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

とは AWS Application Discovery Service

AWS Application Discovery Service は、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することで、 AWS クラウドへの移行を計画するのに役立ちます。Application Discovery Service は、 AWS Migration Hub および AWS Database Migration Service Fleet Advisor と統合されています。Migration Hub は、移行ステータス情報を 1 つのコンソールに集約するため、移行の追跡を簡素化します。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を表示し、アプリケーションにグループ化して、各アプリケーションの移行ステータスを追跡できます。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。

検出されたデータはすべて AWS Migration Hub ホームリージョンに保存されます。したがって、検出および移行アクティビティを実行する前に、Migration Hub コンソールまたは CLI コマンドで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 AWS Amazon Athena や Amazon QuickSight などの分析ツールで分析用にエクスポートできます。

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、それらのサーバーを実行するコストを計算します AWS。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、検出プロセス AWS Migration Hub を開始する前にホームリージョンを に設定する必要があります。ホームリージョンの操作の詳細については、「ホームリージョン」を参照してください。

Application Discovery Service には、オンプレミスサーバーに関する検出とデータ収集を実行する 3 つの方法があります。

- エージェントレス検出は、VMware vCenter を介して 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) (OVA ファイル) をデプロイすることで実行できます。Agentless Collector を設定すると、vCenter に関連付けられた仮想マシン (VMs) とホストを識別します。Agentless Collector は、サーバーのホスト名、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 VM 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 などのメトリクス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の検出は、各 VMs と物理サーバーに AWS Application Discovery Agent (Discovery Agent) をデプロイすることで実行できます。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。
- ファイルベースのインポートを使用すると、エージェントレスコレクターまたは Discovery Agent を使用せずにオンプレミス環境の詳細を Migration Hub に直接インポートできるため、インポートしたデータから直接移行の評価と計画を実行できます。取り込まれるデータは、提供されたデータによって異なります。

Application Discovery Service は、 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検出ソリューションと統合されています。これらのサードパーティーソリューションは、エージェントレスコレクターや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を Migration Hub に直接インポートするのに役立ちます。サードパーティーのアプリケーション検出ツールは Application Discovery Service AWS をクエリし、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 検出

VMware vCenter 環境で実行されている仮想マシン (VMs) がある場合は、Agentless Collector を使用してシステム情報を収集できます。各 VM にエージェントをインストールする必要はありません。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、使用中のオペレーティングシステムに関係なく、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 VMs の場合、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。各検出ツールが収集するデータの正確なタイプの詳細

については、「」を参照してくださいVMware vCenter Agentless Collector データ収集モジュールの使用。

データベースの検出

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、 Agentless Collector 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。その後、環境内の各コンピュータに Agentless Collector をインストールしなくても、各データベースサーバーのパフォーマンスメトリクスを収集できます。

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インサイトを提供するメタデータとパフォーマンスメトリクス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、ディスク容量の実際の使用率メトリクスを収集します。収集されたメトリクスの詳細については、「」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詳細な分析と移行の計画を行うことができます。例えば、 で最適な移行ターゲットを選択するには AWS クラウド、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。詳細については、「データベースおよび分析データ収集モジュールの使用」を参照してください。

エージェントレスコレクターと検出エージェントを比較する

次の表は、Application Discovery Service がサポートするデータ収集方法の簡単な比較を示しています。

	エージェントレスコレクター	Discovery Agent	Migration Hub テンプレート	RVTools エクスポート
Supported server types				
VMware 仮想マシン	あり	あり	Yes	Yes
物理サーバー	いいえ	はい	Yes	Yes
Deployment				

	エージェントレスコレクター	Discovery Agent	Migration Hub テンプレート	RVTools エクスポート
サーバーごと	いいえ	はい	N/A	No
vCenter ごと	はい	いいえ	N/A	Yes
同じネットワーク上のデータセンターごと	いいえ	いいえ	該当なし	いいえ
Collected data				
サーバープロファイル (静的設定) データ	Yes	Yes	Yes	Yes
Hypervisor からのサーバー使用率メトリクス (CPU、RAM など)	Yes	Yes	Yes	No
サーバーからのサーバー使用率メトリクス (CPU、RAM など)	Yes	Yes	Yes	No
サーバーネットワーク接続 (TCP のみ)	Yes	Yes	No	No
実行中のプロセス	No	Yes	No	No
収集間隔	-60 minutes	-15 seconds	Single snapshot	Single snapshot
Server data use cases				

	エージェントレスコレクター	Discovery Agent	Migration Hub テンプレート	RVTools エクスポート
Migration Hub でサーバーデータを表示する	Yes	Yes	Profile only	No
サーバープロファイルに基づいて Amazon EC2 レコメンデーションを生成する	Yes	Yes	Yes	Yes
使用率データに基づいて Amazon EC2 レコメンデーションを生成する	Yes	Yes	Yes	No
最新の使用率スナップショットデータのエクスポート	Yes	Yes	Yes	No
時系列使用率データのエクスポート	No	Yes	No	No
Network data use cases				
Migration Hub での視覚化	Yes	Yes	No	No
Amazon Athena にエクスポートしてさらに探索する	No	Yes	No	No

	エージェントレスコレクター	Discovery Agent	Migration Hub テンプレート	RVTools エクスポート
CSV ファイルへのエクスポート	No	Yes	No	No
Database use cases				
データベースサーバープロファイル (静的設定) データ	Yes	No	No	No
サポートされているデータベースエンジン	Oracle、SQL Server、MySQL、PostgreSQL	None	None	None
データベーススキーマの複雑さと重複	Yes	No	No	No
データベーススキーマオブジェクト	Yes	No	No	No
Platform support				
サポートされるオペレーティングシステム	VMware Center v5.5 以降のバージョンで実行されている OS	Linux または Windows サーバー	Linux または Windows サーバー	Linux サーバー、Windows サーバー、または VMware v5.5 以降のバージョン

前提

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

- にサインアップしました AWS。詳細については、「Application Discovery Service のセットアップ」を参照してください。
- Migration Hub ホームリージョンを選択しました。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。
- 検出エージェント、コネクタ、インポートは、選択した Migration Hub ホームリージョンでのみ使用できます。
- Application Discovery Service を使用できる AWS 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 のセットアップ

AWS Application Discovery Service を初めて使用する場合は、事前に以下のタスクを完了してください。

Amazon ウェブサービスにサインアップする

IAM ユーザーを作成する

Migration Hub コンソールにサインインしてホームリージョンを選択する

Amazon ウェブサービスにサインアップする

がない場合は AWS アカウント、次の手順を実行して作成します。

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、電話またはテキストメッセージを受け取り、電話キーパッドで検証コードを入力します。

   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。セキュリティベストプラクティスとして、ユーザーに管理アクセス権を割り当て、ルートユーザーアクセスが必要なタスクの実行にはルートユーザーのみを使用するようにしてください。

IAM ユーザーを作成する

AWS アカウントを作成すると、アカウント内のすべての AWS サービスとリソースへの完全なアクセス権を持つ単一のサインイン ID を取得します。この ID は AWS アカウントのルートユーザーと呼ばれます。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 AWS Management Console を使用して にサインインすると、アカウント内のすべての AWS リソースへのフルアクセスが可能になります。

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、セキュリティのベストプラクティス「個々の IAM ユーザーの作成」に従い、 AWS

Identity and Access Management (IAM) 管理者ユーザーを作成します。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

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

- AWS アカウントに管理者ユーザーを作成します。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 管理ポリシー 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. で AWS Management Console、IAM コンソールに移動します。
2. 「IAM ユーザーガイド」のAWS 「アカウントで IAM ユーザーを作成する」の説明に従って、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 ユーザーガイドの手順に従ってください。

- アクセス許可の設定ページのステップで、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 のマネージド 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 管理ポリシー 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 IDs とシークレットアクセスキー) を表示するステップでは、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かつ安全な場所に保存することに関する重要な注意事項のガイダンスに従ってください。

3. ユーザーを作成したら、「プログラムによるユーザーアクセスのサポート」の説明に従って、プログラムによるアクセスを提供します。

Migration Hub コンソールにサインインしてホームリージョンを選択する

に使用している AWS アカウントで AWS Migration Hub 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 アカウントを使用して にサインイン AWS Management Console し、https://console.aws.amazon.com/migrationhub/ で 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 データは、検出、計画、移行追跡の目的でホームリージョンに保存されます。詳細については、「Migration Hub Home Region」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 Application Discovery Agent (Discovery Agent) は、検出と移行の対象となるオンプレミスサーバーと VMs 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**
>
> Discovery Agent 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。エージェントはホームリージョンに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。

- たとえば、 `eu-central-1`がホームリージョンである場合、Application Discovery Service に登録`arsenal-discovery.eu-central-1.amazonaws.com`されます。
- または、必要に応じてホームリージョンを us-west-2 を除く他のすべてのリージョンに置き換えます。
- `us-west-2` がホームリージョンの場合、Application Discovery Service に登録`arsenal.us-west-2.amazonaws.com`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、 でこれらのサーバーを実行するコストを決定 AWS し、移行を計画するのに役立ちます。

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、「Discovery Agent 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。

Discovery Agent によって収集されたデータ

AWS Application Discovery Agent (Discovery Agent) は、オンプレミスサーバーと VMs。Discovery Agent は、システム設定、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、および Transmission Control Protocol (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。
- ポーリング期間は約 15 秒間隔で、15 分 AWS ごとに に送信されます。
- アスタリスク (*) で示されているデータフィールドは、エージェントの API エクスポート関数から生成された`.csv`ファイルでのみ使用できます。

データフィールド	説明
agentAssignedProcessId*	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
agentProvidedTimeStamp*	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

データフィールド	説明
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
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

データフィールド	説明
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
totalCpuUsagePct	ポーリング間隔中のホストの CPU 使用率
totalDiskBytesReadPerSecond (Kbps)	すべてのディスクで 1 秒あたりに読み取られる合計キロビット
totalDiskBytesWrittenPerSecond (Kbps)	すべてのディスクで 1 秒あたりに書き込まれた合計キロビット
totalDiskFreeSize (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
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
totalNumLogicalProcessors*	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
totalNumNetworkCards	サーバーのネットワークカードの合計数

データフィールド	説明
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

Discovery Agent の前提条件

以下は、 AWS Application Discovery Agent (Discovery Agent) を正常にインストールする前に実行する必要がある前提条件とタスクです。

- 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。
- Discovery Agent のインストールに必要なアクセスキーを生成します。
- 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、15 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 の場合`eu-central-1`、 を使用します。 `https://arsenal-discovery.eu-central-1.amazonaws.com:443`
- 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 IAM `AWSApplicationDiscoveryAgentAccess` 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 管理ポリシー 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。

Discovery Agent のインストール

このページでは、Linux および Microsoft Windows に Discovery Agent をインストールする方法について説明します。

Linux に Discovery Agent をインストールする

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 プラットフォームに関する考慮事項」を参照してください。

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

1. 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.region.amazonaws.com/aws-discovery-agent.region/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. にサインイン AWS Management Console し、https://console.aws.amazon.com/migrationhub/ で Migration Hub コンソールを開きます。

      ii. 左側のナビゲーションページの「検出」で、「ツール」を選択します。

      iii. Discovery AWS Agent ボックスで、Download agent を選択し、Download for 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.region.amazonaws.com/aws-discovery-agent.region/linux/latest/aws-discovery-agent.tar.gz.sig
   ```

   ```
   curl -o ./discovery.gpg https://s3.region.amazonaws.com/aws-discovery-agent.region/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、*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、および *aws-secret-access-key* を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 の場合eu-central-1、 を使用します。 https://arsenal-discovery.*eu-central-1*.amazonaws.com:443

古い Linux プラットフォームに関する考慮事項

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は、エージェント更新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旧式暗号化スイートの影響を受ける可能性があります。

Curl

Application Discovery エージェントは、 AWS サーバーとの安全な通信curlに を必要とします。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

以前の Linux システムの認証機関 (CA) バンドルは古いため、安全なインターネット通信が確保できない場合があります。

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
```

Microsoft Windows に Discovery Agent をインストールする

Microsoft 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。

実行方法	手順
	オプションで、LOGANDCONFIGLOCATION を使用してエージェントの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) を上書きすることができます。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。 **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。

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

パッケージ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てください。

```
AWSDiscoveryAgentUpdater.exe /Q
```

Discovery Agent プロセスの管理

このページでは、Linux および Microsoft Windows で Discovery Agent を管理する方法について説明します。

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	コマンド
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

Application Discovery Agent の管理コマンド

タスク	コマンド
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

Application Discovery Agent の管理コマンド

タスク	コマンド
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`

Microsoft Windows で Discovery Agent プロセスを管理する

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 検出エージェント AWS Discovery Updater	Started
エージェントの開始	AWS 検出エージェント AWS Discovery Updater	[Start (開始)] を選択
エージェントの停止	AWS 検出エージェント AWS Discovery Updater	[Stop (停止)] を選択
エージェントの再起動	AWS 検出エージェント AWS Discovery Updater	[Restart (再起動)] を選択

Discovery Agent のアンインストール

このページでは、Linux および Microsoft Windows で Discovery Agent をアンインストールする方法について説明します。

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
```

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

このセクションでは、Microsoft Windows で Discovery Agent をアンインストールする方法について説明します。

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
```

> **Note**
>
> .exe ファイルがサーバーに存在する場合は、次のコマンドを使用してエージェントをサーバーから完全にアンインストールできます。このコマンドを使用してアンインストールする場合、エージェントを再インストールするときに /repairおよび /norestartオプションを使用する必要はありません。

```
.\AWSDiscoveryAgentInstaller.exe /quiet /uninstall
```

Discovery Agent データ収集の開始と停止

Discovery Agent を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。コンソールでデータ収集を開始または停止するには、「」のステップに従うかAWS Migration Hub コンソールでのデータコレクターの起動と停止、「」を使用して API コールを実行します AWS CLI。開始する前に、Discovery Agent の管理に必要なアクセスキーを生成してください。

をインストール AWS CLI 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、OS タイプ (Windows または Mac/Linux) AWS CLI に適した 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 と AWS シークレットアクセスキーを入力します。
   c. デフォルトのリージョン名のホームリージョンを入力します。例: *`us-west-2`*。(この例では、 `us-west-2`がホームリージョン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>
   ```

Discovery Agent のトラブルシューティング

このページでは、Linux および Microsoft Windows での Discovery Agent のトラブルシューティングについて説明します。

Linux での Discovery Agent 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その 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リクエスト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、「Discovery Agent の前提条件」を参照してください。

