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

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Configurer
  - Activez Cisco Multicloud Defense sur le locataire SCC
  - Intégrer un compte AWS (compte CSP)
  - Créer un VPC de service
  - Démarrer l'Assistant Passerelle FTDv
  - Configurer les propriétés de passerelle
  - Configuration des paramètres avancés (facultatif)
  - Révision et déploiement
- Vérifier
- Dépannage
- Résumé
- Informations connexes

Introduction

Ce document décrit comment intégrer votre compte AWS à Cisco Multicloud Defense (MCD) et déployer des passerelles FTDv à l'aide du contrôleur Cisco MCD.

Conditions préalables

- Un centre de gestion des pare-feu (cdFMC) fourni dans le cloud pour le locataire SCC.
- Une paire de clés AWS EC2 est disponible dans la région à déployer.
- Un compte AWS avec des autorisations IAM suffisantes pour déployer une pile CloudFormation.

- Un abonnement/droit Cisco Multicloud Defense actif sur le client SCC, ainsi que les types de licences FTDv et les droits de niveau de performance applicables.
- Accès administratif SCC avec droits de gestion des abonnements à la plate-forme et de l'infrastructure de défense multicloud.
- Accès à la console AWS avec des autorisations pour créer et surveiller les piles CloudFormation et les ressources EC2.

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Navigation dans Cisco Security Cloud Control (SCC)
- Concepts de réseau AWS de base (VPC, CIDR, passerelle de transit, zones de disponibilité)
- Déploiement et analyse de la pile AWS CloudFormation

Composants utilisés

- Contrôle du cloud de sécurité Cisco (SCC)
- Cisco Multicloud Defense (MCD)
- Cisco Secure Firewall Threat Defense Virtual (FTDv)
- Centre de gestion des pare-feu (cdFMC) fourni dans le cloud
- Amazon Web Services (AWS) - CloudFormation, EC2, VPC, Transit Gateway

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.

Informations générales

Ce document couvre un déploiement MCD pour la première fois dans un compte AWS unique et une région utilisant un type de réseau de passerelle de transit (TGW). Les types de réseau WAN cloud AWS et les déploiements de passerelles d'entrée ne sont pas abordés dans ce document, car les passerelles d'entrée ne sont actuellement pas prises en charge par MCD.



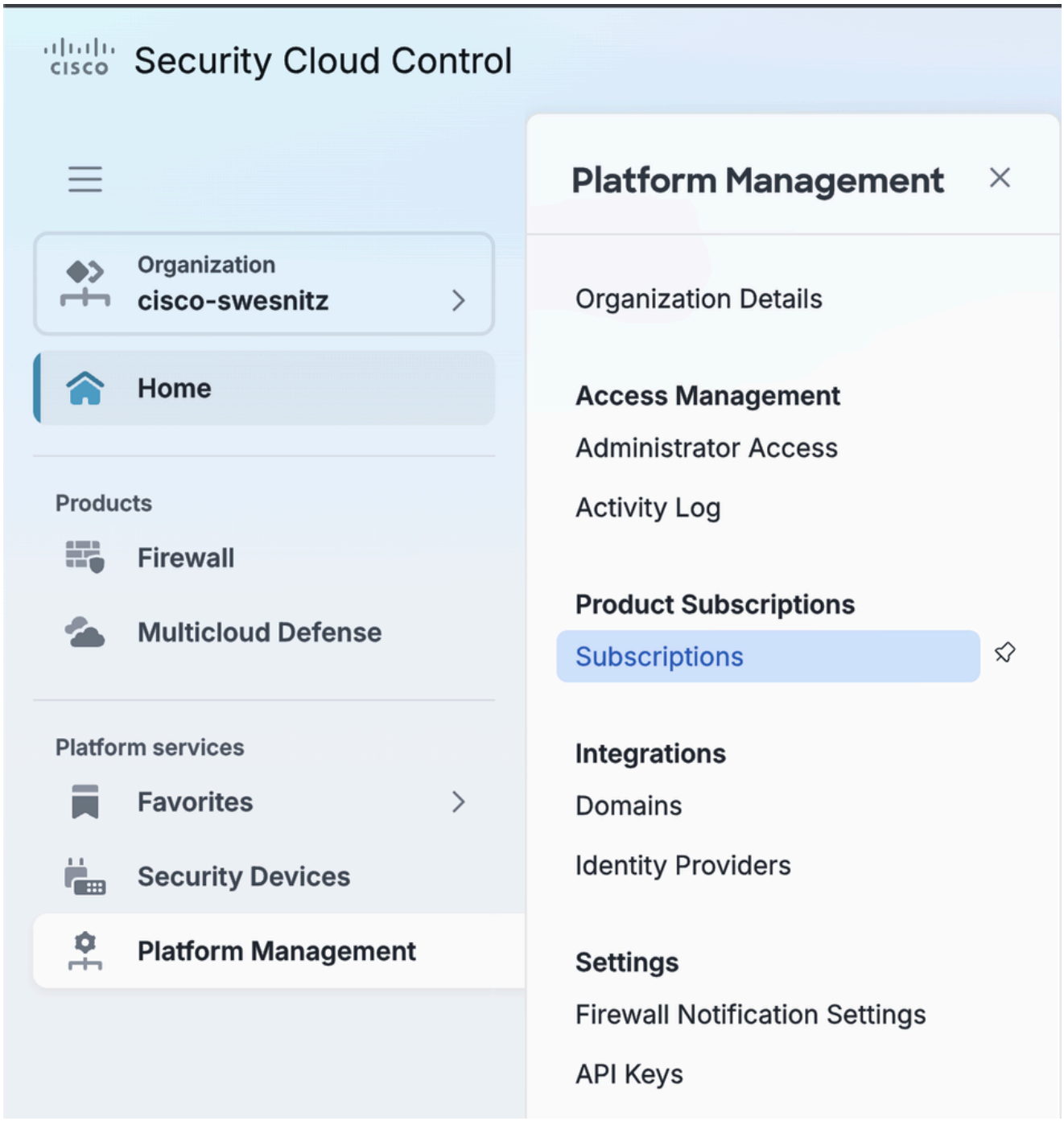
Remarque : Les passerelles d'entrée ne sont actuellement pas prises en charge par Multicloud Defense. Seuls les déploiements de passerelle en sortie/est-ouest sont traités dans ce document.

Remarque : Si la tentative d’enregistrement cdFMC initiale échoue ou expire, il s’agit du comportement attendu. Laissez plus de temps au cluster pour réessayer l'inscription automatiquement avant de poursuivre le dépannage.

