

Déployer une passerelle FTDv dans Azure à l'aide de MCD

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Enregistrer une demande](#)

[Créer un rôle personnalisé](#)

[Attribuer le rôle personnalisé](#)

[Connecter le compte Azure à MCD](#)

[Créer un réseau virtuel](#)

[Créer la passerelle Azure MCD FTDv](#)

[Vérifier](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer les conditions préalables Microsoft Azure et déployer une passerelle virtuelle de défense contre les menaces de pare-feu (FTDv) via MCD.

Conditions préalables

- Abonnement Azure acquis et enregistré, et associé à l'ID Microsoft Entra. Confirmez-le dans la liste des inscriptions d'applications dans le portail Azure.
- Rôle personnalisé créé pour l'abonnement Azure qui accorde à Multicloud Defense (MCD) l'accès aux ressources et actions spécifiques qui seraient autrement bloquées.
- Un abonnement à Azure Event Grid, afin que MCD puisse recevoir des mises à jour en temps réel de l'abonnement Azure.
- L'abonnement Azure est connecté au contrôleur de défense multicloud à partir du tableau de bord MCD.
- Conditions de Cisco Marketplace acceptées dans Azure, si c'est la première fois que le compte Azure est intégré à MCD.
- (Facultatif) Identité gérée attribuée par l'utilisateur configurée, si vous avez besoin d'un

accès au coffre de clés ou au stockage Blob.

- Un nouveau réseau virtuel de service. Les réseaux virtuels créés avant l'introduction de la prise en charge de la passerelle FTDv ne peuvent pas être utilisés pour un déploiement de passerelle FTDv.
- Un abonnement actif au centre de gestion des pare-feu fourni dans le cloud (cdFMC), qui gère la stratégie de contrôle d'accès pour le périphérique FTDv.
- Au moins une licence FTDv achetée auprès de votre vendeur ou partenaire Cisco.

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Navigation sur le portail Microsoft Azure
- Enregistrement d'application Microsoft Entra ID (Azure AD) et contrôle d'accès basé sur les rôles (RBAC)
- Cisco Multicloud Defense (MCD)
- Cisco Secure Firewall Threat Defense Virtual (FTDv)

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

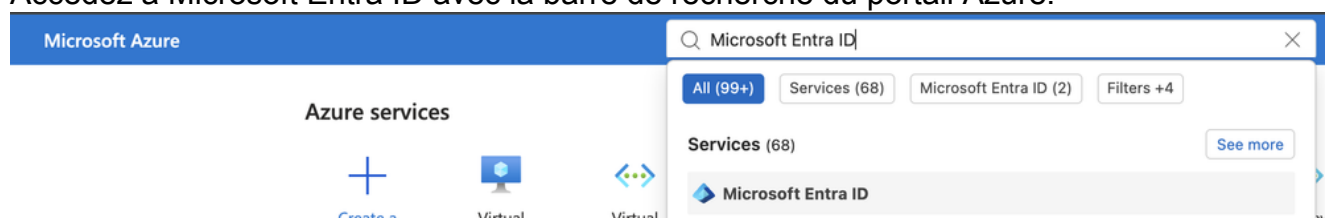
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

Utilisez ces procédures afin de préparer Microsoft Azure, de connecter votre compte Azure à MCD et de déployer une passerelle FTDv.

Enregistrer une demande

1. Accédez à Microsoft Entra ID avec la barre de recherche du portail Azure.



2. Cliquez sur Add, puis sélectionnez App registration.

Home

i

cxsecurity | Overview

...

×

«

+ Add ▾

⚙ Manage tenants

📄 What's new

i Overview

Preview features

Diagnose and solve problems

> Manage

> Monitoring

> Troubleshooting + Support

User >

Group

Enterprise application

App registration

pler, integrated experier

Properties

Recon

Basic information

Name

cxsecurity

Tenant ID

af42bac0-52aa-429f-92

Primary domain

cxsecurity.onmicrosoft.com

3. Dans le formulaire Register an application, saisissez les valeurs suivantes :

- Name : Nom facilement identifiable pour l'application.
- Types de comptes pris en charge : Sélectionnez l'option qui convient le mieux à votre environnement. Ce document utilise le service partagé unique uniquement.

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. Pour URI de redirection (facultatif), choisissez l'option appropriée pour votre environnement. Ce document ne configure pas d'URI de redirection.

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. Cliquez sur Register.
6. Une fois l'application enregistrée, la page de présentation apparaît. Copiez et enregistrez l'ID d'application (client) et l'ID de répertoire (locataire) dans un bloc-notes.

Home > cxsecurity | Overview

Multicloud Defense Controller

Search

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Support + Troubleshooting

Essentials

Display name	: Multicloud Defense Controller	Client credentials	: Add a certificate or secret
Application (client) ID	: e5e0d63d-6f62-4f99-aaed-2eabd850cf72	Redirect URIs	: Add a Redirect URI
Object ID	: ec1746e4-bd16-4a00-aa7d-3b8e7e52496a	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	: af42bac0-52aa-429f-92db-925819967d17	Managed application in L...	: Multicloud Defense Controller
Supported account types	: My organization only	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. Dans le volet de navigation gauche de la page de l'application, accédez à Manage > Certificates & secrets.



