GCP

GCP の概要

GCP プロジェクトと GCP フォルダ

Multicloud Defense は現在、GCP プロジェクトと GCP フォルダの両方をサポートしていますが、これらのコンポーネントは個別にサポートされています。これらの両方のオプションについて、次の制限事項と例外に注意してください。

GCP プロジェクトには、仮想マシン、ストレージバケット、データベースなどの GCP リソースを含めることができます。すべての Google Cloud サービスを作成、有効化、および使用するために使用できます。

- プロジェクトは、Terraform、手動オンボーディング、およびスクリプト化されたオンボーディングを使用してオンボーディングできます。
- プロジェクトは、検出や調査などのオーケストレーションを必要とする環境に最適です。
- 各プロジェクトは Multicloud Defense ダッシュボードから個別に操作できます。

バージョン 23.10 では、Terraform を使用して GCP フォルダを接続できます。GCPフォルダには、プロジェクト、他のフォルダ、またはその両方の組み合わせが含まれます。組織リソースは、フォルダを使用して、階層内の組織リソースノードの下にプロジェクトをグループ化できます。

- `roles/compute.admin` 権限が有効になっていないフォルダは空と見なされ、使用されません。
- オンボーディングされたフォルダに関連付けられているプロジェクトは、アセットとトラフィックの検出にのみ使用されます。

- オンボーディングされたフォルダに関連付けられているプロジェクトは、サービス VPC のオーケストレーションまたはゲートウェイの作成には対応していません。
- GCP コンソールからフォルダに付与する権限は、フォルダレベルで付与する必要があります。そのため、Multicloud Defense のアクションはフォルダレベルでも行われます。

GCP フォルダをオンボードする場合は、「Terraform リポジトリ」を参照してください。

手順の概要

次に、GCP プロジェクトを接続する方法の概要を示します。シェル**スクリプト**が Multicloud Defense によって提供されるため、接続プロセスをウィザードの一部として簡単に進めることができます。次の手順はスクリプトによって自動化されるため、実行する必要はありません。

1. サービスアカウントを 2 つ作成します。
2. 次の API（Compute Engine、Secret Manager）を有効にします。
3. 次の 2 つの VPC（管理、データパス）を作成します。
4. データパス VPC で Multicloud Defense Gateway へのトラフィック（アプリケーション トラフィック）を許可するファイアウォールルールを作成します。
5. 管理 VPC で Multicloud Defense Controller から Multicloud Defense Gateway への管理トラフィックを許可するファイアウォールルールを作成します。

スクリプトが機能しない場合、または設定を手動で変更する必要がある場合は、GCP クラウドコンソールの Web UI または gcloud CLI を使用してこれらのアクションを実行できます。プロジェクトを接続する別のメソッドについては、こちらを参照してください。

GCP コントローラ サービス アカウントの作成

コントローラ サービス アカウントは、GCP プロジェクトのリソースにアクセスして管理するために Multicloud Defense Controller によって使用されます。アカウントを作成し、キーを生成する必要があります。キーは、コントローラへのアカウントオンボーディングの一部としてコントローラに追加されます。

手順

ステップ 1 GCP ダッシュボードで、GCP プロジェクトの IAM を開きます。

ステップ 2 [サービスアカウント（Service Account）] をクリックします。

ステップ 3 サービスアカウントを作成します。

ステップ 4 名前と ID（`multicloud-firewall`など）を入力し、[作成（Create）] をクリックします。

ステップ 5 [コンピューティング管理者（Computing Admin）] ロールと [サービスアカウントユーザー（Service Account User）] ロールを追加します。

ステップ 6 [続行（Continue）] をクリックします。

ステップ 7 [完了（Done）] をクリックします。

ステップ 8 新しく作成したアカウントをクリックし、[キー（Keys）] までスクロールして、[キーの追加（Add Key）] ドロップダウンで [新しいキーの作成（Create New Key）] を選択します。

ステップ 9 [JSON]（デフォルトオプション）を選択し、[作成（Create）] をクリックします。

ステップ 10 ファイルがコンピュータにダウンロードされます。このファイルをローカルドライブに保存します。

GCP ファイアウォール サービス アカウントの作成

ファイアウォール サービス アカウントは、GCP プロジェクト内で実行されている Multicloud Defense Gateway インスタンスによって使用されます。ゲートウェイは、TLS 復号のために Secret Manager に保存されている秘密キーにアクセスし、PCAP ファイルなどを保存するためのストレージにアクセスする必要があります（ユーザーが設定した場合）。また、多くのゲートウェイには、Multicloud Defense Gateway から GCP ロギングインスタンスにログを送信するためのログ作成者権限が必要です（ユーザーが設定した場合）。