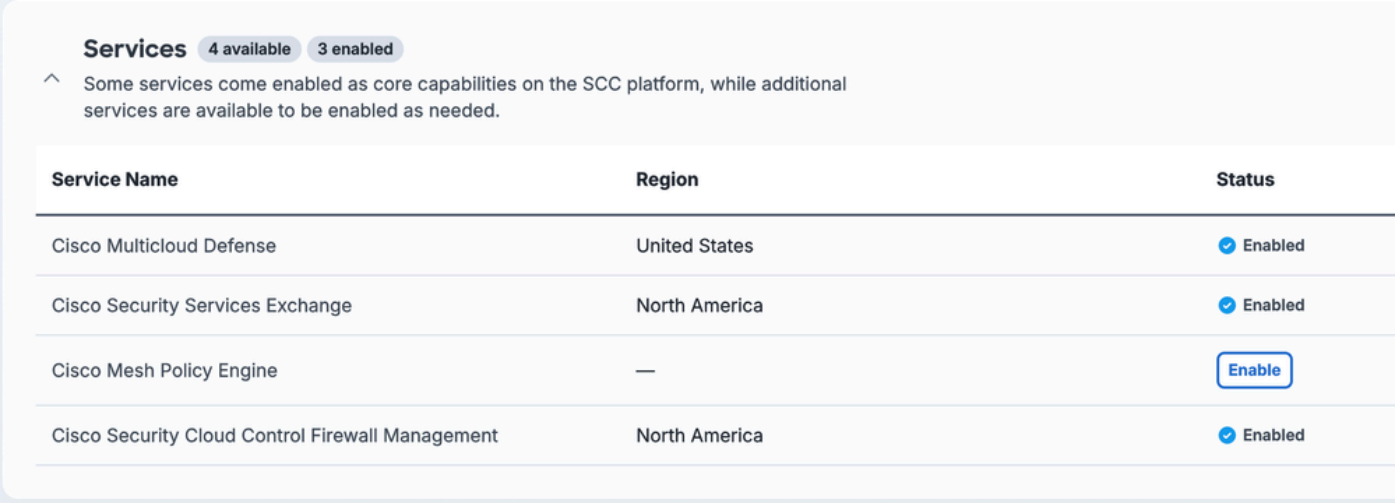
Configurer

Activez Cisco Multicloud Defense sur le locataire SCC

1. Dans la console Cisco Security Cloud Control (SCC), accédez à Home > Platform Management > Subscriptions.



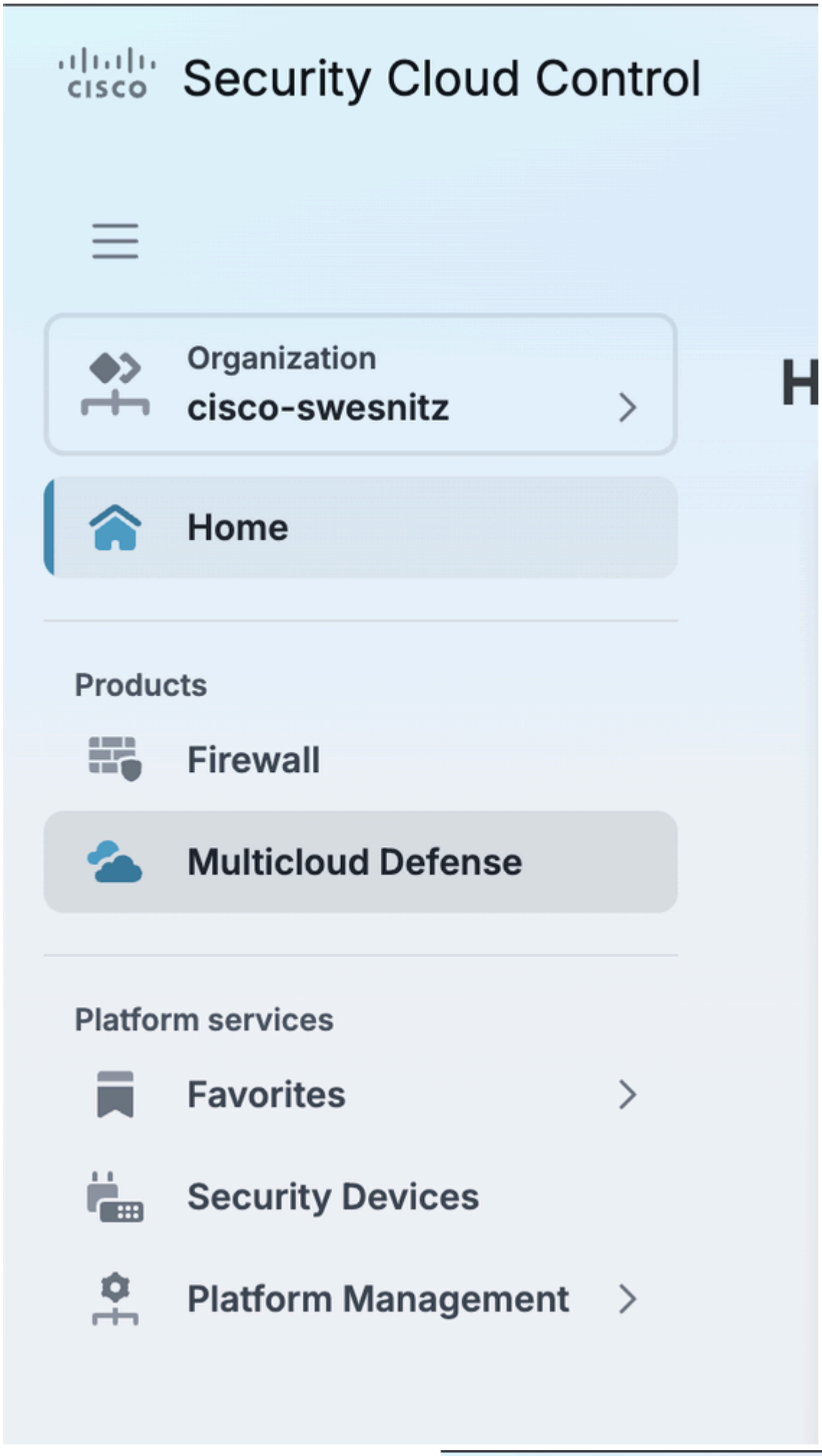
2. Activez l'abonnement Multicloud Defense pour le locataire.

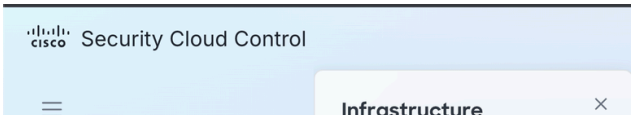


Intégrer un compte AWS (compte CSP)

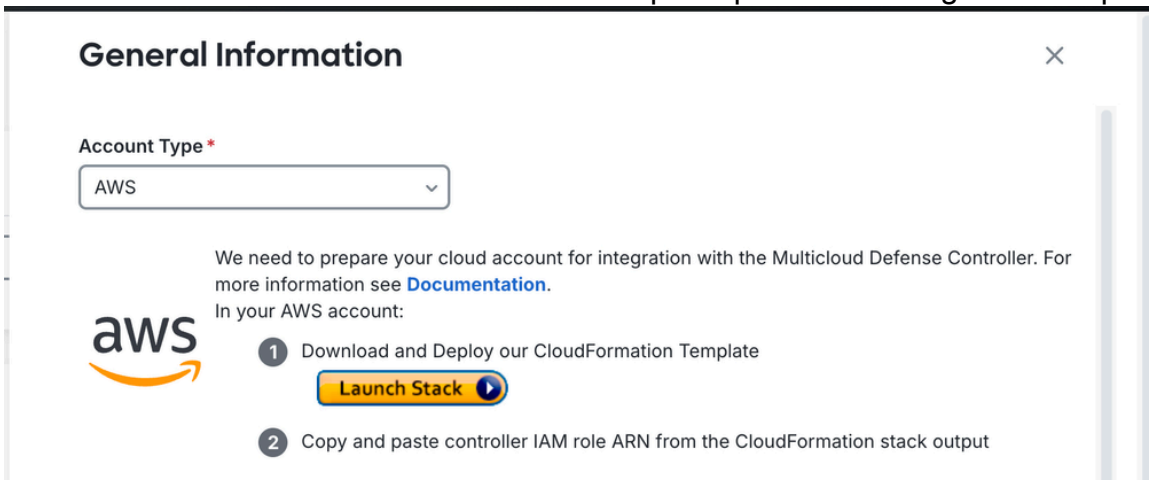
Cette étape permet de connecter un compte AWS au contrôleur de défense multicloud afin que MCD puisse déployer et gérer des ressources pour son compte. Cet exemple utilise AWS comme fournisseur de services cloud (CSP).