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 Controller](#)

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

Object ID : ec1746e4-bd16-4a

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

Supported account types : [My organization or personal Microsoft account](#)



Welcome to the new and improved App registration



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

Get Started

Documentation

The Microsoft

8. Cliquez sur Nouveau secret client.



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. Sur la page Add a client secret, entrez ces valeurs, puis cliquez sur Add :

- Description: Description appropriée du secret client.
- Expire : Dans le menu déroulant, choisissez l'option qui convient le mieux à votre environnement.



Remarque : Vous devez créer un nouveau secret lorsque le secret actuel expire.

Add a client secret

Description

Expires

10. Copiez et enregistrez la valeur et l'ID secret dans un bloc-notes.



Avertissement : Vous ne pouvez afficher la valeur secrète qu'au moment de la création.

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]



Conseil : Le secret client est répertorié dans la colonne Valeur.

Créer un rôle personnalisé

1. Accédez à Abonnements avec la barre de recherche du portail Azure.

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) See more

Subscriptions

2. Cliquez sur votre abonnement.

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. Cliquez sur Contrôle d'accès (IAM).

Microsoft Azure

Search resources, services, and docs (G+)

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...

Subscription

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. Cliquez sur Add, puis sélectionnez Add custom role dans le menu déroulant.

azure (cxsecurity)

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

Subscription

Search

+ Add Download role assignments Edit

Add role assignment

Add custom role

users have elevated access in your tenant root scope that is not inherited. [View role assignments](#)

Overview

Activity log

Access control (IAM)

Tags

5. Entrez les valeurs suivantes :

- Nom du rôle personnalisé : Nom facilement identifiable pour le rôle personnalisé.
- Description: Description du rôle.
- Autorisations de base : Cliquez sur le bouton radio Démarrer à partir de zéro, s'il n'est pas déjà sélectionné.

Microsoft Azure

Search resources, services, and docs (G+)

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 * Multicloud Defense-controller-role

Description mcd azure test swesnitz

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

Remarque : Le fichier JSON que vous fournissez, et non l'onglet Autorisations, attribue des autorisations au rôle personnalisé.

6. Cliquez sur JSON.
7. Cliquez sur Modifier.
8. Collez ce bloc de code entre crochets pour les 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",
"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 }
```



Remarque : Vérifiez l'espacement et les tabulations corrects pour le bloc de code JSON.

Voici un exemple de la définition de rôle terminée :

