ユーザーガイド

AWS Application Discovery Service

AWS Application Discovery Service: ユーザーガイド

Table of Contents

AWS Application Discovery Service の概要

AWS Application Discovery Serviceオンプレミスサーバーとデータベースに関する使用状況と設定のデータを収集することで、AWSクラウドへの移行を計画できます。Application Discovery Service は AWS Migration HubAWS Database Migration Serviceと統合されています。Migration Hub は、移行ステータス情報を単一のコンソールに集約するため、移行の追跡が簡素化されます。ホームリージョン内の Migration Hub コンソールから、検出されたサーバーを表示し、それらをアプリケーション別に分類して、各アプリケーションの移行ステータスを追跡することができます。DMS Fleet Advisor を使用して、データベースワークロードの移行オプションを評価できます。

検出されたすべてのデータは、AWS Migration Hubホームリージョンに保存されます。このため、検出および移行アクティビティを実行する前に、Migration Hub コンソールで、または CLI コマンドを使用して、ホームリージョンを設定する必要があります。データは、Microsoft Excel、または Amazon Athena および AmazonAWS などの分析ツールでの分析のためにエクスポートできます QuickSight。

Application Discovery Service API を使用して、検出されたサーバーのシステムパフォーマンスと使用率データをエクスポートできます。このデータをコストモデルに入力して、AWSそれらのサーバーの運用コストを計算します。さらに、サーバー間に存在するネットワーク接続に関するデータをエクスポートできます。この情報により、サーバー間のネットワーク依存関係を確認し、サーバーをアプリケーションとしてグループ化して、移行計画に役立てることができます。

> **Note**
>
> データはホームリージョンに保存されるため、AWS Migration Hub検出プロセスを開始する前に、ホームリージョンを設定する必要があります。ホームリージョンの使用の詳細については、「ホームリージョン」を参照してください。

Application Discovery Service は、オンプレミスサーバーを検出してそれらに関するデータを収集する方法を 2 つ提供します。

- エージェントレス検出は、VMware vCenter を通じて Application Discovery Service Agentless Connector (エージェントレスコレクター) (OVA ファイル) をデプロイすることによって実行できます。エージェントレスコレクターが設定されると、vCenter に関連付けられている仮想マシン (VM) とホストを特定します。Agentless Collector は、サーバーホスト名、IP アドレス、MAC アドレス、ディスクリソースの割り当て、データベースエンジンのバージョン、データベーススキー

マの静的設定データを収集します。さらに、各仮想マシンとデータベースの使用率データを収集し、CPU、RAM、ディスク I/O などの指標の平均使用率とピーク使用率を提供します。

- エージェントベース検出は、VM と物理サーバーのそれぞれにAWS Application Discovery Agent をデプロイすることによって実行できます。エージェントのインストーラは Windows および Linux オペレーティングシステムで使用できます。これにより、静的な設定データ、詳細な時系列のシステムパフォーマンス情報、着信/発信のネットワーク接続、および実行中のプロセスが収集されます。

Application Discovery Service、AWSパートナーネットワーク (APN) パートナーのアプリケーションディスカバリーソリューションと統合します。これらのサードパーティソリューションを使用すると、エージェントレスコレクターまたは検出エージェントを使用せずに、オンプレミス環境に関する詳細情報を Migration Hub に直接インポートできます。サードパーティのアプリケーション検出ツールは、AWS Application Discovery Service クエリを実行でき、パブリック API を使用して Application Discovery Service データベースに書き込むことができます。このようにして、Migration Hub にデータをインポートして表示できるため、アプリケーションをサーバーに関連付けたり、移行を追跡したりできます。

VMware Discovery

VMware vCenter 環境で実行されている仮想マシン (VM) がある場合は、エージェントレスコレクターを使用すると、各 VM にエージェントをインストールしなくてもシステム情報を収集できます。代わりに、このオンプレミスアプライアンスを vCenter 内にロードし、このアプライアンスですべてのホストと VM を検出することを許可します。

Agentless Collector は、使用されているオペレーティングシステムを問わず、vCenter で実行されている各 VM のシステムパフォーマンス情報とリソース使用率をキャプチャします。ただし、各 VM の「内部を見る」ことはできません。したがって、各 VM で実行されているプロセスや使用されているネットワーク接続を判断することはできません。したがって、移行の計画を補助するためにこのレベルの詳細情報が必要で、既存の VM の一部を精査したいという場合は、必要に応じて Discovery Agent をインストールできます。

また、VMware でホストされている VM については、エージェントレスコレクターとDiscovery Agent の両方を使用して検出を同時に実行できます。各検出ツールで収集される正確なデータタイプの詳細については、「エージェントレスコレクターによって収集されたデータ」と「ディスカバリー・エージェントが収集したデータ」を参照してください。

データベース検出

オンプレミス環境にデータベースサーバーと分析サーバーがある場合は、エージェントレスコレクターを使用してこれらのサーバーを検出してインベントリできます。これにより、環境内の各コンピューターにAgentless Collectorをインストールしなくても、データベースサーバーごとにパフォーマンスメトリックを収集できます。

Agentless Collector データベースおよび分析データ収集モジュールは、データインフラストラクチャに関する洞察を提供するメタデータとパフォーマンスメトリックをキャプチャします。データベースおよび分析データ収集モジュールは、Microsoft Active Directory の LDAP を使用して、ネットワーク内の OS、データベース、および分析サーバーに関する情報を収集します。次に、データ収集モジュールは定期的にクエリを実行して、データベースと分析サーバーのCPU、メモリ、およびディスク容量の実際の使用率メトリックを収集します。収集されたメトリックの詳細については、を参照してくださいデータベースと分析モジュールによって収集されたデータ。

Agentless Collector が環境からのデータ収集を完了したら、AWS DMSコンソールを使用してさらに分析し、移行を計画できます。たとえば、で最適なマイグレーションターゲットを選択する場合 AWS クラウド、ソースデータベースのターゲット推奨を生成できます。詳細については、「データベースと分析データ収集モジュール」を参照してください。

エージェントレスコレクタとディスカバリーエージェントの比較

以下の表は、Application Discovery Service データ収集ツールの簡単な比較です。

	エージェントレスコレクター	Discovery Agent
Supported server types		
VMware 仮想マシン	はい	はい
物理サーバー	いいえ	はい
Deployment		
サーバーごと	いいえ	はい
vCenter ごと	はい	いいえ
Collected data		

	エージェントレスコレクター	Discovery Agent
静的サーバー構成データ	Yes	Yes
データベース設定データ	Yes	No
VM 使用率メトリクス	Yes	No
データベース使用率のメトリクス	Yes	No
時系列のパフォーマンス情報	No	Yes (Export only)
ネットワーク着信/発信接続	No	Yes (Export only)
実行中のプロセス	No	Yes (Export only)
サポートされる OS	Any OS running in VMware vCenter V5.5+	サポートされる Linux および Windows オペレーティングシステムのリストについては、「ディスカバリー・エージェントの前提条件」を参照してください。
サポート対象データベース	Oracle, SQL Server, MySQL, and PostgreSQL	なし

前提

Application Discovery Service の使用は、以下を前提としています。

- AWS へのサインアップが完了している。詳細については、「Application Discovery Service セットアップ」を参照してください。
- Migration Hub ホームリージョンの選択が完了している。詳細については、ホームリージョンに関するドキュメントを参照してください。

期待する内容は次のとおりです。

- Migration Hub ホームリージョンは、Application Discovery Service が検出データと計画データを保存する唯一のリージョンです。
- Discovery Agent、Connector、およびインポートは、選択された Migration Hub ホームリージョンのみで使用できます。
- Application Discovery ServiceAWS を使用できるリージョンのリストについては、「」を参照してくださいAmazon Web Services 全般のリファレンス。

Application Discovery Service セットアップ

AWS Application Discovery Service 初めて使用する前に、以下のタスクを完了してください。

アマゾン ウェブ サービスにサインアップ

IAM ユーザーを作成する

Migration Hub コンソールにサインインし、ホームリージョンを選択してください

アマゾン ウェブ サービスにサインアップ

をお持ちでない場合は AWS アカウント、次の手順を実行して作成してください。

にサインアップするには AWS アカウント

1. https://portal.aws.amazon.com/billing/signup を開きます。
2. オンラインの手順に従います。

   サインアップ手順の一環として、通話呼び出しを受け取り、電話キーパッドで検証コードを入力するように求められます。

   にサインアップすると AWS アカウント、AWS アカウントのルートユーザーが作成されます。ルートユーザーには、アカウントのすべての AWS のサービス とリソースへのアクセス権があります。セキュリティ上のベストプラクティスとして、ユーザーに管理アクセスを割り当て、root ユーザーアクセスを必要とするタスクを実行するときは root ユーザーのみを使用してください。

IAM ユーザーを作成する

アカウントを作成すると、 AWS AWS そのアカウントのすべてのサービスとリソースに完全にアクセスできるシングルサインイン ID が取得されます。この ID AWS はアカウントルートユーザーと呼ばれます。 AWS Management Console アカウントの作成に使用したメールアドレスとパスワードを使用してにログインすると、 AWS アカウントのすべてのリソースに完全にアクセスできます。

日常的なタスクには (それが管理タスクであっても)、ルートユーザーを使用しないよう強くお勧めします。代わりに、セキュリティ上のベストプラクティスである個別の IAM ユーザーを作成し、 AWS Identity and Access Management (IAM) 管理者ユーザーを作成してください。その後、ルートユー

ザーの認証情報を安全な場所に保管し、それらを使用して少数のアカウントおよびサービス管理タスクのみを実行します。

管理者ユーザーの作成に加えて、管理者以外の IAM ユーザーも作成する必要があります。以下のトピックでは、両タイプの IAM ユーザーを作成する方法を説明します。

トピック

- IAM 管理者ユーザーの作成
- 管理者以外の IAM ユーザーの作成

IAM 管理者ユーザーの作成

デフォルトでは、管理者アカウントはApplication Discovery Service へのアクセスに必要なすべてのポリシーを継承します。

管理者ユーザーを作成する

- アカウントに管理者ユーザーを作成します。 AWS 手順については、IAM ユーザーガイドの「最初の IAM ユーザーと管理者グループの作成」を参照してください。

管理者以外の IAM ユーザーの作成

管理者以外の IAM ユーザーを作成するときは、セキュリティベストプラクティスである最小特権の付与に従って、ユーザーに最小限の許可を付与します。

IAM マネージドポリシーを使用して、管理者以外の IAM ユーザーによる Application Discovery Service へのアクセス権のレベルを定義します。Application Discovery Service マネージドポリシーについては、「AWS の マネージドポリシー AWS Application Discovery Service」を参照してください。

管理者以外の IAM ユーザーを作成するには

1. AWS Management Consoleで IAM コンソールに移動します。
2. 『IAM ユーザーガイド』の「AWS アカウントに IAM ユーザーを作成する」で説明されているように、コンソールでユーザーを作成する手順に従って、管理者以外の IAM ユーザーを作成します。

   IAM ユーザーガイドの指示に従っている場合:

- アクセスのタイプを選択する手順では、「プログラムによるアクセス」を選択します。注:お勧めしませんが、同じ IAM ユーザー認証情報を使用してコンソールにアクセスする予定がある場合にのみ、AWS 管理コンソールアクセスを選択してください。 AWS
- 「権限の設定」ページの手順では、「既存のポリシーをユーザーに直接アタッチする」オプションを選択します。次に、ポリシーのリストからApplication Discovery Service マネージド IAM ポリシーを選択します。Application Discovery Service マネージドポリシーについては、「AWS の マネージドポリシー AWS Application Discovery Service」を参照してください。
- ユーザーのアクセスキー (アクセスキー ID とシークレットアクセスキー) を確認する手順では、「ユーザーの新しいアクセスキー ID とシークレットアクセスキーを安全な場所に保存することに関する重要事項」のガイダンスに従ってください。

Migration Hub コンソールにサインインし、ホームリージョンを選択してください

AWS Migration Hub AWS に使用しているアカウントでホームリージョンを選択する必要がありますAWS Application Discovery Service。

ホームリージョンを選択するには

1. AWS AWS Management Console アカウントを使用してにサインインし、https://console.aws.amazon.com/migrationhub/ にある Migration Hub コンソールを開きます。
2. Migration Hub コンソールのナビゲーションペインで、[設定] を選択し、ホームリージョンを選択します。

   Migration Hub のデータは、発見、計画、移行の追跡を目的として、ホームリージョンに保存されます。詳細については、「Migration Hub ホームリージョン」を参照してください。

AWS アプリケーション検出エージェント

AWS アプリケーション検出エージェント (検出エージェント) は、検出と移行の対象となるオンプレミスのサーバーと VM にインストールするソフトウェアです。エージェントは、システム設定、システムパフォーマンス、実行中のプロセス、およびシステム間のネットワーク接続の詳細をキャプチャします。エージェントは、Linux および Windows オペレーティングシステムの大半をサポートし、物理的なオンプレミスサーバー、Amazon EC2 インスタンス、および仮想マシンにデプロイできます。

> **Note**
>
> ディスカバリーエージェントをデプロイする前に、Migration Hub ホームリージョンを選択する必要があります。ホームリージョンにはエージェントを登録する必要があります。

Discovery Agent はローカル環境で実行され、root 権限を必要とします。Discovery Agent を起動すると、ホームリージョンにセキュアに接続され、Application Discovery Service に登録されます。

- 例えば、`eu-central-1` がホームリージョンである場合、`arsenal-discovery.eu-central-1.amazonaws.com` が Application Discovery Service に登録されます。
- または、us-west-2 を除く他のすべてのリージョンで、必要に応じてホームリージョンが置き換えられます。
- `us-west-2` がホームリージョンである場合は、`arsenal.us-west-2.amazonaws.com` が Application Discovery Service に登録されます。

仕組み

登録後、エージェントはデプロイ先のホストまたは VM のデータの収集を開始します。エージェントは、15 分間隔で設定情報について Application Discovery Service を ping します。

収集されるデータには、システム仕様、時系列の使用状況やパフォーマンスのデータ、ネットワーク接続、処理データなどが含まれます。この情報を使用して IT アセットとネットワーク依存関係をマッピングできます。これらのデータポイントはすべて、 AWS これらのサーバーを稼働させるコストの決定や移行の計画に役立ちます。

データは、Discovery Agent が Transport Layer Security (TLS) 暗号化を使用して Application Discovery Service にセキュアに転送します。エージェントは、新しいバージョンが利用可能になると自動的にアップグレードするように設定されています。必要に応じて、この設定は変更できます。

> **Tip**
>
> Discovery Agent をダウンロードしてインストールを開始する前に、「ディスカバリー・エージェントの前提条件」に記載されているすべての必須前提条件に目を通しておくようにしてください。

トピック

ディスカバリー・エージェントの前提条件

AWS アプリケーション検出エージェント (Discovery Agent) を正常にインストールするために実行する必要がある前提条件とタスクは次のとおりです。

- Discovery Agent のインストールを開始する前に、AWS Migration Hub ホームリージョンを設定する必要があります。
- 1.x バージョンのエージェントがインストールされている場合は、最新バージョンをインストールする前に削除する必要があります。
- エージェントがインストールされているホストが Linux を実行している場合は、ホストが少なくともインテル i686 CPU アーキテクチャ (P6 マイクロアーキテクチャとしても知られています) をサポートすることを確認します。
- 使用しているオペレーティングシステム (OS) 環境がサポートされていることを確認します。

  Linux

  Amazon Linux 2012.03、2015.03

  Amazon Linux 2 (2018 年 9 月 25 日更新以降)

  Ubuntu 12.04、14.04、16.04、18.04、20.04

Red Hat 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

- ネットワークからの発信接続が制限されている場合は、ファイアウォール設定を更新する必要があります。エージェントには、TCP ポート 443 を介した `arsenal` へのアクセスが必要です。着信ポートを開く必要はありません。

  たとえば、ホームリージョンが `eu-central-1` の場合、`https://arsenal-discovery.eu-central-1.amazonaws.com:443` を使用できます。
- 自動アップグレードを機能させるには、ホームリージョン内の Amazon S3 へのアクセスが必要です。
- コンソールで AWS Identity and Access Management (IAM) ユーザーを作成し、既存の `AWSApplicationDiscoveryAgentAccess` IAM 管理ポリシーをアタッチします。このポリシーにより、ユーザーはお客様に代わって必要なエージェントアクションを実行できます。管理ポリシーの詳細については、「AWS の マネージドポリシー AWS Application Discovery Service」を参照してください。
- ネットワークタイムプロトコル (NTP) サーバーからの時刻のずれを確認し、必要に応じて修正します。時刻の同期が正しくないと、エージェント登録コールが失敗します。

> **Note**
>
> Discovery Agent には 32 ビットのエージェント実行可能ファイルがあり、32 ビットと 64 ビットのオペレーティングシステムで動作します。実行可能ファイルを 1 つにすることで、デプロイに必要なインストールパッケージの数が減ります。この実行可能エージェントは、Linux および Windows OS で動作します。これについては、以降のそれぞれのインストールセクションで説明します。

Linux にディスカバリーエージェントをインストールします。

Linux で次の手順を完了します。この手順を開始する前に、Migration Hub ホームリージョンが設定されていることを確認してください。

> **Note**
>
> 以前の Linux バージョンを使用している場合は、「古い Linux プラットフォームでの要件」を参照してください。

AWS データセンターにアプリケーションディスカバリーエージェントをインストールするには

1. Linux ベースのサーバーまたは VM にサインインし、エージェントコンポーネントを格納するための新しいディレクトリを作成します。
2. 新しいディレクトリに切り替え、コマンドラインまたはコンソールからインストールスクリプトをダウンロードします。

   a. コマンドラインからダウンロードするには、次のコマンドを実行します。

   ```
   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. Migration Hub コンソールからダウンロードするには、以下の手順を実行します。

      i. コンソールを開いて、[Discovery Tools (検出ツール)] ページに移動します。

      ii. [Discovery Agent (検出エージェント)] ボックスで、[Download agent (エージェントのダウンロード)] を選択し、表示されたリストボックスで [Linux] を選択します。ダウンロードがすぐに開始されます。
3. 次の 3 つのコマンドを使用して、インストールパッケージの暗号署名を確認します。

   ```
   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
```

エージェントパブリックキー (discovery.gpg) のフィンガープリントは、7638 F24C 6717 F97C 4F1B 3BC0 5133 255E 4DF4 2DA2 です。

4. 次に示すように、tarball から抽出します。

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

5. エージェントをインストールするには、以下のインストール方法のどちらかを選択します。

実行方法	手順
Discovery Agent をインストールする	エージェントをインストールするには、以下の例にあるエージェントインストールコマンドを実行します。この例では、ホームリージョンの名前、*aws-access-key-id* アクセスキー ID、*your-home-region aws-secret-access-key* シークレットアクセスキーに置き換えます。 `sudo bash install -r your-home-region -k aws-access-key-id -s aws-secret-access-key` エージェントはデフォルトで、更新が利用可能になると、それらを自動的にダウンロードして適用します。 このデフォルト設定の使用が推奨されます。 ただし、エージェントによる更新の自動ダウンロードと適用を希望しない場合は、エージェントインストールコマンドを実行するときに `-u false` パラメータを含めてください。

実行方法	手順
(オプション) Discovery Agent をインストールして非透過プロキシを設定する	非透過プロキシを設定するには、エージェントインストールコマンドに以下のパラメータを追加します。 • -e プロキシパスワード。 • -f プロキシポート番号。 • -g プロキシスキーム。 • -i プロキシユーザーネーム。 以下は、非透過プロキシパラメータを使用したエージェントインストールコマンドの例です。 `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` プロキシに認証が必要ではない場合、-e と -i パラメータは使用しません。 このインストールコマンド例では https が使用されていますが、プロキシが HTTP を使用する場合は -g パラメータ値に http を指定してください。

6. ネットワークからの発信接続が制限されている場合は、ファイアウォール設定を更新する必要があります。エージェントには、TCP ポート 443 を介した arsenal へのアクセスが必要です。着信ポートを開く必要はありません。

   たとえば、ホームリージョンが eu-central-1 の場合、https://arsenal-discovery.*eu-central-1*.amazonaws.com:443 を使用できます。

トピック

古い Linux プラットフォームでの要件

一部の古い Linux プラットフォーム (SUSE 10、CentOS 5、RHEL 5 など) はサポートが終了しているか、最低限のサポート対象となります。これらのプラットフォームには、 out-of-dateエージェントアップデートスクリプトによるインストールパッケージのダウンロードを妨げる暗号スイートが存在する可能性があります。

Curl

Application Discovery `curl` エージェントは、サーバーとの安全な通信を必要とします。 AWS 一部の古いバージョンの `curl` は、最新のウェブサービスと安全に通信することはできません。

すべてのオペレーションで`curl` バージョンが含まれるアプリケーション検出エージェントを使用するには、`-c true` パラメータでインストールスクリプトを実行します。

認証機関バンドル

古い Linux システムには、 out-of-date 安全なインターネット通信に不可欠な認証局 (CA) バンドルが含まれている場合があります。

すべてのオペレーションで CA バンドルが含まれるアプリケーション検出エージェントを使用するには、`-b true` パラメータでインストールスクリプトを実行します。

これらのインストールスクリプトオプションは併用可能です。以下のコマンド例では、両方のスクリプトパラメータがインストールスクリプトに渡されます。

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

Linux で Discovery Agent プロセスを管理する

Discovery Agent の動作は、systemd、Upstart、または System V init ツールを使用してシステムレベルで管理することができます。以下のタブは、それぞれのツールでサポートされているタスクのコマンドの概要を示しています。

systemd

Application Discovery Agent の管理コマンド

タスク	Command
エージェントが実行されていることを確認	`sudo systemctl status aws-discovery-daemon.service`
エージェントの開始	`sudo systemctl start aws-discovery-daemon.service`
エージェントの停止	`sudo systemctl stop aws-discovery-daemon.service`
エージェントの再起動	`sudo systemctl restart aws-discovery-daemon.service`

Upstart

アプリケーション検出エージェントの管理コマンド

タスク	Command
エージェントが実行されていることを確認	`sudo initctl status aws-discovery-daemon`
エージェントの開始	`sudo initctl start aws-discovery-daemon`
エージェントの停止	`sudo initctl stop aws-discovery-daemon`
エージェントの再起動	`sudo initctl restart aws-discovery-daemon`

System V init

アプリケーション検出エージェントの管理コマンド。

タスク	Command
エージェントが実行されていることを確認	`sudo /etc/init.d/aws-discovery-daemon status`
エージェントの開始	`sudo /etc/init.d/aws-discovery-daemon start`
エージェントの停止	`sudo /etc/init.d/aws-discovery-daemon stop`
エージェントの再起動	`sudo /etc/init.d/aws-discovery-daemon restart`

Linux から Discovery Agent をアンインストールする

このセクションでは、Linux から Discovery Agent をアンインストールする方法を説明します。

yum パッケージマネージャの使用時にエージェントをアンインストールする

- yum を使用している場合は、以下のコマンドを使用してエージェントをアンインストールします。

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

apt-get パッケージマネージャの使用時にエージェントをアンインストールする

- apt-get を使用している場合は、以下のコマンドを使用してエージェントをアンインストールします。

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

zypper パッケージマネージャの使用時にエージェントをアンインストールする

- zypper を使用している場合は、以下のコマンドを使用してエージェントをアンインストールします。

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

Linux ディスカバリーエージェントのトラブルシューティング

Linux での Discovery Agent のインストール中、または使用中に問題が発生した場合は、ロギングと設定に関する以下のガイダンスを参照してください。エージェントまたはApplication Discovery Service への接続に関する潜在的な問題のトラブルシューティングを支援する場合、 AWS Support はこれらのファイルを要求することがよくあります。

- ログファイル

  Discovery Agent のログファイルは、以下のディレクトリにあります。

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

  ログファイルには、それらがメインデーモン、自動アップグレーダー、またはインストーラのどれによって生成されたかを示す名前が付けられています。

- 設定ファイル

  Discovery Agent バージョン 2.0.1617.0 以降の設定ファイルは、以下のディレクトリにあります。

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

  2.0.1617.0 より前の Discovery Agent バージョンの設定ファイルは、以下のディレクトリにあります。

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

- 旧バージョンの Discovery Agent を削除する手順については、「ディスカバリー・エージェントの前提条件」を参照してください。

Windows に をインストールする

Windows にエージェントをインストールするには、次の手順を実行します。この手順を開始する前に、Migration Hub ホームリージョンが設定されていることを確認してください。

AWS Application Discovery Agent をデータセンターにインストールするには

1. Windows エージェントインストーラをダウンロードします。ただし、Windows 内ではインストーラをダブルクリックして実行しないでください。

   > **Important**
   >
   > インストールが失敗するので、Windows 内ではインストーラをダブルクリックして実行しないでください。エージェントのインストールはコマンドプロンプトからのみ可能です (インストーラーをダブルクリックしてしまった場合は、[プログラムの追加と削除] に移動し、エージェントをアンインストールしてから残りのインストール手順を続行する必要があります)。
   >
   > Windows エージェントインストーラがホスト上で Visual C++ x86 ランタイムのバージョンを検出しない場合、エージェントソフトウェアをインストールする前に Visual C++ x86 2015—2019 ランタイムが自動的にインストールされます。

2. 管理者としてコマンドプロンプトを開き、インストールパッケージを保存した場所に移動します。
3. エージェントをインストールするには、以下のインストール方法のどちらかを選択します。

実行方法	手順
Discovery Agent をインストールする	エージェントをインストールするには、以下の例にあるエージェントインストールコマンドを実行します。この例では、*your-home-region* をホームリージョンの名前、*aws-access-key-id* をアクセスキー ID、*aws-secret-access-key* をシークレットアクセスキーに置き換えます。 オプションで、INSTALLLOCATION パラメータにフォルダパス *C:\install-location* を指定して、エージェントの

実行方法	手順
	インストール場所を設定できます。例えば、INSTALLLOCATION=" *C:\install-location* " などです。結果のフォルダ階層は [INSTALLLOCATION パス]\AWS Discovery になります。デフォルトのインストール場所は Program Files フォルダです。 オプションで、LOGANDCONFIGLOCATION を使用してエージェントログフォルダと設定ファイルのデフォルトディレクトリ (ProgramData) をオーバーライドできます。その結果、フォルダ階層は [*LOGANDCONFIGLOCATION path*]\AWS Discovery になります。 `.\AWSDiscoveryAgentInstaller.exe REGION=" your-home-region " KEY_ID="aws-access-key-id " KEY_SECRET=" aws-secret-access-key " /quiet` エージェントはデフォルトで、更新が利用可能になると、それらを自動的にダウンロードして適用します。 このデフォルト設定の使用が推奨されます。 ただし、エージェントによる更新の自動ダウンロードと適用を希望しない場合は、エージェントインストールコマンドを実行するときに AUTO_UPDATE=false パラメータを含めてください。

実行方法	手順
	Warning 自動アップグレードを無効にすると、最新のセキュリティパッチがインストールされなくなります。

実行方法	手順
(オプション) Discovery Agent をインストールして非透過プロキシを設定する	非透過プロキシを設定するには、エージェントインストールコマンドに以下のパブリックプロパティを追加します。 • PROXY_HOST – プロキシホストの名前 • PROXYSCHEME – プロキシスキーム • PROXY_PORT – プロキシポート番号 • PROXY_USER – プロキシユーザーネーム • PROXYPASSWORD – プロキシユーザーパスワード 以下は、非透過プロキシプロパティを使用したエージェントインストールコマンドの例です。 `.\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` プロキシに認証が必要ではない場合は、PROXY_USER と PROXY_PASSWORD プロパティを省略します。このインストールコマンド例では https が使用されています。プロキシが HTTP を使用する場合は PROXY_SCHEME 値に http を指定してください。

4. ネットワークからのアウトバウンド接続が制限されている場合は、ファイアウォール設定を更新する必要があります。エージェントには、TCP ポート 443 を介した `arsenal` へのアクセスが必要です。着信ポートを開く必要はありません。

   例えば、ホームリージョンが `eu-central-1` の場合は、`https://arsenal-discovery.eu-central-1.amazonaws.com:443` を使用します。

Package 署名と自動アップグレード

Windows Server 2008 以降については、Amazon が SHA256 証明書を使用して Application Discovery Service エージェントインストールパッケージに暗号的に署名します。Windows Server 2008 SP2 での SHA2 署名付き自動更新プログラムについては、ホストに SHA2 署名認証をサポートするための修正プログラムがインストールされていることを確認してください。マイクロソフトの最新サポート修正プログラムは、Windows Server 2008 SP2 での SHA2 認証のサポートに役立ちます。

> **Note**
>
> マイクロソフトからの Windows 2003 向けの SHA256 サポート用修正プログラムの一般公開は終了しました。Windows 2003 ホストにこれらの修正プログラムがまだインストールされていない場合は、手動でアップグレードする必要があります。

アップグレードを手動で実行する

1. Windows Agent Updater をダウンロードします。
2. 管理者としてコマンドプロンプトを開きます。
3. アップデータが保存された場所に移動します。
4. 以下のコマンドを実行します。

