Guide de présentation de CX Agent v3.1

Table des matières

- Introduction
  - Conditions préalables
  - Accès aux domaines critiques
  - Domaines spécifiques au portail cloud CX
  - Domaines spécifiques à la machine virtuelle agent CX
  - Versions prises en charge par Catalyst Center
  - Navigateurs pris en charge
  - Liste des produits pris en charge
  - Mise à niveau/installation de CX Agent v3.1.5
  - Mise à niveau des machines virtuelles existantes vers une configuration étendue et moyenne
- Mise à niveau vers CX Agent v3.1.5
  - Mises à niveau automatiques
  - Mises à niveau manuelles
- Ajout d'un agent CX
- Configuration de CX Agent pour BCS/LCS
  - Conditions préalables
  - Configuration de l'agent CX
- Configuration des fonctionnalités RADKit
  - Intégration du client RADKit via CLI
- Configuration du coffre-fort pour les agents CX existants
  - Intégration de CX Agent avec HashiCorp Vault via CLI
    - Conditions préalables
    - Intégration à HashiCorp Vault
  - Activation de l'intégration HashiCorp Vault
  - Désactivation de l'intégration HashiCorp Vault
  - Schéma des identifiants de périphérique HashiCorp Vault
  - Configuration des identifiants de périphérique dans HashiCorp Vault (première fois)
  - Ajout d'informations d'identification à HashiCorp Vault
  - Fichier d'amorçage cloud CX avec informations d'identification par défaut
- Ajout de Catalyst Center comme source de données
- Ajout de sources de données BCS/LCS
  - Ajout de SolarWinds®
  - Ajout d'EPNM
  - Ajout d'APIC
- Ajout d'autres ressources comme sources de données
  - Protocoles de détection
  - Protocoles de connectivité
  - Limitations du traitement de télémétrie pour les périphériques

- Ajout d'autres ressources à l'aide d'un fichier initial
  - Ajout d'autres ressources à l'aide d'un nouveau fichier de démarrage
  - Ajout d'autres ressources à l'aide d'un fichier de démarrage modifié
  - Informations d'identification par défaut du fichier de démarrage
- Ajout d'autres ressources via des plages IP
  - Ajout d'autres ressources par plages IP
  - Modification des plages IP
  - Suppression de plages IP
  - À propos des périphériques détectés à partir de plusieurs contrôleurs
- Ajout d'autres ressources via CDP ou LLDP
  - Modification des détails CDP ou LLDP
- Planification des analyses de diagnostic
- Mise à niveau des machines virtuelles agent CX vers des configurations moyennes et grandes
  - Reconfiguration à l'aide du client lourd VMware vSphere
  - Reconfiguration à l'aide du client Web ESXi v6.0
  - Reconfiguration à l'aide de Web Client vCenter
- Déploiement et configuration du réseau
  - Déploiement OVA
    - Installation de ThickClient ESXi 5.5/6.0
    - Installation de WebClient ESXi 6.0
    - Installation de WebClient vCenter
    - Installation d'OracleVirtual Box 7.0.12
    - Installation de Microsoft Hyper-V
    - Paramètres du processeur
    - Validation des signatures d'image Microsoft Hyper-V
  - Configuration du réseau
  - Autre approche pour générer un code de jumelage à l'aide de CLI
  - Configuration des périphériques pour transférer Syslog vers CX Cloud Agent
    - Conditions préalables
    - Configuration du paramètre Syslog Forward
  - Configuration d'autres ressources (collecte directe des périphériques) pour transférer Syslog à l'agent CX
    - Serveurs Syslog existants avec fonctionnalité de transfert
    - Serveurs Syslog existants sans fonction de transfert OU sans serveur Syslog
  - Activation des paramètres Syslog au niveau des informations pour Cisco Catalyst Center
- Sauvegarde et restauration de la machine virtuelle cloud CX
  - Sauvegarde de la VM cloud CX
  - Restauration de la machine virtuelle du cloud CX
- Sécurité
  - Sécurité physique
  - Sécurité de compte
  - Sécurité du réseau
  - Authentification
  - Durcissement
  - Sécurité des données
  - Transmission de données

Connexions et surveillance

Commandes de télémétrie Cisco

Résumé de la sécurité

Introduction

Ce document décrit l'agent Cisco Customer Experience (CX). Cisco CX Agent est une plate-forme hautement évolutive qui collecte des données de télémétrie à partir des périphériques réseau des clients afin de fournir des informations exploitables aux clients. CX Agent permet la transformation de l'intelligence artificielle (AI)/apprentissage automatique (ML) des données de configuration en cours actives en informations proactives et prédictives affichées dans le cloud CX (y compris les pistes de réussite, Smart Net Total Care (SNTC) et les offres Business Critical Services (BCS) ou Lifecycle Services (LCS)).

Ce guide est destiné aux administrateurs cloud et partenaires CX uniquement. Les utilisateurs dotés des rôles Super User Admin (SUA) et Admin disposent des autorisations nécessaires pour effectuer les actions décrites dans ce guide.

Ce guide est spécifique à l'agent CX v3.1.5. Reportez-vous à la page Agent Cisco CX pour accéder aux versions antérieures.

Remarque : les images de ce guide sont fournies à titre de référence uniquement. Le contenu réel peut varier.

Conditions préalables

CX Agent fonctionne en tant que machine virtuelle (VM) et peut être téléchargé en tant qu'appliance virtuelle ouverte (OVA) ou disque dur virtuel (VHD).

Exigences de déploiement

- L'un des hyperviseurs suivants est requis pour une nouvelle installation :
  - VMware ESXi v5.5 ou ultérieure
  - Oracle Virtual Box v5.2.30 ou ultérieure
  - Hyperviseur Windows versions 2012 à 2022 et version 2025
- Les configurations du tableau suivant sont requises pour le déploiement d'une machine virtuelle :

Type de déploiement d'agent CX	Nombre de coeurs de processeur	BÉLIER	Disque dur	*Nombre maximal d'actifs directement connecté à CX Agent	Hyperviseurs pris en charge
OVA petite	8 QUATER	16 Go	200 Go	10,000	VMware ESXi, Oracle VirtualBox et Windows Hyper-V

Type de déploiement d'agent CX	Nombre de coeurs de processeur	BÉLIER	Disque dur	*Nombre maximal d'actifs directement connecté à CX Agent	Hyperviseurs pris en charge
OVA moyen	16 TASSES	32 Go	600 Go	20,000	VMware ESXi, Windows Hyper-V
OVA volumineux	32 TASSES	64 Go	1 200 Go	50,000	VMware ESXi, Windows Hyper-V

*Outre la connexion de 20 non-clusters Cisco Catalyst Center (Catalyst Center) ou de 10 clusters Catalyst Center pour chaque instance CX Cloud Agent.

- Pour les clients utilisant des data centers américains désignés comme région de données principale pour stocker les données du cloud CX, l'agent CX doit être en mesure de se connecter aux serveurs indiqués ici, en utilisant le nom de domaine complet (FQDN) et HTTPS sur le port TCP 443 :
  - Nom de domaine complet (FQDN) : agent.us.csco.cloud
  - Nom de domaine complet (FQDN) : ng.acs.agent.us.csco.cloud
- Pour les clients utilisant des data centers désignés en Europe comme principale région de données pour stocker les données du cloud CX : l'agent CX doit pouvoir se connecter aux deux serveurs présentés ici, à l'aide du nom de domaine complet et du protocole HTTPS sur le port TCP 443 :
  - Nom de domaine complet (FQDN) : agent.us.csco.cloud
  - Nom de domaine complet (FQDN) : agent.emea.csco.cloud
  - Nom de domaine complet (FQDN) : ng.acs.agent.emea.csco.cloud
- Pour les clients utilisant des data centers Asie-Pacifique désignés comme région de données principale pour stocker les données du cloud CX : l'agent CX doit pouvoir se connecter aux deux serveurs présentés ici, à l'aide du nom de domaine complet et du protocole HTTPS sur le port TCP 443 :
  - Nom de domaine complet (FQDN) : agent.us.csco.cloud
  - Nom de domaine complet (FQDN) : agent.apjc.csco.cloud
  - Nom de domaine complet (FQDN) : ng.acs.agent.apjc.csco.cloud
- Pour les clients utilisant des data centers désignés en Europe et en Asie-Pacifique comme leur principale région de données, la connectivité au FQDN : agent.us.csco.cloud est requis uniquement pour l'enregistrement de CX Cloud Agent avec CX Cloud lors de la configuration initiale. Une fois que CX Cloud Agent est correctement enregistré auprès de CX Cloud, cette connexion n'est plus nécessaire.
- Pour la gestion locale de CX Cloud Agent, le port 22 doit être accessible.
- Pour les clients utilisant RADKit avec le nom de domaine complet et HTTPS sur le port TCP 443 :
  - FQDN US : radkit.us.csco.cloud
  - FQDN EMEA : radkit.emea.csco.cloud
  - FQDN APJC : radkit.apjc.csco.cloud

- Pour permettre à RADKit d'associer la sortie à une demande de service, le FQDN cxd.cisco.com doit être accessible pour l'agent CX.
- Le tableau suivant récapitule les ports et les protocoles qui doivent être ouverts et activés pour que CX Cloud Agent fonctionne correctement :

Source	Destination	Protocol	Port	Objectif	Type
Agent CX Cloud	Toutes les régions : ◦ agent.us.csco.cloud ◦ Centre Catalyst Région AMER : ◦ ng.acs.agent.us.csco.cloud ◦ radkit.us.csco.cloud* Région EMEA : ◦ agent.emea.csco.cloud ◦ ng.acs.agent.emea.csco.cloud ◦ radkit.emea.csco.cloud* Région APJC : ◦ agent.apjc.csco.cloud ◦ ng.acs.agent.apjc.csco.cloud ◦ radkit.apjc.csco.cloud*	HTTPS	TCP/443	◦ Configuration initiale ◦ Mises à niveau ◦ Transferts d'inventaire et de télémétrie ◦ Accès au cloud RADKit	Sortant vers les data centers régionaux Cisco AWS et Catalyst Center
Agent CX Cloud	Périphériques réseau	SNMP	UDP/161	◦ Détection initiale ◦ Collecte continue des stocks	Sortant vers le LAN
Agent CX Cloud	Périphériques réseau	SSH	TCP/22	Collecte de données télémétriques à partir de commandes CLI	Sortant vers le LAN
Agent CX Cloud	Périphériques réseau	Telnet	TCP/23	Collecte de données télémétriques à partir des commandes CLI	Sortant vers le LAN

Périphériques réseau	Agent CX Cloud	Syslog	UDP/514	Transférer les syslogs pour la gestion des erreurs d'alerte	Entrant depuis le réseau local
Poste De Travail	Agent CX Cloud	SSH	TCP/22	Maintenance de CX Cloud Agent	Entrant depuis le réseau local

*Non obligatoire sauf si RADKit est utilisé.

Remarques :
- Une adresse IP est automatiquement détectée si le protocole DHCP (Dynamic Host Configuration Protocol) est activé dans l'environnement de machine virtuelle ; sinon, une adresse IPv4 gratuite, un masque de sous-réseau, une adresse IP de passerelle par défaut et une adresse IP de serveur DNS (Domain Name Service) doivent être disponibles.
- Seul IPv4 est pris en charge.
- Les versions certifiées de Catalyst Center en cluster haute disponibilité (HA) et à noeud unique sont les versions 2.1.2.x à 2.2.3.x, 2.3.3.x, 2.3.5.x, 2.3.7.x et Catalyst Center Virtual Appliance.
- Si le réseau dispose d'une interception SSL, indiquez l'adresse IP de l'agent CX.
- Pour toutes les ressources directement connectées, le niveau de privilège SSH 15 est requis.
- Utilisez uniquement les noms d'hôte fournis ; Les adresses IP statiques ne doivent pas être utilisées.

Accès aux domaines critiques

Pour commencer le parcours CX Cloud, les utilisateurs doivent avoir accès aux domaines suivants : Utilisez uniquement les noms d'hôte fournis ; n'utilisez pas d'adresses IP statiques.

Domaines spécifiques au portail cloud CX

Principaux domaines	Autres domaines
csco.cloud	cloudfront.net
	eum-appdynamics.com

split.io	appdynamics.com
	tiqcdn.com
	jquery.com

Domaines spécifiques à la machine virtuelle agent CX

AMÉRIQUE	EMEA	APJC
agent.us.csco.cloud	agent.us.csco.cloud	agent.us.csco.cloud
ng.acs.agent.us.csco.cloud	agent.emea.csco.cloud	agent.apjc.csco.cloud
	ng.acs.agent.emea.csco.cloud	ng.acs.agent.apjc.csco.cloud

Remarque : L'accès sortant doit être autorisé avec la redirection activée sur le port 443 pour les noms de domaine complets spécifiés.

Versions prises en charge par Catalyst Center

Les versions prises en charge de Catalyst Center à noeud unique et cluster haute disponibilité sont les versions 2.1.2.x à 2.2.3.x, 2.3.3.x, 2.3.5.x, 2.3.7.x et Catalyst Center Virtual Appliance et Catalyst Center Virtual Appliance.

Navigateurs pris en charge

Pour une expérience optimale sur Cisco.com, la dernière version officielle de ces navigateurs est recommandée :

- Google Chrome
- Microsoft Edge
- Mozilla Firefox

Liste des produits pris en charge

Pour afficher la liste des produits pris en charge par CX Agent, reportez-vous à la Liste des produits pris en charge.

Mise à niveau/installation de CX Agent v3.1.5

- Les clients existants effectuant une mise à niveau vers la nouvelle version doivent se reporter à Mise à niveau de CX Agent v3.1.5
- Les nouveaux clients qui mettent en oeuvre une nouvelle installation flexible d'OVA v3.1 doivent se reporter à Ajout d'un agent CX.

Mise à niveau des machines virtuelles existantes vers une configuration étendue et moyenne

Les clients peuvent mettre à niveau leur configuration VM existante vers une configuration moyenne ou grande à l'aide d'options OVA flexibles en fonction de la taille et de la complexité de leur réseau.

Pour mettre à niveau la configuration de machine virtuelle existante de petite à moyenne ou grande, référez-vous à la section Mise à niveau des machines virtuelles de l'agent CX vers une configuration de moyenne et grande.

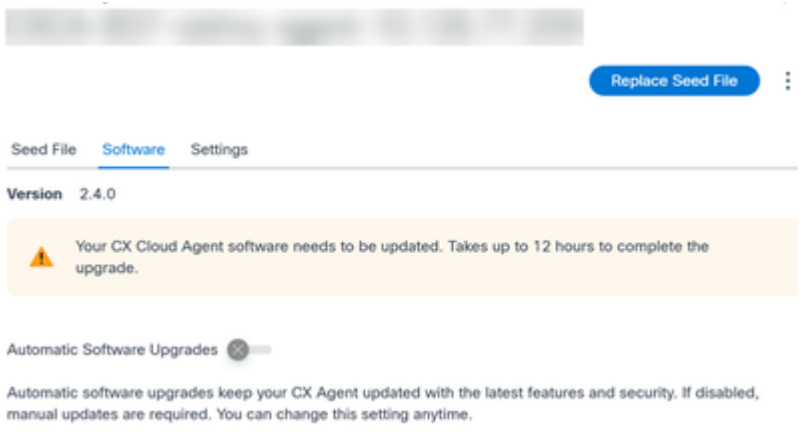
Mise à niveau vers CX Agent v3.1.5

Les clients existants peuvent effectuer une mise à niveau vers la dernière version en activant des mises à niveau automatiques ou en choisissant de procéder à une mise à niveau manuelle à partir de leur version existante.

Remarque : Les images de ce guide sont fournies à titre de référence uniquement. Le contenu réel peut varier.

Mises à niveau automatiques

Les clients peuvent activer l'option Mises à niveau logicielles automatiques pour s'assurer que leur système est mis à jour lorsque de nouvelles versions sont publiées. Cette option est activée par défaut pour les nouvelles installations, mais elle peut être modifiée à tout moment pour s'aligner sur les politiques de l'entreprise ou pour planifier des mises à niveau pendant les fenêtres de maintenance planifiées.



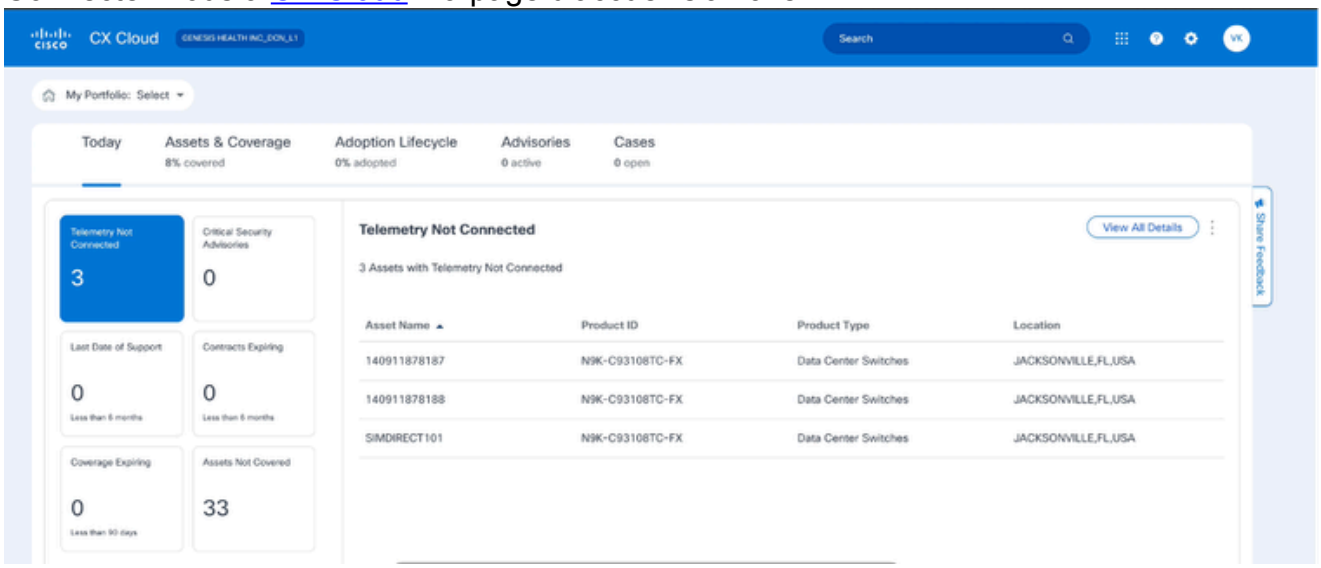
Remarque : les mises à niveau automatiques sont désactivées par défaut pour les instances d'agent CX existantes, mais les utilisateurs peuvent les activer à tout moment.

Mises à niveau manuelles

Les clients qui préfèrent ne pas utiliser les mises à niveau automatiques et qui n'ont pas activé les mises à niveau automatiques du logiciel peuvent choisir de procéder à une mise à niveau manuelle. CX Agent prend en charge les mises à niveau directes vers la version 3.1.5.

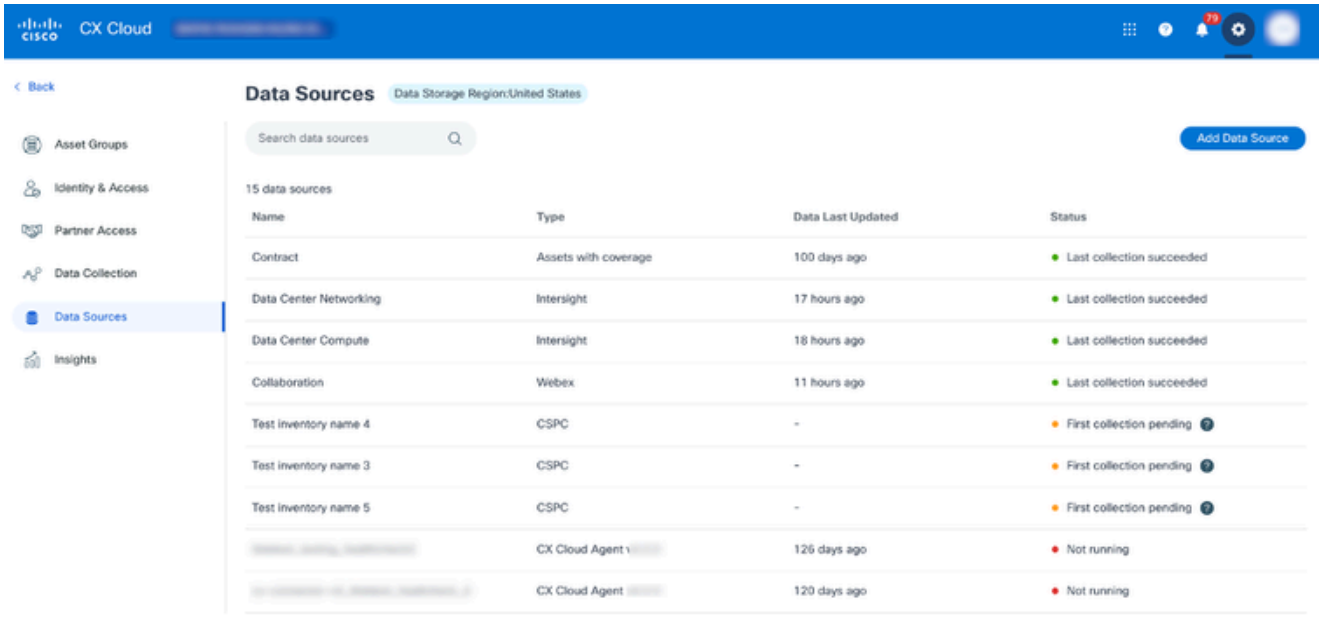
Pour installer la mise à niveau CX Agent v3.1.5 à partir du cloud CX :

1. Connectez-vous à CX Cloud. La page d'accueil s'affiche.



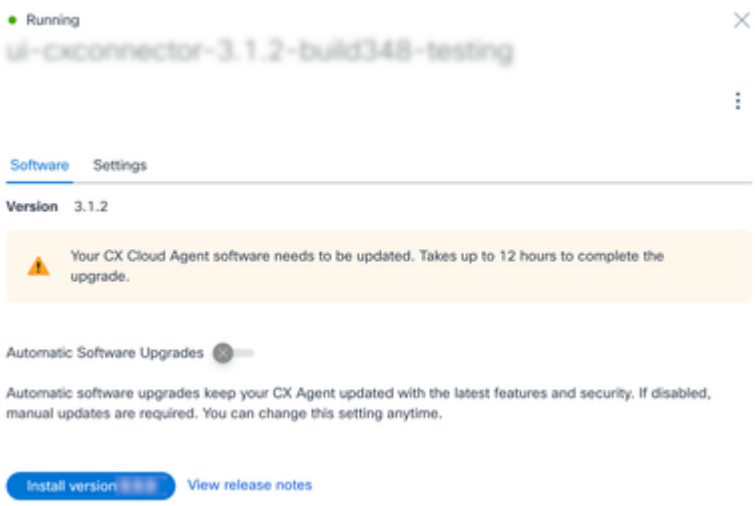
Page d'accueil de CX Cloud

2. Sélectionnez l'icône Centre d'administration. La fenêtre Sources de données s'ouvre.



Source de données

3. Cliquez sur une source de données d'agent CX. La fenêtre CX Agent details s'ouvre.



Installer la version

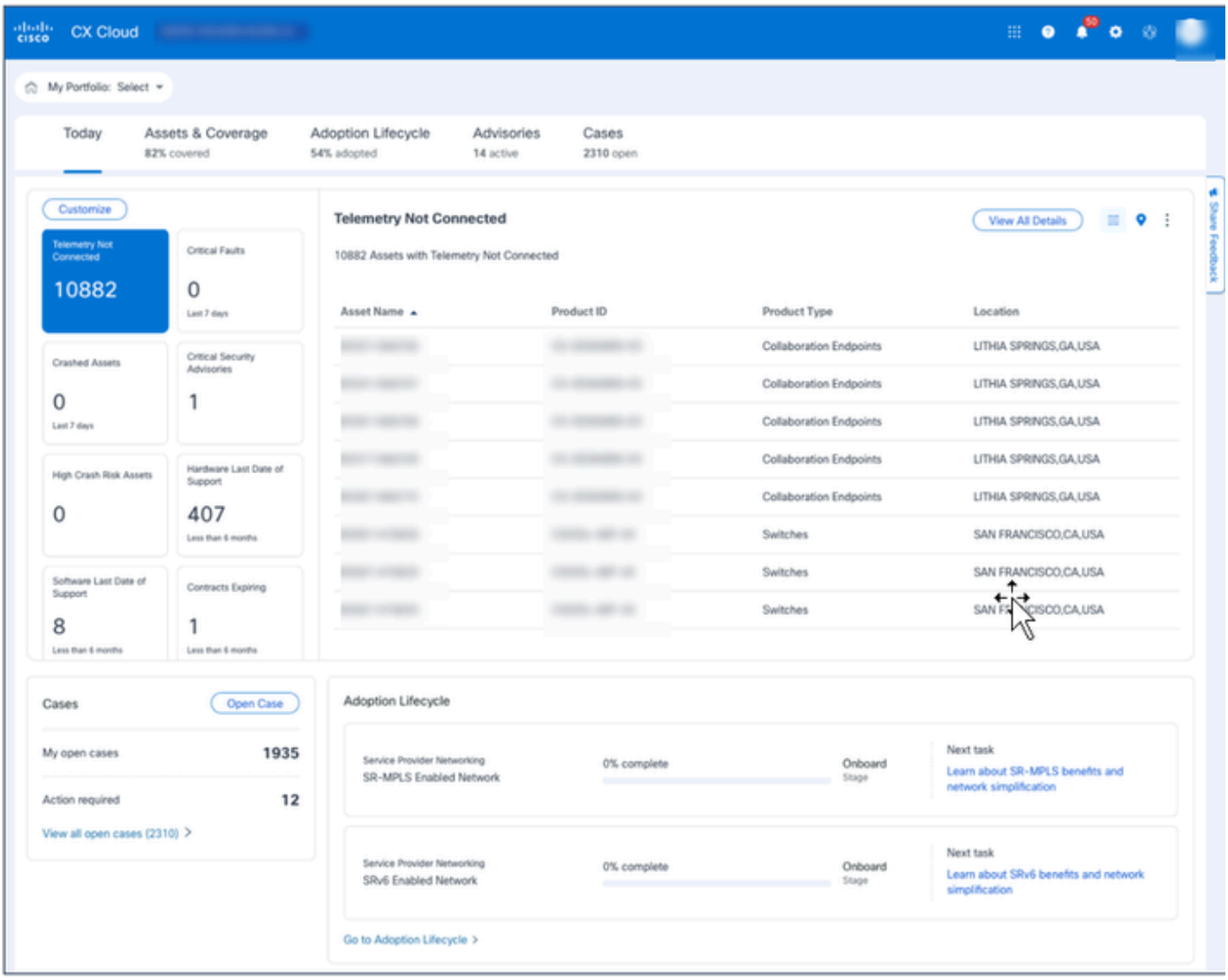
4. Cliquez sur l'onglet Logiciel.
5. Cliquez sur Installer la version.

Ajout d'un agent CX

Les clients peuvent ajouter jusqu'à 20 instances d'agent CX dans le cloud CX.

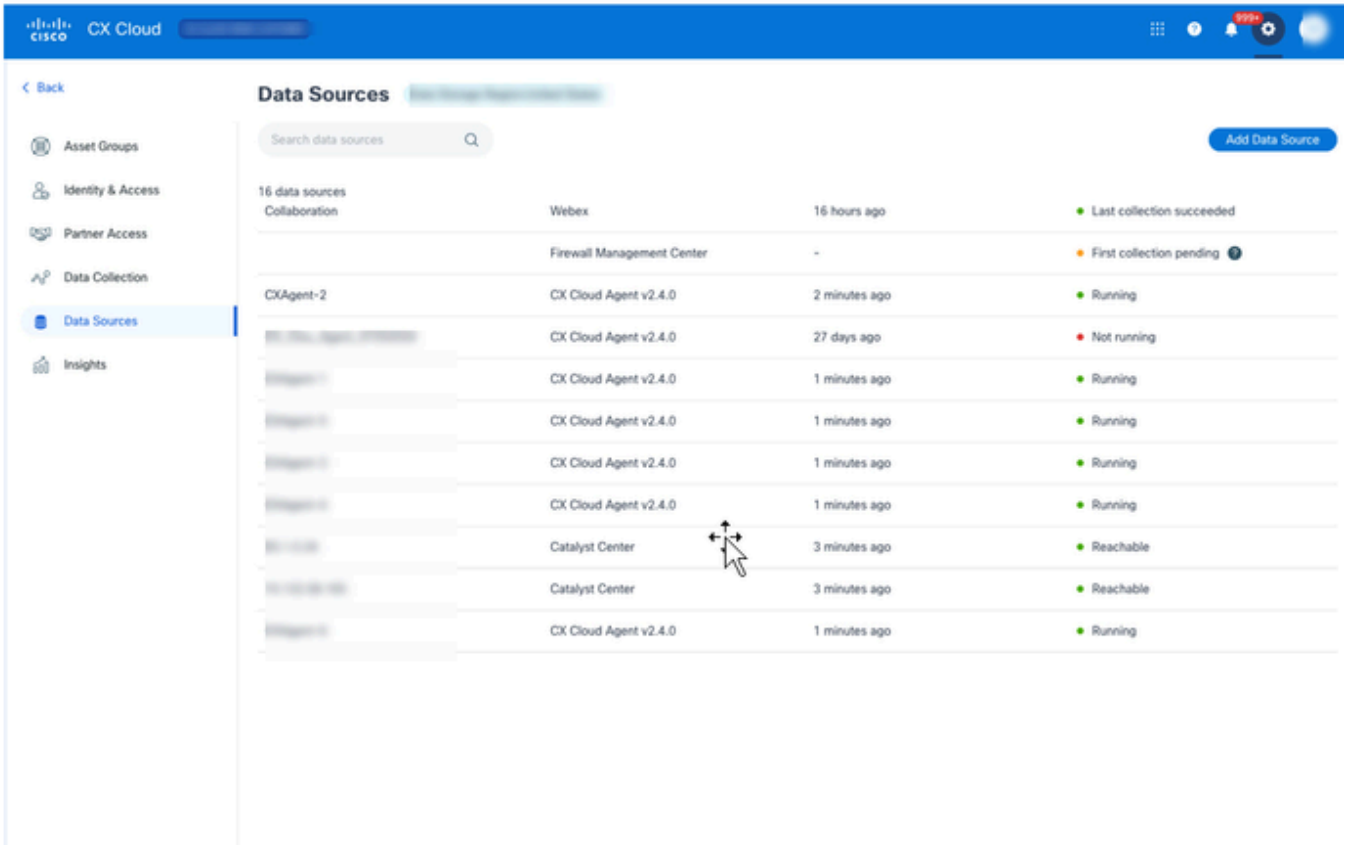
Pour ajouter un agent CX :

1. Connectez-vous à CX Cloud. La page d'accueil s'affiche.



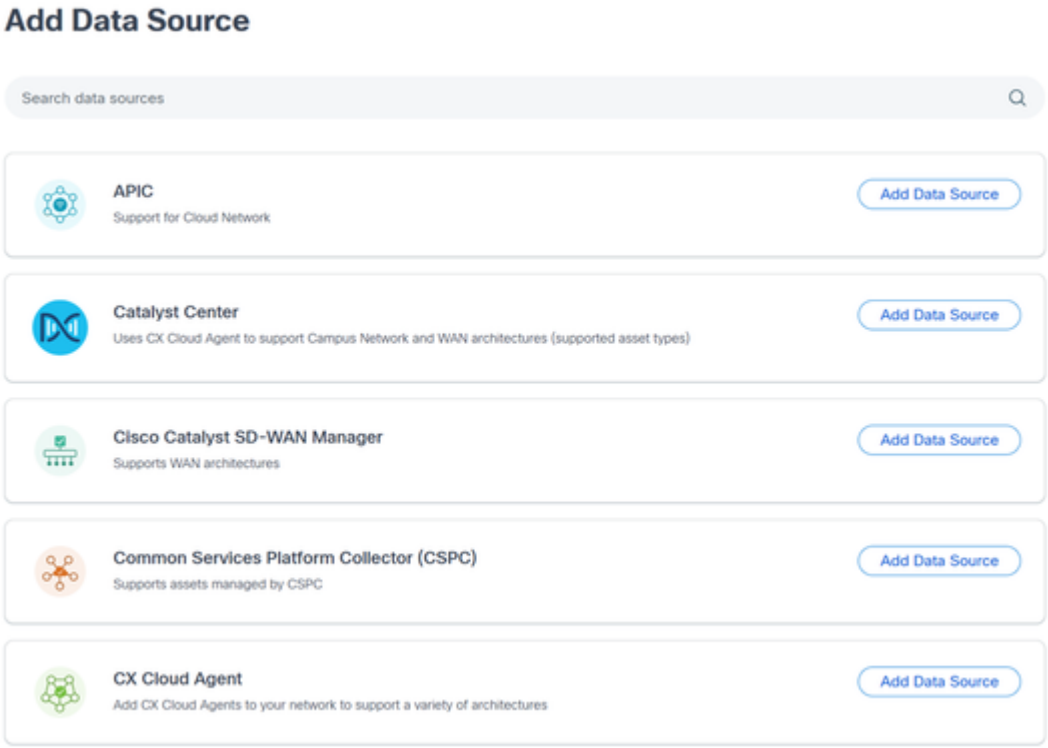
Page d'accueil de CX Cloud

2. Sélectionnez l'icône Centre d'administration. La fenêtre Sources de données s'ouvre.

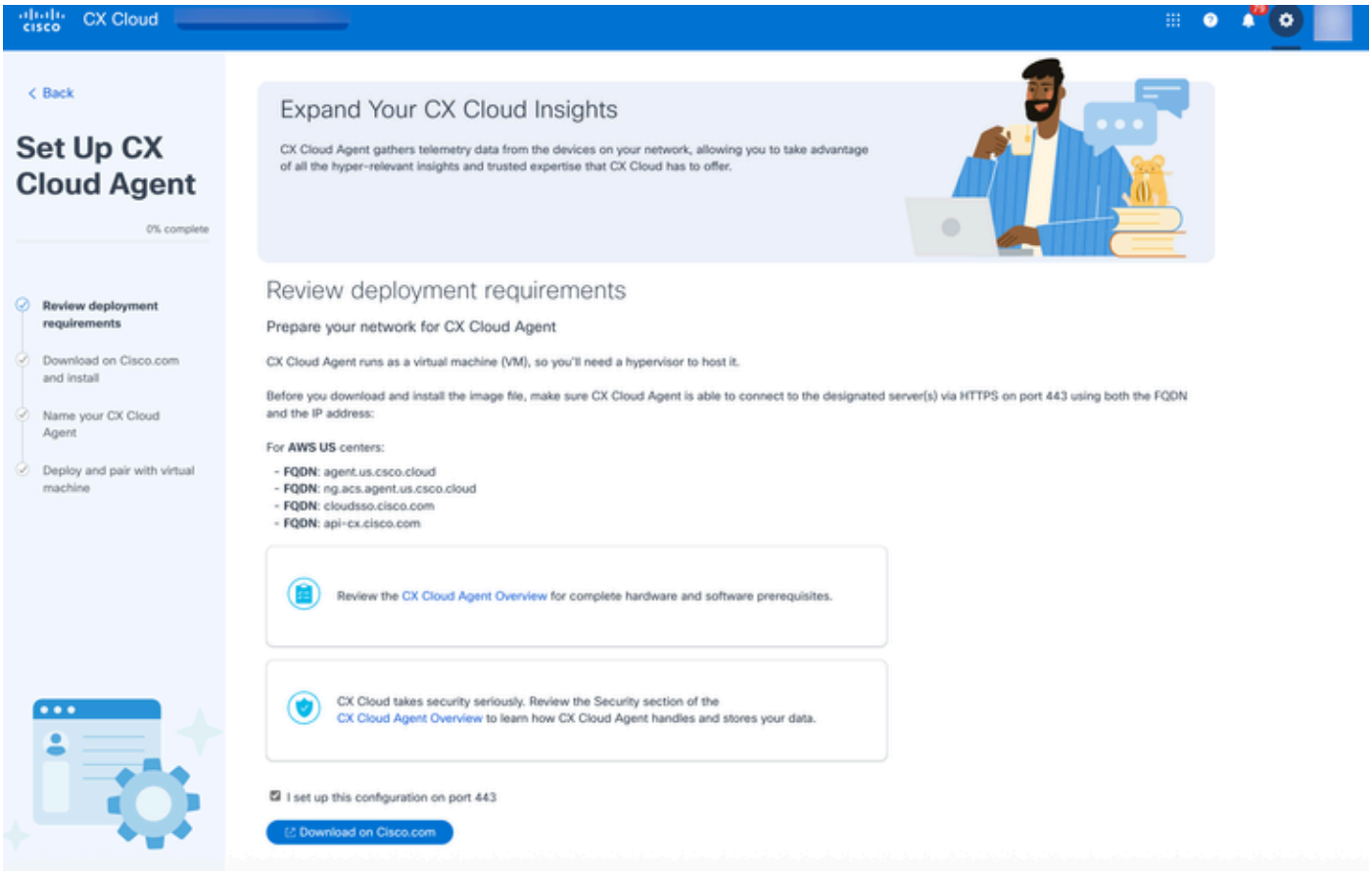


Source de données

3. Cliquez sur Ajouter une source de données. La page Ajouter une source de données s'ouvre.



4. Cliquez sur Ajouter une source de données dans l'option CX Cloud Agent. La fenêtre Set Up CX Agent s'ouvre.



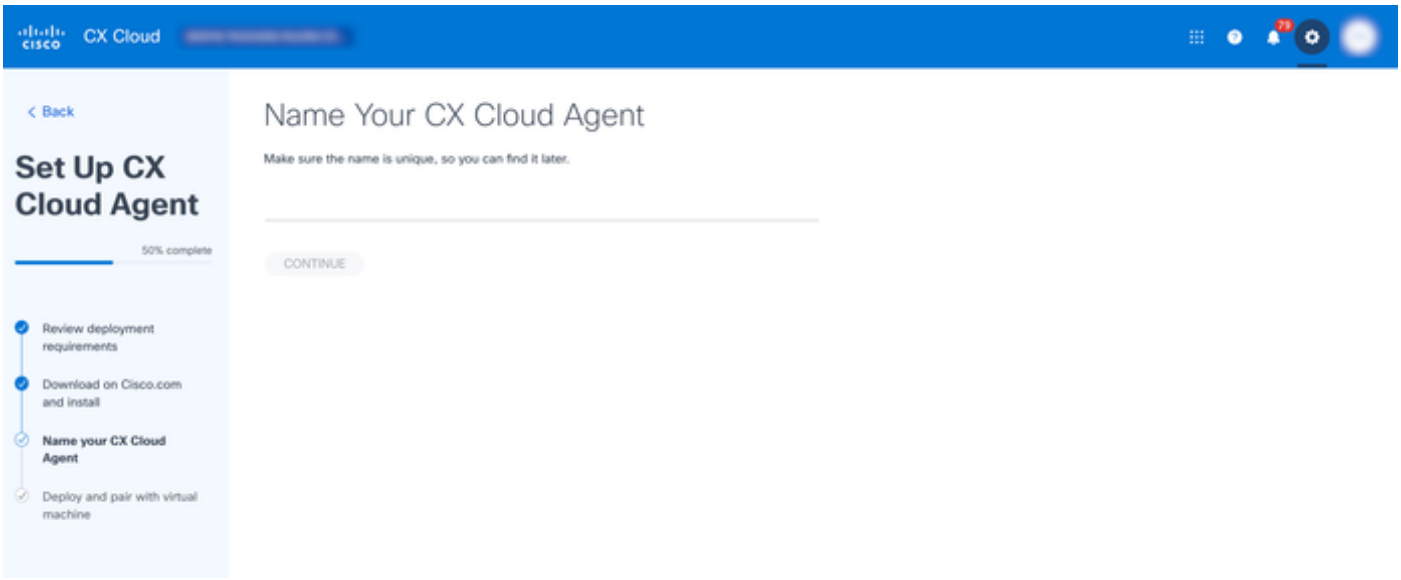
Ajout d'un agent CX

5. Consultez la section Vérifier les exigences de déploiement et activez la case à cocher Je configure cette configuration sur le port 443.
6. Cliquez sur Download sur Cisco.com. La fenêtre Téléchargement de logiciel s'ouvre dans un autre onglet.
7. Téléchargez le fichier « CX Agent v3.1.5 OVA ».

Remarque : un code d'appariement requis pour terminer la configuration de l'agent CX est généré après le déploiement de la machine virtuelle.

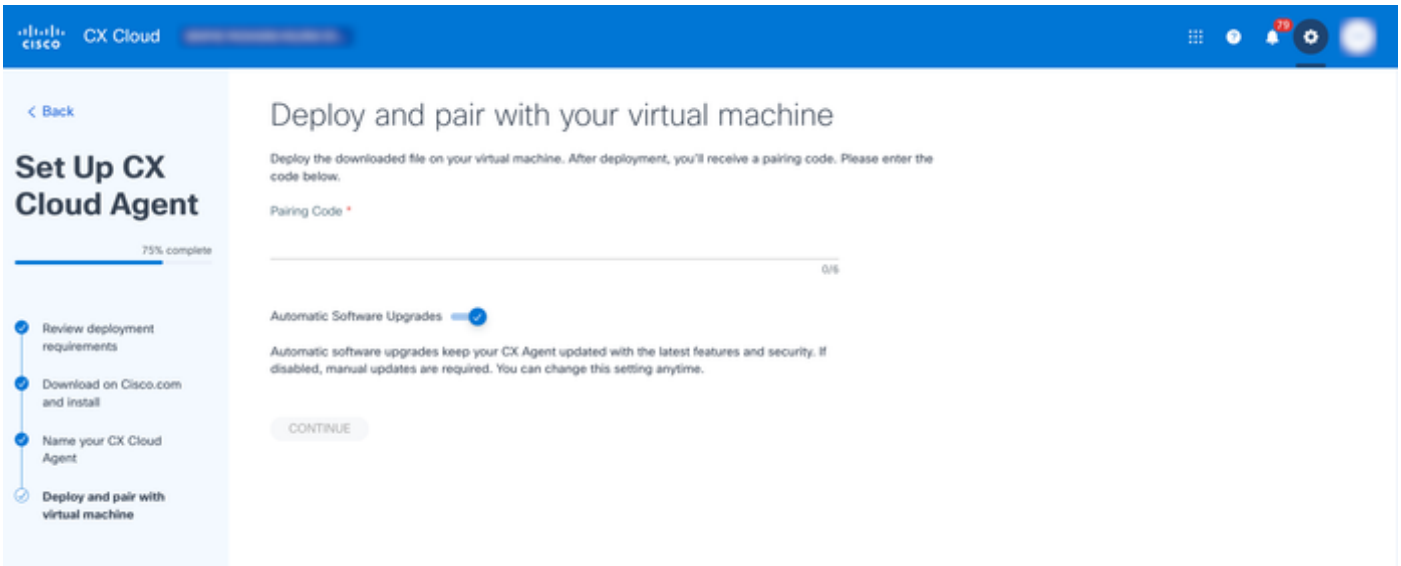
---

8. Saisissez le nom de l'agent CX dans le champ Name Your CX Cloud Agent.



Nom Agent CX

9. Cliquez sur Continuer. La fenêtre Déployer et associer à votre machine virtuelle s'affiche.



Code de jumelage

10. Entrez le code d'appariement reçu après le déploiement de la VM.

11. Cliquez sur Continuer. La progression de l'inscription s'affiche, suivie d'un message de confirmation.

Remarque : Répétez les étapes ci-dessus pour ajouter des instances d'agent CX supplémentaires en tant que source de données.

Configuration de CX Agent pour BCS/LCS

La nouvelle fonctionnalité de collecte convergente de Cisco rationalise la configuration de CX Agent v3.1 pour BCS/LCS, simplifiant ainsi l'expérience du client.

Les clients BCS/LCS peuvent visiter la communauté cloud CX pour en savoir plus sur l'intégration des utilisateurs et d'autres informations connexes.

Remarque : cette configuration est spécifique aux ingénieurs d'assistance Cisco chargés de la configuration du collecteur pour les clients BCS/LCS.

Conditions préalables

Les ingénieurs d'assistance disposant d'un accès Super User Administrator (SUA) et Administrator peuvent uniquement effectuer la configuration de l'agent CX pour BCS/LCS.

Configuration de l'agent CX

Pour configurer l'agent CX pour BCS/LCS, contactez l'ingénieur-conseil technique BCS/LCS qui vous a été affecté.

Configuration des fonctionnalités RADKit

CX Agent v3.1.5 fournit une configuration RADKit en option conçue pour améliorer la gestion et le dépannage à distance des périphériques Cisco dans le cloud CX. Lorsque cette option est activée, les utilisateurs autorisés peuvent effectuer des opérations à distance, telles que la capture de données, la configuration et les mises à niveau logicielles, en toute sécurité. Ces paramètres peuvent être activés ou désactivés à tout moment en fonction des besoins opérationnels du client.

Pour des détails complets sur RADKit, référez-vous à Cisco RADKit.

Intégration du client RADKit via CLI

Pour intégrer le service client RADKit, créez un compte administrateur et inscrivez-le en procédant comme suit :

Remarque : les étapes suivantes nécessitent un accès racine à la machine virtuelle de l'agent CX.

1. Ouvrez le terminal et Secure Shell (SSH) dans une machine virtuelle à l'aide des informations d'identification appropriées, par exemple :

```
ssh your_username@your_vm_ip
```

2. Exécutez la commande suivante pour activer la connectivité réseau :

```
kubectl get netpol deny-from-other-namespaces -o yaml >
/home/cxcadmin/deny-from-other-namespaces.yaml

kubectl delete netpol deny-from-other-namespaces
```

3. Sur l'ordinateur local, envoyez une requête POST au point de terminaison du gestionnaire pour créer un compte administrateur. Le corps de la demande doit inclure :

- admin_name (obligatoire) : Le nom d'utilisateur du compte administrateur
- email (facultatif) : Adresse e-mail du compte administrateur
- nom_complet (facultatif) : Le nom complet de l'administrateur
- description (facultatif) : Description du compte d'administrateur

L'exemple suivant montre comment envoyer cette demande à l'aide de cURL :

```
curl -X POST \

  http://<votre_vm_ip>:30100/radkitmanager/v1/createAdmin \

  -H "Content-Type : application/json" \

  -d'{

        "nom_admin" : "admin_user123",

        "e-mail" : "admin@example.com",

        "nom_complet" : "Utilisateur admin",

        "description" : "Compte administrateur pour la gestion du
système"

      }'
```

Une fois le compte administrateur créé, le serveur répond par un message de confirmation indiquant que le compte administrateur a été créé avec succès. Cette réponse inclut également un mot de passe temporaire qui doit être modifié lors de la connexion initiale. Toutefois, si le compte administrateur existe déjà, le serveur renvoie un code d'état 400 avec le message « Admin already created ».

4. Ouvrez le navigateur Web et accédez à l'interface utilisateur Web de RADKit : https://<ip_vm_your>:30101/.
5. Connectez-vous à l'aide du nom d'utilisateur de l'administrateur (admin_name) et du mot de passe temporaire fournis dans la réponse.

✎ Remarque : Lors de la connexion initiale, les utilisateurs sont invités à modifier le mot de passe. Suivez les instructions à l'écran pour définir un nouveau mot de passe.

