aws

ユーザーガイド

Migration Hub Strategy の推奨事項

Migration Hub Strategy の推奨事項: ユーザーガイド

Table of Contents

Migration Hub Strategy Recommendations とは

Migration Hub Strategy Recommendations は、アプリケーションの実行可能なトランスフォーメーションパスに関する移行とモダナイズ戦略のレコメンデーションを提供することで、移行とモダナイズの取り組みを計画するのに役立ちます。

Strategy Recommendations では、Microsoft IIS、Java Tomcat、Jboss アプリケーションのサーバーインベントリ、ランタイム環境、アプリケーションバイナリを分析して、アンチパターンレポートを生成します。さらに、Strategy Recommendations がすべてのアプリケーションのソースコードとデータベース分析を実行できるようにソースコードを設定できます。Strategy Recommendations は、この分析をビジネス目標および、ユーザーが提供したアプリケーションやデータベースの変換に関する設定と比較し、レコメンデーションを行います。

- 各アプリケーションにとって最も効果的な移行戦略。
- 移行とモダナイズに使用できるツールまたはサービス。
- アプリケーションの非互換性と特定のオプションを解決するためのアンチパターン。

Migration Hub Strategy Recommendations では、関連するデプロイ先、ツール、プログラムを使用して、リホスト、リプラットフォーム、およびリファクタリングを行うための移行とモダナイズ戦略を推奨しています。リホスト、リプラットフォーム、リファクタリングについては、「AWS 規範的ガイダンス」用語集の「移行用語 - 7 R」を参照してください。

Strategy Recommendations によって、AWS Application Migration Service (AWS MGN) を使用して Amazon Elastic Compute Cloud (Amazon EC2) にリホストするなどの簡単なオプションが推奨される場合があります。より最適化されたレコメンデーションとしては、AWS App2Container を使用するコンテナへのリプラットフォームや、.NET Core や PostgreSQL などのオープンソーステクノロジへのリファクタリングなどがあります。

Strategy Recommendations を初めてお使いになる方向けの情報

Strategy Recommendations を初めて使用する方には、以下のセクションを最初に読むことをお勧めします。

- Strategy Recommendations の概要
- Strategy Recommendations のセットアップ
- Strategy Recommendations の開始方法

Strategy Recommendations の概要

AWS Migration Hub コンソールの Migration Hub Strategy Recommendations を使用して、サーバーとアプリケーションのポートフォリオの評価を開始できます。コンソールを使用して、評価を設定して実行できます。評価後、コンソールを使用して、各サーバーとアプリケーションの評価データを、推奨される変換ツールとともに表示できます。

リファクタリングに関するレコメンデーションや非互換性のリストを受信するには、Strategy Recommendations を使用してアプリケーションのソースコードとデータベースを評価できます。

レコメンデーションデータを Microsoft Excel ファイルでダウンロードすることもできます。

関連サービス

- AWS Migration Hub — AWS Migration Hub コンソールを使用して Migration Hub Strategy Recommendations コンソールにアクセスします。データを収集しているサーバーに関する情報も表示されます。
- AWS Application Discovery Service — Strategy Recommendations を使用する前に、Application Discovery Service を使用して AWS Migration Hub コンソールでサーバーとアプリケーションに関するデータを収集します。
- AWS Application Migration Service – AWS Application Migration Service (MGN) は、AWS へのリフトアンドシフト移行のためのプライマリ移行サービスが推奨されます。
- AWS Database Migration Service — AWS Database Migration Service は、オンプレミス、Amazon Relational Database Service (Amazon RDS) DB インスタンス、または、AWS サービス上のデータベースへの Amazon Elastic Compute Cloud (Amazon EC2) インスタンス上のデータベースからデータを移行するために使用できるウェブサービスです。
- AWS App2Container –AWS App2Container (A2C) は、.NET および Java アプリケーションをコンテナ化されたアプリケーションに最新化するためのコマンドラインツールです。
- Porting Assistant for .NET - .NET ソースコード分析に使用します。Porting Assistant for .NET は、Microsoft .NET Framework アプリケーションを .NET Core に移植するのに必要な手作業を減らす互換性スキャナーです。Porting Assistant for .NET は .NET アプリケーションのソースコードを評価し、互換性のない API やサードパーティパッケージを識別します。
- Windows Server 用サポート終了移行プログラム — サービス終了移行プログラム (EMP) には、レガシーアプリケーションを Windows Server 2003、2008、2008 R2 から、AWS でサポートされている新しいバージョンに、リファクタリング不要で移行するためのツールが含まれています。

- AWS Schema Conversion Tool — AWS Schema Conversion Tool (AWS SCT) を使用して、既存のデータベーススキーマをあるデータベースエンジンから別のデータベースエンジンに変換できます。
- Windows Web アプリケーション移行アシスタント — AWS Elastic Beanstalk 用 Windows Web アプリケーション移行アシスタントは、ASP.NET アプリケーションと ASP.NET Core アプリケーションをオンプレミスの IIS Windows サーバーから Elastic Beanstalk に移行するインタラクティブな PowerShell ユーティリティです。
- Babelfish for Aurora PostgreSQL -Babelfish for Aurora PostgreSQL は Amazon Aurora PostgreSQL 互換エディションの新機能です。これにより Aurora は Microsoft SQL サーバー用に作成されたアプリケーションからのコマンドを理解できるようになります。

Strategy Recommendations のセットアップ

Migration Hub Strategy Recommendations を初めて使用する前に、以下のタスクを完了してください。

トピック

にサインアップする AWS アカウント

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、通話呼び出しを受け取り、電話キーパッドで検証コードを入力するように求められます。

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

AWS サインアッププロセスが完了すると、 から確認メールが送信されます。https://aws.amazon.com/ の [マイアカウント] を選んで、いつでもアカウントの現在のアクティビティを表示し、アカウントを管理できます。

管理アクセスを持つユーザーを作成する

にサインアップしたら AWS アカウント、 を保護し AWS アカウントのルートユーザー、 を有効にして AWS IAM Identity Center、日常的なタスクにルートユーザーを使用しないように管理ユーザーを作成します。

のセキュリティ保護 AWS アカウントのルートユーザー

1. ルートユーザーを選択し、 AWS アカウント E メールアドレスを入力して、アカウント所有者AWS Management Consoleとして にサインインします。次のページでパスワードを入力します。

   ルートユーザーを使用してサインインする方法については、AWS サインイン ユーザーガイドの「ルートユーザーとしてサインインする」を参照してください。
2. ルートユーザーの多要素認証 (MFA) を有効にします。

   手順については、「IAM ユーザーガイド」の AWS アカウント 「ルートユーザーの仮想 MFA デバイスを有効にする (コンソール) 」を参照してください。

管理アクセスを持つユーザーを作成する

1. IAM アイデンティティセンターを有効にします。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「AWS IAM Identity Centerの有効化」を参照してください。
2. IAM アイデンティティセンターで、ユーザーに管理アクセスを付与します。

   を ID ソース IAM アイデンティティセンターディレクトリ として使用する方法のチュートリアルについては、「 ユーザーガイド」の「デフォルト でユーザーアクセス IAM アイデンティティセンターディレクトリを設定するAWS IAM Identity Center 」を参照してください。

管理アクセス権を持つユーザーとしてサインインする

- IAM アイデンティティセンターのユーザーとしてサインインするには、IAM アイデンティティセンターのユーザーの作成時に E メールアドレスに送信されたサインイン URL を使用します。

  IAM Identity Center ユーザーを使用してサインインする方法については、「 AWS サインイン ユーザーガイド」の AWS 「 アクセスポータルにサインインする」を参照してください。

追加のユーザーにアクセス権を割り当てる

1. IAM アイデンティティセンターで、最小特権のアクセス許可を適用するというベストプラクティスに従ったアクセス許可セットを作成します。

手順については、「AWS IAM Identity Center ユーザーガイド」の「権限設定を作成する」を参照してください。

2. グループにユーザーを割り当て、そのグループにシングルサインオンアクセス権を割り当てます。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「グループの参加」を参照してください。

Strategy Recommendations のユーザーと役割

Strategy Recommendations に対して次の 2 つのロールを作成することをお勧めします。

- コンソールにアクセスするには、`AWSMigrationHubFullAccess` および `AWSMigrationHubStrategyConsoleFullAccess` マネージドポリシーの両方をアタッチしたロールを作成します。
- Strategy Recommendations アプリケーションデータコレクターにアクセスするには、`AWSMigrationHubStrategyCollector` マネージドポリシーをアタッチしたロールを作成します。

IAM マネージドポリシーは、ユーザーによるサービスへのアクセスのレベルを定義します。`AWSMigrationHubFullAccess` 管理ポリシーは AWS Migration Hub 、Migration Hub コンソールへのアクセスを許可します。詳細については、「Migration Hub のロールとポリシー」を参照してください。`AWSMigrationHubStrategyConsoleFullAccess` および `AWSMigrationHubStrategyCollector` のマネージドポリシーの詳細については、「AWS マイグレーション・ハブ戦略提言の管理ポリシー」を参照してください。

アクセス権限を付与するには、ユーザー、グループ、またはロールにアクセス許可を追加します。

- のユーザーとグループ AWS IAM Identity Center :

  アクセス許可セットを作成します。「AWS IAM Identity Center ユーザーガイド」の「権限設定を作成する」の手順に従ってください。

- IAM 内で、ID プロバイダーによって管理されているユーザー:

  ID フェデレーションの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) 用のロールの作成」を参照してください。

- IAM ユーザー:
  - ユーザーが担当できるロールを作成します。手順については、「IAM ユーザーガイド」の「IAM ユーザー用ロールの作成」を参照してください。
  - (お奨めできない方法) ポリシーをユーザーに直接アタッチするか、ユーザーをユーザーグループに追加する。詳細については、「IAM ユーザーガイド」の「ユーザー (コンソール) へのアクセス権限の追加」を参照してください。

Strategy Recommendations の開始方法

このセクションでは、Migration Hub Strategy Recommendations の開始方法について説明します。

トピック

Strategy Recommendations の前提条件

Migration Hub Strategy Recommendations 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 アカウントが必要で、ユーザーはこれらのアカウントにセットアップする必要があります。詳細については、「Strategy Recommendations のセットアップ」を参照してください。
- Strategy Recommendations アプリケーションのデータコレクタークライアントは、サーバーからリモートでデータを収集できる必要があります。そのためには、すべての Windows サーバーで機能する一連の認証情報と、すべての Linux サーバーで機能する一連の認証情報を使用する必要があります。認証情報には、サーバーでディレクトリを作成および削除するための、アクセス許可が付与されている必要があります。
- vCenter にデプロイされている コレクターのバージョンは、VMware vCenter Server V6.0、V6.5、V6.7、または V7.0 をサポートしています。

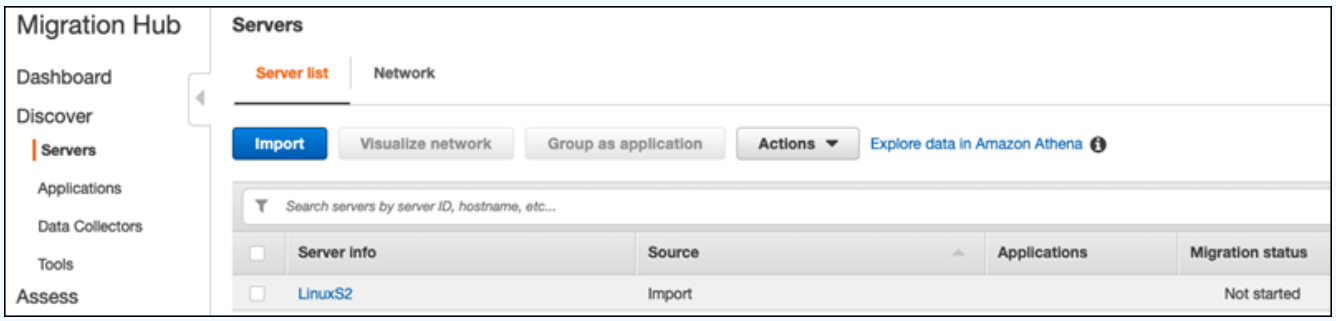
  また、コレクター AMI を使用して、Amazon EC2 インスタンスに コレクターをデプロイすることもできます。
- 使用しているオペレーティングシステム (OS) 環境がサポートされていることを確認します。
  - Linux
    - Amazon Linux 2012.03、2015.03
    - Amazon Linux 2 (2018 年 9 月 25 日更新以降)

    - Ubuntu 12.04、14.04、16.04、18.04、20.04
    - Red Hat Enterprise Linux 5.11、6.10、7.3、7.7、8.1
    - CentOS 5.11、6.9、7.3
    - SUSE 11 SP4、12 SP5
  - Windows
    - Windows Server 2008 R1 SP2、2008 R2 SP1
    - Windows Server 2012 R1、2012 R2
    - Windows Server 2016
    - [Windows Server 2019]
- ソースコード分析では、 リポジトリ GitHub と GitHub エンタープライズリポジトリに、Strategy Recommendations コレクタークライアントと共有できるリポジトリスコープを持つ個人用アクセストークンが必要です。リポジトリスコープを使用した個人用アクセストークンの作成の詳細については、Docs の「個人用アクセストークンの作成」を参照してください。 https://docs.github.com/en/free-pro-team@latest/github/authenticating-to-github/creating-a-personal-access-token GitHub

  Porting Assistant for .NET に関するレコメンデーションの .NET リポジトリを分析するには、Porting Assistant for .NET 移植評価ツールがセットアップされた Windows マシンを用意する必要があります。詳細については、「Porting Assistant for .NET ユーザーガイド」の「Porting Assistant for .NET を開始する」を参照してください。
- データベース分析の Strategy Recommendations を有効にするには、 AWS Secrets Managerで認証情報を入力する必要があります。詳細については、「Strategy Recommendations データベース分析」を参照してください。
- Strategy Recommendations を使用する前に、 AWS Application Discovery Service を使用して AWS Migration Hub コンソールでサーバーとアプリケーションに関するデータを収集する必要があります。データを収集するためには、次のいずれかの方法を使用できます。
  - Migration Hub のインポート — Migration Hub のインポートでは、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。詳細については、「Application Discovery Service ユーザーガイド」の「Migration Hub インポート」を参照してください。
  - AWS Application Discovery Service Agentless Collector – Agentless Collector は、VMware 仮想マシン (VM) に関する情報のみを収集できる VMware アプライアンスです。詳細については、「Application Discovery Service ユーザーガイド」の「エージェントレスコレクター」を参照してください。

- AWS Application Discovery Agent – Discovery Agent は、オンプレミスサーバーと VMs にインストールして、システム情報とシステム間のネットワーク接続の詳細をキャプチャする AWS ソフトウェアです。詳細については、「Application Discovery Service ユーザーガイド」の「AWS Application Discovery Agent」を参照してください。
- Strategy Recommendations データコレクター — サーバーが VMware vCenter でホストされており、アクセスを提供すると、スト Strategy Recommendations がサーバーインベントリを自動的に取得できます。Strategy Recommendations コンソールは、収集した情報を評価に役立てます。

> **Note**
>
> Migration Hub のインポートが正常に完了したことを確認するには、Migration Hub コンソールのナビゲーションペインの [検出] で [サーバー] を選択します。インポートされたすべてのサーバーが表示されます。



ステップ 1: Strategy Recommendations コレクターをダウンロードする

Migration Hub Strategy Recommendations アプリケーションデータコレクターは、オンプレミス VMware 環境にインストールできる、仮想アプライアンスです。Strategy Recommendations アプリケーションデータコレクターは、Amazon マシンイメージ (AMI) としても利用できます。AMI バージョンのコレクターを使用して AWS アプリケーションを評価する場合、またはその他の理由でコレクターをダウンロードする必要はありません。このセクションは飛ばして Amazon EC2 インスタンスに Strategy Recommendations コレクターをデプロイする に進むことができます。

このセクションでは、コレクターを仮想マシン (VM) として VMware 環境にデプロイするために使用するコレクターのオープン仮想化アーカイブ (OVA) ファイルをダウンロードする方法について説明します。

Collector OVA ファイルをダウンロードするには

1. で AWS 作成したアカウントを使用して にサインイン AWS Management Console しStrategy Recommendations のセットアップ、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、[ストラテジー] を選択します。
3. [Migration Hub Strategy Recommendations] ページで、[データコレクターのダウンロード] を選択します。
4. アプリケーションデータをインポートする場合は、オプションで [インポートテンプレートをダウンロード] を選択できます。データのインポートの詳細については、「Strategy Recommendations へのデータのインポート」を参照してください。
5. [レコメンデーションを見る] ボタンをクリックし、[同意する] を選択すると、Migration Hub がお客様のアカウントにサービスリンクロール (SLR) を作成できるようになります。Strategy Recommendations を最初に設定する際には、SLR を作成する必要があります。詳細については、「Strategy Recommendations のサービスリンクロールを使用する」を参照してください。