```
AWSDiscoveryAgentUpdater.exe /Q
```

Windows でのディスカバリーエージェントプロセスの管理

Discovery Agent の動作は、Windows Server Manager Services コンソールを通じてシステムレベルで管理することができます。次の表に管理方法を示します。

タスク	サービス名	サービス状況/アクション
エージェントが実行されていることを確認	AWS ディスカバリーエージェント AWS ディスカバリー・アップデーター	Started
エージェントの開始	AWS ディスカバリー・エージェント AWS ディスカバリー・アップデーター	[Start (開始)] を選択
エージェントの停止	AWS ディスカバリー・エージェント AWS ディスカバリー・アップデーター	[Stop (停止)] を選択
エージェントの再起動	AWS ディスカバリー・エージェント AWS ディスカバリー・アップデーター	[Restart (再起動)] を選択

Windows から Discovery Agent をアンインストールする

1. Windows でコントロールパネルを開きます。
2. [プログラム] を選択します。
3. [プログラムと機能] を選択します。
4. [AWS Discovery Agent] を選択します。
5. アンインストール を選択します。

> **Note**
>
> エージェントのアンインストール後に再インストールする場合は、/repair および /norestart オプションを使用して以下のコマンドを実行します。
>
> ```
> .\AWSDiscoveryAgentInstaller.exe REGION="your-home-region" KEY_ID="aws-access-key-id" KEY_SECRET="aws-secret-access-key" /quiet /repair /norestart
> ```

コマンドラインを使用して Windows から Discovery Agent をアンインストールする

1. [Start] (スタート) を右クリックします。
2. [Command Prompt] (コマンドプロント) を選択します。
3. 以下のコマンドを使用して Windows から検出エージェントをアンインストールします。

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

Windows のディスカバリーエージェントのトラブルシューティング

Windows AWS にApplication Discovery Agentをインストールまたは使用中に問題が発生した場合は、ロギングと構成に関する次のガイダンスを参照してください。 AWS Supportエージェントまたはは Application Discovery Service への接続に関する潜在的な問題のトラブルシューティングに役立つときに、これらのファイルを要求することがよくあります。

- インストールログギング

  エージェントインストールコマンドが失敗したように見受けられる場合があります。たとえば、Windows Services Manager の失敗により、検出サービスは作成されていないと表示される場合があります。このような場合は、コマンドに /log install.log を追加して、詳細なインストールログを生成します。

- 運用ログ

  Windows Server 2008 以降の場合、エージェントログファイルは次のディレクトリにあります。

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

Windows Server 2003 の場合、エージェントログファイルは次のディレクトリにあります。

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

ログファイルには、それらがメインサービス、自動アップグレード、またはインストーラのどれによって生成されたかを示す名前が付けられています。

- 設定ファイル

  Windows Server 2008 以降の場合、エージェント設定ファイルは次の場所にあります。

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

  Windows Server 2003 の場合、エージェント設定ファイルは次の場所にあります。

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

- 以前のバージョンの Discovery Agent を削除する手順については、「ディスカバリー・エージェントの前提条件」を参照してください。

ディスカバリー・エージェントが収集したデータ

AWS アプリケーション検出エージェント (検出エージェント) は、オンプレミスのサーバーと VM にインストールするソフトウェアです。Discovery Agent は、システム構成、時系列使用率またはパフォーマンスデータ、プロセスデータ、伝送制御プロトコル (TCP) ネットワーク接続を収集します。このセクションでは、収集されるデータについて説明します。

Discovery Agent が収集するデータの表の凡例:

- ホストという用語は、物理サーバーまたは VM を指します。
- 収集されたデータは、特に断らない限り、キロバイト (KB) 単位です。
- Migration Hub コンソール内の同等データはメガバイト (MB) 単位で報告されます。
- ポーリング間隔は約 15 秒で、15 AWS 分ごとに送信されます。

- アスタリスク (*) の付いたデータフィールドは、エージェントの API `.csv` エクスポート機能で作成されたファイルでのみ使用できます。

データフィールド	説明
agentAssignedProcess[ID] *	エージェントによって検出されたプロセスのプロセス ID
agentId	エージェント固有の ID
agentProvidedTimeスタンプ *	エージェントの監視日時 (mm/dd/yyyy hh:mm:ss am/pm)
cmdLine*	コマンドラインに入力されるプロセス
cpuType	ホストで使用される CPU (中央処理装置) のタイプ
destinationIp*	パケットを送信する先のデバイスの IP アドレス
destinationPort*	データ/リクエストを送信する先のポート番号
family*	ルーティングファミリーのプロトコル
freeRAM (MB)	アプリケーションで即時に使用できる無料 RAM およびキャッシュ RAM (MB 単位)
gateway*	ネットワークのノードアドレス
hostName	データを収集したホストの名前
hypervisor	ハイパーバイザーのタイプ
ipAddress	ホストの IP アドレス
ipVersion*	IP バージョン番号
isSystem*	OS がプロセスを所有しているかどうかを示すブール属性

データフィールド	説明
macAddress	ホストの MAC アドレス
name*	収集されているホスト、ネットワーク、メトリクスなどのデータの名前
netMask*	ネットワークホストが属する IP アドレスプレフィックス
osName	ホストのオペレーティングシステムの名前
osVersion	ホストのオペレーティングシステムのバージョン
パス	コマンドラインから発信されるコマンドのパス
sourceIp*	IP パケットの送信元デバイスの IP アドレス
sourcePort*	データ/リクエストの送信元のポート番号
timestamp*	報告された属性がエージェントでログに記録された日時
totalCpuUsage協定	ポーリング間隔中のホストの CPU 使用率
totalDiskBytesReadPerSecond (Kbps)	全ディスクの 1 秒あたりの読み取り合計キロビット数
totalDiskBytesWrittenPerSecond (Kbps)	すべてのディスクで 1 秒あたりに書き込まれる合計キロビット数
totalDiskFreeサイズ (GB)	ディスク空き容量 (GB 単位)
totalDiskReadOpsPerSecond	1 秒あたりの読み取り I/O オペレーションの合計数
totalDiskSize (GB)	ディスクの合計容量 (GB 単位)
totalDiskWriteOpsPerSecond	1 秒あたりの書き込み I/O オペレーションの合計数

データフィールド	説明
totalNetworkBytesReadPerSecond (Kbps)	1 秒あたりに読み取られたバイトスループットの合計値
totalNetworkBytesWrittenPerSecond (Kbps)	1 秒あたりに書き込まれたバイトスループットの合計値
totalNumCores	CPU 内の独立した処理装置の合計数
totalNumCpus	CPU の合計数
totalNumDisks	ホストの物理ハードディスクの数
totalNumLogicalプロセッサ*	物理コアの合計数と各コアで実行できるスレッド数を乗算した値
totalNumNetworkカード	サーバーのネットワークカードの合計数
totalRAM (MB)	ホストで使用可能な RAM の合計量
transportProtocol*	トランスポートプロトコルの使用タイプ

ディスカバリーエージェントのデータ収集を開始または停止する

Discovery Agent をデプロイして構成した後、データ収集が停止した場合は再起動できます。データ収集は、コンソールを使用する、または AWS CLI経由で API コールを実行することによって開始または停止できます。以下の手順には、これら両方の手法が説明されています。

Using the Migration Hub console

以下の手順では、Migration Hub コンソールの [Data Collectors] (データコレクタ) ページで Discovery Agent のデータ収集プロセスを開始または停止する方法を説明します。

データ収集を開始または停止する

1. ナビゲーションペインで、[Data Collectors] (データコレクタ) を選択します。
2. [Agents] (エージェント) タブを選択します。
3. 開始または停止するエージェントのチェックボックスをオンにします。

> **Tip**
>
> 複数のエージェントをインストールしており、特定のホストだけでデータ収集を開始または停止したいという場合は、エージェントの行にある [Hostname] (ホスト名) 列にエージェントがインストールされているホストが特定されています。

4. [Start data collection (データ収集の開始)] または [Stop data collection (データ収集の停止)] を選択します。

Using the AWS CLI

からDiscovery Agentのデータ収集プロセスを開始または停止するには AWS CLI、まず環境にをインストールし、次に、選択したMMigration Hub のホームリージョンを使用するようにCLI を設定する必要があります。 AWS CLI

AWS CLI をインストールしてデータ収集を開始または停止するには

1. まだインストールしていない場合は、お使いの OS タイプ (Windows または Mac/Linux) AWS CLI に適したものをインストールします。手順については、AWS Command Line Interface ユーザーガイドを参照してください。
2. コマンドプロンプト (Windows) またはターミナル (MAC/Linux) を開きます。
   a. `aws configure` を入力して、[Enter] を押します。
   b. AWS アクセスキー ID AWS とシークレットアクセスキーを入力します。
   c. デフォルトリージョン名に、*`us-west-2`* などホームリージョンを入力します。(この例では、ホームリージョンが `us-west-2` であると仮定しています)。
   d. デフォルトの出力形式として「`text`」と入力します。
3. データ収集を停止または開始したいエージェントの ID を見つけるには、以下のコマンドを入力します。

```
aws discovery describe-agents
```

4. エージェントによるデータ収集を開始するには、以下のコマンドを入力します。

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

エージェントによるデータ収集を停止するには、以下のコマンドを入力します。

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

Application Discovery Service エージェントレスコレクター

Application Discovery Service Agentless Collector (Agentless Collector) は、サーバープロファイル情報 (OS、CPUs 数、RAM 量など) 、データベースメタデータ、使用率メトリクスなど、オンプレミス環境に関するエージェントレスメソッドを通じて情報を収集するオンプレミスアプリケーションです。Agentless Collector は、Open Virtualization Archive (OVA) ファイルを使用して VMware vCenter Server 環境に仮想マシン (VM) としてインストールします。

Agentless Collector はモジュラーアーキテクチャを採用しているため、複数のエージェントレスコレクションメソッドを使用できます。Agentless Collector は現在、VMware VMs、およびデータベースサーバーと分析サーバーからのデータ収集用のモジュールをサポートしています。今後のモジュールは、ネットワーク接続の収集、追加の仮想化プラットフォームからの収集、オペレーティングシステムレベルの収集をサポートします。

Agentless Collector は、 AWS Application Discovery Service (Application Discovery Service) のデータ収集をサポートしています。これにより、オンプレミスサーバーとデータベースに関する使用状況と設定データを収集 AWS クラウド することで、 への移行を計画できます。

Application Discovery Service は と統合されているため AWS Migration Hub、移行ステータス情報を 1 つのコンソールに集約できるため、移行の追跡が簡単になります。ホームリージョンの Migration Hub コンソールから、検出されたサーバーの表示、Amazon EC2 のレコメンデーションの取得、ネットワーク接続の視覚化、サーバーをアプリケーションにグループ化し、各アプリケーションの移行ステータスを追跡できます。

Agentless Collector データベースおよび分析データ収集モジュールは、 AWS Database Migration Service () と統合されていますAWS DMS。この統合は、 への移行を計画するのに役立ちます AWS クラウド。データベースおよび分析データ収集モジュールを使用して、環境内のデータベースサーバーと分析サーバーを検出し、 に移行するサーバーのインベントリを構築できます AWS クラウド。このデータ収集モジュールは、CPU、メモリ、ディスク容量のデータベースメタデータと実際の使用率メトリクスを収集します。これらのメトリクスを AWS DMS 収集したら、 コンソールを使用してソースデータベースのターゲットレコメンデーションを生成できます。

トピック

- エージェントレスコレクタのトラブルシューティング

エージェントレスコレクター入門

このセクションでは、Application Discovery Service エージェントレスコレクター (エージェントレスコレクター) の使用を開始する方法について説明します。

トピック

- エージェントレスコレクタの前提条件
- ステップ 1: エージェントレスコレクター用の IAM ユーザーを作成する
- ステップ 2: エージェントレスコレクターをダウンロードする
- ステップ 3: エージェントレスコレクタをデプロイする
- ステップ 4: エージェントレスコレクターコンソールにアクセスする
- ステップ 5: エージェントレスコレクタの設定
- ステップ 6: エージェントレスコレクタデータ収集モジュールをセットアップする
- ステップ 7: 収集したデータを表示する

エージェントレスコレクタの前提条件

Application Discovery Service エージェントレスコレクター (エージェントレスコレクター) を使用するための前提条件は次のとおりです。

- 1 つ以上のアカウント。AWS
- AWSAWS Migration Hubホームリージョンが設定されたアカウントMigration Hub コンソールにサインインし、ホームリージョンを選択してください。を参照してください。Migration Hub のデータは、発見、計画、移行の追跡を目的として、ホームリージョンに保存されます。
- AWSAWSAWSApplicationDiscoveryAgentlessCollectorAccess管理ポリシーを使用するように設定されているアカウント IAM ユーザー。データベースと分析データ収集モジュールを使用するには、この IAM ユーザーは顧客管理の 2 つの IAM ポリシーとも使用する必要があります。DMSCollectorPolicy FleetAdvisorS3Policy詳細については、「ステップ 1: エージェントレスコレクター用の IAM ユーザーを作成する」を参照してください。IAM ユーザーは、Migration Hub AWS ホームリージョンが設定されたアカウントで作成する必要があります。
- VMware vCenter Server V5.5、V6、V6.5、6.7 または 7.0。

> **Note**
>
> エージェントレスコレクタはこれらのバージョンの VMware をすべてサポートしていますが、現在はバージョン 6.7 と 7.0 に対してテストを行っています。

- VMware vCenter Serverのセットアップでは、システムグループの読み取り権限と表示権限が設定されたvCenter認証情報を指定できることを確認してください。
- エージェントレスコレクタには、TCP ポート 443 を介した複数のドメインへのアウトバウンドアクセスが必要です。AWSこれらのドメインのリストについては、を参照してください。ドメインへのアウトバウンドアクセス用にファイアウォールを設定します。AWS
- データベースと分析データ収集モジュールを使用するには、Migration Hub AWS リージョン ホームリージョンとして設定した場所に Amazon S3 バケットを作成します。データベースと分析データ収集モジュールは、この Amazon S3 バケットにインベントリメタデータを格納します。詳細については、Amazon S3 ユーザーガイドのバケットの作成を参照してください。

ドメインへのアウトバウンドアクセス用にファイアウォールを設定します。AWS

ネットワークからのアウトバウンド接続が制限されている場合は、Agentless Collector AWS が必要とするドメインへのアウトバウンドアクセスを許可するようにファイアウォール設定を更新する必要があります。AWSアウトバウンドアクセスが必要なドメインは、Migration Hub のホームリージョンが米国西部 (オレゴン) リージョン、us-west-2 リージョン、またはその他のリージョンのいずれであるかによって異なります。

AWSアカウントのホームリージョンが us-west-2 の場合、次のドメインにはアウトバウンドアクセスが必要です。

- `arsenal-discovery.us-west-2.amazonaws.com`— コレクターはこのドメインを使用して、必要な IAM ユーザー認証情報で設定されていることを確認します。ホームリージョンは us-west-2 なので、コレクターは収集したデータの送信と保存にもこのドメインを使用します。
- `migrationhub-config.us-west-2.amazonaws.com`— コレクターはこのドメインを使用して、提供された IAM ユーザー認証情報に基づいてコレクターがデータを送信するホームリージョンを決定します。
- `api.ecr-public.us-east-1.amazonaws.com`— コレクターはこのドメインを使用して、利用可能なアップデートを検出します。
- `public.ecr.aws`— コレクターはこのドメインを使用してアップデートをダウンロードします。

- dms.*your-migrationhub-home-region*.amazonaws.com— AWS DMS コレクターはこのドメインを使用してデータコレクターに接続します。
- s3.amazonaws.com— コレクターはこのドメインを使用して、データベースと分析データ収集モジュールによって収集されたデータを Amazon S3 バケットにアップロードします。

AWSアカウントのホームリージョンがそうでない場合、以下のドメインにはアウトバウンドアクセスが必要です。**us-west-2**

- arsenal-discovery.us-west-2.amazonaws.com— コレクターはこのドメインを使用して、必要な IAM ユーザー認証情報で設定されていることを確認します。
- arsenal-discovery.*your-migrationhub-home-region*.amazonaws.com— コレクターは、収集したデータの送信と保存にこのドメインを使用します。
- migrationhub-config.us-west-2.amazonaws.com— コレクターはこのドメインを使用して、提供された IAM ユーザー認証情報に基づいてコレクターがデータを送信するホームリージョンを決定します。
- api.ecr-public.us-east-1.amazonaws.com— コレクターはこのドメインを使用して、利用可能なアップデートを検出します。
- public.ecr.aws— コレクターはこのドメインを使用してアップデートをダウンロードします。
- dms.*your-migrationhub-home-region*.amazonaws.com— AWS DMS コレクターはこのドメインを使用してデータコレクターに接続します。
- s3.amazonaws.com— コレクターはこのドメインを使用して、データベースと分析データ収集モジュールによって収集されたデータを Amazon S3 バケットにアップロードします。

Agentless Collector をセットアップするときに、「セットアップに失敗しました — 認証情報を確認して再試行してください。そうしないと、AWSアクセスできません」などのエラーが表示されることがあります。ネットワーク設定を確認してください。これらのエラーは、AWSエージェントレスコレクターがアウトバウンドアクセスが必要なドメインの 1 つに HTTPS 接続を確立しようとして失敗したことが原因である可能性があります。

AWSへの接続を確立できない場合、Agentless Collector はオンプレミス環境からデータを収集できません。への接続を修正する方法については、を参照してください。AWS セットアップ中にエージェントレスコレクターにアクセスできない問題を修正しました。 AWS

ステップ 1: エージェントレスコレクター用の IAM ユーザーを作成する

エージェントレスコレクターを使用するには、AWS使用したアカウントで (IAMMigration Hub コンソールにサインインし、ホームリージョンを選択してください) ユーザーを作成する必要があります。AWS Identity and Access Management次に、この IAM ユーザーが次の管理ポリシーを使用するように設定します。AWS AWSApplicationDiscoveryAgentlessCollectorAccessこの IAM ポリシーは、IAM ユーザーを作成するときにアタッチします。

データベースと分析データ収集モジュールを使用するには、顧客管理の IAM ポリシーを 2 つ作成します。これらのポリシーは Amazon S3 バケットと AWS DMS API へのアクセスを提供します。詳細については、IAM ユーザーガイドの「カスタマー管理ポリシーの作成」を参照してください。

- 次の JSON **DMSCollectorPolicy** コードを使用してポリシーを作成します。

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

- 次の JSON **FleetAdvisorS3Policy** コードを使用してポリシーを作成します。

```
{
    "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/*"
            ]
        }
    ]
}
```

前の例では、*bucket_name*前提条件のステップで作成した Amazon S3 バケットの名前に置き換えます。

エージェントレスコレクターで使用する非管理用 IAM ユーザーを作成することをお勧めします。管理者以外の IAM ユーザーを作成するときは、セキュリティベストプラクティスである最小特権の付与に従って、ユーザーに最小限の許可を付与します。

エージェントレスコレクターで使用する管理者以外の IAM ユーザーを作成するには

1. でAWS Management Console、AWSホームリージョンの設定に使用したアカウントを使用して IAM コンソールに移動します。Migration Hub コンソールにサインインし、ホームリージョンを選択してください
2. 『IAM ユーザーガイド』の「AWSアカウントに IAM ユーザーを作成する」で説明されているように、コンソールでユーザーを作成する手順に従って、管理者以外の IAM ユーザーを作成します。

   IAM ユーザーガイドの指示に従っている場合:

   - アクセスのタイプを選択する手順では、「プログラムによるアクセス」を選択します。注:お勧めしませんが、同じ IAM ユーザー認証情報を使用してコンソールにアクセスする予定がある場合にのみ、AWS管理コンソールアクセスを選択してください。AWS
   - 「権限の設定」ページの手順では、「既存のポリシーをユーザーに直接アタッチする」オプションを選択します。次に、`AWSApplicationDiscoveryAgentlessCollectorAccess`AWSポリシーのリストから管理ポリシーを選択します。

     次に、`DMSCollectorPolicyFleetAdvisorS3Policy`とカスタマー管理の IAM ポリシーを選択します。
   - ユーザーのアクセスキー (アクセスキー ID とシークレットアクセスキー) を確認する手順では、「ユーザーの新しいアクセスキー ID とシークレットアクセスキーを安全な場所に保存す

ることについての重要事項」のガイダンスに従ってください。これらのアクセスキーは必要ですステップ 5: エージェントレスコレクタの設定。

AWSセキュリティ上のベストプラクティスは、アクセスキーをローテーションすることです。キーのローテーションについては、IAM ユーザーガイドの「長期認証情報を必要とするユースケースのためのアクセスキーを定期的にローテーションする」を参照してください。

ステップ 2: エージェントレスコレクターをダウンロードする

Application Discovery Service エージェントレスコレクター (エージェントレスコレクター) をセットアップするには、エージェントレスコレクターオープン仮想化アーカイブ (OVA) ファイルをダウンロードしてデプロイする必要があります。エージェントレスコレクタは、オンプレミスの VMware 環境にインストールする仮想アプライアンスです。このステップではコレクター OVA ファイルをダウンロードする方法を説明し、次のステップではそれをデプロイする方法について説明します。

コレクタ OVA ファイルをダウンロードし、そのチェックサムを確認するには

1. VMware 管理者として vCenter にサインインし、エージェントレスコレクタ OVA ファイルをダウンロードするディレクトリに切り替えます。
2. 次の URL から OVA ファイルをダウンロードします。

   エージェントレスコレクター OVA
3. システム環境で使用するハッシュアルゴリズムに応じて、MD5 または SHA256 をダウンロードし、チェックサム値が含まれているファイルを取得します。ダウンロードした値を使用して、ApplicationDiscoveryServiceAgentlessCollector前のステップでダウンロードしたファイルを検証します。
4. Linux のバリエーションに応じて、適切なバージョンの MD5 コマンドまたは SHA256 コマンドを実行して、ApplicationDiscoveryServiceAgentlessCollector.ova ファイルの暗号署名が、ダウンロードした各 MD5 / SHA256 ファイルの値と一致することを確認します。

   ```
   $ md5sum ApplicationDiscoveryServiceAgentlessCollector.ova
   ```

   ```
   $ sha256sum ApplicationDiscoveryServiceAgentlessCollector.ova
   ```

ステップ 3: エージェントレスコレクタをデプロイする

Application Discovery Service エージェントレスコレクター (エージェントレスコレクター) は、オンプレミスの VMware 環境にインストールする仮想アプライアンスです。このセクションでは、前のステップでダウンロードしたオープン仮想化アーカイブ (OVA) ファイルを VMware 環境にデプロイする方法について説明します。

エージェントレスコレクター:仮想マシンの仕様

- オペレーティングシステム — Amazon リナックス 2
- RAM — 16 GB
- CPU — 4 コア

以下の手順では、VMware 環境にエージェントレスコレクター OVA ファイルをデプロイする手順を順を追って説明します。

エージェントレスコレクタをデプロイするには

1. VMware 管理者として vCenter にサインインします。
2. 以下のいずれかの方法で OVA ファイルをインストールします。
   - UI を使用する:[ファイル]、[OVF テンプレートのデプロイ] の順に選択し、前のセクションでダウンロードしたコレクター OVA ファイルを選択して、ウィザードを完了します。
   - コマンドラインを使用する：コレクタ OVA ファイルをコマンドラインからインストールするには、VMware Open Virtualization Format Tool (ovftool) をダウンロードして使用します。ovftool をダウンロードするには、OVF ツールのドキュメントページからリリースを選択します。

     以下は、ovftool コマンドラインツールを使用してコレクター OVA ファイルをインストールする例です。

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

     以下では、**********。

     - この名前は、エージェントレスコレクタ VM に使用したい名前です。
     - データストアは、vCenter 内のデータストアの名前です。

- OVA ファイル名は、ダウンロードされたコレクタ OVA ファイルの名前です。
- ユーザー名/パスワードは vCenter の認証情報です。
- vcenterurl は vCenter の URL です。
- vi パスは VMware ESXi ホストへのパスです。

3. vCenter にデプロイされたエージェントレスコレクタを探します。VM を右クリックして、[パワー]、[パワーオン] を選択します。
4. 数分後、コレクタの IP アドレスが vCenter に表示されます。この IP アドレスを使用してコレクタに接続します。

ステップ 4: エージェントレスコレクターコンソールにアクセスする

以下の手順では、Application Discovery Service のエージェントレスコレクター (エージェントレスコレクター) コンソールにアクセスする方法について説明します。

エージェントレスコレクターコンソールにアクセスするには

1. Web ブラウザを開き、アドレスバーに次の URL を入力します。**https://**<ip_address>、<ip_address>はコレクターの送信元の IP アドレスです。ステップ 3: エージェントレスコレクタをデプロイする
2. エージェントレスコレクターに初めてアクセスするときは、「はじめに」を選択します。その後、ログインを求められます。

エージェントレスコレクターコンソールに初めてアクセスする場合は、次にアクセスします。ステップ 5: エージェントレスコレクタの設定それ以外の場合は、次に表示されます。エージェントレスコレクタダッシュボード

ステップ 5: エージェントレスコレクタの設定

Application Discovery Service エージェントレスコレクター (エージェントレスコレクター) は Amazon Linux 2 ベースの仮想マシン (VM) です。次のセクションでは、エージェントレスコレクターコンソールの [エージェントレスコレクターの設定] ページでコレクター VM を設定する方法について説明します。

「エージェントレスコレクタの設定」ページでコレクタ VM を設定するには

1. [コレクタ名] には、コレクタを識別するための名前を入力します。名前にはスペースを使用できますが、特殊文字は使用できません。
2. 「データ同期」で、AWSコレクターが発見したデータを受信する宛先アカウントとして IAM AWS ユーザーが指定するアカウントのアクセスキーとシークレットキーを入力します。IAM ユーザーの要件については、を参照してください。ステップ 1: エージェントレスコレクター用の IAM ユーザーを作成する

   a. AWSaccess-key には、AWS宛先アカウントとして指定するアカウント IAM ユーザーのアクセスキーを入力します。

   b. AWSsecret-key には、AWS移行先アカウントとして指定しているアカウント IAM ユーザーのシークレットキーを入力します。

   c. (オプション) ネットワークのアクセスにプロキシの使用が必要な場合は、プロキシホスト AWS、プロキシポート、およびオプションで、既存のプロキシサーバーでの認証に必要な認証情報を入力します。
3. [エージェントレスコレクタのパスワード] で、エージェントレスコレクタへのアクセスの認証に使用するパスワードを設定します。

   - パスワードは、大文字と小文字が区別されます。
   - パスワードは、8～64 文字の長さにする必要があります。
   - パスワードには、次の 4 つカテゴリから少なくとも 1 文字を含める必要があります。
     - 小文字 a〜z
     - 大文字 A〜Z
     - 数字 0〜9
     - 英数字以外の文字 (@$! #%*? &)
   - パスワードには、次の文字以外の特殊文字は使用できません:@$! #%*? &

   a. [エージェントレスコレクタのパスワード] には、コレクタへのアクセスの認証に使用するパスワードを入力します。

   b. [エージェントレスコレクタのパスワードを再入力] には、確認のためパスワードをもう一度入力します。
4. [その他の設定] で、使用許諾契約をお読みください。同意する場合は、チェックボックスを選択してください。

5. エージェントレスコレクターの自動更新を有効にするには、「その他の設定」で「エージェントレスコレクターを自動的に更新する」を選択します。このチェックボックスを選択しない場合は、で説明されているように、エージェントレスコレクタを手動で更新する必要があります。エージェントレスコレクターの手動更新
6. [設定を保存] を選択します。

以下のトピックでは、コレクターのオプション設定タスクについて説明します。

オプション設定タスク

- (オプション) エージェントレスコレクタ VM の固定 IP アドレスを設定します。
- (オプション) エージェントレスコレクタ VM を DHCP を使用するようにリセットし直します。
- (オプション) Kerberos 認証プロトコルを設定します。

(オプション) エージェントレスコレクタ VM の固定 IP アドレスを設定します。

次の手順では、Application Discovery Service エージェントレスコレクタ (エージェントレスコレクタ) 仮想マシンの固定 IP アドレスを設定する方法について説明します。コレクタ VM を初めてインストールすると、動的ホスト構成プロトコル (DHCP) を使用するように構成されます。

> **Note**
>
> エージェントレスコレクタは IPv4 をサポートします。IPv6 はサポートしていません。

コレクタ VM の固定 IP アドレスを設定するには

1. VMware vCenter から次のネットワーク情報を収集します。
   - 固定 IP アドレス — サブネット内の署名されていない IP アドレス。たとえば 192.168.1.138 などです。
   - ネットワークマスク — コレクタ仮想マシンをホストする VMware vCenter ホストの IP アドレス設定を確認することで取得できます。たとえば、255.255.255.0 などです。
   - デフォルトゲートウェイ — コレクタ仮想マシンをホストする VMware vCenter ホストの IP アドレス設定を確認することで取得できます。たとえば、192.168.1.1 などです。
   - プライマリ DNS — コレクタ仮想マシンをホストする VMware vCenter ホストの IP アドレス設定を確認することで取得できます。たとえば、192.168.1.1 などです。

- (オプション) セカンダリ DNS
- (オプション) ローカルドメイン名 — コレクタがドメイン名なしで vCenter ホスト URL にアクセスできるようにします。

2. コレクタの VM コンソールを開き、**ec2-usercollector**次の例のようにパスワードを使用してサインインします。

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

3. リモートターミナルで以下のコマンドを入力して、ネットワークインターフェースを無効にします。

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

4. 以下の手順でインターフェース eth0 の設定を更新します。

   a. 次のコマンドを使用して ifcfg-eth0 を vi エディターで開きます。

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

   b. 次の例に示すように、「ネットワーク情報の収集」ステップで収集した情報でインターフェースの値を更新します。

   ```
   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. 次の手順を使用してドメインネームシステム (DNS) を更新します。

   a. 次のコマンドを使用して vi `resolv.conf` でファイルを開きます。

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

b. 次のコマンドを使用して vi resolv.conf 内のファイルを更新します。

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

次の例は、resolv.conf編集されたファイルを示しています。

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

6. 以下のコマンドを入力して、ネットワークインターフェースを有効にします。

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

7. 次の例のように VM を再起動します。

```
sudo reboot
```

8. 次の手順を使用してネットワーク設定を確認します。

a. 次のコマンドを入力して、IP アドレスが正しく設定されているかどうかを確認してください。

```
ifconfig

ip addr show
```

b. 次のコマンドを入力して、ゲートウェイが正しく追加されたことを確認します。

```
route -n
```

出力は次の例のようになるはずです。

```
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. 次のコマンドを入力して、パブリック URL に ping を送信できることを確認します。

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

d. 次の例に示すように、vCenter IP アドレスまたはホスト名に ping を送信できることを確認します。

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

(オプション) エージェントレスコレクタ VM を DHCP を使用するようにリセットし直します。

次の手順では、DHCP を使用するようにエージェントレスコレクタ VM を再構成する方法について説明します。

DHCP を使用するようにコレクタ VM を設定するには

1. リモートターミナルで次のコマンドを入力して、ネットワークインターフェースを無効にします。

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

2. 以下の手順でネットワーク設定を更新します。

a. 次のコマンドを使用して vi `ifcfg-eth0` エディターでファイルを開きます。

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

b. 次の例のように、`ifcfg-eth0` ファイル内の値を更新します。

```
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. 次のコマンドを入力して DNS 設定をリセットします。

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

4. 次のコマンドを入力して、ネットワークインターフェースを有効にします。

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

5. 次の例のようにコレクタ VM を再起動します。

```
sudo reboot
```

(オプション) Kerberos 認証プロトコルを設定します。

OS サーバーが Kerberos 認証プロトコルをサポートしている場合、このプロトコルを使用してサーバーに接続できます。そのためには、Application Discovery Service エージェントレスコレクタ VM を設定する必要があります。

以下の手順では、Application Discovery Service エージェントレスコレクタ仮想マシンで Kerberos 認証プロトコルを設定する方法について説明します。

コレクタ VM で Kerberos 認証プロトコルを設定するには

1. コレクタの VM コンソールを開き、**ec2-usercollector**次の例のようにパスワードを使用してサインインします。

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

2. krb5.conf/etcフォルダ内の設定ファイルを開きます。そのためには、次のコード例を使用できます。

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

3. krb5.conf設定ファイルを以下の情報で更新します。

```
[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
```

ファイルを保存し、テキストエディタを終了します。

4. 次の例のようにコレクタ VM を再起動します。

```
sudo reboot
```

ステップ 6: エージェントレスコレクタデータ収集モジュールをセットアップする

Application Discovery Service Agentless Collector (エージェントレスコレクター) コンソールのダッシュボードページの [データ収集] で、サーバーからインベントリ、プロファイル、および使用状況データを収集するデータ収集モジュールを設定します。

エージェントレスコレクターは現在、VMware VM、データベース、分析サーバーからのデータ収集をサポートしています。将来のモジュールでは、他の仮想化プラットフォームからの収集とオペレーティングシステムレベルの収集がサポートされる予定です。

トピック

- VMware vCenter エージェントレスコレクタデータ収集モジュール
- データベースと分析データ収集モジュール

VMware vCenter エージェントレスコレクタデータ収集モジュール

このセクションでは、VMware VMからサーバーのインベントリ、プロファイル、および使用率データを収集するために使用されるApplication Discovery Service エージェントレスコレクター (エージェントレスコレクター) VMware vCenterデータ収集モジュールについて説明します。

トピック

VMware vCenter 用のエージェントレスコレクタデータ収集モジュールをセットアップする方法

このセクションでは、エージェントレスコレクタのVMware vCenterデータ収集モジュールを設定して、VMware VMからサーバのインベントリ、プロファイル、および使用率データを収集する方法について説明します。

> **Note**
>
> vCenterのセットアップを開始する前に、システムグループに設定された読み取り権限と表示権限を持つvCenter認証情報を指定できることを確認してください。

VMware vCenter データ収集モジュールをセットアップするには

1. エージェントレスコレクタのダッシュボードページの [データ収集] で、[VMware vCenter] セクションの [セットアップ] を選択します。
2. VMware vCenter データ収集のセットアップページで、以下を実行します。
    a. vCenter の認証情報の下:
        i. vCenter URL/IP には、VMware vCenter サーバホストの IP アドレスを入力します。
        ii. vCenter ユーザー名には、コレクタが vCenter との通信に使用するローカルユーザーまたはドメインユーザーの名前を入力します。ドメインユーザーの場合、domain\username または username@domain 形式を使用します。
        iii. [vCenter Password] で、ローカルユーザーまたはドメインユーザーのパスワードを入力します。

b. [データ収集設定] で:

   - セットアップが成功した直後に自動的にデータ収集を開始するには、「データ収集を自動的に開始する」を選択します。

c. [Set up (セットアップ)] を選択します。

次に、次のトピックで説明する VMware データ収集の詳細ページが表示されます。

VMware データ収集の詳細

VMware データ収集の詳細ページには、設定した vCenter に関する詳細が表示されますVMware vCenter 用のエージェントレスコレクタデータ収集モジュールをセットアップする方法。