---

6. Exécutez le client RADKit sur l'ordinateur local pour inscrire le service.
7. Après l'authentification, générez un mot de passe à usage unique en exécutant la commande suivante :

```
grant_service_otp()
```

8. Sur l'ordinateur local, envoyez une requête POST au point de terminaison du gestionnaire pour inscrire le service. Le corps de la demande doit inclure :

- OTP (obligatoire) : Chaîne de mot de passe à usage unique

L'exemple suivant montre comment envoyer cette demande à l'aide de cURL :

```
curl -X POST \

  http://<your_vm_ip>:30100/radkitmanager/v1/enrollService \

  -H "Content-Type : application/json" \

  -d'{

        "one_time_password" : "PROD : 1234-1234-1234"

      }'
```

Une fois l'inscription réussie, un message de confirmation s'affiche et les utilisateurs peuvent gérer le service RADKit à l'aide d'un compte administrateur.

Pour désactiver la connectivité réseau, exécutez la commande suivante :

```
kubectl apply -f /home/cxcadmin/deny-from-other-namespaces.yaml
```

Configuration du coffre-fort pour les agents CX existants

La fonction facultative de configuration du coffre-fort permet à CX Cloud de se connecter en toute sécurité à un service de coffre-fort pour accéder aux données sensibles, telles que les jetons et les listes d'inventaire, à l'aide des informations d'identification les plus récentes. Lorsqu'elle est activée, CX Cloud utilise automatiquement l'adresse et le jeton configurés. Ce paramètre peut être activé ou désactivé à tout moment. Actuellement, seule la configuration de coffre de HashiCorp est prise en charge.

Le coffre peut être configuré via l'interface de ligne de commande.

Intégration de CX Agent avec HashiCorp Vault via CLI

Cette section décrit la procédure de configuration de la connexion entre l'agent Cisco CX et une instance HashiCorp Vault. Cette intégration permet un stockage et une récupération sécurisés des informations d'identification des périphériques, améliorant ainsi la sécurité globale.

Conditions préalables

- Accès cxcroot à la machine virtuelle CX Agent



Remarque : Un dossier d'assistance doit être ouvert pour accéder aux utilisateurs cxroot et root.

- Une instance de coffre-fort en cours d'exécution et accessible

Intégration à HashiCorp Vault

- Pour activer l'intégration de coffre-fort, exécutez la commande suivante :

```
cxcli agent vault on
```

- Pour désactiver l'intégration du coffre-fort, exécutez la commande suivante :

```
cxcli agent vault off
```

- Pour vérifier l'état actuel de l'intégration au coffre-fort, exécutez la commande suivante :

```
état cxcli agent vault
```

Activation de l'intégration HashiCorp Vault

Pour activer l'intégration en chambre forte :

1. Connectez-vous à l'agent CX via SSH en utilisant le compte utilisateur cxcroot pour accéder à l'agent CX.
2. Basculez vers l'utilisateur racine pour élever les privilèges en exécutant la commande suivante :

```
sudo su
```

3. Exécutez la commande suivante pour vérifier l'état actuel de l'intégration du coffre :

```
root@cxcloudagent: /home/cxcroot# cxcli agent vault status
```

intégration vault désactivée

4. Exécutez la commande suivante pour activer l'intégration de coffre-fort :

```
cxcli agent vault on
```

5. Mettez à jour les champs suivants :

- Adresse du coffre
- Jeton racine de coffre-fort

6. Pour vérifier, vérifiez l'état de l'intégration avec le coffre-fort. Le message de réponse doit confirmer que l'intégration est activée :

```
root@cxcloudagent: /home/cxcroot# cxcli agent vault on
```

```
Saisissez l'adresse HashiCorp Vault :

Saisissez le jeton de coffre-fort HashiCorp :

intégration vault activée root@cxcloudagent: /home/cxcroot#
```

Désactivation de l'intégration HashiCorp Vault

Pour accéder à l'agent CX :

1. Connectez-vous à CX Agent via SSH à l'aide du compte utilisateur cxcroot.
2. Basculez vers l'utilisateur racine pour élever les privilèges en exécutant la commande suivante :

```
sudo su
```

3. Exécutez la commande suivante pour désactiver HashiCorp Vault Integration :

```
root@cxcloudagent: /home/cxcroot# cxcli agent vault off

intégration vault désactivée

root@cxcloudagent: /home/cxcroot# |
```

Schéma des identifiants de périphérique HashiCorp Vault

Schéma des informations d'identification Vault : Pour obtenir des informations détaillées sur les options disponibles et les champs pris en charge pour les informations d'identification des périphériques, reportez-vous au fichier « Schéma des informations d'identification du coffre-fort ».

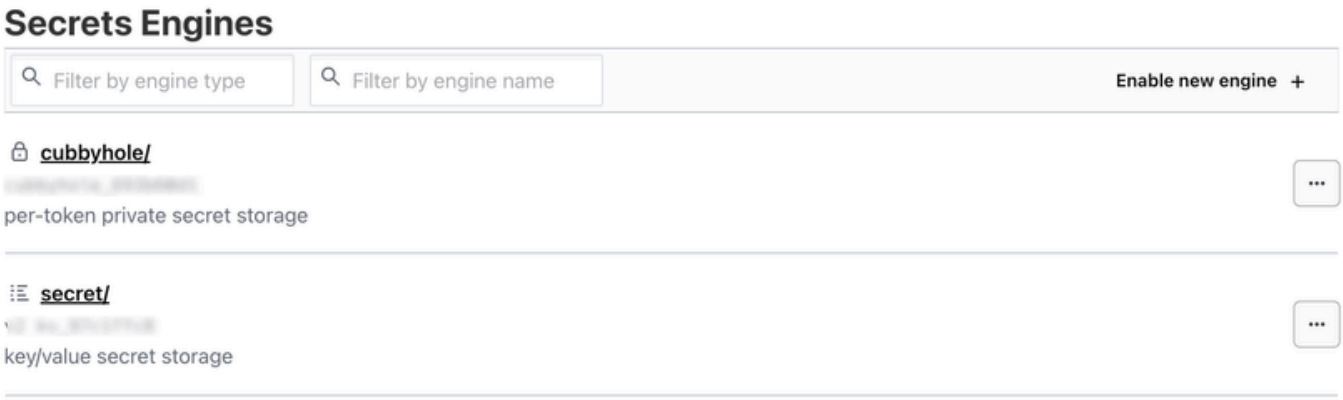
Exemple : Voici un exemple d'informations d'identification JSON basées sur le schéma :

```
{
"targetIp": "5.0.1.*",
"credentials": {
"snmpv3": {
"user": "cisco",
"authPassword": "*******",
"authAlgorithm": "MD5",
"privacyPassword": "*******",
"privacyAlgorithm": "AES-256"
},
"telnet": {
"user": "cisco",
"password": "*******",
"enableUser": "cisco",
"enablePassword": "*******"
}
}
}
```

Remarque : les utilisateurs peuvent spécifier plusieurs protocoles dans un seul fichier JSON d'informations d'identification. Cependant, évitez d'inclure des protocoles dupliqués de la même famille (par exemple, n'incluez pas SNMPv2c et SNMPv3 dans le même fichier d'informations d'identification).

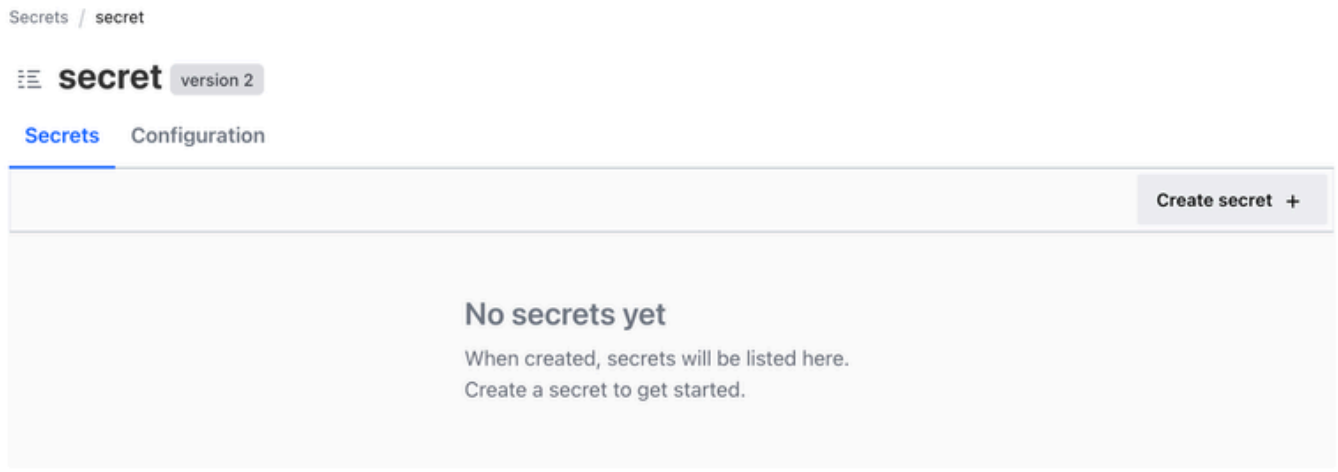
Configuration des identifiants de périphérique dans HashiCorp Vault (première fois)

1. Connectez-vous à une instance Vault.



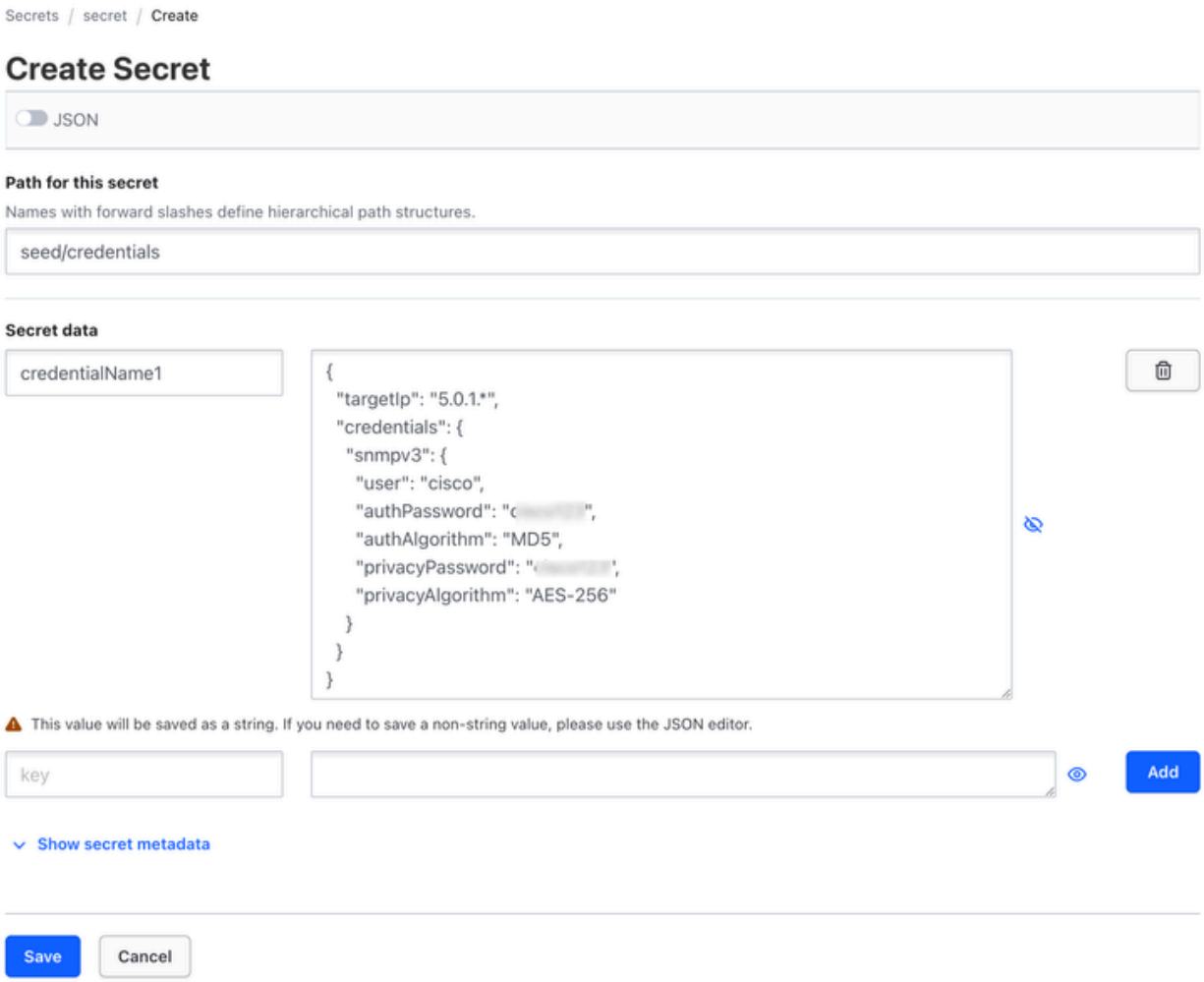
Secret

2. Créez un nouveau secret clé-valeur en utilisant le chemin suivant : secret/amorce/références.
3. Sélectionnez le moteur de stockage secret de valeur de clé (secret/).



Clé secrète de valeur

4. Cliquez sur Créer un secret. La fenêtre Create Secret s'affiche.

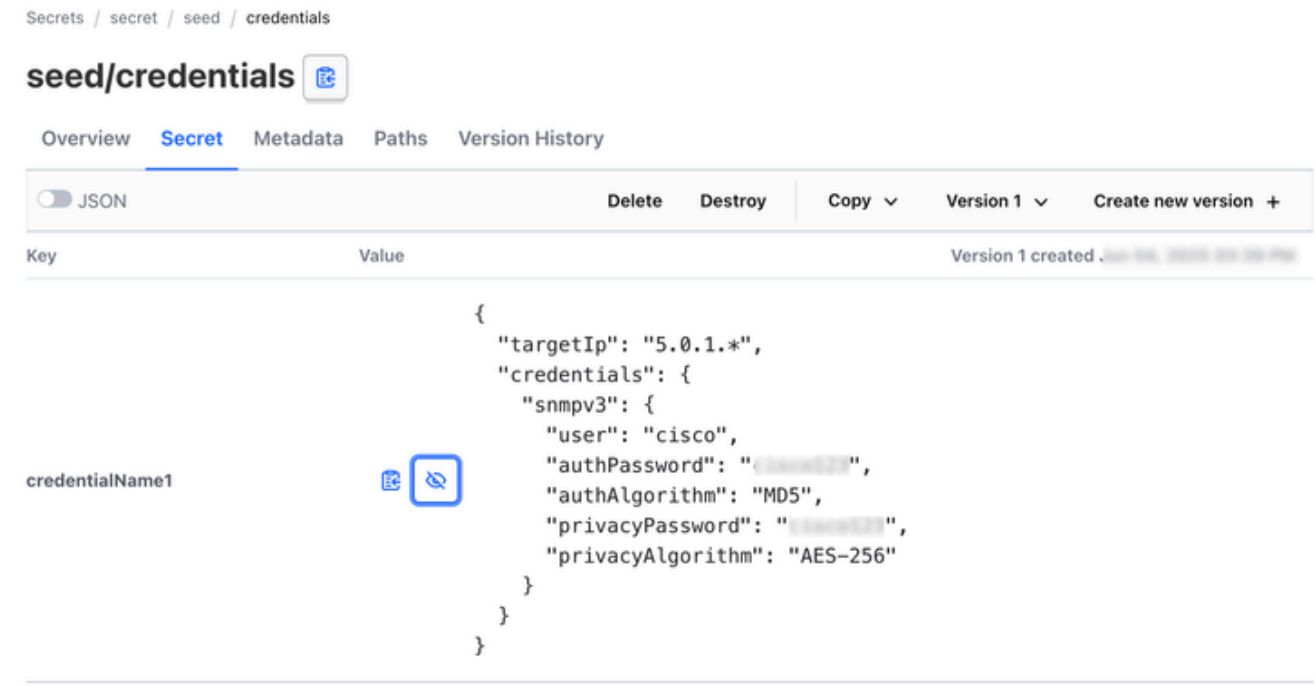


Secret client

5. Mettez à jour les champs suivants :

- Chemin d'accès du secret : amorce/références
- Données secrètes : collection de clés - secrets de valeur
- clé : nom d'identification unique personnalisé
- valeur: lettres de créance JSON

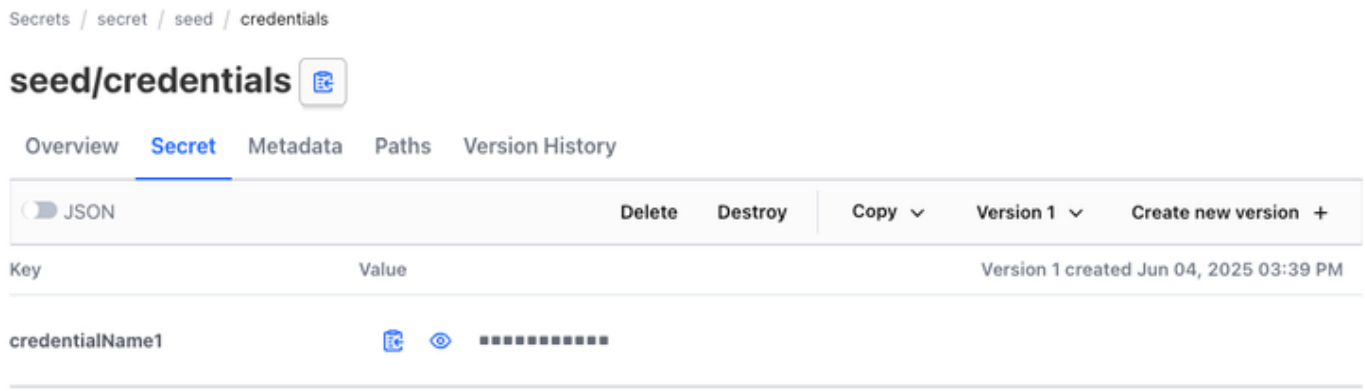
6. Cliquez sur Enregistrer. Le secret devrait maintenant être stocké dans le coffre-fort de HashiCorp.



Identifiants

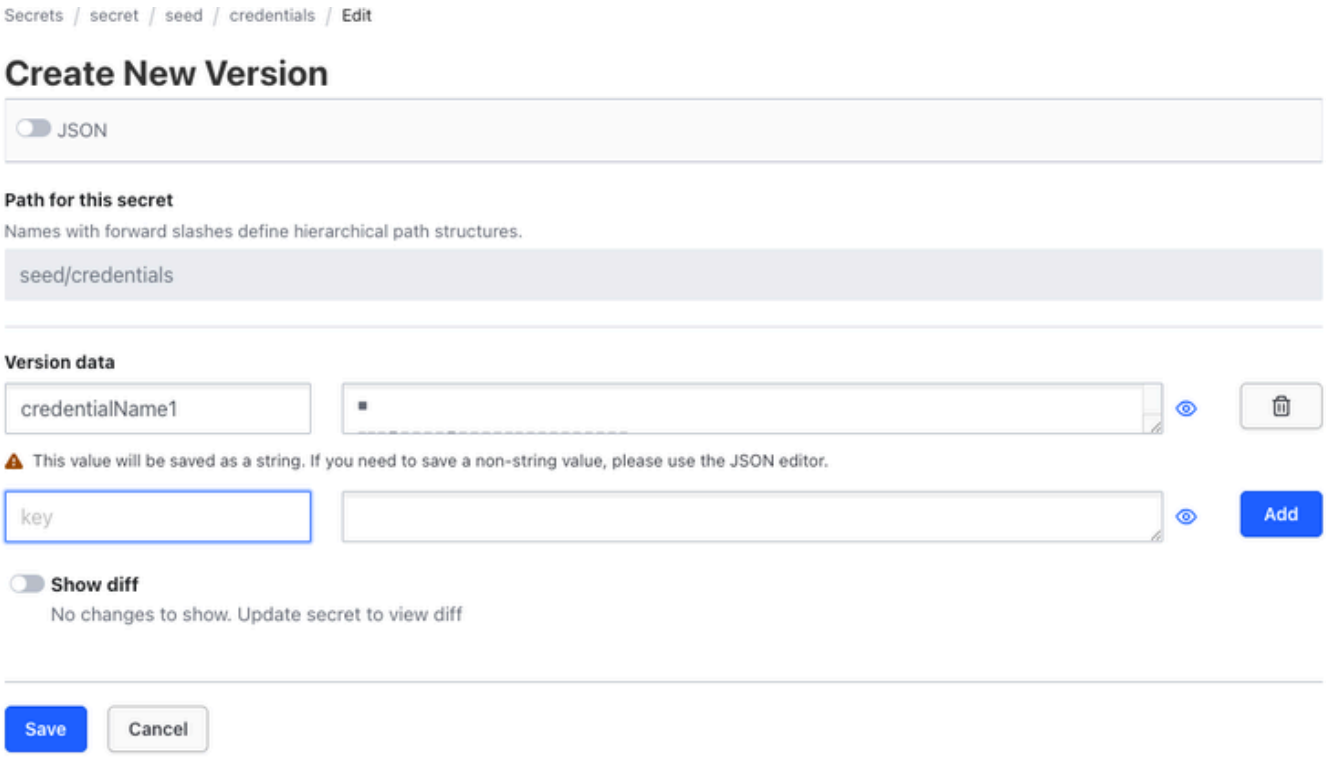
Ajout d'informations d'identification à HashiCorp Vault

1. Connectez-vous à une instance de coffre-fort HashiCorp.



Ajouter des identifiants

2. Accédez à la clé secrète « secret/amorce/informations d'identification » déjà créée.



Créer une version

3. Cliquez sur Créer une nouvelle version.

4. Ajoutez de nouveaux secrets en fournissant autant de paires clé-valeur que nécessaire.

5. Cliquez sur Enregistrer.

Fichier d'amorçage cloud CX avec informations d'identification par défaut

- Simplifier le fichier d'amorçage : Lorsque vous utilisez des informations d'identification configurées via Hashicorp vault, simplifiez le fichier de départ en omettant les informations sensibles
- Spécifiez uniquement l'adresse IP ou le nom d'hôte : Les utilisateurs ne peuvent transmettre que l'adresse IP ou le nom d'hôte dans le fichier d'amorçage, en laissant d'autres champs vides

```
5.0.1.2,,,,,,,,,,,,,,,,,,
5.0.1.3,,,,,,,,,,,,,,,,,,
5.0.1.4,,,,,,,,,,,,,,,,,,
```

IP ou nom d'hôte

- Utilisez les informations d'identification HashiCorp vault et Seed File : Fournir des informations d'identification pour certains périphériques dans le fichier d'amorçage tout en s'appuyant sur le coffre pour gérer les informations d'identification pour d'autres périphériques

```
5.0.1.1,snmpv3,,username,,,,,,,cliUser,cliPassword,,enablePassword,,,
25.0.1.2,snmpv2c,readOnlyPassword,,,,,,,sshv2,,cliUser,cliPassword,,,,
5.0.1.3,,,,,,,,,,,,,,,,,,,,
5.0.1.4,,,,,,,,,,,,,,,,,,,,
```

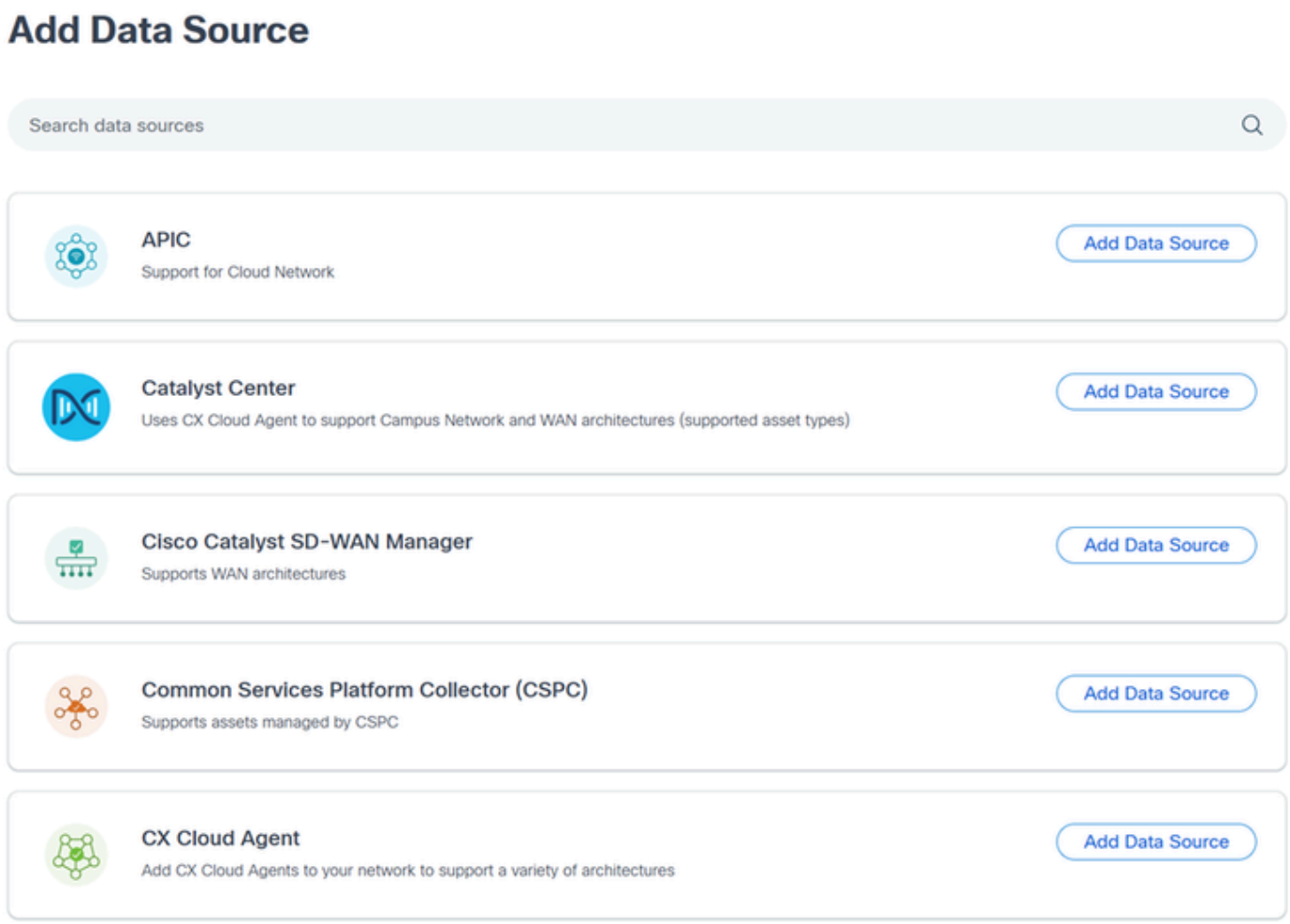
IP ou nom d'hôte

Ajout de Catalyst Center comme source de données

Les utilisateurs dotés du rôle d'utilisateur super administrateur peuvent ajouter la source de données du centre Catalyst.

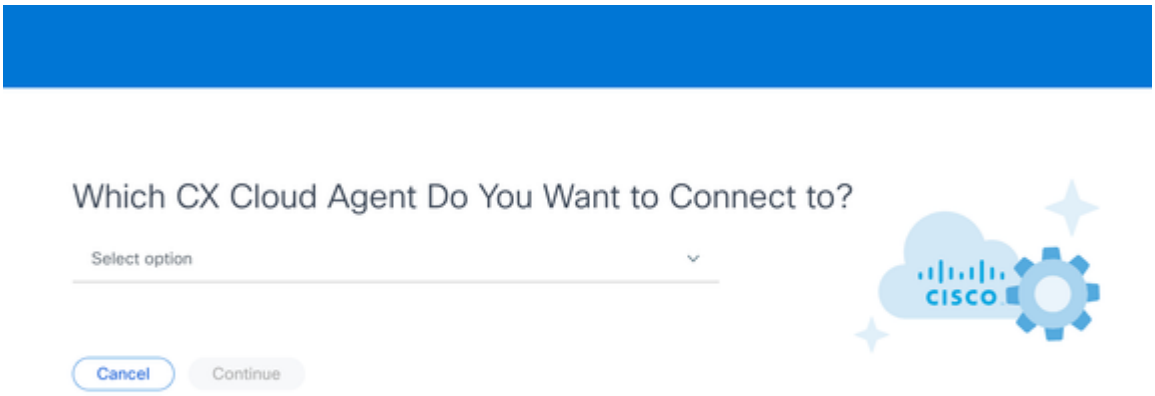
Pour ajouter Catalyst Center en tant que source de données :

1. Sélectionnez l'icône Centre d'administration. La fenêtre Sources de données s'ouvre.
2. Cliquez sur Ajouter une source de données. La page Ajouter une source de données s'affiche.



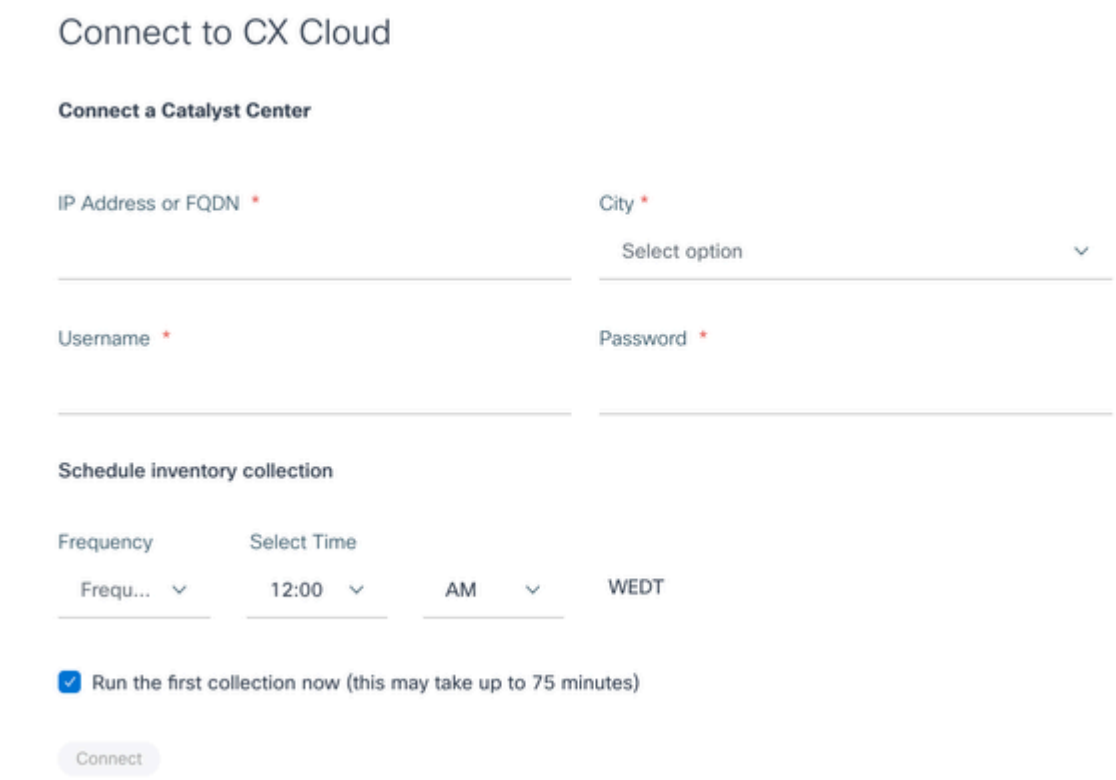
Centre Catalyst

3. Cliquez sur Add Data Source dans l'option Catalyst Center.



Sélectionner un agent CX

4. Sélectionnez l'agent CX dans la liste déroulante À quel agent CX voulez-vous vous connecter ?.
5. Cliquez sur Continue. La fenêtre Connect to CX Cloud s'affiche.



Fréquence

6. Saisissez les informations suivantes :

- Adresse IP virtuelle ou nom de domaine complet (c.-à-d. adresse IP de Catalyst Center)
- Ville (c'est-à-dire l'emplacement du centre Catalyst)
- Nom d’utilisateur
- Mot de passe

- Fréquence et durée de sélection pour indiquer la fréquence à laquelle l'agent CX doit effectuer des analyses de réseau dans les sections Planifier la collecte d'inventaire

Remarque : Activez la case à cocher Exécuter la première collection maintenant pour exécuter la collection maintenant.

7. Cliquez sur Connect. Une confirmation s'affiche avec l'adresse IP de Catalyst Center.

Ajout de sources de données BCS/LCS



Avertissement : Les sources de données suivantes concernent uniquement les ressources de transfert BCS.

Ajout de SolarWinds®



Remarque : Si vous devez ajouter la source de données SolarWinds®, contactez l'assistance Cisco pour obtenir de l'aide.

Les clients BCS/LCS peuvent désormais utiliser la fonctionnalité CX Agent pour une intégration externe avec SolarWinds®, offrant ainsi une plus grande transparence, une facilité de gestion améliorée et une expérience utilisateur améliorée grâce à une automatisation accrue. L'agent CX collecte l'inventaire et d'autres données requises pour générer divers rapports cohérents en termes de format, d'exhaustivité et d'exactitude des données par rapport aux rapports actuels générés par Operational Insights Collector. L'agent CX prend en charge l'intégration avec SolarWinds® en permettant à un client BCS/LCS de remplacer OIC par CX Agent pour collecter des données à partir de Solarwinds®.



Remarque : Cette fonctionnalité, y compris la source de données Solarwinds®, est disponible exclusivement pour les clients BCS/LCS.

L'agent CX doit être configuré dans le transfert BCS avant la première collecte ; sinon, les fichiers ne sont pas traités. Référez-vous à la section Configuration de l'agent CX pour BCS ou LCS pour plus d'informations sur la configuration du transfert BCS.



Remarques :
- Plusieurs collections de la même instance SolarWinds® remplacent les fichiers précédents (les téléchargements ultérieurs ont priorité).
- Plusieurs sources sont prises en charge, mais chaque instance SolarWinds® doit avoir une adresse IP et un ID d'appareil uniques.

Ajout d'EPNM

Les clients BCS/LCS peuvent désormais utiliser la fonctionnalité CX Agent pour une intégration externe avec EPNM (Evolved Programmable Network Manager). L'agent CX collecte l'inventaire et d'autres données nécessaires pour générer divers rapports qui sont cohérents en termes de format, d'exhaustivité et d'exactitude des données par rapport aux rapports actuels générés par OIC.

Ajout d'APIC

Les clients BCS/LCS peuvent désormais utiliser la fonctionnalité CX Agent pour une intégration externe avec le contrôleur APIC (Application Policy Infrastructure Controller). L'agent CX collecte l'inventaire et d'autres données nécessaires pour générer divers rapports qui sont cohérents en termes de format, d'exhaustivité et d'exactitude des données par rapport aux rapports actuels générés par OIC.

Ajout d'autres ressources comme sources de données

La collecte de données télémétriques a été étendue aux périphériques non gérés par Catalyst Center, ce qui permet aux utilisateurs d'afficher et d'interagir avec les données et analyses issues de la télémétrie pour un plus grand nombre de périphériques. Après la configuration initiale de CX Agent, les utilisateurs ont la possibilité de configurer CX Agent pour qu'il se connecte à 20 Catalyst Centers supplémentaires au sein de l'infrastructure surveillée par CX Cloud.

Les utilisateurs peuvent identifier les périphériques à intégrer dans le cloud CX en les identifiant de manière unique à l'aide d'un fichier d'amorçage ou en spécifiant une plage d'adresses IP, qui doit être analysée par l'agent CX. Les deux approches reposent sur le protocole SNMP (Simple Network Management Protocol) pour la détection et sur SSH (Secure Shell) pour la connectivité. Ils doivent être correctement configurés pour permettre une collecte télémétrique réussie.

Pour ajouter d'autres ressources en tant que sources de données, utilisez l'une des options suivantes :

- Télécharger un fichier de départ à l'aide d'un modèle de fichier de départ
- Fournir une plage d'adresses IP

Protocoles de détection

La détection directe des périphériques basée sur des fichiers d'amorce et la détection basée sur la plage d'adresses IP utilisent SNMP comme protocole de détection. Il existe différentes versions de SNMP, mais CX Agent prend en charge SNMPv2c et SNMPv3 et l'une ou les deux versions peuvent être configurées. Les mêmes informations, décrites ci-dessous en détail, doivent être fournies par l'utilisateur pour terminer la configuration et activer la connectivité entre le périphérique géré par SNMP et le gestionnaire de service SNMP.

SNMPv2c et SNMPv3 diffèrent en termes de sécurité et de modèle de configuration à distance. SNMPV3 utilise un système de sécurité cryptographique amélioré prenant en charge le cryptage SHA pour authentifier les messages et garantir leur confidentialité. Il est recommandé d'utiliser SNMPv3 sur tous les réseaux publics et Internet afin de se protéger contre les risques et les

menaces de sécurité. Sur CX Cloud, il est préférable que SNMPv3 soit configuré et non SNMPv2c, sauf pour les périphériques hérités plus anciens qui ne prennent pas en charge SNMPv3. Si les deux versions de SNMP sont configurées par l'utilisateur, l'agent CX tente, par défaut, de communiquer avec chaque périphérique respectif à l'aide de SNMPv3 et revient à SNMPv2c si la communication ne peut pas être négociée avec succès.

Protocoles de connectivité

Dans le cadre de la configuration de la connectivité directe des périphériques, les utilisateurs doivent spécifier les détails du protocole de connectivité des périphériques : SSH (ou Telnet). SSHv2 doit être utilisé, sauf dans le cas de ressources héritées individuelles qui ne disposent pas de la prise en charge intégrée appropriée. Sachez que le protocole SSHv1 présente des vulnérabilités fondamentales. En l'absence de sécurité supplémentaire, les données de télémétrie et les ressources sous-jacentes peuvent être compromises en raison de ces vulnérabilités lors de l'utilisation de SSHv1. Telnet n'est pas non plus sécurisé. Les informations d'identification (par exemple, les noms d'utilisateur et les mots de passe) soumises via Telnet ne sont pas chiffrées et sont donc vulnérables aux compromissions, en l'absence d'une sécurité supplémentaire.

Limitations du traitement de télémétrie pour les périphériques

Les limitations suivantes s'appliquent au traitement des données de télémétrie pour les périphériques :

- Certains périphériques peuvent apparaître comme accessibles dans le Résumé de la collecte mais ne sont pas visibles dans la page Ressources cloud CX.
- Si un périphérique du fichier d'amorce ou des collections de plages IP fait également partie de l'inventaire Catalyst Center, le périphérique n'est signalé qu'une seule fois pour l'entrée Catalyst Center. Les périphériques respectifs dans le fichier de départ ou l'entrée de plage IP sont ignorés pour éviter la duplication.
- Les téléphones IP Cisco ne sont pas pris en charge dans CX Cloud pour la collecte de données par CX Agent. Par conséquent, les téléphones IP Cisco ne s'affichent pas dans la liste des ressources.

Ajout d'autres ressources à l'aide d'un fichier initial

Un fichier d'amorçage est un fichier .csv dans lequel chaque ligne représente un enregistrement de données système. Dans un fichier d'amorçage, chaque enregistrement de fichier d'amorçage correspond à un périphérique unique à partir duquel la télémétrie doit être collectée par l'agent CX. Tous les messages d'erreur ou d'information pour chaque entrée de périphérique du fichier de départ importé sont capturés dans les détails du journal des travaux. Tous les périphériques d'un fichier d'amorçage sont considérés comme des périphériques gérés, même s'ils sont inaccessibles au moment de la configuration initiale. Dans le cas où un nouveau fichier d'amorce est téléchargé pour remplacer un précédent, la date du dernier téléchargement est affichée dans CX Cloud.

L'agent CX tente de se connecter aux périphériques, mais peut ne pas être en mesure de traiter

chacun d'eux pour les afficher dans les pages Ressources dans les cas où il n'est pas en mesure de déterminer les PID ou les numéros de série.

Toute ligne du fichier de départ commençant par un point-virgule est ignorée. La ligne d'en-tête du fichier d'amorce commence par un point-virgule et peut être conservée telle quelle (option recommandée) ou supprimée lors de la création du fichier d'amorce client.

Les utilisateurs peuvent télécharger un fichier d'amorçage CSPC (Common Services Platform Collector) de la même manière qu'un fichier d'amorçage cloud CX standard, et tout reformatage requis est géré dans le cloud CX.

Pour CX Agent v3.1.5 et versions ultérieures, les clients peuvent télécharger des fichiers d'amorçage au format CSPC ou CX ; seul le fichier d'amorçage au format CX est pris en charge pour les versions antérieures de l'agent CX.

Il est important que le format de l'exemple de fichier d'amorce, y compris les en-têtes de colonne, ne soit en aucune façon modifié.

Le tableau suivant identifie toutes les colonnes du fichier d'amorce nécessaires et les données qui doivent être incluses dans chaque colonne.

