie unter Zusammenfassung der Empfehlungen einen Überblick über die Strategieempfehlungen für den Server. Sie können sich auch identifizierte Anti-Pattern ansehen. Bei Anti-Pattern handelt es sich um eine Liste bekannter Probleme in Ihrem Portfolio, die nach Schweregrad kategorisiert sind.
 6. Wählen Sie die Registerkarte Strategieoptionen, um die Migrationsempfehlung für den Server anzuzeigen. Sie können die empfohlene Strategie außer Kraft setzen, indem Sie eine andere Strategie auswählen und dann Als bevorzugt festlegen auswählen.
 7. Wählen Sie die Registerkarte Anwendungskomponenten, um die Liste der Anwendungskomponenten anzuzeigen, die dem Server zugeordnet sind.
 8. Um Details zur Anwendungskomponente anzuzeigen, wählen Sie die Komponente aus der Liste aus und klicken Sie dann auf Details anzeigen. Weitere Informationen zu Anwendungskomponenten finden Sie unter [Arbeiten 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 beschrieben [Schritt 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 haben [Erstellung 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](#)
- [Strategie, Empfehlungen, Anwendungsdatensammler](#)
- [Daten in Strategy Recommendations importieren](#)
- [Ihre Daten aus den Strategieempfehlungen entfernen](#)

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 haben [Erstellung 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 unter [Strategie, 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 unter [Schritt 1: Laden Sie den Strategy Recommendations Collector herunter](#).

Themen

- [Vom Kollektor für Strategieempfehlungen gesammelte Daten](#)
- [Den Strategy Recommendations Collector aktualisieren](#)

Vom Kollektor für Strategieempfehlungen gesammelte Daten

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

Datenfeld	Beschreibung
Typ des Betriebssystems	Windows oder Linux
Betriebssystemversion	Die spezifische Version des Betriebssystems. Zum Beispiel Windows Server 2003, RHEL 5.2.
Betriebssystem-Architektur	32-Bit- oder 64-Bit-Betriebssystem
Ist Server-VM	Der Server ist eine VM oder eine physische Maschine.
Virtualisierungssoftware	Zum Beispiel vCenter Hyper-V.
Ort	Zum Beispiel die Amazon Elastic Compute Cloud-Konsole (AmazonEC2) oder lokal.
Ist dualBoot	Ermöglicht das Booten in mehrere OSs
Firmware-Typ	BIOS, UEFI

Datenfeld	Beschreibung
Bootloader	GRUB, GRUB 2
Typ der Partitionstabelle	MBR, GPT
CPU-Geschwindigkeit	CPU-schnell rein GHz. Zum Beispiel 2.4 GHz.
Windows OS data	
Windows-Ausgabe	Standard, Rechenzentrum, Unternehmen
.NET Framework-Version	Die Version der .NET Framework installiert.
.NET Kernversion	Die Version von .NET Core ist installiert.
Linux data	
Linux-Betriebssystemverteilung	RHEL, CentOS SUSE und so weiter.
Kernel-Version	Ausgabe von <code>uname -r</code> , z. B. <code>4.9.217-0.1.ac.205.84.332.meta11.x86_64</code>
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 <code>SQLServr EXE</code> , <code>MSDtsSrvr EXE</code> und so weiter.
Anwendungstyp	IIS, JBoss, Tomcat und so weiter.

Datenfeld	Beschreibung
Programmiersprache und Version	C#, Java
JDKVersion	Die Version der JDK installierten.
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	
.NETVon der App verwendete Framework-Version	Die Version von .NETFrameworkDLL, das zur Laufzeit für die Anwendung geladen wird.
.NETKernversion	Die Version. NETDer Kern DLL wird zur Laufzeit der Anwendung geladen.
Verwendet WPF Framework?	Ermittelt, ob der .NETDie basierte Anwendung ist eine Art WPF App oder nicht.
Verwendet WCF Framework?	Ermittelt, ob der .NETDie basierte Anwendung ist eine Art von WCF App oder nicht.
ASP.NETVersion	Die Version vonASP.NET.
IISVersion	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, zu finden. NETVersion und so weiter.

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	MSSQL, OracleSQL, My 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 Support](#) und 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 über einen SSH Client 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 haben [Erstellung 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 das 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“, "DEBIANSL ES", "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
MacAdresses	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“
AssociateServerIds	Eine Liste der Server, IDs auf denen der Prozess läuft.	String	Ja	Der ResourceId aus dem "ResourceType,:" SERVER ", den Sie definiert haben.
ApplicationType	Die Art der Anwendung	String	Ja	„Tomcat“, „JBoss“, „Spring“, „IIS“, „Mongo DB“, „DB2“, „Maria DB“, „MeinSQL“, „Oracle“,

Name	Beschreibung	Typ	Erforderlich	Zulässige Werte
				"", SQLServer „Sybase“, „PostgreSQLServer“, „Cassandra“, „Oracle IBM WebSphere“, „Java WebLogic Generic“
ApplicationVersion	Die Version der Anwendung	String	Ja	"IIS1.0", "IIS 2.0", "IIS3.0", "IIS 4.0", "IIS5.0", "IIS 5.1", "IIS6.0", "IIS 7.5", "8.5", "8.5", "10.0" IIS IIS IIS IIS
ProgrammingLanguage	Die Programmiersprache für die Anwendung	String	Nein	„Java“, "CSharp“

Name	Beschreibung	Typ	Erforderlich	Zulässige Werte
DotNetFrameworkVersion	Die Version von.NETFramework, wenn die Anwendung ist.NETFramework-basiert	String	Nein	"DotnetFramework 1,0"," DotnetFramework 1,0 SP1 "," 1,0 "," DotnetFramework 1,0 SP2 "," DotnetFramework 1,1", "DotnetFramework 1,1"," 2,0", "DotnetFramework DotnetFramework2,0"," 2,0 SP1 "," DotnetFramework 3,0", "DotnetFramework DotnetFramework 3,0 SP2 "," 3,5", "DotnetFramework 3,5"," DotnetFramework 4,5", "DotnetFramework4,5"," 4,5", "4,5,1"DotnetFramework ," DotnetFramework DotnetFramework 4,5,2", "4,6"," DotnetFramework 4,6,1", "DotnetFramework DotnetFramework 4,6,2"," 4,7", "DotnetFramework 4,7"," 4,6" 7,1", " SP3 SP1 SP1 SP2 SP1 DotnetFramework DotnetFramework DotnetFramework 4,7,2 Zoll, "DotnetFramework 4,8 Zoll