```

{
  "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/*",

```

```

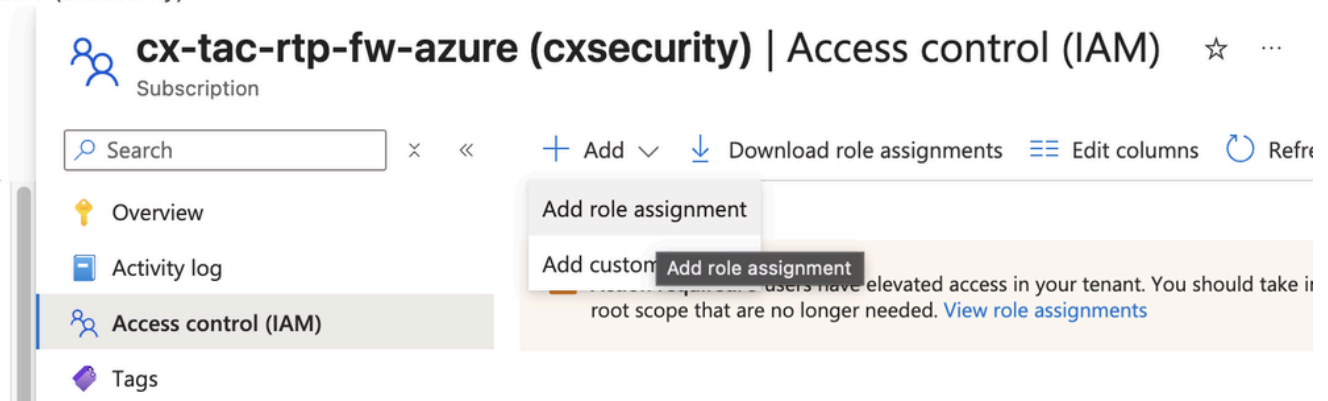
"Microsoft.Network/routeTables/*",
"Microsoft.Network/virtualNetworks/*",
"Microsoft.Network/virtualNetworks/subnets/*",
"Microsoft.Resources/subscriptions/resourcegroups/*",
"Microsoft.Storage/storageAccounts/blobServices/*",
"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Network/networkWatchers/*",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

```

Attribuer le rôle personnalisé

1. Dans la page Contrôle d'accès aux abonnements (IAM), cliquez sur Ajouter une affectation de rôle.

zure (cxsecurity)



2. Recherchez le rôle que vous avez créé dans la section Créer un rôle personnalisé.

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. Cliquez sur Suivant et laissez Affecter l'accès défini sur Utilisateur, groupe ou principal de service.

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. Cliquez sur Sélectionner les membres.

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. Ajoutez le rôle que vous avez créé dans la section Créer un rôle personnalisé.

Select members



 Multi 



Multicloud - Azure - RTP
Application



Multicloud Defense Controller
Application

Selected members:



Multicloud Defense Controller
Application



6. Cliquez sur Next, puis copiez l'ID d'abonnement.

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. Cliquez sur Vérifier + affecter.

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. La page de présentation de l'abonnement s'affiche. Dans le menu de gauche, accédez à Overview et copiez l'ID d'abonnement.

Home > Subscriptions

cx-tac-rtp-fw-azure (cxsecurity) ☆ ... [Show me recent resource deployments in this Subscription.](#) [Can you help me](#)

Subscription

Search

[Cancel subscription](#) [Rename](#) [Change directory](#) [Feedback](#)

Overview

- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Security
- Resource visualizer
- Events

Essentials

Change service administrator functionality is no longer supported. [Learn more.](#) For any other issues, contact support.

Subscription ID : 560f3235-2739-42bf-947e-e6ee1cc2b999 [Copy to clipboard](#)