1. Dans le volet de navigation gauche de SCC, sélectionnez Multicloud Defense.

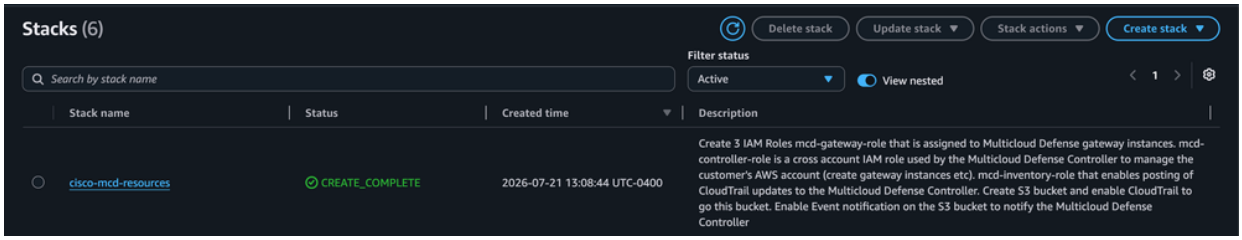

Security Cloud Control
Organization
cisco-swesnitz
Home
Products
Firewall
Multicloud Defense
Platform services
Favorites
Security Devices
Platform Management


Security Cloud Control

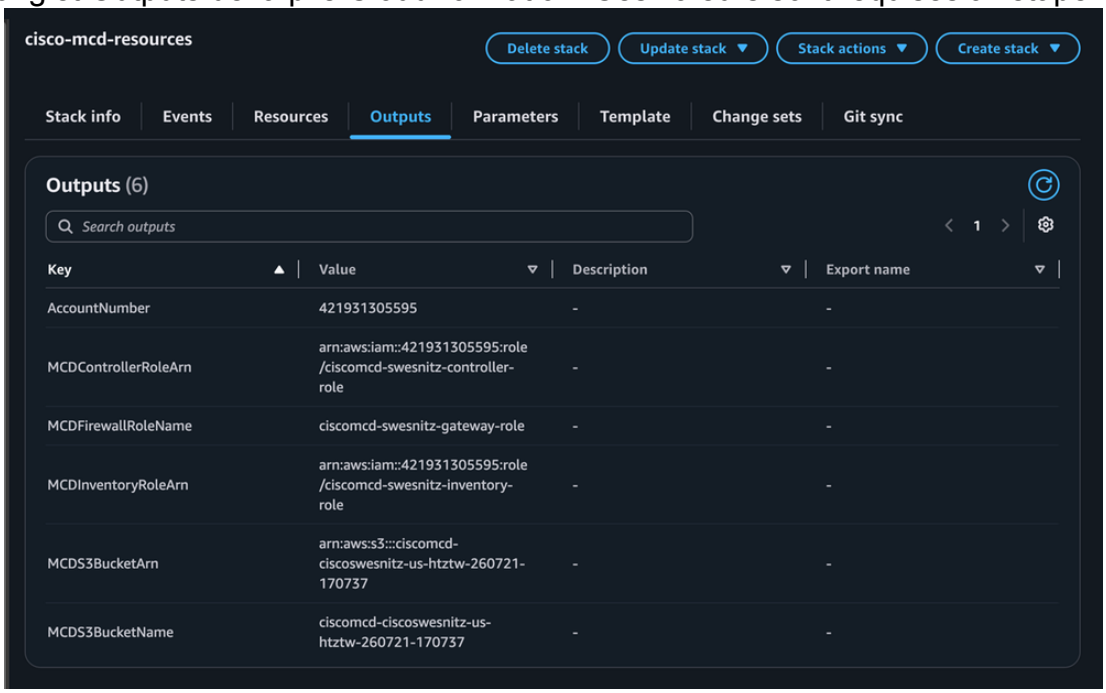
. Cela ouvre un nouvel onglet de navigateur et lance une pile AWS CloudFormation qui déploie les rôles IAM et les ressources nécessaires pour que MCD s'intègre au compte AWS.



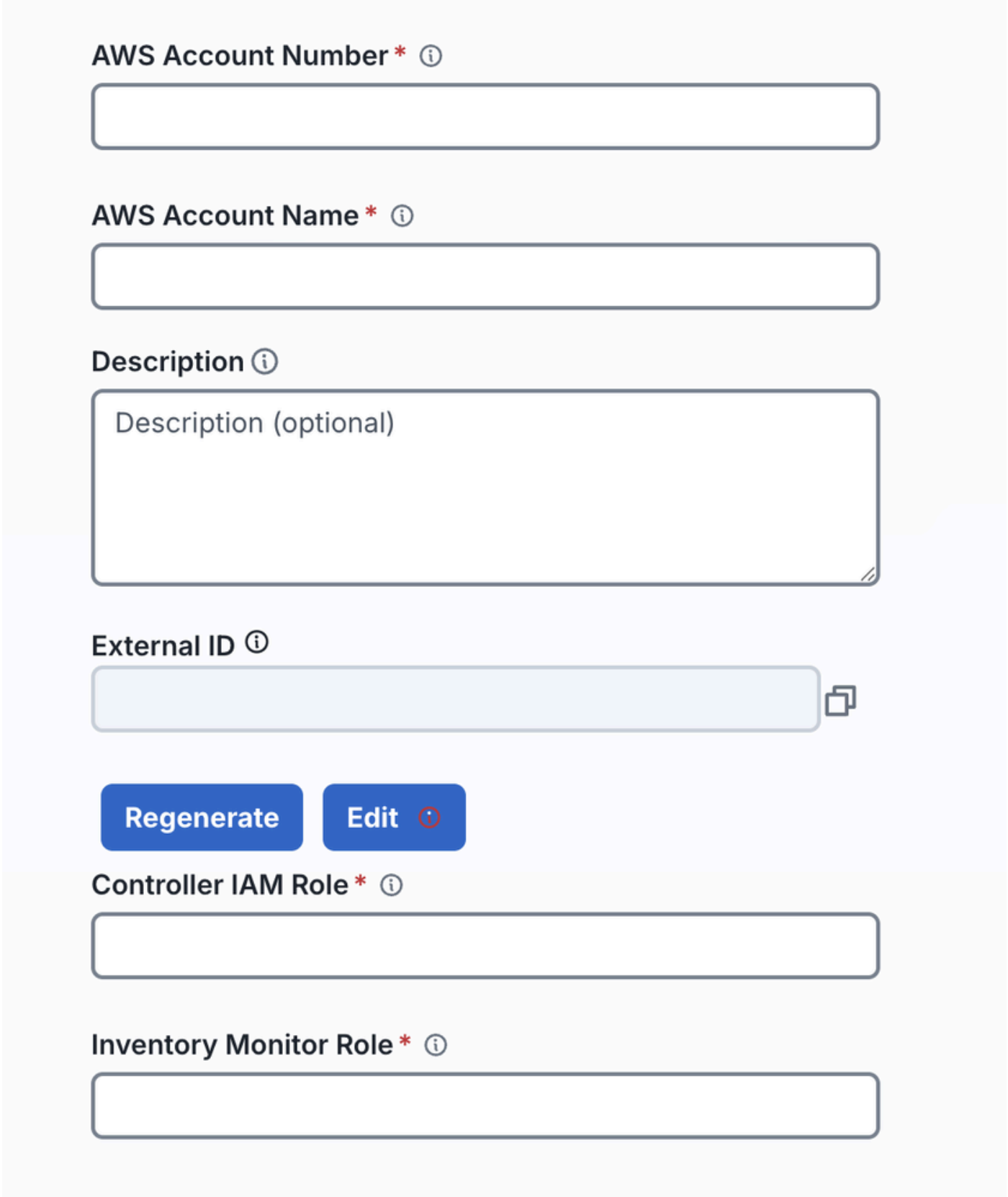
6. Dans la console AWS, vérifiez que la pile CloudFormation s'exécute correctement.