Microsoft Windows での Discovery Agent のトラブルシューティング

Microsoft Windows で AWS Application Discovery Agent をインストールまたは使用する際に問題が発生した場合は、ログ記録と設定に関する次のガイダンスを参照してください。 は、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に役立つときに、これらのファイルをリクエスト AWS サポート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、「Discovery Agent の前提条件」を参照してください。

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 の数、RAM の量など) 、データベースメタデータ、使用率メトリクス、オンプレミスサーバー間のネットワークトラフィックに関するデータなど、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 にはモジュラーアーキテクチャがあり、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、VMware VMs とデータベースおよび分析サーバーからデータ収集するためのモジュールを提供します。また、オンプレミスサーバー間のネットワークトラフィックに関するデータを収集するためのモジュールも提供します。

Agentless Collector は、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し、オンプレミスサーバー間のネットワークトラフィックに関するデータを収集することで、 AWS Application Discovery Service (Application Discovery Service) のデータ収集をサポートします。

Application Discovery Service は AWS Migration Hub、移行ステータス情報を 1 つのコンソールに集約する際に移行追跡を簡素化するサービスである と統合されています。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 レコメンデーションの取得、ネットワーク接続の視覚化、アプリケーションへのサーバーのグループ化、各アプリケーションの移行ステータスの追跡を行うことができます。

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および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収集したら、 AWS DMS 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。

エージェントレスコレクターの前提条件

Application Discovery Service Agentless Collector (Agentless Collector) 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 AWS アカウント。

- AWS Migration Hub ホームリージョンが設定されている AWS アカウントについては、「」を参照してくださいMigration Hub コンソールにサインインしてホームリージョンを選択する。Migration Hub データは、検出、計画、移行追跡の目的でホームリージョンに保存されます。
- AWS 管理ポリシー を使用するように設定された AWS アカウント IAM ユーザーAWSApplicationDiscoveryAgentlessCollectorAccess。データベースおよび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 2 つのカスタマー管理 IAM ポリシー DMSCollectorPolicyと も使用する必要がありますFleetAdvisorS3Policy。詳細については、「Application Discovery Service エージェントレスコレクターのデプロイ」を参照してください。IAM ユーザーは、Migration Hub ホームリージョンが設定された AWS 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ーは、VMware のすべてのバージョンをサポートしていますが VMware 、現在、バージョン 6.7 および 7.0 に対してテストされています。

- VMware vCenter Server のセットアップでは、システムグループに設定された読み取りアクセス許可と表示アクセス許可を vCenter 認証情報に提供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ーには、TCP ポート 443 経由で複数の AWS ドメインへのアウトバウンドアクセスが必要です。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AWS 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する。
- データベースおよび分析データ収集モジュールを使用するには、Migration Hub ホームリージョンとして AWS リージョン 設定した に Amazon S3 バケットを作成します。データベースおよび分析データ収集モジュールは、インベントリメタデータをこの Amazon S3 バケットに保存します。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。
- エージェントレスコレクターバージョン 2 には、ESXi 6.5 以降のバージョンが必要です。

AWS 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する

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 が必要とする AWS 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。アウトバウンドアクセスが必要な AWS ドメインは、Migration Hub 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かどう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。コレクターは、ホームリージョンが us-west-2 であるため、収集したデータの送信と保存にも使用します。
- `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、利用可能な更新を検出します。
- `public.ecr.aws` – コレクターはこのドメインを使用して更新をダウンロードします。
- `dms.`*`your-migrationhub-home-region`*`.amazonaws.com` – コレクターはこのドメインを使用して AWS DMS 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、データベースおよび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。
- `sts.amazonaws.com` – コレクターはこのドメインを使用して、コレクターが設定されているアカウントを理解します。

AWS アカウントのホームリージョンが でない場合、次のドメインにはアウトバウンドアクセスが必要です**`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` – コレクターはこのドメインを使用して、収集されたデータを送信および保存します。
- `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、利用可能な更新を検出します。
- `public.ecr.aws` – コレクターはこのドメインを使用して更新をダウンロードします。

- dms.*your-migrationhub-home-region*.amazonaws.com – コレクターはこのドメインを使用して AWS DMS 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、データベースおよび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。
- sts.amazonaws.com – コレクターはこのドメインを使用して、コレクターが設定されているアカウントを理解します。

エージェントレスコレクターを設定すると、セットアップが失敗したなどのエラーが表示される場合があります。認証情報を確認してからもう一度試すかAWS 、アクセスできません。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、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 AWS ドメインのいずれかへの HTTPS 接続を確立しようとして失敗したために発生する可能性があります。

への接続を確立 AWS 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 AWS、「」を参照してくださいエージェントレスコレクターがセットアップ AWS 中に到達できない修正。

Application Discovery Service エージェントレスコレクターのデプロイ

Application Discovery Service エージェントレスコレクターをデプロイするには、まず IAM ユーザーを作成し、コレクターをダウンロードする必要があります。このページでは、コレクターをデプロイするための手順について説明します。

エージェントレスコレクターの 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、 で使用した AWS アカウントで (IAM) ユーザーを作成Migration Hub コンソールにサインインしてホームリージョンを選択する AWS Identity and Access Management する必要があります。次に、次の AWS 管理ポリシー AWSApplicationDiscoveryAgentlessCollectorAccess を使用するようにこの IAM ユーザーを設定します。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。

データベースおよび分析データ収集モジュールを使用するには、2 つのカスタマー管理 IAM ポリシーを作成します。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 コードを使用して**DMSCollectorPolicy**ポリシーを作成します。

  JSON

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

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

  JSON

```
{
    "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、 を前提条件ステップで作成した Amazon S3 バケットの名前*bucket_name*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管理者以外の 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、 でホームリージョンの設定に使用した AWS 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てホームリージョンを選択する。
2. 管理者以外の IAM ユーザーを作成するには、「IAM ユーザーガイド」のAWS 「アカウントでの IAM ユーザーの作成」の説明に従って、コンソールでユーザーを作成します。

   IAM ユーザーガイドの手順に従ってください。

   - アクセスのタイプを選択するステップで、プログラムによるアクセスを選択します。推奨されませんが、AWS コンソールへのアクセスに同じ IAM ユーザー認証情報を使用する予定がある場合にのみ、マネジメント AWS コンソールアクセスを選択してください。
   - アクセス許可の設定ページに関するステップで、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AWSApplicationDiscoveryAgentlessCollectorAccess AWS 管理ポリシーを選択します。

     次に、 DMSCollectorPolicyおよびFleetAdvisorS3Policy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 IDs とシークレットアクセスキー) を表示するステップでは、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かつ安全な場所に保存することに関する重要な注意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 で必要になりますエージェントレスコレクターの設定。

     アクセスキーをローテーションすることは、 AWS セキュリティのベストプラクティスです。キーのローテーションの詳細については、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で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。

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 Agentless Collector (Agentless Collector) を設定するには、Agentless Collector Open Virtualization Archive (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について説明し、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。

コレクター OVA ファイルをダウンロードしてチェックサムを検証するには

1. VMware 管理者として vCenter にサインインし、Agentless Collector 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、前のステップでダウンロードしたApplicationDiscoveryServiceAgentlessCollectorファイルを確認します。
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
```

エージェントレスコレクターをデプロイする

Application Discovery Service Agentless Collector (Agentless Collector) 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、VMware 環境でダウンロードした Open Virtualization Archive (OVA) ファイルを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

Agentless Collector version 2

- オペレーティングシステム – Amazon Linux 2023
- RAM – 16 GB
- CPU – 4 コア
- VMware の要件 – VMware で AL2023 を実行するための VMware ホスト要件」を参照してください。

Agentless Collector version 1

- オペレーティングシステム – Amazon Linux 2
- RAM – 16 GB
- CPU – 4 コア

次の手順では、Agentless Collector OVA ファイルを VMware 環境にデプロイする手順を示します。

エージェントレスコレクター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. OVA ファイルをインストールするには、次のいずれかの方法を使用します。
   - UI を使用する: ファイルを選択し、OVF テンプレートのデプロイを選択し、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。サーバー管理ダッシュボードのプロキシ設定が正しく設定されていることを確認します。
   - コマンドラインを使用する: コマンドラインからコレクター OVA ファイルを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/'
     ```

     以下に、この例で*******値を示します。

     - 名前は、Agentless Collector VM に使用する名前です。
     - 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、ダウンロードしたコレクター OVA ファイルの名前です。
     - ユーザー名/パスワードは vCenter 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 でデプロイされた Agentless Collector を見つけます。VM を右クリックし、Power、Power On を選択します。
4. 数分後、コレクターの 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ーに接続します。

Agentless Collector コンソールへのアクセス

次の手順では、Application Discovery Service Agentless Collector (Agentless Collector) コンソールにアクセスする方法について説明します。

Agentless Collector コンソールにアクセスするには

1. ウェブブラウザを開き、アドレスバーに次の URL を入力します: **https://***<ip_address>***/**。*<ip_address>* は からのコレクターの IP アドレスですエージェントレスコレクターをデプロイする。
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の開始方法を選択します。その後、ログインするよう求められます。

Agentless Collector コンソールに初めてアクセスする場合は、次は になりますエージェントレスコレクターの設定。それ以外の場合は、次に が表示されますエージェントレスコレクターダッシュボード。

エージェントレスコレクターの設定

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ーの設定ページでコレクター VM を設定するには

1. コレクター名に、コレクターが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。
2. データ同期で、 AWS アカウント IAM ユーザーの AWS アクセスキーとシークレットキーを入力して、コレクターによって検出されたデータを受信する送信先アカウントとして を指定します。IAM ユーザーの要件については、「」を参照してくださいApplication Discovery Service エージェントレスコレクターのデプロイ。

a. AWS access-key には、送信先 AWS 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. AWS secret-key には、送信先 AWS アカウントとして指定するアカウント 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) ネットワークが にアクセスするためにプロキシを使用する必要がある場合は AWS、プロキシホスト、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ーのパスワードで、エージェントレスコレクターへのアクセスを認証するため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 (@$!#%*?&)
- パスワードには、@$!#%*?& 以外の特殊文字を含めることはできません。

a. エージェントレスコレクターのパスワードには、コレクター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。

b. エージェントレスコレクターのパスワードを再入力するには、検証のためにパスワードを再度入力します。

4. その他の設定で、ライセンス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オンにします。

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を選択します。このチェックボックスをオンにしない場合は、「」の説明に従って Agentless Collector を手動で更新する必要がありますApplication Discovery Service エージェントレスコレクターの手動更新。

6. 設定の保存 を選択します。

以下のトピックでは、オプションのコレクター設定タスクについて説明します。

オプションの設定タスク

- (オプション) Agentless Collector VM の静的 IP アドレスを設定する
- (オプション) エージェントレスコレクター VM を DHCP を使用して にリセットする
- (オプション) Kerberos 認証プロトコルを設定する

(オプション) Agentless Collector VM の静的 IP アドレスを設定する

次の手順では、Application Discovery Service Agentless Collector (Agentless Collector) VM の静的 IP アドレスを設定する方法について説明します。初めてインストールすると、コレクター VM は Dynamic Host Configuration Protocol (DHCP) を使用するように設定されます。

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

Agentless Collector version 2

コレクター VM の静的 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。
   - 静的 IP アドレス – サブネット内の署名なし IP アドレス。たとえば、192.168.1.138 です。
   - CIDR ネットマスク – CIDR ネットマスクを取得するには、コレクター VM をホストする VMware vCenter ホストの IP アドレス設定を確認します。たとえば、/24 です。
   - デフォルトゲートウェイ – デフォルトゲートウェイを取得するには、コレクター VM をホストする VMware vCenter ホストの IP アドレス設定を確認します。たとえば、192.168.1.1 です。
   - プライマリ DNS – プライマリ DNS を取得するには、コレクター VM をホストする VMware vCenter ホストの IP アドレス設定を確認します。たとえば、192.168.1.1 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 – これにより、コレクターはドメイン名なしで vCenter ホスト URL に到達できます。

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. 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イスを無効にします。

```
sudo ip link set ens192 down
```

4. 次の手順を使用してインターフェイス設定を更新します。

   a. 次のコマンドを使用して、vi エディタで 10-cloud-init-ens192.network を開きます。

   ```
   sudo vi /etc/systemd/network/10-cloud-init-ens192.network
   ```

   b. 次の例に示すように、ネットワーク情報収集ステップで収集した情報を使用して値を更新します。

   ```
   [Match]
   Name=ens192

   [Network]
   DHCP=no
   Address=static-ip-value/CIDR-netmask
   Gateway=gateway-value
   DNS=dnsserver-value
   ```

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 で `resolv.conf` 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 の `resolv.conf` 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、編集されたresolv.conf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. 次のコマンドを入力して、ネットワークインターフェイスを有効にします。

```
sudo ip link set ens192 up
```

7. 次の例に示すように、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ます。

```
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ります。

```
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 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 できることを確認します。

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

Agentless Collector version 1

コレクター VM の静的 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。
   - 静的 IP アドレス – サブネット内の署名なし IP アドレス。たとえば、192.168.1.138 です。
   - ネットワークマスク – ネットワークマスクを取得するには、コレクター VM をホストする VMware vCenter ホストの IP アドレス設定を確認します。たとえば、255.255.255.0 です。
   - デフォルトゲートウェイ – デフォルトゲートウェイを取得するには、コレクター VM をホストする VMware vCenter ホストの IP アドレス設定を確認します。たとえば、192.168.1.1 です。
   - プライマリ DNS – プライマリ DNS を取得するには、コレクター VM をホストする VMware vCenter ホストの IP アドレス設定を確認します。たとえば、192.168.1.1 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 – これにより、コレクターはドメイン名なしで vCenter ホスト URL に到達できます。
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. 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イスを無効にします。

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

4. 次の手順を使用して、インターフェイス eth0 設定を更新します。

   a. 次のコマンドを使用して、vi エディタで ifcfg-eth0 を開きます。

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

b. 次の例に示すように、ネットワーク情報収集ステップで収集した情報を使用してインターフェイス値を更新します。

```
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 で resolv.conf 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 の resolv.conf 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、編集されたresolv.conf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. 次のコマンドを入力して、ネットワークインターフェイスを有効にします。

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

7. 次の例に示すように、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ます。

   ```
   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ります。

   ```
   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 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 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ー VM を DHCP を使用して にリセットする

次の手順では、DHCP を使用するように Agentless Collector VM を再設定する方法について説明します。

Agentless Collector version 2

DHCP を使用するようにコレクター 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実行して、ネットワークインターフェイスを無効にします。

```
sudo ip link set ens192 down
```

2. 次の手順を使用してインターフェイス設定を更新します。

   a. 次のコマンドを使用して、vi エディタで 10-cloud-init-ens192.network ファイルを開きます。