ステップ 2: Strategy Recommendations コレクターをデプロイする

このセクションでは、Strategy Recommendations アプリケーションデータコレクターのデプロイ方法について説明します。アプリケーションデータコレクターは、サーバー上で実行中のアプリケーションを識別し、ソースコード分析を行い、データベースを分析するエージェントレスのデータコレクターです。

コレクターをデプロイするには、次の 2 通りの方法があります。

- VMware vCenter サーバーに仮想マシン (VM) としてデプロイします。詳細については、「vCenter に Strategy Recommendations コレクターをデプロイする」を参照してください。
- 評価する AWS アプリケーションがある場合は、Strategy Recommendations コレクターの Amazon マシンイメージ (AMI) を使用できます。詳細については、「Amazon EC2 インスタンスに Strategy Recommendations コレクターをデプロイする」を参照してください。

vCenter に Strategy Recommendations コレクターをデプロイする

Migration Hub Strategy Recommendations アプリケーションデータコレクターは、オンプレミス VMware 環境にインストールできる、仮想アプライアンスです。このセクションでは、コレクター

オープン仮想化アーカイブ (OVA) を VMware 環境内の仮想マシン (VM) として デプロイする方法について説明します。

次の手順では、VMware vCenter Server 環境に Strategy Recommendations コレクターをデプロイする方法について説明します。

vCenter に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. ステップ 1 でダウンロードした OVA ファイルをデプロイします。OVA ファイルには、Strategy Recommendations API へのアクセスに使用できるコレクターと CLI が含まれています。

   また、次のリンクから OVA ファイルをダウンロードすることもできます。

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

VM に次の仕様をお勧めします。

Strategy Recommendations コレクター VM の仕様

- RAM — 8 GB 以上
- CPU — 4 個以上

> **Note**
>
> すべての新機能とバグ修正が適用された最新バージョンのコレクターを使用していることを確認するには、コレクターの OVA ファイルをデプロイした後でコレクターをアップグレードしてください。更新する方法については、「Strategy Recommendations のアップグレード」を参照してください。

Amazon EC2 インスタンスに Strategy Recommendations コレクターをデプロイする

評価する AWS アプリケーションがある場合は、Strategy Recommendations アプリケーションデータコレクターの Amazon マシンイメージ (AMI) を使用できます。

次の手順では、Collector AMI から Amazon EC2 インスタンスを起動する方法について説明します。

Collector Amazon EC2 インスタンスをデプロイするには

1. Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。
2. 画面の上のナビゲーションバーで、現在の リージョンが表示されます (例: 米国東部 (オハイオ))。Strategy Recommendations が使用するリージョンから、ニーズに合ったリージョンを選択します。これらのリージョンのリストについては、「AWS 全般のリファレンス」の「Strategy Recommendations エンドポイント」を参照してください。
3. ナビゲーションペインの [イメージ] で、[AMI] を選択します。
4. [自己所有]ドロップダウンから、[公開イメージ] を選択します。
5. 検索バーを選択し、メニューから [AMI の名前] を選択します。
6. AWSMHubApplicationDataCollector という名前を入力します。
7. AMI が安全なソースからのものであることを確認するには、アカウントの所有者が 703163444405 であることを確認してください。
8. この AMI からインスタンスを起動するには、インスタンスを選択し、[起動] を選択します。コンソールを使用してインスタンスを起動する方法の詳細については、Amazon EC2 ユーザーガイド」の「AMI からのインスタンスの起動」を参照してください。

   Amazon EC2 には、次の仕様をお勧めします。

   Strategy Recommendations コレクター Amazon EC2 インスタンス仕様

   - RAM — 8 GB 以上
   - CPU — 4 個以上

Strategy Recommendations AMI には、Strategy Recommendations API へのアクセスに使用できるコレクターと CLI が含まれています。

> **Note**
>
> すべての新機能とバグ修正が適用された最新バージョンのコレクターを使用していることを確保するには、Strategy Recommendations コレクターを Amazon EC2 インスタンスとしてデプロイ後にコレクターをアップグレードします。更新する方法については、「Strategy Recommendations のアップグレード」を参照してください。

ステップ 3: Strategy Recommendations コレクターにサインインする

このセクションでは、デプロイされた Migration Hub Strategy Recommendations アプリケーションデータコレクターにサインインする方法を説明します。コレクターへのサインイン方法は、コレクターをどのようにデプロイしたかによって異なります。

- vCenter ベースの環境にデプロイされたコレクターにサインインします。
- Amazon EC2 インスタンスとしてデプロイされているコレクターにサインインする

vCenter ベースの環境にデプロイされたコレクターにサインインします。

vCenter ベースの環境にデプロイされた Strategy Recommendations コレクターにサインインするには

1. SSH クライアントを使用してコレクターに接続する場合は、次のコマンドを使用します。

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

2. パスワードの入力を求められたら、デフォルトパスワード aq1@WSde3 を入力します。初回サインイン時にパスワードを変更する必要があります。

Amazon EC2 インスタンスとしてデプロイされているコレクターにサインインする

Amazon EC2 インスタンスとしてデプロイされた Strategy Recommendations Collector にサインインするには

- SSH クライアントを使用してコレクターに接続する場合は、次のコマンドを使用します。

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

  Keyname.pem は、Amazon EC2 インスタンスをコレクター AMI から起動したときに生成されたプライベートキーです。

ステップ 4: Strategy Recommendations コレクターをセットアップする

このセクションでは、`collector setup` コマンドラインコマンドを使用して Migration Hub Strategy Recommendations アプリケーションデータコレクターを設定する方法について説明します。これらの構成はローカルに保存されます。

`collector setup` コマンドを使用する前に、以下の `docker exec` コマンドを使用してコレクターの Docker コンテナーに bash シェルセッションを作成する必要があります。

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

`collector setup` コマンドは以下のコマンドをすべて連続して実行しますが、個別に実行することもできます。

- `collector setup --aws-configurations` — AWS 設定をセットアップします。
- `collector setup --vcenter-configurations` — vCenter 設定をセットアップします。

> **Note**
>
> vCenter の設定は、コレクターが vCenter でホストされている場合にのみ使用できます。ただし、`collector setup --vcenter-configurations` コマンドを使用して vCenter 設定を強制的にセットアップできます。

- `collector setup --remote-server-configurations` — リモートサーバー設定をセットアップします。
- `collector setup --version-control-configurations` — バージョン管理設定をセットアップします。

すべてのコレクター設定を同時にセットアップするには

1. 次のコマンドを入力します。

   ```
   collector setup
   ```

2. AWS 設定をセットアップする の説明に従って AWS 設定の情報を入力します。
3. vCenter 設定をセットアップする の説明に従って、vCenter 構成の情報を入力します。

4. リモートサーバー設定をセットアップする の説明に従って、リモートサーバー設定の情報を入力します。
5. バージョン管理設定をセットアップする の説明に従って、バージョン管理設定の情報を入力します。
6. リモート Windows サーバーと Linux サーバーをデータ収集用に準備します。 の指示に従って、Windows サーバと Linux サーバーをコレクターデータ収集用に準備します。

AWS 設定をセットアップする

`collector setup` コマンドまたは `collector setup --aws-configurations` コマンドを使用するときに、AWS 構成をセットアップするには。

1. 「IAM 権限を設定しましたか...」という質問に、「はい」を意味する「Y」を入力します。これらのアクセス許可は、Strategy Recommendations のユーザーと役割 の手順に従って `AWSMigrationHubStrategyCollector` マネージドポリシーを使用してコレクターにアクセスするユーザーを作成したときに設定します。
2. Strategy Recommendations のユーザーと役割 の手順に従って、コレクターにアクセスするために作成したユーザーがいる AWS アカウントから、アクセスキーとシークレットキーを入力します。
3. リージョンを入力します (例: `us-west-2`)。ストラテジーレコメンデーションが使用するリージョンから、ニーズに合ったリージョンを選択します。これらのリージョンのリストについては、「AWS 全般のリファレンス」の「ストラテジーレコメンデーションエンドポイント」を参照してください。
4. 「コレクター関連のメトリックを移行ハブ戦略サービスにアップロードしますか?」という質問に、「はい」を意味する「Y」を入力します。メトリクス情報は、AWS が適切なサポートを提供するのに役立ちます。
5. 「コレクター関連ログをマイグレーションハブストラテジーサービスにアップロードしますか?」という質問に、「はい」を意味する「Y」と入力します。ログからの情報は、AWS が適切なサポートを提供するのに役立ちます。

次の例は、AWS 設定のエントリの例を含め、表示される内容を示しています。

```
Have you setup IAM permissions in you AWS account as per the user guide? [Y/N]: Y
Choose one of the following options for providing user credentials:
1. Long term AWS credentials
```

```
2. Temporary AWS credentials
Enter your options [1-2]: 2
AWS session token:
AWS access key ID [None]:
AWS secret access Key [None]:
AWS region name [us-west-2]:
AWS configurations are saved successfully
Upload collector related metrics to migration hub strategy service? By default
 collector will upload metrics. [Y/N]: Y
Upload collector related logs to migration hub strategy service? By default collector
 will upload logs. [Y/N]: Y
Application data collector configurations are saved successfully
Start registering application data collector
Application data collector is registered successfully.
```

vCenter 設定をセットアップする

`collector setup` コマンドまたは `collector setup --vcenter-configurations` コマンドを使用するときに vCenter 構成をセットアップするには:

1. VMware vCenter 認証情報を使用して認証する場合は、「VMware vCenter 認証情報を使用して認証しますか?」という質問に「はい」を意味する「Y」を入力します。

   > **Note**
   >
   > VMware vCenter 認証情報を使用して認証するには、VMware ツールがターゲットサーバーにインストールされている必要があります。

   ホスト URL を入力します。これは vCenter IP アドレスまたは URL のどちらでもかまいません。次に、VMware vCenter の ユーザー名 と パスワード を入力します。

2. Windows サーバーを設定する場合は、「VMware vCenter によって管理されている Windows マシンはありますか?」という質問に「はい」を意味する「Y」を入力します。

   Windows のユーザー名とパスワードを入力します。

> **Note**
>
> お使いの Windows リモートサーバーが Active Directory ドメインに属している場合、CLI を使用してリモートサーバーの設定を行う際には、ユーザ名を *domain-name**username* として入力する必要があります。たとえば、ドメインの名前が exampledomain で、ユーザー名が管理者の場合、CLI に入力するユーザー名は exampledomain\Administrator になります。

3. Linux サーバーを設定する場合は、「VMware vCenter を使用する Linux のセットアップをしますか?」の質問に「はい」を意味する「Y」を入力します。

   Linux 用のユーザーネームとパスワードを入力します。

4. vCenter 以外のサーバーのリモートサーバー認証情報を設定する場合は、「Windows では NTLM を使用し、Linuxでは SSH/Cert ベースを使用して vCenter 外部のサーバーの認証情報を設定しますか?」という質問に、「はい」を意味する「Y」を入力します。

5. vCenter の外部で管理されている Windows マシンの認証情報が、vCenter Windows マシンの認証情報を構成するときに提供された認証情報と同じであれば、「vCenter のセットアップ時に使用したものと同じ Windows 認証情報を使用しますか?」という質問に「はい」を意味する「Y」を入力します。それ以外の場合は、「いいえ」を意味する「N」を入力します。

   「はい」を意味する「Y」と答えると、次の質問が表示されます。

   a. 「Windows サーバーとの最初の対話中に、コレクターがユーザーに代わってサーバー証明書を受け入れてローカルに保存しても問題ありませんか?」という質問に「はい」を意味する「Y」を入力します。

   b. SSH 認証を設定する場合は、「オプションを入力してください」の質問に「1」を入力します。

      SSH 認証を使用する場合は、生成されたキー認証情報を Linux サーバーにコピーする必要があります。詳細については、「Linux サーバーでのキーベース認証をセットアップする」を参照してください。

次の例は、VMware vCenter 設定の入力例を含め、表示される内容を示しています。

```
Your Linux remote server configurations are saved successfully.
collector setup –vcenter-configurations
```

```
Start setting up vCenter configurations for remote execution
Note: Authenticating using VMware vCenter credentials requires VMware tools to be
 installed on the target servers
Would you like to authenticate using VMware vCenter credentials? [Y/N]: y

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

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

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

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

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

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

リモートサーバー設定をセットアップする

`collector setup` コマンドまたは `collector setup --remote-server-configurations` コマンドを使用するときにリモートサーバー設定をセットアップするには:

1. Windows サーバーを設定する場合は、「Windows 用 NLTM を使用して vCenter で管理されていないサーバーの認証情報をセットアップしますか?」という質問に「はい」を意味する「Y」を入力します。

   WinRM 用の[ユーザーネーム] と [パスワード] を入力します。

   > **Note**
   >
   > お使いの Windows リモートサーバーが Active Directory ドメインに属している場合、CLI を使用してリモートサーバーの設定を行う際には、ユーザ名を *domain-name**username* として入力する必要があります。たとえば、ドメインの名前が exampledomain で、ユーザー名が管理者の場合、CLI に入力するユーザー名は exampledomain\Administrator になります。

「Windows サーバーとの最初の対話中に、コレクターがユーザーに代わってサーバー証明書を受け入れてローカルに保存しても問題ありませんか?」という質問に「はい」を意味する「Y」を入力します。Windows サーバー証明書はディレクトリ `/opt/amazon/application-data-collector/remote-auth/windows/certs` に保存されます。

生成されたサーバー認証情報を Windows サーバーにコピーする必要があります。詳細については、「Windows サーバーでリモートサーバー構成をセットアップする」を参照してください。

2. Linux サーバーを設定する場合は、「SSH または Cert を使用する Linux のセットアップをしますか?」の質問に、「はい」を意味する「Y」と入力します。
3. SSH キーベースの認証を設定する場合は、「オプションを入力してください」の質問に「1」を入力します。

   SSH 認証を使用する場合は、生成されたキー認証情報を Linux サーバーにコピーする必要があります。詳細については、「Linux サーバーでのキーベース認証をセットアップする」を参照してください。
4. 証明書ベースの認証を設定する場合は、「オプションを入力してください」の質問に「2」を入力します。

   証明書ベースの認証の設定に関する詳細については、「Linux サーバーでの証明書ベースの認証をセットアップする」を参照してください。

次の例は、リモートサーバー設定の入力例を含め、表示される内容を示しています。

```
Setting up target server for remote execution
Would you like to setup credentials for servers not managed by vCenter using NLTM for
 Windows [Y/N]: y

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

Username for WinRM (Domain\User): username
Password for WinRM: password
Reenter password for WinRM: password
Are you okay with collector accepting and locally storing server certificates on your
 behalf during first interaction with windows servers? These certificates will be used
 by collector for secure communication with windows servers [Y/N]: Y
Successfully stored windows server credentials...
```

```
Please note that all windows server certificates are stored in directory /opt/amazon/
application-data-collector/remote-auth/windows/certs

Please note the IP address of the collector and run the script specified in the user
 documentation on all the windows servers in your inventory
Would you like to setup credentials for servers not managed by vCenter using SSH/Cert
 based for Linux? [Y/N]: Y
Choose one of the following options for remote authentication:
1. SSH based authentication
2. Certificate based authentication
Enter your options [1-2]: 1
User name for remote server: username
Generating SSH key on this machine...
SSH key pair path: /opt/amazon/application-data-collector/remote-auth/linux/keys/
id_rsa_assessment
Please add the public key "id_rsa_assessment.pub" to the "$HOME/.ssh/authorized_keys"
 file in your remote machines.
Your Linux remote server configurations are saved successfully.
```

バージョン管理設定をセットアップする

`collector setup` コマンドまたは `collector setup --version-control-configurations` コマンドを使用するときにバージョンコントロール設定をセットアップするには:

1. 「ソースコード分析のセットアップをしますか?」という質問に、「はい」を意味する「Y」を入力します。
2. Git サーバーのエンドポイントを設定する場合は、「オプションを入力してください」の質問に「1」を入力します。

   GIT サーバーエンドポイントとして,github.com と入力します。
3. GitHub Enterprise Server を設定したいなら、「オプションを入力してください」の質問に「2」を入力します。

   次のように、https:// を付けずにエンタープライズ エンドポイントを入力します。GIT サーバーエンドポイント: *git-enterprise-endpoint*
4. Git *######################*。
5. 「Windows マシンで分析すべき csharp リポジトリはありますか?」という質問に C# コードを分析する場合、「はい」を意味する「Y」を入力します。

> **Note**
>
> Porting Assistant for .NET に関するレコメンデーションの .NET リポジトリを分析するには、Porting Assistant for .NET 移植評価ツールがセットアップされた Windows マシンを用意する必要があります。詳細については、「Porting Assistant for .NET ユーザーガイド」の「Porting Assistant for .NET を開始する」を参照してください。

6. 「このマシンで既存の Windows 認証情報を再利用しますか?」といつ質問の場合。C# ソースコード分析用の Windows マシンが、`--remote-server-configurations` または `--vcenter-configurations` のセットアップ時に以前に提供した認証情報と同じ認証情報を使用している場合は、「はい」を意味する「Y」を入力します。

   新しい認証情報を入力する場合は、「いいえ」の場合は「N」を入力します。

7. VMware vCenter Windows マシンの認証情報を使用するには、Windows 認証情報の次のオプションのいずれかを選択してください に 「1」を入力します。
8. Windows マシンの IP アドレスを入力します。

次の例は、バージョン制御設定のエントリの例を含め、表示される内容を示しています。

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

