

Implantar um Gateway FTDv no Azure Usando o MCD

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Registrar um aplicativo](#)

[Criar uma Função Personalizada](#)

[Atribuir a função personalizada](#)

[Conectar a Conta do Azure ao MCD](#)

[Criar uma Rede Virtual](#)

[Criar o Gateway FTDv do MCD do Azure](#)

[Verificar](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como configurar os pré-requisitos do Microsoft Azure e implantar um Gateway Virtual de Defesa contra Ameaças (FTDv) de Firewall através do MCD.

Pré-requisitos

- Uma assinatura do Azure que é adquirida e registrada, e associada à ID do Microsoft Entra. Confirme isso na lista de Registros do Aplicativo no portal do Azure.
- Uma função personalizada criada para a assinatura do Azure que concede acesso de MCD (Defesa em Nuvem Múltipla) a recursos e ações específicos que são bloqueados de outra forma.
- Uma assinatura do Azure Event Grid, para que o MCD possa receber atualizações em tempo real da assinatura do Azure.
- A assinatura do Azure conectada ao Controlador de Defesa de Multicloud no painel MCD.
- Os Termos do Cisco Marketplace aceitos no Azure, se esta for a primeira vez que a conta do Azure é integrada ao MCD.
- (Opcional) Uma identidade gerenciada atribuída pelo usuário configurada, se você precisar

de acesso ao Cofre da Chave ou ao Armazenamento de Blob.

- Uma nova Rede Virtual de Serviços. As redes virtuais que foram criadas antes da introdução do suporte de gateway FTDv não podem ser usadas para uma implantação de gateway FTDv.
- Uma assinatura ativa do Cloud-Delivered Firewall Management Center (cdFMC), que gerencia a política de controle de acesso para o dispositivo FTDv.
- Pelo menos uma licença de FTDv adquirida através do seu vendedor ou parceiro da Cisco.

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Navegação no portal do Microsoft Azure
- Registro de aplicativo do Microsoft Entra ID (Azure AD) e controle de acesso baseado em função (RBAC)
- Cisco Multicloud Defense (MCD)
- Cisco Secure Firewall Threat Defense Virtual (FTDv)

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

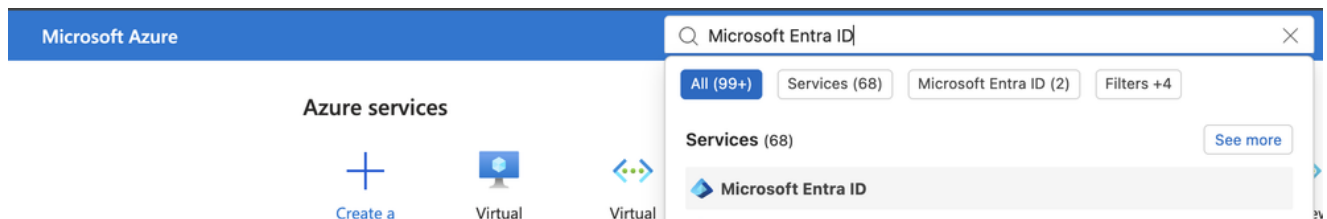
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

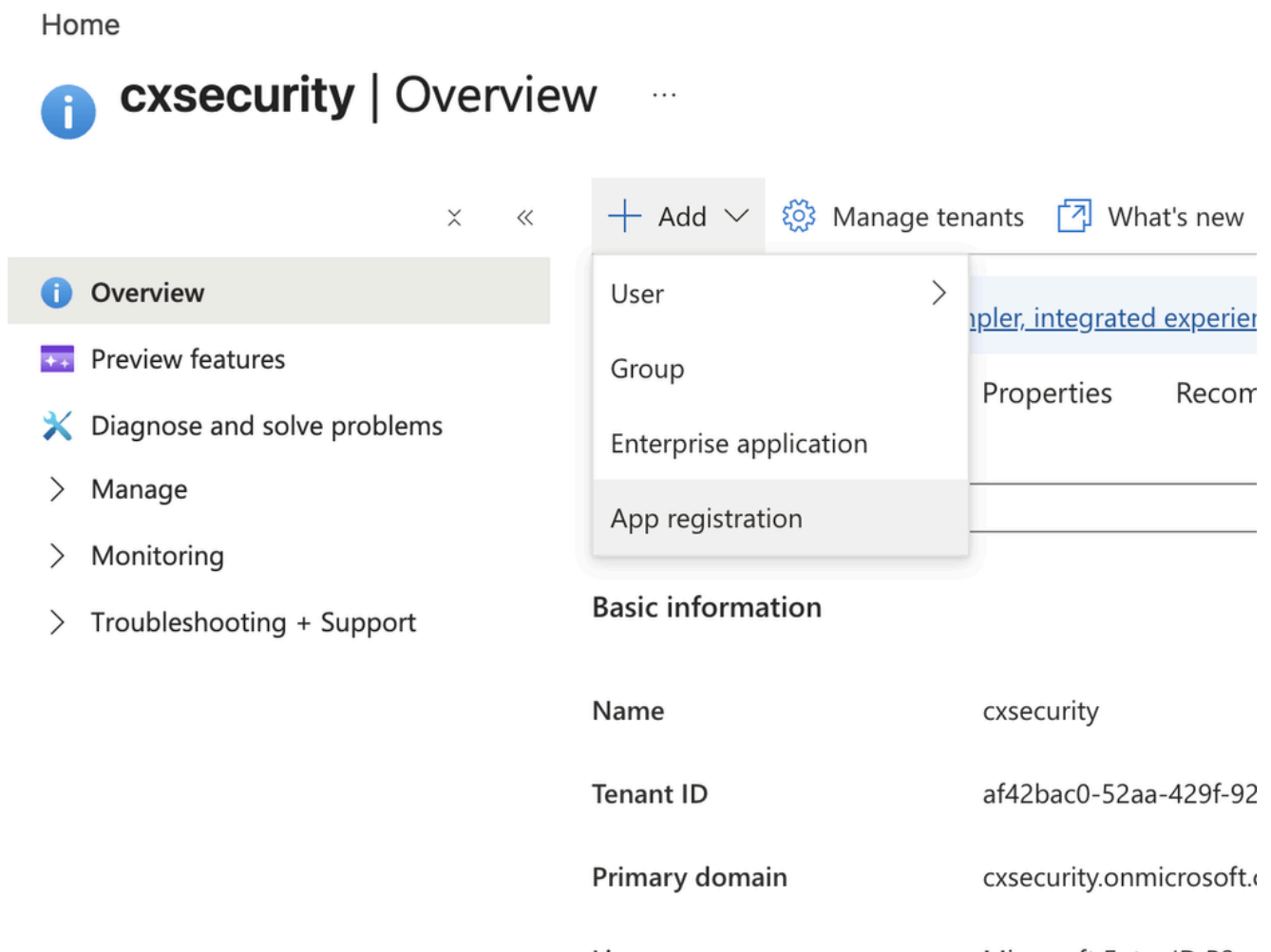
Use estes procedimentos para preparar o Microsoft Azure, conectar sua conta do Azure ao MCD e implantar um Gateway FTDv.

