



OCI

- 멀티 클라우드 방어 컨트롤러 개요에 [Oracle OCI 테넌트 연결](#), on page 1
- OCI에 로그인, on page 2
- 그룹 생성, on page 2
- 정책 생성, on page 2
- 사용자 생성, on page 4
- 사용자를 그룹에 추가, on page 4
- API 키 생성, on page 4
- 구성 파일 미리 보기, on page 5
- 약관 동의, on page 5
- 멀티 클라우드 방어 대시보드에서 [Oracle OCI 테넌트를 멀티 클라우드 방어 컨트롤러에 연결합니다.](#), 5 페이지

멀티 클라우드 방어 컨트롤러 개요에 **Oracle OCI** 테넌트 연결

OCI 테넌트를 멀티 클라우드 방어 컨트롤러에 온보딩하려면 테넌트를 올바르게 설정해야 합니다. 다음은 테넌트를 준비하는 데 필요한 일반적인 단계입니다. 자세한 지침은 [OCI 설정](#)에서 제공됩니다.



Note 멀티 클라우드 방어(은) OCI에 대한 인그레스 및 이그레스/이스트-웨스트 보호를 모두 지원합니다. 재고 목록 및 트래픽 검색은 지원되지 않습니다.

OCI 테넌트를 온보딩하려면 미국 West(San Jose) 지역을 구독해야 합니다. 이 지역이 구독되지 않은 경우 OCI 테넌트가 온보딩할 때 오류가 발생합니다.

OCI에 멀티 클라우드 방어 게이트웨이(를) 구축하려면 각 OCI 구역에서 멀티 클라우드 방어 컴퓨팅 이미지에 대한 이용 약관에 동의해야 합니다. 그렇지 않으면 무단 오류와 함께 구축에 오류가 발생합니다.

단계 개요

테넌트 설정

1. 그룹을 생성합니다.
2. 정책을 생성합니다.
3. 사용자를 생성합니다.
4. 사용자를 그룹에 추가합니다.
5. 사용자에 대한 API 키를 생성합니다.
6. 사용자 및 테넌트 OCID를 기록합니다.
7. 사용 약관을 수락합니다.

다음 작업:

멀티 클라우드 방어 대시보드에서 Oracle OCI 테넌트를 멀티 클라우드 방어 컨트롤러에 연결합니다., [on page 5](#)을(를) 사용하여 OCI 테넌트를 온보딩합니다.

OCI에 로그인

1. OCI 테넌트에 로그인합니다.

그룹 생성

단계 1 Identity & Security(ID 및 보안) > Groups(그룹)로 이동합니다.

단계 2 Create Group(그룹 생성)을 클릭합니다.

단계 3 다음 항목을 지정합니다.

- **Name(이름):** 멀티 클라우드 방어-controller-group
- **Description(설명):** 멀티 클라우드 방어 그룹

단계 4 Create(생성)를 클릭합니다.

정책 생성

단계 1 Identity & Security(ID 및 보안) > Policies(정책)로 이동합니다.

단계 2 **Compartment**(컴파트먼트) *root*(루트)를 선택합니다.

단계 3 **Create Policy**(정책 생성)를 클릭합니다.

단계 4 다음 항목을 지정합니다.

- **Name**(이름): 멀티 클라우드 방어-controller-policy.
- **Description**(설명): 멀티 클라우드 방어 정책.
- **Compartment**(컴파트먼트): ["root" 컴파트먼트여야 함].

단계 5 **Policy Builder**(정책 빌더)에서 **Show manual Editor**(수동 편집기 표시)를 활성화합니다.

단계 6 다음 정책 수정 및 붙여넣기

```
Allow group <group_name> to inspect instance-images in compartment<compartment_name>
Allow group <group_name> to read app-catalog-listing in compartment<compartment_name>
Allow group <group_name> to use volume-family in compartment<compartment_name>
Allow group <group_name> to use virtual-network-family in compartment<compartment_name>
Allow group <group_name> to manage volume-attachments in compartment<compartment_name>
Allow group <group_name> to manage instances in compartment<compartment_name>
Allow group <group_name> to {INSTANCE_IMAGE_READ} in compartment<compartment_name>
Allow group <group_name> to manage load-balancers in compartment<compartment_name>
Allow group <group_name> to inspect instance-images in compartment<compartment_name>
Allow group <group_name> to read app-catalog-listing in compartment<compartment_name>
Allow group <group_name> to use volume-family in compartment<compartment_name>
Allow group <group_name> to use virtual-network-family in compartment<compartment_name>
Allow group <group_name> to manage volume-attachments in compartment<compartment_name>
Allow group <group_name> to manage instances in compartment<compartment_name>
Allow group <group_name> to {INSTANCE_IMAGE_READ} in compartment<compartment_name>
Allow group <group_name> to manage load-balancers in compartment<compartment_name>
Allow group <group_name> to read marketplace-listings in tenancy
Allow group <group_name> to read marketplace-community-listings in tenancy
Allow group <group_name> to inspect compartments in tenancy
Allow group <group_name> to read marketplace-listings in tenancy
Allow group <group_name> to read marketplace-community-listings in tenancy
Allow group <group_name> to inspect compartments in tenancy
```

- **group_name**: 멀티 클라우드 방어-controller-group.
- **compartment_name**: [멀티 클라우드 방어이(가) 구축될 컴파트먼트].

