

# 使用MCD在Azure中部署FTDv网关

## 目录

---

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[注册应用程序](#)

[创建自定义角色](#)

[分配自定义角色](#)

[将Azure帐户连接到MCD](#)

[创建VNet](#)

[创建Azure MCD FTDv网关](#)

[验证](#)

[相关信息](#)

---

## 简介

本文档介绍如何配置Microsoft Azure必备条件和通过MCD部署防火墙威胁防御虚拟(FTDv)网关。

## 先决条件

- 已获取并注册并与Microsoft Entra ID关联的Azure订阅。在Azure门户中的应用注册列表中确认此项。
- 为Azure订阅创建的自定义角色，授予多云防御(MCD)对特定资源和操作的访问权限，否则这些资源和操作将被阻止。
- 对Azure Event Grid的订阅，以便MCD可以从Azure订阅接收实时更新。
- Azure订阅从MCD控制面板连接到多云防御控制器。
- 在Azure中接受思科应用商店条款，如果这是Azure帐户首次登录MCD。
- （可选）配置用户分配的托管身份（如果需要Key Vault或Blob存储访问）。
- 新的服务VNet。在引入FTDv网关支持之前创建的VNet不能用于FTDv网关部署。
- 云交付防火墙管理中心(cdFMC)的活动订用，用于管理FTDv设备的访问控制策略。
- 通过思科销售商或合作伙伴购买的至少一个FTDv许可证。

## 要求

Cisco 建议您了解以下主题：

- Microsoft Azure门户的导航
- Microsoft Entra ID(Azure AD)应用注册和基于角色的访问控制(RBAC)
- 思科多云防御(MCD)
- 思科安全防火墙威胁防御虚拟(FTDv)

## 使用的组件

本文档不限于特定的软件和硬件版本。

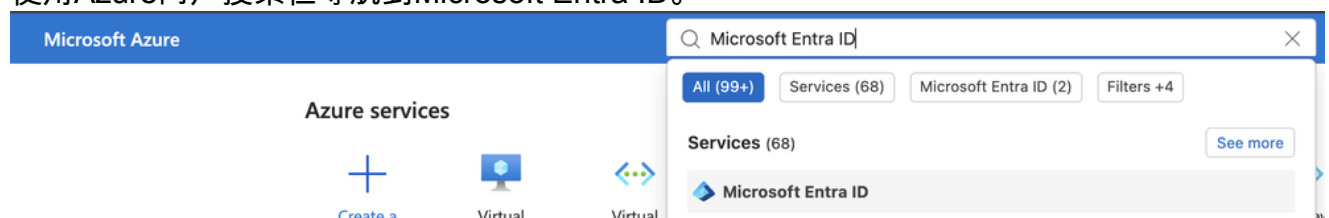
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

## 配置

使用以下过程准备Microsoft Azure、将Azure帐户连接到MCD以及部署FTDv网关。

### 注册应用程序

1. 使用Azure门户搜索栏导航到Microsoft Entra ID。



2. 单击Add，然后选择App registration。

Home



## cxsecurity | Overview

× <<

+ Add ▾



Manage tenants



What's new



Overview



Preview features



Diagnose and solve problems



Manage



Monitoring



Troubleshooting + Support

User



Group

Enterprise application

App registration

[App registration, integrated experience](#)

Properties

Recommendations

### Basic information

Name

cxsecurity

Tenant ID

af42bac0-52aa-429f-92

Primary domain

cxsecurity.onmicrosoft.com

3. 在注册应用表单上，输入以下值：

- 名称：应用的易于识别的名称。
- 支持的帐户类型:选择最适合您的环境的选项。本文档仅使用单租户。

Home > cxsecurity | Overview

## Register an application

### \* Name

The user-facing display name for this application (this can be changed later).

Multicloud Defense Controller



### Supported account types

Choose the account types that can use this application or access this API

Single tenant only - cxsecurity



Single tenant only - cxsecurity

Multiple Entra ID tenants

Any Entra ID Tenant + Personal Microsoft accounts

Personal accounts only

Indicates the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Select a platform



e.g. https://example.com/auth

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

4. 对于重定向URI（可选），请选择适合您的环境的选项。本文档不配置重定向URI。

### Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Select a platform

Public client/native (mobile & desktop)  
Web  
Single-page application (SPA)

e.g. https://example.com/auth

Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

5. 单击Register。

6. 注册应用后，系统将显示概述页面。将应用（客户）ID和目录（租户）ID复制并保存到记事本

Home > cxsecurity | Overview

## Multicloud Defense Controller

Search

Overview

- Quickstart
- Integration assistant
- Diagnose and solve problems
- Manage
- Support + Troubleshooting

Deactivate Delete Endpoints

### Essentials

|                         |                                        |                             |                                                 |
|-------------------------|----------------------------------------|-----------------------------|-------------------------------------------------|
| Display name            | : Multicloud Defense Controller        | Client credentials          | : <a href="#">Add a certificate or secret</a>   |
| Application (client) ID | : e5e0d63d-6f62-4ff9-aaed-2eabd850cf72 | Redirect URIs               | : <a href="#">Add a Redirect URI</a>            |
| Object ID               | : ec1746e4-bd16-4a00-aa7d-3b8e7e52496a | Application ID URI          | : <a href="#">Add an Application ID URI</a>     |
| Directory (tenant) ID   | : af42bac0-52aa-429f-92db-925819967d17 | Managed application in L... | : <a href="#">Multicloud Defense Controller</a> |
| Supported account types | : <a href="#">My organization only</a> | State                       | : <a href="#">Activated</a>                     |

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? [Learn more](#)

Azure Active Directory Authentication Library (ADAL) and Azure AD Graph no longer receive new feature updates. We continue to provide technical support and security updates. Applications should be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

[Get Started](#) [Documentation](#)

7. 在应用页面的左侧导航中，导航到管理>证书和密钥。



# Multicloud Defense Controller



Deactivate



Delete



Endpoints



## Overview



Quickstart



Integration assistant



Diagnose and solve problems



Manage



Branding & properties



Authentication (Preview)



Certificates & secrets



Token configuration



API permissions



Expose an API



App roles



Owners



Roles and administrators



Manifest

> Support + Troubleshooting

## ^ Essentials

Display name : [Multicloud Defense](#)

Application (client) ID : e5e0d63d-6f62-4ff

Object ID : ec1746e4-bd16-4a

Directory (tenant) ID : af42bac0-52aa-429

Supported account types : [My organization o](#)



Welcome to the new and improved App reg



Azure Active Directory Authentication Librai  
Library (MSAL) and Microsoft Graph. [Learn i](#)

Get Started

Documentation

The Mi

8. 单击New client secret.



## Multicloud Defense Controller | Certificates &amp; secrets

[Got feedback?](#)[Overview](#)[Quickstart](#)[Integration assistant](#)[Diagnose and solve problems](#)[Manage](#)[Branding & properties](#)[Authentication \(Preview\)](#)[Certificates & secrets](#)[Token configuration](#)[API permissions](#)[Expose an API](#)[App roles](#)[Owners](#)[Roles and administrators](#)[Manifest](#)[Support + Troubleshooting](#)

Credentials enable confidential applications to identify themselves to the authentication service when receiving to scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credent

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0)

**Client secrets (0)**

Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as

[+ New client secret](#)

New client secret

Expires

Value ⓘ

No client secrets have been created for this application.

9. 在Add a client secret页上，输入以下值，然后单击Add:

- 描述:客户端密钥的正确说明。
- 过期:从下拉菜单中，选择最适合您的环境的选项。



注意：当前密钥到期时，必须创建新密钥。

Copilot swesnitz@cisco.com  
CXSECURITY (CXSECURITY.ONMI...