Registrar um aplicativo

1. Navegue até Microsoft Entra ID com a barra de pesquisa do portal do Azure.



2. Clique em Add e selecione App registration.



3. No formulário Registrar um aplicativo, insira estes valores:

- Nome: Um nome facilmente identificável para o aplicativo.
- Tipos de conta com suporte: Selecione a opção mais adequada ao seu ambiente. Este documento usa somente espaço único.

Register an application ...

* Name

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

Supported account types

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

[Help me choose](#)

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

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

4. Para Redirect URI (opcional), escolha a opção apropriada para seu ambiente. Este documento não configura um URI de redirecionamento.

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.

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

5. Clique em Registrar.
6. Após registrar o aplicativo, a página de visão geral é exibida. Copie e salve a ID do aplicativo (cliente) e a ID do diretório (espaço) em um bloco de notas.

Multicloud Defense Controller ...

 Deactivate Delete Endpoints

Overview

[Quickstart](#)[Integration assistant](#)[Diagnose and solve problems](#)[Manage](#)[Support + Troubleshooting](#)

Essentials

Display name : [Multicloud Defense Controller](#)

Application (client) ID : e5e0d63d-6f62-4f99-aaed-2eabd850cf72

Object ID : ec1746e4-bd16-4a00-aa7d-3b8e7e52496a

Directory (tenant) ID : af42bac0-52aa-429f-92db-925819967d17

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

Client credentials : [Add a certificate or secret](#)

Redirect URIs : [Add a Redirect URI](#)

Application ID URI : [Add an Application ID URI](#)

Managed application in L... : [Multicloud Defense Controller](#)

State : [Activated](#)

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. Na navegação à esquerda da página do aplicativo, navegue para Gerenciar > Certificados e segredos.



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. Clique em Novo segredo do cliente.



Multicloud Defense Controller | Certificates & 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. Na página Add a client secret, digite estes valores e clique em Add:

- Descrição: Uma descrição apropriada para o segredo do cliente.
- validade: No menu suspenso, escolha a opção mais adequada ao seu ambiente.



Note: Você deve criar um novo segredo quando o segredo atual expirar.

Add a client secret

Description

Expires

10. Copie e salve o Valor e a ID do segredo em um bloco de notas.



aviso: Você pode exibir o valor secreto somente no momento da criação.

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	[REDACTED]	[REDACTED]



Tip: O segredo do cliente é listado na coluna Valor.

Criar uma Função Personalizada

1. Navegue para Assinaturas com a barra de pesquisa do portal do Azure.

Microsoft Azure

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

Create a custom role ...

Search: sub

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

Services (19) See more

Subscriptions

2. Clique em sua assinatura.

Home > Subscriptions

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

cxsecurity (cxsecurity.onmicrosoft.com)

+ 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. Clique em Controle de acesso (IAM).

Microsoft Azure

Search resources, services, and docs (G+/I)

Home > Subscriptions

Subscriptions

cxsecurity (cxsecurity.onmicrosoft.com)

+ Add Manage Policies ...

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

My role

Status

Administrators

cx-tac-rtp-fw-azure (cxsecurity)

Subscription

Search

Cancel subscription Rename Change directory

Change service administrator functionality is no longer supported

Essentials

Subscription ID	: 560f3235-2739-42bf-947e-e6ee1cc2b
Directory	: cxsecurity (cxsecurity.onmicrosoft.com)
My role	: Specified access
Offer	: Enterprise Agreement
Offer ID	: MS-AZR-0017P
Parent management group	: Americas

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Security

Resource visualizer

Events

4. Clique em Add e selecione Add custom role no menu suspenso.

azure (cxsecurity)

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

Subscription

Search

+ Add Download role assignments Edit

Overview

Activity log

Access control (IAM)

Tags

Add role assignment

Add custom role

users have elevated access in your tenant. View role assignments

5. Insira estes valores:

- Nome da função personalizada: Um nome facilmente identificável para a função personalizada.
- Descrição: Uma descrição para a função.
- Permissões da linha de base: Clique no botão de opção Iniciar do zero, se ainda não estiver selecionado.

