aws

Benutzerhandbuch

AWS Application Discovery Service

AWS Application Discovery Service: Benutzerhandbuch

Table of Contents

Was ist AWS Application Discovery Service?

AWS Application Discovery ServiceHilft Ihnen bei der Planung Ihrer Migration in dieAWS - Cloud durch Sammeln von Nutzungs- und Konfigurationsdaten über Ihre lokalen Server und Datenbanken. Application Discovery Service ist inAWS Migration Hub undAWS Database Migration Service Fleet Advisor integriert. Migration Hub vereinfacht Ihre Migrationsverfolgung, da er Ihre Migrationsstatusinformationen in einer einzigen Konsole zusammenfasst. Sie können die erkannten Server anzeigen, sie in Anwendungen gruppieren und dann den Migrationsstatus jeder Anwendung von der Migration Hub Hub-Konsole in Ihrer Heimatregion aus verfolgen. Sie können DMS Fleet Advisor verwenden, um die Migrationsoptionen für Datenbank-Workloads zu bewerten.

Alle entdeckten Daten werden in IhrerAWS Migration Hub Heimatregion gespeichert. Daher müssen Sie Ihre Heimatregion in der Migration Hub Hub-Konsole oder mit CLI-Befehlen festlegen, bevor Sie Erkennungs- und Migrationsaktivitäten durchführen. Ihre Daten können zur Analyse in Microsoft Excel oderAWS Analysetools wie Amazon Athena und Amazon exportiertQuickSight werden.

Mithilfe der Application Discovery Service Service-APIs können Sie die Systemleistungs- und Nutzungsdaten für Ihre erkannten Server exportieren. Geben Sie diese Daten in Ihr Kostenmodell ein, um die Kosten für den Betrieb dieser Server zu berechnenAWS. Darüber hinaus können Sie Daten über die Netzwerkverbindungen exportieren, die zwischen Servern bestehen. Auf diese Weise können Sie die Netzwerkabhängigkeiten zwischen Servern leichter bestimmen und sie zur Planung der Migration in Anwendungen gruppieren.

> **Note**
>
> Ihre Heimatregion muss eingerichtet sein,AWS Migration Hub bevor Sie mit dem Erkennungsprozess beginnen, da Ihre Daten in Ihrer Heimatregion gespeichert werden. Weitere Informationen zur Arbeit mit einer Heimatregion finden Sie unter Heimatregion.

Application Discovery Service bietet zwei Möglichkeiten, Daten über Ihre lokalen Server zu ermitteln und zu sammeln:

- Die agentenlose Erkennung kann durchgeführt werden, indem Sie den Application Discovery Service Agentless Collector (Agentless Collector) (OVA-Datei) über Ihr VMware vCenter bereitstellen. Nach der Konfiguration von Agentless Collector identifiziert er virtuelle Maschinen (VMs) und Hosts, die mit vCenter verknüpft sind. Agentless Collector sammelt die

folgenden statischen Konfigurationsdaten: Server-Hostnamen, IP-Adressen, MAC-Adressen, Festplattenressourcenzuweisungen, Versionen der Datenbank-Engine und Datenbankschemas. Darüber hinaus erfasst es die Nutzungsdaten für jede VM und Datenbank und liefert die durchschnittliche und maximale Auslastung für Kennzahlen wie CPU, RAM und Festplatten-I/O.

- Die agentenbasierte Erkennung kann durchgeführt werden, indem Sie denAWS Application Discovery Agent auf jeder Ihrer virtuellen Maschinen und physischen Server bereitstellen. Das Installationsprogramm für den Agenten ist für Windows- und für Linux-Betriebssysteme verfügbar. Es sammelt statische Konfigurationsdaten, detaillierte Zeitreihendaten der Systemleistung, ein- und ausgehende Netzwerkverbindungen sowie derzeit ausgeführte Prozesse.

Application Discovery Service lässt sich in Application Discovery-Lösungen vonAWS Partner Network (APN) -Partnern integrieren. Diese Drittanbieterlösungen können Ihnen helfen, Details zu Ihrer lokalen Umgebung direkt in den Migration Hub zu importieren, ohne einen agentenlosen Collector oder Discovery Agent zu verwenden. Tools zur Anwendungserkennung von Drittanbietern könnenAWS Application Discovery Service abfragen und mithilfe der öffentlichen API in die Application Discovery Service Service-Datenbank schreiben. Auf diese Weise können Sie Daten in den Migration Hub importieren und aufrufen, damit Sie Anwendungen mit Servern verknüpfen und Migrationen verfolgen können.

VMware-Erkennung

Wenn Sie virtuelle Maschinen (VMs) haben, die in der VMware vCenter-Umgebung ausgeführt werden, können Sie den Agentless Collector verwenden, um Systeminformationen zu sammeln, ohne auf jeder VM einen Agenten installieren zu müssen. Stattdessen laden Sie diese lokale Appliance in vCenter und erlauben ihr, alle ihre Hosts und VMs zu erkennen.

Agentless Collector erfasst Informationen zur Systemleistung und Ressourcenauslastung für jede VM, die im vCenter ausgeführt wird, unabhängig davon, welches Betriebssystem verwendet wird. Er kann die einzelnen VMs jedoch nicht einsehen und daher nicht feststellen, welche Prozesse derzeit auf den einzelnen VM ausgeführt werden oder welche Netzwerkverbindungen vorhanden sind. Wenn Sie diesen Detaillierungsgrad benötigen und sich einige Ihrer vorhandenen VMs genauer ansehen möchten, um Sie bei der Planung Ihrer Migration zu unterstützen, können Sie den Discovery Agent daher nach Bedarf installieren.

Außerdem können Sie für virtuelle Maschinen, die auf VMware gehostet werden, sowohl den Agentless Collector als auch den Discovery Agent verwenden, um die Erkennung gleichzeitig durchzuführen. Ausführliche Informationen zu den Arten von Daten, die im Einzelnen mit jedem

Erkennungstool gesammelt werden, finden Sie unter Von Agentless Collector gesammelte Daten und Von Discovery Agent gesammelte Daten.

Erkennung von Datenbanken

Wenn Sie Datenbank- und Analyseserver in Ihrer lokalen Umgebung haben, können Sie den Agentless Collector verwenden, um diese Server zu ermitteln und zu inventarisieren. Sie können dann Leistungsmetriken für jeden Datenbankserver erfassen, ohne Agentless Collector auf jedem Computer in Ihrer Umgebung installieren zu müssen.

Das Datenbank- und Analysedatenerfassungsmodul Agentless Collector erfasst Metadaten und Leistungsmetriken, die Einblicke in Ihre Dateninfrastruktur bieten. Das Datenbank- und Analysedatenerfassungsmodul verwendet LDAP in Microsoft Active Directory, um Informationen über das Betriebssystem, die Datenbank und die Analyseserver in Ihrem Netzwerk zu sammeln. Anschließend führt das Datenerfassungsmodul in regelmäßigen Abständen Abfragen aus, um die tatsächliche Auslastung von CPU-, Arbeitsspeicher- und Festplattenkapazität für die Datenbanken und Analyseserver zu erfassen. Einzelheiten zu den gesammelten Metriken finden Sie unterVom Datenbank- und Analysemodul gesammelte Daten.

Nachdem Agentless Collector die Datenerfassung in Ihrer Umgebung abgeschlossen hat, können Sie dieAWS DMS Konsole für weitere Analysen und für die Planung Ihrer Migration verwenden. Um beispielsweise ein optimales Migrationsziel in der auszuwählenAWS Cloud, können Sie Zielempfehlungen für Ihre Quelldatenbanken generieren. Weitere Informationen finden Sie unter Modul zur Erfassung von Datenbank- und Analysedaten.

Vergleichen Sie Agentless Collector und Discovery Agent

Die folgende Tabelle bietet einen schnellen Vergleich der Datenerfassungstools von Application Discovery Service.

	Agentenloser Sammler	Discovery-Agent
Supported server types		
Virtuelle VMware-Maschine	Ja	Ja
Physischer Server	Nein	Ja

	Agentenloser Sammler	Discovery-Agent
Deployment		
Pro Server	Nein	Ja
Pro vCenter	Ja	Nein
Collected data		
Statische Serverkonfiguratio nsdaten	Yes	Yes
Datenbankkonfigurationsdaten	Yes	No
VM-Auslastungsmetriken	Yes	No
Metriken zur Datenbank auslastung	Yes	No
Zeitreihen mit Leistungs informationen	No	Yes (Export only)
Eingehende/ausgehende Netzwerkverbindungen	No	Yes (Export only)
Ausgeführte Prozesse	No	Yes (Export only)
Unterstützes Betriebssystem	Any OS running in VMware vCenter V5.5+	Eine Liste der unterstüt zten Linux- und Windows-Betriebssysteme finden Sie unterVoraussetzungen für Discovery Agent.
Unterstützte Datenbanken	Oracle, SQL Server, MySQL, and PostgreSQL	Keine

Annahmen

Für die Verwendung des Application Discovery Service wird Folgendes vorausgesetzt:

- Sie haben sich registriert beiAWS. Weitere Informationen finden Sie unter Application Discovery Service einrichten.
- Sie haben eine Migration Hub Hub-Heimatregion ausgewählt. Weitere Informationen finden Sie in der Dokumentation über Heimatregionen.

Folgendes ist zu erwarten:

- Die Migration Hub Hub-Heimatregion ist die einzige Region, in der Application Discovery Service Ihre Ermittlungs- und Planungsdaten speichert.
- Discovery-Agents, Connectors und Importe können nur in der ausgewählten Migration Hub Hub-Heimatregion verwendet werden.
- Eine Liste derAWS Regionen, in denen Sie den Application Discovery Service verwenden können, finden Sie unter Allgemeine Amazon Web Services-Referenz.

Application Discovery Service einrichten

Führen Sie AWS Application Discovery Service vor der ersten Verwendung die folgenden Aufgaben aus:

- Bei Amazon Web Services registrieren
- IAM-Benutzer erstellen
- Melden Sie sich bei der Migration Hub Hub-Konsole an und wählen Sie eine Heimatregion

Bei Amazon Web Services registrieren

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

Um sich für eine anzumelden AWS-Konto

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

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

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

IAM-Benutzer erstellen

Wenn Sie ein AWS Konto erstellen, erhalten Sie eine einzige Anmeldeidentität, mit der Sie vollständigen Zugriff auf alle AWS Dienste und Ressourcen im Konto haben. Diese Identität wird als Root-Benutzer des AWS Kontos bezeichnet. Wenn Sie sich AWS Management Console mit der E-Mail-Adresse und dem Passwort, mit denen Sie das Konto erstellt haben, anmelden, erhalten Sie vollständigen Zugriff auf alle AWS Ressourcen in Ihrem Konto.

Es wird ausdrücklich empfohlen, den Root-Benutzer nicht für Alltagsaufgaben einschließlich administrativer Aufgaben zu verwenden. Folgen Sie stattdessen der bewährten Sicherheitsmethode

„Individuelle IAM-Benutzer erstellen“ und erstellen Sie einen AWS Identity and Access Management (IAM-) Administratorbenutzer. Anschließend legen Sie die Anmeldedaten für den Root-Benutzer an einem sicheren Ort ab und verwenden sie nur, um einige Konto- und Service-Verwaltungsaufgaben durchzuführen.

Zusätzlich zur Erstellung eines Administratorbenutzers müssen Sie auch IAM-Benutzer ohne Administratorrechte erstellen. In den folgenden Themen wird erklärt, wie Sie beide Arten von IAM-Benutzern erstellen.

Themen

Einen IAM-Administratorbenutzer erstellen

Standardmäßig erbt ein Administratorkonto alle Richtlinien, die für den Zugriff auf den Application Discovery Service erforderlich sind.

So erstellen Sie einen Administratorbenutzer

- Erstellen Sie einen Administratorbenutzer in Ihrem AWS Konto. Weitere Anweisungen finden Sie unter Creating Your First IAM User and Administrators Group (Erstellen Ihrer ersten IAM-Benutzer- und Administratorengruppe) im IAM User Guide (IAM-Benutzerhandbuch).

Einen IAM-Benutzer ohne Administratorrechte erstellen

Beachten Sie beim Erstellen von IAM-Benutzern ohne Administratorrechte die bewährte Sicherheitsmethode Grant Least Privilege, d. h. gewähren Sie Benutzern Mindestberechtigungen.

Verwenden Sie von IAM verwaltete Richtlinien, um die Zugriffsebene für IAM-Benutzer ohne Administratorrechte auf den Application Discovery Service zu definieren. Informationen zu den verwalteten Richtlinien von Application Discovery Service finden Sie unterAWS Von verwaltete Richtlinien für AWS Application Discovery Service.

So erstellen Sie einen IAM-Benutzer ohne Administratorrechte

1. Navigieren Sie in AWS Management Console zur IAM-Konsole.

2. Erstellen Sie einen IAM-Benutzer ohne Administratorrechte, indem Sie den Anweisungen zum Erstellen eines Benutzers mit der Konsole folgen, wie unter Erstellen eines IAM-Benutzers in Ihrem AWS Konto im IAM-Benutzerhandbuch beschrieben.

   Folgen Sie dabei den Anweisungen im IAM-Benutzerhandbuch:

   - Wählen Sie im Schritt zur Auswahl des Zugriffstyps die Option Programmatischer Zugriff aus. Hinweis: Wählen Sie den Zugriff auf die AWS Managementkonsole nur aus, wenn Sie dieselben IAM-Benutzeranmeldedaten für den Zugriff auf die AWS Konsole verwenden möchten.
   - Wählen Sie im nächsten Schritt auf der Seite „Berechtigungen festlegen“ die Option „Bestehende Richtlinien direkt an den Benutzer anhängen“. Wählen Sie dann eine verwaltete IAM-Richtlinie für Application Discovery Service aus der Richtlinienliste aus. Informationen zu den verwalteten Richtlinien von Application Discovery Service finden Sie unterAWS Von verwaltete Richtlinien für AWS Application Discovery Service.
   - Wenn Sie sich die Zugriffsschlüssel des Benutzers (Zugriffsschlüssel-IDs und geheime Zugangsschlüssel) ansehen, folgen Sie den Anweisungen im Abschnitt Wichtiger Hinweis zur Aufbewahrung der neuen Zugriffsschlüssel-ID und des geheimen Zugangsschlüssels des Benutzers an einem sicheren Ort.

Melden Sie sich bei der Migration Hub Hub-Konsole an und wählen Sie eine Heimatregion

Sie müssen in dem AWS Konto, das Sie für das verwenden, eine AWS Migration Hub Heimatregion auswählen AWS Application Discovery Service.

Um die Heimatregion auszuwählen

1. Melden Sie sich mit Ihrem AWS Konto bei der Migration Hub Hub-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/migrationhub/.
2. Wählen Sie im Navigationsbereich der Migration Hub Hub-Konsole Einstellungen und anschließend eine Heimatregion aus.

   Ihre Migration Hub Hub-Daten werden in Ihrer Heimatregion zu Ermittlungs-, Planungs- und Migrationsverfolgungszwecken gespeichert. Weitere Informationen finden Sie unter Die Heimatregion des Migration Hub.

AWS Agent zur Anwendungserkennung

Der AWS Application Discovery Agent (Discovery Agent) ist eine Software, die Sie auf lokalen Servern und VMs installieren, die für die Erkennung und Migration vorgesehen sind. Agenten sammeln Daten zu Systemkonfiguration, Systemleistung, laufenden Prozessen und Details der Netzwerkverbindungen zwischen Systemen. Agenten unterstützen die meisten Linux- und Windows-Betriebssysteme, und Sie können sie auf physischen lokalen Servern, Amazon EC2 EC2-Instances und virtuellen Maschinen bereitstellen.

> **Note**
>
> Bevor Sie den Discovery Agent bereitstellen, müssen Sie eine Migration Hub Hub-Heimatregion auswählen. Sie müssen den Agenten in Ihrer Heimatregion registrieren.

Der Discovery Agent wird in Ihrer lokalen Umgebung ausgeführt und benötigt Root-Rechte. Wenn Sie den Discovery Agent starten, stellt er eine sichere Verbindung mit Ihrer Heimatregion her und registriert sich beim Application Discovery Service.

- Wenn es `eu-central-1` sich beispielsweise um Ihre Heimatregion handelt, registriert sie sich `arsenal-discovery.eu-central-1.amazonaws.com` beim Application Discovery Service.
- Oder ersetzen Sie Ihre Heimatregion nach Bedarf für alle anderen Regionen außer us-west-2.
- Wenn es `us-west-2` sich um Ihre Heimatregion handelt, registriert sie sich `arsenal.us-west-2.amazonaws.com` beim Application Discovery Service.

Funktionsweise

Nach der Registrierung beginnt der Agent mit der Erfassung von Daten für den Host oder die VM, auf dem er sich befindet. Der Agent sendet in Intervallen von 15 Minuten ein Ping-Signal an den Application Discovery Service, um Konfigurationsinformationen zu erhalten.

Zu den erfassten Daten gehören Systemspezifikationen, Zeitreihen mit Nutzungs- oder Leistungsdaten, Netzwerkverbindungen und Prozessdaten. Sie können anhand dieser Informationen Ihre IT-Komponenten und deren Netzwerkabhängigkeiten zuordnen. All diese Datenpunkte können Ihnen helfen, die Kosten für den Betrieb dieser Server zu ermitteln AWS und die Migration zu planen.

Daten werden von den Discovery Agents mithilfe der Transport Layer Security (TLS) - Verschlüsselung sicher an den Application Discovery Service übertragen. Agenten sind so konfiguriert, dass automatisch ein Upgrade durchgeführt wird, wenn neue Versionen verfügbar sind. Sie können diese Konfigurationseinstellung auf Wunsch ändern.

> **Tip**
>
> Bevor Sie den Discovery Agent herunterladen und mit der Installation beginnen, sollten Sie sich mit allen erforderlichen Voraussetzungen vertraut machen Voraussetzungen für Discovery Agent

Themen

Voraussetzungen für Discovery Agent

Im Folgenden sind die Voraussetzungen und die Aufgaben aufgeführt, die Sie ausführen müssen, bevor Sie den AWS Application Discovery Agent (Discovery Agent) erfolgreich installieren können.

- Sie müssen eine AWS Migration Hub Heimatregion festlegen, bevor Sie mit der Installation von Discovery Agent beginnen.
- Wenn eine 1.x-Version des Agenten installiert ist, muss diese entfernt werden, bevor die neueste Version installiert wird.
- Wenn auf dem Host, auf dem der Agent installiert wird, Linux ausgeführt wird, stellen Sie sicher, dass der Host mindestens die Intel i686 CPU-Architektur (auch bekannt als P6-Mikroarchitektur) unterstützt.
- 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 2003 R2 SP2

Windows Server 2008 R1 SP2, 2008 R2 SP1

Windows Server 2012 R1, 2012 R2

Windows Server 2016

Windows Server 2019

Windows Server 2022

- Wenn von Ihrem Netzwerk ausgehende Verbindungen eingeschränkt sind, müssen Sie Ihre Firewall-Einstellungen aktualisieren. Agenten benötigen Zugriff auf `arsenal` über den TCP-Port 443. Es ist nicht erforderlich, dass eingehende Ports geöffnet sind.

  Wenn Ihre Heimatregion beispielsweise `eu-central-1` ist, würden Sie `https://arsenal-discovery.eu-central-1.amazonaws.com:443` verwenden.
- Damit das automatische Upgrade funktioniert, ist Zugriff auf Amazon S3 in Ihrer Heimatregion erforderlich.
- Erstellen Sie einen AWS Identity and Access Management (IAM-) Benutzer in der Konsole und fügen Sie die bestehende verwaltete `AWSApplicationDiscoveryAgentAccess` IAM-Richtlinie an. Diese Richtlinie ermöglicht es dem Benutzer, die erforderlichen Agentenaktionen in Ihrem Namen auszuführen. Weitere Informationen über verwaltete Richtlinien finden Sie unter AWS Von verwaltete Richtlinien für AWS Application Discovery Service.
- Überprüfen Sie die Zeitverzögerung von Ihren Network Time Protocol(NTP)-Servern und korrigieren Sie sie gegebenenfalls. Eine falsche Zeitsynchronisierung führt dazu, dass der Agentenregistrierungsaufruf fehlschlägt.

> **Note**
>
> Der Discovery Agent verfügt über eine ausführbare 32-Bit-Agent-Datei, die auf 32-Bit- und 64-Bit-Betriebssystemen funktioniert. Durch eine einzige ausführbare Datei wird die Anzahl der

erforderlichen Installationspakete für die Bereitstellung reduziert. Dieser ausführbare Agent funktioniert für Linux und Windows OS. Dies wird in den jeweiligen Installationsabschnitten angesprochen, die folgen.

Installieren Sie Discovery Agent unter Linux

Führen Sie das folgende Verfahren unter Linux aus. Stellen Sie sicher, dass Ihre Heimatregion für Migration Hub festgelegt wurde, bevor Sie mit diesem Verfahren beginnen.

> **Note**
>
> Wenn Sie eine nicht aktuelle Linux-Version verwenden, lesen Sie unter Anforderungen auf älteren Linux-Plattformen nach.

Um den AWS Application Discovery Agent in Ihrem Rechenzentrum zu installieren

1. Melden Sie sich bei Ihrem Linux-basierten Server oder Ihrer VM an und erstellen Sie ein neues Verzeichnis, das Ihre Agentenkomponenten enthält.
2. Wechseln Sie zu dem neuen Verzeichnis und laden Sie das Installationsskript über die Befehlszeile oder über die Konsole herunter.

   a. Führen Sie zum Herunterladen über die Befehlszeile den folgenden Befehl aus.

   ```
   curl -o ./aws-discovery-agent.tar.gz https://s3-us-west-2.amazonaws.com/aws-discovery-agent.us-west-2/linux/latest/aws-discovery-agent.tar.gz
   ```

   b. Gehen Sie wie folgt vor, um von der Migration Hub Hub-Konsole herunterzuladen:

      i. Öffnen Sie die Konsole und wechseln Sie zur Seite Discovery Tools (Erkennungstools).

      ii. Wählen Sie im Feld Discovery Agent die Option Download agent (Agenten herunterladen). Wählen Sie dann in der resultierende Liste Linux aus. Ihr Download beginnt sofort.

3. Überprüfen Sie die kryptografische Signatur des Installationspakets mit den drei folgenden Befehlen:

```
curl -o ./agent.sig https://s3.us-west-2.amazonaws.com/aws-discovery-agent.us-west-2/linux/latest/aws-discovery-agent.tar.gz.sig
```

```
curl -o ./discovery.gpg https://s3.us-west-2.amazonaws.com/aws-discovery-agent.us-west-2/linux/latest/discovery.gpg
```

```
gpg --no-default-keyring --keyring ./discovery.gpg --verify agent.sig aws-discovery-agent.tar.gz
```

Der Fingerabdruck des öffentlichen Schlüssel des Agenten (`discovery.gpg`) ist `7638 F24C 6717 F97C 4F1B 3BC0 5133 255E 4DF4 2DA2`.

4. Extrahieren Sie den Tarball wie im Folgenden dargestellt.

```
tar -xzf aws-discovery-agent.tar.gz
```

5. Wählen Sie eine der folgenden Installationsmethoden, um den Agenten zu installieren.

Zu …	Vorgehensweise
Installieren Sie Discovery Agent	Um den Agenten zu installieren, führen Sie den Befehl agent install aus, wie im folgenden Beispiel gezeigt. Ersetzen Sie es im Beispiel *your-home-region* durch den Namen Ihrer Heimatregion, *aws-access-key-id*durch Ihre Zugriffsschlüssel-ID und *aws-secret-access-key* durch Ihren geheimen Zugriffsschlüssel. `sudo bash install -r your-home-region -k aws-access-key-id -s aws-secret-access-key` Standardmäßig laden Agenten Updates automatisch herunter und installieren sie, sobald sie verfügbar sind.

Zu …	Vorgehensweise
	Wir empfehlen die Verwendung dieser Standard-Konfiguration. Wenn Sie jedoch nicht möchten, dass Agenten Updates automatisch herunterladen und anwenden, geben Sie den `-u false` Parameter bei der Ausführung des Agent-Installationsbefehls an.

Zu …	Vorgehensweise
(Optional) Installieren Sie Discovery Agent und konfigurieren Sie einen nicht transparenten Proxy	Um einen nicht transparenten Proxy zu konfigurieren, fügen Sie dem Installationsbefehl des Agenten die folgenden Parameter hinzu: • -e Das Proxy-Passwort. • -f Die Proxy-Portnummer. • -g Das Proxyschema. • -i Der Proxy-Benutzername. Im Folgenden finden Sie ein Beispiel für den Agenteninstallationsbefehl, der die nicht transparenten Proxyparameter verwendet. `sudo bash install -r your-home-region -k aws-access-key-id -s aws-secret-access-key -d myproxy.mycompany.com -e mypassword -f proxy-port-number -g https -i myusername` Wenn Ihr Proxy keine Authentifizierung erfordert, lassen Sie die `-i` Parameter `-e` und weg. Der Beispielbefehl install verwendet`https`, wenn Ihr Proxy HTTP verwendet, `http` für den `-g` Parameterwert „specify“.

6. Wenn von Ihrem Netzwerk ausgehende Verbindungen eingeschränkt sind, müssen Sie Ihre Firewall-Einstellungen aktualisieren. Agenten benötigen Zugriff auf `arsenal` über den TCP-Port 443. Es ist nicht erforderlich, dass eingehende Ports geöffnet sind.

   Wenn Ihre Heimatregion beispielsweise `eu-central-1` ist, würden Sie `https://arsenal-discovery.eu-central-1.amazonaws.com:443` verwenden.

Themen

Anforderungen auf älteren Linux-Plattformen

Einige ältere Linux-Plattformen, wie SUSE 10, CentOS 5 und RHEL 5, sind entweder am Ende ihrer Betriebslebensdauer angelangt oder werden nur noch minimal unterstützt. Auf diesen Plattformen kann es zu out-of-date Verschlüsselungssammlungen kommen, die verhindern, dass das Agent-Aktualisierungsskript Installationspakete herunterlädt.

Curl

Der Application Discovery Agent benötigt eine `curl` sichere Kommunikation mit dem AWS Server. Einige alte Versionen von `curl` sind nicht in der Lage, eine sichere Kommunikation mit einem modernen Web-Service durchzuführen.

Um die im Application Discovery-Agenten enthaltene Version von `curl` zu verwenden, führen Sie das Installationsskript mit dem Parameter `-c true` aus.

Zertifizierungsstellen-Bundle

Ältere Linux-Systeme verfügen möglicherweise über ein out-of-date Certificate Authority (CA) -Paket, das für eine sichere Internetkommunikation von entscheidender Bedeutung ist.

Um das im Application Discovery-Agenten enthaltene CA-Bundle zu verwenden, führen Sie das Installationsskript mit dem Parameter `-b true` aus.

Diese Installationsskriptoptionen können zusammen verwendet werden. Im folgenden Beispielbefehl werden beide Skriptparameter an das Installationsskript übergeben:

```
sudo bash install -r your-home_region -k aws-access-key-id -s aws-secret-access-key -c
 true -b true
```

Verwalten Sie den Discovery Agent-Prozess unter Linux

Sie können das Verhalten des Discovery Agents auf Systemebene mithilfe der `System V init` Tools `systemd`Upstart, oder verwalten. Die folgenden Registerkarten beschreiben die Befehle für die unterstützten Aufgaben in den jeweiligen Tools.

systemd

Management-Befehle für den Application Discovery Agent

Aufgabe	Befehl
Überprüfen Sie, ob ein Agent ausgeführt wird	`sudo systemctl status aws-discovery-daemon.service`
Starten Sie einen Agenten	`sudo systemctl start aws-discovery-daemon.service`
Beenden Sie einen Agenten	`sudo systemctl stop aws-discovery-daemon.service`
Starten Sie einen Agenten neu	`sudo systemctl restart aws-discovery-daemon.service`

Upstart

Verwaltungsbefehle für den Application Discovery Agent

Aufgabe	Befehl
Überprüfen Sie, ob ein Agent ausgeführt wird	`sudo initctl status aws-discovery-daemon`
Starten Sie einen Agenten	`sudo initctl start aws-discovery-daemon`
Beenden Sie einen Agenten	`sudo initctl stop aws-discovery-daemon`
Starten Sie einen Agenten neu	`sudo initctl restart aws-discovery-daemon`

System V init

Verwaltungsbefehle für den Application Discovery Agent

Aufgabe	Befehl
Überprüfen Sie, ob ein Agent ausgeführt wird	`sudo /etc/init.d/aws-discovery-daemon status`
Starten Sie einen Agenten	`sudo /etc/init.d/aws-discovery-daemon start`
Beenden Sie einen Agenten	`sudo /etc/init.d/aws-discovery-daemon stop`
Starten Sie einen Agenten neu	`sudo /etc/init.d/aws-discovery-daemon restart`

Deinstallieren Sie Discovery Agent unter Linux

In diesem Abschnitt wird beschrieben, wie Sie Discovery Agent unter Linux deinstallieren.

Um einen Agenten zu deinstallieren, wenn Sie den Yum-Paketmanager verwenden

- Verwenden Sie den folgenden Befehl, um einen Agenten zu deinstallieren, wenn Sie Yum verwenden.

```
rpm -e --nodeps aws-discovery-agent
```

Um einen Agenten zu deinstallieren, wenn Sie den Paketmanager apt-get verwenden

- Verwenden Sie den folgenden Befehl, um einen Agenten zu deinstallieren, wenn Sie apt-get verwenden.

```
apt-get remove aws-discovery-agent:i386
```

Um einen Agenten zu deinstallieren, wenn Sie den Zypper-Paketmanager verwenden

- Verwenden Sie den folgenden Befehl, um einen Agenten zu deinstallieren, wenn Sie Zypper verwenden.

```
zypper remove aws-discovery-agent
```

Problembehandlung für den Linux Discovery Agent

Wenn bei der Installation oder Verwendung des Discovery Agent unter Linux Probleme auftreten, lesen Sie die folgenden Anleitungen zur Protokollierung und Konfiguration. Bei der Behebung potenzieller Probleme mit dem Agenten oder seiner Verbindung zum Application Discovery Service fordert der AWS Support häufig diese Dateien an.

- Protokolldateien

  Die Protokolldateien für Discovery Agent befinden sich im folgenden Verzeichnis.

```
/var/log/aws/discovery/
```

  Protokolldateien werden so benannt, dass sie angeben, ob sie vom Haupt-Daemon, dem automatischen Upgrader oder dem Installationsprogramm generiert wurden.

- Konfigurationsdateien

  Die Konfigurationsdateien für Discovery Agent Version 2.0.1617.0 oder neuer befinden sich im folgenden Verzeichnis.

```
/etc/opt/aws/discovery/
```

  Die Konfigurationsdateien für Versionen von Discovery Agent vor 2.0.1617.0 befinden sich im folgenden Verzeichnis.

```
/var/opt/aws/discovery/
```

- Anweisungen zum Entfernen älterer Versionen des Discovery Agents finden Sie unter. Voraussetzungen für Discovery Agent

Installieren von unter Windows.

Führen Sie das folgende Verfahren durch, um einen Agenten unter Windows zu installieren. Stellen Sie sicher, dass Ihre Heimatregion für Migration Hub festgelegt wurde, bevor Sie mit diesem Verfahren beginnen.

Um den AWS Application Discovery Agent in Ihrem Rechenzentrum zu installieren

1. Laden Sie das Windows Agent-Installationsprogramm herunter, doppelklicken Sie jedoch nicht, um das Installationsprogramm in Windows auszuführen.

   > **Important**
   >
   > Doppelklicken Sie nicht, um das Installationsprogramm in Windows auszuführen, da es sonst nicht installiert werden kann. Die Installation von Agenten ist nur über die Eingabeaufforderung möglich. (Wenn Sie bereits auf das Installationsprogramm doppelt geklickt haben, müssen Sie zu Software navigieren und den Agenten deinstallieren, bevor Sie mit den verbleibenden Installationsschritten fortfahren.)
   > Wenn das Windows Agent-Installationsprogramm keine Version der Visual C++ x86-Laufzeit auf dem Host erkennt, installiert es automatisch die Visual C++ x86 2015—2019-Runtime vor der Installation der Agentsoftware.

2. Öffnen Sie als Administrator eine Eingabeaufforderung und navigieren Sie zum Speicherort des Installationspakets.
3. Wählen Sie eine der folgenden Installationsmethoden, um den Agenten zu installieren.

Zu …	Vorgehensweise
Installieren Sie Discovery Agent	Um den Agenten zu installieren, führen Sie den Befehl agent install aus, wie im folgenden Beispiel gezeigt. Ersetzen Sie es im Beispiel *your-home-region* durch den Namen Ihrer Heimatregion, *aws-access-key-id*durch Ihre Zugriffsschlüssel-ID und *aws-secret-access-key* durch Ihren geheimen Zugriffsschlüssel.

Zu …	Vorgehensweise
	Optional können Sie den Installationsort für den Agenten festlegen, indem Sie den Ordnerpfad *C:\install-location* für den Parameter INSTALLLOCATION angeben. z. B. `INSTALLLOCATION="` *C:\install-location* `"`. Die daraus resultierende Ordnerhierarchie lautet [INSTALLLOCATION-Pfad]\AWS Discovery . Standardmäßig ist das Installationsverzeichnis der `Program Files` Ordner. Optional können `LOGANDCONFIGLOCATION` Sie das Standardverzeichnis (ProgramData) für den Protokollordner und die Konfigurationsdatei des Agenten überschreiben. Die resultierende Ordnerhierarchie ist[*LOGANDCONFIGLOCATION path*]`\AWS Discovery` . `.\AWSDiscoveryAgentInstaller.exe REGION="` *your-home-region* `" KEY_ID="`*aws-access-key-id* `" KEY_SECRET="` *aws-secret-access-key* `" /quiet` Standardmäßig laden Agenten Updates automatisch herunter und installieren sie, sobald sie verfügbar sind. Wir empfehlen die Verwendung dieser Standard-Konfiguration. Wenn Sie jedoch nicht möchten, dass Agenten Updates automatisch herunterladen und anwenden, geben Sie bei der

Zu …	Vorgehensweise
	Ausführung des Agent-Installationsbefehls den folgenden Parameter an: `AUTO_UPDATE=false` **Warning** Durch Deaktivieren von automatischen Upgrades wird verhindert, dass die neuesten Sicherheits-Patches installiert werden.

Zu …	Vorgehensweise
(Optional) Installieren Sie Discovery Agent und konfigurieren Sie einen nicht transparenten Proxy	Um einen intransparenten Proxy zu konfigurieren, fügen Sie dem Installationsbefehl des Agenten die folgenden öffentlichen Eigenschaften hinzu: • PROXY_HOST — Der Name des Proxy-Hosts • PROXY_SCHEME — Das Proxyschema • PROXY_PORT — Die Proxy-Portnummer • PROXY_USER — Der Proxy-Benutzername • PROXY_PASSWORD — Das Proxy-Benutzerkennwort Im Folgenden finden Sie ein Beispiel für den Agent-Installationsbefehl, der die nicht transparenten Proxyeigenschaften verwendet . `.\AWSDiscoveryAgentInstaller.exe REGION=" your-home-region " KEY_ID="aws-access-key-id " KEY_SECRET=" aws-secret-access-key " PROXY_HOST=" myproxy.mycompany.com " PROXY_SCHEME="https" PROXY_PORT=" proxy-port-number " PROXY_USER=" myusername " PROXY_PASSWORD=" mypassword " /quiet` Wenn Ihr Proxy keine Authentifizierung erfordert, lassen Sie die Eigenschaften `PROXY_USER` und `PROXY_PASSWORD` weg. Der Beispielbefehl install verwendet `https`. Wenn Ihr Proxy HTTP verwendet,

Zu …	Vorgehensweise
	geben Sie `http` als `PROXY_SCHEME` Wert an.

4. Wenn ausgehende Verbindungen aus Ihrem Netzwerk eingeschränkt sind, müssen Sie Ihre Firewall-Einstellungen aktualisieren. Agenten benötigen Zugriff auf `arsenal` über den TCP-Port 443. Es ist nicht erforderlich, dass eingehende Ports geöffnet sind.

   Wenn Ihre Heimatregion beispielsweise lautete`eu-central-1`, würden Sie Folgendes verwenden: `https://arsenal-discovery.`*`eu-central-1`*`.amazonaws.com:443`

Paketsignierung und automatische Upgrades

Für Windows Server 2008 und höher signiert Amazon das Installationspaket für den Application Discovery Service Agent kryptografisch mit einem SHA256-Zertifikat. Stellen Sie bei SHA2-signierten automatischen Updates unter Windows Server 2008 SP2 sicher, dass auf den Hosts ein Hotfix zur Unterstützung der SHA2-Signaturauthentifizierung installiert ist. Der neueste Support-Hotfix von Microsoft unterstützt die SHA2-Authentifizierung unter Windows Server 2008 SP2.

> **Note**
>
> Die Hotfixes für die SHA256-Unterstützung für Windows 2003 sind bei Microsoft nicht mehr öffentlich erhältlich. Wenn diese Fixes nicht bereits auf Ihrem Windows 2003-Host installiert sind, sind manuelle Upgrades erforderlich.

Um Upgrades manuell durchzuführen

1. Laden Sie den Windows Agent Updater herunter.
2. Öffnen Sie die Eingabeaufforderung als Administrator.
3. Navigieren Sie zu dem Speicherort, an dem der Updater gespeichert wurde.
4. Führen Sie den folgenden Befehl aus.

```
AWSDiscoveryAgentUpdater.exe /Q
```

Verwalten Sie den Discovery Agent-Prozess in Windows

Sie können das Verhalten des Discovery Agents auf Systemebene über die Windows Server Manager Services-Konsole verwalten. In der folgende Tabelle wird beschrieben, wie dies möglich ist.

Aufgabe	Service-Name	Service-Status/Aktion
Überprüfen Sie, ob ein Agent ausgeführt wird	AWS Discovery Agent AWS Discovery Updater	Started
Starten Sie einen Agenten	AWS Discovery-Agent AWS Discovery Updater	Wählen Sie Starten
Beenden Sie einen Agenten	AWS Discovery-Agent AWS Discovery Updater	Wählen Sie Stop (Anhalten) aus
Starten Sie einen Agenten neu	AWS Discovery-Agent AWS Discovery Updater	Klicken Sie auf Restart (Neu starten).

So deinstallieren Sie einen Erkennungsagenten unter Windows

1. Öffnen Sie die Systemsteuerung in Windows.
2. Wählen Sie Programme.
3. Wählen Sie Programme und Funktionen.
4. Wählen Sie AWS Discovery Agent aus.
5. Wählen Sie Deinstallieren.

> **Note**
>
> Wenn Sie den Agenten nach der Deinstallation erneut installieren möchten, führen Sie den folgenden Befehl mit den `/norestart` Optionen `/repair` und aus.

```
.\AWSDiscoveryAgentInstaller.exe REGION="your-home-region" KEY_ID="aws-access-key-id" KEY_SECRET="aws-secret-access-key" /quiet /repair /norestart
```

Um einen Discovery Agent unter Windows über die Befehlszeile zu deinstallieren

1. Rechtsklicken Sie auf Start.
2. Wählen Sie Command Prompt.
3. Verwenden Sie den folgenden Befehl, um einen Discovery Agent unter Windows zu deinstallieren.

```
wmic product where name='AWS Discovery Agent' call uninstall
```

Problembehandlung für Discovery Agent unter Windows

Wenn bei der Installation oder Verwendung des AWS Application Discovery Agent unter Windows Probleme auftreten, lesen Sie die folgenden Anleitungen zur Protokollierung und Konfiguration. AWS Support fordert diese Dateien häufig an, um mögliche Probleme mit dem Agenten oder seiner Verbindung zum Application Discovery Service zu beheben.

- Protokollierung der Installation

  In einigen Fällen scheint der Installationsbefehl für den Agenten fehl zu schlagen. Beispielsweise kann ein Fehler bei dem Windows Services Manager auftreten, der besagt, dass die Erkennungsdienste nicht erstellt werden. Fügen Sie dem Befehl in diesem Fall /log install.log hinzu, um ein ausführliches Installationsprotokoll zu erstellen.

- Betriebsprotokollierung

  Unter Windows Server 2008 und höher finden Sie Agenten-Protokolldateien in dem folgenden Verzeichnis.

  ```
  C:\ProgramData\AWS\AWS Discovery\Logs
  ```

  Unter Windows Server 2003 finden Sie Agenten-Protokolldateien in dem folgenden Verzeichnis.

```
C:\Documents and Settings\All Users\Application Data\AWS\AWS Discovery\Logs
```

Die Namen der Protokolldateien geben an, ob sie vom Hauptdienst, von automatischen Upgrades oder vom Installationsprogramm generiert wurden.

- Konfigurationsdatei

  Unter Windows Server 2008 und höher finden Sie die Agenten-Konfigurationsdatei in dem folgenden Verzeichnis.

  ```
  C:\ProgramData\AWS\AWS Discovery\config
  ```

  Unter Windows Server 2003 finden Sie die Agenten-Konfigurationsdatei in dem folgenden Verzeichnis.

  ```
  C:\Documents and Settings\All Users\Application Data\AWS\AWS Discovery\config
  ```

- Anweisungen zum Entfernen früherer Versionen des Discovery Agents finden Sie unterVoraussetzungen für Discovery Agent.

Von Discovery Agent gesammelte Daten

AWS Application Discovery Agent (Discovery Agent) ist Software, die Sie auf lokalen Servern und VMs installieren. Discovery Agent sammelt Systemkonfigurations-, Zeitreihenauslastungs- oder Leistungsdaten, Prozessdaten und TCP-Netzwerkverbindungen (Transmission Control Protocol). In diesem Abschnitt werden die gesammelten Daten beschrieben.