## Add a client secret

Description

Expires

10. 将Value和Secret ID复制并保存到记事本。



警告：只能在创建时查看加密值。

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) Client secrets (1) Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Client secret values cannot be viewed, except for immediately after creation. Be sure to save the secret when created before leaving the page.

| Description         | Expires   | Value | Secret ID |
|---------------------|-----------|-------|-----------|
| swesnitz-mcd-secret | 3/14/2027 |       |           |



提示：客户端密码列在Value列中。

创建自定义角色

1. 使用Azure门户搜索栏导航到Subscriptions。

Microsoft Azure

Home > cx-tac-rtp-fw-azure (cxsecurity) | Access control (IAM)

Create a custom role

sub

All (99+) Services (19) Resources (30) Filters +4

Services (19)

Subscriptions

2. 单击您的订阅。

Home > Subscriptions

**Subscriptions**

cxsecurity (cxsecurity.onmicrosoft.com)

Compare the different Azure subscription types Forecast my cost for next billing period

+ Add Manage Policies View Requests View eligible subscriptions Export to CSV Analyze

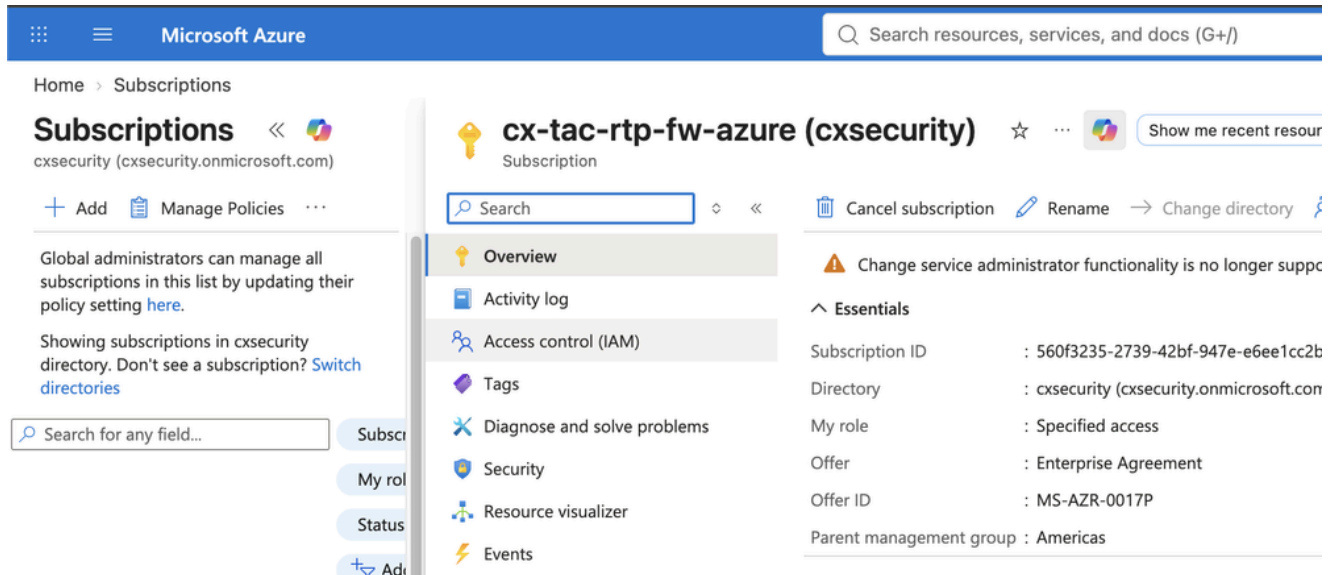
Global administrators can manage all subscriptions in this list by updating their policy setting here.

Showing subscriptions in cxsecurity directory. Don't see a subscription? Switch directories

Search for any field... Subscriptions : Filtered (1 of 1) My role == all Status == all Add filter

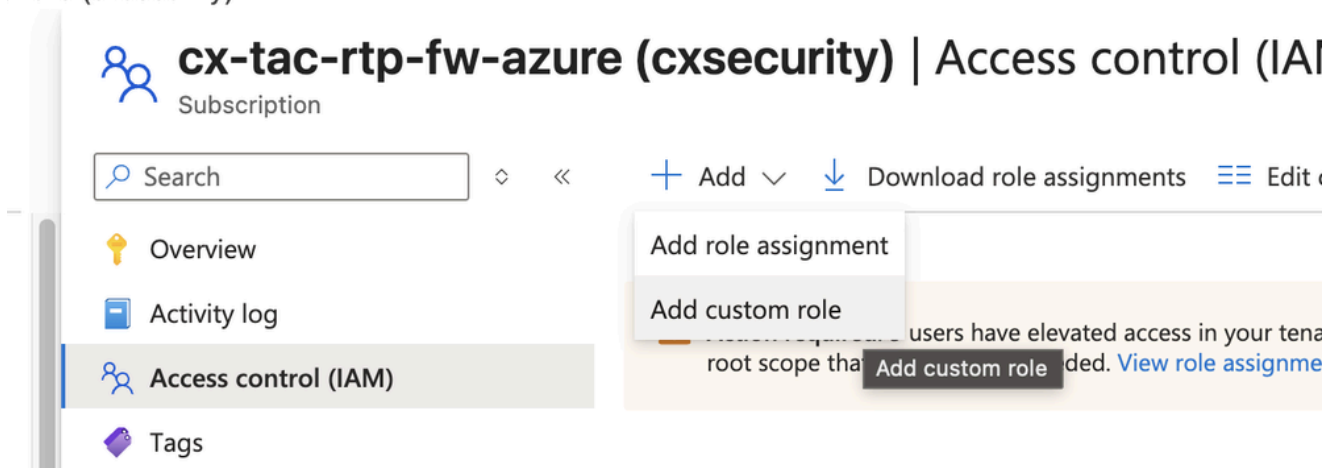
| Subscription name                | Subscription ID                      | My role          | Current cost |
|----------------------------------|--------------------------------------|------------------|--------------|
| cx-tac-rtp-fw-azure (cxsecurity) | 560f3235-2739-42bf-947e-e6ee1cc2b999 | Specified access | \$1,418.01   |

3. 单击Access control(IAM)。



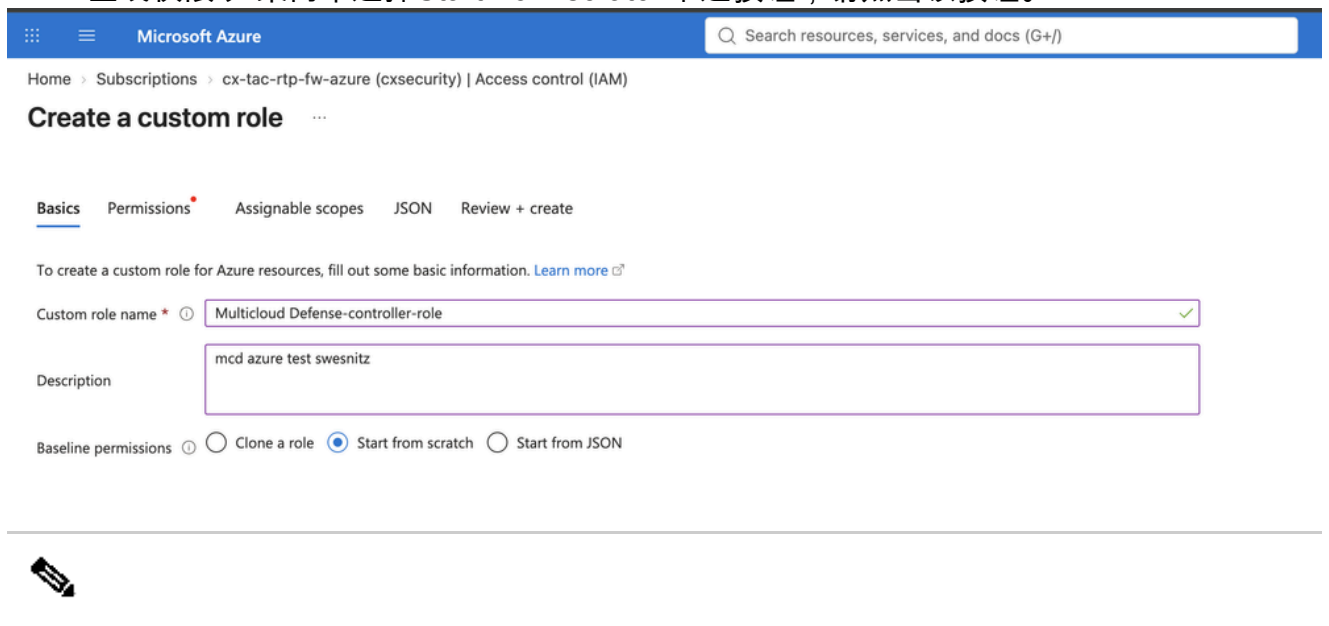
4. 单击Add，然后从下拉菜单中选择Add custom role。

azure (cxsecurity)



5. 输入以下值：

- 自定义角色名称:自定义角色的易识别名称。
- 描述:角色的说明。
- 基线权限:如果尚未选择Start from scratch单选按钮，请点击该按钮。



---

注意：您提供的JSON（而不是“权限”选项卡）为自定义角色分配权限。

---

6. 单击JSON。

7. 单击 Edit。

8. 将此代码块粘贴到方括号内，以便执行以下操作：

```
"Microsoft.ApiManagement/service/*",
"Microsoft.Compute/disks/*",
"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/natGateways/*",
"Microsoft.Network/networkInterfaces/*",
"Microsoft.Network/networkSecurityGroups/*",
"Microsoft.Network/publicIPAddresses/*",
"Microsoft.Network/routeTables/*",
"Microsoft.Network/virtualNetworks/*",
"Microsoft.Network/virtualNetworks/subnets/*",
"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",
"Microsoft.Network/locations/serviceTagDetails/read",
"Microsoft.Network/locations/serviceTags/read",
"Microsoft.CognitiveServices/*/read",
"Microsoft.CognitiveServices/accounts/listkeys/action",
"Microsoft.Network/virtualHubs/*",
"Microsoft.Network/virtualHubs/hubRouteTables/*",
"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/*",
"Microsoft.Authorization/roleAssignments/read",
"Microsoft.Authorization/roleDefinitions/read"
```

## Create a custom role ...

 If you change tabs and have unsaved edits, those changes will be discarded.