Microsoft Azure

Search resources, services, and docs (G+/I)

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

Create a custom role

Basics Permissions Assignable scopes JSON Review + create

To create a custom role for Azure resources, fill out some basic information. [Learn more](#)

Custom role name *

Description

Baseline permissions ☐ Clone a role ☒ Start from scratch ☐ Start from JSON



Note: O JSON fornecido, não a guia Permissões, atribui permissões à função personalizada.

6. Clique em JSON.
7. Clique em Editar.
8. Cole esse bloco de código dentro dos colchetes para as ações:

```
"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 }
```



Note: Verifique o espaçamento e as guias corretos para o bloco de código JSON.

Este é um exemplo da definição de função concluída:

```

{
  "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/*",

```

```

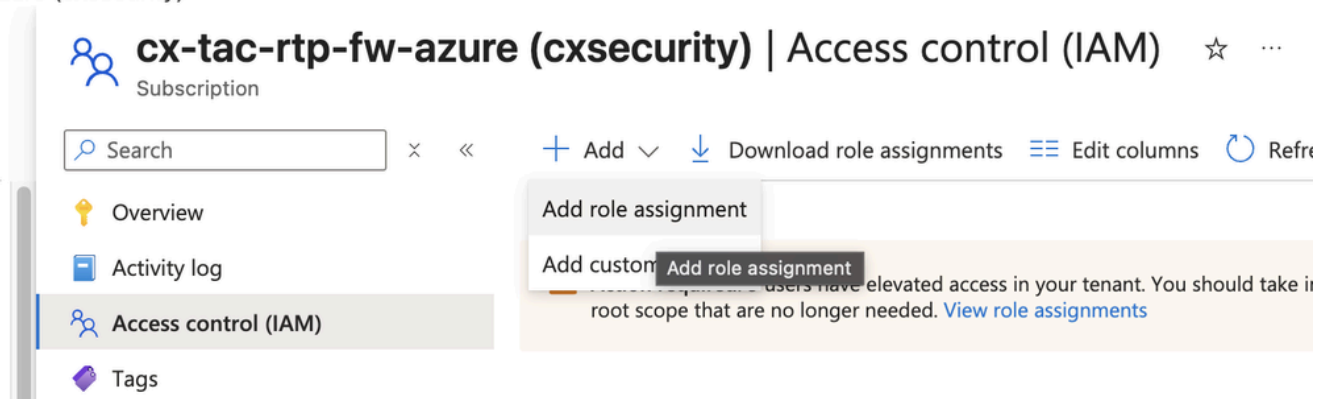
"Microsoft.Network/routeTables/*",
"Microsoft.Network/virtualNetworks/*",
"Microsoft.Network/virtualNetworks/subnets/*",
"Microsoft.Resources/subscriptions/resourcegroups/*",
"Microsoft.Storage/storageAccounts/blobServices/*",
"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Network/networkWatchers/*",
"Microsoft.Network/applicationSecurityGroups/*",
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Insights/Metrics/Read",
"Microsoft.Network/locations/serviceTagDetails/read",
"Microsoft.Network/locations/serviceTags/read",
"Microsoft.CognitiveServices/*/read",
...

```

Atribuir a função personalizada

1. Na página Controle de acesso (IAM) da assinatura, clique em Adicionar atribuição de função.

zure (cxsecurity)



2. Procure a função que você criou na seção Criar uma função personalizada.

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. Clique em Próximo e deixe Atribuir acesso a definido como Usuário, grupo ou serviço principal.

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

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

Optional

4. Clique em Selecionar membros.

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

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

Optional

5. Adicione a função que você criou na seção Criar uma função personalizada.

Select members



 Multi 



Multicloud - Azure - RTP
Application



Multicloud Defense Controller
Application

Selected members:



Multicloud Defense Controller
Application



6. Clique em Avançar e copie a assinatura 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. Clique em Revisar + atribuir.