Colonne du fichier de démarrage	En-tête / Identificateur de colonne	Objet de la colonne
A	Adresse IP ou nom d'hôte	Fournissez une adresse IP ou un nom d'hôte valide et unique pour le périphérique.
B	Version du protocole SNMP	Le protocole SNMP est requis par l'agent CX et est utilisé pour la détection des périphériques sur le réseau du client. Les valeurs peuvent être snmpv2c ou snmpv3, mais snmpv3 est recommandé pour des raisons de sécurité.
C	snmpRo : Obligatoire si col#=3 sélectionné comme 'snmpv2c'	Si la variante héritée de SNMPv2 est sélectionnée pour un périphérique spécifique, alors les informations d'identification snmpRO (lecture seule) pour la collection SNMP du périphérique doivent être spécifiées. Sinon, l'entrée peut être vide.
D	snmpv3NomUtilisateur : Obligatoire si col#=3 sélectionné comme	Si SNMPv3 est sélectionné pour communiquer avec un périphérique spécifique, le nom d'utilisateur de connexion correspondant doit

Colonne du fichier de démarrage	En-tête / Identificateur de colonne	Objet de la colonne
	'snmpv3'	être fourni.
E	snmpv3AuthAlgorithm : Les valeurs peuvent être MD5 ou SHA	Le protocole SNMPv3 autorise l'authentification via l'algorithme MD5 (Message Digest) ou SHA (Secure Hash Algorithm). Si le périphérique est configuré avec une authentification sécurisée, l'algorithme d'authentification correspondant doit être fourni.  Remarque : MD5 est considéré comme non sécurisé et SHA peut être utilisé sur tous les périphériques qui le prennent en charge.
F	snmpv3AuthPassword : mot de passe	Si un algorithme de chiffrement MD5 ou SHA est configuré sur le périphérique, le mot de passe d'authentification approprié doit être fourni pour l'accès au périphérique.
G	snmpv3PrivAlgorithm : Les valeurs possibles sont DES , 3DES, AES-128, AES-192, AES-256	Si le périphérique est configuré avec l'algorithme de confidentialité SNMPv3 (cet algorithme est utilisé pour chiffrer la réponse), l'algorithme correspondant doit être fourni.  Remarque : Les clés 56 bits utilisées par la norme DES (Data Encryption Standard) sont considérées comme trop courtes pour assurer la sécurité cryptographique, et la norme 3DES (Triple Data Encryption Standard) peut être utilisée sur tous les périphériques qui la prennent en charge.
H	snmpv3PrivPassword : mot de passe	Si l'algorithme de confidentialité SNMPv3 est configuré sur le périphérique, son mot de passe de confidentialité respectif doit être

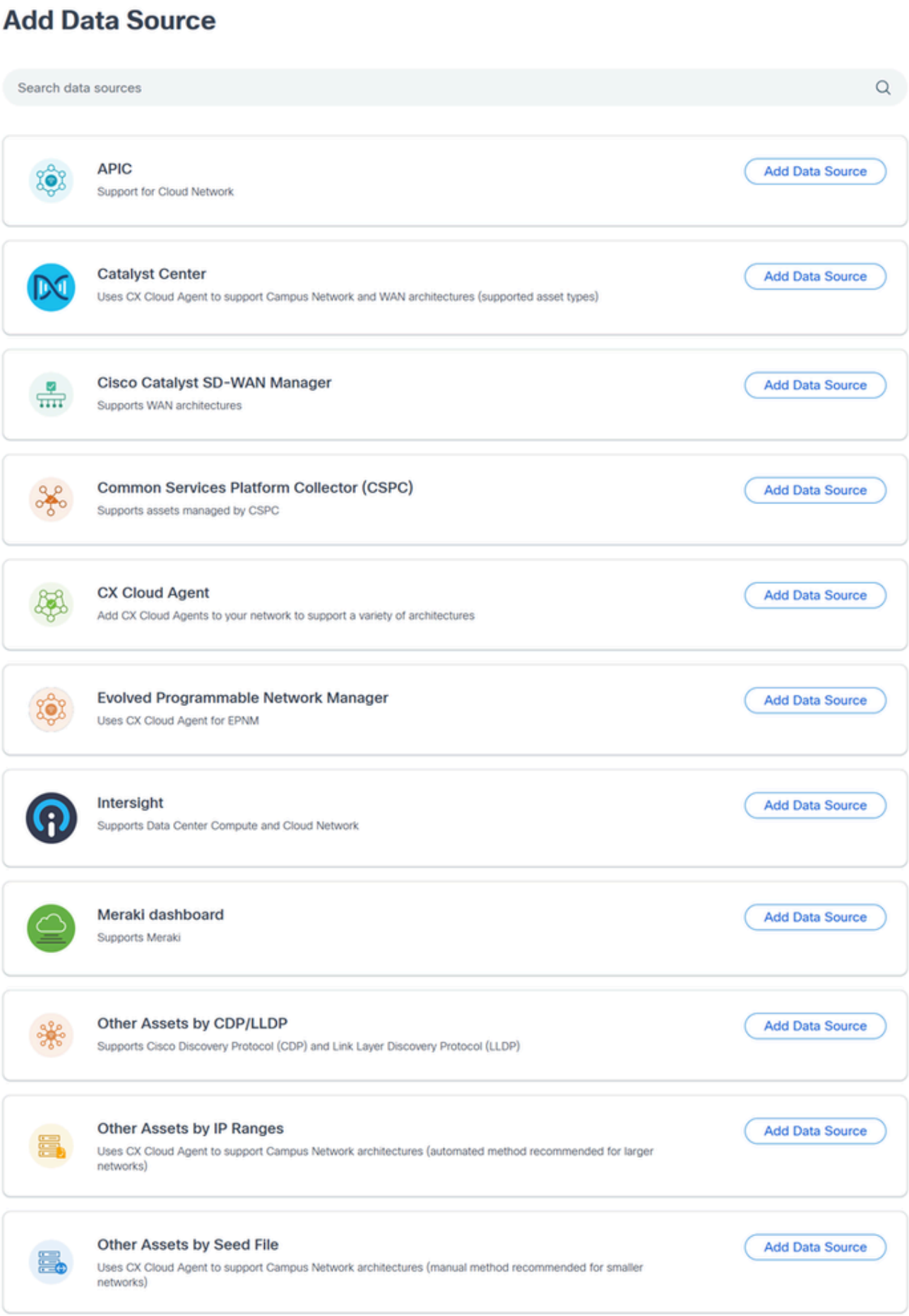
Colonne du fichier de démarrage	En-tête / Identificateur de colonne	Objet de la colonne
		fourni pour la connexion du périphérique.
I	snmpv3EngineId : ID de moteur, ID unique représentant le périphérique, spécifier l'ID de moteur si configuré manuellement sur le périphérique	L'ID de moteur SNMPv3 est un ID unique représentant chaque périphérique. Cet ID de moteur est envoyé comme référence lors de la collecte des jeux de données SNMP par l'agent CX. Si le client configure l'ID de moteur manuellement, alors l'ID de moteur respectif doit être fourni.
J	cliProtocol : les valeurs peuvent être 'telnet', 'sshv1', 'sshv2'. Si vide, peut être défini sur « sshv2 » par défaut	L'interface de ligne de commande (CLI) est conçue pour interagir directement avec le périphérique. CX Agent utilise ce protocole pour la collecte CLI d'un périphérique spécifique. Ces données de collecte CLI sont utilisées pour les rapports sur les ressources et autres informations dans le cloud CX. SSHv2 est recommandé ; En l'absence d'autres mesures de sécurité réseau, les protocoles SSHv1 et Telnet ne fournissent pas en eux-mêmes une sécurité de transport adéquate.
K	cliPort : Numéro de port du protocole CLI	Si un protocole CLI est sélectionné, son numéro de port respectif doit être fourni. Par exemple, 22 pour SSH et 23 pour Telnet.
L	cliUser : Nom d'utilisateur CLI (nom d'utilisateur/mot de passe CLI ou LES DEUX peuvent être fournis, MAIS les deux colonnes (col#=12 et col#=13) ne peuvent pas être vides.)	Le nom d'utilisateur CLI correspondant du périphérique doit être fourni. Il est utilisé par CX Cloud Agent au moment de la connexion au périphérique lors de la collecte CLI.
L	Mot de passe cli : Mot de passe utilisateur CLI (le nom d'utilisateur/mot de passe CLI ou les DEUX peuvent	Le mot de passe CLI correspondant du périphérique doit être fourni. Il est utilisé par l'agent CX au moment de la connexion au périphérique pendant la collecte de l'interface

Colonne du fichier de démarrage	En-tête / Identificateur de colonne	Objet de la colonne
	être fournis, MAIS les deux colonnes (col#=12 et col#=13) ne peuvent pas être vides.)	de ligne de commande.
n	cliEnableUser	Si enable est configuré sur le périphérique, la valeur enableUsername du périphérique doit être fournie.
O	cliEnablePassword	Si enable est configuré sur le périphérique, la valeur enablePassword du périphérique doit être fournie.
P	Assistance future (aucune entrée requise)	Réservé pour une utilisation ultérieure
Q	Assistance future (aucune entrée requise)	Réservé pour une utilisation ultérieure
R	Assistance future (aucune entrée requise)	Réservé pour une utilisation ultérieure
S	Assistance future (aucune entrée requise)	Réservé pour une utilisation ultérieure

Ajout d'autres ressources à l'aide d'un nouveau fichier de démarrage

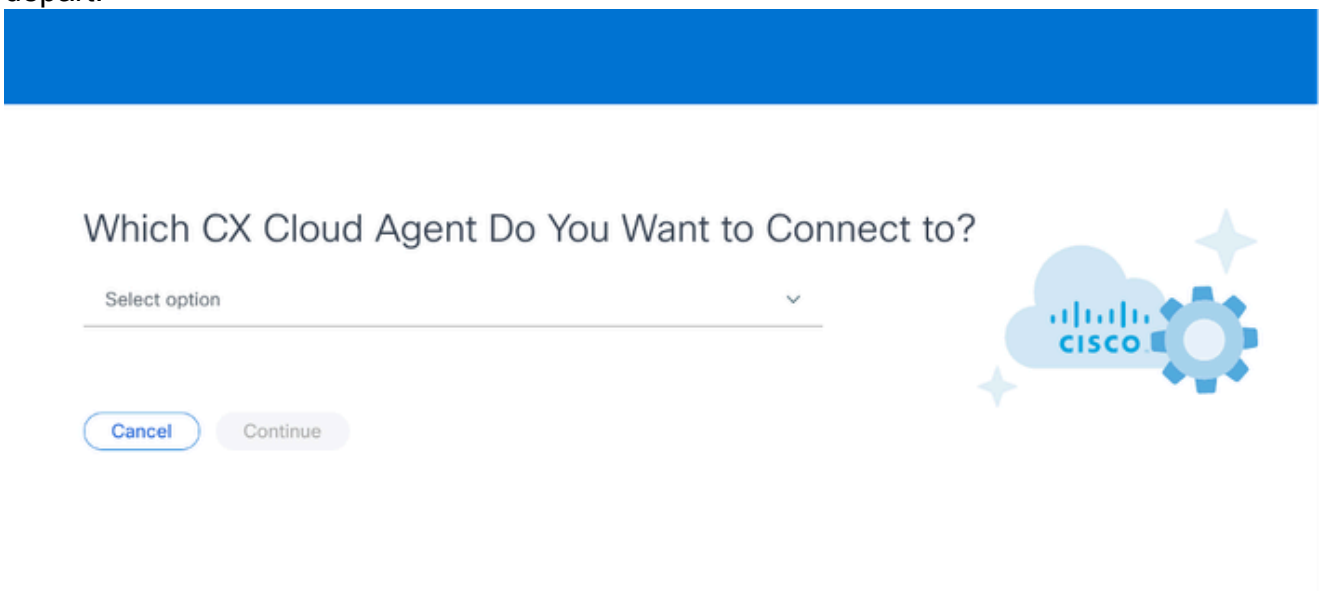
Pour ajouter d'autres ressources à l'aide d'un nouveau fichier de démarrage :

1. Cliquez sur Ajouter une source de données dans la fenêtre Centre d'administration > Sources de données.



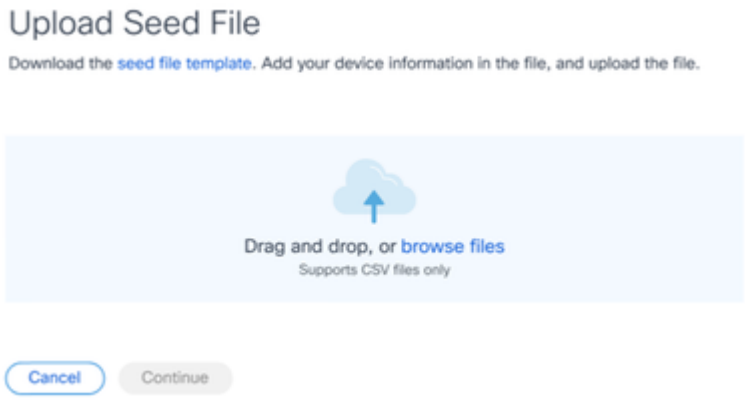
Autres actifs par fichier de démarrage

2. Cliquez sur Ajouter une source de données dans l'option Autres ressources par fichier de départ.



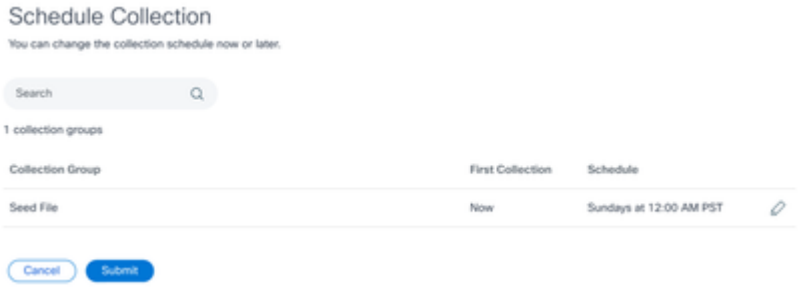
Sélectionner un agent CX

3. Sélectionnez l'agent CX dans la liste déroulante Quel agent cloud CX voulez-vous connecter.
4. Cliquez sur Continue. La page Charger le fichier de démarrage s'affiche.



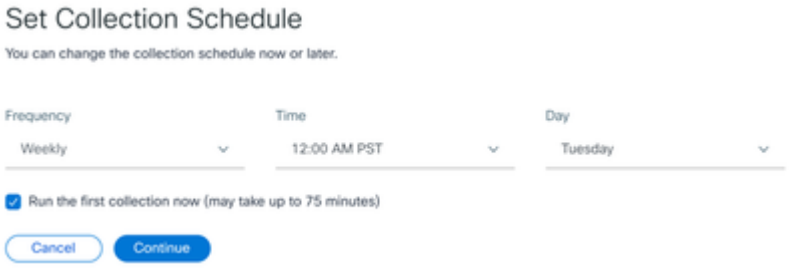
Charger le fichier de démarrage

5. Cliquez sur le modèle de fichier de départ hyperlié pour télécharger le modèle.
6. Saisissez ou importez manuellement des données dans le fichier. Une fois terminé, enregistrez le modèle en tant que fichier .csv pour importer le fichier dans CX Agent.
7. Faites glisser et déposez ou cliquez sur parcourir les fichiers pour télécharger le fichier .csv.
8. Une fois le fichier téléchargé, cliquez sur Continue. La page Schedule Collection s'affiche.



Planifier la collecte

9. Cliquez sur l'icône Edit. La page Définir la planification de la collecte s'affiche.



Définir la planification de collecte

10. Sélectionnez une option dans les listes déroulantes suivantes :
    - Fréquence
    - Heure
    - Jour
11. Activez la case à cocher Exécuter la première collection maintenant pour exécuter la collection.

Remarque : Avant que la configuration initiale de CX Cloud ne soit terminée, CX Cloud Agent doit effectuer la première collecte télémétrique en traitant le fichier d'amorce et en établissant la connexion avec tous les périphériques identifiés. La collecte peut être lancée à la demande ou exécutée selon un calendrier défini ici. Les utilisateurs peuvent établir la première connexion de télémétrie en cochant la case Exécuter la première collecte maintenant. Selon le nombre d'entrées spécifié dans le fichier de départ et d'autres facteurs, ce processus peut prendre un temps considérable.

---

12. Cliquez sur Continue. La page Schedule Collection s'affiche à nouveau.
13. Cliquez sur Submit. La fenêtre Sources de données s'ouvre et affiche un message de confirmation.

Ajout d'autres ressources à l'aide d'un fichier de démarrage modifié

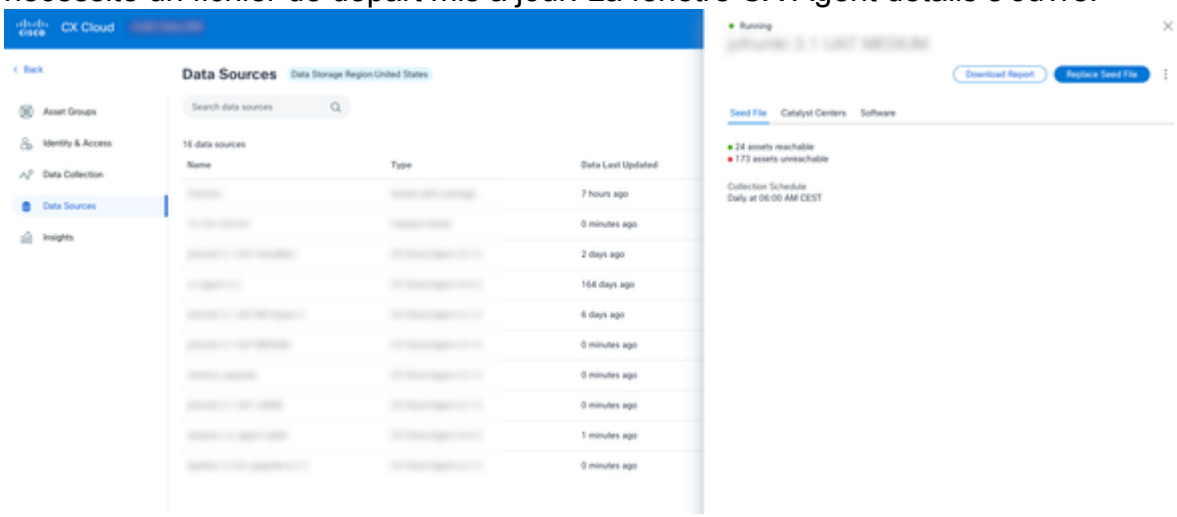
Pour ajouter, modifier ou supprimer des périphériques à l'aide du fichier d'amorçage actuel :

1. Ouvrez le fichier d'amorçage précédemment créé, apportez les modifications nécessaires et enregistrez le fichier.

Remarque : Pour ajouter des éléments au fichier d'amorçage, ajoutez-les au fichier d'amorçage précédemment créé et rechargez le fichier. Cette opération est nécessaire car le téléchargement d'un nouveau fichier d'amorce remplace le fichier d'amorce actuel. Seul le dernier fichier de départ téléchargé est utilisé pour la détection et la collecte.

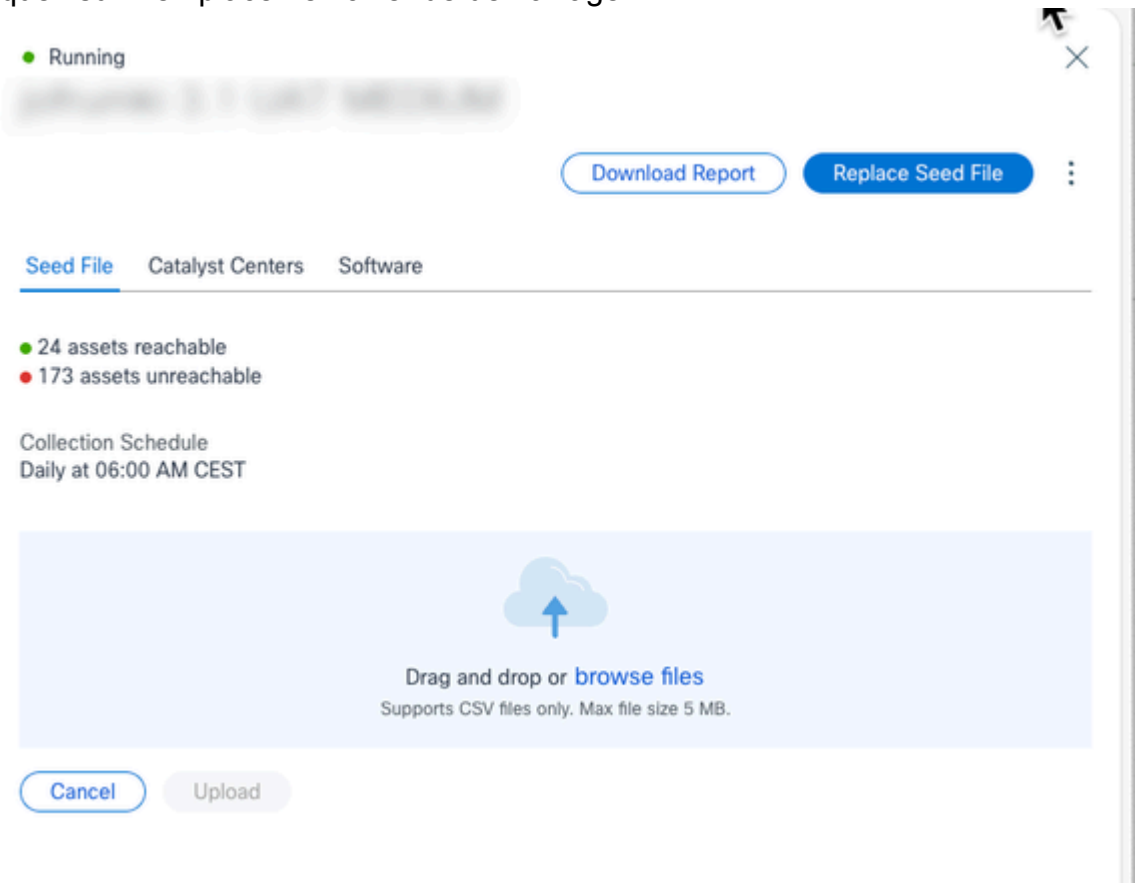
---

2. Dans la page Sources de données, cliquez sur la source de données de l'agent CX qui nécessite un fichier de départ mis à jour. La fenêtre CX Agent details s'ouvre.



Fichier De Départ

3. Cliquez sur Remplacer le fichier de démarrage.



Remplacer le fichier de démarrage

4. Faites glisser et déposez ou cliquez sur Parcourir les fichiers pour télécharger le fichier de départ modifié.
5. Cliquez sur Upload (charger).

Informations d'identification par défaut du fichier de démarrage

CX Agent élimine le besoin d'inclure des mots de passe sensibles directement dans le fichier d'amorçage. Cela renforce la sécurité en réduisant l'exposition des informations confidentielles et en répondant aux principales préoccupations des clients. Référez-vous à Configuration du coffre-fort pour les agents CX existants pour des informations sur l'activation de cette fonctionnalité.

Ajout d'autres ressources via des plages IP

Les plages IP permettent aux utilisateurs d'identifier les ressources matérielles et, par la suite, de collecter des données télémétriques à partir de ces périphériques en fonction des adresses IP. Il est possible d'identifier de manière unique les périphériques de collecte télémétrique en spécifiant une plage IP unique au niveau du réseau, qui peut être analysée par CX Agent à l'aide du protocole SNMP. Si la plage IP est choisie pour identifier un périphérique connecté directement, les adresses IP référencées peuvent être aussi restrictives que possible, tout en permettant la couverture de toutes les ressources requises.

- Des adresses IP spécifiques peuvent être fournies ou des caractères génériques peuvent être utilisés pour remplacer des octets d'une adresse IP afin de créer une plage.
- Si une adresse IP spécifique n'est pas incluse dans la plage d'adresses IP identifiée lors de la configuration, l'agent CX ne tente pas de communiquer avec un périphérique qui possède une telle adresse IP et ne collecte pas de données télémétriques à partir d'un tel périphérique.
- La saisie de *.*.*.* permet à l'agent CX d'utiliser les informations d'identification fournies par l'utilisateur avec n'importe quelle adresse IP. Exemple : 172.16.*.* permet d'utiliser les informations d'identification pour tous les périphériques du sous-réseau 172.16.0.0/16.
- Si des modifications sont apportées au réseau ou à la base installée (IB), la plage IP peut être modifiée. Reportez-vous à la section Modification des plages IP

L'agent CX tente de se connecter aux périphériques, mais peut ne pas être en mesure de traiter chacun d'eux pour l'afficher dans la vue Assets dans les cas où il n'est pas en mesure de déterminer les PID ou les numéros de série.

Remarques :
Cliquez sur Edit IP Address Range pour lancer la détection des périphériques à la demande. Lorsqu'un nouveau périphérique est ajouté ou supprimé (à l'intérieur ou à l'extérieur) d'une plage d'adresses IP spécifiée, le client doit toujours cliquer sur Modifier la plage d'adresses IP (reportez-vous à la section Modification des plages d'adresses IP) et effectuer les étapes requises pour lancer la détection de périphérique à la demande afin d'inclure tout nouveau périphérique ajouté à l'inventaire de collecte d'agent CX.

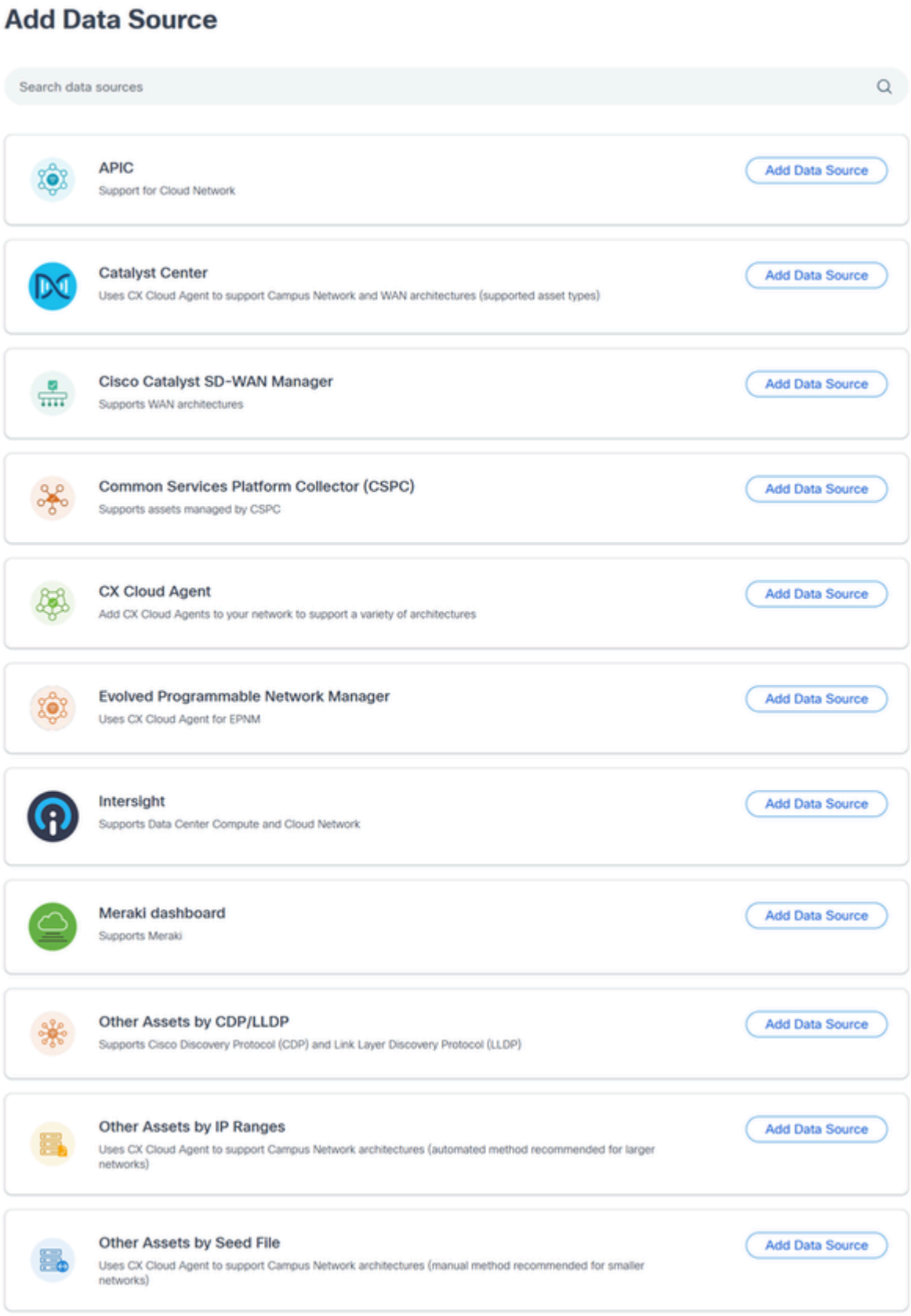
L'ajout de périphériques à l'aide d'une plage IP nécessite que les utilisateurs spécifient toutes les informations d'identification applicables via l'interface de configuration. Les champs visibles varient en fonction des protocoles sélectionnés dans les fenêtres précédentes. Si plusieurs sélections sont effectuées pour le même protocole, par exemple, en sélectionnant SNMPv2c et SNMPv3 ou SSHv2 et SSHv1, CX Agent négocie automatiquement la sélection du protocole en fonction des capacités de chaque périphérique.

Lors de la connexion de périphériques à l'aide d'adresses IP, le client doit s'assurer que tous les protocoles appropriés dans la plage IP, ainsi que les versions SSH et les informations d'identification Telnet sont valides, sinon les connexions échoueront.

Ajout d'autres ressources par plages IP

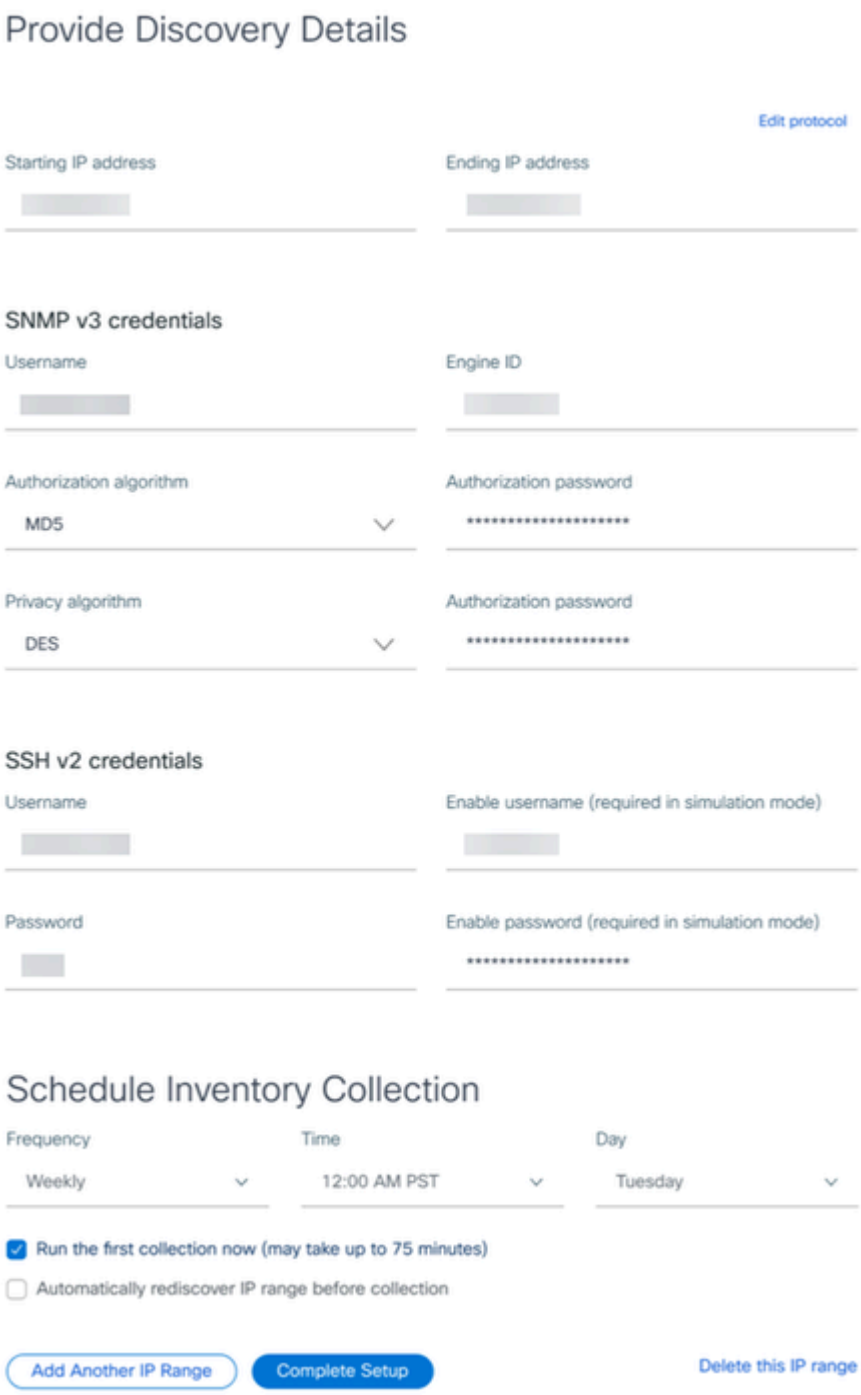
Pour ajouter des périphériques à l'aide de la plage IP :

1. Sélectionnez l'icône Centre d'administration. La fenêtre Sources de données s'ouvre.
2. Cliquez sur Ajouter une source de données dans la fenêtre Centre d'administration > Sources de données.



Autres ressources par plage IP

3. Cliquez sur Ajouter une source de données dans l'option Autres ressources par plage IP. La page Fournir des détails de détection s'affiche.

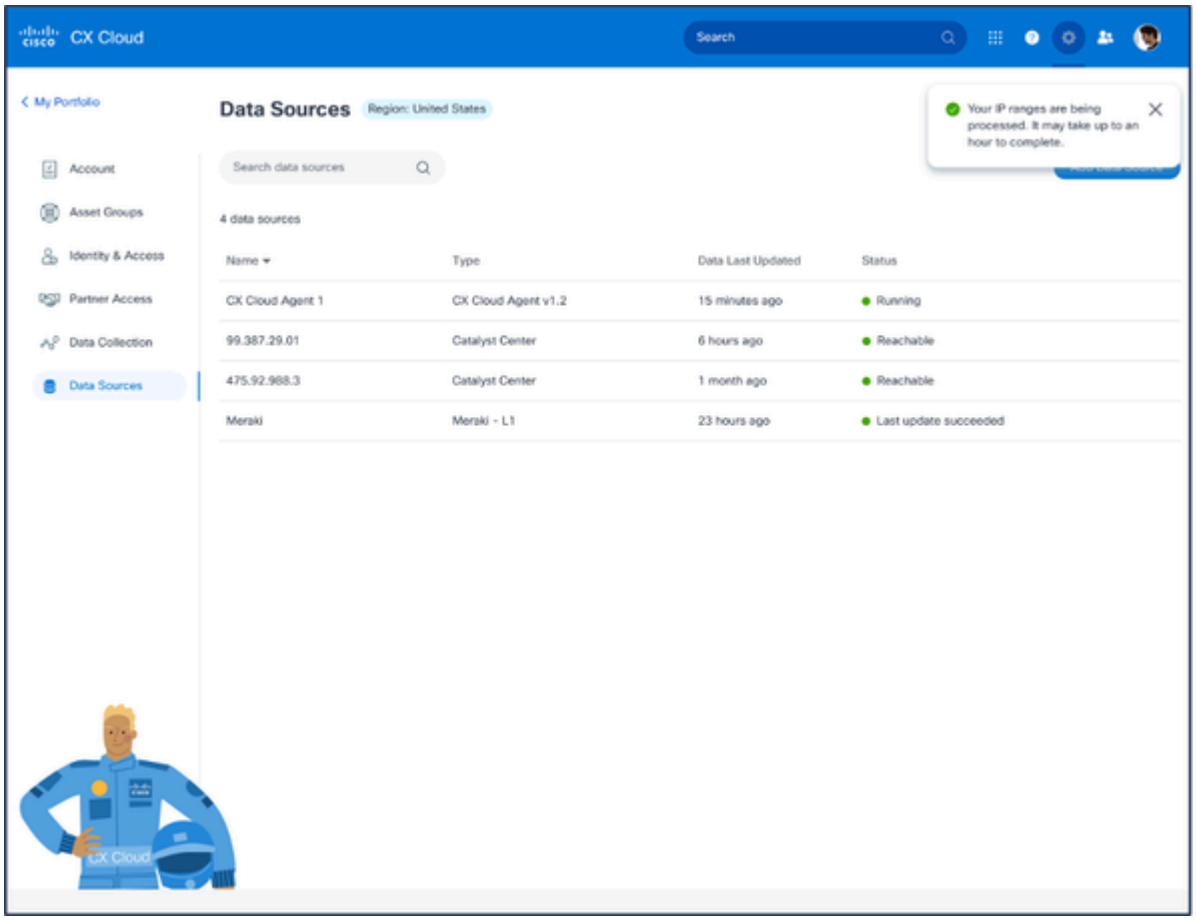


Fournir les détails de détection

4. Entrez une adresse IP de début et une adresse IP de fin.
5. Saisissez les informations requises dans les sections Informations d'identification SNMP et CLI.
6. Dans la section Planifier la collecte d'inventaire, sélectionnez des options dans les listes déroulantes suivantes.
    - Fréquence
    - Heure
    - Jour
7. Activez la case à cocher Exécuter la première collection maintenant pour exécuter la collection.
8. Le cas échéant, activez la case à cocher Redécouvrir automatiquement la plage IP avant la

collecte pour activer la redécouverte automatique des plages IP.

9. Cliquez sur Terminer la configuration. Une confirmation s'affiche lorsque le déploiement a réussi.

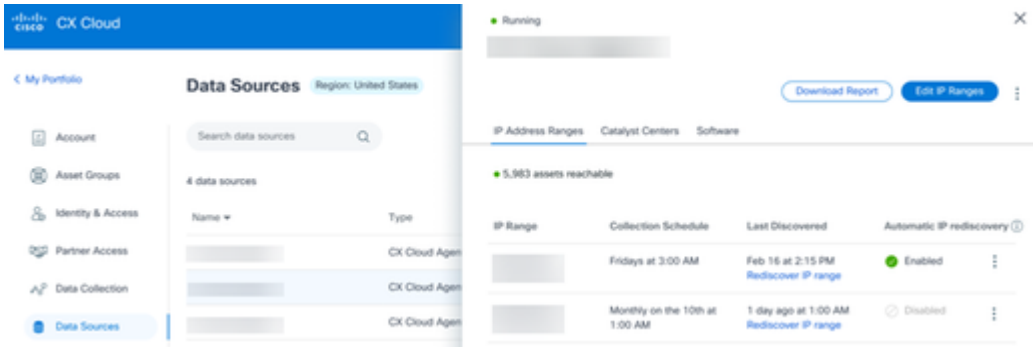


Message de confirmation

Modification des plages IP

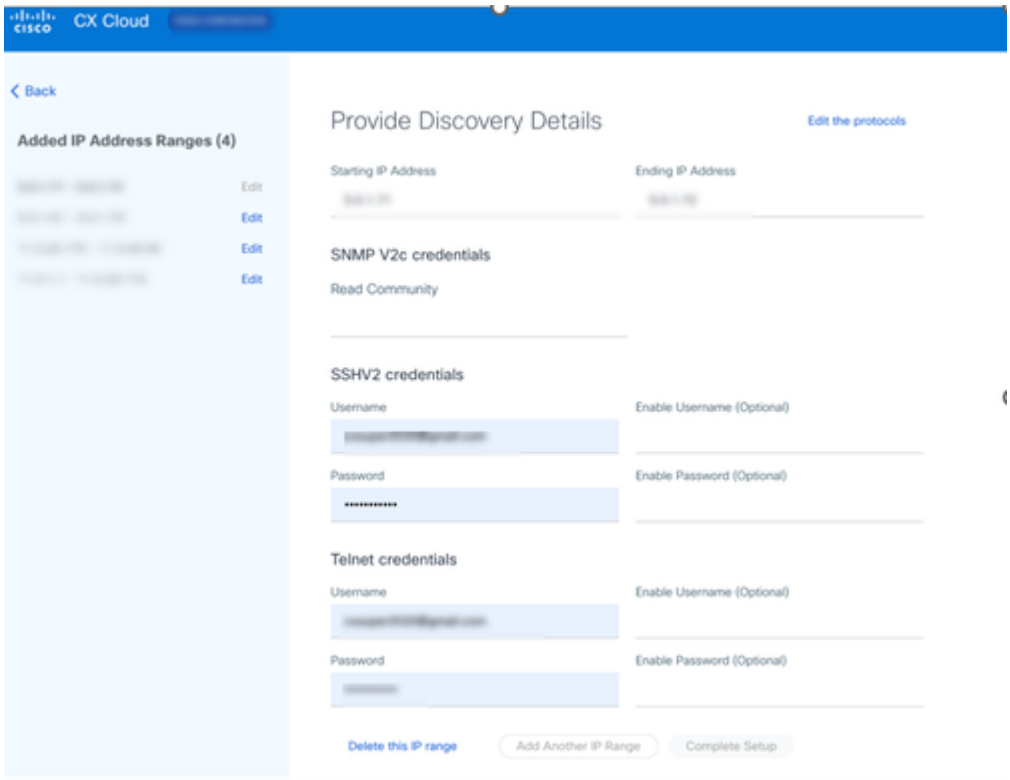
Pour modifier une plage IP :

1. Accédez à la fenêtre Sources de données.
2. Cliquez sur l'agent CX qui nécessite une modification de la plage IP dans Sources de données. La fenêtre des détails s'ouvre.

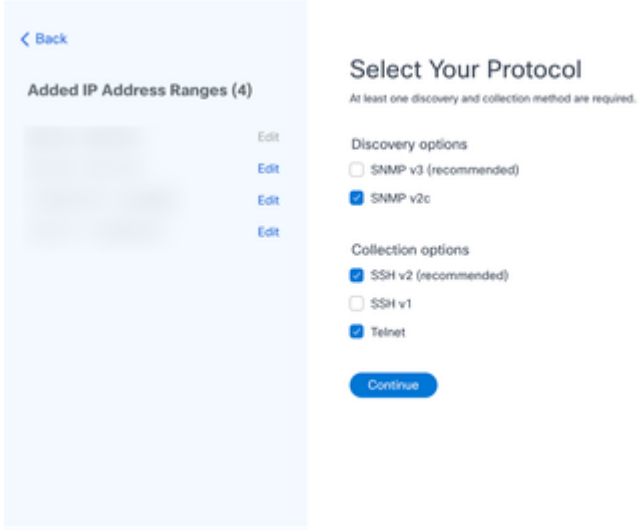


Fenêtre IP Range Details

3. Cliquez sur Edit IP Address Range.

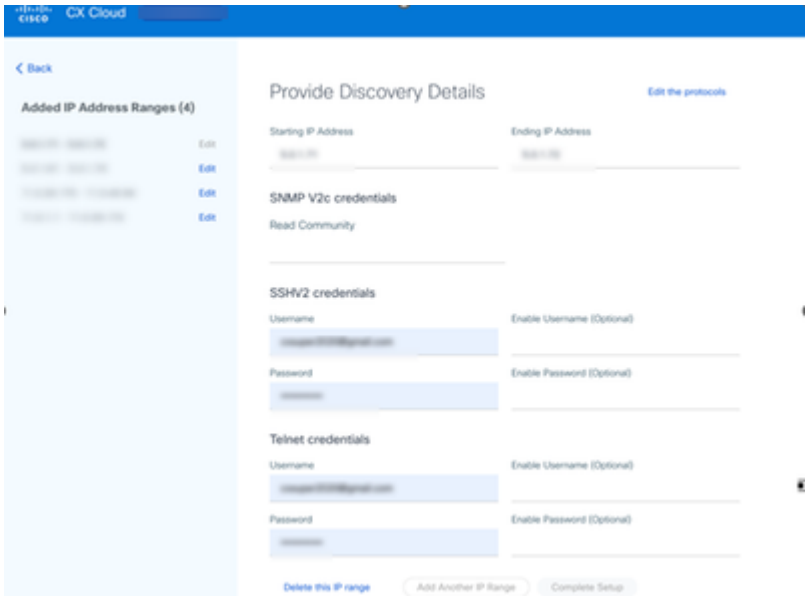


4. Cliquez sur Edit the protocols. La fenêtre Sélectionner votre protocole s'affiche.



Sélectionnez votre protocole

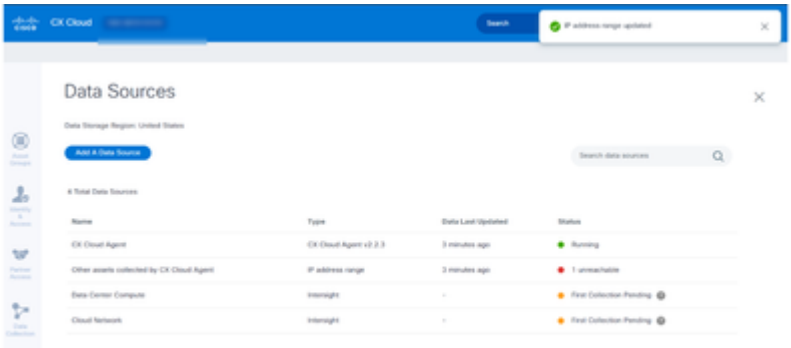
5. Cochez les cases appropriées pour choisir les protocoles applicables et cliquez sur Continue pour revenir à la fenêtre Provider Discovery Details.



Fournir les détails de détection

6. Modifiez les détails comme requis et cliquez sur Terminer la configuration. La fenêtre Sources de données s'ouvre et affiche un message confirmant l'ajout de la ou des plages d'adresses IP nouvellement ajoutées.

Remarque : Ce message de confirmation ne vérifie pas si les périphériques dans la plage modifiée sont accessibles ou si leurs informations d'identification sont acceptées. Cette confirmation se produit lorsque le client lance le processus de détection.

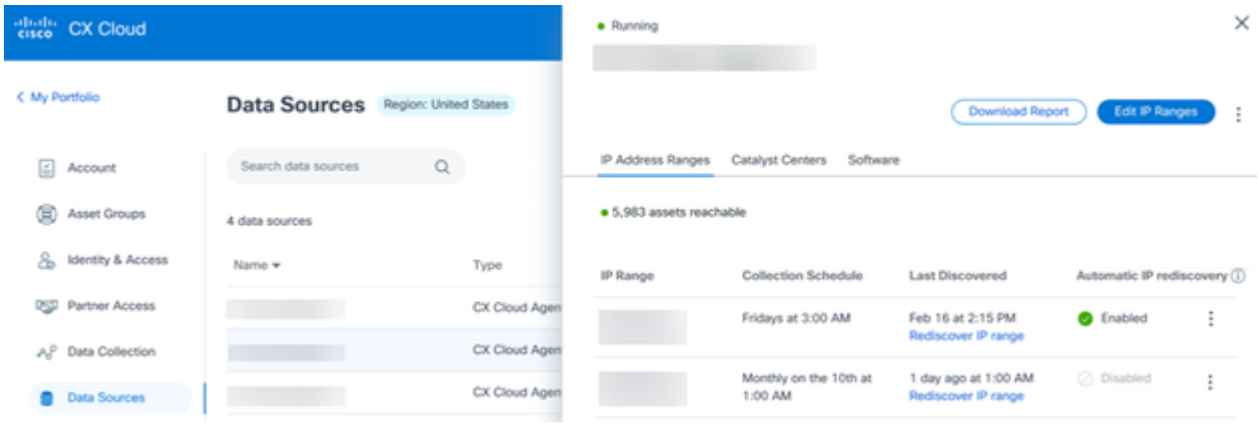


Confirmation

Suppression de plages IP

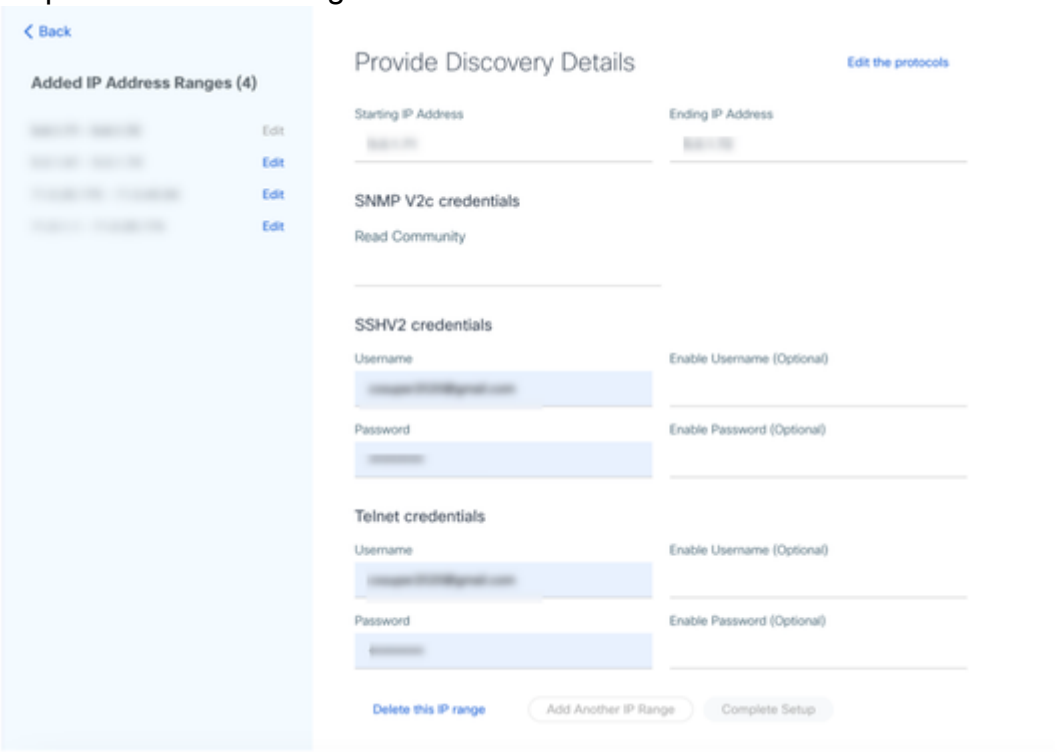
Pour supprimer une plage IP :

1. Accédez à la fenêtre Sources de données.
2. Sélectionnez l'agent CX correspondant avec la plage d'adresses IP à supprimer. La fenêtre des détails s'ouvre.



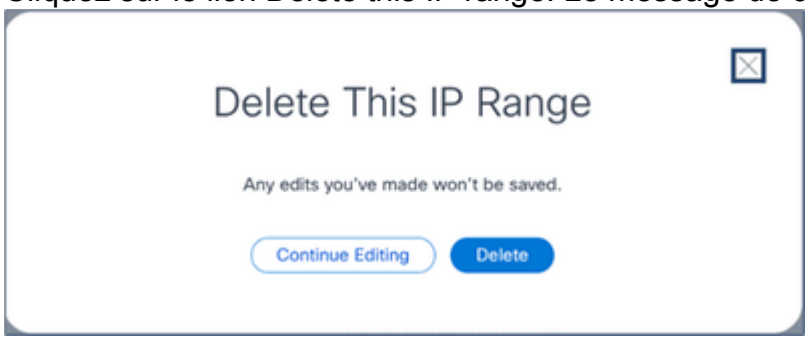
Modifier les plages IP

3. Cliquez sur Edit IP Ranges. La fenêtre Fournir les détails de la détection s'affiche.



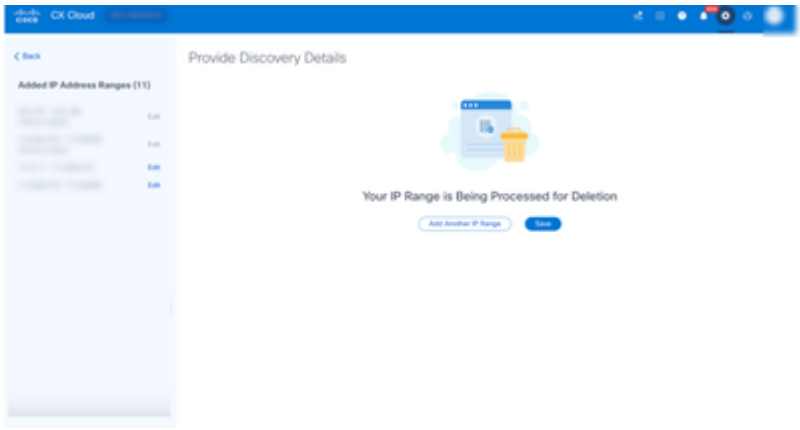
Suppression de plages IP

4. Cliquez sur le lien Delete this IP range. Le message de confirmation s'affiche.

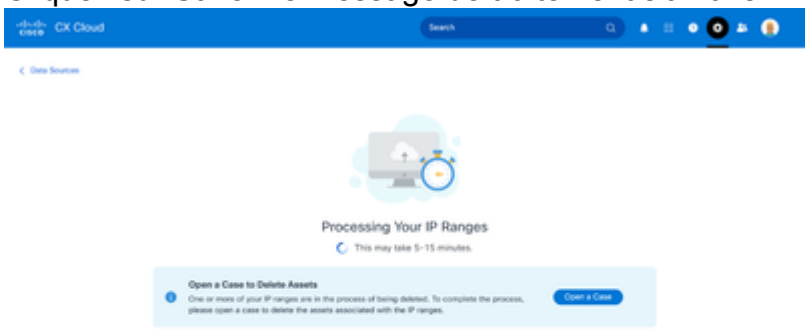


Message de confirmation de suppression

5. Cliquez sur Delete.



6. Cliquez sur Save. Le message de traitement s'affiche.



Suppression de plages IP

Une fois terminé, la fenêtre Sources de données s'ouvre et affiche un message de confirmation.