```
Using VMWare vCenter Windows Machine credentials
Successfully stored windows server credentials...
```

リモート Windows サーバーと Linux サーバーをデータ収集用に準備します。

> **Note**
>
> vCenter 認証情報を使用して Strategy Recommendations アプリケーションデータコレクターを設定する場合、この手順は必要ありません。

リモートサーバーの設定後、`collector setup command` または `collector setup --remote-server-configurations` コマンドを使用している場合は、Strategy Recommendations アプリケーションのデータコレクターがリモートサーバーからデータを収集できるようにリモートサーバーを準備する必要があります。

> **Note**
>
> プライベート IP アドレスを使用してサーバーにアクセスできることを確認する必要があります。リモート実行用に AWS の仮想プライベートクラウド (VPC) を介して環境を設定する方法の詳細については、Amazon Virtual Private Cloud ユーザーガイドを参照してください。

リモート Linux サーバーを準備するには、「リモート Linux サーバーを準備します。」を参照してください。

リモート Windows サーバーを準備するには、「Windows サーバーでリモートサーバー構成をセットアップする」を参照してください。

リモート Linux サーバーを準備します。

Linux サーバーでのキーベース認証をセットアップする

リモートサーバーの設定時に Linux に SSH キーベース認証を設定する場合は、Strategy Recommendations アプリケーションデータコレクターがデータを収集できるように、以下の手順を実行してサーバー上でキーベース認証を設定する必要があります。

Linux サーバーでキーベース認証をセットアップするには

1. id_rsa_assessment.pub という名前で生成された公開鍵を、コンテナ内の次のフォルダーからコピーします。

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

2. コピーした公開鍵をすべてのリモートマシンの `$HOME/.ssh/authorized_keys` ファイルに追加します。使用可能なファイルがない場合は、`touch` または `vim` コマンドを使用して作成します。
3. リモートサーバーのホームフォルダーのアクセス許可レベル 755 以下であることを確認してください。777 でない場合、動作しません。`chmod` コマンドを使用してアクセス許可を制限できます。

Linux サーバーでの証明書ベースの認証をセットアップする

リモートサーバーの設定時に Linux に証明書ベース認証を設定する場合は、Strategy Recommendations アプリケーションデータコレクターがデータを収集できるように、以下の手順を実行する必要があります。

既に Certificate Authority (CA) がアプリケーションサーバーに設定されている場合は、このオプションをお勧めします。

Linux サーバーで証明書ベースの認証をセットアップするには

1. すべてのリモートサーバーで機能するユーザー名をコピーします。
2. コレクターの公開鍵を CA にコピーします。

   コレクターの公開鍵は次の場所にあります。

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

   証明書を生成するには、この公開鍵を CA に追加する必要があります。
3. 前のステップで生成された証明書をコレクター内の次の場所にコピーします。

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

   証明書の名前は id_rsa_assessment-cert.pub である必要があります。
4. セットアップの手順で証明書ファイル名を指定します。

Windows サーバーでリモートサーバー構成をセットアップする

コレクターのセットアップでリモート サーバー構成を構成するときに Windows のセットアップを選択した場合は、Strategy Recommendations がデータを収集できるように次の手順を実行する必要があります。

> リモートサーバーで実行される PowerShell スクリプトの詳細については、このメモをお読みください。
>
> このスクリプトは PowerShell リモートを有効にし、ネゴシエート以外のすべての認証方法を無効にします。これは Windows NT LAN Manager (NTLM) に使用され、"AllowUnencrypted" WSMman プロトコルを false に設定して、新しく作成されたリスナーが暗号化されたトラフィックのみを受け付けるようにします。Microsoft が提供しているスクリプト `New-SelfSignedCertificateEx.ps1` を使用して、自己署名証明書を作成します。
> HTTP リスナーを持つ WSMan インスタンスは、既存の HTTPS リスナーとともに削除されます。次に、新しい HTTPS リスナーを作成します。また、TCP ポート 5986 のインバウンドファイアウォールルールも作成します。最後のステップでは、WinRM サービスが再起動されます。

Windows 2008 サーバーのリモート接続によるデータ収集をセットアップするには

1. サーバーにインストールされている PowerShell のバージョンを確認するには、次のコマンドを使用します。

   ```
   $PSVersionTable
   ```

2. PowerShell のバージョンが 5.1 でない場合は、Microsoft ドキュメントの「WMF 5.1 のインストールと設定」の手順に従って WMF 5.1 をダウンロードしてインストールします。
3. 新しい PowerShell ウィンドウで次のコマンドを使用して、PowerShell 5.1 がインストールされていることを確認します。

   ```
   $PSVersionTable
   ```

4. Windows 2012 以降でリモート接続によるデータ収集を設定する方法を説明する次の手順に従います。

Windows 2012 以降のサーバーでリモート接続によるデータ収集をセットアップするには

1. 次の URL から設定スクリプトをダウンロードします。

   https://application-data-collector-release.s3.us-west-2.amazonaws.com/scripts/WinRMSetup.ps1
2. 次の URL から `New-SelfSignedCertificateEx.ps1` をダウンロードし、ダウンロードした `WinRMSetup.ps1` と同じフォルダにスクリプトを貼り付けます。

   https://github.com/Azure/azure-libraries-for-net/blob/master/Samples/Asset/New-SelfSignedCertificateEx.ps1
3. セットアップを完了するには、ダウンロードした PowerShell スクリプトをすべてのアプリケーションサーバーで実行します。

   ```
   .\WinRMSetup.ps1
   ```

> **Note**
>
> Windows リモート管理 (WinRM) が Windows リモートサーバーで正しく設定されていない場合、そのサーバーからデータを収集しようとすると失敗します。その場合は、そのサーバーに対応する証明書をコンテナの次の場所から削除する必要があります。/opt/amazon/application-data-collector/remote-auth/windows/certs/***ads-server-id***.cer 証明書を削除後、データ収集プロセスが再試行されるまでお待ちください。

コレクターとサーバーがデータ収集用に設定されていることを確認する

次のコマンドで、コレクターとサーバーがデータ収集用に正しく設定されていることを確認します。

```
collector diag-check
```

このコマンドは、サーバー構成について一連の診断チェックを行い、チェックに失敗した場合は情報を表示します。

コマンドを -a モードで使用すると、チェックの完了後に DiagnosticCheckResult.txt ファイルに出力が表示されます。

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

1 つのサーバーのサーバー構成を、そのサーバーの IP アドレスを使用して診断チェックできます。

次の例は、成功したセットアップの統合を示しています。

[Linux サーバー]

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

Windows Server

```
            Windows PowerShell Version Check succeeded
Provide your test server IP address: IP address
-------------------------------------------------------------
Start checking connectivity & credentials...
Connectivity and Credential Checks succeeded
-------------------------------------------------------------
Start checking permissions...
Permission Check succeeded
-------------------------------------------------------------
Start checking OS version...
OS version check succeeded
-------------------------------------------------------------
Start checking Windows architecture type...
Windows Architecture Type Check succeeded
-------------------------------------------------------------
```