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	

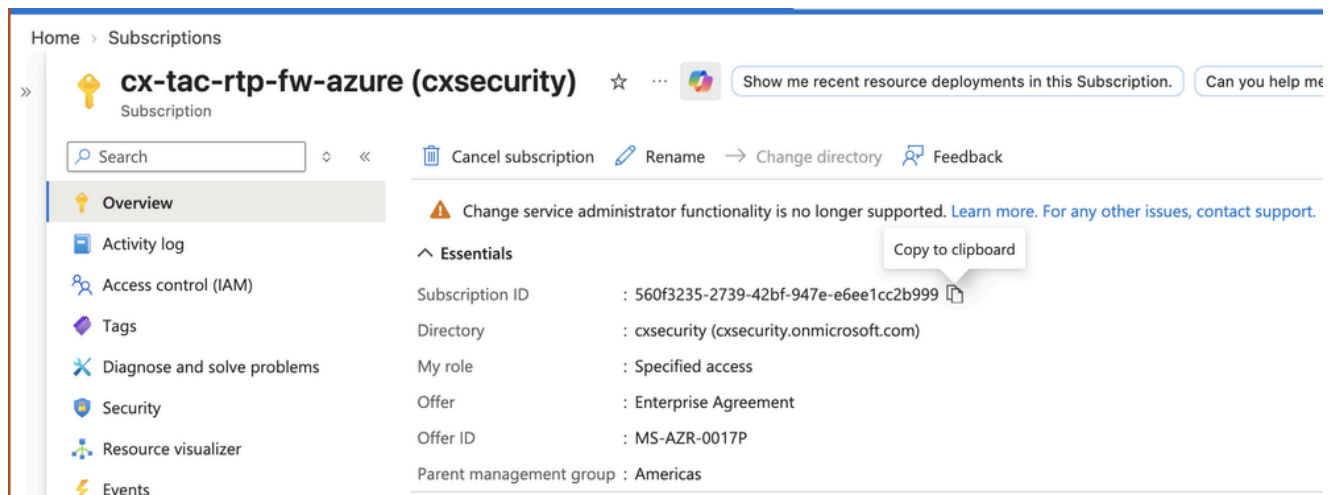
Review + assign

Review + assign

Previous

Next

8. A página de visão geral da assinatura é exibida. No menu à esquerda, navegue para Visão geral e copie a assinatura ID.



Isso conclui os pré-requisitos do Azure para adicionar a Conta do Azure ao MCD. Esses procedimentos descrevem a integração e a implantação por meio do MCD.

Conectar a Conta do Azure ao MCD

1. Navegue até SCC > Defesa em várias nuvens.



Security Cloud Control



Organization
cisco-swesnitz



Home

Products



Firewall



Multicloud Defense

Platform services



Favorites



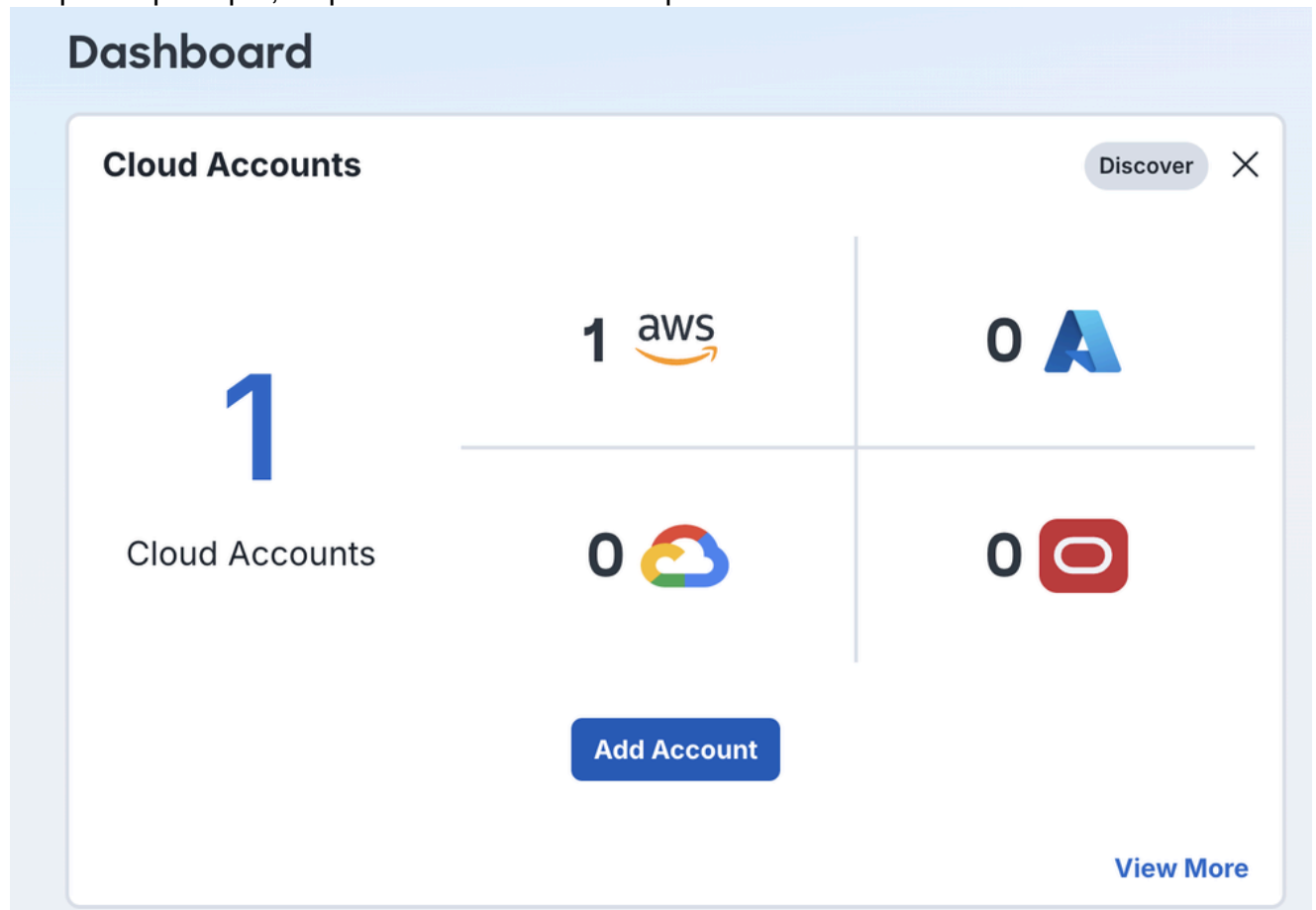
Security Devices



Platform Management



2. No painel principal, clique em Add Account no painel Cloud Accounts.



3. Clique no ícone Azure.

Select Your Cloud Account
Please select Account Type you want to set up









CloseBack

4. Na página Conectar sua Conta do Azure, insira estes valores:

- Nome da Conta do Azure: O nome da conta do Azure da perspectiva do MCD.
- ID do diretório: A ID do diretório que você salvou na seção Registrar um aplicativo.
- ID da assinatura: A ID da assinatura salva na seção Atribuir a função personalizada.
- ID do aplicativo: A ID do aplicativo que você salvou na seção Registrar um aplicativo.
- Segredo do cliente: O valor que você salvou na seção Registrar um aplicativo.