```
sudo vi /etc/systemd/network/10-cloud-init-ens192.network
```

   b. 次の例に示すように、値を更新します。

```
[Match]
Name=ens192

[Network]
DHCP=yes

[DHCP]
ClientIdentifier=mac
```

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イスを有効にします。

```
sudo ip link set ens192 up
```

5. 次の例に示すように、コレクター VM を再起動します。

```
sudo reboot
```

Agentless Collector version 1

DHCP を使用するようにコレクター 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実行して、ネットワークインターフェイスを無効にします。

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

2. 次の手順を使用して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 エディタで ifcfg-eth0 ファイルを開きます。

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

   b. 次の例に示すように、 ifcfg-eth0 ファイルの値を更新します。

```
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イスを有効にします。

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

5. 次の例に示すように、コレクター 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する

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は、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ー VM を設定する必要があります。

次の手順では、Application Discovery Service Agentless Collector VM 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。

コレクター VM で Kerberos 認証プロトコルを設定するには

1. 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
```

2. /etc フォルダでkrb5.conf設定ファイルを開きます。以下のコード例を使用してこれを行うことができます。

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

3. 次の情報を使用してkrb5.conf設定ファイルを更新します。

```
[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. 次の例に示すように、コレクター VM を再起動します。

```
sudo reboot
```

エージェントレスコレクターネットワークデータ収集モジュールの使用

ネットワークデータ収集モジュールを使用すると、オンプレミスデータセンター内のサーバー間の依存関係を検出できます。このネットワークデータは、アプリケーションがサーバー間で通信する方法を可視化することで、移行計画を加速します。

ネットワークデータ収集モジュールは、VMware vCenter モジュールが識別するサーバーに接続し、それらのサーバーの送信元 IP から送信先 IP/ポートトラフィックを分析します。

トピック

- ネットワークデータ収集モジュールのセットアップ
- ネットワークデータ収集の試行
- Network Data Collection モジュールのサーバーステータス

ネットワークデータ収集モジュールのセットアップ

Network Data Collection モジュールは、VMware vCenter モジュールから取得されるサーバーインベントリのネットワークデータを収集します。したがって、ネットワークデータ収集モジュールを使用するには、まず VMware vCenter モジュールを設定します。手順については、以下のトピックのガイダンスに従ってください。

1. the section called “コレクターのデプロイ”
2. the section called “コレクターコンソールへのアクセス”
3. the section called “コレクターの設定”
4. the section called “VMware データ収集モジュールの使用”

ネットワーク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ーダッシュボードのネットワークデータ収集セクションで、ネットワーク接続の表示を選択します。
2. ネットワーク接続ページで、コレクターの編集を選択します。
3. 認証情報セクションに、認証情報のセットを少なくとも 1 つ入力します。最大 10 セットの認証情報を入力できます。モジュールがサーバーのデータ収集を初めて試みるときは、機能する認証情報のセットが見つかるまですべての認証情報を試行します。その後、そのセットを保存し、その後の試行で再度使用します。認証情報の設定については、「」を参照してくださいthe section called “認証情報の設定”。
4. データ収集設定セクションで、サーバーの再起動時にデータ収集を自動的に開始するには、データ収集を自動的に開始を選択します。
5. WinRM 証明書を設定していない場合は、WinRM 証明書チェックを無効にするを選択します。
6. [保存] を選択します。
7. 収集は 15 秒ごとにサーバーで行われます。特定のサーバーのコレクション試行の詳細を表示するには、サーバーテーブルでサーバーの左側にあるチェックボックスをオンにします。

認証情報の設定

ネットワークデータ収集モジュールは、WinRM を使用して Windows サーバーからデータを収集します。SNMPv2 と SNMPv3 を使用して Linux サーバーからデータを収集します。

WinRM 認証情報：

- 以下を持つ Windows アカウントのユーザー名とパスワードを指定します。
  - `\root\standardcimv2` 名前空間への読み取りアクセス
  - `MSFT_NetTCPConnection` クラスの読み取りアクセス許可
  - リモート WMI アクセス
- 最小限のアクセス許可で専用サービスアカウントを作成することをお勧めします。
- ドメイン管理者アカウントまたはローカル管理者アカウントを使用しないでください。
- ポート 5986 (HTTPS) は、コレクターサーバーとターゲットサーバーの間で開いている必要があります。

- WinRM 証明書チェックを無効にしないでください。WinRM 証明書の設定については、「」を参照してくださいthe section called “WinRM 証明書を設定する際の自己署名証明書の問題に対処する”。

SNMPv2 認証情報：

- 1.3.6.1.2.1.6.13.* にアクセスできる読み取り専用コミュニティ文字列を指定します。 OID
- SNMPv3 のセキュリティが向上するため、SNMPv2SNMPv32 よりも優先されます。
- ポート 161/UDP はコレクターサーバーとターゲットサーバーの間で開いている必要があります
- デフォルト以外の複雑なコミュニティ文字列を使用する
- 「パブリック」や「プライベート」などの一般的な文字列を避ける
- コミュニティ文字列をパスワードとして扱う

SNMPv3 認証情報

- 1.3.6.1.2.1.6.13.* にアクセスできる読み取り専用アクセス許可を持つユーザー名/パスワードと認証/プライバシーの詳細を指定します。 OID。
- ポート 161/UDP はコレクターサーバーとターゲットサーバーの間で開いている必要があります
- 認証とプライバシーの両方を有効にする
- 強力な認証プロトコルを使用する (MD5 よりも SHA が推奨)
- 強力な暗号化プロトコルを使用する (DES よりも AES が優先)
- 認証とプライバシーの両方に複雑なパスワードを使用する
- 一意のユーザー名を使用する (共通名は避ける)

認証情報管理の一般的なベストプラクティス

- 認証情報を安全に保存する
- すべての認証情報を定期的に更新する
- パスワードマネージャーまたは安全なボールトを使用する
- 認証情報の使用状況をモニタリングする
- 最小特権の原則に従い、必要な最小限のアクセス許可のみを付与する

ネットワークデータ収集の試行

新しいサーバーが検出されると、コレクターは IP アドレスごとに設定された各認証情報を試行します。コレクターは有効な認証情報を見つけた後、その認証情報のみを使用します。2 回連続して障害が発生すると、コレクターは 30 分、2 時間、8 時間、24 時間後にサーバーのネットワークデータの収集を試みます。試行が 6 回失敗すると、コレクターは設定されたすべての認証情報を毎日 1 回試行し続けます。この問題を解決するには、現在の認証情報を編集するか、コレクターの編集を選択して追加の認証情報を追加するか、モニタリング対象のターゲットサーバーを変更します。

Network Data Collection モジュールのサーバーステータス

次の表に、コレクションのステータス値を示します。

ステータス	意味
収集または収集	ネットワーク接続の最後の収集試行は成功しました。
エラーまたはエラー	ネットワーク接続の最後の収集試行が、ネットワークまたはアクセス許可の問題により失敗しました。詳細については、エラーのあるサーバーの左側にあるチェックボックスをオンにします。
スキップ済み	有効な認証情報が指定されていないサーバー。追加のサーバー認証情報を更新または設定します。
データなし	サーバーのデータ収集が開始されていません。データ収集を開始するには、コレクターの開始を選択します。
保留中	収集は開始されましたが、収集の試行は行われていません。数分待ってから、リストを更新します。

VMware vCenter Agentless Collector データ収集モジュールの使用

このセクションでは、Application Discovery Service Agentless Collector (Agentless Collector) VMware vCenter データ収集モジュールについて説明します。このモジュールは、VMware VMs 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ます。

トピック

VMware vCenter 用の Agentless Collector データ収集モジュールのセットアップ

このセクションでは、Agentless Collector VMware vCenter データ収集モジュールを設定して、VMware VMs 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および表示アクセス許可を vCenter 認証情報に提供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設定するには

1. 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 セクションで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 認証情報の下：
        i. vCenter URL/IP の場合は、VMware vCenter Server ホストの IP アドレスを入力します。

ii. vCenter ユーザー名には、コレクターが 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. データ収集設定の下：

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

c. [設定] 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 データ収集の詳細の表示

VMware データ収集の詳細ページには、 で設定した vCenter の詳細が表示されますVMware vCenter 用の Agentless Collector データ収集モジュールのセットアップ。

検出された vCenter サーバーの下に、セットアップした vCenter が vCenter に関する次の情報とともに一覧表示されます。

- vCenter サーバーの IP アドレス。
- vCenter 内のサーバーの数。
- データ収集のステータス。
- 前回の更新からの期間。

vCenter サーバーの削除 を選択して表示された vCenter サーバーを削除し、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を停止に変わります。

収集ステータス列に収集と表示されている場合、データ収集が開始されています。

収集されたデータは AWS Migration Hub コンソールで表示します。VMware vCenter サーバーインベントリのデータを収集する場合は、データ収集をオンにしてから約 15 分後に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 でサーバーの表示を選択して 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 コンソールにアクセスする方法については、「」を参照してください収集されたデータの表示。

以下は、移行計画アクティビティに従って推奨されるデータ収集期間に関するガイドラインです。

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

vCenter データ収集の範囲の制御

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 のすべてのホストと仮想マシンをインベントリ対象にするか、ケースバイケースで許可を付与することができます。

> **Note**
>
> セキュリティの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アクセス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 Client 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、アクセス許可を選択します。
3. vCenter ユーザーを選択し、ユーザーロールを追加、編集、削除する記号を選択します。
4. ロールメニューから読み取り専用を選択します。
5. 子に伝播を選択し、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。

特定の 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] を選択してください。

> **Note**
>
> [Propagate to children] を選択した場合でも引き続き、ケースバイケースで、ESX ホストと VM から読み取り専用アクセス許可を削除することができます。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。

Agentless Collector 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 Agentless Collector (Agentless Collector) 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 Agentless Collector データ収集モジュールのセットアップ。

Agentless Collector VMware vCenter が収集したデータのテーブル凡例：

- 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 (*) で示されているデータフィールドは、Application Discovery Service API エクスポート関数から生成された .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ーは、 CLI AWS を使用したデータエクスポートをサポートします。AWS CLI を使用して収集され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「Export Collected Data」ページの「Export System Performance Data for All Servers」に記載されている手順に従ってください。
- 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	ポーリング期間における 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 オペレーションの平均数 null。

データフィールド	説明
avgDiskWriteOpsPerSecond**	1 秒あたりの書き込み I/O オペレーションの平均数。
avgFreeRAM	平均空き RAM は MB で表されます。
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。
computerManufacturer	ESXi ホストによって報告されるベンダー。
computerModel	ESXi ホストによって報告されるコンピュータモデル。
configId	Application Discovery Service によって検出された VM に割り当てられた 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	VM 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。
lastModifiedTimeStamp*	データエクスポート前のデータ収集の最新の日時。

データフィールド	説明
macAddress	VM の MAC アドレス。
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 オペレーションの最大数。
maxDiskWriteOpsPerSecond**	1 秒あたりの書き込み I/O オペレーションの最大数。
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バイトの最大スループット。
memoryReservation*	VM のメモリが過剰にコミットされないように制限します。
moRefId	一意の vCenter マネージド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。

データフィールド	説明
numDisks**	VM 上のディスクの数。
numNetworkCards**	VM 上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名。
osVersion	VM のオペレーティングシステムのバージョン。
portGroupId*	VLAN のメンバーポートのグループの ID。
portGroupName*	VLAN のメンバーポートのグループの名前。
powerState*	電源のステータス。
serverId	Application Discovery Service が、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 ツールの運用状態
totalDiskFreeSize	MB で表される空きディスク容量。vCenter Server 7.0 以降のバージョンで使用できます。
totalDiskSize	MB で表されるディスクの合計容量。
totalRAM	VM で使用可能な RAM の合計量を MB 単位で表します。
type	ホストのタイプ。
vCenterId	VM の一意の ID 番号。
vCenterName*	vCenter ホストの名前。
virtualSwitchName*	仮想スイッチの名前。

データフィールド	説明
vmFolderPath	VM ファイルのディレクトリパス。
vmName	仮想マシンの名前。

データベースおよび分析データ収集モジュールの使用

このセクションでは、データベースおよび分析データ収集モジュールをセットアップ、設定、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クスを収集できます。このモジュールで収集できるメトリクスについては、「」を参照してくださいAgentless Collector データベースおよび分析データ収集モジュールによって収集されたデータ。

> **Important**
>
> サポート終了通知: 2026 年 5 月 20 日、 AWS は AWS Database Migration Service Fleet Advisor のサポートを終了します。2026 年 5 月 20 日以降、Fleet AWS DMS Advisor コンソールまたは AWS DMS Fleet Advisor リソースにアクセスできなくなります。詳細については、AWS DMS 「Fleet Advisor のサポート終了」を参照してください。

大まかに言うと、データベースおよび分析データ収集モジュールを使用する場合は、次の手順を実行します。

1. 前提条件のステップを完了し、IAM ユーザーを設定し、データコレクターを作成します AWS DMS 。
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クスを 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 サーバーを手動で追加するか、 を使用しますVMware データ収集モジュールの使用。
4. OS サーバーへの接続認証情報を設定し、それらを使用してデータベースサーバーを検出します。
5. データベースサーバー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のデータ収集」を参照してください。

6. コンソールで収集したデータを表示 AWS DMS し、それを使用して への移行のターゲットレコメンデーションを生成します AWS クラウド。詳細については、「データベースと分析のデータ収集」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 サーバーの追加
- データベースサーバーの検出
- Agentless Collector データベースおよび分析データ収集モジュールによって収集されたデータ

サポートされている OS、データベース、分析サーバー

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、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ています。

- Amazon Linux 2
- CentOS Linux バージョン 6 以降
- Debian バージョン 10 以降
- Red Hat Enterprise Linux バージョン 7 以降
- SUSE Linux Enterprise Server バージョン 12 以降
- Ubuntu バージョン 16.01 以降
- Windows Server 2012 以降
- Windows XP 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、次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 から 2019
- MySQL バージョン 5.6 から 8

- Oracle バージョン 11g リリース 2 から 12c、19c、21c
- PostgreSQL バージョン 9.6 から 13

AWS DMS データコレクターの作成

データベースおよび分析データ収集モジュールは、 AWS DMS データコレクターを使用して AWS DMS コンソールを操作します。収集されたデータを AWS DMS コンソールで表示することも、それを使用して適切なサイズの AWS ターゲットエンジンを決定することもできます。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。