7. Ouvrez l'onglet Outputs de la pile CloudFormation. Ces valeurs sont requises à l'étape suivante.



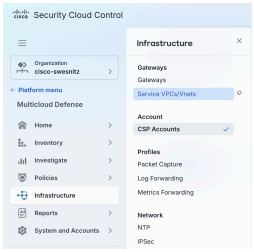
8. Dans le formulaire Ajouter un compte MCD, saisissez les valeurs suivantes :
   Numéro de compte AWS : Le résultat `AccountNumber` de la pile CloudFormation.
   Nom du compte AWS : Un nom convivial et identifiable pour ce compte AWS dans MCD.
   Rôle IAM du contrôleur : Le résultat de `MCDControllerRoleArn` de la pile CloudFormation.
   Rôle de moniteur d'inventaire : Le résultat de `MCDInventoryRoleArn` de la pile CloudFormation.

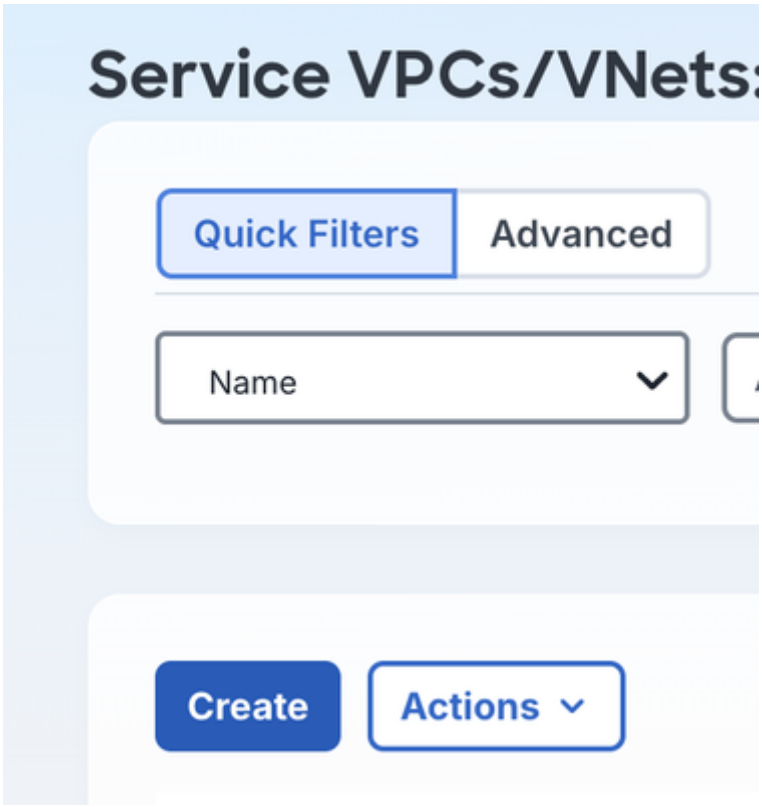


9. Sauvegardez le compte. Le compte AWS est intégré à MCD.

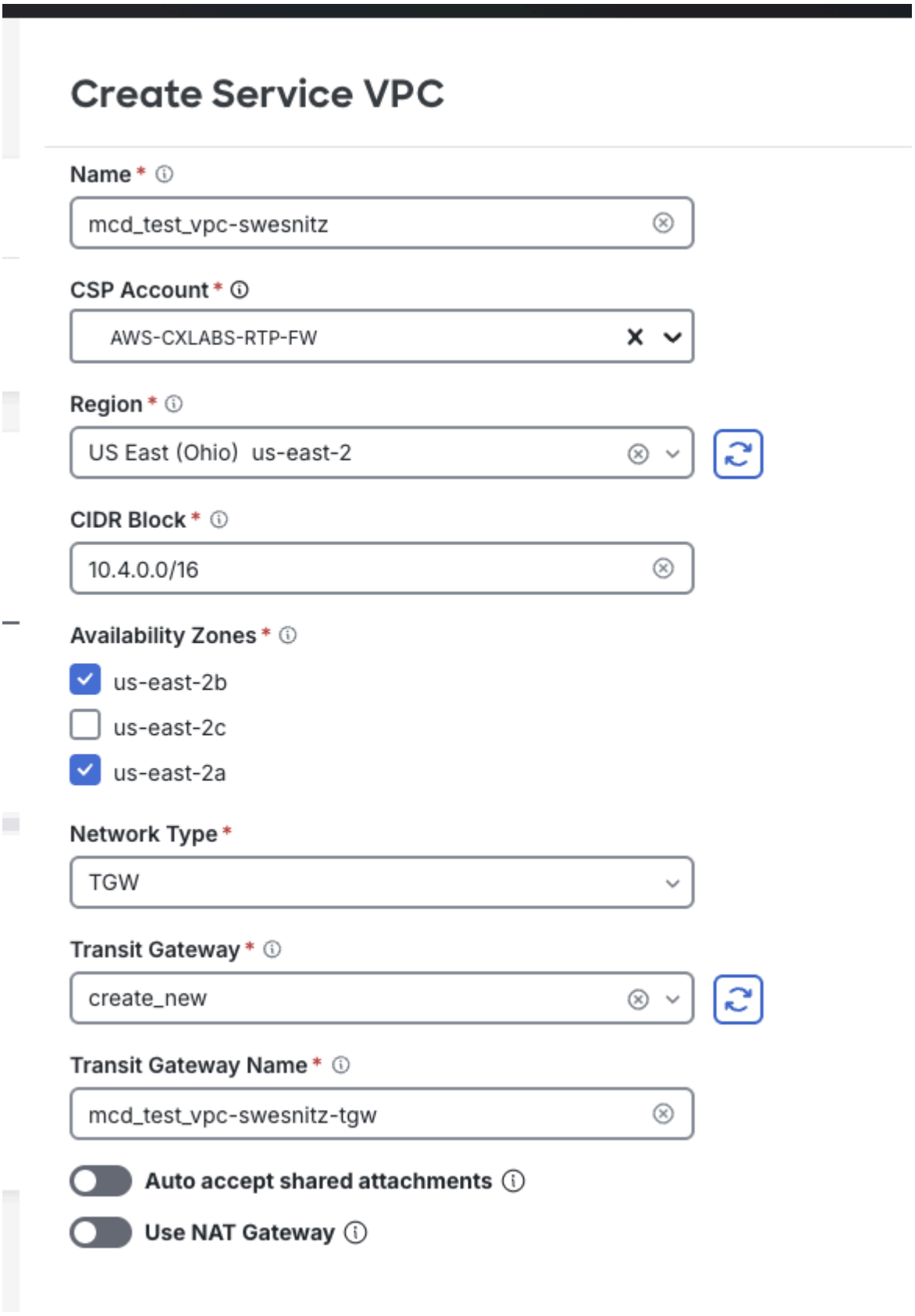
Créer un VPC de service

Le VPC de service héberge l'infrastructure réseau (sous-réseaux, tables de routage, passerelle de transit) utilisée par la passerelle FTDv.