検出されたvCenterサーバには、セットアップしたvCenterとそのvCenterに関する次の情報が表示されます。

- vCenter サーバーの IP アドレス。
- vCenter 内のサーバの数。
- データ収集のステータス。
- 前回の更新からどれくらいの時間が経過したか。

[vCenter サーバの削除] を選択すると、表示された vCenter サーバが削除され、[VMware vCenter データ収集のセットアップ] ページに戻ります。

データ収集を自動的に開始することを選択しなかった場合は、このページの [データ収集の開始] ボタンを使用してデータ収集を開始できます。データ収集が開始されると、[開始] ボタンが [データ収集の停止] に変わります。

収集状況列に「収集中」と表示されている場合は、データ収集が開始されています。

AWS Migration Hub収集されたデータはコンソールに表示されます。VMware vCenter Server インベントリのデータを収集する場合、データ収集を有効にしてから約 15 分でコンソールに表示されるデータにアクセスできます。

インターネットへのアクセスがブロックされていない場合は、このページの [Migration Hub のサーバーを表示] を選択して Migration Hub コンソールを開くことができます。このボタンを選択するかどうかにかかわらず、Migration Hub コンソールへのアクセス方法については、を参照してくださいステップ 7: 収集したデータを表示する。

移行計画活動に基づく推奨データ収集期間のガイドラインは次のとおりです。

- TCO (総所有コスト)-2 ~ 4 週間
- 移行計画-2 ~ 6 週間

vCenter データ収集範囲の制御

Application Discovery Service を使用してインベントリを行うには、vCenter ユーザーに各 ESX ホストまたは VM に対する読み取り専用許可が必要です。許可設定を使用すると、データ収集に組み込まれるホストと VM を制御できます。現在の vCenter にあるすべてのホストと VM のインベントリを許可することも、case-by-case権限を個別に付与することもできます。

> **Note**
>
> セキュリティベストプラクティスとして、Application Discovery Service の vCenter ユーザーに追加の不要な許可を付与しないことをお勧めします。

次の手順では、細分化がおおまかなものから細かいものまでの設定シナリオを順に説明します。これらの手順は vSphere クライアント v6.7.0.2 用です。他のバージョンのクライアントの手順は、使用している vSphere クライアントのバージョンによって異なる場合があります。

現在の vCenter のすべての ESX ホストと VM に関するデータを検出するには

1. VMware vSphere クライアントでは、[vCenter] を選択してから [Hosts and Clusters] または [VMs and Templates] を選択します。
2. データセンターリソースを選択し、[権限] を選択します。
3. vCenter ユーザーを選択し、シンボルを選択してユーザーロールを追加、編集、または削除します。
4. 「ロール」メニューから「読み取り専用」を選択します。
5. 「子どもに伝達」を選択し、「OK」 を選択します。

特定の ESX ホストとそのすべての子オブジェクトに関するデータを検出するには

1. VMware vSphere クライアントでは、[vCenter] を選択してから [Hosts and Clusters] または [VMs and Templates] を選択します。
2. [Related Objects]、[Hosts] の順に選択します。

3. ホスト名を右クリックしてコンテキストメニューを開き、[All vCenter Actions]、[Add Permission] の順に選択します。
4. [Add Permission] で、vCenter ユーザーをホストに追加します。[Assigned Role] では、[Read-only] を選択します。
5. [Propagate to children]、[OK] を選択します。

specific の ESX ホストまたは子 VM に関するデータを検出するには

1. VMware vSphere クライアントでは、[vCenter] を選択してから [Hosts and Clusters] または [VMs and Templates] を選択します。
2. [Related Objects] を選択します。
3. [Hosts] (vCenter に認識される ESX ホストのリストを表示) または [Virtual Machines] (すべてのホスト ESX ホストにわたる VM のリストを表示) を選択します。
4. ホストあるいは VM 名を右クリックしてコンテキストメニューを開き、[All vCenter Actions]、[アクセス許可の追加] の順に選択します。
5. [Add Permission] で、vCenter ユーザーをホストまたは VM に追加します。[Assigned Role] では、[読み取り専用] を選択します。
6. [OK] を選択します。

> **Note**
>
> [子に伝達] を選択した場合でも、ESX ホストと VMcase-by-case から読み取り専用権限を段階的に削除できます。このオプションは、他の ESX ホストや VM に適用される、継承された許可には影響しません。

データベースと分析データ収集モジュール

このセクションでは、データベースと分析データ収集モジュールをセットアップ、設定、および使用する方法について説明します。このデータ収集モジュールを使用してデータ環境に接続し、オンプレミスのデータベースと分析サーバーからメタデータとパフォーマンスメトリックを収集できます。このモジュールで収集できるメトリクスの詳細については、「」を参照してくださいAgentless Collector データベースと分析データ収集モジュールによって収集されたデータ。

大まかに言うと、データベースと分析データ収集モジュールを使用するときは、次の手順を実行します。

1. 前提条件となるステップを完了し、IAM ユーザーを設定し、AWS DMSデータコレクターを作成します。
2. データ転送を設定して、データ収集モジュールが収集したメタデータとパフォーマンスメトリックをに送信できるようにしますAWS。
3. LDAP サーバーを追加し、それらを使用してデータ環境内の OS サーバーを検出します。または、OS サーバを手動で追加するか、を使用してくださいVMware データ収集モジュール。
4. OS サーバーへの接続認証情報を設定し、それを使用してデータベースサーバーを検出します。
5. データベースと分析サーバーへの接続認証情報を設定し、データ収集を実行します。詳細については、「データベースと分析データの収集」を参照してください。
6. AWS DMS収集されたデータをコンソールに表示し、そのデータを使用してへの移行に関するターゲット推奨事項を生成しますAWS クラウド。詳細については、「データベースと分析データの収集」を参照してください。

トピック

- サポートされている OS、データベース、分析サーバー
- AWS DMSデータコレクターの作成
- データ転送の設定
- LDAP サーバーと OS サーバーを追加します
- データベースサーバーを確認

サポートされている OS、データベース、分析サーバー

エージェントレスコレクターのデータベースおよび分析データ収集モジュールは、Microsoft Active Directory LDAP サーバーをサポートしています。

このデータ収集モジュールは、次の OS サーバーをサポートします。

- Amazon Linux 2
- CentOS Linux バージョン 6 およびそれ以降
- Debian バージョン 10 以降
- Red Hat Enterprise Linux 7 以降
- SUSE Linux Enterprise Server バージョン 12 以降
- ウブントゥバージョン 16.01 およびそれ以降

- Windows Server 2012 以降
- ウィンドウズ XP およびそれ以降

また、データベースおよび分析データ収集モジュールは、以下のデータベースサーバーをサポートしています。

- Microsoft SQL Server バージョン 2012 以降 2019
- MySQL バージョン 5.6 以降 8
- オラクル· バージョン 11g リリース 2 および最大 12c、19c、21c
- PostgreSQL バージョン 9.6 以降 13

AWS DMSデータコレクターの作成

データベースと分析データ収集モジュールは、AWS DMSAWS DMSデータコレクターを使用してコンソールを操作します。AWS DMS収集したデータをコンソールで表示したり、AWSそのデータを使用して適切なサイズのターゲットエンジンを決定したりできます。詳細については、「AWS DMS フリートアドバイザーのターゲットレコメンデーション機能の使用」を参照してください。

データコレクターを作成する前に、AWS DMSデータコレクターが Amazon S3AWS DMS バケットにアクセスするために使用する IAM ロールを作成します。この Amazon S3 バケットは、の前提条件を満たしたときに作成されましたエージェントレスコレクタの前提条件。

AWS DMSデータコレクターから Amazon S3 にアクセスするための IAM ロールを作成するには

1. AWS Management Console にサインインして、IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. ナビゲーションペインで [ロール] を選択し、[ロールの作成] を選択します。
3. [信頼済みエンティティの選択] ページの [信頼済みエンティティタイプ] で、[AWSサービス] を選択します。AWS他のサービスのユースケースについては、DMS を選択してください。
4. DMS チェックボックスを選択し、[次へ] を選択します。
5. [権限の追加] ページで、以前に作成した FleetAdvisorS3Policy を選択します。[Next] (次へ) を選択します。
6. [名前、確認、作成] ページで、[ロール名]**FleetAdvisorS3Role** に入力し、[ロールの作成] を選択します。
7. 作成したロールを開き、「信頼関係」タブを選択します。[Edit trust policy] (信頼ポリシーを編集) を選択します。

8. 「信頼ポリシーの編集」 ページで、次の JSON を エディターに貼り付け、既存のコードを置き換えます。

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

9. [ポリシーの更新] を選択します。

次に、AWS DMSコンソールにデータコレクターを作成します。

AWS DMSデータコレクターを作成するには

1. AWS Management Consoleにログインし、https://console.aws.amazon.com/dms/v2/AWS DMS でコンソールを開きます。
2. Migration HubAWS リージョン ホームリージョンとして設定したものを選択します。詳細については、「Migration Hub にサインインして、ホームリージョンを選択してください」を参照してください。
3. ナビゲーションペインで、[Discover] の下の [データコレクター] を選択します。[Data collectors] (データコレクター) ページが開きます。
4. [Create data collector] (データコレクターの作成) を選択します。[Create data collector] (データコレクターの作成) ページが開きます。
5. 「一般設定」セクションの「名前」に、データコレクターの名前を入力します。
6. [Connectivity] (接続) セクションで、[Browse S3] (S3 を参照) を選択します。以前に作成した Amazon S3 バケットをリストから選択します。
7. IAM ロールには、`FleetAdvisorS3Role`以前に作成したロールを選択します。
8. [Create data collector] (データコレクターの作成) を選択します。

データ転送の設定

AWS必要なリソースを作成したら、AWS DMSデータベースおよび分析データ収集モジュールからコレクターへのデータ転送を設定します。

データ転送を設定するには

1. エージェントレスコレクタコンソールを開きます。詳細については、「ステップ 4: コレクターコンソールにアクセスする」を参照してください。
2. [データベースと分析コレクターを表示] を選択します。
3. ダッシュボードページの「データ転送」セクションで「データ転送の設定」を選択します。
4. IAM アクセスキー ID と IAM シークレットアクセスキーについてはAWS リージョン、エージェントレスコレクターは以前に設定した値を使用します。詳細については、Migration Hub にサインインして、ホームリージョンを選択してくださいおよびステップ 1: IAM ユーザーを作成するを参照してください。
5. Connected DMS データコレクタについては、AWS DMSコンソールで作成したデータコレクタを選択します。
6. [Save] (保存) を選択します。

データ転送を設定したら、ダッシュボードページの「データ転送」セクションを確認します。データベースと分析データ収集モジュールに

[DMS へのアクセスは接続済み] と [S3 へのアクセス] が表示されていることを確認します。

LDAP サーバーと OS サーバーを追加します

データベースおよび分析データ収集モジュールは、Microsoft Active Directory の LDAP を使用して、ネットワーク内の OS、データベース、および分析サーバーに関する情報を収集します。LDAP (ライトウェイトディレクトリアクセスプロトコル) はオープンスタンダードのアプリケーションプロトコルです。このプロトコルを使用すると、IP ネットワーク上の分散ディレクトリ情報サービスにアクセスして管理できます。

既存の LDAP サーバーをデータベースおよび分析データ収集モジュールに追加して、ネットワーク内の OS サーバーを自動的に検出できます。LDAP を使用しない場合は、OS サーバーを手動で追加できます。

LDAP サーバーをデータベースおよび分析データ収集モジュールに追加するには

1. エージェントレスコレクタコンソールを開きます。詳細については、「ステップ 4: コレクターコンソールにアクセスする」を参照してください。
2. [データベースと分析コレクターを表示] を選択し、ナビゲーションペインの [検出] で [LDAP サーバー] を選択します。
3. 「LDAP サーバーの追加」を選択します。「LDAP サーバーの追加」ページが開きます。
4. [ホスト名] に、LDAP サーバーのホスト名を入力します。
5. [ポート] (LDAP) リクエストに使用するポート番号を入力します。
6. [ユーザー名] (LDAP) サーバーへの接続に使用するユーザー名を入力します。
7. パスワード] に、LDAP サーバーへの接続に使用するパスワードを入力します。
8. (オプション)「接続を確認」を選択し、LDAP サーバーの認証情報が正しく追加されていることを確認します。または、後で LDAP サーバーページのリストから LDAP サーバーの接続認証情報を確認することもできます。
9. 「LDAP サーバーの追加」を選択します。
10. 「LDAP サーバー」ページで、リストから LDAP サーバーを選択し、「OS サーバーの検出」を選択します。

> **Important**
>
> OS 検出の場合、データ収集モジュールには、LDAP プロトコルを使用してリクエストを実行するためのドメインサーバー用の認証情報が必要です。

データベースおよび分析データ収集モジュールは LDAP サーバーに接続し、OS サーバーを検出します。データ収集モジュールが OS サーバーの検出を完了したら、[OS サーバーを表示] を選択すると、検出された OS サーバーのリストが表示されます。

または、OS サーバーを手動で追加するか、サーバーリストをカンマ区切り値 (CSV) ファイルからインポートすることもできます。また、VMware vCenter エージェントレスコレクタデータ収集モジュールを使用して OS サーバを検出することもできます。詳細については、「VMware データ収集モジュール」を参照してください。

OS サーバーをデータベースおよび分析データ収集モジュールに追加するには

1. データベースと分析のコレクターページで、ナビゲーションペインの「検出」で「OS サーバー」を選択します。
2. [OS サーバーの追加] を選択します。「OS サーバーの追加」ページが開きます。
3. OS サーバーの認証情報を入力します。

   a. OS タイプには、サーバーのオペレーティングシステムを選択します。

   b. [ホスト名] (IP) OS サーバーのホスト名または IP アドレスを入力します。

   c. [ポート] (リモートクエリに使用するポート番号) を入力します。

   d. [認証タイプ] で、OS サーバーが使用する認証タイプを選択します。

   e. [ユーザー名] (OS) サーバーへの接続に使用するユーザー名を入力します。

   f. パスワード] に、OS サーバーへの接続に使用するパスワードを入力します。

   g. [Verify] を選択して、OS サーバーの認証情報が正しく追加されていることを確認します。
4. (オプション) CSV ファイルから複数の OS サーバを追加します。

   a. [CSV から OS サーバーの一括インポート] を選択します。

   b. [テンプレートをダウンロード] を選択して、カスタマイズ可能なテンプレートを含む CSV ファイルを保存します。

   c. テンプレートに従って、OS サーバーの接続認証情報をファイルに入力します。次の例は、OS Server 接続認証情報を CSV V) で提供する方法を示しています。

   ```
   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
   ```

   すべての OS サーバーの認証情報を追加したら、CSV ファイルを保存します。

   d. 「ブラウズ」 を選択し、CSV ファイルを選択します。
5. [OS サーバーの追加] を選択します。
6. すべての OS サーバーの認証情報を追加したら、OS サーバーを選択し、[データベースサーバーの検出] を選択します。

データベースサーバーを確認

データベースを検出するには、データ収集モジュールに必要な最低限の権限を持つソースデータベース用のユーザーを作成します。詳細については、ユーザーガイドの「AWS DMSFleet AdvisorAWS DMS のデータベースユーザーの作成」を参照してください。

以前に追加したOSサーバーで実行されているデータベースを検出するには、データ収集モジュールがオペレーティングシステムとデータベースサーバーにアクセスする必要があります。接続設定で指定したポートでデータベースにアクセスできることを確認します。次に、データベースサーバーのリモート認証を有効にします。これに加えて、データ収集モジュールに次の権限を与えてください。

Windows でデータベースサーバーを検出するには

1. Windows 管理インストルメンテーション (WMI) および WMI クエリ言語 (WQL) クエリを実行したり、レジストリを読み取ったりするための認証情報を付与します。
2. OS サーバー接続資格情報で指定した Windows ユーザーを、分散 COM ユーザー、パフォーマンスログユーザー、パフォーマンスモニターユーザー、およびイベントログリーダーのグループに追加します。そのためには、次のコード例を使用します。

   ```
   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
   ```

   前述の例では、OS Server*username* 接続認証情報で指定した Windows ユーザーの名前に置き換えます。
3. OS サーバー接続認証情報で指定した Windows ユーザーに必要な権限を付与します。
   - Windows の管理とインストルメンテーションのプロパティでは、「ローカル起動」と「リモートアクティベーション」を選択します。
   - WMI コントロールでは、、、WMIおよび名前空間の [実行方法]、[アカウントの有効化]、[リモート有効化]CIMV2DEFAULTStandartCimv2、および [セキュリティ読み取り権限] を選択します。
   - WMI プラグインの場合は、winrm configsddl defaultを実行してから [読み取りと実行] を選択します。
4. 次のコード例を使用して Windows ホストを設定します。

```
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
```

Linux でデータベースサーバーを検出するには

1. ssnetstatおよびコマンドへの sudo アクセスを提供します。

   次のコード例では、sudossnetstat におよびコマンドへのアクセス権を付与しています。

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

   前述の例では、OS Server*username* 接続認証情報で指定した Linux ユーザーの名前に置き換えます。

   前の例では、/usr/bin/ssnetstatおよびコマンドへのパスを使用しています。このパスは環境によって異なる場合があります。ssnetstatおよびコマンドへのパスを確認するには、which sswhich netstatおよびコマンドを実行します。

2. リモート SSH スクリプトの実行を許可し、インターネット制御メッセージプロトコル (ICMP) トラフィックを許可するように Linux サーバーを設定します。

データベースサーバーの検出を開始するには

1. データベースと分析のコレクターページで、ナビゲーションペインの「検出」で「OS サーバー」を選択します。
2. データベースサーバーと分析サーバーを含む OS サーバーを選択し、[アクション] メニューの [接続の検証] を選択します。
3. 接続ステータスが「失敗」のサーバの場合は、接続認証情報を編集します。

   a. 認証情報が同じ場合は 1 台のサーバーまたは複数のサーバーを選択し、[アクション] メニューの [編集] を選択します。「OS サーバーの編集」ページが開きます。

   b. [ポート] (リモートクエリに使用するポート番号) を入力します。

   c. [認証タイプ] で、OS サーバーが使用する認証タイプを選択します。

   d. [ユーザー名] (OS) サーバーへの接続に使用するユーザー名を入力します。

   e. パスワード] に、OS サーバーへの接続に使用するパスワードを入力します。

   f. [接続を確認] を選択して、OS サーバーの認証情報が正しく更新されていることを確認します。次に [保存] を選択します。
4. すべての OS サーバーの認証情報を更新したら、OS サーバーを選択し、[データベースサーバーの検出] を選択します。

データベースおよび分析データ収集モジュールは OS サーバーに接続し、サポートされているデータベースおよび分析サーバーを検出します。データ収集モジュールが検出を完了すると、[データベースサーバーを表示] を選択すると、検出されたデータベースサーバーと分析サーバーのリストが表示されます。

または、データベースと分析サーバーをインベントリに手動で追加することもできます。また、サーバーのリストを CSV ファイルからインポートすることもできます。すでにすべてのデータベースサーバーと分析サーバーをインベントリのに追加している場合は、このステップをスキップできます。

データベースまたは分析サーバーを手動で追加するには

1. データベースと分析コレクターページのナビゲーションペインで、「データ収集」を選択します。
2. [データベースサーバーの追加] を選択します。「データベースサーバーの追加」ページが開きます。
3. データベースサーバーの認証情報を入力します。

a. [データベースエンジン] では、サーバーのデータベースエンジンを選択します。詳細については、「サポートされている OS、データベース、分析サーバー」を参照してください。

b. [ホスト名] (IP) データベースまたは分析サーバーのホスト名または IP アドレスを入力します。

c. [ポート] には、サーバーが稼働しているポートを入力します。

d. 認証タイプには、データベースまたは分析サーバーが使用する認証タイプを選択します。

e. [ユーザー名] (サーバーへの接続に使用するユーザー名) を入力します。

f. パスワード] に、サーバーへの接続に使用するパスワードを入力します。

g. Verify を選択して、データベースまたは分析サーバーの認証情報が正しく追加されていることを確認します。

4. (オプション) CSV ファイルから複数のサーバーを追加します。

a. [CSV からデータベースサーバーを一括インポート] を選択します。

b. [テンプレートをダウンロード] を選択して、カスタマイズ可能なテンプレートを含む CSV ファイルを保存します。

c. テンプレートに従って、データベースと分析サーバーの接続認証情報をファイルに入力します。次の例は、データベースまたは分析サーバーの接続認証情報を CSV V V) ファイルで指定する方法を示しています。

```
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,
```

すべてのデータベースと分析サーバーの認証情報を追加したら、CSV ファイルを保存します。

d. 「ブラウズ」 を選択し、CSV ファイルを選択します。

5. [データベースサーバーの追加] を選択します。

6. すべての OS サーバーの認証情報を追加したら、OS サーバーを選択し、[データベースサーバーの検出] を選択します。

すべてのデータベースサーバーと分析サーバーをデータ収集モジュールに追加したら、それらをインベントリに追加します。データベースと分析データ収集モジュールは、インベントリからサーバーに接続し、メタデータとパフォーマンスメトリックを収集できます。

データベースと分析サーバーをインベントリに追加するには

1. データベースと分析のコレクターページで、ナビゲーションペインの「検出」で「データベースサーバー」を選択します。
2. メタデータとパフォーマンスメトリックを収集するデータベースと分析サーバーを選択します。
3. [インベントリに追加] を選択します。

すべてのデータベースサーバーと分析サーバーをインベントリに追加したら、メタデータとパフォーマンス指標の収集を開始できます。詳細については、「データベースと分析データの収集」を参照してください。

ステップ 7: 収集したデータを表示する

Application Discovery Service エージェントレスコレクター (エージェントレスコレクター) が収集したデータは、Migration Hub コンソールで表示できます。データベースサーバーと分析サーバーについて収集されたメトリクスはコンソールで確認できます。AWS DMS

VMware vCenter エージェントレスコレクタデータ収集モジュールによって検出されたデータを表示するには

1. AWS Management Consoleにサインインし、https://console.aws.amazon.com/migrationhub/ にある Migration Hub コンソールを開きます。このタスクでは、Agentless Collector をセットアップしてアクセスするために作成した IAM ユーザーとは別の IAM ユーザーアカウントを使用することをお勧めします。
2. Migration Hub コンソールのナビゲーションペインの「検出」で、「サーバー」を選択します。
3. サーバーの詳細を表示するには、「サーバー情報」列からサーバーのホスト名を選択します。サーバーの詳細ページには、ホスト名、IP アドレス、パフォーマンスメトリックなど、サーバーに関する情報が表示されます。

データベースと分析データ収集モジュールによって検出されたデータを表示するには

1. AWS Management Consoleにサインインし、https://console.aws.amazon.com/dms/v2/ AWS DMS のコンソールを開きます。
2. 「ディスカバー」で「インベントリ」を選択します。[Inventory] (インベントリ) ページが開きます。
3. [インベントリの分析] を選択して、類似性や複雑性などのデータベーススキーマのプロパティを判断します。
4. 「スキーマ」タブを選択すると、分析結果が表示されます。

AWS DMSコンソールを使用して、重複するスキーマを特定し、移行の複雑さを判断し、future 分析のためにインベントリ情報をエクスポートできます。詳細については、「AWS DMSFleet Advisor でのインベントリーの分析への使用」を参照してください。

エージェントレスコレクターによって収集されたデータ

Application Discovery Service のエージェントレスコレクター (エージェントレスコレクター) データ収集モジュールを設定して、サーバーからインベントリ、プロファイル、および使用状況データを収集します。

エージェントレスコレクターは現在、VMware VM、データベースサーバー、分析サーバーからのデータ収集をサポートしています。将来のモジュールでは、他の仮想化プラットフォームからの収集とオペレーティングシステムレベルの収集がサポートされる予定です。データ収集の設定については、を参照してくださいステップ 6: エージェントレスコレクタデータ収集モジュールをセットアップする。

以下のトピックでは、Application Discovery Service eのエージェントレスコレクター (エージェントレスコレクター) データ収集モジュールによって収集されるデータについて説明します。

トピック

- エージェントレスコレクタ VMware vCenter データ収集モジュールによって収集されたデータ
- Agentless Collector データベースと分析データ収集モジュールによって収集されたデータ

エージェントレスコレクタ VMware vCenter データ収集モジュールによって収集されたデータ

次の情報は、Application Discovery Service エージェントレスコレクター (エージェントレスコレクター) VMware vCenter データ収集モジュールによって収集されるデータについて説明しています。データ収集の設定については、を参照してください。VMware vCenter 用のエージェントレスコレクタデータ収集モジュールをセットアップする方法

エージェントレスコレクタ VMware vCenter で収集されたデータの表の凡例:

- 収集されたデータは、特に断らない限り、キロバイト (KB) 単位です。
- Migration Hub コンソール内の同等データはメガバイト (MB) 単位で報告されます。
- アスタリスク (*) で示されたデータフィールドは、Application Discovery Service API エクスポート機能から生成される.csv ファイルでのみ使用できます。

  エージェントレスコレクタは CLI を使用したデータエクスポートをサポートします。 AWS AWS CLI を使用して収集したデータをエクスポートするには、Application Discovery Service ユーザーガイドの「収集データのエクスポート」ページの「すべてのサーバーのシステムパフォーマンスデータのエクスポート」で説明されている手順に従います。
- ポーリング間隔は約 60 分です。
- データフィールドは二重アスタリスク (**) で表され、現在 null 値を返します。

データフィールド	説明
applicationConfigurationId*	VM がグループ化されている移行アプリケーションの ID。
avgCpuUsagePct	ポーリング期間中の CPU 使用率の平均。
avgDiskBytesReadPerSecond	ポーリング期間中にディスクから読み取られた平均バイト数。
avgDiskBytesWrittenPerSecond	ポーリング期間中にディスクに書き込まれた平均バイト数。
avgDiskReadOpsPerSecond**	1 秒あたりの読み取り I/O 操作の平均回数 null。

データフィールド	説明
avgDiskWriteOpsPerSecond**	1 秒あたりの書き込み I/O 操作の平均回数。
avgFreeRAM	RAM の平均空き容量 (MB 単位)。
avgNetworkBytesReadPerSecond	1 秒あたりの読み取りバイト数の平均スループット。
avgNetworkBytesWrittenPerSecond	1 秒あたりの書き込みバイト数の平均スループット。
コンピューターメーカー	ESXi ホストから報告されたベンダー。
コンピュータモデル	ESXi ホストによって報告されたコンピュータモデル。
configId	検出された仮想マシンにApplication Discovery Service によって割り当てられた ID。
configType	検出されたリソースのタイプ。
connectorId	仮想アプライアンスの ID。
cpuType	仮想マシンのvCPU、ホストの実際のモデル。
datacenterId	vCenter の ID。
hostId*	VM ホストの ID。
hostName	仮想化ソフトウェアを実行しているホストの名前。
hypervisor	ハイパーバイザーのタイプ。
id	サーバーの ID。
lastModifiedTimeスタンプ *	データエクスポート前のデータ収集の最新の日付と時刻。
macAddress	VM の MAC アドレス。

データフィールド	説明
manufacturer	仮想化ソフトウェアのメーカー。
maxCpuUsagePct	ポーリング期間中の CPU 使用率の最大パーセンテージ。
maxDiskBytesReadPerSecond	ポーリング期間中にディスクから読み取られた最大バイト数。
maxDiskBytesWrittenPerSecond	ポーリング期間中にディスクに書き込まれた最大バイト数。
maxDiskReadOpsPerSecond**	1 秒あたりの読み取り I/O 操作の最大回数。
maxDiskWriteOpsPerSecond**	1 秒あたりの書き込み I/O 操作の最大数。
maxNetworkBytesReadPerSecond	1 秒あたりの読み取りバイト数の最大スループット。
maxNetworkBytesWrittenPerSecond	1 秒あたりに書き込まれる最大スループット量。
memoryReservation*	VM 上のメモリのオーバーコミットを避けるための制限。
moRefId	一意の vCenter 管理オブジェクトリファレンス ID。
name*	VM またはネットワークの名前 (ユーザー指定)。
numCores	VM に割り当てられた CPU コアの数。
numCpus	ESXi ホスト上の CPU ソケットの数。
numDisks**	VM 上のディスク数。
numNetworkCards**	VM 上のネットワークカードの数。
osName	VM 上のオペレーティングシステム名。

データフィールド	説明
osVersion	VM 上のオペレーティングシステムバージョン。
portGroupId*	VLAN のメンバーポートのグループの ID。
portGroupName*	VLAN のメンバーポートグループの名前。
powerState*	電源ステータス。
serverId	Application Discovery Service、検出された VM に ID を割り当てました。
smBiosId*	システム管理 BIOS の ID /バージョン。
state*	仮想アプライアンスのステータス。
toolsStatus	VMware ツールの動作状態
totalDiskFreeサイズ	空きディスク容量 (MB 単位)。vCenter Server 7.0 以降のバージョンで使用できます。
totalDiskSize	ディスクの合計容量は MB 単位で表されます。
totalRAM	VM で使用可能な RAM の合計容量 (MB 単位)。
type	ホストのタイプ。
vCenterId	VM の固有の ID 番号。
vCenterName*	vCenter ホストの名前。
virtualSwitchName*	仮想スイッチの名前。
vmFolderPath	VM ファイルのディレクトリパス。
vmName	仮想マシンの名前。

Agentless Collector データベースと分析データ収集モジュールによって収集されたデータ

Application Discovery Service エージェントレスコレクター（エージェントレスコレクター）データベースおよび分析データ収集モジュールは、データ環境から次のメトリックを収集します。データ収集の設定については、「」を参照してくださいデータベースと分析データ収集モジュール。

データベースおよび分析データ収集モジュールを使用してメタデータとデータベース容量を収集すると、次のメトリックがキャプチャされます。

- OS サーバーで使用可能なメモリ
- OS サーバー上の使用可能なストレージ
- データベースのバージョンとエディション
- OS サーバー上の CPU の数
- スキーマの数
- ストアドプロシージャの
- テーブルの数
- トリガーの
- ビュー
- スキーマ構造

AWS DMSコンソールでスキーマ分析を開始すると、データ収集モジュールは次のメトリックを分析して表示します。

- データベースサポート日
- コード行数
- スキーマの複雑さ
- スキーマの類似性

データベースおよび分析データ収集モジュールを使用してメタデータ、データベース容量、およびリソース使用率を収集すると、次の指標が取得されます。

- データベースサーバーの I/O スループット
- データベースサーバーの 1 秒あたりの入出力オペレーション数

- OS サーバーが使用する CPU の数
- OS サーバーのメモリ使用量
- OS サーバーのストレージ使用量

データベースおよび分析データ収集モジュールを使用して、Oracle および SQL Server データベースからメタデータ、容量、および使用率メトリックを収集できます。同時に、PostgreSQL データベースと MySQL データベースの場合、データ収集モジュールはメタデータのみを収集できます。

エージェントレスコレクタコンソールの使用

このセクションでは、Application Discovery Service エージェントレスコレクター (エージェントレスコレクター) コンソールを使用する方法について説明します。

トピック

エージェントレスコレクタダッシュボード

Application Discovery Service Agentless Collector (Agentless Collector) ダッシュボードページでは、コレクターのステータスを確認し、次のトピックで説明されているようにデータ収集方法を選択できます。

トピック

コレクターステータス

コレクターステータスには、コレクターに関するステータス情報が表示されます。コレクター名、コレクターの AWS への接続のステータス、Migration Hub ホームリージョン、およびバージョン。

AWS接続に問題がある場合は、エージェントレスコレクターの構成設定を編集する必要がある場合があります。

コレクター構成設定を編集するには、「コレクター設定の編集」 を選択し、に記載されている指示に従いますエージェントレスコレクタ設定の編集。

データ収集

[データ収集] で、データ収集方法を選択できます。Application Discovery Service エージェントレスコレクター (エージェントレスコレクター) は、現在、VMware VM、データベースおよび分析サーバーからのデータ収集をサポートしています。将来のモジュールでは、他の仮想化プラットフォームからの収集とオペレーティングシステムレベルの収集がサポートされる予定です。