Tabellenlegende für die von Discovery Agent gesammelten Daten:

- Der Begriff "Host" bezieht sich auf einen physischen Server oder eine VM.
- Gesammelte Daten sind Messungen in Kilobyte (KB), sofern nicht anders angegeben.
- Entsprechende Daten in der Migration Hub Hub-Konsole werden in Megabyte (MB) gemeldet.
- Die Abfrage erfolgt in Intervallen von etwa 15 Sekunden und wird AWS alle 15 Minuten gesendet.
- Datenfelder, die mit einem Sternchen (*) gekennzeichnet sind, sind nur in den `.csv` Dateien verfügbar, die mit der API-Exportfunktion des Agenten erstellt wurden.

Datenfeld	Beschreibung
agentAssignedProcessID *	Prozess-ID der vom Agenten erkannten Prozesse
agentId	Eindeutige ID des Agenten
agentProvidedTimeStempel *	Datum und Uhrzeit der Agent-Beobachtung (mm/tt/jjjj hh:mm:ss am/pm)
cmdLine*	In der Befehlszeile eingegebener Prozess
cpuType	Im Host verwendeter Typ der CPU (Zentrale inheit)
destinationIp*	IP-Adresse des Geräts, zu dem das Paket gesendet wird
destinationPort*	Portnummer, an die die Daten/Anfrage gesendet werden sollen
family*	Protokoll der Routing-Familie
freeRAM (MB)	Freier RAM und zwischengespeicherter RAM, der Anwendungen unmittelbar zur Verfügung gestellt werden kann, gemessen in MB
gateway*	Knotenadresse des Netzwerks
hostName	Name des Hosts, für den Daten gesammelt wurden
hypervisor	Typ des Hypervisors
ipAddress	IP-Adresse des Hosts
ipVersion*	IP-Versionsnummer
isSystem*	Boolesches Attribut, das angibt, ob ein Prozess zum Betriebssystem gehört

Datenfeld	Beschreibung
macAddress	MAC-Adresse des Hosts
name*	Name des Hosts, des Netzwerks, der Metrik usw., für die Daten gesammelt werden
netMask*	IP-Adressen-Präfix, zu der ein Netzwerk-Host gehört
osName	Name des Betriebssystems auf dem Host
osVersion	Version des Betriebssystems auf dem Host
Pfad	Pfad der Befehle, die ihren Ursprung in der Befehlszeile haben
sourceIp*	IP-Adresse des Geräts, vom dem das IP-Paket gesendet wird
sourcePort*	Portnummer, von der die Daten/Anfrage stammen/stammt
timestamp*	Datum und Uhrzeit des gemeldeten Attributs, die vom Agenten protokolliert wurden
totalCpuUsagePct	Prozentsatz der CPU-Nutzung auf dem Host während des Abrufzeitraums
totalDiskBytesReadPerSecond (Kbit/s)	Gesamtzahl der pro Sekunde gelesenen Kilobits auf allen Festplatten
totalDiskBytesWrittenPerSecond (Kbit/s)	Gesamtzahl der pro Sekunde geschriebenen Kilobits auf allen Festplatten
totalDiskFreeGröße (GB)	Freier Speicherplatz in GB
totalDiskReadOpsPerSecond	Gesamtzahl der E/A-Lesevorgänge pro Sekunde

Datenfeld	Beschreibung
totalDiskSize (GB)	Gesamtkapazität der Festplatte in GB
totalDiskWriteOpsPerSecond	Gesamtzahl der E/A-Schreibvorgänge pro Sekunde
totalNetworkBytesReadPerSecond (Kbit/s)	Gesamtdurchsatz der pro Sekunde gelesenen Bytes
totalNetworkBytesWrittenPerSecond (Kbit/s)	Gesamtdurchsatz der pro Sekunde geschrieb enen Bytes
totalNumCores	Gesamtzahl der unabhängigen Verarbeit ungseinheiten innerhalb der CPU
totalNumCpus	Gesamtzahl der Zentraleinheiten
totalNumDisks	Die Anzahl der physischen Festplatten auf einem Host
totalNumLogical[Prozessoren *]	Gesamtzahl der physischen Kerne multipliziert mit der Anzahl der Threads, die auf jedem Kern ausgeführt werden können
totalNumNetworkKarten	Gesamtzahl der Netzwerkkarten auf dem Server
totalRAM (MB)	Gesamtmenge des auf dem Host verfügbaren RAM
transportProtocol[*]	Verwendeter Typ von Transportprotokoll

Starten oder beenden Sie die Datenerfassung durch Discovery Agent

Wenn der Discovery Agent nach der Bereitstellung und Konfiguration nicht mehr erfasst wird, können Sie ihn neu starten. Sie können die Datenerfassung über die Konsole oder durch API-Aufrufe über die starten oder beenden AWS CLI. Beide Methoden werden in den folgenden Verfahren beschrieben.

Using the Migration Hub console

Das folgende Verfahren zeigt, wie der Discovery Agent-Datenerfassungsprozess auf der Seite Data Collectors der Migration Hub Hub-Konsole gestartet oder gestoppt wird.

Um die Datenerfassung zu starten oder zu beenden

1. Klicken Sie im Navigationsbereich auf Data Collectors (Datensammler).
2. Wählen Sie die Registerkarte Agents (Agenten).
3. Aktivieren Sie das Kontrollkästchen des Agenten, den Sie starten oder beenden möchten.

   > **Tip**
   >
   > Wenn Sie mehrere Agenten installiert haben, die Datenerfassung aber nur auf bestimmten Hosts starten oder beenden möchten, identifiziert die Spalte Hostname in der Zeile des Agenten den Host, auf dem der Agent installiert ist.

4. Wählen Sie Start data collection (Beginnen der Datensammlung) oder Stop data collection (Beenden der Datensammlung).

Using the AWS CLI

Um den Discovery Agent-Datenerfassungsprozess von aus zu starten oder zu beenden AWS CLI, müssen Sie zuerst den AWS CLI in Ihrer Umgebung installieren und dann die CLI so einrichten, dass sie Ihre ausgewählte Migration Hub Hub-Heimatregion verwendet.

Um die Datenerfassung zu installieren AWS CLI und zu starten oder zu beenden

1. Falls Sie dies noch nicht getan haben, installieren Sie das für Ihren Betriebssystemtyp (Windows oder Mac/Linux) AWS CLI geeignete. Anweisungen finden Sie im AWS Command Line Interface Benutzerhandbuch.

2. Öffnen Sie die Eingabeaufforderung (Windows) oder das Terminal (MAC/Linux).

   a. Geben Sie `aws configure` ein und drücken Sie die Eingabetaste.

   b. Geben Sie Ihre AWS Zugangsschlüssel-ID und Ihren AWS geheimen Zugriffsschlüssel ein.

   c. Geben Sie Ihre Heimatregion ein. Geben Sie z. B. für den Standardregionennamen *`us-west-2`* ein. (Wir gehen davon aus, dass `us-west-2` in diesem Beispiel Ihre Heimatregion ist.)

   d. Geben Sie als Standard-Ausgabeformat `text` ein.

3. Geben Sie den folgenden Befehl ein, um die ID des Agenten zu ermitteln, für den Sie die Datenerfassung beenden oder starten möchten:

```
aws discovery describe-agents
```

4. Geben Sie den folgenden Befehl ein, um die Datenerfassung durch den Agenten zu starten:

```
aws discovery start-data-collection-by-agent-ids --agent-ids <agent ID>
```

   Geben Sie den folgenden Befehl ein, um die Datenerfassung durch den Agenten zu beenden:

```
aws discovery stop-data-collection-by-agent-ids --agent-ids <agent ID>
```

Agentloser Collector für Application Discovery Service

Application Discovery Service Agentless Collector (Agentless Collector) ist eine lokale Anwendung, die mithilfe agentenloser Methoden Informationen über Ihre lokale Umgebung sammelt, einschließlich Serverprofilinformationen (z. B. Betriebssystem, Anzahl der CPUs, Größe des Arbeitsspeichers), Datenbankmetadaten und Nutzungsmetriken. Installieren Sie den Agentless Collector als virtuelle Maschine (VM) in Ihrer VMware-vCenter-Server-Umgebung mithilfe einer Open Virtualization Archive (OVA)-Datei.

Agentless Collector verfügt über eine modulare Architektur, die die Verwendung mehrerer agentenloser Erfassungsmethoden ermöglicht. Agentless Collector unterstützt derzeit Module für die Datenerfassung von VMware-VMs sowie von Datenbank- und Analyseservern. Zukünftige Module werden die Erfassung von Netzwerkverbindungen, die Erfassung von zusätzlichen Virtualisierungsplattformen und die Erfassung auf Betriebssystemebene unterstützen.

Agentless Collector unterstützt die Datenerfassung für den AWS Application Discovery Service (Application Discovery Service), der Sie bei der Planung Ihrer Migration zum unterstützt, AWS Cloud indem Nutzungs- und Konfigurationsdaten über Ihre lokalen Server und Datenbanken gesammelt werden.

Der Application Discovery Service ist in integriert AWS Migration Hub, was Ihre Migrationsverfolgung vereinfacht, da Ihre Migrationsstatusinformationen in einer einzigen Konsole zusammengefasst werden. Sie können die erkannten Server anzeigen, Amazon EC2 EC2-Empfehlungen abrufen, Netzwerkverbindungen visualisieren, Server zu Anwendungen gruppieren und dann den Migrationsstatus jeder Anwendung von der Migration Hub Hub-Konsole in Ihrer Heimatregion aus verfolgen.

Das Agentless Collector Datenbank- und Analysedatenerfassungsmodul ist in AWS Database Migration Service ()AWS DMS integriert. Diese Integration hilft Ihnen bei der Planung Ihrer Migration zum AWS Cloud. Sie können das Modul zur Erfassung von Datenbank- und Analysedaten verwenden, um Datenbank- und Analyseserver in Ihrer Umgebung zu ermitteln und eine Bestandsaufnahme der Server zu erstellen, auf die Sie migrieren möchten AWS Cloud. Dieses Datenerfassungsmodul erfasst Datenbankmetadaten und Messdaten zur tatsächlichen Auslastung von CPU, Arbeitsspeicher und Festplattenkapazität. Nachdem Sie diese Metriken erfasst haben, können Sie mit der AWS DMS Konsole Zielempfehlungen für Ihre Quelldatenbanken generieren.

Themen

Erste Schritte mit Agentless Collector

In diesem Abschnitt werden die ersten Schritte mit der Verwendung von Application Discovery Service Agentless Collector (Agentless Collector) beschrieben.

Themen

Voraussetzungen für Agentless Collector

Im Folgenden sind die Voraussetzungen für die Verwendung von Application Discovery Service Agentless Collector (Agentless Collector) aufgeführt:

- Ein oder mehrere AWS Konten.
- Ein AWS Konto mit AWS Migration Hub festgelegter Heimatregion, sieheMelden Sie sich bei der Migration Hub Hub-Konsole an und wählen Sie eine Heimatregion. Ihre Migration Hub Hub-Daten werden in Ihrer Heimatregion zu Ermittlungs-, Planungs- und Migrationsverfolgungszwecken gespeichert.
- Ein AWS Konto-IAM-Benutzer, der für die Verwendung der AWS verwalteten Richtlinie `AWSApplicationDiscoveryAgentlessCollectorAccess` eingerichtet ist. Um das Modul zur Erfassung von Datenbank- und Analysedaten verwenden zu können, muss dieser IAM-Benutzer außerdem zwei vom Kunden verwaltete IAM-Richtlinien und verwenden. `DMSCollectorPolicy`

`FleetAdvisorS3Policy` Weitere Informationen finden Sie unter Schritt 1: Erstellen Sie einen IAM-Benutzer für Agentless Collector. Der IAM-Benutzer muss in einem AWS Konto erstellt werden, für das die Heimatregion von Migration Hub festgelegt ist.

- VMware vCenter Server V5.5, V6, V6.5, 6.7 oder 7.0.

> **Note**
>
> Der Agentless Collector unterstützt alle diese Versionen von VMware, aber wir testen derzeit mit den Versionen 6.7 und 7.0.

- Stellen Sie für die Einrichtung von VMware vCenter Server sicher, dass Sie vCenter-Anmeldeinformationen mit den für die Systemgruppe festgelegten Lese- und Anzeigeberechtigungen angeben können.
- Agentless Collector benötigt ausgehenden Zugriff über TCP-Port 443 auf mehrere Domänen. AWS Eine Liste dieser Domänen finden Sie unter. Konfigurieren Sie die Firewall für den ausgehenden Zugriff auf Domains AWS
- Um das Modul zur Erfassung von Datenbank- und Analysedaten zu verwenden, erstellen Sie einen Amazon S3 S3-Bucket in der RegionAWS-Region, die Sie als Ihre Migration Hub Hub-Heimatregion festgelegt haben. Die Module zur Erfassung von Datenbank- und Analysedaten speichern Inventarmetadaten in diesem Amazon S3 S3-Bucket. Weitere Informationen finden Sie unter Erstellen eines Buckets im Amazon S3 S3-Benutzerhandbuch.

Konfigurieren Sie die Firewall für den ausgehenden Zugriff auf Domains AWS

Wenn ausgehende Verbindungen aus Ihrem Netzwerk eingeschränkt sind, müssen Sie Ihre Firewall-Einstellungen aktualisieren, um ausgehenden Zugriff auf die AWS Domänen zu ermöglichen, die Agentless Collector benötigt. Welche AWS Domains ausgehenden Zugriff erfordern, hängt davon ab, ob Ihre Heimatregion von Migration Hub die Region USA West (Oregon), US-West-2 oder eine andere Region ist.

Für die folgenden Domains ist ausgehender Zugriff erforderlich, wenn die Heimatregion Ihres AWS Kontos US-West-2 lautet:

- `arsenal-discovery.us-west-2.amazonaws.com`— Der Collector verwendet diese Domain, um zu überprüfen, ob sie mit den erforderlichen IAM-Benutzeranmeldedaten konfiguriert ist. Der Collector verwendet es auch zum Senden und Speichern gesammelter Daten, da die Heimatregion us-west-2 ist.

- `migrationhub-config.us-west-2.amazonaws.com`— Der Collector verwendet diese Domain, um anhand der angegebenen IAM-Benutzeranmeldedaten zu ermitteln, in welche Heimatregion der Collector Daten sendet.
- `api.ecr-public.us-east-1.amazonaws.com`— Der Collector verwendet diese Domain, um verfügbare Updates zu ermitteln.
- `public.ecr.aws`— Der Collector verwendet diese Domain zum Herunterladen der Updates.
- `dms.`*`your-migrationhub-home-region`*`.amazonaws.com`— Der Collector verwendet diese Domain, um eine Verbindung zum AWS DMS Datensammelpunkt herzustellen.
- `s3.amazonaws.com`— Der Collector verwendet diese Domain, um Daten, die vom Datenbank- und Analysedatenerfassungsmodul gesammelt wurden, in Ihren Amazon S3 S3-Bucket hochzuladen.

Für die folgenden Domains ist ausgehender Zugriff erforderlich, sofern die Heimatregion Ihres AWS Kontos nicht **`us-west-2`** der Fall ist:

- `arsenal-discovery.us-west-2.amazonaws.com`— Der Collector verwendet diese Domain, um zu überprüfen, ob sie mit den erforderlichen IAM-Benutzeranmeldeinformationen konfiguriert ist.
- `arsenal-discovery.`*`your-migrationhub-home-region`*`.amazonaws.com`— Der Collector verwendet diese Domain zum Senden und Speichern der gesammelten Daten.
- `migrationhub-config.us-west-2.amazonaws.com`— Der Collector verwendet diese Domain, um anhand der bereitgestellten IAM-Benutzeranmeldedaten zu bestimmen, an welche Heimatregion der Collector Daten senden soll.
- `api.ecr-public.us-east-1.amazonaws.com`— Der Collector verwendet diese Domain, um verfügbare Updates zu ermitteln.
- `public.ecr.aws`— Der Collector verwendet diese Domain zum Herunterladen der Updates.
- `dms.`*`your-migrationhub-home-region`*`.amazonaws.com`— Der Collector verwendet diese Domain, um eine Verbindung zum AWS DMS Datensammelpunkt herzustellen.
- `s3.amazonaws.com`— Der Collector verwendet diese Domain, um Daten, die vom Datenbank- und Analysedatenerfassungsmodul gesammelt wurden, in Ihren Amazon S3 S3-Bucket hochzuladen.

Bei der Einrichtung von Agentless Collector erhalten Sie möglicherweise folgende Fehler: Setup ist fehlgeschlagen — Überprüfen Sie Ihre Anmeldeinformationen und versuchen Sie es erneut,

andernfalls ist AWS keine Verbindung möglich. Bitte überprüfen Sie die Netzwerkeinstellungen. Diese Fehler können durch einen fehlgeschlagenen Versuch des Agentless Collectors verursacht werden, eine HTTPS-Verbindung zu einer der AWS Domänen herzustellen, auf die er ausgehenden Zugriff benötigt.

Wenn keine Verbindung zu hergestellt werden AWS kann, kann Agentless Collector keine Daten aus Ihrer lokalen Umgebung sammeln. Informationen darüber, wie Sie die Verbindung zu reparieren habenAWS, finden Sie unter. Behebung von Problemen, die Agentless Collector während der Installation nicht erreichen kann AWS

Schritt 1: Erstellen Sie einen IAM-Benutzer für Agentless Collector

Um Agentless Collector verwenden zu können, müssen Sie in dem AWS Konto, das Sie verwendet habenMelden Sie sich bei der Migration Hub Hub-Konsole an und wählen Sie eine Heimatregion, einen AWS Identity and Access Management (IAM-) Benutzer erstellen. Richten Sie diesen IAM-Benutzer dann so ein, dass er die folgende AWS verwaltete Richtlinie verwendet. AWSApplicationDiscoveryAgentlessCollectorAccess Sie fügen diese IAM-Richtlinie bei der Erstellung des IAM-Benutzers hinzu.

Um das Modul zur Erfassung von Datenbank- und Analysedaten zu verwenden, erstellen Sie zwei vom Kunden verwaltete IAM-Richtlinien. Diese Richtlinien ermöglichen den Zugriff auf Ihren Amazon S3 S3-Bucket und die AWS DMS API. Weitere Informationen finden Sie unter Erstellen einer vom Kunden verwalteten Richtlinie im IAM-Benutzerhandbuch.

- Verwenden Sie den folgenden JSON-Code, um die **`DMSCollectorPolicy`** Richtlinie zu erstellen.

```
{
 "Version": "2012-10-17",
 "Statement": [{
  "Effect": "Allow",
  "Action": [
   "dms:DescribeFleetAdvisorCollectors",
   "dms:ModifyFleetAdvisorCollectorStatuses",
   "dms:UploadFileMetadataList"
  ],
  "Resource": "*"
 }]
}
```

- Verwenden Sie den folgenden JSON-Code, um die **`FleetAdvisorS3Policy`** Richtlinie zu erstellen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject*",
                "s3:GetBucket*",
                "s3:List*",
                "s3:DeleteObject*",
                "s3:PutObject*"
            ],
            "Resource": [
                "arn:aws:s3:::bucket_name",
                "arn:aws:s3:::bucket_name/*"
            ]
        }
    ]
}
```

  Ersetzen Sie es im vorherigen Beispiel *`bucket_name`* durch den Namen des Amazon S3 S3-Buckets, den Sie im Schritt Voraussetzungen erstellt haben.

Wir empfehlen, dass Sie einen IAM-Benutzer ohne Administratorrechte für die Verwendung mit Agentless Collector erstellen. Wenn Sie IAM-Benutzer ohne Administratorrechte erstellen, befolgen Sie die bewährte Sicherheitsmethode Grant Least Privilege, d. h. gewähren Sie Benutzern Mindestberechtigungen.

Um einen IAM-Benutzer ohne Administratorrechte zur Verwendung mit Agentless Collector zu erstellen

1. Navigieren Sie in AWS Management Console zur IAM-Konsole und verwenden Sie dabei das AWS Konto, mit dem Sie die Heimatregion eingerichtet haben. Melden Sie sich bei der Migration Hub Hub-Konsole an und wählen Sie eine Heimatregion
2. Erstellen Sie einen IAM-Benutzer ohne Administratorrechte, indem Sie den Anweisungen zum Erstellen eines Benutzers mit der Konsole folgen, wie unter Erstellen eines IAM-Benutzers in Ihrem AWS Konto im IAM-Benutzerhandbuch beschrieben.

Folgen Sie dabei den Anweisungen im IAM-Benutzerhandbuch:

- Wählen Sie im Schritt zur Auswahl des Zugriffstyps die Option Programmatischer Zugriff aus. Hinweis: Wählen Sie den Zugriff auf die AWS Managementkonsole nur aus, wenn Sie dieselben IAM-Benutzeranmeldedaten für den Zugriff auf die AWS Konsole verwenden möchten.
- Wählen Sie im nächsten Schritt auf der Seite „Berechtigungen festlegen“ die Option „Bestehende Richtlinien direkt an den Benutzer anhängen“. Wählen Sie dann die `AWSApplicationDiscoveryAgentlessCollectorAccess` AWS verwaltete Richtlinie aus der Liste der Richtlinien aus.

  Wählen Sie als Nächstes die `DMSCollectorPolicy` und vom `FleetAdvisorS3Policy` Kunden verwalteten IAM-Richtlinien aus.
- Wenn Sie sich die Zugangsschlüssel des Benutzers (Zugangsschlüssel-IDs und geheime Zugangsschlüssel) ansehen, folgen Sie den Anweisungen im Abschnitt Wichtiger Hinweis zum Speichern der neuen Zugriffsschlüssel-ID und des geheimen Zugangsschlüssels des Benutzers an einem sicheren Ort. Sie benötigen diese Zugangsschlüssel inSchritt 5: Agentless Collector konfigurieren.

  Es ist eine bewährte AWS Sicherheitsmethode, die Zugangsschlüssel abwechselnd zu verwenden. Informationen zur Rotation von Schlüsseln finden Sie im IAM-Benutzerhandbuch unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern.

Schritt 2: Laden Sie den Agentless Collector herunter

Um den Application Discovery Service Agentless Collector (Agentless Collector) einzurichten, müssen Sie die Agentless Collector Open Virtualization Archive (OVA) -Datei herunterladen und bereitstellen. Der Agentless Collector ist eine virtuelle Appliance, die Sie in Ihrer lokalen VMware-Umgebung installieren. In diesem Schritt wird beschrieben, wie Sie die Collector-OVA-Datei herunterladen, und im nächsten Schritt wird beschrieben, wie Sie sie bereitstellen.

Um die Collector-OVA-Datei herunterzuladen und ihre Prüfsumme zu überprüfen

1. Melden Sie sich als VMware-Administrator bei vCenter an und wechseln Sie zu dem Verzeichnis, in das Sie die Agentless Collector OVA-Datei herunterladen möchten.
2. Laden Sie die OVA-Datei von der folgenden URL herunter:

Agentenloser Collector, OVA

3. Je nachdem, welchen Hashing-Algorithmus Sie in Ihrer Systemumgebung verwenden, laden Sie entweder MD5 oder SHA256 herunter, um die Datei mit dem Prüfsummenwert zu erhalten. Verwenden Sie den heruntergeladenen Wert, um die im vorherigen Schritt heruntergeladene `ApplicationDiscoveryServiceAgentlessCollector` Datei zu überprüfen.
4. Führen Sie je nach Linux-Variante den entsprechenden MD5-Befehl oder SHA256-Befehl aus, um sicherzustellen, dass die kryptografische Signatur der Datei `ApplicationDiscoveryServiceAgentlessCollector.ova`mit dem Wert in der entsprechenden MD5/SHA256-Datei übereinstimmt, die Sie heruntergeladen haben.

```
$ md5sum ApplicationDiscoveryServiceAgentlessCollector.ova
```

```
$ sha256sum ApplicationDiscoveryServiceAgentlessCollector.ova
```

Schritt 3: Stellen Sie Agentless Collector bereit

Application Discovery Service Agentless Collector (Agentless Collector) ist eine virtuelle Appliance, die Sie in Ihrer lokalen VMware-Umgebung installieren. In diesem Abschnitt wird beschrieben, wie Sie die Open Virtualization Archive (OVA) -Datei, die Sie im vorherigen Schritt heruntergeladen haben, in Ihrer VMware-Umgebung bereitstellen.

Technische Daten der virtuellen Maschine mit Agentless Collector

- Betriebssystem — Amazon Linux 2
- Arbeitsspeicher — 16 GB
- CPU — 4 Kerne

Das folgende Verfahren führt Sie durch die Bereitstellung der Agentless Collector OVA-Datei in Ihrer VMware-Umgebung.

So stellen Sie Agentless Collector bereit

1. Melden Sie sich bei vCenter als VMware-Administrator an.
2. Verwenden Sie eine der folgenden Methoden, um die OVA-Datei zu installieren:

- Verwenden Sie die Benutzeroberfläche: Wählen Sie „Datei“, wählen Sie „OVF-Vorlage bereitstellen“, wählen Sie die Collector-OVA-Datei aus, die Sie im vorherigen Abschnitt heruntergeladen haben, und schließen Sie dann den Assistenten ab.
- Verwenden Sie die Befehlszeile: Um die Collector-OVA-Datei von der Befehlszeile aus zu installieren, laden Sie das VMware Open Virtualization Format Tool (ovftool) herunter und verwenden Sie es. Um ovftool herunterzuladen, wählen Sie auf der Seite mit der OVF-Tool-Dokumentation eine Version aus.

  Im Folgenden finden Sie ein Beispiel für die Verwendung des Befehlszeilentools ovftool zur Installation der Collector-OVA-Datei.

  ```
  ovftool --acceptAllEulas --name=AgentlessCollector --datastore=datastore1
   -dm=thin ApplicationDiscoveryServiceAgentlessCollector.ova
   'vi://username:password@vcenterurl/Datacenter/host/esxi/'
  ```

  Im Folgenden werden die ***ersetzbaren*** Werte im Beispiel beschrieben

  - Der Name ist der Name, den Sie für Ihre Agentless Collector-VM verwenden möchten.
  - Der Datenspeicher ist der Name des Datenspeichers in Ihrem vCenter.
  - Der OVA-Dateiname ist der Name der heruntergeladenen Collector-OVA-Datei.
  - Der Benutzername/das Passwort sind Ihre vCenter-Anmeldeinformationen.
  - Die vcenterurl ist die URL Ihres vCenter.
  - Der vi-Pfad ist der Pfad zu Ihrem VMware ESXi-Host.

3. Suchen Sie den bereitgestellten Agentless Collector in Ihrem vCenter. Klicken Sie mit der rechten Maustaste auf die VM und wählen Sie dann Power, Power On.
4. Nach einigen Minuten wird die IP-Adresse des Collectors in vCenter angezeigt. Sie verwenden diese IP-Adresse, um eine Verbindung zum Collector herzustellen.

Schritt 4: Greifen Sie auf die Agentless Collector-Konsole zu

Das folgende Verfahren beschreibt, wie Sie auf die Application Discovery Service Agentless Collector (Agentless Collector) -Konsole zugreifen.

So greifen Sie auf die Agentless Collector-Konsole zu

1. Öffnen Sie einen Webbrowser und geben Sie dann die folgende URL in die Adressleiste ein: **https://**<ip_address>, woher <ip_address>die IP-Adresse des Collectors stammtSchritt 3: Stellen Sie Agentless Collector bereit.
2. Wählen Sie Erste Schritte, wenn Sie zum ersten Mal auf Agentless Collector zugreifen. Danach werden Sie aufgefordert, sich anzumelden.

Wenn Sie zum ersten Mal auf die Agentless Collector-Konsole zugreifen, tun Sie dies als Nächstes. Schritt 5: Agentless Collector konfigurieren Andernfalls werden Sie als Nächstes sehenDas Agentless Collector-Dashboard.

Schritt 5: Agentless Collector konfigurieren

Application Discovery Service Agentless Collector (Agentless Collector) ist eine auf Amazon Linux 2 basierende virtuelle Maschine (VM). Im folgenden Abschnitt wird beschrieben, wie Sie eine Collector-VM auf der Seite „Agentless Collector konfigurieren“ der Agentless Collector-Konsole konfigurieren.

So konfigurieren Sie eine Collector-VM auf der Seite „Agentless Collector konfigurieren“

1. Geben Sie unter Collector-Name einen Namen für den Collector ein, um ihn zu identifizieren. Der Name kann Leerzeichen, aber keine Sonderzeichen enthalten.
2. Geben Sie unter Datensynchronisierung den AWS Zugriffsschlüssel und den geheimen Schlüssel für den AWS Konto-IAM-Benutzer ein, der als Zielkonto für den Empfang der vom Collector erkannten Daten angegeben werden soll. Informationen zu den Anforderungen für den IAM-Benutzer finden Sie unter. Schritt 1: Erstellen Sie einen IAM-Benutzer für Agentless Collector
    a. Geben Sie für den AWSZugriffsschlüssel den Zugriffsschlüssel des AWS Konto-IAM-Benutzers ein, den Sie als Zielkonto angeben.
    b. Geben Sie unter AWSSecret-Key den geheimen Schlüssel des IAM-Benutzers des AWS Kontos ein, den Sie als Zielkonto angeben.
    c. (Optional) Wenn Ihr Netzwerk die Verwendung eines Proxys für den Zugriff erfordertAWS, geben Sie den Proxyhost, den Proxy-Port und optional die Anmeldeinformationen ein, die für die Authentifizierung bei Ihrem vorhandenen Proxy-Server erforderlich sind.
3. Richten Sie unter Agentless Collector-Passwort ein Passwort ein, mit dem der Zugriff auf Agentless Collector authentifiziert werden soll.

- Passwörter unterscheiden Groß- und Kleinschreibung
- Passwörter müssen zwischen 8 und 64 Zeichen lang sein
- Passwörter müssen mindestens ein Zeichen aus jeder der folgenden vier Kategorien enthalten:
  - Kleinbuchstaben (a – z)
  - Großbuchstaben (A – Z)
  - Zahlen (0 – 9)
  - Nicht-alphanumerische Zeichen (@$! #%*? &)
- Passwörter dürfen keine anderen Sonderzeichen als die folgenden enthalten: @$! #%*? &

a. Geben Sie für das Agentless Collector-Passwort ein Passwort ein, mit dem der Zugriff auf den Collector authentifiziert werden soll.

b. Wenn Sie das Agentless Collector-Passwort erneut eingeben möchten, geben Sie das Passwort zur Bestätigung erneut ein.

4. Lesen Sie unter Andere Einstellungen die Lizenzvereinbarung. Wenn Sie damit einverstanden sind, sie zu akzeptieren, aktivieren Sie das Kontrollkästchen.
5. Um automatische Updates für Agentless Collector zu aktivieren, wählen Sie unter Andere Einstellungen die Option Agentless Collector automatisch aktualisieren aus. Wenn Sie dieses Kontrollkästchen nicht aktivieren, müssen Sie Agentless Collector manuell aktualisieren, wie unter beschrieben. Manuelles Aktualisieren von Agentless Collector
6. Wählen Sie Konfigurationen speichern aus.

In den folgenden Themen werden optionale Collector-Konfigurationsaufgaben beschrieben.

Optionale Konfigurationsaufgaben

- (Optional) Konfigurieren Sie eine statische IP-Adresse für die Agentless Collector-VM
- (Optional) Setzen Sie die Agentless Collector-VM wieder auf die Verwendung von DHCP zurück
- (Optional) Konfigurieren Sie das Kerberos-Authentifizierungsprotokoll

(Optional) Konfigurieren Sie eine statische IP-Adresse für die Agentless Collector-VM

In den folgenden Schritten wird beschrieben, wie Sie eine statische IP-Adresse für die VM Application Discovery Service Agentless Collector (Agentless Collector) konfigurieren. Bei der ersten Installation

ist die Collector-VM für die Verwendung des Dynamic Host Configuration Protocol (DHCP) konfiguriert.

> **Note**
>
> Der Agentless Collector unterstützt IPv4. Er unterstützt IPv6 nicht.

Um eine statische IP-Adresse für die Collector-VM zu konfigurieren

1. Sammeln Sie die folgenden Netzwerkinformationen von VMware vCenter:
   - Statische IP-Adresse — Eine unsignierte IP-Adresse im Subnetz. Zum Beispiel 192.168.1.138.
   - Netzwerkmaske — Diese erhalten Sie, indem Sie die IP-Adresseinstellung des VMware vCenter-Hosts überprüfen, der die Collector-VM hostet. Zum Beispiel 255.255.255.0.
   - Standard-Gateway — Dieses erhalten Sie, indem Sie die IP-Adresseinstellung des VMware vCenter-Hosts überprüfen, der die Collector-VM hostet. Zum Beispiel 192.168.1.1.
   - Primärer DNS — Dieser kann abgerufen werden, indem die IP-Adresseinstellung des VMware vCenter-Hosts überprüft wird, der die Collector-VM hostet. Zum Beispiel 192.168.1.1.
   - (Optional) Sekundäres DNS
   - (Optional) Lokaler Domänenname — Dadurch kann der Collector die vCenter-Host-URL ohne den Domänennamen erreichen.
2. Öffnen Sie die VM-Konsole des Collectors und melden Sie sich **`ec2-user`** mit dem Passwort an, **`collector`** wie im folgenden Beispiel gezeigt.

   ```
   username: ec2-user
   password: collector
   ```

3. Deaktivieren Sie die Netzwerkschnittstelle, indem Sie den folgenden Befehl in das Remote-Terminal eingeben.

   ```
   sudo /sbin/ifdown eth0
   ```

4. Aktualisieren Sie die Konfiguration der Schnittstelle eth0 mithilfe der folgenden Schritte.

   a. Öffnen Sie ifcfg-eth0 im vi-Editor mit dem folgenden Befehl.

```
sudo vi /etc/sysconfig/network-scripts/ifcfg-eth0
```

b. Aktualisieren Sie die Schnittstellenwerte, wie im folgenden Beispiel gezeigt, mit den Informationen, die Sie im Schritt Netzwerkinformationen sammeln gesammelt haben.

```
DEVICE=eth0
BOOTPROTO=static
ONBOOT=yes
IPADDR=static-ip-value
NETMASK=netmask-value
GATEWAY=gateway-value
TYPE=Ethernet
USERCTL=yes
PEERDNS=no
RES_OPTIONS="timeout:2 attempts:5"
```

5. Aktualisieren Sie das Domain Name System (DNS) mithilfe der folgenden Schritte.

a. Öffnen Sie die `resolv.conf` Datei in vi mit dem folgenden Befehl.

```
sudo vi /etc/resolv.conf
```

b. Aktualisieren Sie die `resolv.conf` Datei in vi mit dem folgenden Befehl.

```
search localdomain-name
options timeout:2 attempts:5
nameserver dnsserver-value
```

Das folgende Beispiel zeigt eine bearbeitete `resolv.conf` Datei.

```
search vsphere.local
options timeout:2 attempts:5
nameserver 192.168.1.1
```

6. Aktivieren Sie die Netzwerkschnittstelle, indem Sie den folgenden Befehl eingeben.

```
sudo /sbin/ifup eth0
```

7. Starten Sie die VM neu, wie im folgenden Beispiel gezeigt.

```
sudo reboot
```

8. Überprüfen Sie Ihre Netzwerkeinstellungen mithilfe der folgenden Schritte.

   a. Überprüfen Sie, ob die IP-Adresse korrekt konfiguriert ist, indem Sie die folgenden Befehle eingeben.

   ```
   ifconfig

   ip addr show
   ```

   b. Überprüfen Sie, ob das Gateway korrekt hinzugefügt wurde, indem Sie den folgenden Befehl eingeben.

   ```
   route -n
   ```

   Die Ausgabe sollte dem folgenden Beispiel ähneln.

   ```
   Kernel IP routing table
   Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
   0.0.0.0         192.168.1.1     0.0.0.0         UG    0      0        0 eth0
   172.17.0.0      0.0.0.0         255.255.0.0     U     0      0        0 docker0
   192.168.1.0     0.0.0.0         255.255.255.0   U     0      0
   ```

   c. Stellen Sie sicher, dass Sie eine öffentliche URL pingen können, indem Sie den folgenden Befehl eingeben.

   ```
   ping www.google.com
   ```

   d. Stellen Sie sicher, dass Sie die vCenter-IP-Adresse oder den Hostnamen wie im folgenden Beispiel gezeigt pingen können.

   ```
   ping vcenter-host-url
   ```

(Optional) Setzen Sie die Agentless Collector-VM wieder auf die Verwendung von DHCP zurück

In den folgenden Schritten wird beschrieben, wie Sie die Agentless Collector-VM für die Verwendung von DHCP neu konfigurieren.

So konfigurieren Sie die Collector-VM für die Verwendung von DHCP

1. Deaktivieren Sie die Netzwerkschnittstelle, indem Sie den folgenden Befehl in das Remote-Terminal eingeben.

   ```
   sudo /sbin/ifdown eth0
   ```

2. Aktualisieren Sie die Netzwerkkonfiguration mithilfe der folgenden Schritte.

   a. Öffnen Sie die `ifcfg-eth0` Datei mit dem folgenden Befehl im vi-Editor.

      ```
      sudo /sbin/ifdown eth0
      ```

   b. Aktualisieren Sie die Werte in der `ifcfg-eth0` Datei wie im folgenden Beispiel gezeigt.

      ```
      DEVICE=eth0
      BOOTPROTO=dhcp
      ONBOOT=yes
      TYPE=Ethernet
      USERCTL=yes
      PEERDNS=yes
      DHCPV6C=yes
      DHCPV6C_OPTIONS=-nw
      PERSISTENT_DHCLIENT=yes
      RES_OPTIONS="timeout:2 attempts:5"
      ```

3. Setzen Sie die DNS-Einstellung zurück, indem Sie den folgenden Befehl eingeben.

   ```
   echo "" | sudo tee /etc/resolv.conf
   ```

4. Aktivieren Sie die Netzwerkschnittstelle, indem Sie den folgenden Befehl eingeben.

   ```
   sudo /sbin/ifup eth0
   ```

5. Starten Sie die Collector-VM neu, wie im folgenden Beispiel gezeigt.

```
sudo reboot
```

(Optional) Konfigurieren Sie das Kerberos-Authentifizierungsprotokoll

Wenn Ihr Betriebssystemserver das Kerberos-Authentifizierungsprotokoll unterstützt, können Sie dieses Protokoll verwenden, um eine Verbindung zu Ihrem Server herzustellen. Dazu müssen Sie die Application Discovery Service Agentless Collector VM konfigurieren.

In den folgenden Schritten wird beschrieben, wie Sie das Kerberos-Authentifizierungsprotokoll auf Ihrer Application Discovery Service Agentless Collector-VM konfigurieren.

So konfigurieren Sie das Kerberos-Authentifizierungsprotokoll auf Ihrer Collector-VM

1. Öffnen Sie die VM-Konsole des Collectors und melden Sie sich **`ec2-user`** mit dem Passwort an, **`collector`** wie im folgenden Beispiel gezeigt.

   ```
   username: ec2-user
   password: collector
   ```

2. Öffnen Sie die `krb5.conf` Konfigurationsdatei im `/etc` Ordner. Dazu können Sie das folgende Codebeispiel verwenden.

   ```
   cd /etc
   sudo nano krb5.conf
   ```

3. Aktualisieren Sie die `krb5.conf` Konfigurationsdatei mit den folgenden Informationen.

   ```
   [libdefaults]
       forwardable = true
       dns_lookup_realm = true
       dns_lookup_kdc = true
       ticket_lifetime = 24h
       renew_lifetime = 7d
       default_realm = default_Kerberos_realm

   [realms]
    default_Kerberos_realm = {
        kdc = KDC_hostname
        server_name = server_hostname
        default_domain = domain_to_expand_hostnames
   ```

```
 }

[domain_realm]
 .domain_name = default_Kerberos_realm
 domain_name = default_Kerberos_realm
```

Speichern Sie die Datei und schließen Sie den Texteditor.

4. Starten Sie die Collector-VM neu, wie im folgenden Beispiel gezeigt.