```
All diagnostic checks complete successfully.
This server is correctly set up and ready for data collection.
```

次の例は、リモートサーバーの資格情報が間違っている場合に表示されるエラーメッセージを示しています。

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

ステップ 5: Migration Hub コンソールの Strategy Recommendations を使用してレコメンデーションを取得する

このセクションでは、Migration Hub コンソールの Strategy Recommendations を使用して移行のレコメンデーションを初めて取得する方法について説明します。

推奨事項を取得するには

1. Strategy Recommendations のセットアップ で作成した AWS アカウントを使用して、AWS Management Console にサインインし、https://console.aws.amazon.com/migrationhub/ にある Migration Hub コンソールを開きます。
2. Migration Hub コンソールのナビゲーションペインで、[ストラテジー] を選択します。
3. [Migration Hub Strategy Recommendations] ページで、[レコメンデーションを取得] を選択します。
4. Migration Hub がサービスリンクロール (SLR) をアカウントに対して作成することを許可することに同意する場合は、[同意する] を選択します。SLR の詳細については、「Strategy Recommendations のサービスリンクロールを使用する」を参照してください。
5. [データソースを設定]

    a. [データソースの設定] ページでは、分析するサーバーのソースを以下のオプションから選択する必要があります。

i. Strategy Recommendations データコレクター — Strategy Recommendations コレクターを使用して、VMware vCenter でホストされている VM に関する情報を自動的に取得できます。このオプションを使用すると、追加の設定を行う必要はありません。

ii. 手動インポート — サーバーとアプリケーションに関するデータを個別に取り込む場合は、Strategy Recommendations インポートテンプレートを使用できます。インポートテンプレートは JSON ファイルで、VM に関する利用可能な情報を入力できます。

iii. Application Discovery Service — Application Discovery Service を使用して、オンプレミスのアプリケーションとサーバーに関する情報を収集できます。Migration Hub コンソールの [ツール] セクションでは、[検出ツール] にある複数のオプションから選択できます。たとえば、[Application Discovery Service Agentless Collector]、[AWS 検出エージェント]、または [インポート] (CSV ファイルの場合) を選択できます。

b. [サーバー] テーブルには、データソースセクションでの選択に基づいて、使用可能なすべてのサーバーが一覧表示されます。

c. [登録済みアプリケーションデータコレクター] に、設定したアプリケーションデータコレクターが表示されます。データコレクターをまだ設定していない場合は、データコレクターをダウンロードしてデプロイできます。詳細については、「ステップ 1: Strategy Recommendations コレクターをダウンロードする」と「ステップ 2: Strategy Recommendations コレクターをデプロイする」を参照してください。

> **Note**
>
> Strategy Recommendations を取得するには、少なくとも 1 つのアプリケーションデータコレクターを設定するか、アプリケーションデータのインポートを実行する必要があります。コレクターを設定せずにアプリケーションレベルのデータを追加したい場合は、アプリケーションデータインポートテンプレートを使用できます。後で追加のデータソースを追加できます。

d. [手動インポート] を選択した場合は、[インポートの詳細] で [新しいインポートを追加] を選択します。

e. [インポート名] に、インポートの名前を入力します。

f. [S3 バケット URI] には、インポート JSON ファイルのアップロード先の S3 バケット URI を入力します。

> **Important**
>
> S3 バケット名は **`migrationhub-strategy`** のプレフィックスで始まる必要があります。

g. [次へ] をクリックします。

6. [プリファレンスを指定]

   a. [プリファレンスの指定] ページで、ビジネス目標とマイグレーションプリファレンスを設定します。Strategy Recommendations は、指定した設定に基づいて、アプリケーションとデータベースを移行とモダナイズするための最適な戦略をレコメンデーションします。この設定は後で変更できます。

   b. [次へ] をクリックします。

7. [確認して送信します]。

   a. 設定したデータソースと移行設定を確認してください。

   b. すべて正しければ、[データ分析を開始] を選択します。これにより、サーバーインベントリとランタイム環境、および Microsoft IIS および Java アプリケーションのアプリケーションバイナリの分析が実行されます。

> **Note**
>
> バイナリ分析のステータスはコンソールには表示されません。分析が完了すると、アンチパターンレポートへのリンクまたは分析が失敗したことを示すメッセージが表示されます。

Strategy Recommendations のレコメンデーション

このセクションでは、移行ポートフォリオに含まれるサーバーとアプリケーションについて、Strategy Recommendations の移行とモダナイズのレコメンデーションを確認する方法について説明します。

トピック

Strategy Recommendations での戦略的レコメンデーションの表示

このセクションでは、 AWS Migration Hub コンソールで Strategy Recommendations を使用して移行戦略の推奨事項を表示する方法について説明します。

Strategy Recommendations を表示するには

1. で AWS 作成したアカウントを使用して にサインイン AWS Management Console しStrategy Recommendations のセットアップ、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、[ストラテジー] を選択し、次に [レコメンデーション] を選択します。
3. [レコメンデーション] ページでは、ポートフォリオのレコメンデーションの概要と移行「R」ストラテジーの詳細なレコメンデーションを表示およびエクスポートできます。また、移行やモダナイゼーションのツールや移行先、サーバーやアプリケーションコンポーネントのアンチパターンも表示できます。

   アンチパターンは、ポートフォリオで見つかった既知の問題を、重大度別に分類したリストです。重要度が高いアンチパターンは解決が必要な非互換性を表し、重要度が中程度のアンチパターンは警告を表し、重要度が低いアンチパターンは情報上の問題を表します。「R」戦略について詳しくは、「AWS 規範ガイダンス用語集」の「移行用語 - 7 R」を参照してください。

- データセンターに変更が生じた場合や、設定を更新した場合は、データを再分析することをお勧めします。データを再分析して新しいレコメンデーションを取得するには、[データの再分析] を選択します。

  再分析プロセスが完了するまでは、レコメンデーションデータの結果は以前のデータと新しいデータが混在することができます。

  レコメンデーションを含むレポートファイルをダウンロードするには、[レコメンデーションをエクスポート] を選択します。

4. [アプリケーションコンポーネント] タブでは、移行ポートフォリオに含まれるアプリケーションコンポーネントのレコメンデーションを確認できます。詳細については、「Strategy Recommendations アプリケーションコンポーネントレコメンデーション」を参照してください。
5. [サーバー] タブでは、移行ポートフォリオに含まれるサーバーに関するレコメンデーションを確認できます。詳細については、「Strategy Recommendations サーバーレコメンデーション」を参照してください。
6. [プリファレンス] タブでは、ステップ 5: レコメンデーションを取得する で指定したプリファレンスを編集できます。プリファレンスの編集については、「Strategy Recommendations 設定」を参照してください。

Strategy Recommendations アプリケーションコンポーネントレコメンデーション

このセクションでは、Migration Hub コンソールで Strategy Recommendations を使用してアプリケーションコンポーネント用の移行戦略のレコメンデーションを表示し、分析する方法について説明します。

トピック

- Strategy Recommendations におけるアプリケーションコンポーネントの操作
- Strategy Recommendations ソースコード分析
- Strategy Recommendations データベース分析
- Strategy Recommendations バイナリ分析

Strategy Recommendations におけるアプリケーションコンポーネントの操作

このセクションでは、Migration Hub コンソールの Migration Hub Strategy Recommendations を使用して、移行とモダナイズ戦略のレコメンデーションを表示および設定する方法について説明します。

トピック

アプリケーションコンポーネントのレコメンデーションを表示する

このセクションでは、Migration Hub コンソールで Strategy Recommendations を使用してアプリケーションコンポーネント用の移行戦略のレコメンデーションを表示する方法について説明します。

アプリケーションコンポーネントのレコメンデーションの詳細を表示するには

1. で AWS 作成したアカウントを使用して にサインイン AWS Management Console しStrategy Recommendations のセットアップ、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、[ストラテジー] を選択し、次に [レコメンデーション] を選択します。
3. [レコメンデーション] ページで、[アプリケーションコンポーネント] タブを選択します。

    a. [アプリケーションコンポーネントの概要] には、サーバーポートフォリオ内で実行しているさまざまなタイプのアプリケーションコンポーネントの概要が表示されます。

    b. [アプリケーションコンポーネント] には、コンポーネント名、コンポーネントタイプ、および移行「R」戦略のレコメンデーションが表示されます。また、移行先や、サーバーポートフォリオ内で稼働しているさまざまなアプリケーションコンポーネントに使用する移行ツールやモダナイズツールも表示できます。「R」戦略について詳しくは、「AWS 規範ガイダンス用語集」の「移行用語 - 7 R」を参照してください。
4. アプリケーションコンポーネントの詳細を表示するには、アプリケーションコンポーネントを選択し、[詳細を表示] を選択します。
5. アプリケーションコンポーネントの詳細ページ (見出しがコンポーネント名のページ) の [レコメンデーションの概要] で、そのアプリケーションコンポーネントの [レコメンデーション] を表示

できます。特定された [アンチパターン] も表示できます。アンチパターンは、ポートフォリオで見つかった既知の問題を、重大度別に分類したリストです。

6. [Strategy オプション] タブを選択すると、アプリケーションコンポーネントの移行に関する推奨事項が表示されます。推奨ストラテジーは、別のストラテジーを選択し、[優先設定] を選択することでオーバーライドできます。
7. 表示しているアプリケーションコンポーネントのタイプに応じて、[ソース設定] タブまたは [データベース設定] タブがあります。[ソースの設定] の詳細については、「アプリケーションコンポーネントのソースコード分析を設定する」を参照してください。[データベース設定] についての詳細は、「アプリケーションコンポーネントのデータベース分析を設定する」を参照してください。

アプリケーションコンポーネントのソースコード分析を設定する

このセクションでは、Migration Hub コンソールで Strategy Recommendations を使用してアプリケーションコンポーネントのソースコード分析を設定する方法について説明します。

アプリケーションコンポーネントのソースコード分析を設定するには

1. Migration Hub コンソールのナビゲーションペインで、[ストラテジー] を選択し、次に [レコメンデーション] を選択します。
2. [レコメンデーション] ページで、[アプリケーションコンポーネント] タブを選択します。
3. [アプリケーションコンポーネント] の下のコンポーネントのリストから、コンポーネントの種類が [java]、[dotnetframework]、または [IIS] のアプリケーション コンポーネントを選択し、[詳細の表示] を選択します。
4. アプリケーションコンポーネントの詳細ページ (コンポーネントの名前が見出しになっているページ) で、[ソースコード設定] タブを選択します。
5. [ソースコード設定の詳細] で、[ソースコードの分析] を選択します。
6. [ソースコードの分析] ページで、アプリケーションコンポーネントのソースコードを格納するリポジトリ名、ブランチ名、およびプロジェクト名 (該当する場合) を指定します。使用する GitHub ソースコードのバージョン管理のタイプを選択し、分析 を選択します。

   分析が完了すると、アプリケーションコンポーネントの詳細ページで更新されたレコメンデーションを確認できます。

ソースコード分析の詳細については、「Strategy Recommendations ソースコード分析」を参照してください。

アプリケーションコンポーネントのデータベース分析を設定する

このセクションでは、Migration Hub コンソールで Strategy Recommendations を使用してアプリケーションコンポーネントのデータベース分析を設定する方法について説明します。

アプリケーションコンポーネントのデータベース分析を設定するには

1. Migration Hub コンソールのナビゲーションペインで、[ストラテジー] を選択し、次に [レコメンデーション] を選択します。
2. [レコメンデーション] ページで、[アプリケーションコンポーネント] タブを選択します。
3. [アプリケーションコンポーネント] の下にあるコンポーネントのリストから、コンポーネントタイプが [SQLServer] のアプリケーションコンポーネントを選択し、[詳細を表示] を選択します。
4. アプリケーションコンポーネントの詳細ページ (コンポーネントの名前が見出しになっているページ) で、[データベース設定] タブを選択します。
5. [データベース設定の詳細] で、[データベース詳細の分析] を選択します。
6. AWS Secrets Manager で作成したデータベース認証情報に使用するシークレット名をドロップダウンメニューから選択し、[分析] を選択します。

   分析が完了すると、アプリケーションコンポーネントの詳細ページで更新されたレコメンデーションを確認できます。

データベース分析とシークレットネームの設定の詳細については、「Strategy Recommendations データベース分析」を参照してください。

Strategy Recommendations ソースコード分析

Migration Hub Strategy Recommendations は、ポートフォリオ内のアプリケーションを自動的に識別し、そのアプリケーションコンポーネントを作成します。たとえば、ポートフォリオに Java アプリケーションがある場合、そのアプリケーションはコンポーネントタイプが Java のアプリケーションコンポーネントとして識別されます。

Strategy Recommendations は、アプリケーションコンポーネントのソースコードを分析するように設定した場合、そのソースコードを分析します。ソースコード分析用のアプリケーションコンポーネントの設定については、「アプリケーションコンポーネントのソースコード分析を設定する」を参照してください。

Strategy Recommendations は Java と C# プログラミング言語のソースコード分析を行います。

Strategy Recommendations のソースコード分析を使用するための前提条件については、「Strategy Recommendations の前提条件」を参照してください。

Strategy Recommendations データベース分析

Strategy Recommendations は、ポートフォリオ内のデータベースサーバーを自動的に識別し、そのサーバー用のアプリケーションコンポーネントを作成します。たとえば、ポートフォリオに SQL Server データベースがある場合、そのデータベースはアプリケーションコンポーネント sqlservr.exe として識別されます。

Strategy Recommendations は、 AWS Schema Conversion Tool を使用して、特定された SQL Server アプリケーションコンポーネント sqlservr.exe 内の個々のデータベースを分析します。Strategy Recommendations は、データベースを Amazon Aurora MySQL 互換エディション、Amazon Aurora PostgreSQL 互換エディション、Amazon RDS for MySQL、Amazon RDS for PostgreSQL などの AWS データベースに移行する際の非互換性も特定します。

