멀티 클라우드 방어에서 클라우드 서비스 제공자 제거

다음 절차에 따라 멀티 클라우드 방어 및 클라우드 서비스 제공자 간의 통신 및 권한을 종료할 수 있습니다. 이 작업에는 멀티 클라우드 방어 컨트롤러 내에서 생성된 게이트웨이 또는 Vnet은 물론 클라우드 서비스 제공자 내에 설정한 역할 또는 위험을 제거하는 작업이 포함됩니다. 모든 멀티 클라우드 방어 인스턴스를 정리하려면 모든 단계를 수행해야 합니다.

이러한 절차 중 일부는 멀티 클라우드 방어 컨트롤러에서 발생하지 않으며, 이러한 절차를 실행하기 위해 클라우드 서비스 제공자의 대시보드에 액세스해야 할 수 있습니다.

GCP 프로젝트 삭제 위치 멀티 클라우드 방어

멀티 클라우드 방어 컨트롤러에서 GCP 계정을 삭제하고 멀티 클라우드 방어의 모든 인스턴스를 GCP 프로젝트에서 제거하려면 다음 절차를 사용합니다. 계정에서 멀티 클라우드 방어을(를) 삭제하기 전에 멀티 클라우드 방어 컨트롤러에서 생성한 서브넷, VNet 또는 게이트웨이를 계정에서 삭제해야 합니다.

참고 이 절차를 수행하려면 멀티 클라우드 방어 UI 및 GCP 대시보드 모두에서 오케스트레이션 준비를 제거해야 합니다.

단계 **1** 멀티 클라우드 방어에서 현재 게이트웨이 또는 VNet을 삭제합니다.

a) 멀티 클라우드 방어 컨트롤러에서 **Manage(**관리**)** > **Gateways(**게이트웨이**)** > **Gateways(**게이트웨이**)**로 이동합니다.

b) 계정과 연결된 게이트웨이를 선택하여 확인란을 선택합니다.

c) **Actions(**작업**)** 드롭다운 메뉴를 확장하고 **Delete(**삭제**)**를 선택합니다.
d) 삭제를 확인합니다.
e) 멀티 클라우드 방어 컨트롤러에서 **Manage(**관리**)** > **Gateways(**게이트웨이**)** > **Service VPCs/VNets(**서비스 **VPCs/VNets)**로 이동합니다.
f) 계정과 연결된 VPC를 선택하여 확인란을 선택합니다.
g) **Actions(**작업**)** 드롭다운 메뉴를 확장하고 **Delete(**삭제**)**를 선택합니다.
h) 삭제를 확인합니다.

참고 VPC 및 게이트웨이를 삭제한 후에는 계열사 서브넷을 삭제할 필요가 없습니다.

단계 **2** 멀티 클라우드 방어 컨트롤러에서 GCP 프로젝트를 삭제합니다.
a) 멀티 클라우드 방어 컨트롤러에서 **Manage(**관리**)** > **Cloud Accounts(**클라우드 어카운트**)** > **Accounts(**어카운트**)**로 이동합니다.
b) Azure 계정을 선택하여 확인란을 선택합니다.
c) **Actions(**작업**)** 드롭다운 메뉴를 확장하고 **Delete(**삭제**)**를 선택합니다.
d) 삭제를 확인합니다.

단계 **3** GCP에서 멀티 클라우드 방어 컨트롤러 서비스 어카운트를 삭제합니다.
a) GCP 대시보드에 로그인합니다.
b) GCP 프로젝트에서 IAM을 엽니다.
c) 왼쪽 탐색창에서 **Service Accounts(**서비스 어카운트**)**를 클릭합니다.
d) 멀티 클라우드 방어과(와) 연결된 프로젝트를 선택합니다.
e) **View by Principals(**보안 주체별 보기**)** 탭에서 `ciscomcd-controller`를 검색합니다.
f) 행의 확인란이 선택된 다음 **Delete(**삭제**)**를 클릭합니다.