Basics Permissions Assignable scopes **JSON** Review + create

Here is your custom role in JSON format. [Learn more](#)

Download



Discard changes

Save

```
1 {
2   "properties": {
3     "roleName": "Multicloud Defense-controller-role",
4     "description": "mcd azure test swesnitz",
5     "assignableScopes": [
6       "/subscriptions/560f3235-2739-42bf-947e-e6ee1cc2b999"
7     ],
8     "permissions": [
9       {
10        "actions": [],
11        "notActions": [],
12        "dataActions": [],
13        "notDataActions": []
14      }
15    ]
16  }
17 }
```



注意：验证JSON代码块的间距和制表符是否正确。

以下是已完成角色定义的示例：

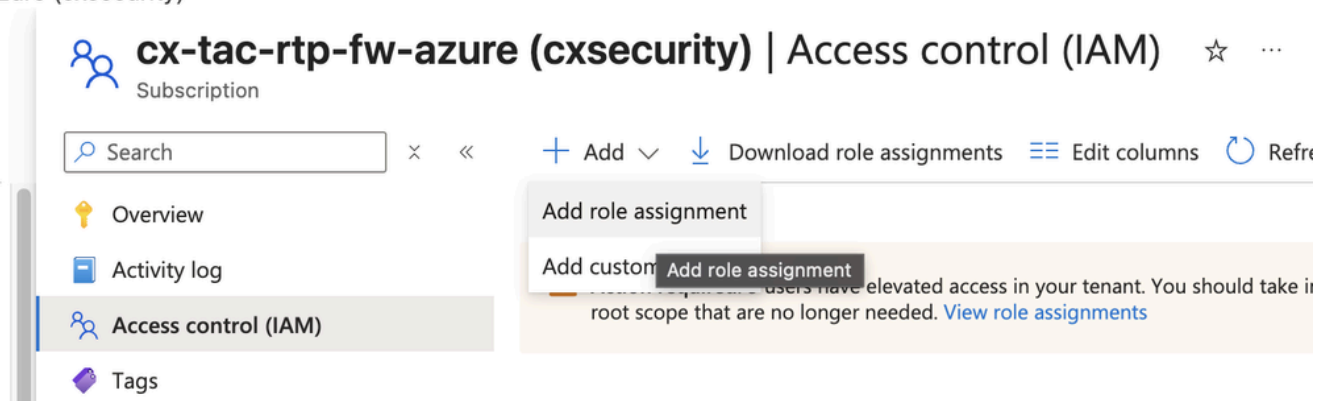
```
{
  "id": "/subscriptions/redacted/providers/Microsoft.Authorization/roleDefinitions/redacted",
  "properties": {
    "roleName": "Multicloud Defense-controller-role",
    "description": "mcd azure test swesnitz",
    "assignableScopes": [
      "/subscriptions/redacted"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.ApiManagement/service/*",
          "Microsoft.Compute/disks/*",
          "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/natGateways/*",
          "Microsoft.Network/networkInterfaces/*",
          "Microsoft.Network/networkSecurityGroups/*",
          "Microsoft.Network/publicIPAddresses/*",
```

```
"Microsoft.Network/routeTables/*",
"Microsoft.Network/virtualNetworks/*",
"Microsoft.Network/virtualNetworks/subnets/*",
"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",
"Microsoft.Network/locations/serviceTagDetails/read",
"Microsoft.Network/locations/serviceTags/read",
"Microsoft.CognitiveServices/*/read",
...
```

## 分配自定义角色

1. 从订用访问控制(IAM)页面，点击添加角色分配。

zure (cxsecurity)



2. 搜索在创建自定义角色部分创建的角色。

Home > Subscriptions > cx-tac-rtp-fw-azure (cxsecurity) | Access control (IAM)

### Add role assignment

**Role** Members Conditions Assignment type Review + assign

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. [Learn more](#)



Copilot can help pick a role

**Job function roles**

Privileged administrator roles

Grant access to Azure resources based on job function, such as the ability to create virtual machines.

Search: mcd

Type: All

Category: All

Name ↑↓

Description ↑↓

Multicloud Defense-controller-role

mcd azure test swesnitz

Showing 1 - 1 of 1 results.

3. 点击Next，将Assign access to保留为User、group或服务principal。

## Add role assignment

Role **Members** Conditions Assignment type Review + assign

**Selected role** Multicloud Defense-controller-role

**Assign access to** ☒ User, group, or service principal  
☐ Managed identity

**Members** [+ Select members](#)

| Name | Object ID | Type |
|------|-----------|------|
|------|-----------|------|

No members selected

**Description**

### 4. 单击选择成员。

## Add role assignment

Role **Members** Conditions Assignment type Review + assign

**Selected role** Multicloud Defense-controller-role

**Assign access to** ☒ User, group, or service principal  
☐ Managed identity

**Members** [+ Select members](#)

| Name | Object ID | Type |
|------|-----------|------|
|------|-----------|------|

No members selected

**Description**

### 5. 添加在创建自定义角色部分创建的角色。

## Select members



 Multi 



Multicloud - Azure - RTP  
Application



Multicloud Defense Controller  
Application

Selected members:



Multicloud Defense Controller  
Application



6. 单击下一步，然后复制订用ID。

## Add role assignment ...

Role   Members   Conditions   Assignment type   Review + assign

 If you changed your role or member selection, your assignment type might have changed. Please review the assignment before submitting.

|                     |                                                     |                                      |      |
|---------------------|-----------------------------------------------------|--------------------------------------|------|
| Role                | Multicloud Defense-controller-role                  |                                      |      |
| Scope               | /subscriptions/560f3235-2739-42bf-947e-e6ee1cc2b999 |                                      |      |
| Members             | Name                                                | Object ID                            | Type |
|                     | Multicloud Defense Controller                       | 309bad3d-eb32-4c16-b2bb-0289b3d491f6 | App  |
| Description         | No description                                      |                                      |      |
| Assignment type     | Active                                              |                                      |      |
| Assignment duration | Permanent                                           |                                      |      |

7. 单击Review + assign。

# Add role assignment ...

Role    Members    Conditions    Assignment type    Review + assign

 If you changed your role or member selection, your assignment type might have changed. Please review the assignment before submitting.

|                     |                                                     |                                      |
|---------------------|-----------------------------------------------------|--------------------------------------|
| Role                | Multicloud Defense-controller-role                  |                                      |
| Scope               | /subscriptions/560f3235-2739-42bf-947e-e6ee1cc2b999 |                                      |
| Members             | Name                                                | Object ID                            |
|                     | Multicloud Defense Controller                       | 309bad3d-eb32-4c16-b2bb-0289b3d491f6 |
| Description         | No description                                      |                                      |
| Assignment type     | Active                                              |                                      |
| Assignment duration | Permanent                                           |                                      |