現在、Strategy Recommendations データベース分析は SQL Server でのみ利用できます。

Strategy Recommendations を設定してデータベースを分析するには、Strategy Recommendations アプリケーションデータコレクターがデータベースに接続するための認証情報を入力する必要があります。これを行うには、 AWS アカウントの AWS Secrets Manager にシークレットを作成します。

指定する認証情報のアクセス許可と権限については、「AWS Schema Conversion Tool 認証情報に必要な権限」を参照してください。認証情報を使用したシークレットの作成の詳細については、「Secrets Manager でデータベース認証情報用のシークレットの作成」を参照してください。

認証情報とシークレットを設定したら、データベースサーバーで AWS Schema Conversion Tool 分析を設定できます。詳細については、「アプリケーションコンポーネントのデータベース分析を設定する」を参照してください。

アプリケーションコンポーネントのデータベース分析を設定すると、 AWS Schema Conversion Tool インベントリタスクがスケジュールされます。このタスクが完了すると、そのデータベースサーバー上の個々のデータベースごとに、新しいアプリケーションコンポーネントが作成されているのがわかります。たとえば、SQL Server に 2 つのデータベース (exampledbs1 と exampledbs2) がある場合、データベースごとに exampledbs1 と exampledbs2 という名前のアプリケーションコンポーネントが作成されます。

特定した各データベースを AWS データベースに移行する際にアンチパターンを確認したい場合は、アプリケーションコンポーネントのデータベース分析を設定する の手順に従って各データベースの分析を設定します。

AWS Schema Conversion Tool 認証情報に必要な権限

AWS Secrets Manager に提供するサインイン認証情報は、 `VIEW SERVER STATE`と `VIEW ANY DEFINITION` 権限のみを必要とします。オプションで、https://gitlab.aws.dev/dmaf-pub/dmaf/-/blob/master/create_mssql_ro_user.sql にあるスクリプトを使用して新しいログインを作成できます。

SQL Server ログインを作成するときには、任意のログイン名とパスワードを指定できます。

Secrets Manager でデータベース認証情報用のシークレットの作成

Strategy Recommendations アプリケーションデータコレクターがデータベースに接続するための認証情報の準備ができたら、次の手順で説明するように、 AWS アカウントの AWS Secrets Manager にシークレットを作成します。

AWS アカウントで AWS Secrets Manager を使用してシークレットを作成するには

1. で AWS 作成したアカウントを使用して にサインイン AWS Management Console しStrategy Recommendations のセットアップ、https://console.aws.amazon.com/secretsmanager/ で AWS Secrets Manager コンソールを開きます。
2. [新しいシークレットを保存] を選択します。
3. シークレットタイプとして [他の種類のシークレット] を選択します。
4. [キー/値ペア] で、次の情報を入力します。

   ユーザー名 - *#########*

   その後、[+ 行の追加] を選択し、次の情報を入力します。

   Password — *########*
5. [次へ] をクリックします。
6. [シークレット名] には、migrationhub-strategy- というプレフィックスを付けた任意の文字列を入力します。たとえば、migrationhub-strategy-one です。

   > **Note**
   >
   > シークレットネームは後で使用できるように安全な場所に保管してください。
7. [次へ] を選択し、もう一度 [次へ] を選択します。
8. [保存する] を選択します。

Strategy Recommendations でデータベース分析を設定するときに、データベース認証情報用に作成したシークレットを使用できます。

Strategy Recommendations バイナリ分析

Migration Hub Strategy Recommendations は、ポートフォリオ内のアプリケーションとそれらに属するアプリケーションコンポーネントを自動的に識別します。たとえば、ポートフォリオに Java アプリケーションがある場合、Strategy Recommendations はそのアプリケーションをコンポーネントタイプ java のアプリケーションコンポーネントとして識別します。ソースコードへのアクセスを設定しなくても、Strategy Recommendations は、Windows では IIS アプリケーション DLL、Linux ではアプリケーション JAR ファイルを検査することでバイナリ分析を行い、アンチパターンレポートや非互換性レポートを提供できます。アンチパターンレポートは、Strategy Recommendations がポートフォリオ内で検出した既知の問題を、重大度別に分類して一覧にしたものです。非互換性レポートには、API 互換性、Nuget Package、移植アクションなどのアンチパターンのサブセットが含まれます。

Strategy Recommendations は、Windows IIS、Java Tomcat、Jboss アプリケーションの分析を行います。IIS アプリケーションを使用している場合、Strategy Recommendations はデフォルトで非互換性レポートを生成します。完全なアンチパターンレポートを受け取るには、ソースコードへのアクセスを設定する必要があります。Java アプリケーションを使用している場合、Strategy Recommendations はデフォルトで完全なアンチパターンレポートを生成します。

非互換性レポートまたはアンチパターンレポートは、分析が完了した後に表示されます。分析に失敗した場合は、バージョン管理設定をセットアップする で説明されているようにソースコードへのアクセスを提供して、ソースコード分析を実行してみてください。

Strategy Recommendations サーバーレコメンデーション

このセクションでは、Migration Hub コンソールの Migration Hub Strategy Recommendations を使用して、移行ポートフォリオ内のサーバーの移行戦略のレコメンデーションを表示する方法について説明します。

サーバーのレコメンデーションを表示するには

1. で AWS 作成したアカウントを使用して にサインイン AWS Management Console しStrategy Recommendations のセットアップ、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、[ストラテジー] を選択し、次に [レコメンデーション] を選択します。

3. [レコメンデーション] ページで [サーバー] タブを選択します。

   a. [サーバーの概要] には、ポートフォリオ内で稼働しているさまざまなタイプのサーバーの概要が表示されます。

   b. [サーバー] には、サーバーとオペレーティングシステムの詳細、および移行「R」戦略のレコメンデーションが表示されます。また、移行先や、レコメンデーションに基づいてサーバー上で特定されたアンチパターンの数も表示できます。「R」戦略について詳しくは、「AWS 規範ガイダンス用語集」の「移行用語 - 7 R」を参照してください。

4. サーバーに関する詳細な推奨事項の詳細を表示するには、一覧からサーバーを選択し、[詳細を表示] を選択します。サーバーについて収集されたメタデータと、サーバー上で実行されているアプリケーションコンポーネントに基づく詳細な分析とレコメンデーションを表示できます。

5. サーバー詳細ページ (サーバー名が見出しになっているページ) の [レコメンデーションの概要] には、そのサーバー向けの [戦略レコメンデーション] の概要が表示されます。特定された [アンチパターン] も表示できます。アンチパターンは、ポートフォリオで見つかった既知の問題を、重大度別に分類したリストです。

6. [ストラテジーオプション] タブを選択すると、サーバーの移行に関する推奨事項が表示されます。推奨ストラテジーは、別のストラテジーを選択し、[優先設定] を選択することでオーバーライドできます。

7. [アプリケーションコンポーネント] タブを選択すると、サーバーに関連するアプリケーションコンポーネントのリストが表示されます。

8. アプリケーションコンポーネントの詳細を表示するには、一覧からコンポーネントを選択し、[詳細を表示] を選択します。アプリケーションコンポーネントの詳細については、「アプリケーションコンポーネントの操作」を参照してください。

Strategy Recommendations 設定

このセクションでは、Migration Hub コンソールで Migration Hub Strategy Recommendations 設定を表示および編集する方法について説明します。

ステップ 5: レコメンデーションを取得する で説明されているように、Strategy Recommendations を初めて設定するときに、レコメンデーション設定を選択します。これらの設定を編集できます。

レコメンデーション設定を編集するには

1. で AWS 作成したアカウントを使用して にサインイン AWS Management Console しStrategy Recommendations のセットアップ、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、[ストラテジー] を選択し、次に [レコメンデーション] を選択します。
3. [レコメンデーション] ページで、[設定] タブを選択します。
4. [優先順位付けされたビジネス目標] では、ビジネス目標をドラッグアンドドロップして再配置できます。
5. 目的の [アプリケーション設定] および [データベース設定] を選択し、[変更を保存] を選択します。

設定を変更すると、[データを再分析] を選択するように促すバナーが表示されます。

Strategy Recommendations データソース

このセクションでは、Strategy Recommendations が使用するデータソースについて説明します。

トピック

Strategy Recommendations のデータソースを表示する

このセクションでは、 で Strategy Recommendations データソースを表示する方法について説明します AWS Management Console。

データソースを表示するには

1. で AWS 作成したアカウントを使用して にサインイン AWS Management Console しStrategy Recommendations のセットアップ、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、[ストラテジー]、[データソース] の順に選択します。
3. [コレクター] タブでは、設定した Strategy Recommendations アプリケーションデータコレクターを表示できます。コレクターの詳細情報は、「Strategy Recommendations アプリケーションデータコレクター」を参照してください。
4. [インポート] タブでは、データをインポートしたり、データインポートを表示したりできます。詳細については、「Strategy Recommendations へのデータのインポート」を参照してください。
5. [ツール] タブでは、コレクターとアプリケーションのインポートデータテンプレートをダウンロードできます。

Strategy Recommendations アプリケーションデータコレクター

このセクションでは、Strategy Recommendations アプリケーションデータコレクターの使用方法について説明します。

アプリケーションデータコレクターのダウンロードと設定については、「ステップ 1: Strategy Recommendations コレクターをダウンロードする」を参照してください。

トピック

Strategy Recommendations によって収集されたデータ。

このセクションでは、Migration Hub Strategy Recommendations アプリケーションデータコレクターが収集するデータの種類について説明します。アプリケーションデータコレクターは、サーバー上で実行中のアプリケーションを識別し、ソースコード分析を行い、データベースを分析するエージェントレスのデータコレクターです。

データフィールド	説明
OS タイプ	Windows または Linux
OS バージョン	OS の特定のバージョン。たとえば、Windows サーバー 2003、RHEL 5.2 などです。
OS のアーキテクチャ	32 ビットまたは 64 ビット OS
サーバー VM である	サーバーは VM または物理マシンです。
仮想化ソフトウェア	たとえば、vCenter、Hyper-V などです。
ロケーション	例えば、Amazon Elastic Compute Cloud (Amazon EC2) コンソールまたはオンプレミス。
dualBoot である	複数の OS で起動できます。
ファームウェアタイプ	BIOS、UEFI

データフィールド	説明
ブートローダー	GRUB、GRUB 2
パーティションテーブルタイプ	MBR、GPT
CPU 速度	CPU 速度 (GHz 単位)。たとえば、2.4 GHz などです。
Windows OS data	
Windows のエディション	スタンダード、データセンター、エンタープライズ
.NET Framework のバージョン	インストールされている .NET フレームワークのバージョン。
.NET Core バージョン	インストールされている .NET Core のバージョン。
Linux data	
Linux OS ディストリビューション	RHEL、CentOS、SUSE など。
カーネルバージョン	uname-r の出力 (例: `4.9.217-0.1.ac.205.84.332.metal1.x86_64`)
For each disk volume	
ファイルシステムのタイプ	FAT32、NTFS、ReFS、ext4、jfs など。
ディスクボリュームサイズ	合計ディスクサイズ
ディスクボリュームの空き容量	空きディスク容量
仮想ディスクイメージフォーマット	vmdk、vhd、vhdx
ディスクタイプ (Windows)	ベーシック、ダイナミクス
Application level data	

データフィールド	説明
アプリケーション名	実行するプロセスの名前。たとえば、SQLServr.exe、MSdtsservr.exe などです。
アプリケーションタイプ	IIS、JBoss、Tomcat など。
プログラミング言語とバージョン	C#、Java
JDK バージョン	インストールされている JDK のバージョン。
ソースコードが入手できる	ソースコードリポジトリを提供すると、ソースコードが入手可能であることが示されます。
アプリケーションビットサイズ	16 ビット、32 ビット、64 ビット
Windows	
アプリが使用する.NET フレームワークのバージョン	アプリケーションの実行時にロードされる.NET Framework DLL のバージョン。
.NET Core バージョン	アプリケーションの実行時にロードされる.NET Core DLL のバージョン。
WPF フレームワークを使用していますか?	.NET ベースのアプリケーションが WPF アプリケーションタイプかどうかを判断します。
WCF フレームワークを使用していますか?	.NET ベースのアプリケーションが WCF アプリケーションタイプかどうかを判断します。
ASP.NET バージョン	ASP.NET のバージョン。
IIS バージョン	Windows マシンにインストールされている IIS サーバーのバージョン。
アプリケーション OS ドライバーのビットサイズ	32 ビット、64 ビット
Windows レジストリの使用状況	マシンのレジストリキーをクエリして、データベースバージョン、Java バージョン、.NET バージョンなどの情報を検索します。

データフィールド	説明
アプリケーションが使用するすべての DLL	Windows プロセスによってランタイムにロードされたすべての DLL のリストを取得します。
PowerShell バージョン	マシンにインストールされている PowerShell バージョンを確認します。バージョンは 5.1 以降である必要があります。
Linux	
アプリケーションフレームワークのタイプ	Tomcat、Spring Boot、JBoss 、 WebLogic、WebSphere
アプリケーションフレームワークのバージョン	アプリケーションフレームワークのバージョン。
Database	
データベースタイプ	MS SQL、オラクル、MySQL など。
データベースのバージョン	データベースのバージョン。

Strategy Recommendations からデータを削除する

Strategy Recommendations からすべてのデータを削除する場合は、AWS Support に連絡し、全データの削除をリクエストしてください。

Strategy Recommendations のアップグレード

Migration Hub Strategy Recommendations アプリケーションデータコレクターは自動的にアップグレードされます。必要に応じて、次の手順を使用して、コレクターを手動でアップグレードできます。

Strategy Recommendations コレクターをアップグレードするには

1. SSH クライアントを使用してコレクタ VM に接続する場合は、次のコマンドを使用します。

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

2. 次の例に示すように、コレクター VM のアップグレードディレクトリに移動します。