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 * ⓘ

[Show](#)

Cancel

Back

Next

5. O MCD descobre e exibe os ativos do Azure. Clique em 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. Clique em Close.

Success!

Now that you have added an account, you can take full advantage of our feature set to view traffic and secure your VPCs and VNets.

Step 1

Connect Account



Connect a cloud account with the Multicloud Defense Controller

Connect Account

Step 2

Enable Traffic Visibility



Enable traffic visibility on specific VPCs to allow for more insight into the traffic in and out of your account

Enable Visibility

Step 3

Secure Your Account



Setup a Service VPC and Multicloud Defense Gateway to secure your Account

Secure Account

Close

Back

7. Agora você pode visualizar a conta integrada em Infraestrutura > Contas CSP.



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

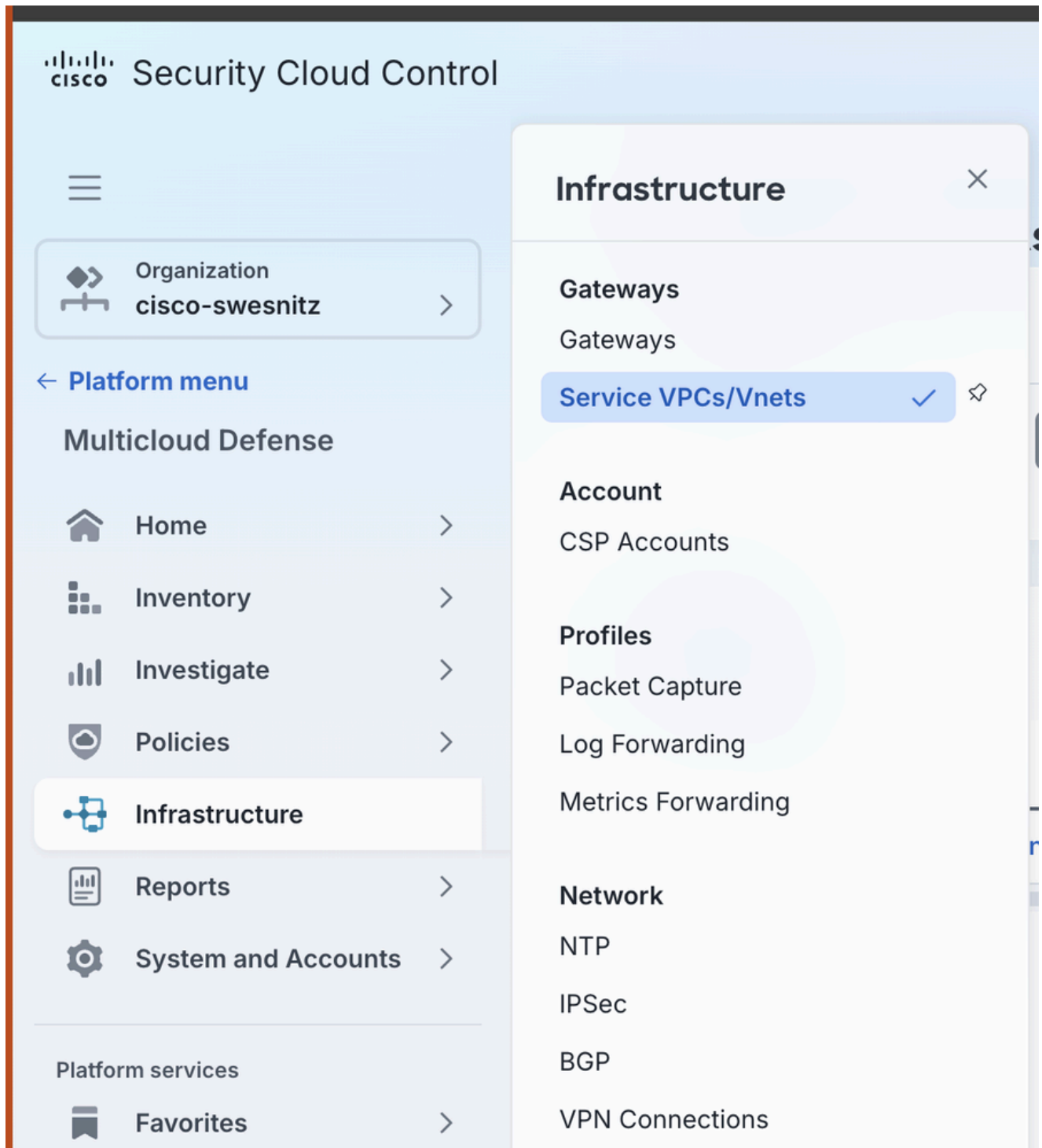
IPSec

BGP

VPN Connections

Criar uma Rede Virtual

1. Navegue até Infrastructure > Service VPCs/VNets.



2. Clique em Criar.

Service VPCs/VNets: 1

Quick Filters

Advanced

Name ▼

All Accounts ▼

CSP Type

Create

Actions ▼

☐	Name ▼	ID ▼	Account ▼
☐	mcd_test_vpc-swesnitz	1	AWS-CXLABS-RTP-FW

3. Insira estes valores:

- Nome: Um nome facilmente identificável para a Rede Virtual que este procedimento cria para o Gateway FTDv.