Directory : cxsecurity (cxsecurity.onmicrosoft.com)

My role : Specified access

Offer : Enterprise Agreement

Offer ID : MS-AZR-0017P

Parent management group : Americas

Les conditions préalables Azure permettant d'ajouter le compte Azure au MCD sont remplies. Ces procédures décrivent l'intégration et le déploiement via MCD.

Connecter le compte Azure à MCD

1. Accédez à SCC > Multicloud Defense.



Security Cloud Control



Organization
cisco-swesnitz



Home

Products



Firewall



Multicloud Defense

Platform services



Favorites



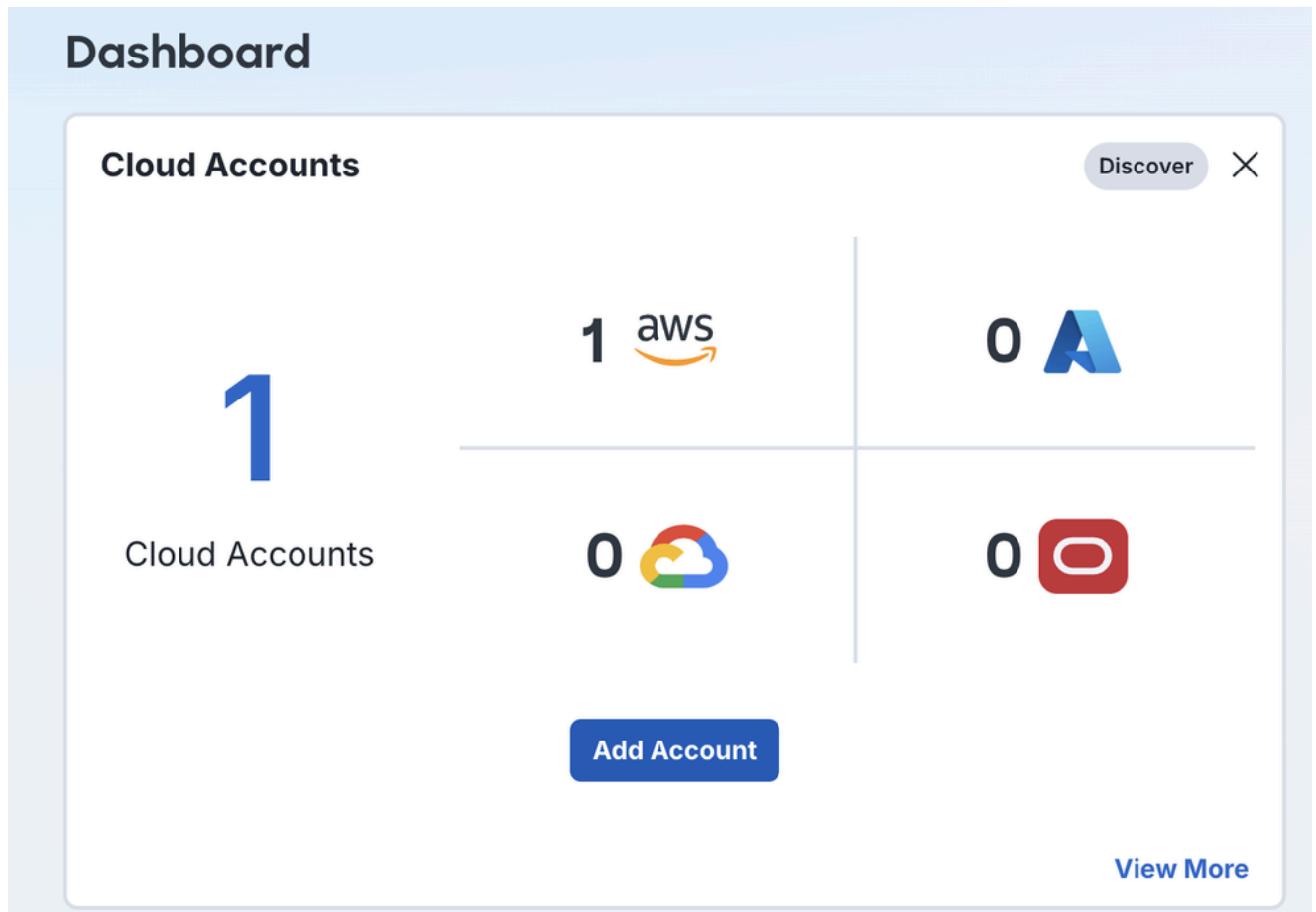
Security Devices



Platform Management



2. Dans le tableau de bord principal, cliquez sur Ajouter un compte dans le volet Cloud Accounts.



3. Cliquez sur l'icône Azure.

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









[Close](#)[Back](#)

4. Sur la page Connectez votre compte Azure, entrez les valeurs suivantes :
- Nom du compte Azure : Nom du compte Azure du point de vue de MCD.
 - ID de répertoire : ID de répertoire que vous avez enregistré dans la section Register an Application.
 - ID d'abonnement : ID d'abonnement que vous avez enregistré dans la section Affecter le rôle personnalisé.
 - ID d'application : ID d'application que vous avez enregistré dans la section Register an Application.
 - Secret client : Valeur que vous avez enregistrée dans la section Register an Application.

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. MCD détecte et affiche les ressources Azure. Cliquez sur Suivant.

Discovering Assets

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

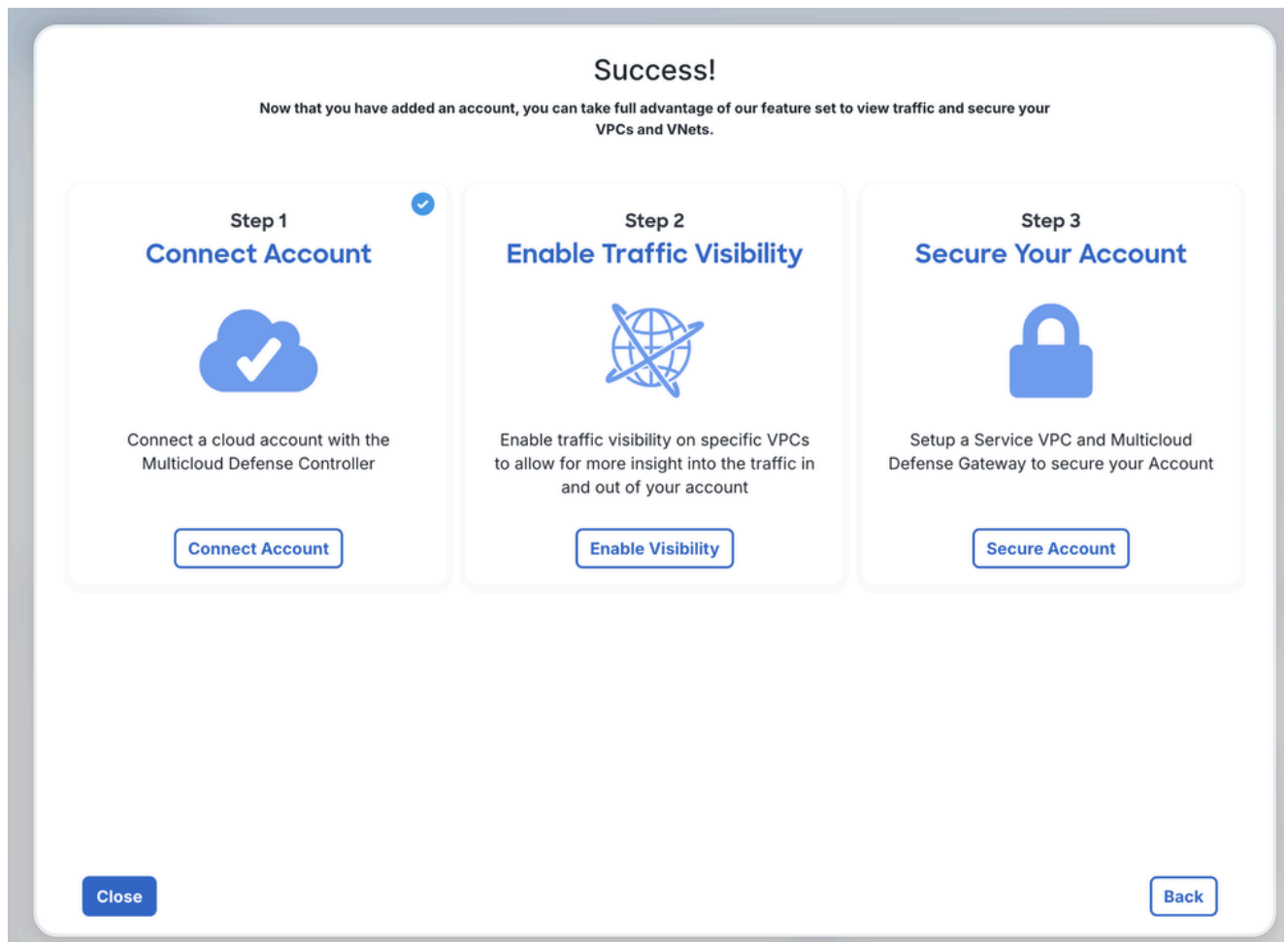
1 Cloud Accounts	63 Regions	- Network ACL	- Network ACL Rules
- Application Security Groups (Azure)	- AI Inventory	- VPCs/VNets	- Subnets
- Security Groups	- Load Balancers	- Instances	- Network Interfaces
- Tags	- Route Tables	- Applications	- Certificates

Cancel

Back

Next

6. Cliquez sur Fermer.



7. Vous pouvez maintenant afficher le compte intégré à partir de Infrastructure > CSP Accounts.



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

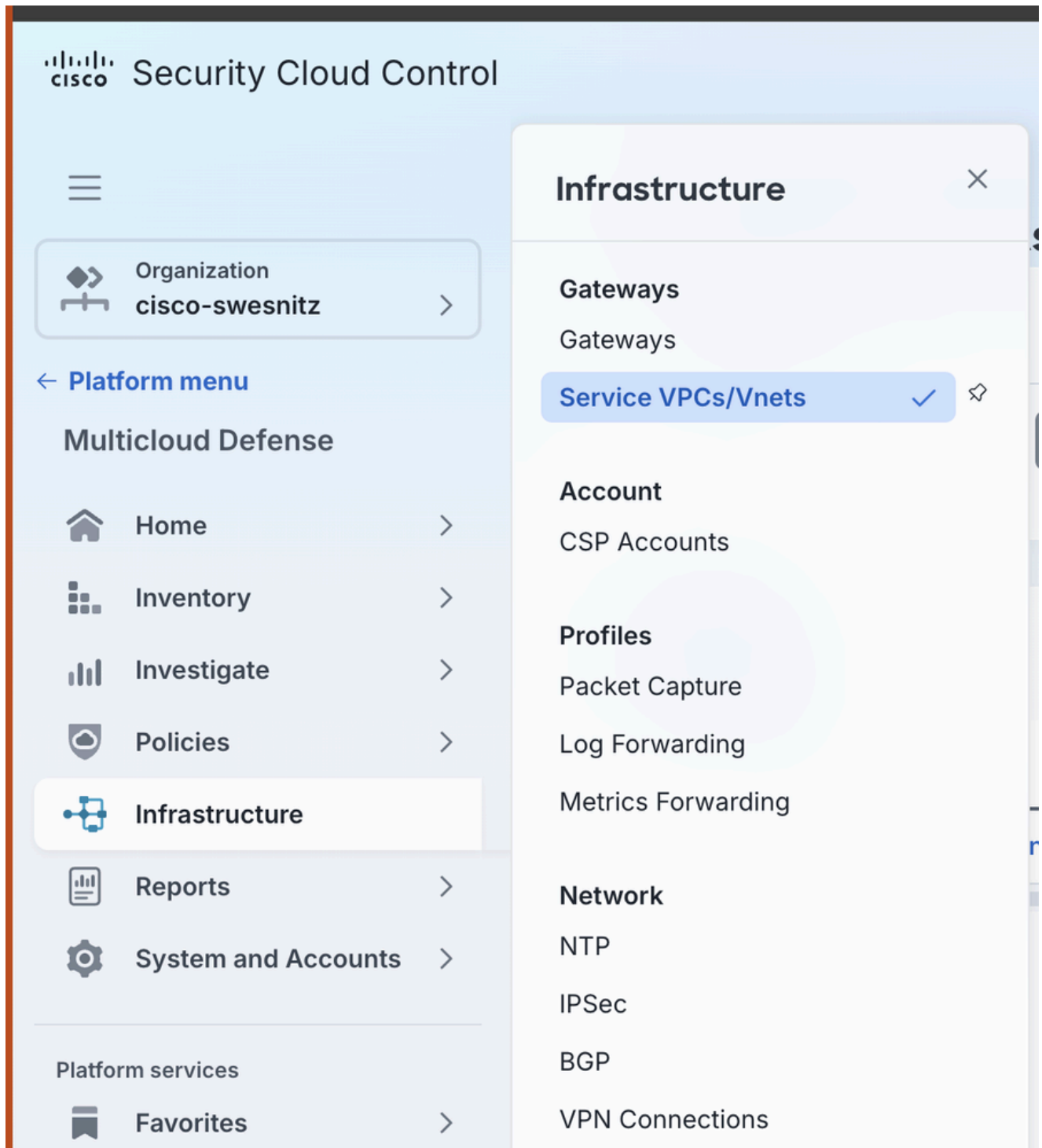