トピック

- VMware vCenter データ収集
- データベースと分析データの収集

VMware vCenter データ収集

VMware VM からサーバインベントリ、プロファイル、および使用率データを収集するには、vCenter サーバへの接続を設定します。接続をセットアップするには、VMware vCenter セクションで [セットアップ] を選択し、に記載されている指示に従いますステップ 6: エージェントレスコレクタデータ収集モジュールをセットアップする。

vCenter データ収集をセットアップしたら、ダッシュボードから次の操作を実行できます。

- データ収集ステータスの表示
- データ収集の開始します
- データ収集の停止

> **Note**
>
> ダッシュボードページの vCenter データ収集を設定すると、VMware vCenter セクションの [セットアップ] ボタンが、データ収集ステータス情報、[データ収集の停止] ボタン、[表示と編集] ボタンに置き換わります。

データベースと分析データの収集

データベースと分析データ収集モジュールは、次の 2 つのモードで実行できます。

メタデータとデータベース容量

データ収集モジュールは、データベースや分析サーバーからスキーマ、バージョン、エディション、CPU、メモリ、ディスク容量などの情報を収集します。この収集した情報を使用して、AWS DMSコンソールでターゲットの推奨値を計算できます。ソースデータベースがオーバープロビジョニングまたはアンダープロビジョニングの場合、ターゲットのレコメンデーションもオーバープロビジョニングまたはアンダープロビジョニングになります。

これはデフォルトモードです。

メタデータ、データベース容量、リソース使用率

データ収集モジュールは、メタデータとデータベース容量情報に加えて、データベースと分析サーバーのCPU、メモリ、ディスク容量の実際の使用率メトリックを収集します。このモードでは、推奨が実際のデータベースワークロードに基づいているため、デフォルトモードよりも正確なターゲット推奨が提供されます。このモードでは、データ収集モジュールは毎分パフォーマンスメトリックを収集します。

データベースと分析サーバーからメタデータとパフォーマンス指標の収集を開始するには

1. データベースと分析コレクターページのナビゲーションペインで、「データ収集」を選択します。
2. データベースインベントリリストから、メタデータとパフォーマンスメトリックを収集するデータベースと分析サーバーを選択します。
3. [データ収集を実行] を選択します。[データ収集タイプ] ダイアログボックスが開きます。
4. 分析用にデータを収集する方法を選択します。

   メタデータ、データベース容量、およびリソース使用率オプションを選択した場合は、データ収集期間を設定します。今後 7 日間にデータを収集することも、カスタム範囲を 1 ~ 60 日間に設定することもできます。
5. [データ収集を実行] を選択します。データ収集ページが開きます。
6. データ収集のステータスを確認するには、「コレクションヘルス」タブを選択します。

データ収集の完了すると、データ収集モジュールは収集したデータを Amazon S3 バケットにアップロードします。次に、で説明されているように、この収集されたデータを表示できますステップ 7: 収集したデータを表示する。

エージェントレスコレクタ設定の編集

コレクターは、で説明されているように、Application Discovery Service エージェントレスコレクター (エージェントレスコレクター) を初めて設定したときに構成しましたステップ 5: エージェントレスコレクタの設定。以下の手順では、エージェントレスコレクターの構成設定を編集する方法を説明します。

コレクター構成設定を編集するには

- エージェントレスコレクターダッシュボードの「コレクター設定の編集」ボタンを選択します。

  コレクター設定の編集ページで、次の操作を行います。

  a. 「コレクター名」には、コレクターを識別する名前を入力します。名前にはスペースを含めることができますが、特殊文字を含めることはできません。

  b. 「AWS検出データの宛先アカウント」に、AWSAWSコレクターが検出したデータを受信する宛先アカウントとして指定するアカウントのアクセスキーとシークレットキーを入力します。IAM ユーザーの要件については、を参照してくださいステップ 1: エージェントレスコレクター用の IAM ユーザーを作成する。

     i. AWSaccess-key には、AWS宛先アカウントとして指定しているアカウント IAM ユーザーのアクセスキーを入力します。

     ii. AWSsecret-key には、AWS宛先アカウントとして指定しているアカウント IAM ユーザーのシークレットキーを入力します。

  c. 「エージェントレスコレクタパスワード」で、エージェントレスコレクタへのアクセスを認証するために使用するパスワードを変更します。

     i. 「エージェントレスコレクタパスワード」には、エージェントレスコレクタへのアクセスを認証するために使用するパスワードを入力します。

     ii. Agentless Collector のパスワードを再入力するには、確認のためにパスワードをもう一度入力します。

  d. [設定を保存] を選択します。

次に表示されますエージェントレスコレクタダッシュボード。

VMware vCenter 認証情報の編集

VMware VM からサーバインベントリ、プロファイル、および使用率データを収集するには、vCenter サーバへの接続を設定します。VMware vCenter 接続の設定については、「」を参照してくださいステップ 6: エージェントレスコレクタデータ収集モジュールをセットアップする。

このセクションでは、vCenter 認証情報を編集する方法について説明します。

> **Note**
>
> vCenter認証情報を編集する前に、システムグループに設定されている読み取り権限と表示権限をvCenter認証情報に指定できることを確認してください。

VMware vCenter の認証情報を編集するには

VMware データ収集の詳細ページで、[vCenter サーバの編集] を選択します。

- vCenter の編集ページで、以下を実行します。
  a. vCenter の認証情報の下:
     i. vCenter URL/IP には、お使いの VMware vCenter サーバホストの IP アドレスを入力します。
     ii. [vCenter Username] には、コネクタが vCenter との通信に使用するローカルまたはドメインユーザーの名前を入力します。ドメインユーザーの場合、domain\username または username@domain 形式を使用します。
     iii. [vCenter Password] で、ローカルユーザーまたはドメインユーザーのパスワードを入力します。
  b. [Save] (保存) を選択します。

エージェントレスコレクターの手動更新

Application Discovery Service エージェントレスコレクター (エージェントレスコレクター) を設定する場合、「」の説明に従って自動更新を有効にすることを選択できますステップ 5: エージェントレスコレクタの設定。自動更新を有効にしない場合は、エージェントレスコレクターを手動で更新する必要があります。

次の手順では、エージェントレスコレクターを手動で更新する方法について説明します。

エージェントレスコレクターを手動で更新するには

1. 最新の Agentless Collector Open Virtualization Archive (OVA) ファイルを取得します。
2. （オプション) 最新の Agentless Collector OVA ファイルをデプロイする前に、以前の Agentless Collector OVA ファイルを削除することをお勧めします。
3. エージェントレスコレクター入門 セクションで、 ステップ 3: エージェントレスコレクタをデプロイする のステップに従いますステップ 6: エージェントレスコレクタデータ収集モジュールをセットアップする。

前の手順では、エージェントレスコレクターのみを更新します。OS を最新の状態に保つのはお客様の責任です。

Amazon EC2 インスタンスを更新するには

1. VMware vCenter から Agentless Collector の IP アドレスを取得します。
2. 次の例**collector**に示すように、コレクターの VM コンソールを開き、パスワード**ec2-user**を使用して としてサインインします。

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

3. 「Amazon Linux 2 ユーザーガイド」の「AL2 インスタンスのインスタンスソフトウェアの更新」の手順に従います。

Amazon Linux 2 でのカーネルライブパッチ

Agentless Collector 仮想マシンは、「」で説明されているように Amazon Linux 2 を使用しますステップ 3: エージェントレスコレクタをデプロイする。

Amazon Linux 2 のライブパッチを有効にして使用するには、「Amazon Amazon EC2ユーザーガイド」の「Amazon Linux 2 でのカーネルライブパッチ」を参照してください。

エージェントレスコレクタのトラブルシューティング

このセクションには、Application Discovery Service エージェントレスコレクター (エージェントレスコレクター) に関する既知の問題のトラブルシューティングに役立つトピックが含まれています。

トピック

セットアップ中にエージェントレスコレクターにアクセスできない問題を修正しました。 AWS

エージェントレスコレクタは、TCP ポート 443 を介した複数のドメインへのアウトバウンドアクセスを必要とします。 AWS コンソールでエージェントレスコレクタを設定すると、次のエラーメッセージが表示されることがあります。

> アクセスできませんでした AWS
>
> AWS 連絡が取れない。ネットワーク設定を確認してください。

このエラーは、エージェントレスコレクターが、 AWS セットアップ処理中にコレクターが通信する必要のあるドメインへの HTTPS 接続を確立しようとして失敗したことが原因で発生します。接続を確立できない場合、エージェントレスコレクタの設定は失敗します。

接続を修正するには AWS

1. IT 管理者に問い合わせて、会社のファイアウォールが、 AWS アウトバウンドアクセスを必要とするドメインへのポート 443 のアウトバウンドトラフィックをブロックしていないか確認してください。 AWS アウトバウンドアクセスが必要なドメインは、ホームリージョンが米国西部 (オレゴン) リージョン、us-west-2、またはその他のリージョンのいずれであるかによって異なります。

AWS アカウントのホームリージョンが us-west-2 の場合、次のドメインにはアウトバウンドアクセスが必要です。

- `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`

AWS アカウントのホームリージョンがそうでない場合、以下のドメインにはアウトバウンドアクセスが必要です。**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`

Agentless Collector AWS が通信する必要のあるドメインへのアウトバウンドアクセスをファイアウォールがブロックしている場合は、Collector 設定の「データ同期」セクションでプロキシホストを設定します。

2. ファイアウォールを更新しても接続の問題が解決しない場合は、次の手順を実行して、コレクタ仮想マシンが前のステップでリストされたドメインへのアウトバウンドネットワーク接続を確立していることを確認します。

   a. VMware vCenter からエージェントレスコレクタの IP アドレスを取得します。

   b. コレクタの VM コンソールを開き、**ec2-usercollector**次の例のようにパスワードを使用してサインインします。

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

   c. 次の例のように、ポート 443 で telnet を実行して、一覧表示されたドメインへの接続をテストします。

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

3. telnet でドメインを解決できない場合は、Amazon Linux 2 の手順に従って静的 DNS サーバーを設定してみてください。
4. エラーが続く場合は、詳細なサポートについては、を参照してくださいAWS エージェントレスコレクタの問題に関するSupport への連絡。

プロキシホストに接続するときの自己署名証明書の問題の解決

オプションで提供されるプロキシとの通信が HTTPS 経由で、プロキシに自己署名証明書がある場合は、証明書の提供が必要になることがあります。

1. VMware vCenter からエージェントレスコレクタの IP アドレスを取得します。
2. コレクターの VM コンソールを開き、`ec2-usercollector`次の例のようにパスワードを使用してサインインします。

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

3. セキュアプロキシに関連付けられている証明書の本文 (`-----BEGIN CERTIFICATE----------END CERTIFICATE-----`との両方を含む) を次のファイルに貼り付けます。

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

4. 新しい証明書をインストールするには、以下のコマンドを実行します。

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

5. 以下のコマンドを実行して、エージェントレスコレクターを再起動します。

```
sudo shutdown -r now
```

異常のあるコレクターの検索

各コレクターのステータス情報は、 AWS Migration Hub (Migration Hub) コンソールのデータコレクターページにあります。ステータスが 「要注意」のコレクターを見つけることで、問題のあるコレクターを特定できます。

次の手順では、エージェントレスコレクターコンソールにアクセスしてヘルス問題を特定する方法について説明します。

エージェントレスコレクターコンソールにアクセスするには

1. AWS AWS Management Console アカウントを使用してにサインインし、https://console.aws.amazon.com/migrationhub/ にある Migration Hub コンソールを開きます。
2. Migration Hub コンソールのナビゲーションペインの [検出] で、[データコレクター] を選択します。
3. エージェントレスコレクタータブから、ステータスが「要注意」になっている各コネクタの IP アドレスを書き留めておきます。
4. エージェントレスコレクターコンソールを開くには、Web ブラウザーを開きます。次に、アドレスバーに次の URL を入力します。**https://**<ip_address>ip_address は異常のあるコレクターの IP アドレスです。
5. [ログイン] を選択し、コレクタの設定時に設定したエージェントレスコレクタのパスワードを入力します。ステップ 5: エージェントレスコレクタの設定
6. エージェントレスコレクターダッシュボードページの [データ収集] で、[VMware vCenter] セクションの [表示と編集] を選択します。
7. の指示に従って URL VMware vCenter 認証情報の編集 と認証情報を修正します。

ヘルス問題を修正すると、コレクタは vCenter Server との接続を再確立し、コレクタのステータスは収集状態に変わります。問題が解決しない場合は、を参照してください。AWS エージェントレスコレクタの問題に関するSupport への連絡

コレクターが異常を起こす最も一般的な原因は、IP アドレスと認証情報の問題です。 IP アドレス問題の解決そしてvCenter 認証情報に関する問題の修正、これらの問題を解決し、コレクターを正常な状態に戻すのに役立ちます。

IP アドレス問題の解決

コレクタのセットアップ時に提供された vCenter エンドポイントの形式が誤っているか無効である場合、または vCenter サーバが現在ダウンしていてアクセスできない場合、コレクタは異常状態になる可能性があります。この場合、接続エラーメッセージが表示されます。

次の手順は、IP アドレスの問題を解決するのに役立ちます。

コレクター IP アドレスの問題を解決するには

1. VMware vCenter からエージェントレスコレクタの IP アドレスを取得します。
2. Web ブラウザを開いてエージェントレスコレクタコンソールを開き、アドレスバーに次の URL を入力します。<ip_address>ip_address はコレクタの送信元の IP アドレスです。**https://**
/ステップ 3: エージェントレスコレクタをデプロイする
3. [ログイン] を選択し、コレクタの設定時に設定したエージェントレスコレクタのパスワードを入力します。ステップ 5: エージェントレスコレクタの設定
4. エージェントレスコレクターダッシュボードページの [データ収集] で、[VMware vCenter] セクションの [表示と編集] を選択します。
5. VMware データ収集の詳細ページの [検出された vCenter サーバ] で、[vCenter] 列の IP アドレスを書き留めます。
6. pingまたはなどの別のコマンドラインツールを使用してtraceroute、関連する vCenter Server がアクティブで、コレクタ VM から IP にアクセスできることを確認します。
   - IP アドレスが正しくなく、vCenter サービスがアクティブな場合は、コレクタコンソールで IP アドレスを更新し、[次へ] を選択します。
   - IP アドレスは正しいが、vCenter サーバーが非アクティブの場合は、アクティブにします。
   - IP アドレスが正しく、vCenter サーバーがアクティブな場合は、ファイアウォールの問題により侵入ネットワーク接続がブロックされているかどうかを確認します。「はい」の場合は、コレクタ仮想マシンからの着信接続を許可するようにファイアウォール設定を更新してください。

vCenter 認証情報に関する問題の修正

コレクタの設定時に提供された vCenter ユーザー認証情報が無効であるか、vCenter の読み取り権限とアカウント表示権限がない場合は、コレクタが異常状態になる可能性があります。

vCenter 認証情報に関連する問題が発生した場合は、システムグループに vCenter の読み取り権限と表示権限が設定されていることを確認してください。

vCenter 認証情報の編集については、を参照してくださいVMware vCenter 認証情報の編集。

データベースと分析データ収集モジュールにおけるデータ転送の問題の解決

Agentless Collector のデータベースおよび分析データ収集モジュールのホームページには、DMS へのアクセスと S3 へのアクセスの接続ステータスが表示されます。[DMS へのアクセス権なし] と [S3 へのアクセス] と表示される場合は、データ転送を設定します。詳細については、「データ転送の設定」を参照してください。

データ転送を設定した後にこの問題が発生した場合は、データ収集モジュールがインターネットにアクセスできるかどうかを確認してください。次に、DMS CollectorPolicy ポリシーと FleetAdvisorS3Policy ポリシーを IAM ユーザーに追加したことを確認します。詳細については、「ステップ 1: エージェントレスコレクター用の IAM ユーザーを作成する」を参照してください。

データ収集モジュールがに接続できない場合は AWS、以下のドメインへのアウトバウンドアクセスを提供してください。

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

データベースと分析データ収集モジュールにおける接続問題の修正

Agentless Collector のデータベースおよび分析データ収集モジュールは LDAP サーバーに接続して、データ環境内の OS サーバーを検出します。次に、データ収集モジュールは OS サーバーに接続して、データベースサーバーと分析サーバーを検出します。データ収集モジュールは、これらのデータベースサーバーから容量とパフォーマンスの指標を収集します。データ収集モジュールがこれらのサーバーに接続できない場合は、サーバーに接続できることを確認してください。

以下の例では、*##########*。

- LDAP サーバーに接続できることを確認するには、ldap-utilパッケージをインストールします。そうするには、以下のコマンドを実行します。

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

  次に、以下のコマンドを実行します。

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

- Linux OS サーバーに接続できることを確認するには、以下のコマンドを使用します。

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

  前の例を Windows の管理者として実行します。

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

  先ほどの例を Linux で実行します。

- Windows OS サーバーに接続できることを確認するには、以下のコマンドを使用します。

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

  前の例を Windows の管理者として実行します。

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

  先ほどの例を Linux で実行します。

- SQL Server データベースに接続できることを確認するには、次のコマンドを使用します。

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

- MySQL データベースに接続できることを確認するには、次のコマンドを使用します。

```
mysql -u username -p 'password' -h [hostname or IP] -P [port]
SELECT NOW() FROM DUAL
```

- Oracle データベースに接続できることを確認するには、以下のコマンドを使用します。

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

- PostgreSQL データベースに接続できることを確認するには、次のコマンドを使用します。

```
psql -U username -h [hostname or IP] -p port -d database
```

```
SELECT CURRENT_TIMESTAMP AS sysdate
```

データベースと分析サーバーに接続できない場合は、必要な権限を必ず付与してください。詳細については、「データベースサーバーを確認」を参照してください。

スタンドアロン ESX ホストのサポート

エージェントレスコレクタはスタンドアロンの ESX ホストをサポートしていません。ESX ホストは vCenter Server インスタンスの一部であることが必要です。

AWS エージェントレスコレクタの問題に関するSupport への連絡

Application Discovery Service のエージェントレスコレクター (エージェントレスコレクター) で問題が発生し、Support が必要な場合は、AWS サポートに連絡してください。連絡があり、コレクターログの送信を求められる場合があります。

エージェントレスコレクターのログを取得するには

1. VMware vCenter からエージェントレスコレクタの IP アドレスを取得します。
2. コレクタの VM コンソールを開き、**ec2-usercollector**次の例のようにパスワードを使用してサインインします。

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

3. 以下のコマンドを使用してログフォルダに移動します。

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

4. 以下のコマンドを使用してログファイルを ZIP 圧縮します。

   ```
   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. エージェントレスコレクタ VM からログファイルをコピーします。

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

6. `tar.gz` AWS ファイルをエンタープライズSupport に渡してください。

Migration Hub のインポート

AWS Migration Hub(Migration Hub) のインポートを使用すると、Application Hub に直接オンプレミス環境の詳細情報を Migration Hub にインポートできます。AWSApplication Discovery Agent デバイスをアプリケーションとしてグループ化し、それらの移行ステータスを追跡することもできます。

インポートリクエストを開始するには

- 特別な形式のカンマ区切り値 (CSV) インポートテンプレートをダウンロードします。
- 既存のオンプレミスサーバーデータを入力します。
- Migration Hub にアップロードするAWS CLIまたはAWSSDK

複数のインポートリクエストを送信できます。各リクエストは順番に処理されます。インポートリクエストのステータスは、コンソールまたはインポート API を使用していつでも確認できます。

インポートリクエストが完了したら、インポートされた各レコードの詳細を表示することができます。使用率データ、タグ、およびアプリケーションマッピングを、Migration Hub コンソール内から直接表示します。インポート中にエラーが発生した場合は、成功したレコードと失敗したレコードの数や、失敗した各レコードのエラー詳細を確認できます。

エラー処理 エラーログと失敗したレコードのファイルを CSV ファイルとして圧縮アーカイブにダウンロードするためのリンクが用意されています。これらのファイルを使用して、エラーを修正してから、インポートリクエストを再送信します。

インポートされたレコード、インポートされたサーバー、および保持できる削除されたレコードの数には、制限が適用されます。詳細については、「AWS Application Discovery Service のクォータ」を参照してください。

サポートされているインポートファイルフィールド

Migration Hub のインポートでは、あらゆるソースからデータをインポートできます。提供されるデータは、CSV ファイルでサポートされている形式である必要があります。また、データには、サポートされている範囲を持つサポートされているフィールドのみが含まれている必要があります。

次の表のインポートフィールド名の横にあるアスタリスクは、必須フィールドであることを示しています。インポートファイルの各レコードには、サーバーまたはアプリケーションを一意に識別する

ために、必須フィールドが 1 つ以上含まれている必要があります。必須フィールドが 1 つもないレコードはインポートできません。

> **Note**
>
> いずれかの VMware を使用している場合。MoRefId またはVMware.vCenterIdでの、レコードを識別するには、同じレコードに両方のフィールドが必要です。

インポートフィールド名	説明	例
ExternalId*	各レコードに一意であることをマークすることができるカスタム識別子。例:ExternalIdは、データセンター内のサーバーのインベントリ ID を指します。	Inventory Id 1 Server 2 CMBD Id 3
SMBiosId	システム管理 BIOS (SMBIOS) ID。	
IPAddress*	サーバーの IP アドレスのカンマ区切りリスト (引用符で囲む)。	192.0.0.2 "10.12.31.233, 10.12.32.11"
MACAddress*	サーバーの MAC アドレスのカンマ区切りリスト (引用符で囲む)。	00:1B:44:11:3A:B7 "00-15-E9-2B-99-3C, 00-14-22-01-23-45"
HostName*	サーバーのホスト名。この値には完全修飾ドメイン名 (FQDN) を使用することをお勧めします。	ip-1-2-3-4 localhost.domain
VMwareMoRefId*	マネージド型オブジェクトのリファレンス ID。VMware	

インポートフィールド名	説明	例
	.Vで指定する必要がありますCenterId。	
VMware.vCenterId*	仮想マシンの一意のID。VMware と共に提供される必要があります。MoRefId。	
CPUNumberOfProcessors	CPU の数。	4
CPUNumberOfCores	物理コアの合計数。	8
CPUNumberOfLogicalCores	サーバー内のすべての CPU で同時に実行できるスレッドの合計数。一部の CPU は、単一の CPU コアにおける複数のスレッドの同時実行をサポートしています。このような場合、この数は物理 (または仮想) コアの数よりも大きくなります。	16
OS.Name	オペレーティングシステムの名前。	Linux Windows.Hat
OS.Version	オペレーティングシステムのバージョン。	16.04.3 NT 6.2.8
VMware.VMName	仮想マシンの名前。	Corp1
RAM.TotalSizeInMB	サーバーで使用可能な合計RAM (MB)。	64 128

インポートフィールド名	説明	例
RAM.UsedSizeInmb.avg	サーバーで使用されている RAM の平均容量 (MB)。	64 128
RAM.UsedSizeInmb.max	サーバーで使用できる RAM の最大容量 (MB)。	64 128
CPUUsagePctAvg	検出ツールでデータを収集していたときの平均 CPU 使用率。	45 23.9
CPUUsagePct.Max	検出ツールでデータを収集していたときの最大 CPU 使用率。	55.34 24
DiskReadsPerSecondInkb.avg	1 秒あたりのディスク読み取りの平均数 (KB)。	1159 84506
DiskWritesPerSecondInkb.avg	1 秒あたりのディスク書き込みの平均数 (KB)。	199 6197
DiskReadsPerSecond Inkb.max	1 秒あたりのディスク読み取りの最大数 (KB)。	37892 869962
DiskWritesPerSecon dInkb.max	1 秒あたりのディスク書き込みの最大数 (KB)。	18436 1808
DiskReadsOpsPerSecondAvg	1 秒あたりのディスク読み取り操作の平均回数。	45 28
DiskWritesOpsPerSecondAvg	1 秒あたりのディスク書き込み 操作の平均回数。	8 3

インポートフィールド名	説明	例
DiskReadsOpsPerSecond.Max	1 秒あたりのディスク読み取りオペレーションの最大数。	1083 176
DiskWritesOpsPerSecond.Max	1 秒あたりのディスク書き込みオペレーションの最大数。	535 71
NetworkReadsPerSecondInkb.avg	1 秒あたりのネットワーク読み取りオペレーションの平均数 (KB)。	45 28
NetworkWritesPerSecondInkb.avg	1 秒あたりのネットワーク書き込みオペレーションの平均数 (KB)。	8 3
NetworkReadsPerSecondInkb.max	1 秒あたりのネットワーク読み取りオペレーションの最大数 (KB)。	1083 176
NetworkWritesPerSecondInkb.max	1 秒あたりのネットワーク書き込みオペレーションの最大数 (KB)。	535 71
アプリケーション	このサーバーを含むアプリケーションのカンマ区切りリスト (引用符で囲む)。この値には、既存のアプリケーションや、インポート時に作成された新規アプリケーションを含めることができます。	Application1 "Application2, Application3"

インポートフィールド名	説明	例
タグ	name:value 形式のタグのカンマ区切りリスト。 **Important** タグに機密情報 (個人データなど) を保存しないでください。	"zone:1, critical:yes" "zone:3, critical:no, zone:1"

インポートテンプレートで定義されているすべてのフィールドにデータが入力されていなくても、各レコードに 1 つ以上の必須フィールドが含まれていれば、データをインポートすることができます。重複は、外部または内部の一致キーを使用して、複数のインポートリクエスト間で管理されます。独自の一致キー `External ID` を入力する場合は、このフィールドでレコードを一意に識別してインポートします。一致キーが指定されていない場合、インポートテンプレートの一部の列から派生した内部生成の一致キーがインポートに使用されます。この一致の詳細については、「検出されたサーバーとアプリケーションのマッチングロジック」を参照してください。

Note

Migration Hub のインポートは、インポートテンプレートで定義されているもの以外のフィールドをサポートしません。カスタムフィールドは無視され、インポートもされません。

インポートのアクセス許可の設定

データをインポートする前に、IAM ユーザーにアップロードに必要な Amazon S3 許可が IAM ユーザーにあることを確認します。`s3:PutObject`) のインポートファイルを Amazon S3 にインポートして、オブジェクト (`s3:GetObject`). また、プログラムによるアクセスを確立する必要があります (AWS CLI) または、IAM ポリシーを作成し、でインポートを行う IAM ユーザーにそのポリシーをアタッチすることで、AWSアカウント.

Console Permissions

でインポートリクエストを行う IAM ユーザーの許可ポリシーを編集するには、以下の手順を実行しますAWSコンソールを使用してアカウントを作成します。

ユーザーにアタッチされている管理ポリシーを編集する

1. AWS Management Consoleにサインインして、IAM コンソールを開きます https://console.aws.amazon.com/iam/。
2. ナビゲーションペインで [Users] (ユーザー) を選択します。
3. アクセス許可ポリシーを変更する対象のユーザーの名前を選択します。
4. [アクセス許可] タブを選択後、[アクセス許可の追加] を選択します。
5. [Attach existing policies directly (既存のポリシーを直接アタッチ)]、[ポリシーの作成] の順に選択します。

   a. 表示された [ポリシーの作成] ページで [JSON] を選択し、次のポリシーに貼り付けます。バケットの名前を、IAM ユーザーがインポートファイルをアップロードする実際のバケットの名前に置き換えることを忘れないでください。

```
{
  "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. [Review policy] (ポリシーの確認) を選択します。

c. ポリシーに新しい [名前] と説明 (オプション) を入力してから、ポリシーの概要を確認します。

d. [Create policy] (ポリシーを作成) を選択します。

6. に戻りますアクセス許可の付与でインポートリクエストを行うユーザーの IAM コンソールページAWSアカウント.

7. ポリシーのテーブルを更新し、先ほど作成したポリシーの名前を検索します。

8. [Next: (次へ:)] を選択します 確認.