1. Accédez à Multicloud Defense > Infrastructure > Service VPC/VNets. 



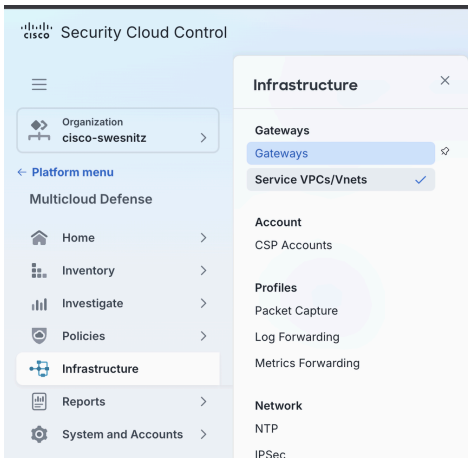
2. Sélectionnez Créer.
3. Configurez les paramètres VPC :
   Name : Nom unique et facilement identifiable du VPC.
   Compte CSP : Compte AWS intégré à l'étape 2.
   Région : Région AWS où le cluster FTDv est lancé.
   Bloc CIDR : Une plage CIDR dédiée à ce déploiement MCD (ne doit pas chevaucher les VPC existants).
   Zones de disponibilité : au moins une AZ ; deux sont recommandés pour la redondance.
   Type de réseau : Sélectionnez Transit Gateway (TGW). CloudWAN est un type de réseau distinct utilisé spécifiquement pour les déploiements de WAN cloud AWS et n'est pas couvert par ce document.
   Passerelle de transit : Sélectionnez create_new, avec un nom unique pour la nouvelle passerelle de transit.
   Passerelle NAT (en option) : Active le routage de tout le trafic de sortie via une passerelle NAT. Non activé dans cet exemple ; La configuration de la passerelle NAT est hors de portée pour ce document.