Name	Beschreibung	Typ	Erforderlich	Zulässige Werte
DotNetCoreVersion	Die Version von.NETKern, wenn die Anwendung ist.NETKernbasiert	String	Nein	".NETKern 1.0", ".NETKern 1.1", ".NETKern 2.0", ".NETKern 2.1", ".NETKern 2.2", ".NETKern 3.0", ".NETKern 3.1"
JdkVersion	Die Version vonJDK, falls die Anwendung die verwendet JDK	String	Nein	"JDK1.0", "JDK2 .0", ".0", ..., "JDK3" .0" JDK11
DatabaseType	Der Typ Datenbank	String	Nein	"SQLServer", "Oracle", "Sybase", "Mongo DB", "Maria DB", "Apache Cassandra", "Mein", "SQL", "IBM DB2", "PostgreSQLServer"
DatabaseEdition	Die Ausgabe der Datenbank	String	Nein	
DatabaseVersion	Die Version der Datenbank	String	Nein	Sehen Sie sich die HTML Version der Dokumentation an.

Ihre Daten aus den Strategieempfehlungen entfernen

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

Strategieempfehlungen für Sicherheit im Migration Hub

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

Sicherheit ist eine übergreifende Verantwortlichkeit zwischen AWS und Ihnen. Das [Modell der geteilten Verantwortung](#) beschreibt dies als Sicherheit der Cloud selbst und als Sicherheit in der Cloud:

- Sicherheit der Cloud – AWS ist dafür verantwortlich, die Infrastruktur zu schützen, mit der AWS-Services in der AWS Cloud ausgeführt werden. AWS stellt Ihnen außerdem Services bereit, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der [AWS-Compliance-Programme](#) regelmäßig. Weitere Informationen zu den Compliance-Programmen, die für die Strategieempfehlungen von Migration Hub gelten, finden Sie unter [AWS Services im Umfang nach Compliance-Programm AWS](#).
- Sicherheit in der Cloud – Ihr Verantwortungsumfang wird durch den AWS-Dienst bestimmt, den Sie verwenden. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

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

Themen

- [Datenschutz in den Strategieempfehlungen des Migration Hub](#)
- [Strategieempfehlungen für Identitäts- und Zugriffsmanagement für Migration Hub](#)
- [Überprüfung der Einhaltung der Vorschriften für die Strategieempfehlungen von Migration Hub](#)

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 im [Abschnitt Datenschutz FAQ](#). Informationen zum Datenschutz in Europa finden Sie im [AWS Shared Responsibility Model und](#) im GDPR Blogbeitrag auf dem AWS Security Blog.

Aus Datenschutzgründen empfehlen wir, dass Sie Ihre 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 eine Multi-Faktor-Authentifizierung (MFA).
- Verwenden Sie SSL/TLS, um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Einrichtung API und Protokollierung von Benutzeraktivitäten mit AWS CloudTrail.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie FIPS 140-3 validierte kryptografische Module für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine benötigen API, verwenden Sie einen Endpunkt. FIPS Weitere Informationen zu den verfügbaren FIPS Endpunkten finden Sie unter [Federal Information Processing Standard](#) () 140-3. FIPS

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 arbeiten, API, AWS CLI oder 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 einem externen Server eine URL zur Verfügung stellen, empfehlen wir dringend, dass Sie keine Anmeldeinformationen angeben, URL um Ihre Anfrage an diesen Server zu validieren.

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 AWS Ressourcen sicher zu kontrollieren. IAMAdministratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Ressourcen von Strategy Recommendations zu nutzen. IAMist eine AWS-Service , die Sie ohne zusätzliche Kosten nutzen können.

Themen

- [Zielgruppe](#)
- [Authentifizierung mit Identitäten](#)
- [Verwalten des Zugriffs mit Richtlinien](#)
- [So funktioniert Migration Hub Strategy Recommendations mit IAM](#)
- [AWS verwaltete Richtlinien für Strategieempfehlungen für den Migration Hub](#)
- [Identitätsbasierte Politikbeispiele für Strategieempfehlungen Migration Hub Migrationszentren](#)
- [Fehlerbehebung bei der Migration Hub-Strategie, Empfehlungen, Identität und Zugriff](#)
- [Verwenden von serviceverknüpften Rollen für Strategieempfehlungen](#)
- [Migrations-Hub-Strategieempfehlungen und Schnittstellen-VPC-Endpunkte \(AWS PrivateLink\)](#)

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, die 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 unter [Fehlerbehebung 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 Anfragen an Ihren IAM Administrator senden, um die Berechtigungen Ihrer Servicebenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die grundlegenden Konzepte von zu verstehen IAM. Weitere Informationen darüber, wie Ihr Unternehmen Strategieempfehlungen nutzen IAM kann, finden Sie unter [So 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 Strategy Recommendations zu verwalten. Beispiele für identitätsbasierte Richtlinien von Strategy Recommendations, die Sie in verwenden können IAM, 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 sich als IAM Benutzer authentifizieren (angemeldet bei AWS) oder indem Sie eine IAM Rolle übernehmen. 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-) Nutzer, die Single-Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als föderierte Identität anmelden, hat Ihr Administrator zuvor einen Identitätsverbund mithilfe von Rollen eingerichtet. IAM Wenn Sie AWS mithilfe eines Verbunds darauf zugreifen, 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, mit der Sie Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch signieren können. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode, um Anfragen selbst zu [signieren, finden Sie im IAMBenutzerhandbuch unter AWS API Anfragen signieren](#).

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. 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 [Verwenden der Multi-Faktor-Authentifizierung \(MFA\) AWS im IAM Benutzerhandbuch](#).