AWS DMS 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 S3 バケットへのアクセスに使用する IAM ロールを作成します。の前提条件を完了したときに、この Amazon S3 バケットを作成しましたエージェントレスコレクターの前提条件。

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

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/iam/ で IAM コンソールを開きます。
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. [信頼されたエンティティを選択] ページの [信頼されたエンティティタイプ] では、AWS [サービス] を選択します。他のサービスのユースケースでは AWS 、DMS を選択します。
4. [DMS] チェックボックスをオンにして、[次へ] をクリックします。
5. アクセス許可の追加ページで、前に作成した FleetAdvisorS3Policy を選択します。[次へ] を選択します。
6. [名前、確認、および作成] ページで、[ロール名] に **`FleetAdvisorS3Role`** と入力して、[ロールの作成] をクリックします。
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 をエディタに貼り付け、既存のコードを置き換えます。

   JSON

```
{
```

```
 "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] を選択してください。

次に、 AWS DMS コンソールで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. にサインイン AWS Management Console し、https://console.aws.amazon.com/dms/v2/ で AWS DMS コンソールを開きます。
2. Migration Hub ホームリージョンとして AWS リージョン 設定した 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する」を参照してください。
3. ナビゲーションペインで、[検出] の下にある [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. [一般的な設定] セクションの [名前] にデータコレクター名を入力します。
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 ロールの場合は、以前に作成した `FleetAdvisorS3Role` 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

必要な AWS リソースを作成したら、データベースおよび分析データ収集モジュールから AWS DMS 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ーコンソールを開きます。詳細については、「コレクターコンソールへのアクセス」を参照してください。
2. データベースと分析コレクターの表示を選択します。
3. ダッシュボードページで、「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. AWS リージョン、IAM アクセスキー ID、IAM シークレットアクセスキーの場合、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する」および「コレクターのデプロイ」を参照してください。
5. Connected DMS データコレクターで、 AWS DMS コンソールで作成したデータコレクターを選択します。
6. [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 へのアクセスと S3 へのアクセスのための
接続が表示されていることを確認します。

LDAP サーバーと OS サーバーの追加

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。Lightweight Directory Access Protocol (LDAP) は、オープン標準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して、IP ネットワーク経由で分散ディレクトリ情報サービスにアクセスして維持できます。

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ーコンソールを開きます。詳細については、「コレクターコンソールへのアクセス」を参照してください。
2. データベースと分析コレクターの表示を選択し、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. Hostname には、LDAP サーバーのホスト名を入力します。
5. ポートには、LDAP リクエストに使用されるポート番号を入力します。
6. ユーザー名 に、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 には、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) 接続の検証を選択して、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 サーバー接続認証情報を検証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、Discover OS サーバーを選択します。

> **Important**
>
> OS 検出の場合、データ収集モジュールには、ドメインサーバーが LDAP プロトコルを使用してリクエストを実行するため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すると、検出された OS サーバーのリストを表示するには、OS サーバーの表示を選択します。

または、OS サーバーを手動で追加するか、カンマ区切り値 (CSV) ファイルからサーバーのリストをインポートすることもできます。また、VMware vCenter Agentless Collector データ収集モジュールを使用して OS サーバー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の使用」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コレクターページで、ナビゲーションペインの Discovery 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 タイプで、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 には、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. ポートには、リモートクエリに使用され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 に、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 には、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. 検証 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 サーバーを追加します。

a. CSV から OS サーバーの一括インポートを選択します。

b. テンプレートのダウンロードを選択して、カスタマイズできる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、CSV ファイルで OS サーバー接続認証情報を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後、CSV ファイルを保存します。

d. 参照を選択し、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の検出

このセクションでは、オペレーティングシステムとデータベースサーバーを設定するために必要な手順について説明します。次に、サーバーを検出し、データベースまたは分析サーバーを手動で追加するオプションがあります。

データベース検出では、データ収集モジュールに必要な最小限のアクセス許可を持つソースデータベースのユーザーを作成する必要があります。詳細については、「 AWS DMS ユーザーガイドAWS DMS 」の「Fleet Advisor のデータベースユーザーの作成」を参照してください。

セットアップの設定

以前に追加された 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。このページ

では、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ようにするために必要な手順の概要を説明します。また、データベースサーバーでリモート認証を有効にし、データ収集モジュールにアクセス許可を付与します。

Linux でのセットアップを設定する

Linux でデータベースサーバーを検出するように設定するには、次の手順を実行します。

データベースサーバーを検出するように Linux を設定するには

1. ss および netstat 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、 ssおよび netstat コマンドへの sudo アクセスを許可します。

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

   前の例では、 を OS サーバー接続認証情報で指定した Linux ユーザーの名前*username*に置き換えます。

   前の例では、 ssおよび netstat コマンドへの/usr/bin/パスを使用します。このパスは環境によって異なる場合があります。ss および netstat コマンドへのパスを確認するには、which ssおよび which netstat コマンドを実行します。
2. リモート SSH スクリプトの実行と Internet Control Message Protocol (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。

Microsoft Windows でのセットアップを設定する

Microsoft Windows でデータベースサーバーを検出するように設定するには、次の手順を実行します。

データベースサーバーを検出するように Microsoft Windows を設定するには

1. Windows Management Instrumentation (WMI) クエリと WMI クエリ言語 (WQL) クエリを実行し、レジストリを読み取るための許可を持つ認証情報を提供します。
2. OS サーバー接続認証情報で指定した 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、イベントログリーダーのグループに追加します。これを行うには、以下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
```

前の例では、 を OS サーバー接続認証情報で指定した Windows ユーザーの名前*username*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 ユーザーに必要なアクセス許可を付与します。
   - Windows の管理プロパティと計測プロパティで、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 Control では、、、、および WMI名前空間の Execute Methods、Enable Account、Remote EnableStandartCimv2、および Read Security CIMV2 DEFAULTアクセス許可を選択します。
   - WMI プラグインの場合は、 を実行しwinrm configsddl default、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
```

データベースサーバーの検出

コンソールでデータベースサーバーを検出して追加するには、次の一連のタスクを実行します。

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コレクターページで、ナビゲーションペインの Discovery 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で接続の検証を選択します。
3. 接続ステータスが Failed のサーバーの場合は、接続認証情報を編集します。
   a. 同一の認証情報を持つサーバーを 1 つまたは複数選択し、アクションメニューで編集を選択します。OS サーバーの編集ページが開きます。
   b. ポートには、リモートクエリに使用され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. ユーザー名には、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 には、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. 接続の検証を選択して、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の表示を選択して、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を表示できます。

または、データベースサーバーと分析サーバーを手動でインベントリに追加することもできます。また、CSV ファイルからサーバーのリストをインポートすることもできます。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既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で、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、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 には、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、サーバーが実行されるポートを入力します。

d. 認証タイプで、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. ユーザー名には、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. パスワードには、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. 検証 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の一括インポートを選択します。

b. テンプレートのダウンロードを選択して、カスタマイズできる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、データベースサーバー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、CSV ファイルでデータベースまたは分析サーバーの接続認証情報を提供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サーバーと分析サーバーの認証情報を追加した後、CSV ファイルを保存します。

d. 参照を選択し、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、インベントリに追加します。データベースおよび分析データ収集モジュールは、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クスを収集できます。

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するには

1. データベースと分析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クスを収集するデータベースサーバー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メトリクス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のデータ収集」を参照してください。

Agentless Collector データベースおよび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 Agentless Collector (Agentless Collector) データベースおよび分析データ収集モジュールは、データ環境から次のメトリクスを収集します。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および分析データ収集モジュールの使用。

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、次のメトリクスがキャプチャされます。

- OS サーバーの使用可能なメモリ
- OS サーバー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 数
- スキーマの数
- ストアドプロシージャ数
- テーブルの数

- トリガー数
- ビュー数
- スキーマ構造

AWS DMS コンソールでスキーマ分析を起動すると、データ収集モジュールは次のメトリクスを分析して表示します。

- データベースサポート日
- コードの行数
- 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、リソース使用率を収集すると、次のメトリクスがキャプチャされます。

- 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 (IOPS)
- OS サーバーが使用する CPU の数
- OS サーバーのメモリ使用状況
- OS サーバーのストレージ使用状況

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クスを収集できます。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。

収集されたデータの表示

> **Important**
>
> サポート終了通知: 2026 年 5 月 20 日、 AWS は AWS Database Migration Service Fleet Advisor のサポートを終了します。2026 年 5 月 20 日以降、Fleet AWS DMS Advisor コンソールまたは AWS DMS Fleet Advisor リソースにアクセスできなくなります。詳細については、AWS DMS 「Fleet Advisor のサポート終了」を参照してください。

「」の手順に従って、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 Migration Hub コンソールで収集したデータを表示できますAWS Migration Hub コンソールでのサーバーの表示。

次の手順を実行して、データベースサーバーと分析サーバーの収集されたメトリクスを AWS DMS コンソールで表示することもできます。

AWS DMS コンソールでデータベースおよび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. にサインイン AWS Management Console し、https://console.aws.amazon.com/dms/v2/ で AWS DMS コンソールを開きます。
2. 検出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. インベントリを分析する を選択して、類似性や複雑さなどのデータベーススキーマプロパティを決定します。
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、将来の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、「Fleet Advisor で AWS DMS インベントリを分析に使用する」を参照してください。

エージェントレスコレクターへのアクセス

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) 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ーダッシュボード
- エージェントレスコレクター設定の編集
- VMware vCenter 認証情報の編集

エージェントレスコレクターダッシュボード

Application Discovery Service Agentless Collector (Agentless Collector) ダッシュボードページで、コレクターのステータスを表示し、次のトピックで説明するようにデータ収集方法を選択できます。

トピック

コレクターのステータス

コレクターのステータスは、コレクターに関するステータス情報を提供します。コレクター名、AWS へのコレクターの接続ステータス、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、Agentless Collector の設定を編集する必要がある場合があります。

コレクター設定を編集するには、コレクター設定の編集を選択し、「」で説明されている手順に従いますエージェントレスコレクター設定の編集。

データ収集

データ収集では、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 VMsからのデータ収集、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をサポートしています。今後のモジュールは、追加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をサポートします。

トピック

VMware vCenter データ収集

VMware VMs からサーバーのインベントリ、プロファイル、使用率データを収集するには、vCenter サーバーへの接続を設定します。接続を設定するには、VMware vCenter セクションでセットアップを選択し、「」で説明されている手順に従いますVMware vCenter Agentless Collector データ収集モジュールの使用。

vCenter データ収集を設定したら、ダッシュボードから以下を実行できます。

- データ収集ステータスの表示
- データ収集を開始する。

- データ収集の停止

> **Note**
>
> ダッシュボードページで、vCenter データ収集を設定すると、VMware vCenter セクションの設定ボタンがデータ収集ステータス情報、データ収集停止ボタン、表示および編集ボタンに置き換えられます。

データベースと分析のデータ収集

データベースおよび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のキャパシティ

データ収集モジュールは、データベースおよび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。この収集された情報を使用して、 AWS DMS コンソールでターゲットのレコメンデーションを計算できます。ソースデータベースが過剰プロビジョニングまたは過小プロビジョニングされている場合、ターゲットレコメンデーションも過剰プロビジョニングまたは過小プロビジョニングされます。

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の情報に加えて、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クスを収集します。このモードは、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レコメンデーションを提供します。このモードでは、データ収集モジュールは 1 分ごとにパフォーマンスメトリクスを収集します。

データベースサーバー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クス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で、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クスを収集するデータベースサーバーと分析サーバーを選択します。
3. データ収集の実行 を選択します。データ収集タイプのダイアログボックスが開きます。

4. 分析のため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、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。データ収集の期間に [Next 7 days] を選択したり、1～60 日の範囲の [カスタム範囲] を設定したりできます。
5. データ収集の実行 を選択します。データ収集ページが開きます。
6. コレクションヘルスタブを選択すると、データ収集のステータスが表示されます。

データ収集が完了すると、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。その後、「」の説明に従って、この収集されたデータを表示できます収集されたデータの表示。

エージェントレスコレクター設定の編集

「」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) を初めてセットアップしたときにコレクターを設定しましたエージェントレスコレクターの設定。次の手順では、エージェントレスコレクターの設定を編集する方法について説明します。

コレクター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、以下を実行します。

  a. コレクター名に、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. 検出データの送信先 AWS アカウントで、コレクターによって検出されたデータを受信する送信先アカウントとして指定する AWS アカウントの AWS 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Application Discovery Service エージェントレスコレクターのデプロイ。

     i. AWS access-key には、送信先 AWS 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。

     ii. AWS secret-key には、送信先 AWS アカウントとして指定するアカウント 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ーのパスワードで、エージェントレスコレクター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ーのパスワードには、エージェントレスコレクター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. エージェントレスコレクターのパスワードを再入力するには、検証のためにパスワードを再度入力します。

d. 設定の保存 を選択します。

次に、 が表示されますエージェントレスコレクターダッシュボード。

VMware vCenter 認証情報の編集

VMware VMs からサーバーのインベントリ、プロファイル、使用率データを収集するには、vCenter サーバー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VMware vCenter Agentless Collector データ収集モジュールの使用。

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た読み取りおよび表示アクセス許可で vCenter 認証情報を提供できることを確認してください。

VMware vCenter 認証情報を編集するには

VMware データ収集の詳細の表示 ページで、vCenter サーバー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 認証情報の下：

     i. vCenter URL/IP の場合は、VMware vCenter Server 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. [保存] を選択します。

Application Discovery Service 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) を設定するときに、「」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エージェントレスコレクターの設定。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、前の Agentless Collector OVA ファイルを削除することをお勧めします。
3. 「」のステップに従いますエージェントレスコレクターをデプロイする。

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 AL2 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を更新する」の手順に従います。

カーネルライブパッチ

Agentless Collector version 2

エージェントレスコレクターバージョン 2 仮想マシンは、「」で説明されているように Amazon Linux 2023 を使用しますエージェントレスコレクターをデプロイする。

Amazon Linux 2023 のライブパッチを有効にして使用するには、「Amazon EC2 ユーザーガイド」のAL2023 でのカーネルライブパッチ」を参照してください。

Agentless Collector version 1

エージェントレスコレクターバージョン 1 仮想マシンは、「」で説明されているように Amazon Linux 2 を使用しますエージェントレスコレクターをデプロイする。

Amazon Linux 2 のライブパッチを有効にして使用するには、「Amazon EC2 ユーザーガイド」のAL2 でのカーネルライブパッチ」を参照してください。

Agentless Collector バージョン 1 からバージョン 2 にアップグレードするには

1. 最新のイメージを使用して、新しい Agentless Collector OVA をインストールします。
2. 認証情報を設定します。
3. 古い仮想アプライアンスを削除します。

エージェントレスコレクターのトラブルシューティング

このセクションでは、Application Discovery Service Agentless Collector (Agentless Collector) 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について説明します。

トピック

- 修正 Unable to retrieve manifest or certificate file error
- WinRM 証明書を設定する際の自己署名証明書の問題に対処する
- エージェントレスコレクターがセットアップ AWS 中に到達できない修正
- プロキシホストへの接続時の自己署名証明書の問題の修正
- 異常なコレクターの検索
- IP アドレスの問題の修正
- vCenter 認証情報の問題の修正
- データベースおよび分析データ収集モジュールのデータ転送の問題の修正
- データベースおよび分析データ収集モジュールの接続の問題の修正
- 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ーの問題 AWS のサポートへのお問い合わせ

修正 Unable to retrieve manifest or certificate file error

VMware vCenter UI の Amazon S3 URL から OVA をデプロイしようとしたときにこのエラーが表示された場合は、vCenter サーバーが次の要件を満たしていることを確認してください。

- VMware vCenter Server バージョン 8.0 更新 1 以降
- VMware vCenter Server 7.0 Update 3q (ISO ビルド 23788036) 以降

WinRM 証明書を設定する際の自己署名証明書の問題に対処する

WinRM 証明書チェックを有効にすると、自己署名認証機関を Agentless Collector にインポートする必要がある場合があります。

自己署名認証機関をインポートするには

1. VMware vCenter でコレクターの VM ウェブコンソールを開き、次の例collectorに示すようにパスワードec2-userを使用して としてサインインします。

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

2. WinRM 証明書の署名に使用されるすべての自己署名 CA 証明書がディレクトリ にあることを確認します/etc/pki/ca-trust/source/anchors。例:

