GCP

- GCP 프로젝트 연결을 위한 사전 요건, on page 1
- 멀티 클라우드 방어 대시보드에서 멀티 클라우드 방어 컨트롤러에 GCP 프로젝트 연결, on page 8

GCP 프로젝트 연결을 위한 사전 요건

GCP 프로젝트를 멀티 클라우드 방어에 연결하기 전에 수동으로 구성하려면 다음 단계를 모두 완료하십시오.

1. 2개의 서비스 계정을 생성합니다.
2. 다음 API를 활성화합니다.
   - 계산 엔진
   - 비밀 관리자
3. 다음 2개의 VPC를 생성합니다.
   - 관리
   - 데이터 경로
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.

이러한 작업은 GCP 클라우드 콘솔 웹 UI 또는 gcloud CLI를 사용하여 실행할 수 있습니다. 컴퓨터가 GCP CLI 액세스용으로 구성되지 않은 경우 GCP 클라우드 콘솔에서 명령줄 쉘을 사용할 수 있습니다.

쉘 스크립트

기본 서비스 계정 옵션을 사용하는 위의 모든 단계를 수행하는 셸 스크립트는 여기의 온보딩 지침과 함께 사용할 수 있습니다.

이 단계를 수동으로 수행하려면 또는 위에서 언급한 스크립트로 작성된 설정을 실행할 수 없는 경우 다음 항목의 단계를 수행하십시오.

1. 멀티 클라우드 방어 컨트롤러 서비스 계정을 생성합니다.
   - GCP 클라우드 콘솔을 사용하여 멀티 클라우드 방어 컨트롤러 서비스 계정 생성, on page 3
   - CLI를 사용하여 멀티 클라우드 방어 컨트롤러 서비스 계정 생성, on page 3
2. 멀티 클라우드 방어 방화벽 서비스 계정을 생성합니다.
   - GCP 클라우드 콘솔을 사용하여 멀티 클라우드 방어 방화벽 서비스 계정 생성, on page 5
   - CLI를 사용하여 멀티 클라우드 방어 컨트롤러 방화벽 서비스 계정 생성, on page 5
3. API 활성화
   - API 활성화-GCP 클라우드 콘솔 사용, on page 6
   - API 활성화-CLI 사용, on page 6
4. VPC 설정.
5. 멀티 클라우드 방어 대시보드에서 멀티 클라우드 방어 컨트롤러에 GCP 프로젝트 연결, on page 8
6. 데이터 경로 VPC에서 멀티 클라우드 방어 게이트웨이(앱 트래픽)에 대한 트래픽을 허용하는 방화벽 규칙을 생성합니다.
7. 관리 VPC에서 관리 트래픽이 멀티 클라우드 방어 게이트웨이에서 멀티 클라우드 방어 컨트롤러(으)로 이동할 수 있도록 방화벽 규칙을 생성합니다.

GCP 폴더 제한 사항

23.10부터는 GCP 폴더를 Terraform에 연결할 수 있습니다. 수동 프로세스에서 멀티 클라우드 방어은(는) 환경을 개선할 수 있는 여러 작업을 자동화하지 않습니다. 다음과 같은 제한 사항을 고려하십시오.

- `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.

서비스 어카운트

멀티 클라우드 방어에는 GCP 프로젝트에서 2개의 서비스 계정을 생성해야 합니다.

- 멀티 클라우드 방어**-controller**: 이 계정은 멀티 클라우드 방어 컨트롤러이(가) GCP 프로젝트에 액세스하여 멀티 클라우드 방어 게이트웨이에 대한 리소스(멀티 클라우드 방어 게이트웨이), 로드 밸런서를 생성하고 VPC, 서브넷, 보안 그룹 태그 등에 대한 정보를 읽는 데 사용됩니다.
- 멀티 클라우드 방어**-gateway**: 이 계정은 멀티 클라우드 방어 게이트웨이(컴퓨팅 VM 인스턴스)에 할당됩니다. 계정은 암호 관리자(TLS 암호 해독용 개인 키) 및 스토리지에 대한 액세스를 제공합니다.