```
sudo reboot
```

Schritt 6: Richten Sie die Agentless Collector-Datenerfassungsmodule ein

Auf der Dashboardseite der Application Discovery Service Agentless Collector (Agentless Collector) -Konsole unter Datenerfassung richten Sie das Datenerfassungsmodul ein, um Inventar-, Profil- und Nutzungsdaten von Ihren Servern zu sammeln.

Agentless Collector unterstützt derzeit die Datenerfassung von VMware-VMs sowie von Datenbank- und Analyseservern. Zukünftige Module werden die Erfassung von zusätzlichen Virtualisierungsplattformen sowie die Erfassung auf Betriebssystemebene unterstützen.

Themen

- Datenerfassungsmodul für VMware vCenter Agentless Collector
- Modul zur Erfassung von Datenbank- und Analysedaten

Datenerfassungsmodul für VMware vCenter Agentless Collector

In diesem Abschnitt wird das VMware vCenter-Datenerfassungsmodul Application Discovery Service Agentless Collector (Agentless Collector) beschrieben, mit dem Serverinventar-, Profil- und Nutzungsdaten Ihrer VMware-VMs erfasst werden.

Themen

- So richten Sie das Agentless Collector-Datenerfassungsmodul für VMware vCenter ein
- enden Datensammlung ammlung ammlung ammlung ammlung ammlung ammlung
- Steuern Sie den Umfang der vCenter-Datenerfassung

So richten Sie das Agentless Collector-Datenerfassungsmodul für VMware vCenter ein

In diesem Abschnitt wird beschrieben, wie Sie das VMware-vCenter-Datenerfassungsmodul von Agentless Collector einrichten, um Serverinventar-, Profil- und Nutzungsdaten von Ihren VMware-VMs zu sammeln.

> **Note**
>
> Bevor Sie das vCenter-Setup starten, stellen Sie sicher, dass Sie vCenter-Anmeldeinformationen mit den für die Systemgruppe festgelegten Lese- und Anzeigeberechtigungen angeben können.

So richten Sie das VMware vCenter-Datenerfassungsmodul ein

1. Wählen Sie auf der Agentless Collector-Dashboardseite unter Datenerfassung im Abschnitt VMware vCenter die Option Einrichten aus.
2. Gehen Sie auf der Seite „VMware vCenter-Datenerfassung einrichten“ wie folgt vor:
   a. Unter vCenter-Anmeldeinformationen:
      i. Geben Sie für vCenter URL/IP die IP-Adresse Ihres VMware vCenter Server-Hosts ein.
      ii. Geben Sie als vCenter-Benutzername den Namen eines lokalen Benutzers oder Domänenbenutzers ein, den der Collector für die Kommunikation mit vCenter verwendet. Für Domänenbenutzer: Verwenden Sie die Form Domäne\Benutzername oder Benutzername@Domäne.
      iii. Geben Sie für vCenter Password (vCenter-Passwort) das lokale oder Domänenbenutzerpasswort ein.
   b. Unter Präferenzen für die Datenerfassung:
      - Um unmittelbar nach einer erfolgreichen Einrichtung automatisch mit der Datenerfassung zu beginnen, wählen Sie Datenerfassung automatisch starten aus.
   c. Wählen Sie Set up (Festlegen).

Als Nächstes wird die Seite mit den Details zur VMware-Datenerfassung angezeigt, die im nächsten Thema beschrieben wird.

enden Datensammlung ammlung ammlung ammlung ammlung ammlung ammlung

Auf der Seite mit den Details zur VMware-Datenerfassung werden Details zu dem vCenter angezeigt, in dem Sie es eingerichtet habenSo richten Sie das Agentless Collector-Datenerfassungsmodul für VMware vCenter ein.

Unter Entdeckte vCenter-Server wird das von Ihnen eingerichtete vCenter mit den folgenden Informationen zum vCenter aufgeführt:

- Die IP-Adresse des vCenter-Servers des vCenter-Servers zu nutzen.
- Die Anzahl der Server im vCenter.
- Der DatensDatensammlung ammlung ammlung ammlung ammlung ammlung ammlung ammlung ammlung ammlung ammlung ammlung
- Wie lange ist seit dem letzten Update vergangen.

Wählen Sie vCenter Server entfernen, um den angezeigten vCenter-Server zu entfernen, und kehren Sie zur Seite „VMware vCenter-Datenerfassung einrichten“ zurück.

Wenn Sie sich nicht dafür entschieden haben, die Datenerfassung automatisch zu starten, können Sie die Datenerfassung starten, indem Sie auf dieser Seite auf die Schaltfläche Datenerfassung starten klicken. Nach dem Start der Datenerfassung ändert sich die Startschaltfläche in Datenerfassung beenden.

Wenn in der Spalte Sammlungsstatus Erfassung angezeigt wird, hat die Datenerfassung begonnen.

Sie sehen die gesammelten Daten in derAWS Migration Hub Konsole. Wenn Sie Daten für eine VMware vCenter-Serverinventur sammeln, können Sie auf Daten zugreifen, die etwa 15 Minuten nach dem Aktivieren der Datenerfassung in der Konsole angezeigt werden.

Sie können auf dieser Seite Server in Migration Hub anzeigen wählen, um die Migration Hub Hub-Konsole zu öffnen, sofern Ihr Internetzugang nicht blockiert ist. Unabhängig davon, ob Sie diese Schaltfläche wählen oder nicht, finden Sie Informationen zum Zugriff auf die Migration Hub Hub-Konsole unterSchritt 7: Gesammelte Daten anzeigen.

Im Folgenden finden Sie die Richtlinien für die empfohlene Dauer der Datenerfassung gemäß den Aktivitäten zur Migrationsplanung:

- TCO (Gesamtbetriebskosten): 2 bis 4 Wochen
- Migrationsplanung — 2 bis 6 Wochen

Steuern Sie den Umfang der vCenter-Datenerfassung

Für die Inventarisierung mithilfe des Application Discovery Service benötigt der vCenter-Benutzer auf jedem ESX-Host oder jeder VM nur Leserechte. Über die Berechtigungseinstellungen können Sie festlegen, welche Hosts und VMs in die Datensammlung einbezogen werden sollen. Sie können entweder zulassen, dass alle Hosts und VMs unter dem aktuellen vCenter inventarisiert werden, oder Berechtigungen auf einercase-by-case Basis gewähren.

> **Note**
>
> Im Sinne bewährter Sicherheitsmethoden wird empfohlen, dem vCenter-Benutzer des Application Discovery -Services zu erenden enden

In den folgenden Verfahren werden Konfigurationsszenarien in aufsteigender Reihenfolge von der geringsten zur höchsten Feinabstimmung beschrieben. Diese Verfahren gelten für vSphere Client v6.7.0.2. Die Verfahren für andere Versionen des Clients können unterschiedlich sein, je nachdem, welche Version des vSphere-Clients Sie verwenden.

Informationen über alle ESX-Hosts und VMs unter dem aktuellen vCenter entdecken

1. Wählen Sie in Ihrem aktuellen VMware vSphere-Client vCenter und dann entweder Hosts and Clusters oder VMs and Templates aus.
2. Wählen Sie eine Rechenzentrumsressource und dann Berechtigungen aus.
3. Wählen Sie den vCenter-Benutzer und dann das Symbol aus, um eine Benutzerrolle hinzuzufügen, zu bearbeiten oder zu entfernen.
4. Wählen Sie im Menü „Rolle“ die Option „Schreibgeschützt“.
5. Wählen Sie An Kinder weitergeben und dann OK.

Entdecken von Informationen über einen bestimmten ESX-Host und alle seine untergeordneten Objekte

1. Wählen Sie in Ihrem aktuellen VMware vSphere-Client vCenter und dann entweder Hosts and Clusters oder VMs and Templates aus.
2. Wählen Sie nacheinander Related Objects und Hosts aus.

3. Öffnen Sie das Kontextmenü (rechte Maustaste) für den Host-Namen und wählen Sie nacheinander All vCenter Actions und Add Permission aus.
4. Fügen Sie den Benutzer von vCenter unter Add Permission dem Host hinzu. Wählen Sie für Assigned Role die Option Read-only aus.
5. Wählen Sie Propagate to children und dann OK aus.

Um Daten über einen bestimmten ESX-Host oder eine untergeordnete VM zu ermitteln

1. Wählen Sie in Ihrem aktuellen VMware vSphere-Client vCenter und dann entweder Hosts and Clusters oder VMs and Templates aus.
2. Wählen Sie Related Objects aus.
3. Wählen Sie Hosts (mit Anzeige einer Liste der vCenter bekannten ESX-Hosts) oder Virtual Machines (mit Anzeige einer Liste aller VMs auf allen ESX-Hosts) aus.
4. Öffnen Sie das Kontextmenü (rechte Maustaste) für den Host- oder VM-Namen und wählen Sie nacheinander All vCenter Actions und Add Permission aus.
5. Fügen Sie den Benutzer von vCenter unter Add Permission dem Host oder der VM hinzu. Wählen Sie für Assigned Role die Option Read-only aus.
6. Wählen Sie OK.

> **Note**
>
> Wenn Sie „An Kinder weitergeben“ ausgewählt haben, können Sie trotzdem die Leseberechtigung für ESX-Hosts und VMs einzelncase-by-case entfernen. Diese Option hat keine Auswirkungen auf geerbte Berechtigungen für andere ESX-Hosts und VMs.

Modul zur Erfassung von Datenbank- und Analysedaten

In diesem Abschnitt wird die Einrichtung, Konfiguration und Verwendung eines Datenbank- und Analysedatenerfassungsmoduls beschrieben. Sie können dieses Datenerfassungsmodul verwenden, um eine Verbindung zu Ihrer Datenumgebung herzustellen und Metadaten und Leistungsmetriken aus Ihren lokalen Datenbanken und Analyseservern zu sammeln. Weitere Informationen zu den Metriken, die Sie mit diesem Modul erfassen können, finden Sie unterDaten, die vom Agentless Collector-Datenbank- und Analysedatenerfassungsmodul gesammelt wurden.

Im Allgemeinen führen Sie bei der Verwendung des Datenbank- und Analysedatenerfassungsmoduls die folgenden Schritte aus.

1. Führen Sie die erforderlichen Schritte aus, konfigurieren Sie Ihren IAM-Benutzer und erstellen Sie denAWS DMS Datensammelpunkt.
2. Konfigurieren Sie die Datenweiterleitung, um sicherzustellen, dass Ihr Datenerfassungsmodul die gesammelten Metadaten und Leistungskennzahlen an senden kannAWS.
3. Fügen Sie Ihre LDAP-Server hinzu und verwenden Sie sie, um Betriebssystemserver in Ihrer Datenumgebung zu finden. Alternativ können Sie Ihre Betriebssystemserver manuell hinzufügen oder den verwendenMDatensammlung ammlung ammlung ammlung ammlung ammlung ammlung.
4. Konfigurieren Sie die Verbindungsdaten zu Ihren Betriebssystemservern und verwenden Sie sie dann, um Datenbankserver zu finden.
5. Konfigurieren Sie die Verbindungsdaten zu Ihren Datenbank- und Analyseservern und führen Sie dann die Datenerfassung aus. Weitere Informationen finden Sie unter Erfassung von Datenbank- und Analysedaten.
6. Sehen Sie sich die gesammelten Daten in derAWS DMS Konsole an und verwenden Sie sie, um Zielempfehlungen für eine Migration auf die zu generierenAWS Cloud. Weitere Informationen finden Sie unter Erfassung von Datenbank- und Analysedaten.

Themen

- Unterstützte Betriebssystem-, Datenbank- und Analyseserver
- Erstellen Sie denAWS DMS Datensammler
- Datenweiterleitung konfigurieren
- Fügen Sie Ihre LDAP- und Betriebssystemserver hinzu
- Entdecken Sie Ihre Datenbankserver

Unterstützte Betriebssystem-, Datenbank- und Analyseserver

Das Datenbank- und Analysedatenerfassungsmodul im Agentless Collector unterstützt Microsoft Active Directory-LDAP-Server.

Dieses Datenerfassungsmodul unterstützt die folgenden Betriebssystemserver.

- Amazon Linux 2

- CentOS Linux Version 6 und höher
- Debian-Version 10 und höher
- Red Hat Enterprise Enterprise Linux Version 7 und höher
- SUSE Linux Linux Enterprise Server Version 12 und höher
- Ubuntu Version 16.01 und höher
- Windows Server 2012 und höher
- Windows XP und höher

Außerdem unterstützt das Datenbank- und Analysedatenerfassungsmodul die folgenden Datenbankserver.

- Microsoft SQL Server Version 2012 und bis 2019
- MySQL Version Version Version Version Version Version Version Version 5.6 und bis zu 8
- Oracle Version 11g Release 2 und bis zu 12c, 19c und 21c
- PostgreSQL Version Version 9.6 und bis Version Version Version Version Version Version Version Version Version Version Version Version

Erstellen Sie denAWS DMS Datensammler

Ihr Datenbank- und Analysedatenerfassungsmodul verwendet einenAWS DMS Datensammler, um mit derAWS DMS Konsole zu interagieren. Sie können die gesammelten Daten in derAWS DMS Konsole anzeigen oder sie verwenden, um dieAWS Ziel-Engine mit der richtigen Größe zu bestimmen. Weitere Informationen finden Sie unter Verwenden der Funktion „AWS DMSFleet Advisor Target Recommendations“.

Bevor Sie einenAWS DMS Datensammelpunkt erstellen, erstellen Sie eine IAM-Rolle, die IhrAWS DMS Datensammler für den Zugriff auf Ihren Amazon S3 S3-Bucket verwendet. Sie haben diesen Amazon S3 S3-Bucket erstellt, als Sie die Voraussetzungen in erfüllt habenVoraussetzungen für Agentless Collector.

So erstellen Sie eine IAM-Rolle für IhrenAWS DMS Datensammler zum Zugriff auf Amazon S3

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Roles und Create erstellen Sie Rolle erstellen.

3. Wählen Sie auf der Seite Vertrauenswürdige Entität auswählen für Vertrauenswürdigen Entitätstyp die Option AWSService aus. Wählen Sie für Anwendungsfälle für andereAWS Dienste DMS.
4. Markieren Sie das Kontrollkästchen DMS und wählen Sie Weiter.
5. Wählen Sie auf der Seite Berechtigungen hinzufügen die zuvor erstellte FleetAdvisorS3Policy aus. Wählen Sie Weiter.
6. Geben**`FleetAdvisorS3Role`** Sie auf der Seite Name, Überprüfung und Erstellen den Namen der Rolle ein und wählen Sie dann Rolle erstellen aus.
7. Öffnen Sie die von Ihnen erstellte Rolle und wählen Sie die Registerkarte Vertrauensbeziehungen. Wählen Sie Edit trust policy (Vertrauensrichtlinie bearbeiten) aus.
8. Fügen Sie auf der Seite „Vertrauensrichtlinie bearbeiten“ den folgenden JSON-Code in den Editor ein und ersetzen Sie den vorhandenen Code.

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

9. Wählen Sie Update policy.

Erstellen Sie nun einen Datensammler in derAWS DMS Konsole.

Um einenAWS DMS Datensammler zu erstellen

1. Melden Sie sich bei der anAWS Management Console und öffnen Sie dieAWS DMS Konsole unter https://console.aws.amazon.com/dms/v2/.

2. Wählen Sie dieAWS-Region, die Sie als Ihre Migration Hub Hub-Heimatregion festgelegt haben. Weitere Informationen finden Sie unter Melden Sie sich bei Migration Hub an und wählen Sie eine Heimatregion.
3. Wählen Sie im Navigationsbereich unter Discover die Option Datensammler aus. Die Seite Datensammler wird geöffnet.
4. Wählen Sie Datensammler erstellen. Die Seite Datensammler erstellen wird geöffnet.
5. Geben Sie im Abschnitt Allgemeine Konfiguration unter Name einen Namen Ihres Datensammlers ein.
6. Wählen Sie im Abschnitt Konnektivität die Option S3 durchsuchen aus. Wählen Sie den Amazon S3 S3-S3-Bucket, den Sie zuvor erstellt haben.
7. Wählen Sie als IAM-Rolle die Rolle aus`FleetAdvisorS3Role`, die Sie zuvor erstellt haben.
8. Wählen Sie Datensammler erstellen.

Datenweiterleitung konfigurieren

Nachdem Sie die erforderlichenAWS Ressourcen erstellt haben, konfigurieren Sie die Datenweiterleitung vom Datenbank- und Analysedatenerfassungsmodul an IhrenAWS DMS Collector.

So konfigurieren Sie die Datenweiterleitung

1. Öffnen Sie die Agentless Collector-Konsole. Weitere Informationen finden Sie unter Schritt 4: Greifen Sie auf die Collector-Konsole zu.
2. Wählen Sie „Datenbank und Analytics-Collector anzeigen“.
3. Wählen Sie auf der Dashboard-Seite im Abschnitt Datenweiterleitung die Option Datenweiterleitung konfigurieren aus.
4. Für die AWS-RegionIAM-Zugriffsschlüssel-ID und den geheimen IAM-Zugriffsschlüssel verwendet Ihr Agentless Collector die Werte, die Sie zuvor konfiguriert haben. Weitere Informationen erhalten Sie unter Melden Sie sich bei Migration Hub an und wählen Sie eine Heimatregion und Schritt 1: Erstellen Sie einen IAM-Benutzer.
5. Wählen Sie für Connected DMS-Datensammelpunkt Ihren Datensammelpunkt aus, den Sie in derAWS DMS Konsole erstellt haben.
6. Wählen Sie Speichern.

Nachdem Sie die Datenweiterleitung konfiguriert haben, überprüfen Sie den Abschnitt Datenweiterleitung auf der Dashboard-Seite. Stellen Sie

sicher, dass in Ihrem Datenbank- und Analysedatenerfassungsmodul

Conne

for Access to DMS und Access to S3 angezeigt werden.

Fügen Sie Ihre LDAP- und Betriebssystemserver hinzu

Das Datenbank- und Analysedatenerfassungsmodul verwendet LDAP in Microsoft Active Directory, um Informationen über das Betriebssystem, die Datenbank und die Analyseserver in Ihrem Netzwerk zu sammeln. Lightweight Directory Access Protocol (LDAP) ist ein offenes Standardanwendungsprotokoll. Sie können dieses Protokoll verwenden, um über Ihr IP-Netzwerk auf verteilte Verzeichnisinformationsdienste zuzugreifen und diese zu verwalten.

Sie können Ihrem Datenbank- und Analysedatenerfassungsmodul einen vorhandenen LDAP-Server hinzufügen, um Betriebssystemserver in Ihrem Netzwerk automatisch zu erkennen. Wenn Sie LDAP nicht verwenden, können Sie Betriebssystemserver manuell hinzufügen.

So fügen Sie Ihrem Datenbank- und Analysedatenerfassungsmodul einen LDAP-Server hinzu

1. Öffnen Sie die Agentless Collector-Konsole. Weitere Informationen finden Sie unter Schritt 4: Greifen Sie auf die Collector-Konsole zu.
2. Wählen Sie Datenbank und Analytics Collector anzeigen und wählen Sie dann im Navigationsbereich unter Discovery die Option LDAP-Server aus.
3. Wählen Sie LDAP-Server hinzufügen. Die Seite LDAP-Server hinzufügen wird geöffnet.
4. Geben Sie als Hostname den Hostnamen Ihres LDAP-Servers ein.
5. Geben Sie für Port die Portnummer ein, die für LDAP-Anforderungen verwendet wird.
6. Geben Sie unter Benutzername den Benutzernamen ein, den Sie für die Verbindung zu Ihrem LDAP-Server verwenden.
7. Für Passwort geben Sie das Passwort ein, das Sie für die Verbindung zu Ihrem LDAP-Server verwenden.
8. (Optional) Wählen Sie Verbindung überprüfen, um sicherzustellen, dass Sie Ihre LDAP-Serveranmeldeinformationen korrekt hinzugefügt haben. Alternativ können Sie Ihre Anmeldeinformationen für die LDAP-Serververbindung später anhand der Liste auf der LDAP-Serverseite überprüfen.
9. Wählen Sie LDAP-Server hinzufügen.

10. Wählen Sie auf der Seite LDAP-Server Ihren LDAP-Server aus der Liste aus und wählen Sie Discover OS-Server aus.

> **Important**
>
> Für die Betriebssystemerkennung benötigt das Datenerfassungsmodul Anmeldeinformationen für den Domainserver, um Anfragen mithilfe des LDAP-Protokolls auszuführen.

Das Modul zur Erfassung von Datenbank- und Analysedaten stellt eine Verbindung zu Ihrem LDAP-Server her und erkennt Ihre Betriebssystemserver. Nachdem das Datenerfassungsmodul die Betriebssystemserversuche abgeschlossen hat, können Sie die Liste der erkannten Betriebssystemserver einsehen, indem Sie „Betriebssystemserver anzeigen“ wählen.

Sie können Ihre Betriebssystem-Server auch manuell hinzufügen oder die Serverliste mit einer CSV-Datei herunterladen. Sie können auch das Datenerfassungsmodul von VMware vCenter Agentless Collector verwenden, um Ihre Betriebssystemserver zu ermitteln. Weitere Informationen finden Sie unter MDatensammlung ammlung ammlung ammlung ammlung ammlung ammlung.

So fügen Sie Ihrem Datenbank- und Analysedatenerfassungsmodul einen Betriebssystemserver hinzu

1. Wählen Sie auf der Seite Database and Analytics Collector im Navigationsbereich unter Discovery die Option Betriebssystemserver aus.
2. Wählen Sie Betriebssystemserver hinzufügen. Die Seite Betriebssystemserver hinzufügen wird geöffnet.
3. Geben Sie Ihre Anmeldeinformationen für den Betriebssystemserver ein.

    a. Wählen Sie als Betriebssystemtyp das Betriebssystem Ihres Servers aus.

    b. Geben Sie für Hostname/IP den Hostnamen oder die IP-Adresse Ihres Betriebssystemservers ein.

    c. Geben Sie für Port die Portnummer ein, die für Remote-Abfragen verwendet wird.

    d. Wählen Sie als Authentifizierungstyp den Authentifizierungstyp aus, den Ihr Betriebssystemserver verwendet.

    e. Geben Sie unter Benutzername den Benutzernamen ein, den Sie für die Verbindung zu Ihrem Betriebssystem-Server verwenden.

f. Für Passwort geben Sie das Passwort ein, das Sie für die Verbindung zu Ihrem Betriebssystem-Server verwenden.

g. Wählen Sie Überprüfen, um sicherzustellen, dass Sie Ihre Betriebssystemserver-Anmeldeinformationen korrekt hinzugefügt haben.

4. (Optional) Fügen Sie mehrere Betriebssystemserver aus einer CSV-Datei hinzu.

   a. Wählen Sie Massenimport von Betriebssystemservern aus CSV.

   b. Wählen Sie Vorlage herunterladen, um eine CSV-Datei zu speichern, die eine Vorlage enthält, die Sie anpassen können.

   c. Geben Sie die Verbindungsdaten für Ihre Betriebssystemserver gemäß der Vorlage in die Datei ein. Das folgende Beispiel zeigt, wie Sie Anmeldeinformationen zu Betriebssystem-Server-Verbindung in einer CSV-Datei in einer CSV-Datei herunterladen können.

```
OS type,Hostname/IP,Port,Authentication type,Username,Password
Linux,192.0.2.0,22,Key-based authentication,USER-EXAMPLE,ANPAJ2UCCR6DPCEXAMPLE
Windows,203.0.113.0,,NTLM,USER2-EXAMPLE,AKIAIOSFODNN7EXAMPLE
```

   Speichern Sie Ihre CSV-Datei, nachdem Sie Anmeldeinformationen für alle Ihre Betriebssystemserver hinzugefügt haben.

   d. Wähle „Durchsuchen“ und wähle dann deine CSV-Datei aus.

5. Wählen Sie Betriebssystemserver hinzufügen.

6. Nachdem Sie Anmeldeinformationen für alle Betriebssystemserver hinzugefügt haben, wählen Sie Ihre Betriebssystemserver aus und wählen Sie Discover database servers.

Entdecken Sie Ihre Datenbankserver

Erstellen Sie für die Datenbankerkennung Benutzer für Ihre Quelldatenbanken mit den für das Datenerfassungsmodul erforderlichen Mindestberechtigungen. Weitere Informationen finden Sie im Benutzerhandbuch unter Datenbankbenutzer fürAWS DMS Fleet Advisor erstellen.AWS DMS

Um die Datenbanken zu ermitteln, die auf den zuvor hinzugefügten Betriebssystemservern laufen, benötigt das Datenerfassungsmodul Zugriff auf das Betriebssystem und die Datenbankserver. Stellen Sie sicher, dass Ihre Datenbank mit dem Port zugänglich ist, den Sie in den Verbindungseinstellungen angegeben haben. Als Nächstes schalten Sie die Remote-Authentifizierung auf Ihrem Datenbankserver ein. Geben Sie Ihrem Datenerfassungsmodul zusätzlich die folgenden Berechtigungen.

So finden Sie Datenbankserver in Windows

1. Geben Sie Anmeldeinformationen mit Zuschüssen an, um Windows Management Instrumentation (WMI) und WMI Query Language (WQL) -Abfragen auszuführen und die Registrierung zu lesen.
2. Fügen Sie den Windows-Benutzer, den Sie in den Anmeldeinformationen für die Betriebssystemserververbindung angegeben haben, den folgenden Gruppen hinzu: Verteilte COM-Benutzer, Leistungsprotokollbenutzer, Systemmonitorbenutzer und Ereignisprotokollleser. Verwenden Sie dazu das folgende Codebeispiel.

   ```
   net localgroup "Distributed COM Users" username /ADD
   net localgroup "Performance Log Users" username /ADD
   net localgroup "Performance Monitor Users" username /ADD
   net localgroup "Event Log Readers" username /ADD
   ```

   Ersetzen Sie*username* im vorherigen Beispiel den Namen des Windows-Benutzers, den Sie in den Anmeldeinformationen zum Betriebssystem-Server in den Anmeldeinformationen für den Betriebssystem-Server angegeben haben.
3. Gewähren Sie dem Windows-Benutzer, den Sie in den Anmeldeinformationen für die Betriebssystemserververbindung angegeben haben, die erforderlichen Berechtigungen.

   - Wählen Sie für die Eigenschaften der Windows-Verwaltung und Instrumentierung die Option Lokaler Start und Remoteaktivierung aus.
   - Wählen Sie für die WMI-Steuerung die Berechtigungen Execute Methods, Enable Account, Remote Enable und Read Security für die`WMI` Namespaces`CIMV2`,`DEFAULT`,`StandartCimv2`, und aus.
   - Führen Sie das WMI-Plug-In aus`winrm configsddl default` und wählen Sie dann Lesen und Ausführen.
4. Konfigurieren Sie Ihren Windows-Host mithilfe des folgenden Codebeispiels.

   ```
   netsh advfirewall firewall add rule name="Open Ports for WinRM incoming traffic"
    dir=in action=allow protocol=TCP localport=5985, 5986 # Opens ports for WinRM
   netsh advfirewall firewall add rule name="All ICMP V4" protocol=icmpv4:any,any
    dir=in action=allow # Allows ICPM traffic

   Enable-PSRemoting -Force # Enables WinRM
   Set-Service WinRM -StartMode Automatic # Allows WinRM service to run on host
    startup
   ```

```
Set-Item WSMan:\localhost\Client\TrustedHosts -Value {IP} -Force # Sets the
 specific IP from which the access to WinRM is allowed

winrm set winrm/config/service '@{Negotiation="true"}' # Allow Negosiate auth usage
winrm set winrm/config/service '@{AllowUnencrypted="true"}' # Allow unencrypted
 connection
```

Um Datenbankserver in Linux zu entdecken

1. Gewähren Sie Sudo Zugriff auf die`netstat` Befehle`ss` und.

   Das folgende Codebeispiel gewährt sudo Zugriff auf die`netstat` Befehle`ss` und.

   ```
   sudo bash -c "cat << EOF >> /etc/sudoers.d/username
   username ALL=(ALL) NOPASSWD: /usr/bin/ss
   username ALL=(ALL) NOPASSWD: /usr/bin/netstat
   EOF"
   ```

   Ersetzen Sie*username* im vorherigen Beispiel den Namen des Linux-Benutzers, den Sie in den Anmeldeinformationen für den Linux-Benutzer den Linux-Benutzer in den Anmeldeinformationen für den Linux-Benutzer verwenden.

   Im vorherigen Beispiel wird der`/usr/bin/` Pfad zu den`netstat` Befehlen`ss` und verwendet. Dieser Pfad kann in Ihrer Umgebung anders sein. Führen Sie die AND-Befehle aus, um den`ss` Pfad zu den`netstat`which netstat Befehlen`which ss` und zu ermitteln.
2. Konfigurieren Sie Ihre Linux-Server so, dass sie die Ausführung von Remote-SSH-Skripten und den ICMP-Verkehr (Internet Control Message Protocol) zulassen.

Um mit der Suche nach Ihren Datenbankservern zu beginnen

1. Wählen Sie auf der Seite Database and Analytics Collector im Navigationsbereich unter Discovery die Option Betriebssystemserver aus.
2. Wählen Sie die Betriebssystemserver aus, zu denen Ihre Datenbank- und Analyseserver gehören, und wählen Sie dann im Menü Aktionen die Option Verbindung überprüfen aus.
3. Bearbeiten Sie für Server mit dem Konnektivitätsstatus Fehlgeschlagen die Verbindungsanmeldeinformationen.

a. Wählen Sie einen einzelnen Server oder mehrere Server aus, wenn sie identische Anmeldeinformationen haben, und wählen Sie dann im Menü Aktionen die Option Bearbeiten aus. Die Seite „Betriebssystemserver bearbeiten“ wird geöffnet.

b. Geben Sie für Port die Portnummer ein, die für Remote-Abfragen verwendet wird.

c. Wählen Sie als Authentifizierungstyp den Authentifizierungstyp aus, den Ihr Betriebssystemserver verwendet.

d. Geben Sie unter Benutzername den Benutzernamen ein, den Sie für die Verbindung zu Ihrem Betriebssystem-Server verwenden.

e. Für Passwort geben Sie das Passwort ein, das Sie für die Verbindung zu Ihrem Betriebssystem-Server verwenden.

f. Wählen Sie Verbindung überprüfen, um sicherzustellen, dass Sie Ihre Betriebssystemserver-Anmeldeinformationen korrekt aktualisiert haben. Wählen Sie anschließend Speichern.

4. Nachdem Sie die Anmeldeinformationen für alle Betriebssystemserver aktualisiert haben, wählen Sie Ihre Betriebssystemserver aus und wählen Sie Discover database servers.

Das Datenbank- und Analysedatenerfassungsmodul stellt eine Verbindung zu Ihren Betriebssystemservern her und ermittelt die unterstützten Datenbank- und Analyseserver. Nachdem das Datenerfassungsmodul die Erkennung abgeschlossen hat, können Sie die Liste der erkannten Datenbank- und Analyseserver einsehen, indem Sie Datenbankserver anzeigen wählen.

Alternativ können Sie Ihre Datenbank- und Analyseserver manuell zum Inventar hinzufügen. Sie können auch die Serverliste aus einer CSV-Datei importieren. Sie können diesen Schritt überspringen, wenn Sie bereits alle Datenbank- und Analysesver zum Bestand haben.

So fügen Sie manuell einen Datenbank- oder Analyseserver hinzu

1. Wählen Sie auf der Seite Datenbank- und Analytics-Collector im Navigationsbereich die Option Datenerfassung aus.
2. Wählen Sie Datenbankserver hinzufügen. Die Seite Datenbankserver hinzufügen wird geöffnet.
3. Geben Sie Ihre Datenbankserver-Anmeldedaten ein.

a. Wählen Sie für Datenbank-Engine die Datenbank-Engine Ihres Servers aus. Weitere Informationen finden Sie unter Unterstützte Betriebssystem-, Datenbank- und Analyseserver.

b. Geben Sie für Hostname/IP den Hostnamen oder die IP-Adresse Ihrer Datenbank oder Ihres Analyseservers ein.

c. Geben Sie für Port den Port ein, auf dem Ihr Server läuft.

d. Wählen Sie als Authentifizierungstyp den Authentifizierungstyp aus, den Ihre Datenbank oder Ihr Analyseserver verwendet.

e. Geben Sie unter Benutzername den Benutzernamen ein, den Sie für die Verbindung zu Ihrem Server verwenden.

f. Für Passwort geben Sie das Passwort ein, das Sie für die Verbindung zu Ihrem Server verwenden.

g. Wählen Sie Überprüfen, um sicherzustellen, dass Sie Ihre Datenbank- oder Analytics-Server-Anmeldeinformationen korrekt hinzugefügt haben.

4. (Optional) Fügen Sie mehrere Server aus einer CSV-Datei hinzu.

a. Wählen Sie Massenimport von Datenbankservern aus CSV.

b. Wählen Sie Vorlage herunterladen, um eine CSV-Datei zu speichern, die eine Vorlage enthält, die Sie anpassen können.

c. Geben Sie die Verbindungsdaten für Ihre Datenbank und Ihre Analyseserver gemäß der Vorlage in die Datei ein. Das folgende Beispiel zeigt, wie Sie Datenbank- oder Analytic-Server-Verbindungsanmeldeinformationen in einer CSV-Datei in einer CSV-Datei herunterladen können.