- Conta do CSP: O nome que você atribuiu na seção Conectar a Conta do Azure ao MCD.
- Região: A região onde o Gateway FTDv é implantado.
- Bloco CIDR: Um bloco IP exclusivo para o gateway de trânsito associado à rede virtual.
- Zonas de disponibilidade: Selecione pelo menos duas zonas de disponibilidade para resiliência.
- Grupo de recursos: Selecione + Criar grupo de recursos no menu suspenso.
- Nome do grupo de recursos: Um nome para o grupo de recursos.
- Região do Grupo de Recursos: A região que se alinha à região selecionada para Região.

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. Uma mensagem de êxito é exibida.



Success

Service VPC/VNet created successfully.

OK

Confirme a criação da Rede Virtual no Azure. Navegue até Network foundation > Virtual networks overview > Virtual Networks.

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

[+ Create](#) [Manage view](#) [Refresh](#) [Export to CSV](#) [Open query](#)

Subscription equals all Resource Group equals all

☐	Name ↑	
☐	mcd_test_vnet-swesnitz	...

A Rede Virtual passa para um estado Ativo depois de criada.

Create

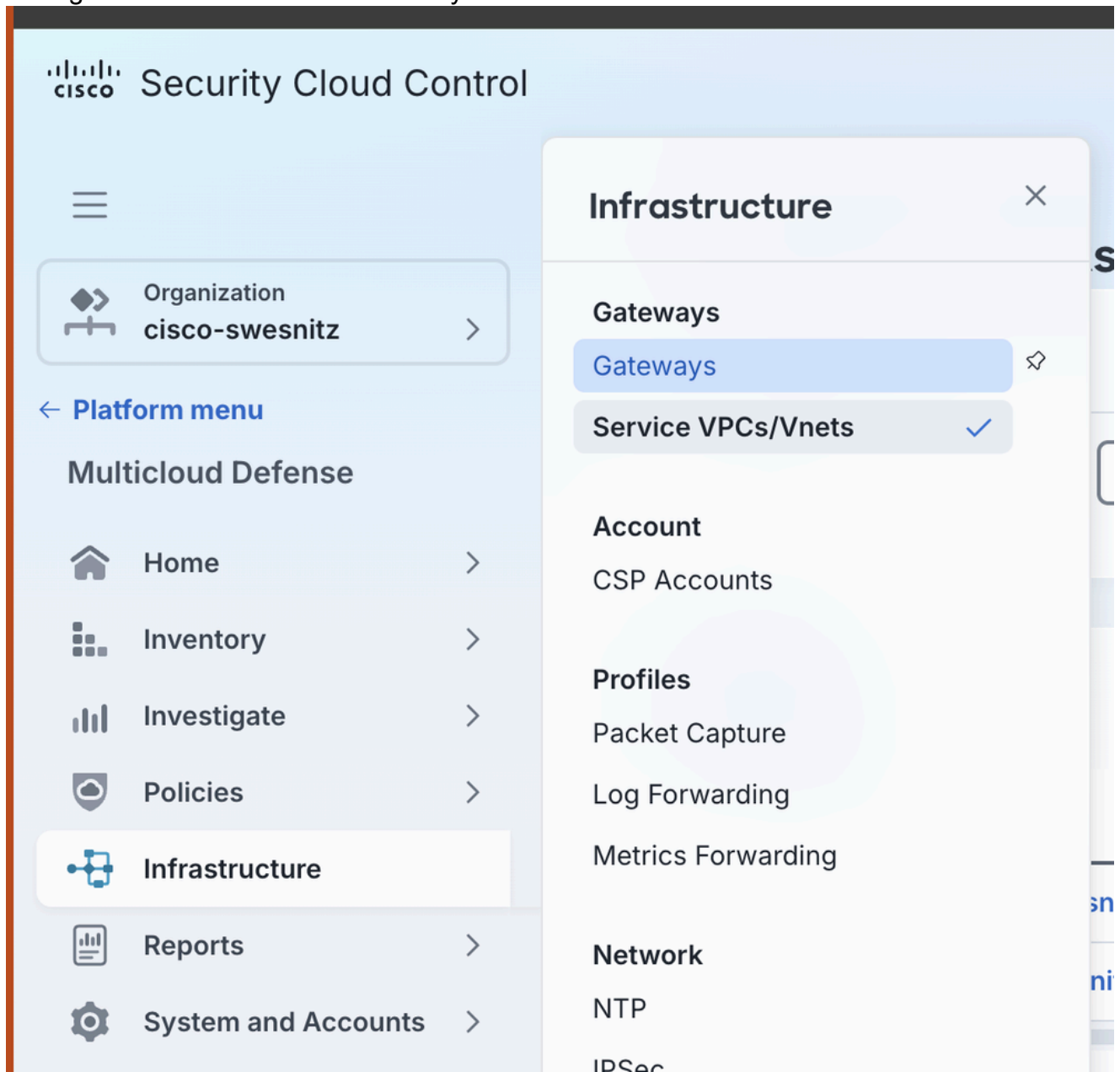
Actions

Refresh

☐	Name	ID	Account	CSP Type	Region	State
☐	mcd_test_vnet-swesnitz	2	cx-tac-rtp-fw-azure	AZURE	eastus	ACTIVE