À propos des périphériques détectés à partir de plusieurs contrôleurs

Si les plages Catalyst Center et IP ou les fichiers d'amorçage se trouvent sur le même agent CX, il est possible que certains périphériques soient détectés à la fois par Cisco Catalyst Center et par la connexion directe du périphérique à l'agent CX, ce qui entraîne la collecte de données en double à partir de ces périphériques. Pour éviter de collecter des données en double et d'avoir un seul contrôleur pour gérer les périphériques, il est nécessaire de déterminer une priorité pour laquelle CX Agent gère les périphériques.

- Si un périphérique est d'abord découvert par Cisco Catalyst Center, puis redécouvert par connexion directe du périphérique (à l'aide d'un fichier d'amorçage ou d'une plage IP), Cisco Catalyst Center est prioritaire pour le contrôle du périphérique.

Remarque : Les protocoles CDP (Cisco Discovery Protocol) et LLDP (Link Layer

---

Discovery Protocol) ne sont pas inclus dans le processus de déduplication.

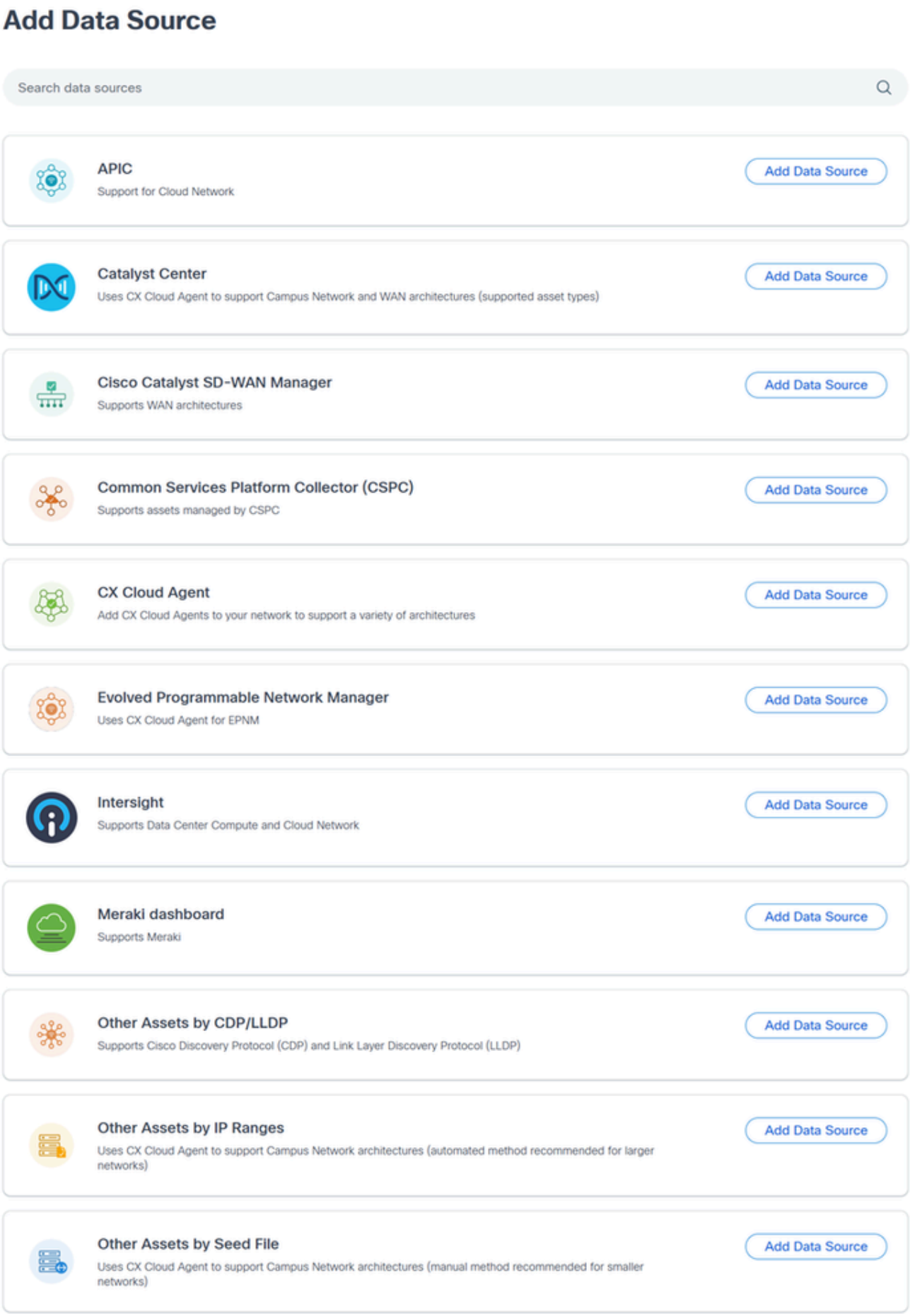
- Si un périphérique est d'abord détecté par une connexion de périphérique directe à l'agent CX, puis redécouvert par Cisco Catalyst Center, Cisco Catalyst Center est prioritaire pour le contrôle du périphérique.

Ajout d'autres ressources via CDP ou LLDP

CDP et LLDP sont des protocoles réseau qui permettent aux périphériques de découvrir automatiquement des informations sur les périphériques connectés directement sur le réseau. Lorsque la détection est activée via CDP ou LLDP, l'agent CX communique avec les périphériques réseau pour collecter des informations détaillées sur les périphériques voisins, telles que le type de périphérique, l'adresse IP et les détails de connectivité, sans nécessiter de saisie manuelle ni de préconfiguration. Ce processus automatisé permet à l'agent CX d'identifier et d'ajouter dynamiquement de nouveaux périphériques à l'inventaire lorsqu'ils sont détectés sur le réseau, garantissant ainsi que la liste des périphériques reste à jour même au fur et à mesure de l'évolution du réseau. Toutes les erreurs ou tous les messages liés à la détection de périphériques via CDP ou LLDP sont capturés dans les détails du journal des travaux dans le cloud CX. L'utilisation du protocole CDP ou LLDP pour la détection des périphériques simplifie la gestion du réseau, réduit les tâches manuelles et permet de conserver un inventaire précis et à jour de tous les périphériques connectés.

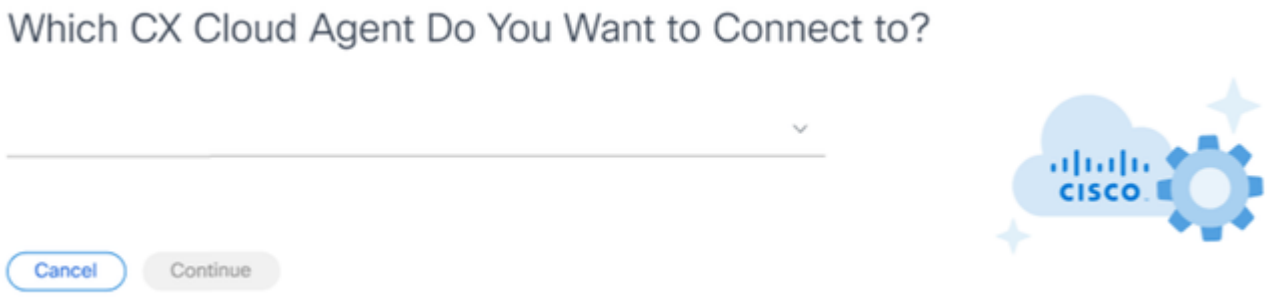
Pour ajouter d'autres ressources à l'aide de CDP ou LLDP :

1. Sélectionnez l'icône Centre d'administration. La fenêtre Sources de données s'ouvre.
2. Cliquez sur Ajouter une source de données. La page Ajouter une source de données s'affiche.



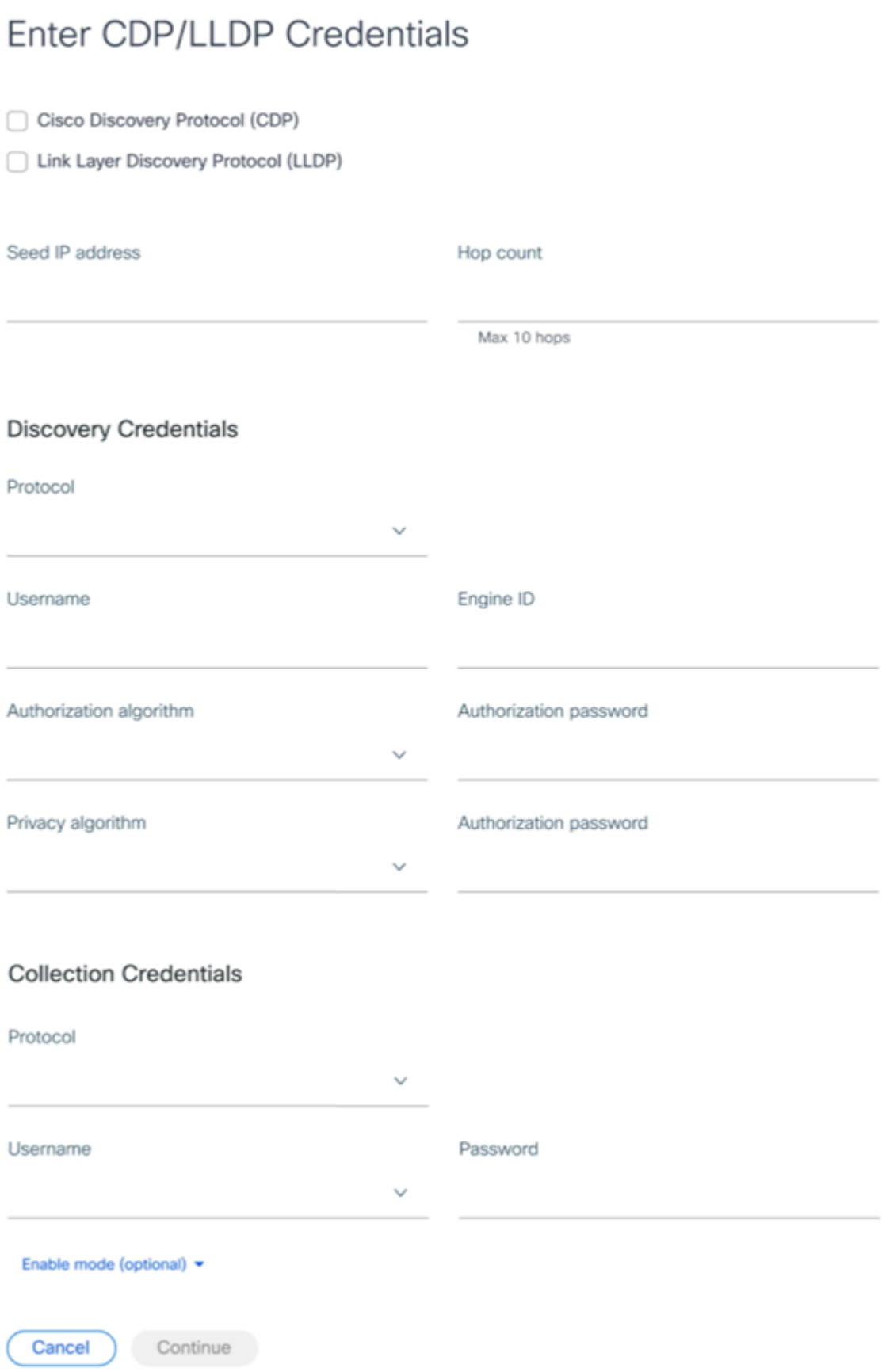
Autres ressources par CDP/LLDP

3. Cliquez sur Add Data Source dans l'option Other Assets by CDP/LLDP. À quel agent cloud CX voulez-vous vous connecter ? s'affiche.



À quel agent CX voulez-vous vous connecter ?

4. Sélectionnez une option dans la liste déroulante.
5. Cliquez sur Continue. La page Enter CDP/LLDP Credentials s'affiche.

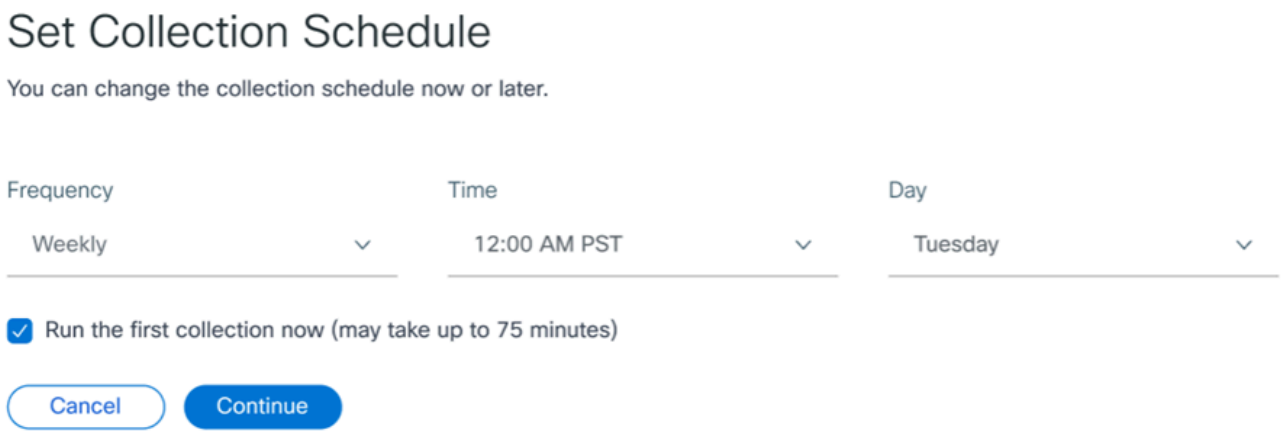


Saisir les informations d'identification CDP/LLDP

6. Activez la case à cocher CDP (Cisco Discovery Protocol) ou LLDP (Link Layer Discovery Protocol).
7. Entrez une adresse IP de début et un nombre de sauts (en d'autres termes, le nombre de

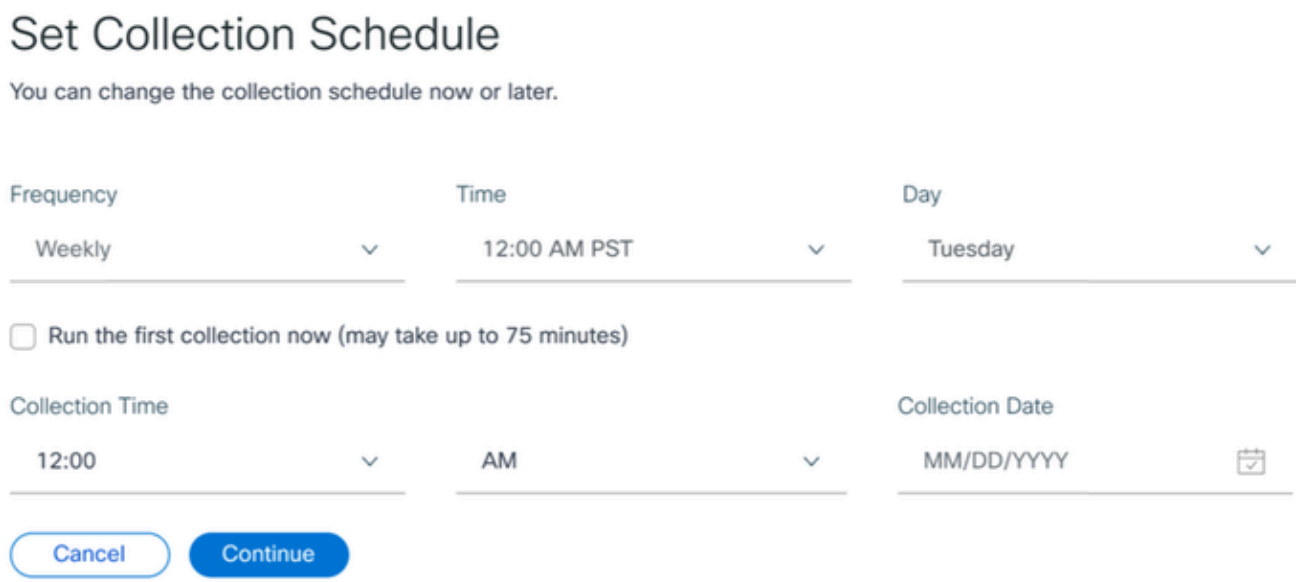
sauts que le processus de détection doit traverser).

8. Dans la section Discovery Credentials, sélectionnez SNMP v3 ou SNMP v2 dans la liste déroulante Protocol.
9. Saisissez les identifiants SNMP.
10. Dans la section Collection Credentials, sélectionnez SSH v2 (recommandé) dans la liste déroulante Protocol.
11. Saisissez un nom d'utilisateur et un mot de passe.
12. Cliquez sur Continue. La page Définir la planification de la collecte s'affiche.



Définir la planification de collecte

13. Sélectionnez des options dans les listes déroulantes suivantes :
    - Fréquence
    - Heure
    - Jour
14. Activez la case à cocher Exécuter la première collecte maintenant.
15. Cliquez sur Continue.



Définition du programme de collecte (suite)

16. Sélectionnez des options dans les listes déroulantes suivantes :
    - Heure de collecte
    - AM/PM

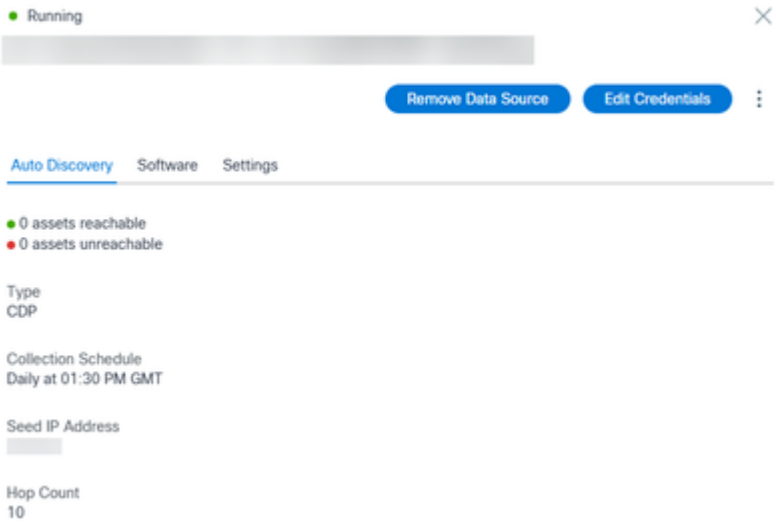
- Date de collecte

17. Cliquez sur Continue. Une fois la source de données ajoutée, une confirmation s'affiche.

Modification des détails CDP ou LLDP

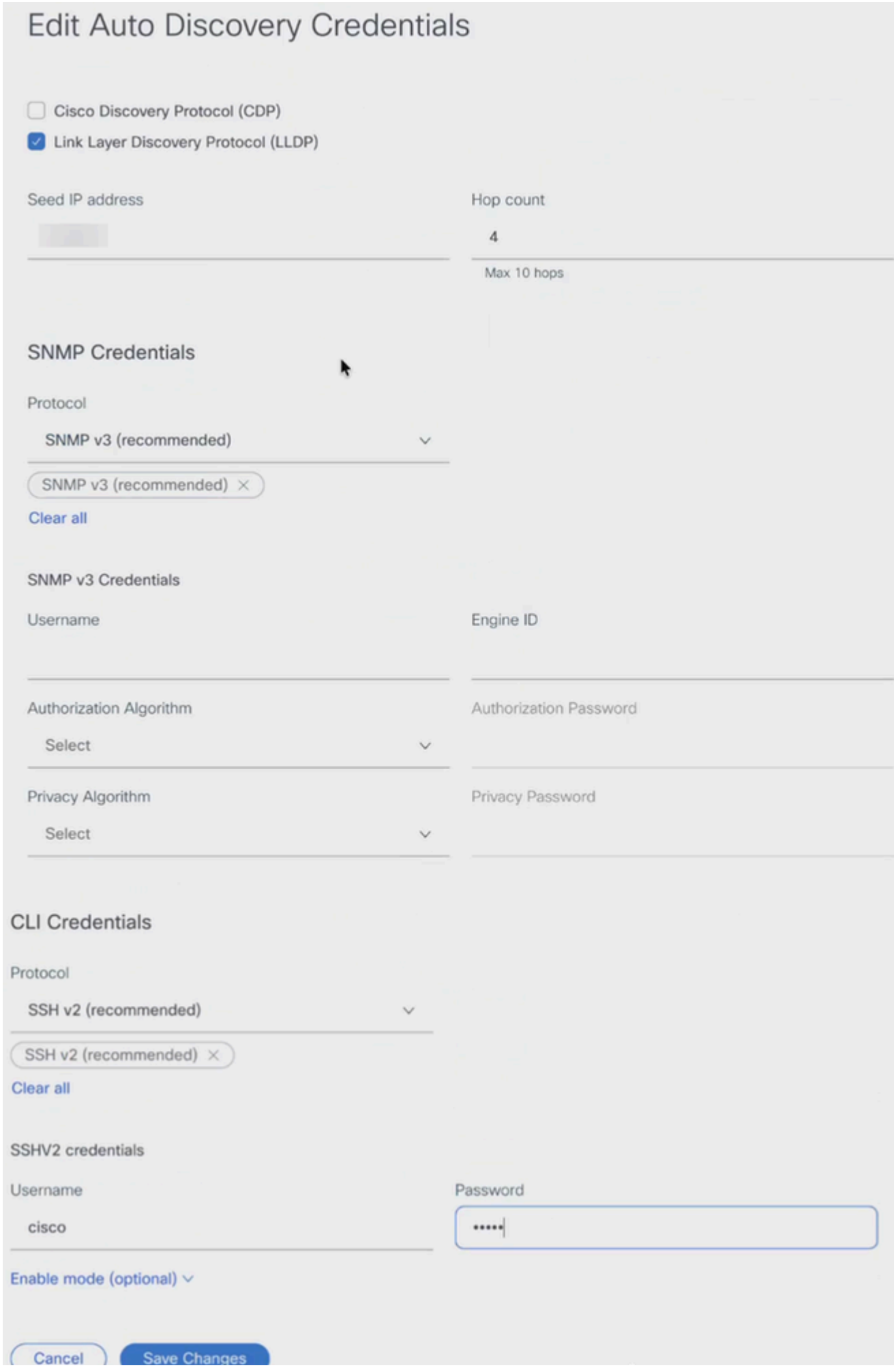
Pour modifier les détails CDP ou LLDP :

1. Accédez à la fenêtre Sources de données.
2. Cliquez sur l'agent CX qui nécessite l'affichage de la fenêtre détaillée de l'agent CX.



Fenêtre Détails agent CX

3. Cliquez sur Edit Credentials. La page Edit Auto Discovery Credentials s'affiche.



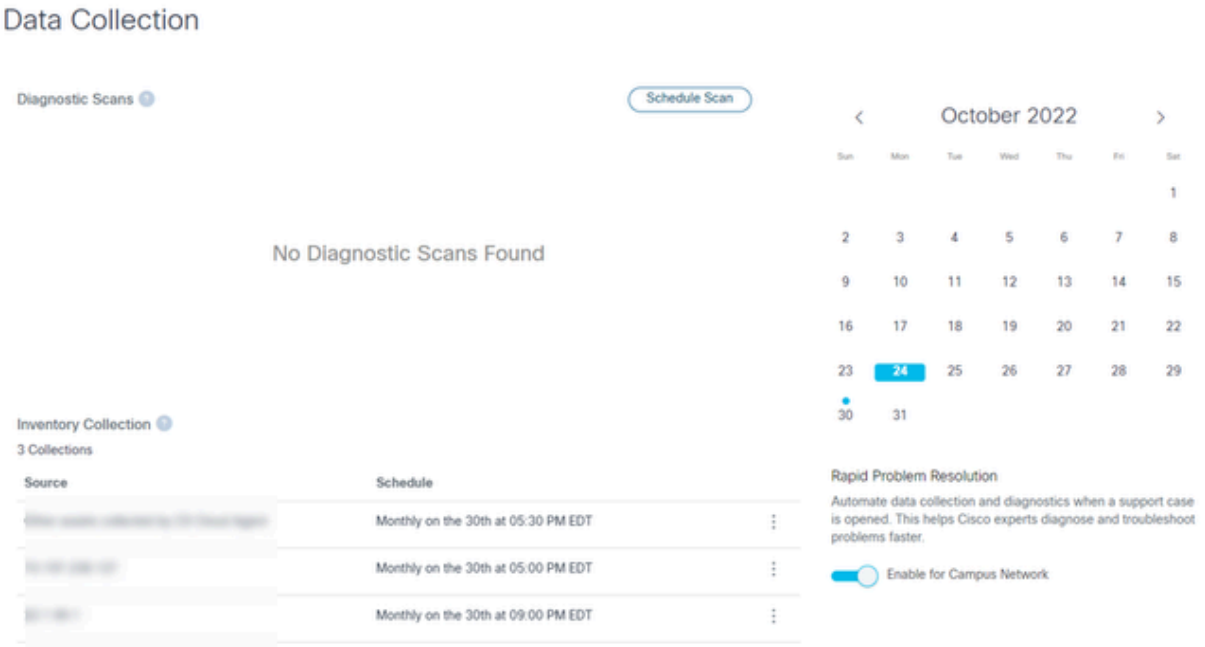
Modifier les identifiants de détection automatique

4. Effectuez les modifications souhaitées.

Cisco recommande de planifier des analyses de diagnostic ou de lancer des analyses à la demande au moins 6 à 7 heures à l'écart des calendriers de collecte d'inventaire afin qu'elles ne se chevauchent pas. L'exécution simultanée de plusieurs analyses de diagnostic peut ralentir le processus d'analyse et entraîner des échecs d'analyse.

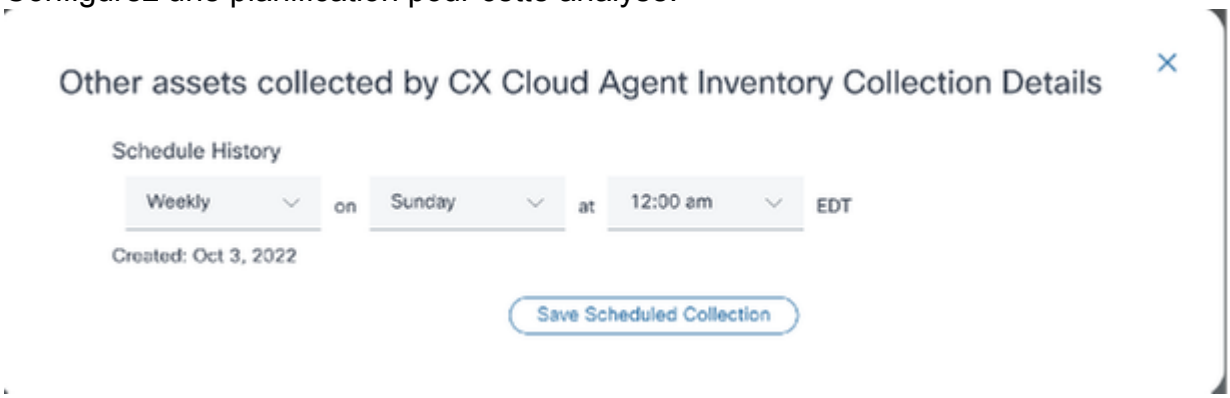
Pour planifier des analyses de diagnostic :

1. Sur la page d'accueil, cliquez sur l'icône Paramètres (engrenage).
2. Sur la page Sources de données, sélectionnez Collecte de données dans le volet gauche.
3. Cliquez sur Planifier l'analyse.



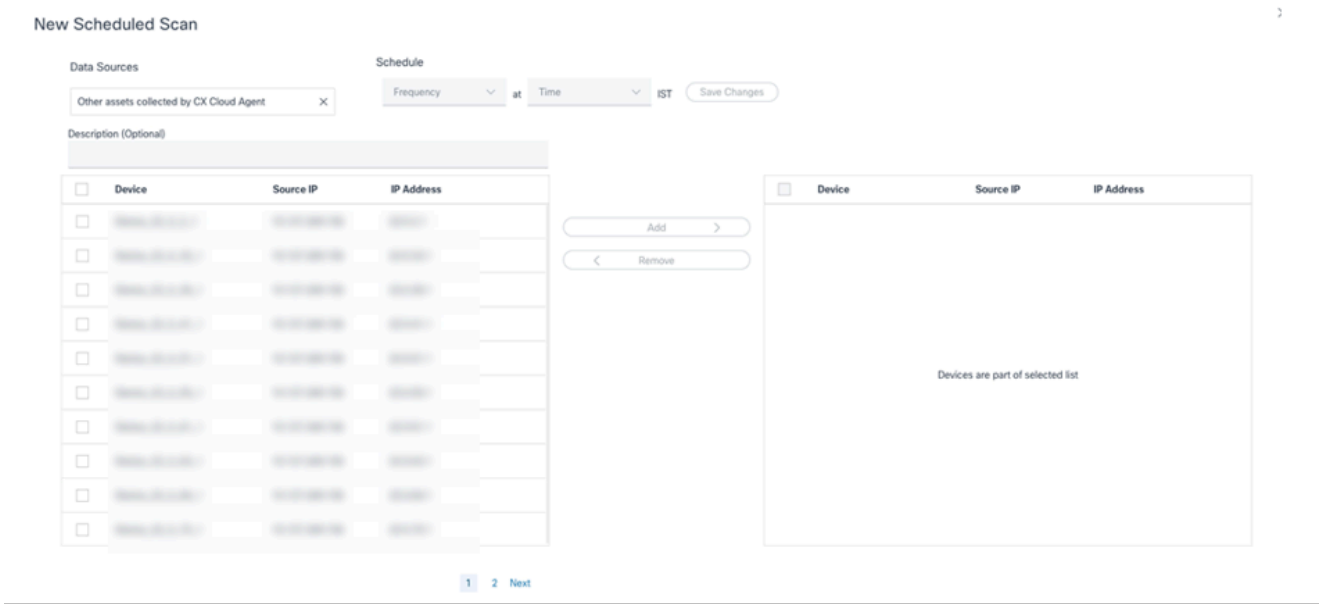
Planification des analyses

4. Configurez une planification pour cette analyse.



Configurer la planification d'analyse

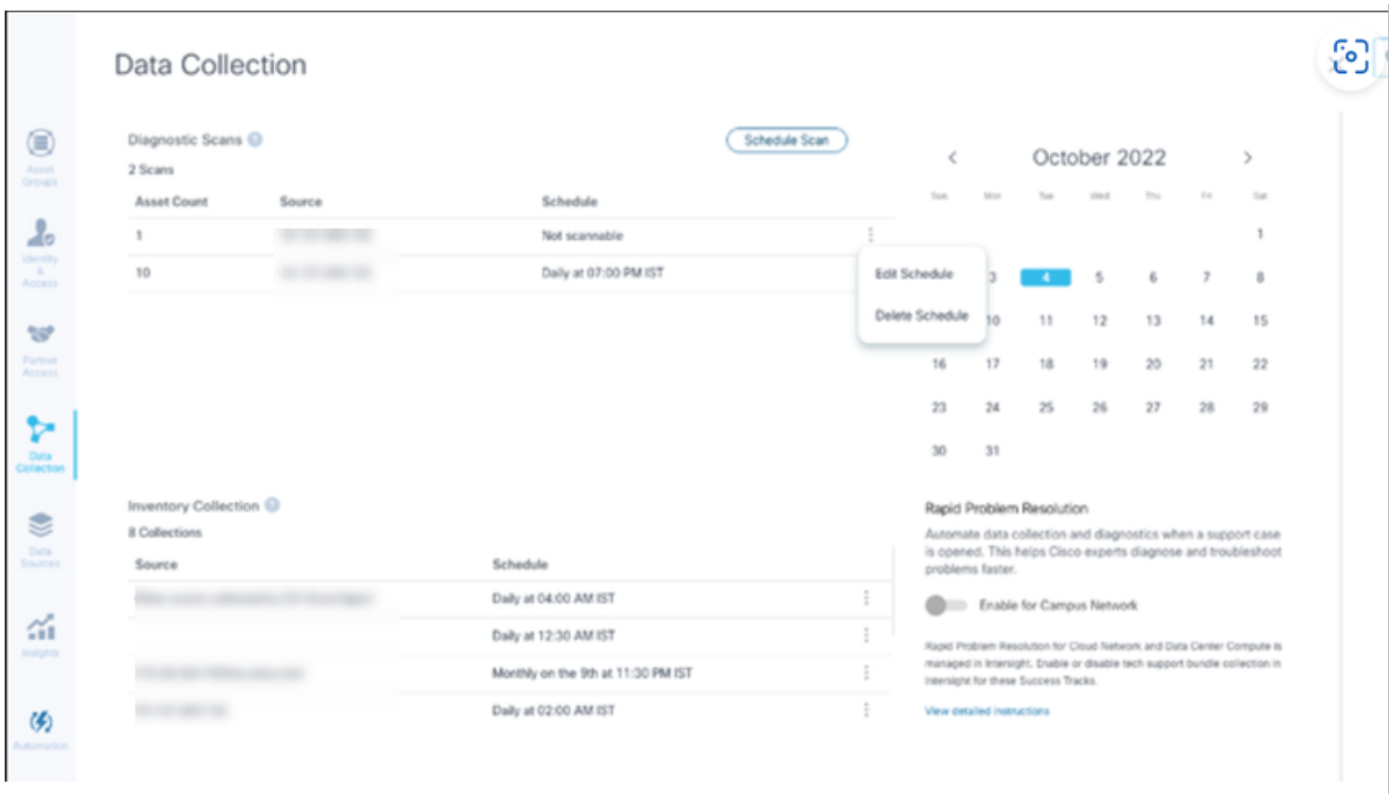
5. Dans la liste des périphériques, sélectionnez tous les périphériques pour l'analyse et cliquez sur Add.



Planifier le scan

6. Cliquez sur Save Changes lorsque la planification est terminée.

Les analyses de diagnostic et les planifications de collecte d'inventaire peuvent être modifiées et supprimées de la page Collecte de données.



Collecte de données avec les options Modifier et Supprimer la planification

Mise à niveau des machines virtuelles agent CX vers des

configurations moyennes et grandes

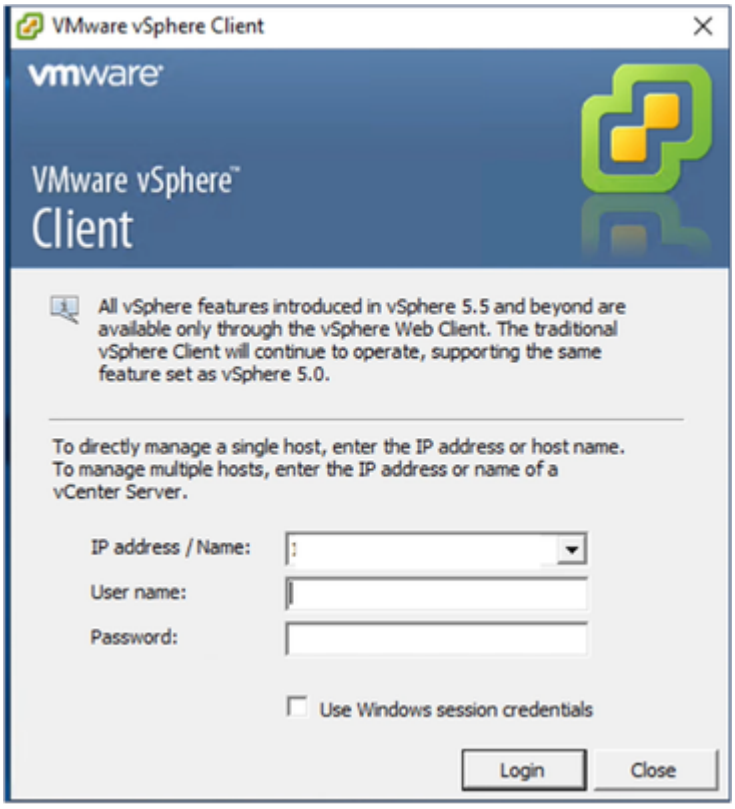
Une fois les machines virtuelles mises à niveau, il est impossible de :

- Rétrogradation d'une configuration de grande ou moyenne taille à une configuration de petite taille
- Rétrograder d'une configuration de grande à moyenne envergure
- Mise à niveau d'une configuration moyenne à grande

Avant de mettre à niveau la machine virtuelle, Cisco recommande de prendre un snapshot à des fins de récupération en cas de panne. Référez-vous à Sauvegarde et restauration de la machine virtuelle de cloud CX pour plus de détails.

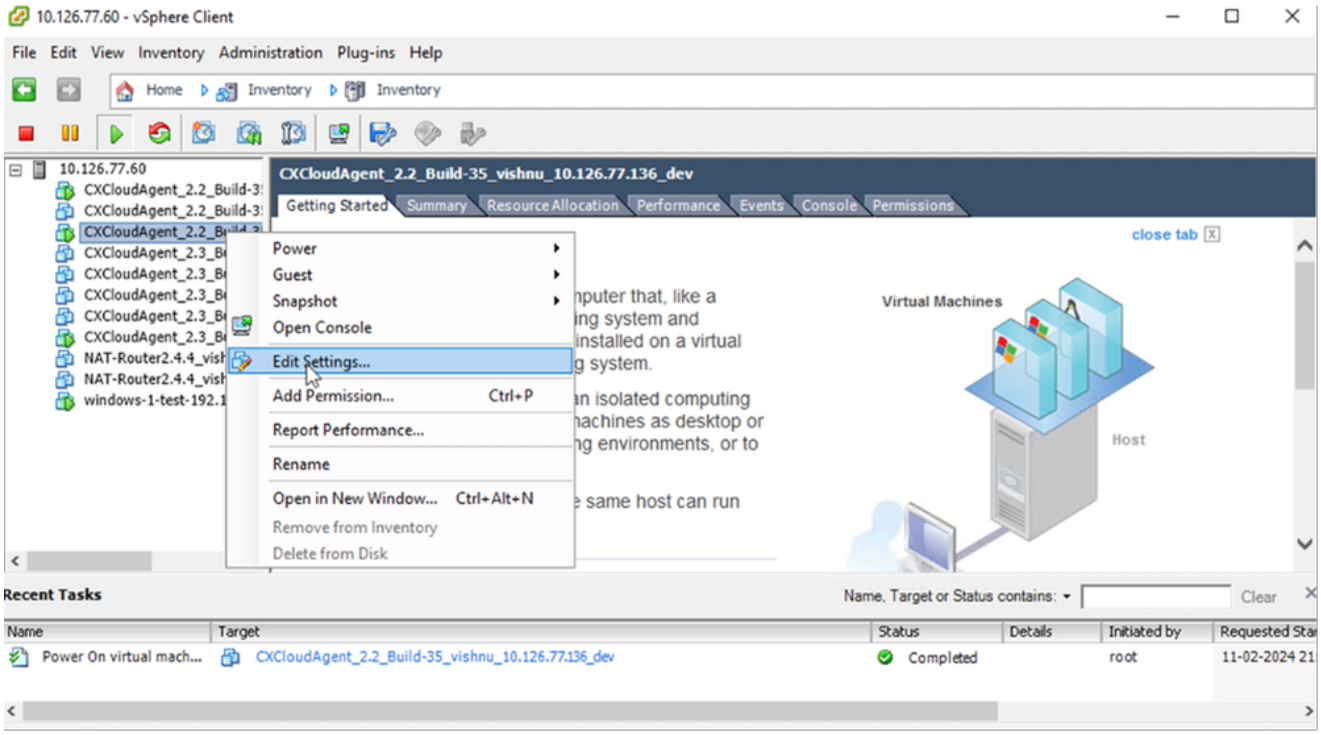
Reconfiguration à l'aide du client lourd VMware vSphere

Pour mettre à niveau la configuration de VM à l'aide du client lourd VMware vSphere existant :



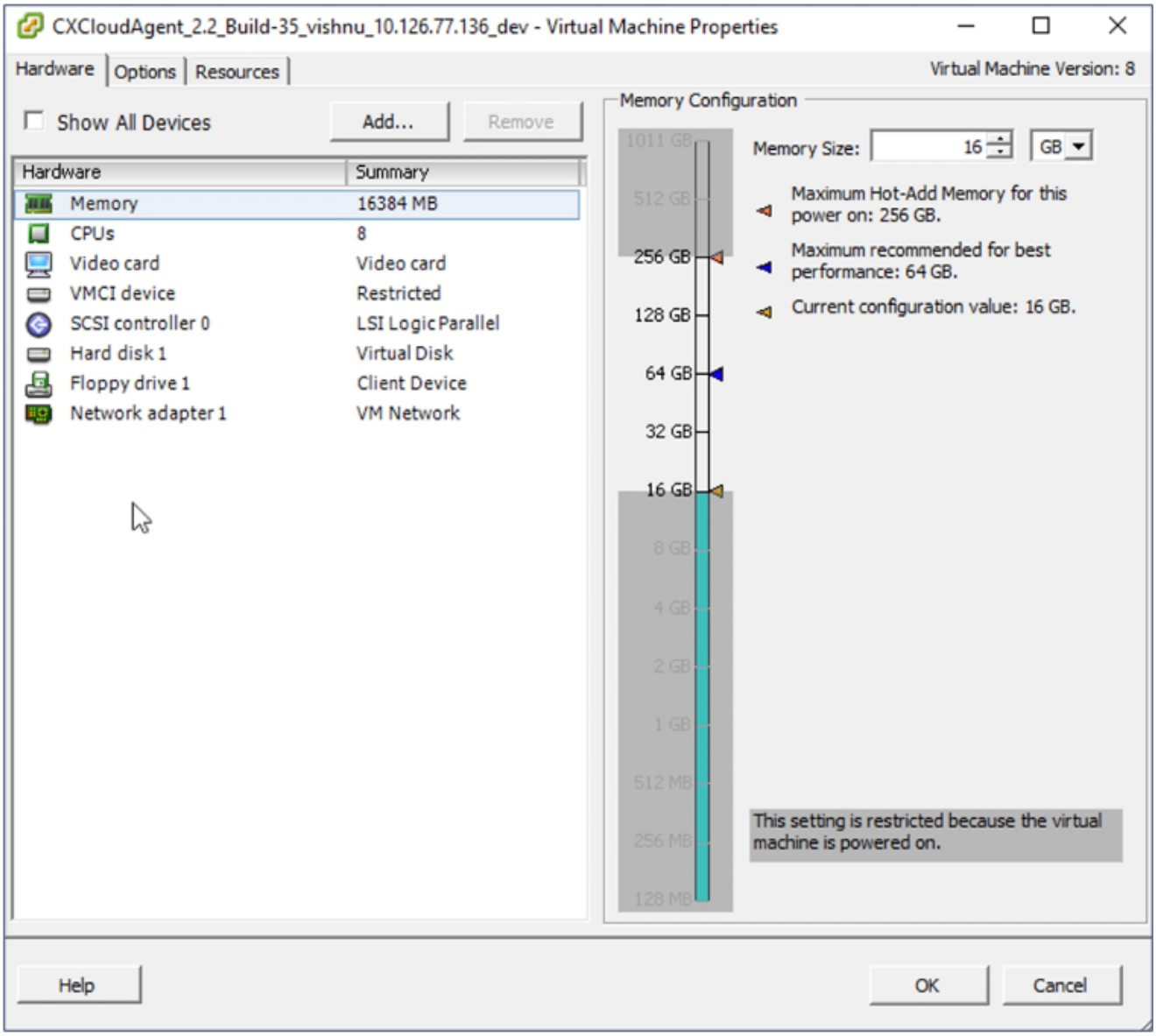
vSphere Client

1. Connectez-vous au client VMware vSphere. La page d'accueil affiche la liste des machines virtuelles.



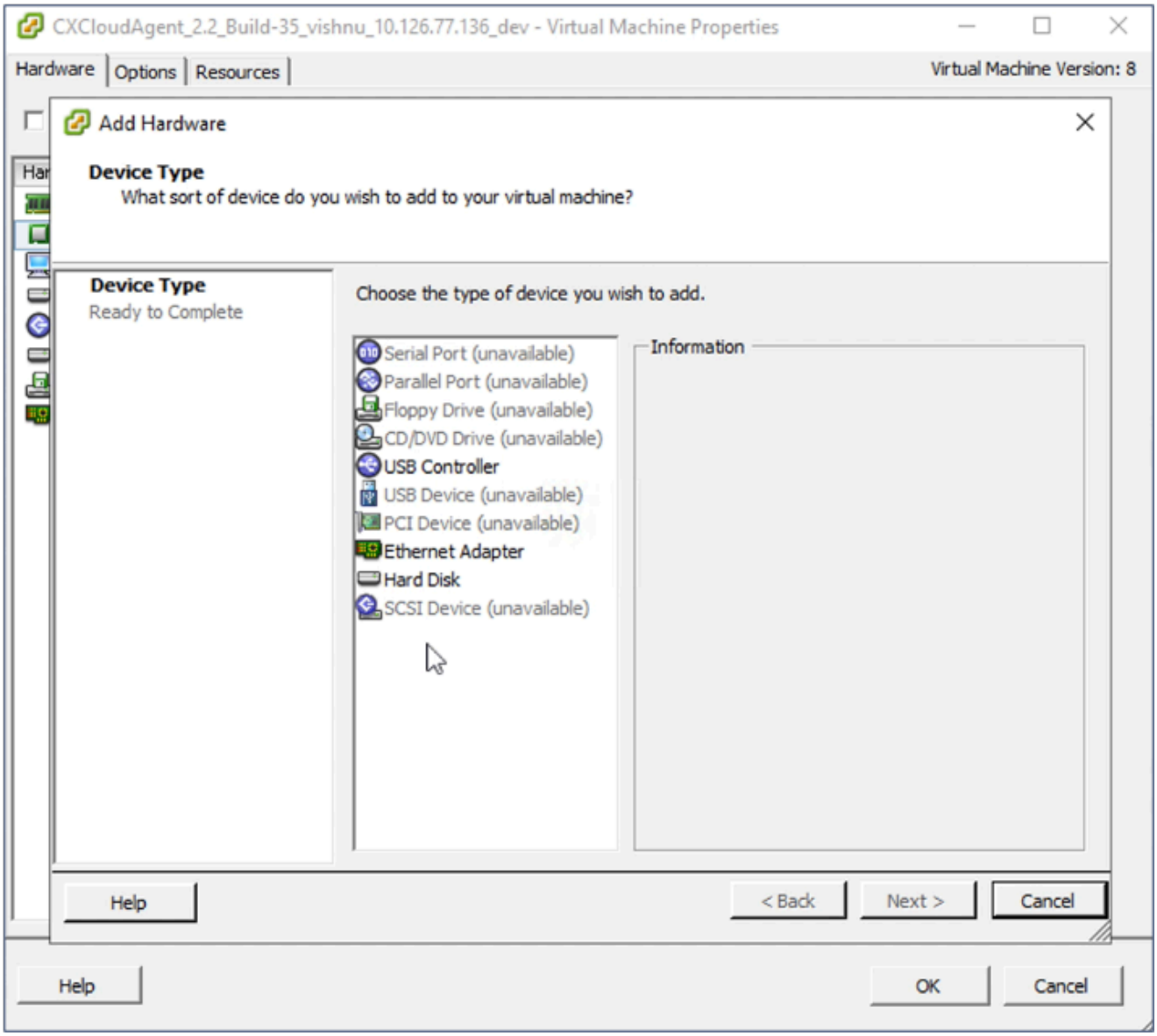
Modifier les paramètres

2. Cliquez avec le bouton droit sur la machine virtuelle cible et sélectionnez Modifier les paramètres dans le menu. La fenêtre Propriétés VM s'ouvre.