9. [Add permissions] (許可の追加) を選択します。

IAM ユーザーにポリシーを追加したところで、インポートプロセスを開始する準備が整いました。

AWS CLI Permissions

以下の手順を使用して、IAM ユーザーに、を使用してデータのインポートリクエストを行うアクセス権限を付与するために必要な管理ポリシーを作成します。AWS CLI。

管理ポリシーを作成してアタッチするには

1. `aws iam create-policy` AWS CLI コマンドを使用して、以下の許可を持つ IAM ポリシーを作成します。バケットの名前を、IAM ユーザーがインポートファイルをアップロードする実際のバケットの名前に置き換えることを忘れないでください。

```
{
  "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/*"]
    }
  ]
}
```

このコマンドの使用に関する詳細については、AWS CLI コマンドリファレンスの「create-policy」を参照してください。

2. を使用するaws iam create-policy AWS CLIのコマンドを実行して、次のアクセス許可が付与された追加の IAM ポリシーを作成します。

```
{
    "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. を使用するaws iam attach-user-policy AWS CLIのコマンドを実行して、前の 2 つのステップで作成したポリシーを IAM ユーザーにアタッチしますAWSアカウントを使用してAWS CLI。このコマンドの使用の詳細については、「」を参照してください。attach-user-policyのAWS CLIコマンドリファレンス。

IAM ユーザーにポリシーを追加したところで、インポートプロセスを開始できるようになりました。

IAM ユーザーが指定された Amazon S3 バケットにオブジェクトをアップロードするときは、ユーザーがそのオブジェクトを読み取ることができるように、オブジェクトセットに対するデフォルトのアクセス許可の設定は保持する必要があります。

Amazon S3 へのインポートファイルのアップロード

次に、CSV 形式のインポートファイルをインポートできるように、それを Amazon S3 にアップロードする必要があります。開始する前に、インポートファイルを格納する Amazon S3 バケットを事前に作成および/または選択しておく必要があります。

Console S3 Upload

Amazon S3 にインポートファイルをアップロードする

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. [Bucket name (バケット名)] リストで、オブジェクトのアップロード先のバケットの名前を選択します。
3. [Upload] (アップロード) を選択します。
4. [Upload (アップロード)] ダイアログボックスで、[Add files (ファイルの追加)] を選択してアップロードするファイルを選択します。
5. アップロードするファイルを選択し、続いて [Open (オープン)] を選択します。
6. [Upload] (アップロード) を選択します。
7. ファイルがアップロードされたら、バケットのダッシュボードからデータファイルオブジェクトの名前を選択します。
8. オブジェクトの詳細ページの [概要] タブから、[オブジェクト URL] をコピーします。この情報は、インポートリクエストを作成するときに必要になります。
9. に移動しますインポートで説明されているように、Migration Hub コンソールのページデータのインポート。次に、オブジェクトの URL をAmazon S3 オブジェクトフィールド。

AWS CLI S3 Upload

Amazon S3 にインポートファイルをアップロードする

1. ターミナルウィンドウを開き、インポートファイルが保存されているディレクトリに移動します。

2. 次のコマンドを入力します。

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

3. これにより、次の結果が返ります。

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

4. 返された完全な Amazon S3 オブジェクトパスをコピーします。この情報は、インポートリクエストを作成するときに必要です。

データのインポート

Migration Hub コンソールからインポートテンプレートをダウンロードし、それに既存のオンプレミスサーバーのデータを入力したら、Migration Hub へのデータのインポートを開始する準備が整います。次の手順では、2 つの方法について説明します。AWS CLI。

Console Import

Migration Hub コンソールの [Tools] (ツール) ページでデータのインポートを開始します。

データのインポートを開始する

1. ナビゲーションペインの [Discover (検出)] で [Tools (ツール)] を選択します。
2. インポートテンプレートへの入力が完了していない場合は、[Import] (インポート) ボックスで [import template] (インポートテンプレート) を選択することによってテンプレートをダウンロードできます。ダウンロードしたテンプレートを開き、既存のオンプレミスサーバーデータを入力します。インポートテンプレートは、https://s3.us-west-2.amazonaws.com/templates-7cffcf56-bd96-4b1c-b45b-a5b42f282e46/import_template.csv にある Amazon S3 バケットからもダウンロードできます。
3. [(マテリアルエディタ)] を開くにはインポート[] ページでインポートのインポートボックスに移動するとそのように表示されます。
4. []インポート名で、インポートの名前を指定します。
5. に入力しますAmazon S3 オブジェクトフィールド。このステップを実行するには、インポートデータファイルを Amazon S3 にアップロードする必要があります。詳細については、「Amazon S3 へのインポートファイルのアップロード」を参照してください。
6. 右下エリアにある [インポート] を選択します。[インポート] ページが開きます。テーブルには、インポートとそのステータスが表示されます。

前の手順に従って、データのインポートを開始したら、各インポートリクエストの詳細 (例: 進行状況のステータス、完了時間、レコードの成功/失敗数 (ダウンロード可能)) が [インポート] ページに表示されます。この画面から、[Discover] (検出) の [Servers] (サーバー) ページに移動して、インポートされた実際のデータを確認することもできます。

[サーバー] ページでは、検出されたすべてのサーバー (デバイス) とインポート名を確認できます。から移動するとインポート(インポート履歴) ページに表示されているインポートの名前を選択して[Name] (名前)の列に自動的に移動しますサーバー選択したインポートのデータセットに基づいてフィルタが適用されるページ。すると、その特定のインポートに属するデータのみが表示されます。

アーカイブは、.zip 形式で提供され、`errors-file` と `failed-entries-file` の 2 つのファイルが含まれます。エラーファイルには、失敗した各行に関連付けられたエラーメッセージのリストと、インポートに失敗したデータファイルの関連付けられた列の名前が含まれます。このファイルを使用して、問題の発生原因をすばやく特定することができます。失敗したエントリファイルには、失敗した各行と提供されたすべての列が含まれます。このファイルのエラーファイルで変更を呼び出し、修正した情報を使用してファイルのインポートを再試行することができます。

AWS CLI Import

AWS CLI からデータのインポートプロセスを開始するには、最初に AWS CLI を環境にインストールする必要があります。詳細については、AWS Command Line Interface ユーザーガイドのAWS コマンドラインインターフェイスのインストールを参照してください。

> **Note**
>
> インポートテンプレートへの入力が完了していない場合は、https://s3.us-west-2.amazonaws.com/templates-7cffcf56-bd96-4b1c-b45b-a5b42f282e46/import_template.csv にある Amazon S3 バケットからインポートテンプレートをダウンロードできます。

データのインポートを開始する

1. ターミナルウィンドウを開いて、次のコマンドを入力します。

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

2. これにより、インポートタスクが作成され、次のステータス情報が返ります。

```
{
    "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"
    }
}
```

Migration Hub のインポートリクエストの追跡

Migration Hub のインポートリクエストのステータスは、コンソールを使用して追跡できます。AWS CLI、またはAWSSDK

Console Tracking

Migration Hub コンソールの [Imports] (インポート) ダッシュボードからは、以下の要素を確認できます。

- 名前 – インポートリクエストの名前。
- インポート ID – インポートリクエストの固有 ID。
- インポート時間 – インポートリクエストが作成された日時。
- インポートステータス – インポートリクエストのステータス。これは、以下の値のいずれかになります。
  - インポート中 – このデータファイルは現在インポート中です。
  - インポート済み – データファイル全体が正常にインポートされました。
  - インポート時にエラーが発生 – データファイル内の 1 つ、または複数のレコードのインポートが失敗しました。失敗したレコードを解決するには、インポートタスクの [Download failed records (失敗したレコードのダウンロード)] を選択し、失敗したエントリの csv ファイルのエラーを解消してから、再度インポートを行います。

- インポート失敗 – データファイル内のどのレコードもインポートされませんでした。失敗したレコードを解決するには、インポートタスクの [Download failed records (失敗したレコードのダウンロード)] を選択し、失敗したエントリの csv ファイルのエラーを解消してから、再度インポートを行います。
- インポートされたレコード – 特定のデータファイル内の正常にインポートされたレコードの数です。
- 失敗したレコード – 特定のデータファイル内のインポートされなかったレコードの数です。

CLI Tracking

インポートタスクのステータスは、AWS CLI の `aws discovery describe-import-tasks` コマンドを使用して追跡できます。

1. ターミナルウィンドウを開いて、次のコマンドを入力します。

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

2. これにより、すべてのインポートタスクのリストが JSON 形式で返り、ステータスやその他の関連情報が含まれます。必要に応じて、インポートタスクのサブセットが返るように結果をフィルタリングすることができます。

インポートタスクを追跡すると、返った `serverImportFailure` 値がゼロより大きいことがわかります。この場合、インポートファイルには、インポートできなかったエントリが 1 つ以上含まれています。この問題を解消するには、失敗したレコードのアーカイブをダウンロードして、中のファイルを確認し、変更した failed-entries.csv ファイルを使用してインポートリクエストを行います。

インポートタスクを作成したら、データ移行の管理と追跡に役立つ他の操作を実行できます。たとえば、特定のリクエストに対して失敗したレコードのアーカイブをダウンロードできます。失敗したレコードのアーカイブを使用して、インポートの問題を解消する方法については、「失敗したインポートレコードのトラブルシューティング」を参照してください。

検出されたデータの表示、エクスポート、検索

Application Discovery Service エージェントレスコレクタ (エージェントレスコレクタ) と AWSDiscovery Agent (Discovery Agent) は、使用率の平均とピークに基づいたシステムパフォーマンスデータを提供します。収集されたシステムパフォーマンスデータを使用して、おおおおまかな TCO (総保有コスト) を実行できます。Discovery Agent は、システムパフォーマンス情報、インバウンドとアウトバウンドのネットワーク接続、およびサーバーで実行されているプロセスなど、より詳細な時系列データを収集します。このデータを使用して、サーバー間のネットワーク依存関係を確認し、関連するサーバーをアプリケーションとしてグループ化して移行計画に役立てることができます。

このセクションでは、コンソールとの両方から Agent Less Collector と Discovery Agent が検出したデータを表示し、使用する手順を説明します。AWS CLI。

トピック

- Migration Hub コンソールを使用して収集されたデータを表示する
- 収集されたデータをエクスポートする
- Amazon Athena でのデータ探索

Migration Hub コンソールを使用して収集されたデータを表示する

Application Discovery Service Agent Agent Agent (エージェントレスコレクター) とAWS Discovery Agent (Discovery Agent) の両方で、データ収集プロセスの開始後に、コンソールを使用して収集されたサーバーと VM に関するデータを表示できます。コンソールには、データ収集開始後約 15 分後にデータが表示されます。を使用して API を呼び出して収集したデータをエクスポートすることで、このデータを CSV 形式で表示することもできますAWS CLI。収集データのエクスポートについては、次のセクション「収集されたデータをエクスポートする」で説明します。

検出したサーバーに関する収集データを表示するには

1. コンソールのナビゲーションペインで、[Servers (サーバー)] を選択します。検出したサーバーがサーバリストに表示されます。
2. 収集データの詳細を表示するには、[Server info (サーバー情報)] 列のサーバー名のリンクを選択します。表示される画面で、システム情報やパフォーマンスメトリクスなどの詳細情報を確認できます。

コンソールを使用してエージェントレスコレクタまたは Discovery Agent が検出したサーバーの表示、ソート、およびタグ付けを行うためのコンソールの使用に関する詳細については、「」を参照してくださいAWS Application Discovery Serviceコンソールのチュートリアル。

Agentless Collector データベースと分析データ収集モジュールは、収集したデータを Amazon S3 バケットにアップロードします。このバケットのデータはAWS DMS コンソールで表示できます。

検出されたデータベースと分析サーバーに関する収集データを表示するには

1. AWS Management Consoleにログインし、https://console.aws.amazon.com/dms/v2/ でAWS DMS コンソールを開きます。
2. ディスカバーから「インベントリ」を選択します。インベントリページが開き、検出されたデータベースと分析サーバーのリストが表示されます。

検出されたサーバーとアプリケーションのマッチングロジック

AWS Application Discovery Service(Application Discovery Service) には、検出したサーバが既存のエントリと一致するタイミングを識別するマッチングロジックが組み込まれています。このロジックで一致が見つかると、検出済みの既存のサーバーの情報は、新しい値で更新されます。

この一致ロジックは、AWS Migration Hub (Migration Hub) のインポート、Application Discovery Service Agent (エージェントレスコレクター)、AWS Application Discovery Agent (Discovery Agent)、およびその他の移行ツールを含めた複数ソースからの重複したサーバーを処理します。Migration Hub のインポートに関する詳細については、「Migration Hub のインポート」を参照してください。

サーバーが検出されると、インポートされたサーバーが存在していないことを確認するために、各エントリは、以前にインポートされたレコードと照合されます。一致が見つからない場合は、新しいレコードが作成され、一意の新しいサーバー ID が割り当てられます。一致が見つからない場合でも新しいエントリは作成されますが、既存のサーバーと同じ一意のサーバー ID が割り当てられます。Migration Hub コンソールでこのサーバーを表示している場合は、サーバーに対して 1 つの固有エントリのみが表示されます。

このエントリに関連付けられたサーバー属性は、使用可能な以前のレコードや、新しくインポートされたレコードの属性値が表示されるようにマージされます。複数のソースの特定のサーバー属性の値が複数ある場合 (インポートおよび Discovery Agent によって検出された特定のサーバーに関連付けられた `Total RAM` の 2 つの異なる値など)、サーバーの一致レコードには、最後に更新された値が表示されます。

一致フィールド

次のフィールドは、検出ツールの使用時にサーバーを一致させるために使用されます。

- ExternalId— サーバーの一致に使用される主要フィールドです。このフィールドの値が別のエントリ内にある別の `ExternalId` の値と同一である場合、Application Discovery Serviceは、他のフィールドが一致するかどうかにかかわらず、これら 2 つのエントリを一致させます。
- IPAddress
- HostName
- MacAddress
- VMware VMware。 MoRefIdとヴイエムウェア。 vCenterId— Application Discovery Service が一致を実行するには、これらの両方の値が別のエントリ内の対応するフィールドの値と同一である必要があります。

収集されたデータをエクスポートする

Application Discovery Service Agent less Connector (エージェントレスコレクター (Discovery Agent (Discovery Agent の両方で、データ収集プロセスの開始後に、収集されたサーバーと VM に関するデータをエクスポートできます。AWSこのデータは、データ収集に使用した検出ツールに応じて、コンソールを操作する、または AWS CLI 経由で API コールを実行することによってエクスポートできます。

各方法の手順を示します。次のいずれかを選択して展開してください。

を使用して、収集したデータをすべてのサーバーにエクスポートしますAWS CLI

ホストと VM で実行されているすべてのエージェントレスコレクタと Discovery Agent から収集されたデータは、AWS Command Line Interface (AWS CLI) を使用して一括でエクスポートできます。データをエクスポートする前に、AWS CLIを環境にインストールする必要があります。

AWS CLI をインストールして収集データをエクスポートするには

1. OS のタイプ (Windows または Mac/Linux) に適切な AWS CLI をインストールします (まだインストールしていない場合)。インストール手順については、AWS Command Line Interfaceユーザーガイドを参照してください。
2. コマンドプロンプト (Windows) またはターミナル (MAC/Linux) を開きます。

   a. `aws configure` を入力して、[Enter] を押します。

b. AWSアクセスキー IDAWS とシークレットアクセスキーを入力します。

c. デフォルトのリージョン名として「us-west-2」と入力します。

d. デフォルトの出力形式として「text」と入力します。

3. 次のコマンドを入力してエクスポート ID を生成します。

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

4. 次のコマンドで、前のステップで生成したエクスポート ID を使用し、パラメータ "configurationsDownloadUrl" の値として S3 URL を生成します。

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

5. 前のステップで生成した URL をコピーしてブラウザに貼り付け、検出したサーバーの収集データの zip ファイルをダウンロードします。

コンソールを使用してエージェントが収集したデータをエクスポートする

特定のサーバーに関する詳細ページでは、エージェントが収集したデータのコンソールからのエクスポートが 1 つのエージェントに制限されます。詳細ページでは、画面最下部にある [Exports] (エクスポート) の下にサーバーのエクスポートジョブがリストされています。エクスポートジョブがない場合、テーブルは空になります。サーバーデータのエクスポートは、1 度に最大 5 つまで実行できます。

検出したサーバーに関する収集データをエクスポートするには

1. ナビゲーションペインで [Servers] (サーバー) を選択します。
2. [Server info (サーバー情報)] 列で、データをエクスポートするサーバーのリンクを選択します。
3. 画面下部の [Exports (エクスポート)] セクションで、[Export server details (サーバー詳細のエクスポート)] を選択します。
4. [Export server details (サーバー詳細のエクスポート)] で、[Start date (開始日)] と [Time (時刻)] を入力します。

> **Note**
>
> 開始時刻は、現在の時刻から 72 時間より前にすることはできません。

5. ジョブを開始するには、[Export (エクスポート)] を選択します。最初のステータスは [In-progress (進行中)] です。ステータスを更新するには、[Exports (エクスポート)] セクションの更新アイコンをクリックします。
6. エクスポートジョブが完了したら、[Download (ダウンロード)] を選択して .zip ファイルを保存します。
7. 保存されたファイルを解凍します。エクスポートデータは、一連の .csv ファイルに含まれています。

   .csv ファイルを Microsoft Excel で開き、エクスポートしたサーバーデータを確認できます。

   複数のファイルの 1 つは JSON ファイルであり、これにはエクスポートタスクとその結果に関するデータが含まれています。

> **Note**
>
> AWS Migration Hubコンソールで Amazon Elastic Compute Cloud (Amazon EC2) インスタンスの推奨事項を生成およびエクスポートする方法については、AWS Migration Hubユーザーガイドの「Amazon EC2 インスタンスの推奨事項」を参照してください。

Amazon Athena でのデータ探索

Amazon Athena でのデータ探索では、Discovery Agent が検出したすべてのオンプレミスサーバーから収集されたデータを 1 か所で分析することができます。Amazon Athena でのデータ探索が Migration Hub コンソールから有効になったら (または StartContinousExport API) でエージェントのデータ収集を有効にすると、エージェントによって収集されたデータが一定の間隔で自動的に S3 バケットに保存されるようになります。

その後、Amazon Athena にアクセスして、各サーバーに関する時系列のシステムパフォーマンス、各サーバーで実行されているプロセスのタイプ、および異なるサーバー間でのネットワーク依存関係を分析するために、事前定義されたクエリを実行することができます。これに加えて、Amazon Athena を使用して独自のカスタムクエリを記述する、設定管理データベース (CMDB) エクスポートなどの追加の既存データソースをアップロードする、および検出されたサーバーを実際のビジネスアプリケーションと関連付けることができます。Athena データベースと Amazon を統合することも可能です。 QuickSight クエリ出力を視覚化し、追加の分析を実行する

ステップ

1. Amazon Athena でのデータ探索の有効化
2. Amazon Athena でのデータ探索の使用

Amazon Athena でのデータ探索の有効化

Amazon Athena でのデータ探索は、Migration Hub コンソール、またはからの API コールを使用して Continuous Export を有効にすることによって有効化します。AWS CLI。データ探索は、Amazon Athena で検出されたデータを表示して探索する前に有効にしておく必要があります。

Continuous Export を有効にすると、アカウントでサービスリンクロール `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport` が自動的に使用されます。このサービスにリンクされたロールの詳細については、「Application Discovery Service 用のサービスリンクロール許可」を参照してください。

以下の手順では、コンソールとを使用して Amazon Athena でのデータ探索を有効にする方法を説明します。AWS CLI。

Enable with the console

Amazon Athena でのデータ探索は、「データ収集の開始」の選択時に Continuous Export を黙示的に有効にする、またはから「Amazon Athena でのデータ探索」というラベルが付けられたトグルをクリックすることによって有効になります。データコレクターMigration Hub コンソールの

コンソールから Amazon Athena でのデータ探索を有効にする

1. ナビゲーションペインで、[Data Collectors] (データコレクタ) を選択します。
2. [Agents] (エージェント) タブを選択します。
3. [Start data collection] (データ収集の開始) を選択、またはデータ収集がすでに有効になっている場合は [Data exploration in Amazon Athena] (Amazon Athena でのデータ探索) トグルをクリックします。
4. 前のステップで作成したダイアログボックスで、関連するコストに同意するチェックボックスをオンにして、[Continue (続行)] または [Enable (有効)] を選択します。

> **Note**
>
> これでエージェントが「継続的なエクスポート」モードで実行されるようになります。このモードは、Amazon Athena で検出されたデータを表示し、使用することを可能にします。これを初めて有効にする場合は、Amazon Athena にデータが表示されるまで最大 30 分かかる場合があります。

Enable with the AWS CLI

Amazon Athena でのデータ探索は、からの API コールを通じて Continuous Export を明示的に有効にすることによって、有効化します。AWS CLI。これを行うには、まず AWS CLI が環境にインストールされている必要があります。

をインストールするにはAWS CLIAmazon Athena でのデータ探索を有効にする

1. オペレーティングシステム (Linux、macOS、または Windows) 用の AWS CLI をインストールします。手順については、AWS Command Line Interface ユーザーガイドを参照してください。
2. コマンドプロンプト (Windows) またはターミナル (Linux/macOS) を開きます。
   a. `aws configure` を入力して、[Enter] を押します。
   b. あなたの情報を入力してくださいAWSアクセスキー ID とAWSシークレットアクセスキー。
   c. デフォルトのリージョン名として「`us-west-2`」と入力します。
   d. デフォルトの出力形式として「`text`」と入力します。
3. 次のコマンドを入力します。

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

> **Note**
>
> これでエージェントが「継続的なエクスポート」モードで実行されるようになります。このモードは、Amazon Athena で検出されたデータを表示し、使用することを可能にします。これを初めて有効にする場合は、Amazon Athena にデータが表示されるまで最大 30 分かかる場合があります。

Amazon Athena でのデータ探索の使用

Amazon Athena でのデータ探索を有効にしたら、エージェントが検出した詳細な最新データを Athena で直接クエリすることによって、そのデータの探索と使用を開始できます。このデータを使用して、スプレッドシートの作成、コスト分析の実行、視覚化プログラムへのクエリの移植などを行うことができます。

このセクションのトピックでは、ローカル環境への移行を評価および計画するために、計画するために、計画するために、計画するために、Athena でデータを使用する方法を説明します。AWS。

トピック

Amazon Athena でのデータの直接探索

次の手順では、エージェントデータを直接探索Athena。Athena にデータがない、または Amazon Athena でのデータ探索をまだ有効にしていない場合は、「」で説明されているように Amazon Athena でのデータ探索を有効化することを求めるダイアログボックスが表示されます。Amazon Athena でのデータ探索の有効化。

Athena でエージェントが検出したデータを直接検索する

1. AWS Migration Hub コンソールを開き、ナビゲーションペインで [Servers (サーバー)] を選択します。
2. Amazon Athena コンソールを開くには、[Explore data in Amazon Athena] (Amazon Athena でのデータ探索) を選択します。
3. [Query Editor (クエリエディタ)] ページのナビゲーションペインの [Database (データベース)] で、application_discovery_service_database が選択されていることを確認します。

> **Note**
>
> [Tables (テーブル)] で、以下のテーブルは、エージェントによってグループ化されたデータセットを表しています。
>
> - os_info_agent

- network_interface_agent
- sys_performance_agent
- processes_agent
- inbound_connection_agent
- outbound_connection_agent
- id_mapping_agent

4. Athena クエリエディタで SQL クエリを記述して実行することによって、Amazon Athena コンソールでデータをクエリします。たとえば、以下のクエリを使用して、検出されたすべてのサーバー IP アドレスを確認できます。

```
SELECT * FROM network_interface_agent;
```

クエリの例については、「Athena で使用する事前定義されたクエリ」を参照してください。

Amazon Athena データの視覚化

データを視覚化するには、Amazon などの視覚化プログラムにクエリを移植できます。 QuickSight または、Cytoscape、yEd、Gelphi などのオープンソースの視覚化ツール ネットワーク図、要約グラフなどのグラフィカルな表現をレンダリングするには、これらのツールを使用します。この方法を使用するときは、視覚化プログラム経由で Athena に接続して、Athena がビジュアライゼーションを生成するためのソースとして収集されたデータにアクセスできるようにします。

Amazon Athena データを視覚化する QuickSight

1. にサインインします。アマゾン QuickSight。
2. [Connect to another data source or upload a file (別のデータソースに接続するか、ファイルをアップロードします)] を選択します。
3. [Athena] を選択します。[New Athena data source] (新しい Athena データソース) ダイアログボックスが表示されます。
4. [Data source name (データソース名)] フィールドに名前を入力します。
5. [Create data source (データソースを作成)] を選択します。
6. Select the あるgents-servers-osのテーブルテーブルの選択ダイアログボックスを開き、選択。

7. [Finish data set creation (データセット作成の終了)] ダイアログボックスで、[Import to SPICE for quicker analytics (SPICE にインポートしてクイック分析)] を選択して、[Visualize (視覚化)] を選択します。

   ビジュアライゼーションがレンダリングされます。

Athena で使用する事前定義されたクエリ

このセクションでは、TCO 分析やネットワークの可視化などの一般的なユースケースを実行する、一連の事前定義されたクエリを示します。これらのクエリをそのまま、あるいは必要に応じて変更して使用できます。

事前定義されたクエリを使用するには

1. AWS Migration Hub コンソールを開き、ナビゲーションペインで [Servers (サーバー)] を選択します。
2. Amazon Athena コンソールを開くには、[Explore data in Amazon Athena] (Amazon Athena でのデータ探索) を選択します。
3. [Query Editor (クエリエディタ)] ページのナビゲーションペインの [Database (データベース)] で、application_discovery_service_database が選択されていることを確認します。
4. クエリエディタでプラス記号 (+) を選択して、新しいクエリのタブを作成します。
5. 「事前に定義されたクエリ」からいずれかのクエリをコピーします。
6. 作成した新しいクエリタブのクエリウィンドウにそのクエリを貼り付けます。
7. [Run Query] (クエリの実行) をクリックします。

事前に定義されたクエリ

タイトルを選択すると、クエリに関する情報が表示されます。

サーバの IP アドレスとホスト名の取得

このビューヘルパー関数では、特定のサーバーの IP アドレスとホスト名を取得します。このビューは他のクエリで使用できます。ビューを作成する方法については、Amazon Athena ユーザーガイドの「CREATE VIEW」を参照してください。

```
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");
```

エージェントの有無にかかわらずサーバーを識別

このクエリは、データ検証を実行するのに役立ちます。ネットワーク内の多数のサーバーにエージェントをデプロイした場合は、このクエリを使用して、エージェントが配置されていない他のサーバーがネットワーク内にあるかどうかを確認できます。このクエリでは、インバウンドとアウトバウンドのネットワークトラフィックを調べ、プライベート IP アドレスについてのみトラフィックをフィルタリングします。つまり、192、10、172 で始まる IP アドレスです。

```
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.%'));
```

エージェントを使用してサーバのシステムパフォーマンスデータを分析

このクエリを使用して、エージェントがインストールされているオンプレミスサーバーのシステムパフォーマンスと使用パターンデータを分析できます。このクエリでは、system_performance_agent テーブルと os_info_agent テーブルを組み合わせて、各サーバーのホスト名を識別します。このクエリでは、エージェントが稼働しているすべてのサーバーの時系列の使用状況データ (15 分間隔) が返ります。

```
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;
```

ポート番号とプロセスの詳細に基づいてサーバー間のアウトバウンド通信を追跡します

このクエリでは、ポート番号とプロセスの詳細と共に、各サービスのアウトバウンドトラフィックの詳細が返されます。

クエリを実行する前に、まだ行っていない場合は、IANA からダウンロードした IANA ポートレジストリデータベースを含む iana_service_ports_import テーブルを作成する必要があります。こ

のテーブルを作成する方法については、「IANA ポートレジストリのインポートテーブルの作成」を参照してください。

iana_service_ports_import テーブルが作成されたら、アウトバウンドトラフィックを追跡する 2 つのビューヘルパー関数を作成します。ビューを作成する方法については、Amazon Athena ユーザーガイドの「CREATE VIEW」を参照してください。

アウトバウンド追跡ヘルパー関数を作成するには

1. https://console.aws.amazon.com/athena/ で Athena コンソールを開きます。
2. 個別のアウトバウンド送信先 IP アドレスのすべてをリストする以下のヘルパー関数を使用して、valid_outbound_ips_helper ビューを作成します。

```
CREATE OR REPLACE VIEW valid_outbound_ips_helper AS
SELECT DISTINCT "destination_ip"
FROM outbound_connection_agent;
```

3. アウトバウンドトラフィックの通信頻度を決定する以下のヘルパー関数を使用して、ビュー outbound_query_helper を作成します。

```
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. iana_service_ports_import テーブルと 2 つのヘルパー関数を作成したら、以下のクエリを実行して、各サービスのアウトバウンドトラフィックの詳細をポート番号とプロセスの詳細と共に取得できます。

```
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
```

ポート番号とプロセスの詳細に基づいてサーバー間の受信通信を追跡します

このクエリでは、ポート番号とプロセスの詳細と共に、各サービスのインバウンドトラフィックに関する情報が返されます。

このクエリを実行する前に、まだ行っていない場合は、IANA からダウンロードした IANA ポートレジストリデータベースを含む `iana_service_ports_import` テーブルを作成する必要があります。このテーブルを作成する方法については、「IANA ポートレジストリのインポートテーブルの作成」を参照してください。

`iana_service_ports_import` テーブルが作成されたら、インバウンドトラフィックを追跡する 2 つのビューヘルパー関数を作成します。ビューを作成する方法については、Amazon Athena ユーザーガイドの「CREATE VIEW」を参照してください。

インポートの追跡ヘルパー関数を作成するには

1. https://console.aws.amazon.com/athena/ で Athena コンソールを開きます。
2. すべての個別のインバウンド元 IP アドレスのリストを取得する以下のヘルパー関数を使用して、ビュー `valid_inbound_ips_helper` を作成します。

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

3. インバウンドトラフィックの通信頻度を決定する以下のヘルパー関数を使用して、ビュー inbound_query_helper を作成します。

```
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. iana_service_ports_import テーブルと 2 つのヘルパー関数を作成したら、以下のクエリを実行して、各サービスのインバウンドトラフィックの詳細をポート番号とプロセスの詳細と共に取得できます。

```
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
```

実行中のソフトウェアをポート番号から識別

このクエリでは、ポート番号に基づいて実行中のソフトウェアが識別されます。

このクエリを実行する前に、まだ行っていない場合は、IANA からダウンロードした IANA ポートレジストリデータベースを含む iana_service_ports_import テーブルを作成する必要があります。このテーブルを作成する方法については、「IANA ポートレジストリのインポートテーブルの作成」を参照してください。

以下のクエリを実行して、ポート番号に基づき、実行中のソフトウェアを識別します。

```
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;
```

IANA ポートレジストリのインポートテーブルの作成

事前定義されたクエリによっては、Internet Assigned Numbers Authority (IANA) からダウンロードした情報を含む `iana_service_ports_import` という名前のテーブルが必要になる場合があります。

iana_service_ports_import テーブルを作成するには

1. iana.org の Service Name and Transport Protocol Port Number Registry から IANA ポートレジストリデータベース CSV ファイルをダウンロードします。
2. このファイルを Amazon S3 にアップロードします。詳細については、「S3 バケットにファイルとフォルダをアップロードする方法」を参照してください。
3. Athena で `iana_service_ports_import` という名前の新しいテーブルを作成します。手順については、Amazon Athena ユーザーガイドの「テーブルを作成する」を参照してください。以下の例では、`my_bucket_name` を、前の手順で CSV ファイルをアップロードした S3 バケットの名前に置き換える必要があります。

```
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 Serviceコンソールのチュートリアル

AWS Application Discovery Service(Application Discovery Service) はAWS Migration Hub(Migration Hub) とお客様はそのデータコレクタ、サーバー、およびアプリケーションを Migration Hub で表示して、管理することができます。Application Discovery Service コンソールを使用するときは、Migration Hub コンソールにリダイレクトされます。Migration Hub コンソールでの作業に、お客様による追加のステップやセットアップは不要です。

このセクションでは、Application Discovery Service Agentless Collector (エージェントレスコレクタ) を管理し、モニタリングする方法を説明します。AWSコンソールを使用するアプリケーション検出エージェント (検出エージェント)。

トピック

メインダッシュボード

メインダッシュボードを表示するには、ダッシュボードからのAWS Migration Hub(Migration Hub) コンソールのナビゲーションペイン。Migration Hub メインダッシュボードでは、サーバー、アプリケーション、および Application Discovery Service エージェントレスコレクタ (エージェントレスコレクタ) などのデータコレクタに関するおまかな統計を表示できます。AWSアプリケーション検出エージェント (検出エージェント)。

メインダッシュボード

メインダッシュボードでは、中央にある [Discover (検出)] ダッシュボードと [Migrate (移行)] ダッシュボードからのデータを収集します。メインダッシュボードには、ステータスと情報のペインが 4 つあり、クイックアクセス用のリンクのリストもあります。各ペインでは、直近に更新されたアプリケーションのステータスの概要を確認できます。また、すべてのアプリケーションにすばやくアクセスしたり、異なる状態のアプリケーションの概要を取得したり、時間の経過とともに移行の進行状況を追跡したりできます。

メインダッシュボードを表示するには、ダッシュボードMigration Hub コンソールホームページの左側にあるナビゲーションペインから。

データ収集ツール

Application Discovery Service エージェントレスコレクタ (エージェントレスコレクタ) とAWSアプリケーションディスカバリーエージェント (ディスカバリーエージェント) とは、次のようなデータ収集ツールです。AWS Application Discovery Service(Application Discovery Service) は、既存インフラストラクチャの検出を支援するために 1 つを使用します。以下のトピックでは、これらのDiscovery Data収集ツールをダウンロードしてデプロイする方法について説明します。エージェントレスコレクター入門そしてAWS アプリケーション検出エージェント。

これらのデータ収集ツールは Application Discovery Service のリポジトリにデータを保存して、各サーバーと、それらで実行されているプロセスに関する詳細情報を提供します。これらのツールのいずれかがデプロイされていると、データの収集を開始、停止、および表示できます。AWS Migration Hub(Migration Hub) コンソール。

トピック

- データコレクターの開始と停止
- データコレクターの表示と並べ替え

データコレクターの開始と停止

の後にAWSApplication Discovery Agent (Discovery Agent) が導入されたら、でデータ収集プロセスを開始または停止できますデータコレクターのページAWS Migration Hub(Migration Hub) コンソール。

データ収集ツールを開始または停止するには

1. を使用するAWSアカウント、サインインAWS Management ConsoleMigration Hub コンソール () を開きます。https://console.aws.amazon.com/migrationhub/。
2. Migration Hub コンソールのナビゲーションペインで発見、選択してくださいデータコレクター。
3. [Agents] (エージェント) タブを選択します。
4. 開始または停止する収集ツールのチェックボックスをオンにします。
5. [Start data collection (データ収集の開始)] または [Stop data collection (データ収集の停止)] を選択します。

データコレクターの表示と並べ替え

多数のデータコレクタをデプロイした場合は、表示されているデプロイ済みコレクタのリストをデータコレクターコンソール (コンソール)。検索バーにフィルターを適用して、リストを並べ替えます。検索とフィルタ処理は、[Data Collectors (データコレクタ)] で指定したほとんどの条件で実行できます。

次の表に、使用できる検索条件を示します。エージェントには、演算子、値、値の定義が含まれます。

検索条件	演算子	値: 定義
エージェント ID	==	収集ツールのインストール元となる、事前入力されたリストから選択した任意のエージェント ID。
ホスト名	== !=	エージェントの場合、エージェントがインストールされているホストの事前設定されたリストから選択された任意のホスト名です。
収集ステータス	== !=	開始: データが収集され、Application Discovery Service に送信されています。 開始予定: データ収集の開始がスケジュールされています。データは次の ping で Application Discovery Service に送信され、ステータスが [Started] (開始済み) に変わります。 停止: データは収集されておらず、Application Discovery Service に送信されていません。

検索条件	演算子	値: 定義
		停止スケジュール: データ収集の停止がスケジュールされています。データの Application Discovery Service への送信は次の ping で停止され、ステータスが [Stopped] (停止済み) に変わります。
ヘルス	== !=	正常: データ収集は有効になっていません。ツールは正常に機能しています。 非正常: ツールがエラー状態になっています。データの収集または報告は行われていません。 不明: 接続が確立されていない状態が 1 時間を超えています。 シャットダウン中: ツールの最後の通信は、システム、サービス、またはデーモンのシャットダウンが原因の「シャットダウン中」でした。再起動やツールのアップグレードが発生した場合、ステータスは最初のレポートサイクルで別の状態に変わります。 Running: データ収集が有効になっています。ツールは正常に機能しています。