AWS-Konto Root-Benutzer

Wenn Sie ein AWS-Konto erstellen, 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 und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie im Benutzerhandbuch unter [Aufgaben, für die Root-Benutzeranmeldedaten erforderlich](#) sind. IAM

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 [IAMBenutzer](#) ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wir empfehlen, sich nach Möglichkeit auf temporäre Anmeldeinformationen zu verlassen, anstatt IAM Benutzer mit langfristigen Anmeldeinformationen wie Passwörtern und Zugriffsschlüsseln zu erstellen. Wenn Sie jedoch spezielle Anwendungsfälle haben, für die langfristige Anmeldeinformationen von IAM Benutzern erforderlich sind, empfehlen wir, die Zugriffsschlüssel abwechselnd zu verwenden. Weitere Informationen finden Sie im Benutzerhandbuch unter [Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, für die IAM langfristige Anmeldeinformationen erforderlich sind](#).

Eine [IAMGruppe](#) ist eine Identität, die eine Sammlung von IAM Benutzern spezifiziert. 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 IAMAdmins und 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 [Wann sollte ein IAM Benutzer \(statt einer Rolle\) erstellt werden?](#) im IAMBenutzerhandbuch.

IAMRollen

Eine [IAMRolle](#) ist eine Identität innerhalb von Ihnen AWS-Konto , für die bestimmte Berechtigungen gelten. Sie ähnelt einem IAM Benutzer, ist jedoch keiner bestimmten Person zugeordnet. Sie können vorübergehend eine IAM Rolle in der übernehmen, AWS Management Console indem Sie die [Rollen wechseln](#). Sie können eine Rolle übernehmen, indem Sie eine AWS CLI AWS API OR-Operation

aufrufen oder eine benutzerdefinierte Operation verwenden URL. Weitere Informationen zu Methoden zur Verwendung von Rollen finden Sie [unter Verwenden von IAM Rollen](#) im IAM Benutzerhandbuch.

IAM Rollen mit temporären Anmeldeinformationen sind in den folgenden Situationen nützlich:

- **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 im IAM Benutzerhandbuch unter [Erstellen einer Rolle für einen externen Identitätsanbieter](#). Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Um zu kontrollieren, 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 verschiedene Berechtigungen für eine bestimmte Aufgabe zu übernehmen.
- **Kontoübergreifender Zugriff** — Sie können eine IAM Rolle verwenden, um jemandem (einem vertrauenswürdigen Principal) 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 zum Unterschied zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie [IAM im Benutzerhandbuch unter Kontoübergreifender Ressourcenzugriff](#). IAM
- **Serviceübergreifender Zugriff** — Einige AWS-Services verwenden Funktionen in anderen. AWS-Services Wenn Sie beispielsweise einen Service aufrufen, 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.
- **Zugriffssitzungen weiterleiten (FAS)** — Wenn Sie einen IAM Benutzer oder eine 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 an aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen AWS-Service an 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 beim Stellen von FAS Anfragen finden Sie unter [Zugriffssitzungen weiterleiten](#).

- **Servicerolle** — Eine Servicerolle ist eine [IAMRolle](#), die ein Dienst übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM Administrator kann eine Servicerolle von innen heraus erstellen, ändern und löschenIAM. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter [Erstellen einer Rolle zum Delegieren von Berechtigungen AWS-Service an eine](#).
- **Dienstbezogene Rolle** — Eine dienstverknüpfte 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 dienstbezogene 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 IAMBenutzerhandbuch unter [Verwenden einer IAM Rolle zur Erteilung von Berechtigungen für Anwendungen, die auf EC2 Amazon-Instances ausgeführt werden](#).

Informationen darüber, ob Sie IAM Rollen oder IAM Benutzer verwenden sollten, finden [Sie im Benutzerhandbuch unter Wann sollte eine IAM Rolle \(anstelle eines IAM Benutzers\) erstellt werden](#).

Verwalten des Zugriffs mit Richtlinien

Sie steuern 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. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden in AWS Form von JSON Dokumenten gespeichert. Weitere Informationen zur Struktur und zum Inhalt von JSON Richtliniendokumenten finden Sie im IAMBenutzerhandbuch unter [Überblick über JSON Richtlinien](#).

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

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Um Benutzern die Erlaubnis zu erteilen, Aktionen mit den Ressourcen durchzuführen, die sie benötigen, kann ein IAM Administrator IAM Richtlinien erstellen. Der Administrator kann dann die IAM Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen übernehmen.

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

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind Dokumente mit JSON Berechtigungsrichtlinien, die Sie an eine Identität anhängen können, z. B. an einen IAM Benutzer, eine Benutzergruppe oder eine Rolle. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen einer identitätsbasierten Richtlinie finden Sie unter [IAM Richtlinien erstellen im Benutzerhandbuch](#). IAM

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 zur Auswahl zwischen einer verwalteten Richtlinie und einer Inline-Richtlinie finden Sie im IAM Benutzerhandbuch unter [Auswahl zwischen verwalteten Richtlinien und Inline-Richtlinien](#).

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele für ressourcenbasierte Richtlinien sind IAM Rollenvertrauensrichtlinien und Amazon S3 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 nicht IAM 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 AWS WAF Amazon VPC sind Beispiele für Dienste, die Unterstützung bieten ACLs. 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 eine erweiterte Funktion, mit der Sie die maximalen Berechtigungen festlegen, die eine identitätsbasierte Richtlinie einer IAM Entität (IAM Benutzer oder Rolle) gewähren 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 zu Berechtigungsgrenzen finden Sie im IAM Benutzerhandbuch unter [Berechtigungsgrenzen für IAM Entitäten](#).
- **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 Geräte 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. Weitere Informationen zu

Organizations und SCPs finden Sie unter [Richtlinien zur Servicesteuerung](#) 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 im IAMBenutzerhandbuch unter [Sitzungsrichtlinien](#).

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 IAMBenutzerhandbuch unter [Bewertungslogik für Richtlinien](#).

So funktioniert Migration Hub Strategy Recommendations mit IAM

Bevor Sie IAM den Zugriff auf Strategy Recommendations verwalten, sollten Sie sich darüber informieren, welche IAM Funktionen für Strategy Recommendations verfügbar sind.

IAMFunktionen, die Sie mit den Strategieempfehlungen von Migration Hub verwenden können

IAMFunktion	Unterstützung von Strategieempfehlungen
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Nein
Bedingungsschlüssel für die Richtlinie	Nein
ACLs	Nein

IAMFunktion	Unterstützung von Strategieempfehlungen
ABAC(Tags in Richtlinien)	Nein
Temporäre Anmeldeinformationen	Ja
Hauptberechtigungen	Ja
Servicerollen	Nein
Serviceverknüpfte Rollen	Ja

Einen allgemeinen Überblick darüber, wie Strategieempfehlungen und andere AWS Dienste mit den meisten IAM Funktionen funktionieren, finden Sie IAM im IAMBenutzerhandbuch unter [AWS Dienste, die mit funktionieren](#).