```
cd  /home/ec2-user/collector/upgrades
```

3. 次のコマンドを使用して、更新スクリプトを実行します。

```
bash application-data-collector-upgrade
```

Strategy Recommendations へのデータのインポート

アプリケーションデータコレクターを使用する代わりに、移行とモダナイズのレコメンデーションの対象となるアプリケーションとサーバーに関する情報をインポートできます。

データをインポートするときのレコメンデーションは、データコレクターを使用するときほど詳細ではありません。たとえば、インポートされたデータにはソースコード分析を使用できません。

このセクションでは、アプリケーションインポートテンプレートを使用して、Migration Hub コンソールの Strategy Recommendations にデータをインポートする方法について説明します。

データをインポートするには

1. で AWS 作成したアカウントを使用して にサインイン AWS Management Console しStrategy Recommendations のセットアップ、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、[ストラテジー]、[データソース] の順に選択します。
3. [インポート] タブを選択します。
4. [インポートテンプレートのダウンロード] を選択して、アプリケーションインポートテンプレートをダウンロードします。
5. テンプレートに記入し、Amazon S3 バケットにアップロードします。バケットの名前は必ずプレフィックス `migrationhub-strategy` で始まるようにします。
6. [インポート] タブに戻り、[インポート] を選択します。
7. インポートの名前を入力し、入力したデータテンプレートの Amazon S3 オブジェクト URI を入力して、[インポートを開始] を選択します。

Strategy Recommendations のインポートテンプレート。

ダウンロードするインポートテンプレートは、次の例に示されている .json ファイルです。

```
{
    "ImportFormatVersion": 1,
    "Resources": [
        {
            "ResourceType": "SERVER",
            "ResourceName": "",
            "ResourceId": "",
            "IpAddress": "",
            "OSDistribution": "",
            "OSType": "",
            "HostName": "",
            "OSVersion": "",
            "CPUArchitecture": ""
        },
        {
            "ResourceType": "PROCESS",
            "ResourceName": "",
            "ResourceId": "",
            "ApplicationType": "",
            "DotNetFrameworkVersion": "",
            "ApplicationVersion": "",
            "DotNetCoreVersion": "",
            "JdkVersion": "",
            "ProgrammingLanguage": "",
            "DatabaseType": "",
            "DatabaseVersion": "",
            "DatabaseEdition": "",
            "AssociatedServerIds": []
        }
    ]
}
```

インポートテンプレートの入力に役立つように、データフィールドの有効な値を以下の表に示します。

以下の表に、サーバーの必須フィールドの一覧を示します。

名前	説明	タイプ	必須	有効値
ResourceId	リソースの一意の ID	文字列	はい	任意の一意の文字列
ResourceName	リソースの名前	文字列	はい	任意の文字列
ResourceType	インポートするリソースのタイプ	文字列	はい	"サーバー"、"プロセス"
OSDistribution	Windows、Windows Server、Ubuntu	文字列	はい	Windows: "Windows PC"、"Windows Server" Linux: "Ubuntu"、"RHEL"、"Amazon Linux"、"DEBIAN"、"SLES"、"CENT_OS"、"ORACLE_LINUX"、"FEDORA"、"KALI"
OSType	オペレーティングシステムのタイプ	文字列	はい	"Windows"、"Linux"
OSVersion	カーネルのバージョン	文字列	はい	HTML 版のドキュメントを参照してください。
CPUArchitecture	CPU アーキテクチャ	文字列	いいえ	"32bit"、"64bit"
IpAddress	サーバーの IP アドレス。	配列	いいえ	xxx.xxx.xxx.xxx の形式
MacAddresses	サーバーに関連付けられた Mac アドレス	配列	いいえ	xx:xx:xx:xx:xx:xx の形式

名前	説明	タイプ	必須	有効値
ホスト名	ホストの名前	文字列	いいえ	任意の文字列

以下の表に、プロセスの必須フィールドの一覧を示します。

名前	説明	タイプ	必須	有効値
ResourceId	リソースの一意の ID	文字列	はい	任意の一意の文字列
ResourceName	リソースの名前	文字列	はい	任意の文字列
ResourceType	インポートするリソースのタイプ	文字列	はい	"サーバー"、"プロセス"
AssociatedServerID	プロセスが実行されているサーバー ID のリスト。	文字列	はい	定義したResourceType「」：「SERVER ResourceId 」の 。
ApplicationType	アプリケーションのタイプ	文字列	はい	「Tomcat」、JBoss」、「Spring」、「IIS」、「Mongo DB」、「DB2」、「Maria DB」、MySQL」、「Oracle」、SQLServer」、「Sybase」、PostgreSQLServer」、「Cassandra」、「IBM WebSphere」、「Oracle WebLogic」、「Java Generic」
ApplicationVersion	アプリケーションのバージョン	文字列	はい	"IIS 1.0"、"IIS 2.0"、"IIS 3.0"、"IIS 4.0"、"IIS 5.0"、"IIS 5.1"、"IIS 6.0"、"IIS 7.0"、"IIS

名前	説明	タイプ	必須	有効値
				7.5"、"IIS 8.0"、"IIS 8.5"、"IIS 10.0"
ProgrammingLanguage	アプリケーションのプログラミング言語。	文字列	いいえ	"Java"、"CSharp"
DotNetFrameworkVersion	.NET Framework のバージョン (アプリケーションが.NET Framework ベースの場合)	文字列	いいえ	DotnetFramework 「1.0」、DotnetFramework 「1.0 SP1」、DotnetFramework 「1DotnetFramework .0 SP2SP3」、DotnetFramework 「1.1」、DotnetFramework 「1.1 SP1」、DotnetFramework「2.0」、DotnetFramework 「2.0 SP1」、DotnetFramework 「2.0 SP2」、DotnetFramework 「3.0」、DotnetFramework 「3.0 SP1」、DotnetFramework「3.0 SPSP2DotnetFramework 「3.5」、DotnetFramework 「3.5」、SP1」、DotnetFramework 「4.0」、DotnetFramework 「4.5.1」、DotnetFramework」、DotnetFramework 「4.5.2」、DotnetFramework」、SP2SP1DotnetFramework DotnetFramework DotnetFramework DotnetFramework DotnetFramework DotnetFramework ◆◆

名前	説明	タイプ	必須	有効値
DotNetCoreVersion	.NET Core のバージョン (アプリケーションが.NET Core ベースの場合)	文字列	いいえ	".NET Core 1.0"、".NET Core 1.1"、".NET Core 2.0"、".NET Core 2.1"、".NET Core 2.2"、".NET Core 3.0"、".NET Core 3.1"
JdkVersion	JDK のバージョン (アプリケーションが JDK を使用している場合)	文字列	いいえ	"JDK1.0"、"JDK2.0"、"JDK3.0"、 …、"JDK11.0"
DatabaseType	データベースのタイプ	文字列	いいえ	"SQLServer"、"Oracle"、"Sybase"、"MongoDB"、"Maria DB"、"Apache Cassandra"、"MySQL"、"IBM DB2"、"PostgreSQLServer"
DatabaseEdition	データベースのエディション。	文字列	いいえ	
DatabaseVersion	データベースのバージョン	文字列	いいえ	HTML 版のドキュメントを参照してください。

Strategy Recommendations からデータを削除

Migration Hub 戦略のレコメンデーションからすべてのデータを削除したい場合は、AWS Support までお問い合わせください。

Migration Hub Strategy Recommendations でのセキュリティ

AWS でのクラウドセキュリティは最優先事項です。AWS のユーザーは、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャを利用できます。

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

- クラウドのセキュリティ - AWS は、AWS クラウド で AWS のサービスを実行するインフラストラクチャを保護する責任を担います。また、AWS は、ユーザーが安全に使用できるサービスも提供します。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監査が定期的にセキュリティの有効性をテストおよび検証しています。Migration Hub Strategy Recommendations に適用されるコンプライアンスプログラムの詳細については、「AWS コンプライアンスプログラムによる対象範囲内の サービス」「」を参照してください。
- クラウド内のセキュリティ - ユーザーの責任は、使用する AWS サービスに応じて異なります。また、お客様は、データの機密性、会社の要件、適用される法律や規制など、その他の要因についても責任を負います。

このドキュメントは、Strategy Recommendations を使用する際に責任共有モデルを適用する方法を理解するのに役立ちます。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の目的を達成するように Strategy Recommendations を設定する方法について説明します。また、Strategy Recommendations リソースのモニタリングや保護に役立つ他の AWS サービスを使用する方法についても説明します。

トピック

Migration Hub Strategy Recommendations でのデータ保護

Migration Hub Strategy Recommendations でのデータ保護には、AWS の責任共有モデルが適用されます。このモデルで説明されているように、AWS は、AWS クラウド のすべてを実行するグローバ

ルインフラストラクチャを保護するがあります。お客様は、このインフラストラクチャでホストされているコンテンツに対する管理を維持する責任があります。また、使用する AWS のサービスのセキュリティ設定と管理タスクもユーザーの責任となります。データプライバシーの詳細については、「データプライバシーのよくある質問」を参照してください。欧州でのデータ保護の詳細については、「AWS セキュリティブログ」に投稿された「AWS 責任共有モデルおよび GDPR」のブログ記事を参照してください。

データを保護するため、AWS アカウント の認証情報を保護し、AWS IAM Identity Center または AWS Identity and Access Management (IAM) を使用して個々のユーザーをセットアップすることをお勧めします。この方法により、それぞれのジョブを遂行するために必要な権限のみを各ユーザーに付与できます。また、次の方法でデータを保護することをおすすめします。

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 が必須です。TLS 1.3 が推奨されます。
- AWS CloudTrail で API とユーザーアクティビティロギングをセットアップします。
- AWS のサービス内でデフォルトである、すべてのセキュリティ管理に加え、AWS の暗号化ソリューションを使用します。
- Amazon Macie などの高度なマネージドセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API により AWS にアクセスするときに FIPS 140-2 検証済み暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-2」を参照してください。

顧客の E メールアドレスなどの機密情報や重要情報は、タグや Name フィールドなどの自由形式のフィールドに入力しないことを強くお勧めします。これには、お客様がコンソール、API、AWS CLI または AWS SDK を使用して、Strategy Recommendations またはその他の AWS のサービス と連携する場合が含まれます。名前に使用する自由記述のテキストフィールドやタグに入力したデータは、課金や診断ログに使用される場合があります。外部サーバーへの URL を提供する場合は、そのサーバーへのリクエストを検証するための認証情報を URL に含めないように強くお勧めします。

保管中の暗号化

Strategy Recommendations のデータベースに保存されているデータはすべて暗号化されています。

転送中の暗号化

Strategy Recommendations インターネットワーク通信では、すべてのコンポーネントとクライアントの間の TLS 1.2 暗号化をサポートしています。

Migration Hub Strategy Recommendations の ID とアクセス管理

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、誰を認証 (サインイン) し、誰に Strategy Recommendations リソースの使用を承認する (アクセス許可を付与する) かを制御します。IAM は、追加料金なしで AWS のサービス 使用できる です。

トピック

- 対象者
- アイデンティティを使用した認証
- ポリシーを使用したアクセスの管理
- Migration Hub Strategy Recommendations と IAM を連携する方法
- AWS マイグレーション・ハブ戦略提言の管理ポリシー
- Migration Hub Strategy Recommendations の ID ベースのポリシーの例
- Migration Hub Strategy Recommendations のアイデンティティとアクセスに関するトラブルシューティング
- Strategy Recommendations のサービスリンクロールを使用する
- Migration Hub Strategy Recommendations およびインターフェースVPC エンドポイント (AWS PrivateLink)

対象者

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

サービスユーザー – Strategy Recommendations サービスを使用してジョブを実行する場合は、必要なアクセス許可と認証情報を管理者が用意します。作業を実行するためにさらに多くの Strategy Recommendations の機能を使用するとき、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うえで役立ちます。Strategy Recommendations の機能にアクセスできない場合は、「Migration Hub Strategy Recommendations のアイデンティティとアクセスに関する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 – 社内の Strategy Recommendations リソースを担当している場合は、通常、Strategy Recommendations へのフルアクセスがあります。サービスのユーザーがどの Strategy Recommendations 機能やリソースにアクセスするかを決めるのは、ユーザーの役割です。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。会社で Strategy Recommendations を使用して IAM を利用する方法の詳細については、「Migration Hub Strategy Recommendations と IAM を連携する方法」を参照してください。

IAM 管理者 – 管理者は、Strategy Recommendations へのアクセスを管理するポリシーの作成方法の詳細について確認する場合があります。IAM で使用できる Strategy Recommendations アイデンティティベースのポリシーの例を表示するには、「Migration Hub Strategy Recommendations の ID ベースのポリシーの例」を参照してください。

アイデンティティを使用した認証

認証は、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される (にサインインする AWS) 必要があります。

ID ソース (AWS IAM Identity Center) から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。IAM Identity Center) ユーザー、会社のシングルサインオン認証、Google または Facebook の認証情報は、フェデレーティッド ID の例です。フェデレーションアイデンティティ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。フェデレーションを使用して にアクセスすると、間接的 AWS にロールを引き受けます。

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「 にサインインする方法 AWS アカウント」を参照してください。

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

使用する認証方法を問わず、セキュリティ情報の提供を追加でリクエストされる場合もあります。例えば、 では、多要素認証 (MFA) を使用してアカウントのセキュリティを高めることを AWS 推奨しています。詳細については、「AWS IAM Identity Center ユーザーガイド」の「多要素認証 (MFA)」および「IAM ユーザーガイド」の「AWSでの多要素認証 (MFA) の使用」を参照してください。

AWS アカウント ルートユーザー

を作成するときは AWS アカウント、アカウント内のすべての AWS のサービス およびリソースへの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。このアイデンティティは 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を保護し、それらを使用してルートユーザーのみが実行できるタスクを実行してください。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。

フェデレーション ID

ベストプラクティスとして、管理者アクセスを必要とするユーザーを含む人間のユーザーに、一時的な AWS のサービス 認証情報を使用して にアクセスする ID プロバイダーとのフェデレーションの使用を要求します。

フェデレーティッド ID とは、エンタープライズユーザーディレクトリ、ウェブ ID プロバイダー、AWS Directory Service、、Identity Center ディレクトリのユーザー、または ID ソースから提供された認証情報 AWS のサービス を使用して にアクセスするすべてのユーザーです。フェデレーティッド ID が にアクセスすると AWS アカウント、ロールを引き受け、ロールは一時的な認証情報を提供します。

アクセスを一元管理する場合は、 AWS IAM Identity Centerを使用することをお勧めします。IAM Identity Center でユーザーとグループを作成することも、すべての とアプリケーションで使用する独自の ID ソースのユーザー AWS アカウント とグループのセットに接続して同期することもできます。IAM アイデンティティセンターの詳細については、[AWS IAM Identity Center ユーザーガイド」の「IAM アイデンティティセンターとは」を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、単一のユーザーまたはアプリケーションに対して特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を保有する IAM ユーザーを作成する代わりに、一時的な認証情報を使用することをお勧め

します。ただし、IAM ユーザーでの長期的な認証情報が必要な特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、IAM ユーザーガイドの「長期的な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションする」を参照してください。

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

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

IAM ロール

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

一時的な認証情報を持った IAM ロールは、以下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 – フェデレーションアイデンティティに権限を割り当てるには、ロールを作成してそのロールの権限を定義します。フェデレーションアイデンティティが認証されると、そのアイデンティティはロールに関連付けられ、ロールで定義されている権限が付与されます。フェデレーションの詳細については、「IAM ユーザーガイド」の「Creating a role for a third-party Identity Provider」(サードパーティーアイデンティティプロバイダー向けロールの作成) を参照してください。IAM アイデンティティセンターを使用する場合、権限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。権限セットの詳細については、「AWS IAM Identity Center ユーザーガイド」の「権限セット」を参照してください。
- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで引き受けることができます。

- クロスアカウントアクセス - IAM ロールを使用して、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、一部の では AWS のサービス、(ロールをプロキシとして使用する代わりに) リソースにポリシーを直接アタッチできます。クロスアカウントアクセスにおけるロールとリソースベースのポリシーの違いについては、「IAM ユーザーガイド」の「IAM ロールとリソースベースのポリシーとの相違点」を参照してください。
- クロスサービスアクセス — 一部の では、他の の機能 AWS のサービス を使用します AWS のサービス。例えば、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2 でアプリケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。サービスでは、呼び出し元プリンシパルの許可、サービスロール、またはサービスリンクロールを使用してこれを行う場合があります。
  - 転送アクセスセッション (FAS) – IAM ユーザーまたはロールを使用して でアクションを実行する場合 AWS、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 AWS のサービス を使用し AWS のサービス、ダウンストリームサービスにリクエストを行うリクエストと組み合わせて使用します。FAS リクエストは、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サービスが受信した場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。
  - サービスロール - サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、「IAM ユーザーガイド」の「AWS のサービスにアクセス許可を委任するロールの作成」を参照してください。
  - サービスにリンクされたロール – サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービス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。
- 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 リクエストを作成しているアプリケーションの一時的な認証情報を管理できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。AWS ロールを EC2 インスタンスに割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタン

スプロファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムは一時的な認証情報を取得できます。詳細については、「IAM ユーザーガイド」の「Amazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して権限を付与する」を参照してください。

IAM ロールと IAM ユーザーのどちらを使用するかについては、「IAM ユーザーガイド」の「IAM ロールの作成が適している場合 (ユーザーではなく)」を参照してください。

ポリシーを使用したアクセスの管理

でアクセスを制御する AWS には、ポリシーを作成し、 AWS ID またはリソースにアタッチします。ポリシーは のオブジェクト AWS であり、アイデンティティまたはリソースに関連付けられると、これらのアクセス許可を定義します。 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、これらのポリシー AWS を評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。ほとんどのポリシーは JSON ドキュメント AWS として に保存されます。JSON ポリシードキュメントの構造と内容の詳細については、「IAM ユーザーガイド」の「JSON ポリシー概要」を参照してください。

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがど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継ぐことができます。

IAM ポリシーは、オペレーションの実行方法を問わず、アクションの権限を定義します。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。こ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、ユーザーグループ、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、および条件を制御します。アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「IAM ポリシーの作成」を参照してください。

アイデンティティベースのポリシーは、さらに インラインポリシー または マネージドポリシー に分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込ま

れています。管理ポリシーは、 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。管理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比較」を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーが添付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 IAM の AWS マネージドポリシーを使用することはできません。

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権限を持つかをコントロールします。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、追加の一般的でないポリシータイプをサポートします。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- 権限の境界 - 権限の境界は、アイデンティティベースのポリシーによって IAM エンティティ (IAM ユーザーまたはロール) に付与できる権限の上限を設定する高度な機能です。エンティティに権限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権限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、権限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、許可は無効になります。権限の境界の詳細については、「IAM ユーザーガイド」の「IAM エンティティの権限の境界」を参照してください。

- サービスコントロールポリシー (SCPs) – SCPs は、 の組織または組織単位 (OU) に最大アクセス許可を指定する JSON ポリシーです AWS Organizations。 AWS Organizations は、 AWS アカウント ビジネスが所有する複数の をグループ化して一元管理する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。組織と SCP の詳細については、「AWS Organizations ユーザーガイド」の「SCP の仕組み」を参照してください。
- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限される範囲は、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、許可は無効になります。詳細については、「IAM ユーザーガイド」の「セッションポリシー」を参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成される権限を理解するのがさらに難しくなります。複数のポリシータイプが関連する場合に が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「ポリシーの評価ロジック」を参照してください。

Migration Hub Strategy Recommendations と IAM を連携する方法

IAM を使用して Strategy Recommendations へのアクセスを管理する前に、Strategy Recommendations で使用できる IAM 機能について理解しておく必要があります。

Migration Hub Strategy Recommendations で使用できる IAM の機能

IAM 機能	Strategy Recommendations のサポート
アイデンティティベースのポリシー	あり
リソースベースのポリシー	いいえ
ポリシーアクション	あり

IAM 機能	Strategy Recommendations のサポート
ポリシーリソース	いいえ
ポリシー条件キー	いいえ
ACL	なし
ABAC (ポリシー内のタグ)	いいえ
一時的な認証情報	あり
プリンシパル権限	あり
サービスロール	いいえ
サービスリンクロール	はい

Strategy Recommendations およびその他の AWS のサービスがほとんどの IAM 機能と連携する方法の概要を把握するには、「IAM ユーザーガイド」のAWS 「IAM と連携する のサービス」を参照してください。

Strategy Recommendations の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をサポートする	あり

アイデンティティベースポリシーは、IAM ユーザー、ユーザーグループ、ロールなど、アイデンティティにアタッチできる JSON 権限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、および条件を制御します。アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「IAM ポリシーの作成」を参照してください。

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、およびアクションを許可または拒否する条件を指定できます。プリンシパルは、それが添付されているユーザーまたはロールに適用されるため、アイデンティティベースのポリシーでは指定できません。JSON ポリシーで使用できるすべての要素について学ぶには、「IAM ユーザーガイド」の「IAM JSON ポリシーの要素のリファレンス」を参照してください。

Strategy Recommendations のアイデンティティベースのポリシー例

Strategy Recommendations アイデンティティベースのポリシー例を表示するには、「Migration Hub Strategy Recommendations の ID ベースのポリシーの例」を参照してください。

Strategy Recommendations 内のリソースベースのポリシー

リソースベースのポリシーのサポート	なし

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。ポリシーが添付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。

クロスアカウントアクセスを有効にするには、アカウント全体、または別のアカウントの IAM エンティティをリソースベースのポリシーのプリンシパルとして指定します。リソースベースのポリシーにクロスアカウントのプリンシパルを追加しても、信頼関係は半分しか確立されない点に注意してください。プリンシパルとリソースが異なる にある場合 AWS アカウント、信頼されたアカウントの IAM 管理者は、リソースへのアクセス許可をプリンシパルエンティティ (ユーザーまたはロール) に付与する必要もあります。IAM 管理者は、アイデンティティベースのポリシーをエンティティにアタッチすることで権限を付与します。ただし、リソースベースのポリシーで、同じアカウントのプリンシパルへのアクセス権が付与されている場合は、アイデンティティベースのポリシーを追加する必要はありません。詳細については、「IAM ユーザーガイド」の「IAM ロールとリソースベースのポリシーとの相違点」を参照してください。

Strategy Recommendations に対するポリシーアクション

ポリシーアクションに対するサポート	はい

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

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、関連する 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。

Strategy Recommendations アクションのリストを確認するには、「サービス認可リファレンス」の「Migration Hub Strategy Recommendations で定義されるアクション」を参照してください。

Strategy Recommendations のポリシーアクションでは、アクションの前にプレフィックス を使用します。