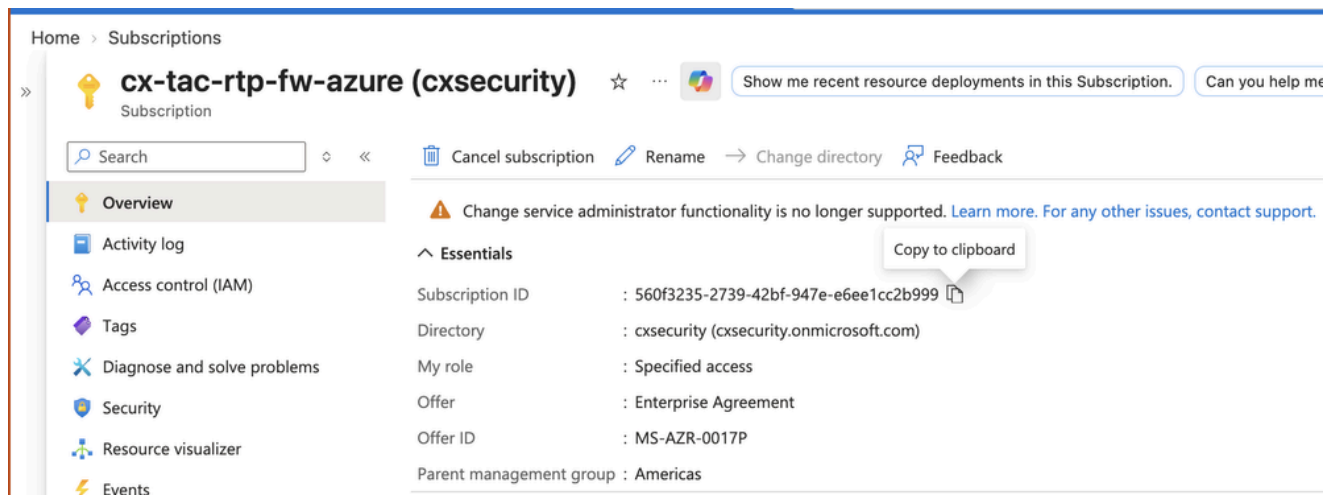
Review + assign

Review + assign

Previous

Next

8. 系统将显示订用的概述页面。从左侧菜单中，导航到Overview并复制订用ID。



这将完成Azure必备条件以将Azure帐户添加到MCD。这些步骤描述通过MCD进行集成和部署。

## 将Azure帐户连接到MCD

1. 导航到SCC > Multicloud Defense。



# Security Cloud Control



Organization  
**cisco-swesnitz**



**Home**

## Products



**Firewall**



**Multicloud Defense**

## Platform services



**Favorites**



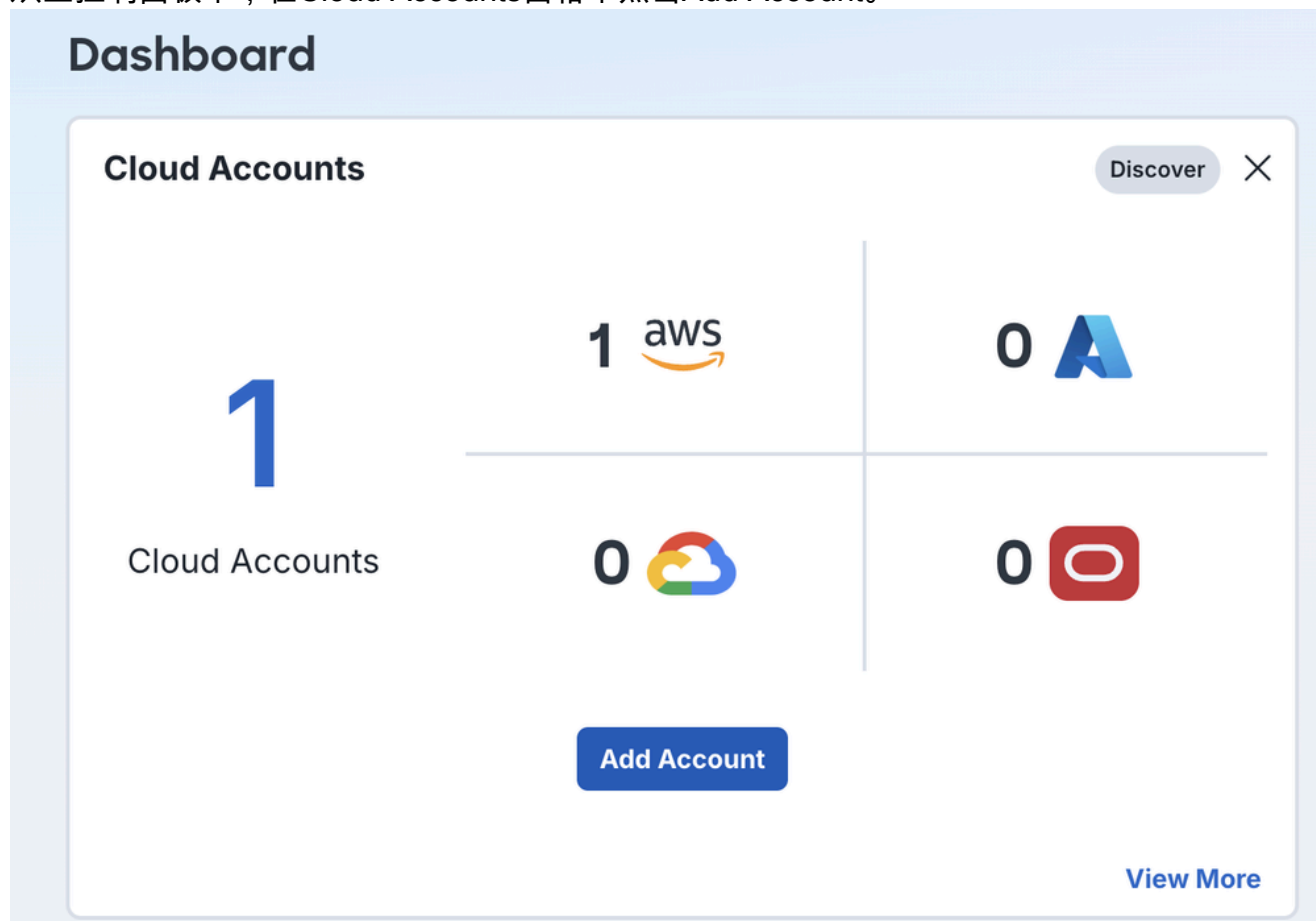
**Security Devices**



**Platform Management**



2. 从主控制面板中，在Cloud Accounts窗格中点击Add Account。



3. 点击Azure图标。

Select Your Cloud Account

Please select Account Type you want to set up









Close

Back

4. 在连接您的Azure帐户页面上，输入以下值：

- Azure帐户名称:从MCD角度而言的Azure帐户的名称。
- 目录ID:您在“注册应用程序”部分中保存的目录ID。
- 订用ID:您在分配自定义角色部分保存的订阅ID。
- 应用程序 ID:您在“注册应用程序”部分中保存的应用程序ID。
- 客户端密码：您在Register an Application部分中保存的值。

## Connect Your AZURE Account

Prepare your cloud account for integration with Cisco Multicloud Defense Controller with following steps:



- 1 Open up [Azure Cloud Shell](#) in bash mode.
- 2 Download and execute Cisco Multicloud Defense onboarding script in the bash shell. This script creates an App Registration for Cisco Multicloud Defense Controller.  
Click [here](#) to see the privilege for the App created.

[Copy](#)

```
bash <( curl -Ls https://raw.githubusercontent.com/valtix-security/cli-azure-setup/master/azure-setup.sh ) -w "https://prod1-webhook.mcd.us.cdo.cisco.com:8093/webhook/ciscoswesnitz-US_htztw/azure"
```

Azure Account Name \* ⓘ

Description ⓘ

Directory ID \* ⓘ

Subscription ID \* ⓘ

Application ID \* ⓘ

Client Secret \* ⓘ

Cancel

Back

Next

5. MCD发现并显示Azure资产。单击 Next。

Discovering Assets

Doing our magic to discover all of your assets. Please give us a minute...

1  
Cloud Accounts

63  
Regions

-  
Network ACL

-  
Network ACL Rules

-  
Application Security Groups (Azure)