이러한 서비스 계정은 UI에서 제공되는 서비스를 사용하거나 클라우드 서비스 제공자의 CLI를 사용하는 두 가지 방법 중 하나로 생성할 수 있습니다.

GCP 클라우드 콘솔을 사용하여 멀티 클라우드 방어 컨트롤러 서비스 계정 생성

멀티 클라우드 방어 컨트롤러 서비스 계정은 멀티 클라우드 방어 컨트롤러에서 GCP 프로젝트의 리소스에 액세스하고 관리하는 데 사용됩니다. 계정을 생성하고 키를 생성해야 합니다. 키는 컨트롤러에 계정을 온보딩할 때 컨트롤러에 추가됩니다.

단계 **1** GCP 프로젝트에서 **IAM**을 엽니다.

단계 **2** **Service Accounts(**서비스 계정**)**를 클릭합니다.

단계 **3** **Service Account(**서비스 계정**)**를 생성합니다.

단계 **4** 이름 및 ID(예: 멀티 클라우드 방어-fcontroller)를 제공하고 **Create(**생성**)**를 클릭합니다.

단계 **5** 컴퓨팅 관리자 및 서비스 계정 사용자 역할을 추가합니다.

단계 **6** **Continue(**계속**)**를 클릭합니다.

단계 **7** **Done(**완료**)**을 클릭합니다.

Note 사용자를 추가할 필요는 없습니다.

단계 **8** 새로 생성된 계정을 클릭하고 **Keys(**키**)**가 나올 때까지 아래로 스크롤한 다음 **Add Key(**키 추가**)** 드롭다운에서 **Create New Key(**새 키 생성**)**를 선택합니다.

단계 **9** JSON(기본 옵션)을 선택하고 **Create(**생성**)**를 클릭합니다.

단계 **10** 파일이 컴퓨터에 다운로드됩니다. 이 파일을 저장합니다.

CLI를 사용하여 멀티 클라우드 방어 컨트롤러 서비스 계정 생성

멀티 클라우드 방어 컨트롤러 서비스 계정을 생성하는 명령:

```
# change these two (2) variable values
ciscomcd_controller_account_name="ciscomcd-controller"
project_name="project1-lastname-123456"

ciscomcd_controller_account_email="$ciscomcd_controller_account_name@$project_name.iam.gserviceaccount.com"
```

```
gcloud iam service-accounts create $ciscomcd_controller_account_name \
    --description="service account used by Multicloud to create resources in the project"
\
    --display-name="ciscomcd-controller-account"

gcloud projects add-iam-policy-binding $project_name \
    --member serviceAccount:$ciscomcd_controller_account_email \
    --role "roles/compute.admin"

gcloud projects add-iam-policy-binding $project_name \
    --member serviceAccount:$ciscomcd_controller_account_email \
    --role "roles/iam.serviceAccountUser"

gcloud iam service-accounts keys create ~/key.json \
    --iam-account $ciscomcd_controller_account_emailmail
```

GCP 프로젝트 권한

콘솔에서 제공되는 스크립트를 사용하면 이러한 권한이 프로젝트에 자동으로 적용됩니다. CLI를 사용하여 GCP 프로젝트에 연결하고 온보딩할 때는 프로젝트 레벨에서 다음 권한이 활성화되어 있는지 확인합니다.

- # 로깅 관리자 - roles/loggingg.admin
- # Pub/Sub 관리자 - roles/pubsub.admin
- # 보안 관리자 - roles/iam.securityAdmin
- # 서비스 계정 관리자 - roles/iam.serviceAccountAdmin
- # 서비스 계정 키 관리자 - roles/iam.serviceAccountKeyAdmin
- # 서비스 사용 관리자 - roles/serviceusage.serviceUsageAdmin
- # 스토리지 관리자 - roles/storage.admin
- # 컴퓨팅 관리자 - roles/compute.admin
- # DNS 관리자 - roles/dns.admin

GCP 폴더 권한

terraform을 사용하여 GCP 폴더를 멀티 클라우드 방어 컨트롤러에 온보딩하는 경우 서비스 계정을 만들고 온보딩할 폴더 아래에 중첩된 프로젝트 중 하나에 연결해야 합니다. 서비스 계정이 생성되면 프로젝트가 포함된 폴더에 다음 권한을 적용해야 합니다.