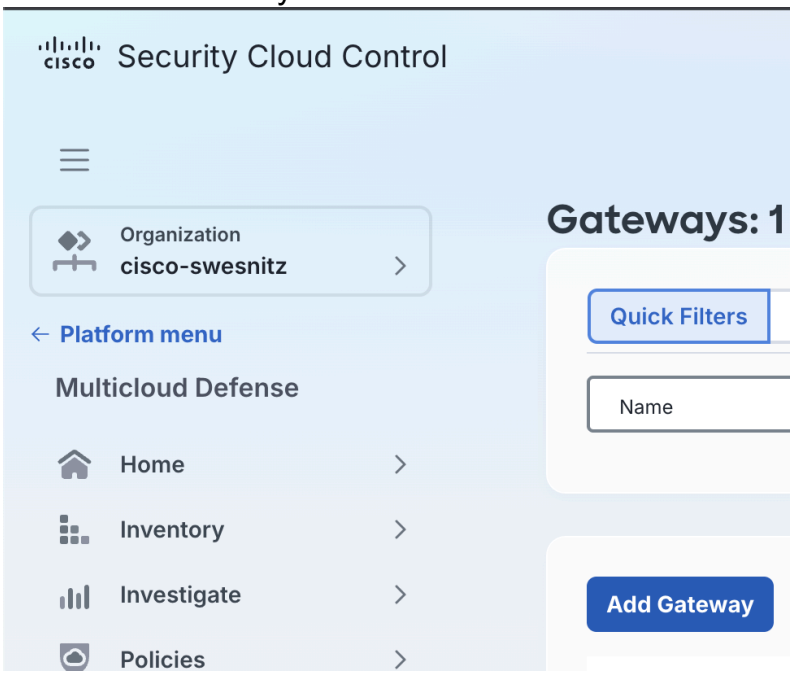


4. Sélectionnez Enregistrer.

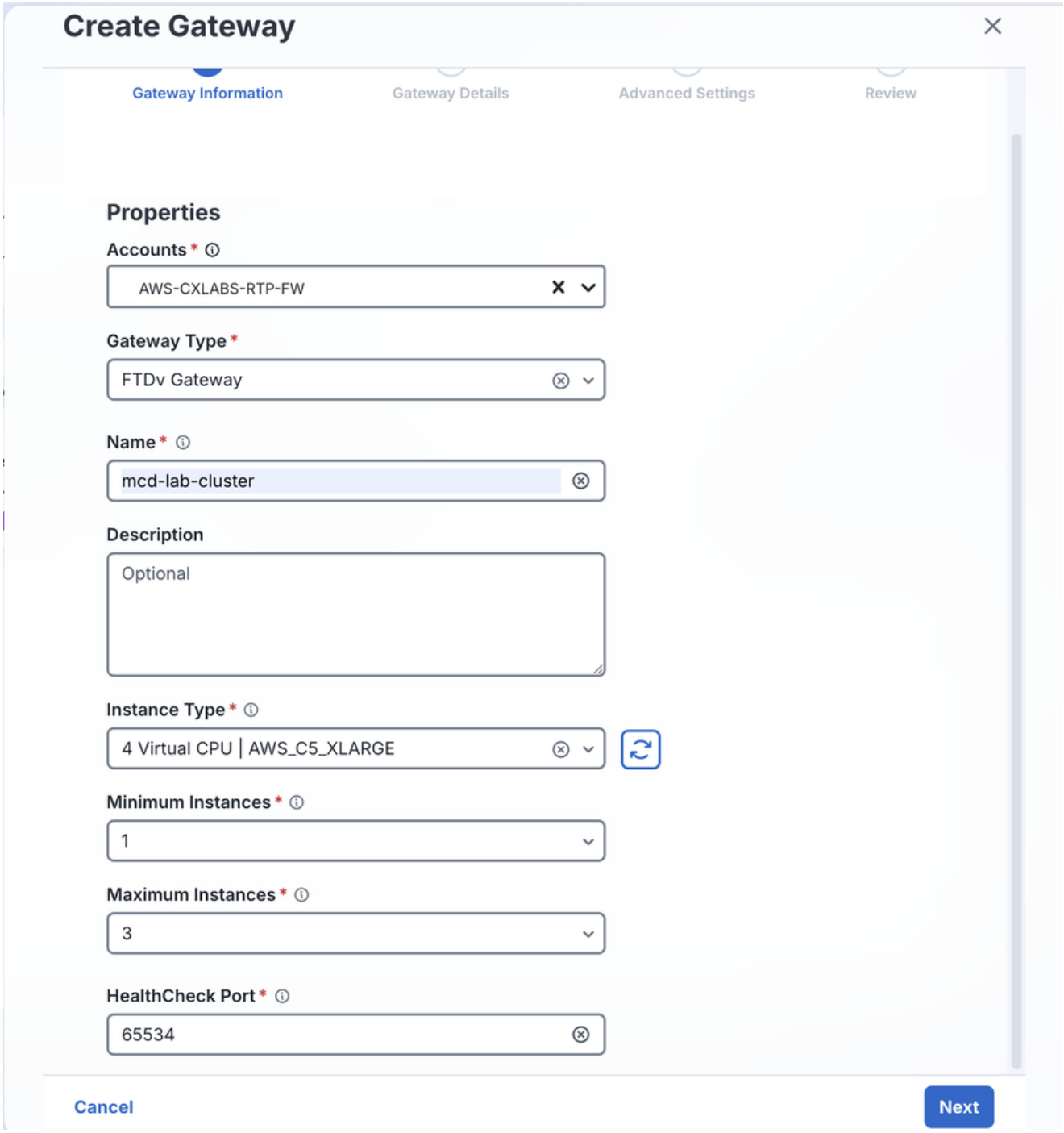
Démarrer l'Assistant Passerelle FTDv

1. Accédez à Multicloud Defense > Infrastructure > Gateways.





2. Sélectionnez Ajouter une passerelle.
3. Configurez les paramètres initiaux :
   Comptes : Compte CSP intégré à l'étape 2.
   Type de passerelle : Sélectionnez Passerelle FTDv.
   Name : Nom complet de ce cluster dans MCD.
   Type d'instance : Taille de l'instance correspondant aux besoins en débit et en performances. Cet exemple utilise le type minimal pris en charge, `C5_XLARGE`.
   Instances minimum/maximum : Plage de mise à l'échelle souhaitée. La valeur minimale est 1 instance ; le maximum est 10.
   Port HealthCheck : La valeur par défaut est 65534 ; ne change que si un port différent a été spécifié pour l'équilibreur de charge MCD. En cas de modification, le port doit être autorisé dans tous les groupes de sécurité de chemin de données associés aux instances FTDv.



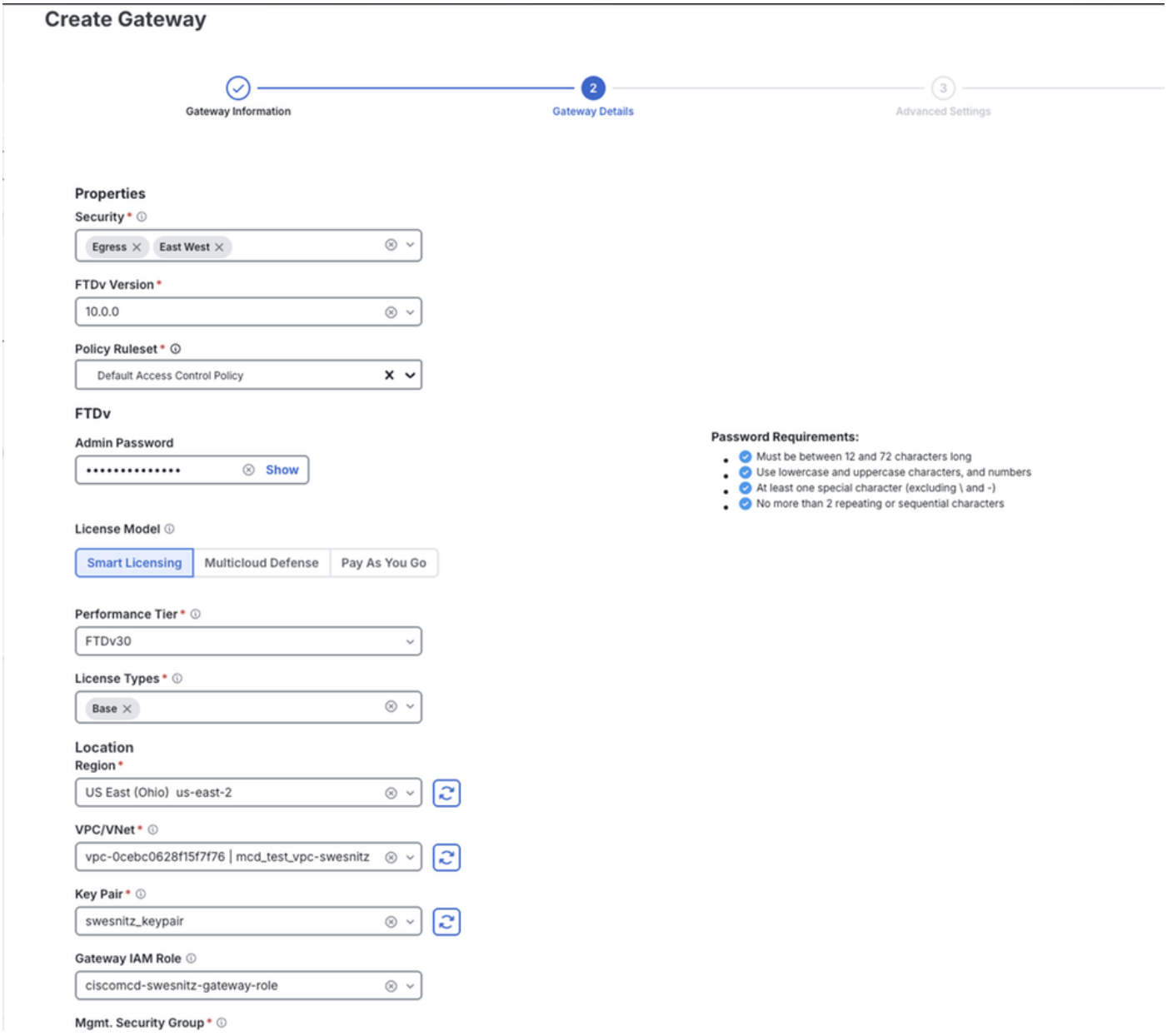
4. Sélectionnez Suivant.

Configurer les propriétés de passerelle

Propriétés : Sélectionnez Egress/East-West. Les passerelles d'entrée ne sont actuellement pas prises en charge.
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: Le VPC de service créé à l'étape 3.
Paire de clés: Une paire de clés AWS existante.
Rôle IAM de passerelle : Rôle contenant la passerelle dans son nom, correspondant à `MCDFirewallRoleName` de la pile CloudFormation à l'étape 2. La sélection de ce rôle renseigne automatiquement les groupes de sécurité associés.
Cryptage EBS: Le chiffrement géré par AWS est sélectionné par défaut. Amazon EBS chiffre automatiquement et en toute transparence les volumes de stockage en mode bloc, les données en transit et les instantanés.

1. Sélectionnez Suivant.





Configuration des paramètres avancés (facultatif)

Les paramètres avancés permettent de configurer des options telles que la désactivation des adresses IP publiques pour les instances FTDv. Les paramètres avancés ne sont pas configurés dans cet exemple.