-  
AI Inventory

-  
VPCs/VNets

-  
Subnets

-  
Security Groups

-  
Load Balancers

-  
Instances

-  
Network Interfaces

-  
Tags

-  
Route Tables

-  
Applications

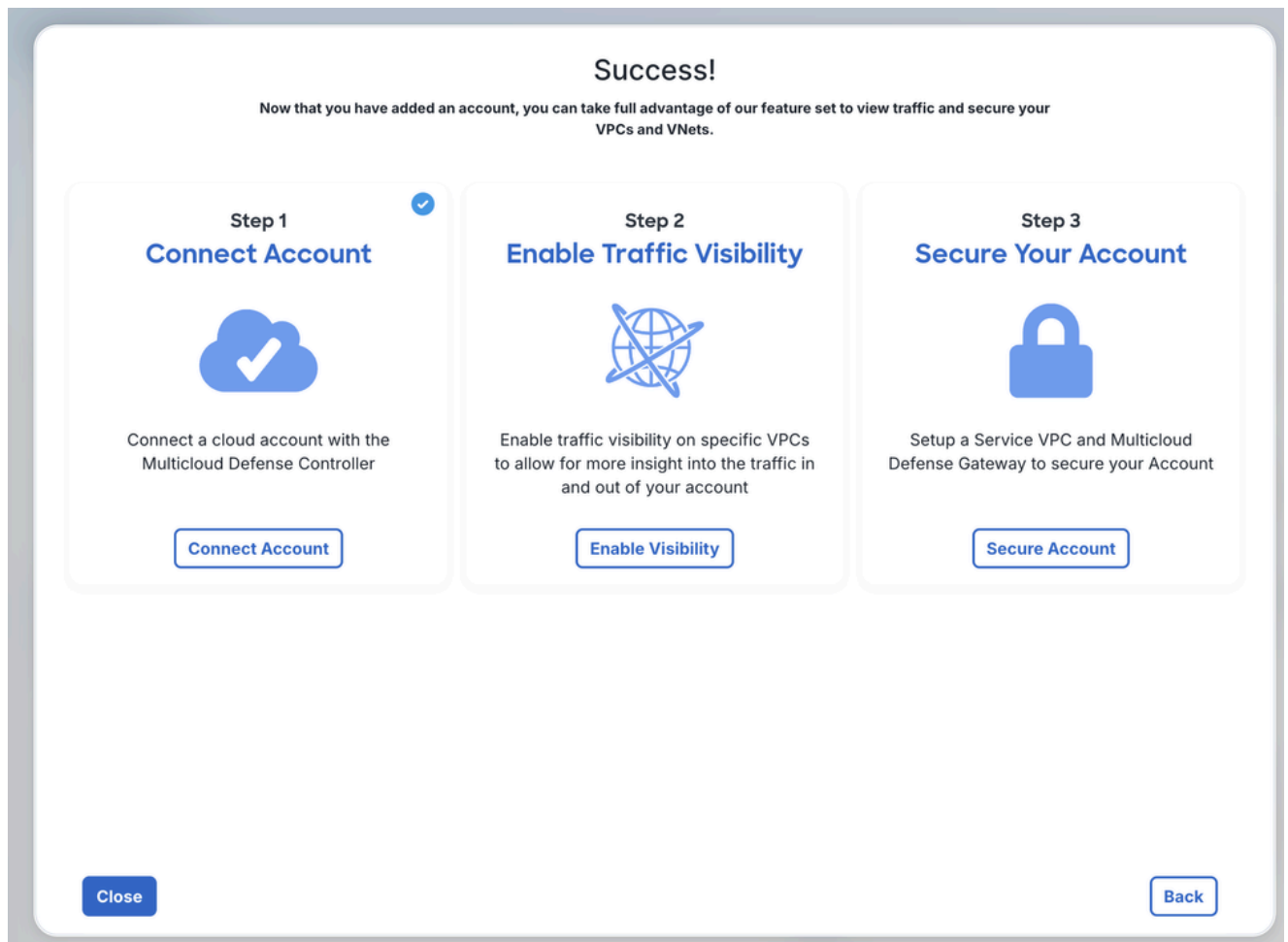
-  
Certificates

Cancel

Back

Next

6. 单击 Close。



7. 您现在可以从基础设施(Infrastructure)> CSP帐户(CSP Accounts)查看已注册帐户。



Organization  
cisco-swesnitz



← Platform menu

Multicloud Defense



Home



Inventory



Investigate



Policies



Infrastructure



Reports



System and Accounts



Platform services



Favorites



Security Devices



Platform Management



Infrastructure



Gateways

Gateways

Service VPCs/Vnets

Account

CSP Accounts



Profiles

Packet Capture

Log Forwarding

Metrics Forwarding

Network

NTP

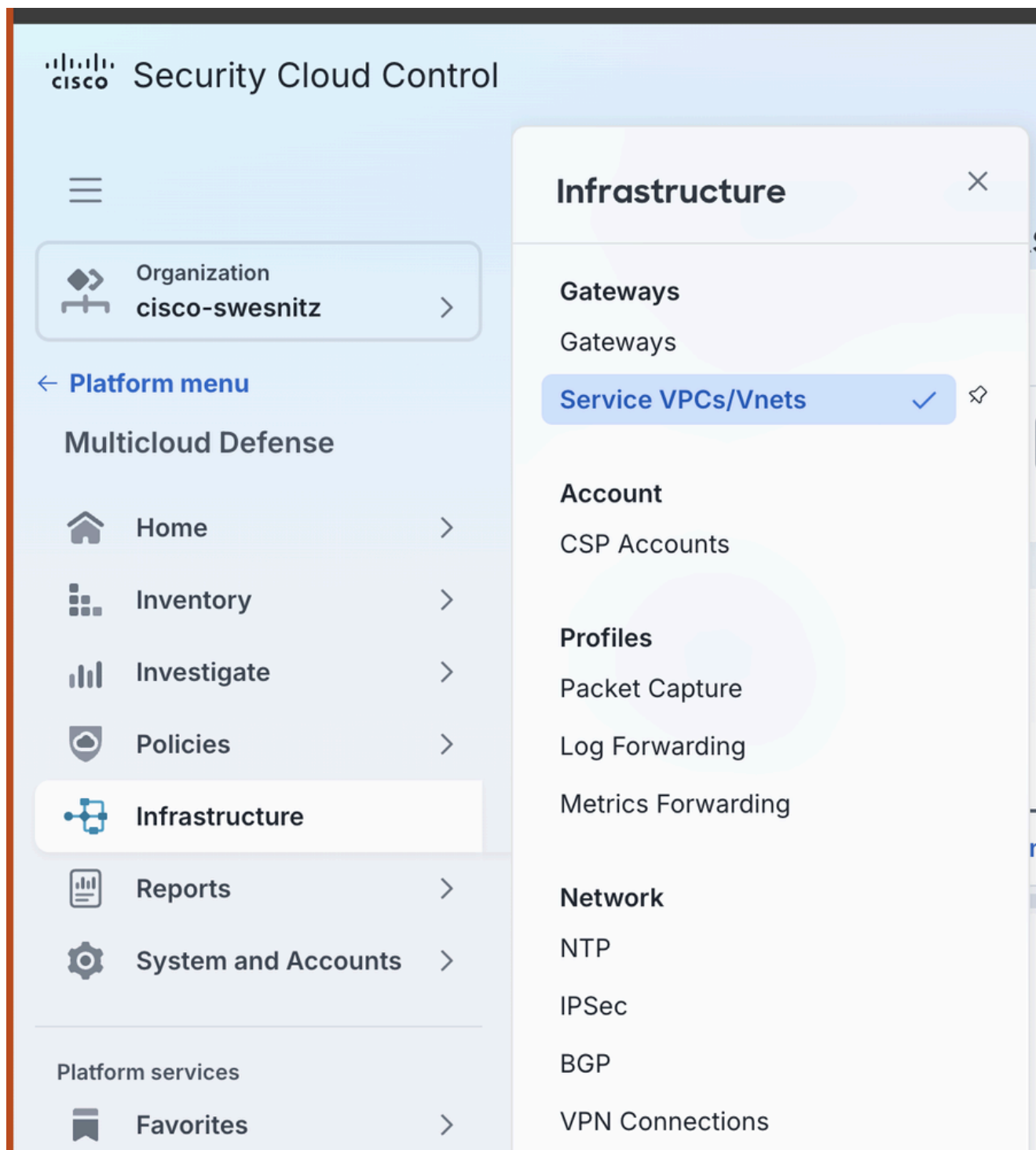
IPSec

BGP

VPN Connections

创建VNet

1. 导航到基础设施>服务VPC/VNets。



2. Click Create.

## Service VPCs/VNets: 1

Quick Filters

Advanced

Name

All Accounts

CSP Type

Create

Actions

| <input type="checkbox"/> | Name                  | ID | Account           |
|--------------------------|-----------------------|----|-------------------|
| <input type="checkbox"/> | mcd_test_vpc-swesnitz | 1  | AWS-CXLABS-RTP-FW |

3. 输入以下值：

- 名称：此过程为FTDv网关创建的VNet的易识别名称。
- CSP帐户:在“将Azure帐户连接到MCD”部分中分配的名称。
- 地区:部署FTDv网关的区域。
- CIDR块:与VNet关联的传输网关的唯一IP块。
- 可用区:至少选择两个可用区域以实现恢复能力。
- 资源组:从下拉菜单中选择+创建资源组。
- 资源组名称:资源组的名称。
- 资源组区域:与为“区域”选择的区域对齐的区域。

Click Save.

## Create Service VPC



Name \* ⓘ

mcd\_azure\_vnet

CSP Account \* ⓘ

cx-tac-rtp-fw-azure

Region \* ⓘ

East US eastus

CIDR Block \* ⓘ

10.4.0.0/16

Availability Zones \* ⓘ

☒ 1

☒ 2

☐ 3

Resource Group \*

+ Create Resource Group

Resource Group Name \*

mcd\_swesnitz

Resource Group Region \*

East US eastus

☐ Use NAT Gateway ⓘ

vWAN Attachment

☐ Enable vWAN Attachment

Cancel

Save

4. 系统将显示成功消息。

**Success**

Service VPC/VNet created successfully.