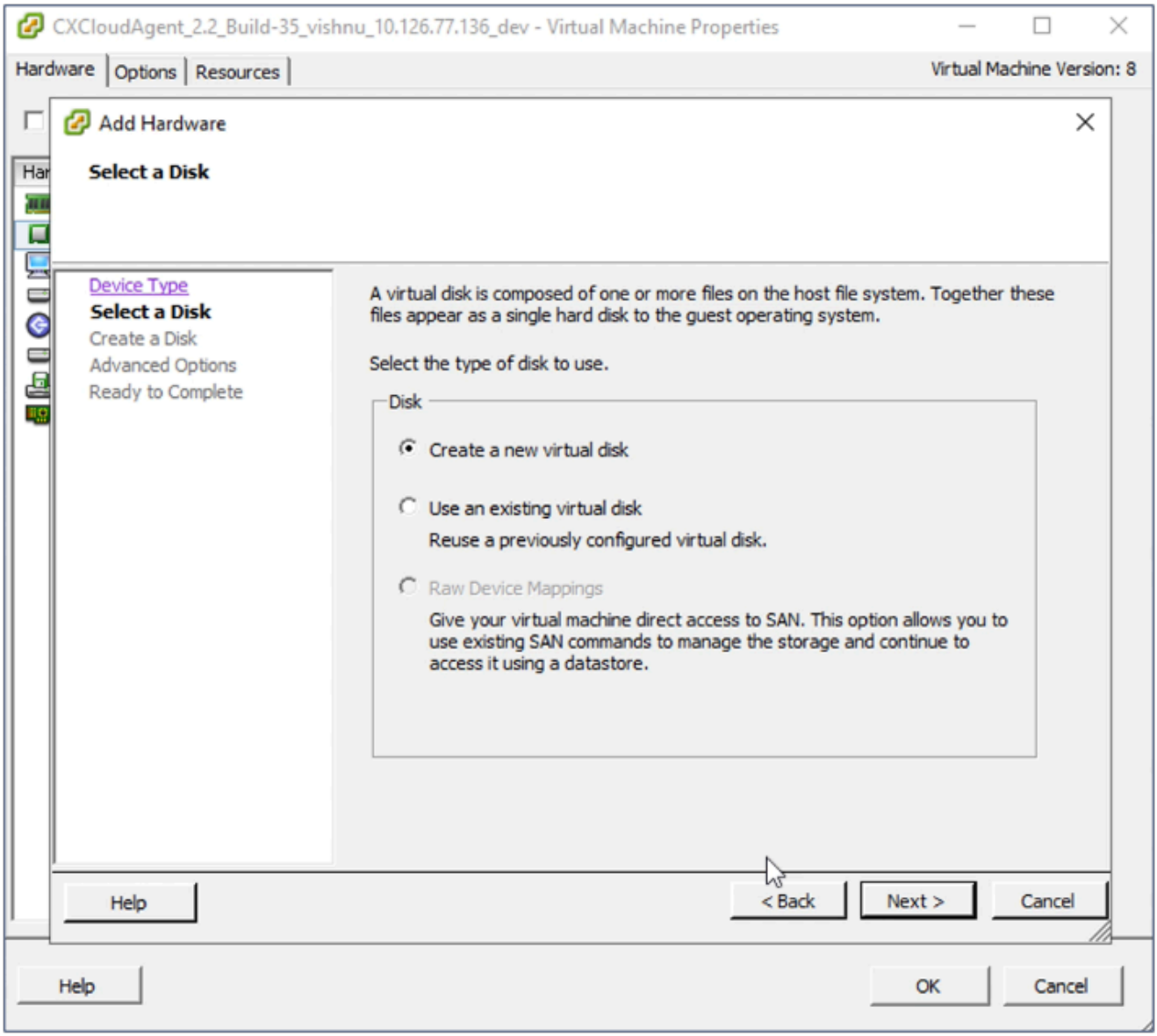
Propriétés VM

3. Mettez à jour les valeurs Memory Size comme indiqué :
   Moyenne : 32 Go (32768 Mo)
   Grande : 64 Go (65536 Mo)
4. Sélectionnez les processeurs et mettez à jour les valeurs comme indiqué :
   Moyenne : 16 coeurs (8 connecteurs *2 coeurs/connecteurs)
   Grande : 32 coeurs (16 connecteurs *2 coeurs/connecteurs)
5. Cliquez sur Add. La fenêtre Ajouter du matériel s'affiche.



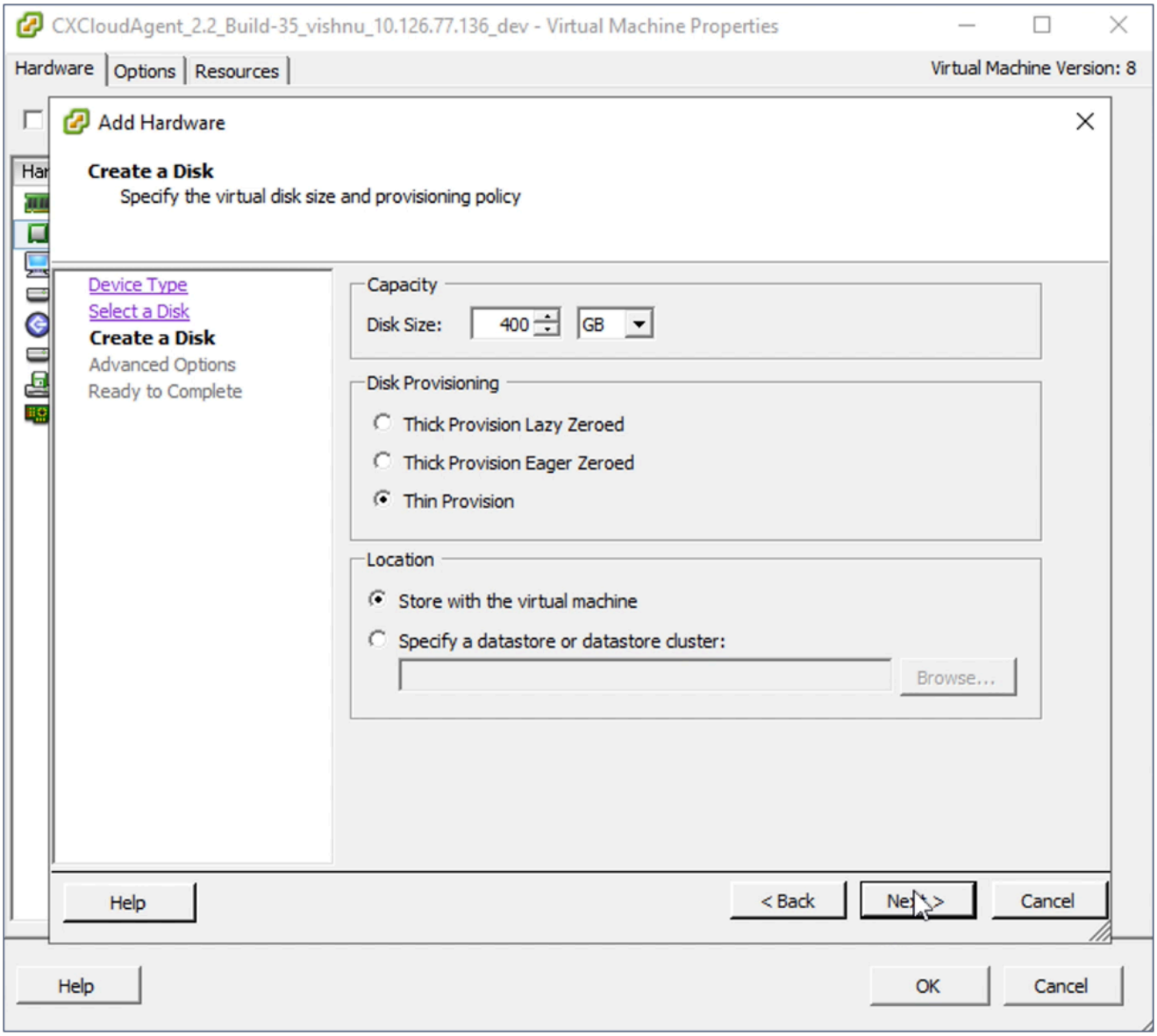
Type de périphérique

6. Sélectionnez Disque dur comme type de périphérique.
7. Cliquez sur Next (Suivant).



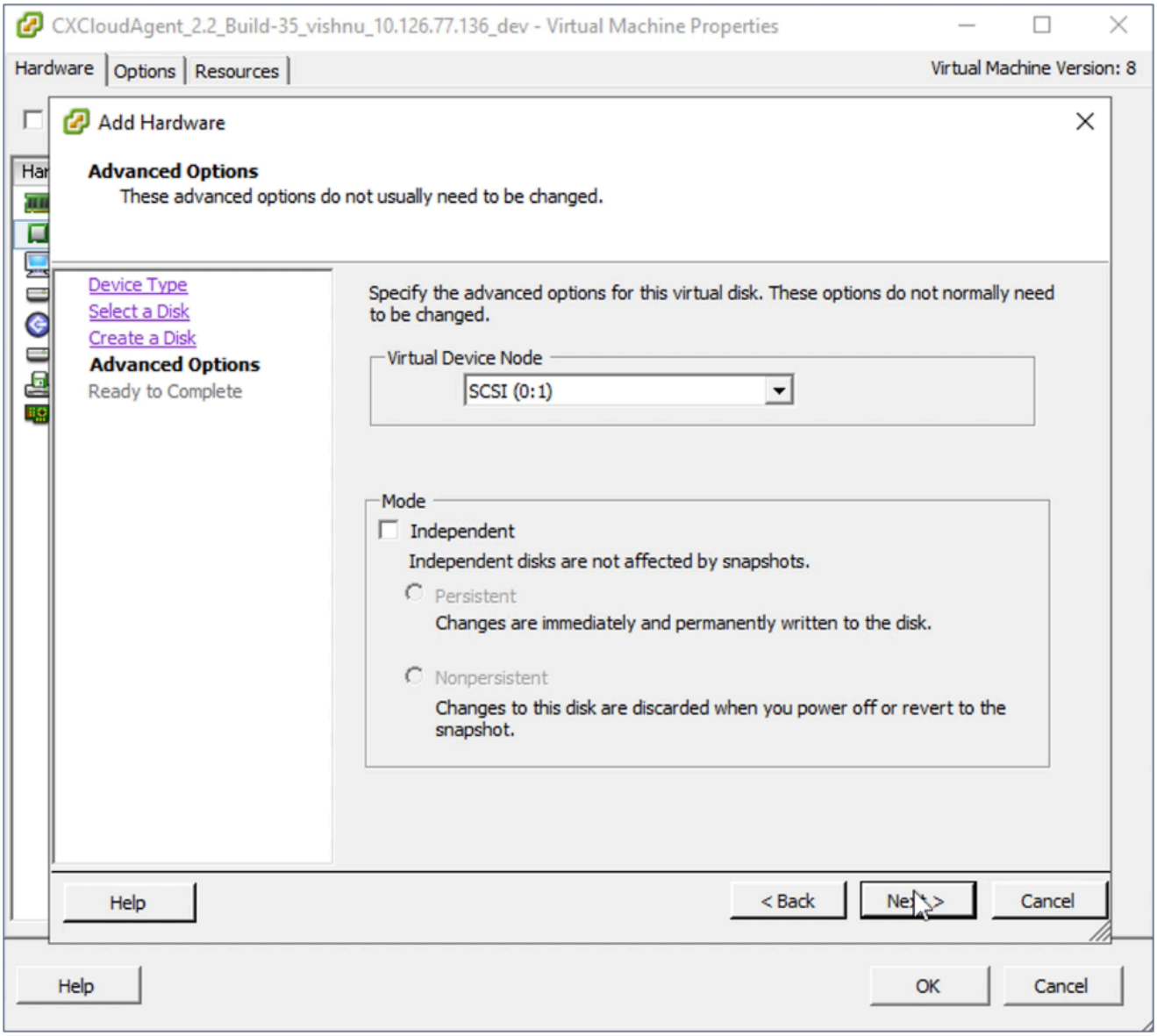
Sélectionner un disque

8. Sélectionnez la case d'option Create a new virtual disk et cliquez sur Next.



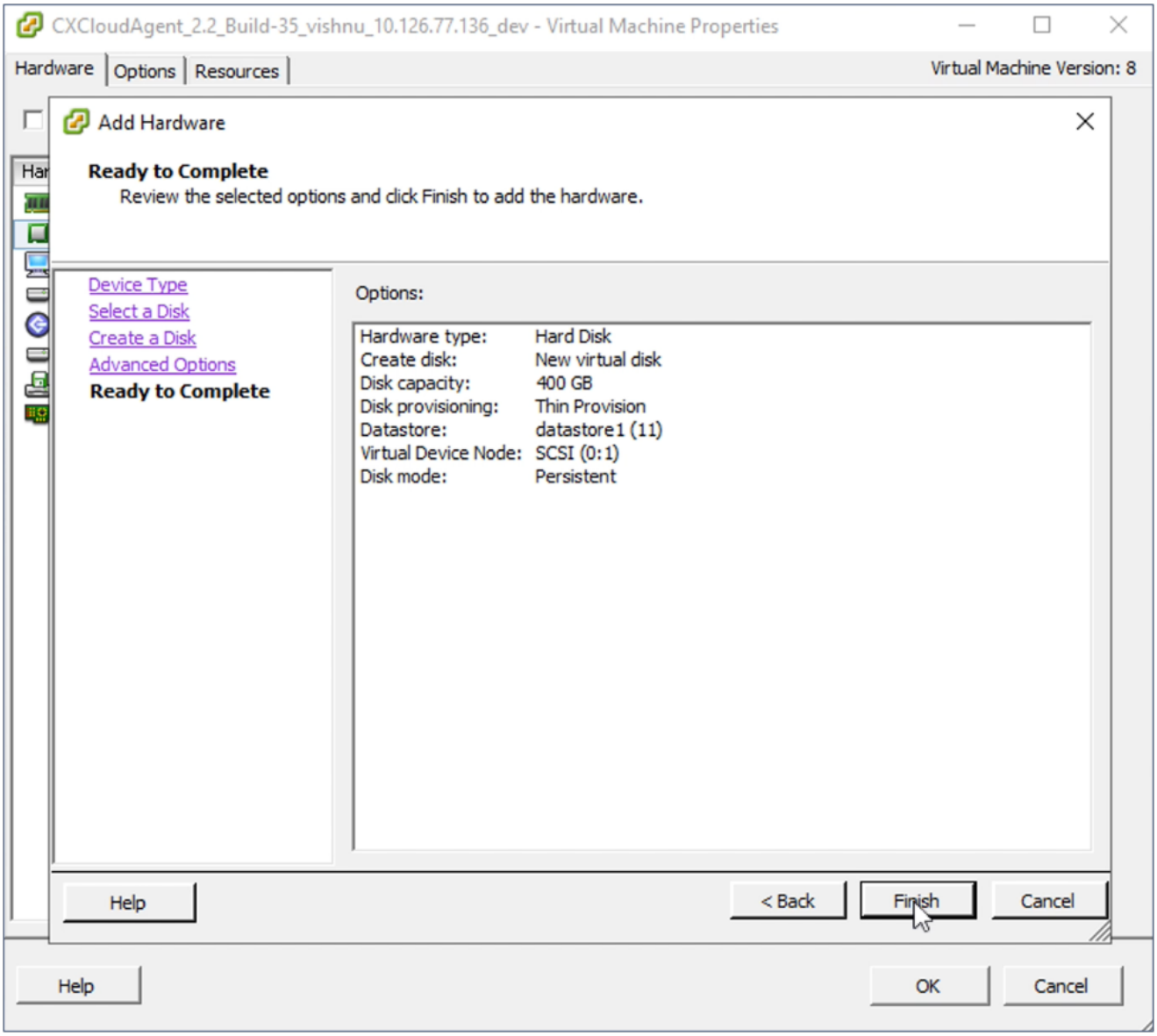
Créer un disque

9. Mettez à jour Capacity > Disk Size comme indiqué :
   Petite à moyenne : 400 Go (taille initiale : 200 Go, augmentant l'espace total à 600 Go)
   Petite à grande : 1 000 Go (taille initiale : 200 Go, augmentant l'espace total à 1 200 Go)
10. Sélectionnez la case d'option Provisionnement léger pour le provisionnement de disque.
11. Cliquez sur Next (Suivant). La fenêtre Options avancées s'affiche.



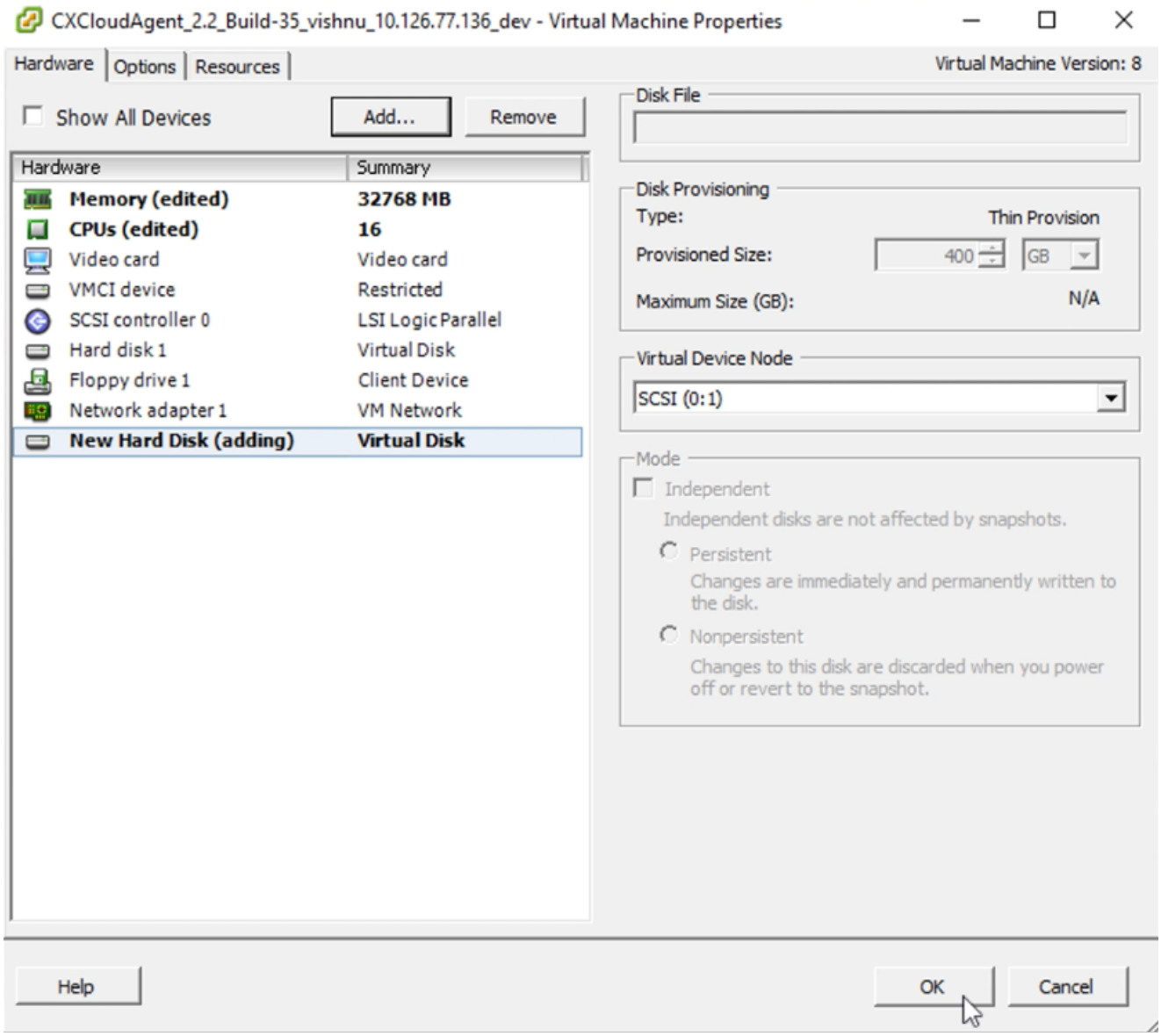
Options avancées

12. N'apportez pas de modifications. Cliquez sur Next pour continuer.



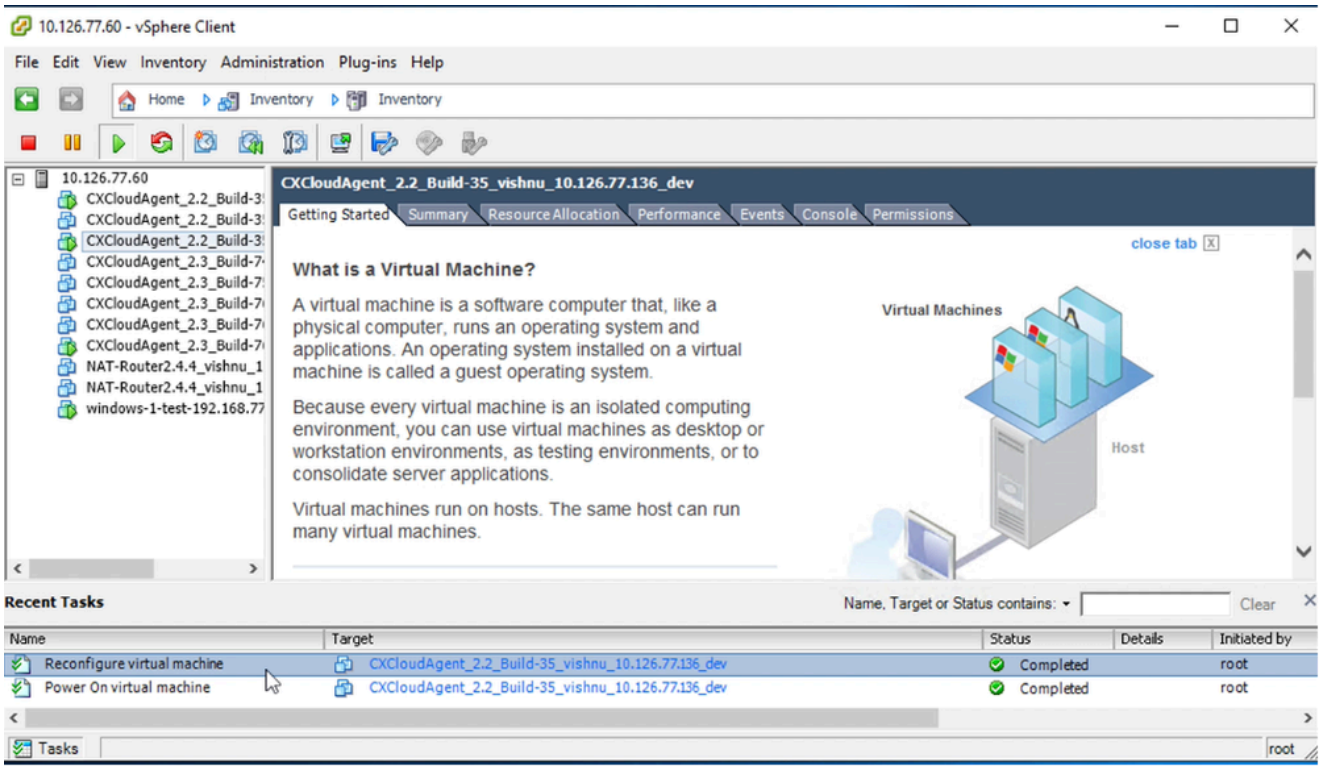
Prêt pour la confirmation

13. Cliquez sur Finish (Terminer).



Matériel

14. Cliquez sur OK pour terminer la reconfiguration. La reconfiguration terminée s'affiche dans le panneau Tâches récentes.

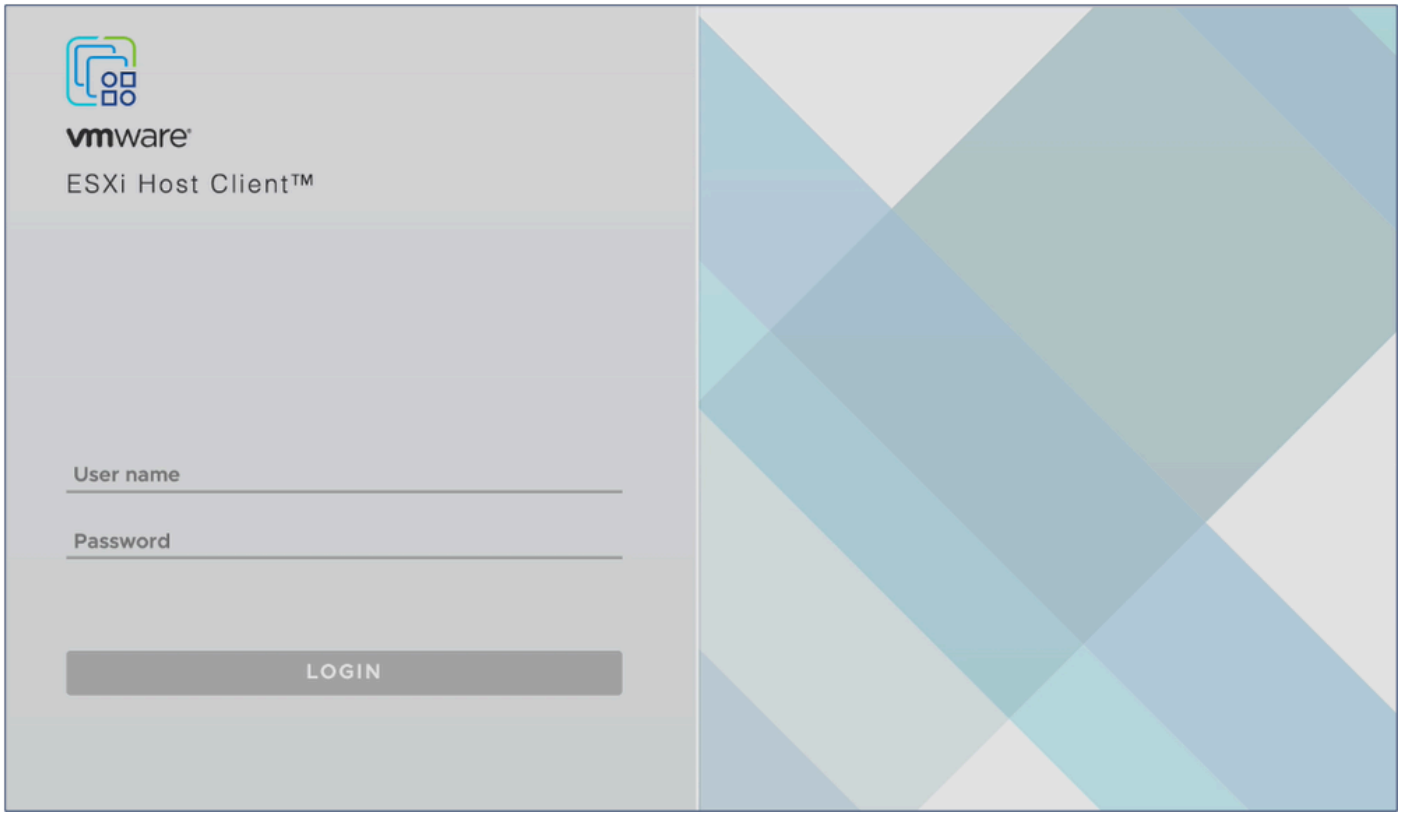


Tâches récentes

Remarque : Les modifications de configuration prennent environ cinq minutes.

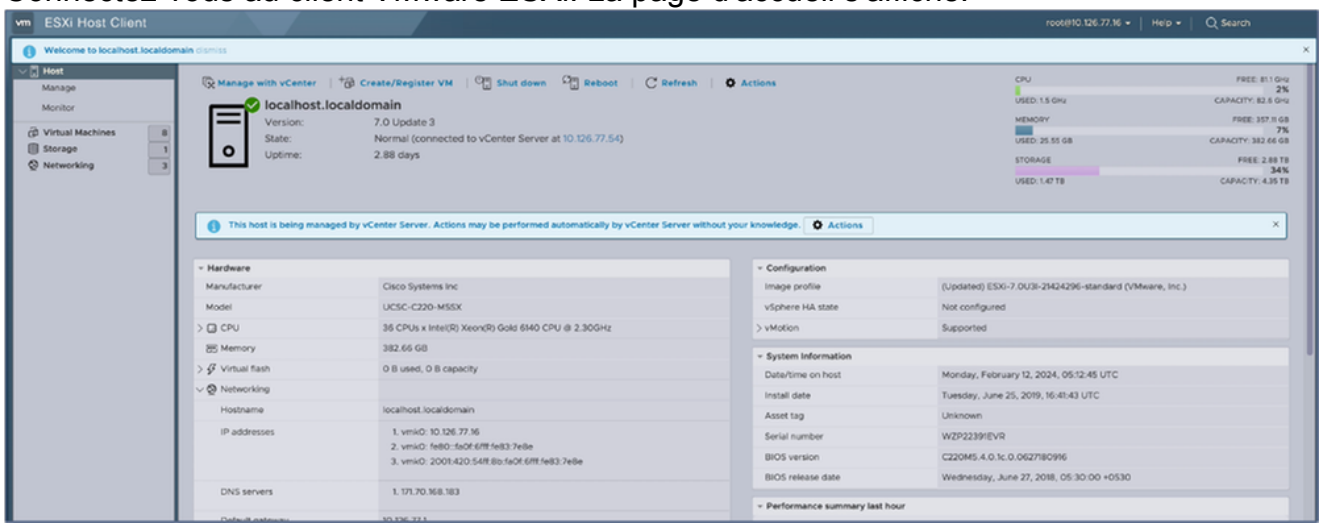
Reconfiguration à l'aide du client Web ESXi v6.0

Pour mettre à jour les configurations de VM à l'aide de Web Client ESXi v6.0 :



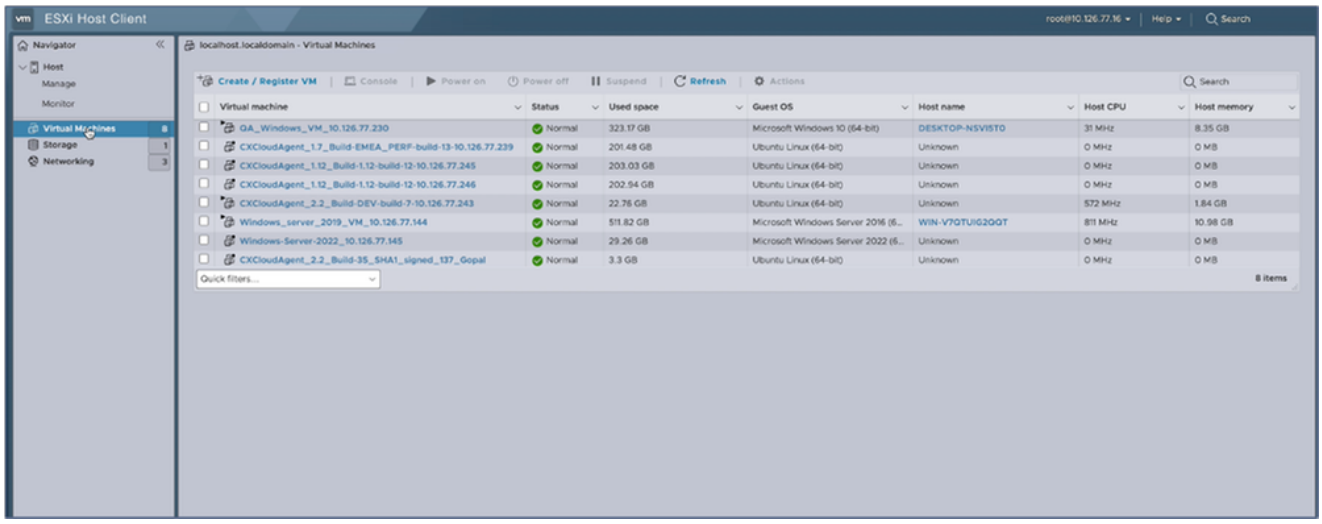
Client ESXi

1. Connectez-vous au client VMware ESXi. La page d'accueil s'affiche.



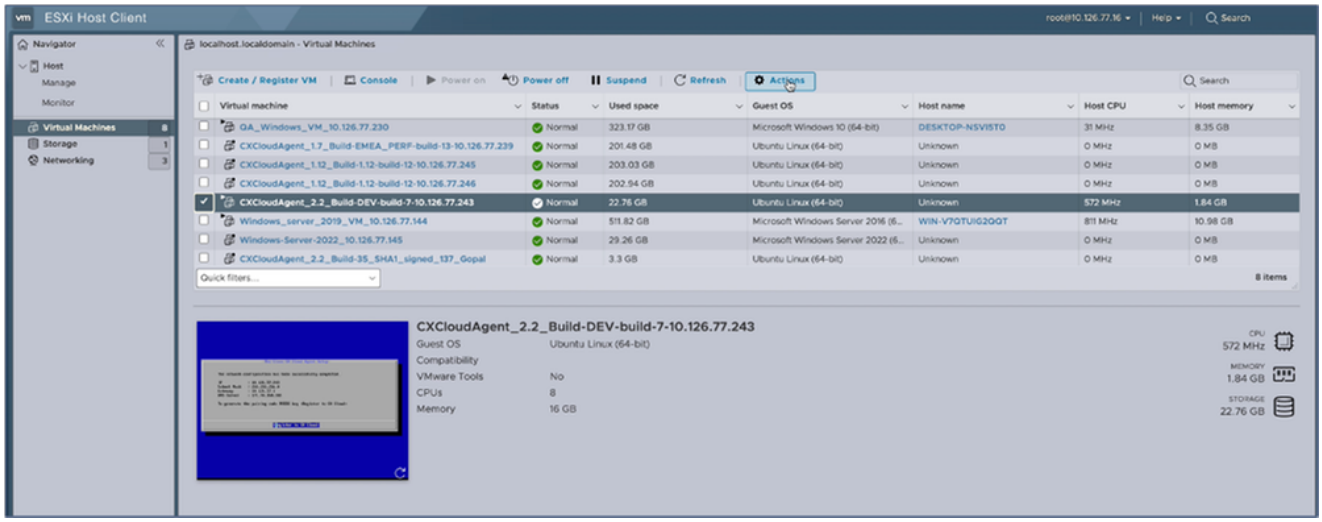
Page d'accueil ESXi

2. Cliquez sur Machine virtuelle pour afficher la liste des machines virtuelles.



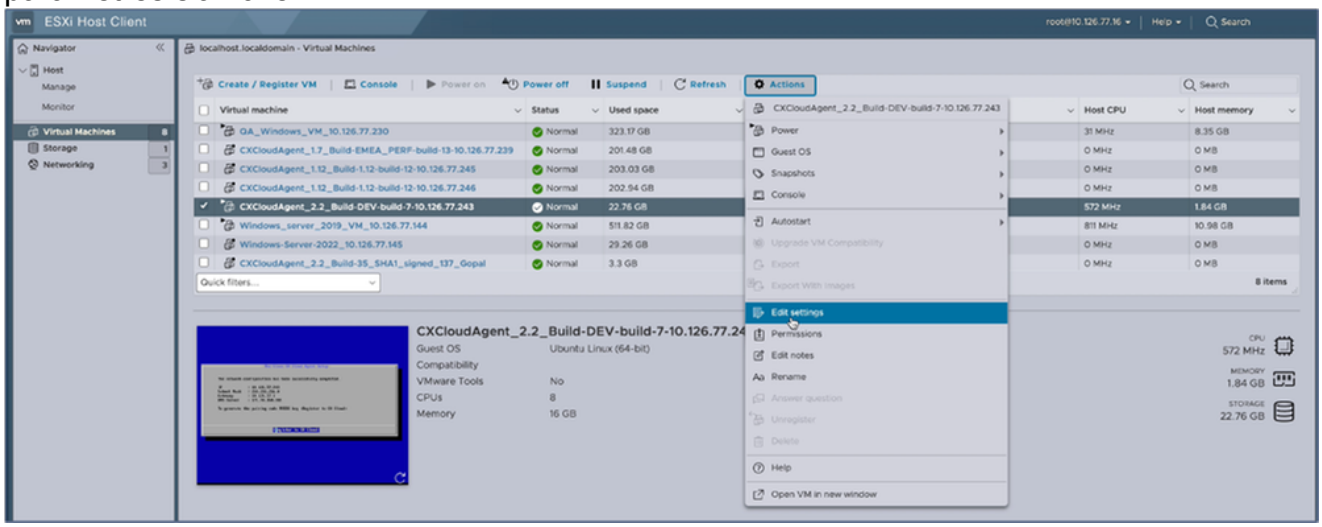
Liste des VM

3. Sélectionnez la machine virtuelle cible.

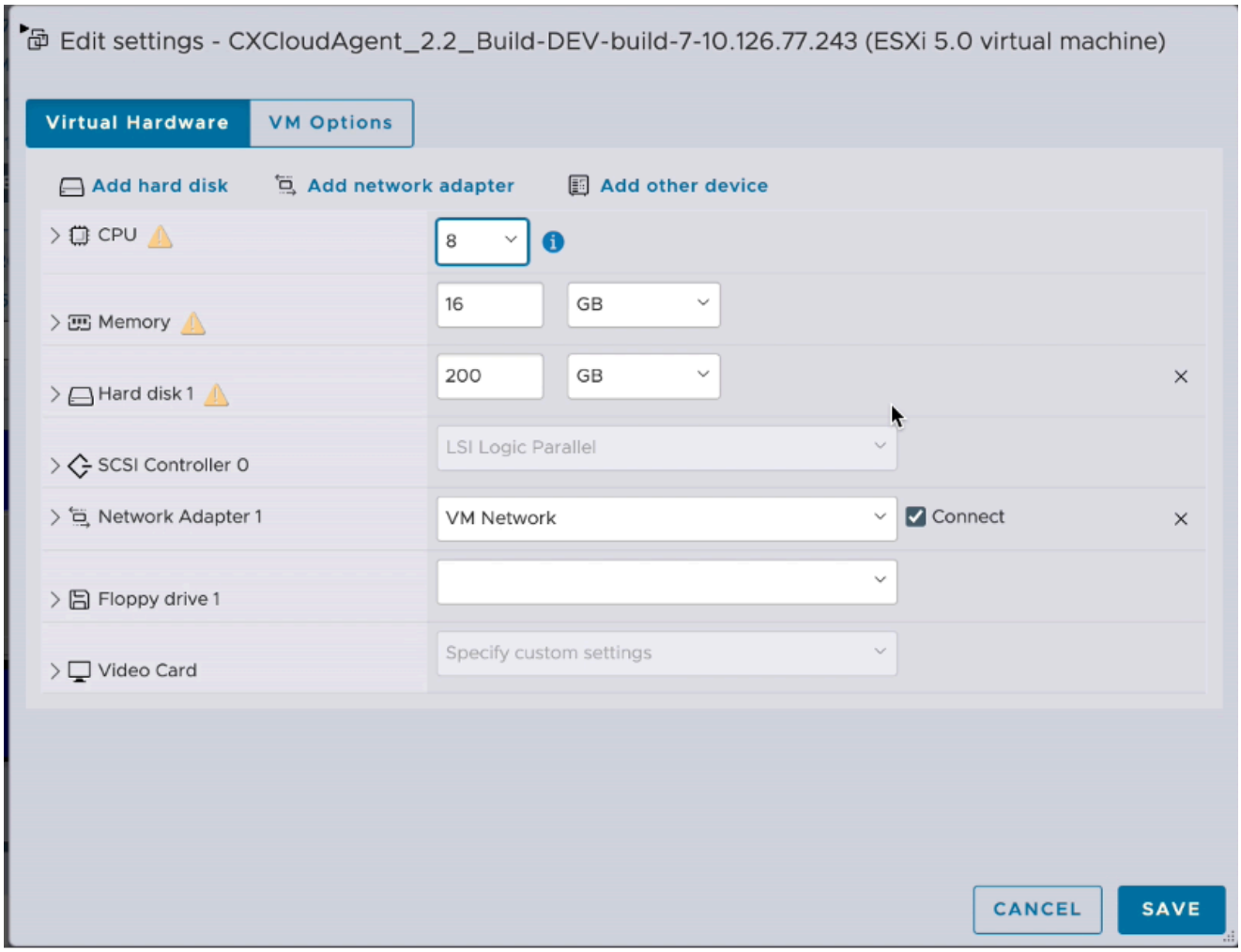


VM cible

4. Cliquez sur Actions et sélectionnez Modifier les paramètres. La fenêtre Modifier les paramètres s'affiche.

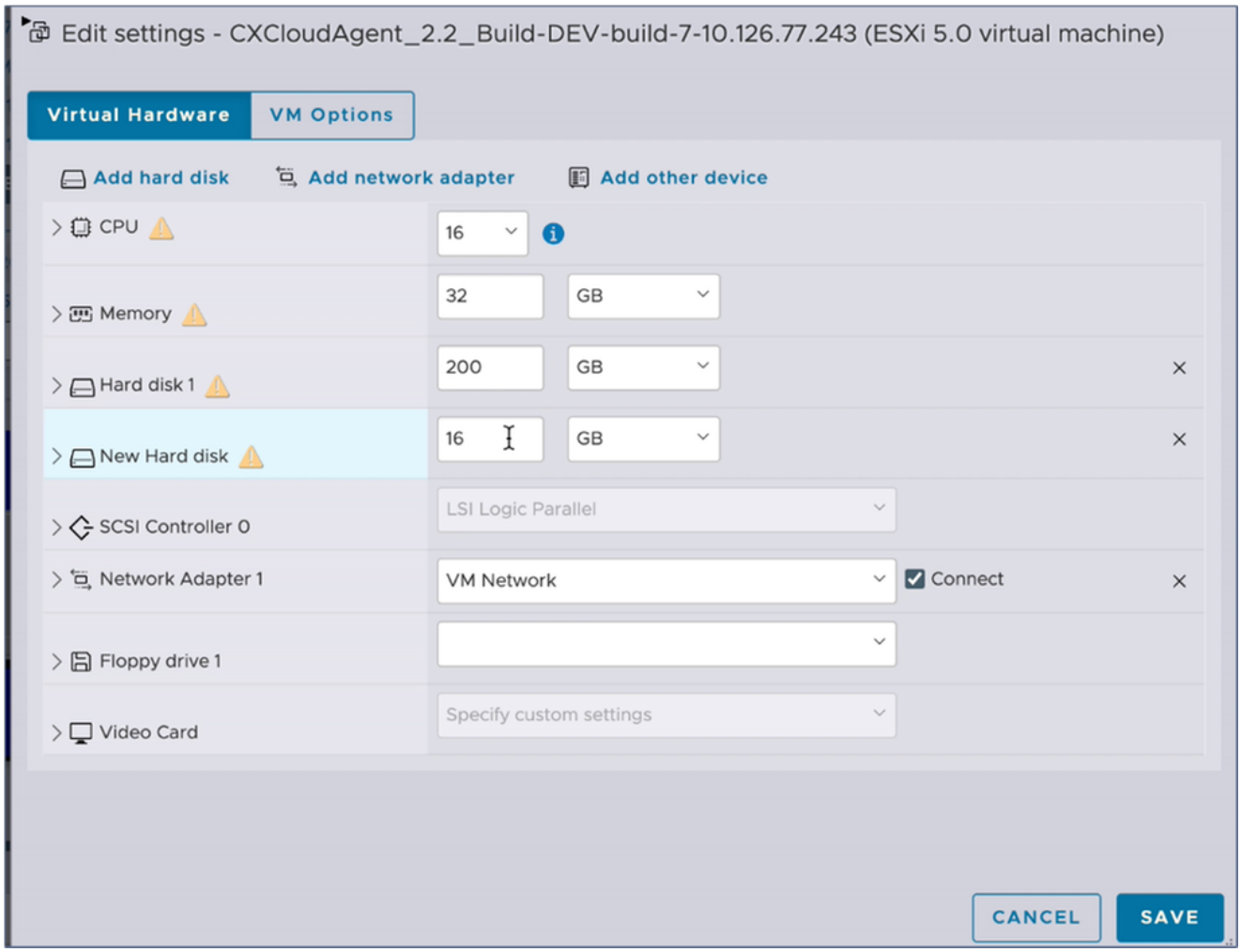


Actions



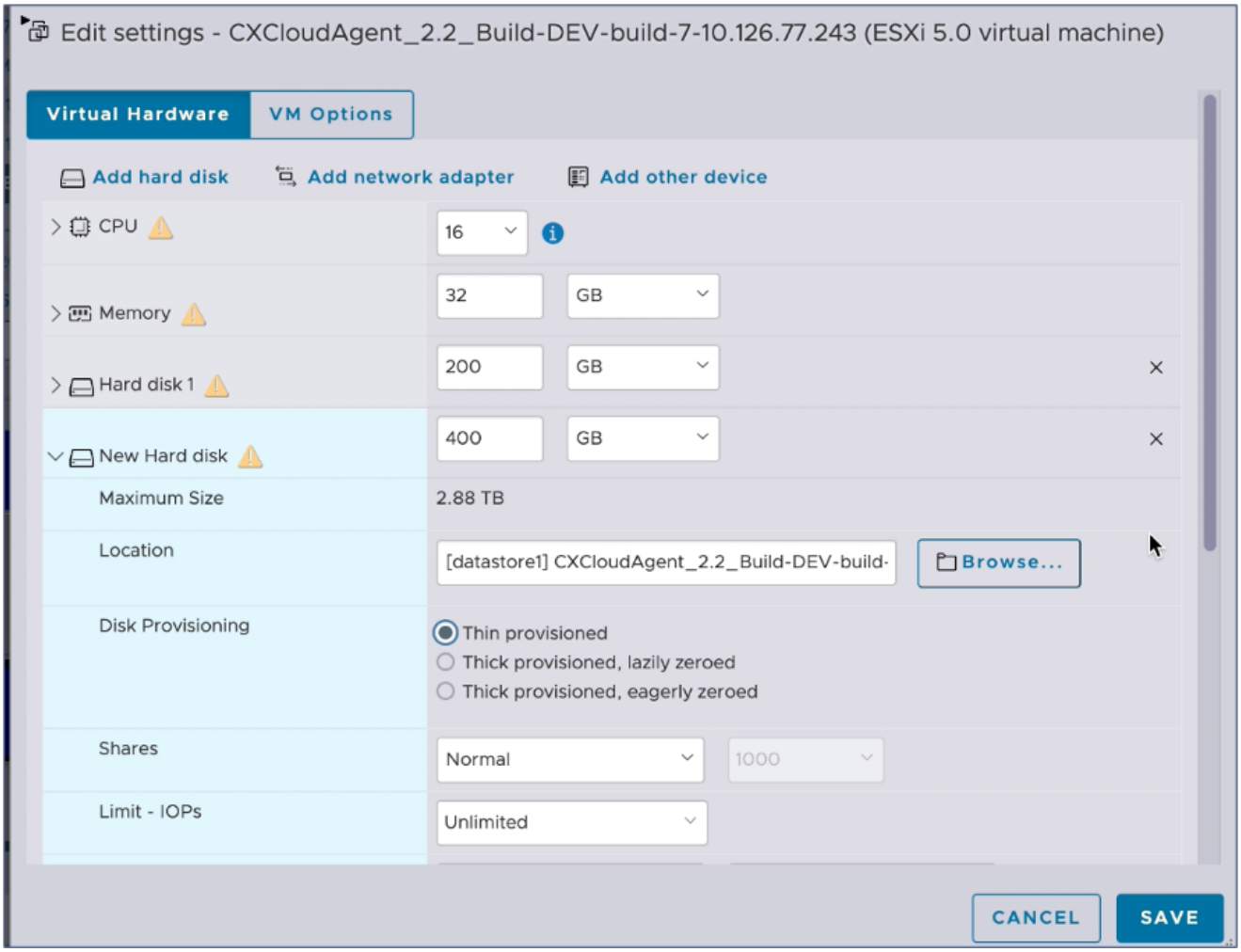
Modifier les paramètres

5. Mettez à jour la valeur CPU comme indiqué :
   Moyenne : 16 coeurs (8 connecteurs *2 coeurs/connecteurs)
   Grande : 32 coeurs (16 connecteurs *2 coeurs/connecteurs)
6. Mettez à jour la valeur Mémoire comme indiqué :
   Moyenne : 32 Go
   Grand : 64 Go
7. Cliquez sur Add hard disk > New standard hard disk. La nouvelle entrée de disque dur s'affiche dans la fenêtre Modifier les paramètres.