```
Database engine,Hostname/IP,Port,Authentication type,Username,Password,Oracle
 service name,Database,Allow public key retrieval,Use SSL,Trust server
 certificate
Oracle,192.0.2.1,1521,Login/Password authentication,USER-
EXAMPLE,AKIAI44QH8DHBEXAMPLE,orcl,,,,
PostgreSQL,198.51.100.1,1533,Login/Password authentication,USER2-
EXAMPLE,bPxRfiCYEXAMPLE,,postgre,,TRUE,
MSSQL,203.0.113.1,1433,Login/Password authentication,USER3-
EXAMPLE,h3yCo8nvbEXAMPLE,,,,,TRUE
MySQL,2001:db8:4006:812:ffff:200e,8080,Login/Password authentication,USER4-
EXAMPLE,APKAEIVFHP46CEXAMPLE,,mysql,TRUE,TRUE,
```

Speichern Sie Ihre CSV-Datei, nachdem Sie Anmeldeinformationen für all Ihre Datenbank- und Analyseserver hinzugefügt haben.

d. Wähle „Durchsuchen“ und wähle dann deine CSV-Datei aus.

5. Wählen Sie Datenbankserver hinzufügen.

6. Nachdem Sie Anmeldeinformationen für alle Betriebssystemserver hinzugefügt haben, wählen Sie Ihre Betriebssystemserver aus und wählen Sie Discover database servers.

Nachdem Sie alle Ihre Datenbank- und Analyseserver zum Datenerfassungsmodul hinzugefügt haben, fügen Sie sie dem Inventar hinzu. Das Datenbank- und Analysedatenerfassungsmodul kann vom Inventar aus eine Verbindung zu den Servern herstellen und erfasst Metadaten und Leistungskennzahlen.

Um Ihre Datenbank- und Analyseserver zum Inventar hinzuzufügen

1. Wählen Sie auf der Seite Database and Analytics Collector im Navigationsbereich unter Discovery die Option Datenbankserver aus.
2. Wählen Sie die Datenbank- und Analyseserver aus, für die Sie Metadaten und Leistungsmetriken sammeln möchten.
3. Wählen Sie Zum Inventar hinzufügen.

Nachdem Sie alle Datenbank- und Analyseserver zu Ihrem Inventar hinzugefügt haben, können Sie mit der Erfassung von Metadaten und Leistungskennzahlen beginnen. Weitere Informationen finden Sie unter Erfassung von Datenbank- und Analysedaten.

Schritt 7: Gesammelte Daten anzeigen

Sie können die Daten, die Ihr Application Discovery Service Agentless Collector (Agentless Collector) gesammelt hat, in der Migration Hub Hub-Konsole anzeigen. Sie können die gesammelten Metriken für Datenbank- und Analyseserver in der AWS DMS Konsole einsehen.

So zeigen Sie die vom Datenerfassungsmodul VMware vCenter Agentless Collector erkannten Daten an

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Migration Hub Hub-Konsole unter https://console.aws.amazon.com/migrationhub/. Für diese Aufgabe empfehlen wir, dass Sie ein anderes IAM-Benutzerkonto als den IAM-Benutzer verwenden, den Sie für die Einrichtung und den Zugriff auf Agentless Collector erstellt haben.
2. Wählen Sie im Navigationsbereich der Migration Hub Hub-Konsole unter Discover die Option Servers aus.

3. Um Details zu einem Server anzuzeigen, wählen Sie den Hostnamen des Servers aus der Spalte Serverinformationen aus. Auf der Detailseite des Servers werden Informationen über den Server angezeigt, wie Hostname, IP-Adresse, Leistungsmetriken usw.

Um die Daten anzuzeigen, die vom Modul zur Erfassung von Datenbank- und Analysedaten ermittelt wurden

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS DMS Konsole unter https://console.aws.amazon.com/dms/v2/.
2. Wählen Sie unter Entdecken die Option Inventar aus. Die Seite Inventar wird geöffnet.
3. Wählen Sie Inventare analysieren, um Eigenschaften des Datenbankschemas wie Ähnlichkeit und Komplexität zu ermitteln.
4. Wählen Sie die Registerkarte Schemas, um die Ergebnisse der Analyse zu sehen.

Sie können die AWS DMS Konsole verwenden, um doppelte Schemas zu identifizieren, die Komplexität der Migration zu bestimmen und die Inventarinformationen für die future Analyse zu exportieren. Weitere Informationen finden Sie unter Verwenden von Inventaren für Analysen in AWS DMS Fleet Advisor.

Von Agentless Collector gesammelte Daten

Sie richten das Datenerfassungsmodul Application Discovery Service Agentless Collector (Agentless Collector) ein, um Inventar-, Profil- und Nutzungsdaten von Ihren Servern zu sammeln.

Agentless Collector unterstützt derzeit die Datenerfassung von VMware-VMs sowie von Datenbank- und Analyseservern. Zukünftige Module werden die Erfassung von zusätzlichen Virtualisierungsplattformen sowie die Erfassung auf Betriebssystemebene unterstützen. Informationen zum Einrichten der Datenerfassung finden Sie unterSchritt 6: Richten Sie die Agentless Collector-Datenerfassungsmodule ein.

In den folgenden Themen werden die Daten beschrieben, die von den Datenerfassungsmodulen Application Discovery Service Agentless Collector (Agentless Collector) gesammelt werden.

Themen

- Vom Agentless Collector VMware vCenter-Datenerfassungsmodul erfasste Daten
- Daten, die vom Agentless Collector-Datenbank- und Analysedatenerfassungsmodul gesammelt wurden

Vom Agentless Collector VMware vCenter-Datenerfassungsmodul erfasste Daten

Die folgenden Informationen beschreiben die Daten, die vom VMware vCenter-Datenerfassungsmodul Application Discovery Service Agentless Collector (Agentless Collector) gesammelt werden. Informationen zum Einrichten der Datenerfassung finden Sie unter. So richten Sie das Agentless Collector-Datenerfassungsmodul für VMware vCenter ein

Tabellenlegende für Agentless Collector Die von VMware vCenter gesammelten Daten:

- Gesammelte Daten sind Messungen in Kilobyte (KB), sofern nicht anders angegeben.
- Entsprechende Daten in der Migration Hub Hub-Konsole werden in Megabyte (MB) gemeldet.
- Datenfelder, die mit einem Sternchen (*) gekennzeichnet sind, sind nur in den CSV-Dateien verfügbar, die mit der API-Exportfunktion des Application Discovery Service erstellt wurden.

  Der Agentless Collector unterstützt den Datenexport über die AWS CLI. Um gesammelte Daten mit der AWS CLI zu exportieren, folgen Sie den Anweisungen, die unter Exportieren von Systemleistungsdaten für alle Server auf der Seite Gesammelte Daten exportieren im Application Discovery Service Service-Benutzerhandbuch beschrieben sind.
- Der Abrufzeitraum ist in Intervallen von ca. 60 Minuten.
- Datenfelder mit einem doppelten Sternchen (**) geben derzeit den Wert Null zurück.

Datenfeld	Beschreibung
applicationConfigurationId*	ID der Migrationsanwendung, unter der die VM gruppiert ist.
avgCpuUsagePct	Durchschnittlicher Prozentsatz der CPU-Auslastung während des Abfragezeitraums.
avgDiskBytesReadPerSecond	Durchschnittliche Anzahl von Byte, die während des Abfragezeitraums von der Festplatte gelesen wurden.
avgDiskBytesWrittenPerSecond	Durchschnittliche Anzahl von Byte, die während des Abfragezeitraums auf die Festplatte geschrieben wurden.

Datenfeld	Beschreibung
avgDiskReadOpsPerSecond**	Durchschnittliche Anzahl von I/O-Lesev orgängen pro Sekunde Null.
avgDiskWriteOpsPerSecond**	Durchschnittliche Anzahl von I/O-Schre ibvorgängen pro Sekunde.
avgFreeRAM	Durchschnittlicher freier Arbeitsspeicher, ausgedrückt in MB.
avgNetworkBytesReadPerSecond	Durchschnittlicher Durchsatz der pro Sekunde gelesenen Byte.
avgNetworkBytesWrittenPerSecond	Durchschnittlicher Durchsatz an geschriebenen Byte pro Sekunde.
Computer-Hersteller	Vom ESXi-Host gemeldeter Anbieter.
Computermodell	Vom ESXi-Host gemeldetes Computermodell.
configId	ID, die der erkannten VM vom Application Discovery Service zugewiesen wurde.
configType	Art der erkannten Ressource.
connectorId	ID der virtuellen Appliance.
cpuType	vCPU für eine VM, aktuelles Modell für einen Host.
datacenterId	ID des vCenter.
hostId*	ID des VM-Hosts.
hostName	Name des Hosts, auf dem die Virtualis ierungssoftware ausgeführt wird.
hypervisor	Typ des Hypervisors.
id	ID des Servers.

Datenfeld	Beschreibung
lastModifiedTimeStempel *	Spätestes Datum und Uhrzeit der Datenerfassung vor dem Datenexport.
macAddress	MAC-Adresse der VM.
manufacturer	Hersteller der Virtualisierungssoftware.
maxCpuUsagePct	Maximaler Prozentsatz der CPU-Auslastung während des Abfragezeitraums.
maxDiskBytesReadPerSecond	Max. Anzahl der während des Abfragezeitraums von der Festplatte gelesenen Byte.
maxDiskBytesWrittenPerSecond	Max. Anzahl von Byte, die während des Abfragezeitraums auf die Festplatte geschrieben wurden.
maxDiskReadOpsPerSecond**	Max. Anzahl von I/O-Lesevorgängen pro Sekunde.
maxDiskWriteOpsPerSecond**	Max. Anzahl von I/O-Schreibvorgängen pro Sekunde.
maxNetworkBytesReadPerSecond	Max. Durchsatzmenge der pro Sekunde gelesenen Byte.
maxNetworkBytesWrittenPerSecond	Max. Durchsatzmenge der pro Sekunde geschriebenen Byte.
memoryReservation*	Grenzwert, um eine Überbelegung des Arbeitsspeichers auf der VM zu vermeiden.
moRefId	Eindeutige Referenz-ID für verwaltete vCenter-Objekte.
name*	Name der VM oder des Netzwerks (vom Benutzer angegeben).

Datenfeld	Beschreibung
numCores	Anzahl der CPU-Kerne, die der VM zugewiesen sind.
numCpus	Anzahl der CPU-Sockel auf dem ESXi-Host.
numDisks**	Anzahl der Festplatten auf der VM.
numNetworkCards**	Anzahl der Netzwerkkarten auf der VM.
osName	Name des Betriebssystems auf der VM.
osVersion	Betriebssystemversion auf der VM.
portGroupId*	ID der Gruppe von Mitgliedsports des VLAN.
portGroupName*	Name der Gruppe von Mitgliedsports des VLAN.
powerState*	Status der Stromversorgung.
serverId	Der Application Discovery Service hat der erkannten VM eine ID zugewiesen.
smBiosId*	ID/Version des Systemmanagement-BIOS.
state*	Status der virtuellen Appliance.
toolsStatus	Betriebszustand der VMware-Tools
totalDiskFreeGröße	Freier Festplattenspeicher, ausgedrückt in MB. Verfügbar für vCenter Server 7.0 und spätere Versionen.
totalDiskSize	Gesamtkapazität der Festplatte, ausgedrückt in MB.
totalRAM	Gesamtmenge des auf der virtuellen Maschine verfügbaren Arbeitsspeichers in MB.

Datenfeld	Beschreibung
Typ	Art des Hosts.
vCenterId	Eindeutige ID-Nummer einer VM.
vCenterName*	Name des vCenter-Hosts.
virtualSwitchName*	Name des virtuellen Switches.
vmFolderPath	Verzeichnispfad der VM-Dateien.
vmName	Name der virtuellen Maschine.

Daten, die vom Agentless Collector-Datenbank- und Analysedatenerfassungsmodul gesammelt wurden

Das Datenbank- und Analysedatenerfassungsmodul Application Discovery Service Agentless Collector (Agentless Collector) erfasst die folgenden Metriken aus Ihrer Datenumgebung. Weitere Informationen zum Einrichten einer Datenerfassung finden Sie unterModul zur Erfassung von Datenbank- und Analysedaten.

Wenn Sie das Datenbank- und Analysedatenerfassungsmodul verwenden, um Metadaten und Datenbankkapazität zu sammeln, erfasst es die folgenden Metriken.

- Verfügbarer Speicher auf Ihren Betriebssystemservern
- Verfügbarer Speicher auf Ihren Betriebssystemservern
- Datenbankversion und Ausgabe
- Anzahl der CPUs auf Ihren Betriebssystemservern
- Anzahl der Schemata
- Anzahl der gespeicherten Prozeduren
- Anzahl der Tabellen
- Anzahl der Auslöser
- Anzahl der Ansichten
- Schemastruktur

Nachdem Sie die Schemaanalyse in derAWS DMS Konsole gestartet haben, analysiert Ihr Datenerfassungsmodul die folgenden Metriken und zeigt sie an.

- Termine für die Datenbankunterstützung
- Anzahl der Codezeilen
- Komplexität des Schemas
- Ähnlichkeit der Schemas

Wenn Sie das Datenbank- und Analysedatenerfassungsmodul verwenden, um Metadaten, Datenbankkapazität und Ressourcenauslastung zu sammeln, erfasst es die folgenden Metriken.

- I/O-Durchsatz auf Ihren Datenbankservern
- Anzahl der Eingabe-/Ausbevorgänge pro Sekunde (IOPS) auf Ihren Daten-/Ausgabevorgänge pro Sekunde
- Anzahl der CPUs, die Ihre Betriebssystemserver verwenden
- Speichernutzung auf Ihren Betriebssystemservern
- Speichernutzung auf Ihren Betriebssystemservern

Sie können das Datenbank- und Analysedatenerfassungsmodul verwenden, um Metadaten, Kapazitäts- und Nutzungsmetriken aus Ihren Oracle- und SQL Server-Datenbanken zu sammeln. Gleichzeitig kann das Datenerfassungsmodul für PostgreSQL- und MySQL-Datenbanken nur Metadaten sammeln.

Verwenden der Agentless Collector-Konsole

In diesem Abschnitt wird beschrieben, wie Sie die Application Discovery Service Agentless Collector Konsole verwenden.

Themen

Das Agentless Collector-Dashboard

Auf der Dashboardseite Application Discovery Service Agentless Collector (Agentless Collector) können Sie den Status des Collectors sehen und eine Methode der Datenerfassung auswählen, wie in den folgenden Themen beschrieben.

Themen

Sammlerstatus

Der Collector-Status gibt Ihnen Statusinformationen über den Collector. Der Collector-Name, der Status der Verbindung des Collectors zu AWS, die Migration Hub Hub-Heimatregion und die Version.

Wenn SieAWS Verbindungsprobleme haben, müssen Sie möglicherweise die Konfigurationseinstellungen für Agentless Collister bearbeiten.

Um die Collector-Konfigurationseinstellungen zu bearbeiten, wählen Sie Collector-Einstellungen bearbeiten und folgen Sie den Anweisungen unterAgentless Collector-Einstellungen bearbeiten.

Datenerfassung

Unter Datenerfassung können Sie eine Datenerfassungsmethode wählen. Application Discovery Service Agentless Collector (Agentless Collector) unterstützt derzeit die Datenerfassung von VMware-VMs sowie von Datenbank- und Analyseservern. Zukünftige Module werden die Erfassung von zusätzlichen Virtualisierungsplattformen sowie die Erfassung auf Betriebssystemebene unterstützen.

Themen

VMware vCenter Datenauflister

Um Serverinventar-, Profil- und Nutzungsdaten von Ihren VMware-VMs zu sammeln, richten Sie Verbindungen zu Ihren vCenter-Servern ein. Um die Verbindungen einzurichten, wählen Sie im

Abschnitt VMware vCenter die Option Einrichten und folgen Sie den Anweisungen unterSchritt 6: Richten Sie die Agentless Collector-Datenerfassungsmodule ein.

Nachdem Sie die vCenter-Datenerfassung eingerichtet haben, können Sie vom Dashboard aus Folgendes ausführen:

- Datenauflister
- Starten der Datensammlung
- Beenden der Datensammlung

> **Note**
>
> Nachdem Sie die vCenter-Datenerfassung eingerichtet haben, wird auf der Dashboard-Seite die Schaltfläche Einrichten im Abschnitt VMware vCenter durch Statusinformationen zur Datenerfassung, die Schaltfläche Datenerfassung beenden und die Schaltfläche Anzeigen und Bearbeiten ersetzt.

Erfassung von Datenbank- und Analysedaten

Sie können Ihr Datenbank- und Analysedatenerfassungsmodul in den folgenden zwei Modi ausführen.

Metadaten und Datenbankkapazität

Das Datenerfassungsmodul sammelt Informationen wie Schemas, Versionen, Editionen, CPU-, Arbeitsspeicher- und Festplattenkapazität von Ihren Datenbank- und Analyseservern. Sie können diese gesammelten Informationen verwenden, um Zielempfehlungen in derAWS DMS Konsole zu berechnen. Wenn Ihre Quelldatenbank über- oder unterprovisioniert ist, werden die Zielempfehlungen ebenfalls über- oder unterprovisioniert sein.

Das ist der Standardmodus.

Metadaten, Datenbankkapazität und Ressourcenauslastung

Zusätzlich zu den Metadaten und Informationen zur Datenbankkapazität erfasst das Datenerfassungsmodul die tatsächliche Auslastung der CPU-, Speicher- und Festplattenkapazität für die Datenbanken und Analyseserver. Dieser Modus bietet genauere Zielempfehlungen als der Standardmodus, da die Empfehlungen auf den tatsächlichen Datenbank-Workloads basieren. In diesem Modus sammelt das Datenerfassungsmodul jede Minute Leistungskennzahlen.

Um mit der Erfassung von Metadaten und Leistungsmetriken von Ihren Datenbank- und Analyseservern zu beginnen

1. Wählen Sie auf der Seite Datenbank- und Analytics-Collector im Navigationsbereich die Option Datenerfassung aus.
2. Wählen Sie aus der Liste Datenbankinventar die Datenbank- und Analyseserver aus, für die Sie Metadaten und Leistungsmetriken sammeln möchten.
3. Wählen Sie Datenerfassung ausführen. Das Dialogfeld Datenerfassungstyp wird geöffnet.
4. Wählen Sie aus, wie Daten für die Analyse gesammelt werden sollen.

   Wenn Sie die Option Metadaten, Datenbankkapazität und Ressourcenauslastung wählen, legen Sie den Zeitraum der Datenerfassung fest. Sie können Daten in den nächsten 7 Tagen sammeln oder den benutzerdefinierten Zeitraum von 1—60 Tagen festlegen.
5. Wählen Sie Datenerfassung ausführen. Die Seite Datenerfassung wird geöffnet.
6. Wählen Sie die Registerkarte „Zustand der Sammlung“, um den Status der Datenerfassung zu sehen.

Nach Abschluss der Datenerfassung lädt Ihr Datenerfassungsmodul die gesammelten Daten in Ihren Amazon S3 S3-Bucket hoch. Anschließend können Sie diese gesammelten Daten wie unter beschrieben einsehenSchritt 7: Gesammelte Daten anzeigen.

Agentless Collector-Einstellungen bearbeiten

Sie haben den Collector konfiguriert, als Sie Application Discovery Service Agentless Collector (Agentless Collector) zum ersten Mal eingerichtet haben, wie unter beschriebenSchritt 5: Agentless Collector konfigurieren. Im folgenden Verfahren wird beschrieben, wie Sie die Agentless Collector bearbeiten.

Um die Collector-Konfigurationseinstellungen zu bearbeiten

- Wählen Sie im Agentless Collector-Dashboard die Schaltfläche Collector-Einstellungen bearbeiten.

  Gehen Sie auf der Seite Collector-Einstellungen bearbeiten wie folgt vor:

  a. Geben Sie für Collister Name einen Namen zum Identifizieren des Datenauflister. Der Name kann Leerzeichen, aber keine Sonderzeichen enthalten.

b. Geben Sie unter AWSZielkonto für Ermittlungsdaten denAWS Zugriffsschlüssel und den geheimen Schlüssel für dasAWS Konto ein, das als Zielkonto für den Empfang der vom Collector erkannten Daten angegeben werden soll. Hinweise zu den Anforderungen für den IAM-Benutzer finden Sie unterSchritt 1: Erstellen Sie einen IAM-Benutzer für Agentless Collector.

   i. Geben Sie als AWSZugriffsschlüssel den Zugriffsschlüssel desAWS IAM-Kontos ein, das Sie als Zielkonto angeben.

   ii. Geben Sie als AWSSecret-Key den geheimen Schlüssel desAWS IAM-Konto-Benutzers ein, den Sie als Zielkonto angeben.

c. Ändern Sie unter Agentless Collector password das Passwort, das für die Authentifizierung des Zugriffs auf den Agentless Collector verwendet werden soll.

   i. Geben Sie als Agentless Collector-Passwort ein Passwort ein, mit dem der Zugriff auf den Agentless Collector authentifiziert werden soll.

   ii. Um das Agentless Collector-Passwort erneut einzugeben, geben Sie das Passwort zur Bestätigung erneut ein.

d. Wählen Sie Konfigurationen speichern.

Als Nächstes wirst du sehenDas Agentless Collector-Dashboard.

Bearbeiten der VMware vCenter-Anmeldeinformationen

Um Serverinventar-, Profil- und Nutzungsdaten von Ihren VMware-VMs zu sammeln, richten Sie Verbindungen zu Ihren vCenter-Servern ein. Weitere Informationen zum Einrichten von VMware vCenter-Verbindungen finden Sie unterSchritt 6: Richten Sie die Agentless Collector-Datenerfassungsmodule ein.

In diesem Abschnitt wird beschrieben, wie Sie die vCenter-Anmeldeinformationen bearbeiten.

> **Note**
>
> Bevor Sie die vCenter-Anmeldeinformationen bearbeiten, stellen Sie sicher, dass Sie vCenter-Anmeldeinformationen mit den für die Systemgruppe festgelegten Lese- und Anzeigeberechtigungen angeben können.

So bearbeiten Sie die VMware vCenter-Anmeldeinformationen

Wählen Sie auf derenden Datensammlung ammlung ammlung ammlung ammlung ammlung ammlung Seite vCenter-Server bearbeiten aus.

- Gehen Sie auf der Seite „vCenter bearbeiten“ wie folgt vor:

  a. Unter vCenter-Anmeldeinformationen:

     i. Geben Sie für vCenter URL/IP die IP-Adresse Ihres VMware vCenter Server-Hosts ein.

     ii. Geben Sie bei vCenter Username (vCenter-Benutzername) den Namen eines lokalen oder Domänenbenutzers ein, den der Konnektor zur Kommunikation mit vCenter verwendet. Für Domänenbenutzer: Verwenden Sie die Form Domäne\Benutzername oder Benutzername@Domäne.

     iii. Geben Sie für vCenter Password (vCenter-Passwort) das lokale oder Domänenbenutzerpasswort ein.

  b. Wählen Sie Speichern.

Manuelles Aktualisieren von Agentless Collector

Wenn Sie Application Discovery Service Agentless Collector (Agentless Collector) konfigurieren, können Sie wählen, ob automatische Updates aktiviert werden sollen, wie unter beschrieben. Schritt 5: Agentless Collector konfigurieren Wenn Sie automatische Updates nicht aktivieren, müssen Sie Agentless Collector manuell aktualisieren.

Im folgenden Verfahren wird beschrieben, wie Agentless Collector manuell aktualisiert wird.

Um Agentless Collector manuell zu aktualisieren

1. Besorgen Sie sich die neueste Agentless Collector Open Virtualization Archive (OVA) -Datei.
2. (Optional) Wir empfehlen, dass Sie die vorherige Agentless Collector OVA-Datei löschen, bevor Sie die neueste bereitstellen.
3. Gehen Sie in Erste Schritte mit Agentless Collector diesem Abschnitt Schritt für Schritt vorSchritt 3: Stellen Sie Agentless Collector bereit. Schritt 6: Richten Sie die Agentless Collector-Datenerfassungsmodule ein

Das vorherige Verfahren aktualisiert nur den Agentless Collector. Es liegt in Ihrer Verantwortung, das Betriebssystem auf dem neuesten Stand zu halten.

So aktualisieren Sie Ihre Amazon EC2 EC2-Instance

1. Rufen Sie die IP-Adresse des Agentless Collectors von VMware vCenter ab.
2. Öffnen Sie die VM-Konsole des Collectors und melden Sie sich **`ec2-user`** mit dem Passwort an, **`collector`** wie im folgenden Beispiel gezeigt.

   ```
   username: ec2-user
   password: collector
   ```

3. Folgen Sie den Anweisungen unter Instance-Software auf Ihrer AL2-Instance aktualisieren im Amazon Linux 2-Benutzerhandbuch.

Kernel-Live-Patching auf Amazon Linux 2

Die virtuelle Maschine Agentless Collector verwendet Amazon Linux 2, wie unter beschriebenSchritt 3: Stellen Sie Agentless Collector bereit.

Informationen zur Aktivierung und Verwendung von Live-Patching für Amazon Linux 2 finden Sie unter Kernel Live Patching on Amazon Linux 2 im Amazon EC2 EC2-Benutzerhandbuch.

Fehlerbehebung bei Agentless Collector

Dieser Abschnitt enthält Themen, die Ihnen bei der Behebung bekannter Probleme mit Application Discovery Service Agentless Collector (Agentless Collector) helfen können.

Themen

- Behebung von Problemen, die Agentless Collector während der Installation nicht erreichen kann AWS
- Behebung von Problemen mit selbstsignierten Zertifizierungen beim Herstellen einer Verbindung zum Proxyhost
- Suche nach fehlerhaften Collectors
- Behebung von IP-Adressproblemen
- Behebung von Problemen mit vCenter-Anmeldeinformationen

- Behebung von Problemen bei der Datenweiterleitung im Modul zur Erfassung von Datenbank- und Analysedaten
- Behebung von Verbindungsproblemen im Modul zur Erfassung von Datenbank- und Analysedaten
- Unterstützung eigenständiger ESX-Hosts
- Kontaktaufnahme mit dem AWS Support bei Problemen mit Agentless Collector

Behebung von Problemen, die Agentless Collector während der Installation nicht erreichen kann AWS

Agentless Collector benötigt ausgehenden Zugriff über TCP-Port 443 auf mehrere Domänen. AWS Bei der Konfiguration von Agentless Collector in der Konsole kann die folgende Fehlermeldung angezeigt werden.

> Konnte nicht erreicht werden AWS
>
> AWS kann nicht erreicht werden. Bitte überprüfen Sie die Netzwerkeinstellungen.

Dieser Fehler tritt aufgrund eines fehlgeschlagenen Versuchs von Agentless Collector auf, eine HTTPS-Verbindung zu einer AWS Domain herzustellen, mit der der Collector während des Einrichtungsvorgangs kommunizieren muss. Die Agentless Collector-Konfiguration schlägt fehl, wenn keine Verbindung hergestellt werden kann.

Um die Verbindung zu zu reparieren AWS

1. Erkundigen Sie sich bei Ihrem IT-Administrator, ob die Firewall Ihres Unternehmens ausgehenden Datenverkehr auf Port 443 zu AWS Domänen blockiert, für die ausgehenden Zugriff erforderlich ist. Für welche AWS Domains ein ausgehender Zugriff erforderlich ist, hängt davon ab, ob Ihre Heimatregion die Region USA West (Oregon), US-West-2 oder eine andere Region ist.

   Für die folgenden Domains ist ausgehender Zugriff erforderlich, wenn die Heimatregion Ihres AWS Kontos US-West-2 ist:

   - `arsenal-discovery.us-west-2.amazonaws.com`
   - `migrationhub-config.us-west-2.amazonaws.com`
   - `api.ecr-public.us-east-1.amazonaws.com`

- `public.ecr.aws`

Für die folgenden Domains ist ausgehender Zugriff erforderlich, wenn die Heimatregion Ihres AWS Kontos nicht der Fall ist: **`us-west-2`**

- `arsenal-discovery.us-west-2.amazonaws.com`
- `arsenal-discovery.`*`your-home-region`*`.amazonaws.com`
- `migrationhub-config.us-west-2.amazonaws.com`
- `api.ecr-public.us-east-1.amazonaws.com`
- `public.ecr.aws`

Wenn Ihre Firewall den ausgehenden Zugriff auf die AWS Domains blockiert, mit denen Agentless Collector kommunizieren muss, konfigurieren Sie im Abschnitt Datensynchronisierung unter Collector-Konfiguration einen Proxyhost.

2. Wenn das Verbindungsproblem durch die Aktualisierung der Firewall nicht behoben wird, gehen Sie wie folgt vor, um sicherzustellen, dass die virtuelle Collector-Maschine über eine ausgehende Netzwerkverbindung zu den im vorherigen Schritt aufgeführten Domänen verfügt.

   a. Rufen Sie die IP-Adresse des Agentless Collectors von VMware vCenter ab.

   b. Öffnen Sie die VM-Konsole des Collectors und melden Sie sich **`ec2-user`** mit dem Passwort an, **`collector`** wie im folgenden Beispiel gezeigt.

   ```
   username: ec2-user
   password: collector
   ```

   c. Testen Sie die Verbindung zu den aufgelisteten Domänen, indem Sie Telnet auf den Ports 443 ausführen, wie im folgenden Beispiel gezeigt.

   ```
   telnet migrationhub-config.us-west-2.amazonaws.com 443
   ```

3. Wenn Telnet die Domain nicht auflösen kann, versuchen Sie, einen statischen DNS-Server anhand der Anweisungen für Amazon Linux 2 zu konfigurieren.

4. Falls der Fehler weiterhin besteht, finden Sie weitere Unterstützung unterKontaktaufnahme mit dem AWS Support bei Problemen mit Agentless Collector.

Behebung von Problemen mit selbstsignierten Zertifizierungen beim Herstellen einer Verbindung zum Proxyhost

Wenn die Kommunikation mit dem optional bereitgestellten Proxy über HTTPS erfolgt und der Proxy über ein selbstsigniertes Zertifikat verfügt, müssen Sie möglicherweise ein Zertifikat bereitstellen.

1. Rufen Sie die IP-Adresse des Agentless Collectors von VMware vCenter ab.
2. Öffnen Sie die VM-Konsole des Collectors und melden Sie sich `ec2-user` mit dem Passwort an, `collector` wie im folgenden Beispiel gezeigt.

   ```
   username: ec2-user
   password: collector
   ```

3. Fügen Sie den Hauptteil des Zertifikats, das dem sicheren Proxy zugeordnet ist, einschließlich `-----BEGIN CERTIFICATE-----` sowohl als auch`-----END CERTIFICATE-----`, in die folgende Datei ein:

   ```
   /etc/pki/ca-trust/source/anchors/https-proxy-ca.pem
   ```

4. Führen Sie die folgenden Befehle aus, um das neue Zertifikat zu installieren:

   ```
   sudo update-ca-trust
   ```

5. Starten Sie den Agentless Collector neu, indem Sie den folgenden Befehl ausführen:

   ```
   sudo shutdown -r now
   ```

Suche nach fehlerhaften Collectors

Statusinformationen für jeden Collector finden Sie auf der Seite Datensammler der AWS Migration Hub (Migration Hub) -Konsole. Sie können Collectors mit Problemen identifizieren, indem Sie alle Collectors mit dem Status Erfordert Aufmerksamkeit suchen.

Im folgenden Verfahren wird beschrieben, wie Sie auf die Agentless Collector-Konsole zugreifen können, um Gesundheitsprobleme zu identifizieren.

So greifen Sie auf die Agentless Collector-Konsole zu

1. Melden Sie sich mit Ihrem AWS Konto bei der Migration Hub Hub-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/migrationhub/.
2. Wählen Sie im Navigationsbereich der Migration Hub Hub-Konsole unter Discover die Option Datensammler aus.
3. Notieren Sie sich auf der Registerkarte Agentless Collectors die IP-Adresse für jeden Connector, der den Status Erfordert Aufmerksamkeit.
4. Öffnen Sie einen Webbrowser, um die Agentless Collector-Konsole zu öffnen. Geben Sie dann die folgende URL in die Adressleiste ein: **`https://`**<ip_address>, wobei ip_address die IP-Adresse eines fehlerhaften Collectors ist.
5. Wählen Sie Anmelden und geben Sie dann das Agentless Collector-Passwort ein, das bei der Konfiguration des Collectors eingerichtet wurde. Schritt 5: Agentless Collector konfigurieren
6. Wählen Sie auf der Agentless Collector-Dashboard-Seite unter Datenerfassung im Abschnitt VMware vCenter die Option Anzeigen und bearbeiten aus.
7. Folgen Sie den Anweisungen unterBearbeiten der VMware vCenter-Anmeldeinformationen, um die URL und die Anmeldeinformationen zu korrigieren.

Nach der Behebung der Integritätsprobleme stellt der Collector die Konnektivität mit dem vCenter Server wieder her, und der Status des Collectors ändert sich in den Status Collecting. Falls die Probleme weiterhin bestehen, finden Sie weitere Informationen unter. Kontaktaufnahme mit dem AWS Support bei Problemen mit Agentless Collector

Die häufigsten Ursachen für fehlerhafte Collectors sind Probleme mit IP-Adressen und Anmeldeinformationen. Behebung von IP-Adressproblemenund Behebung von Problemen mit vCenter-Anmeldeinformationen kann Ihnen helfen, diese Probleme zu lösen und einen Collector wieder in einen fehlerfreien Zustand zu versetzen.

Behebung von IP-Adressproblemen

Ein Collector kann in einen fehlerhaften Zustand übergehen, wenn der beim Collector-Setup angegebene vCenter-Endpoint fehlerhaft oder ungültig ist oder wenn der vCenter Server derzeit ausgefallen und nicht erreichbar ist. In diesem Fall erhalten Sie eine Verbindungsfehlermeldung.

Das folgende Verfahren kann bei der Behebung von IP-Adressproblemen helfen.

Um Probleme mit der Collector-IP-Adresse zu beheben

1. Rufen Sie die IP-Adresse des Agentless Collectors von VMware vCenter ab.
2. Öffnen Sie die Agentless Collector-Konsole, indem Sie einen Webbrowser öffnen, und geben Sie dann die folgende URL in die Adressleiste ein: **`https://`**`/`<ip_address>, wobei ip_address die IP-Adresse des Collectors ist. Schritt 3: Stellen Sie Agentless Collector bereit
3. Wählen Sie Anmelden und geben Sie dann das Agentless Collector-Passwort ein, das bei der Konfiguration des Collectors eingerichtet wurde. Schritt 5: Agentless Collector konfigurieren
4. Wählen Sie auf der Agentless Collector-Dashboard-Seite unter Datenerfassung im Abschnitt VMware vCenter die Option Anzeigen und bearbeiten aus.
5. Notieren Sie sich auf der Seite mit den Details zur VMware-Datenerfassung unter Entdeckte vCenter-Server die IP-Adresse in der Spalte vCenter.
6. Überprüfen Sie mithilfe eines separaten Befehlszeilentools wie `ping` oder`traceroute`, ob der zugehörige vCenter Server aktiv ist und die IP von der Collector-VM aus erreichbar ist.
   - Wenn die IP-Adresse falsch ist und der vCenter-Dienst aktiv ist, aktualisieren Sie die IP-Adresse in der Collector-Konsole und wählen Sie Weiter.
   - Wenn die IP-Adresse richtig, der vCenter-Server aber inaktiv ist, aktivieren Sie den Server.
   - Wenn die IP-Adresse richtig und der vCenter-Server aktiv ist, prüfen Sie, ob er aufgrund der Firewall-Einstellungen eingehende Netzwerkverbindungen blockiert. Falls ja, aktualisieren Sie Ihre Firewall-Einstellungen, um eingehende Verbindungen von der Collector-VM zuzulassen.

Behebung von Problemen mit vCenter-Anmeldeinformationen

Collectors können in einen fehlerhaften Zustand übergehen, wenn die bei der Konfiguration eines Collectors angegebenen vCenter-Benutzeranmeldedaten ungültig sind oder keine vCenter Read- und View-Kontoberechtigungen haben.

Wenn Sie Probleme mit den vCenter-Anmeldeinformationen haben, stellen Sie sicher, dass Sie die vCenter-Lese- und View-Berechtigungen für die Systemgruppe festgelegt haben.

Informationen zum Bearbeiten von vCenter-Anmeldeinformationen finden Sie unterBearbeiten der VMware vCenter-Anmeldeinformationen.

Behebung von Problemen bei der Datenweiterleitung im Modul zur Erfassung von Datenbank- und Analysedaten

Auf der Startseite des Moduls zur Erfassung von Datenbank- und Analysedaten in Agentless Collector wird der Verbindungsstatus für Access to DMS und Access to S3 angezeigt. Wenn für Access to DMS und Access to S3 die Option Kein Zugriff angezeigt wird, konfigurieren Sie die Datenweiterleitung. Weitere Informationen finden Sie unter Datenweiterleitung konfigurieren.

Wenn dieses Problem nach der Konfiguration der Datenweiterleitung auftritt, überprüfen Sie, ob Ihr Datenerfassungsmodul auf das Internet zugreifen kann. Stellen Sie anschließend sicher, dass Sie Ihrem IAM-Benutzer die DMS CollectorPolicy - und FleetAdvisorS3Policy-Richtlinien hinzugefügt haben. Weitere Informationen finden Sie unter Schritt 1: Erstellen Sie einen IAM-Benutzer für Agentless Collector.

Wenn Ihr Datenerfassungsmodul keine Verbindung zu den folgenden Domänen herstellen kann AWS, gewähren Sie ausgehenden Zugriff auf die folgenden Domänen.

- `dms.`*`your-home-region`*`.amazonaws.com`
- `s3.amazonaws.com`

Behebung von Verbindungsproblemen im Modul zur Erfassung von Datenbank- und Analysedaten

Das Modul zur Erfassung von Datenbank- und Analysedaten in Agentless Collector stellt eine Verbindung zu Ihren LDAP-Servern her, um Betriebssystemserver in Ihrer Datenumgebung zu erkennen. Anschließend stellt das Datenerfassungsmodul eine Verbindung zu Ihren Betriebssystemservern her, um Datenbank- und Analyseserver zu ermitteln. Von diesen Datenbankservern sammelt das Datenerfassungsmodul Kapazitäts- und Leistungskennzahlen. Wenn Ihr Datenerfassungsmodul keine Verbindung zu diesen Servern herstellen kann, überprüfen Sie, ob Sie eine Verbindung zu Ihren Servern herstellen können.

Ersetzen Sie in den folgenden Beispielen *`ersetzbare`* Werte durch Ihre Werte.

- Um zu überprüfen, ob Sie eine Verbindung zu Ihrem LDAP-Server herstellen können, installieren Sie das `ldap-util` Paket. Führen Sie dazu den folgenden Befehl aus.

```
sudo apt-get install ldap-util
```

Führen Sie anschließend den folgenden Befehl aus.

```
ldapsearch -x -D "CN=user,CN=Users,DC=example,DC=com" -w "password" -b
 "dc=example,dc=com" -h
```

- Verwenden Sie die folgenden Befehle, um zu überprüfen, ob Sie eine Verbindung zu einem Linux-Betriebssystemserver herstellen können.

```
ssh -i C:\Users\user\private_key.pem -p 22 username@my-linux-host.domain.com
```

Führen Sie das vorherige Beispiel als Administrator in Windows aus.

```
ssh username@my-linux-host.domain.com
```

Führen Sie das vorherige Beispiel unter Linux aus.

- Verwenden Sie die folgenden Befehle, um zu überprüfen, ob Sie eine Verbindung zu einem Windows-Betriebssystemserver herstellen können.

```
winrs -r:[hostname or ip] -u:username -p:password cmd
```

Führen Sie das vorherige Beispiel als Administrator in Windows aus.

```
sudo apt install -y winrm
winrm --user=username --password=password [http or https]://[hostname or ip]:[port]
 "[cmd.exe or any other CLI command]"
```

Führen Sie das vorherige Beispiel unter Linux aus.

- Verwenden Sie die folgenden Befehle, um zu überprüfen, ob Sie eine Verbindung zu einer SQL Server-Datenbank herstellen können.

```
sqlcmd -S [hostname or IP] -U username -P 'password'
SELECT GETDATE() AS sysdate
```

- Verwenden Sie die folgenden Befehle, um zu überprüfen, ob Sie eine Verbindung zu einer MySQL-Datenbank herstellen können.

```
mysql -u username -p 'password' -h [hostname or IP] -P [port]
```

```
SELECT NOW() FROM DUAL
```

- Verwenden Sie die folgenden Befehle, um zu überprüfen, ob Sie eine Verbindung zu einer Oracle-Datenbank herstellen können.

```
sqlplus username/password@[hostname or IP]:port/servicename
SELECT SYSDATE FROM DUAL
```

- Verwenden Sie die folgenden Befehle, um zu überprüfen, ob Sie eine Verbindung zu einer PostgreSQL-Datenbank herstellen können.

```
psql -U username -h [hostname or IP] -p port -d database
SELECT CURRENT_TIMESTAMP AS sysdate
```

Wenn Sie keine Verbindung zu Ihren Datenbank- und Analyseservern herstellen können, stellen Sie sicher, dass Sie die erforderlichen Berechtigungen bereitstellen. Weitere Informationen finden Sie unter Entdecken Sie Ihre Datenbankserver.

Unterstützung eigenständiger ESX-Hosts

Der Agentless Collector unterstützt keinen eigenständigen ESX-Host. Der ESX-Host muss Teil der vCenter Server-Instance sein.

Kontaktaufnahme mit dem AWS Support bei Problemen mit Agentless Collector

Wenn Sie Probleme mit Application Discovery Service Agentless Collector (Agentless Collector) haben und Hilfe benötigen, wenden Sie sich an den AWS Support. Sie werden kontaktiert und möglicherweise aufgefordert, die Collector-Protokolle zu senden.

Um Agentless Collector-Protokolle zu erhalten

1. Rufen Sie die IP-Adresse des Agentless Collectors von VMware vCenter ab.
2. Öffnen Sie die VM-Konsole des Collectors und melden Sie sich **`ec2-user`** mit dem Passwort an, **`collector`** wie im folgenden Beispiel gezeigt.

```
username: ec2-user
password: collector
```

3. Verwenden Sie den folgenden Befehl, um zum Protokollordner zu navigieren.

```
cd /var/log/aws/collector
```

4. Komprimieren Sie die Protokolldateien mithilfe der folgenden Befehle.

```
sudo cp /local/agentless_collector/compose.log .
docker inspect $(docker ps --format {{.Names}}) | sudo tee docker_inspect.log >/
dev/null
sudo tar czf logs_$(date '+%d-%m-%Y_%H.%M.%S').tar.gz * --exclude='db.mv*'
```

5. Kopieren Sie die Protokolldatei von der Agentless Collector-VM.

```
scp logs*.tar.gz targetuser@targetaddress
```

6. Geben Sie die `tar.gz` Datei an AWS Enterprise Support weiter.

Migration Hub Hub-Import

AWS Migration HubDer -Import (Migration Hub) ermöglicht es Ihnen, Details Ihrer lokalen Umgebung direkt in Migration Hub zu importieren, ohne dass der Application Discovery Service Agentless Collector (Agentless Collector) oderAWSApplication Discovery Agent (Discovery Agent), so dass Sie die Migrationsbewertung und -planung direkt aus Ihren importierten Daten heraus durchführen können. Sie können auch Ihre Geräte als Anwendungen gruppieren und deren Migrationsstatus nachverfolgen.

So starten Sie eine Importanforderung

- Laden Sie die speziell formatierte CSV-Importvorlage (kommagetrennte Werte) herunter.
- Füllen Sie diese mit Ihren vorhandenen lokalen Serverdaten aus.
- Laden Sie es mithilfe der Migration Hub-Konsole auf den Migration Hub hoch.AWS CLIoder einer derAWS-SDKs.

Sie können mehrere Importanforderungen übermitteln. Jede Anforderung wird sequentiell verarbeitet. Sie können den Status Ihrer Importanforderungen jederzeit über die Konsole oder mit den Import-APIs überprüfen.

Nachdem eine Importanfrage abgeschlossen ist, können Sie die Details der einzelnen importierten Datensätze anzeigen. Zeigen Sie Nutzungsdaten, Tags und Anwendungszuordnungen direkt in der Migration Hub Hub-Konsole an. Wenn während des Importvorgangs Fehler aufgetreten sind, können Sie die Anzahl der erfolgreichen und fehlgeschlagenen Datensätze sowie die Fehlerdetails für jeden fehlgeschlagenen Datensatz prüfen.

Fehlerbehandlung: Ein Link wird bereitgestellt, um das Fehlerprotokoll und fehlgeschlagene Datensatzdateien im CSV-Format in einem komprimierten Archiv herunterzuladen. Verwenden Sie diese Dateien, um Ihre Importanfrage erneut zu senden, nachdem Sie die Fehler korrigiert haben.

Es gibt Beschränkungen in Bezug auf die Anzahl der importierten Datensätze, der importierten Server und der gelöschten Datensätze, die Sie behalten können. Weitere Informationen finden Sie unter AWS Application Discovery Service-Kontingente.

Unterstützte Importdateifelder

Migration Hub Hub-Import ermöglicht Ihnen, Daten aus jeder Quelle zu importieren. Die bereitgestellten Daten müssen im unterstützten Format für eine CSV-Datei vorliegen, und die Daten dürfen nur die unterstützten Felder mit den unterstützten Bereichen für diese Felder enthalten.

Ein Sternchen neben einem Importfeldnamen in der folgenden Tabelle zeigt an, dass es sich um ein Pflichtfeld handelt. Für jeden Datensatz Ihrer Importdatei müssen mindestens eines oder mehrere dieser Pflichtfelder ausgefüllt sein, damit die eindeutige Identifizierung eines Servers oder einer Anwendung möglich ist. Ein Datensatz ohne Angaben in einem der erforderlichen Felder wird nicht importiert.

> **Note**
>
> Wenn Sie VMware verwenden.MoRefId oder VMware.VCenterId, müssen Sie beide Felder im selben Datensatz haben.

Importfeldname	Beschreibung	Beispiele
ExternalId*	Eine benutzerdefinierte Kennung, die es Ihnen ermöglicht, die Datensätze als eindeutig zu kennzeichnen. Beispiel,ExternalIdkann die Inventar-ID für den Server in Ihrem Rechenzentrum sein.	Inventory Id 1 Server 2 CMBD Id 3
SMBiosId	Systemmanagement-BIOS-(SMBIOS) ID.	
IPAddress*	Eine durch Kommata getrennte Liste von IP-Adressen des Servers, in Anführungszeichen.	192.0.0.2 „10.12.31.233, 10.12.32.11“
MACAddress*	Eine durch Kommata getrennte Liste von MAC-	00:1B:44:11:3A:B7

Importfeldname	Beschreibung	Beispiele
	Adressen des Servers, in Anführungszeichen.	„00-15-E9-2B-99-3C, 00-14-22-01-23-45“
HostName*	Der Hostname des Servers. Wir empfehlen die Verwendung des vollständig qualifizierten Domänennamens (FQDN, Fully Qualified Domain Name) für diesen Wert.	ip-1-2-3-4 localhost.domain
VMware.MoRefId*	Die verwaltete Objektreferenz-ID Muss mit einer VMware angegeben werden.CenterId.	
VMware.VCenterId*	Eindeutige Kennung einer virtuellen Maschine. Muss mit einer VMware angegeben werden.MoRefId.	
CPU.NumberOfProcessors	Die Anzahl der CPUs.	4
CPU.NumberOfCores	Die Gesamtzahl der physischen Kerne.	8
CPU.NumberOfLogicalCores	Die Gesamtanzahl der Threads, die gleichzeitig auf allen CPUs in einem Server ausgeführt werden können. Einige CPUs unterstützen die Ausführung mehrerer Threads gleichzeitig auf einem einzelnen CPU-Kern. In diesen Fällen ist diese Zahl größer als die Anzahl der physischen (oder virtuellen) Kerne.	16

Importfeldname	Beschreibung	Beispiele
OS.Name	Der Name des Betriebss ystems.	Linux Windows.Hat
OS.Version	Die Version des Betriebss ystems.	16.04.3 NT 6.2.8
VMware.VMName	Der Name der virtuellen Maschine.	Corp1
RAMTotalSizeInMB	Der gesamte auf dem Server verfügbare RAM in MB.	64 128
RAMUsedSizeInmb.AVG	Die durchschnittliche Menge an verwendetem RAM auf dem Server in MB.	64 128
RAMUsedSizeInMB.max	Die maximale Menge von auf dem Server verfügbaren verwendeten RAM in MB.	64 128
CPU.UsagePct.Avg	Die durchschnittliche CPU-Auslastung während der Datenerfassung durch das Discovery-Tool.	45 23.9
CPU.UsagePct.Max	Die maximale CPU-Ausla stung während der Datenerfa ssung durch das Discovery-Tool.	55.34 24
DiskReadsPerSecond Inkb.AVG	Die durchschnittliche Anzahl der Festplattenlesevorgänge pro Sekunde, in KB.	1159 84506

Importfeldname	Beschreibung	Beispiele
DiskWritesPerSecondInkb.AVG	Die durchschnittliche Anzahl der Festplattenschreibvorgänge pro Sekunde, in KB.	199 6197
DiskReadsPerSecondInkb.max	Die maximale Anzahl der Festplattenlesevorgänge pro Sekunde, in KB.	37892 869962
DiskWritesPerSecondInkb.max	Die maximale Anzahl der Festplattenschreibvorgänge pro Sekunde, in KB.	18436 1808
DiskReadsOpsPerSecond.Avg	Durchschnittliche Anzahl der Lesevorgänge pro Sekunde.	45 28
DiskWritesOpsPerSecond.Avg	Durchschnittliche Anzahl der Festplattenschreibvorgänge pro Sekunde.	8 3
DiskReadsOpsPerSecond.Max	Die maximale Anzahl der Festplattenlesevorgänge pro Sekunde.	1083 176
DiskWritesOpsPerSecond.Max	Die maximale Anzahl der Festplattenschreibvorgänge pro Sekunde.	535 71
NetworkReadsPerSecondInkb.AVG	Die durchschnittliche Anzahl der Netzwerklesevorgänge pro Sekunde, in KB.	45 28
NetworkWritesPerSecondInkb.AVG	Die durchschnittliche Anzahl der Netzwerkschreibvorgänge pro Sekunde, in KB.	8 3

Importfeldname	Beschreibung	Beispiele
NetworkReadsPerSecondInkb.max	Die maximale Anzahl der Netzwerklesevorgänge pro Sekunde, in KB.	1083 176
NetworkWritesPerSecondInkb.max	Die maximale Anzahl der Netzwerkschreibvorgänge pro Sekunde, in KB.	535 71
Anwendungen	Eine durch Kommata getrennte Liste der Anwendungen, die diesen Server enthalten, in Anführungszeichen. Dieser Wert kann vorhandene Anwendungen und/oder neue Anwendungen, die beim Import erstellt werden, beinhalten.	Application1 „Application2, Application3“
Tags (Markierungen)	Eine durch Kommata getrennte Liste der als Name:Wert formatierten Tags. **Important** Speichern Sie keine sensiblen Informationen (wie persönliche Daten) in Tags.	„zone:1, critical:yes“ „zone:3, critical:no, zone:1“

Sie können Daten importieren, auch wenn Sie nicht für alle in der Importvorlage definierten Felder Daten eingegeben haben, sofern jeder Datensatz mindestens eines der Pflichtfelder enthält. Duplikate werden über mehrere Importanfragen hinweg über einen externen oder internen Abgleichschlüssel verwaltet. Wenn Sie Ihren eigenen Abgleichschlüssel eingeben, `External ID`, wird dieses Feld zur eindeutigen Identifizierung und zum Import der Datensätze verwendet.

Wenn kein Abgleichschlüssel angegeben wird, verwendet der Import einen intern generierten Abgleichschlüssel, der aus einigen der Spalten in der Importvorlage abgeleitet wird. Weitere Informationen zu diesem Abgleich finden Sie unter Abgleichslogik für entdeckte Server und Anwendungen.

> **Note**
>
> Der -Import des Migration Hub unterstützt keine Felder außer den in der Importvorlage definierten. Jegliche benutzerdefinierte Felder werden ignoriert und nicht importiert.

Einrichten Ihrer Importberechtigungen

Bevor Sie Ihre Daten importieren können, müssen Sie sicherstellen, dass Ihr IAM-Benutzer über die erforderlichen Amazon S3 S3-Berechtigungen zum Hochladen verfügt (`s3:PutObject`) Ihre Importdatei nach Amazon S3 und das Objekt zu lesen (`s3:GetObject`) enthalten. Dazu müssen Sie auch den programmatischen ZugriffAWS CLI) oder Konsolenzugriff, indem Sie eine IAM-Richtlinie erstellen und mit dem IAM-Benutzer verbinden, der Importe in IhremAWSKonto.

Console Permissions

Gehen Sie wie folgt vor, um die Berechtigungsrichtlinie für den IAM-Benutzer zu bearbeiten, der Importanfragen in Ihrem erstellen wirdAWSKonto über die Konsole.

Die einem Benutzer hinzugefügten verwalteten Richtlinien bearbeiten

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Klicken Sie im Navigationsbereich auf Users (Benutzer).
3. Wählen Sie den Namen des Benutzers aus, dessen Berechtigungsrichtlinie Sie ändern möchten.
4. Wählen Sie die Registerkarte Permissions (Berechtigungen) und anschließend die Option Add Permissions (Berechtigungen hinzufügen) aus.
5. Wählen Sie Attach existing policies directly (Vorhandene Richtlinien direkt zuweisen) und dann Create policy (Richtlinie erstellen).

    a. Wählen Sie auf der dann angezeigten Seite Create policy (Richtlinie erstellen) die Option JSON, und fügen Sie die folgende Richtlinie ein. Denken Sie daran, den Namen Ihres

Buckets durch den tatsächlichen Namen des Buckets zu ersetzen, in den der IAM-Benutzer die importierten Dateien hochladen wird.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": ["s3:ListBucket"],
      "Resource": ["arn:aws:s3:::importBucket"]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource": ["arn:aws:s3:::importBucket/*"]
    }
  ]
}
```

b. Wählen Sie Review policy (Richtlinie prüfen).

c. Geben Sie Ihrer Richtlinie unter Name einen neuen Namen, und fügen Sie optional eine Beschreibung hinzu, bevor Sie die Zusammenfassung der Richtlinie anzeigen.

d. Wählen Sie Create Policy (Richtlinie erstellen) aus.

