어카운트 연결 문제 해결

어카운트 수동으로 온보딩

어카운트 온보딩에서 제공하는 방법을 사용하여 클라우드 서비스 제공자 계정을 멀티 클라우드 방어에 온보딩하는 경우, 계정을 수동으로 온보딩해야 할 수 있습니다. 대안으로 다음 옵션을 사용합니다.

GCP 프로젝트 수동 온보딩

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. GCP 프로젝트 수동 온보딩에서 프로젝트를 연결하는 다른 방법를 참조하십시오.

서비스 어카운트

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

- 멀티 클라우드 방어-**controller**: 이 계정은 멀티 클라우드 방어 컨트롤러가 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 Secret Manager(TLS 암호 해독용 개인 키) 및 스토리지에 대한 액세스를 제공합니다.

이러한 서비스 어카운트는 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 어카운트 생성

멀티 클라우드 방어 컨트롤러 서비스 어카운트는 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 어카운트**)**를 클릭합니다.

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

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

단계 **5** 컴퓨팅 관리자 및 서비스 어카운트 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.

GCP 클라우드 콘솔을 사용하여 멀티 클라우드 방어 방화벽 서비스 어카운트 생성

멀티 클라우드 방어방화벽 서비스 어카운트는 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 어카운트를 생성하는 두(2) 가지 방법입니다.

단계 **1** GCP 프로젝트에서 **IAM**을 엽니다.

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

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

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

단계 **5** **Secret Manager(**암호 관리자**)**, **Secret Accessor(**암호 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.

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 컨트롤러가 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.

VPC 설정

멀티 클라우드 방어 게이트웨이 인스턴스는 엣지 또는 허브 모드에서 구축할 수 있습니다. 엣지 모드에서 게이트웨이 인스턴스는 애플리케이션과 동일한 VPC에서 실행됩니다. 이 문서에서는 엣지 모드에서 멀티 클라우드 방어 게이트웨이을 구축하기 위해 준비하는 방법을 중점적으로 설명합니다.

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 데이터 경로용 서브넷 1개와 관리용 서브넷 1개가 필요합니다.

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.

*CLI*를 사용하여 샘플 *VPC* 및 서브넷

다음 명령을 예로 들어 고유한 명령을 실행하여 GCP 어카운트에 대한 VPC를 생성하겠습니다. 다음 특정 명령에 대해 Google Cloud Shell 창을 엽니다.

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 규칙을 2개 이상 생성합니다.

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

단계 **4** VPC 앱에 대한 방화벽 규칙을 3개 이상 생성합니다. 다음의 사례를 예로 들 수 있습니다.