Révision et déploiement

1. Vérifiez la précision de tous les paramètres configurés.



2. Sélectionnez Terminer pour commencer le déploiement.

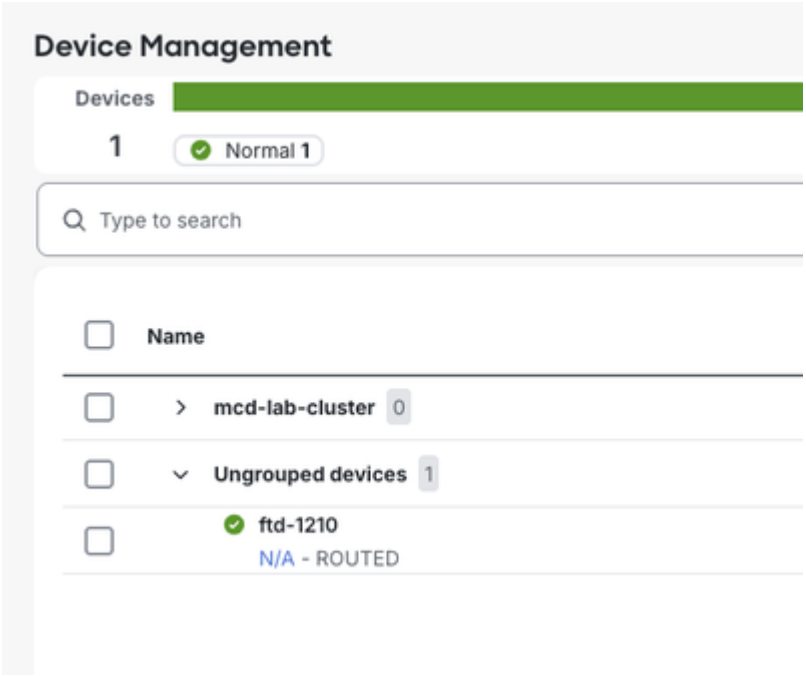
Remarque : Le déploiement peut prendre jusqu'à 30 minutes. Pendant ce temps, MCD provisionne et regroupe le nombre spécifié d'instances FTDv et les enregistre auprès de cdFMC.

Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

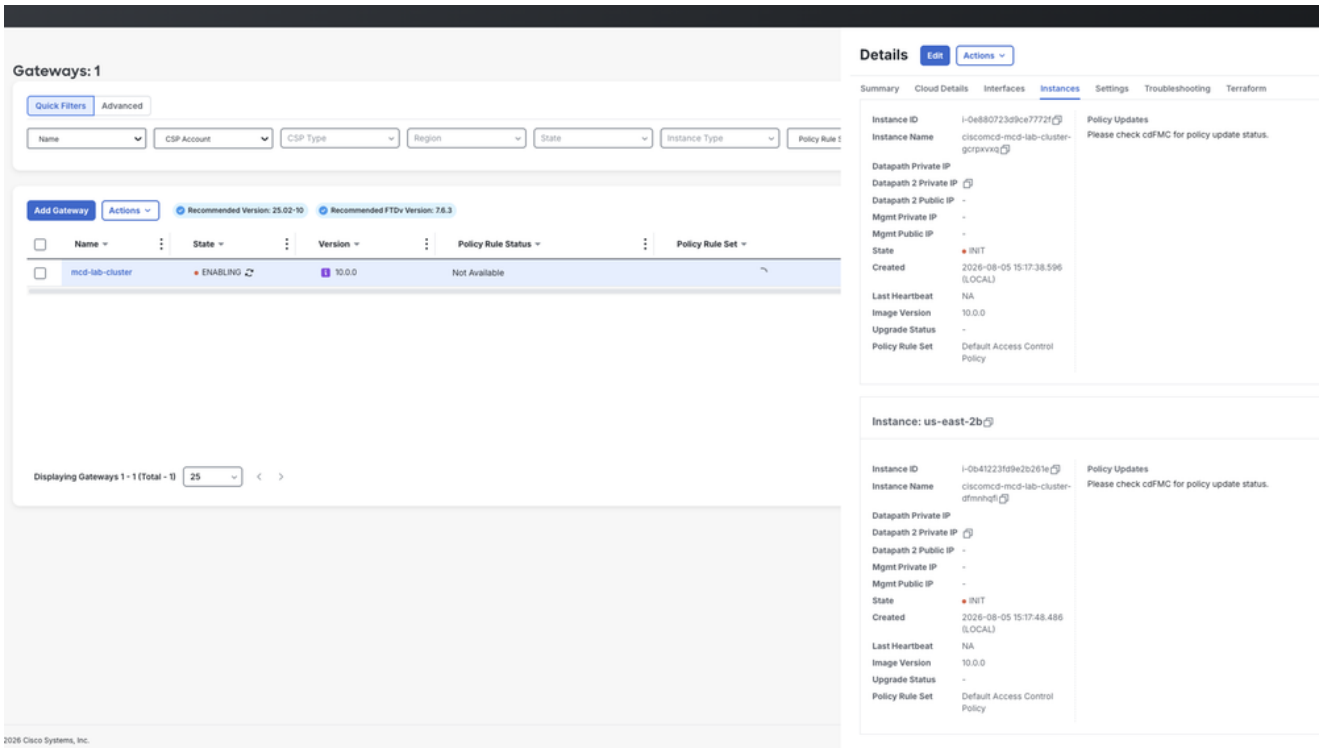
La réussite du déploiement et de l'enregistrement peut être confirmée à partir de plusieurs emplacements :

- cdFMC : Immédiatement après avoir sélectionné Terminer, le nouveau cluster apparaît (dans un état en attente) dans cdFMC sous Périphériques > Gestion des périphériques.

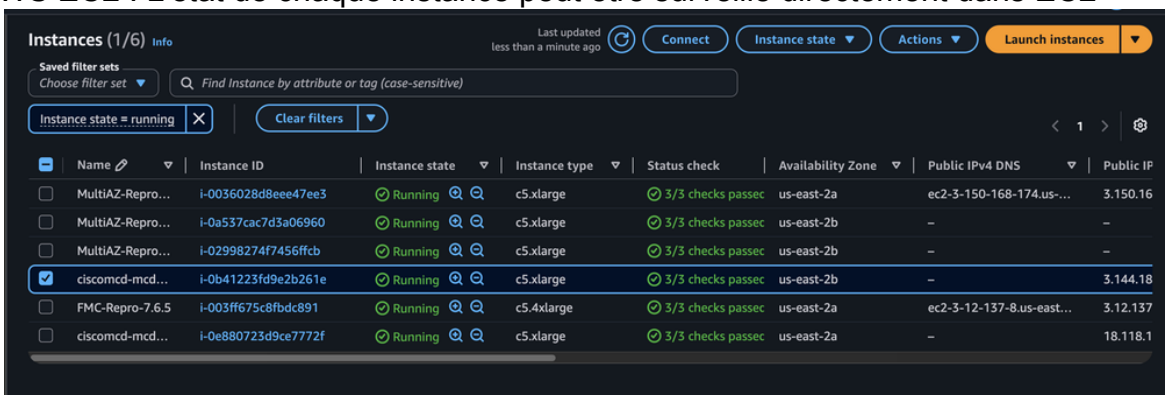


- Détails de la passerelle MCD : La sélection du nom de la passerelle ouvre un panneau de détails indiquant la progression du lancement.

  Sélectionnez le nom spécifié, puis cliquez sur l'onglet Instances.