6. Kehren Sie zuErteilen Sie BerechtigungenIAM-Konsolenseite für den -Benutzer, der Importanfragen in IhremAWSKonto.

7. Aktualisieren Sie die Richtlinientabelle, und suchen Sie nach dem Namen der soeben erstellten Richtlinie.

8. Wählen Sie Weiter. Prüfen.

9. Wählen Sie Add permissions.

Nachdem Sie die Richtlinie Ihrem IAM-Benutzer hinzugefügt haben, können Sie den Importvorgang starten.

AWS CLI Permissions

Gehen Sie wie folgt vor, um die verwalteten Richtlinien zu erstellen, die erforderlich sind, um einem IAM-Benutzer die Berechtigungen zu erteilen, um Importdatenanforderungen mithilfe derAWS CLI.

So erstellen und fügen Sie die verwalteten Richtlinien hinzu

1. Verwenden der`aws iam create-policy` AWS CLI-Befehl zur Erstellung einer IAM-Richtlinie mit den folgenden Berechtigungen Denken Sie daran, den Namen Ihres Buckets durch den tatsächlichen Namen des Buckets zu ersetzen, in den der IAM-Benutzer die importierten Dateien hochladen wird.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["s3:ListBucket"],
      "Resource": ["arn:aws:s3:::importBucket"]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource": ["arn:aws:s3:::importBucket/*"]
    }
  ]
}
```

Weitere Informationen zur Verwendung dieses Befehls finden Sie untercreate-policyimAWS CLIBefehlsreferenz.

2. Verwenden Sie den `aws iam create-policy` AWS CLI-Befehl zur Erstellung einer zusätzlichen IAM-Richtlinie mit den folgenden Berechtigungen

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "discovery:ListConfigurations",
                "discovery:CreateApplication",
                "discovery:UpdateApplication",
                "discovery:AssociateConfigurationItemsToApplication",
                "discovery:DisassociateConfigurationItemsFromApplication",
                "discovery:GetDiscoverySummary",
                "discovery:StartImportTask",
                "discovery:DescribeImportTasks",
                "discovery:BatchDeleteImportData"
            ],
            "Resource": "*"
        }
    ]
}
```

3. Verwenden Sie den `aws iam attach-user-policy` AWS CLI-Befehl, um die Richtlinien, die Sie in den beiden vorherigen Schritten erstellt haben, dem IAM-Benutzer zuzuweisen, der Importanfragen in Ihrem AWS Konto mit dem AWS CLI. Weitere Informationen zur Verwendung dieses Befehls finden Sie unter attach-user-policy im AWS CLI Befehlsreferenz.

Nachdem Sie die Richtlinien Ihrem IAM-Benutzer hinzugefügt haben, können Sie den Importvorgang starten.

Denken Sie daran: Wenn der IAM-Benutzer Objekte in den von Ihnen angegebenen Amazon S3 S3-Bucket hochlädt, müssen die für die Objekte eingerichteten Standardberechtigungen unverändert gelassen werden, damit der Benutzer das Objekt lesen kann.

Hochladen Ihrer Importdatei in Amazon S3

Anschließend müssen Sie Ihre Importdatei im CSV-Format zu Amazon S3 hochladen, sodass sie importiert werden kann. Vorher müssen Sie über einen Amazon S3 S3-Bucket für die erstellte und/oder vorab ausgewählte Importdatei verfügen.

Console S3 Upload

So laden Sie Ihre Importdatei in Amazon S3

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-S3-Konsole unter https://console.aws.amazon.com/s3/.
2. Wählen Sie in der Liste Bucket name (Bucket-Name) den Namen des Buckets aus, zu dem Sie Ihr Objekt hochladen möchten.
3. Klicken Sie auf Upload.
4. Wählen Sie im Dialogfeld Upload (Hochladen) die Option Add Files (Dateien hinzufügen) aus, um die hochzuladende Datei auszuwählen.
5. Wählen Sie eine hochzuladende Datei und dann Open (Öffnen) aus.
6. Klicken Sie auf Upload.
7. Nachdem Sie die Datei hochgeladen haben, wählen Sie den Namen Ihres Datendatei-Objekts aus Ihrem Bucket-Dashboard.
8. Kopieren Sie von der Registerkarte Overview (Übersicht) der Objektdetails-Seite die Object URL (Objekt-URL). Sie benötigen diese beim Erstellen Ihrer Importanforderung.
9. Wechseln Sie zuImportin der Migration Hub Hub-Konsole wie unter beschriebenImportieren von Daten. Fügen Sie dann die Objekt-URL in das FeldAmazon S3 Objekt-URLfield.

AWS CLI S3 Upload

So laden Sie Ihre Importdatei in Amazon S3

1. Öffnen Sie ein Terminalfenster, und navigieren Sie zu dem Verzeichnis, in dem Ihre Importdatei gespeichert ist.
2. Geben Sie den folgenden Befehl ein:

```
aws s3 cp ImportFile.csv s3://BucketName/ImportFile.csv
```

3. Dies gibt folgende Ergebnisse zurück:

```
upload: .\ImportFile.csv to s3://BucketName/ImportFile.csv
```

4. Kopieren Sie den vollständigen Amazon-S3-Objektpfad, der zurückgegeben wurde. Dies benötigen Sie, wenn Sie Ihre Importanfrage erstellen.

Importieren von Daten

Nach dem Herunterladen der Importvorlage aus der Migration Hub-Konsole und der Eingabe Ihrer vorhandenen lokalen Serverdaten können Sie die Daten in Migration Hub importieren. Die folgenden Anweisungen beschreiben dazu zwei Möglichkeiten: Entweder mithilfe der Konsole oder durch Senden von API-Aufrufen über dieAWS CLI.

Console Import

Starten Sie den Datenimport auf-ToolsSeite der Migration Hub Hub-Konsole.

So starten Sie den Datenimport:

1. Wählen Sie im Navigationsbereich unter Discover (Entdecken) Tools aus.
2. Wenn Sie nicht bereits eine Importvorlage ausgefüllt haben, können Sie die Vorlage herunterladen, indem Sie Import template (Importvorlage) im Feld Import auswählen. Öffnen Sie die heruntergeladene Vorlage, und füllen Sie sie mit Ihren vorhandenen lokalen Serverdaten aus. Sie können die Importvorlage auch aus unserem Amazon S3 Bucket unterhttps://s3.us-west-2.amazonaws.com/templates-7cffcf56-bd96-4b1c-b45b-a5b42f282e46/import_template.csv
3. So öffnen Sie denImport-Seite, wählenImportimImportaus.
4. UnderName, geben Sie einen Namen für den Import an.
5. Füllen Sie dieAmazon S3 Objekt-URLfield. Dazu müssen Sie Ihre Importdatendatei zu Amazon S3 hochladen. Weitere Informationen finden Sie unter Hochladen Ihrer Importdatei in Amazon S3.
6. Wählen Sie Import im unteren rechten Bereich. Dadurch wird die Seite Imports (Importe) geöffnet, auf der Sie Ihren Import und seinen Status in der Tabelle sehen können.

Nachdem Sie die vorangegangenen Schritte zum Starten Ihres Datenimports durchgeführt haben, zeigt die Seite Imports (Importe) Details zu jeder Importanfrage einschließlich ihres Fortschritts,

des Abschlusszeitpunkts und der Anzahl der erfolgreichen und fehlgeschlagenen Datensätze an; diese Datensätze können heruntergeladen werden. Von diesem Bildschirm können Sie auch zur Seite Servers (Server) unterDiscover (Entdecken) navigieren, um die tatsächlichen importierten Daten anzuzeigen.

Auf der Seite Servers (Server) sehen Sie eine Liste aller erkannten Server (Geräte) zusammen mit dem jeweiligen Importnamen. Wenn Sie von derImporte(Importverlauf), indem Sie den Namen des Imports auswählen, der in derNamewerden Sie zu-ServerSeite, auf der ein Filter basierend auf dem Datensatz des ausgewählten Imports angewendet wird. Dann sehen Sie nur Daten, die zu diesem bestimmten Import gehören.

Das Archiv ist im .zip-Format und enthält zwei Dateien; `errors-file` (Fehlerdatei) und `failed-entries-file` (Datei mit den fehlgeschlagenen Einträgen). Die Fehlerdatei enthält eine Liste der Fehlermeldungen zu jeder fehlgeschlagenen Zeile und dem zugehörigen Spaltennamen aus Ihrer Datendatei, deren Import fehlgeschlagen ist. Sie können diese Datei verwenden, um schnell zu identifizieren, wo Probleme aufgetreten sind. Die Datei mit den fehlgeschlagenen Einträgen enthält jede Zeile und die angegebenen fehlgeschlagenen Spalten. Sie können die in der Fehlerdatei angegebenen Korrekturen vornehmen und versuchen, die Datei erneut mit den korrigierten Informationen zu importieren.

AWS CLI Import

Um den Importvorgang mithilfe der AWS CLI starten zu können, muss die AWS CLI zuerst in Ihrer Umgebung installiert werden. Weitere Informationen finden Sie unterInstallieren vonAWS-Befehlszeilenschnittstelleim AWS Command Line InterfaceBenutzerhandbuch.

> **Note**
>
> Wenn Sie noch keine Importvorlage ausgefüllt haben, können Sie die Importvorlage auch aus unserem Amazon S3 S3-Bucket unter herunterladen.https://s3.us-west-2.amazonaws.com/templates-7cffcf56-bd96-4b1c-b45b-a5b42f282e46/import_template.csv

So starten Sie den Datenimport:

1. Öffnen Sie ein Terminalfenster, und geben Sie den folgenden Befehl ein:

```
aws discovery start-import-task --import-url s3://BucketName/ImportFile.csv --
name ImportName
```

2. Dadurch wird Ihre Importaufgabe erstellt und es werden die folgenden Statusinformationen zurückgegeben:

```
{
    "task": {
        "status": "IMPORT_IN_PROGRESS",
        "applicationImportSuccess": 0,
        "serverImportFailure": 0,
        "serverImportSuccess": 0,
        "name": "ImportName",
        "importRequestTime": 1547682819.801,
        "applicationImportFailure": 0,
        "clientRequestToken": "EXAMPLE1-abcd-1234-abcd-EXAMPLE1234",
        "importUrl": "s3://BucketName/ImportFile.csv",
        "importTaskId": "import-task-EXAMPLE1229949eabfEXAMPLE03862c0"
    }
}
```

Verfolgen Ihrer MigrationsHub-Importanforderungen

Sie können den Status Ihrer Migration Hub Hub-Importanfragen über die Konsole überprüfen.AWS CLIoder einer derAWS-SDKs.

Console Tracking

Aus derImporte-Dashboard in der Migration Hub Hub-Konsole finden Sie die folgenden Elemente.

- Name— Der Name der Importanfrage.
- ID importieren— Die eindeutige ID der Importanfrage.
- Zeit des Imports— Datum und Uhrzeit der Erstellung der Importanfrage.
- Status— Der Status der Importanfrage. Dabei kann es sich um einen der folgenden Werte handeln:
  - Importing— Diese Datendatei wird derzeit importiert.
  - Importiert— Die gesamte Datendatei wurde erfolgreich importiert.

  - Mit Fehlern importiert— Ein oder mehrere Datensätze in der Datendatei konnten nicht importiert werden. Wählen Sie zum Umgang mit fehlgeschlagenen Datensätzen Download failed records (Fehlgeschlagene Datensätze herunterladen) für Ihre Importaufgabe, und beheben Sie die Fehler in der .csv-Datei mit fehlgeschlagenen Einträgen. Wiederholen Sie dann den Import.
  - Import ist fehlgeschlagen— Keiner der Datensätze in der Datendatei wurde importiert. Wählen Sie zum Umgang mit fehlgeschlagenen Datensätzen Download failed records (Fehlgeschlagene Datensätze herunterladen) für Ihre Importaufgabe, und beheben Sie die Fehler in der .csv-Datei mit fehlgeschlagenen Einträgen. Wiederholen Sie dann den Import.
- Importierte Datensätze— Die Anzahl der Datensätze in einer bestimmten Datendatei, die erfolgreich importiert wurden.
- Fehlerhafte Aufzeichnungen— Die Anzahl der Datensätze in einer bestimmten Datendatei, die nicht importiert wurden.

CLI Tracking

Sie können den Status Ihrer Importaufgaben mit dem AWS CLI-Befehl `aws discovery describe-import-tasks` überprüfen.

1. Öffnen Sie ein Terminalfenster, und geben Sie den folgenden Befehl ein:

   ```
   aws discovery describe-import-tasks
   ```

2. Dadurch wird eine Liste aller Importaufgaben im JSON-Format zurückgegeben, vollständig mit Status- und weiteren relevanten Informationen. Optional können Sie die Ergebnisse filtern, um eine Teilmenge Ihrer Importaufgaben auszugeben.

Bei der Nachverfolgung Ihrer Importaufgaben kann es vorkommen, dass der ausgegebene `serverImportFailure`-Wert größer als Null ist. Wenn dies der Fall ist, enthielt Ihre Importdatei einen oder mehrere Einträge, die nicht importiert werden konnten. Sie können dies beheben, indem Sie Ihr Archiv fehlgeschlagener Datensätze herunterladen, die darin befindlichen Dateien überprüfen und mit der modifizierten Datei failed-entries.csv eine weitere Importanfrage erstellen.

Nach dem Erstellen der Importaufgabe können Sie weitere Aktionen durchführen, um Ihre Datenmigration zu unterstützen und nachzuverfolgen. Sie können beispielsweise ein Archiv fehlgeschlagener Datensätze für eine bestimmte Anfrage herunterladen. Informationen zur

Verwendung des Archivs fehlgeschlagener Datensätze für die Behebung von Importproblemen, finden Sie unter Fehlerbehebung bei fehlgeschlagenen Datensätzen.

Erkannte Daten anzeigen, exportieren und untersuchen

Sowohl Application Discovery Service Agentless Collector (Agentless Collector) alsAWSDiscovery Agent (Discovery Agent) stellt Systemleistungsdaten basierend auf durchschnittlicher und Spitzenauslastung bereit. Sie können die gesammelten Systemleistungsdaten verwenden, um die Gesamtbetriebskosten (TCO) auf hoher Ebene zu ermitteln. Discovery Agents sammeln detailliertere Daten, einschließlich Zeitreihendaten für Systemleistungsinformationen, eingehende und ausgehende Netzwerkverbindungen und Prozesse, die auf dem Server ausgeführt werden. Sie können mithilfe dieser Daten die Netzwerkabhängigkeiten zwischen Servern besser verstehen und die zugehörigen Server für die Migrationsplanung als Anwendungen gruppieren.

In diesem Abschnitt finden Sie Anweisungen zum Anzeigen und Arbeiten mit Daten, die von Agentless Collector und Discovery Agent sowohl über die Konsole als auch über dasAWS CLI.

Themen

Gesammelte Daten mithilfe der Migration Hub Hub-Konsole anzeigen

Sowohl für den Application Discovery Service Agentless Collector (Agentless Collector) als auch für denAWS Discovery Agent (Discovery Agent) können Sie nach dem Start des Datenerfassungsprozesses die Konsole verwenden, um die gesammelten Daten über Ihre Server und virtuellen Maschinen einzusehen. Die Daten werden etwa 15 Minuten nach Beginn der Datenerfassung in der Konsole angezeigt. Sie können diese Daten auch im CSV-Format anzeigen, indem Sie die gesammelten Daten exportieren, indem Sie API-Aufrufe mit dem durchführenAWS CLI. Auf das Exportieren von gesammelten Daten wird im nächsten Abschnitt, Export collected data, eingegangen.

So zeigen Sie gesammelte Daten über erkannte Server an

1. Klicken Sie im Navigationsbereich der Konsole auf Servers (Server). Die erkannten Server erscheinen in der Serverliste.

2. Um Details der gesammelten Daten anzuzeigen, wählen Sie in der Spalte Server info (Serverinformationen) den Link des Servernamens aus. Auf diese Weise wird ein Bildschirm mit detaillierten Informationen, wie z. B. Systeminformationen, Leistungsmetriken und vieles mehr, angezeigt.

Weitere Informationen zur Verwendung der Konsole zum Anzeigen, Sortieren und Taggen von Servern, die von Ihren Agentless Collectors oder Discovery Agents entdeckt wurden, finden Sie unterAWS Application Discovery ServiceAnleitungen zur Konsole.

Das Datenbank- und Analysedatenerfassungsmodul Agentless Collector lädt die gesammelten Daten in den Amazon S3 S3-Bucket hoch. Sie können die Daten aus diesem Bucket in derAWS DMS-Konsole einsehen.

Um gesammelte Daten über entdeckte Datenbank- und Analyseserver einzusehen

1. Melden Sie sich bei der anAWS Management Console und öffnen Sie dieAWS DMS-Konsole unter https://console.aws.amazon.com/dms/v2/.
2. Wähle Inventar unter Entdecken aus. Die Inventarseite wird geöffnet und zeigt eine Liste der erkannten Datenbank- und Analyseserver an.

Abgleichslogik für entdeckte Server und Anwendungen

AWS Application Discovery Service(Application Discovery Service) verfügt über eine integrierte Abgleichslogik, die ermittelt, wann gefundene Server mit vorhandenen Einträgen übereinstimmen. Wenn diese Logik eine Übereinstimmung findet, werden die Informationen für den bereits vorhandenen erkannten Server mit den neuen Werten aktualisiert.

Diese Abgleichslogik verarbeitet doppelte Server aus mehreren Quellen, darunter den ImportAWS Migration Hub (Migration Hub), Application Discovery Service Agentless Collector (Agentless Collector),AWS Application Discovery Agent (Discovery Agent) und andere Migrationstools. Weitere Informationen zum Migration Hub Hub-Import finden Sie unter Migration Hub Hub-Import.

Wenn ein Server erkannt wird, wird jeder Eintrag anhand vorher importierter Datensätze geprüft, um sicherzustellen, dass der importierte Server nicht bereits vorhanden ist. Wenn keine Übereinstimmung gefunden wird, wird ein neuer Datensatz erstellt und eine neue eindeutige Server-ID zugewiesen. Wenn eine Übereinstimmung gefunden wird, wird ebenfalls ein neuer Eintrag erstellt, diesem wird jedoch dieselbe eindeutige Server-ID zugewiesen wie dem vorhandenen Server. Wenn

Sie diesen Server in der Migration Hub Hub-Konsole anzeigen, finden Sie nur einen eindeutigen Eintrag für den Server.

Server-Attribute für diesen Eintrag werden zusammengeführt, um Attributwerte von einem vorher verfügbaren Datensatz und von dem neu importierten Datensatz anzuzeigen. Wenn mehr als ein Wert für ein Serverattribut aus mehreren Quellen vorliegt, etwa zwei unterschiedliche Werte für `Total RAM` zu einem Server, der mittels Import und vom Discovery Agent erkannt wurde, wird der neueste aktualisierte Wert in dem abgeglichenen Datensatz für den Server gezeigt.

Passende Felder

Die folgenden Felder werden bei der Verwendung von Erkennungstools für den Abgleich von Servern verwendet.

- ExternalId— Dies ist das primäre Feld, das für den Abgleich von Servern verwendet wird. Wenn der Wert in diesem Feld mit einem anderen Wert`ExternalId` in einem anderen Eintrag identisch ist, gleicht Application Discovery Service die beiden Einträge ab, unabhängig davon, ob die anderen Felder übereinstimmen oder nicht.
- IPAddress
- HostName
- MacAddress
- VMWare. MoRefIdund VMWare. vCenterId— Beide Werte müssen mit den entsprechenden Feldern in einem anderen Eintrag identisch sein, damit Application Discovery Service eine Übereinstimmung durchführen kann.

Export collected data

Sowohl für den Application Discovery Service Agentless Collector (Agentless Collector) als auch für denAWS Application Discovery Agent (Discovery Agent) können Sie nach dem Start des Datenerfassungsprozesses die gesammelten Daten über Ihre Server und virtuellen Maschinen exportieren. Diese Daten können entweder durch Interaktion mit der Konsole oder durch API-Aufrufe über die exportiert werdenAWS CLI, je nachdem, welches Discovery-Tool Sie zum Sammeln von Daten verwendet haben.

Anweisungen für beide Methoden sind durch Erweitern der jeweils gewählten Methode verfügbar:

Exportieren Sie die Daten, die für alle Server gesammelt wurden, mithilfe desAWS CLI

Die Daten, die von allen agentenlosen Collectors und Discovery Agents gesammelt wurden, die auf Ihren Hosts und VMs ausgeführt werden, können mithilfe vonAWS Command Line Interface (AWS CLI) in großen Mengen exportiert werden. DerAWS CLI muss in Ihrer Umgebung installiert sein, bevor Sie Daten exportieren können.

So installieren Sie die AWS CLI und exportieren gesammelte Daten

1. Sofern noch nicht geschehen, installieren Sie die AWS CLI entsprechenden dem Typ Ihres Betriebssystems (Windows oder Mac/Linux). Installationsanweisungen finden Sie im AWS Command Line InterfaceBenutzerhandbuch.
2. Öffnen Sie die Eingabeaufforderung (Windows) oder das Terminal (MAC/Linux).
   a. Geben Sie `aws configure` ein und drücken Sie die Eingabetaste.
   b. Geben Sie IhreAWS Zugangsschlüssel-ID und IhrenAWS geheimen Zugriffsschlüssel ein.
   c. Geben Sie als standardmäßigen Regionsnamen `us-west-2` ein.
   d. Geben Sie als Standard-Ausgabeformat `text` ein.
3. Geben Sie den folgenden Befehl ein, um eine Exports-ID zu generieren:

```
aws discovery start-export-task
```

4. Geben Sie unter Verwendung der im vorherigen Schritt erstellten ID den folgenden Befehl ein, um einen S3-URL als Wert für den Parameter `"configurationsDownloadUrl"` zu generieren:

```
aws discovery describe-export-tasks --export-ids <export ID>
```

5. Kopieren Sie den im vorherigen Schritt erstellten URL und fügen Sie ihn in einen Browser ein, um die ZIP-Datei mit den gesammelten Daten der erkannten Server herunterzuladen.

Exportieren Sie die vom Agenten gesammelten Daten mithilfe der Konsole

Das Exportieren von Agentendaten aus der Konsole ist auf einen Agenten beschränkt, wenn Sie sich auf der Detailseite für einen bestimmten Server befinden. Auf der Detailseite finden Sie die Exportaufträge des Servers, die am unteren Bildschirmrand unter Exporte aufgeführt sind. Wenn keine Datensenden Sie können bis zu fünf Exporte von Serverdaten gleichzeitig ausführen.

So exportieren Sie die über einen erkannten Server gesammelten Daten

1. Klicken Sie im Navigationsbereich auf Servers (Server).
2. Wählen Sie in der Spalte Server info (Server-Info) den Server-Link für den Server aus, für den Sie Daten exportieren möchten.
3. Wählen Sie im Bereich Exports (Exporte) unten auf dem Bildschirm Export server details (Serverdetails exportieren) aus.
4. Machen Sie für Export server details (Serverdetails exportieren) Angaben unter Start date (Startdatum) und Time (Uhrzeit).

   > **Note**
   >
   > Die Startzeit darf nicht mehr als 72 Stunden vor der aktuellen Uhrzeit liegen.

5. Wählen Sie Export, um den Auftrag zu starten. Der anfängliche Status ist In-progress (In Bearbeitung). Um den Status zu aktualisieren, klicken Sie auf das Aktualisierungssymbol für den Bereich Exports (Exporte).
6. Wenn der Exportauftrag abgeschlossen ist, klicken Sie auf Download (Herunterladen) und speichern Sie die ZIP-Datei.
7. Entpacken Sie die gespeicherte Zipdatei. Eine Reihe von CSV-Dateien enthält die Exportdaten.

   Sie können die CSV-Dateien in Microsoft Excel öffnen und die exportierten Serverdaten überprüfen.

   Unter den Dateien finden Sie eine JSON-Datei mit Daten über den Exportauftrag und seine Ergebnisse.

> **Note**
>
> Informationen zum Generieren und Exportieren von Amazon Elastic Compute Cloud (Amazon EC2) -Instance-Empfehlungen in derAWS Migration Hub Konsole finden Sie unter Amazon EC2-Instance-Empfehlungen im AWS Migration HubBenutzerhandbuch.

Datenauflister in Amazon Athena

Mit der Datenexploration in Amazon Athena können Sie die Daten, die von Discovery Agents von allen erkannten lokalen Servern gesammelt wurden, an einem Ort analysieren. Sobald die Datenexploration in Amazon Athena über die Migration Hub Hub-Konsole aktiviert ist (oder mithilfe der StartContinousExport API) und die Datenerfassung für Agenten aktiviert ist, werden Daten, die von Agenten gesammelt werden, automatisch in regelmäßigen Abständen in Ihrem S3-Bucket gespeichert.

Sie können dann Amazon Athena besuchen, um vordefinierte Abfragen auszuführen, um die Systemleistung der Zeitreihen für jeden Server, die Art der Prozesse, die auf jedem Server ausgeführt werden, und die Netzwerkabhängigkeiten zwischen verschiedenen Servern zu analysieren. Darüber hinaus können Sie mithilfe von Amazon Athena Ihre eigenen benutzerdefinierten Abfragen schreiben, zusätzliche vorhandene Datenquellen wie CMDB-Exporte (Configuration Management Database) hochladen und die erkannten Server den tatsächlichen Geschäftsanwendungen zuordnen. Sie können die Athena-Datenbank auch mit Amazon integrieren QuickSight um die Abfrageausgaben zu visualisieren und zusätzliche Analysen durchzuführen

Schritte

1. Aktivierung der Datenexploration in Amazon Athena
2. Arbeiten mit der Datenexploration in Amazon Athena

Aktivierung der Datenexploration in Amazon Athena

Die Datenexploration in Amazon Athena wird aktiviert, indem Sie Continuous Export über die Migration Hub Hub-Konsole oder einen API-Aufruf vomAWS CLI. Sie müssen die Datenexploration aktivieren, bevor Sie Ihre entdeckten Daten in Amazon Athena sehen und untersuchen können.

Wenn Sie Continuous Export aktivieren, wird die serviceverknüpfte RolleAWSServiceRoleForApplicationDiscoveryServiceContinuousExportwird automatisch von Ihrem Konto verwendet. Weitere Informationen zu dieser serviceverknüpften Rolle finden Sie unter Berechtigungen von servicegebundenen Rollen für Application Discovery Service.

Die folgenden Anweisungen zeigen, wie Sie die Datenexploration in Amazon Athena mithilfe der Konsole und derAWS CLI.

Enable with the console

Die Datenexploration in Amazon Athena wird dadurch aktiviert, dass der kontinuierliche Export implizit aktiviert ist, wenn Sie „Datenerfassung starten“ wählen oder auf den Schalter mit der Bezeichnung „Datenexploration in Amazon Athena“ auf derDatenauflisterSeite der Migration Hub Hub-Konsole.

So aktivieren Sie die Datenexploration in Amazon Athena über die Konsole

1. Klicken Sie im Navigationsbereich auf Data Collectors (Datensammler).
2. Wählen Sie die Registerkarte Agents (Agenten).
3. WählenDatenauflister starten, oder wenn Sie die Datenerfassung bereits aktiviert haben, klicken Sie aufDatenauflister in Amazon Athenaumschalten.
4. Klicken Sie in dem im vorherigen Schritt erstellten Dialogfeld auf das Kontrollkästchen, um sich mit den anfallenden Gebühren einverstanden zu erklären. Klicken Sie dann auf Continue (Fortfahren) oder Enable (Aktivieren).

> **Note**
>
> Ihre Agenten laufen jetzt im Modus „Kontinuierlicher Export“, der es Ihnen ermöglicht, Ihre erkannten Daten in Amazon Athena anzuzeigen und mit ihnen zu arbeiten. Wenn dies zum ersten Mal aktiviert ist, kann es bis zu 30 Minuten dauern, bis Ihre Daten in Amazon Athena angezeigt werden.

Enable with the AWS CLI

Die Datenexploration in Amazon Athena wird dadurch ermöglicht, dass Continuous Export explizit über einen API-Aufruf vomAWS CLI. Hierzu muss die AWS CLI zunächst in Ihrer Umgebung installiert werden.

So installieren Sie dasAWS CLIund ermöglichen Sie die Datenexploration in Amazon Athena

1. Installieren Sie die AWS CLI für Ihr Betriebssystem (Linux, macOS oder Windows). Siehe dasAWS Command Line InterfaceBenutzerhandbuchfür Anweisungen.
2. Öffnen Sie die Eingabeaufforderung (Windows) oder das Terminal (Linux oder macOS).
   a. Geben Sie `aws configure` ein und drücken Sie die Eingabetaste.

b. Gib deineAWSZugriffsschlüssel-ID undAWSGeheimer Zugriffsschlüssel.

c. Geben Sie als standardmäßigen Regionsnamen `us-west-2` ein.

d. Geben Sie als Standard-Ausgabeformat `text` ein.

3. Geben Sie den folgenden Befehl ein:

```
aws discovery start-continuous-export
```

> **Note**
>
> Ihre Agenten laufen jetzt im Modus „Kontinuierlicher Export“, der es Ihnen ermöglicht, Ihre erkannten Daten in Amazon Athena anzuzeigen und mit ihnen zu arbeiten. Wenn dies zum ersten Mal aktiviert ist, kann es bis zu 30 Minuten dauern, bis Ihre Daten in Amazon Athena angezeigt werden.

Arbeiten mit der Datenexploration in Amazon Athena

Nachdem Sie die Datenexploration in Amazon Athena aktiviert haben, können Sie mit der Untersuchung und Bearbeitung detaillierter aktueller Daten beginnen, die von Ihren Agenten ermittelt wurden, indem Sie die Daten direkt in Athena abfragen. Sie können die Daten verwenden, um Tabellen zu generieren, eine Kostenanalyse auszuführen, die Abfrage zum Erstellen eines Diagramms der Netzwerkabhängigkeiten auf ein Visualisierungsprogramm portieren und vieles mehr.

In den Themen in diesem Abschnitt wird beschrieben, wie Sie mit Ihren Daten in Athena arbeiten können, um die Migration Ihrer lokalen Umgebung zu bewerten und zu planenAWS.

Themen

- Erkundung von Daten direkt in Amazon Athena
- Visualisieren von Amazon Athena Athena-Daten
- Vordefinierte Abfragen zur Verwendung in Athena

Erkundung von Daten direkt in Amazon Athena

Im Folgenden wird beschrieben, wie Sie Ihre Agentendaten direkt in der Athena-Konsole durchsuchen. Wenn Sie keine Daten in Athena haben oder die Datenexploration in Amazon Athena

nicht aktiviert haben, werden Sie in einem Dialogfeld aufgefordert, die Datenexploration in Amazon Athena zu aktivieren, wie unterAktivierung der Datenexploration in Amazon Athena.

So untersuchen Sie von Agenten entdeckte Daten direkt in Athena

1. Wählen Sie in der AWS Migration Hub-Konsole im Navigationsbereich die Option Servers (Server) aus.
2. Um die Amazon Athena Athena-Konsole zu öffnen, wählen SieErkunden Sie Daten in Amazon Athena.
3. Prüfen Sie auf der Seite Query Editor (Abfrage-Editor) im Navigationsbereich unter Database (Datenbank), ob application_discovery_service_database ausgewählt ist.

   > **Note**
   >
   > In Tables (Tabellen) stellen die folgenden Tabellen die nach Agenten gruppierten Datensätze dar.
   >
   > - os_info_agent
   > - network_interface_agent
   > - sys_performance_agent
   > - processes_agent
   > - inbound_connection_agent
   > - outbound_connection_agent
   > - id_mapping_agent

4. Fragen Sie die Daten in der Amazon Athena Athena-Konsole ab, indem Sie SQL-Abfragen im Athena Query Editor schreiben und ausführen. Beispielsweise können Sie die folgende Abfrage verwenden, um alle erkannten Server-IP-Adressen anzuzeigen.

   ```
   SELECT * FROM network_interface_agent;
   ```

   Weitere Beispiele für Abfragen finden Sie unter Vordefinierte Abfragen zur Verwendung in Athena.

Visualisieren von Amazon Athena Athena-Daten

Um Ihre Daten zu visualisieren, kann eine Abfrage an ein Visualisierungsprogramm wie Amazon portiert werden. QuickSight oder andere Open-Source-Visualisierungstools wie Cytoscape, yEd oder Gelphi. Verwenden Sie diese Tools zum Rendern von Netzwerkdiagrammen, zusammenfassenden Diagrammen und anderen grafischen Darstellungen. Wenn diese Methode verwendet wird, stellen Sie über das Visualisierungsprogramm eine Verbindung zu Athena her, sodass es auf Ihre gesammelten Daten als Quelle für die Erstellung der Visualisierung zugreifen kann.

So visualisieren Sie Ihre Amazon Athena Athena-Daten mit Amazon QuickSight

1. Melden Sie sich beiAmazon QuickSight.
2. Wählen Sie Connect to another data source or upload a file (Mit einer anderen Datenquelle verbinden oder eine Datei hochladen).
3. WählenAthena. DieNeue Athena-Datenquellewird ein Dialogfeld angezeigt.
4. Geben Sie einen Namen in das Feld Data source name (Datenquellennamen) ein.
5. Klicken Sie auf Create data source.
6. Select-EINgents-servers-os-Tabelle in derSelect-Tabelleund wählen SieSelect.
7. Wählen Sie im Dialogfeld Finish data set creation (Datensatzerstellung fertigstellen) die Option Import to SPICE for quicker analytics (Für schnellere Analysen in SPICE importieren) aus. Wählen Sie anschließend Visualize (Visualisieren) aus.

   Ihre Visualisierung wird gerendert.

Vordefinierte Abfragen zur Verwendung in Athena

Dieser Abschnitt enthält eine Reihe von vordefinierten Abfragen, die typische Anwendungsfälle wie die Analyse der Gesamtbetriebskosten und die Netzwerk-Visualisierung ausführen. Sie können diese Abfragen unverändert verwenden oder sie Ihren Anforderungen entsprechend anpassen.

So verwenden Sie eine vordefinierte Abfrage

1. Wählen Sie in der AWS Migration Hub-Konsole im Navigationsbereich die Option Servers (Server) aus.
2. Um die Amazon Athena Athena-Konsole zu öffnen, wählen SieErkunden Sie Daten in Amazon Athena.

3. Prüfen Sie auf der Seite Query Editor (Abfrage-Editor) im Navigationsbereich unter Database (Datenbank), ob application_discovery_service_database ausgewählt ist.
4. Wählen Sie das Pluszeichen (+) im Abfrage-Editor aus, um eine Registerkarte für eine neue Abfrage zu erstellen.
5. Kopieren Sie eine der Abfragen aus Vordefinierte Abfragen.
6. Fügen Sie die Abfrage in den Abfragebereich der neuen Abfrage-Registerkarte ein, die Sie gerade erstellt haben.
7. Klicken Sie auf Run Query (Abfrage ausführen).

Vordefinierte Abfragen

Wählen Sie einen Titel aus, um Informationen über die Abfrage anzuzeigen.

Abrufen von IP-Adressen und Hostnamen für Server

Diese Ansichts-Hilfsfunktion ruft die IP-Adressen und Hostnamen für einen bestimmten Server ab. Sie können diese Ansicht bei anderen Abfragen verwenden. Weitere Informationen, wie Sie eine Ansicht erstellen können, finden Sie unterCREATE VIEWin derAmazon-Athena-Benutzerhandbuch.

```
CREATE OR REPLACE VIEW hostname_ip_helper AS
SELECT DISTINCT
  "os"."host_name"
, "nic"."agent_id"
, "nic"."ip_address"
FROM
  os_info_agent os
, network_interface_agent nic
WHERE ("os"."agent_id" = "nic"."agent_id");
```

Identifizieren von Servern mit oder ohne Agenten

Diese Abfrage kann bei der Datenvalidierung helfen. Wenn Sie auf einer Reihe von Servern in Ihrem Netzwerk Agenten bereitgestellt haben, können Sie diese Abfrage verwenden, um zu erfahren, ob es weitere Server in Ihrem Netzwerk ohne Agenten gibt. In dieser Abfrage wird der ein- und ausgehende Netzwerkdatenverkehr untersucht und der Datenverkehr ausschließlich nach privaten IP-Adressen gefiltert. Dies sind IP-Adressen, die mit 192, 10 oder 172 beginnen.

```
SELECT DISTINCT "destination_ip" "IP Address" ,
         (CASE
```

```
    WHEN (
    (SELECT "count"(*)
    FROM network_interface_agent
    WHERE ("ip_address" = "destination_ip") ) = 0) THEN
        'no'
        WHEN (
        (SELECT "count"(*)
        FROM network_interface_agent
        WHERE ("ip_address" = "destination_ip") ) > 0) THEN
            'yes' END) "agent_running"
    FROM outbound_connection_agent
WHERE ((("destination_ip" LIKE '192.%')
        OR ("destination_ip" LIKE '10.%'))
        OR ("destination_ip" LIKE '172.%'))
UNION
SELECT DISTINCT "source_ip" "IP ADDRESS" ,
         (CASE
    WHEN (
    (SELECT "count"(*)
    FROM network_interface_agent
    WHERE ("ip_address" = "source_ip") ) = 0) THEN
        'no'
        WHEN (
        (SELECT "count"(*)
        FROM network_interface_agent
        WHERE ("ip_address" = "source_ip") ) > 0) THEN
            'yes' END) "agent_running"
    FROM inbound_connection_agent
WHERE ((("source_ip" LIKE '192.%')
        OR ("source_ip" LIKE '10.%'))
        OR ("source_ip" LIKE '172.%'));
```

Analysieren Sie Systemleistungsdaten für Server mit Agenten

Mit dieser Abfrage können Sie die Systemleistung und Nutzungsmusterdaten für Ihre lokalen Server mit installierten Agenten analysieren. Die Abfrage kombiniert die Tabellen `system_performance_agent` und `os_info_agent`, um den Hostnamen für die einzelnen Server zu identifizieren. Diese Abfrage gibt die Zeitreihen-Nutzungsdaten (in 15-Minuten-Intervallen) für alle Server zurück, auf denen Agenten ausgeführt werden.

```
SELECT "OS"."os_name" "OS Name" ,
    "OS"."os_version" "OS Version" ,
    "OS"."host_name" "Host Name" ,
```

```
    "SP"."agent_id" ,
    "SP"."total_num_cores" "Number of Cores" ,
    "SP"."total_num_cpus" "Number of CPU" ,
    "SP"."total_cpu_usage_pct" "CPU Percentage" ,
    "SP"."total_disk_size_in_gb" "Total Storage (GB)" ,
    "SP"."total_disk_free_size_in_gb" "Free Storage (GB)" ,
    ("SP"."total_disk_size_in_gb" - "SP"."total_disk_free_size_in_gb") "Used
 Storage" ,
    "SP"."total_ram_in_mb" "Total RAM (MB)" ,
    ("SP"."total_ram_in_mb" - "SP"."free_ram_in_mb") "Used RAM (MB)" ,
    "SP"."free_ram_in_mb" "Free RAM (MB)" ,
    "SP"."total_disk_read_ops_per_sec" "Disk Read IOPS" ,
    "SP"."total_disk_bytes_written_per_sec_in_kbps" "Disk Write IOPS" ,
    "SP"."total_network_bytes_read_per_sec_in_kbps" "Network Reads (kbps)" ,
    "SP"."total_network_bytes_written_per_sec_in_kbps" "Network Write (kbps)"
FROM "sys_performance_agent" "SP" , "OS_INFO_agent" "OS"
WHERE ("SP"."agent_id" = "OS"."agent_id") limit 10;
```

Verfolgen Sie die ausgehende Kommunikation zwischen Servern basierend auf Portnummer und Prozessdetails

Über diese Abfrage werden die Details zum ausgehenden Datenverkehr für jeden Dienst abgerufen, zusammen mit der Portnummer und den Prozessdetails.