1. target-tags가 `멀티 클라우드 방어datapath`인 모든 아웃바운드 트래픽을 허용하는 하나의 이그레스 규칙.
2. target-tags가 `멀티 클라우드 방어-datapath`인 게이트웨이 인스턴스로의 HTTP 및 HTTPS를 허용하는 하나의 인그레스 규칙.
3. target-tags가 `app-instance`인 모든 아웃바운드 트래픽을 허용하는 하나의 이그레스 규칙.
4. `target-tags`가 `app-instance`인 `tcp:8000`을 허용하는 하나의 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 ciscomcd-mgmt \
    --target-tags ciscomcd-mgmt --allow tcp:22
gcloud compute firewall-rules create ciscomcd-datapath-out --direction EGRESS --network apps \
    --target-tags ciscomcd-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
```

네트워크 태그(**GCP** 게이트웨이용)

관리 및 데이터 경로 네트워크 태그는 위의 서브넷 섹션에서 설명한 대로 멀티 클라우드 방어 게이트웨이 인스턴스의 각 인터페이스와 연결됩니다.

관리 VPC에서 게이트웨이 규칙을 생성하고 이를 멀티 클라우드 방어**-management** 네트워크 태그와 연결합니다. 이렇게 하면 게이트웨이 인스턴스가 컨트롤러와 통신하도록 하는 모든 아웃바운드 트래픽을 허용해야 합니다. 선택적으로, 인바운드 규칙의 경우 포트 22(SSH)를 활성화하여 게이트웨이 인스턴스에 대한 SSH 액세스를 허용합니다. 멀티 클라우드 방어 방화벽이 제대로 작동하기 위해 SSH가 반드시 필요한 것은 아닙니다.

데이터 경로 VPC에서 게이트웨이 규칙을 생성하고 이를 멀티 클라우드 방어**-datapath** 네트워크 태그와 연결합니다. 이렇게 하면 활성화한(활성화할 예정) 모든 서비스에 대한 멀티 클라우드 방어 게이트웨이의 트래픽을 허용해야 합니다.

예를 들어 애플리케이션이 포트 3000에서 실행 중이며 포트 443에서 멀티 클라우드 방어 게이트웨이에 의해 프록시되는 경우, 멀티 클라우드 방어-datapath 네트워크 보안 태그에서 포트 443을 열어야 합니다.

게이트웨이 생성

멀티 클라우드 방어 게이트웨이 생성 페이지에서 다음 매개변수를 사용합니다.

1. 데이터 경로 VPC: **apps**.
2. 데이터 경로 네트워크 태그: 멀티 클라우드 방어**-datapath**.
3. 관리 VPC: 멀티 클라우드 방어**-mgmt**.
4. 관리 네트워크 태그: 멀티 클라우드 방어**-mgmt**.
5. **us-east1-b** 영역을 사용합니다.
6. 관리 서브넷: 멀티 클라우드 방어**-mgmt-us-east1**.
7. 데이터 경로 서브넷: **apps-us-east1**.

다른 지역에 서브넷을 생성하여 멀티 클라우드 방어 게이트웨이을 다중 가용성 영역 모드에서 테스트할 수 있습니다.

Azure 구독 수동 온보딩

멀티 클라우드 방어 컨트롤러 대시보드에서 제공되는 스크립트를 사용하여 Azure 구독을 직접 연결할 수 없는 경우 아래 워크플로우를 사용하여 구독을 수동으로 연결합니다.

(선택 사항) 키 저장소 및 Blob 저장소 액세스를 위해 사용자가 할당하는 관리 ID

멀티 클라우드 방어 게이트웨이은(는) 선택적으로 Azure 키 저장소와 통합하여 TLS 인증서를 검색하고, PCAP(패킷 캡처) 파일을 저장하기 위해 Blob 저장소와 통합할 수 있습니다. 사용자가 할당하는 관리형 ID는 이러한 서비스에 대한 액세스 권한을 부여하는 데 사용됩니다.

Azure Portal에서 **Managed Identities(**관리되는 **ID)**로 이동하여 ID를 생성합니다.

또는 Azure Cloud Shell에서 다음 명령을 실행합니다.

```
az identity create -g <RESOURCE GROUP> -n <USER ASSIGNED IDENTITY NAME>
```

Azure 키 저장소에서 TLS 인증서 암호를 생성하는 방법에 대한 자세한 내용은 Azure 키 저장소의 내용을 참조하십시오.

Azure Active Directory에 애플리케이션 등록

단계 **1** **Azure Active Directory**로 이동합니다.

단계 **2** **App registrations(**앱 등록**)**를 선택합니다.

단계 **3** **New registration(**새 등록**)**을 클릭합니다.

단계 **4** 새 앱 등록을 참조할 이름을 제공합니다. 예를 들어 멀티 클라우드 방어 컨트롤러. *Supported account types(*지원되는 계정 유형*)*에서 두 번째 옵션인 *Accounts in any organizational directory(*조직 디렉터리의 계정*)*를 선택합니다.

단계 **5** 조직에 적절한 옵션을 선택합니다. **Redirect URI(**리디렉션 **URI)**는 앱 등록을 생성하는 데 필요하지 않습니다.

단계 **6** **Register(**등록**)**를 클릭합니다.

단계 **7** 새로 생성된 애플리케이션 아래의 왼쪽 탐색 모음에서 **Certificates and secrets(**인증서 및 암호**)**를 클릭합니다.

단계 **8** **+ New client secret(+** 새 클라이언트 비밀번호**)**를 클릭한 다음 *Add client secret(*클라이언트 비밀번호 추가*)* 대화상자에 필요한 정보를 입력합니다.

- **Description(**설명**)**- 설명을 추가합니다(예: 멀티 클라우드 방어-controller-secret1).
- **Expires(**만료**) - Never(**안 함**)**를 선택합니다. 또한 편의에 따라 선택할 수 있습니다. 현재 암호가 만료되면 새 암호를 생성해야 함)를 선택합니다.

단계 **9** **Add(**추가**)**를 클릭합니다. 클라이언트 비밀이 **Value(**값**)** 열에 채워집니다.

단계 **10** 클라이언트 비밀은 한 번만 표시되고 다시 표시되지 않으므로 메모장에 복사합니다.

단계 **11** 왼쪽 내비게이션 바에서 **Overview(**개요**)**를 클릭합니다.

단계 **12** 애플리케이션**(**클라이언트**) ID** 및 디렉터리**(**테넌트**) ID**를 메모장에 복사합니다.

애플리케이션에 할당할 사용자 지정 역할 생성

멀티 클라우드 방어 컨트롤러를 위해 생성된 애플리케이션에 할당할 맞춤형 역할을 생성합니다. 사용자 지정 역할은 인벤토리 목록 정보를 읽고 리소스(예: VM, 로드 밸런서 등)를 생성할 수 있는 애플리케이션 권한을 제공합니다. 사용자 지정 역할은 여러 방법으로 생성할 수 있습니다.

단계 **1** **Subscription(**구독**)**으로 이동하여 **Access Control (IAM)(**액세스 제어**(IAM))**을 클릭합니다.

단계 **2** **Roles(**역할**)**를 클릭하고 상단 메뉴 모음에서 **+Add(+**추가 **)** > **Add Custom Role(**맞춤형 역할 추가**)**로 이동하여 클릭합니다.

단계 **3** 맞춤형 역할에 이름을 지정합니다(예: `멀티 클라우드 방어-controller-role`).

단계 **4** JSON 편집 화면이 표시될 때까지 **Next(**다음**)**를 계속 클릭합니다.

단계 **5** 화면에서 **Edit(**편집**)**를 클릭하고 JSON 텍스트에서 **permissions(**권한**) > Action(**작업**)** 섹션 아래의 다음 내용을 복사하여 대괄호 사이에 붙여넣습니다(들여쓰기는 유지할 필요 없음).