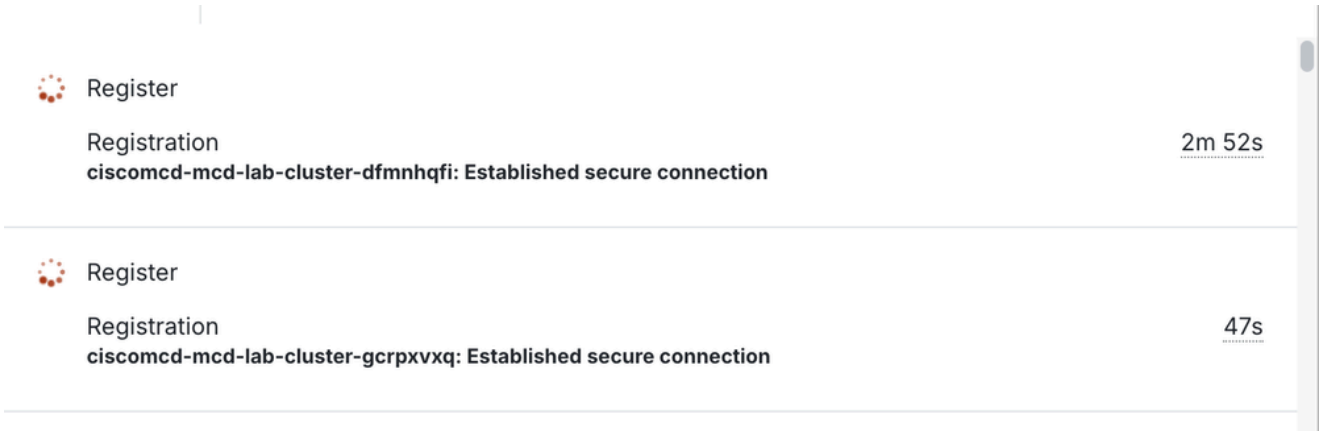


- Console AWS EC2 : L'état de chaque instance peut être surveillé directement dans EC2 > Instances.

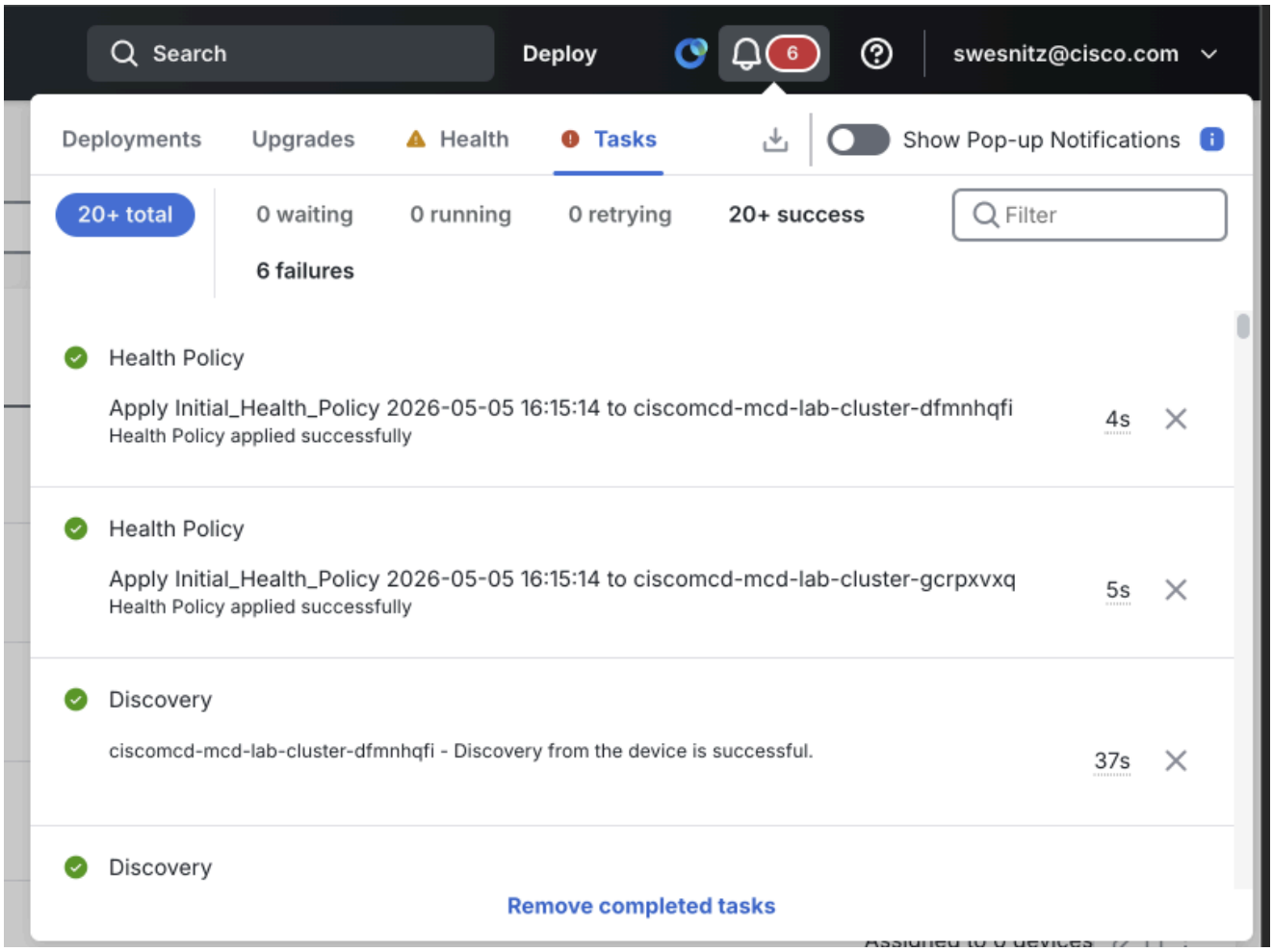


- Onglet Tâches cdFMC : La progression de l'inscription est suivie ici :

  Inscription en cours :



  Succès de l'inscription :



- État final : Une fois l'enregistrement réussi, la passerelle affiche l'état Actif - En attente avant de passer à l'état Actif complet, confirmant que le cluster est déployé et opérationnel.

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

- La tentative d'enregistrement initiale échoue ou expire dans l'onglet Tâches cdFMC - Comportement attendu lors de la première tentative d'enregistrement. Laissez plus de temps au cluster pour réessayer l'inscription automatiquement avant de poursuivre le dépannage.
- Échec de la pile CloudFormation - Vérifiez que l'utilisateur/le rôle AWS IAM déployant la pile dispose d'autorisations suffisantes et consultez l'onglet Événements pour connaître la raison de l'échec spécifique.
- Le rôle IAM de passerelle ou les groupes de sécurité ne sont pas renseignés dans l'assistant de passerelle - Confirmez que la pile CloudFormation de l'étape 2 s'est terminée correctement et que le compte CSP et la région corrects ont été sélectionnés.

Résumé

Cette procédure aboutit aux résultats suivants :

- Défense multicloud activée sur le client SCC.
- Compte AWS intégré via CloudFormation.

- Service VPC créé avec une passerelle de transit.
- Passerelle FTDv en cluster déployée et enregistrée sur cdFMC.

La passerelle FTDv est active et prête pour la configuration des politiques et l'inspection du trafic.

Informations connexes

- Pare-feu Threat Defense virtuel
- Connectez un compte AWS au contrôleur de défense multicloud à partir du tableau de bord de défense multicloud
- Créer un VPC ou un VNet de service
- Créer une passerelle FTDv
- 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.