```
migrationhub-strategy
```

単一のステートメントで複数のアクションを指定するには、アクションをカンマで区切ります。

```
"Action": [
      "migrationhub-strategy:action1",
      "migrationhub-strategy:action2"
         ]
```

Strategy Recommendations アイデンティティベースのポリシー例を表示するには、「Migration Hub Strategy Recommendations の ID ベースのポリシーの例」を参照してください。

Strategy Recommendations のポリシーリソース

ポリシーリソースに対するサポート	いいえ

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがど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。

Resource JSON ポリシーの要素は、オブジェクトあるいはアクションが適用されるオブジェクトを指定します。ステートメントには、Resource または NotResource 要素を含める必要がありま

す。ベストプラクティスとしては、Amazon リソースネーム (ARN) を使用してリソースを指定します。これは、リソースレベルの権限と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルのアクセス許可をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (*) を使用します。

```
"Resource": "*"
```

Strategy Recommendations リソースのタイプとその ARN のリストを確認するには、「サービス認証リファレンス」の「Migration Hub Strategy Recommendations で定義されるリソース」を参照してください。どのアクションで各リソースの ARN を指定できるかについては、「Migration Hub Strategy Recommendations で定義されるアクション」を参照してください。

Strategy Recommendations アイデンティティベースのポリシー例を表示するには、「Migration Hub Strategy Recommendations の ID ベースのポリシーの例」を参照してください。

Strategy Recommendations のポリシー条件キー

サービス固有のポリシー条件キーのサポート	いいえ

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

`Condition` 要素 (または `Condition` ブロック) を使用すると、ステートメントが有効な条件を指定できます。`Condition` 要素はオプションです。equal や less than などの条件演算子を使用して条件式を作成することによって、ポリシーの条件とリクエスト内の値を一致させることができます。

1 つのステートメントに複数の `Condition` 要素を指定する場合、または 1 つの `Condition` 要素に複数のキーを指定する場合、 AWS は `AND` 論理演算子を使用してそれらを評価します。1 つの条件キーに複数の値を指定すると、 は論理OR演算を使用して条件 AWS を評価します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば IAM ユーザーに、IAM ユーザー名がタグ付けされている場合のみリソースにアクセスできる権限を付与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「IAM ポリシーの要素: 変数およびタグ」を参照してください。

AWS は、 グローバル条件キーとサービス固有の条件キーをサポートします。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。

Strategy Recommendations 条件キーのリストについては、「サービス認可リファレンス」の「Migration Hub Strategy Recommendations の条件キー」を参照してください。条件キーを使用できるアクションとリソースについては、「Migration Hub Strategy Recommendations で定義されるアクション」を参照してください。

Strategy Recommendations アイデンティティベースのポリシー例を表示するには、「Migration Hub Strategy Recommendations の ID ベースのポリシーの例」を参照してください。

Strategy Recommendations でのアクセスコントロールリスト (ACL)

ACL のサポート	なし

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権限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。

Strategy Recommendations を持つ属性ベースのアクセス制御 (ABAC)

ABAC (ポリシー内のタグ) のサポート	いいえ

属性ベースのアクセス制御 (ABAC) は、属性に基づいて権限を定義する認可戦略です。では AWS、これらの属性はタグ と呼ばれます。タグは、IAM エンティティ (ユーザーまたはロール) および多くの AWS リソースにアタッチできます。エンティティとリソースのタグ付けは、ABAC の最初の手順です。次に、プリンシパルのタグがアクセスを試行するリソースのタグと一致したときにオペレーションを許可するよう、ABAC ポリシーを設計します。

ABAC は、急成長する環境やポリシー管理が煩雑になる状況で役立ちます。

タグに基づいてアクセスを制御するには、`aws:ResourceTag/key-name`、`aws:RequestTag/key-name`、または `aws:TagKeys` の条件キーを使用して、ポリシーの条件要素 でタグ情報を提供します。

サービスがすべてのリソースタイプに対して 3 つの条件キーすべてをサポートする場合、そのサービスの値ははいです。サービスが一部のリソースタイプに対してのみ 3 つの条件キーすべてをサポートする場合、値は Partial です。

ABAC の詳細については、「IAM ユーザーガイド」の [ABAC とは?」を参照してください。ABAC をセットアップする手順を説明するチュートリアルについては、「IAM ユーザーガイド」の「属性ベースのアクセス制御 (ABAC) を使用する」を参照してください。

Strategy Recommendations での一時的な認証情報の使用

一時的な認証情報のサポート	はい

一部の AWS のサービス は、一時的な認証情報を使用してサインインすると機能しません。一時的な認証情報 AWS のサービス を使用する などの詳細については、IAM ユーザーガイドの「IAM AWS のサービス と連携する 」を参照してください。

ユーザー名とパスワード以外の AWS Management Console 方法で にサインインする場合は、一時的な認証情報を使用しています。例えば、会社の Single Sign-On (SSO) リンク AWS を使用して にアクセスすると、そのプロセスは自動的に一時的な認証情報を作成します。また、ユーザーとしてコンソールにサインインしてからロールを切り替える場合も、一時的な認証情報が自動的に作成されます。ロールの切り替えに関する詳細については、「IAM ユーザーガイド」の「ロールへの切り替え (コンソール)」を参照してください。

一時的な認証情報は、 AWS CLI または AWS API を使用して手動で作成できます。その後、これらの一時的な認証情報を使用して、長期的なアクセスキーを使用する代わりに、動的に一時的な認証情報を生成する AWS. AWS recommends にアクセスできます。詳細については、「IAM の一時的セキュリティ認証情報」を参照してください。

Strategy Recommendations のクロスサービスプリンシパル許可

フォワードアクセスセッション (FAS) をサポート	はい

IAM ユーザーまたはロールを使用して でアクションを実行する場合 AWS、ユーザーはプリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可 AWS のサービス を使用し AWS のサービス、ダウンストリームサービスにリクエストを行うリクエ

ストと組み合わせて使用します。FAS リクエストは、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サービスが受信し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。

Strategy Recommendations のサービスロール

サービスロールのサポート	いいえ

サービスロールとは、サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、「IAM ユーザーガイド」の「AWS のサービスにアクセス許可を委任するロールの作成」を参照してください。

> **Warning**
>
> サービスロールの許可を変更すると、Strategy Recommendations の機能が損なわれる可能性があります。Strategy Recommendations が指示する場合以外は、サービスロールを編集しないでください。

Strategy Recommendations のサービスリンクロール

サービスリンクロールのサポート	はい

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許可を表示できますが、編集することはできません。

Strategy Recommendations 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、「Strategy Recommendations のサービスリンクロールを使用する」を参照してください。

AWS マイグレーション・ハブ戦略提言の管理ポリシー

ユーザー、グループ、ロールに権限を追加するには、 AWS 自分でポリシーを作成するよりも管理ポリシーを使用する方が簡単です。チームに必要な許可のみを提供する IAM カスタマーマネージドポリシーを作成するには、時間と専門知識が必要です。すぐに始めるには、 AWS 管理ポリシーをご利用ください。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 AWS サービスは管理ポリシーを維持および更新します。 AWS 管理ポリシーの権限は変更できません。新しい機能をサポートするために、 AWS サービスによって管理ポリシーに権限が追加されることがあります。この種の更新は、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、ロール) に影響を与えます。新しい機能がリリースされたとき、または新しい操作が可能になったときに、 AWS サービスが管理ポリシーを更新する可能性が最も高くなります。AWS サービスは管理ポリシーから権限を削除しないため、ポリシーを更新しても既存の権限が損なわれることはありません。

さらに、 AWS 複数のサービスにまたがるジョブ機能の管理ポリシーもサポートされます。たとえば、ReadOnlyAccess AWS AWS 管理ポリシーはすべてのサービスとリソースへの読み取り専用アクセスを提供します。サービスが新しい機能を起動すると、 AWS 新しい操作やリソースに対する読み取り専用権限が追加されます。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 管理ポリシー: AWSMigrationHubStrategyConsoleFullAccess

`AWSMigrationHubStrategyConsoleFullAccess` ポリシーは IAM ID にアタッチできます。

`AWSMigrationHubStrategyConsoleFullAccess` ポリシーは、 AWS Management Consoleを通じて Strategy Recommendations サービスへのフルアクセスをユーザーに許可します。

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。

- `discovery` — Application Discovery Service の概要を取得するためのアクセス許可をユーザーに付与します。
- `iam` — Strategy Recommendations を使用するための要件である、サービスリンクロールをユーザー用に作成できます。

- `migrationhub-strategy` — ユーザーに Strategy Recommendations へのフルアクセスを許可します。
- `s3` — Strategy Recommendations で使用される S3 バケットの作成と読み取りをユーザーに許可します。
- `secretsmanager` — Secrets Manager にシークレットアクセスを一覧表示することをユーザーに許可します。

このポリシーの権限を確認するには、『AWS 管理ポリシーリファレンスガイド』のを参照してくださいAWSMigrationHubStrategyConsoleFullAccess。

AWS 管理ポリシー: AWSMigrationHubStrategyCollector

`AWSMigrationHubStrategyCollector` ポリシーは IAM ID にアタッチできます。

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。

- `application-transformation`— アプリケーション変換操作用のログとメトリックデータをアップロードし、移植互換性の評価と推奨事項に取り組む権限を付与します。
- `execute-api` — ユーザーが Amazon API Gateway にアクセスしてログとメトリクスを AWSにアップロードできるようにします。
- `migrationhub-strategy`— ユーザーに、メッセージの登録、メッセージの送信、ログデータのアップロード、ストラテジーレコメンデーションへの指標データのアップロードを行う権限を付与します。
- `s3`— バケットとその場所を一覧表示するアクセス権をユーザーに付与します。ユーザーには、Strategy Recommendations で使用される S3 バケットのライフサイクル設定への書き込み、オブジェクトの取得、追加、アクセス制御リスト (ACL) の返却、作成、アクセス、暗号化の設定、`PublicAccessBlock`設定の変更、バージョニング状態の設定、作成または置換を行うためのアクセス権限も付与されます。
- `secretsmanager` — Strategy Recommendations が使用する Secrets Manager のシークレットにユーザーがアクセスできるようにします。

このポリシーの権限を確認するには、『AWS 管理ポリシーリファレンスガイド』AWSMigrationHubStrategyCollectorのを参照してください。

戦略、推奨事項、 AWS 管理ポリシーの更新

このサービスがストラテジーレコメンデーションの変更を追跡し始めて以降の、 AWS ストラテジーレコメンデーションの管理ポリシーの更新に関する詳細を表示します。このページの変更に関する自動通知を入手するには、Strategy Recommendations ドキュメントの履歴ページから、RSS フィードにサブスクライブしてください。

変更	説明	日付
AWSMigrationHubStrategyCollector - 既存ポリシーへの更新	このポリシーはPutLogData 、、StartPortingCompatibilityAssessment GetPortingCompatibilityAssessment 、StartPortingRecommendationAssessment GetPortingRecommendationAssessment アプリケーション変換アクションを含むように更新され、アプリケーション変換サービスがログとメトリックをサービスに送信できるようになりました。ListBucket ログとメトリックスのアップロードをサポートするために、Amazon Simple Storage Service (Amazon S3) GetBucketLocation におよびが追加されました。また、PutLogData Strategy Recommendations PutMetricData コレクターがサービスのエンドポ	2024 年 4 月 1 日

変更	説明	日付
	イントにログとメトリックスを送信できるようにするためにも追加されました。	
AWSMigrationHubStrategyCollector – 既存ポリシーへの更新	本ポリシーは、PutMetricData PutLogData およびアクションにより更新されます。これらのアクションは、アプリケーション変換操作用のログとメトリックデータのアップロードを許可します。この更新では、付属の Amazon Simple Storage Service aws:ResourceAccount AWS Secrets Manager とアクションを使用する権限と同等であることを保証する条件も追加されています。aws:PrincipalAccount	2024 年 2 月 5 日
AWSMigrationHubStrategyCollector – 既存ポリシーへの更新	このポリシーは次の CreateBucket 、PutEncryptionConfiguration 、PutBucketPublicAccessBlock 、PutBucketPolicy 、PutBucketVersioning 、および PutLifecycleConfiguration の Amazon S3 API で更新されます。	2023 年 9 月 15 日

変更	説明	日付
AWSMigrationHubStrategyCollector – 既存ポリシーへの更新	このポリシー更新により、ソースコードの分析を可能にするアクセス許可が付与されます。	2023 年 3 月 8 日
AWSMigrationHubStrategyConsoleFullAccess – 既存ポリシーへの更新	このポリシーは、DescribeConfigurations DescribeTags 、AWS Application Discovery Service および ListConfigurations 3 つの API で更新されました。	2022 年 11 月 10 日
AWSMigrationHubStrategyCollector – 既存ポリシーへの更新	このポリシーは、UpdateCollectorConfiguration アクションによって更新されます。このアクションはコレクターの設定を保存し、簡単に取得できるようにします。	2022 年 9 月 7 日
AWSMigrationHubStrategyConsoleFullAccess— リリース時に新しいポリシーが公開されました。	AWS Management Console を通じて、AWSMigrationHubStrategyConsoleFullAccess は Strategy Recommendations サービスへのフルアクセスをユーザーに付与します。	2021 年 10 月 25 日

変更	説明	日付
AWSMigrationHubStrategyCollector— 発売時に新しいポリシーが利用可能になった	`AWSMigrationHubStrategyCollector` は Strategy Recommendations サービスへのユーザーアクセスと、サービスに関連する S3 バケットへの読み取り/書き込みアクセス権をユーザーに付与します。また、Amazon API Gateway にログとメトリックスをアップロードするためのアクセス権限と AWS、認証情報を取得するための AWS Secrets Manager アクセス権も付与されます。	2021 年 10 月 25 日
AWSMigrationHubStrategyServiceRolePolicy— リリース時に新しいポリシーが利用可能になりました	`AWSMigrationHubStrategyServiceRolePolicy` サービスにリンクされたロールポリシーは、 AWS Migration Hub およびへのアクセスを提供します。 AWS Application Discovery Service このポリシーにより、レポートを Amazon Simple Storage Service (Amazon S3) に格納する権限も付与されます。	2021 年 10 月 25 日
Strategy Recommendations は変更の追跡を開始しました	ストラテジー・レコメンデーションズは、 AWS 管理ポリシーの変更を追跡し始めました。	2021 年 10 月 25 日

Migration Hub Strategy Recommendations の ID ベースのポリシーの例

デフォルトでは、IAM ユーザーおよびロールには、Strategy Recommendations リソースを作成または変更するアクセス許可はありません。また、、 AWS Command Line Interface （ AWS CLI ） AWS Management Console、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、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、管理者がロールに IAM ポリシーを追加すると、ユーザーはロールを引き受けることができます。

これらサンプルの JSON ポリシードキュメントを使用して、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「IAM ポリシーの作成」を参照してください。

Direct Connect が定義するアクションとリソースタイプ (リソースタイプごとの ARN の形式を含む) の詳細については、「サービス認証リファレンス」の「Strategy Recommendations 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。

トピック

- ポリシーのベストプラクティス
- Strategy Recommendations コンソールの使用
- 自分の許可の表示をユーザーに許可する
- 1 つの Amazon S3 バケットへのアクセス

ポリシーのベストプラクティス

ID ベースのポリシーは、ユーザーのアカウントで誰かが Strategy Recommendations リソースを作成、アクセス、または削除できるどうかを決定します。これらのアクションを実行すると、 AWS アカウントに料金が発生する可能性があります。アイデンティティベースの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 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する – ユーザーとワークロードにアクセス許可を付与するには、多くの一般的ユースケースにアクセス許可を付与する AWS 管理ポリシーを使用します。これらは で使用できます AWS アカウント。ユースケースに固有の AWS カスタマー管理ポリシーを定義して、アクセス許可をさらに減らすことをお勧めします。詳細については、IAM ユーザーガイドの「AWS マネージドポリシー」または「AWS ジョブ機能の管理ポリシー」を参照してください。

- 最小特権を適用する – IAM ポリシーで権限を設定するときは、タスクの実行に必要な権限のみを付与します。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、最小特権とも呼ばれています。IAM を使用して権限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 でのポリシーと権限」を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。条件を使用して、 などの特定の を通じてサービスアクションを使用する場合 AWS のサービス、サービスアクションへのアクセスを許可することもできます AWS CloudFormation。詳細については、「IAM ユーザーガイド」の [IAM JSON policy elements: Condition] (IAM JSON ポリシー要素：条件) を参照してください。
- IAM Access Analyzer を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM Access Analyzer は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、「IAM ユーザーガイド」の「IAM Access Analyzer ポリシーの検証」を参照してください。
- 多要素認証 (MFA) を要求する – で IAM ユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、セキュリティを強化するために MFA を有効にします。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、「IAM ユーザーガイド」の「MFA 保護 API アクセスの設定」を参照してください。

IAM でのベストプラクティスの詳細については、『IAM ユーザーガイド』の「IAM でのセキュリティのベストプラクティス」を参照してください。

Strategy Recommendations コンソールの使用

Migration Hub Strategy Recommendations コンソールにアクセスするには、最小限のアクセス許可が必要です。これらのアクセス許可により、 の Strategy Recommendations リソースの詳細をリストおよび表示できます AWS アカウント。最小限必要な許可よりも制限が厳しいアイデンティティベースのポリシーを作成すると、そのポリシーを持つエンティティ (ユーザーまたはロール) に対してコンソールが意図したとおりに機能しません。

AWS CLI または AWS API のみを呼び出すユーザーには、最小限のコンソールアクセス許可を付与する必要はありません。代わりに、実行しようとしている API オペレーションに一致するアクションのみへのアクセスが許可されます。

ユーザーとロールが引き続き Strategy Recommendations コンソールを使用できるようにするには、エンティティに Strategy Recommendations `ConsoleAccess`または `ReadOnly` AWS 管理ポリシーもアタッチします。詳細については、『IAM ユーザーガイド』の「ユーザーへの権限の追加」を参照してください。

自分の許可の表示をユーザーに許可する

この例では、ユーザーアイデンティティに添付されたインラインおよびマネージドポリシーの表示を IAM ユーザーに許可するポリシーを作成する方法を示します。このポリシーには、コンソールで、または AWS CLI または AWS API を使用してプログラムでこのアクションを実行するアクセス許可が含まれています。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

1 つの Amazon S3 バケットへのアクセス

この例では、 の IAM ユーザーに Amazon S3 バケットの 1 つである AWS アカウント へのアクセス権を付与しますexamplebucket。また、ユーザーがオブジェクトを追加、更新、および削除できるようにします。

このポリシーでは、ユーザーに s3:PutObject、s3:GetObject、s3:DeleteObject のアクセス許可を付与するだけでなく、s3:ListAllMyBuckets、s3:GetBucketLocation、および s3:ListBucket のアクセス許可も付与します。これらが、コンソールで必要とされる追加のアクセス許可です。またコンソール内のオブジェクトのコピー、カット、貼り付けを行うためには、s3:PutObjectAcl および s3:GetObjectAcl アクションが必要となります。コンソールを使用して、ユーザーにアクセス許可を付与し、テストする例の解説については、「チュートリアル例: ユーザーポリシーを使用したバケットへのアクセスのコントロール」を参照してください。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"ListBucketsInConsole",
         "Effect":"Allow",
         "Action":[
            "s3:ListAllMyBuckets"
         ],
         "Resource":"arn:aws:s3:::*"
      },
      {
         "Sid":"ViewSpecificBucketInfo",
         "Effect":"Allow",
         "Action":[
            "s3:ListBucket",
            "s3:GetBucketLocation"
         ],
         "Resource":"arn:aws:s3:::examplebucket"
      },
      {
         "Sid":"ManageBucketContents",
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
```

```
            "s3:PutObjectAcl",
            "s3:GetObject",
            "s3:GetObjectAcl",
            "s3:DeleteObject"
         ],
         "Resource":"arn:aws:s3:::examplebucket/*"
      }
   ]
}
```

Migration Hub Strategy Recommendations のアイデンティティとアクセスに関するトラブルシューティング

次の情報は、Strategy Recommendations と IAM の使用に伴って発生する可能性がある一般的な問題の診断や修復に役立ちます。

トピック

- Strategy Recommendations でアクションを実行する権限がない
- iam を実行する権限がありません。PassRole
- アクセスキーを表示したい
- 管理者であり、他のユーザーが Strategy Recommendations にアクセスできるようにしたいと考えている
- 自分の 以外のユーザーに Strategy Recommendations リソース AWS アカウント へのアクセスを許可したい

Strategy Recommendations でアクションを実行する権限がない

から、アクションを実行する権限がないと AWS Management Console 通知された場合は、管理者に連絡してサポートを依頼する必要があります。管理者とは、ユーザーにユーザー名とパスワードを提供した人です。

以下のエラー例は、`mateojackson` IAM ユーザーがコンソールを使用して架空の *`my-example-widget`* リソースに関する詳細情報を表示しようとしているが、架空の `migrationhub-strategy:`*`GetWidget`* アクセス許可がないという場合に発生します。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 migrationhub-strategy:GetWidget on resource: my-example-widget
```

この場合、Mateo は、migrationhub-strategy:*GetWidget* アクションを使用して *my-example-widget* リソースにアクセスできるように、ポリシーの更新を管理者に依頼します。

iam を実行する権限がありません。PassRole

iam:PassRole アクションを実行する権限がないというエラーが表示された場合は、ポリシーを更新して Strategy Recommendations にロールを渡せ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アクセス許可が必要です。

以下の例のエラーは、marymajor という IAM ユーザーがコンソールを使用して Strategy Recommendations 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。Mary には、ロールをサービスに渡す権限がありません。

```
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 Mary 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。

アクセスキーを表示したい

IAM ユーザーアクセスキーを作成した後は、いつでもアクセスキー ID を表示できます。ただし、シークレットアクセスキーを再表示することはできません。シークレットアクセスキーを紛失した場合は、新しいアクセスキーペアを作成する必要があります。

アクセスキーは、アクセスキー ID (例: AKIAIOSFODNN7EXAMPLE) とシークレットアクセスキー (例: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY) の 2 つの部分で構成されています。ユーザー名とパスワードと同様に、リクエストを認証するために、アクセスキー ID とシークレットアクセス

キーの両方を使用する必要があります。ユーザー名とパスワードと同様に、アクセスキーは安全に管理してください。

> **Important**
>
> 正規のユーザー ID を検索するためであっても、アクセスキーを第三者に提供しないでください。これにより、 への永続的なアクセス権を誰かに付与できます AWS アカウント。

アクセスキーペアを作成する場合、アクセスキー ID とシークレットアクセスキーを安全な場所に保存するように求めるプロンプトが表示されます。このシークレットアクセスキーは、作成時にのみ使用できます。シークレットアクセスキーを紛失した場合、IAM ユーザーに新規アクセスキーを追加する必要があります。アクセスキーは最大 2 つまで持つことができます。既に 2 つある場合は、新規キーペアを作成する前に、いずれかを削除する必要があります。手順を表示するには、「IAM ユーザーガイド」の「アクセスキーの管理」を参照してください。

管理者であり、他のユーザーが Strategy Recommendations にアクセスできるようにしたいと考えている

Strategy Recommendations へのアクセスを他のユーザーに許可するには、アクセスを必要とする人またはアプリケーションの IAM エンティティ (ユーザーまたはロール) を作成する必要があります。ユーザーまたはアプリケーションは、そのエンティティの認証情報を使用して AWSにアクセスします。次に、Strategy Recommendations の適切なアクセス許可を付与するポリシーを、そのエンティティにアタッチする必要があります。

すぐにスタートするには、「IAM ユーザーガイド」の「IAM が委任した初期のユーザーおよびグループの作成」を参照してください。

自分の 以外のユーザーに Strategy Recommendations リソース AWS アカウント へのアクセスを許可したい

他のアカウントのユーザーや組織外の人が、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまたはアクセスコントロールリスト (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

詳細については、以下を参照してください:

- Strategy Recommendations がこれらの機能をサポートしているかどうかについては、「Migration Hub Strategy Recommendations と IAM を連携する方法」を参照してください。

- 所有 AWS アカウント する のリソースへのアクセスを提供する方法については、IAM ユーザーガイドの「所有 AWS アカウント する別の の IAM ユーザーへのアクセスを許可する」を参照してください。
- リソースへのアクセスをサードパーティーの に提供する方法については AWS アカウント、IAM ユーザーガイドの「第三者 AWS アカウント が所有する へのアクセス権を付与する」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、「IAM ユーザーガイド」の「外部で認証されたユーザー (ID フェデレーション) へのアクセス権の提供」を参照してください。
- クロスアカウントアクセスでのロールとリソースベースのポリシーの使用の違いの詳細については、「IAM ユーザーガイド」の「IAM ロールとリソースベースのポリシーとの相違点」を参照してください。

Strategy Recommendations のサービスリンクロールを使用する

Migration Hub Strategy Recommendations 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、Strategy Recommendations 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、Strategy Recommendations 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 の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。

サービスリンクロールを使用すると、必要なアクセス許可を手動で追加する必要がないため、Strategy Recommendations のセットアップが簡単になります。Strategy Recommendations は、サービスリンクロールのアクセス許可を定義します。別の指定がない限り、Strategy Recommendations のみがそのロールを引き受けることができます。定義されたアクセス許可には、信頼ポリシーとアクセス権限ポリシーが含まれ、そのアクセス権限ポリシーを他の IAM エンティティに適用することはできません。

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ロールに関するドキュメントをサービスで表示するには、[はい] リンクを選択します。

Strategy Recommendations のサービスリンクロールのアクセス許可

Strategy Recommendations は、 という名前のサービスにリンクされたロールを使用して AWSServiceRoleForMigrationHubStrategy IAM AWSMigrationHubStrategyServiceRolePolicy ポリ

シーに関連付けます。これにより、 AWS Migration Hub および へのアクセスが可能になります AWS Application Discovery Service。このポリシーにより、レポートを Amazon Simple Storage Service (Amazon S3) に格納する権限も付与されます。

AWSServiceRoleForMigrationHubStrategy サービスにリンクされたロールは、ロールの引き受けについて以下のサービスを信頼します。

- `migrationhub-strategy.amazonaws.com`

ロールのアクセス許可ポリシーは、以下のアクションを実行することを Strategy Recommendations に許可します。

AWS Application Discovery Service アクション

```
discovery:ListConfigurations

discovery:DescribeConfigurations
```

AWS Migration Hub アクション

```
mgh:GetHomeRegion
```

Amazon S3 のアクション

```
s3:GetBucketAcl

s3:GetBucketLocation

s3:GetObject

s3:ListAllMyBuckets

s3:ListBucket

s3:PutObject

s3:PutObjectAcl
```

このポリシーのアクセス許可を確認するには、「 AWS マネージドポリシーリファレンスガイドAWSMigrationHubStrategyServiceRolePolicy」の「」を参照してください。