Bevor Sie die Abfrage ausführen, müssen Sie, falls noch nicht geschehen, die `iana_service_ports_import`-Tabelle erstellen, die die von der IANA heruntergeladene Datenbank des IANA-Portregisters enthält. Weitere Informationen zum Erstellen dieser Tabelle finden Sie unter Erstellen der IANA-Portregistrierungs-.

Nach der Erstellung der Tabelle `iana_service_ports_import` erstellen Sie zwei Ansichtshilfsfunktionen zur Verfolgung des ausgehenden Datenverkehrs. Weitere Informationen, wie Sie eine Ansicht erstellen können, finden Sie unterCREATE VIEWin derAmazon-Athena-Benutzerhandbuch.

So erstellen Sie Hilfsfunktionen für die Nachverfolgung des ausgehenden Datenverkehrs

1. Öffnen Sie die Athena-Konsole unter https://console.aws.amazon.com/athena/.
2. Erstellen der`valid_outbound_ips_helper`view, mit der folgenden Hilfsfunktion, die alle unterschiedlichen ausgehenden Ziel-IP-Adressen auflistet.

```
CREATE OR REPLACE VIEW valid_outbound_ips_helper AS
```

```
SELECT DISTINCT "destination_ip"
FROM outbound_connection_agent;
```

3. Erstellen Sie die Ansicht `outbound_query_helper` über die folgende Hilfsfunktion, die die Häufigkeit der Kommunikation für den ausgehenden Datenverkehr ermittelt.

```
CREATE OR REPLACE VIEW outbound_query_helper AS
SELECT "agent_id" ,
         "source_ip" ,
         "destination_ip" ,
         "destination_port" ,
         "agent_assigned_process_id" ,
         "count"(*) "frequency"
FROM outbound_connection_agent
WHERE (("ip_version" = 'IPv4')
        AND ("destination_ip" IN
    (SELECT *
    FROM valid_outbound_ips_helper )))
GROUP BY  "agent_id", "source_ip", "destination_ip", "destination_port",
 "agent_assigned_process_id";
```

4. Nachdem Sie die `iana_service_ports_import`-Tabelle und Ihre zwei Hilfsfunktionen erstellt haben, können Sie die folgende Abfrage ausführen, um die Details zum ausgehenden Datenverkehr für die jeweiligen Dienste in Verbindung mit der Portnummer und den Prozessdetails abzurufen.

```
SELECT hip1.host_name "Source Host Name",
         outbound_connections_results0.source_ip "Source IP Address",
         hip2.host_name "Destination Host Name",
         outbound_connections_results0.destination_ip "Destination IP Address",
         outbound_connections_results0.frequency "Connection Frequency",
         outbound_connections_results0.destination_port "Destination Communication
 Port",
         outbound_connections_results0.servicename "Process Service Name",
         outbound_connections_results0.description "Process Service Description"
FROM
    (SELECT DISTINCT o.source_ip,
         o.destination_ip,
         o.frequency,
         o.destination_port,
         ianap.servicename,
         ianap.description
    FROM outbound_query_helper o, iana_service_ports_import ianap
```

```
    WHERE o.destination_port = TRY_CAST(ianap.portnumber AS integer)) AS
 outbound_connections_results0 LEFT OUTER
JOIN hostname_ip_helper hip1
    ON outbound_connections_results0.source_ip = hip1.ip_address LEFT OUTER
JOIN hostname_ip_helper hip2
    ON outbound_connections_results0.destination_ip = hip2.ip_address
```

Verfolgen Sie die eingehende Kommunikation zwischen Servern basierend auf Portnummer und Prozessdetails

Über diese Abfrage werden die Informationen über den ausgehenden Datenverkehr für jeden Dienst abgerufen, zusammen mit der Portnummer und den Prozessdetails.

Bevor Sie diese Abfrage ausführen, müssen Sie, falls noch nicht geschehen, die `iana_service_ports_import`-Tabelle erstellen, die die von der IANA heruntergeladene Datenbank des IANA-Portregisters enthält. Weitere Informationen zum Erstellen dieser Tabelle finden Sie unter Erstellen der IANA-Portregistrierungs-.

Nach der Erstellung der Tabelle `iana_service_ports_import` erstellen Sie zwei Ansichtshilfsfunktionen zur Verfolgung des eingehenden Datenverkehrs. Weitere Informationen, wie Sie eine Ansicht erstellen können, finden Sie unterCREATE VIEWin derAmazon-Athena-Benutzerhandbuch.

So erstellen Sie Hilfsfunktionen für die Nachverfolgung des Imports

1. Öffnen Sie die Athena-Konsole unter https://console.aws.amazon.com/athena/.
2. Erstellen Sie die Ansicht `valid_inbound_ips_helper` über die folgende Hilfsfunktion, die alle unterschiedlichen IP-Quelladressen für den eingehenden Datenverkehr auflistet.

   ```
   CREATE OR REPLACE VIEW valid_inbound_ips_helper AS
   SELECT DISTINCT "source_ip"
   FROM inbound_connection_agent;
   ```

3. Erstellen Sie die Ansicht `inbound_query_helper` über die folgende Hilfsfunktion, die die Häufigkeit der Kommunikation für den eingehenden Datenverkehr ermittelt.

   ```
   CREATE OR REPLACE VIEW inbound_query_helper AS
   SELECT "agent_id" ,
            "source_ip" ,
            "destination_ip" ,
   ```

```
         "destination_port" ,
         "agent_assigned_process_id" ,
         "count"(*) "frequency"
FROM inbound_connection_agent
WHERE (("ip_version" = 'IPv4')
        AND ("source_ip" IN
    (SELECT *
    FROM valid_inbound_ips_helper )))
GROUP BY  "agent_id", "source_ip", "destination_ip", "destination_port",
 "agent_assigned_process_id";
```

4. Nachdem Sie die `iana_service_ports_import`-Tabelle und Ihre zwei Hilfsfunktionen erstellt haben, können Sie die folgende Abfrage ausführen, um die Details zum eingehenden Datenverkehr für die jeweiligen Dienste in Verbindung mit der Portnummer und den Prozessdetails abzurufen.

```
SELECT hip1.host_name "Source Host Name",
         inbound_connections_results0.source_ip "Source IP Address",
         hip2.host_name "Destination Host Name",
         inbound_connections_results0.destination_ip "Destination IP Address",
         inbound_connections_results0.frequency "Connection Frequency",
         inbound_connections_results0.destination_port "Destination Communication
 Port",
         inbound_connections_results0.servicename "Process Service Name",
         inbound_connections_results0.description "Process Service Description"
FROM
    (SELECT DISTINCT i.source_ip,
         i.destination_ip,
         i.frequency,
         i.destination_port,
         ianap.servicename,
         ianap.description
    FROM inbound_query_helper i, iana_service_ports_import ianap
    WHERE i.destination_port = TRY_CAST(ianap.portnumber AS integer)) AS
 inbound_connections_results0 LEFT OUTER
JOIN hostname_ip_helper hip1
    ON inbound_connections_results0.source_ip = hip1.ip_address LEFT OUTER
JOIN hostname_ip_helper hip2
    ON inbound_connections_results0.destination_ip = hip2.ip_address
```

Identifizieren Sie laufende Software anhand der Portnummer

Mit dieser Abfrage wird die ausgeführte Software basierend auf den Portnummern identifiziert.

Bevor Sie diese Abfrage ausführen, müssen Sie, falls noch nicht geschehen, die `iana_service_ports_import`-Tabelle erstellen, die die von der IANA heruntergeladene Datenbank des IANA-Portregisters enthält. Weitere Informationen zum Erstellen dieser Tabelle finden Sie unter Erstellen der IANA-Portregistrierungs-.

Mit der folgenden Abfrage können Sie die ausgeführte Software basierend auf Portnummern identifizieren.

```
SELECT o.host_name "Host Name",
       ianap.servicename "Service",
       ianap.description "Description",
       con.destination_port,
       con.cnt_dest_port "Destination Port Count"
FROM   (SELECT agent_id,
               destination_ip,
               destination_port,
               Count(destination_port) cnt_dest_port
        FROM   inbound_connection_agent
        GROUP  BY agent_id,
                  destination_ip,
                  destination_port) con,
       (SELECT agent_id,
               host_name,
               Max("timestamp")
        FROM   os_info_agent
        GROUP  BY agent_id,
                  host_name) o,
       iana_service_ports_import ianap
WHERE  ianap.transportprotocol = 'tcp'
       AND con.destination_ip NOT LIKE '172%'
       AND con.destination_port = ianap.portnumber
       AND con.agent_id = o.agent_id
ORDER BY cnt_dest_port DESC;
```

Erstellen der IANA-Portregistrierungs-

Für einige der vordefinierten Abfragen ist eine Tabelle namens `iana_service_ports_import` erforderlich, die von der IANA (Internet Assigned Numbers Authority) heruntergeladene Informationen enthält.

So erstellen Sie die iana_service_ports_import-Tabelle

1. Laden Sie die IANA Portregister-Datenbank-CSV-Datei vom Service Name and Transport Protocol Port Number Registry auf iana.org herunter.
2. Laden Sie die Datei in Amazon S3 hoch. Weitere Informationen finden Sie unter Wie lade ich Dateien und Ordner in einen S3-Bucket hoch?.
3. Erstellen einer neuen Tabelle in Athena mit dem Name`iana_service_ports_import`. Anweisungen finden Sie unterErstellen einer Tabellein derAmazon-Athena-Benutzerhandbuch. Im folgenden Beispiel müssen Sie `my_bucket_name` durch den Namen des S3-Buckets ersetzen, in den Sie die CSV-Datei im vorherigen Schritt hochgeladen haben.

```
CREATE EXTERNAL TABLE IF NOT EXISTS iana_service_ports_import (
         ServiceName STRING,
         PortNumber INT,
         TransportProtocol STRING,
         Description STRING,
         Assignee STRING,
         Contact STRING,
         RegistrationDate STRING,
         ModificationDate STRING,
         Reference STRING,
         ServiceCode STRING,
         UnauthorizedUseReported STRING,
         AssignmentNotes STRING
)
ROW FORMAT SERDE 'org.apache.hadoop.hive.serde2.lazy.LazySimpleSerDe'
WITH SERDEPROPERTIES (
  'serialization.format' = ',',
  'quoteChar' = '"',
  'field.delim' = ','
) LOCATION 's3://my_bucket_name/'
TBLPROPERTIES ('has_encrypted_data'='false',"skip.header.line.count"="1");
```

AWS Application Discovery ServiceAnleitungen zur Konsole

AWS Application Discovery Service(Application Discovery Service) ist integriert inAWS Migration Hub(Migration Hub) und Kunden können ihre Datensammler, Server und Anwendungen in Migration Hub anzeigen und verwalten. Wenn Sie die Application Discovery Service Service-Konsole verwenden, werden Sie zur Migration Hub Hub-Konsole umgeleitet. Die Arbeit mit der Migration Hub Hub-Konsole erfordert keine zusätzlichen Schritte oder Einstellungen von Ihrer Seite.

In diesem Abschnitt erfahren Sie, wie Sie Application Discovery Service Agentless Collector (Agentless Collector) verwalten und überwachenAWSApplication Discovery Agent (Discovery Agent), der die Konsole verwendet.

Themen

Haupt-Dashboard

Um das Haupt-Dashboard anzuzeigen, wählen SieDashboardausAWS Migration HubNavigationsbereich der (Migration Hub) -Konsole. Im Haupt-Dashboard von Migration Hub können Sie allgemeine Statistiken zu Servern, Anwendungen und Datensammelpunkten wie Application Discovery Service Agentless Collector (Agentless Collector) undAWSApplication Discovery Agent (Discovery Agent).

Haupt-Dashboard

Das Haupt-Dashboard sammelt Daten aus den Dashboards Discover (Erkennen) und Migrate (Migrieren) an einem zentralen Ort. Es verfügt über vier Status- und Informationsbereiche und eine Liste von Links, um schnellen Zugriff zu ermöglichen. Über die Bereiche erhalten Sie eine Zusammenfassung des Status Ihres zuletzt aktualisierten Anwendungen. Außerdem können Sie schnell auf jede Ihrer Anwendungen zugreifen, einen Überblick über Anwendungen mit unterschiedlichem Status erhalten und den Fortschritt der Migration im Laufe der Zeit verfolgen.

Um das Haupt-Dashboard anzuzeigen, wählen SieDashboardim Navigationsbereich, der sich auf der linken Seite der Homepage der Migration Hub Hub--Konsole befindet.

Tools zur Datensammlung

Application Discovery Service Agentless Collector (Agentless Collector)AWSApplication Discovery Agent (Discovery Agent) sind die Datenerfassungstools, dieAWS Application Discovery Service(Application Discovery Service) unterstützt Sie bei der Erkennung Ihrer vorhandenen Infrastruktur. In den folgenden Themen wird beschrieben, wie Sie diese Tools zur Erfassung von Ermittlungsdaten herunterladen und bereitstellen.Erste Schritte mit Agentless CollectorundAWS Agent zur Anwendungserkennung.

Diese Datenerfassungstools speichern ihre Daten im Repository des Application Discovery Service und stellen Details zu jedem Server und den auf ihnen ausgeführten Prozessen bereit. Wenn eines dieser Tools bereitgestellt wird, können Sie die gesammelten Daten starten, beenden und anzeigenAWS Migration Hub(Migration Hub) -Konsole.

Themen

Datensammler starten und stoppen

Nach demAWSApplication Discovery Agent (Discovery Agent) wird bereitgestellt. Sie können den Datenerfassungsprozess auf demDatenauflisterSeite desAWS Migration Hub(Migration Hub) -Konsole.

So starten oder beenden Sie die Tools zur Datensammlung

1. Verwenden IhrerAWS-Konto an, melden Sie sich beiAWS Management Consoleund öffnen Sie die Migration Hub Hub-Konsole unterhttps://console.aws.amazon.com/migrationhub/.
2. Im Navigationsbereich der Migration Hub Hub-Konsole unterEntdecken, wählenDatenauflister.
3. Wählen Sie die Registerkarte Agents (Agenten).
4. Aktivieren Sie das Kontrollkästchen des Sammlungstools, das Sie starten oder beenden möchten.
5. Wählen Sie Start data collection (Beginnen der Datensammlung) oder Stop data collection (Beenden der Datensammlung).

Datensammler anzeigen und sortieren

Wenn Sie viele Datensammelpunkte bereitgestellt haben, können Sie die angezeigte Liste der bereitgestellten Collectors auf derDatenauflisterSeite der -Konsole. Sie sortieren die Liste, indem Sie Filter in der Suchleiste an. Sie können die meisten in der Liste Data Collectors (Datensammler) angegebenen Kriterien suchen und filtern.

In der folgenden Tabelle sind die Suchkriterien aufgeführt, für die Sie verwenden könnenAgenten, einschließlich Operatoren, Werten und einer Definition der Werte.

Suchkriterium	Operator	Wert: Definition
Kundendienstmitarbeiter-ID	==	Jede Agenten-ID, die aus der vorab ausgefüllten Liste ausgewählt wurde, aus der ein Sammlungstool installiert wurde.
Hostname	== !=	Für Agenten ein beliebige r Host-Namen aus der vorausgefüllten Liste von Hosts, auf denen ein Agent installiert ist.
Sammlungsstatus	== !=	Gestoppen: Daten werden gesammelt und an Application Discovery Service gesendet Geplanter Start: Die Datensammlung soll planmäßig starten. Die Daten werden beim nächsten Ping an den Application Discovery Service gesendet und der Status ändert sich inGestart. Gestoppen: Es werden keine Daten gesammelt oder an

Suchkriterium	Operator	Wert: Definition
		Application Discovery Service gesendet. Angehaltener Anhalten Die Datenerfassung wird planmäßig beendet. Beim nächsten Ping werden keine Daten mehr an den Application Discovery Service gesendet und der Status ändert sich inAngehalten.

Suchkriterium	Operator	Wert: Definition
Integrität	== !=	fehlerfrei: Die Datenerfassung ist nicht aktiviert. Das Tool funktioniert normal. fehlerfrei: Das Tool befindet sich in einem Fehlerstatus. Es werden keine Daten gesammelt oder gemeldet. Unbekannt: Seit über einer Stunde wurde keine Verbindung hergestellt. Herunterfahren: Das Tool hat zuletzt das „Herunterfahren“ aufgrund eines Herunterfahrens eines Systems, eines Dienstes oder eines Daemons gemeldet. Wenn ein Neustart stattfand oder ein Tool aktualisiert wurde, ändert sich der Status beim ersten Meldezyklus in einen anderen Status. Ausführen: Die Datenerfassung ist aktiviert. Das Tool funktioniert normal.
IP-Adresse	== !=	Eine beliebige IP-Adresse aus der vorausgefüllten Liste, an der ein Sammlungstool installiert ist.

In der folgenden Tabelle sind die Suchkriterien aufgeführt, für die Sie verwenden könnenAgentenauflister, einschließlich Operatoren, Werten und einer Definition der Werte.

Suchkriterium	Operator	Wert: Definition
ID	==	Jede agentenlose Collector-ID, die aus der vorab ausgefüllten Liste ausgewählt wurde, aus der ein Sammlungstool installiert wurde
Hostname	== !=	Bei agentenlosen Collectors ist dies jeder Hostname, der aus der vorab ausgefüllten Liste der Hosts ausgewählt wurde, auf denen ein agentenloser Collector
Status	== !=	Daten auflister: Die Datenerfassung ist aktiviert. Das Tool funktioniert normal. Bereit zur Konfiguration — Die Datenerfassung ist nicht aktiviert. Das Tool funktioniert normal. Erfordert Aufmerksamkeit - Das Tool befindet sich in einem fehlerhaften Zustand und muss beachtet werden. Unbekannt: Seit über einer Stunde wurde keine Verbindung hergestellt. Herunterfahren: Das Tool hat zuletzt das „Herunterfahren“ aufgrund eines Herunterf

Suchkriterium	Operator	Wert: Definition
		ahrens eines Systems, eines Dienstes oder eines Daemons gemeldet. Wenn ein Neustart stattfand oder ein Tool aktualisiert wurde, ändert sich der Status beim ersten Meldezyklus in einen anderen Status.
IP-Adresse	== !=	Eine beliebige IP-Adresse aus der vorausgefüllten Liste, an der ein Sammlungstool installiert ist.

So sortieren Sie Datensammler durch Anwenden von Suchfiltern

1. Verwenden IhrerAWS-Konto an, melden Sie sich beiAWS Management Consoleund öffnen Sie die Migration Hub Hub-Konsole unterhttps://console.aws.amazon.com/migrationhub/.
2. Im Navigationsbereich der Migration Hub Hub-Konsole unterEntdecken, wählenDatenauflister.
3. Wählen Sie entwederAgentenauflisteroderAgentenTabulator.
4. Klicken Sie auf die Suchleiste und wählen Sie ein Suchkriterium aus der Liste aus.
5. Wählen Sie einen Operator aus der Liste aus.
6. Wählen Sie einen Wert aus der Liste aus.

Serverdaten anzeigen, exportieren und untersuchen

Die Seite Servers (Server) enthält Daten über die Systemkonfiguration und Leistung zu jeder Server-Instance, die den Datensammlungstools bekannt ist. Sie können Serverinformationen anzeigen, Servern mithilfe von Filtern sortieren, Servern mit Schlüssel-Wert-Paaren markieren und detaillierte Server- und Systeminformationen exportieren.

Themen

- Anzeigen und Sortieren von Servern

- Markieren von Servern
- Exportieren von Serverdaten
- Datenauflister in Athena
- Anwendungen

Anzeigen und Sortieren von Servern

Sie können Informationen zu den Servern anzeigen, die von den Datensammelungstools erkannt werden, und die Server mithilfe von Filtern sortieren.

Server anzeigen

Sie können eine allgemeine Ansicht und eine detaillierte Ansicht der Server erhalten, die mit den Datensammlungstools erkannt werden.

So zeigen Sie erkannte Server an

1. Verwenden IhrerAWS-Konto an, melden Sie sich beiAWS Management Consoleund öffnen Sie die Migration Hub Hub-Konsole unterhttps://console.aws.amazon.com/migrationhub/.
2. Im Navigationsbereich der Migration Hub Hub-Konsole unterEntdecken, wählenServer. Die erkannten Server erscheinen in der Serverliste.
3. Um weitere Informationen zu einem Server zu erhalten, wählen Sie seinen Link in der Spalte Server info (Server-Info) aus. Dadurch wird ein Bildschirm mit einer Beschreibung des Servers angezeigt.

Der Bildschirm mit Details zum Server zeigt Systeminformationen und Leistungsmetriken an. Sie finden dort auch eine Schaltfläche zum Exportieren von Netzwerkabhängigkeiten und Prozessinformationen. Weitere Informationen zum Exportieren detaillierter Serverinformationen finden Sie unter Exportieren von Serverdaten.

Server mit Suchfiltern sortieren

Um auf einfache Weise bestimmte Server zu finden, können Sie zum Sortieren aller mit den Sammlungstools erkannten Server Suchfilter anwenden. Sie können nach zahlreichen Kriterien suchen und filtern.

So sortieren Sie Server durch Anwenden von Suchfiltern

1. Verwenden IhrerAWS-Konto an, melden Sie sich beiAWS Management Consoleund öffnen Sie die Migration Hub Hub-Konsole unterhttps://console.aws.amazon.com/migrationhub/.
2. Im Navigationsbereich der Migration Hub Hub-Konsole unterEntdecken, wählenServer.
3. Klicken Sie auf die Suchleiste und wählen Sie ein Suchkriterium aus der Liste aus.
4. Wählen Sie einen Operator aus der Liste aus.
5. Geben Sie unter Beachtung der Groß-/Kleinschreibung einen Wert für das ausgewählte Suchkriterium ein und drücken Sie die Eingabetaste.
6. Es können mehrere Filter angewendet werden, indem Sie die Schritte 2 bis 4 wiederholen.

Markieren von Servern

Zur Unterstützung der Migrationsplanung und zur Erleichterung der Organisation können Sie für jeden Server mehrere Tags erstellen. Tags sind benutzerdefinierte Schlüssel-Wert-Paare, mit denen beliebige benutzerdefinierte Daten oder Metadaten zu Servern gespeichert werden können. Sie können einen einzelnen Server oder mehrere Server in einem einzigen Vorgang kennzeichnen.AWS Application Discovery Service (Application Discovery Service) -Tags sind ähnlichAWS-Tags, aber die beiden Arten von Tags können nicht synonym verwendet werden.

Sie können mehrere Tags für einen oder mehrere Server auf der Servers (Server)-Hauptseite hinzufügen oder entfernen. Auf der Detailseite eines Servers können Sie einen oder mehrere Tags für den ausgewählten Server hinzufügen oder entfernen. Sie können jede Art von Tagging-Aufgabe mit mehreren Servern oder Tags in einer einzigen Operation durchführen. Außerdem können Sie Tags entfernen.

So fügen Sie Tags zu einem oder mehreren Servern hinzu

1. Verwenden IhrerAWS-Konto an, melden Sie sich beiAWS Management Consoleund öffnen Sie die Migration Hub Hub-Konsole unterhttps://console.aws.amazon.com/migrationhub/.
2. Im Navigationsbereich der Migration Hub Hub-Konsole unterEntdecken, wählenServer.
3. Wählen Sie in der Spalte Server info (Server-Info) den Server-Link für den Server aus, für den Sie Tags hinzufügen möchten. Um zu mehr als einem Server gleichzeitig Tags hinzuzufügen, klicken Sie auf das Kontrollkästchen für mehrere Server.
4. WählenHinzufügen von Tagsund dann wählen SieHinzufügen eines Tags.

5. Geben Sie im Dialogfeld einen Schlüssel in das FeldSchlüsselund optional ein Wert im FeldWertaus.

   Fügen Sie weitere Tags hinzu, indem SieHinzufügen eines Tagsund weitere Informationen hinzufügen.

6. Wählen Sie Save (Speichern) aus.

So entfernen Sie Tags von einem oder mehreren Servern

1. Verwenden IhrerAWS-Konto an, melden Sie sich beiAWS Management Consoleund öffnen Sie die Migration Hub Hub-Konsole unterhttps://console.aws.amazon.com/migrationhub/.
2. Im Navigationsbereich der Migration Hub Hub-Konsole unterEntdecken, wählenServer.
3. Wählen Sie in der Spalte Server info (Server-Info) den Server-Link für den Server aus, von dem Sie Tags entfernen möchten. Aktivieren Sie die Kontrollkästchen mehrerer Server, um Tags von mehreren Servern gleichzeitig zu entfernen.
4. WählenEntfernen Sie Tags.
5. Wählen Sie jedes Tags aus, das Sie entfernen möchten.
6. Wählen Sie Confirm (Bestätigen).

Exportieren von Serverdaten

Um Netzwerkabhängigkeiten und Prozessinformationen für jeweils einen Server zu exportieren, können Sie dazu die Detailseite des Servers verwenden. Sie finden die Exportaufträge für einen Server in einer Tabelle im Bereich Exports (Exporte) auf der Detailseite des Servers. Wenn noch keine Exportaufträge vorhanden sind, ist die Tabelle leer. Sie können bis zu fünf Datensammlungen gleichzeitig exportieren.

> **Note**
>
> Das Exportieren von Serverdaten über die Konsole ist nur für Daten verfügbar, die von einem auf diesem Server ausgeführten Agent gesammelt wurden. Informationen zum Massenexport von Daten für alle Server, auf denen Agents installiert wurden, finden Sie unterDatenauflister in Amazon Athena.

So exportieren Sie detaillierte Serverdaten

1. Verwenden IhrerAWS-Konto an, melden Sie sich beiAWS Management Consoleund öffnen Sie die Migration Hub Hub-Konsole unterhttps://console.aws.amazon.com/migrationhub/.
2. Im Navigationsbereich der Migration Hub Hub-Konsole unterEntdecken, wählenServer.
3. Wählen Sie in der Spalte Server info (Serverinfo) die ID des Servers aus, für den Sie Daten exportieren möchten.
4. Wählen Sie im Bereich Exports (Exporte) unten auf dem Bildschirm Export server details (Serverdetails exportieren) aus.
5. Machen Sie für Export server details (Serverdetails exportieren) Angaben unter Start date (Startdatum) und Time (Uhrzeit).

   > **Note**
   >
   > Die Startzeit darf nicht mehr als 72 Stunden vor der aktuellen Uhrzeit liegen.

6. Wählen Sie Export, um den Auftrag zu starten. Der anfängliche Status ist In-progress (In Bearbeitung). Um den Status zu aktualisieren, klicken Sie auf das Aktualisierungssymbol für den Bereich Exports (Exporte).
7. Wenn der Exportauftrag abgeschlossen ist, klicken Sie auf Download (Herunterladen) und speichern Sie die ZIP-Datei.
8. Entpacken Sie die gespeicherte Zipdatei. Ein Satz von .csv-Dateien enthält die Exportdaten, wie in etwa:

   - *<AWS-Konto-ID>*_destinationProcessConnection.CSV-
   - *<AWS-Konto-ID>*_networkInterface.csv
   - *<AWS-Konto-ID>*_osInfo.csv
   - *<AWS-Konto-ID>*_process.csv
   - *<AWS-Konto-ID>*_sourceProcessConnection.CSV-
   - *<AWS-Konto-ID>*_systemPerformance.csv

   Sie können die CSV-Dateien in Microsoft Excel öffnen und die exportierten Serverdaten überprüfen.

Unter den Dateien finden Sie eine JSON-Datei mit Daten über den Exportauftrag und seine Ergebnisse.

Datenauflister in Athena

Mit der Datenexploration in Amazon Athena können Sie die Daten, die von Discovery Agent von allen erkannten lokalen Servern gesammelt wurden, an einem Ort analysieren. Sobald die Datenexploration in Amazon Athena über die Migration Hub Hub-Konsole aktiviert ist (oder mithilfe der StartContinousExport API) und die Datenerfassung für Agenten aktiviert ist, werden Daten, die von Agenten gesammelt werden, automatisch in regelmäßigen Abständen in Ihrem S3-Bucket gespeichert. Weitere Informationen finden Sie unter Datenauflister in Amazon Athena.

Anwendungen

Einige Ihrer erkannten Server müssen möglicherweise gemeinsam migriert werden, um funktionsfähig zu bleiben. In diesem Fall können Sie die erkannten Server logisch definieren und Gruppen in Anwendungen gruppieren.

Im Rahmen der Gruppierung können Sie Tags suchen, filtern und hinzufügen.

So gruppieren Sie Server in eine neue oder vorhandene Anwendung

1. Verwenden IhrerAWS-Konto an, melden Sie sich beiAWS Management Consoleund öffnen Sie die Migration Hub Hub-Konsole unterhttps://console.aws.amazon.com/migrationhub/.
2. Im Navigationsbereich der Migration Hub Hub-Konsole unterEntdecken, wählenServer.
3. Wählen Sie in der Serverliste die einzelnen Server aus, die Sie in eine neue oder vorhandene Anwendung gruppieren möchten.

   Um die Auswahl von Servern für Ihre Gruppe zu erleichtern, können Sie beliebe Kriterien, die Sie in der Serverliste angeben, suchen und filtern. Klicken Sie auf die Suchleiste und wählen Sie ein Element aus der Liste aus, wählen Sie einen Operator aus der nächsten Liste aus und geben Sie dann in Ihrer Kriterien ein.
4. Fakultativ: Für jeden ausgewählten Server wählen SieHinzufügen Tags, geben Sie einen Wert ein fürSchlüssel, und geben Sie dann optional einen Wert fürWert.
5. Wählen Sie Group as application (Als Anwendung gruppieren), um Ihre Anwendung zu erstellen oder zu einer vorhandenen hinzuzufügen.

6. Wählen Sie im Dialogfeld Group as application (Als Anwendung gruppieren) die Option Group as a new application (Als neue Anwendung gruppieren) oder Add to an existing application (Zu einer vorhandenen Anwendung hinzufügen).

   a. Wenn Sie Group as a new application (Als neue Anwendung gruppieren) gewählt haben, geben Sie einen Namen für Application name (Anwendungsname) ein. Optional können Sie eine Beschreibung für Application description (Anwendungsbeschreibung) eingeben.

   b. Wählen Sie bei Wahl von Add to an existing application (Zu einer vorhandenen Anwendung hinzufügen) in der Liste den Namen der Anwendung aus, zu der Sie hinzufügen möchten.

7. Wählen Sie Save (Speichern) aus.

Abfragen von erkannten Konfigurationselementen mithilfe der Application Discovery Service API

Ein Konfigurationselement ist ein IT-Asset, das in Ihrem Rechenzentrum von einem Agenten oder durch einen Import entdeckt wurde. Wenn Sie AWS Application Discovery Service (Application Discovery Service) verwenden, verwenden Sie die API, um Filter anzugeben und spezifische Konfigurationselemente für Server-, Anwendungs-, Prozess- und Verbindungsressourcen abzufragen. Informationen zur API finden Sie unter Application Discovery Service API-Referenz.

In den Tabellen in den folgenden Abschnitten sind die verfügbaren Eingabefilter und Ausgabesortieroptionen für zwei Application Discovery Service Service-Aktionen aufgeführt:

- `DescribeConfigurations`
- `ListConfigurations`

Die Filter- und Sortieroptionen sind nach dem Asset-Typ (Server, Anwendung, Prozess oder Verbindung) organisiert.

> **Important**
>
> Die von`DescribeConfigurations`,`ListConfigurations`, zurückgegebenen Ergebnisse enthalten `StartExportTask` möglicherweise keine aktuellen Aktualisierungen. Weitere Informationen finden Sie unter Letztendliche Datenkonsistenz.

Verwenden der **`DescribeConfigurations`** Aktion

Die `DescribeConfigurations`-Aktion ruft Attribute für eine Liste von Konfigurationselement-IDs ab. Alle bereitgestellten IDs müssen sich auf denselben Asset-Typ (Server, Anwendung, Prozess oder Verbindung) beziehen. Ausgabefelder sind für den gewählten Komponententyp spezifisch. Beispiel: Die Ausgabe für ein Server-Konfigurationselement enthält eine Liste von Attributen zum Server, z. B. den Host-Namen, das Betriebssystem und die Anzahl der Netzwerkkarten. Weitere Hinweise zur Befehlssyntax finden Sie unter DescribeConfigurations.

Die `DescribeConfigurations`-Aktion unterstützt keine Filterung.

Ausgabefelder für **`DescribeConfigurations`**

In den folgenden nach Asset-Typ geordneten Tabellen sind die unterstützten Ausgabefelder der `DescribeConfigurations`-Aktion aufgeführt. Zwingend erforderliche Felder sind immer in der Ausgabe vorhanden.

Serverressourcen

Feld	zwingend erforderlich
`server.agentId`	
`server.applications`	
`server.applications.hasMore Values`	
`server.configurationId`	x
`server.cpuType`	
`server.hostName`	
`server.hypervisor`	
`server.networkInterfaceInfo`	
`server.networkInterfaceInfo .hasMoreValues`	
`server.osName`	
`server.osVersion`	
`server.tags`	
`server.tags.hasMoreValues`	
`server.timeOfCreation`	x
`server.type`	

Feld	zwingend erforderlich
server.performance.avgCpuUsagePct	
server.performance.avgDiskReadIOPS	
server.performance.avgDiskReadsPerSecondInKB	
server.performance.avgDiskWriteIOPS	
server.performance.avgDiskWritesPerSecondInKB	
server.performance.avgFreeRAMInKB	
server.performance.avgNetworkReadsPerSecondInKB	
server.performance.avgNetworkWritesPerSecondInKB	
server.performance.maxCpuUsagePct	
server.performance.maxDiskReadIOPS	
server.performance.maxDiskReadsPerSecondInKB	
server.performance.maxDiskWriteIOPS	
server.performance.maxDiskWritesPerSecondInKB	

Feld	zwingend erforderlich
server.performance.maxNetwo rkReadsPerSecondInKB	
server.performance.maxNetwo rkWritesPerSecondInKB	
server.performance.minFreeR AMInKB	
server.performance.numCores	
server.performance.numCpus	
server.performance.numDisks	
server.performance.numNetwo rkCards	
server.performance.totalRAMInKB	

Verarbeitungs-Assets

Feld	zwingend erforderlich
process.commandLine	
process.configurationId	x
process.name	
process.path	
process.timeOfCreation	x

Anwendungs-Assets

Feld	zwingend erforderlich
`application.configurationId`	x
`application.description`	
`application.lastModifiedTime`	x
`application.name`	x
`application.serverCount`	x
`application.timeOfCreation`	x

Die **`ListConfigurations`** Aktion verwenden

Die `ListConfigurations`-Aktion ruft eine Liste von Konfigurationselementen nach den Kriterien ab, die Sie in einem Filter angeben. Weitere Hinweise zur Befehlssyntax finden Sie unter ListConfigurations.

Ausgabefelder für **`ListConfigurations`**

In den folgenden nach Asset-Typ geordneten Tabellen sind die unterstützten Ausgabefelder der `ListConfigurations`-Aktion aufgeführt. Zwingend erforderliche Felder sind immer in der Ausgabe vorhanden.

Serverressourcen

Feld	zwingend erforderlich
`server.configurationId`	x
`server.agentId`	
`server.hostName`	
`server.osName`	
`server.osVersion`	

Feld	zwingend erforderlich
server.timeOfCreation	x
server.type	

Verarbeitungs-Assets

Feld	zwingend erforderlich
process.commandLine	
process.configurationId	x
process.name	
process.path	
process.timeOfCreation	x
server.agentId	
server.configurationId	x

Anwendungs-Assets

Feld	zwingend erforderlich
application.configurationId	x
application.description	
application.name	x
application.serverCount	x
application.timeOfCreation	x
application.lastModifiedTime	x

Verbindungs-Assets

Feld	zwingend erforderlich
connection.destinationIp	x
connection.destinationPort	x
connection.ipVersion	x
connection.latestTimestamp	x
connection.occurrence	x
connection.sourceIp	x
connection.transportProtocol	
destinationProcess.configurationId	
destinationProcess.name	
destinationServer.configurationId	
destinationServer.hostName	
sourceProcess.configurationId	
sourceProcess.name	
sourceServer.configurationId	
sourceServer.hostName	

Unterstützte Filter für **ListConfigurations**

In den folgenden nach Asset-Typ geordneten Tabellen sind die unterstützten Filter für die ListConfigurations-Aktion aufgeführt. Filter und Werte befinden sich in einer Schlüssel-Wert-

Beziehung, die durch eine der unterstützten logischen Bedingungen definiert ist. Sie können die Ausgabe der angegebenen Filter sortieren.

Serverressourcen

Filter	Unterstützte Bedingungen	Unterstützte Werte	Unterstützte Sortierung
`server.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• Jede gültige Serverkonfigurationen-ID	None
`server.hostName`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`server.osName`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`server.osVersion`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`server.agentId`	• EQUALS	• String	None

Filter	Unterstützte Bedingungen	Unterstützte Werte	Unterstützte Sortierung
	• NOT_EQUALS • EQ • NE		
`server.connectorId`	• EQUALS • NOT_EQUALS • EQ • NE	• String	None
`server.type`	• EQUALS • NOT_EQUALS • EQ • NE	String mit einem der folgenden Werte: • EC2 • OTHER • VMWARE_VM • VMWARE_HOST • VMWARE_VM_TEMPLATE	None
`server.vmWareInfo.morefId`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	None

Filter	Unterstützte Bedingungen	Unterstützte Werte	Unterstützte Sortierung
`server.vmWareInfo.vcenterId`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	None
`server.vmWareInfo.hostId`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	None
`server.networkInterfaceInfo.portGroupId`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	None
`server.networkInterfaceInfo.portGroupName`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	None

Filter	Unterstützte Bedingungen	Unterstützte Werte	Unterstützte Sortierung
`server.networkInterfaceInfo.virtualSwitchName`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	None
`server.networkInterfaceInfo.ipAddress`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	None
`server.networkInterfaceInfo.macAddress`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	None
`server.performance.avgCpuUsagePct`	• GE • LE • GT • LT	• Prozentsatz	None
`server.performance.totalDiskFreeSizeInKB`	• GE • LE • GT • LT	• Double	None

Filter	Unterstützte Bedingungen	Unterstützte Werte	Unterstützte Sortierung
`server.performance.avgFreeRAMInKB`	• GE • LE • GT • LT	• Double	None
`server.tag.value`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	None
`server.tag.key`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	None
`server.application.name`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	None

Filter	Unterstützte Bedingungen	Unterstützte Werte	Unterstützte Sortierung
`server.application.description`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	None
`server.application.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• Jede gültige Anwendungskonfigurations-ID	None
`server.process.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• ProcessId	None
`server.process.name`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	None
`server.process.commandLine`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	None

Anwendungs-Assets

Filter	Unterstützte Bedingungen	Unterstützte Werte	Unterstützte Sortierung
`application.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• ApplicationId	None
`application.name`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`application.description`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`application.serverCount`	Filtern wird nicht unterstützt.	Filtern wird nicht unterstützt.	• ASC • DESC
`application.timeOfCreation`	Filtern wird nicht unterstützt.	Filtern wird nicht unterstützt.	• ASC • DESC

Filter	Unterstützte Bedingungen	Unterstützte Werte	Unterstützte Sortierung
`application.lastModifiedTime`	Filtern wird nicht unterstützt.	Filtern wird nicht unterstützt.	• ASC • DESC
`server.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• ServerId	None

Verarbeitungs-Assets

Filter	Unterstützte Bedingungen	Unterstützte Werte	Unterstützte Sortierung
`process.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• ProcessId	
`process.name`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`process.commandLine`	• EQUALS • NOT_EQUALS • EQ • NE	• String	• ASC • DESC

Filter	Unterstützte Bedingungen	Unterstützte Werte	Unterstützte Sortierung
	• CONTAINS • NOT_CONTAINS		
`server.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• ServerId	
`server.hostName`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`server.osName`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`server.osVersion`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC

Filter	Unterstützte Bedingungen	Unterstützte Werte	Unterstützte Sortierung
`server.agentId`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	

Verbindungs-Assets

Filter	Unterstützte Bedingungen	Unterstützte Werte	Unterstützte Sortierung
`connection.sourceIp`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• IP	• ASC • DESC
`connection.destinationIp`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• IP	• ASC • DESC
`connection.destinationPort`	• EQUALS • NOT_EQUALS • EQ • NE	• Ganzzahl	• ASC • DESC

Filter	Unterstützte Bedingungen	Unterstützte Werte	Unterstützte Sortierung
`sourceServer.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• ServerId	
`sourceServer.hostName`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`destinationServer.osName`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`destinationServer.osVersion`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC

Filter	Unterstützte Bedingungen	Unterstützte Werte	Unterstützte Sortierung
`destinationServer.agentId`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	
`sourceProcess.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• ProcessId	
`sourceProcess.name`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`sourceProcess.commandLine`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`destinationProcess.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• ProcessId	

Filter	Unterstützte Bedingungen	Unterstützte Werte	Unterstützte Sortierung
`destinationProcess.name`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`destinationprocess.commandLine`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC

Eventuelle Konsistenz in der API AWS Application Discovery Service

Die folgenden Aktualisierungsvorgänge sind letztendlich konsistent. Aktualisierungen sind für die Lesevorgänge StartExportTask DescribeConfigurations, und möglicherweise nicht sofort sichtbar ListConfigurations.