IPSec

BGP

VPN Connections

Créer un réseau virtuel

1. Accédez à Infrastructure > Service VPC/VNets.



2. Cliquez sur Créer.

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. Entrez les valeurs suivantes :

- Name : Nom facilement identifiable du réseau virtuel créé par cette procédure pour la passerelle FTDv.
- Compte CSP : Nom que vous avez attribué dans la section Connecter le compte Azure à MCD.
- Région : Région dans laquelle la passerelle FTDv est déployée.
- Bloc CIDR : Bloc IP unique pour la passerelle de transit associée au réseau virtuel.
- Zones de disponibilité : Sélectionnez au moins deux zones de disponibilité pour la résilience.
- Groupe de ressources : Sélectionnez + Créer un groupe de ressources dans le menu déroulant.
- Nom du groupe de ressources : Nom du groupe de ressources.
- Région du groupe de ressources : Région alignée sur la région que vous avez sélectionnée pour Région.

Cliquez sur 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. Un message de réussite s'affiche.



Success

Service VPC/VNet created successfully.

OK

Confirmez la création du VNet du côté Azure, accédez à Fondation du réseau > Vue d'ensemble des réseaux virtuels > Réseaux virtuels.

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

mcd

Subscription equals all

Resource Group equals all

Name ↑

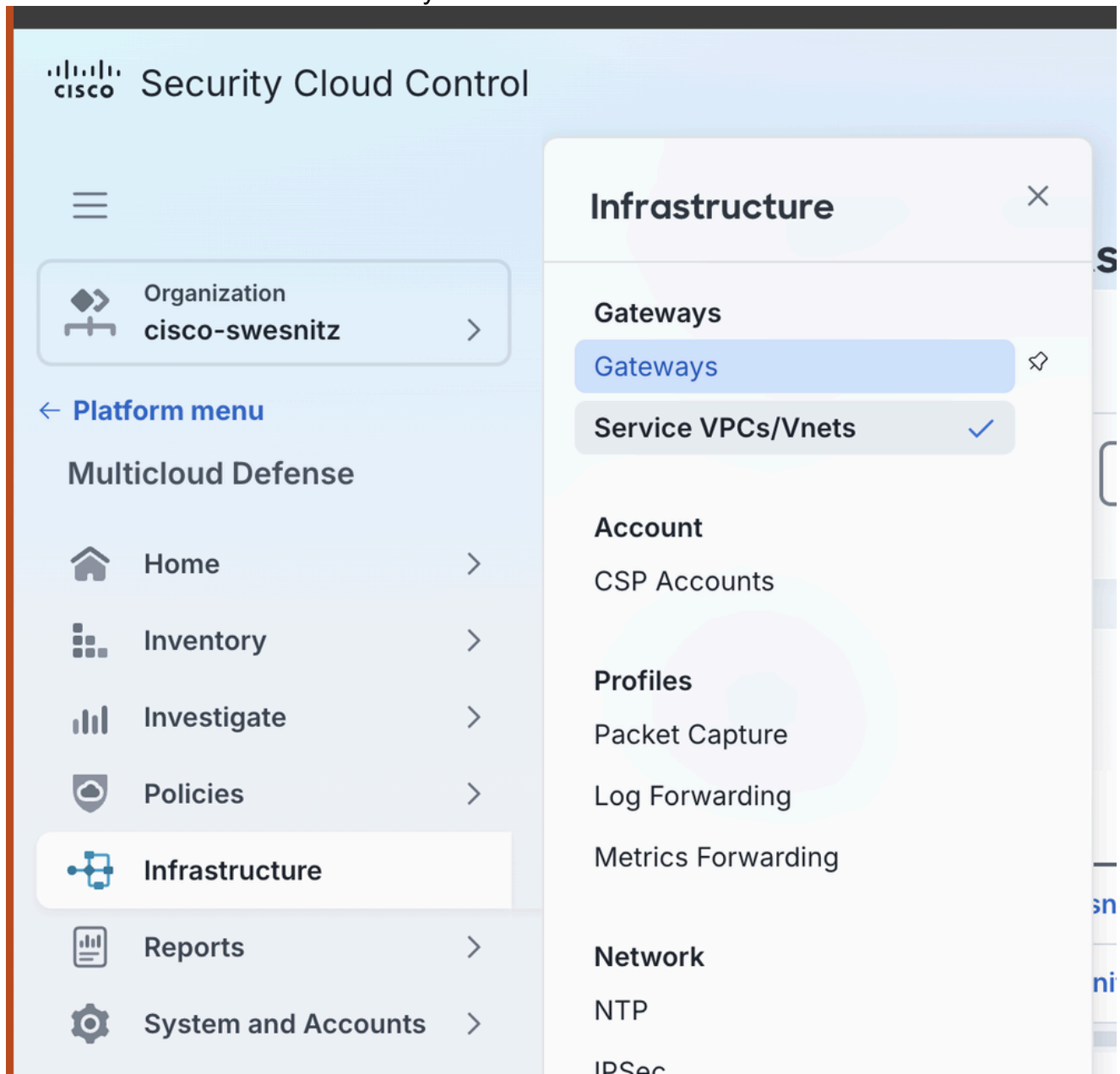
mcd_test_vnet-swesnitz

Une fois créé, le réseau virtuel passe à l'état Actif.

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

Créer la passerelle Azure MCD FTDv

1. Accédez à Infrastructure > Gateways.



2. Cliquez sur Add Gateway.

The screenshot shows the Cisco Security Cloud Control interface. On the left is a navigation menu with the following items: Organization (cisco-swesnitz), Platform menu, Multicloud Defense, Home, Inventory, Investigate, Policies, and Infrastructure (highlighted). The main content area is titled 'Gateways: 1' and contains a 'Quick Filters' section with 'Name' and 'CSP Account' dropdowns. Below this is a table with columns 'Name', 'Actions', and 'State'. The table has one row with the name 'med lab cluster' and state 'ACTIVE'.