```
"Microsoft.ApiManagement/service/*",
"Microsoft.Compute/disks/*",
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Compute/images/read",
"Microsoft.Compute/sshPublicKeys/read",
"Microsoft.Compute/virtualMachines/*",
"Microsoft.ManagedIdentity/userAssignedIdentities/read",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
"Microsoft.Network/loadBalancers/*",
"Microsoft.Network/locations/serviceTags/read",
"Microsoft.Network/networkinterfaces/*",
"Microsoft.Network/networkSecurityGroups/*",
"Microsoft.Network/publicIPAddresses/*",
"Microsoft.Network/routeTables/*",
"Microsoft.Network/virtualNetworks/*",
"Microsoft.Resources/subscriptions/resourcegroups/*",
"Microsoft.Storage/storageAccounts/blobServices/*",
"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Network/networkWatchers/*",
"Microsoft.Network/applicationSecurityGroups/*",
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Insights/Metrics/Read"
```

단계 **6** 선택 사항 - 여러 구독을 멀티 클라우드 방어과(와) 함께 사용하려는 경우 `assignableScopes`에서 JSON을 편집하여 다른 구독 라인을 추가하거나 모든 구독에 사용자 지정 역할을 사용할 수 있도록 *****(별표)로 변경해야 합니다.

단계 **7** 텍스트 상자 맨 위에서 **Save(**저장**)**를 클릭합니다.

단계 **8** **Review + Create(**검토 + 생성**)**를 클릭하고 역할을 생성합니다.

단계 **9** Custom Role(사용자 지정 역할)이 생성되면 **Access Control(IAM)(**액세스 제어**(IAM))**으로 돌아갑니다.

단계 **10** 상단 메뉴 모음에서 **Add(**추가**)** > **Add role assignment(**역할 할당 추가**)**를 클릭합니다.

단계 **11** **Role(**역할**)** 드롭다운에서 위에서 생성한 Custom Role(사용자 지정 역할)을 선택합니다.

단계 **12** **Assign access to(**액세스 권한 할당 대상**)** 드롭다운에서 이를 기본값(Azure AD 사용자, 그룹, 서비스 주체)으로 유지합니다.

단계 **13** **Select(**선택**)** 텍스트 상자에 이전에 생성한 애플리케이션 이름(예: `멀티 클라우드 방어controllerapp`)을 입력하고 **Save(**저장**)**를 클릭합니다.

단계 **14** **Subscription(**구독**)** 페이지의 왼쪽 메뉴 모음에서 **Overview(**개요**)**를 클릭하고 구독 ID를 메모장에 복사합니다.

멀티 클라우드 방어 컨트롤러 온보딩에 필요한 값

계속 진행하기 전에 다음 정보가 있는지 확인하십시오.

- 구독 ID(*subscription overview(*구독 개요*)* 페이지)
- 디렉터리(테넌트) ID(*Azure AD app overview(Azure AD* 앱 개요*)* 페이지)
- 애플리케이션(클라이언트) ID(*Azure AD app overview(Azure AD* 앱 개요*)* 페이지)
- 클라이언트 암호(클라이언트 암호 생성 시 복사됨)

마켓플레이스 약관 동의

멀티 클라우드 방어 컨트롤러는 Azure Marketplace에서 멀티 클라우드 방어 VM(가상 머신) 이미지를 사용하여 게이트웨이 인스턴스를 생성합니다. 각 구독에 대해 약관에 동의해야 합니다. Azure 포털 웹사이트(오른쪽 상단 메뉴 모음)에서 Azure Cloud 쉘을 엽니다. Bash 쉘을 선택하거나 전환하고 다음 명령을 실행합니다(subscription-id를 이전 섹션에서 복사한 구독 ID로 대체).