단계 **4** GCP에서 멀티 클라우드 방어 방화벽 서비스 어카운트를 삭제합니다.
a) GCP 대시보드에 로그인합니다.
b) GCP 프로젝트에서 IAM을 엽니다.
c) 왼쪽 탐색창에서 **Service Accounts(**서비스 어카운트**)**를 클릭합니다.
d) 멀티 클라우드 방어과(와) 연결된 프로젝트를 선택합니다.
e) **View by Principals(**보안 주체별 보기**)** 탭에서 `ciscomcd-gateway`를 검색합니다.
f) 행의 확인란이 선택된 다음 **Delete(**삭제**)**를 클릭합니다.

멀티 클라우드 방어에서 **AWS** 어카운트 삭제

다음 절차를 사용하여 멀티 클라우드 방어에서 AWS 어카운트를 완전히 제거합니다.

AWS 어카운트를 삭제한 후 클라우드 서비스 공급자가 사용자의 어카운트와 연결된 S3 버킷 내의 모든 개체를 정리하는 데 최대 24시간이 걸릴 수 있습니다.

단계 **1** CDO에 로그인하고 멀티 클라우드 방어 컨트롤러를 실행합니다.

단계 **2** 상단 메뉴 모음에서 **Manage(**관리**)** > **Gateways(**게이트웨이**)**를 클릭합니다.
단계 **3** 어카운트와 연결된 게이트웨이를 찾고 확인란을 선택한 다음 **Actions(**작업**)** 드롭다운 메뉴를 클릭합니다.
단계 **4** **Disable(**비활성화**)**을 선택합니다. 이 작업을 수행하면 어카운트와 연결된 모든 가상 머신이 자동으로 제거됩니다.
단계 **5** 게이트웨이의 확인란이 여전히 선택되어 있는지 확인하고 **Actions(**작업**)** 드롭다운 메뉴를 다시 클릭합니다.
단계 **6** **Delete(**삭제**)**를 선택합니다. 이 작업은 AWS 어카운트와 연결된 로드 밸런서를 제거합니다.
단계 **7** **Manage(**관리**)** > **Cloud Accounts(**클라우드 어카운트**)** > **Accounts(**어카운트**)**로 이동합니다.
단계 **8** 목록에서 AWS 어카운트를 찾아 선택하여 확인란을 선택합니다.
단계 **9** **Actions(**작업**)** 드롭다운 메뉴를 클릭하고 **Delete(**삭제**)**를 선택합니다.
단계 **10** 어카운트를 삭제할 것인지 확인합니다.

멀티 클라우드 방어에서 **Azure** 계정 삭제

다음 절차를 사용하여 멀티 클라우드 방어에서 Azure 계정의 모든 인스턴스를 제거합니다.

시작하기 전에

Azure 계정에서 멀티 클라우드 방어을(를) 삭제하기 전에 멀티 클라우드 방어 컨트롤러에서 생성한 서브넷 및 VNet을 삭제해야 합니다.

참고 이 절차를 수행하려면 멀티 클라우드 방어 UI 및 GCP 대시보드 모두에서 오케스트레이션 준비를 제거해야 합니다.

단계 **1** CDO에 로그인하고 멀티 클라우드 방어 컨트롤러을(를) 실행합니다.
단계 **2** 키 저장소에 대해 사용자 할당 관리 ID를 생성하지 않은 경우 4단계를 계속합니다. Azure 계정에 대한 키를 생성한 경우 다음을 수행합니다.
  a) **Manage(**관리**)** > **Security Policies(**보안 정책**)** > **Certificates(**인증서**)**로 이동합니다.
  b) 계정과 연결된 인증서를 선택한 다음 **Actions(**작업**)** 드롭다운 메뉴를 엽니다.
  c) **Delete(**삭제**)**를 선택하고 키 저장소에 대한 인증서 삭제를 확인합니다.
단계 **3** 멀티 클라우드 방어 컨트롤러에서 계정과 연결된 게이트웨이 또는 VNet을 삭제합니다.
  a) **Manage(**관리**)** > **Gateways(**게이트웨이**)** > **Gateways(**게이트웨이**)**로 이동하여 이전에 생성한 모든 게이트웨이를 삭제합니다.
  b) 계정과 연결된 게이트웨이를 선택하여 확인란을 선택합니다.
  c) **Actions(**작업**)** 드롭다운 메뉴를 확장하고 **Delete(**삭제**)**를 선택합니다.
  d) 삭제를 확인합니다.
  e) 멀티 클라우드 방어 컨트롤러에서 **Manage(**관리**)** > **Gateways(**게이트웨이**)** > **Service VPCs/VNets(**서비스 **VPC/VNet)**로 이동하여 이전에 만든 VNet을 삭제합니다.
  f) 계정과 연결된 VNet을 선택하면 확인란이 선택됩니다.

