GCP

- GCP 개요, on page 1
- 멀티 클라우드 방어 대시보드에서 멀티 클라우드 방어 컨트롤러에 GCP 프로젝트 연결, on page 2

GCP 개요

GCP 프로젝트 및 **GCP** 폴더

멀티 클라우드 방어 현재는 GCP 프로젝트 및 GCP 폴더를 모두 지원합니다. 단 이러한 구성 요소는 별도로 지원됩니다. 이러한 두 옵션에 대해 다음과 같은 제한 및 예외를 참고하십시오.

GCP 프로젝트에는 가상 머신, 스토리지 버킷, 데이터베이스 등과 같은 GCP 리소스가 포함되어야 합니다. 모든 Google Cloud 서비스를 생성, 활성화, 사용하는 데 사용할 수 있습니다.

- 프로젝트는 Terraform, 수동 온보딩, 스크립트 온보딩을 통해 온보딩할 수 있습니다.
- 프로젝트는 검색 및 조사 등 오케스트레이션이 필요한 환경에 적합합니다.
- 멀티 클라우드 방어 대시보드를 통해 각 프로젝트와 개별적으로 상호 작용할 수 있습니다.

버전 23.10부터는 GCP 폴더를 Terraform에 연결할 수 있습니다. GCP 폴더에는 프로젝트, 다른 폴더 또는 이 둘의 조합이 포함됩니다. 조직 리소스는 폴더를 사용하여 계층 구조의 조직 리소스 노드 아래에 프로젝트를 그룹화할 수 있습니다.

- `roles/compute.admin` 권한이 활성화되지 않은 폴더는 비어 있는 것으로 간주되어 사용되지 않습니다.
- 온보딩된 폴더와 연결된 프로젝트는 자산 및 트래픽 검색에만 사용됩니다.
- 온보딩된 폴더와 연결된 프로젝트에서는 오케스트레이션 서비스 VPC 또는 게이트웨이 생성을 수용하지 않습니다.
- GCP 콘솔에서 폴더에 만든 권한은 폴더 레벨에서 만들어야 합니다. 따라서 멀티 클라우드 방어 작업은 폴더 레벨에서도 이루어집니다.

GCP 폴더를 온보딩하려는 경우 Terraform 저장소를 참조하십시오.

절차 개요

다음은 GCP 프로젝트를 연결하는 방법에 대한 개요입니다. 셸 스크립트는 멀티 클라우드 방어에서 제공하며 마법사의 일부로 간편한 연결 프로세스를 지원합니다. 스크립트는 다음 단계를 자동화하므로 사용자가 수행할 필요가 없습니다.

1. 2개의 서비스 어카운트를 생성합니다.
2. 다음 API(Compute Engine, Secret Manager)를 활성화합니다.
3. 다음 2개의 VPC(management, datapath)를 생성합니다.
4. 데이터 경로 VPC에서 멀티 클라우드 방어 게이트웨이(앱 트래픽)에 대한 트래픽을 허용하는 방화벽 규칙을 생성합니다.
5. 관리 VPC에서 관리 트래픽이 멀티 클라우드 방어 게이트웨이에서 멀티 클라우드 방어 컨트롤러(으)로 이동할 수 있도록 방화벽 규칙을 생성합니다.

스크립트가 작동하지 않거나 설정을 수동으로 변경해야 하는 경우 GCP 클라우드 콘솔 웹 UI 또는 gcloud CLI를 사용하여 이러한 작업을 실행할 수 있습니다. 여기에서 프로젝트를 연결하는 다른 방법를 참조하십시오.

멀티 클라우드 방어 대시보드에서 멀티 클라우드 방어 컨트롤러에 **GCP** 프로젝트 연결

이전 섹션에서 설명한 대로 GCP 프로젝트를 준비했다면, 멀티 클라우드 방어 컨트롤러에 연결할 수 있습니다.

Before you begin

Google Cloud Platform(GCP) 프로젝트를 이미 생성했고 VPC, 서브넷, 서비스 어카운트를 생성할 수 있는 권한이 있어야 합니다.

단계 **1** CDO 메뉴 바에서 멀티 클라우드 방어을(를) 클릭합니다.

단계 **2** 멀티 클라우드 방어 컨트롤러 버튼을 클릭합니다.

단계 **3** **Cloud Accounts(**클라우드 어카운트**)** 창에서 **Add Account(**어카운트 추가**)**를 클릭합니다.

단계 **4** **General Information(**일반 정보**)** 페이지에 있는 Account Type(계정 유형) 목록 상자에서 **GCP**를 선택합니다.

단계 **5** 멀티 클라우드 방어 대시보드에 로그인합니다.

단계 **6** **Manage(**관리**)**, **Accounts(**계정**)**를 클릭합니다.

단계 **7** **Add Account(**어카운트 추가**)**를 클릭합니다.

단계 **8** 1단계에서 링크를 클릭하여 Google Cloud Platform Cloud Shell을 엽니다.

단계 **9** 2단계에서 **Copy(**복사**)** 버튼을 클릭합니다.

단계 **10** Google Cloud Platform Cloud Shell에서 bash 스크립트를 실행합니다.

단계 **11** 이 GCP 계정의 이름을 입력합니다. GCP 프로젝트 이름과 동일하게 이름을 지정할 수 있습니다. 이 이름은 멀티 클라우드 방어 컨트롤러에서만 표시됩니다.

단계 **12** (선택 사항) 설명을 입력합니다.

단계 **13** GCP 프로젝트의 프로젝트 **ID**를 입력합니다.

단계 **14** 멀티 클라우드 방어 컨트롤러에 대해 생성된 서비스 어카운트의 **Client Email(**클라이언트 이메일**)**을 입력합니다.

단계 **15** 서비스 어카운트의 개인 키를 입력합니다.

단계 **16** **Save & Continue(**저장 후 계속**)**를 클릭합니다.

What to do next

트래픽 가시성을 활성화합니다.

역할 생성자: 멀티 클라우드 방어

제공된 스크립트를 사용하여 클라우드 서비스 어카운트를 멀티 클라우드 방어 컨트롤러에 온보딩할 경우 서비스 간 통신이 보호되도록 클라우드 서비스 제공자의 매개변수 내에서 사용자 역할이 생성됩니다. 클라우드 서비스 제공자에 따라 서로 다른 역할 및 권한이 생성됩니다.

계정을 온보딩할 때 다음 역할이 생성됩니다.

GCP IAM 역할

이 문서에서는 이전 섹션에서 사용된 CloudFormation 템플릿으로 생성된 서비스 어카운트에 대해 자세히 설명합니다.

CloudFormation 템플릿은 다음 계정을 생성합니다.

- **ciscomcd-controller service account** - 이 어카운트는 멀티 클라우드 방어 컨트롤러가 GCP 프로젝트에 액세스하여 게이트웨이에 대한 리소스(멀티 클라우드 방어 게이트웨이), 로드 밸런서를 생성하고 VPC, 서브넷, 보안 그룹 태그 등에 대한 정보를 읽는 데 사용됩니다.
- **ciscomcd-firewall** 서비스 어카운트 - 이 어카운트는 멀티 클라우드 방어 게이트웨이(컴퓨팅 VM 인스턴스)에 할당됩니다. 계정은 Secret Manager(TLS 암호 해독용 개인 키) 및 스토리지에 대한 액세스를 제공합니다. 또한 여러 게이트웨이에는 (사용자가 구성한 경우) 멀티 클라우드 방어 게이트웨이에서 GCP 로그를 전송하려면 로그 작성자 권한이 필요합니다.