このポリシーの更新履歴を確認するには、「戦略、推奨事項、 AWS 管理ポリシーの更新」を参照してください。

サービスリンクロールの作成、編集、削除を IAM エンティティ (ユーザー、グループ、ロールなど) に許可するには、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権限」を参照してください。

Strategy Recommendations のサービスリンクロールの作成

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。Migration Hub が のアカウントにサービスにリンクされたロール (SLR) を作成することを許可することに同意した場合 AWS Management Console、Strategy Recommendations によってサービスにリンクされたロールが作成されます。

このサービスリンクロールを削除した後で再度作成する必要が生じた場合は、同じ方法でアカウントにロールを再作成できます。Migration Hub がアカウントにサービスリンクロール (SLR) を作成する許可に同意すると、Strategy Recommendations によって再度、サービスリンクロールが作成されます。

Strategy Recommendations のサービスリンクロールの編集

Strategy Recommendations では、AWSServiceRoleForMigrationHubStrategyサービスにリンクされたロールを編集することはできません。サービスリンクロールを作成すると、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、Strategy Recommendations コンソール、CLI、または API を使用してロールの説明を編集することはできます。

Strategy Recommendations のサービスリンクロールの削除

サービスにリンクされたロールを IAM で手動削除するには

IAM コンソール、、または AWS API を使用して AWS CLI、AWSServiceRoleForMigrationHubStrategyサービスにリンクされたロールを削除します。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削除」を参照してください。

AWSServiceRoleForMigrationHubStrategy SLR で使用されている Strategy Recommendations リソースを削除する場合、実行中の評価 (レコメンデーションを生成するためのタスク) は使用できません。バックグラウンド評価も実行できません。評価が実行中の場合、IAM コンソールでの SLR の削除は失敗します。SLR の削除が失敗した場合は、すべてのバックグラウンドタスクが完了した後に削除を再試行できます。SLR を削除する前に、作成されたリソースをクリーンアップする必要はありません。

Strategy Recommendations のサービスリンクロールでサポートされるリージョン

Strategy Recommendations は、サービスが利用可能なすべてのリージョンでサービスリンクロールの使用をサポートします。詳細については、「AWS リージョンとエンドポイント」を参照してください。

Migration Hub Strategy Recommendations およびインターフェースVPC エンドポイント (AWS PrivateLink)

VPC と Migration Hub Strategy Recommendations とのプライベート接続を確立するには、インターフェース VPC 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は を使用しますAWS PrivateLink AWS PrivateLink を使用すると、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 接続なしで、API オペレーションにプライベートにアクセスできます。VPC 内のインスタンスは、パブリック IP アドレスがなくても Strategy Recommendations API と通信できます。VPC と Strategy Recommendations 間のトラフィックは、Amazon ネットワーク内に留まります。

各インターフェースエンドポイントは、サブネット内の 1 つ以上の Elastic Network Interface によって表されます。

詳細については、Amazon VPC ユーザーガイド の インターフェース VPC エンドポイント (AWS PrivateLink) をご参照ください。

Strategy Recommendations VPC エンドポイントに関する考慮事項

Strategy Recommendations のインターフェイス VPC エンドポイントを設定する前に、「Amazon VPC ユーザーガイド」の「インターフェイスエンドポイントのプロパティと制限」および「AWS PrivateLink クォータ」を確認してください。

Strategy Recommendations は、VPC からのすべての API アクションの呼び出しをサポートしています。Strategy Recommendations をすべて使用するには、VPC エンドポイントを作成する必要があります。

ストラテジーレコメンデーション用のインターフェイス VPC エンドポイントの作成

Strategy Recommendations 用の VPC エンドポイントは、Amazon VPC コンソールまたは AWS Command Line Interface (AWS CLI) で作成できます。詳細については、Amazon VPC ユーザーガイドのインターフェイスエンドポイントの作成を参照してください。

Strategy Recommendations 用の VPC エンドポイントは、以下のサービス名を使用して作成します。

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

エンドポイントのプライベート DNS を使用すると、リージョンのデフォルト DNS 名を使用して、Strategy Recommendations への API リクエストを実行できます。たとえば、名前の `migrationhub-strategy.us-east-1.amazonaws.com` を使用できます。

詳細については、「Amazon VPC ユーザーガイド」の「インターフェイスエンドポイントを介したサービスへのアクセス」を参照してください。

Strategy Recommendations 用の VPC エンドポイントポリシーの作成

VPC エンドポイントには、Strategy Recommendations へのアクセスを制御するエンドポイントポリシーをアタッチできます。このポリシーでは、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。
- 実行可能なアクション。
- これらのアクションを実行できるリソース。

詳細については、Amazon VPC ユーザーガイドのVPC エンドポイントによるサービスのアクセスコントロールを参照してください。

例: Strategy Recommendations アクションの VPC エンドポイントポリシー

Strategy Recommendations のエンドポイントポリシーの例を次に示します。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 Strategy Recommendations アクションへのアクセス権を付与します。

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

```
    ]
}
```

Migration Hub Strategy Recommendations 向けコンプライアンスの検証

AWS のサービス が特定のコンプライアンスプログラムの範囲内にあるかどうかを確認するには、コンプライアンスプログラムAWS のサービス による対象範囲内のコンプライアンスプログラムを参照し、関心のあるコンプライアンスプログラムを選択します。一般的な情報については、AWS 「コンプライアンスプログラム」を参照してください。

を使用して、サードパーティーの監査レポートをダウンロードできます AWS Artifact。詳細については、「 でのレポートのダウンロード AWS Artifact」の」を参照してください。

を使用する際のお客様のコンプライアンス責任 AWS のサービス は、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および規制によって決まります。 では、コンプライアンスに役立つ以下のリソース AWS を提供しています。

- セキュリティとコンプライアンスのクイックスタートガイド – これらのデプロイガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスに重点を置いたベースライン環境 AWS を にデプロイする手順について説明します。
- アマゾン ウェブ サービスにおける HIPAA セキュリティとコンプライアンスのアーキテクチャ — このホワイトペーパーでは、企業が AWS を使用して HIPAA 対象アプリケーションを作成する方法について説明します。

  > **Note**
  >
  > すべて AWS のサービス HIPAA の対象となるわけではありません。詳細については、「HIPAA 対応サービスのリファレンス」を参照してください。

- AWS コンプライアンスリソース – このワークブックとガイドのコレクションは、お客様の業界や地域に適用される場合があります。
- AWS カスタマーコンプライアンスガイド — コンプライアンスの観点から責任共有モデルを理解します。このガイドでは、ガイダンスを保護し AWS のサービス 、複数のフレームワーク (米国国立標準技術研究所 (NIST)、Payment Card Industry Security Standards Council (PCI)、国際標準化機構 (ISO) を含む) のセキュリティコントロールにマッピングするためのベストプラクティスをまとめています。

- 「 デベロッパーガイド」の「 ルールによるリソースの評価」 – この AWS Config サービスは、リソース設定が社内プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。 AWS Config
- AWS Security Hub – これにより AWS のサービス 、 内のセキュリティ状態を包括的に確認できます AWS。Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セキュリティ業界標準とベストプラクティスに対するコンプライアンスをチェックします。サポートされているサービスとコントロールのリストについては、「Security Hub のコントロールリファレンス」を参照してください。
- Amazon GuardDuty – これにより AWS アカウント、疑わしいアクティビティや悪意のあるアクティビティがないか環境を監視することで、、、ワークロード、コンテナ、データに対する潜在的な脅威 AWS のサービス を検出します。 GuardDuty は、特定のコンプライアンスフレームワークで義務付けられている侵入検知要件を満たすことで、PCI DSS などのさまざまなコンプライアンス要件への対応に役立ちます。
- AWS Audit Manager – これにより AWS のサービス 、 AWS 使用状況を継続的に監査し、リスクの管理方法と規制や業界標準への準拠を簡素化できます。

他の サービスでの使用

このセクションでは、Migration Hub Strategy Recommendations と提携するその他の AWS サービスについて説明します。

トピック

- AWS CloudTrail を持つ Strategy Recommendations API 呼び出しのログ記録

AWS CloudTrail を持つ Strategy Recommendations API 呼び出しのログ記録

Migration Hub Strategy Recommendations は、ストラテジーレコメンデーションのユーザー、ロール、または AWS サービスによって実行されたアクションを記録するサービス AWS CloudTrail と統合されています。CloudTrail の API コールをイベントとして、Strategy Recommendations にキャプチャします。キャプチャされたコールには、Strategy Recommendations コンソールからの呼び出しと Strategy Recommendations API オペレーションへのコード呼び出しが含まれます。

証跡を作成する場合は、Strategy Recommendations 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。追跡を設定しない場合でも、CloudTrail コンソールの [Event history] (イベント履歴) で最新のイベントを表示できます。CloudTrail で収集された情報を使用して、Strategy Recommendations に対するリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。

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 での Strategy Recommendations の情報

CloudTrail は、アカウント作成時に AWS アカウント で有効になります。Strategy Recommendations 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 サービスのイベントとともに CloudTrail イベントに記録されます。最近のイベントは、AWS アカウント で表示、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。

Strategy Recommendations 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きに、証跡がすべての AWS リージョン に

適用されます 証跡は、AWS パーティションのすべてのリージョンからのイベントを口グに記録し、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 ログで収集したイベントデータをより詳細に分析し、それに基づく対応するためにその他の AWS の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。

- 「追跡を作成するための概要」
- CloudTrail がサポートされているサービスと統合
- CloudTrail の Amazon SNS 通知の設定
- 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

Strategy Recommendations は、CloudTrail ログファイルのイベントとして次のアクションのログ記録をサポートします。

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

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から以下を判断することができます。

- リクエストが、ルートと AWS Identity and Access Management (IAM) ユーザー認証情報のどちらを使用して送信されたか
- リクエストの送信に使用された一時的なセキュリティ認証情報に、ロールとフェデレーティッドユーザーのどちらが使用されたか
- リクエストが、別の AWS のサービスによって送信されたかどうか

詳細については、「CloudTrail userIdentity エレメント」を参照してください。

Strategy Recommendations ログファイルエントリについて

「トレイル」は、指定した Simple Storage Service (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 のログファイルには、単一か複数のログエントリがあります。イベントはあらゆるソースからの単一のリクエストを表し、リクエストされたアクション、アクションの日時、リクエストのパラメータなどの情報が含まれます。CloudTrail ログファイルは、パブリック API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

GetServerDetails のアクションを示す CloudTrail ログエントリの例を次に示します。

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

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

Migration Hub Strategy Recommendations のクォータ

AWS アカウントには、AWS のサービスごとにデフォルトのクォータ (以前は制限と呼ばれていました) があります。特に明記されていない限り、クォータはリージョンごとに存在します。一部のクォータについては引き上げをリクエストできますが、その他のクォータについてはリクエストできません。

Migration Hub Strategy Recommendations のクォータのリストを表示するには、「Strategy Recommendations サービスクォータ」を参照してください。

Service Quotas コンソールを開いて、Strategy Recommendations のクォータを確認することもできます。ナビゲーションペインで [AWS サービス] を選択し、[Migration Hub Strategy Recommendations] を選択します。

クォータの引き上げをリクエストするには、「Service Quotas ユーザーガイド」の「クォータ引き上げリクエスト」を参照してください。Service Quotas でクォータがまだ利用できない場合は、[制限の引き上げ] のフォームを使用してください。

リリースノート

トピック

2023 年 11 月 17 日

新しい特徴

- コレクター v1.1.47
- .NET 8 アプリケーションのSupport。

2023 年 10 月 12 日

新しい特徴

- コレクター v1.1.45

- マルチデータソースのSupport。

2023 年 4 月 17 日

新しい特徴

- コレクター v1.1.22
- スクリプトの強化に関するアップグレード。これには、最新バージョンの Collector が必要です。

2023 年 3 月 17 日

新機能

ソースコードなしでアンチパターンや非互換性を検出できるバイナリ分析が追加されました。

2022 年 11 月 7 日

新機能

- アプリケーション用アプリケーションフィルタリング
- AWS Application Discovery Service タグによるサーバーフィルタリング

2022 年 9 月 27 日

新機能

- コレクター v1.1.12
  - SCT バージョン 667
  - EMPAnalyzer 2.2.0.368
- サーバーインサイト用の `diag check` コマンドが追加されました。
- ポテンシャルレコメンデーションのサポートが追加されました。
- 設定と評価のステータスを確認できるユーザーインターフェースが強化されました。

バグ修正

- アシスタントトランスレーターの移植とその他の修正。

2022 年 6 月 30 日

新機能

- コレクター v1.1.11
  - VMware API サポートが追加されました。
  - A2C は、バイナリファイルのダウンロード中にユーザーヘッダーを追加するように変更を要求しました。
  - Linux ホームパス、デフォルトシェル、すべてのシェルのリモートターミネーションを追加しました。
- A2C v1.17 パブリックバイナリ
  - DevOps パイプラインデプロイターゲットとして Azure のサポートが追加されました。

2022 年 4 月 18 日

新機能

- コレクター v1.1.7
- パブリック URL から A2C バイナリを動的にダウンロードする機能が追加されました。

バグ修正

- A2C v1.1.5

2022 年 2 月 25 日

バグ修正

- SCT v5.6.9
- A2C v1.1.2
- コレクター v1.1.4

2022 年 2 月 10 日

バグ修正

- SCT v5.6.8
- A2C v1.1.1
  - Linux での tar コマンドのチェックを追加しました。
  - Amazon ECR でのアプリケーションイメージチェックの問題を修正しました。
  - 事前検証を行うためにコンテナを削除する必要がある問題を修正しました。
- コレクター v1.1.3
  - リモート 32 ビットマシンの 4xx エラーを修正しました。
  - A2C エラーコードを更新しました。
  - リモートマシンのソースコード分析用に C# の IP アドレスを検証しました。

2022 年 1 月 28 日

新機能

- コレクター v1.1.2
- ソースコード分析用の Azure DevOps Git リポジトリサポートを追加しました。

2022 年 1 月 14 日

新機能

- コレクター v1.1.1
- SQL データベースの Babelfish レコメンデーションが追加されました。

2021 年 12 月 21 日

[解決された問題]

- コレクター v1.1.0
- データベース分析が復元されました。

2021 年 12 月 15日

[既知の問題]

- コレクター v1.0.4
- 現在、データベース分析はサポートされていません (CVE-2021-44228)。

2021 年 10 月 25 日

新機能

- コレクター v1.0.0
- Migration Hub Strategy Recommendations ユーザーガイドの初回リリース。

ドキュメントとバージョン履歴

次の表は、Strategy Recommendations のドキュメントリリースの一覧です。詳細については、「リリースノート」を参照してください。

変更	説明	日付
AWS 管理ポリシーの更新-更新 AWSMigrationHubStrategyCollector	新しい、`s3application-transformation` 、AWSMigrationHubStrategyCollector`migrationhub-strategy` アクションを含むようにポリシーを更新しました。	2024 年 4 月 1 日
AWS 管理ポリシーの更新-更新 AWSMigrationHubStrategyCollector	AWSMigrationHubStrategyCollector`application-transformation` 新しいアクションを含むようにポリシーを更新しました。今回の更新では、`aws:ResourceAccount` `aws:PrincipalAccount` と等しくなければならないさまざまなアクションを制限する条件も追加されています。	2024 年 2 月 5 日
新機能	ストラテジー推奨アプリケーションデータコレクタクライアント v1.1.47 は、.NET 8 アプリケーションをサポートして提供されています。	2023 年 11 月 17 日
新機能	Strategy Recommendations アプリケーションデータコレクタークライアント v1.1.45	2023 年 10 月 12 日

	は、複数のデータソースをサポートしています。	
AWS 管理ポリシーの更新-に更新 AWSMigrationHubStrategyCollector	新しい Amazon S3 API AWSMigrationHubStrategyCollectorを含むようにポリシーを更新しました。	2023 年 9 月 15 日
AWS 管理ポリシーの更新-更新 AWSMigrationHubStrategyCollector	AWSMigrationHubStrategyCollectorソースコード用の新しいアナライザーを含むようにポリシーを更新しました。	2023 年 3 月 8 日
IAM ベストプラクティスの更新	詳細については、「IAM 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。	2023 年 2 月 25 日
AWS 管理ポリシーの更新-既存のポリシーへの更新	Migration Hub 戦略提言では、AWS Application Discovery Service 既存のポリシーに3つのAPIが追加されました。	2022 年 11 月 10 日
セキュリティ更新	インターフェイス VPC エンドポイントとのプライベート接続を確立します。	2022 年 3 月 7 日
新機能	ソースコード分析用の Azure DevOps Git リポジトリサポートを追加しました。	2022 年 1 月 28 日
新機能	SQL データベースの Babelfish レコメンデーションが追加されました。	2022 年 1 月 14 日
初回リリース	Migration Hub Strategy Recommendations ユーザーガイドの初回リリース。	2021 年 10 月 25 日

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。