g) **Actions(**작업**)** 드롭다운 메뉴를 확장하고 **Delete(**삭제**)**를 선택합니다.
h) 삭제를 확인합니다.
i) 멀티 클라우드 방어 컨트롤러에서 **Manage(**관리**)** > **Cloud Accounts(**클라우드 어카운트**)** > **Accounts(**어카운트**)**로 이동합니다.
j) Azure 계정을 선택하여 확인란을 선택합니다.
k) **Actions(**작업**)** 드롭다운 메뉴를 확장하고 **Delete(**삭제**)**를 선택합니다.
l) 삭제를 확인합니다.

단계 **4** Azure에서 멀티 클라우드 방어 컨트롤러 역할을 삭제합니다.

a) Azure 포털에 로그인합니다.
b) **App Registrations(**앱 등록**)**로 이동합니다.
c) **Owned Appications(**소유 애플리케이션**)** 탭을 선택합니다.
d) **ciscomcd-controller-app** 애플리케이션을 선택합니다.
e) 선택이 끝나면 창 맨 위의 **Delete(**삭제**)**를 클릭합니다.
f) 삭제를 확인합니다.
g) **Subscription(**구독**)**으로 이동하거나 검색하고 **Access Control (IAM)(**액세스 제어**(IAM))**을 클릭합니다.
h) 창의 맨 위의 **Roles(**역할**)** 탭을 선택합니다.
i) **ciscomcd-controller-role-rw**를 검색하고 선택하면 확인란이 선택됩니다.
j) 창 맨 위의 **Remove(**제거**)**를 클릭합니다.

멀티 클라우드 방어에서 **OCI** 계정 삭제

다음 절차를 사용하여 멀티 클라우드 방어에서 OCI 클라우드 환경을 제거합니다.

단계 **1** OCI 콘솔에 로그인합니다.

단계 **2** API 키를 삭제합니다. 자세한 내용은 Oracle Cloud Infrastructure Documentation(오라클 클라우드 인프라 설명서)의 "**Deleting API Signing Keys from a Roaving Edge Infrastructure Device(Roaving Edge** 인프라 장치에서 **API** 서명 키 삭제**)**" 장을 참조하십시오.

단계 **3** 멀티 클라우드 방어 사용자를 삭제합니다. 자세한 내용은 Oracle Cloud Infrastructure Documentation의 "**Deleting a User(**사용자 삭제**)**" 장을 참조하십시오.

참고 즉, OCI 계정에서 사용자를 제거해도 사용자의 감사 데이터가 유효했을 때 삭제되지 않습니다.

단계 **4** 멀티 클라우드 방어 그룹을 삭제합니다. 자세한 내용은 Oracle Cloud Infastructure Documentation의 "**Deleting Groups(**그룹 삭제**)**" 장을 참조하십시오.

단계 **5** 모든 멀티 클라우드 방어 액세스 정책을 삭제합니다. 자세한 내용은 Oracle Cloud Infastructure Documentation의 "액세스 정책 삭제" 장을 참조하십시오.

단계 **6** 멀티 클라우드 방어 컨트롤러에서 OCI 계정을 삭제합니다. .

a) 멀티 클라우드 방어 컨트롤러에서 **Manage(**관리**)** > **Cloud Accounts(**클라우드 어카운트**)** > **Accounts(**어카운트**)**로 이동합니다.

b) OCI 계정을 선택하여 확인란을 선택합니다.
c) **Actions(**작업**)** 드롭다운 메뉴를 확장하고 **Delete(**삭제**)**를 선택합니다.
d) 삭제를 확인합니다.