検索条件	演算子	値: 定義
IP アドレス	== !=	収集ツールのインストール先の事前設定されたリストから選択された任意の IP アドレスです。

次の表に、使用できる検索条件を示します。エージェントレスコレクターには、演算子、値、値の定義が含まれます。

検索条件	演算子	値: 定義
ID	==	収集ツールのインストール元となる事前入力されたリストから選択した任意のエージェントレスコレクター ID。
ホスト名	== !=	エージェントレスコレクタの場合、エージェントレスコレクタがインストールされているホストのリストから選択した任意のホスト名。
ステータス	== !=	データ収集: データ収集が有効になっています。ツールは正常に機能しています。 設定準備完了 — データ収集は有効になっていません。ツールは正常に機能しています。 要注意:ツールがエラー状態になっており、注意が必要です。 不明: 接続が確立されていない状態が 1 時間を超えています。

検索条件	演算子	値: 定義
		シャットダウンする: ツールの最後の通信は、システム、サービス、またはデーモンのシャットダウンが原因の「シャットダウン中」でした。再起動やツールのアップグレードが発生した場合、ステータスは最初のレポートサイクルで別の状態に変わります。
IP アドレス	== !=	収集ツールのインストール先の事前設定されたリストから選択された任意の IP アドレスです。

検索フィルタを適用してデータコレクタをソートするには

1. を使用するAWSアカウント、サインインAWS Management ConsoleMigration Hub コンソール () を開きます。https://console.aws.amazon.com/migrationhub/。
2. Migration Hub コンソールのナビゲーションペインで発見、選択してくださいデータコレクター。
3. 次のいずれかを選択してくださいエージェントレスコレクターまたはエージェント(タブ)。
4. 検索バー内をクリックし、リストから検索条件を選択します。
5. 次のリストから演算子を選択します。
6. 最後のリストから値を選択します。

サーバーデータの表示、エクスポート、検索

[Servers (サーバー)] ページには、データ収集ツールが認識している各サーバーインスタンスのシステム設定およびパフォーマンスのデータが表示されます。ここで、サーバー情報の表示、フィルタを使用したサーバーのソート、キーと値のペアを使用したサーバーのタグ付け、およびサーバーとシステムの詳細情報のエクスポートを行うことができます。

トピック

サーバーの表示と並べ替え

データ収集ツールで検出したサーバーの情報を表示し、フィルタを使用してサーバーをソートできます。

サーバーを表示する

データ収集ツールで検出したサーバーの全般表示と詳細表示を取得できます。

検出したサーバーを表示するには

1. を使用するAWSアカウント、サインインAWS Management ConsoleMigration Hub コンソール () を開きます。https://console.aws.amazon.com/migrationhub/。
2. Migration Hub コンソールのナビゲーションペインで発見、選択してくださいサーバー。検出したサーバーがサーバリストに表示されます。
3. 各サーバーの詳細情報を表示するには、[Server info (サーバー情報)] 列でサーバーのリンクを選択します。このサーバーを説明する画面が表示されます。

サーバーの詳細画面には、システムとパフォーマンスのメトリクスが表示されます。ネットワークの依存関係やプロセスの情報を エクスポートするためのボタンも表示されます。サーバーの詳細情報を エクスポートするには、「サーバーデータのエクスポート」を参照してください。

検索フィルターによるサーバーの並べ替え

特定のサーバーを簡単に見つけるには、収集ツールで検出したすべてのサーバーに検索フィルタを適用してソートします。検索とフィルタ処理は、さまざまな条件で実行できます。

検索フィルタを適用してサーバーをソートするには

1. を使用するAWSアカウント、サインインAWS Management ConsoleMigration Hub コンソール () を開きます。https://console.aws.amazon.com/migrationhub/。
2. Migration Hub コンソールのナビゲーションペインで発見、選択してくださいサーバー。
3. 検索バー内をクリックし、リストから検索条件を選択します。
4. 次のリストから演算子を選択します。
5. 選択した検索条件の値を大文字と小文字を区別して入力し、Enter キーを押します。
6. 複数のフィルタを適用するには、ステップ 2〜4 を繰り返します。

サーバーのタグ付け

移行計画と情報の整理に役立てるために、サーバーごとに複数のタグを作成できます。タグは、ユーザー定義のキーと値のペアであり、サーバーに関するカスタムデータやメタデータを保存できます。1 回の操作で、個別または複数のサーバーにタグを付けることができます。AWS Application Discovery Service(Application Discovery Service) タグは次のようになります。AWSタグですが、これらの 2 タイプを同じものとして交互に利用することはできません。

メイン [サーバー] ページから複数のタグを 1 つ以上のサーバーに対して追加または削除できます。選択したサーバーに対して 1 つ以上のタグを追加または削除するには、サーバーの詳細ページを使用します。複数のサーバーに対するタグ付け作業は、作業の種類を問わず、1 回のオペレーションで実行できます。また、タグを削除することもできます。

1 つ以上のサーバーにタグを追加するには

1. を使用するAWSアカウント、サインインAWS Management ConsoleMigration Hub コンソール () を開きます。https://console.aws.amazon.com/migrationhub/。
2. Migration Hub コンソールのナビゲーションペインで発見、選択してくださいサーバー。
3. [Server info (サーバー情報)] 列で、タグを追加するサーバーのリンクを選択します。複数のサーバーに同時にタグを追加するには、各サーバーのチェックボックス内をクリックします。
4. 選択してくださいタグの追加[]、[] の順に選択します新しいタグを追加。
5. ダイアログボックスで、キーフィールド、およびオプションでValue。

   選択してさらにタグを追加します新しいタグを追加さらに情報を追加します。
6. [Save] (保存) を選択します。

1 つ以上のサーバーからタグを追加するには

1. を使用するAWSアカウント、サインインAWS Management ConsoleMigration Hub コンソール () を開きます。https://console.aws.amazon.com/migrationhub/。
2. Migration Hub コンソールのナビゲーションペインで発見、選択してくださいサーバー。
3. [Server info (サーバー情報)] 列で、タグを削除するサーバーのリンクを選択します。複数のサーバーのチェックボックスを選択して、一度に複数のサーバーからタグを削除します。
4. 選択してくださいタグの削除。
5. 削除するタグをそれぞれ選択します。
6. [Confirm] (確認) を選択します。

サーバーデータのエクスポート

1 つのサーバーのネットワーク依存関係とプロセスの情報をエクスポートするには、サーバーの詳細画面を使用できます。サーバーのエクスポートジョブは、サーバーの詳細画面で [Exports (エクスポート)] セクションのテーブルにあります。まだエクスポートジョブがない場合、テーブルは空になります。データ収集を最大 5 つまで同時にエクスポートできます。

> **Note**
>
> コンソールからサーバーデータをエクスポートできるのは、そのサーバーで実行されているエージェントによって収集されたデータのみです。エージェントがインストールされているすべてのサーバのデータを一括エクスポートする場合は、Amazon Athena でのデータ探索。

サーバーの詳細データをエクスポートするには

1. を使用するAWSアカウント、サインインAWS Management ConsoleMigration Hub コンソール () を開きます。https://console.aws.amazon.com/migrationhub/。
2. Migration Hub コンソールのナビゲーションペインで発見、選択してくださいサーバー。
3. [Server info (サーバー情報)] 列で、データをエクスポートするサーバーの ID を選択します。
4. 画面下部の [Exports (エクスポート)] セクションで、[Export server details (サーバー詳細のエクスポート)] を選択します。
5. [Export server details (サーバー詳細のエクスポート)] で、[Start date (開始日)] と [Time (時刻)] を入力します。

> **Note**
>
> 開始時刻は、現在の時刻から 72 時間より前にすることはできません。

6. ジョブを開始するには、[Export (エクスポート)] を選択します。最初のステータスは [In-progress (進行中)] です。ステータスを更新するには、[Exports (エクスポート)] セクションの更新アイコンをクリックします。
7. エクスポートジョブが完了したら、[Download (ダウンロード)] を選択して .zip ファイルを保存します。
8. 保存されたファイルを解凍します。エクスポートデータは、次のような .csv ファイルのセットに含まれています。

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

   .csv ファイルを Microsoft Excel で開き、エクスポートしたサーバーデータを確認できます。

   複数のファイルの 1 つは JSON ファイルであり、これにはエクスポートタスクとその結果に関するデータが含まれています。

Athena でのデータ探索

Amazon Athena でのデータ探索では、Discovery Agent が検出したすべてのオンプレミスサーバーから収集されたデータを 1 か所で分析することができます。Amazon Athena でのデータ探索が Migration Hub コンソールから有効になったら (または StartContinousExport API) を有効にすると、エージェントによって収集されたデータが一定の間隔で自動的に S3 バケットに保存されるようになります。詳細については、「Amazon Athena でのデータ探索」を参照してください。

アプリケーション

一部の検出したサーバーは、グループとして移行することで、引き続き動作できます。この場合、検出したサーバーをアプリケーションとして論理的に定義してグループ化できます。

グループ化のプロセスの一環として、タグの検索、フィルタ処理、および追加を行うことができます。

サーバーを新規または既存のアプリケーションにグループ化するには

1. を使用するAWSアカウント、サインインAWS Management ConsoleMigration Hub コンソール () を開きます。https://console.aws.amazon.com/migrationhub/。
2. Migration Hub コンソールのナビゲーションペインで発見、選択してくださいサーバー。
3. サーバーリストで、新規または既存のアプリケーションにグループ化する各サーバーを選択します。

   グループに含めるサーバーを選択しやすくするために、サーバーリストで任意の条件を指定して検索およびフィルタできます。検索バー内をクリックしてリストから項目を選択し、次のリストから演算子を選択して、条件を入力します。
4. オプション: 選択した各サーバーについて、タグの追加、次の値を入力します。キーを選択し、オプションで次の値を入力しますValue。
5. [Group as application (アプリケーションとしてグループ化する)] を選択してアプリケーションを作成します。または、既存のアプリケーションに追加します。
6. [Group as application (アプリケーションとしてグループ化する)] ダイアログボックスで、[Group as a new application (新規アプリケーションとしてグルーかする)] または [Add to an existing application (既存のアプリケーションに追加する)] を選択し ます。

   a. [Group as a new application (新規アプリケーションとしてグルーかする)] を選択した場合は、[Application name (アプリケーション名)] に名前を入力します。必要に応じて、[Application description (アプリケーションの説明)] に説明を入力できます。

   b. [Add to an existing application (既存のアプリケーション追加する)] を選択した場合は、リストで追加先のアプリケーションの名前を選択します。
7. [Save] を選択します。

Application Discovery Service API を使用して検出された設定項目をクエリする

設定項目は、エージェントまたはインポートによってデータセンターで検出された IT アセットです。 AWS Application Discovery Service (Application Discovery Service) を使用する場合、 API を使用してフィルターを指定し、サーバー、アプリケーション、プロセス、および接続アセットの特定の設定項目をクエリします。API の詳細については、「Application Discovery Service API リファレンス」を参照してください。

以下のセクションの表は、2 つの Application Discovery Service アクションで使用できる入力フィルターと出力ソートオプションのリストです。

- `DescribeConfigurations`
- `ListConfigurations`

フィルタリングおよびソートのオプションは、適用するアセットのタイプ (サーバー、アプリケーション、プロセス、接続) 別に整理されています。

> **Important**
>
> `DescribeConfigurations`、、および によって返された結果に はListConfigurations、最近の更新が含まれていないStartExportTask可能性があります。詳細については、「結果整合性」を参照してください。

`DescribeConfigurations` アクションの使用

`DescribeConfigurations` アクションは、設定 ID のリストの属性を取得します。提供される ID はすべて、アセットタイプ (サーバー、アプリケーション、プロセス、または接続) が同じである必要があります。出力フィールドは、選択されたアセットタイプに固有です。たとえば、サーバー設定項目の出力には、ホスト名、オペレーティングシステム、ネットワークカード数など、サーバーに関する属性のリストが含まれています。コマンド構文の詳細については、「」を参照してくださいDescribeConfigurations。

`DescribeConfigurations` アクションはフィルタリングをサポートしていません。

`DescribeConfigurations` の出力フィールド

以下の表は、アセットタイプ別に整理された、DescribeConfigurations アクションでサポートされる出力フィールドの一覧です。必須とマークされたものは、常に出力に存在します。

サーバーアセット

フィールド	必須
server.agentId	
server.applications	
server.applications.hasMoreValues	
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	
server.performance.avgCpuUsagePct	

フィールド	必須
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	
server.performance.maxNetworkReadsPerSecondInKB	

フィールド	必須
server.performance.maxNetwo rkWritesPerSecondInKB	
server.performance.minFreeR AMInKB	
server.performance.numCores	
server.performance.numCpus	
server.performance.numDisks	
server.performance.numNetwo rkCards	
server.performance.totalRAMInKB	

アセットの処理

フィールド	必須
process.commandLine	
process.configurationId	x
process.name	
process.path	
process.timeOfCreation	x

アプリケーションアセット

フィールド	必須
application.configurationId	x

フィールド	必須
application.description	
application.lastModifiedTime	x
application.name	x
application.serverCount	x
application.timeOfCreation	x

ListConfigurations アクションの使用

ListConfigurations アクションは、フィルタで指定した条件に従って、構成項目のリストを取得します。コマンド構文の詳細については、「」を参照してくださいListConfigurations。

ListConfigurations の出力フィールド

以下の表は、アセットタイプ別に整理された、ListConfigurations アクションでサポートされる出力フィールドの一覧です。必須とマークされたものは、常に出力に存在します。

サーバーアセット

フィールド	必須
server.configurationId	x
server.agentId	
server.hostName	
server.osName	
server.osVersion	
server.timeOfCreation	x
server.type	

アセットの処理

フィールド	必須
process.commandLine	
process.configurationId	x
process.name	
process.path	
process.timeOfCreation	x
server.agentId	
server.configurationId	x

アプリケーションアセット

フィールド	必須
application.configurationId	x
application.description	
application.name	x
application.serverCount	x
application.timeOfCreation	x
application.lastModifiedTime	x

接続アセット

フィールド	必須
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	

ListConfigurations でサポートされているフィルタ

以下の表は、アセットタイプ別に整理された、ListConfigurations アクションでサポートされるフィルタの一覧です。フィルタと値は、サポートされている論理条件のいずれかによって定義されたキー/値の関係にあります。指定したフィルタの出力は並べ替えることができます。

サーバーアセット

フィルター	サポートされる条件	サポートされる値	サポートされるソート
server.configurationId	• EQUALS • NOT_EQUALS • EQ • NE	• 任意の有効なサーバ設定 ID	なし
server.hostName	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 文字列	• ASC • DESC
server.osName	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 文字列	• ASC • DESC
server.osVersion	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 文字列	• ASC • DESC
server.agentId	• EQUALS • NOT_EQUALS • EQ • NE	• 文字列	なし

フィルター	サポートされる条件	サポートされる値	サポートされるソート
server.connectorId	• EQUALS • NOT_EQUALS • EQ • NE	• 文字列	なし
server.type	• EQUALS • NOT_EQUALS • EQ • NE	次のいずれかの値を持つ文字列: • EC2 • OTHER • VMWARE_VM • VMWARE_HOST • VMWARE_VM_TEMPLATE	なし
server.vmWareInfo.morefId	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 文字列	なし
server.vmWareInfo.vcenterId	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 文字列	なし

フィルター	サポートされる条件	サポートされる値	サポートされるソート
server.vmWareInfo.hostId	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 文字列	なし
server.networkInterfaceInfo.portGroupId	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 文字列	なし
server.networkInterfaceInfo.portGroupName	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 文字列	なし
server.networkInterfaceInfo.virtualSwitchName	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 文字列	なし

フィルター	サポートされる条件	サポートされる値	サポートされるソート
server.networkInterfaceInfo.ipAddress	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 文字列	なし
server.networkInterfaceInfo.macAddress	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 文字列	なし
server.performance.avgCpuUsagePct	• GE • LE • GT • LT	• 割合 (%)	なし
server.performance.totalDiskFreeSizeInKB	• GE • LE • GT • LT	• ダブル	なし
server.performance.avgFreeRAMInKB	• GE • LE • GT • LT	• ダブル	なし

フィルター	サポートされる条件	サポートされる値	サポートされるソート
server.tag.value	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 文字列	なし
server.tag.key	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 文字列	なし
server.application.name	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 文字列	なし
server.application.description	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 文字列	なし

フィルター	サポートされる条件	サポートされる値	サポートされるソート
server.application.configurationId	• EQUALS • NOT_EQUALS • EQ • NE	• 任意の有効なアプリケーション構成 ID	なし
server.process.configurationId	• EQUALS • NOT_EQUALS • EQ • NE	• ProcessId	なし
server.process.name	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 文字列	なし
server.process.commandLine	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 文字列	なし

アプリケーションアセット

フィルター	サポートされる条件	サポートされる値	サポートされるソート
application.configurationId	• EQUALS • NOT_EQUALS • EQ • NE	• ApplicationId	なし
application.name	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 文字列	• ASC • DESC
application.description	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 文字列	• ASC • DESC
application.serverCount	フィルタリングはサポートされていません。	フィルタリングはサポートされていません。	• ASC • DESC
application.timeOfCreation	フィルタリングはサポートされていません。	フィルタリングはサポートされていません。	• ASC • DESC
application.lastModifiedTime	フィルタリングはサポートされていません。	フィルタリングはサポートされていません。	• ASC • DESC

フィルター	サポートされる条件	サポートされる値	サポートされるソート
server.configurationId	• EQUALS • NOT_EQUALS • EQ • NE	• ServerId	なし

アセットの処理

フィルター	サポートされる条件	サポートされる値	サポートされるソート
process.configurationId	• EQUALS • NOT_EQUALS • EQ • NE	• ProcessId	
process.name	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 文字列	• ASC • DESC
process.commandLine	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 文字列	• ASC • DESC

フィルター	サポートされる条件	サポートされる値	サポートされるソート
server.configurationId	• EQUALS • NOT_EQUALS • EQ • NE	• ServerId	
server.hostName	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 文字列	• ASC • DESC
server.osName	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 文字列	• ASC • DESC
server.osVersion	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 文字列	• ASC • DESC

フィルター	サポートされる条件	サポートされる値	サポートされるソート
server.agentId	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 文字列	

接続アセット

フィルター	サポートされる条件	サポートされる値	サポートされるソート
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	• 整数	• ASC • DESC

フィルター	サポートされる条件	サポートされる値	サポートされるソート
sourceServer.configurationId	• EQUALS • NOT_EQUALS • EQ • NE	• ServerId	
sourceServer.hostName	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 文字列	• ASC • DESC
destinationServer.osName	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 文字列	• ASC • DESC
destinationServer.osVersion	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 文字列	• ASC • DESC

フィルター	サポートされる条件	サポートされる値	サポートされるソート
destinationServer.agentId	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 文字列	
sourceProcess.configurationId	• EQUALS • NOT_EQUALS • EQ • NE	• ProcessId	
sourceProcess.name	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 文字列	• ASC • DESC
sourceProcess.commandLine	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 文字列	• ASC • DESC
destinationProcess.configurationId	• EQUALS • NOT_EQUALS • EQ • NE	• ProcessId	

フィルター	サポートされる条件	サポートされる値	サポートされるソート
destinationProcess.name	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 文字列	• ASC • DESC
destinationprocess.commandLine	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• 文字列	• ASC • DESC

AWS Application Discovery Service API の結果整合性

次の更新オペレーションは結果整合性があります。更新は、読み取りオペレーションStartExportタスク 、、DescribeConfigurationsおよび にすぐに表示されない場合がありますListConfigurations。

- AssociateConfigurationItemsToアプリケーション
- CreateTags
- DeleteApplications
- DeleteTags
- DescribeBatchDeleteConfigurationタスク
- DescribeImportタスク
- DisassociateConfigurationItemsFromアプリケーション
- UpdateApplication

結果整合性を管理するための提案：

- 読み取りオペレーションStartExportタスク 、、または ListConfigurations (または対応する AWS CLI コマンド) を呼び出すときはDescribeConfigurations、エクスポネンシャルバックオフアルゴリズムを使用して、以前の更新オペレーションがシステム内を伝播するのに十分な時間を確保します。これを行うには、読み取りオペレーションを繰り返し実行し、2 秒の待機時間から開始して、最大 5 分間の待機時間を徐々に増やします。
- 更新オペレーションが 200 - OK レスポンスを返す場合でも、後続のオペレーションの間に待機時間を追加します。数秒の待機時間から始まる指数バックオフアルゴリズムを適用し、最大約 5 分間の待機時間を徐々に増やします。

AWS Application Discovery Service のセキュリティ

AWS では、クラウドセキュリティが最優先事項です。AWS のお客様は、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャから利点を得られます。

セキュリティは、AWS と顧客の間の責任共有です。責任共有モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティとして説明しています。

- クラウドのセキュリティ - AWS は、AWS クラウドで AWS サービスを実行するインフラストラクチャを保護する責任を負います。また、AWS は、使用するサービスを安全に提供します。セキュリティの有効性は、AWS コンプライアンスプログラムの一環として、サードパーティーの審査機関によって定期的にテストおよび検証されています。
- クラウド内のセキュリティ - お客様の責任は、使用する AWS のサービスに応じて異なります。また、お客様は、お客様のデータの機密性、組織の要件、および適用可能な法律および規制などの他の要因についても責任を担います。

AWSアプリケーション検出エージェントまたはApplication Discovery Service エージェントレスコレクターを使用するには、AWSアカウントへのアクセスキーを提供する必要があります。その後、この情報はローカルインフラストラクチャに保存されます。責任分担モデルの一環として、インフラへのアクセスを保護する責任はお客様にあります。

このドキュメントは、Application Discovery Service の使用時に責任共有モデルを適用する方法を理解するために役立ちます。以下のトピックでは、セキュリティおよびコンプライアンス上の目的に合わせて Application Discovery Service を設定する方法について説明します。また、Application Discovery Service AWS リソースの監視と保護に役立つ他のサービスの使用方法についても学びます。

トピック

の Identity and Access Management AWS Application Discovery Service

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に制御 AWS のサービス するのに役立つ です。IAM 管理者は、Application Discovery Service リソースの使用について誰が認証され (サインインされる)、承認される (許可を持つ) かを制御します。IAM は、追加料金なしで AWS のサービス 使用できる です。

トピック

対象者

AWS Identity and Access Management (IAM) の使用方法は、Application Discovery Service で行う作業によって異なります。

サービスユーザー – 業務を行うために Application Discovery Service サービスを使用する場合は、管理者から必要な認証情報と許可が提供されます。作業を行うために使用する Application Discovery Service 機能が増えるとともに、追加の許可が必要になる場合があります。アクセスの管理方法を理解しておくと、管理者に適切な許可をリクエストするために役に立ちます。Application Discovery Service の機能にアクセスできない場合は、「AWS Application Discovery Service Identity and Access のトラブルシューティング」を参照してください。

サービス管理者 – 社内で Application Discovery Service リソースに対する責任を担っている場合は、Application Discovery Service への完全なアクセス権があると思われます。サービスユーザーがどの Application Discovery Service 機能やリソースにアクセスするかを決めるのは管理者の仕事です。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を点検して、IAM の基本概念を理解してください。企業

が Application Discovery Service で IAM を使用する方法の詳細については、「と IAM の AWS Application Discovery Service 連携方法」を参照してください。

IAM 管理者 – IAM 管理者である場合は、Application Discovery Service へのアクセスを管理するポリシーの作成方法に関する詳細を理解しておくことをお勧めします。IAM で使用できる Application Discovery Service のアイデンティティベースポリシーの例を確認するには、「AWS Application Discovery Service ID ベースのポリシーの例」を参照してください。

アイデンティティを使用した認証

認証とは、ID 認証情報 AWS を使用して にサインインする方法です。として、IAM ユーザーとして AWS アカウントのルートユーザー、または IAM ロールを引き受けて認証（ にサインイン AWS) される必要があります。

ID ソースを介して提供された認証情報を使用して、フェデレーティッド ID AWS として にサインインできます。 AWS IAM Identity Center（ IAM Identity Center) ユーザー、会社のシングルサインオン認証、Google または Facebook の認証情報は、フェデレーション ID の例です。フェデレーティッド ID としてサインインする場合、IAM ロールを使用して、前もって管理者により ID フェデレーションが設定されています。フェデレーション AWS を使用して にアクセスすると、間接的にロールを引き受けることになります。

ユーザーのタイプに応じて、 AWS Management Console または AWS アクセスポータルにサインインできます。へのサインインの詳細については AWS、「 ユーザーガイド」の「 へのサインイン AWS アカウント方法AWS サインイン 」を参照してください。

AWS プログラムで にアクセスする場合、 は Software Development Kit (SDK) とコマンドラインインターフェイス (CLI) AWS を提供し、認証情報を使用してリクエストに暗号で署名します。 AWS ツールを使用しない場合は、リクエストに自分で署名する必要があります。推奨される方法を使用してリクエストを自分で署名する方法の詳細については、IAM ユーザーガイドの API AWS リクエストの署名を参照してください。

使用する認証方法を問わず、追加セキュリティ情報の提供をリクエストされる場合もあります。例えば、 AWS では、多要素認証 (MFA) を使用してアカウントのセキュリティを向上させることをお勧めします。詳細については、「AWS IAM Identity Center ユーザーガイド」の「Multi-factor authentication」(多要素認証) および「IAM ユーザーガイド」の「AWSでの多要素認証 (MFA) の使用」を参照してください。

AWS アカウント ルートユーザー

を作成するときは AWS アカウント、アカウント内のすべての およびリソースへの AWS のサービス 完全なアクセス権を持つ 1 つのサインインアイデンティティから始めます。この ID は AWS アカウント ルートユーザーと呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることでアクセスできます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報は保護し、ルートユーザーでしか実行できないタスクを実行するときに使用します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、IAM ユーザーガイドの「ルートユーザー認証情報が必要なタスク」を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、単一のユーザーまたはアプリケーションに対して特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を保有する IAM ユーザーを作成する代わりに、一時的な認証情報を使用することをお勧めします。ただし、IAM ユーザーでの長期的な認証情報が必要な特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、IAM ユーザーガイドの長期的な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションするを参照してください。

IAM グループは、IAM ユーザーの集団を指定するアイデンティティです。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できます。多数のユーザーグループがある場合、グループを使用することで権限の管理が容易になります。例えば、IAMAdminsという名前のグループを設定して、そのグループにIAM リソースを管理する許可を与えることができます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時的な認証情報が提供されます。詳細については、「IAM ユーザーガイド」の「IAM ユーザー (ロールではなく) の作成が適している場合」を参照してください。

IAM ロール

IAM ロールは、特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。これは IAM ユーザーに似ていますが、特定のユーザーには関連付けられていません。ロール を切り替える AWS Management Console ことで、 で IAM ロールを一時的に引き受けることができます。ロール

を引き受けるには、 または AWS API AWS CLI オペレーションを呼び出すか、カスタム URL を使用します。ロールを使用する方法の詳細については、「IAM ユーザーガイド」の「IAM ロールの使用」を参照してください。

IAM ロールと一時的な認証情報は、次の状況で役立ちます:

- フェデレーションユーザーアクセス – フェデレーティッド ID に許可を割り当てるには、ロールを作成してそのロールの許可を定義します。フェデレーティッド ID が認証されると、その ID はロールに関連付けられ、ロールで定義されている許可が付与されます。フェデレーションの詳細については、「IAM ユーザーガイド」の「Creating a role for a third-party Identity Provider」(サードパーティーアイデンティティプロバイダー向けロールの作成) を参照してください。IAM Identity Center を使用する場合は、許可セットを設定します。アイデンティティが認証後にアクセスできるものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。アクセス許可セットの詳細については、「AWS IAM Identity Center ユーザーガイド」の「アクセス許可セット」を参照してください。
- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで引き受けることができます。
- クロスアカウントアクセス - IAM ロールを使用して、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、一部の では AWS のサービス、 (ロールをプロキシとして使用する代わりに) ポリシーをリソースに直接アタッチできます。クロスアカウントアクセスにおけるロールとリソースベースのポリシーの違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。
- クロスサービスアクセス — 一部の は、他の の機能 AWS のサービス を使用します AWS のサービス。例えば、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2 でアプリケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。サービスでは、呼び出し元プリンシパルの許可、サービスロール、またはサービスリンクロールを使用してこれを行う場合があります。
  - 転送アクセスセッション (FAS) – IAM ユーザーまたはロールを使用して でアクションを実行する場合 AWS、ユーザーはプリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストのリクエストと組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するため

のアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

- サービスロール - サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、「IAM ユーザーガイド」の「AWS のサービスにアクセス許可を委任するロールの作成」を参照してください。
- サービスにリンクされたロール – サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールのアクセス許可を表示できますが、編集することはできません。

- Amazon EC2 で実行されているアプリケーション – IAM ロールを使用して、EC2 インスタンスで実行され、 AWS CLI または AWS API リクエストを行うアプリケーションの一時的な認証情報を管理できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。 AWS ロールを EC2 インスタンスに割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムは一時的な認証情報を取得できます。詳細については、IAM ユーザーガイドのAmazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して許可を付与するを参照してください。

IAM ロールと IAM ユーザーのどちらを使用するかについては、IAM ユーザーガイドの(IAM ユーザーではなく) IAM ロールをいつ作成したら良いのか?を参照してください。

ポリシーを使用したアクセスの管理

でアクセスを制御する AWS には、ポリシーを作成し、 AWS ID またはリソースにアタッチします。ポリシーは AWS 、アイデンティティまたはリソースに関連付けられているときにアクセス許可を定義する のオブジェクトです。 は、プリンシパル (ユーザー、ルートユーザー、またはロールセッション) がリクエストを行うときに、これらのポリシー AWS を評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。ほとんどのポリシーは JSON ドキュメント AWS として に保存されます。JSON ポリシードキュメントの構造と内容の詳細については、IAM ユーザーガイドのJSON ポリシー概要を参照してください。

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

デフォルトでは、ユーザーやロールに権限はありません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き継ぐことができます。

IAM ポリシーは、オペレーションの実行方法を問わず、アクションの許可を定義します。例えば、`iam:GetRole`アクションを許可するポリシーがあるとします。そのポリシーを持つユーザーは、 AWS Management Console、、 AWS CLIまたは AWS API からロール情報を取得できます。

アイデンティティベースのポリシー

アイデンティティベースポリシーは、IAM ユーザーグループ、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、IAM ユーザーガイドのIAM ポリシーの作成を参照してください。

アイデンティティベースのポリシーは、さらにインラインポリシーまたはマネージドポリシーに分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれています。管理ポリシーは、 内の複数のユーザー、グループ、ロールにアタッチできるスタンドアロンポリシーです AWS アカウント。管理ポリシーには、 AWS 管理ポリシーとカスタマー管理ポリシーが含まれます。マネージドポリシーまたはインラインポリシーのいずれかを選択する方法については、IAM ユーザーガイドのマネージドポリシーとインラインポリシーの比較を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシー や Amazon S3 バケットポリシー があげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。リソースベースのポリシーでは、IAM の AWS マネージドポリシーを使用できません。

アクセスコントロールリスト (ACL)

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための許可を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

Amazon S3、 AWS WAF、および Amazon VPC は、ACLs。ACL の詳細については、Amazon Simple Storage Service デベロッパーガイドのアクセスコントロールリスト (ACL) の概要を参照してください。