Note Cisco IOS 시스템을 교체할 때 **<compartment_name>**을 정책을 적용할 구역의 이름으로 바꿉니다. 구역이 하위 구역인 경우, 이름 형식은 **compliance:sub-compartment**(예: Prod:App1)입니다.

<compartment_name>이 루트 컴파트먼트(예: multicloud (root))로 지정된 경우 OCI는 정책을 수락하지 않고 오류: *Invalid parameter*(잘못된 매개변수)가 생성됩니다. 특정 컴파트먼트에 대해 정책을 정의해야 하며 해당 컴파트먼트는 루트 컴파트먼트일 수 없습니다.

단계 7 **Create**(생성)를 클릭합니다.

사용자 생성

단계 1 **Identity & Security**(ID 및 보안) > **Users**(사용자)로 이동합니다.

단계 2 **Create User**(사용자 생성)를 클릭합니다.

단계 3 다음 항목을 지정합니다.

- **Name**(이름): 멀티 클라우드 방어-*controller-user*
- **Description**(설명): 멀티 클라우드 방어 *User*(사용자)

단계 4 **Create**(생성)를 클릭합니다.

사용자를 그룹에 추가

단계 1 사용자에 대한 **User Details**(사용자 세부 정보) 보기에서 **Groups**(그룹)를 선택합니다.

단계 2 **Add User to Group**(그룹에 사용자 추가)을 클릭합니다.

단계 3 다음 항목을 지정합니다.

- 사용자: 멀티 클라우드 방어-*controller-user*.

단계 4 **Add**(추가)를 클릭합니다.

API 키 생성

단계 1 사용자에 대한 **User Details**(사용자 세부 정보) 보기에서 **API Keys**(API 키)를 선택합니다.

단계 2 **Add API Key**(API 키 추가)를 클릭합니다.

단계 3 **Download Private Key**(개인 키 다운로드)를 선택하고 나중에 사용할 수 있도록 개인 키를 보관합니다.

단계 4 **Download Public Key**(공개 키 다운로드)를 선택하고 나중에 사용할 수 있도록 공개 키를 보관합니다.

단계 5 **Add**(추가)를 클릭합니다.

구성 파일 미리 보기

1. **Configuration File Preview**(구성 파일 미리 보기)에서 다음을 기록합니다.

- **user:** [user=ocid1.user.oc1...]
- **tenancy:** [tenancy=ocid1.tenancy.oc1...]

약관 동의

-
- 단계 1 **Compute**(계산) > **Instance**(인스턴스)를 선택합니다.
- 단계 2 원하는 **Compartment**(컴파트먼트)를 선택합니다.
- 단계 3 **Create instance**(인스턴스 생성)를 클릭합니다.
- 단계 4 **Image and shape**(이미지 및 모양)에서 **Change image**(이미지 변경)를 선택합니다.
- 단계 5 **Image source**(이미지 소스)에서 **Community Images**(커뮤니티 이미지)를 선택합니다.
- 단계 6 멀티 클라우드 방어 검색을 수행합니다.
- 단계 7 멀티 클라우드 방어에 대한 확인란을 선택합니다.
- 단계 8 *I have reviewed and accept the Publishers terms of use, Oracle Terms of Use, and the Oracle General Privacy Policy*(본인은 게시자 이용 약관, 오라클 이용 약관 및 오라클 일반 개인정보 취급방침을 검토하고 이에 동의합니다.)에 대한 상자를 선택합니다.
- 단계 9 **Select Image**(이미지 선택)를 클릭합니다.
- 단계 10 종료합니다(이미지를 구축하지 않음).
- 멀티 클라우드 방어 게이트웨이(를) 구축하려는 각 컴파트먼트에 대해 단계를 반복합니다.
-

멀티 클라우드 방어 대시보드에서 **Oracle OCI** 테넌트를 멀티 클라우드 방어 컨트롤러에 연결합니다.

시작하기 전에

멀티 클라우드 방어 컨트롤러 개요에 [Oracle OCI 테넌트 연결](#), 1 페이지의 요구 사항을 검토합니다.

-
- 단계 1 CDO 대시보드의 CDO 메뉴 모음에서 멀티 클라우드 방어(를) 클릭합니다.
- 단계 2 멀티 클라우드 방어 컨트롤러 버튼을 클릭합니다.
- 단계 3 Cloud Accounts(클라우드 계정) 창에서 **Add Account**(계정 추가)를 클릭합니다..

멀티 클라우드 방어 대시보드에서 **Oracle OCI** 테넌트를 멀티 클라우드 방어 컨트롤러에 연결합니다.

단계 4 General Information(일반 정보) 페이지의 Account Type(계정 유형) 목록 상자에서 **OCI**를 선택합니다.

단계 5 다음 필드에 내용을 입력합니다.

- **OCI Account Name**(OCI 계정 이름) - 멀티 클라우드 방어 컨트롤러 내에서 이 OCI 테넌트를 식별하는 데 사용됩니다.
- **Tenancy OCID**(테넌시 OCID) - OCI 사용자로부터 가져온 테넌시 Oracle Cloud 식별자입니다.
- **User OCID**(사용자 OCID) - OCI 사용자로부터 가져온 사용자 OCID입니다.
- **Private Key**(개인 키) - OCI 사용자에게 할당된 API 개인 키입니다.

다음에 수행할 작업

트래픽 가시성을 활성화합니다.

번역에 관하여

Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.