OK

确认从Azure端创建VNet，导航到网络基础>虚拟网络概述>虚拟网络。

Home > Network foundation

Network foundation | Virtual Network overview

Preview

Search

Overview

Virtual network

Virtual Network overview

Virtual networks

NAT gateways

Public IP addresses

Network interfaces

Network security groups

Application security groups

Virtual network

Network foundation

Service to provision private networks. Build an isolated, secure environment to run virtual machines (VMs) and applications.

Enhanced security through isolated, secure environments.

Flexible, scalable without physical changes.

Secure connectivity across Azure regions

Learn more

Create

View resources

Connectivity

Home > Network foundation

Network foundation | Virtual networks

Preview

Search

Overview

Virtual network

Virtual Network overview

Virtual networks

NAT gateways

Public IP addresses

Network interfaces

Create

Manage view

Refresh

Export to CSV

Open query

Check health of virtual networks

Check the s

mcd

Subscription equals all

Resource Group equals all

Name ↑

mcd\_test\_vnet-swesnitz

VNet创建后会转换为“活动”状态。

Create

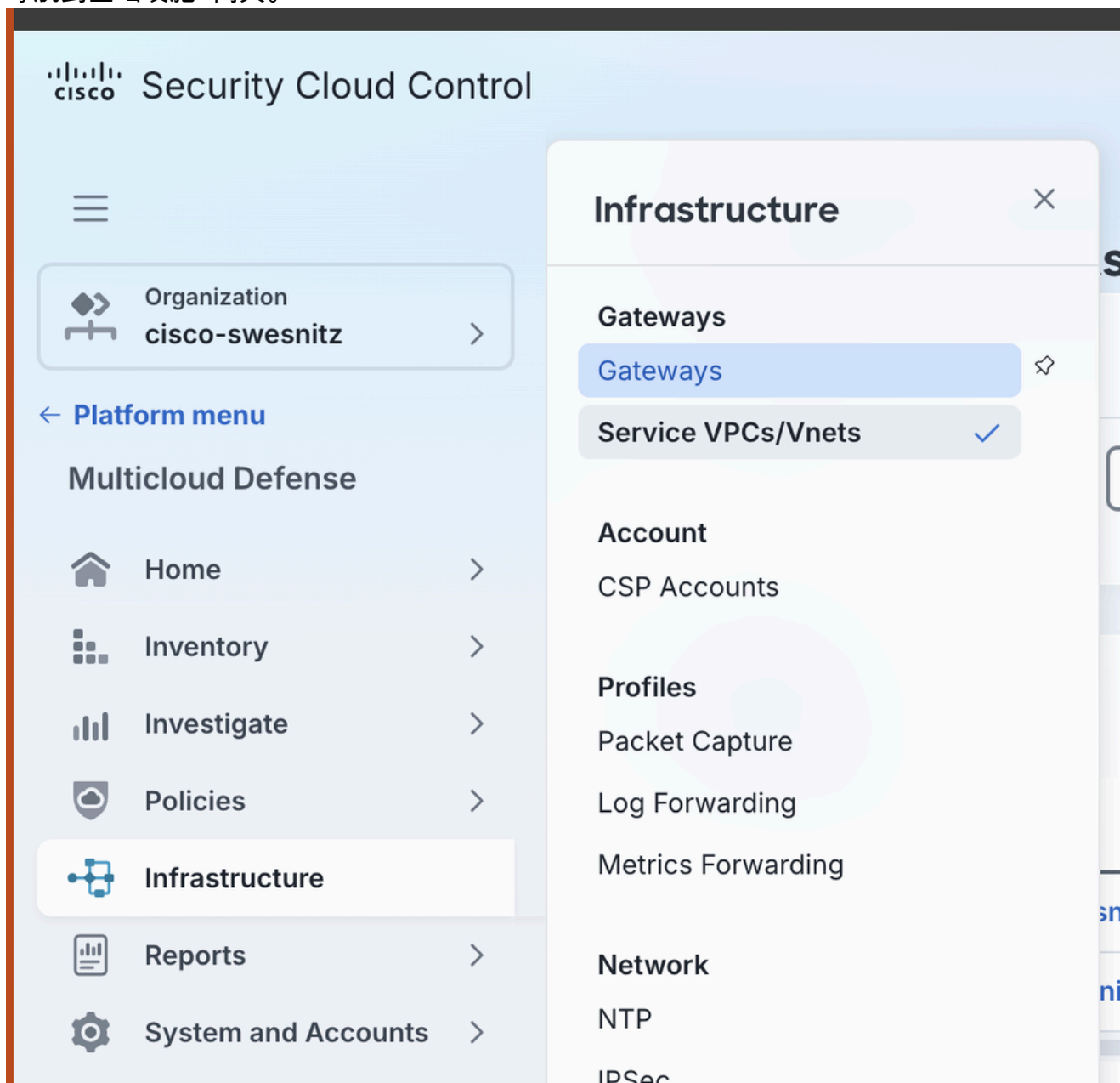
Actions

Refresh

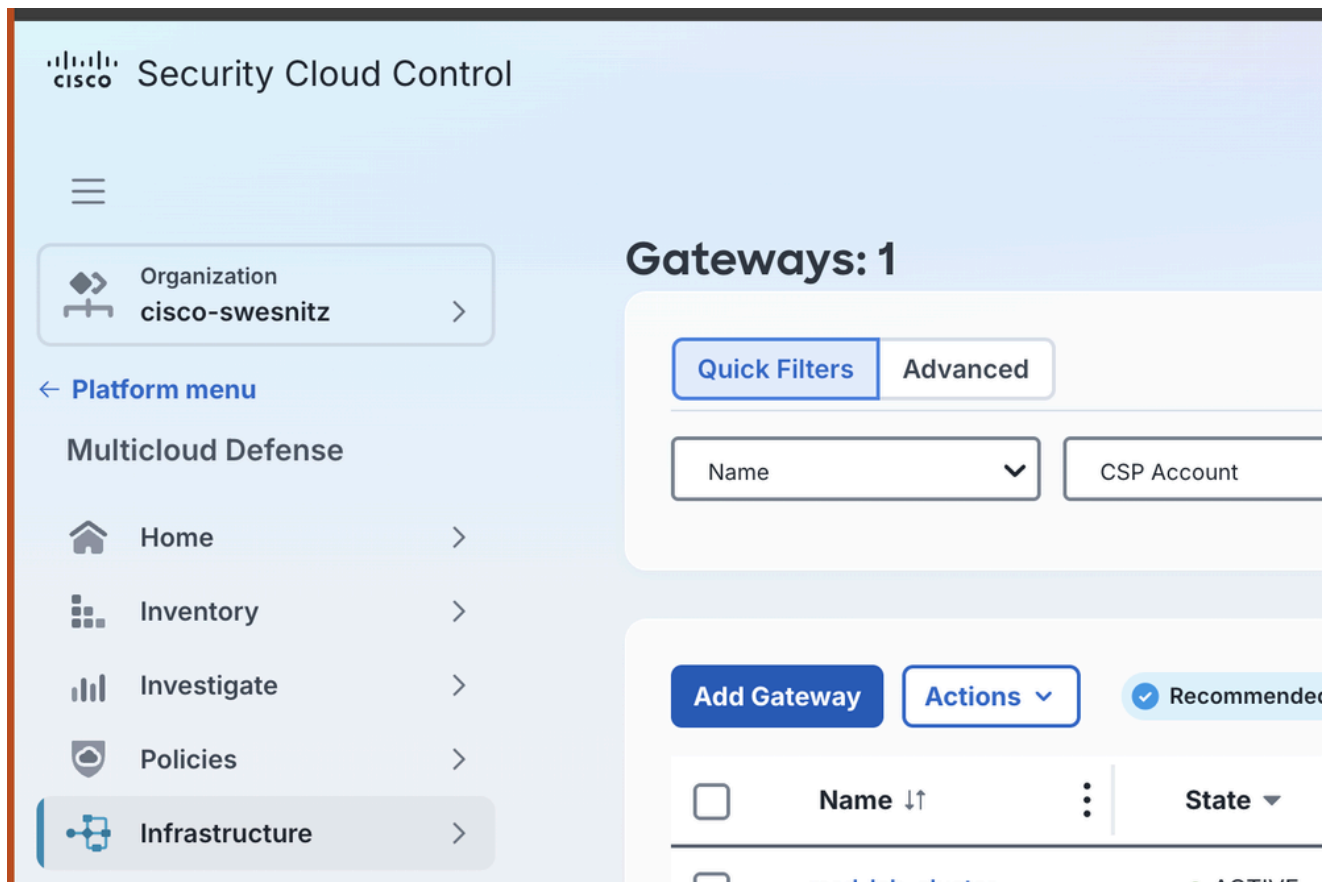
| <input type="checkbox"/> | Name                   | ID | Account             | CSP Type | Region | State  |
|--------------------------|------------------------|----|---------------------|----------|--------|--------|
| <input type="checkbox"/> | mcd_test_vnet-swesnitz | 2  | cx-tac-rtp-fw-azure | AZURE    | eastus | ACTIVE |