3. Entrez les valeurs suivantes :

- Comptes : Dans le menu déroulant, sélectionnez le compte Azure que vous avez lié dans la section Connecter le compte Azure à MCD.
- Type de passerelle : Sélectionnez Passerelle FTDv.
- Name : Nom facilement identifiable pour la passerelle FTDv.
- Type d'instance : Type d'instance approprié à votre environnement.
- Instances minimales : Sélectionnez au moins une instance dans le menu déroulant.
- Nombre maximal d'instances : Nombre maximal d'instances FTDv souhaité pour votre environnement. Le maximum autorisé est 10.
- Port HealthCheck : La valeur par défaut est 65534. Ce document ne modifie pas cette valeur.

Create Gateway

Gateway InformationGateway DetailsAdvanced SettingsReview

Properties

Accounts * ⓘ
cx-tac-rtp-fw-azure X v

Gateway Type *
FTDv Gateway X v

Name * ⓘ
mcd-azure-lab X

Description
Optional

Instance Type * ⓘ
8 Virtual CPU | AZURE_D8S_V5 X v 

Minimum Instances * ⓘ
1 v

Maximum Instances * ⓘ
3 v

HealthCheck Port * ⓘ
65534 X

CancelNext



Remarque : Le port HealthCheck est le numéro de port que l'équilibreur de charge de la défense multicloud utilise pour vérifier l'intégrité des instances. Les groupes de sécurité de chemin de données affectés aux instances doivent autoriser le trafic sur ce port.

4. Entrez les valeurs suivantes :

- Propriétés : Sélectionnez Egress ou East-West.
- Version FTDv : La version logicielle la mieux adaptée à l'environnement.
- Ensemble de règles de stratégie : Stratégie de contrôle d'accès (ACP) à appliquer à ce cluster FTDv.

- Mot de passe : Mot de passe pour les instances FTDv.
- Modèle de licence : Le modèle de licence souhaité.
- Niveau de performances : Niveau approprié pour le débit de périphérique attendu.
- Types de licence : Types de licence achetés pour ce déploiement.
- Région : Région dans laquelle ces instances FTDv sont déployées.
- ID VPC/VNet : VNet de service que vous avez créé dans la section Créer un VNet.

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

Back

Next

5. Créez une paire de clés publiques. Référez-vous à [Créer une paire de clés SSH sur Windows](#) pour obtenir de l'aide.