```
az vm image terms accept --publisher valtix --offer datapath --plan valtix_dp_image
--subscription subscription-id
```

클라우드 어카운트용 **Terraform** 온보딩 스크립트

온보딩 마법사 또는 수동 프로세스를 사용하는 대신 terraform 스크립트를 사용하여 클라우드 서비스 제공자 어카운트를 온보딩합니다.

Terraform 정보

멀티 클라우드 방어고객은 **Terraform Provider**를 사용하여 검색 - 퍼블릭 클라우드 어카운트 온보딩, 지속적인 자산 가시성 확보, 침해 지표(IoC) 탐지, 구축 - 멀티 클라우드 방어 게이트웨이에서 인그레스, 이스트-웨스트 트래픽 보호, 방어 - 지속적으로 검색되는 클라우드 자산으로 멀티 클라우드(AWS, Azure, GCP, OCI) 동적 정책으로 방어 등의 작업을 수행할 수 있습니다.

Attention 멀티 클라우드 방어 컨트롤러 버전 23.10부터는 Terraform 제공자를 사용하여 GCP 폴더와 GCP 프로젝트를 연결할 수 있습니다. 자세한 내용은 Terraform 저장소, on page 10를 참조하십시오.

멀티 클라우드 방어 Terraform 제공자는 Terraform 레지스트리에서 제공되는 "확인된" 제공자입니다. 이제 고객은 멀티 클라우드 방어용 Terraform 제공업체를 사용하여 클라우드 어카운트를 멀티 클라우드 방어에 온보딩하고, 멀티 클라우드 방어 게이트웨이를 구축하고, 인터넷으로부터의 인그레스

공격(WAF, IDS/IPS, Geo-IP)을 방어하고, 송신 트래픽의 유출을 차단하고(TLS 암호 해독, IDS/IPS, AV, DLP, FQDN/URL 필터링), VPC/VNet 간의 이스트-웨스트 공격을 방지하기 위한 보안 정책을 지정하여 보안을 운영에 통합할 수 있습니다. 클라우드 자산 태그를 기반으로 보안 정책을 지정할 수 있습니다(예: "dev", "test", "prod", "pci", "web", "app1" 등).

자세한 내용은 다음을 참조하십시오.

- 멀티 클라우드 방어용 Terraform 제공자를 다운로드합니다.
- GitHub의 예.
- Terraform의 멀티 클라우드 방어 블로그.

Terraform 저장소

활용 사례	설명	**Github** 저장소
AWS 온보딩	Terraform을 사용하여 AWS 계정을 온보딩하기 위한 것입니다.	Github 저장소
AWS 검색 CFT	이 CFT 구축에는 멀티 클라우드 방어의 검색 기능을 사용하는 데 필요한 모든 권한이 포함됩니다. 전체 기능 집합을 보려면 제품 CFT를 사용하십시오.	Github 저장소
AWS 검색	이 모드는 Terraform을 사용하는 검색 전용 모드로 AWS 계정을 온보딩하기 위한 것입니다.	Github 저장소
Azure 온보딩	Terraform을 사용하여 Azure 구독을 온보딩하는 데 사용됩니다.	Github 저장소
GCP 프로젝트 온보딩	Terraform을 사용하여 GCP 프로젝트를 온보딩하기 위한 것입니다.	Github 저장소
GCP 폴더 온보딩	Terraform을 사용하여 GCP 폴더를 온보딩하기 위한 것입니다.	Github 저장소

설정을 Terraform 블록으로 내보내기

고객은 보안 프로파일을 멀티 클라우드 방어 컨트롤러에서 Terraform 리소스 블록으로 내보낼 수 있습니다. 설정을 Terraform 블록으로 내보내려면 원하는 보안 프로파일로 이동하여 선택한 다음 **Export(**내보내기**)** 버튼을 클릭합니다. 이렇게 하면 선택한 개체/보안 프로파일에 대한 Terraform 블록이 포함된 파일이 다운로드됩니다.

다음을 제외한 모든 개체 및 프로파일은 terraform 내보내기를 지원합니다.

- 게이트웨이
- 서비스 VPC/VNet
- 진단