Identitätsbasierte Richtlinien für Strategieempfehlungen

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identitätsbasierte Richtlinien sind Dokumente mit JSON Berechtigungsrichtlinien, die Sie an eine Identität anhängen können, z. B. an einen IAM Benutzer, eine Benutzergruppe oder eine Rolle. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen einer identitätsbasierten Richtlinie finden Sie unter [IAMRichtlinien erstellen im Benutzerhandbuch](#). IAM

Mit IAM identitätsbasierten Richtlinien können Sie zulässige oder verweigerte Aktionen und Ressourcen sowie die Bedingungen angeben, unter denen Aktionen zulässig oder verweigert werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Weitere Informationen zu allen Elementen, die Sie in einer JSON Richtlinie verwenden können, finden Sie in der [Referenz zu den IAM JSON Richtlinienelementen](#) im IAMBenutzerhandbuch.

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 einer Ressource anhängen. Beispiele für ressourcenbasierte Richtlinien sind IAM Rollenvertrauensrichtlinien und Amazon S3 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 den kontoübergreifenden Zugriff zu ermöglichen, können Sie in einer ressourcenbasierten Richtlinie ein ganzes Konto oder IAM Entitäten in einem anderen Konto als Prinzipal 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 Prinzipalentsität (Benutzer oder Rolle) die Berechtigung zum Zugriff auf die Ressource gewähren. 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 [IAMim IAMBenutzerhandbuch unter Kontenübergreifender Ressourcenzugriff](#).

Politische Maßnahmen für Strategieempfehlungen

Unterstützt Richtlinienaktionen: Ja

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

Das `Action` Element 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, für die nur eine Genehmigung erforderlich ist und für die es keinen entsprechenden Vorgang gibt. API 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 bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das `Resource` JSON Richtlinienelement gibt das Objekt oder die Objekte an, für die die Aktion gilt. Anweisungen müssen entweder ein `Resource` oder ein `NotResource`-Element enthalten. Es hat sich bewährt, eine Ressource mit ihrem [Amazon-Ressourcennamen \(ARN\)](#) anzugeben. 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 zu den Aktionen, mit denen Sie die einzelnen Ressourcen spezifizieren können, finden Sie unter In den [Strategieempfehlungen ARN 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 Bedingungschlüssel 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. Sie können einem IAM Benutzer beispielsweise nur dann Zugriff auf eine Ressource gewähren, wenn sie mit seinem IAM Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter [IAMRichtlinienelemente: Variablen und Tags](#).

AWS unterstützt globale Bedingungschlüssel und dienstspezifische Bedingungschlüssel. Eine Übersicht aller AWS globalen Bedingungschlüssel finden Sie unter [Kontext-Schlüssel für AWS globale Bedingungen](#) im IAMBenutzerhandbuch.

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 () mit Strategieempfehlungen ABAC

Unterstützt ABAC (Tags in Richtlinien): Nein

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen auf der Grundlage von Attributen definiert werden. In werden AWS diese Attribute als Tags bezeichnet. Sie können Tags an IAM Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC Richtlinien, die Operationen zulassen, wenn das Tag des Prinzipals mit dem Tag auf der Ressource übereinstimmt, auf die er zugreifen möchte.

ABAC ist hilfreich in Umgebungen, die schnell wachsen, und hilft in Situationen, in denen die Richtlinienverwaltung umständlich wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungelement 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 finden Sie ABAC unter [Was ist? ABAC](#) im IAM Benutzerhandbuch. Ein Tutorial mit Schritten zur Einrichtung finden Sie im ABAC Benutzerhandbuch unter [Verwenden der attributbasierten Zugriffskontrolle \(ABAC\)](#). IAM

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 darüber, AWS-Services wie Sie mit temporären Anmeldeinformationen [arbeiten können AWS-Services](#), finden Sie IAM im IAMBenutzerhandbuch.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Kennwort 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 Rollenwechsel finden Sie unter [Wechseln zu einer Rolle \(Konsole\)](#) im IAMBenutzerhandbuch.

Mit dem AWS CLI oder können Sie manuell temporäre Anmeldeinformationen erstellen AWS API. 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 unter IAM](#).

Serviceübergreifende Prinzipalberechtigungen für Strategieempfehlungen

Unterstützt Forward-Access-Sitzungen (FAS): Ja

Wenn Sie einen IAM Benutzer oder eine 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. FASverwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen AWS-Service an nachgelagerte Dienste zu stellen. FASANfragen 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 beim Stellen von FAS Anfragen finden Sie unter [Zugriffssitzungen weiterleiten](#).

Servicerollen für Strategieempfehlungen

Unterstützt Servicerollen: Nein

Eine Servicerolle ist eine [IAMRolle](#), die ein Dienst übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM Administrator kann eine Servicerolle von innen heraus erstellen, ändern und löschen IAM. Weitere Informationen finden Sie im IAM Benutzerhandbuch unter [Erstellen einer Rolle zum Delegieren von Berechtigungen AWS-Service an eine](#).

 Warning

Das Ändern der Berechtigungen für eine Servicerolle kann die Funktionalität von Strategy Recommendations beeinträchtigen. 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 dienstbezogene 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: `AWSMigrationHubStrategyConsoleFullAccess`

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

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

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `discovery`— Gewährt dem Benutzer Zugriff auf den Abruf einer Discovery-Zusammenfassung im Application Discovery Service.
- `iam`— Ermöglicht die Erstellung einer dienstbezogenen Rolle für den Benutzer. Dies ist eine Voraussetzung für die Verwendung von Strategy Recommendations.
- `migrationhub-strategy`— Gewährt dem Benutzer vollen Zugriff auf Strategy Recommendations.

- `s3`— Ermöglicht dem Benutzer, die von Strategy Recommendations verwendeten S3-Buckets zu erstellen und aus ihnen zu lesen.
- `secretsmanager`— Ermöglicht dem Benutzer, den Zugriff auf geheime Daten im Secrets Manager aufzulisten.