```

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. Entrez les valeurs des groupes de clés publiques et de ressources SSH.

Create Gateway

×

Key Selection

SSH Public Key

SSH Key Pair

SSH Public key *

ssh-rsa
AAAAAB3NzaC1yc2EAAAADAQABAAQChvSlgyD
Kk+X6zGCgM3AxV3iPcxZIF7QtWB7WiagDgo+IRKcH
cPNUofBzsgyIOSuP1mYf6LZQp6Xdhk/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. Désactivez l'adresse IP publique, puis cliquez sur Suivant.

Create Gateway

✓

✓

3

4

Gateway InformationGateway DetailsAdvanced SettingsReview

Public IP

☒ Disable Public IP

8. Vérifiez toutes les valeurs que vous avez spécifiées.

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 AAAAB3NzaC1yc2EAAAADAQABAAQChvSlgyDk
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. Après avoir vérifié les valeurs et terminé le chargement des ressources, cliquez sur Terminer.

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

Affichage Tableau de bord une fois les ressources chargées.

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



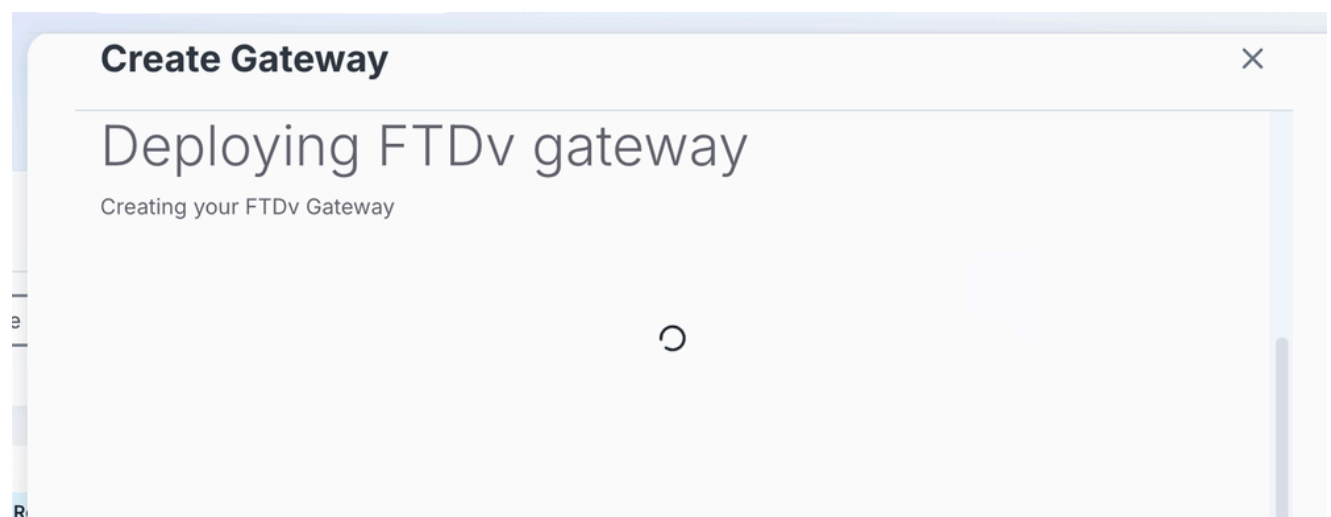
Resource	Limit	In Use	Min Usage for Gateway	Max Usage for Gateway	Recommendation
Private IPs in Subnets	254	0	1	3	
Elastic IPs	1000	51	1	3	
Load Balancers	1000	8	1	1	
Instances	25000	31	2	6	
Virtual CPUs	350	0	16	48	