Criar o Gateway FTDv do MCD do Azure

1. Navegue até Infraestrutura > Gateways.



2. Clique em Add Gateway.

The screenshot displays the Cisco Security Cloud Control web interface. On the left is a navigation sidebar with a 'Platform menu' containing 'Multicloud Defense' and 'Infrastructure' (highlighted). The main content area is titled 'Gateways: 1' and includes a 'Quick Filters' section with 'Name' and 'CSP Account' dropdowns. Below this is a table with columns for 'Name' and 'State'. The first row shows a gateway named 'med lab cluster' in an 'ACTIVE' state. Buttons for 'Add Gateway' and 'Actions' are visible above the table.

3. Insira estes valores:

- Contas: No menu suspenso, seleccione a conta do Azure que você vinculou na seção Conectar a Conta do Azure ao MCD.
- Tipo de gateway: Seleccione FTDv Gateway.
- Nome: Um nome facilmente identificável para o Gateway FTDv.
- Tipo de instância: O tipo de instância apropriado para seu ambiente.
- Mínimo de Instâncias: Seleccione pelo menos uma instância no menu suspenso.
- Máximo de instâncias: O número desejado de instâncias máximas de FTDv para seu ambiente. O máximo permitido é 10.
- Porta HealthCheck: O padrão é 65534. Este documento não altera este valor.

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

Note: A Porta de Verificação de Integridade é o número da porta que o balanceador de carga do Multicloud Defense utiliza para verificar a integridade das instâncias. Os grupos de segurança do caminho de dados atribuídos às instâncias devem permitir o tráfego nesta porta.

4. Insira estes valores:

- Propriedades: Selecione Egress ou East-West.
- Versão do FTDv: A versão de software mais adequada ao ambiente.
- Conjunto de regras de política: A política de controle de acesso (ACP) a ser aplicada a

este cluster de FTDv.

- Senha: Uma senha para as instâncias de FTDv.
- Modelo de licença: O modelo de licenciamento desejado.
- Nível de desempenho: A camada apropriada para a taxa de transferência esperada do dispositivo.
- Tipos de licença: Os tipos de licença adquiridos para esta implantação.
- Região: A região em que essas instâncias de FTDv são implantadas.
- ID do VPC/VNet: A Rede Virtual de Serviços que você criou na seção Criar uma Rede Virtual.