Die Berechtigungen für diese Richtlinie finden Sie [AWSMigrationHubStrategyConsoleFullAccess](#) im Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: `AWSMigrationHubStrategyCollector`

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

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `application-transformation`— Erteilt Berechtigungen zum Hochladen von Protokoll- und Metrikdaten für Operationen zur Anwendungstransformation und zur Arbeit mit Portierungskompatibilitätsbewertungen und Empfehlungen.
- `execute-api`— Ermöglicht dem Benutzer den Zugriff auf Amazon API Gateway, um Protokolle und Metriken hochzuladen AWS.
- `migrationhub-strategy`— Gewährt dem Benutzer Zugriff zum Registrieren von Nachrichten, Senden von Nachrichten, Hochladen von Protokolldaten und Hochladen von Metrikdaten in Strategy Recommendations.
- `s3`— Gewährt dem Benutzer Zugriff auf Listenbereiche und deren Standorte. Benutzern wird außerdem Zugriff auf die von Strategy Recommendations verwendeten S3-Buckets gewährt, sie können Objekte abrufen, Objekte hinzufügen, deren Zugriffskontrollliste (ACL) zurückgeben, sie erstellen, darauf zugreifen, die Verschlüsselung für konfigurieren, die `PublicAccessBlock` Konfiguration ändern, den Versionsstatus für festlegen und eine Lebenszykluskonfiguration für die von Strategy Recommendations verwendeten S3-Buckets erstellen oder ersetzen.
- `secretsmanager`— Ermöglicht dem Benutzer den Zugriff auf Geheimnisse im Secrets Manager, die von Strategy Recommendations verwendet werden.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie

[AWSMigrationHubStrategyCollector](#) im Referenzhandbuch für AWS verwaltete Richtlinien.

Strategieempfehlungen und Aktualisierungen AWS verwalteter Richtlinien

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

Änderung	Beschreibung	Datum
AWSMigrationHubStrategyCollector – Aktualisierung auf eine bestehende Richtlinie	Diese Richtlinie wurde aktualisiert und umfasst nun die Aktionen <code>PutLogData</code> , <code>StartPortingCompatibilityAssessment</code> , <code>GetPortingCompatibilityAssessment</code> , <code>StartPortingRecommendationAssessment</code> und <code>GetPortingRecommendationAssessment</code> Anwendungstransformation, damit der Anwendungstransformationsservice Protokolle und Metriken an den Dienst senden kann. Die <code>ListBucket</code> und <code>GetBucketLocation</code> wurden für Amazon Simple Storage Service (Amazon S3) hinzugefügt, um Protokoll- und Metrik-Uploads zu unterstützen.	1. April 2024

Änderung	Beschreibung	Datum
	<p>zen. Die beiden PutLogData und PutMetricData wurden auch hinzugefügt, damit der Strategy Recommendations-Collector Logs und Metriken an den Endpunkt des Services senden kann.</p>	
<p>AWSMigrationHubStrategyCollector – Aktualisierung auf eine bestehende Richtlinie</p>	<p>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, dass die Genehmigung aws:ResourceAccount der aws:PrincipalAccount zur Nutzung des enthaltenen Amazon Simple Storage Service und der entsprechenden AWS Secrets Manager Aktionen entsprechen.</p>	<p>5. Februar 2024</p>

Änderung	Beschreibung	Datum
AWSMigrationHubStrategyCollector – Aktualisierung auf eine bestehende Richtlinie	Diese Richtlinie wurde mit den folgenden Amazon S3 S3-APIs aktualisiert — CreateBucket PutEncryptionConfiguration ,PutBucketPublicAccessBlock ,PutBucketPolicy ,PutBucketVersioning , undPutLifecycleConfiguration .	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 mit drei AWS Application Discovery Service APIs aktualisiert — DescribeConfigurations DescribeTags , undListConfigurations .	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
<p>AWSMigrationHubStrategyConsoleFullAccess— Neue Richtlinie wird beim Start veröffentlicht</p>	<p>AWSMigrationHubStrategyConsoleFullAccess gewährt einem Benutzer vollen Zugriff auf den Strategy Recommendations-Service über die AWS Management Console.</p>	<p>25. Oktober 2021</p>
<p>AWSMigrationHubStrategyCollector— Neue Richtlinie wird beim Start verfügbar gemacht</p>	<p>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</p>	<p>25. Oktober 2021</p>
<p>AWSMigrationHubStrategyServiceRolePolicy— Neue Richtlinie wird beim Start zur Verfügung gestellt</p>	<p>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).</p>	<p>25. Oktober 2021</p>

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 von AWS Management Console, AWS Command Line Interface (AWS CLI) oder ausführen AWS API. Um Benutzern die Berechtigung zu erteilen, Aktionen mit den Ressourcen durchzuführen, die sie benötigen, kann ein IAM Administrator IAM Richtlinien erstellen. Der Administrator kann dann die IAM Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen übernehmen.

Informationen zum Erstellen einer IAM identitätsbasierten Richtlinie anhand dieser JSON Beispieldokumente finden Sie unter [IAM Richtlinien erstellen](#) 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 Konsole „Strategy Recommendations“](#)
- [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 AWS im IAMBenutzerhandbuch unter [AWS Verwaltete Richtlinien oder Verwaltete Richtlinien für Jobfunktionen](#).
- Berechtigungen mit den geringsten Rechten anwenden — Wenn Sie Berechtigungen mit IAM Richtlinien festlegen, gewähren Sie nur die Berechtigungen, die für die Ausführung 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 IAM zum Anwenden von Berechtigungen finden Sie [IAMim Benutzerhandbuch unter Richtlinien und Berechtigungen](#). IAM
- Verwenden Sie Bedingungen in IAM Richtlinien, um den Zugriff weiter einzuschränken — Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen einzuschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um anzugeben, dass alle Anfragen über gesendet werden müssenSSL. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese über einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter [IAMJSONRichtlinienelemente: Bedingung](#).
- Verwenden Sie IAM Access Analyzer, um Ihre IAM Richtlinien zu validieren, um sichere und funktionale Berechtigungen zu gewährleisten. IAM Access Analyzer validiert neue und bestehende Richtlinien, sodass die Richtlinien der IAM Richtliniensprache (JSON) und den IAM bewährten Methoden entsprechen. IAMAccess Analyzer bietet mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen, um Sie bei der Erstellung sicherer und funktionaler Richtlinien zu unterstützen. Weitere Informationen finden Sie unter [IAMAccess Analyzer-Richtlinienväldierung](#) im IAMBenutzerhandbuch.
- Multi-Faktor-Authentifizierung erforderlich (MFA) — Wenn Sie ein Szenario haben, in dem IAM Benutzer oder ein Root-Benutzer erforderlich sind AWS-Konto, aktivieren Sie die Option MFA für zusätzliche Sicherheit. Wenn Sie festlegen möchten, MFA wann API Operationen aufgerufen werden, fügen Sie MFA Bedingungen zu Ihren Richtlinien hinzu. Weitere Informationen finden Sie unter [Konfiguration des MFA -geschützten API Zugriffs](#) im IAMBenutzerhandbuch.