```
/etc/pki/ca-trust/source/anchors/https-winrm-ca-1.pem
```

3. 新しい証明書をインストールするには、次のコマンドを実行します。

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

4. 次のコマンドを実行して Agentless Collector を再起動します。

```
sudo shutdown -r now
```

5. (オプション) 証明書が正常にインポートされたことを確認するには、次のコマンドを実行します。

```
sudo trust list --filter=ca-anchors | less
```

エージェントレスコレクターがセットアップ AWS 中に到達できない修正

エージェントレスコレクターには、TCP ポート 443 経由で複数の AWS ドメインへのアウトバウンドアクセスが必要です。コンソールで Agentless Collector 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。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セットアッププロセス中にコレクター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、エージェントレスコレクターの設定は失敗します。

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 でのアウトバウンド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。アウトバウンドアクセスが必要な AWS 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かどう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 でない場合、次のドメインにはアウトバウンドアクセスが必要です**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`

ファイアウォールが Agentless Collector が通信する必要がある AWS ドメインへのアウトバウンドアクセスをブロックしている場合は、コレクター設定の「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、次のステップを使用して、コレクター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があることを確認します。

   a. VMware vCenter から Agentless Collector の IP アドレスを取得します。

   b. 次の例**collector**に示すように、コレクターの VM ウェブコンソールを開き、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
   ```

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

3. telnet がドメインを解決できない場合は、Amazon Linux 2 の手順を使用して静的 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、さらなるサポートについては、「」を参照してくださいエージェントレスコレクターの問題 AWS のサポートへのお問い合わせ。

プロキシホストへの接続時の自己署名証明書の問題の修正

オプションで提供されるプロキシとの通信が HTTPS 経由であり、プロキシに自己署名証明書がある場合は、証明書を提供する必要がある場合があります。

1. VMware vCenter から Agentless Collector の IP アドレスを取得します。

2. コレクターの VM ウェブコンソールを開き、次の例collectorに示すようにパスワードec2-userを使用して としてサインインします。

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

3. -----BEGIN CERTIFICATE----- と の両方を含む、セキュアプロキシに関連付けられている証明書の本文-----END CERTIFICATE-----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、次のコマンドを実行します。

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

5. 次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
```

異常なコレクターの検索

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「注意が必要」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の問題を特定する方法について説明します。

Agentless Collector コンソールにアクセスするには

1. AWS アカウントを使用して にサインイン AWS Management Console し、https://console.aws.amazon.com/migrationhub/ で Migration Hub コンソールを開きます。
2. Discover の Migration Hub コンソールナビゲーションペインで、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で、ステータスが「注意が必要」の各コネクタの IP アドレスを書き留めます。
4. エージェントレスコレクターコンソールを開くには、ウェブブラウザを開きます。次に、アドレスバーに次の URL を入力します: **https://***<ip_address>***/**。ip_address は異常なコレクターの IP アドレスです。
5. ログインを選択し、 でコレクターが設定されたときに設定された Agentless Collector パスワードを入力しますエージェントレスコレクターの設定。
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 セクションで表示と編集を選択します。

7. の手順に従って VMware vCenter 認証情報の編集 URL と認証情報を修正します。

ヘルスの問題を修正すると、コレクターは vCenter サーバーとの接続を再確立し、コレクターのステータスは収集状態に変更されます。問題が解決しない場合は、「」を参照してくださいエージェントレスコレクターの問題 AWS のサポートへのお問い合わせ。

異常なコレクターの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 アドレスの問題の修正と vCenter 認証情報の問題の修正は、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 アドレスの問題の修正

コレクター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、無効であるか、vCenter サーバーが現在ダウンしていて到達できない場合、コレクターは異常な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。

コレクターの IP アドレスの問題を修正するには

1. VMware vCenter から Agentless Collector の IP アドレスを取得します。
2. ウェブブラウザを開いて Agentless Collector コンソールを開き、アドレスバーに次の URL を入力します: **`https://`***`<ip_address>`***`/`**。ip_address は からのコレクターの IP アドレスですエージェントレスコレクターをデプロイする。
3. ログインを選択し、 でコレクターが設定されたときに設定された Agentless Collector パスワードを入力しますエージェントレスコレクターの設定。
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 セクションで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 サーバー」で、vCenter 列の IP アドレスを書き留めます。
6. `ping` や などの別のコマンドラインツールを使用して`traceroute`、関連付けられた vCenter サーバーがアクティブで、コレクター 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である場合は、コレクターコンソールで 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、コレクター VM からの受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。

vCenter 認証情報の問題の修正

コレクター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 の読み取りおよび表示アカウント権限がない場合、コレクターは異常な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 の読み取りおよび表示アクセス許可が設定されていることを確認します。

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。

データベースおよび分析データ収集モジュールのデータ転送の問題の修正

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 へのアクセスと S3 へのアクセスにアクセスできない場合は、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ことを確認してください。次に、DMSCollectorPolicy 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、「Application Discovery Service エージェントレスコレクターのデプロイ」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、次のドメインへのアウトバウンドアクセスを提供します。

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

データベースおよび分析データ収集モジュールの接続の問題の修正

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。これらのデータベースサーバーから、

データ収集モジュールは容量とパフォーマンスのメトリクスを収集します。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ます。

次の例では、*#######*値を自分の値に置き換えます。

- 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、次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
  ```

  Windows で管理者として前の例を実行します。

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

  Linux で前の例を実行します。

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

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

  Windows で管理者として前の例を実行します。

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

  Linux で前の例を実行します。

- 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、次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
```

データベースサーバーと分析サーバーに接続できない場合は、必要なアクセス許可を必ず指定してください。詳細については、「データベースサーバーの検出」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ーは、スタンドアロン 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。

エージェントレスコレクターの問題 AWS のサポートへのお問い合わせ

Application Discovery Service Agentless Collector (Agentless Collector) に問題が発生し、ヘルプが必要な場合は、 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ログを取得するには

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 ウェブコンソールを開き、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. ログフォルダに移動するには、次のコマンドを使用します。

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

4. 次のコマンドを使用してログファイルを圧縮します。

```
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ー 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 ファイルを AWS エンタープライズサポートに渡します。

Migration Hub へのデータのインポート

AWS Migration Hub (Migration Hub) インポートを使用すると、Application Discovery Service Agentless Collector (Agentless Collector) または AWS Application Discovery Agent (Discovery Agent) を使用せずに、オンプレミス環境の詳細を Migration Hub に直接インポートできるため、インポートしたデータから直接移行評価と計画を実行できます。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。

このページでは、インポートリクエストを完了する手順について説明します。まず、次の 2 つのオプションのいずれかを使用してオンプレミスサーバーデータを準備します。

- 一般的なサードパーティーツールを使用して、オンプレミスサーバーデータを含むファイルを生成します。
- 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、オンプレミスサーバーデータを入力します。

前述の 2 つの方法のいずれかを使用してオンプレミスデータファイルを作成したら、Migration Hub コンソール AWS CLI、または SDK のいずれか AWS を使用してファイルを Migration Hub にアップロードします。 SDKs 2 つのオプションの詳細については、「」を参照してくださいthe section called “サポートされているインポート形式”。

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。

エラーの処理: 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 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形式

Migration Hub は、次のインポート形式をサポートしています。

- RVTools
- Migration Hub インポートテンプレート

RVTools

Migration Hub は、RVTools を介した VMware vSphere のエクスポートのインポートをサポートしています。RVTools からデータを保存するときは、まずすべての を csv にエクスポート オプションを選択するか、すべての を Excel にエクスポート オプションを選択し、次にフォルダを圧縮して、ZIP ファイルを Migration Hub にインポートします。ZIP では、次のファイルが必要です: vInfo、vNetwork、vCpu、vMemory、vDisk、vPartition、vSource、vTools、vHost、vNic、vSC_VMK。

Migration Hub インポートテンプレート

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、それが必須フィールドであることを示します。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。

次の表のインポートファイル名の横にあるキャレット (^) は、serverId が指定されている場合、読み取り専用であることを示します。

> **Note**
>
> VMware.MoRefId または VMWare.VCenterId を使用してレコードを識別している場合は、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。たとえば、[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
VMware.MoRefId*^	マネージド型オブジェクトのリファレンス ID。VMware.VCenterId で指定する必要があります。	
VMware.VCenterId*^	仮想マシンの一意の ID。VMware.MoRefId で指定する必要があります。	
CPU.NumberOfProcessors^	CPU の数。	4
CPU.NumberOfCores^	物理コアの合計数。	8

インポートフィールド名	説明	例
CPU.NumberOfLogicalCores^	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。	リナックス 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
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
CPU.UsagePct.Avg^	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

インポートフィールド名	説明	例
CPU.UsagePct.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
DiskReadsPerSecondInKB.Max^	1 秒あたりのディスク読み取りの最大数 (KB)。	37892 869962
DiskWritesPerSecondInKB.Max^	1 秒あたりのディスク書き込みの最大数 (KB)。	18436 1808
DiskReadsOpsPerSecond.Avg^	1 秒あたりのディスク読み取り操作の平均回数。	45 28
DiskWritesOpsPerSecond.Avg^	1 秒あたりのディスク書き込み 操作の平均回数。	8 3
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

インポートフィールド名	説明	例
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"
ApplicationWave	このサーバーの移行ウェーブ。	
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"
serverId	Migration Hub サーバーリストに表示されるサーバー識別子。	`d-server-01kk9i6ywwaxmp`

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一致ロジック」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。

インポート許可の設定

データをインポートする前に、IAM ユーザーにインポートファイルを Amazon S3 にアップロード (`s3:PutObject`) し、オブジェクトを読み取るために必要な Amazon S3 アクセス許可があることを確認してください ()`s3:GetObject`。また、IAM ポリシーを作成し、 AWS アカウントでインポートを実行する IAM ユーザーにアタッチして、プログラムによるアクセス (の場合 AWS CLI) またはコンソールアクセスを確立する必要があります。

Console Permissions

次の手順を使用して、 コンソールを使用して AWS アカウントでインポートリクエストを行う IAM ユーザーのアクセス許可ポリシーを編集します。

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. にサインイン AWS Management Console し、https://console.aws.amazon.com/iam/ で IAM コンソールを開きます。
2. ナビゲーションペインで [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。

JSON

```
{
  "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. [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] (ポリシーの作成) を選択します。

6. アカウント AWS でインポートリクエストを行うユーザーのアクセス許可を付与する IAM コンソールページに戻ります。

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. [次へ: レビュー] を選択します。
9. [Add permissions] 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、 を使用してデータインポートリクエストを行うアクセス許可を IAM ユーザーに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、次のアクセス許可を持つ 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。

   JSON

```
{
  "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. `aws iam create-policy` AWS CLI コマンドを使用して、次のアクセス許可を持つ追加の IAM ポリシーを作成します。

   JSON

```
{
    "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. `aws iam attach-user-policy` AWS CLI コマンドを使用して、 を使用してアカウントでインポートリクエストを実行する IAM ユーザーに、前の 2 つのステップで作成したポリシーをアタッチします AWS AWS CLI。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「attach-user-policy」を参照してください。

ポリシーを IAM ユーザーに追加したので、インポートプロセスを開始する準備が整いました。

IAM ユーザーが指定した 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、ユーザーがオブジェクトを読み取れるように、設定されたオブジェクトのデフォルトのアクセス許可を残す必要があることに注意してください。

インポートファイルを Amazon S3 にアップロードする

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. にサインイン AWS Management Console し、https://console.aws.amazon.com/s3/ で Amazon S3 コンソールを開きます。
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. [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 [オープン] を選択します。
6. [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. 「」の説明に従って、Migration Hub コンソールのインポートページに移動します データのインポート。次に、Amazon Amazon S3を貼り付けます。

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、次の結果が返されます。

```
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。これは、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。

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、既存のオンプレミスサーバーデータを入力すると、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、 コンソールを使用するか、 を使用して API コールを実行するという 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. インポートページを開くには、インポートボックスでインポートを選択します。
4. インポート名で、インポートの名前を指定します。
5. Amazon S3 オブジェクト URL フィールドに入力します。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、「インポートファイルを Amazon S3 にアップロードする」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。名前列にリストされているインポートの名前を選択してインポート (インポート履歴) ページから移動すると、サーバーページに移動し、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ーが適用されます。次に、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

からデータインポートプロセスを開始するには AWS CLI、まず を環境にインストール AWS CLI 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 インポートリクエストのステータスは、 コンソール AWS CLI、またはいずれかの AWS SDKs を使用して追跡できます。

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

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

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と探索

Application Discovery Service Agentless Collector (Agentless Collector) と AWS Discovery Agent (Discovery Agent) の両方が、平均使用率とピーク使用率に基づいて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、総保有コスト (TCO) の概要を実行できます。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 Agentless Collector と Discovery Agent によって検出されたデータを表示して操作する方法について説明します 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
- Amazon Athena でのデータの探索