その他のポリシータイプ

AWS は、一般的ではない追加のポリシータイプをサポートします。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- アクセス許可の境界 - アクセス許可の境界は、アイデンティティベースのポリシーによって IAM エンティティ (IAM ユーザーまたはロール) に付与できる権限の上限を設定する高度な機能です。エンティティにアクセス許可の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。`Principal` フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。アクセス許可の境界の詳細については、IAM ユーザーガイドのIAM エンティティのアクセス許可の境界を参照してください。
- サービスコントロールポリシー (SCPs) – SCPs は、 の組織または組織単位 (OU) に対する最大アクセス許可を指定する JSON ポリシーです AWS Organizations。 AWS Organizations は、 AWS アカウント ビジネスが所有する複数の をグループ化して一元管理するサービスです。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCP) を一部またはすべてのアカウントに適用できます。SCP は、各 を含むメンバーアカウントのエンティティのアクセス許可を制限します AWS アカウントのルートユーザー。Organizations と SCP の詳細については、AWS Organizations ユーザーガイドの「SCP の仕組み」を参照してください。
- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、IAM ユーザーガイドのセッションポリシーを参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成される権限を理解するのがさらに難しくなります。複数のポリシータイプが関与する場合にリクエストを許可するかどうか AWS を決定する方法については、IAM ユーザーガイドの「ポリシー評価ロジック」を参照してください。

と IAM の AWS Application Discovery Service 連携方法

IAM を使用して Application Discovery Service へのアクセスを管理する前に、Application Discovery Service で使用できる IAM 機能を理解しておく必要があります。Application Discovery Service およびその他の AWS のサービスが IAM と連携する方法の概要を把握するには、「IAM ユーザーガイド」のAWS 「IAM と連携する のサービス」を参照してください。

トピック

- Application Discovery Service のアイデンティティベースポリシー
- Application Discovery Service のリソースベースポリシー
- Application Discovery Service タグに基づく承認
- Application Discovery Service の IAM ロール

Application Discovery Service のアイデンティティベースポリシー

IAM アイデンティティベースのポリシーでは、許可または拒否するアクションとリソース、アクションを許可または拒否する条件を指定できます。Application Discovery Service は、特定のアクション、リソース、および条件キーをサポートします。JSON ポリシーで使用するすべての要素については、「IAM ユーザーガイド」の「IAM JSON ポリシー要素のリファレンス」を参照してください。

アクション

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

JSON ポリシーの`Action`要素には、ポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。ポリシーアクションの名前は通常、関連付けられた AWS API オペレーションと同じです。一致する API オペレーションのない許可のみのアクションなど、いくつかの例外があります。また、ポリシーに複数のアクションが必要なオペレーションもあります。これらの追加アクションは、依存アクションと呼ばれます。

このアクションは、関連付けられたオペレーションを実行するための権限を付与するポリシーで使用されます。

Application Discovery Service のポリシーアクションは、アクションの前にプレフィックス `discovery:` を使用します。ポリシーステートメントには、`Action` または `NotAction` 要素を含める必要があります。Application Discovery Service は、このサービスで実行できるタスクを記述する、独自のアクション一式を定義します。

単一ステートメントに複数アクションを指定するには、次のようにカンマで区切ります:

```
"Action": [
      "discovery:action1",
      "discovery:action2"
```

ワイルドカード (*) を使用して複数アクションを指定できます。例えば、`Describe` という単語で始まるすべてのアクションを指定するには、次のアクションを含めます。

```
"Action": "discovery:Describe*"
```

Application Discovery Service アクションのリストを確認するには、IAM ユーザーガイドの「AWS Application Discovery Serviceで定義されるアクション」を参照してください。

リソース

Application Discovery Service は、ポリシー内でのリソース ARN の指定をサポートしません。アクセスを分離するには、個別の を作成して使用します AWS アカウント。

条件キー

Application Discovery Service はサービス固有の条件キーを提供しませんが、いくつかのグローバル条件キーの使用がサポートされています。すべての AWS グローバル条件キーを確認するには、「IAM ユーザーガイドAWS 」の「グローバル条件コンテキストキー」を参照してください。

例

Application Discovery Service のアイデンティティベースポリシーの例を確認するには、「AWS Application Discovery Service ID ベースのポリシーの例」を参照してください。

Application Discovery Service のリソースベースポリシー

Application Discovery Service は、リソースベースポリシーをサポートしません。

Application Discovery Service タグに基づく承認

Application Discovery Service は、リソースのタグ付け、またはタグに基づいたアクセスの制御をサポートしません。

Application Discovery Service の IAM ロール

IAM ロールは、特定のアクセス許可を持つ AWS アカウント内のエンティティです。

Application Discovery Service での一時的な認証情報の使用

Application Discovery Service は一時的な認証情報の使用をサポートしません。

サービスリンクロール

サービスにリンクされたロールを使用すると、 AWS サービスは他の サービスのリソースにアクセスして、ユーザーに代わってアクションを実行できます。サービスリンクロールは IAM アカウント内に表示され、サービスによって所有されます。IAM 管理者は、サービスリンクロールの許可を表示できますが、編集することはできません。

Application Discovery Service はサービスリンクロールをサポートします。Application Discovery Service のサービスリンクロールの作成または管理の詳細については、「Application Discovery Service 用のサービスリンクロールの使用」を参照してください。

サービスロール

この機能により、ユーザーに代わってサービスがサービスロールを引き受けることが許可されます。このロールにより、サービスがお客様に代わって他のサービスのリソースにアクセスし、アクションを完了することが許可されます。サービスロールは、IAM アカウントに表示され、アカウントによって所有されます。つまり、IAM 管理者は、このロールの権限を変更できます。ただし、それにより、サービスの機能が損なわれる場合があります。

Application Discovery Service はサービスロールをサポートします。

AWS の マネージドポリシー AWS Application Discovery Service

ユーザー、グループ、ロールにアクセス許可を追加するには、自分でポリシーを作成するよりも、AWS 管理ポリシーを使用する方が簡単です。チームに必要な許可のみを提供する IAM カスタマーマネージドポリシーを作成するには、時間と専門知識が必要です。すぐに使用を開始するには、 AWS マネージドポリシーを使用できます。これらのポリシーは、一般的なユースケースをターゲット範囲に含めており、 AWS アカウント で利用できます。 AWS 管理ポリシーの詳細については、IAM ユーザーガイドの「 AWS 管理ポリシー」を参照してください。

AWS のサービスは、 AWS マネージドポリシーを維持および更新します。 AWS 管理ポリシーのアクセス許可は変更できません。サービスでは、新しい機能を利用できるようにするために、 AWS マネージドポリシーに権限が追加されることがあります。この種類の更新は、ポリシーがアタッチされている、すべてのアイデンティティ (ユーザー、グループおよびロール) に影響を与えます。新しい機能が立ち上げられた場合や、新しいオペレーションが使用可能になった場合に、各サービスが AWS マネージドポリシーを更新する可能性が最も高くなります。サービスは AWS マネージドポリシーからアクセス許可を削除しないため、ポリシーの更新によって既存のアクセス許可が破棄されることはありません。

さらに、 は、複数の サービスにまたがる職務機能の管理ポリシー AWS をサポートします。例えば、 ReadOnlyAccess AWS 管理ポリシーは、すべての AWS サービスとリソースへの読み取り専用アクセスを提供します。サービスが新しい機能を起動すると、 は新しいオペレーションとリソースに読み取り専用アクセス許可 AWS を追加します。ジョブ機能のポリシーの一覧および詳細については、「IAM ユーザーガイド」の「AWS のジョブ機能のマネージドポリシー」を参照してください。

AWS マネージドポリシー： AWSApplicationDiscoveryServiceFullAccess

`AWSApplicationDiscoveryServiceFullAccess` ポリシーは、Application Discovery Service API と Migration Hub API へのアクセス権を IAM ユーザーアカウントに付与します。

このポリシーがアタッチされた IAM ユーザーアカウントは、Application Discovery Service の設定、エージェントの起動と停止、エージェントレス検出の開始と停止、および AWS Discovery Service データベースからのデータのクエリを行うことができます。このポリシーの例については、「Application Discovery Service へのフルアクセスの付与」を参照してください。

AWS マネージドポリシー： AWSApplicationDiscoveryAgentlessCollectorAccess

`AWSApplicationDiscoveryAgentlessCollectorAccess` マネージドポリシーは、Application Discovery Service Agentless Collector (Agentless Collector) に、Application Discovery Service を登録して通信し、他の AWS サービスと通信するためのアクセス許可を付与します。

このポリシーは、 Agentless Collector の設定に認証情報を使用する IAM ユーザーにアタッチする必要があります。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- `arsenal` — コレクターが Application Discovery Service アプリケーションに登録できるようにします。これは、収集したデータを に送信できるようにするために必要です AWS。
- `ecr-public` — コレクターが、コレクターの最新の更新が見つかった Amazon Elastic Container Registry Public (Amazon ECR Public) を呼び出すことを許可します。
- `mgh` — コレクターが を呼び出し AWS Migration Hub て、コレクターの設定に使用されるアカウントのホームリージョンを取得できるようにします。これは、収集されたデータの送信先となるリージョンを知るために必要です。
- `sts` – コレクターがサービスベアラートークンを取得できるようにします。これにより、コレクターは Amazon ECR Public を呼び出して最新の更新を取得できます。

```
{
    "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 マネージドポリシー： AWSApplicationDiscoveryAgentAccess

AWSApplicationDiscoveryAgentAccess ポリシーは、Application Discovery Service に登録して通信するためのアクセス権を Application Discovery Agent に付与します。

このポリシーをアタッチする対象ユーザーは、その認証情報が Application Discovery Service で使用されるすべてのユーザーです。

このポリシーは、ユーザーに Arsenal へのアクセス権も付与します。Arsenal は、 によって管理およびホストされるエージェントサービスです AWS。Arsenal は、クラウド内で Application Discovery Service にデータを転送します。このポリシーの例については、「検出エージェントへのアクセスの許可」を参照してください。

AWS マネージドポリシー: AWSAgentlessDiscoveryService

このAWSAgentlessDiscoveryServiceポリシーは、VMware vCenter Server で実行されている AWS Agentless Discovery Connector に、Application Discovery Service へのコネクタヘルスメトリクスの登録、通信、および共有を行うためのアクセス権を付与します。

このポリシーをアタッチする対象のユーザーは、その認証情報がコネクタで使用されるすべてのユーザーです。

AWS マネージドポリシー: ApplicationDiscoveryServiceContinuousExportServiceRole ポリシー

IAM アカウントに AWSApplicationDiscoveryServiceFullAccessポリシー がアタッチされている場合、Amazon Athena でデータ探索を有効にすると、ApplicationDiscoveryServiceContinuousExportServiceRolePolicyが自動的にアカウントにアタッチされます。

このポリシーにより AWS Application Discovery Service 、 は Amazon Data Firehose ストリームを作成して、 AWS Application Discovery Service エージェントによって収集されたデータを変換し、AWS アカウントの Amazon S3 バケットに配信できます。

さらに、このポリシーは application_discovery_service_database という新しいデータベースと、エージェントが収集したデータをマッピングするためのテーブルスキーマ AWS Glue Data Catalog を使用して を作成します。このポリシーの例については、「 エージェントデータ収集のアクセス許可の付与」を参照してください。

AWS マネージドポリシー： AWSDiscoveryContinuousExportFirehosePolicy

このAWSDiscoveryContinuousExportFirehosePolicyポリシーは、Amazon Athena でのデータ探索を使用するために必要です。これにより、Amazon Data Firehose は Application Discovery Service から収集されたデータを Amazon S3 に書き込むことができます。このポリシーの使用方法については、「 AWSApplicationDiscoveryServiceFirehose ロールの作成」を参照してください。このポリシーの例については、「データ探索のアクセス許可の付与」を参照してください。

AWSApplicationDiscoveryServiceFirehose ロールの作成

管理者は、IAM ユーザーアカウントにマネージドポリシーをアタッチします。AWSDiscoveryContinuousExportFirehosePolicy ポリシーを使用する場合、管理者は最初に Firehose AWSApplicationDiscoveryServiceFirehoseを信頼されたエンティティとして という名前のロールを作成し、次に次の手順に示すように、AWSDiscoveryContinuousExportFirehosePolicyポリシーをロールにアタッチする必要があります。

AWSApplicationDiscoveryServiceFirehose IAM ロールを作成する

1. IAM コンソールのナビゲーションペインで [Roles] (ロール) を選択します。
2. [ロールの作成] を選択します。
3. [Kinesis] を選択します。

4. ユースケースとして、[Kinesis Firehose] を選択します。
5. [次へ: アクセス許可] を選択します。
6. フィルターポリシー で を検索しますAWSDiscoveryContinuousExportFirehosePolicy。
7. の横にあるボックスを選択しAWSDiscoveryContinuousExportFirehosePolicy、次へ: 確認 を選択します。
8. ロール名AWSApplicationDiscoveryServiceFirehoseとして「」と入力し、「ロールの作成」を選択します。

Application Discovery Service の AWS マネージドポリシーへの更新

Application Discovery Service がこれらの変更の追跡を開始してからの、Application Discovery Service の AWS マネージドポリシーの更新に関する詳細を表示します。このページへの変更に関する自動アラートについては、AWS Application Discovery Service のドキュメント履歴 ページの RSS フィードを購読してください。

変更	説明	日付
AWSApplicationDiscoveryAgentlessCollectorAccess – エージェントレスコレクターの起動で新しいポリシーが利用可能に	Application Discovery Service は、Application Discovery Service を登録して通信し、他の AWS サービスと通信するためのアクセス権限を Agentless Collector に付与`AWSApplicationDiscoveryAgentlessCollectorAccess` する新しいマネージドポリシーを追加しました。	2022 年 8 月 16 日
Application Discovery Service が変更の追跡を開始	Application Discovery Service が AWS マネージドポリシーの変更の追跡を開始しました。	2021 年 3 月 1 日

AWS Application Discovery Service ID ベースのポリシーの例

デフォルトで、IAM ユーザーとロールには Application Discovery Service リソースを作成または変更する許可がありません。また、、 AWS Management Console AWS CLI、または AWS API を使用してタスクを実行することはできません。IAM 管理者は、ユーザーとロールに必要な、指定されたリソースで特定の API オペレーションを実行する権限をユーザーとロールに付与する IAM ポリシーを作成する必要があります。続いて、管理者はそれらの権限が必要な IAM ユーザーまたはグループにそのポリシーをアタッチする必要があります。

JSON ポリシードキュメントのこれらの例を使用して、IAM アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「JSON タブでのポリシーの作成」を参照してください。

トピック

- ポリシーのベストプラクティス
- Application Discovery Service へのフルアクセスの付与
- 検出エージェントへのアクセスの許可
- エージェントデータ収集のアクセス許可の付与
- データ探索のアクセス許可の付与
- Migration Hub コンソールのネットワーク図を使用するためのアクセス許可の付与

ポリシーのベストプラクティス

ID ベースのポリシーは、ユーザーのアカウントで誰かが Application Discovery Service リソースを作成、アクセス、または削除できるどうかを決定します。これらのアクションを実行すると、 AWS アカウントに料金が発生する可能性があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する – ユーザーとワークロードにアクセス許可を付与するには、多くの一般的なユースケースにアクセス許可を付与する AWS 管理ポリシーを使用します。これらは で使用できます AWS アカウント。ユースケースに固有の AWS カスタマー管理ポリシーを定義して、アクセス許可をさらに減らすことをお勧めします。詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」または「ジョブ機能のAWS マネージドポリシー」を参照してください。
- 最小特権を適用する – IAM ポリシーで許可を設定する場合は、タスクの実行に必要な許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定

義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用して許可を適用する方法の詳細については、IAM ユーザーガイドのIAM でのポリシーとアクセス許可を参照してください。

- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。条件を使用して、 などの特定の を介してサービスアクションが使用される場合に AWS のサービス、サービスアクションへのアクセスを許可することもできます AWS CloudFormation。詳細については、「IAM ユーザーガイド」の [IAM JSON policy elements: Condition] (IAM JSON ポリシー要素:条件) を参照してください。
- IAM Access Analyzer を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM Access Analyzer は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、IAM ユーザーガイドのIAM Access Analyzer ポリシーの検証を参照してください。
- 多要素認証 (MFA) を要求する – で IAM ユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、セキュリティを強化するために MFA を有効にします。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、IAM ユーザーガイドのMFA 保護 API アクセスの設定を参照してください。

IAM でのベストプラクティスの詳細については、IAM ユーザーガイドのIAM でのセキュリティのベストプラクティスを参照してください。

Application Discovery Service へのフルアクセスの付与

AWSApplicationDiscoveryServiceFullAccess 管理ポリシーは、Application Discovery Service および Migration Hub APIs。

このポリシーがそのアカウントにアタッチされている IAM ユーザーは、Application Discovery Service の設定、エージェントの起動と停止、エージェントレス検出の開始と停止、および AWS Discovery Service データベースからのデータのクエリを行うことができます。このポリシーの詳細については、「AWS の マネージドポリシー AWS Application Discovery Service」を参照してください。

Example AWSApplicationDiscoveryServiceFullAccess ポリシー

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

```
    "Statement": [
        {
            "Action": [
                "mgh:*",
                "discovery:*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "iam:GetRole"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

検出エージェントへのアクセスの許可

AWSApplicationDiscoveryAgentAccess 管理ポリシーは、Application Discovery Service に登録して通信するためのアクセスを Application Discovery Agent に付与します。このポリシーの詳細については、「AWS の マネージドポリシー AWS Application Discovery Service」を参照してください。

このポリシーは、その認証情報が Application Discovery Agent で使用されるすべてのユーザーにアタッチしてください。

このポリシーは、ユーザーに Arsenal へのアクセス権も付与します。Arsenal は、 によって管理およびホストされるエージェントサービスです AWS。Arsenal は、クラウド内で Application Discovery Service にデータを転送します。

Example AWSApplicationDiscoveryAgentAccess ポリシー

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "arsenal:RegisterOnPremisesAgent"
            ],
            "Resource": "*"
```

```
        }
    ]
}
```

エージェントデータ収集のアクセス許可の付与

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy 管理ポリシーにより、 AWS Application Discovery Service は Amazon Data Firehose ストリームを作成して、Application Discovery Service エージェントによって収集されたデータを変換し、 AWS アカウントの Amazon S3 バケットに配信できます。

さらに、このポリシーは、 という新しいデータベースapplication_discovery_service_databaseと、エージェントによって収集されたデータをマッピングするためのテーブルスキーマを持つ AWS Glue Data Catalog を作成します。

このポリシーの使用方法については、「AWS の マネージドポリシー AWS Application Discovery Service」を参照してください。

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"
                }
            }
        }
    ]
}
```

データ探索のアクセス許可の付与

この AWSDiscoveryContinuousExportFirehosePolicy ポリシーは、Amazon Athena でデータ探索を使用するために必要です。これにより、Amazon Data Firehose は Application Discovery Service から収集されたデータを Amazon S3 に書き込むことができます。このポリシーの使用方法については、「AWSApplicationDiscoveryServiceFirehose ロールの作成」を参照してください。

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:*"
            ]
        }
    ]
}
```

Migration Hub コンソールのネットワーク図を使用するためのアクセス許可の付与

Application Discovery Service または Migration Hub へのアクセスを許可または拒否するアイデンティティベースのポリシーを作成するときに AWS Migration Hub コンソールネットワーク図へのアクセスを許可するには、ポリシーに `discovery:GetNetworkConnectionGraph`アクションを追加する必要がある場合があります。

新しいポリシーで `discovery:GetNetworkConnectionGraph`アクションを使用するか、ポリシーに次の条件が当てはまる場合は古いポリシーを更新する必要があります。

- このポリシーは、Application Discovery Service または Migration Hub へのアクセスを許可または拒否します。
- このポリシーは、 `discovery:`*`action-name`*ではなく、 のようなより具体的な検出アクションを使用してアクセス許可を付与しますdiscovery:*。

次の例は、IAM ポリシーで `discovery:GetNetworkConnectionGraph`アクションを使用する方法を示しています。

Example

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

```
        {
            "Effect": "Allow",
            "Action": ["discovery:GetNetworkConnectionGraph"],
            "Resource": "*"
        }
    ]
}
```

Migration Hub ネットワーク図の詳細については、「Migration Hub でのネットワーク接続の表示」を参照してください。

Application Discovery Service 用のサービスリンクロールの使用

AWS Application Discovery Service は AWS Identity and Access Management (IAM) サービスにリンクされたロールを使用します。サービスリンクロールは、Application Discovery Service に直接リンクされた一意のタイプの IAM ロールです。サービスリンクロールは Application Discovery Service によって事前定義されており、サービスがユーザーに代わって AWS の他のサービスを呼び出すために必要となるすべての許可が含まれています。

必要な許可を手動で追加する必要がないため、サービスリンクロールは Application Discovery Service のセットアップを容易にします。サービスリンクロールの許可を定義するのは Application Discovery Service で、別段の定義がない限り、Application Discovery Service のみがその口ールを引き受けることができます。定義される許可には、信頼ポリシーと許可ポリシーが含まれており、その許可ポリシーを他のIAM エンティティにアタッチすることはできません。

サービスリンクロールは、まずその関連リソースを削除しなければ削除できません。このため、リソースにアクセスする許可を不注意に削除することが不可能になり、Application Discovery Service リソースが保護されます。

トピック

- Application Discovery Service 用のサービスリンクロール許可
- Application Discovery Service 用のサービスリンクロールの作成
- Application Discovery Service 用のサービスリンクロールの削除

サービスにリンクされたロールをサポートする他のサービスについては、「IAM と連携するAWS サービス」を参照して、サービスにリンクされたロール列がはいになっているサービスを見つけてください。そのサービスに関するサービスにリンクされたロールのドキュメントを表示するには、リンクが設定されている [はい] を選択します。

Application Discovery Service 用のサービスリンクロール許可

Application Discovery Service では、[] と呼ばれるサービスにリンクされたロールを使用しますAWSServiceRoleForApplicationDiscoveryServiceContinuousExport— へのアクセスを有効にするAWSによって使用または管理されるサービスとリソースAWS Application Discovery Service。

- AWSServiceRoleForApplicationDiscoveryServiceContinuousExport サービスにリンクされたロールは、ロールの引き受けについて以下のサービスを信頼します。

- `continuousexport.discovery.amazonaws.com`

このロール許可ポリシーは、Application Discovery Service が以下のアクションを完了することを許可します。

glue

`CreateDatabase`

`UpdateDatabase`

`CreateTable`

`UpdateTable`

firehose

`CreateDeliveryStream`

`DeleteDeliveryStream`

`DescribeDeliveryStream`

`PutRecord`

`PutRecordBatch`

`UpdateDestination`

s3

`CreateBucket`

`ListBucket`

`GetObject`

ログ

- CreateLogGroup
- CreateLogStream
- PutRetentionPolicy

iam

- PassRole

これは、上記のアクションが適用されるリソースを示す全ポリシーです。

```
{
    "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"
                }
            }
        }
    ]
}
```

サービスにリンクされたロールの作成、編集、削除をIAM エンティティ (ユーザー、グループ、ロールなど) に許可するには、許可を設定する必要があります。詳細については、「IAM ユーザーガイド」の「Service-Linked Role Permissions」(サービスリンクロールのアクセス権限) を参照してください。

Application Discovery Service 用のサービスリンクロールの作成

サービスにリンクされたロールを手動で作成する必要はありません。- AWSServiceRoleForApplicationDiscoveryServiceContinuousExport サービスにリンクされたロールは、a) [Start data viceContinue] を選択した後に [Data Collectors] ページから表示されるダイアログボックスのオプションを確認する、または b) StartContinuousExport を使用する APIAWSCLI。

> **Important**
>
> このサービスリンクロールは、このロールでサポートされている機能を使用する別のサービスでアクションが完了した場合にアカウントに表示されます。詳細については、「IAM アカウントに表示される新しいロール」を参照してください。

Migration Hub コンソールからのサービスリンクロールの作成

Migration Hub コンソールを使用して、AWSServiceRoleForApplicationDiscoveryServiceContinuousExport サービスにリンクされたロール

サービスリンクロールを作成する (コンソール)

1. ナビゲーションペインで、[Data Collectors] (データコレクタ) を選択します。
2. [Agents] (エージェント) タブを選択します。
3. [Data exploration in Athena] (Athena でのデータ探索) スライダーをオンに切り替えます。
4. 前のステップで作成したダイアログボックスで、関連するコストに同意するチェックボックスをオンにして、[Continue (続行)] または [Enable (有効)] を選択します。

からのサービスリンクロールの作成AWS CLI

から Application Discovery Service のコマンドを使用できますAWS Command Line Interfaceを作成するには AWSServiceRoleForApplicationDiscoveryServiceContinuousExportサービスにリンクされたロール

このサービスリンクロールは、AWS CLI から Continuous Export を開始すると、自動的に作成されます (その前に AWS CLI を環境にインストールしておく必要があります)。

AWS CLI から Continuous Export を開始することによってサービスリンクロールを作成する (CLI)

1. オペレーティングシステム (Linux、macOS、または Windows) 用の AWS CLI をインストールします。手順については、AWS Command Line Interface ユーザーガイドを参照してください。
2. コマンドプロンプト (Windows) またはターミナル (Linux/macOS) を開きます。
   a. `aws configure` を入力して、[Enter] を押します。
   b. を入力しますAWSアクセスキー ID とAWSシークレットアクセスキー。
   c. デフォルトのリージョン名として「`us-west-2`」と入力します。
   d. デフォルトの出力形式として「`text`」と入力します。
3. 次のコマンドを入力します。

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

[Discovery Service – Continuous Export] ユースケースでは、IAM コンソールを使用してサービスリンクロールを作成することもできます。IAM CLI または IAM API で、`continuousexport.discovery.amazonaws.com` サービス名でサービスリンクロールを作成します。詳細については、IAM ユーザーガイドの「サービスにリンクされたロールの作成」を参照してください。このサービスリンクロールを削除する場合、この同じプロセスを使用して、もう一度ロールを作成できます。

Application Discovery Service 用のサービスリンクロールの削除

サービスにリンクされたロールが必要な機能またはサービスが不要になった場合には、そのロールを削除することをお勧めします。そうすることで、積極的にモニタリングまたは保守されていない未使用のエンティティを排除できます。ただし、手動で削除する前に、サービスリンクロールをクリーンアップする必要があります。

サービスリンクロールのクリーンアップ

IAM を使用してサービスリンクロールを削除するには、最初にそのロールで使用されているリソースをすべて削除する必要があります。

> **Note**
>
> リソースを削除しようとするときに Application Discovery Service がこのロールを使用している場合、削除が失敗する可能性があります。失敗した場合は、数分待ってから操作を再試行してください。

が使用する Application Discovery Service リソースを削除する AWSServiceRoleForApplicationDiscoveryServiceContinuousExport Migration Hub コンソールからのサービスリンクロール

1. ナビゲーションペインで、[Data Collectors] (データコレクタ) を選択します。
2. [Agents] (エージェント) タブを選択します。
3. [Data exploration in Athena] (Athena でのデータ探索) スライダーをオフに切り替えます。

が使用する Application Discovery Service リソースを削除する AWSServiceRoleForApplicationDiscoveryServiceContinuousExport からのサービスリンクロール AWS CLI

1. オペレーティングシステム (Linux、macOS、または Windows) 用の AWS CLI をインストールします。手順については、AWS Command Line Interface ユーザーガイドを参照してください。
2. コマンドプロンプト (Windows) またはターミナル (Linux/macOS) を開きます。
   a. `aws configure` を入力して、[Enter] を押します。
   b. を入力しますAWSアクセスキー ID とAWSシークレットアクセスキー。
   c. デフォルトのリージョン名として「`us-west-2`」と入力します。
   d. デフォルトの出力形式として「`text`」と入力します。
3. 次のコマンドを入力します。

```
aws discovery stop-continuous-export --export-id <export ID>
```

- 停止する継続的なエクスポートのエクスポート ID がわからない場合は、次のコマンドを入力して継続的なエクスポートの ID を確認します。

```
aws discovery describe-continuous-exports
```

4. 以下のコマンドを入力し、返されるステータスが「INACTIVE」であることを検証して、Continuous Export が停止されたことを確認します。

```
aws discovery describe-continuous-export
```

サービスリンクロールを手動で削除する

を削除できます AWSServiceRoleForApplicationDiscoveryServiceContinuousExport IAM コンソール、IAM CLI、または IAM API を使用したサービスにリンクされたロール このサービスリンクロールを必要とする Discovery Service – Continuous Export 機能を使用する必要がなくなった場合は、そのロールを削除することをお勧めします。そうすることで、積極的にモニタリングまたは保守されていない未使用のエンティティを排除できます。詳細については、IAM ユーザーガイドの「サービスにリンクされたロールの削除」を参照してください。

> **Note**
>
> 削除する前に、まずサービスリンクロールをクリーンアップする必要があります。「サービスリンクロールのクリーンアップ」を参照してください。

AWS Application Discovery Service Identity and Access のトラブルシューティング

以下の情報を使用して、Application Discovery Service と IAM の使用時に発生する可能性がある一般的な問題の診断と修正に役立てます。

トピック

- iam を実行する権限がありません。PassRole

iam を実行する権限がありません。PassRole

iam:PassRole アクションを実行する権限がないというエラーが表示された場合は、ポリシーを更新して Application Discovery Service にロールを渡すことができるようにする必要があります。

一部の AWS のサービス では、新しいサービスロールまたはサービスにリンクされたロールを作成する代わりに、そのサービスに既存のロールを渡すことができます。そのためには、サービスにロールを渡す権限が必要です。

以下のエラー例は、marymajor という名前の IAM ユーザーがコンソールを使用して Application Discovery Service でアクションを実行しようする場合に発生します。ただし、このアクションをサービスが実行するには、サービスロールから付与された権限が必要です。メアリーには、ロールをサービスに渡す許可がありません。

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

この場合、Mary のポリシーを更新してメアリーに iam:PassRole アクションの実行を許可する必要があります。

サポートが必要な場合は、 AWS 管理者にお問い合わせください。サインイン資格情報を提供した担当者が管理者です。

AWS Application Discovery Service での記録とモニタリング

AWS Application Discovery Service は AWS CloudTrail と統合されています。ではを使用できます。CloudTrail トラブルシューティングと監査を目的としたアカウントアクティビティの口ギングと継続的なモニタリングを行い、保持します。 CloudTrail のイベント履歴を記すAWSアカウントアクティビティ (を通じて実行されたアクションを含む) AWSマネジメントコンソール、AWSSDK とコマンドラインツール。このセクションのトピックでは、を使用する方法について説明します。 CloudTrail でApplication Discovery Service

トピック

- AWS CloudTrail を使用した Application Discovery Service API コールのロギング

AWS CloudTrail を使用した Application Discovery Service API コールのロギング

AWS Application Discovery Serviceはと統合されていますAWS CloudTrail、ユーザーやロール、またはAWSApplication Discovery Service サービスのサービス CloudTrail は、Application Discovery Service に対するすべての API コールをイベントとしてキャプチャします キャプチャされたコールには、Application Discovery Service コンソールからのコールと、Application Discovery Service API オペレーションへのコードコールが含まれます。

証跡を作成する場合は、の継続的な配信を有効にすることができます CloudTrail Amazon S3 バケットに対するイベント (Application Discovery Service のイベントなど)。証跡を設定しない場合でも、最新のイベントは CloudTrail コンソールインイベントの履歴。によって収集された情報の使用CloudTrailでは、Application Discovery Service に対してどのようなリクエストが行われたかを判断できます。

詳細を確認するトピック CloudTrail、「」を参照してください。AWS CloudTrailユーザーガイド。

でApplication Discovery Service CloudTrail

CloudTrail で有効になっているAWSアカウント作成時にアカウントを作成してください。Application Discovery Service サービスでアクティビティが発生すると、そのアクティビティは CloudTrail 他のイベントと一緒にAWSのサービスイベントイベントの履歴。AWS アカウントで最近のイベントを表示、検索、ダウンロードできます。詳細については、次を参照してください。でイベントを表示 CloudTrail イベント履歴。

Application Discovery Service のイベントなど、AWS アカウントでのイベントの継続的な記録については、証跡を作成します。あるトレイル可能にする CloudTrail ログファイルを Amazon S3 バケットに配信します。デフォルトでは、コンソールで追跡を作成するときに、追跡がすべての AWS リージョンに適用されます。追跡は、AWSパーティションのすべてのリージョンからのイベントをログに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、その他を設定できます。AWSで収集されたデータをより詳細に分析し、それに基づく対応のためのサービス CloudTrail ログ。詳細については、次を参照してください。

- 追跡を作成するための概要
- CloudTrail でサポートされるサービスと統合
- の Amazon SNS 通知の設定 CloudTrail
- 受信 CloudTrail 複数のリージョンのログファイルそして受信 CloudTrail 複数のアカウントのログファイル

Application Discovery Service アクションはすべてにより ログに記録 CloudTrail そして文書化されていますApplication Discovery Service。たとえば、に対する呼び出しはCreateTags,DescribeTags、およびGetDiscoverySummaryアクションはエントリを生成します CloudTrail ログファイル。

各イベントまたはログエントリには、リクエストの生成者に関する情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます。

- リクエストが、ルート認証情報と AWS Identity and Access Management (IAM) ユーザー認証情報のどちらを使用して送信されたか.
- リクエストがロールまたはフェデレーティッドユーザーのテンポラリなセキュリティ認証情報を使用して行われたかどうか。
- リクエストが、別の AWS のサービスによって送信されたかどうか。

詳細については、「CloudTrail userIdentity 要素」を参照してください。

Application Discovery Service ログファイルエントリについて

追跡は、指定した Amazon S3 バケットにイベントをログファイルとして配信できるようにする設定です。 CloudTrail ログファイルには、1 つ、または複数のログエントリがあります。イベントは、任意のソースからの単一の要求を表し、要求されたアクション、アクションの日時、要求パラメータなどに関する情報が含まれます。 CloudTrail ログファイルは、パブリック API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

以下に、 CloudTrail を示すログエントリDescribeTagsアクション。