Weitere Informationen zu bewährten Methoden finden Sie unter [Bewährte Sicherheitsmethoden IAM im IAM Benutzerhandbuch](#). IAM

Verwenden der Konsole „Strategy Recommendations“

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 Anrufe an AWS CLI oder am tätigen, keine Mindestberechtigungen für die Konsole gewähren AWS API. Erlauben Sie stattdessen nur den Zugriff auf die Aktionen, die dem API Vorgang entsprechen, den sie 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 im [Benutzerhandbuch unter Hinzufügen von Berechtigungen für einen IAM Benutzer](#).

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

Dieses Beispiel zeigt, wie Sie eine Richtlinie erstellen könnten, die es IAM Benutzern ermöglicht, die internen und verwalteten Richtlinien einzusehen, die mit ihrer Benutzeridentität verknüpft sind. Diese Richtlinie umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe von oder. AWS CLI AWS API

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "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. examplebucket Sie möchten dem Benutzer außerdem Berechtigungen zum Hinzufügen, Aktualisieren und Löschen von Objekten gewähren.

Zusätzlich zum Erteilen der Berechtigungen `s3:PutObject`, `s3:GetObject` und `s3:DeleteObject` für den Benutzer, gewährt die Richtlinie die Berechtigungen `s3:ListAllMyBuckets`, `s3:GetBucketLocation` und `s3:ListBucket`. Dies sind die zusätzlichen Berechtigungen, die von der Konsole benötigt werden. Außerdem sind die Aktionen `s3:PutObjectAcl` und `s3:GetObjectAcl` erforderlich, um Objekte in der Konsole kopieren, ausschneiden und einfügen zu können. 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:::examplebucket"
  },
  {
    "Sid": "ManageBucketContents",
    "Effect": "Allow",
    "Action": [
      "s3:PutObject",
      "s3:PutObjectAcl",
      "s3:GetObject",
      "s3:GetObjectAcl",
      "s3:DeleteObject"
    ],
    "Resource": "arn:aws:s3:::examplebucket/*"
  }
]
}

```

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 auftreten können IAM.

Themen

- [Ich bin nicht berechtigt, eine Aktion in Strategy Recommendations durchzuführen](#)
- [Ich bin nicht berechtigt, iam auszuführen: PassRole](#)

- [Ich möchte meine Zugriffsschlüssel anzeigen](#)
- [Ich bin Administrator und möchte anderen den Zugriff auf Strategieempfehlungen ermöglichen](#)
- [Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine Ressourcen für Strategieempfehlungen ermöglichen](#)

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 zu verwenden, um Details zu einer fiktiven `my-example-widget` Ressource anzuzeigen, aber nicht über die fiktiven `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 `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in Strategy Recommendations auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

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

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

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

Ich möchte meine Zugriffsschlüssel anzeigen

Nachdem Sie Ihre IAM Benutzerzugriffsschlüssel erstellt haben, können Sie Ihre Zugriffsschlüssel-ID jederzeit einsehen. 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. wJa1rXUtnFEMI/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 Zugangsschlüssel hinzufügen. Sie können maximal zwei Zugriffsschlüssel besitzen. Wenn Sie bereits zwei Zugriffsschlüssel besitzen, müssen Sie ein Schlüsselpaar löschen, bevor Sie ein neues erstellen. Anweisungen dazu finden Sie im IAMBenutzerhandbuch unter [Verwaltung von Zugangsschlüsseln](#).

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 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 [IAMim IAMBenutzerhandbuch unter IAMIdentitäten und Richtlinien und Berechtigungen](#).

Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine 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 auf einen anderen IAMBenutzer AWS-Konto , der Ihnen gehört](#).
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie [AWS-Konten im IAMBenutzerhandbuch unter Gewähren des Zugriffs für Dritte](#).
- Informationen dazu, wie Sie Zugriff über einen Identitätsverbund [gewähren, finden Sie im Benutzerhandbuch unter Zugriff für extern authentifizierte Benutzer \(Identitätsverbund\)](#). IAM
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie [IAMim Benutzerhandbuch unter Kontoübergreifender Ressourcenzugriff](#). IAM

Verwenden von serviceverknüpften Rollen für Strategieempfehlungen

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

Eine serviceverknüpfte Rolle vereinfacht die Einrichtung von Strategy Recommendations, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Strategy Recommendations definiert die Berechtigungen seiner serviceverknüpften Rollen. Sofern keine andere Konfiguration festgelegt wurde, können nur Strategy Recommendations die Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

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

Berechtigungen von serviceverknüpften Rollen für Strategy Recommendations

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

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

- `migrationhub-strategy.amazonaws.com`

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

AWS Application Discovery Service -Aktionen