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 Agentless Collector (Agentless Collector) と AWS Discovery Agent (Discovery Agent) の両方について、データ収集プロセスの開始後、コンソールを使用してサーバーと VMs に関して収集された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 コールを行い、収集され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。

検出されたサーバーに関する収集データをコンソールに表示するには、「」の手順に従いますAWS Migration Hub コンソールでのサーバーの表示。コンソールを使用して エージェントレスコレクターまたは検出エージェントによって検出されたサーバーを表示、ソート、タグ付けする方法の詳細については、「」を参照してくださいAWS Migration Hub コンソールを使用したデータの検出。

Agentless Collector データベースおよび分析データ収集モジュールは、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。このバケットのデータは、DMS AWS コンソールで表示できます。検出された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データを表示するには、「」の手順に従います収集されたデータの表示。

検出されたサーバーとアプリケーションの一致ロジック

AWS Application Discovery Service (Application Discovery Service) には、検出したサーバー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。

このマッチングロジックは、 (Migration Hub) インポート、Application Discovery Service Agentless Collector (Agentless Collector)、 AWS Application Discovery Agent (Discovery Agent)、その他の移行ツールなど AWS Migration Hub 、複数のソースからの重複サーバーを処理します。Migration Hub のインポートの詳細については、「Migration Hub Import」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。

フィールドの一致

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.MoRefId と VMware.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。

Amazon Athena でのデータの探索

Amazon Athena のデータ探索では、Discovery Agent によって検出され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 か所で分析できます。Amazon Athena でのデータ探索が Migration Hub コンソールから (または StartContinousExport API を使用して) 有効にされ、エージェントのデータ収集がオンになると、エージェントによって収集されたデータは定期的に S3 バケットに自動的に保存されます。詳細については、「Amazon Athena でのデータの探索」を参照してください。

Amazon Athena のデータ探索では、検出エージェントによって検出され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 か所で分析できます。Amazon Athena でのデータ探索が Migration Hub コンソールから (または StartContinousExport API を使用して) 有効にされ、エージェントのデータ収集がオンになると、エージェントによって収集されたデータは定期的に S3 バケットに自動的に保存されます。

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 データベースを Amazon QuickSight と統合して、クエリ出力を視覚化し、追加の分析を実行することもできます。

このセクションのトピックでは、Athena でデータを使用してローカル環境の移行を評価し、計画する方法について説明します AWS。

Amazon Athena でデータ探索を有効にする

Amazon Athena のデータ探索は、Migration Hub コンソールまたは からの API コールを使用して継続的エクスポートを有効にすることで有効になります AWS CLI。Amazon Athena で検出されたデータを表示して探索を開始する前に、データ探索を有効にする必要があります。

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 のサービスにリンクされたロールのアクセス許可」を参照してください。

次の手順は、コンソールと を使用して Amazon Athena でデータ探索を有効にする方法を示しています AWS CLI。

Turn on with the console

Amazon Athena のデータ探索は、Migration Hub コンソールの Data Collectors ページで「データ収集を開始する」を選択するか、Amazon Athena でのデータ探索」というラベルのトグルをクリックすると、継続的エクスポートが暗黙的に有効になります。

コンソールから Amazon Athena でデータ探索を有効にするには

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 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で有効になります AWS CLI。これを行うには、まず を環境にインストール AWS CLI する必要があります。

Amazon Athena で をインストール AWS CLI してデータ探索を有効にするには

1. オペレーティングシステム (Linux、macOS、または Windows) AWS CLI に 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. 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 でのデータの直接調査

Amazon Athena でデータ探索を有効にすると、Athena でデータを直接クエリすることで、エージェントによって検出された詳細な現在のデータの探索と操作を開始できます。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。

次の手順では、Athena コンソールでエージェントデータを直接探索する方法について説明します。Athena にデータがない場合、または Amazon Athena でデータ探索を有効にしていない場合は、「」で説明されているように、Amazon Athena でデータ探索を有効にするダイアログボックスが表示されますAmazon Athena でデータ探索を有効にする。

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 コンソールで、ナビゲーションペインの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、「Amazon Athena での事前定義されたクエリの使用」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 QuickSight などの視覚化プログラム、または Cytoscape、yEd、Gelphi などのオープンソースの視覚化ツールにクエリを移植できます。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。

QuickSight を使用して Amazon Athena データを視覚化するには

1. Amazon QuickSight にサインインします。
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. [データソースを作成] を選択します。
6. [Choose your table (テーブルの選択)] ダイアログボックスで、[Agents-servers-os] テーブルを選択して、[Select (選択)] を選択します。
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。

Amazon Athena での事前定義されたクエリの使用

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 コンソールで、ナビゲーションペインで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。

サーバーの IP アドレスとホスト名を取得する

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特定する

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ーのパフォーマンスデータを分析する

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する

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インバウンド通信を追跡する

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
```

ポート番号から実行中のソフトウェアを特定する

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 Migration Hub コンソールを使用したデータの検出

AWS Application Discovery Service (Application Discovery Service) は AWS Migration Hub (Migration Hub) と統合されており、お客様は Migration Hub 内のデータコレクター、サーバー、アプリケーションを表示および管理できます。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、 コンソールを使用して Application Discovery Service Agentless Collector (Agentless Collector) と AWS Application Discovery Agent (Discovery Agent) を管理およびモニタリングする方法について説明します。

トピック

AWS Migration Hub コンソールダッシュボードでのデータの表示

メインダッシュボードを表示するには、 (Migration Hub) コンソールの AWS Migration Hub ナビゲーションペインからダッシュボードを選択します。Migration Hub メインダッシュボードでは、Application Discovery Service Agentless Collector (Agentless Collector) や Application Discovery Agent (Discovery Agent) などのサーバー、 AWS アプリケーション、データコレクターに関する高レベルの統計を表示できます。

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、Migration Hub コンソールのホームページの左側にあるナビゲーションペインからダッシュボードを選択します。

AWS Migration Hub コンソールでのデータコレクターの起動と停止

Application Discovery Service Agentless Collector (Agentless Collector) と AWS Application Discovery Agent (Discovery Agent) は、 AWS Application Discovery Service (Application Discovery Service) が既存のインフラストラクチャの検出に役立つデータ収集ツールです。次の手順では、これらの検出データ収集ツールである エージェントレスコレクターをデプロイするおよび 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ると、 AWS Migration Hub (Migration Hub) コンソールから収集されたデータを開始、停止、表示できます。

AWS Application Discovery Agent (Discovery Agent) がデプロイされたら、 (Migration Hub) コンソールの AWS Migration Hub Data Collectors ページでデータ収集プロセスを開始または停止できます。

データ収集ツールを開始または停止するには

1. AWS アカウントを使用して にサインイン AWS Management Console し、https://console.aws.amazon.com/migrationhub/ で Migration Hub コンソールを開きます。
2. 検出の下にある Migration Hub コンソールナビゲーションペインで、データコレクターを選択します。
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。

コンソールでのデータコレクターの AWS Migration Hub ソート

多くのデータコレクターをデプロイした場合は、コンソールの Data Collectors ページで、デプロイされたコレクターの のリストをソートできます。検索バーでフィルターを適用してリストをソートします。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。

次の表は、演算子、値、値の定義など、エージェントに使用できる検索条件を示しています。

検索条件	演算子	値: 定義
エージェント ID	==	コレクションツールがインストールされている、事前入力されたリストから選択されたエージェント 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	== !=	Started: データが収集され、Application Discovery Service に送信されています。 Start Scheduled: 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。 Stopped: 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
		Stop scheduled: 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。
健康	== !=	Healthy: 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。 Unhealthy: 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。 Unknown: 接続が確立されていない状態が 1 時間を超えています。 Shutdown: 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。

次の表は、演算子、値、値の定義など、エージェントレスコレクターに使用できる検索条件を示しています。

検索条件	演算子	値: 定義
ID	==	コレクションツールのインストール元として事前入力されたリストから選択された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ーの場合、エージェントレスコレクターがインストールされているホストの事前入力されたリストから選択されたホスト名。
ステータス	== !=	データ収集: データ収集がオンになっています。ツールは正常に機能しています。 設定準備完了 — データ収集はオンになっていません。ツールは正常に機能しています。 注意が必要 — ツールはエラー状態であり、注意が必要です。

検索条件	演算子	値: 定義
		Unknown: 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: システム、サービス、またはデーモンのシャットダウンにより、ツールが「シャットダウン」を最後に通知しました。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. AWS アカウントを使用して にサインイン AWS Management Console し、https://console.aws.amazon.com/migrationhub/ で Migration Hub コンソールを開きます。
2. 検出の下にある Migration Hub コンソールナビゲーションペインで、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またはエージェントタブを選択します。
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。

AWS Migration Hub コンソールでのサーバーの表示

[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。

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. AWS アカウントを使用して にサインイン AWS Management Console し、https://console.aws.amazon.com/migrationhub/ で Migration Hub コンソールを開きます。
2. 検出の下にある Migration Hub コンソールナビゲーションペインで、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。
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、「を使用してサーバーデータをエクスポート AWS Migration Hub する」を参照してください。

AWS Migration Hub コンソールでのサーバーのソート

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. AWS アカウントを使用して にサインイン AWS Management Console し、https://console.aws.amazon.com/migrationhub/ で Migration Hub コンソールを開きます。
2. 検出の下にある Migration Hub コンソールナビゲーションペインで、サーバーを選択します。
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。

AWS Migration Hub コンソールでの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 回のオペレーションで個々のサーバー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 AWS タグと似ていますが、2 種類のタグを同じ意味で使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. AWS アカウントを使用して にサインイン AWS Management Console し、https://console.aws.amazon.com/migrationhub/ で Migration Hub コンソールを開きます。
2. 検出の下にある Migration Hub コンソールナビゲーションペインで、サーバーを選択します。
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. タグの追加 を選択し、新しいタグの追加 を選択します。
5. ダイアログボックスで、キー フィールドにキーを入力し、オプションで値 フィールドに値を入力します。

   新しいタグを追加を選択し、さらに情報を追加して、タグを追加します。
6. [Save] 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. AWS アカウントを使用して にサインイン AWS Management Console し、https://console.aws.amazon.com/migrationhub/ で Migration Hub コンソールを開きます。
2. 検出の下にある Migration Hub コンソールナビゲーションペインで、サーバーを選択します。
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オンにして、複数のサーバーから一度にタグを削除します。
4. タグの削除を選択します。
5. 削除する各タグを選択します。

6. [確認] を選択してください。

を使用してサーバーデータをエクスポート AWS Migration Hub する

このトピックでは、、 AWS Management Console、 AWS Command Line Interfaceまたは API を使用してサーバーデータをエクスポートする方法について説明します。

を使用してすべてのサーバーのサーバーデータを AWS Management Console エクスポートするには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/migrationhub/ で Migration Hub コンソールを開きます。
2. 検出 の左側のナビゲーションペインで、サーバーを選択します。
3. アクションを選択し、検出データのエクスポートを選択します。
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。このアクションは、次の表で説明されている .csv ファイルを含む .zip ファイルを生成します。

ファイル名	説明
{account_id}_Application.csv	サーバー数、名前、説明など、各アプリケーションの詳細。
{account_id}_ApplicationResourceAssociation.csv	サーバーとアプリケーションの関係。
{account_id}_ImportTemplate	各サーバーのアプリケーションとタグの概要。このファイルは、サーバーに関連付けられたアプリケーションを更新するために変更および再インポートできます。
{account_id}_NetworkInterface.csv	関連付けられたサーバー、アドレス、スイッチを含む各ネットワークインターフェイスの詳細。

ファイル名	説明
{account_id}_Server.csv	オペレーティングシステム、ホスト名、ハイパーバイザーなど、各サーバーの詳細。
{account_id}_SystemPerformance.csv	CPU、メモリとストレージの設定、パフォーマンスなど、各サーバーの詳細。
{account_id}_Tags.csv	サーバーに関連付けられている各タグの詳細。
{account_id}_VMwareInfo.csv	moRef、vmName、vCenter など、各 VMware 設定の詳細。

を使用して特定のサーバーのエージェントデータを AWS Management Console エクスポートするには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/migrationhub/ で Migration Hub コンソールを開きます。
2. 検出 の左側のナビゲーションペインで、サーバーを選択します。
3. サーバーの検索フィールドにカーソルを置きます。ドロップダウンリストが表示されます。そのリストのプロパティで、ソースを選択し、= 演算子を選択し、ソース = エージェントを選択します。
4. 検索結果で、データをエクスポートするサーバーの名前を選択します。このアクションにより、そのサーバーの詳細ページに移動します。
5. 開始時刻と終了時刻を入力し、エクスポートを選択します。エクスポートされた .zip ファイルには、次の表で説明する .csv ファイルが含まれています。

{account_id}_destinationProcessConnection.csv	サーバーへのインバウンド接続の詳細。
{account_id}_networkInterface.csv	アドレス、マスク、名前など、各ネットワークインターフェイスの詳細

{account_id}_osInfo.csv	CPU タイプ、ハイパーバイザー、オペレーティングシステム名など、オペレーティングシステムの詳細。
{account_id}_process.csv	サーバーで実行されているプロセスの詳細。
{account_id}_sourceProcessConnection.csv	サーバーから発信されるアウトバウンド接続の詳細。
{account_id}_systemPerformance.csv	サーバーの CPU、メモリ、ストレージの設定とパフォーマンスの詳細。

AWS Command Line Interface または API を使用してサーバーデータをエクスポートするには

1. start-export-task を実行します。対応する API オペレーションは StartExportTask です
2. describe-export-tasks を実行します。対応する API オペレーションは DescribeExportTasks です。

AWS Migration Hub コンソールでのサーバーのグループ化

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. AWS アカウントを使用して にサインイン AWS Management Console し、https://console.aws.amazon.com/migrationhub/ で Migration Hub コンソールを開きます。
2. 検出の下にある Migration Hub コンソールナビゲーションペインで、サーバーを選択します。
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: 選択したサーバーごとに、[Add tag (タグの追加)] を選択し、[Key (キー)] に値を入力します。必要に応じて [Value (値)] にも値を入力し ます。
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、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フィルターを指定し、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、「the section called “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、「DescribeConfigurations」を参照してください。

`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.maxNetworkWritesPerSecondInKB	
server.performance.minFreeRAMInKB	
server.performance.numCores	
server.performance.numCpus	
server.performance.numDisks	
server.performance.numNetworkCards	
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、「ListConfigurations」を参照してください。

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	• String	• ASC • DESC
server.osName	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
server.osVersion	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
server.agentId	• EQUALS • NOT_EQUALS • EQ • NE	• String	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	• String	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	• String	なし
server.vmWareInfo.vcenterId	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	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	• String	なし
server.networkInterfaceInfo.portGroupId	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	なし
server.networkInterfaceInfo.portGroupName	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	なし
server.networkInterfaceInfo.virtualSwitchName	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	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	• String	なし
server.networkInterfaceInfo.macAddress	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	なし
server.performance.avgCpuUsagePct	• GE • LE • GT • LT	• 割合 (%)	なし
server.performance.totalDiskFreeSizeInKB	• GE • LE • GT • LT	• 倍精度	なし
server.performance.avgFreeRAMInKB	• GE • LE • GT • LT	• 倍精度	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	• String	なし
server.tag.key	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	なし
server.application.name	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	なし
server.application.description	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	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	• String	なし
server.process.commandLine	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	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	• String	• ASC • DESC
application.description	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• 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	• String	• ASC • DESC
process.commandLine	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• 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	• String	• ASC • DESC
server.osName	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
server.osVersion	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC

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	• String	

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	• String	• ASC • DESC
destinationServer.osName	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
destinationServer.osVersion	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC

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	• String	
sourceProcess.configurationId	• EQUALS • NOT_EQUALS • EQ • NE	• ProcessId	
sourceProcess.name	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
sourceProcess.commandLine	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
destinationProcess.configurationId	• EQUALS • NOT_EQUALS • EQ • NE	• ProcessId	

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	• String	• ASC • DESC
`destinationprocess.commandLine`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• 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 StartExportTask、DescribeConfigurations、および ListConfigurations にすぐに表示されない場合があります。

- AssociateConfigurationItemsToApplication
- CreateTags
- DeleteApplications
- DeleteTags
- DescribeBatchDeleteConfigurationTask
- DescribeImportTasks
- DisassociateConfigurationItemsFromApplication
- 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 StartExportTask、DescribeConfigurations、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、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を介して伝播され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 秒の待機時間から始めて、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 レスポンスを返した場合でも、後続のオペレーション間の待機時間を追加します。数秒の待機時間から始めて、エクスポネンシャルバックオフアルゴリズムを適用し、最大約 5 分間の待機時間まで徐々に増やします。

インターフェイスエンドポイント (AWS PrivateLink) AWS Application Discovery Service を使用した へのアクセス

を使用して AWS PrivateLink 、VPC と の間にプライベート接続を作成できます AWS Application Discovery Service。インターネットゲートウェイ、NAT デバイス、VPN 接続、または AWS Direct Connect 接続を使用せずに、VPC 内にあるかのように Application Discovery Service にアクセスできます。VPC 内のインスタンスは、Application Discovery Service にアクセスするためにパブリック IP アドレスを必要としません。

このプライベート接続を確立するには、 AWS PrivateLinkを利用したインターフェイスエンドポイントを作成します。インターフェイスエンドポイントに対して有効にする各サブネットにエンドポイントネットワークインターフェイスを作成します。これらは、Application Discovery Service 宛てのトラフィックのエントリポイントとして機能するリクエスタ管理のネットワークインターフェイスです。

詳細については「 AWS PrivateLink Guide (AWS PrivateLink ガイド)」の「Access an AWS のサービス using an interface VPC endpoint (インターフェイス VPC エンドポイントを使用して にアクセスする)」を参照してください。

Application Discovery Service に関する考慮事項

Application Discovery Service のインターフェイスエンドポイントを設定する前に、「 AWS PrivateLink ガイド」の「インターフェイス VPC エンドポイントを使用して AWS サービスにアクセスする」を参照してください。

Application Discovery Service は 2 つのインターフェイスをサポートしています。1 つはすべての API アクションを呼び出すためのインターフェイスで、もう 1 つはエージェントレスコレクターと AWS Application Discovery Agent が検出データを送信するためのものです。

インターフェイスエンドポイントの作成

Amazon VPC コンソールまたは AWS Command Line Interface (AWS CLI) を使用して、インターフェイスエンドポイントを作成できます。詳細については、「 AWS PrivateLink ガイド」の「インターフェイス VPC エンドポイントを使用して AWS サービスにアクセスする」を参照してください。

For Application Discovery Service

次のサービス名を使用して、Application Discovery Service のインターフェイスエンドポイントを作成します。