Advanced Settings

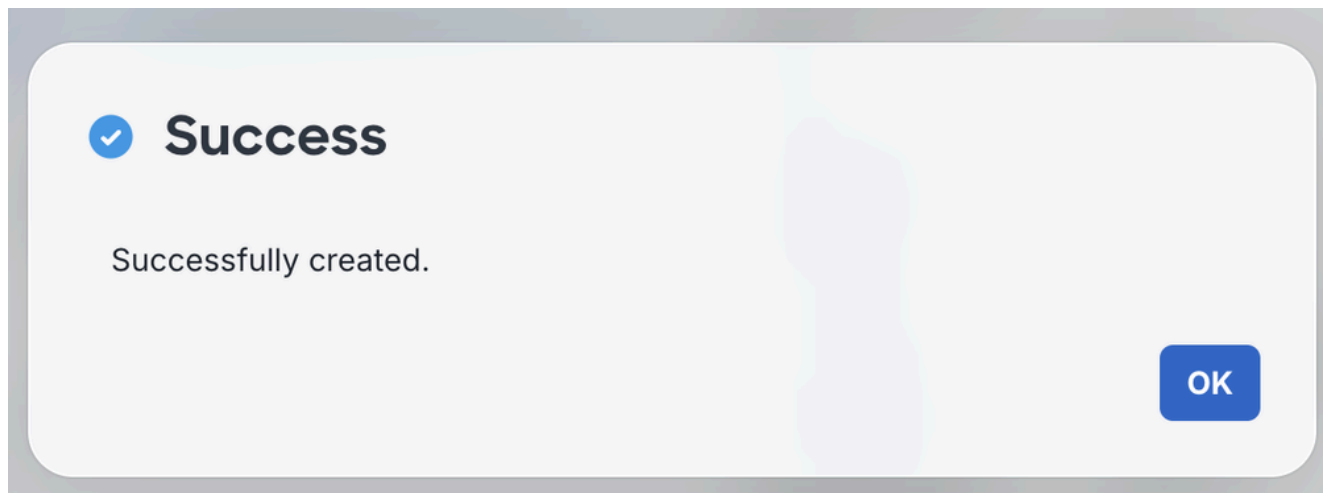
[Edit](#)**Disable Public IP**

enabled

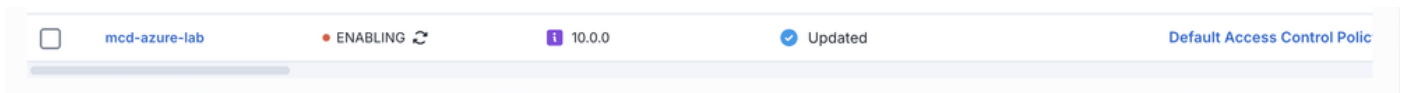
Tableau de bord du déploiement de la passerelle.



10. Une fois la création de la passerelle commencée, un message de réussite s'affiche. Click OK.



Dans le tableau de bord MCD, l'état affiche ENABLING.



Surveillez l'état à partir des onglets Résumé et Instances.

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

Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

- Sous Compute > Virtual machines dans Azure, surveillez les instances FTDv. L'état passe de Création à En cours.
- Home > Compute infrastructure

Compute infrastructure | Virtual machines

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

SearchVirtual machinesGet started

OverviewAll resourcesInfrastructureVirtual machinesVirtual Machine Scale Set (VMSS)Compute FleetArc Machines

CreateReservationsManage viewRefreshExport to CSVOpen queryAssign tagsStartRestartStopDeleteServicesGroup by no

mcdSubscription equals allType equals allResource Group equals allLocation equals allAdd 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 ...
- Confirmez l'état de la passerelle à partir du tableau de bord MCD.

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.

Informations connexes

- [Créer un VPC ou un VNet de service](#)
- [Procédure d'intégration FTDv](#)
- [Configuration des prérequis de passerelle](#)
- [Présentation de Multicloud Defense for Azure](#)
- [Créer et utiliser une paire de clés publique-privée SSH pour les machines virtuelles Linux dans Azure](#)
- [Assistance et documentation techniques - Cisco Systems](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.