```
discovery:ListConfigurations
```

`discovery:DescribeConfigurations`

AWS Migration Hub -Aktionen

`mgh:GetHomeRegion`

Amazon-S3-Aktionen

`s3:GetBucketAcl`

`s3:GetBucketLocation`

`s3:GetObject`

`s3:ListAllMyBuckets`

`s3:ListBucket`

`s3:PutObject`

`s3:PutObjectAcl`

Informationen zum Anzeigen der Berechtigungen für diese Richtlinie finden Sie unter [AWSMigrationHubStrategyServiceRolePolicy](#) im AWS Referenzhandbuch zu verwalteten Richtlinien.

Den Aktualisierungsverlauf dieser Richtlinie finden Sie unter [Strategieempfehlungen und Aktualisierungen AWS verwalteter Richtlinien](#).

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter [serviceverknüpfte Rollenberechtigungen](#) im IAM-Benutzerhandbuch.

Erstellen einer serviceverknüpften Rolle für Strategy Recommendations

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

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie damit einverstanden sind, Migration Hub zu erlauben, eine serviceverknüpfte Rolle (SLR) in Ihrem Konto zu erstellen, erstellt Strategy Recommendations die serviceverknüpfte Rolle erneut für Sie.

Bearbeiten einer serviceverknüpften Rolle für Strategieempfehlungen

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

Löschen einer serviceverknüpften Rolle für Strategy Recommendations

So löschen Sie die serviceverknüpfte Rolle mit IAM

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

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

Unterstützte Regionen für serviceverknüpfte Rollen mit Strategy Recommendations

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

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

Sie können eine private Verbindung zwischen Ihrer VPC und Migration Hub Hub-Strategieempfehlungen herstellen, indem Sie einen Schnittstellen-VPC-Endpunkt aus. Schnittstellenendpunkte werden von unterstützt AWS PrivateLink. mit AWS PrivateLink Sie können privat auf Strategy Recommendations-API-Operationen ohne Internet-Gateway, NAT-Gerät, VPN-Verbindung oder AWS Direct Connect-Verbindung. Die Instances in Ihrer VPC benötigen für die

Kommunikation mit Strategy Recommendations-API-Operationen keine öffentlichen IP-Adressen. Der Datenverkehr zwischen Ihrer VPC und Strategy Recommendations bleibt im Amazon-Netzwerk.

Jeder Schnittstellenendpunkt wird durch eine oder mehrere [Elastic Network-Schnittstellen](#) in Ihren Subnetzen dargestellt.

Weitere Informationen finden Sie unter [Schnittstellen-VPC-Endpunkte \(AWS PrivateLink\)](#) im Amazon VPC User Guide aus.

Überlegungen zu Strategieempfehlungen VPC-Endpunkte

Bevor Sie einen Schnittstellen-VPC-Endpunkt für Strategieempfehlungen einrichten, stellen Sie sicher, dass Sie die Überprüfung einsehen [Eigenschaften und Beschränkungen von Schnittstellenendpunkten](#) und [AWS PrivateLink Quoten](#) im Amazon VPC User Guide aus.

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

Erstellen eines Schnittstellen-VPC-Endpunkts für Strategieempfehlungen

Sie können einen VPC-Endpunkt für Strategieempfehlungen mithilfe der Amazon-VPC-Konsole oder der 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 Servicenamen:

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

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

Weitere Informationen finden Sie unter [Zugriff auf einen Service über einen Schnittstellenendpunkt](#) im Benutzerhandbuch für Amazon VPC.

Erstellen einer VPC-Endpunkttrichtlinie für Strategieempfehlungen

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

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

Weitere Informationen finden Sie unter [Steuerung des Zugriffs auf Services mit VPC-Endpunkten](#) im Amazon-VPC-Benutzerhandbuch.

Beispiel: VPC-Endpunktrichtlinie für Strategieempfehlungsmaßnahmen

Im Folgenden finden Sie ein Beispiel für eine Endpunktrichtlinie für Strategieempfehlungen.

Wenn diese Richtlinie an einen Endpunkt angefügt wird, gewährt sie Zugriff auf die aufgelisteten Strategieempfehlungsaktionen für alle Prinzipale auf allen Ressourcen.

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

Überprüfung der Einhaltung der Vorschriften für die Strategieempfehlungen von Migration Hub

Informationen darüber, ob AWS-Service ein [AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm AWS-Services unter](#) . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter [AWS Compliance-Programme AWS](#) .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter [Berichte herunterladen unter](#) .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen

und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- [Schnellstartanleitungen zu Sicherheit und Compliance](#) — In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Bereitstellung von Basisumgebungen beschrieben AWS , bei denen Sicherheit und Compliance im Mittelpunkt stehen.
- [Architecting for HIPAA Security and Compliance on Amazon Web Services](#) — In diesem Whitepaper wird beschrieben, wie Unternehmen Anwendungen erstellen HIPAA können, die AWS für sie in Frage kommen.

 Note

Nicht alle sind berechtigt AWS-Services . HIPAA Weitere Informationen finden Sie in der [Referenz für HIPAA qualifizierte Dienste](#).

- [AWS Ressourcen zur AWS](#) von Vorschriften — Diese Sammlung von Arbeitsmapen und Leitfäden kann auf Ihre Branche und Ihren Standort zutreffen.
- [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 für 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)) zusammengefasst.
- [Evaluierung von Ressourcen anhand von Regeln](#) im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- [AWS Security Hub](#) — Auf diese AWS-Service Weise erhalten Sie einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der [Security-Hub-Steuerungsreferenz](#).
- [Amazon GuardDuty](#) — Dies AWS-Service erkennt potenzielle Bedrohungen für Ihre Workloads AWS-Konten, Container und Daten, indem es Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen zu erfüllen PCIDSS, z. B. durch die Erfüllung der Anforderungen zur Erkennung von Eindringlingen, die in bestimmten Compliance-Frameworks vorgeschrieben sind.

- [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 beschriebene AWS-Dienste, die mit Migration Hub Hub-Strategieempfehlungen interagieren.

Themen

- [Protokollierung von -API-Aufrufen mit AWS CloudTrail](#)

Protokollierung von -API-Aufrufen mit AWS CloudTrail

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

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

Weitere Informationen zu CloudTrail finden Sie im [AWS CloudTrail-Benutzerhandbuch](#).

Informationen zu Strategieempfehlungen in CloudTrail