```
com.amazonaws.region.discovery
```

インターフェイスエンドポイントのプライベート DNS を有効にすると、デフォルトのリージョン DNS 名を使用して Application Discovery Service に API リクエストを行うことができます。例えば、`discovery.us-east-1.amazonaws.com` と指定します。

For Agentless Collector and AWS Application Discovery Agent

次のサービス名を使用してインターフェイスエンドポイントを作成します。

```
com.amazonaws.region.arsenal-discovery
```

インターフェイスエンドポイントのプライベート DNS を有効にすると、デフォルトのリージョン DNS 名を使用して Application Discovery Arsenal に API リクエストを行うことができます。例えば、`arsenal-discovery.us-east-1.amazonaws.com` と指定します。

インターフェイスエンドポイントのエンドポイントポリシーを作成する

エンドポイントポリシーは、インターフェイスエンドポイントにアタッチできる IAM リソースです。デフォルトのエンドポイントポリシーでは、インターフェイスエンドポイントを介した AWS サービスへのフルアクセスが許可されます。VPC から AWS サービスに許可されるアクセスを制御するには、インターフェイスエンドポイントにカスタムエンドポイントポリシーをアタッチします。

エンドポイントポリシーは以下の情報を指定します。

- アクションを実行できるプリンシパル (AWS アカウント、IAM ユーザー、IAM ロール)。
- 実行可能なアクション。

詳細については[AWS PrivateLink Guide] (ガイド) の[Control access to services using endpoint policies] (エンドポイントポリシーを使用してサービスへのアクセスをコントロール) を参照してください。

例: VPC エンドポイントポリシー

以下は、カスタムエンドポイントポリシーの例です。インターフェイスエンドポイントにアタッチされると、このポリシーは、すべてのリソースですべてのプリンシパルに、リストされている アクションへのアクセス権を付与します。

Example policy for Application Discovery Service

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "discovery:action-1",
            "discovery:action-2",
            "discovery:action-3"
         ],
         "Resource":"*"
      }
   ]
}
```

Example policy for the Agentless Collector and AWS Application Discovery Agent

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "arsenal:RegisterOnPremisesAgent"
         ],
         "Resource":"*"
      }
   ]
}
```

エージェントレスコレクターと AWS アプリケーション検出エージェントの VPC エンドポイントの使用

エージェントレスコレクターと AWS アプリケーション検出エージェントは、設定可能なエンドポイントをサポートしていません。代わりに、arsenal-discoveryAmazon VPC エンドポイントのプライベート DNS 機能を使用します。

- プライベート AWS IP アドレスを VPC にルーティングするように AWS Direct Connect ルートテーブルを設定します。例えば、送信先 = 10.0.0.0/8、ターゲット = local です。この設定では、少なくとも arsenal-discovery Amazon VPC エンドポイントのプライベート IP アドレスを VPC にルーティングする必要があります。
- Agentless Collector は設定可能な Arsenal エンドポイントをサポートしていないため、arsenal-discoveryAmazon VPC エンドポイントのプライベート DNS 機能を使用します。
- AWS Direct Connect トラフィックをルーティングするのと同じ VPC を持つプライベートサブネットに arsenal-discovery Amazon VPC エンドポイントを設定します。
- arsenal-discovery VPC 内からのインバウンドトラフィックを有効にするセキュリティグループ (10.0.0.0/8 など) を使用して Amazon VPC エンドポイントを設定します。
- Amazon VPC エンドポイントのプライベート DNS 名の DNS 解決をルーティングするように arsenal-discovery Amazon Route 53 インバウンドリゾルバーを設定します。これは VPC エンドポイントのプライベート IP に解決されます。そうしないと、コレクターはオンプレミスのリゾルバーを使用して DNS 解決を実行し、パブリック Arsenal エンドポイントを使用し、トラフィックは VPC を通過しません。
- すべてのパブリックトラフィックを無効にしている場合、自動更新機能は失敗します。これは、エージェントレスコレクターが Amazon ECR エンドポイントにリクエストを送信して更新を取得するためです。パブリックインターネット経由でリクエストを送信せずに自動更新機能を使用するには、Amazon ECR サービスの VPC エンドポイントを設定し、このエンドポイントのプライベート DNS 機能を有効にします。

のセキュリティ AWS Application Discovery Service

でのクラウドセキュリティが最優先事項 AWS です。お客様は AWS 、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を活用できます。

セキュリティは、 AWS お客様とお客様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 – クラウドで AWS 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 AWS 責任があります。 AWS また、 では、安全に使用できるサービスも提供しています。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 サービスによって決まります。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 Application Discovery Agent または Application Discovery Service Agentless Collector を使用するには、 AWS アカウントに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。責任共有モデルの一環として、インフラストラクチャへのアクセスを保護する責任があります。

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 リソースのモニタリングや保護に役立つ他の AWS サービスの使用方法についても説明します。

トピック

- の Identity and Access Management AWS Application Discovery Service
- を使用した Application Discovery Service API コールのログ記録 AWS CloudTrail

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、追加料金なしで使用できる AWS のサービス 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 の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、「が IAM と AWS Application Discovery Service 連携する方法」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 アイデンティティ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 ロールを引き受けることによって認証 (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 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、「 AWS サインイン ユーザーガイド」の「 へのサインイン AWS アカウント方法」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、 はソフトウェア開発キット (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を暗号化して署名します。AWS ツールを使用しない場合は、自分でリクエストに署名する必要があります。リクエストに自分で署名する推奨方法の使用については、「IAM ユーザーガイド」の「API リクエストに対するAWS Signature Version 4」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。たとえば、 では、アカウントのセキュリティを高めるために多要素認証 (MFA) を使用する AWS 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「多要素認証」および「IAM ユーザーガイド」の「IAM のAWS 多要素認証」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 ID 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 ユーザーに関するユースケース」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 ID 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。で IAM ロールを一時的に引き受けるには AWS Management Console、ユーザーから IAM ロール (コンソール) に切り替えることができます。ロールを引き受けるには、 または AWS API オペレーションを AWS CLI 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「ロールを引き受けるための各種方法」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ロールについては、「IAM ユーザーガイド」の「サードパーティー ID プロバイダー (フェデレーション) 用のロールを作成する」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 User Guide」の「Permission sets」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、(プロキシとしてロールを使用する代わりに) リソースに直接ポリシーをアタッチできます。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アクションを実行すると AWS、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 へのリクエストをリクエストする 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、削除することができます。詳細については、「IAM ユーザーガイド」の「AWS のサービスに許可を委任するロールを作成する」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、サービスリンク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。EC2 インスタンスに AWS ロールを割り当て、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。

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、ID AWS 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 JSON AWS 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のリソースに対してどのような条件下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受けることができます。

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ポリシーの作成方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」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「管理ポリシーとインラインポリシーのいずれかを選択する」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、および Amazon VPC は AWS WAF、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、一般的でない追加のポリシータイプをサポートしています。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) の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、ビジネスが所有する複数の AWS アカウント をグループ化して一元管理するためのサービスです。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「サービスコントロールポリシー (SCP)」を参照してください。
- リソースコントロールポリシー (RCP) – RCP は、所有する各リソースにアタッチされた IAM ポリシーを更新することなく、アカウント内のリソースに利用可能な最大数のアクセス許可を設定するために使用できる JSON ポリシーです。RCP は、メンバーアカウントのリソースのアクセス許可を制限し、組織に属しているかどうかにかかわらず AWS アカウントのルートユーザー、 を含む ID の有効なアクセス許可に影響を与える可能性があります。RCP をサポートする のリストを含む Organizations と RCP の詳細については、AWS Organizations RCPs「リソースコントロールポリシー (RCPs」を参照してください。 AWS のサービス
- 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。が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。

が IAM と AWS Application Discovery Service 連携する方法

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については、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のポリシー
- Application Discovery Service リソースベースのポリシー
- Application Discovery Service タグに基づく認可
- Application Discovery Service IAM ロール

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

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、また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 JSON AWS 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のリソースに対してどのような条件下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アクセス許可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。

単一のステートメントに複数のアクションを指定するには次のようにコンマで区切ります。

```
"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、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 ユーザーガイドのAWS 「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 アイデンティティベースのポリシーの例」を参照してください。

Application Discovery Service リソースベースのポリシー

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 タグに基づく認可

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 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。

サービスにリンクされた役割

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 のサービスにリンクされたロールの使用」を参照してください。

サービス役割

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役割を引き受けることが許可されます。この役割により、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。サービス役割は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 管理者はこの役割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 管理ポリシー 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、自分でポリシーを記述するよりも AWS 管理ポリシーを使用する方が簡単です。チームに必要な権限のみを提供する 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 サービスは、 AWS 管理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損なわ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ジョブ関数の マネージドポリシー AWS をサポートしています。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。サービスが新機能を起動すると、 は新しいオペレーションとリソースの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、 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権を付与します。

このポリシーは、エージェントレスコレクター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、収集されたデータを 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のリージョンを知るために必要です。
- sts – コレクターが Amazon ECR Public を呼び出して最新の更新を取得できるように、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。

JSON

```
{
    "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 に登録、通信、コネクタのヘルスメトリクスを共有する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: ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

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、 は自動的にアカウントにアタッチApplicationDiscoveryServiceContinuousExportServiceRolePolicy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 AWS Glue Data Catalog を持つ 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

Amazon Athena でデータ探索を使用するには、AWSDiscoveryContinuousExportFirehosePolicy ポリシーが必要です。これにより、Amazon Data Firehose は Application Discovery Service から Amazon S3 に収集されたデータを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、「データ探索のため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、管理者はまず Firehose を信頼されたエンティティとして

AWSApplicationDiscoveryServiceFirehose 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 ロールを作成するには

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. [Next: Permissions] (次のステップ: 許可) を選択します。
6. [フィルタポリシー] で、[AWSDiscoveryContinuousExportFirehosePolicy] を検索します。
7. [AWSDiscoveryContinuousExportFirehosePolicy] の横にあるボックスをオンにして、[次へ: レビュー] を選択します。
8. [AWSApplicationDiscoveryServiceFirehose] をロール名として入力し、[ロールの作成] を選択します。

AWS マネージドポリシーに対する Application Discovery Service 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、のドキュメント履歴 AWS Application Discovery Service 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利用可能になった新しいポリシー	Application Discovery Service は、Application Discovery Service に登録して通信し、他の AWS サービスと通信するためのアクセス権を Agentless Collector に付与AWSApplicationDiscoveryAgen	2022 年 8 月 16 日

変更	説明	日付
	tlessCollectorAccess する新しい マネージドポリシーを追加しました。	
Application Discovery Service が変更の追跡を開始しました	Application Discovery Service は、 AWS 管理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 アイデンティティ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

- ポリシーに関する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
- データ探索のため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

ポリシーに関するベストプラクティス

ID ベースのポリシーは、アカウント内で誰かが Application Discovery Service リソースを作成、アクセス、または削除できるか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 – ユーザーとワークロードにアクセス許可の付与を開始するには、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することで、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、サービスアクションが などの特定の を通じて使用されている場合に 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 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 でポリシーを検証する」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、MFA をオンにしてセキュリティを強化します。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 を使用した安全な API アクセス」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 マネージドポリシーは、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 管理ポリシー AWS Application Discovery Service」を参照してください。

Example AWSApplicationDiscoveryServiceFullAccess ポリシー

JSON