コントローラ サービス アカウントを作成するには、次の手順を実行します。

手順

ステップ 1 GCP ダッシュボードで、GCP プロジェクトの IAM を開きます。

ステップ 2 [サービスアカウント（Service Account）] をクリックします。

ステップ 3 サービスアカウントを作成します。

ステップ 4 名前と ID（`multicloud-firewall`など）を入力し、[作成（Create）] をクリックします。

ステップ 5 [シークレットマネージャ（Secret Manager）]、[シークレットアクセサ（Secret Accessor）]、および [ログ作成者（Logs Writer）] ロールを追加します。

ステップ 6 [続行（Continue）] をクリックします。

ステップ 7 [完了（Done）] をクリックします。

Multicloud Defense ダッシュボードから Multicloud Defense Controller への GCP プロジェクトの接続

前のセクションの説明に従って GCP プロジェクトを準備したら、Multicloud Defense Controller にリンクできます。

始める前に

すでに Google Cloud Platform（GCP）プロジェクトを作成済みで、VPC、サブネット、およびサービスアカウントを作成する権限を持っている必要があります。

手順

ステップ 1 CDO の左側のペインで Multicloud Defense をクリックします。
ステップ 2 Multicloud Defense Controller ボタンをクリックします。
ステップ 3 [クラウドアカウント（Cloud Accounts）] ペインで、[アカウントの追加（Add Account）] をクリックします。
ステップ 4 [一般情報（General Information）] ページで、[アカウントタイプ（Account Type）] リストボックスから [GCP] を選択します。
ステップ 5 Multicloud Defense ダッシュボードにログインします。
ステップ 6 [管理（Manage）]、[アカウント（Account）] の順にクリックします。
ステップ 7 [アカウントの追加（Add account）] をクリックします。
ステップ 8 ステップ 1 で、リンクをクリックして Google Cloud Platform Cloud Shell を開きます。
ステップ 9 ステップ 2 で、[コピー（Copy）] ボタンをクリックします。
ステップ 10 Google Cloud Platform Cloud Shell で bash スクリプトを実行します。
ステップ 11 このGCPアカウントの名前を入力します。GCPプロジェクト名と同じ名前を付けることができます。この名前は、Multicloud Defense Controller でのみ表示されます。
ステップ 12 （任意）説明を入力します。
ステップ 13 GCP プロジェクトの [プロジェクトID（Project ID）] を入力します。
ステップ 14 Multicloud Defense Controller 用に作成されたサービスアカウントの [クライアント電子メール（Client Email）] を入力します。
ステップ 15 サービスアカウントの [秘密キー（Private key）] を入力します。
ステップ 16 [保存して続行（Save & Continue）] をクリックします。

次のタスク

トラフィックの可視性を有効化します。

Multicloud Defense によって作成されるロール

提供されたスクリプトを使用してクラウドサービスアカウントを Multicloud Defense Controller にオンボーディングすると、サービス間の通信を確実に保護するために、クラウド サービス プロバイダーのパラメータ内でユーザーロールが作成されます。クラウド サービス プロバイダーに応じて、さまざまなロールと権限が作成されます。

アカウントをオンボーディングすると、次のロールが作成されます。

GCP IAM ロール

このドキュメントでは、前のセクションで使用したCloudFormationテンプレートによって作成されたサービスアカウントの詳細について説明します。

CloudFormation テンプレートによって次のアカウントが作成されます。

- **ciscomcd-controller サービスアカウント**：このアカウントは、Multicloud Defense Controller が GCP プロジェクトにアクセスしてリソース（Multicloud Defense Gateway）、ゲートウェイのロードバランサを作成し、VPC、サブネット、セキュリティグループタグなどに関する情報を読み取るために使用されます。詳細については、GCP コントローラ サービス アカウントの作成 （2 ページ）を参照してください。
- **ciscomcd-firewall サービスアカウント**：このアカウントは Multicloud Defense Gateway（コンピューティング VM インスタンス）に割り当てられます。アカウントは、シークレットマネージャ（TLS 復号用の秘密キー）とストレージへのアクセスを提供します。また、多くのゲートウェイには、Multicloud Defense Gateway から GCP ロギングインスタンスにログを送信するための権限が必要です（ユーザーが設定した場合）。詳細については、GCP ファイアウォール サービス アカウントの作成 （3 ページ）を参照してください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。