CloudTrail ist auf Ihrem AWS-Konto wenn Sie das -Konto anlegen. Die in Strategieempfehlungen auftretenden Aktivitäten werden als CloudTrail-Ereignis zusammen mit anderen aufgezeichnet AWS Service-Ereignisse in Ereignisverlauf daraus. Sie können aktuelle Ereignisse in Ihrem AWS-Konto aus. Weitere Informationen finden Sie unter [Anzeigen von Ereignissen mit CloudTrail Ereignisverlauf](#) aus.

Zur kontinuierlichen Aufzeichnung von Ereignissen in Ihrem AWS-Konto Erstellen Sie einen Trail, einschließlich Ereignissen für Strategieempfehlungen. Ein Trail ermöglicht es CloudTrail, Protokolldateien in einem Amazon-S3-Bucket bereitzustellen. Wenn Sie einen Pfad in der Konsole anlegen, gilt dieser standardmäßig für alle AWS-Regionen aus. Der Trail protokolliert Ereignisse aus

allen Regionen in der AWS-Partition und stellt die Protokolldateien in dem Amazon-S3-Bucket bereit, den Sie angeben. Darüber hinaus können Sie andere AWS-Services konfigurieren, um die in den CloudTrail-Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie unter:

- [Übersicht zum Erstellen eines Trails](#)
- [In CloudTrail unterstützte Services und Integrationen](#)
- [Konfigurieren von Amazon SNS-Benachrichtigungen für CloudTrail](#)
- [Empfangen von CloudTrail-Protokolldateien aus mehreren Regionen](#) und [Empfangen von CloudTrail-Protokolldateien von mehreren Konten](#).

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

- [getApplicationComponentStrategies](#)
- [getApplicationComponentDetails](#)
- [getAssesment](#)
- [GetImportFileTask](#)
- [getPortfoliopReferences](#)
- [getPortfolioSummary](#)
- [getServerDetails](#)
- [GetServerStrategies](#)
- [listApplicationComponents](#)
- [ListCollectors](#)
- [ListImportFileTask](#)
- [ListServers](#)
- [PutPortfoliopReferences](#)
- [StartAssess](#)
- [StarTimportFileTask](#)
- [StoppBewertung](#)
- [updateApplicationComponetConfig](#)
- [updateServerConfig](#)

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Anhand der Identitätsinformationen zur Benutzeridentität können Sie Folgendes bestimmen:

- Ob die Anfrage mit Root- oder AWS Identity and Access Management (IAM)-Benutzer-Anmeldeinformationen ausgeführt wurde.
- Ob die Anfrage mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen föderierten Benutzer ausgeführt wurde
- Ob die Anforderung von einem anderen AWS-Service getätigt wurde.

Weitere Informationen finden Sie unter [CloudTrail-Element `userIdentity`](#).

Grundlagen zu -Protokolldateieinträgen

Ein Trail ist eine Konfiguration, durch die Ereignisse als Protokolldateien an den von Ihnen angegebenen Amazon S3 Bucket übermittelt werden. CloudTrail-Protokolldateien können einen oder mehrere Einträge enthalten. Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält unter anderem Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion sowie über die Anfrageparameter. CloudTrail-Protokolleinträge sind kein geordnetes Stack-Trace der öffentlichen API-Aufrufe und erscheinen daher in keiner bestimmten Reihenfolge.

Das folgende Beispiel zeigt einen CloudTrail-Protokolleintrag, der die [`getServerDetails`](#)Aktion

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

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

Kontingente für Migrations-Hub-Strategieempfehlungen

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

Eine Liste der Kontingente für Migration Hub Hub-Strategieempfehlungen finden Sie unter [Strategieempfehlungen Servicekontingente](#) aus.

Sie können die Kontingente für Strategieempfehlungen auch anzeigen, indem Sie die [Konsole Service Quotas Servicekontingente](#) aus. Wählen Sie im Navigationsbereich AWS Dienstleistungen und Select Migration Hub Hub-Strategie-Empfehlungen 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](#)
- [12. Oktober 2023](#)
- [17. April 2023](#)
- [17. März 2023](#)
- [07. November 2022](#)
- [27. September 2022](#)
- [30. Juni 2022](#)
- [18. April 2022](#)
- [25. Februar 2022](#)
- [10. Februar 2022](#)
- [28. Januar 2022](#)
- [14. Januar 2022](#)
- [21. Dezember 2021](#)
- [15. Dezember 2021](#)
- [25. Oktober 2021](#)

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

- Anwendungsfiltrierung für Anwendungen
- Serverfiltrierung nach AWS Application Discovery Service Tags

27. September 2022

Neues Feature

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

Fehlerkorrekturen

- Portierung des Assistenzübersetzers und andere Korrekturen.

30. Juni 2022

Neues Feature

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

18. April 2022

Neues Feature

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

Fehlerkorrekturen

- A2C v1.1.5

25. Februar 2022

Fehlerkorrekturen

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

10. Februar 2022

Fehlerkorrekturen

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

28. Januar 2022

Neues Feature

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

14. Januar 2022

Neues Feature

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

21. Dezember 2021

Das Problem wurde behoben

- Collector v1.1.0
- Die Datenbankanalyse wurde wiederhergestellt.

15. Dezember 2021

Bekanntes Problem

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

25. Oktober 2021

Neues Feature

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

Dokument- und Versionshistorie

In der folgenden Tabelle werden die Dokumentationsversionen für Strategieempfehlungen beschrieben. Weitere Informationen finden Sie unter [Versionshinweise](#).

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

	Recommendations ist mit Unterstützung für mehrere Datenquellen verfügbar.	
AWS verwaltete Richtlini enaktualisierungen — Update auf AWSMigrationHubStrategyCollector	Die AWSMigrationHubStrategyCollector Richtlinie wurde aktualisiert, um neue Amazon S3 S3-APIs aufzunehmen.	15. September 2023
AWS verwaltete Richtlini enaktualisierungen — Aktualisierung auf AWSMigrationHubStrategyCollector	Die AWSMigrationHubStrategyCollector Richtlinie 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-Methoden .	25. Februar 2023
AWS verwaltete Richtlini enaktualisierungen — Aktualisierung einer bestehenden Richtlinie	Mit den Strategieempfehlungen von Migration Hub wurden drei AWS Application Discovery Service APIs zu einer bestehenden Richtlinie hinzugefügt.	10. November 2022
Sicherheits-Updates	Stellen Sie eine private Verbindung mit dem VPC-Endpunkt der Schnittstelle her.	07. März 2022
Neues Feature	Unterstützung für Azure DevOps Git Repositorys für die Quellcodeanalyse hinzugefügt.	28. Januar 2022
Neues Feature	Babelfish-Empfehlungen für SQL-Datenbanken hinzugefügt.	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.