```
{
    "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 マネージドポリシーは、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。このポリシーの詳細については、「AWS の 管理ポリシー 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 Policy

JSON

```
{
    "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 データカタログを作成します。

このポリシーの使用方法については、「AWS の 管理ポリシー AWS Application Discovery Service」を参照してください。

Example ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

JSON

```
{
   "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"
                }
            }
        }
    ]
}
```

データ探索のためのアクセス許可の付与

Amazon Athena でデータ探索を使用するには、AWSDiscoveryContinuousExportFirehosePolicy ポリシーが必要です。これにより、Amazon Data Firehose は Application Discovery Service から Amazon S3 に収集されたデータを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

JSON

```
{
    "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、ポリシーに以下の両方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

JSON

```
{
    "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 のサービスにリンクされたロールの使用

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。サービスにリンクされたロールは 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他の AWS サービスを呼び出すために必要なすべてのアクセス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 のみがそのロールを引き受けることができます。定義される許可は信頼ポリシーと許可ポリシーに含まれており、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 のサービスにリンクされたロールのアクセス許可
- Application Discovery Service のサービスにリンクされたロールの作成
- Application Discovery Service のサービスにリンクされたロールの削除

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。サービスにリンクされた役割に関するドキュメントをサービスで表示するには[はい] リンクを選択してください。

Application Discovery Service のサービスにリンクされたロールのアクセス許可

Application Discovery Service は、AWSServiceRoleForApplicationDiscoveryServiceContinuousExport という名前のサービスにリンクされたロールを使用します。これにより、 が使用または管理する AWS サービスとリソースにアクセスできます AWS Application Discovery Service。

AWSServiceRoleForApplicationDiscoveryServiceContinuousExport サービスリンクロールは、以下のサービスを信頼してロールを引き受けます。

- 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。

JSON

```
{
    "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"
                }
            }
```

```
        }
    ]
}
```

サービスリンク役割の作成、編集、削除を IAM エンティティ (ユーザー、グループ、役割など) に許可するにはアクセス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「サービスリンクロールの許可」を参照してください。

Application Discovery Service のサービスにリンクされたロールの作成

サービスリンク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、継続的エクスポートが暗黙的に有効になっているときに自動的に作成されます。これは、a) 「データ収集を開始する」を選択した後、または「Athena でのデータ探索」というラベルの付いたスライダーをクリックした後、または b) AWS CLI を使用して StartContinuousExport API を呼び出すときに、Data Collectors ページに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ものです。

> **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 アカウントに新しいロールが表示される」を参照してください。

Migration Hub コンソールからサービスにリンクされたロールを作成する

Migration Hub コンソールを使用して、AWSServiceRoleForApplicationDiscoveryServiceContinuousExport サービスリンクロールを作成することができます。

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。

からサービスにリンクされたロールを作成する AWS CLI

から Application Discovery Service コマンドを使用して AWS Command Line Interface 、AWSServiceRoleForApplicationDiscoveryServiceContinuousExport サービスにリンクされたロールを作成できます。

このサービスにリンクされたロールは、 AWS CLI から継続的なエクスポートを開始すると自動的に作成されます (最初に を環境にインストール AWS CLI する必要があります) 。

から継続的なエクスポートを開始してサービスにリンクされたロール (CLI) を作成するには AWS CLI

1. オペレーティングシステム (Linux、macOS、または Windows) AWS CLI に 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. 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しても、同じ方法でロールを再作成できます。

Application Discovery Service のサービスにリンクされたロールの削除

サービスリンクロールを必要とする機能やサービスが不要になった場合は、ロールを削除することをお勧めします。そうすることで、モニタリングや保守が積極的に行わ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。

サービスにリンクされた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。

Migration Hub コンソールから AWSServiceRoleForApplicationDiscoveryServiceContinuousExport サービスリンクロールが使用する Application Discovery Service リソースを削除する

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. [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。

AWS CLIから AWSServiceRoleForApplicationDiscoveryServiceContinuousExport サービスリンクロールが使用する Application Discovery Service リソースを削除する

1. オペレーティングシステム (Linux、macOS、または Windows) AWS CLI に 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. 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
```

サービスリンク役割の手動による削除

IAM コンソール、IAM CLI、または IAM API を使用して、AWSServiceRoleForApplicationDiscoveryServiceContinuousExport サービスリンクロールを削除することができます。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、モニタリングや保守が積極的に行わ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。「サービスにリンクされた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:PassRole を実行する権限がない

iam:PassRole を実行する権限がない

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、既存のロールをそのサービスに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。

を使用した Application Discovery Service API コールのログ記録 AWS CloudTrail

AWS Application Discovery Service は AWS CloudTrail、Application Discovery Service のユーザー、ロール、または サービスによって実行されたアクションを記録する AWS サービスである と統合されています。CloudTrail を使用して、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、保持することができます。CloudTrail は、AWS マネジメントコンソール、 AWS SDKs、 AWS アカウントアクティビティのイベント履歴を提供します。

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、Application Discovery Service のイベントなど、Amazon S3 バケットへの CloudTrail イベントの継続的な配信を有効にすることができます。証跡を設定しない場合で

も、CloudTrail コンソールの [イベント履歴] で最新のイベントを表示できます。CloudTrail が収集した情報を使用して、Application Discovery Service に対して行われたリクエスト、リクエストが行われた IP アドレス、リクエスト者、リクエストが行われた日時、および追加の詳細情報を確認できます。

CloudTrail の詳細については、「AWS CloudTrail ユーザーガイド」を参照してください。

CloudTrail の Application Discovery Service 情報

CloudTrail は、 AWS アカウントの作成時にアカウントで有効になります。Application Discovery Service でアクティビティが発生すると、そのアクティビティはイベント履歴の他の AWS サービスイベントとともに CloudTrail イベントに記録されます。 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、「CloudTrailイベント履歴でのイベントの表示」を参照してください。

Application Discovery Service のイベントなど、 AWS アカウント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。追跡により、CloudTrail はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで証跡を作成すると、証跡はすべての AWS リージョンに適用されます。証跡は、 AWS パーティション内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、CloudTrail ログで収集されたイベントデータをより詳細に分析し、それに基づいて行動するように、他の AWS サービスを設定できます。詳細については、次を参照してください:

- 証跡の作成のための概要
- CloudTrail がサポートするサービスと統合
- CloudTrail 用 Amazon SNS 通知の構成
- 「複数のリージョンからCloudTrailログファイルを受け取る」および「複数のアカウントからCloudTrailログファイルを受け取る」

すべての Application Discovery Service アクションは CloudTrail によってログに記録され、これらは Application Discovery Service API リファレンスに記載されています。例えば、`CreateTags`、`DescribeTags`、`GetDiscoverySummary` の各アクションを呼び出すと、CloudTrail ログファイルにエントリが生成されます。

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または AWS Identity and Access Management (IAM) ユーザー認証情報を使用して行われたかどうか。
- リクエストがロールまたはフェデレーション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 サービスによって行われたかどうか。

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

「トレイル」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するように設定できます。CloudTrail のログファイルは、単一か複数のログエントリを含みます。イベントは任意ソースからの単一リクエストを表し、リクエストされたアクション、アクションの日時、リクエストパラメータなどの情報を含みます。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。

以下の例は、`DescribeTags` アクションを示す CloudTrail ログエントリです。

```
{
    "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 ARN 形式

Amazon リソースネーム (ARN) は、 AWS リソースを一意に識別する文字列です。 では、すべての でリソースを明確に指定する場合に ARN AWS が必要です AWS。 では、次の ARNs AWS Application Discovery Service を定義します。

- 検出エージェント: `arn:aws:discovery:region:account:agent/discovery-agent/agentId`
- エージェントレスコレクター: `arn:aws:discovery:region:account:agent/agentless-collector/agentId`
- 移行エバリュエーターコレクター: `arn:aws:discovery:region:account:agent/migration-evaluator-collector/agentId`
- Discovery Connector: `arn:aws:discovery:region:account:agent/discovery-connector/agentId`

AWS Application Discovery Service クォータ

Service Quotas コンソールには AWS Application Discovery Service 、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 Discover > Data Collectors > Agents 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 分かかる場合があります。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」にエラーがまだ表示されていて、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するが、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. 削除します AWS Glue Data Catalog。

   Amazon Athena でデータ探索を有効にすると、アカウント内に Amazon S3 バケットが作成され、ADS エージェントによって定期的に収集されたデータが保存されます。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 も作成されます。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を修正する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、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。これにより`AWSServiceRoleForApplicationDiscoveryServiceContinuousExport`、Amazon S3 バケット、Amazon Kinesis ストリーム、 など、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 管理ポリシー 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、エージェントが開始してから 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 AWS Glue

を使用していて AWS Organizations、Amazon Athena 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 管理ポリシー AWS Application Discovery Service」を参照してください。

Amazon Athena のデータ探索が正しく機能するように、Amazon S3 バケット、Amazon Data Firehose Streams、 など、Amazon Athena の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 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ています。

発生した非制限ベースのエラーを修正するには、`errors-file.csv` を使用して、`failed-entries-file.csv` ファイルの問題を修正してから、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。

のドキュメント履歴 AWS Application Discovery Service

ユーザーガイドドキュメントの最終更新日: 2023 年 5 月 16 日

次の表は、2019 年 1 月 18 日以降の Application Discovery Service ユーザーガイドの重要な変更点をまとめたものです。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
Discovery Connector から Agentless Collector への移行	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。2025 年 11 月 17 日以降、 AWS Application Discovery Service は Discovery Connector からの新しいデータの受け入れを停止します。詳細については、「Discovery Connector」を参照してください。	2024 年 11 月 12 日
エージェントレスコレクターネットワークデータ収集モジュールをリリースしました	ネットワークデータ収集モジュールを使用すると、オンプレミスデータセンター内のサーバー間の依存関係を検出できます。詳細については、「エージェントレスコレクターネットワークデータ収集モジュールの使用」を参照してください。	2024 年 11 月 8 日
依存関係マッピングのエージェントレスコレクションのサポート	詳細については、VMware vCenter Agentless Collector データ収集モジュールの使用」を参照してください。	2024 年 10 月 24 日

Amazon Linux 2023 に基づく Agentless Collector バージョン 2 のリリース	詳細については、「エージェントレスコレクターの前提条件」を参照してください。	2024 年 9 月 26 日
エージェントレスコレクターの前提条件を更新	詳細については、「エージェントレスコレクターの前提条件」を参照してください。	2024 年 9 月 9 日
API の結果整合性	詳細については、AWS Application Discovery Service「 API の結果整合性」を参照してください。	2024 年 6 月 20 日
エージェントレスコレクターの更新	アウトバウンドアクセスを必要とするドメインのリストsts.amazonaws.com にを追加しました。詳細については、「AWS 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する」を参照してください。	2024 年 6 月 20 日
アクセスを分離するには、個別の AWS アカウントを作成して使用します。	詳細については、AWS Application Discovery Service のアクション、リソース、および条件キー」を参照してください。	2024 年 4 月 5 日

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クスを収集できます。詳細については、「データベースと分析の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ーの紹介	Application Discovery Service Agentless Collector (Agentless Collector) は、 AWS Application Discovery Service への移行を効果的に計画できるように、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新しいオンプレミスアプリケーションです AWS クラウド。詳細については、「エージェントレスコレクター」を参照してください。	2022 年 8 月 16 日

IAM 更新	AWS Identity and Access Management (IAM) `discovery:GetNetworkConnectionGraph` アクションが、アイデンティティベースのポリシーの作成時に AWS Migration Hub コンソールネットワーク図へのアクセスを許可できるようになりました。詳細については、「ネットワーク図を使用するアクセス許可の付与」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の検出および移行計画情報の単一のリポジトリと、複数の AWS リージョンへの移行の単一の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

次の表は、2019 年 1 月 18 日以前の Application Discovery Service ユーザーガイドのドキュメントリリースを示しています。

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よう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	が追加され AWS Management Console 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 5 月 12 日

AWS 用語集

最新の AWS 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。

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。2025 年 11 月 17 日以降、 AWS Application Discovery Service は Discovery Connector からの新しいデータの受け入れを停止します。

このセクションでは、 AWS エージェントレス検出コネクタ (検出コネクタ) から 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デプロイしたら、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。

Discovery Connector を使用したデータの収集

> **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。2025 年 11 月 17 日以降、 AWS Application Discovery Service は Discovery Connector からの新しいデータの受け入れを停止します。詳細については、「Discovery Connector」を参照してください。

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 管理ポリシー 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 (*) で示されてい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た .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
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

データフィールド	説明
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
lastModifiedTimeStamp*	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
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)

データフィールド	説明
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
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

データフィールド	説明
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、「コンソールでのデータコレクターの AWS Migration Hub ソート」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 データの収集

Discovery Connector を VMware 環境にデプロイして設定したら、停止した場合にデータ収集を再開できます。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 AWS CLI には AWS CLI、まず を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 に 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. 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. デフォルトの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` と指定します。
   d. デフォルトの出力形式として「`text`」と入力します。
3. 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

> **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。2025 年 11 月 17 日以降、 AWS Application Discovery Service は Discovery Connector からの新しいデータの受け入れを停止します。詳細については、「Discovery Connector」を参照してください。

このセクションでは、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について説明します。

セットアップ AWS 中に Discovery Connector 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。

> **に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、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 接続を確立するために Discovery Connector が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いずれかの 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の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た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 サポートに連絡してトラブルシューティングを依頼する必要があります。

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

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 接続の情報の表示を選択すると、vCenter サーバーの運用ステータスを確認する」というメッセージを含むダイアログボックスが表示されます。または、設定の編集を選択して vCenter エンドポイントを更新します。

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、「編集設定を選択して、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」というメッセージを含む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 エージェントレス検出コネクタコンソールに再度ログインし、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。