```
{
    "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 のクォータ

Service Quotas コンソールには、AWS Application Discovery Service のクォータに関する情報が表示されます。Service Quotas コンソールを使用して、デフォルトのサービスクォータを表示したり、調整可能なクォータのクォータの引き上げをリクエストしたりすることができます。

現在、引き上げ可能なクォータはアカウントあたりのインポート済みサーバー数のみです。

Application Discovery Service には、以下のデフォルトクォータがあります。

- アカウントあたりのアプリケーション数 1,000 個。

  このクォータに到達しているが、新しいアプリケーションをインポートしたいという場合は、`DeleteApplications` API アクションを使用して既存のアプリケーションを削除できます。詳細については、Application Discovery Service API リファレンスの「DeleteApplications」を参照してください。
- 各インポートファイルの最大ファイルサイズ 10 MB。
- アカウントあたりのインポート済みサーバーレコード数 25,000 個。
- 1 日あたりのインポートレコードの削除数 25,000 個。
- アカウントあたりのインポート済みサーバー数 10,000 台 (このクォータは引き上げをリクエストできます)。
- データを収集して Application Discovery Service に送信しているアクティブエージェント数 1,000 個。
- 応答しているがデータは収集していない非アクティブエージェント数 10,000 個。
- アプリケーションあたりのサーバー数 400 台。
- サーバーごとのタグ数 30 個。

トラブルシューティング AWS Application Discovery Service

このセクションでは、 AWS Application Discovery Serviceの一般的な問題の修正方法について説明します。

トピック

データ探索によるデータ収集の停止

データ探索を停止するには、Migration Hub コンソールの「検出 > データコレクター > エージェント」タブでトグルスイッチをオフにするか、 `StopContinuousExport` API を呼び出します。データ収集の停止には最大 30 分かかることがあります。この段階では、コンソールのトグルスイッチと `DescribeContinuousExport` API 呼び出しで、データ探索の状態が「進行中の停止」と表示されます。

> **Note**
>
> コンソールページをリフレッシュした後、切り替えのスイッチがオフにならずエラーメッセージがスローされるか、`DescribeContinuousExport` API が、「Stop_Failed」を返す場合は、再度コンソールでトグルスイッチをオフにするか `StopContinuousExport` API を呼び出します。「データ探索」にエラーが表示され、正常に停止しない場合は、 AWS サポートにお問い合わせください。

または、次の手順で説明されているようにデータ収集を手動で停止できます。

オプション 1: エージェントデータ収集の停止

ADS エージェントを使用した検出がすでに完了していて、ADS データベースリポジトリで追加データをさらに収集しない場合:

1. Migration Hub コンソールから、[Discover] (検出) > [Data Collectors] (データコレクタ) > [Agents] (エージェント) タブの順に選択します。

2. 実行中の既存のすべてのエージェントを選択して、[Stop Data Collection (データ収集の停止)] を選択します。

   これにより、ADS データリポジトリおよび S3 バケットの両方で、エージェントにより、新しいデータが収集されていないことを確認できます。既存のデータには引き続きアクセスできます。

オプション 2: データ探索の Amazon Kinesis Data Streams を削除する

ADS データリポジトリ内のエージェントによるデータ収集を継続したいが、データ探索を使用して Amazon S3 バケット内のデータを収集したくない場合は、データ探索によって作成された Amazon Data Firehose ストリームを手動で削除できます。

1. AWS コンソールから Amazon Kinesis にログインし、ナビゲーションペインから Data Firehose を選択します。
2. データ探索機能によって作成された次のストリームを削除します。

   - `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`

データ探索によって収集されたデータを削除する

データ探索によって収集されたデータを削除するには

1. Amazon S3 に保存されている Discovery Agent データを削除します。

   AWS Application Discovery Service (ADS) によって収集されたデータは、 という名前の S3 バケットに保存されます`aws-application-discover-discovery-service-`*`uniqueid`*。

> **Note**
>
> Amazon Athena でのデータ探索が有効になっている間に Amazon S3 バケットまたはその中のオブジェクトを削除すると、エラーが発生します。 Amazon Athena 新しい検出エージェントデータを S3 に送信し続けます。削除されたデータには、Athena でもアクセスできなくなります。

2. を削除します AWS Glue Data Catalog。

   Amazon Athena でデータ探索を有効にすると、アカウントに Amazon S3 バケットが作成され、ADS エージェントによって収集されたデータが一定の間隔で保存されます。さらに、Amazon Athena から Amazon S3 バケットに保存されているデータをクエリ AWS Glue Data Catalog できる も作成します。 Amazon Athena Amazon Athena でデータ探索をオフにすると、Amazon S3 バケットに新しいデータは保存されませんが、以前に収集されたデータは保持されます。このデータが不要になり、Amazon Athena でのデータ探索がオンになる前にアカウントを 状態に戻す場合。

   a. AWS コンソールから Amazon S3 にアクセスし、aws-application-discover-discovery「-service-uniqueid」という名前のバケットを手動で削除します。

   b. application-discovery-service-database データベースとこれらのすべてのテーブルを削除することで、データ探索 AWS Glue データカタログを手動で削除できます。

      - `os_info_agent`
      - `network_interface_agent`
      - `sys_performance_agent`
      - `processes_agent`
      - `inbound_connection_agent`
      - `outbound_connection_agent`
      - `id_mapping_agent`

からデータを削除する AWS Application Discovery Service

Application Discovery Service からすべてのデータを削除するには、 AWS サポートに連絡して、完全なデータ削除をリクエストしてください。

Amazon Athena でのデータ探索に関する一般的な問題を修正

このセクションでは、Amazon Athena でのデータ探索に関する一般的な問題の修正方法について説明します。

トピック

サービスにリンクされたロールと必要な AWS リソースを作成できないため、Amazon Athena のデータ探索が開始されない

Amazon Athena でデータ探索を有効にすると、Amazon S3 バケット、Amazon Kinesis ストリーム、 など`AWSServiceRoleForApplicationDiscoveryServiceContinuousExport`、エージェントが収集したデータを Amazon Athena でアクセス可能にするために必要な AWS リソースを作成できるサービスにリンクされたロール がアカウントに作成されます AWS Glue Data Catalog。アカウントに Amazon Athena でこのロールを作成するためのデータ探索のための適切なアクセス許可がない場合、初期化は失敗します。「AWS の マネージドポリシー AWS Application Discovery Service」を参照してください。

新しいエージェントデータが Amazon Athena に表示されない

新しいデータが Athena に流れず、エージェントが起動してから 30 分以上経過しており、データ探索ステータスがアクティブである場合は、以下に示すソリューションを確認してください。

- AWS 検出エージェント

  エージェントの [Collection] (収集) ステータスが [Started] (開始済み) になっており、[Health]] （ ヘルス) ステータスが [Running] (実行中) になっていることを確認します。

- Kinesis ロール

  アカウントに `AWSApplicationDiscoveryServiceFirehose` ロールがあることを確認します。

- Firehose のステータス

  次の Firehose 配信ストリームが正しく動作していることを確認します。

  - `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

  `application-discovery-service-database` データベースが にあることを確認します AWS Glue。 AWS Glueに以下のテーブルが存在することを確認します。

  - `os_info_agent`
  - `network_interface_agent`
  - `sys_performance_agent`
  - `processes_agent`
  - `inbound_connection_agent`
  - `outbound_connection_agent`
  - `id_mapping_agent`

- Amazon S3 バケット

  アカウントに `aws-application-discovery-service-`*`uniqueid`* という名前の Amazon S3 バケットがあることを確認します。バケット内のオブジェクトが移動または削除された場合、それらは Athena で適切に表示されません。

- オンプレミスサーバー

  サーバーが実行されていて、エージェントが AWS Application Discovery Serviceにデータを収集して送信できることを確認します。

Amazon S3、Amazon Data Firehose、または にアクセスする権限が不足している AWS Glue

を使用していて AWS Organizations、Amazon Athena でのデータ探索の初期化が失敗した場合、Amazon S3、Amazon Data Firehose、Athena、または にアクセスするアクセス許可がないためである可能性があります AWS Glue。

これらのサービスに対するアクセス権を付与するには、管理者権限を持つ IAM ユーザーが必要です。管理者は、このアクセス権限を付与するために、ユーザーのアカウントを使用できます。AWS の マネージドポリシー AWS Application Discovery Service を参照してください。

Amazon Athena でのデータ探索が正しく機能するように、Amazon S3 バケット、Amazon Athena でデータ探索によって作成された AWS リソースを変更または削除しないでください AWS Glue Data Catalog。これらのリソースを誤って削除または変更してしまった場合は、データ探索を停止して起動すると、これらのリソースが自動的に再作成されます。データ探索によって作成された Amazon S3 バケットを削除すると、バケットで収集されたデータが失われる可能性があります。

失敗したインポートレコードのトラブルシューティング

Migration Hub のインポートを使用すると、Discovery Connector または Discovery Agent を使用せずに、オンプレミス環境の詳細情報を Migration Hub に直接インポートできます。そのため、インポートデータを使用して、直接、移行の評価および計画を行うこともできます。デバイスをアプリケーションとしてグループ化し、それらの移行ステータスを追跡することもできます。

データをインポートする際、エラーが発生する可能性があります。通常、これらのエラーは、次のいずれかの原因により発生します。

- インポート関連のクォータに到達した – インポートタスクに関連付けられたクォータがあります。そのクォータを超えるインポートタスクリクエストを行った場合、そのリクエストは失敗し、エラーが返されます。詳細については、「AWS Application Discovery Service のクォータ」を参照してください。
- 余分なカンマ (,) がインポートファイルに挿入されている – .CSV ファイル内のカンマは、フィールドと後続のフィールドを区別するために使用されます。フィールド内にカンマを入れることはサポートされていません。カンマを入れるとフィールドが分割されます。これが原因で、フォーマットエラーのカスケードが生じることがあります。カンマはフィールド間でのみ使用され、インポートファイルで使用することはできません。

- フィールドにサポート範囲外の値が含まれている – CPU.NumberOfCores など、一部のフィールドにはサポートする値の範囲が必要です。サポートされている範囲よりも多い、または少ない場合、レコードはインポートされません。

インポートリクエストでエラーが発生した場合は、インポートタスクの失敗したレコードをダウンロードしてそれらを解決し、失敗したエントリの CSV ファイルでエラーを解決してから再度インポートします。

Console

失敗したレコードのアーカイブをダウンロードするには

1. にサインインし AWS Management Console、 で Migration Hub コンソールを開きますhttps://console.aws.amazon.com/migrationhub。
2. 左側のナビゲーションペインの [Discover (検出)] で [Tools (ツール)] を選択します。
3. [検出ツール] から、[view imports (インポートの表示)] を選択します。
4. [インポート] ダッシュボードから、[失敗したレコード] をいくつか含むインポートリクエストに関連付けられたラジオボタンを選択します。
5. ダッシュボードのテーブルの上から、[失敗したレコードのダウンロード] を選択します。これにより、アーカイブファイルをダウンロードするためのブラウザのダウンロードダイアログボックスが開きます。

AWS CLI

失敗したレコードのアーカイブをダウンロードするには

1. ターミナルウィンドウを開いて、次のコマンドを入力します。ここで、*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. 出力から、errorsAndFailedEntriesZip で返る値の内容全体をコピーします (引用符で囲まない)。
3. ウェブブラウザを開き、その内容を URL のテキストボックスに貼り付け、ENTER を押します。これにより、失敗したレコードのアーカイブ (.zip 形式で圧縮) がダウンロードされます。

失敗したレコードのアーカイブがダウンロードされました。次に、中の 2 つのファイルを抽出してエラーを修正します。エラーがサービスベースの制限に関連付けられている場合は、制限の引き上げをリクエストするか、アカウントを制限以下にするのに十分な関連リソースを削除する必要があります。アーカイブには次のファイルがあります。

- errors-file.csv – このファイルはエラーログで、失敗した各エントリの失敗した各レコードに関する行、列名、`ExternalId`、および説明的なエラーメッセージを追跡します。
- failed-entries-file.csv – このファイルには、元のインポートファイルからの失敗したエントリのみが含まれます。

発生した non-limit-based エラーを修正するには、 を使用して `failed-entries-file.csv` ファイルの問題`errors-file.csv`を修正し、そのファイルをインポートします。ファイルのインポート手順については、「データのインポート」を参照してください。

AWS Application Discovery Service のドキュメント履歴

ユーザーガイドドキュメントの最新更新:2023 年 5 月 16 日

次の表に、2019 年 1 月 18 Application Discovery Service ユーザーガイドに対する重要な変更点を示します。ドキュメントの更新に関する通知については、RSS フィードにサブスクライブできます。

変更	説明	日付
Agentless Collector データベースと分析データ収集モジュールの紹介	データベースおよび分析データ収集モジュールは、Application Discovery Service エージェントレスコレクター（エージェントレスコレクター）の新しいモジュールです。このデータ収集モジュールを使用して環境に接続し、オンプレミスのデータベースと分析サーバーからメタデータとパフォーマンスメトリックを収集できます。詳細については、「データベースと分析データ収集モジュール」を参照してください。	2023 年 5 月 16 日
Application Discovery Service エージェントレスコレクタの紹介	Application Discovery Service Agentless Collector（エージェントレスコレクター）は、AWS Application Discovery Serviceオンプレミス環境に関する情報をエージェントレス方式で収集する新しいオンプレミスアプリケーションで、への移行を効果的に計画するのに役立ちます。AWS クラウ	2022 年 8 月 16 日

	ド詳細については、「」を参照してください。	
IAM アップデート	ID ベースのポリシーを作成するときに、AWS Identity and Access Management (IAM) `discovery:GetNetworkConnectionGraph` AWS Migration Hub アクションを使用してコンソールのネットワークダイアグラムへのアクセスを許可できるようになりました。詳細については、「ネットワークダイアグラムを使用する権限の付与」を参照してください。	2022 年 5 月 24 日
ホームリージョンの紹介	Migration Hub ホームリージョンは、ポートフォリオ全体に関する検出および移行計画情報の単一リポジトリと、AWS 複数リージョンへの移行の単一ビューを提供します。	2019 年 11 月 20 日
Migration Hub インポート機能の紹介	Migration Hub のインポートでは、サーバーの仕様や使用率データなどのオンプレミスのサーバーおよびアプリケーションに関する情報を Migration Hub にインポートすることができます。このデータを使用して、アプリケーション移行のステータスを追跡することもできます。詳細については、「Migration Hub のインポート」を参照してください。	2019 年 1 月 18 日

以下の表には、2019 年 1 月 18 日より前に行われた Application Discovery Service

変更	説明	日付
新機能	Amazon Athena でのデータ探索をサポートするためにドキュメントを更新し、トラブルシューティングの章を追加しました。	2018 年 8 月 09 日
主な改訂	使用と出力に関する詳細を書き直し、ドキュメント全体を再構成しました。	2018 年 5 月 25 日
検出エージェント 2.0	新しく改善したアプリケーション検出エージェントをリリースしました。	2017 年 10 月 19 日
コンソール	AWS Management Console が追加されました。	2016 年 19 月 12 日
エージェントレス検出	このリリースでは、エージェントレス検出のセットアップおよび設定方法について説明しています。	2016 年 7 月 28 日
Microsoft Windows Server の新しい詳細とコマンド問題の修正	この更新では、Microsoft Windows Server の詳細を追加しています。また、さまざまなコマンド問題の修正について説明しています。	2016 年 5 月 20 日
初版発行	これは Application Discovery Service ユーザーガイドの初回リリースです。	2016 年 12 月 5 日

AWS 用語集

AWS の最新の用語については、「AWS の用語集リファレンス」の「AWS 用語集」を参照してください。

付録

このセクションには、 に関する補足情報が含まれています AWS Application Discovery Service。

トピック

付録: Discovery Connector からエージェントレスコレクターへの移行

このセクションでは、 AWS Agentless Discovery Connector (Discovery Connector) から Application Discovery Service Agentless Collector (Agentless Collector) に移行する方法について説明します。

Discovery Connector を現在使用しているお客様は、新しい Agentless Collector に移行することをお勧めします。

エージェントレスコレクターの使用を開始する方法については、「」を参照してくださいエージェントレスコレクター入門。

エージェントレスコレクターがデプロイされたら、Discovery Connector 仮想マシンを削除できます。以前に収集されたすべてのデータは、引き続き (Migration Hub) で AWS Migration Hub 利用できます。

付録: AWS エージェントレス Discovery Connector

> **Important**
>
> Discovery Connector を現在使用しているお客様は、新しい Agentless Collector に移行することをお勧めします。詳細については、「付録: Discovery Connector からエージェントレスコレクターへの移行」を参照してください。

トピック

- Discovery Connector のデータ収集
- Discovery Connector のトラブルシューティング

Discovery Connector によって収集されたデータ

Discovery Connector は、VMware vCenter Server ホストと VM に関する情報を収集します。ただし、このデータをキャプチャできるのは、VMware vCenter Server ツールがインストールされている場合に限ります。使用している AWS アカウントにこのタスクに必要なアクセス許可があることを確認するには、「」を参照してくださいAWS の マネージドポリシー AWS Application Discovery Service。

以下は、Discovery Connector が収集する情報のリストです。

Discovery Connector が収集するデータの表の凡例:

- 収集されたデータは、特に断らない限り、キロバイト (KB) 単位です。
- Migration Hub コンソール内の同等データはメガバイト (MB) 単位で報告されます。
- アスタリスク (*) で示されるデータフィールドは、コネクタの API エクスポート関数から生成される .csv ファイルでのみ使用できます。
- ポーリング間隔は約 60 分です。
- データフィールドは二重アスタリスク (**) で表され、現在 null 値を返します。

データフィールド	説明
applicationConfigurationId*	VM をグループ化する移行アプリケーションの ID
avgCpuUsagePct	ポーリング間隔中の平均 CPU 使用率
avgDiskBytesReadPerSecond	ポーリング間隔中にディスクから読み取られた平均バイト数
avgDiskBytesWrittenPerSecond	ポーリング間隔中にディスクに書き込まれた平均バイト数
avgDiskReadOpsPerSecond**	1 秒あたりの null の読み取り I/O オペレーションの平均数

データフィールド	説明
avgDiskWriteOpsPerSecond**	1 秒あたりの書き込み I/O オペレーションの平均数
avgFreeRAM	平均空き RAM (MB 単位)
avgNetworkBytesReadPerSecond	1 秒あたりに読み取られたバイトスループットの平均値
avgNetworkBytesWrittenPerSecond	1 秒あたりに書き込まれたバイトスループットの平均値
configId	検出された VM に Application Discovery Service が割り当てた ID
configType	検出したリソースのタイプ
connectorId	Discovery Connector 仮想アプライアンスの ID
cpuType	VM の場合は CPU、ホストの場合は実際のモデル
datacenterId	vCenter の ID
hostId*	VM ホストの ID
hostName	仮想化ソフトウェアを実行しているホストの名前
hypervisor	ハイパーバイザーのタイプ
id	サーバーの ID
lastModifiedTimeタイムスタンプ*	データのエクスポート前の直近にデータを収集した日時
macAddress	VM の MAC アドレス
manufacturer	仮想化ソフトウェアのメーカー

データフィールド	説明
maxCpuUsagePct	ポーリング期間の最大 CPU 使用率
maxDiskBytesReadPerSecond	ポーリング期間のディスクから読み取られた最大バイト数
maxDiskBytesWrittenPerSecond	ポーリング期間のディスクに書き込まれた最大バイト数
maxDiskReadOpsPerSecond**	読み取り I/O オペレーションの最大数 (1 秒あたり)
maxDiskWriteOpsPerSecond**	書き込み I/O オペレーションの最大数 (1 秒あたり)
maxNetworkBytesReadPerSecond	読み取られたバイトスループットの最大値 (1 秒あたり)
maxNetworkBytesWrittenPerSecond	書き込まれたバイトスループットの最大値 (1 秒あたり)
memoryReservation*	VM へのメモリの超過割り当てを避けるための制限
moRefId	vCenter マネージド型オブジェクトの一意のリファレンス ID
name*	VM またはネットワークの名前 (ユーザー指定)
numCores	CPU 内の独立した処理装置の数
numCpus	VM の CPU の数
numDisks**	VM のディスクの数
numNetworkCards**	VM のネットワークカードの数
osName	VM のオペレーティングシステムの名前
osVersion	VM のオペレーティングシステムのバージョン

データフィールド	説明
portGroupId*	VLAN のメンバーポートのグループの ID
portGroupName*	VLAN のメンバーポートのグループの名前
powerState*	電力のステータス
serverId	検出された VM に Application Discovery Service が割り当てた ID
smBiosId*	システム管理 BIOS の ID/バージョン
state*	Discovery Connector 仮想アプライアンスのステータス
toolsStatus	VMware ツールの運用状態 (詳細なリストについては、「データコレクターの表示と並べ替え」を参照)
totalDiskSize	ディスクの合計容量 (MB 単位)
totalRAM	VM で使用可能な RAM の合計量 (MB)
type	ホストのタイプ
vCenterId	VM 固有の ID 番号
vCenterName*	vCenter ホストの名前
virtualSwitchName*	仮想スイッチの名前
vmFolderPath	VM ファイルのディレクトリパス
vmName	仮想マシンの名前

Discovery Connector のデータ収集

Discovery Connector を VMware 環境にデプロイして設定した後、データ収集が停止した場合は再起動できます。データ収集は、コンソールを使用する、または AWS CLI経由で API コールを実行することによって開始または停止できます。以下の手順には、これら両方の手法が説明されています。

Using the Migration Hub Console

以下の手順では、Migration Hub コンソールの [Data Collectors] (データコレクタ) ページで Discovery Connector のデータ収集プロセスを開始または停止する方法を説明します。

データ収集を開始または停止する

1. ナビゲーションペインで、[Data Collectors] (データコレクタ) を選択します。
2. [Connectors (コネクタ)] タブを選択します。
3. 開始または停止するコネクタのチェックボックスをオンにします。
4. [Start data collection (データ収集の開始)] または [Stop data collection (データ収集の停止)] を選択します。

> **Note**
>
> コネクタでデータ収集を開始した後にインベントリ情報が表示されない場合は、コネクタが vCenter Server に登録済みであることを確認します。

Using the AWS CLI

から Discovery Connector データ収集プロセスを開始するには AWS CLI、まず を AWS CLI 環境にインストールしてから、選択した Migration Hub ホームリージョン を使用するように CLI を設定する必要があります。

をインストール AWS CLI してデータ収集を開始するには

1. オペレーティングシステム (Linux、macOS、または Windows) AWS CLI 用の をインストールします。 macOS 手順については、AWS Command Line Interface ユーザーガイドを参照してください。
2. コマンドプロンプト (Windows) またはターミナル (Linux/macOS) を開きます。

   a. `aws configure` を入力して、[Enter] を押します。

b. AWS アクセスキー ID と AWS シークレットアクセスキーを入力します。

c. デフォルトリージョン名のホームリージョンを入力します。例えば us-west-2 です。

d. デフォルトの出力形式として「text」と入力します。

3. データ収集を停止または開始したいコネクタの ID を見つけるには、以下のコマンドを入力してコネクタの ID を表示します。

```
aws discovery describe-agents --filters
 condition=EQUALS,name=hostName,values=connector
```

4. コネクタによるデータ収集を開始するには、以下のコマンドを入力します。

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

> **Note**
>
> コネクタでデータ収集を開始した後にインベントリ情報が表示されない場合は、コネクタが vCenter Server に登録済みであることを確認します。

コネクタによるデータ収集を停止するには、以下のコマンドを入力します。

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

Discovery Connector のトラブルシューティング

このセクションには、Application Discovery Service Discovery Connector の既知の問題のトラブルシューティングに役立つトピックが含まれています。

セットアップ AWS 中に Discovery Connector が に到達できない問題の修正

コンソールで AWS Agentless Discovery Connector を設定すると、次のエラーメッセージが表示されることがあります。

> **到達できませんでした AWS**
>
> AWS に到達できません (接続リセット)。Please verify network and proxy settings。

このエラーは、Discovery Connector がセットアッププロセス中にコネクタが通信する必要がある AWS ドメインへの HTTPS 接続を確立しようとして失敗したために発生します。接続を確立できない場合は、Discovery Connector の設定が失敗します。

への接続を修正するには AWS

1. 会社のファイアウォールが、アウトバウンドアクセスを必要とする AWS ドメインへのポート 443 で送信トラフィックをブロックしているかどうかを IT 管理者に確認してください。

   次の AWS ドメインにはアウトバウンドアクセスが必要です。

   - `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`

   ファイアウォールが送信トラフィックをブロックしている場合は、ブロックを解除します。ファイアウォールを更新したら、コネクタを再設定します。
2. ファイアウォールを更新しても接続問題が解決しない場合は、コネクタ仮想マシンにリストされているドメインへのアウトバウンドネットワーク接続があることを確認してください。仮想マシンにアウトバウンド接続がある場合は、次の例に示すように、ポート 443 で telnet を実行して、リストされたドメインへの接続をテストします。

   ```
   telnet ec2.amazonaws.com 443
   ```
3. 仮想マシンからのアウトバウンド接続が有効になっている場合は、 AWS Support に連絡してさらにトラブルシューティングを行う必要があります。

異常のあるコネクタの修正

各 Discovery Connector のヘルス情報は、Migration Hub コンソールの [Data Collectors] (データコレクタ) ページにあります。[Health (ヘルス)] ステータスが [Unhealthy (異常)] のコネクタを検索すると、問題のあるコネクタを特定できます。次の手順では、コネクタコンソールにアクセスしてヘルスの問題を特定する方法の概要を示します。

コネクタコンソールへのアクセス

1. ウェブブラウザで Migration Hub コンソールを開き、左側のナビゲーションから [Data Collectors] (データコレクタ) を選択します。
2. [Connectors] (コネクタ) タブで、ヘルスステータスが [Unhealthy] (異常) になっている各コネクタの [IP address] (IP アドレス) をメモします。
3. コネクタ仮想マシンに接続できる任意のコンピュータでブラウザを開き、コネクタコンソールの URL、`https://ip_address_of_connector` (`ip_address_of_connector` は、異常のあるコネクタの IP アドレス) を入力します。
4. コネクタの構成時に設定されたコネクタ管理コンソールのパスワードを入力します。

コネクタコンソールにアクセスすると、異常なステータスを解決するためのアクションを実行できます。ここでは、[vCenter connectivity] (vCenter 接続) の [View Info] (情報を表示) を選択することができ、診断メッセージが記載されたダイアログボックスが表示されます。[View Info (情報を表示)] リンクは、バージョン 1.0.3.12 以降のコネクタでのみ使用できます。

ヘルスの問題を修正した後、コネクタは vCenter サーバーとの接続を再確立し、コネクタのステータスが [HEALTHY (正常)] ステータスに変わります。問題が解決しない場合は、 AWS サポートにお問い合わせください。

異常なコネクタの最も一般的な原因は、IP アドレスの問題と認証情報の問題です。以下のセクションは、これらの問題を解決し、コネクタを正常な状態に戻すのに役立ちます。

トピック

- IP アドレスの問題
- 認証情報の問題

IP アドレスの問題

コネクタのセットアップ中に提供された vCenter エンドポイントの形式が正しくないか、無効な場合、または vCenter サーバーが現在ダウンしていて到達不可能な場合、コネクタが異常なステータスになる可能性があります。この場合、vCenter 接続の情報を表示を選択すると、「vCenter サーバーのオペレーションステータスを確認する、または設定の編集を選択して vCenter エンドポイントを更新する」というダイアログボックスが表示されます。

次の手順は、IP アドレスの問題を解決するのに役立ちます。

1. コネクタコンソール (`https://ip_address_of_connector`) から、[Edit Settings (設定の編集)] を選択します。
2. 左側のナビゲーションから、[Step 5: Discovery Connector Set Up] (ステップ 5: Discovery Connector のセットアップ) を選択します。
3. [Configure vCenter credentials (vCenter 認証情報の設定)] で、[vCenter Host (vCenter ホスト)] の IP アドレスをメモします。
4. `ping` または `traceroute` などの個別のコマンドラインツールを使用して、関連付けられた vCenter サーバーがアクティブであり、IP がコネクタ VM から到達可能であることを確認します。

   - IP アドレスが正しくなく、vCenter サービスがアクティブな場合は、コネクタコンソールで IP アドレスを更新し、[Next (次へ)] を選択します。
   - IP アドレスは正しいが、vCenter サーバーが非アクティブの場合は、アクティブにします。
   - IP アドレスが正しく、vCenter サーバーがアクティブな場合は、ファイアウォールの問題により侵入ネットワーク接続がブロックされているかどうかを確認します。ブロックされている場合は、コネクタ VM からの着信接続を許可するようにファイアウォール設定を更新します。

認証情報の問題

コネクタのセットアップ中に提供された vCenter ユーザーの認証情報が無効であるか、vCenter の読み取りおよび表示アカウント権限がない場合、コネクタは異常な状態になる可能性があります。この場合、vCenter 接続の情報を表示を選択すると、「設定の編集を選択して、読み取りおよび表示権限でアカウントの vCenter ユーザー名とパスワードを更新する」というダイアログボックスが表示されます。

次の手順は、認証情報の問題を解決するのに役立ちます。前提条件として、vCenter サーバーでアカウントの読み取り権限と表示権限を持つ vCenter ユーザーを作成していることを確認します。

1. コネクタコンソール (`https://ip_address_of_connector`) から、[Edit Settings (設定の編集)] を選択します。
2. 左側のナビゲーションから、[Step 5: Discovery Connector Set Up] (ステップ 5: Discovery Connector のセットアップ) を選択します。
3. [Configure vCenter credentials (vCenter 認証情報の設定)] で、読み取り権限と表示権限を持つ vCenter ユーザーの認証情報を指定して、[vCenter Username (vCenter ユーザ名)] と [vCenter Password (vCenter パスワード)] を更新します。
4. [Next (次へ)] を選択して設定を完了します。

スタンドアロン ESX ホストのサポート

Discovery Connector はスタンドアロン ESX ホストをサポートしません。ESX ホストは vCenter Server インスタンスの一部であることが必要です。

コネクタの問題に関する追加のサポート

問題が発生し、サポートが必要な場合は、 AWS サポートにお問い合わせください。連絡があり、コネクタログの送信を求められる場合があります。ログを取得するには、次の操作を行います。

- AWS Agentless Discovery Connector コンソールにログインし、ログバンドルのダウンロード を選択します。
- ログバンドルのダウンロードが完了したら、 AWS サポートの指示に従って送信します。

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。