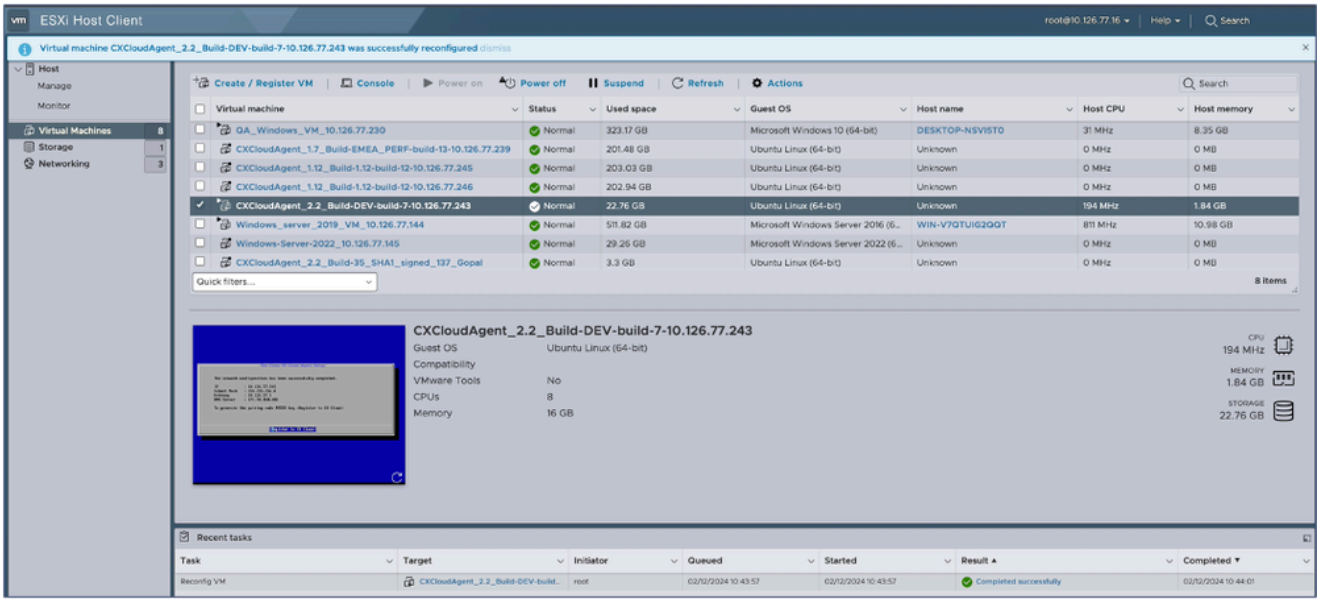
Modifier les paramètres

8. Mettre à jour les nouvelles valeurs de disque dur comme spécifié :
   Petite à moyenne : 400 Go (taille initiale : 200 Go, augmentant l'espace total à 600 Go)
   Petite à grande : 1 000 Go (taille initiale : 200 Go, augmentant l'espace total à 1 200 Go)
9. Cliquez sur la flèche pour développer Nouveau disque dur. Les propriétés s'affichent.



Modifier les paramètres

10. Sélectionnez la case d'option Thin provisioned.
11. Cliquez sur Save pour terminer la configuration. La mise à jour de configuration s'affiche dans les tâches récentes.



Tâches récentes

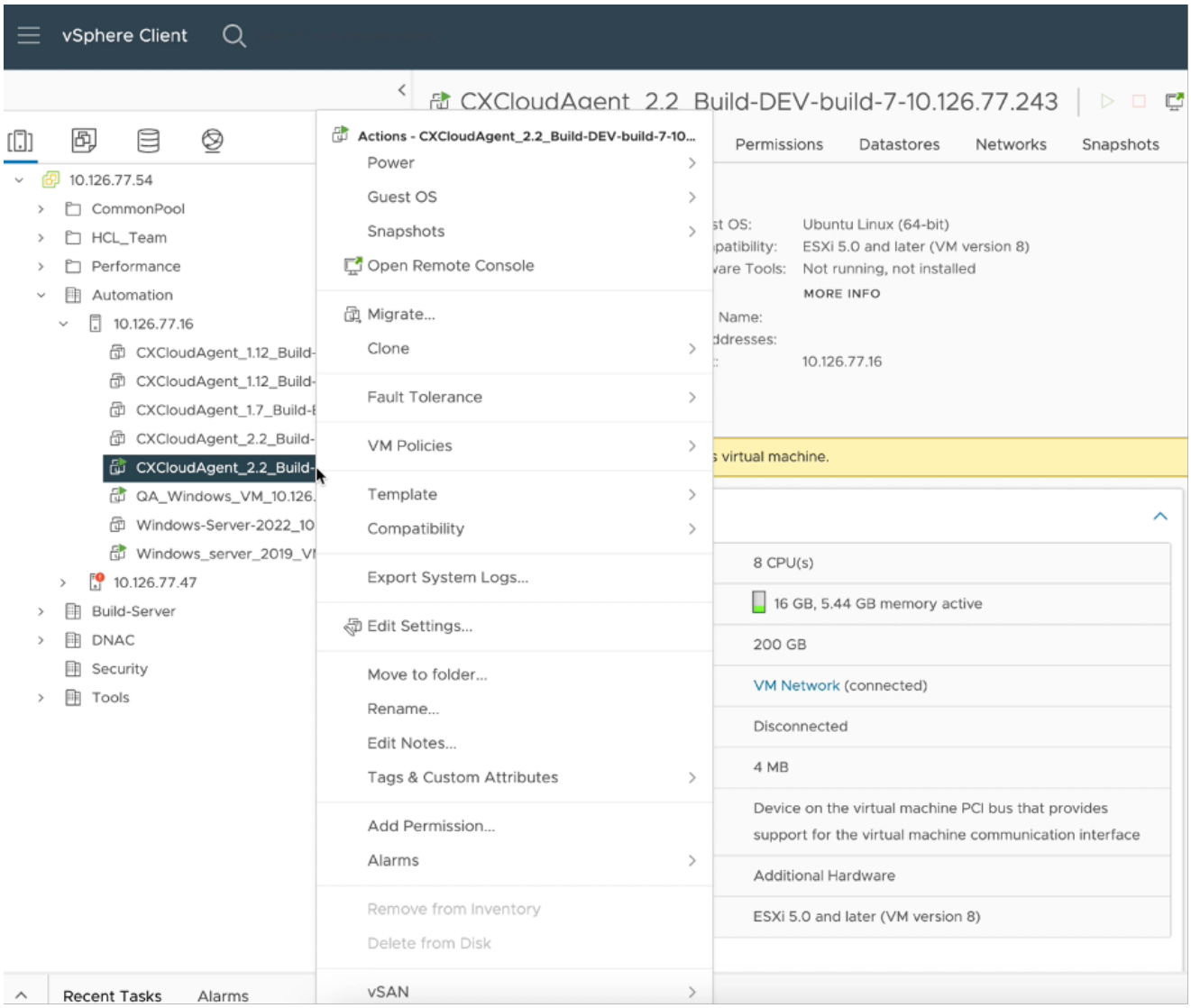
Reconfiguration à l'aide de Web Client vCenter

Pour mettre à jour les configurations de VM à l'aide de Web Client vCenter :



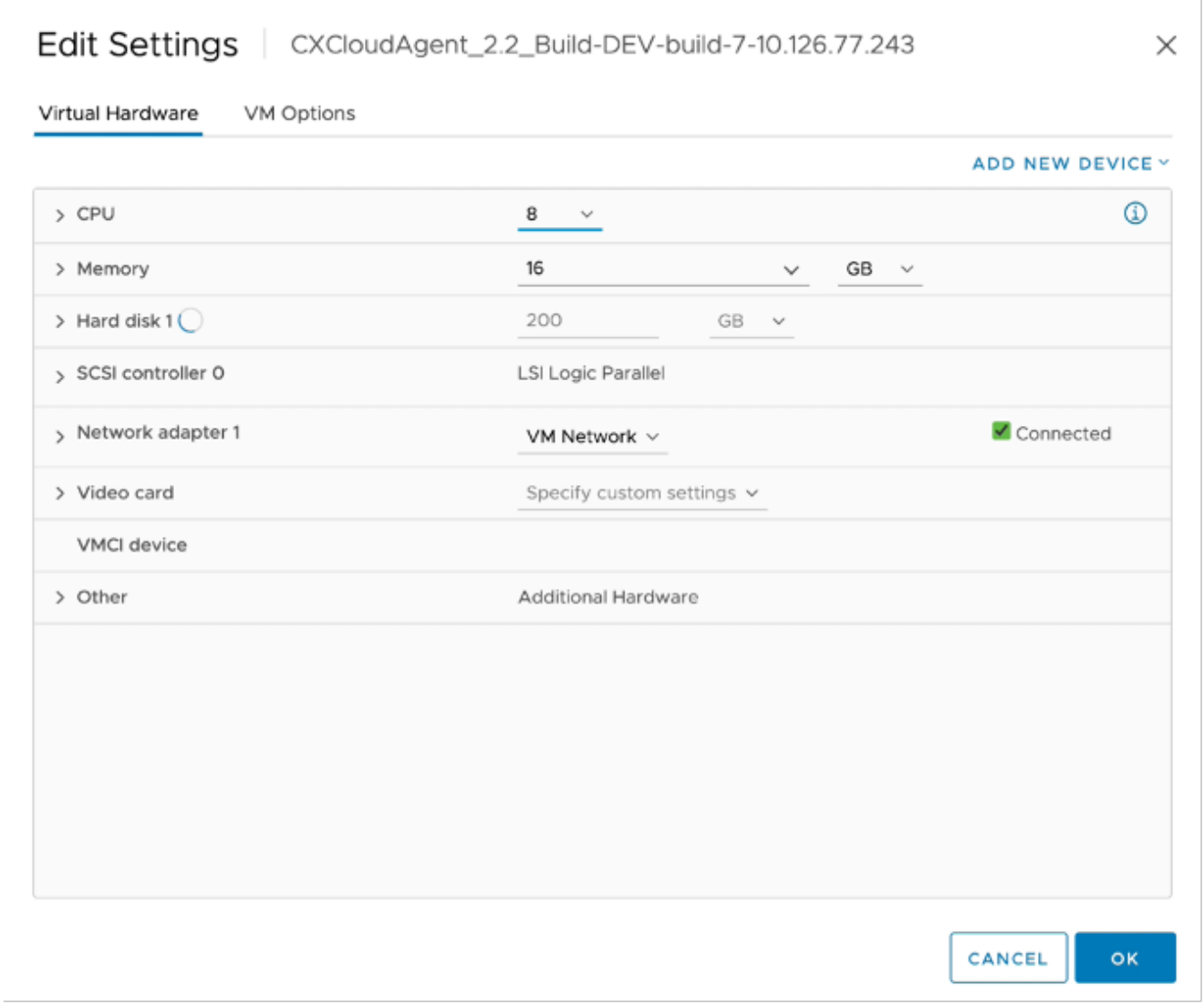
vCenter

1. Connectez-vous à vCenter. La page d'accueil s'affiche.



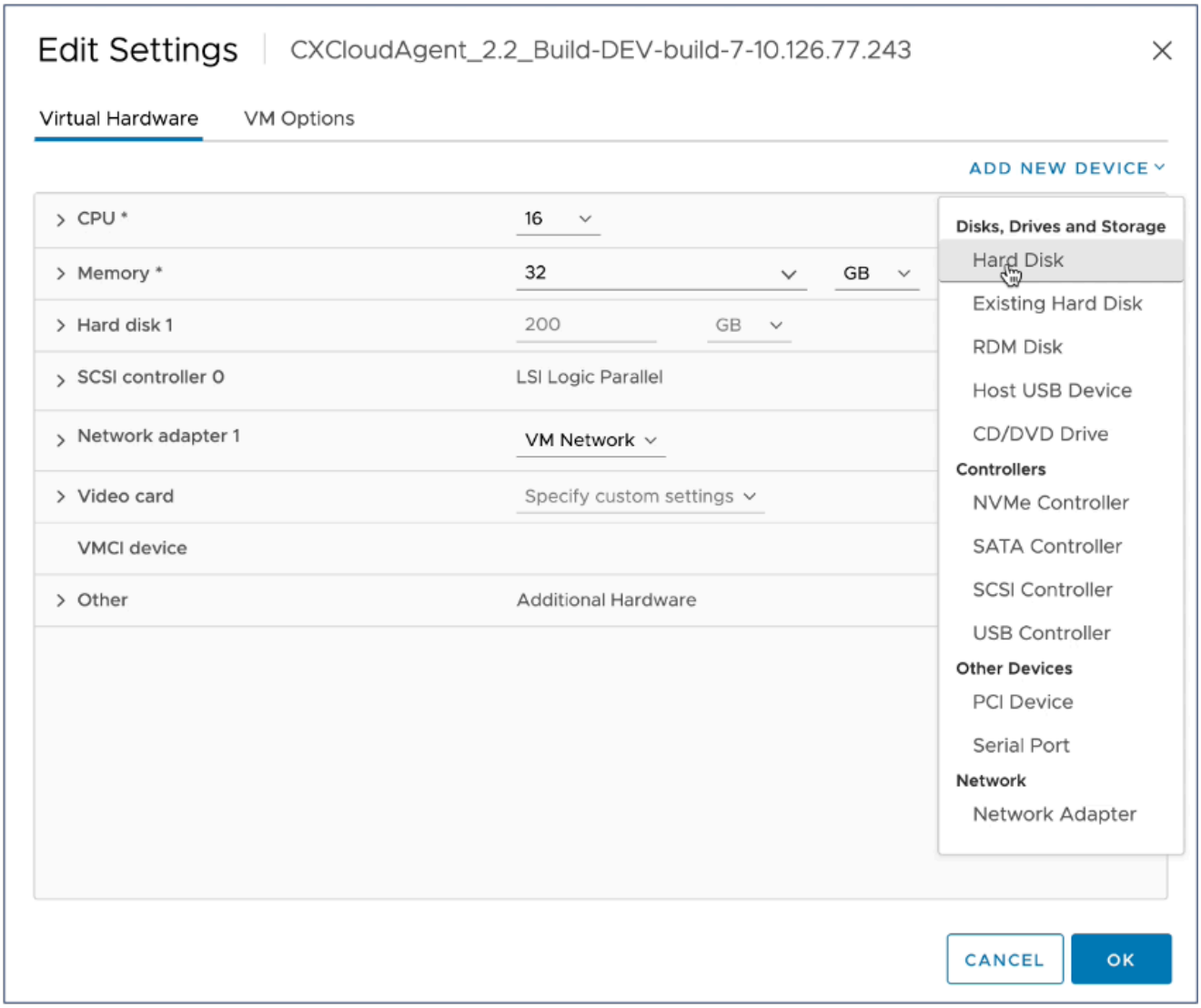
Liste des VM

2. Cliquez avec le bouton droit sur la machine virtuelle cible et sélectionnez Modifier les paramètres dans le menu. La fenêtre Modifier les paramètres s'affiche.



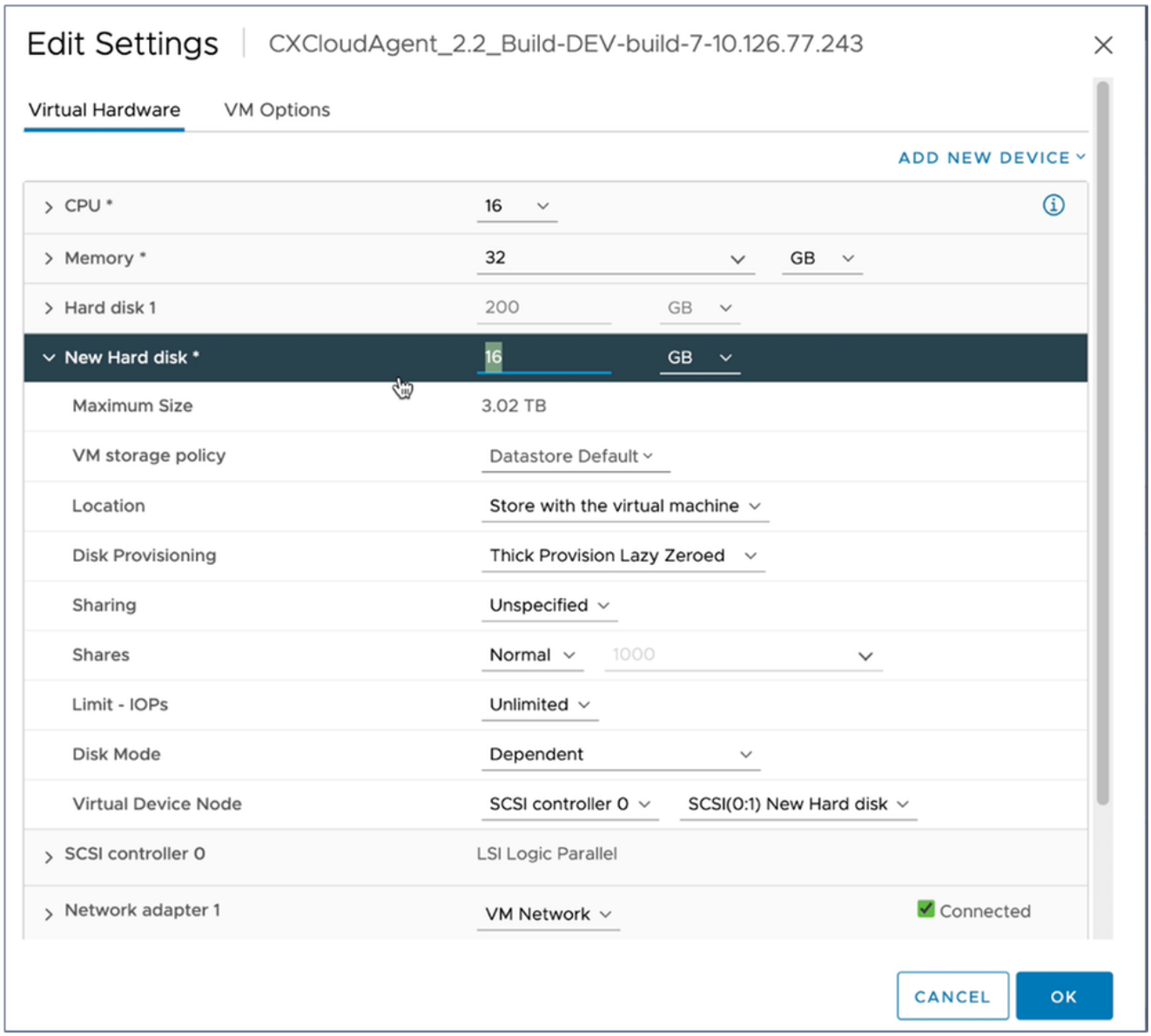
Modifier les paramètres

3. Mettre à jour les valeurs CPU comme spécifié:
   Moyenne : 16 coeurs (8 connecteurs *2 coeurs/connecteurs)
   Grande : 32 coeurs (16 connecteurs *2 coeurs/connecteurs)
4. Mettez à jour les valeurs de mémoire comme indiqué :
   Moyenne : 32 Go
   Grand : 64 Go



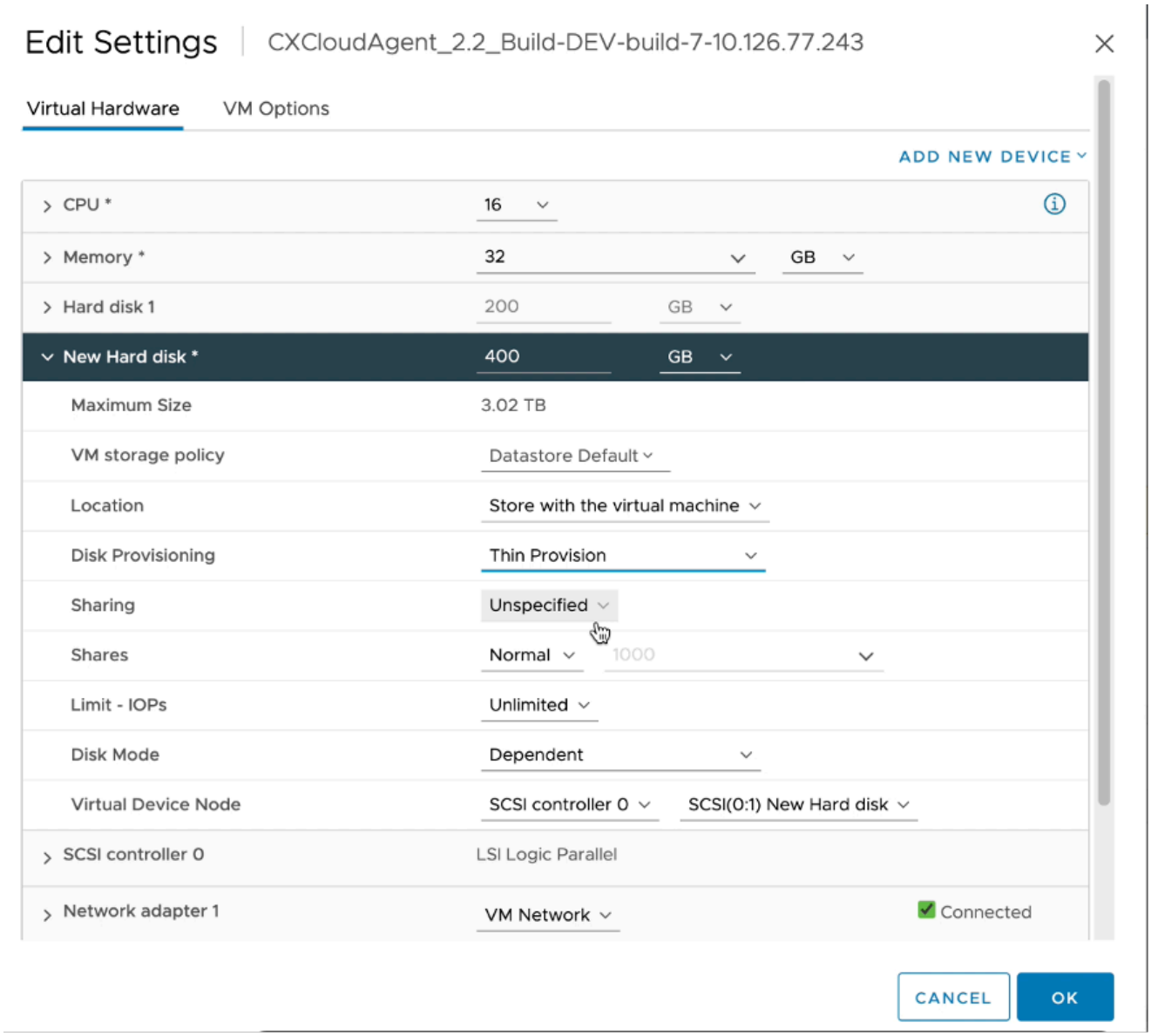
Modifier les paramètres

5. Cliquez sur Add New Device et sélectionnez Hard Disk. L'entrée Nouveau disque dur est ajoutée.



Modifier les paramètres

6. Mettre à jour la nouvelle mémoire du disque dur comme spécifié :
   Petite à moyenne : 400 Go (taille initiale : 200 Go, augmentant l'espace total à 600 Go)
   Petite à grande : 1 000 Go (taille initiale : 200 Go, augmentant l'espace total à 1 200 Go)



Modifier les paramètres

7. Sélectionnez Provisionnement léger dans la liste déroulante Provisionnement de disque.
8. Cliquez sur OK pour terminer la mise à niveau.

Déploiement et configuration du réseau

Sélectionnez l'une des options suivantes pour déployer l'agent CX :

- VMware vSphere/vCenter Thick Client ESXi 5.5/6.0
- Installation de VMware vSphere/vCenter Web Client ESXi 6.0 ou Web Client vCenter
- Oracle Virtual Box 7.0.12
- Installation de Microsoft Hyper-V

Déploiement OVA

Installation du client lourd ESXi 5.5/6.0

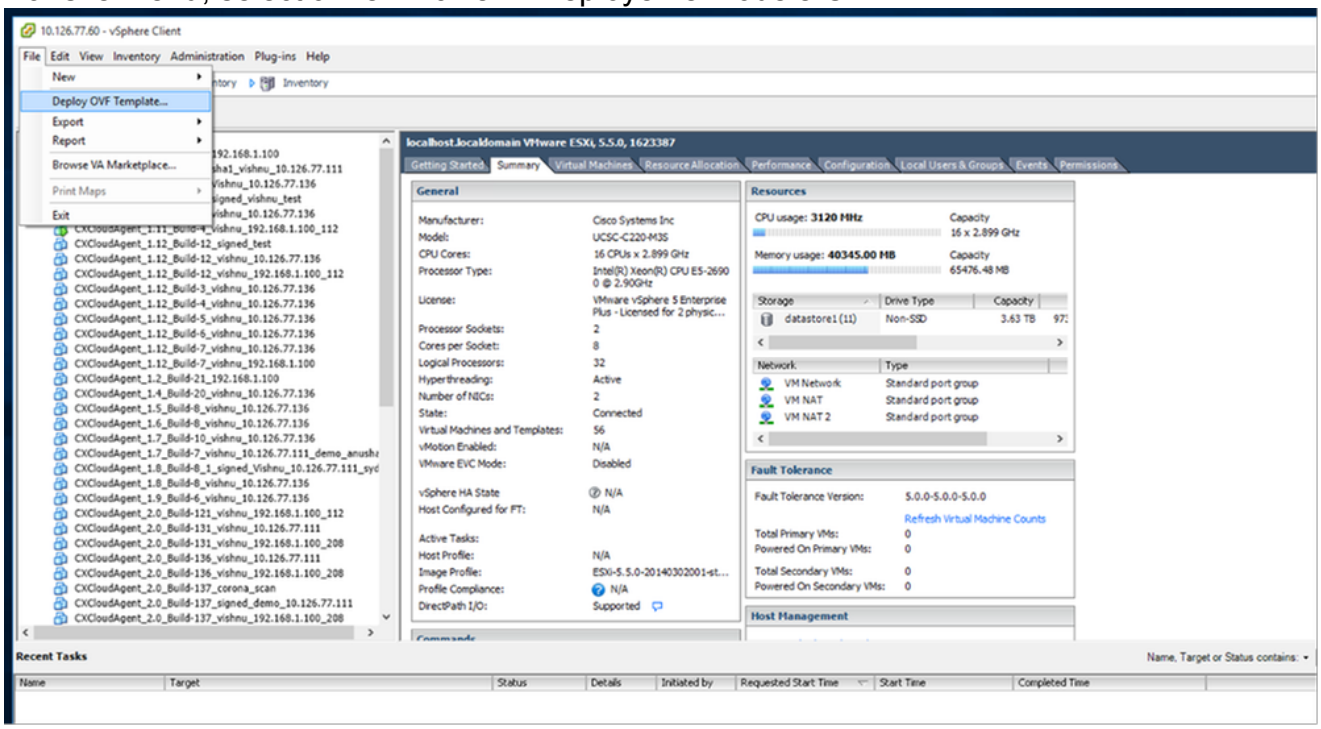
Ce client permet le déploiement de CX Agent OVA en utilisant le client vSphere épais.

1. Après avoir téléchargé l'image, lancez le client VMware vSphere et connectez-vous.



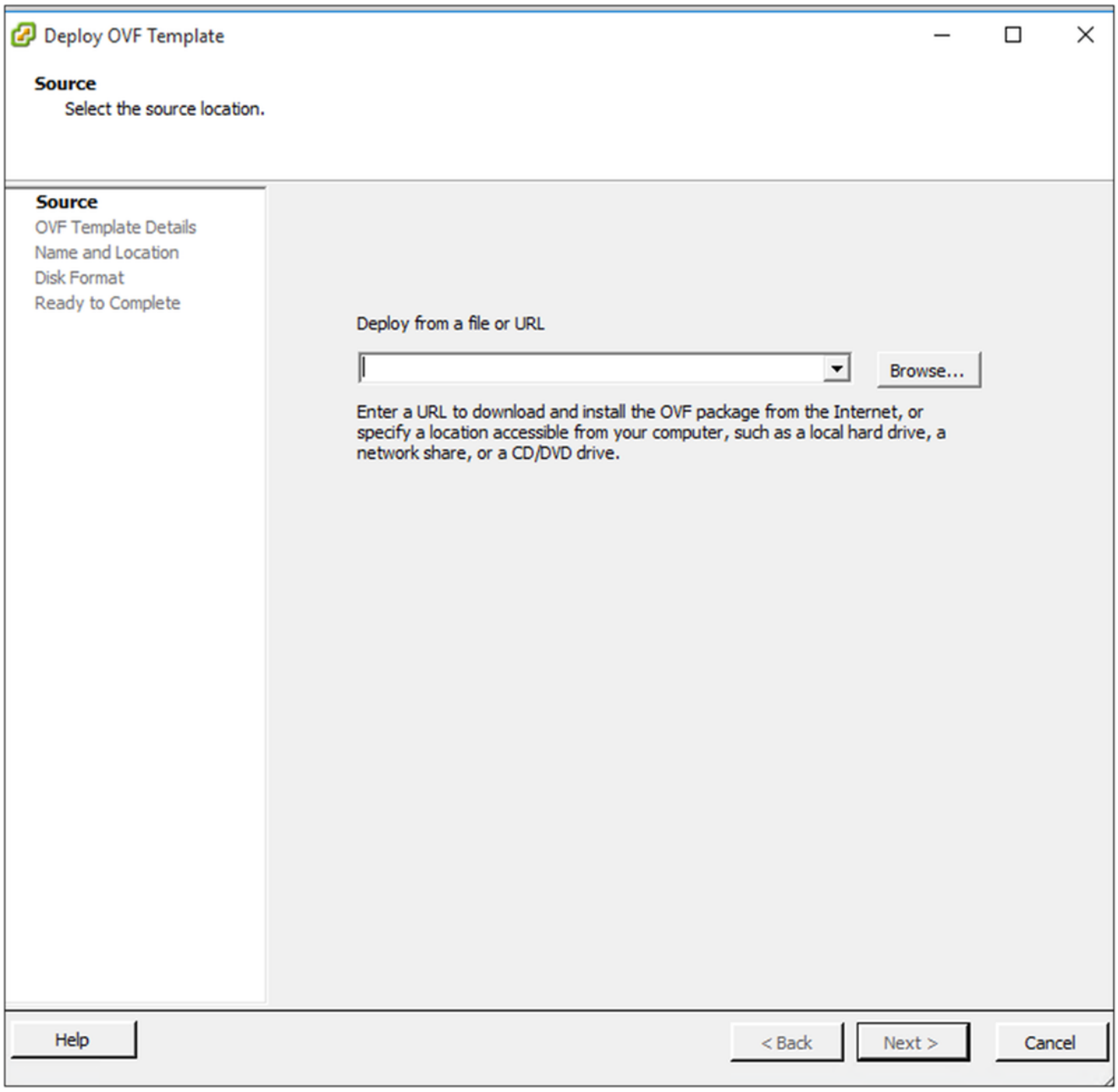
Connexion

2. Dans le menu, sélectionnez Fichier > Déployer le modèle OVF.



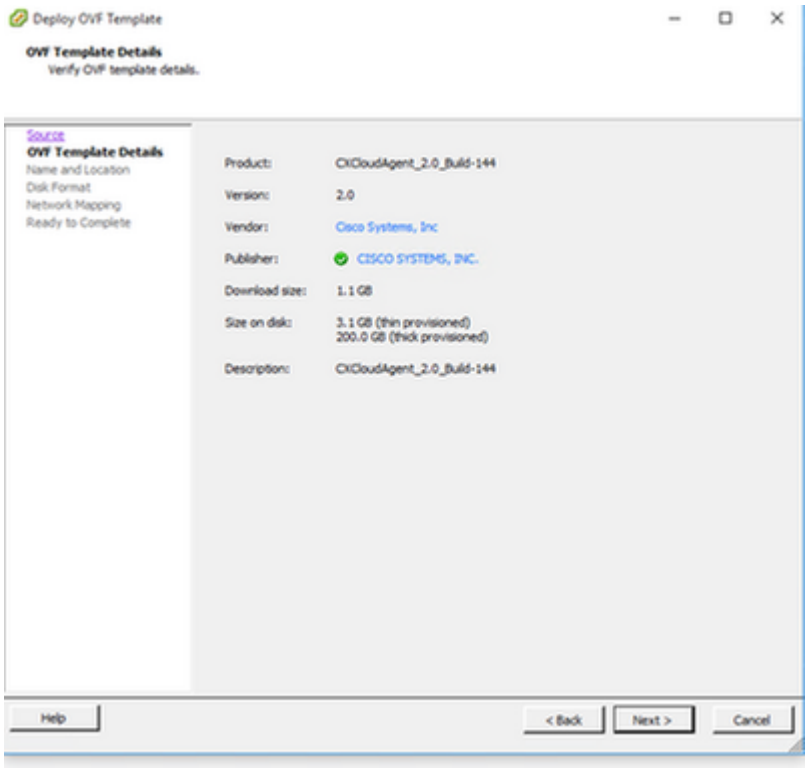
vSphere Client

3. Sélectionnez le fichier OVA, puis cliquez sur Next (Suivant).



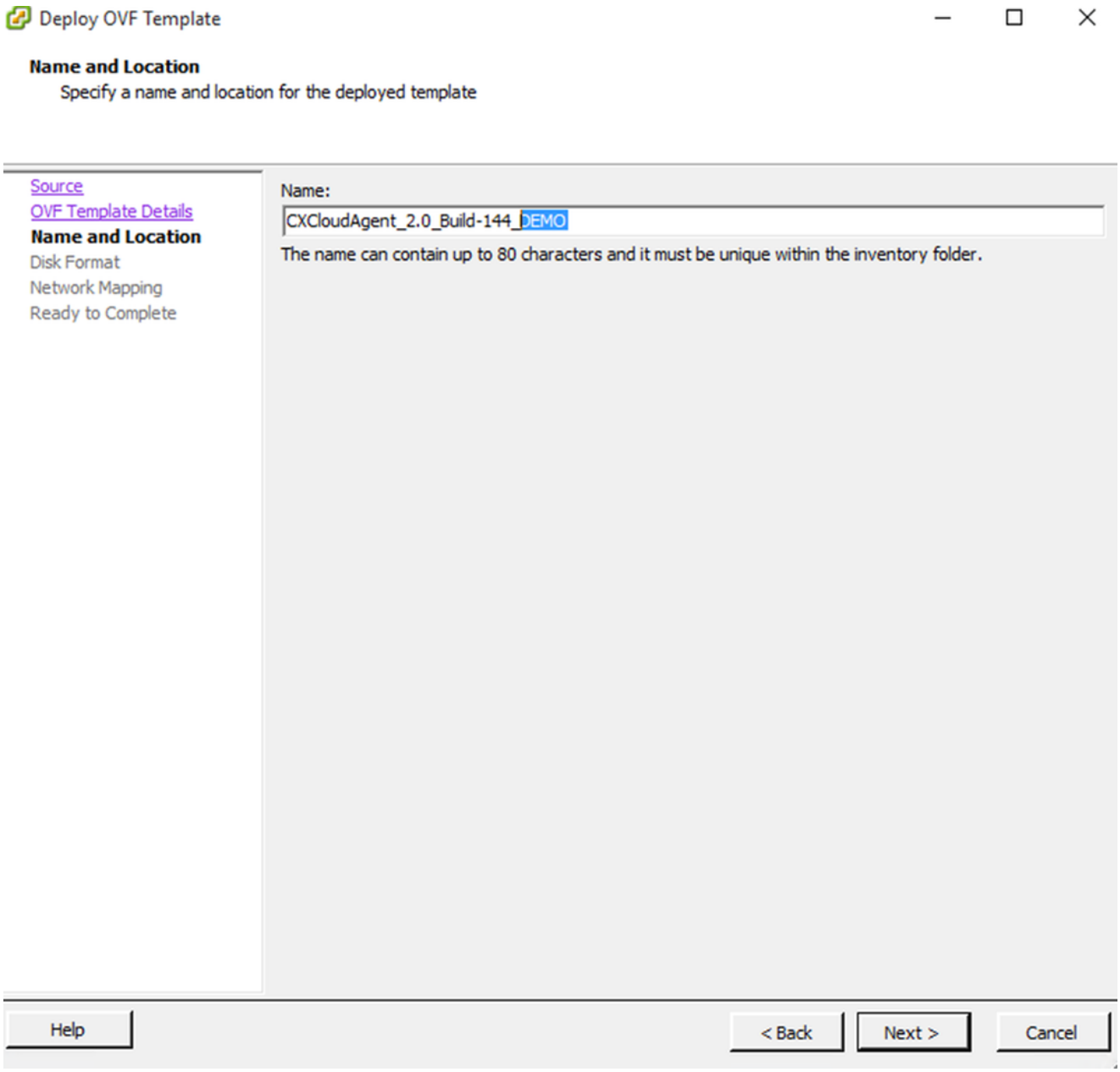
Chemin OVA

4. Vérifiez les détails OVF et cliquez sur Next.



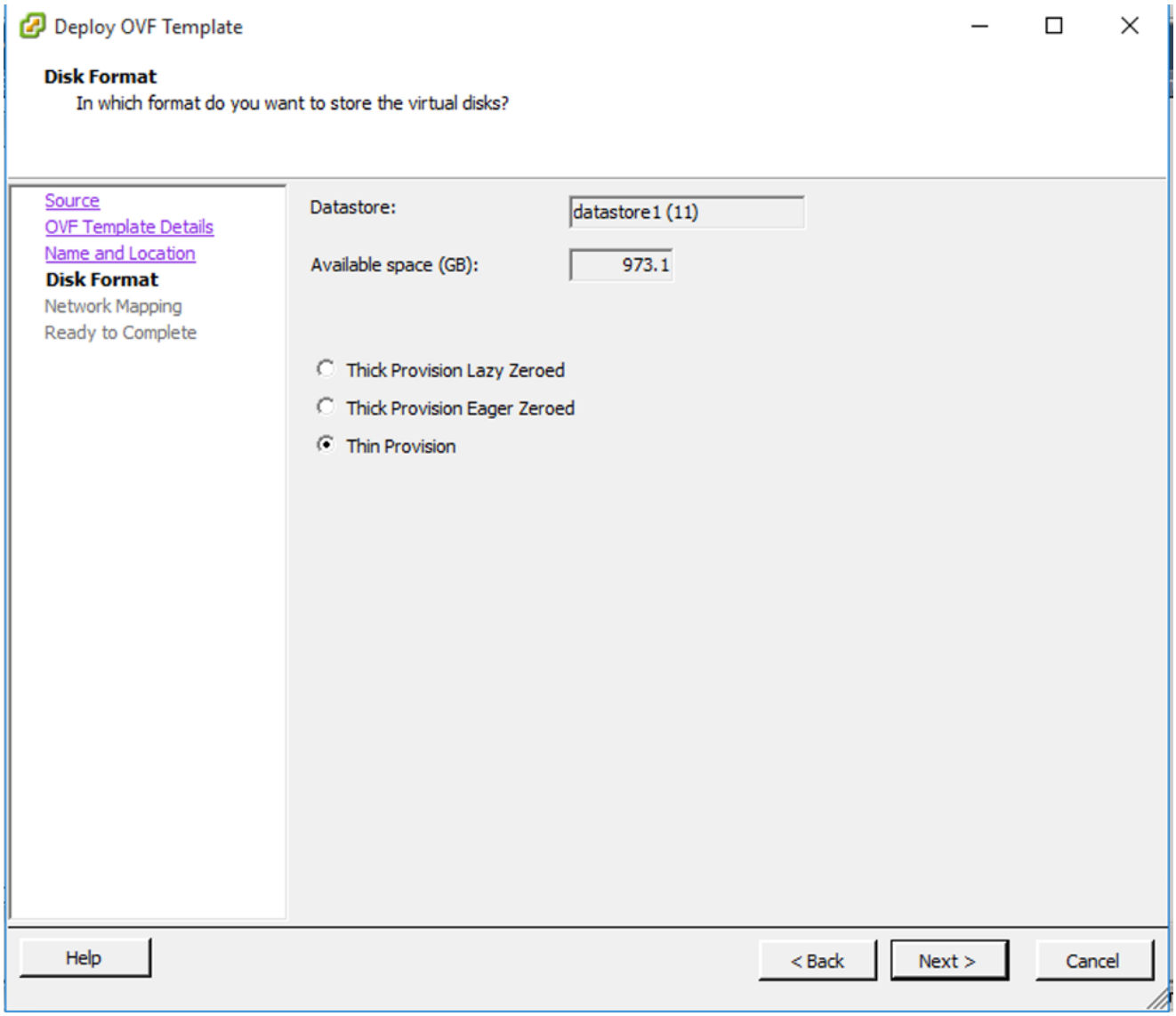
Détails du modèle

5. Entrez un nom unique et cliquez sur Suivant.



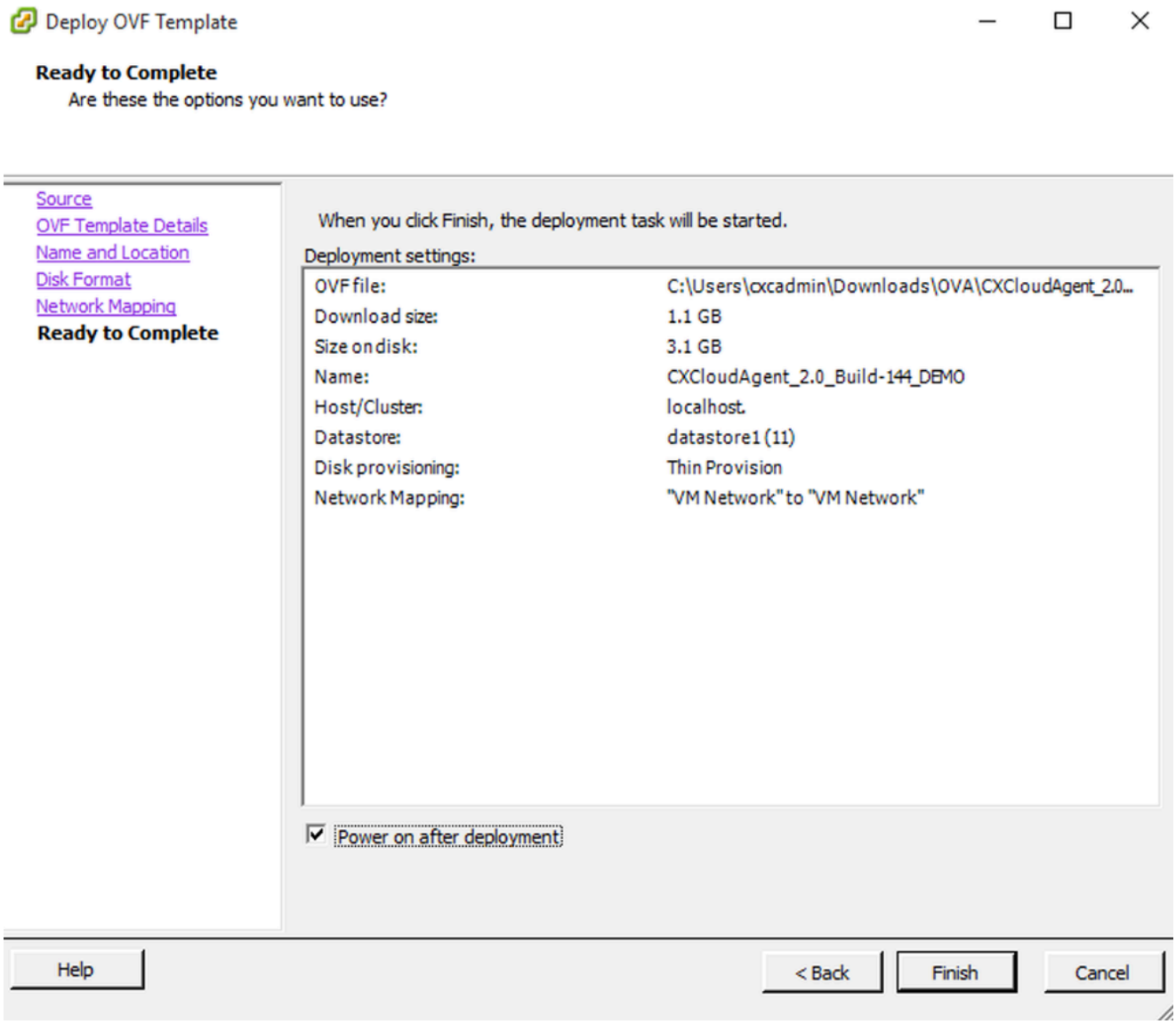
Nom et emplacement

6. Sélectionnez un format de disque et cliquez sur Next (Thin Provisioning est recommandé).



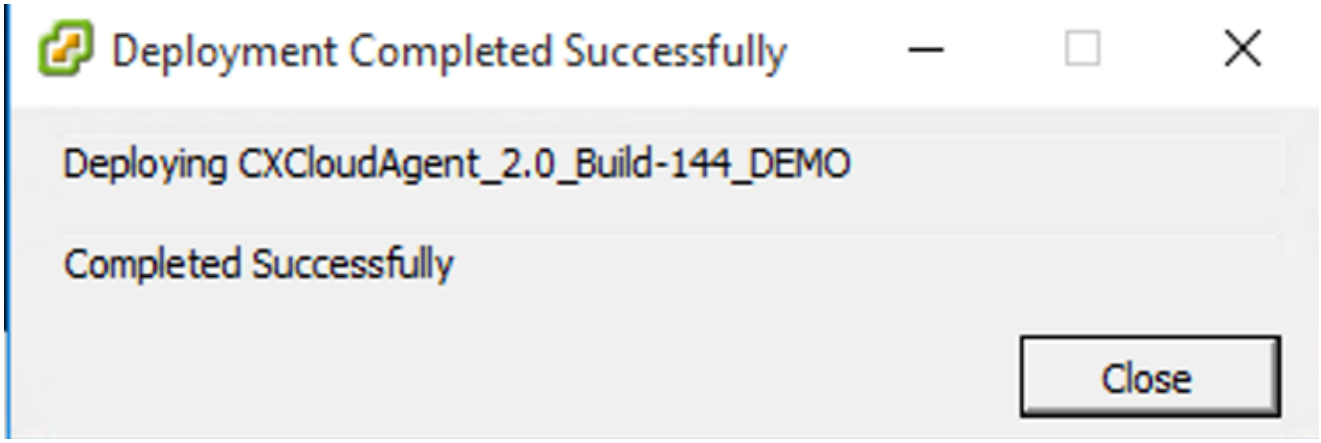
Format de disque

7. Activez la case à cocher Mise sous tension après le déploiement et cliquez sur Fermer.



Prêt pour la confirmation

Le déploiement peut prendre plusieurs minutes. La confirmation s'affiche après un déploiement réussi.