- # roles/viewer
- # roles/resourcemanager.folderViewer

이러한 권한은 반드시 폴더 레벨에서 활성화되어야 하며, 폴더 내에 있는 프로젝트에 대해서는 활성화되지 않습니다. terraform에서 GCP 폴더를 온보딩하는 방법에 대한 자세한 내용은 Terraform 저장소의 내용을 참조하십시오.

GCP 클라우드 콘솔을 사용하여 멀티 클라우드 방어 방화벽 서비스 계정 생성

멀티 클라우드 방어방화벽 서비스 계정은 멀티 클라우드 방어 게이트웨이GCP 프로젝트 내부에서 실행 중인 인스턴스에서 사용합니다. 게이트웨이는 (사용자가 구성한 경우) PCAP 파일 등을 저장하기 위해 TLS 암호 해독 및 액세스 스토리지를 위해 SecretManager에 저장된 개인 키에 액세스해야 할 수 있습니다. 또한 여러 게이트웨이에는 (사용자가 구성한 경우) 멀티 클라우드 방어 게이트웨이에서 GCP 기록 인스턴스로 로그를 전송하려면 로그 작성자 권한이 필요합니다.

다음은 이 서비스 계정을 생성하는 두(2) 가지 방법입니다.

단계 **1** GCP 프로젝트에서 **IAM**을 엽니다.

단계 **2** **Service Accounts(**서비스 계정**)**를 클릭합니다.

단계 **3** **Service Account(**서비스 계정**)**를 생성합니다.

단계 **4** 이름 및 ID(예: 멀티 클라우드 방어-firewall)를 제공하고 **Create(**생성**)**를 클릭합니다.

단계 **5** **Secret Manager(**비밀 관리자**)**, **Secret Accessor(**비밀 접속자**)** 및 **Logs Writer roles(**로그 작성자 역할**)**를 추가합니다.

단계 **6** **Continue(**계속**)**를 클릭합니다.

단계 **7** **Done(**완료**)**을 클릭합니다.

Note 사용자를 추가할 필요는 없습니다.

CLI를 사용하여 멀티 클라우드 방어 컨트롤러 방화벽 서비스 계정 생성

멀티 클라우드 방어 컨트롤러 방화벽 서비스 계정을 생성하는 명령:

```
# change these two (2) variable values
ciscomcd_firewall_account_name="ciscomcd-firewall"
project_name="project1-lastname-123456"

ciscomcd_firewall_account_email="$ciscomcd_firewall_account_name@$project_name.iam.gserviceaccount.com"

gcloud iam service-accounts create $valtix_firewall_account_name \
    --description="service account used by Multicloud firewall to access secrets, storage"
 \
    --display-name="ciscomcd-firewall-account"

gcloud projects add-iam-policy-binding $project_name \
    --member serviceAccount:$ciscomcd_firewall_account_email \
    --role "roles/secretmanager.secretAccessor"

gcloud projects add-iam-policy-binding $project_name \
    --member serviceAccount:$ciscomcd_firewall_account_email \
    --role "roles/logging.logWriter"
```

API 활성화

GCP 콘솔 또는 클라우드 서비스 공급자의 CLI를 사용하여 멀티 클라우드 방어 컨트롤러과(와) GCP 계정 간의 통신에 API를 활성화할 수 있습니다.

API 활성화-GCP 클라우드 콘솔 사용

멀티 클라우드 방어 컨트롤러이(가) 멀티 클라우드 방어 게이트웨이(가상 머신, 로드 밸런서)를 생성할 수 있도록 프로젝트/계정에서 API를 활성화합니다.

단계 **1** 검색 창에서 **Compute Engine API**를 검색합니다.

단계 **2** **Enable(**활성화**)**을 클릭합니다.

단계 **3** 검색 창에서 **Secret Manager API**를 검색합니다.

단계 **4** **Enable(**활성화**)**을 클릭합니다.