- AssociateConfigurationItemsToAnwendung
- CreateTags
- DeleteApplications
- DeleteTags
- DescribeBatchDeleteConfigurationAufgabe
- DescribeImportAufgaben
- DisassociateConfigurationItemsFromBewerbung
- UpdateApplication

Vorschläge für das Management der eventuellen Konsistenz:

- Wenn Sie die Lesevorgänge StartExportTask DescribeConfigurations, oder ListConfigurations(oder die entsprechenden AWS CLI Befehle) aufrufen, verwenden Sie einen exponentiellen Backoff-Algorithmus, damit alle vorherigen Aktualisierungsvorgänge genügend Zeit haben, um sich im System auszubreiten. Führen Sie dazu den Lesevorgang wiederholt aus, wobei Sie mit einer Wartezeit von zwei Sekunden beginnen und die Wartezeit schrittweise auf bis zu fünf Minuten erhöhen.
- Verlängert die Wartezeit zwischen aufeinanderfolgenden Vorgängen, auch wenn ein Aktualisierungsvorgang die Antwort 200 — OK zurückgibt. Wenden Sie einen exponentiellen Backoff-Algorithmus an, der mit einer Wartezeit von einigen Sekunden beginnt, und erhöhen Sie die Wartezeit schrittweise auf etwa fünf Minuten.

Sicherheit in AWS Application Discovery Service

Cloud-Sicherheit hat bei AWS höchste Priorität. Als AWS-Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die eingerichtet wurde, 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 und Sicherheit in der Cloud:

- Sicherheit der Cloud – AWS ist dafür verantwortlich, die Infrastruktur zu schützen, mit der AWS-Services in der AWS-Cloud ausgeführt werden. AWS stellt Ihnen außerdem Services bereit, die Sie sicher nutzen können. Die Wirksamkeit unserer Sicherheitsfunktionen wird regelmäßig von externen Prüfern im Rahmen des AWS-Compliance-Programms getestet und überprüft.
- Sicherheit in der Cloud – Ihr Verantwortungsumfang wird durch den AWS-Service bestimmt, den Sie verwenden. In Ihre Verantwortung fallen außerdem weitere Faktoren, wie z. B. die Vertraulichkeit der Daten, die Anforderungen Ihrer Organisation sowie geltende Gesetze und Vorschriften.

Um den AWS Application Discovery Agent oder den Application Discovery Service Agentless Collector verwenden zu können, müssen Sie Zugangsschlüssel für Ihr AWS Konto angeben. Diese Informationen werden dann in Ihrer lokalen Infrastruktur gespeichert. Im Rahmen des Modells der gemeinsamen Verantwortung sind Sie dafür verantwortlich, den Zugriff auf Ihre Infrastruktur zu sichern.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung von Application Discovery Service anwenden können. In den folgenden Themen erfahren Sie, wie Sie den Application Discovery Service konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere AWS Dienste verwenden können, die Ihnen helfen können, Ihre Application Discovery Service Service-Ressourcen zu überwachen und zu sichern.

Themen

Identity and Access Management für AWS Application Discovery Service

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

Themen

Zielgruppe

Die Art und Weise, wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, die Sie in Application Discovery Service ausführen.

Dienstbenutzer — Wenn Sie den Application Discovery Service Service für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen zur Verfügung, die Sie benötigen. Da Sie für Ihre Arbeit mehr Funktionen von Application Discovery Service verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Fuktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Wenn Sie nicht auf eine Funktion in Application Discovery Service zugreifen können, finden Sie weitere Informationen unterFehlerbehebung bei AWS Application Discovery Service Identität und Zugriff.

Serviceadministrator — Wenn Sie in Ihrem Unternehmen für die Ressourcen des Application Discovery Service verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf den Application

Discovery Service. Es ist Ihre Aufgabe, zu bestimmen, auf welche Funktionen und Ressourcen der Application Discovery Service Ihre Servicebenutzer zugreifen sollen. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Servicenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen darüber, wie Ihr Unternehmen IAM mit Application Discovery Service verwenden kann, finden Sie unterWie AWS Application Discovery Service funktioniert 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 den Application Discovery Service zu verwalten. Beispiele für identitätsbasierte Richtlinien des Application Discovery Service, die Sie in IAM verwenden können, finden Sie unter. AWS Application Discovery Service Beispiele für identitätsbasierte Richtlinien

Authentifizierung mit Identitäten

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

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

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

Wenn Sie AWS programmgesteuert zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, um Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch zu signieren. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode, um Anfragen selbst zu signieren, finden Sie im IAM-Benutzerhandbuch 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) in AWS im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

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

IAM-Benutzer und -Gruppen

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

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

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

IAM-Rollen

Eine IAM-Rolle ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der übernehmen, AWS Management Console indem Sie die Rollen wechseln. Sie können eine Rolle übernehmen, indem Sie eine AWS CLI oder AWS API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter Verwenden von IAM-Rollen im IAM-Benutzerhandbuch.

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

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center -Benutzerhandbuch.
- Temporäre IAM-Benutzerberechtigungen – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können 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 kontenübergreifenden Zugriff finden Sie unter Kontenübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff — Einige verwenden Funktionen in anderen. AWS-Services AWS-Services Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon-EC2 aus oder speichert Objekte in Amazon-S3. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Forward Access Sessions (FAS) — Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services

könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

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

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

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

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Berechtigungen

in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

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

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

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

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

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

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und

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

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

Zugriffssteuerungslisten (ACLs)

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

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

Weitere Richtlinientypen

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

- Berechtigungsgrenzen – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.
- Service Control Policies (SCPs) — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung

mehrerer Objekte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Entitäten. Root-Benutzer des AWS-Kontos Weitere Informationen zu Organizations und SCPs finden Sie unter Funktionsweise von SCPs im AWS Organizations -Benutzerhandbuch.

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

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter Bewertungslogik für Richtlinien.

Wie AWS Application Discovery Service funktioniert mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf den Application Discovery Service zu verwalten, sollten Sie wissen, welche IAM-Funktionen für die Verwendung mit Application Discovery Service verfügbar sind. Einen allgemeinen Überblick darüber, wie Application Discovery Service und andere AWS Dienste mit IAM zusammenarbeiten, finden Sie unter AWS Services That Work with IAM im IAM-Benutzerhandbuch.

Themen

- Identitätsbasierte Richtlinien für den Application Discovery Service
- Ressourcenbasierte Richtlinien für den Application Discovery Service
- Autorisierung auf der Grundlage von Application Discovery Service Tags
- IAM-Rollen für den Application Discovery Service

Identitätsbasierte Richtlinien für den Application Discovery Service

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Der Application Discovery Service unterstützt bestimmte Aktionen, Ressourcen und Bedingungsschlüssel. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Aktionen

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

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

Richtlinienaktionen im Application Discovery Service verwenden das folgende Präfix vor der Aktion:`discovery:`. Richtlinienanweisungen müssen entweder ein – `Action`oder ein `NotAction`-Element enthalten. Der Application Discovery Service definiert eigene Aktionen, die Aufgaben beschreiben, die Sie mit diesem Dienst ausführen können.

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie wie folgt durch Kommata:

```
"Action": [
      "discovery:action1",
      "discovery:action2"
```

Sie können auch Platzhalter verwenden, um mehrere Aktionen anzugeben. Beispielsweise können Sie alle Aktionen festlegen, die mit dem Wort `Describe` beginnen, einschließlich der folgenden Aktion:

```
"Action": "discovery:Describe*"
```

Eine Liste der Application Discovery Service Service-Aktionen finden Sie unter Definierte Aktionen von AWS Application Discovery Service im IAM-Benutzerhandbuch.

Ressourcen

Der Application Discovery Service unterstützt die Angabe von Ressourcen-ARNs in einer Richtlinie nicht. Um den Zugriff zu trennen, erstellen und verwenden Sie ihn separat AWS-Konten.

Bedingungsschlüssel

Der Application Discovery Service stellt keine dienstspezifischen Bedingungsschlüssel bereit, unterstützt jedoch die Verwendung einiger globaler Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter AWS Globale Bedingungskontextschlüssel im IAM-Benutzerhandbuch.

Beispiele

Beispiele für identitätsbasierte Richtlinien des Application Discovery Service finden Sie unter. AWS Application Discovery Service Beispiele für identitätsbasierte Richtlinien

Ressourcenbasierte Richtlinien für den Application Discovery Service

Der Application Discovery Service unterstützt keine ressourcenbasierten Richtlinien.

Autorisierung auf der Grundlage von Application Discovery Service Tags

Der Application Discovery Service unterstützt weder das Markieren von Ressourcen noch das Steuern des Zugriffs auf der Grundlage von Tags.

IAM-Rollen für den Application Discovery Service

Eine IAM-Rolle ist eine Entität innerhalb Ihres AWS Kontos, die über bestimmte Berechtigungen verfügt.

Temporäre Anmeldeinformationen mit dem Application Discovery Service verwenden

Der Application Discovery Service unterstützt die Verwendung temporärer Anmeldeinformationen nicht.

Serviceverknüpfte Rollen

Mit dienstbezogenen Rollen können AWS Dienste auf Ressourcen in anderen Diensten zugreifen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem IAM-Konto angezeigt und gehören zum Service. Ein IAM-Administrator kann die Berechtigungen für serviceverknüpfte Rollen anzeigen, aber nicht bearbeiten.

Der Application Discovery Service unterstützt dienstverknüpfte Rollen. Einzelheiten zum Erstellen oder Verwalten von mit dem Application Discovery Service verknüpften Rollen finden Sie unterVerwenden von servicegebundenen Rollen für Application Discovery Service.

Servicerollen

Dieses Feature ermöglicht einem Service das Annehmen einer Servicerolle in Ihrem Namen. Diese Rolle gewährt dem Service Zugriff auf Ressourcen in anderen Diensten, um eine Aktion in Ihrem Namen auszuführen. Servicerollen werden in Ihrem IAM-Konto angezeigt und gehören zum Konto. Dies bedeutet, dass ein IAM-Administrator die Berechtigungen für diese Rolle ändern kann. Dies kann jedoch die Funktionalität des Dienstes beeinträchtigen.

Der Application Discovery Service unterstützt Dienstrollen.

AWS Von verwaltete Richtlinien für AWS Application Discovery Service

Um Benutzern, Gruppen und Rollen Berechtigungen hinzuzufügen, ist es einfacher, AWS verwaltete Richtlinien zu verwenden, als selbst Richtlinien 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 von AWS verwalteten Richtlinien verwenden. Diese Richtlinien decken allgemeine Anwendungsfälle ab und sind in Ihrem AWS-Konto verfügbar. Weitere Informationen zu von AWS verwalteten Richtlinien finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

AWS -Services verwalten und aktualisieren AWS verwaltete Richtlinien. Sie können die Berechtigungen in AWS verwalteten Richtlinien nicht ändern. Services fügen einer von AWS verwalteten Richtlinien gelegentlich zusätzliche Berechtigungen hinzu, um neue Features zu unterstützen. Diese Art von Update betrifft alle Identitäten (Benutzer, Gruppen und Rollen), an welche die Richtlinie angehängt ist. Services aktualisieren eine von AWS verwaltete Richtlinie am ehesten, ein neues Feature gestartet wird oder neue Vorgänge verfügbar werden. Services entfernen keine

Berechtigungen aus einer von AWS verwalteten Richtlinie, sodass Richtlinienaktualisierungen Ihre vorhandenen Berechtigungen nicht beeinträchtigen.

Darüber hinaus AWS unterstützt verwaltete Richtlinien für Auftragsfunktionen, die sich über mehrere Services erstrecken. Die von ReadOnlyAccess AWS verwaltete Richtlinie bietet beispielsweise schreibgeschützten Zugriff auf alle - AWS Services und -Ressourcen. Wenn ein Service ein neues Feature startet, AWS fügt schreibgeschützte Berechtigungen für neue Vorgänge und Ressourcen hinzu. Eine Liste und Beschreibungen der Richtlinien für Auftragsfunktionen finden Sie in Verwaltete AWS -Richtlinien für Auftragsfunktionen im IAM-Leitfaden.

AWS Von verwaltete Richtlinie: AWSApplicationDiscoveryServiceFullAccess

Die `AWSApplicationDiscoveryServiceFullAccess` Richtlinie gewährt einem IAM-Benutzerkonto Zugriff auf die APIs von Application Discovery Service und Migration Hub APIs.

Ein IAM-Benutzerkonto, dem diese Richtlinie angefügt ist, kann Application Discovery Service konfigurieren, Kundendienstmitarbeiter starten und stoppen, die agentenlose Erkennung starten und beenden und Daten aus der AWS Discovery-Service-Datenbank abfragen. Ein Beispiel für diese Richtlinie finden Sie unter Vollzugriff auf den Application Discovery Service gewähren.

AWS Von verwaltete Richtlinie: AWSApplicationDiscoveryAgentlessCollectorAccess

Die `AWSApplicationDiscoveryAgentlessCollectorAccess` verwaltete Richtlinie gewährt dem Application Discovery Service Agentless Collector (Agentless Collector) Zugriff, um den Application Discovery Service zu registrieren und mit ihm zu kommunizieren und mit anderen - AWS Services zu kommunizieren.

Diese Richtlinie muss an den IAM-Benutzer angehängt werden, dessen Anmeldeinformationen zur Konfiguration des Agentless Collector verwendet werden.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `arsenal` – Ermöglicht dem Kollektor die Registrierung bei der Application Discovery Service-Anwendung. Dies ist erforderlich, um erfasste Daten an zurücksenden zu können AWS.

- `ecr-public` – Ermöglicht dem Kollektor, Aufrufe an die Amazon Elastic Container Registry Public (Amazon ECR Public) zu tätigen, in der die neuesten Updates für den Kollektor gefunden werden.
- `mgh` – Ermöglicht dem Kollektor, aufzurufen, AWS Migration Hub um die Heimatregion des Kontos abzurufen, das zur Konfiguration des Kollektors verwendet wurde. Dies ist erforderlich, um zu wissen, an welche Region die erfassten Daten gesendet werden sollen.
- `sts` – Ermöglicht dem Kollektor das Abrufen eines Service-Bearer-Tokens, sodass der Kollektor Aufrufe an Amazon ECR Public tätigen kann, um die neuesten Updates zu erhalten.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "arsenal:RegisterOnPremisesAgent"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ecr-public:DescribeImages"
            ],
            "Resource": "arn:aws:ecr-
public::446372222237:repository/6e5498e4-8c31-4f57-9991-13b4b992ff7b"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ecr-public:GetAuthorizationToken"

            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "mgh:GetHomeRegion"
            ],
            "Resource": "*"
        },
```

```
        {
            "Effect": "Allow",
            "Action": [
                "sts:GetServiceBearerToken"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS Von verwaltete Richtlinie: AWSApplicationDiscoveryAgentAccess

Die `AWSApplicationDiscoveryAgentAccess` Richtlinie gewährt dem Application Discovery Agent Zugriff auf die Registrierung und Kommunikation mit dem Application Discovery Service.

Sie fügen diese Richtlinie an jeden Benutzer an, dessen Anmeldeinformationen vom Application Discovery Agent verwendet werden.

Diese Richtlinie gewährt dem Benutzer außerdem den Zugriff auf Arsenal. Arsenal ist ein Agent-Service, der von verwaltet und gehostet wird AWS. Arsenal leitet Daten an Application Discovery Service in der Cloud weiter. Ein Beispiel für diese Richtlinie finden Sie unter Discovery-Agents Zugriff gewähren.

AWS Von verwaltete Richtlinie: AWSAgentlessDiscoveryService

Die `AWSAgentlessDiscoveryService` Richtlinie gewährt dem AWS Agentless Discovery Connector, der in Ihrem VMware vCenter Server ausgeführt wird, Zugriff auf die Registrierung, Kommunikation mit und Freigabe von Zustandsmetriken für Konnektoren mit Application Discovery Service.

Fügen Sie diese Richtlinie einem Benutzer an, dessen Anmeldeinformationen von dem Connector verwendet werden.

AWS Von verwaltete Richtlinie: ApplicationDiscoveryServiceContinuousExportServiceRoleRichtlinie

Wenn Ihrem IAM-Konto die `AWSApplicationDiscoveryServiceFullAccess` Richtlinie angefügt ist, `ApplicationDiscoveryServiceContinuousExportServiceRolePolicy` wird automatisch an Ihr Konto angefügt, wenn Sie die Datenexploration in Amazon Athena aktivieren.

Diese Richtlinie ermöglicht es AWS Application Discovery Service , Amazon-Data-Firehose-Streams zu erstellen, um Daten zu transformieren und bereitzustellen, die von AWS Application Discovery Service Kundendienstmitarbeitern in einem Amazon S3-Bucket in Ihrem AWS Konto erfasst werden.

Darüber hinaus erstellt diese Richtlinie eine AWS Glue Data Catalog mit einer neuen Datenbank namens application_discovery_service_database und Tabellenschemata für die Zuordnung von Daten, die von den Agenten erfasst werden. Ein Beispiel für diese Richtlinie finden Sie unter Erteilen von Berechtigungen für die Erfassung von Agentendaten.

AWS Von verwaltete Richtlinie: AWSDiscoveryContinuousExportFirehosePolicy

Die `AWSDiscoveryContinuousExportFirehosePolicy` Richtlinie ist erforderlich, um die Datenexploration in Amazon Athena zu verwenden. Damit kann Amazon Data Firehose Daten schreiben, die vom Application Discovery Service in Amazon S3 gesammelt werden. Weitere Informationen zur Verwendung dieser Richtlinie finden Sie unter Erstellen der AWSApplicationDiscoveryServiceFirehose Rolle. Ein Beispiel für diese Richtlinie finden Sie unter Erteilung von Berechtigungen für die Datenexploration.

Erstellen der AWSApplicationDiscoveryServiceFirehose Rolle

Ein Administrator fügt Ihrem IAM-Benutzerkonto verwaltete Richtlinien an. Wenn Sie die `AWSDiscoveryContinuousExportFirehosePolicy` Richtlinie verwenden, muss der Administrator zunächst eine Rolle mit dem Namen AWSApplicationDiscoveryServiceFirehose mit Firehose als vertrauenswürdige Entität erstellen und dann die `AWSDiscoveryContinuousExportFirehosePolicy` Richtlinie an die Rolle anfügen, wie im folgenden Verfahren gezeigt.

So erstellen Sie die AWSApplicationDiscoveryServiceFirehose IAM-Rolle

1. Wählen Sie in der IAM-Konsole im Navigationsbereich Rollen aus.
2. Wählen Sie Create Role (Rolle erstellen) aus.
3. Wählen Sie Kinesis.
4. Wählen Sie als Ihren Anwendungsfall Kinesis Firehose.
5. Wählen Sie Weiter: Berechtigungen aus.
6. Suchen Sie unter Filterrichtlinien nach AWSDiscoveryContinuousExportFirehosePolicy.
7. Aktivieren Sie das Kontrollkästchen neben AWSDiscoveryContinuousExportFirehosePolicyund wählen Sie dann Weiter: Überprüfen aus.

8. Geben Sie AWSApplicationDiscoveryServiceFirehose als Rollennamen ein und wählen Sie dann Rolle erstellen aus.

Aktualisierungen des Application Discovery Service für - AWS verwaltete Richtlinien

Anzeigen von Details zu Aktualisierungen für - AWS verwaltete Richtlinien für Application Discovery Service, seit dieser Service mit der Verfolgung dieser Änderungen begonnen hat. Um automatische Warnungen über Änderungen an dieser Seite zu erhalten, abonnieren Sie den RSS-Feed auf der Dokumentverlauf für AWS Application Discovery Service-Seite.

Änderung	Beschreibung	Datum
AWSApplicationDiscoveryAgentlessCollectorAccess – Neue Richtlinie, die beim Start von Agentless Collector verfügbar gemacht wird	Application Discovery Service hat die neue verwaltete Richtlinie hinzugefügt `AWSApplicationDiscoveryAgentlessCollectorAccess`, die dem Agentless Collector Zugriff gewährt, um den Application Discovery Service zu registrieren und mit ihm zu kommunizieren und mit anderen - AWS Services zu kommunizieren.	16. August 2022
Application Discovery Service hat mit der Verfolgung von Änderungen begonnen	Application Discovery Service hat mit der Verfolgung von Änderungen für seine AWS -verwalteten Richtlinien begonnen.	1. März 2021

AWS Application Discovery Service Beispiele für identitätsbasierte Richtlinien

Standardmäßig sind IAM-Benutzer und -Rollen nicht berechtigt, Application Discovery Service Service-Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mit der AWS Management Console AWS CLI, oder AWS API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern und Rollen die Berechtigung zum Ausführen bestimmter API-Operationen für die angegebenen Ressourcen gewähren, die diese benötigen. Der Administrator muss diese Richtlinien anschließend den IAM-Benutzern oder -Gruppen anfügen, die diese Berechtigungen benötigen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von Richtlinien auf der JSON-Registerkarte im IAM-Benutzerhandbuch.

Themen

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand Application Discovery Service Service-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Erste Schritte mit AWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um damit zu beginnen, Ihren Benutzern und Workloads Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien

definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien oder AWS -verwaltete Richtlinien für Auftrags-Funktionen im IAM-Benutzerhandbuch.

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

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Vollzugriff auf den Application Discovery Service gewähren

Die AWSApplicationDiscoveryServiceFullAccess verwaltete Richtlinie gewährt dem IAM-Benutzerkonto Zugriff auf die APIs Application Discovery Service und Migration Hub.

Ein IAM-Benutzer, dem diese Richtlinie mit seinem Konto verknüpft ist, kann den Application Discovery Service konfigurieren, Agents starten und beenden, die agentenlose Erkennung starten und beenden und Daten aus der AWS Discovery Service-Datenbank abfragen. Weitere Informationen zu dieser Richtlinie finden Sie unter AWS Von verwaltete Richtlinien für AWS Application Discovery Service.

Example AWSApplicationDiscoveryServiceFullAccess Richtlinie

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "mgh:*",
                "discovery:*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "iam:GetRole"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Discovery-Agents Zugriff gewähren

Die AWSApplicationDiscoveryAgentAccess verwaltete Richtlinie gewährt dem Application Discovery Agent Zugriff auf die Registrierung und Kommunikation mit dem Application Discovery Service. Weitere Informationen zu dieser Richtlinie finden Sie unter AWS Von verwaltete Richtlinien für AWS Application Discovery Service.

Ordnen Sie diese Richtlinie jedem Benutzer zu, dessen Anmeldeinformationen vom Application Discovery Agent verwendet werden.

Diese Richtlinie gewährt dem Benutzer außerdem den Zugriff auf Arsenal. Arsenal ist ein Agentendienst, der von verwaltet und gehostet wird AWS. Arsenal leitet Daten an den Application Discovery Service in der Cloud weiter.

Example AWSApplicationDiscoveryAgentAccess Richtlinie

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "arsenal:RegisterOnPremisesAgent"
            ],
            "Resource": "*"
        }
    ]
}
```

Erteilen von Berechtigungen für die Erfassung von Agentendaten

Die ApplicationDiscoveryServiceContinuousExportServiceRolePolicy verwaltete Richtlinie ermöglicht AWS Application Discovery Service die Erstellung von Amazon Data Firehose-Streams zur Transformation und Übertragung von Daten, die von Application Discovery Service Service-Agenten gesammelt wurden, an einen Amazon S3 S3-Bucket in Ihrem AWS Konto.

Darüber hinaus erstellt diese Richtlinie einen AWS Glue Datenkatalog mit einer neuen Datenbank namens `application_discovery_service_database` und Tabellenschemas für die Zuordnung von Daten, die von den Agenten gesammelt wurden.

Weitere Informationen zur Verwendung dieser Richtlinie finden Sie unter AWS Von verwaltete Richtlinien für AWS Application Discovery Service.

Example ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

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

```
            "Action": [
                "glue:CreateDatabase",
                "glue:UpdateDatabase",
                "glue:CreateTable",
                "glue:UpdateTable",
                "firehose:CreateDeliveryStream",
                "firehose:DescribeDeliveryStream",
                "logs:CreateLogGroup"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "firehose:DeleteDeliveryStream",
                "firehose:PutRecord",
                "firehose:PutRecordBatch",
                "firehose:UpdateDestination"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:firehose:*:*:deliverystream/aws-application-discovery-
service*"
        },
        {
            "Action": [
                "s3:CreateBucket",
                "s3:ListBucket",
                "s3:PutBucketLogging",
                "s3:PutEncryptionConfiguration"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::aws-application-discovery-service*"
        },
        {
            "Action": [
                "s3:GetObject"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::aws-application-discovery-service*/*"
        },
        {
            "Action": [
                "logs:CreateLogStream",
                "logs:PutRetentionPolicy"
```

```
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:logs:*:*:log-group:/aws/application-discovery-service/
firehose*"
        },
        {
            "Action": [
                "iam:PassRole"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:iam::*:role/AWSApplicationDiscoveryServiceFirehose",
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": "firehose.amazonaws.com"
                }
            }
        },
        {
            "Action": [
                "iam:PassRole"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:iam::*:role/service-role/
AWSApplicationDiscoveryServiceFirehose",
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": "firehose.amazonaws.com"
                }
            }
        }
    ]
}
```

Erteilung von Berechtigungen für die Datenexploration

Die AWSDiscoveryContinuousExportFirehosePolicy Richtlinie ist erforderlich, um die Datenexploration in Amazon Athena nutzen zu können. Es ermöglicht Amazon Data Firehose, Daten, die vom Application Discovery Service gesammelt wurden, in Amazon S3 zu schreiben. Weitere Informationen zur Verwendung dieser Richtlinie finden Sie unter Erstellen der AWSApplicationDiscoveryServiceFirehose Rolle.

Example AWSDiscoveryContinuousExportFirehosePolicy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "glue:GetTableVersions"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:GetBucketLocation",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:ListBucketMultipartUploads",
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::aws-application-discovery-service-*",
                "arn:aws:s3:::aws-application-discovery-service-*/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:/aws/application-discovery-service/
firehose:log-stream:*"
            ]
        }
    ]
}
```

Erteilen von Berechtigungen zur Verwendung des Netzwerkdiagramms der Migration Hub Hub-Konsole

Um beim Erstellen einer identitätsbasierten Richtlinie, die den Zugriff auf Application Discovery Service oder Migration Hub erlaubt oder verweigert, Zugriff auf das AWS Migration Hub Konsolen-Netzwerkdiagramm zu gewähren, müssen Sie die `discovery:GetNetworkConnectionGraph` Aktion möglicherweise der Richtlinie hinzufügen.

Sie müssen die `discovery:GetNetworkConnectionGraph` Aktion in neuen Richtlinien verwenden oder ältere Richtlinien aktualisieren, wenn Folgendes für die Richtlinie zutrifft:

- Die Richtlinie erlaubt oder verweigert den Zugriff auf den Application Discovery Service oder den Migration Hub.
- Die Richtlinie gewährt Zugriffsberechtigungen mithilfe einer weiteren spezifischen Discovery-Aktion wie `discovery:`*`action-name`* stattdiscovery:*.

Das folgende Beispiel zeigt, wie die `discovery:GetNetworkConnectionGraph` Aktion in einer IAM-Richtlinie verwendet wird.

Example

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["discovery:GetNetworkConnectionGraph"],
            "Resource": "*"
        }
    ]
}
```

Informationen zum Migration Hub-Netzwerkdiagramm finden Sie unter Netzwerkverbindungen in Migration Hub anzeigen.

Verwenden von servicegebundenen Rollen für Application Discovery Service

AWS Application Discovery Service verwendet serviceverknüpfte Rollen von AWS Identity and Access Management (IAM). Eine serviceverknüpfte Rolle ist ein spezieller Typ einer IAM-Rolle, die direkt mit Application Discovery Service verknüpft ist. Serviceverknüpfte Rollen werden vom Application Discovery Service vordefiniert und schließen alle Berechtigungen ein, die der Service zum Aufrufen andererAWS-Services in Ihrem Namen.

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

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem ihre verwandten Ressourcen gelöscht wurden. Dies schützt Ihre Application Discovery Service Service-Ressourcen, da Sie nicht versehentlich die Berechtigung für den Zugriff auf die Ressourcen entfernen können.

Themen

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

Berechtigungen von servicegebundenen Rollen für Application Discovery Service

Application Discovery Service verwendet die serviceverknüpfte Rolle namensAWSServiceRoleForApplicationDiscoveryServiceContinuousExport— Ermöglicht den Zugriff aufAWSDienste und Ressourcen, die genutzt oder verwaltet werden vonAWS Application Discovery Service.

Die AWSServiceRoleForApplicationDiscoveryServiceContinuousExport Serviceverknüpfte Rolle vertraut darauf, dass die folgenden Services die Rolle annehmen:

- `continuousexport.discovery.amazonaws.com`

Die Rollenberechtigungsrichtlinie erlaubt Application Discovery Service die Durchführung der folgenden Aktionen:

glue

`CreateDatabase`

`UpdateDatabase`

`CreateTable`

`UpdateTable`

firehose

`CreateDeliveryStream`

`DeleteDeliveryStream`

`DescribeDeliveryStream`

`PutRecord`

`PutRecordBatch`

`UpdateDestination`

S3

`CreateBucket`

`ListBucket`

`GetObject`

Protokolle

`CreateLogGroup`

`CreateLogStream`

`PutRetentionPolicy`

iam

```
PassRole
```

Dies ist die vollständige Richtlinie, aus der hervorgeht, für welche Ressourcen die oben genannten Aktionen gelten:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "glue:CreateDatabase",
                "glue:UpdateDatabase",
                "glue:CreateTable",
                "glue:UpdateTable",
                "firehose:CreateDeliveryStream",
                "firehose:DescribeDeliveryStream",
                "logs:CreateLogGroup"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "firehose:DeleteDeliveryStream",
                "firehose:PutRecord",
                "firehose:PutRecordBatch",
                "firehose:UpdateDestination"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:firehose:*:*:deliverystream/aws-application-discovery-
service*"
        },
        {
            "Action": [
                "s3:CreateBucket",
                "s3:ListBucket",
                "s3:PutBucketLogging",
                "s3:PutEncryptionConfiguration"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::aws-application-discovery-service*"
```

```
        },
        {
            "Action": [
                "s3:GetObject"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::aws-application-discovery-service*/*"
        },
        {
            "Action": [
                "logs:CreateLogStream",
                "logs:PutRetentionPolicy"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:logs:*:*:log-group:/aws/application-discovery-service/
firehose*"
        },
        {
            "Action": [
                "iam:PassRole"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:iam::*:role/AWSApplicationDiscoveryServiceFirehose",
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": "firehose.amazonaws.com"
                }
            }
        },
        {
            "Action": [
                "iam:PassRole"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:iam::*:role/service-role/
AWSApplicationDiscoveryServiceFirehose",
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": "firehose.amazonaws.com"
                }
            }
        }
    ]
```

```
}
```

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

Erstellen einer serviceverknüpften Rolle für Application Discovery Service

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Die AWSServiceRoleForApplicationDiscoveryServiceContinuousExport Eine dienstgebundene Rolle wird automatisch erstellt, wenn der kontinuierliche Export implizit aktiviert wird, indem a) Optionen in dem Dialogfeld bestätigt werden, das auf der Seite Datensammler angezeigt wird, nachdem Sie „Datenerfassung starten“ ausgewählt haben, oder auf den Schieberegler mit der Bezeichnung „Datenexploration in Athena“ klicken oder b) wenn Sie StartContinuousExport -API mit derAWSCLI.

> **Important**
>
> Diese serviceverknüpfte Rolle kann in Ihrem Konto erscheinen, wenn Sie eine Aktion in einem anderen Service abgeschlossen haben, der die von dieser Rolle unterstützten Funktionen verwendet. Weitere Informationen finden Sie unter Eine neue Rolle ist in meinem IAM-Konto erschienen.

Erstellen der dienstverknüpften Rolle über die Migration Hub Hub-Konsole

Sie können die Migration Hub Hub-Konsole verwenden, um die AWSServiceRoleForApplicationDiscoveryServiceContinuousExport serviceverknüpfte Rolle.

So erstellen die serviceverknüpfte Rolle (Konsole)

1. Klicken Sie im Navigationsbereich auf Data Collectors (Datensammler).
2. Wählen Sie die Registerkarte Agents (Agenten).
3. Schalten Sie dasDatenexploration in AthenaSchieberegler auf die Position Ein.
4. Klicken Sie in dem im vorherigen Schritt erstellten Dialogfeld auf das Kontrollkästchen, um sich mit den anfallenden Gebühren einverstanden zu erklären. Klicken Sie dann auf Continue (Fortfahren) oder Enable (Aktivieren).

Erstellen der serviceverknüpften Rolle aus demAWS CLI

Sie können Application Discovery Service Service-Befehle aus demAWS Command Line Interfaceum das zu erstellen AWSServiceRoleForApplicationDiscoveryServiceContinuousExportserviceverknüpfte Rolle.

Diese dienstgebundene Rolle wird automatisch erstellt, wenn Sie Continuous Export vonAWS CLI(dasAWS CLImuss zuerst in Ihrer Umgebung installiert werden).

So erstellen Sie die serviceverknüpfte Rolle (CLI), indem Sie Continuous Export vonAWS CLI

1. Installieren Sie die AWS CLI für Ihr Betriebssystem (Linux, macOS oder Windows). Sehen Sie das anAWS Command Line InterfaceBenutzerhandbuchfür Anweisungen.
2. Öffnen Sie die Eingabeaufforderung (Windows) oder das Terminal (Linux oder macOS).
   a. Geben Sie `aws configure` ein und drücken Sie die Eingabetaste.
   b. Gib deineAWSZugriffsschlüssel-ID undAWSGeheimer Zugriffsschlüssel.
   c. Geben Sie als standardmäßigen Regionsnamen `us-west-2` ein.
   d. Geben Sie als Standard-Ausgabeformat `text` ein.
3. Geben Sie den folgenden Befehl ein:

```
aws discovery start-continuous-export
```

Sie können auch die IAM-Konsole verwenden, um eine serviceverknüpfte Rolle mit demDiscovery Service — Kontinuierlicher ExportAnwendungsfall. Erstellen Sie in der IAM CLI oder der IAM API eine serviceverknüpfte Rolle mit dem Servicenamen `continuousexport.discovery.amazonaws.com`. Weitere Informationen finden Sie unter Erstellen einer servicegebundenen Rolle im IAM-Leitfaden. Wenn Sie diese servicegebundene Rolle löschen, können Sie mit demselben Verfahren die Rolle erneut erstellen.

Löschen einer serviceverknüpften Rolle für Application Discovery Service

Wenn Sie eine Funktion oder einen Service, die bzw. der eine servicegebundene Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch Ihre serviceverknüpfte Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

Bereinigen der serviceverknüpften Rolle

Bevor mit IAM eine serviceverknüpfte Rolle löschen können, müssen Sie zunächst alle von der Rolle verwendeten Ressourcen löschen.

> **Note**
>
> Wenn Application Discovery Service die Rolle verwendet, wenn Sie die Ressourcen löschen möchten, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

So löschen Sie Application Discovery Service Service-Ressourcen, die von der AWSServiceRoleForApplicationDiscoveryServiceContinuousExport Serviceverknüpfte Rolle aus der Migration Hub Hub-Konsole

1. Klicken Sie im Navigationsbereich auf Data Collectors (Datensammler).
2. Wählen Sie die Registerkarte Agents (Agenten).
3. Schalten Sie dasDatenexploration in AthenaSchieberegler auf die Position Aus.

So löschen Sie Application Discovery Service Service-Ressourcen, die von der AWSServiceRoleForApplicationDiscoveryServiceContinuousExport Serviceverknüpfte Rolle aus demAWS CLI

1. Installieren Sie die AWS CLI für Ihr Betriebssystem (Linux, macOS oder Windows). Sehen Sie das anAWS Command Line InterfaceBenutzerhandbuchfür Anweisungen.
2. Öffnen Sie die Eingabeaufforderung (Windows) oder das Terminal (Linux oder macOS).
   a. Geben Sie `aws configure` ein und drücken Sie die Eingabetaste.
   b. Gib deineAWSZugriffsschlüssel-ID undAWSGeheimer Zugriffsschlüssel.
   c. Geben Sie als standardmäßigen Regionsnamen `us-west-2` ein.
   d. Geben Sie als Standard-Ausgabeformat `text` ein.
3. Geben Sie den folgenden Befehl ein:

```
aws discovery stop-continuous-export --export-id <export ID>
```

- Wenn Ihnen die Export-ID des fortlaufenden Exports, den Sie beenden möchten, nicht bekannt ist, geben Sie den folgenden Befehl ein, um die ID des fortlaufenden Exports anzuzeigen:

```
aws discovery describe-continuous-exports
```

4. Geben Sie den folgenden Befehl ein, um sicherzustellen, dass der kontinuierliche Export gestoppt wurde, indem Sie sicherstellen, dass der Rückgabestatus „INAKTIV“ lautet

```
aws discovery describe-continuous-export
```

Manuelles Löschen der serviceverknüpften Rolle

Sie können das löschen AWSServiceRoleForApplicationDiscoveryServiceContinuousExport Serviceverknüpfte Rolle unter Verwendung der IAM-Konsole, der IAM-CLI oder der IAM-API. Wenn Sie die Funktionen Discovery Service — Continuous Export, die diese serviceverknüpfte Rolle erfordern, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

> **Note**
>
> Sie müssen Ihre serviceverknüpfte Rolle zunächst bereinigen, bevor Sie sie löschen können. Siehe Bereinigen der serviceverknüpften Rolle.

Fehlerbehebung bei AWS Application Discovery Service Identität und Zugriff

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

Themen

- Ich bin nicht berechtigt, IAM durchzuführen: PassRole

Ich bin nicht berechtigt, IAM durchzuführen: PassRole

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht berechtigt sind, die `iam:PassRole` Aktion auszuführen, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an den Application Discovery Service übergeben 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 im Application Discovery Service 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 zur Verfügung gestellt.

Protokollieren und Überwachen in AWS Application Discovery Service

AWS Application Discovery Service ist in AWS CloudTrail integriert. Sie können es verwenden CloudTrail um Kontoaktivitäten für Fehlerbehebungs- und Überwachungszwecke zu protokollieren, kontinuierlich zu überwachen und beizubehalten. CloudTrail bietet eine Event-Historie IhrerAWSKontoaktivität, einschließlich Aktionen, die über dieAWS-Managementkonsole,AWS-SDKs und Befehlszeilen-Tools. Im Thema in diesem Abschnitt wird erläutert, wie Sie verwenden CloudTrail mit Application Discovery Service.

Themen

- Protokollieren von API-Aufrufen mit Application Discovery ServiceAWS CloudTrail

Protokollieren von API-Aufrufen mit Application Discovery ServiceAWS CloudTrail

AWS Application Discovery Serviceist in integriert.AWS CloudTrail, ein Service, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einemAWSApplication Discovery Service. CloudTrail erfasst alle API-Aufrufe für Application Discovery Service als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von Application Discovery Service und Code-Aufrufe der API-Operationen mit Application Discovery Service.

Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignisse in einem Amazon S3 S3-Bucket, einschließlich Ereignisse für Application Discovery Service. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse in der CloudTrail -Konsole inEreignisverlauf der Ereignisse. Verwendung der gesammelten Informationen von CloudTrailkönnen Sie die an Application Discovery Service, die IP-Adresse, die IP-Adresse, die IP-Adresse, die IP-Adresse, die IP-Adresse, die IP-Adresse, die IP-Adresse, die IP-Adresse, die IP-Adresse, die IP-Adresse, die IP-Adresse, die IP-Adresse, der

Für weitere Informationen über CloudTrailfinden Sie unter.AWS CloudTrailBenutzerhandbuch.

Application Discovery Service in CloudTrail

CloudTrail ist auf Ihrem aktiviertAWS-Konto, wenn Sie das -Konto erstellen. Die in Application Discovery Service wird in einem CloudTrail Veranstaltung zusammen mit anderenAWS-Service-Ereignisse inEreignisverlauf der Ereignisse. Sie können die neusten Ereignisse in Ihr AWS-Konto herunterladen und dort suchen und anzeigen. Weitere Informationen finden Sie unterAnzeigen von Ereignissen mit CloudTrail Geschichte der Veranstaltung.

Zur kontinuierlichen Aufzeichnung von Ereignissen in IhremAWS-Konto, einschließlich Ereignisse für Application Discovery Service, erstellen Sie einen Trail. EINWanderwegaktiviert CloudTrail um Protokolldateien an einen Amazon S3 S3-Bucket zu übermitteln. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS-Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon S3 Bucket bereit. Darüber hinaus können Sie andere konfigurieren.AWSServices zur weiteren Analyse und Reaktion auf die in gesammelten Ereignisdaten CloudTrail protokolliert. Weitere Informationen finden Sie unter:

- Übersicht zum Erstellen eines Trails
- CloudTrail Von unterstützte Services und Integrationen

- Konfigurieren von Amazon SNS-Benachrichtigungen für CloudTrail
- Empfangen CloudTrail Protokolldateien aus mehreren RegionenundEmpfangen CloudTrail Protokolldateien aus mehreren Konten

Alle Application Discovery Service werden von protokolliert. CloudTrail und sind dokumentiert in derApplication Discovery Service. Aufrufe von werden zum Beispiel die`CreateTags`,`DescribeTags`, und`GetDiscoverySummary`Aktionen generieren Einträge im CloudTrail -Protokolldateien.

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 Stammbenutzer- oder AWS Identity and Access Management (IAM)-Anmeldeinformationen ausgeführt wurde.
- Ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer ausgeführt wurde.
- Ob die Anforderung aus einem anderen AWS-Service gesendet wurde

Weitere Informationen finden Sie unter CloudTrail userIdentity-Element.

Grundlegendes Application Discovery Service Logdateieinträgen

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 -Protokolldateien sind kein geordnetes Stack-Trace der öffentlichen API-Aufrufe und erscheinen daher in keiner bestimmten Reihenfolge.