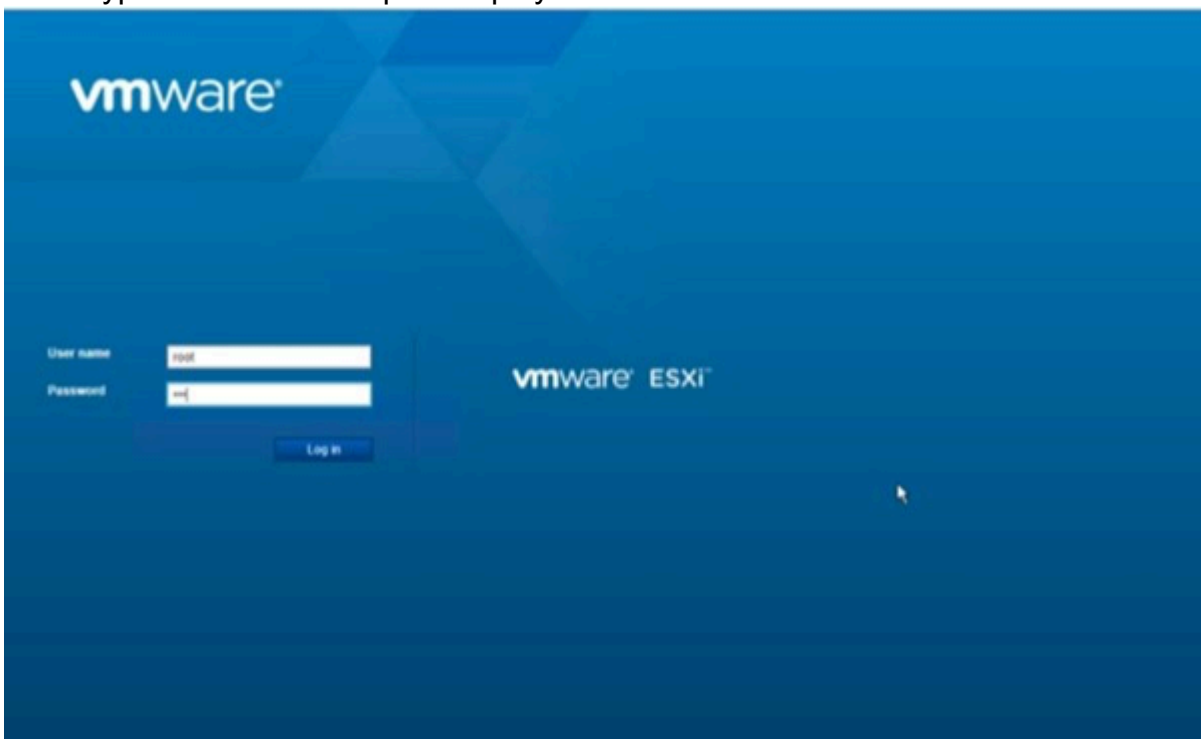
Déploiement terminé

8. Sélectionnez la machine virtuelle déployée, ouvrez la console et accédez à Network Configuration pour passer aux étapes suivantes.

Installation du client Web ESXi 6.0

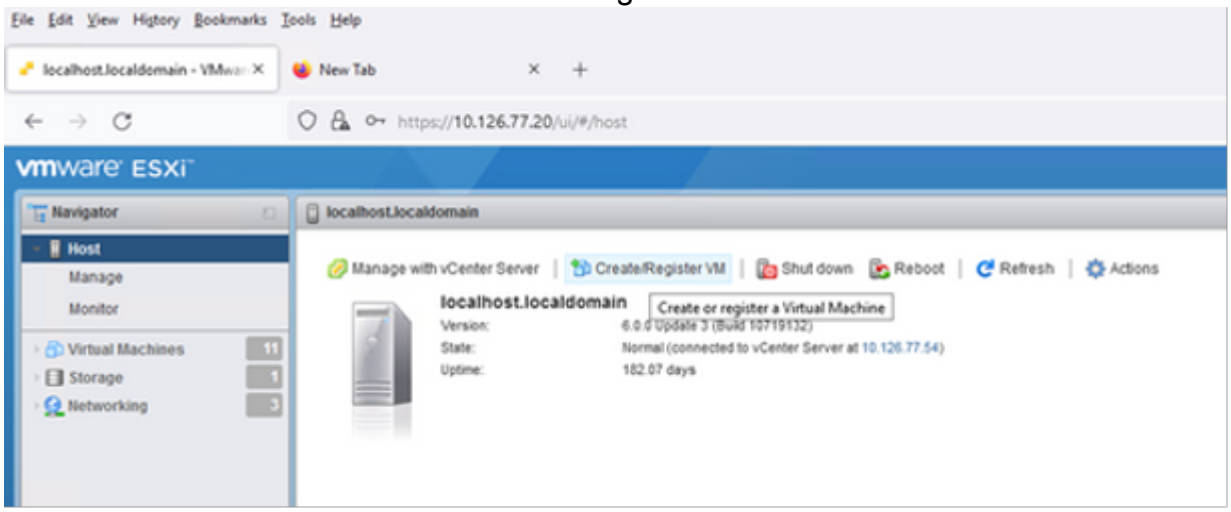
Ce client déploie CX Cloud OVA en utilisant le Web vSphere.

1. Connectez-vous à l'interface utilisateur VMWare avec les informations d'identification ESXi/hyperviseur utilisées pour déployer la machine virtuelle.



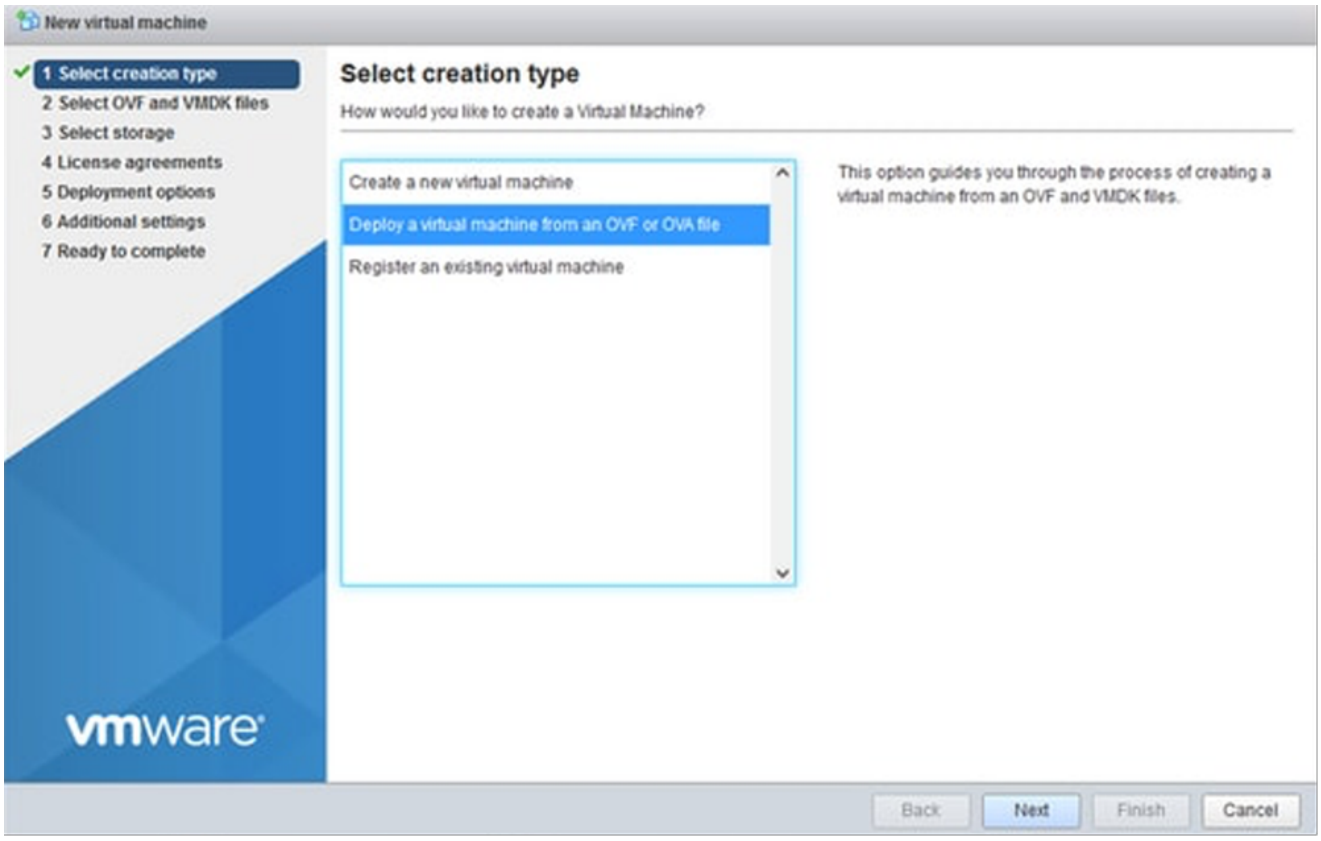
Connexion VMware ESXi

2. Sélectionnez Virtual Machine > Create / Register VM.



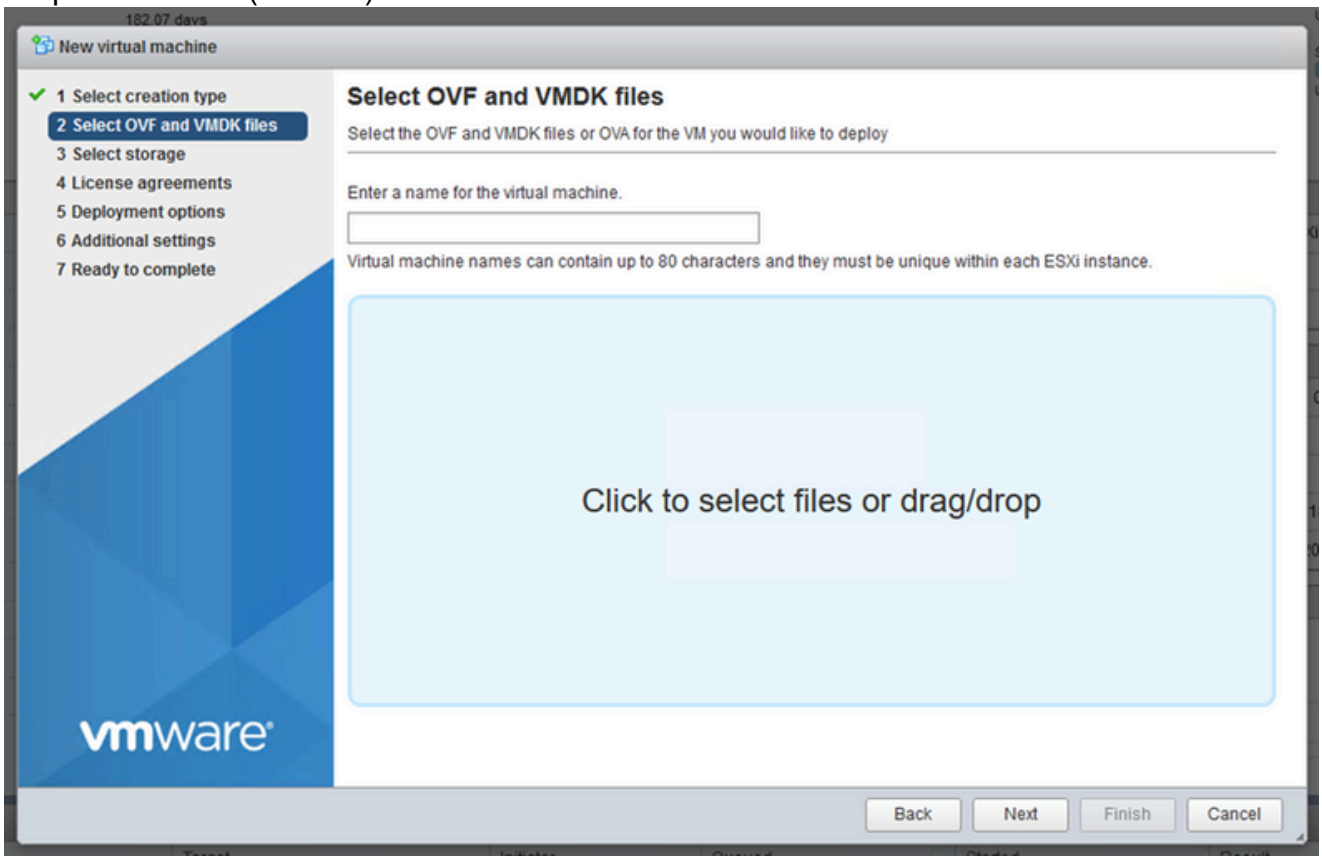
Créer une machine virtuelle

3. Sélectionnez Deploy a virtual machine from an OVF or OVA file et cliquez sur Next.



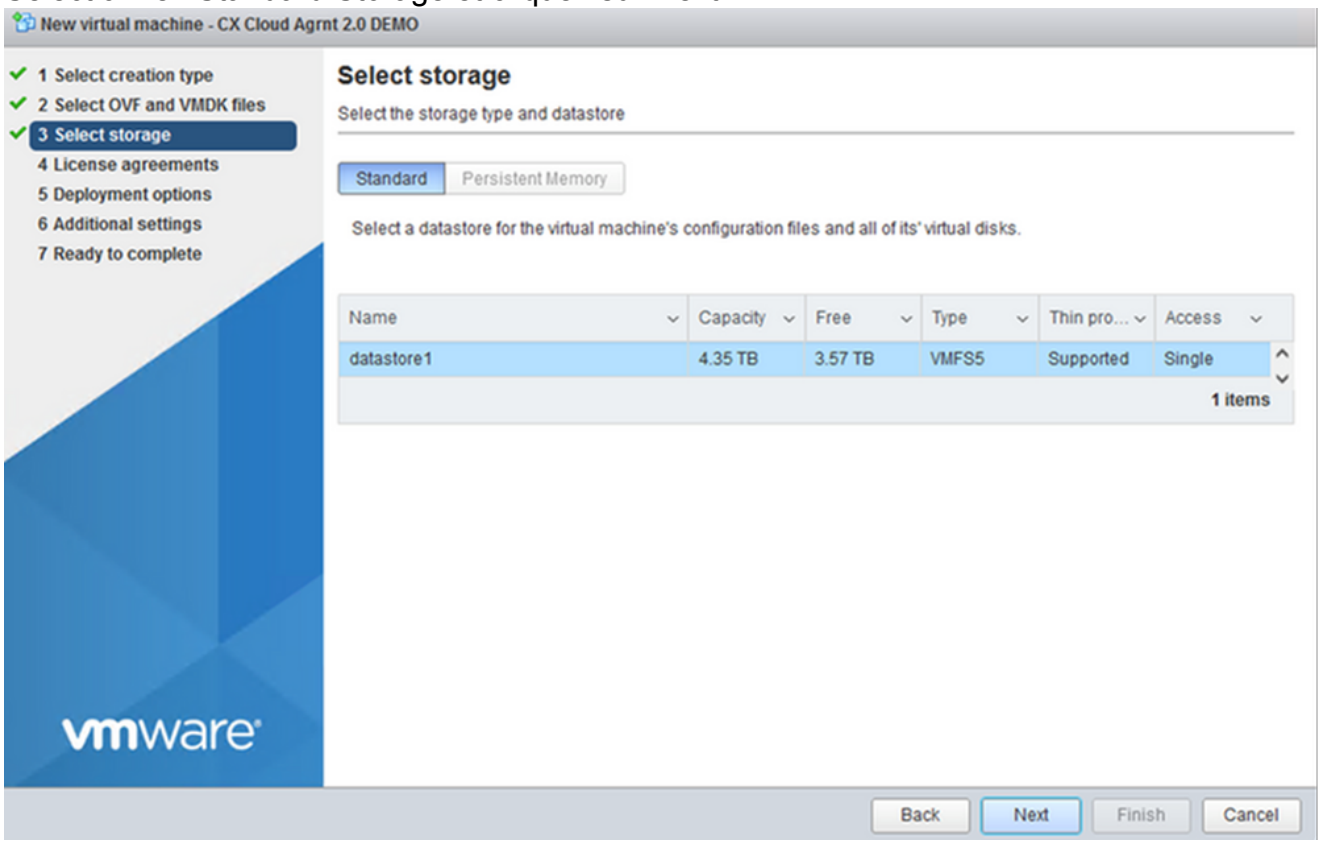
Sélectionner le type de création

4. Saisissez le nom de la machine virtuelle, recherchez le fichier ou faites glisser le fichier OVA téléchargé.
5. Cliquez sur Next (Suivant).



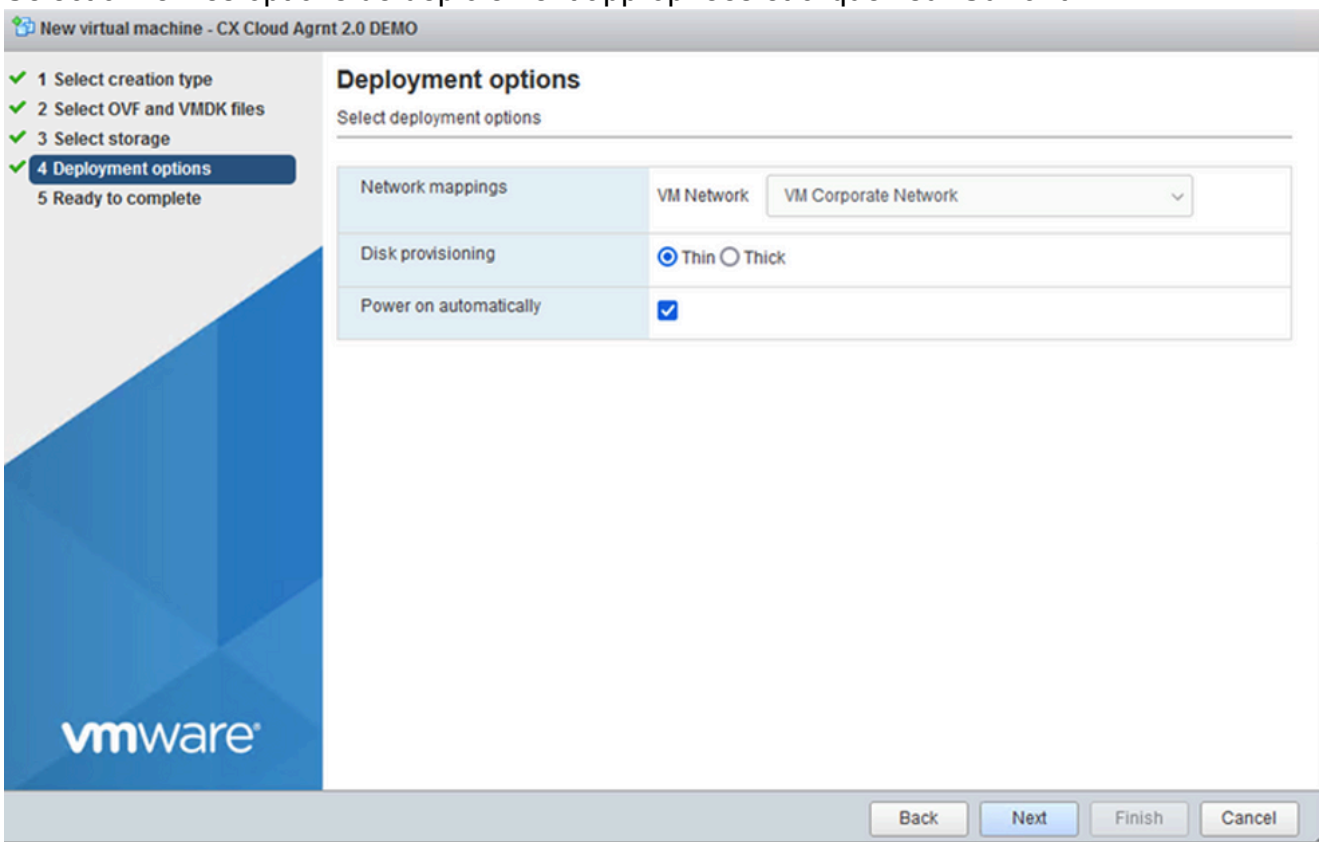
Sélection OVA

6. Sélectionnez Standard Storage et cliquez sur Next.



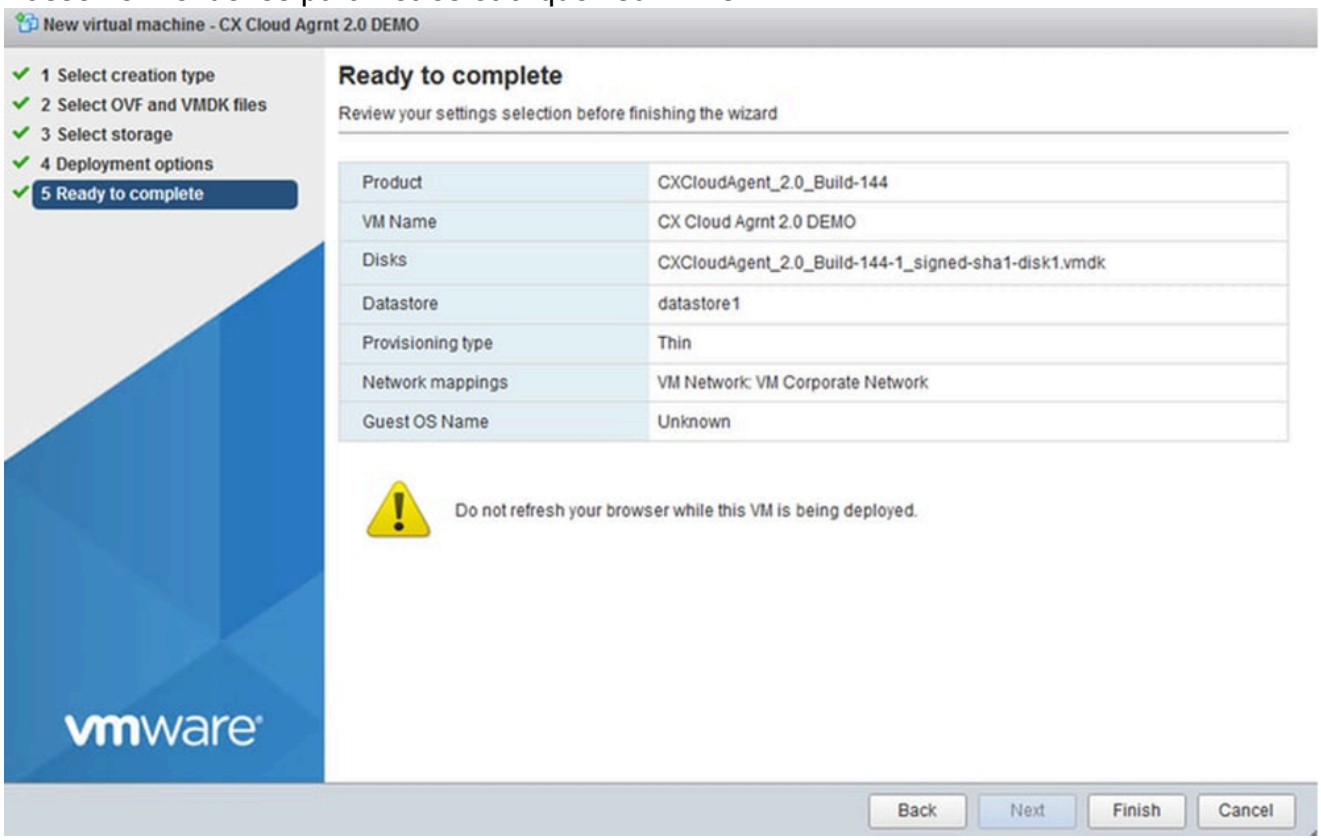
Sélectionner le stockage

7. Sélectionnez les options de déploiement appropriées et cliquez sur Suivant.

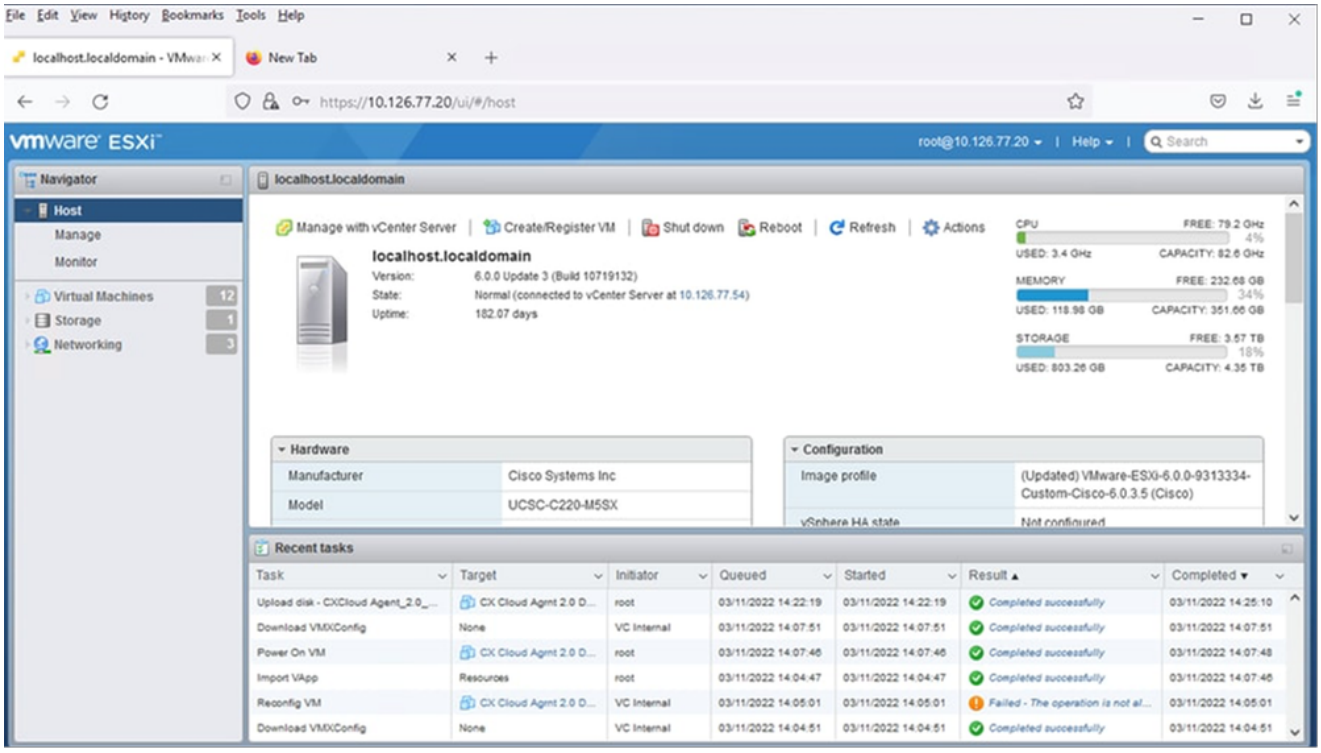


Options de déploiement

8. Passez en revue les paramètres et cliquez sur Finish.

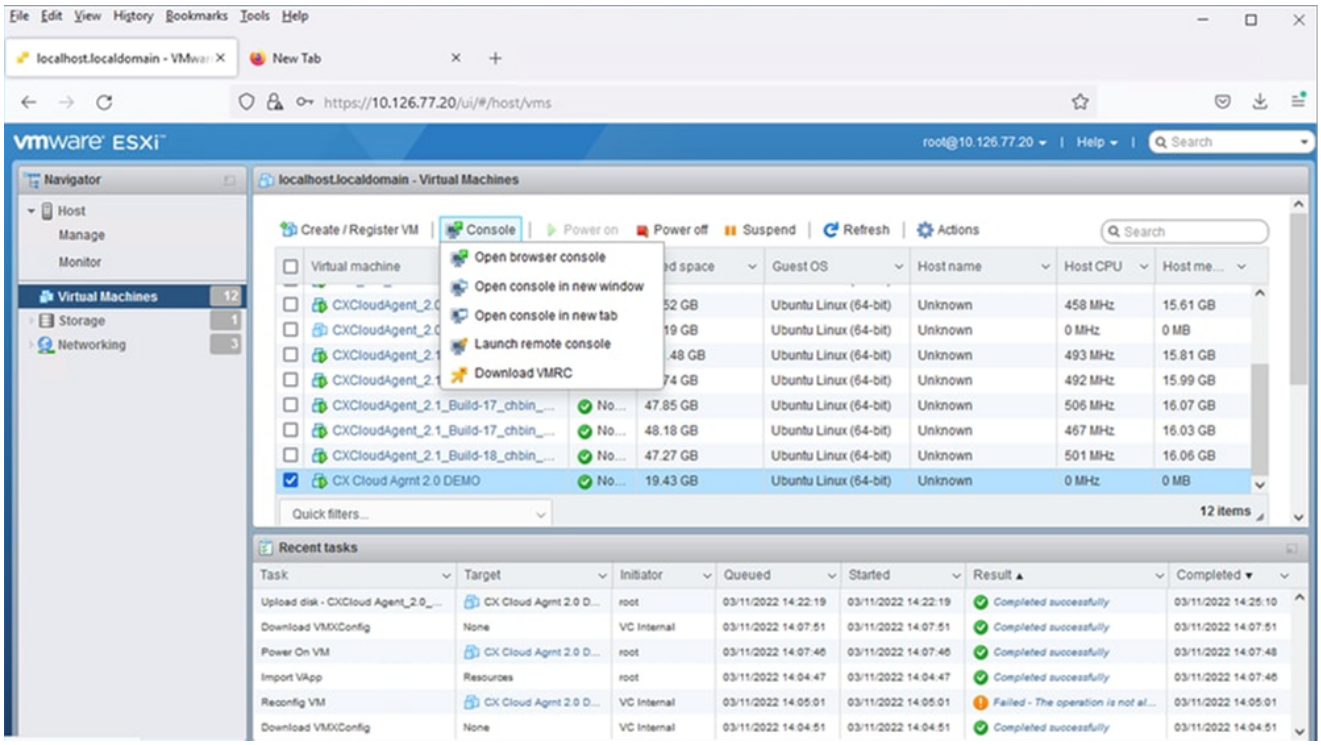


Prêt pour la confirmation



Confirmation réussie

9. Sélectionnez la VM que vous venez de déployer et sélectionnez Console > Ouvrir la console du navigateur.



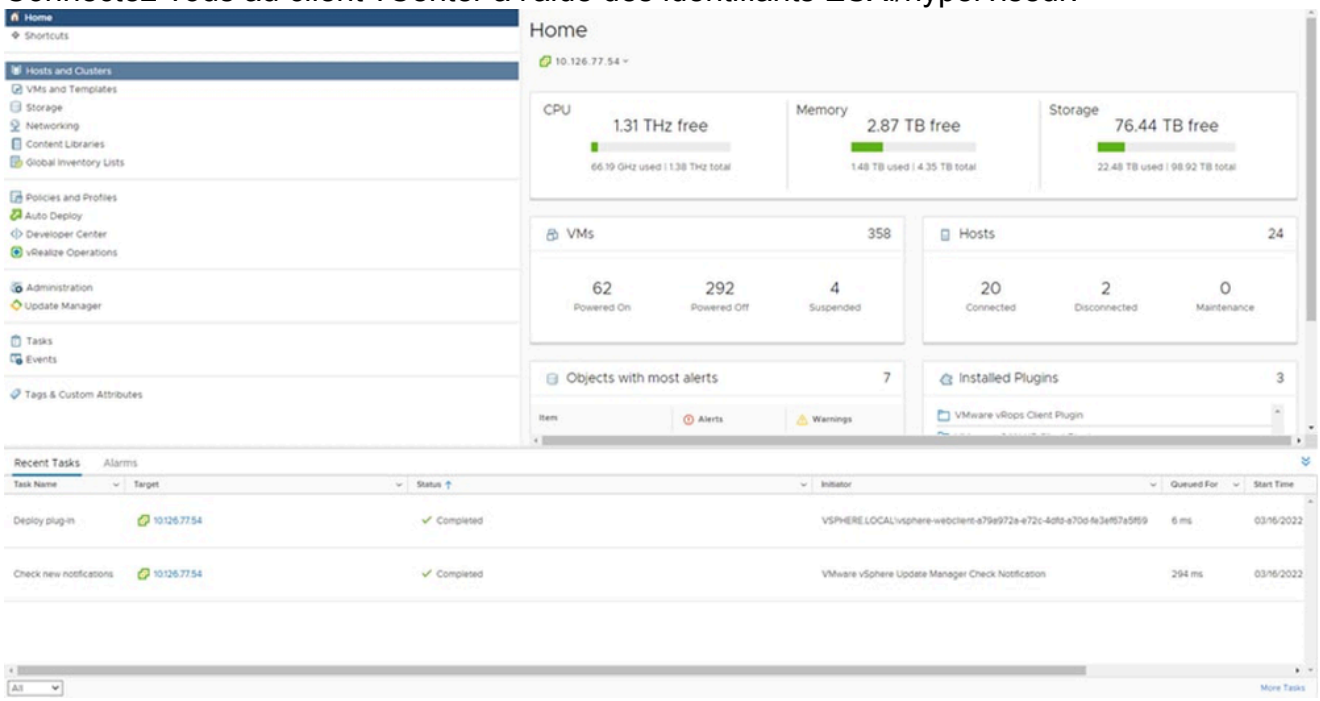
Console

10. Accédez à Network Configuration pour passer aux étapes suivantes.

Installation de client Web vCenter

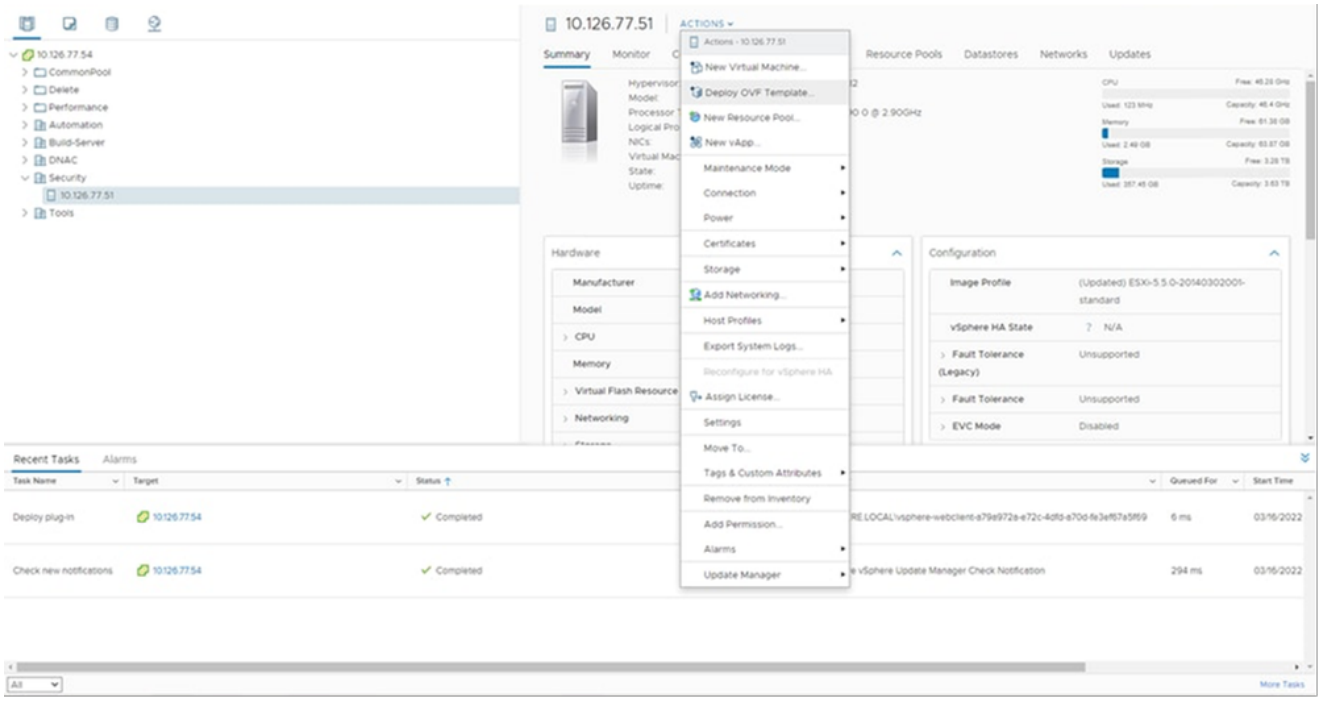
Ce client permet le déploiement de CX Agent OVA à l'aide de Web Client vCenter.