단계 **5** 검색 창에서 **Identity and Access Management(IAM) API**를 검색합니다.

단계 **6** **Enable(**활성화**)**을 클릭합니다.

단계 **7** 검색 창에서 **Cloud Resource Manager API**를 검색합니다.

단계 **8** **Enable(**활성화**)**을 클릭합니다.

API 활성화-CLI 사용

```
json
gcloud services enable secretmanager.googleapis.com
gcloud services enable compute.googleapis.com
gcloud services enable iam.googleapis.com
gcloud services enable cloudresourcemanager.googleapis.com
```

VPC 설정

멀티 클라우드 방어 게이트웨이 인스턴스는 엣지 또는 허브 모드를 사용하여 구축할 수 있습니다. 엣지 모드에서 게이트웨이 인스턴스는 애플리케이션과 동일한 VPC에서 실행됩니다. 이 문서는 엣지 모드 구축을 중점적으로 설명하며, 멀티 클라우드 방어 게이트웨이 구축을 위해 VPC를 준비하는 방법을 안내합니다.

두 VPC에서 모두 멀티 클라우드 방어 게이트웨이이(가) 필요한 지역에서 각각 하나의 서브넷을 생성합니다.

VPC 및 서브넷

멀티 클라우드 방어 게이트웨이 구축 시 멀티 클라우드 방어 컨트롤러에서 관리 및 데이터 경로 VPC 정보를 입력하라는 메시지가 표시됩니다. 멀티 클라우드 방어 게이트웨이 인스턴스에는 2개의 네트워크 인터페이스가 필요합니다. GCP에서 VM 인스턴스의 네트워크 인터페이스는 다른 서브넷에만 있을 수 있는 다른 클라우드 제공자와 달리 다른 VPC에 있어야 합니다. 애플리케이션이 실행 중인 VPC가 이미 있는 경우에는 데이터 경로 VPC 및 서브넷이 있습니다. 관리를 위해 다른 VPC를 생성하거나 다른 기존 VPC를 사용해야 합니다. 자동 생성된 서브넷을 사용하거나 수동으로 생성할 수 있습니다.

*datapath vpc*는 애플리케이션이 실행 중인 *VPC*이며 다음 섹션에서 지칭합니다.

각 VPC에서 멀티 클라우드 방어에는 서브넷이 필요합니다. 멀티 클라우드 방어 게이트웨이를 구축하려는 모든 지역에서 서브넷을 생성합니다.

관리 서브넷은 인터넷에 대한 기본 경로가 있는 라우트 테이블과 연결해야 하는 퍼블릭 서브넷입니다. 멀티 클라우드 방어 게이트웨이 인스턴스에 멀티 클라우드 방어 컨트롤러과(와)의 통신에 사용하는 이 서브넷에 연결된 인터페이스가 있습니다. 이 인터페이스는 멀티 클라우드 방어 컨트롤러 및 멀티 클라우드 방어 게이트웨이 인스턴스 간의 정책 푸시와 기타 관리, 텔레메트리 활동에 사용됩니다. 고객 애플리케이션 트래픽은 이 인터페이스 및 서브넷을 통과하지 않습니다. 인터페이스는 아래의 네트워크 태그 섹션에서 설명하는멀티 클라우드 방어**-management** 네트워크 태그(또는 팀 요구 사항에 기반한 모든 태그)와 연결되어 있습니다.

데이터 경로 서브넷은 인터넷에 대한 기본 경로가 있는 라우트 테이블과 연결해야 하는 퍼블릭 서브넷입니다. 멀티 클라우드 방어 컨트롤러은(는) 이 서브넷에 네트워크 로드 밸런서(NLB)를 생성합니다. 또한, 멀티 클라우드 방어 게이트웨이 인스턴스에 이 서브넷에 연결된 인터페이스가 있습니다. 고객 애플리케이션 트래픽은 이 인터페이스를 통해 흐릅니다. 이 인터페이스를 통해 인그레스하는 트래픽에 보안 정책이 적용됩니다. 인터페이스는 아래의 네트워크 태그 섹션에서 설명하는멀티 클라우드 방어**-datapath** 네트워크 태그(또는 팀 요구 사항에 기반한 모든 태그)와 연결되어 있습니다.