创建Azure MCD FTDv网关

1. 导航到基础设施>网关。



2. 单击Add Gateway。



3. 输入以下值：

- 帐户:从下拉菜单中，选择您在将Azure帐户连接到MCD部分中链接的Azure帐户。
- 网关类型:选择FTDv Gateway。
- 名称：FTDv网关的易识别名称。
- 实例类型:适合您环境的实例类型。
- 最小实例:从下拉菜单中选择至少一个实例。
- 最大实例数:环境所需的最大FTDv实例数。允许的最大值为10。
- 运行状况检查端口：默认值为65534。本文档不更改此值。

# Create Gateway

Gateway Information

Gateway Details

Advanced Settings

Review

Properties

Accounts \* ⓘ

cx-tac-rtp-fw-azure

Gateway Type \*

FTDv Gateway

Name \* ⓘ

mcd-azure-lab

Description

Optional

Instance Type \* ⓘ

8 Virtual CPU | AZURE\_D8S\_V5

Minimum Instances \* ⓘ

1

Maximum Instances \* ⓘ

3

HealthCheck Port \* ⓘ

65534

Cancel

Next

注意：HealthCheck Port是Multicloud Defense负载均衡器用于检查实例运行状况的端口号。分配给实例的数据路径安全组必须允许此端口上的流量。

#### 4. 输入以下值：

- 属性:选择Egress或East-West。
- FTDv版本:最适合该环境的软件版本。
- 策略规则集:要应用于此FTDv集群的访问控制策略(ACP)。
- 密码：FTDv实例的密码。
- 许可证模型：所需的许可模式。

- 性能层:适合预期设备吞吐量的层。
- 许可证类型:为此部署购买的许可证类型。
- 地区:部署这些FTDv实例的区域。
- VPC/VNet ID:您在创建VNet部分创建的服务VNet。

## Create Gateway

Security \* ⓘ

East West X

FTDv Version \*

10.0.0 X

Policy Ruleset \* ⓘ

Default Access Control Policy X

FTDv

Admin Password

..... X Show

Password Requirements:

- Must be between 12 and 72 characters long
- Use lowercase and uppercase characters, and numbers
- At least one special character (excluding \ and -)
- No more than 2 repeating or sequential characters

License Model ⓘ

Smart Licensing

Multicloud Defense

Performance Tier \* ⓘ

FTDv20

License Types \* ⓘ

Base X

Location

Region \*

East US eastus X

VPC/VNet ID \* ⓘ

mcd\_test\_vnet-swesnitz | mcd\_test\_vnet-swesnitz X

Key Selection

Cancel

Back

Next

5. 创建公钥对。有关指南，请参阅[在Windows上创建SSH密钥](#)。

```

Your Cloud Shell session will be ephemeral so no files or system changes will
shelby [ ~ ]$ ssh-keygen -m PEM -t rsa -b 2048
Generating public/private rsa key pair.
Enter file in which to save the key (/home/shelby/.ssh/id_rsa):
Created directory '/home/shelby/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/shelby/.ssh/id_rsa
Your public key has been saved in /home/shelby/.ssh/id_rsa.pub
The key fingerprint is:

```

6. 输入SSH Public Key和Resource Groups的值。

Create Gateway

×

Key Selection

SSH Public Key

SSH Key Pair

SSH Public key \*

ssh-rsa  
AAAAAB3NzaC1yc2EAAAADAQABAAQChvSlgyD  
Kk+X6zGCgM3AxV3iPcxZIF7QtWB7WiagDgo+IRKcH  
cPNUofBzsgvIOSuP1mYf6LZQp6Xdhk/9UG6Cq6R0O  
LYvmuK/DY2LcDm/P0CFeww/cKCMtpG6Qgy8IK/M

Resource Groups \*

mcd\_swesnitz | eastus

⊗

↺

User Assigned Identity ID ⓘ

Enter User Assigned Identity ID

Mgmt. Security Group \* ⓘ

mcd\_test\_vnet-swesnitz-mgmt-sg | mcd\_swesnitz

⊗

↺

Datapath Security Group 1 \* ⓘ

mcd\_test\_vnet-swesnitz-datapath-sg | mcd\_sw...

⊗

↺

Datapath Security Group 2 \*

mcd\_test\_vnet-swesnitz-second-datapath-sg | ...

⊗

↺

Disk Encryption \* ⓘ

Azure managed encryption

▼

Instance Details

You can only modify availability zones for gateways deployed in edge mode for GCP, Azure, and OCI environments

Availability Zone ↺

Mgmt. Subnet ↺

Datapath Subnet 1

Datapath Subnet 2

1

⊗

mcd test vnet-...

⊗

mcd test vne...

⊗

mcd test vne...

⊗

Cancel

Back

Next

7. 禁用公共IP，然后单击Next。

## Create Gateway

✓

✓

3

4

Gateway Information

Gateway Details

Advanced Settings

Review

Public IP

Disable Public IP

8. 查看您指定的所有值。

Create Gateway

Gateway Information

Edit

Name

mcd-azure-lab

Gateway Type

FTDv Gateway

Min Instances

1

Max Instances

3

HealthCheckPort

65534

Policy Ruleset ID

Default Access Control Policy

Property

East West

Instance Type

AZURE\_D8S\_V5

FTDv Version

10.0.0

Gateway Details

Edit

License Model

Smart Licensing

Performance Tier

FTDv20

License Type

Base

Region

eastus

VPC/VNet ID

mcd\_test\_vnet-swesnitz | mcd\_test\_vnet-swesnitz

SSH Public Key

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQChvSlgyDr

Resource Groups

mcd\_swesnitz

Mgmt. Security Group

mcd\_test\_vnet-swesnitz-mgmt-sg

Datapath Security Group 1

mcd\_test\_vnet-swesnitz-datapath-sg

Datapath Security Group 2

mcd\_test\_vnet-swesnitz-second-datapath-sg

Cancel

Back

Finish

9. 查看这些值和资源完成加载后，单击Finish。

Create Gateway

Performance Tier

FTDv20

License Type

Base

Region

eastus

VPC/VNet ID

mcd\_test\_vnet-swesnitz | mcd\_test\_vnet-swesnitz

SSH Public Key

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQChvSlgyDr

Resource Groups

mcd\_swesnitz

Mgmt. Security Group

mcd\_test\_vnet-swesnitz-mgmt-sg

Datapath Security Group 1

mcd\_test\_vnet-swesnitz-datapath-sg

Datapath Security Group 2

mcd\_test\_vnet-swesnitz-second-datapath-sg

EBS Encryption

AZURE EBS encryption key

Instance Details

| Availability Zone | Mgmt. Subnet                  | Datapath Subnet 1                 | Datapath Subnet 2                        |
|-------------------|-------------------------------|-----------------------------------|------------------------------------------|
| 1                 | mcd_test_vnet-swesnitz-mgmt-1 | mcd_test_vnet-swesnitz-datapath-1 | mcd_test_vnet-swesnitz-second-datapath-1 |
| 2                 | mcd_test_vnet-swesnitz-mgmt-2 | mcd_test_vnet-swesnitz-datapath-2 | mcd_test_vnet-swesnitz-second-datapath-2 |

Recommendations

loading...

Resources Info

loading...