Create Gateway

Security * ⓘ

East West X v

FTDv Version *

10.0.0 X v

Policy Ruleset * ⓘ

Default Access Control Policy X v

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 v

License Types * ⓘ

Base X v

Location

Region *

East US eastus X v

VPC/VNet ID * ⓘ

mcd_test_vnet-swesnitz | mcd_test_vnet-swesnitz X v

Key Selection

Cancel

BackNext

5. Crie um par de chaves públicas. Consulte [Criar um par de chaves SSH no Windows](#) para obter orientação.

```

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. Insira os valores para chave pública SSH e grupos de recursos.

Create Gateway

Key Selection

SSH Public Key

SSH Key Pair

SSH Public key *

ssh-rsa
AAAAAB3NzaC1yc2EAAAADAQABAAQChvSlgyD
Kk+X6zGCgM3AxV3iPcxZIF7QtWB7WiagDgo+IRKcH
cPNUofBzsgvIOSuP1mYf6LZQp6Xdhk/9UG6Cg6R0O
IXvmuK/DY2UcDm/P0CFeww/cKCMToG6Oax8IK/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. Desative o IP público e clique em Avançar.

Create Gateway

✓

✓

3

4

Gateway InformationGateway DetailsAdvanced SettingsReview

Public IP

Disable Public IP

8. Revise todos os valores especificados.

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. Depois de revisar os valores e o carregamento dos recursos, clique em Concluir.

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

Exibição do painel após o carregamento dos recursos.

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



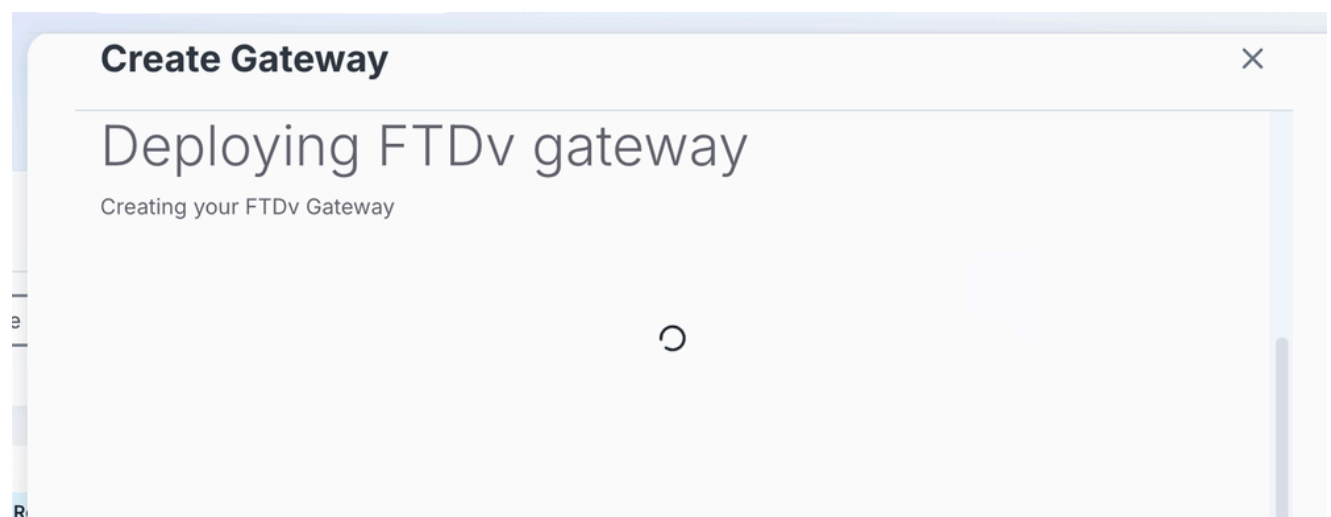
Resource	Limit	In Use	Min Usage for Gateway	Max Usage for Gateway	Recommendation
Private IPs in Subnets	254	0	1	3	
Elastic IPs	1000	51	1	3	
Load Balancers	1000	8	1	1	
Instances	25000	31	2	6	
Virtual CPUs	350	0	16	48	

Advanced Settings

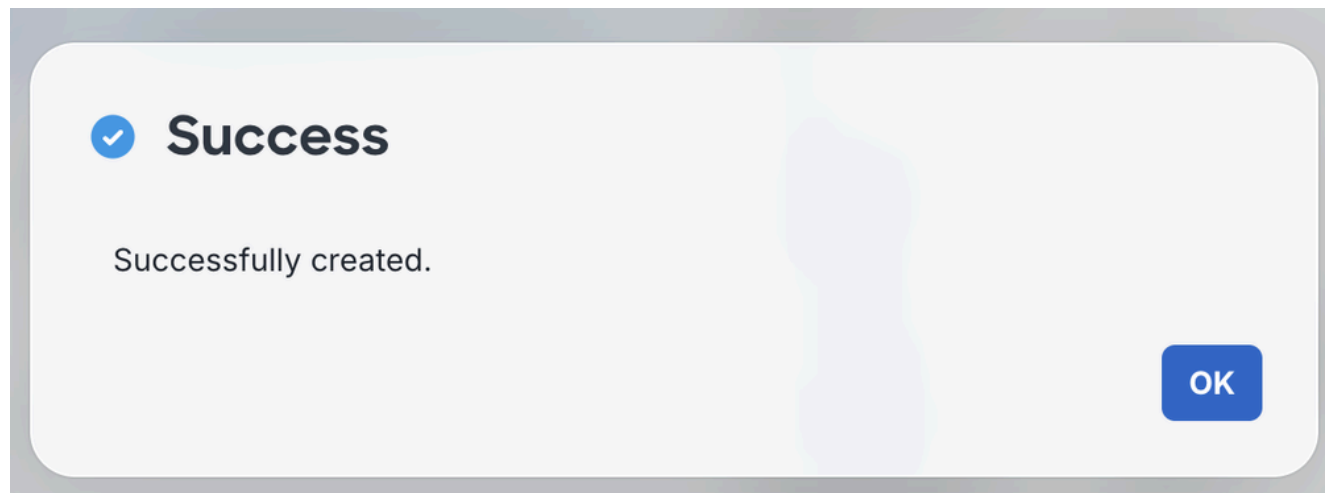
[Edit](#)**Disable Public IP**

enabled

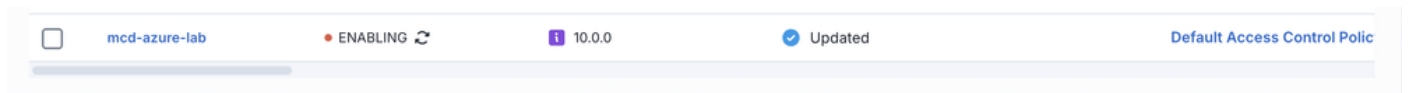
Exibição do painel da implantação do gateway.



10. Após o gateway iniciar a criação, uma mensagem de êxito será exibida. Click OK.



No painel MCD, o status exibe ENABLING.



Monitore o status nas guias Resumo e Instâncias.

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

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

- Em Computação > Máquinas virtuais no Azure, monitore as instâncias de FTDv. O status muda de Creating para Running.

Home > Compute infrastructure

Compute infrastructure | Virtual machines

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

Search

Virtual machines

Get 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-nrbcg	cx-tac-rtg-fw-a...	MCD_SWESNITZ	East US	Creating	Linux	Standard_D8s_v5	-	1	Enable periodic ...
☐	ciscomcd-mcd-azure-lab-psprom	cx-tac-rtg-fw-a...	MCD_SWESNITZ	East US	Creating	Linux	Standard_D8s_v5	-	1	Enable periodic ...

- Confirme o status do gateway no painel MCD.

Summary
Cloud Details
Interfaces
Instances
Settings
Troubleshooting
Terraform

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.

Informações Relacionadas

- [Criar um VPC ou uma Rede Virtual de Serviços](#)
- [Procedimento de integração de FTDv](#)
- [Configurar Pré-requisitos do Gateway](#)
- [Visão geral do Multicloud Defense for Azure](#)
- [Criar e usar um par de chaves públicas e privadas SSH para VMs Linux no Azure](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.