CLI를 사용하여 샘플 VPC 및 서브넷

단계 **1** VPC 앱 및 서브넷 **apps-us-east1**을 생성합니다.

단계 **2** VPC 멀티 클라우드 방어**-mgmt** 및 서브넷 멀티 클라우드 방어**-mgmt-us-east1**을 생성합니다.

단계 **3** 대상 태그가 멀티 클라우드 방어**-mgmt**인 VPC 멀티 클라우드 방어**-mgmt**용 방화벽 규칙.

1. 모든 아웃바운드 트래픽을 허용하는 이그레스 규칙.
2. 방화벽 인스턴스에 대한 SSH를 허용하는 인그레스 규칙.

단계 **4** VPC 앱에 대한 방화벽 규칙.

1. target-tags가 멀티 클라우드 방어**datapath**인 모든 아웃바운드 트래픽을 허용하는 이그레스 규칙.
2. target-tags가 멀티 클라우드 방어**-datapath**인 게이트웨이 인스턴스로의(NLB를 통해) HTTP 및 HTTPS를 허용하는 인그레스 규칙.
3. target-tags가 **app-instance**인 모든 아웃바운드 트래픽을 허용하는 이그레스 규칙.
4. **target-tags**가 **app-instance**인 `tcp:8000`을 허용하는 인그레스 규칙.

```
gcloud config set project <project-name> # incase the project is not set in the gcloud cli shell
gcloud compute networks create apps --subnet-mode custom
gcloud compute networks subnets create apps-us-east1 --network apps --range 10.0.0.0/24 --region us-east1
gcloud compute networks create ciscomcd-mgmt --subnet-mode custom
gcloud compute networks subnets create ciscomcd-mgmt-us-east1 --network ciscomcd-mgmt --range 172.16.0.0/24
 --region us-east1
gcloud compute firewall-rules create ciscomcd-mgmt-out --direction EGRESS --network ciscomcd-mgmt \
    --target-tags ciscomcd-mgmt --allow tcp,udp
gcloud compute firewall-rules create ciscomcd-mgmt-in --direction INGRESS --network valtix-mgmt \
    --target-tags ciscomcd-mgmt --allow tcp:22
gcloud compute firewall-rules create ciscomcd-datapath-out --direction EGRESS --network apps \
    --target-tags valtix-datapath --allow tcp,udp
```

```
gcloud compute firewall-rules create ciscomcd-datapath-in --direction INGRESS --network apps \
    --target-tags ciscomcd-datapath --allow tcp:80,tcp:443
gcloud compute firewall-rules create app-instance-out --direction EGRESS --network apps \
    --target-tags app-instance --allow tcp,udp
gcloud compute firewall-rules create app-instance-in --direction INGRESS --network apps \
    --target-tags app-instance --allow tcp:8000,tcp:22
```

위 명령을 실행한 후에는 앱 VPC에서 VM 인스턴스를 만들고 포트 8000에서 테스트 웹 애플리케이션을 시작할 수 있습니다.

```
gcloud compute instances create app-instance1 \
  --zone=us-east1-b \
  --image-project=ubuntu-os-cloud \
  --image-family=ubuntu-2004-lts \
  --network apps \
  --subnet=apps-us-east1 \
  --tags=app-instance
gcloud compute ssh app-instance1 --zone us-east1-b
echo hello world > index.html
python3 -m http.server 8000
```

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 계정을 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 계정**)** 창에서 **Add Account(**계정 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(**계정 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 계정의 **Client Email(**클라이언트 이메일**)**을 입력합니다.

단계 **15** 서비스 계정의 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 계정을 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 계정에 대해 자세히 설명합니다.

CloudFormation 템플릿은 다음 계정을 생성합니다.

- **ciscomcd-controller service account**- 이 계정은 멀티 클라우드 방어 컨트롤러이(가) 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 계정 - 이 계정은 멀티 클라우드 방어 게이트웨이(컴퓨팅 VM 인스턴스)에 할당됩니다. 계정은 암호 관리자(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.