Advanced Settings

Edit

Disable Public IP

enabled

Cancel

Back

Finish

加载资源后控制面板视图。

Instance Details

| Availability Zone | Mgmt. Subnet          | Datapath Subnet 1         | Datapath Subnet 2                |
|-------------------|-----------------------|---------------------------|----------------------------------|
| 1                 | mcd_azure_vnet-mgmt-1 | mcd_azure_vnet-datapath-1 | mcd_azure_vnet-second-datapath-1 |
| 2                 | mcd_azure_vnet-mgmt-2 | mcd_azure_vnet-datapath-2 | mcd_azure_vnet-second-datapath-2 |

Resources Info

↺

| Resource               | Limit | In Use | Min Usage for Gateway | Max Usage for Gateway | Recommendation |
|------------------------|-------|--------|-----------------------|-----------------------|----------------|
| Private IPs in Subnets | 254   | 0      | 1                     | 3                     |                |
| Elastic IPs            | 1000  | 51     | 1                     | 3                     |                |
| Load Balancers         | 1000  | 8      | 1                     | 1                     |                |
| Instances              | 25000 | 31     | 2                     | 6                     |                |
| Virtual CPUs           | 350   | 0      | 16                    | 48                    |                |

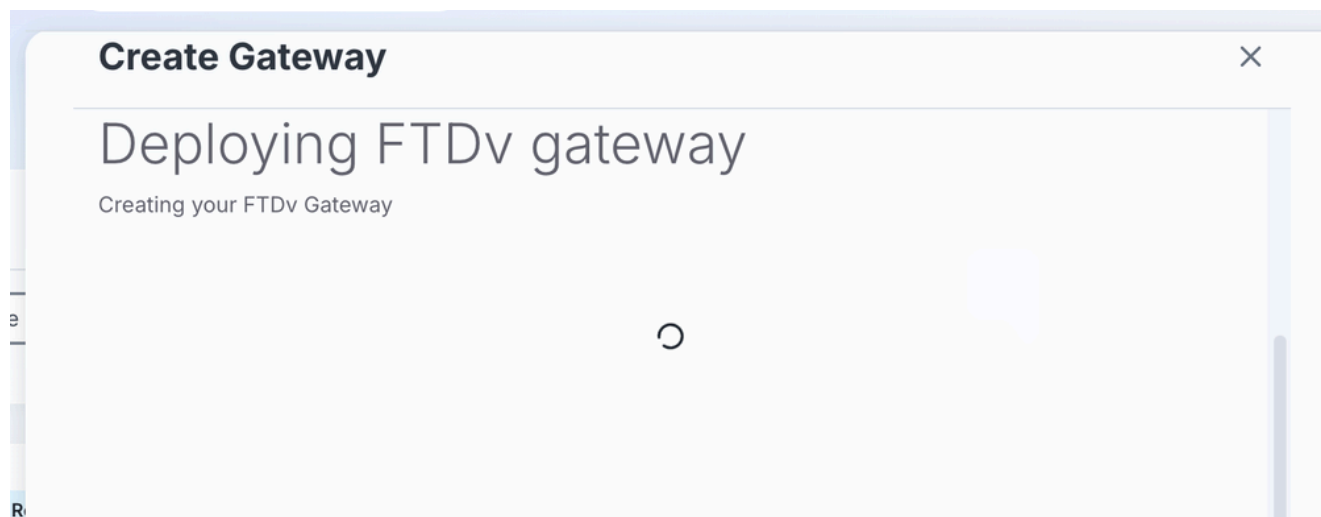
Advanced Settings

Edit

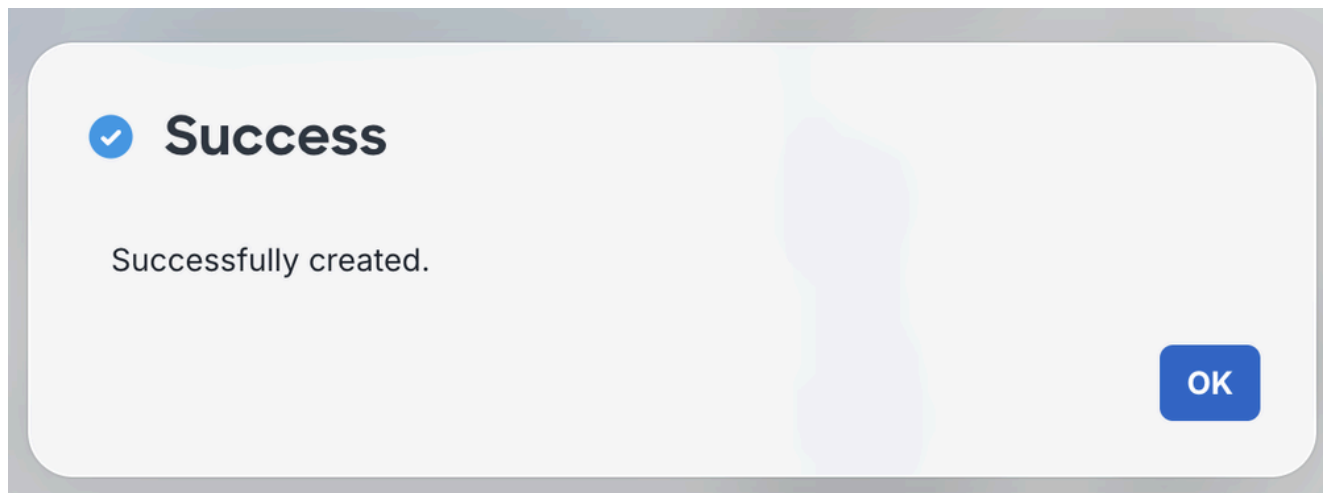
Disable Public IP

enabled

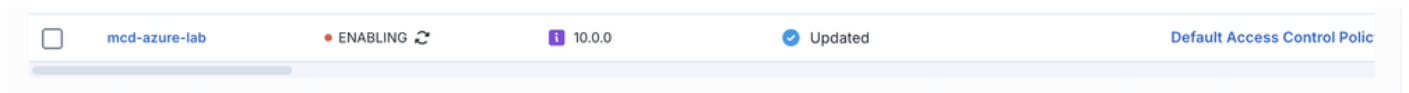
网关部署的控制面板视图。



10. 网关开始创建后，系统将显示成功消息。Click OK.



在MCD控制面板中，状态显示ENABLING。



从Summary和Instances选项卡监控状态。

Details

EditActions

Summary

Cloud Details

Interfaces

Instances

Settings

Troubleshooting

Terraform

Name

mcd-azure-lab

State

ENABLING

Description

Instance Type

AZURE\_D8S\_V5

Type

FTDv Gateway

Min/Max Instances

1 / 3

Mode

HUB

Security Type

East West

Policy Rule Set

Default Access Control Policy

FTDv Version

10.0.0

License Model

Smart Licensing

Performance Tier

FTDv20

License Types

Base

Date Created (Local)

2026-09-15 16:22:37.053

Last Modified (Local)

2026-09-15 16:23:32.156

## 验证

使用本部分可确认配置能否正常运行。

- 在Azure中的计算>虚拟机下，监控FTDv实例。状态从Creating更改为Running。

Home > Compute infrastructure

Compute infrastructure | Virtual machines

Identify VMs with network connectivity issuesAnalyze alerts across virtual machinesGet workload templates for VMs

SearchVirtual machinesGet started

Overview

All resources

Infrastructure

Virtual machines

Virtual Machine Scale Set (VMSS)

Compute Fleet

Arc Machines

Create

Reservations

Manage view

Refresh

Export to CSV

Open query

Assign tags

Start

Restart

Stop

Delete

Services

Group by no

mcd

Subscription equals all

Type equals all

Resource Group equals all

Location equals all

Add filter

| Name                          | Subscription       | Resource Group | Location | Status   | Operating syst... | Size            | Public IP address | Disks | Update status       |
|-------------------------------|--------------------|----------------|----------|----------|-------------------|-----------------|-------------------|-------|---------------------|
| ciscomcd-mcd-azure-lab-nrbcgf | cx-tac-rtg-fw-a... | MCD_SWESNITZ   | East US  | Creating | Linux             | Standard_D8s_v5 | -                 | 1     | Enable periodic ... |
| ciscomcd-mcd-azure-lab-pprom  | cx-tac-rtg-fw-a... | MCD_SWESNITZ   | East US  | Creating | Linux             | Standard_D8s_v5 | -                 | 1     | Enable periodic ... |

- 从MCD控制面板确认网关状态。

SummaryCloud DetailsInterfacesInstancesSettingsTroubleshootingTerraform

| Availability Zone | Number of Instances |
|-------------------|---------------------|
| 1                 | 1                   |
| 2                 | 1                   |

AVAILABILITY ZONES DETAILS

Refresh

Instance: 1

Instance Actions

Instance ID

/subscriptions/560f3235-2739-42bf-947e-e6ee1cc2b999/resourceGroups/mcd\_swesnitz/providers/Microsoft.Compute/virtualMachines/ciscomcd-mcd-azure-lab-psprorne

Instance Name

ciscomcd-mcd-azure-lab-psprorne

Datapath Private IP

Datapath 2 Private IP

Datapath 2 Public IP

-

Mgmt Private IP

-

Mgmt Public IP

-

State

● INIT

Created

2026-09-15 16:26:05.711 (LOCAL)

Last Heartbeat

NA

Image Version

10.0.0

Policy Updates

Please check cdFMC for policy update status.

相关信息

创建服务VPC或VNet

FTDv集成过程

配置网关必备条件

Azure多云防御概述

为Azure中的Linux虚拟机创建并使用SSH公钥 — 私钥对

技术支持和文档 - Cisco Systems

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。