Das folgende Beispiel zeigt eine CloudTrail Logeintrag, der das demonstriert`DescribeTags`-Aktion.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAJBHMC4H6EKEXAMPLE:sample-user",
        "arn": "arn:aws:sts::444455556666:assumed-role/ReadOnly/sample-user",
```

```
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDAJQABLZS4A3QDU576Q",
                "arn": "arn:aws:iam::444455556666:role/ReadOnly",
                "accountId": "444455556666",
                "userName": "sampleAdmin"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2020-05-05T15:19:03Z"
            }
        }
    },
    "eventTime": "2020-05-05T17:02:40Z",
    "eventSource": "discovery.amazonaws.com",
    "eventName": "DescribeTags",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "20.22.33.44",
    "userAgent": "Coral/Netty4",
    "requestParameters": {
        "maxResults": 0,
        "filters": [
            {
                "values": [
                    "d-server-0315rfdjreyqsq"
                ],
                "name": "configurationId"
            }
        ]
    },
    "responseElements": null,
    "requestID": "mgh-console-eb1cf315-e2b4-4696-93e5-b3a3b9346b4b",
    "eventID": "7b32b778-91c9-4c75-9cb0-6c852791b2eb",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

AWS Application Discovery Service-Kontingente

Die Konsole „Servicekontingente“ stellt Informationen zu AWS Application Discovery Service-Kontingenten bereit. Sie können die Service Quotas Quotas-Konsole verwenden, um die Standard-Servicekontingentkontingentkonsole anzuzeigen oderAnfordern Kontingenterhöhungenfür einstellbare Kontingente.

Derzeit ist die einzige Quote, die erhöht werden kannImportierte Server pro Kontoaus.

Der Application Discovery Service hat die folgenden Standardkontingente:

- 1.000 Anwendungen pro Konto.

  Wenn Sie dieses Kontingent erreichen und neue Anwendungen importieren möchten, können Sie vorhandene Anwendungen mit`DeleteApplications`--API-Aktion. Weitere Informationen finden Sie unterDeleteApplicationsimApplication Discovery Service -API-Referenzaus.
- Jede Importdatei kann maximal 10 MB groß sein.
- 25.000 importierte Serverdatensätze pro Konto.
- 25.000 Löschungen von Importdatensätzen pro Tag.
- 10.000 importierte Server pro Konto (Sie können die Erhöhung dieses Kontingents beantragen).
- 1.000 aktive Agenten, die Daten sammeln und an Application Discovery Service senden.
- 10.000 inaktive Agenten, die reagieren, aber keine Daten sammeln.
- 400 Server pro Anwendung.
- 30 Tags pro Server.

Problembehebung AWS Application Discovery Service

In diesem Abschnitt finden Sie Informationen dazu, wie häufige Probleme mit AWS Application Discovery Service behoben werden.

Themen

Stoppen Sie die Datenerfassung durch Datenexploration

Um die Datenexploration zu beenden, können Sie entweder den Kippschalter in der Migration Hub Hub-Konsole unter Discover > Data Collectors > Agents ausschalten oder die `StopContinuousExport` API aufrufen. Es kann bis zu 30 Minuten dauern, bis die Datenerfassung beendet ist. Während dieser Phase wird auf dem Kippschalter an der Konsole und beim `DescribeContinuousExport` API-Aufruf der Status „Stopp In Progress“ angezeigt.

> **Note**
>
> Wenn der Schieberegler nach dem Aktualisieren der Konsolenseite nicht deaktiviert wird und eine Fehlermeldung ausgegeben wird oder wenn die `DescribeContinuousExport`-API als Zustand "Stop_Failed" zurückgibt, können Sie erneut versuchen, den Schieberegler zu deaktivieren oder die `StopContinuousExport`-API aufzurufen. Wenn bei der „Datenexploration“ weiterhin ein Fehler angezeigt wird und der Vorgang nicht erfolgreich beendet werden kann, wenden Sie sich bitte an den AWS Support.

Alternativ können Sie die Datensammlung manuell beenden, wie in den folgenden Schritten beschrieben.

Option 1: Beenden der Agent-Datensammlung

Wenn Sie die Erkennung bereits mit ADS-Agenten durchgeführt haben und im ADS Datenbank-Repository keine weiteren Daten mehr sammeln möchten:

1. Wählen Sie in der Migration Hub Hub-Konsole Discover > Data Collectors > Agents aus.
2. Wählen Sie alle vorhandenen laufenden Agenten aus und klicken Sie auf Stop Data Collection (Beenden der Datensammlung).

   Dadurch wird sichergestellt, dass von den Agenten sowohl im ADS-Daten-Repository als auch in Ihrem S3-Bucket keine neuen Daten gesammelt werden. Ihre vorhandenen Daten bleiben verfügbar.

Option 2: Amazon Kinesis Data Streams von Data Exploration löschen

Wenn Sie weiterhin Daten von Agenten im ADS-Daten-Repository sammeln möchten, aber keine Daten in Ihrem Amazon S3 S3-Bucket mithilfe der Datenexploration sammeln möchten, können Sie die Amazon Data Firehose-Streams, die durch die Datenexploration erstellt wurden, manuell löschen:

1. Melden Sie sich über die AWS Konsole bei Amazon Kinesis an und wählen Sie im Navigationsbereich Data Firehose aus.
2. Löschen Sie die folgenden Streams, die mit der Funktion zur Datenerkundung erstellt wurden:

   - `aws-application-discovery-service-id_mapping_agent`
   - `aws-application-discovery-service-inbound_connection_agent`
   - `aws-application-discovery-service-network_interface_agent`
   - `aws-application-discovery-service-os_info_agent`
   - `aws-application-discovery-service-outbound_connection_agent`
   - `aws-application-discovery-service-processes_agent`
   - `aws-application-discovery-service-sys_performance_agent`

Entfernen Sie die bei der Datenexploration gesammelten Daten

Um Daten zu entfernen, die bei der Datenexploration gesammelt wurden

1. Entfernen Sie die in Amazon S3 gespeicherten Discovery Agent-Daten.

   Daten, die von AWS Application Discovery Service (ADS) gesammelt wurden, werden in einem S3-Bucket mit dem Namen gespeichert`aws-application-discover-discovery-service-`*`uniqueid`*.

> **Note**
>
> Das Löschen des Amazon S3 S3-Buckets oder eines der Objekte darin, während die Datenexploration in Amazon Athena aktiviert ist, führt zu einem Fehler. Es sendet weiterhin neue Discovery-Agent-Daten an S3. Die gelöschten Daten werden auch in Athena nicht mehr zugänglich sein.

2. Entfernen AWS Glue Data Catalog.

   Wenn die Datenexploration in Amazon Athena aktiviert ist, wird in Ihrem Konto ein Amazon S3 S3-Bucket erstellt, in dem die von ADS-Agenten in regelmäßigen Zeitabständen gesammelten Daten gespeichert werden. Darüber hinaus wird eine AWS Glue Data Catalog erstellt, mit der Sie die in einem Amazon S3-Bucket gespeicherten Daten von Amazon Athena abfragen können. Wenn Sie die Datenexploration in Amazon Athena deaktivieren, werden keine neuen Daten in Ihrem Amazon S3 S3-Bucket gespeichert, aber Daten, die zuvor gesammelt wurden, bleiben bestehen. Wenn Sie diese Daten nicht mehr benötigen und Ihr Konto in den Zustand zurückversetzen möchten, in dem die Datenexploration in Amazon Athena aktiviert wurde.

   a. Rufen Sie Amazon S3 von der AWS Konsole aus auf und löschen Sie manuell den Bucket mit dem Namen "aws-application-discover-discovery-service-uniqueid“

   b. Sie können den AWS Glue Data Catalog zur Datenexploration manuell entfernen, indem Sie die application-discovery-service-databaseDatenbank und all diese Tabellen löschen:

      - `os_info_agent`
      - `network_interface_agent`
      - `sys_performance_agent`
      - `processes_agent`
      - `inbound_connection_agent`
      - `outbound_connection_agent`
      - `id_mapping_agent`

Ihre Daten entfernen von AWS Application Discovery Service

Um all Ihre Daten aus dem Application Discovery Service entfernen zu lassen, wenden Sie sich an den AWS Support und fordern Sie die vollständige Datenlöschung an.

Beheben Sie häufig auftretende Probleme bei der Datenexploration in Amazon Athena

In diesem Abschnitt finden Sie Informationen zur Behebung häufiger Probleme bei der Datenexploration in Amazon Athena.

Themen

Die Datenexploration in Amazon Athena kann nicht initiiert werden, da serviceverknüpfte Rollen und erforderliche AWS Ressourcen nicht erstellt werden können

Wenn Sie die Datenexploration in Amazon Athena aktivieren, wird in Ihrem Konto die serviceverknüpfte Rolle erstelltAWSServiceRoleForApplicationDiscoveryServiceContinuousExport, die es ihr ermöglicht, die erforderlichen AWS Ressourcen zu erstellen, um die vom Agenten gesammelten Daten in Amazon Athena zugänglich zu machen, einschließlich eines Amazon S3 S3-Buckets, Amazon Kinesis Kinesis-Streams und. AWS Glue Data Catalog Wenn Ihr Konto nicht über die erforderlichen Berechtigungen für die Datenexploration in Amazon Athena verfügt, um diese Rolle zu erstellen, kann sie nicht initialisiert werden. Weitere Informationen finden Sie unter AWS Von verwaltete Richtlinien für AWS Application Discovery Service.

Neue Agentendaten werden in Amazon Athena nicht angezeigt

Wenn keine neuen Daten in Athena fließen, es mehr als 30 Minuten her ist, dass ein Agent gestartet wurde und der Status der Datenexploration Aktiv lautet, überprüfen Sie die unten aufgeführten Lösungen:

- AWS Discovery-Agenten

Stellen Sie sicher, dass der Status Collection (Sammlung) des Agenten als Started (Gestartet) und der Status Health (Zustand) als Running (Läuft) markiert ist.

- Kinesis-Role

  Stellen Sie sicher, dass Sie in Ihrem Konto über die Rolle `AWSApplicationDiscoveryServiceFirehose` verfügen.

- Firehose-Status

  Stellen Sie sicher, dass die Firehose Firehose-Lieferstreams ordnungsgemäß funktionieren:

  - `aws-application-discovery-service/os_info_agent`
  - `aws-application-discovery-service-network_interface_agent`
  - `aws-application-discovery-service-sys_performance_agent`
  - `aws-application-discovery-service-processes_agent`
  - `aws-application-discovery-service-inbound_connection_agent`
  - `aws-application-discovery-service-outbound_connection_agent`
  - `aws-application-discovery-service-id_mapping_agent`

- AWS Glue Data Catalog

  Stellen Sie sicher, dass die `application-discovery-service-database` Datenbank vorhanden ist. AWS Glue Stellen Sie sicher, dass die folgenden Tabellen in AWS Glue vorhanden sind:

  - `os_info_agent`
  - `network_interface_agent`
  - `sys_performance_agent`
  - `processes_agent`
  - `inbound_connection_agent`
  - `outbound_connection_agent`
  - `id_mapping_agent`

- Amazon S3 Bucket

Stellen Sie sicher, dass `aws-application-discovery-service-uniqueid` in Ihrem Konto ein Amazon S3 S3-Bucket benannt ist. Wenn Objekte im Bucket verschoben oder gelöscht wurden, werden sie in Athena nicht richtig angezeigt.

- Ihre lokalen Server

  Stellen Sie sicher, dass Ihre Servern ausgeführt werden, sodass Ihr Agenten Daten sammeln und zu AWS Application Discovery Service senden können.

Sie verfügen nicht über ausreichende Berechtigungen für den Zugriff auf Amazon S3, Amazon Data Firehose oder AWS Glue

Wenn Sie Amazon Athena verwenden AWS Organizations und die Initialisierung für die Datenexploration in Amazon Athena fehlschlägt, kann dies daran liegen, dass Sie keine Zugriffsberechtigungen für Amazon S3, Amazon Data Firehose, Athena oder haben. AWS Glue

Sie benötigen einen IAM-Benutzer mit Administratorrechten, um Ihnen Zugriff auf diese Dienste zu gewähren. Ein Administrator kann diesen Zugriff über sein Konto gewähren. Siehe AWS Von verwaltete Richtlinien für AWS Application Discovery Service.

Um sicherzustellen, dass die Datenexploration in Amazon Athena ordnungsgemäß funktioniert, dürfen Sie die AWS Ressourcen, die durch die Datenexploration in Amazon Athena erstellt wurden, einschließlich des Amazon S3-Buckets, Amazon Data Firehose Streams und, nicht ändern oder löschen. AWS Glue Data Catalog Wenn Sie diese Ressourcen versehentlich löschen oder ändern, können Sie Data Exploration anhalten und wieder fortsetzen, damit diese Ressourcen automatisch erneut erstellt werden. Wenn Sie den Amazon S3 S3-Bucket löschen, der durch Datenexploration erstellt wurde, können Sie die im Bucket gesammelten Daten verlieren.

Fehlerbehebung bei fehlgeschlagenen Datensätzen

Mit dem Migration Hub-Import können Sie Details Ihrer lokalen Umgebung direkt in Migration Hub importieren, ohne den Discovery Connector oder Discovery Agent zu verwenden. Dadurch haben Sie die Möglichkeit, die Migrationsprüfung und -planung direkt von Ihren importierten Daten aus durchzuführen. Sie können auch Ihre Geräte als Anwendungen gruppieren und deren Migrationsstatus nachverfolgen.

Wenn Sie Daten importieren, ist es möglich, dass Fehler auftreten. Typischerweise treten diese Fehler aus einem der folgenden Gründe auf:

- Ein importbezogenes Kontingent wurde erreicht — Mit Importaufgaben ist ein Kontingent verknüpft. Wenn Sie eine Importaufgabenanfrage stellen, die die Kontingente überschreiten würde, schlägt die Anfrage fehl und es wird ein Fehler zurückgegeben. Weitere Informationen finden Sie unter AWS Application Discovery Service-Kontingente.
- Ein zusätzliches Komma (,) wurde in die Importdatei eingefügt — Kommas in CSV-Dateien werden verwendet, um ein Feld vom nächsten zu unterscheiden. Kommata in einem Feld werden nicht unterstützt, da das Feld dadurch immer geteilt wird. Dies kann zu einer Kaskade von Formatierungsfehlern führen. Stellen Sie sicher, dass Kommata nur zwischen Feldern und nicht in anderer Weise in Ihren Importdateien verwendet werden.
- Ein Feld hat einen Wert außerhalb seines unterstützten Bereichs — Manche Felder, wie z. B., `CPU.NumberOfCores` müssen einen Wertebereich haben, den sie unterstützen. Wenn Sie der unterstützte Bereich unter- oder überschritten wird, wird der Datensatz nicht importiert.

Wenn bei Ihrer Importanfrage Fehler auftreten, können Sie diese beheben, indem Sie die fehlgeschlagenen Datensätze für Ihre Importaufgabe herunterladen, die Fehler in der CSV-Datei mit den fehlgeschlagenen Einträgen beheben und den Import erneut durchführen.

Console

So laden Sie das Archiv mit Ihren fehlgeschlagenen Datensätzen herunter:

1. Melden Sie sich bei an und öffnen Sie die Migration Hub Hub-Konsole unterhttps://console.aws.amazon.com/migrationhub. AWS Management Console
2. Wählen Sie im Navigationsbereich links unter Discover (Entdecken) die Option Tools.
3. Wählen Sie unter Discovery Tools die Option view imports (Importe anzeigen).
4. Wählen Sie im Imports (Importe) -Dashboard das mit einer Importanfrage verbundene Optionsfeld mit einer Anzahl von Failed records (Fehlgeschlagenen Datensätzen).
5. Wählen Sie Download failed records (Fehlgeschlagene Datensätze herunterladen) aus der Tabelle auf dem Dashboard aus. Dadurch wird das Download-Dialogfeld Ihres Browsers für den Download der Archivdatei geöffnet.

AWS CLI

So laden Sie das Archiv mit Ihren fehlgeschlagenen Datensätzen herunter:

1. Öffnen Sie ein Terminalfenster, und geben Sie den folgenden Befehl ein, wobei *`ImportName`* `is the name of the import task with the failed entries that you want to correct.`:

   ```
   aws discovery describe-import-tasks - -name ImportName
   ```

2. Kopieren Sie aus der Ausgabe den gesamten Inhalt der für `errorsAndFailedEntriesZip` zurückgegebenen Wertes ohne die Anführungszeichen.
3. Öffnen Sie einen Webbrowser, fügen Sie den Inhalt in das URL-Textfeld ein, und betätigen Sie `ENTER`. Dadurch wird das Archiv der fehlgeschlagenen Datensätze im komprimierten .zip-Format heruntergeladen.

Nachdem Sie nun Ihr Archiv fehlgeschlagener Datensätze heruntergeladen haben, können Sie die beiden Dateien darin extrahieren und die Fehler korrigieren. Beachten Sie: Wenn Ihre Fehler durch servicebasierte Einschränkungen verursacht wurden, müssen Sie entweder eine Erweiterung dieser Beschränkungen beantragen oder eine ausreichende Menge der entsprechenden Ressourcen löschen, damit Ihr Konto die Grenzwerte wieder einhält. Das Archiv enthält die folgenden Dateien:

- errors-file.csv — Diese Datei ist Ihr Fehlerprotokoll und zeichnet die Zeile, den Spaltennamen und eine beschreibende Fehlermeldung für jeden fehlgeschlagenen Datensatz jedes fehlgeschlagenen Eintrags auf. `ExternalId`
- failed-entries-file.csv — Diese Datei enthält nur die fehlgeschlagenen Einträge aus Ihrer ursprünglichen Importdatei.

Um die aufgetretenen non-limit-based Fehler zu korrigieren, verwenden Sie die, `errors-file.csv` um die Probleme in der `failed-entries-file.csv` Datei zu korrigieren, und importieren Sie dann die Datei. Eine Anleitung zum Importieren dieser Dateien finden Sie unter Importieren von Daten.

Dokumentverlauf für AWS Application Discovery Service

Neuestes Update der Dokumentation zum Benutzerhandbuch: 16. Mai 2023

In der folgenden Tabelle sind wichtige Application Discovery Service nach 18. Januar 2019 beschrieben. Um Benachrichtigungen über Dokumentationsaktualisierungen zu erhalten, können Sie den RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Vorstellung der Agentless Collector-Datenbank und des Analysedatenerfassungsmoduls	Das Modul zur Erfassung von Datenbank- und Analysedaten ist das neue Modul von Application Discovery Service Agentless Collector (Agentless Collector). Sie können dieses Datenerfassungsmodul verwenden, um eine Verbindung zu Ihrer Umgebung herzustellen und Metadaten und Leistungskennzahlen von Ihrer lokalen Datenbank und Ihren Analyseservern zu sammeln. Weitere Informationen finden Sie unter Modul zur Erfassung von Datenbank- und Analysedaten.	16. Mai 2023
Wir stellen vor: Application Discovery Service Agentless Collector	Application Discovery Service Agentless Collector (Agentless Collector) ist die neue AWS Application Discovery Service lokale Anwendung, die mithilfe agentenloser Methoden Informationen über Ihre lokale Umgebung sammelt, um Sie	16. August 2022

	bei der effektiven Planung Ihrer Migration auf die zu unterstützen. AWS Cloud Weitere Informationen finden Sie unter Agentless	
IAM-Aktualisierung	Die `discovery:GetNetworkConnectionGraph` Aktion AWS Identity and Access Management (IAM) ist jetzt verfügbar, um beim Erstellen einer identitätsbasierten Richtlinie Zugriff auf das AWS Migration Hub Konsolennetzwerkdiagramm zu gewähren. Weitere Informationen finden Sie unter Erteilen von Berechtigungen zur Verwendung des Netzwerkschemas.	24. Mai 2022
Wir stellen die Heimatregion vor	Die Heimatregion des Migration Hub bietet ein einziges Repository mit Informationen zur Entdeckung und Migrationsplanung für Ihr gesamtes Portfolio sowie eine einzige Ansicht der Migrationen in mehrere AWS Regionen.	20. November 2019

Vorstellung der Importfunktion von Migration Hub	Mit dem Migration Hub-Import können Sie Informationen über Ihre lokalen Server und Anwendungen in Migration Hub importieren, einschließlich Serverspezifikationen und Nutzungsdaten. Sie können diese Daten auch verwenden, um den Status der Anwendungsmigrationen zu verfolgen. Weitere Informationen finden Sie unter Migration Hub - Benutzerhandbuch.	18. Januar 2019

In der folgenden Tabelle werden Dokumentationsversionen für das Application Discovery Service Service-Benutzerhandbuch beschrieben, die vor dem 18. Januar 2019 veröffentlicht wurden:

Änderung	Beschreibung	Datum
Neue Funktion	Die Dokumente wurden aktualisiert, um die Datenerkundung in Amazon Athena zu unterstützen, und ein Kapitel zur Fehlerbehebung wurde hinzugefügt.	09. August 2018
Hauptrevidierung	Details zur Nutzung und Ausgabe wurden umgeschrieben; das gesamte Dokument wurde umstrukturiert.	25. Mai 2018
Discovery Agent 2.0	Ein neuer und verbesserter Application Discovery-Agent wurde veröffentlicht.	19. Oktober 2017

Änderung	Beschreibung	Datum
Konsole	Der AWS Management Console wurde hinzugefügt.	19. Dezember 2016
Agentenlose Erkennung	In dieser Version wird beschrieben, wie die agentenlose Erkennung eingerichtet und konfiguriert wird.	28. Juli 2016
Neue Details für Microsoft Windows Server und Korrekturen für Probleme mit Befehlen	Dieses Update bietet neue Details zu Microsoft Windows Server. Es dokumentiert auch Korrekturen verschiedener Probleme mit Befehlen.	20. Mai 2016
Erste Veröffentlichung	Dies ist die erste Application Discovery Service Benutzerhandbuch.	12. Mai 2016

AWS-Glossar

Die neueste AWS-Terminologie finden Sie im AWS-Glossar in der AWS-Glossar-Referenz.

Anhang

Dieser Abschnitt enthält zusätzliche Informationen zu AWS Application Discovery Service.

Themen

Anhang: Übergang vom Discovery Connector zum Agentless Collector

In diesem Abschnitt wird beschrieben, wie Sie vom AWS Agentless Discovery Connector (Discovery Connector) zum Application Discovery Service Agentless Collector (Agentless Collector) wechseln.

Wir empfehlen Kunden, die derzeit Discovery Connector verwenden, auf den neuen Agentless Collector umzustellen.

Weitere Informationen zur Verwendung von Agentless Collector finden Sie unter Erste Schritte mit Agentless Collector.

Nachdem der Agentless Collector bereitgestellt wurde, können Sie die virtuelle Maschine des Discovery Connectors löschen. Alle zuvor erfassten Daten sind weiterhin in AWS Migration Hub (Migration Hub) verfügbar.

Anhang: AWS Agentless Discovery Connector

> **Important**
>
> Wir empfehlen Kunden, die derzeit Discovery Connector verwenden, auf den neuen Agentless Collector umzustellen. Weitere Informationen finden Sie unter Anhang: Übergang vom Discovery Connector zum Agentless Collector.

Themen

- Fehlerbehebung beim Discovery Connector

Vom Discovery Connector gesammelte Daten

Der Discovery Connector sammelt Informationen über Ihre Hosts und VMs von VMware vCenter Server. VMs Sie können diese Daten jedoch nur erfassen, wenn VMware vCenter-Servertools installiert sind. Informationen dazu, wie Sie sicherstellen, dass das von Ihnen verwendete AWS Konto über die erforderliche Berechtigung für diese Aufgabe verfügt, finden Sie unter AWS Von verwaltete Richtlinien für AWS Application Discovery Service.

Im Folgenden finden Sie ein Inventar der vom Discovery Connector gesammelten Informationen.

Tabellenlegende für vom Discovery Connector erfasste Daten:

- Gesammelte Daten sind Messungen in Kilobyte (KB), sofern nicht anders angegeben.
- Entsprechende Daten in der Migration Hub-Konsole werden in Megabyte (MB) angegeben.
- Datenfelder, die mit einem Sternchen (*) gekennzeichnet sind, sind nur in den CSV-Dateien verfügbar, die von der API-Exportfunktion des Konnektors erstellt werden.
- Der Abrufzeitraum ist in Intervallen von ca. 60 Minuten.
- Datenfelder mit einem doppelten Sternchen (**) geben derzeit den Wert Null zurück.

Datenfeld	Beschreibung
applicationConfigurationId*	ID der Migrationsanwendung, unter der die VM gruppiert ist
avgCpuUsageProzent	Durchschnittlicher Prozentsatz der CPU-Nutzung über den Abrufzeitraum
avgDiskBytesReadPerSecond	Durchschnittliche Anzahl von Bytes, die über den Abrufzeitraum hinweg von der Festplatte gelesen wurden
avgDiskBytesWrittenPerSecond	Durchschnittliche Anzahl von Bytes, die über den Abrufzeitraum hinweg auf die Festplatte geschrieben wurden

Datenfeld	Beschreibung
avgDiskReadOpsPerSecond**	Durchschnittliche Anzahl von E/A-Lesev orgängen pro Sekunde null
avgDiskWriteOpsPerSecond**	Durchschnittliche Anzahl von E/A-Schre ibvorgängen pro Sekunde
avgFreeRAM	Durchschnittliche kostenlose RAM in MB
avgNetworkBytesReadPerSecond	Durchschnittlicher Durchsatz der pro Sekunde gelesenen Bytes
avgNetworkBytesWrittenPerSecond	Durchschnittlicher Durchsatz der pro Sekunde geschriebenen Bytes
configId	Application Discovery Service hat der erkannten VM eine ID zugewiesen
configType	Typ der erkannten Ressource
connectorId	ID der virtuellen Discovery Connector-Applianc e
cpuType	vCPU für eine VM, tatsächliches Modell für einen Host
datacenterId	ID des vCenter
hostId*	ID des VM-Hosts
hostName	Name des Hosts, auf dem die Virtualis ierungssoftware ausgeführt wird
hypervisor	Typ des Hypervisors
id	ID des Servers
lastModifiedTimeZeitstempel*	Datum und Uhrzeit der letzten Datensammlung vor dem Datenexport

Datenfeld	Beschreibung
macAddress	MAC-Adresse der VM
manufacturer	Hersteller der Virtualisierungssoftware
maxCpuUsageProzent	Max. Prozentsatz der CPU-Nutzung während des Abrufzeitraums
maxDiskBytesReadPerSecond	Max. Anzahl von Bytes, die über den Abrufzeit raum hinweg vom der Festplatte gelesen wurden
maxDiskBytesWrittenPerSecond	Max. Anzahl von Bytes, die über den Abrufzeit raum hinweg auf die Festplatte geschrieben wurden
maxDiskReadOpsPerSecond**	Max. Anzahl der E/A-Lesevorgänge pro Sekunde
maxDiskWriteOpsPerSecond**	Max. Anzahl der E/A-Schreibvorgänge pro Sekunde
maxNetworkBytesReadPerSecond	Max. Durchsatz der pro Sekunde gelesenen Bytes
maxNetworkBytesWrittenPerSecond	Max. Durchsatz der pro Sekunde geschrieb enen Bytes
memoryReservation*	Limit zur Vermeidung hoher Arbeitsspeichernut zung auf der VM
moRefId	Eindeutige vCenter Managed Object-Referenz-ID
name*	Name der VM oder des Netzwerks (vom Benutzer angegeben)
numCores	Anzahl der unabhängigen Verarbeitungseinhe iten innerhalb der CPU

Datenfeld	Beschreibung
numCpus	Anzahl der Zentraleinheiten auf der VM
numDisks**	Anzahl der Festplatten auf der VM
numNetworkCards**	Anzahl der Netzwerkkarten auf der VM
osName	Name des Betriebssystems auf der VM
osVersion	Version des Betriebssystems auf der VM
portGroupId*	ID der Gruppe von Mitgliedsports des VLAN
portGroupName*	Name der Gruppe von Mitgliedsports des VLAN
powerState*	Status der Stormversorgung
serverId	Application Discovery Service hat der erkannten VM eine ID zugewiesen
smBiosId*	ID/Version des Systemverwaltungs-BIOS
state*	Status der virtuellen Appliance des Discovery Connector
toolsStatus	Betriebszustand der VMware-Tools (eine vollständige Liste finden Sie unter Datensammler anzeigen und sortieren)
totalDiskSize	Gesamtkapazität der Festplatte in MB
totalRAM	Gesamtkapazität des verfügbaren Arbeitsspeichers auf der VM in MB
Typ	Hosttyp
vCenterId	Eindeutige ID-Nummer einer VM
vCenterName*	Name des vCenter-Hosts

Datenfeld	Beschreibung
virtualSwitchName*	Name des virtuellen Switch
vmFolderPath	Verzeichnispfad der VM-Dateien
vmName	Name der virtuellen Maschine

Datenerfassung des Discovery Connectors

Nachdem der Discovery Connector in Ihrer VMware-Umgebung bereitgestellt und konfiguriert wurde, können Sie ihn neu starten, wenn Datenerfassungen beendet werden. Sie können die Datenerfassung über die Konsole oder durch API-Aufrufe über die starten oder beenden AWS CLI. Beide Methoden werden in den folgenden Verfahren beschrieben.

Using the Migration Hub Console

Das folgende Verfahren zeigt, wie Sie den Discovery-Connector-Datenerfassungsprozess auf der Seite Data Collectors der Migration-Hub-Konsole starten oder beenden.

So starten oder stoppen Sie die Datenerfassung

1. Klicken Sie im Navigationsbereich auf Data Collectors (Datensammler).
2. Wählen Sie die Registerkarte Connectors (Konnektoren).
3. Aktivieren Sie das Kontrollkästchen des Connectors, den Sie starten oder stoppen möchten.
4. Wählen Sie Start data collection (Beginnen der Datensammlung) oder Stop data collection (Beenden der Datensammlung).

> **Note**
>
> Wenn Sie keine Inventarinformationen sehen, nachdem Sie die Datensammlung mit dem Konnektor begonnen haben, vergewissern Sie sich, dass Sie den Konnektor bei Ihrem vCenter Server registriert haben.

Using the AWS CLI

Um den Discovery-Connector-Datenerfassungsprozess von der aus zu starten AWS CLI, AWS CLI muss zuerst in Ihrer Umgebung installiert werden, und dann müssen Sie die CLI so einstellen, dass sie die von Ihnen ausgewählte Migration-Hub-Heimatregion verwendet.

So installieren Sie die AWS CLI und starten die Datenerfassung

1. Installieren Sie die AWS CLI für Ihr Betriebssystem (Linux, macOS oder Windows). Anweisungen finden Sie im AWS Command Line Interface -Benutzerhandbuch.
2. Öffnen Sie die Eingabeaufforderung (Windows) oder das Terminal (Linux oder macOS).
   a. Geben Sie `aws configure` ein und drücken Sie die Eingabetaste.
   b. Geben Sie Ihre AWS Zugriffsschlüssel-ID und Ihren AWS geheimen Zugriffsschlüssel ein.
   c. Geben Sie Ihre Heimatregion als Standardregionsnamen ein. Beispiel: `us-west-2`
   d. Geben Sie als Standard-Ausgabeformat `text` ein.
3. Um die ID des Connectors zu finden, für den Sie die Datenerfassung starten oder beenden möchten, geben Sie den folgenden Befehl ein, um die ID des Connectors anzuzeigen:

```
aws discovery describe-agents --filters
 condition=EQUALS,name=hostName,values=connector
```

4. Um die Datenerfassung durch den Konnektor zu starten, geben Sie den folgenden Befehl ein:

```
aws discovery start-data-collection-by-agent-ids --agent-ids <connector ID>
```

> **Note**
>
> Wenn Sie keine Inventarinformationen sehen, nachdem Sie die Datensammlung mit dem Konnektor begonnen haben, vergewissern Sie sich, dass Sie den Konnektor bei Ihrem vCenter Server registriert haben.

Um die Datenerfassung durch den Konnektor zu beenden, geben Sie den folgenden Befehl ein:

```
aws discovery stop-data-collection-by-agent-ids --agent-ids <connector ID>
```

Fehlerbehebung beim Discovery Connector

Dieser Abschnitt enthält Themen, die Ihnen bei der Behebung bekannter Probleme mit Application Discovery Service Discovery Connector helfen können.

Behebung von Discovery Connector kann AWS während der Einrichtung nicht erreicht werden

Wenn Sie den AWS Agentless Discovery Connector in der Konsole konfigurieren, erhalten Sie die folgende Fehlermeldung:

> **Nicht erreicht AWS**
>
> AWS kann nicht erreicht werden (Verbindung zurücksetzen). Bitte überprüfen Sie die Netzwerk- und Proxy-Einstellungen.

Dieser Fehler tritt auf, weil der Discovery Connector nicht versucht hat, eine HTTPS-Verbindung zu einer AWS Domäne herzustellen, mit der der Konnektor während des Einrichtungsprozesses kommunizieren muss. Die Konfiguration von Discovery Connector schlägt fehl, wenn keine Verbindung hergestellt werden kann.

So beheben Sie die Verbindung zu AWS

1. Wenden Sie sich an Ihren IT-Administrator, um zu erfahren, ob Ihre Unternehmens-Firewall ausgehenden Datenverkehr auf Port 443 zu einer der AWS Domänen blockiert, die ausgehenden Zugriff benötigen.

   Die folgenden AWS Domains benötigen ausgehenden Zugriff:

   - `awsconnector.`*`Migration Hub home Region`*`.amazonaws.com`
   - `sns.`*`Migration Hub home Region`*`.amazonaws.com`
   - `arsenal-discovery.`*`Migration Hub home Region`*`.amazonaws.com`
   - `iam.amazonaws.com`
   - `aws.amazon.com`

- `ec2.amazonaws.com`

Wenn Ihre Firewall ausgehenden Datenverkehr blockiert, entsperren Sie ihn. Nachdem Sie die Firewall aktualisiert haben, konfigurieren Sie den Connector neu.

2. Wenn das Verbindungsproblem durch das Aktualisieren der Firewall nicht behoben wird, überprüfen Sie, ob die virtuelle Konnektor-Maschine über ausgehende Netzwerkkonnektivität zu den aufgelisteten Domains verfügt. Wenn die virtuelle Maschine über ausgehende Konnektivität verfügt, testen Sie die Verbindung zu aufgelisteten Domains, indem Sie Telnet auf Ports 443 ausführen, wie im folgenden Beispiel gezeigt.

```
telnet ec2.amazonaws.com 443
```

3. Wenn die ausgehende Konnektivität von der virtuellen Maschine aktiviert ist, müssen Sie sich an den -AWS Support wenden, um weitere Informationen zur Fehlerbehebung zu erhalten.

Behebung fehlerhafter Connectors

Zustandsinformationen für jeden Discovery Connector finden Sie auf der Seite Data Collectors der Migration Hub-Konsole. Konnektoren mit Problemen können anhand des Health (Zustand)-Werts Unhealthy (Fehlerhaft) identifiziert werden. Im folgenden Verfahren wird beschrieben, wie Sie auf die Konnektorkonsole zugreifen, um Zustandsprobleme zu identifizieren.

Zugreifen auf eine Konnektorkonsole

1. Öffnen Sie die Migration Hub-Konsole in einem Webbrowser und wählen Sie in der linken Navigation Data Collectors aus.
2. Notieren Sie sich die auf der Registerkarte Connectors (Konnektoren) angezeigte IP address (IP-Adresse) jedes Konnektors mit dem Zustand Unhealthy (Fehlerhaft) hat.
3. Öffnen Sie einen Browser auf jedem Computer, der eine Verbindung zur virtuellen Konnektor-Maschine herstellen kann, und geben Sie die URL der Konnektor-Konsole ein, `https://`*`ip_address_of_connector`*, wobei die IP-Adresse eines fehlerhaften Konnektors `ip_address_of_connector` ist.
4. Geben Sie das Passwort für die Konnektorverwaltungskonsole ein, das beim Konfigurieren des Konnektors eingerichtet wurde.

Sobald Sie Zugriff auf die Konnektorkonsole haben, können Sie Maßnahmen ergreifen, um den fehlerhaften Status zu beheben. Hier können Sie View Info (Informationen anzeigen) für vCenter connectivity (vCenter-Konnektivität) auswählen, damit ein Dialogfeld mit einer Diagnosemeldung angezeigt wird. Der Link View Info (Informationen anzeigen) ist erst für Konnektoren ab Version 1.0.3.12 verfügbar.

Nach dem Beheben der Zustandsprobleme stellt der Konnektor die Verbindung zum vCenter-Server wieder her und der Status des Konnektors wechselt zu HEALTHY (FEHLERFREI). Wenn die Probleme weiterhin bestehen, wenden Sie sich an den -AWS Support.

Die häufigsten Ursachen für fehlerhafte Konnektoren sind falsche IP-Adressen und Anmeldeinformationen. In den folgenden Abschnitten wird beschrieben, wie Sie diese Probleme beheben und den fehlerhaften Zustand von Konnektoren beseitigen können.

Themen

Probleme mit IP-Adressen

Ein Konnektor kann den fehlerhaften Zustand erhalten, wenn der bei der Einrichtung des Konnektors bereitgestellte vCenter-Endpunkt falsch formatiert oder ungültig ist oder der vCenter-Server derzeit heruntergefahren und nicht erreichbar ist. Wenn Sie in diesem Fall View Info (Informationen anzeigen) für vCenter connectivity (vCenter-Konnektivität) auswählen, wird ein Dialogfeld mit der Meldung "Confirm the operational status of your vCenter server, or choose Edit Settings to update the vCenter endpoint. (Bestätigen Sie die Betriebsbereitschaft des vCenter-Servers oder wählen Sie "Edit Settings (Einstellungen bearbeiten)" aus, um den vCenter-Endpunkt zu aktualisieren.)" angezeigt.

Das folgende Verfahren kann bei der Behebung von IP-Adressproblemen helfen.

1. Wählen Sie in der Konnektorkonsole (`https://`*`ip_address_of_connector`*) Edit Settings (Einstellungen bearbeiten) aus.
2. Wählen Sie im linken Navigationsbereich Step 5: Discovery Connector Set Up (Schritt 5: Discovery Connector-Einrichtung) aus.
3. Notieren Sie sich die unter Configure vCenter credentials (vCenter-Anmeldeinformationen konfigurieren) angezeigte vCenter Host (vCenter-Host)-IP-Adresse.
4. Überprüfen Sie mithilfe eines separaten Befehlszeilen-Tools wie `ping` oder `traceroute`, ob der zugehörige vCenter-Server aktiv und die IP von der Konnektor-VM aus erreichbar ist.

- Wenn die IP-Adresse falsch und der vCenter-Service aktiv ist, aktualisieren Sie die IP-Adresse in der Konnektorkonsole und wählen Sie dann Next (Weiter) aus.
- Wenn die IP-Adresse richtig, der vCenter-Server aber inaktiv ist, aktivieren Sie den Server.
- Wenn die IP-Adresse richtig und der vCenter-Server aktiv ist, prüfen Sie, ob er aufgrund der Firewall-Einstellungen eingehende Netzwerkverbindungen blockiert. Ist dies der Fall, aktualisieren Sie die Firewall-Einstellungen, damit eingehende Verbindungen aus der Konnektor-VM zugelassen werden.

Probleme mit Anmeldeinformationen

Konnektoren können in einen fehlerhaften Zustand versetzt werden, wenn die im Rahmen der Konnektoreinrichtung angegebenen vCenter-Anmeldeinformationen ungültig sind oder keine vCenter-Lese- und Anzeigeberechtigungen gewähren. Wenn Sie in diesem Fall View Info (Informationen anzeigen) für vCenter connectivity (vCenter-Konnektivität) auswählen, wird ein Dialogfeld mit der Meldung "Choose Edit Settings to update your vCenter username and password for your account with read and view privileges. (Wählen Sie "Edit settings (Einstellungen bearbeiten)" aus, um dem vCenter-Benutzernamen und -Passwort für das Konto Lese- und Anzeigeberechtigungen zu gewähren.)" angezeigt.

Das folgende Verfahren kann bei der Behebung von Problemen mit den Anmeldeinformationen helfen. Stellen Sie zunächst sicher, dass Sie einen vCenter-Benutzer erstellt haben, der über Lese- und Anzeigeberechtigungen auf dem vCenter-Server verfügt.

1. Wählen Sie in der Konnektorkonsole (`https://`*`ip_address_of_connector`*) Edit Settings (Einstellungen bearbeiten) aus.
2. Wählen Sie im linken Navigationsbereich Step 5: Discovery Connector Set Up (Schritt 5: Discovery Connector-Einrichtung) aus.
3. Aktualisieren Sie unter Configure vCenter credentials (vCenter-Anmeldeinformationen konfigurieren) die Werte für vCenter Username (vCenter-Benutzername) und vCenter Password (vCenter-Passwort) mit den Anmeldeinformationen eines vCenter-Benutzers, der Lese- und Anzeigeberechtigungen besitzt.
4. Wählen Sie Next (Weiter) aus, um die Einrichtung abzuschließen.

Eigenständige ESX-Host-Unterstützung

Der Discovery Connector unterstützt keinen eigenständigen ESX-Host. Der ESX-Host muss Teil der vCenter Server-Instance sein.

Zusätzliche Unterstützung für Konnektor-Probleme erhalten

Wenn Sie Probleme haben und Hilfe benötigen, wenden Sie sich an den -AWS Support. Sie werden möglicherweise gebeten, die Konnektor-Protokolle zu senden. Um die Protokolle zu erhalten, gehen Sie wie folgt vor:

- Melden Sie sich wieder bei der AWS Agentless Discovery Connector-Konsole an und wählen Sie Protokollpaket herunterladen aus.
- Sobald das Protokollpaket ganz heruntergeladen wurde, senden Sie es gemäß den Anweisungen von AWS -Support.

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.