1. Connectez-vous au client vCenter à l'aide des identifiants ESXi/hyperviseur.



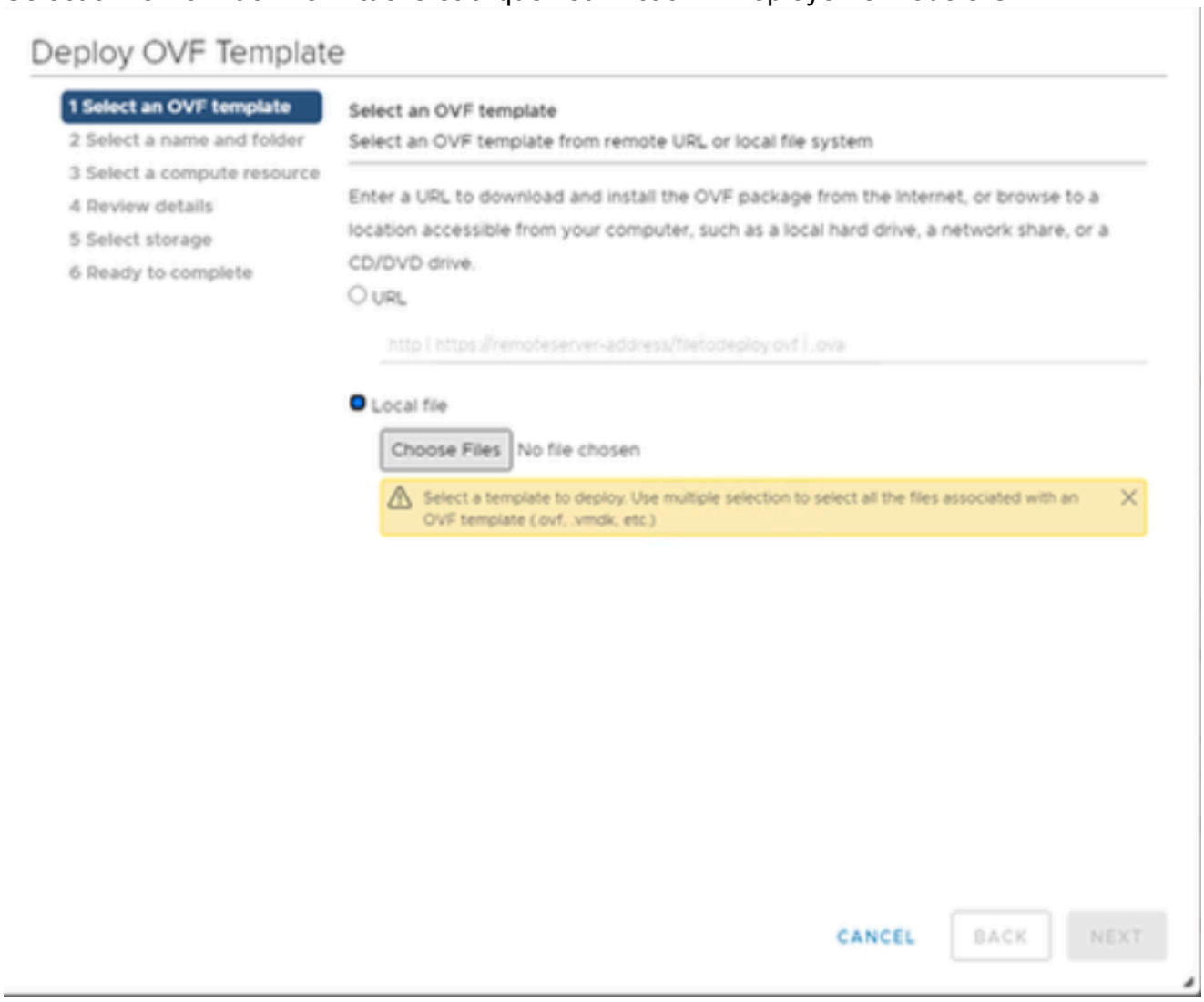
Page d'accueil

2. Sur la page d'accueil, cliquez sur Hosts and Clusters.



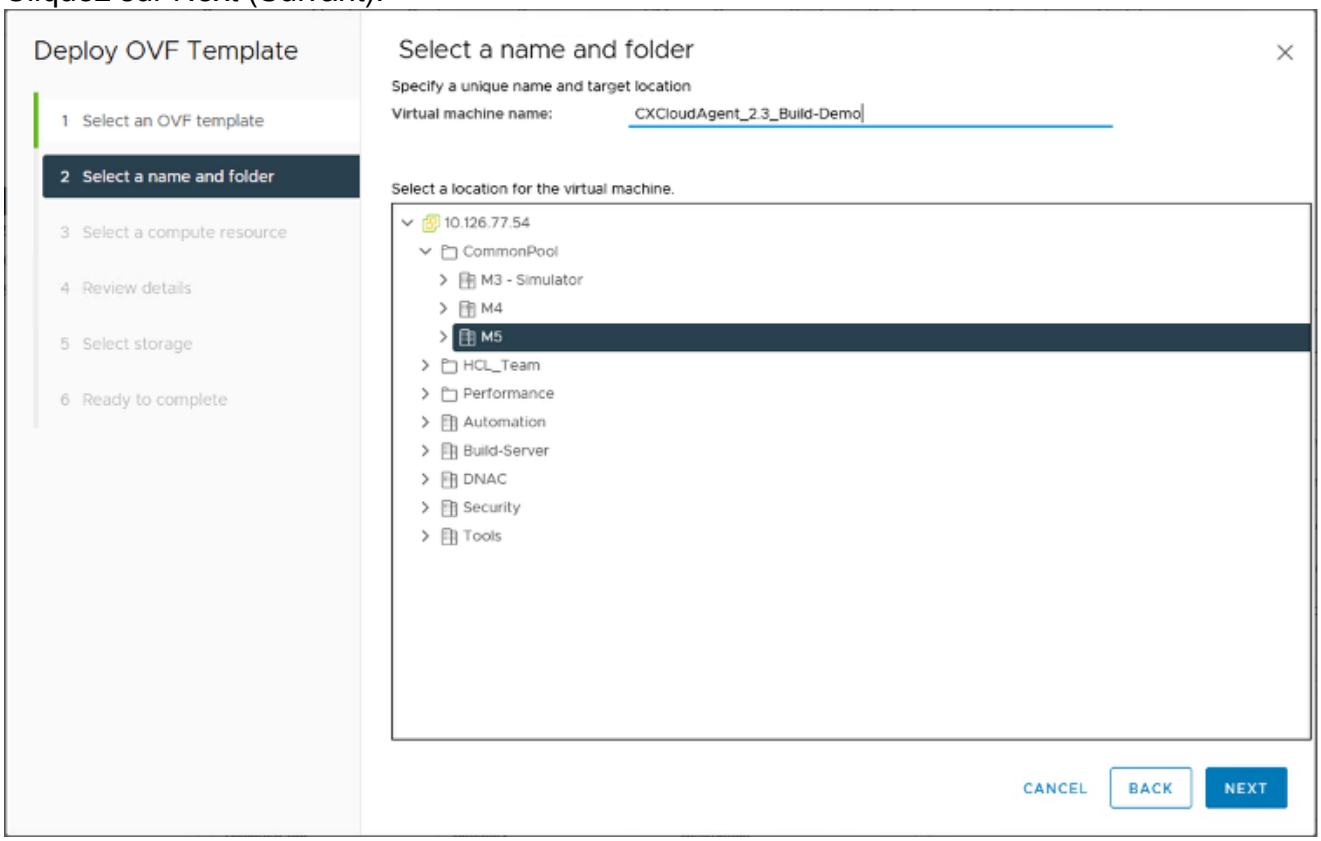
Hôtes et clusters

3. Sélectionnez la machine virtuelle et cliquez sur Action > Déployer le modèle OVF.



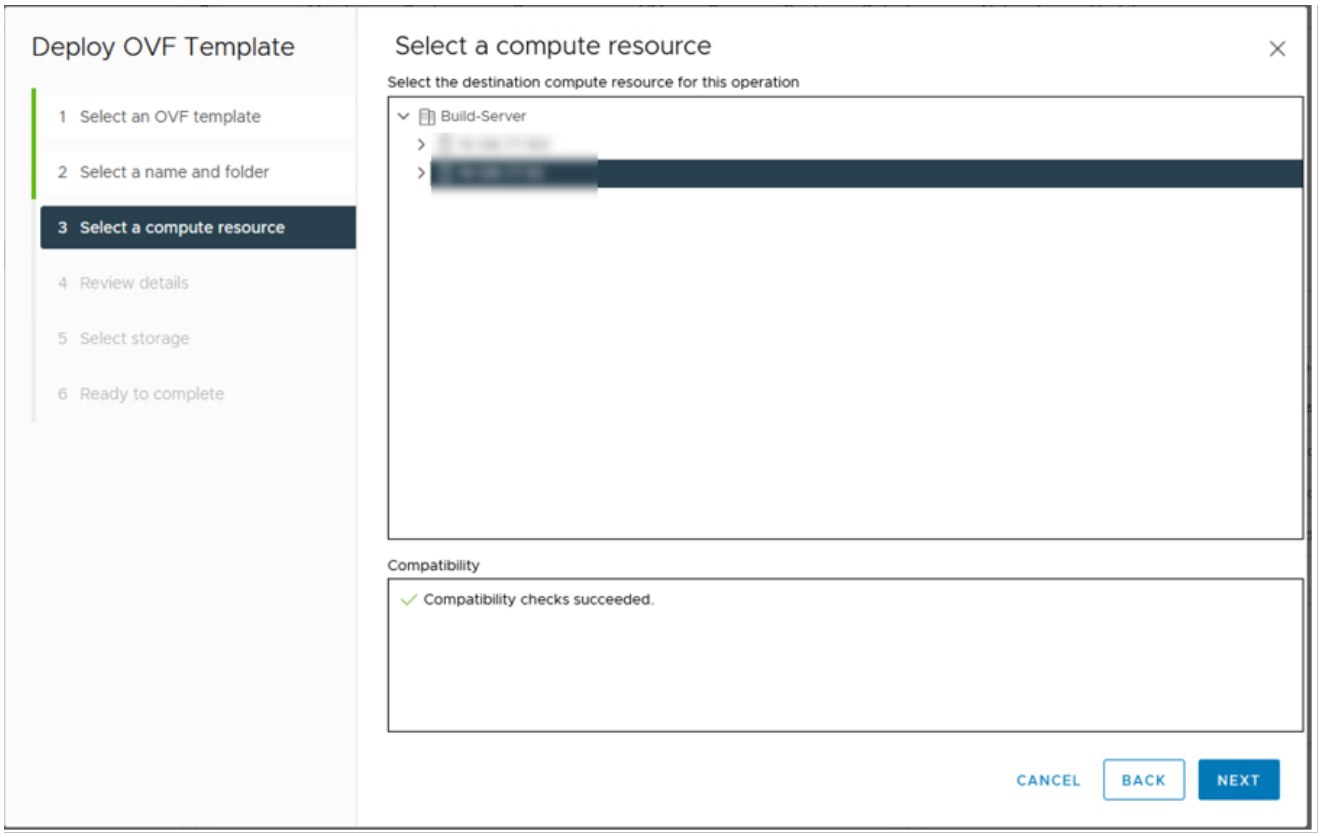
Déployer OVF

4. Ajoutez l'URL directement ou recherchez le fichier OVA.
5. Cliquez sur Next (Suivant).



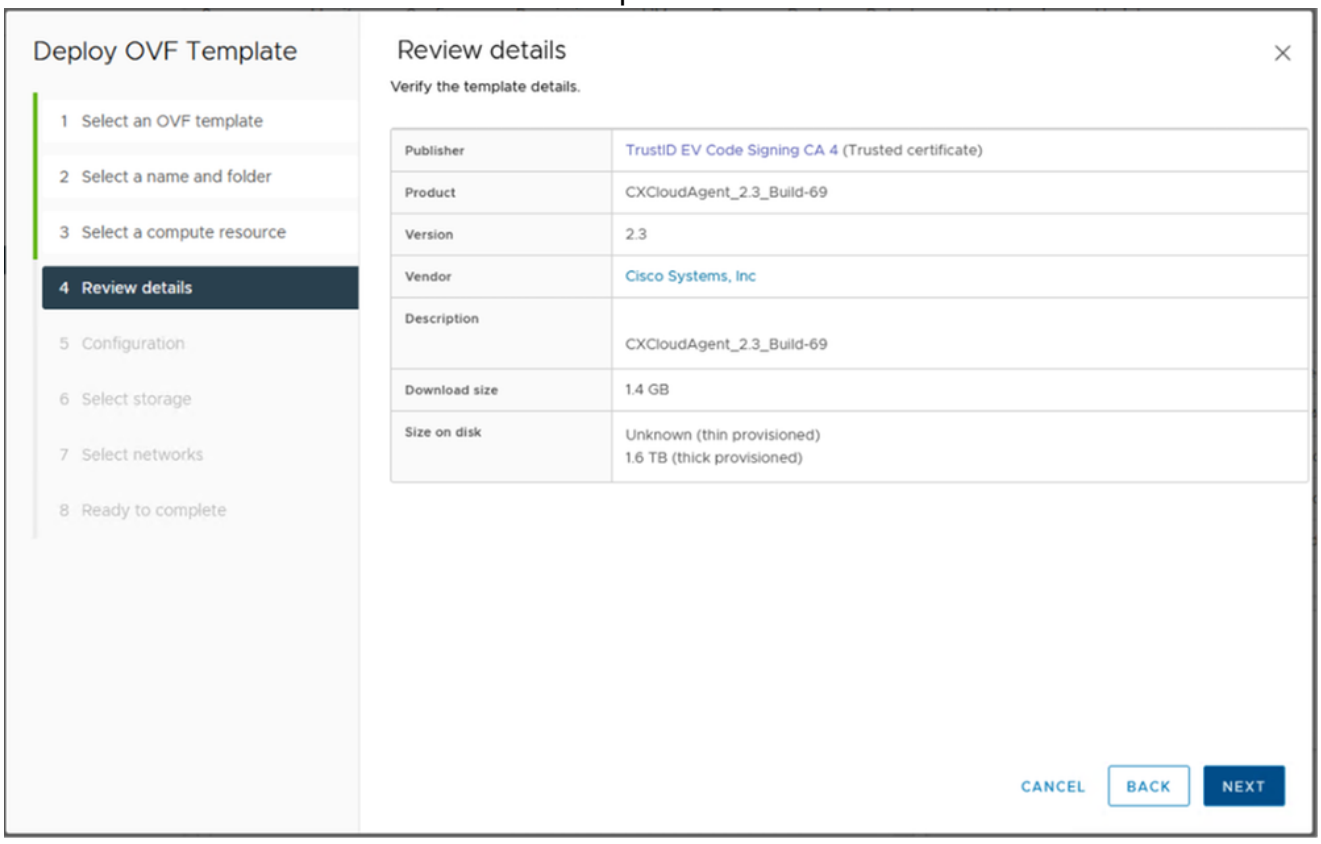
Nom et dossier

6. Entrez un nom unique et accédez à l'emplacement si nécessaire.
7. Cliquez sur Next (Suivant).



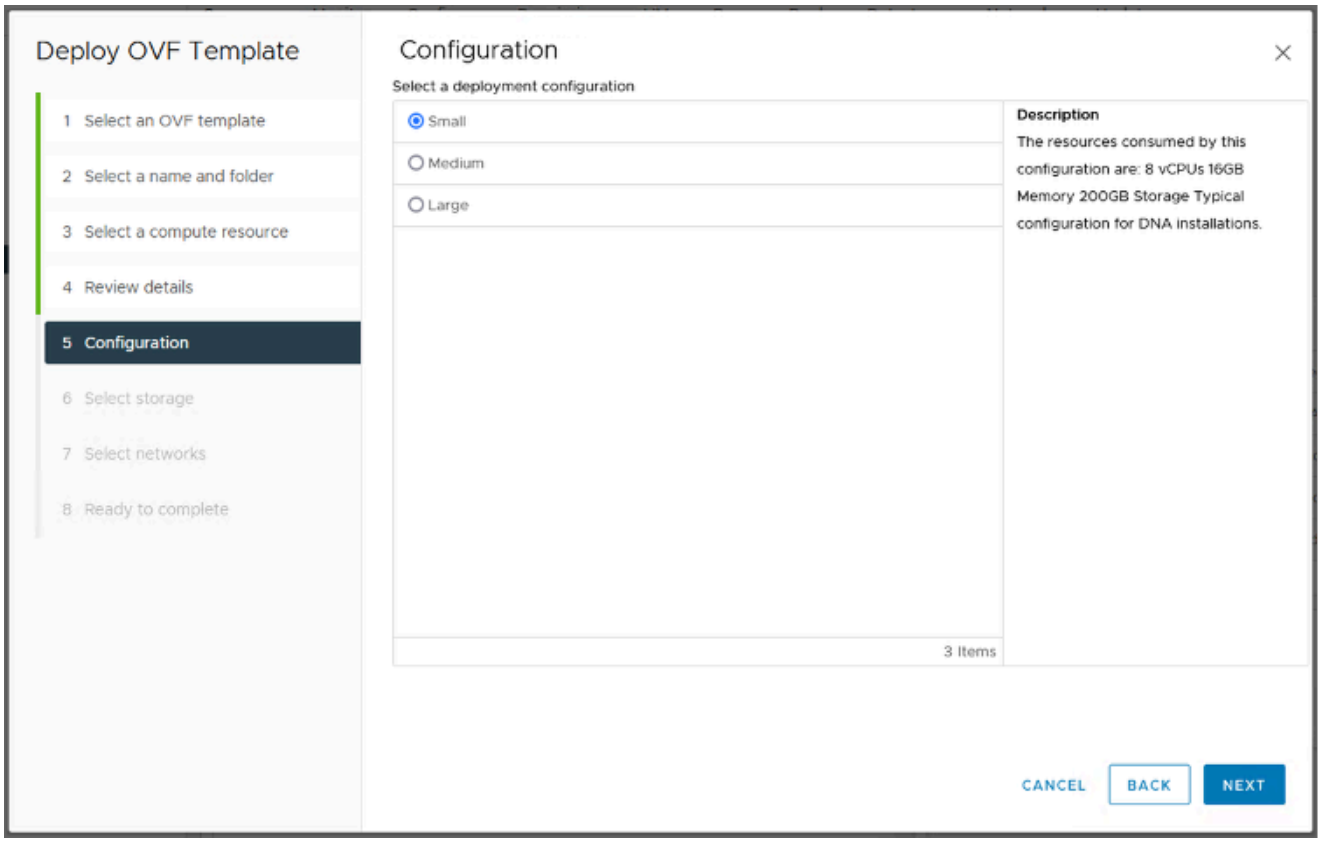
Sélectionner une ressource de calcul

8. Sélectionnez une ressource de calcul et cliquez sur Suivant.



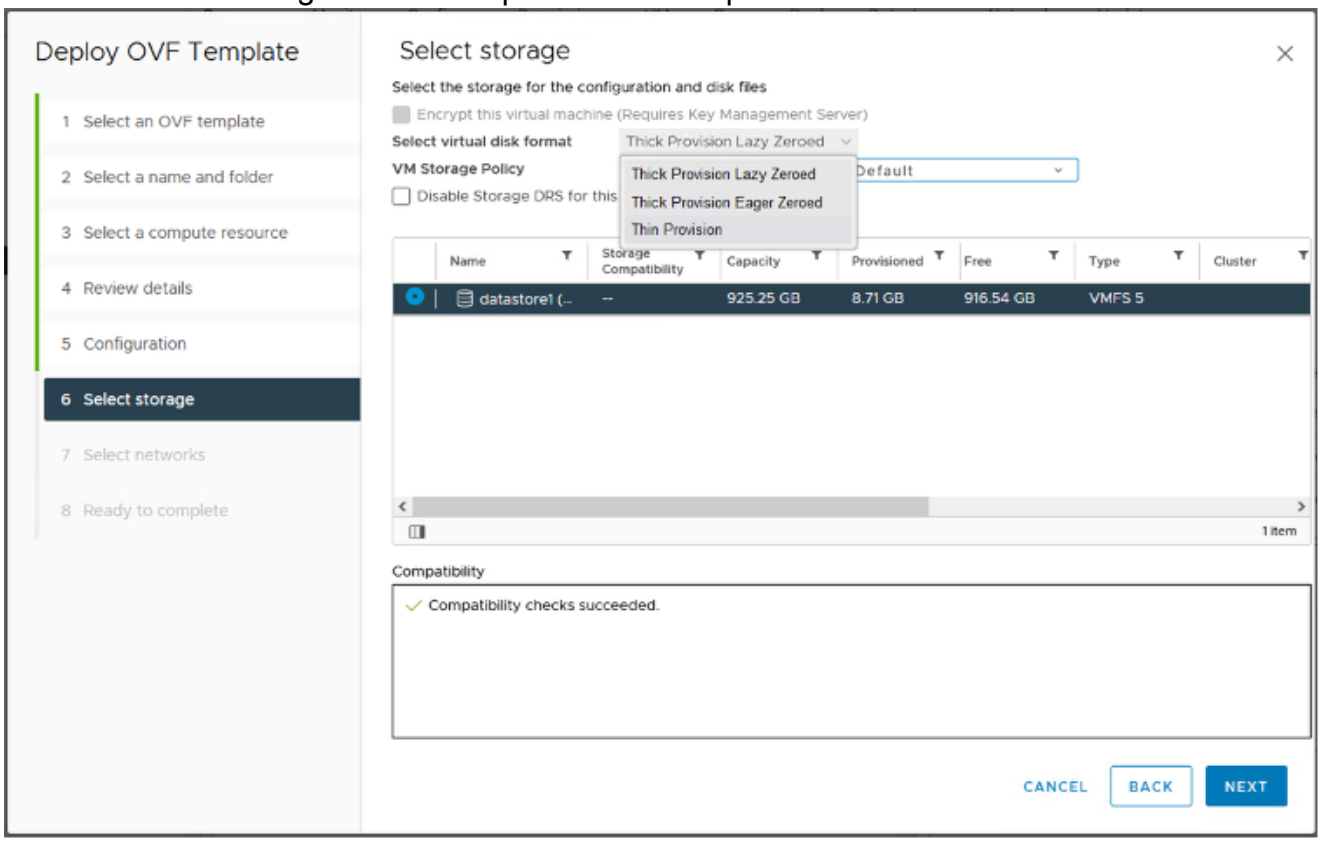
Examiner les détails

9. Passez en revue les détails et cliquez sur Next.



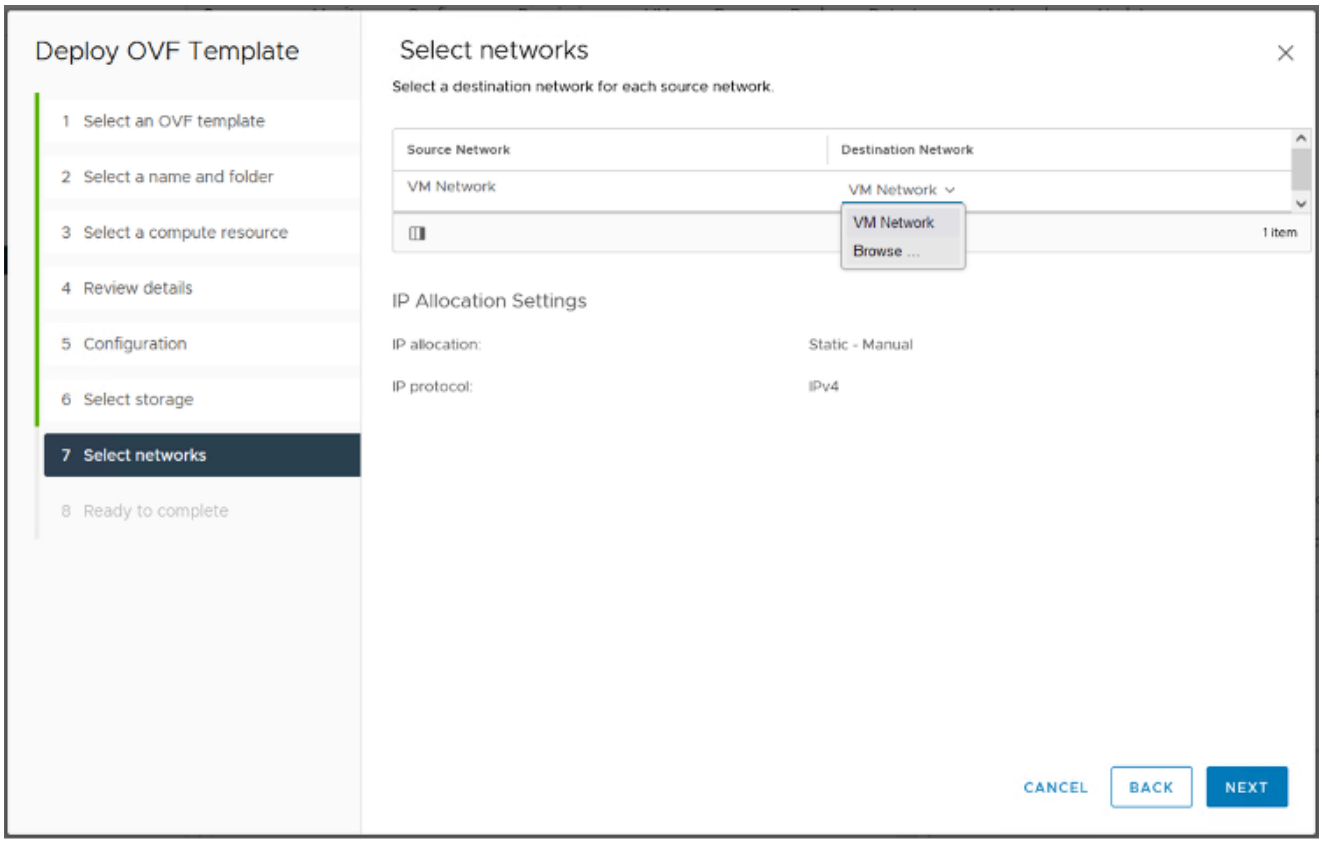
Configuration

10. Sélectionnez la configuration du déploiement et cliquez sur Suivant.



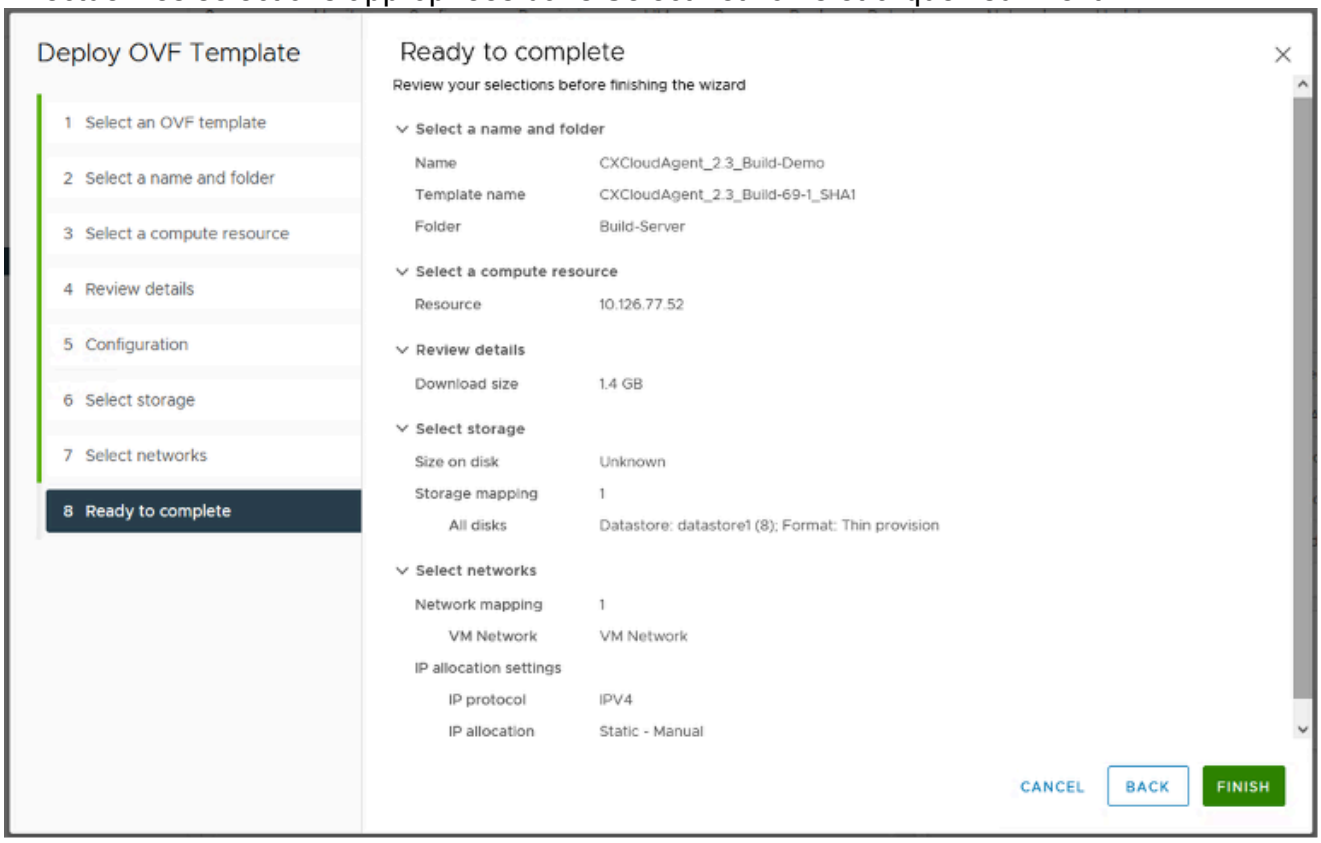
Configuration

11. Sélectionnez Storage > Select virtual disk format dans la liste déroulante et cliquez sur Next.



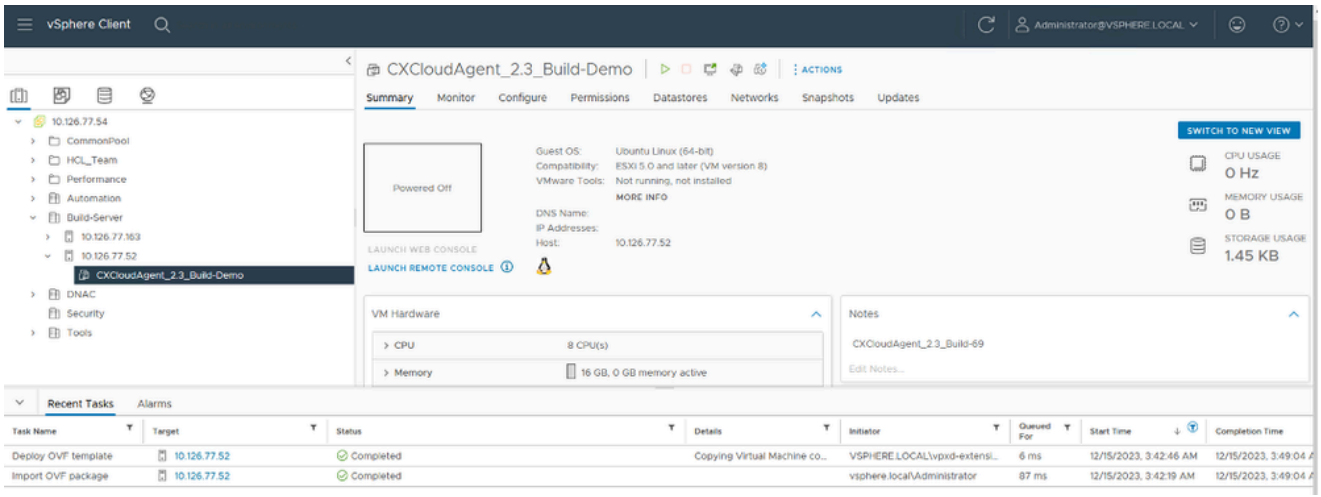
Sélectionner les réseaux

12. Effectuez les sélections appropriées dans Select networks et cliquez sur Next.



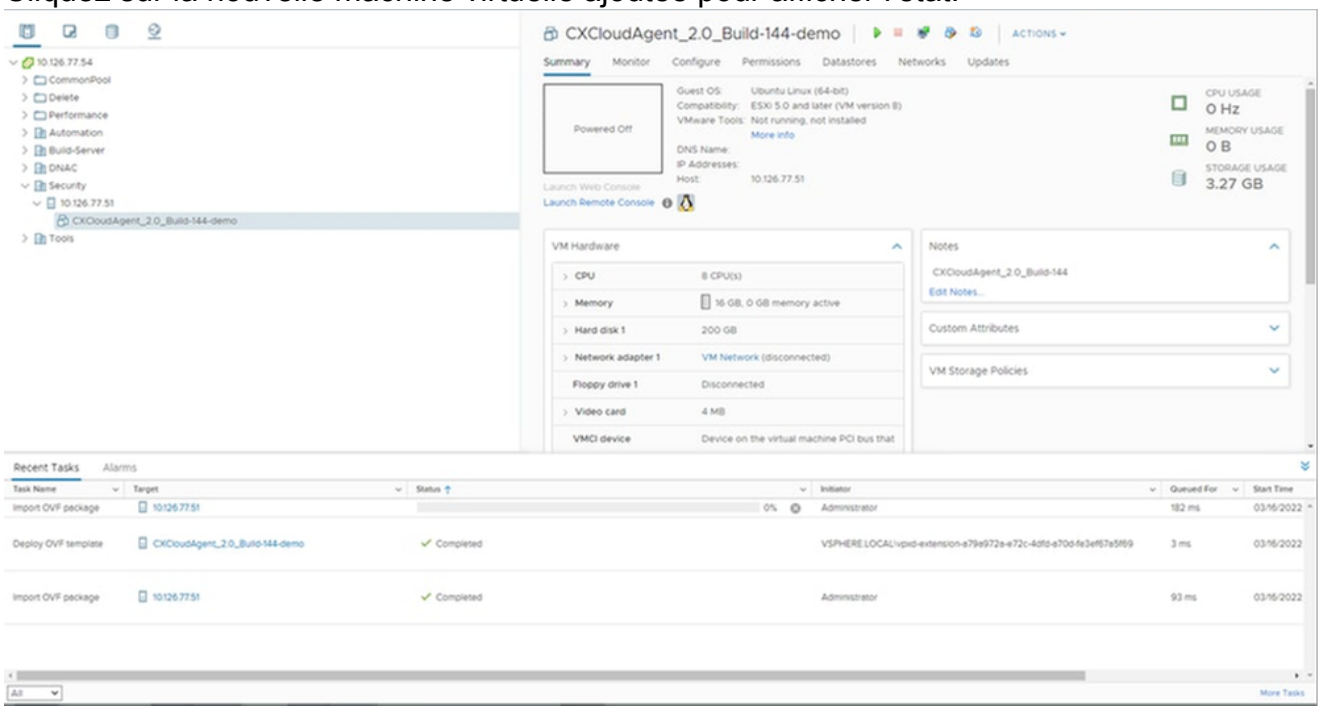
Prêt pour la confirmation

13. Vérifiez les sélections et cliquez sur Finish. La page d'accueil s'affiche.



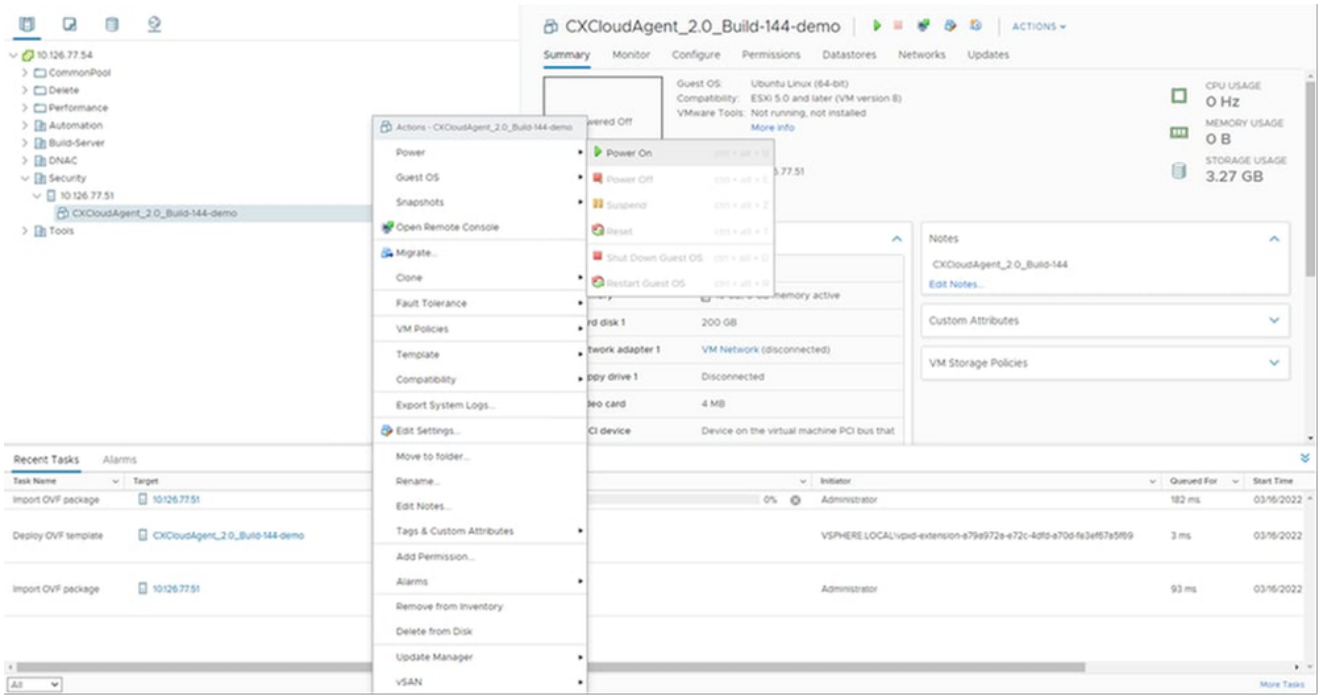
VM ajoutée

14. Cliquez sur la nouvelle machine virtuelle ajoutée pour afficher l'état.



VM ajoutée

15. Une fois installée, mettez la machine virtuelle sous tension et ouvrez la console.



Ouvrir la console

16. Accédez à Network Configuration pour passer aux étapes suivantes.

Installation d'Oracle Virtual Box 7.0.12

Ce client déploie CX Agent OVA via Oracle Virtual Box.

1. Téléchargez l'OVA CXCloudAgent_3.1 dans la zone Windows vers n'importe quel dossier.
2. Accédez au dossier à l'aide de l'interface de ligne de commande.
3. Décompressez le fichier OVA à l'aide de la commande tar -xvf D:\CXCloudAgent_3.1_Build-xx.ova.

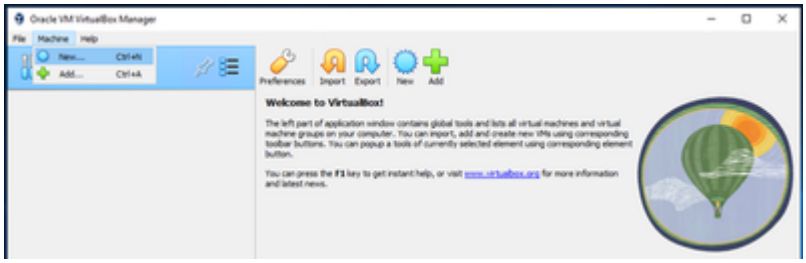
```
D:\>cd CXCAGENT

D:\CXCAGENT>tar -xvf CXCloudAgent_2.3_Build-69-1_SHA1_signed.ova
x CXCloudAgent_2.3_Build-69-1_SHA1.ovf
x CXCloudAgent_2.3_Build-69-1_SHA1.mf
x CXCloudAgent_2.3_Build-69-1_SHA1.cert
x CXCloudAgent_2.3_Build-69-1_SHA1-disk1.vmdk

D:\CXCAGENT>_
```

Décompresser le fichier OVA

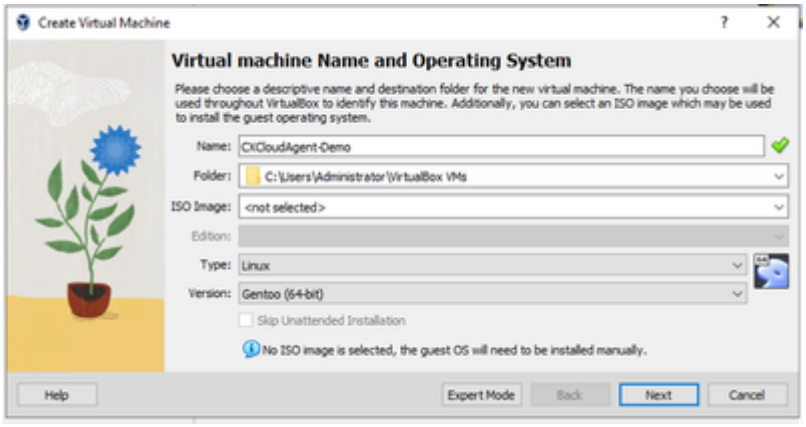
4. Ouvrez l'interface utilisateur Oracle VM.



Machine virtuelle Oracle

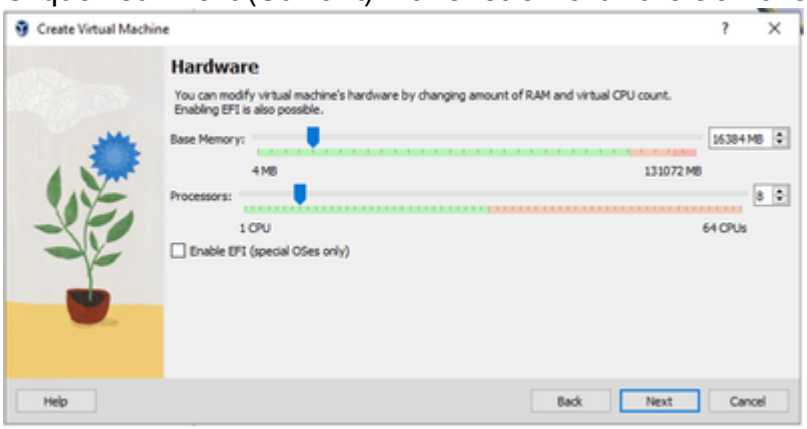
5. Dans le menu, sélectionnez Machine>Nouveau. La fenêtre Créer une machine virtuelle

s'affiche.



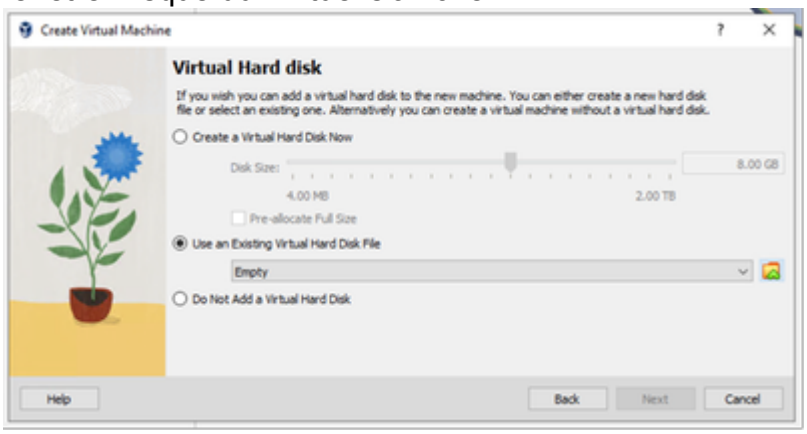
Créer une machine virtuelle

6. Entrez les détails suivants dans la fenêtre Nom de la machine virtuelle et système d'exploitation.
   Name : Nom de VM
   Dossier : Emplacement où les données de VM doivent être stockées
   Image ISO : none
   type : Linux
   Version : Gentoo (64 bits)
7. Cliquez sur Next (Suivant). La fenêtre Hardware s'affiche.



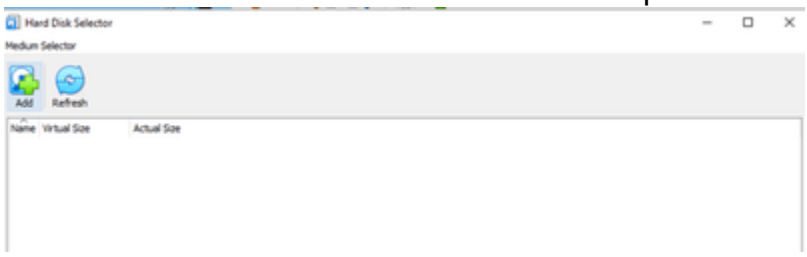
Matériel

8. Saisissez Base Memory (16384 Mo) et Processors (8 CPU), puis cliquez sur Next. La fenêtre Disque dur virtuel s'affiche.



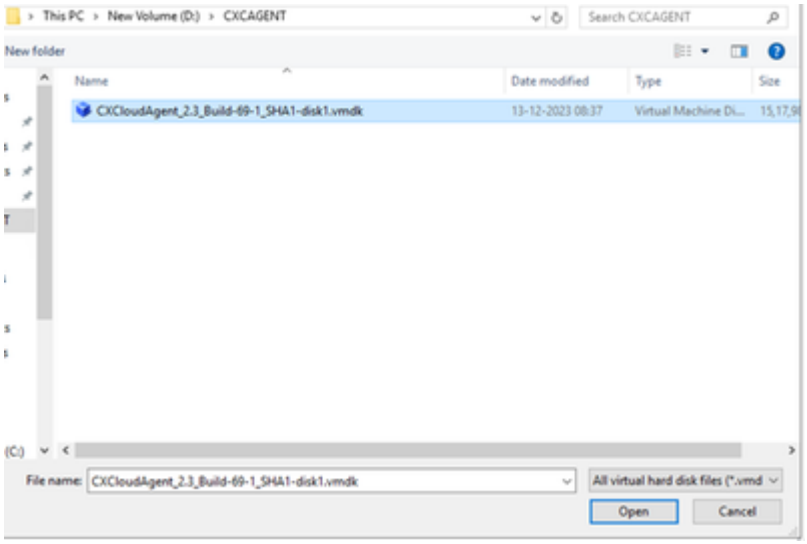
Disque dur virtuel

9. Sélectionnez la case d'option Utiliser un fichier de disque dur virtuel existant et sélectionnez l'icône Parcourir. La fenêtre Sélecteur de disque dur s'ouvre.



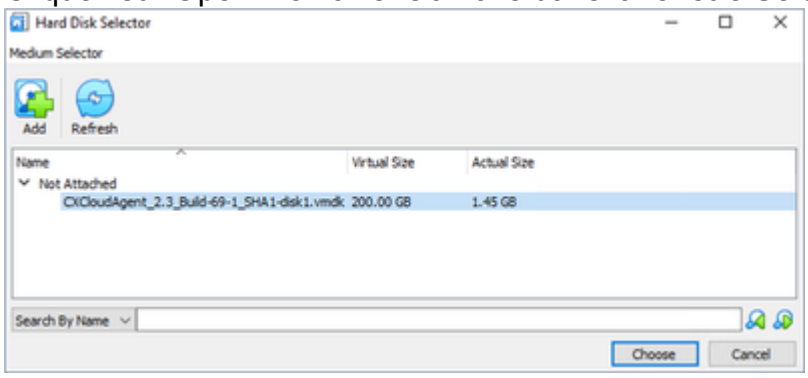
Sélecteur de disque dur

10. Accédez au dossier OVA et sélectionnez le fichier VMDK.



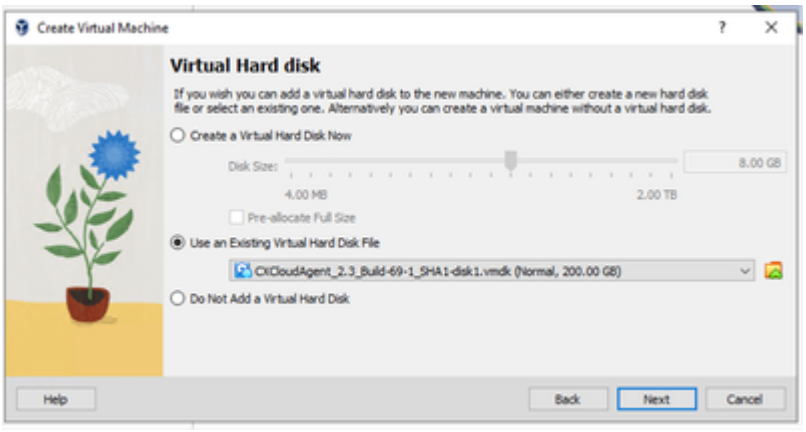
Dossier OVA

11. Cliquez sur Open. Le fichier s'affiche dans la fenêtre Sélecteur de disque matériel.



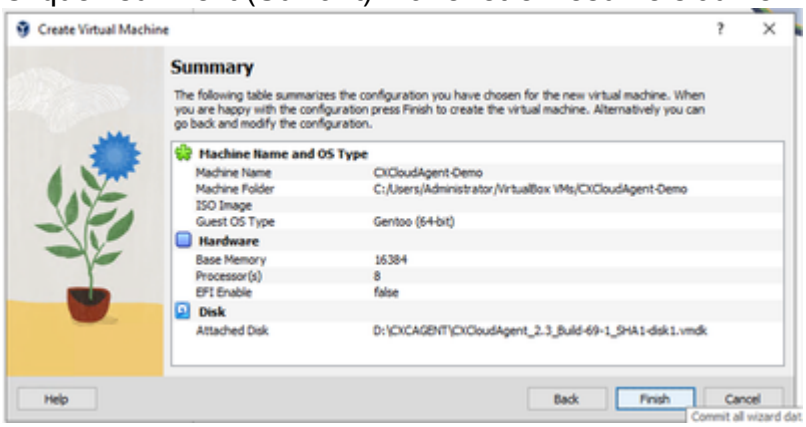
Sélecteur de disque dur

12. Cliquez sur Choisir. La fenêtre Disque dur virtuel s'affiche. Confirmez que l'option affichée est sélectionnée.



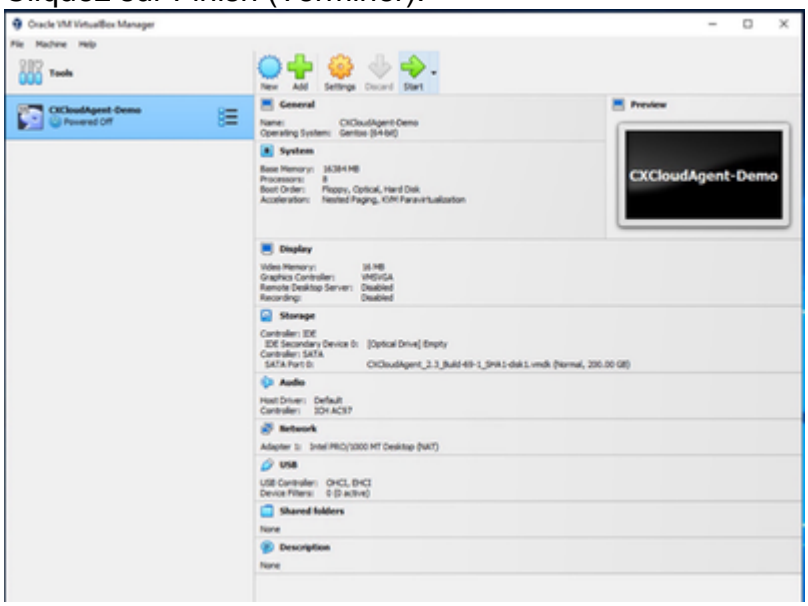
Sélectionner le fichier

13. Cliquez sur Next (Suivant). La fenêtre Résumé s'ouvre.



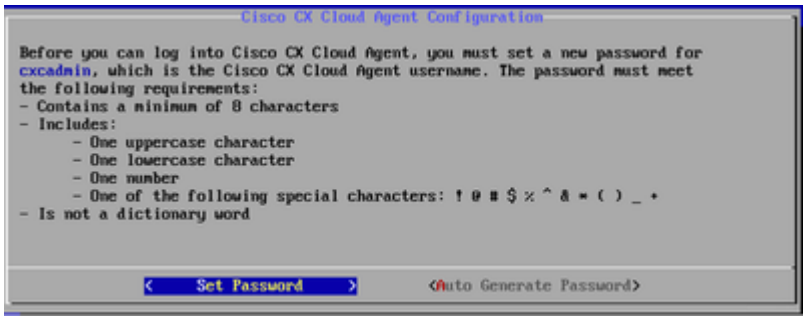
Résumé

14. Cliquez sur Finish (Terminer).



Démarrage de la console de machine virtuelle

15. Sélectionnez la machine virtuelle déployée et cliquez sur Démarrer. La machine virtuelle se met sous tension et l'écran de console s'affiche pour la configuration.



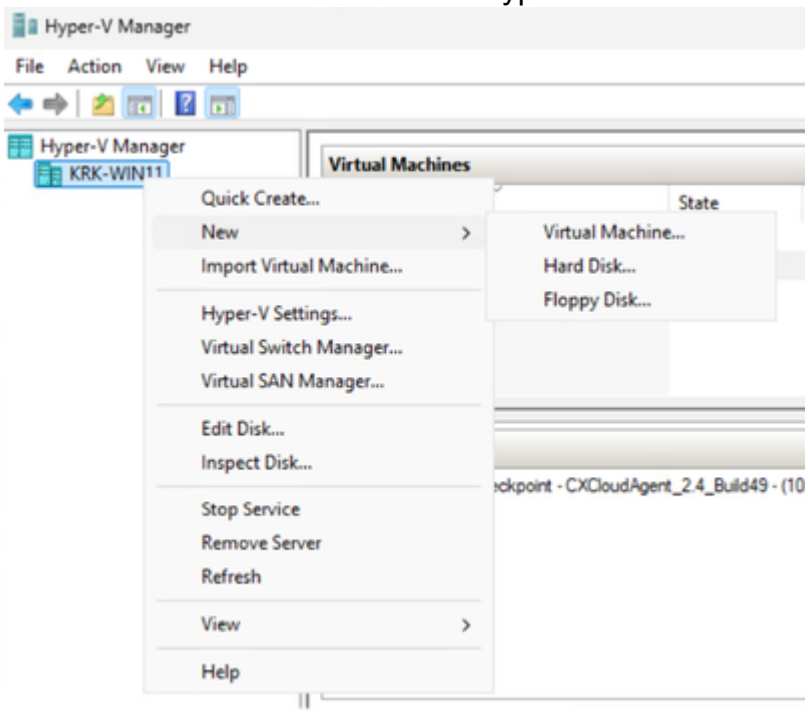
Ouvrir la console

16. Accédez à Network Configuration pour passer aux étapes suivantes.

Installation de Microsoft Hyper-V

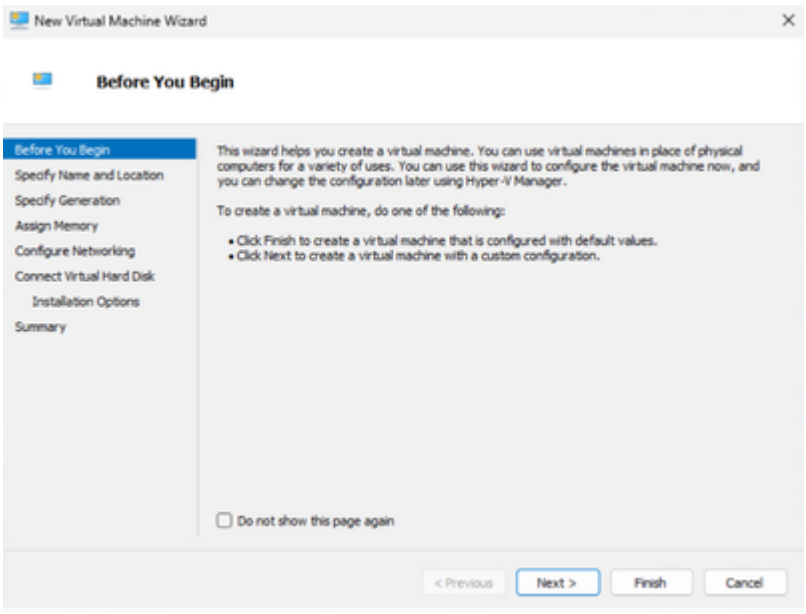
Ce client déploie le disque virtuel agent CX via l'installation de Microsoft Hyper-V.

1. Connectez-vous au Gestionnaire Hyper-V.



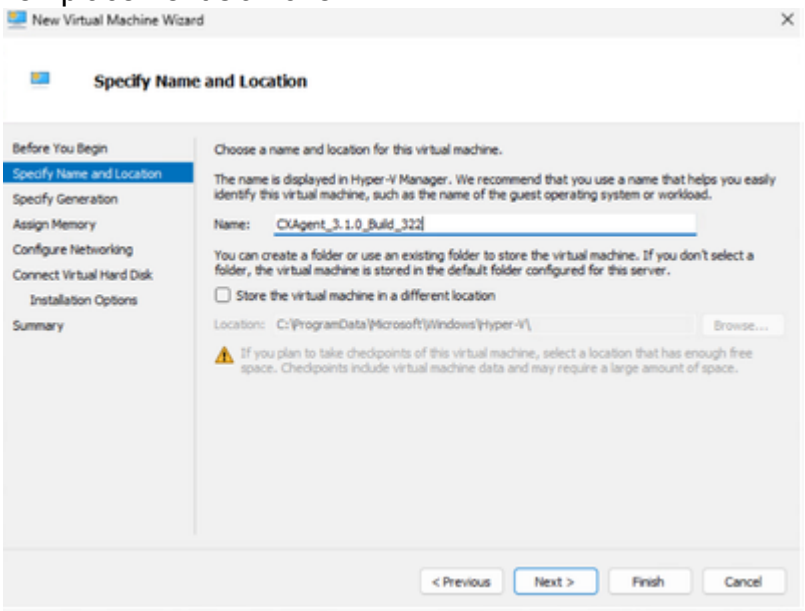
Gestionnaire Hyper-V

2. Cliquez avec le bouton droit sur la machine virtuelle cible pour ouvrir le menu.
3. Sélectionnez Nouveau > Ordinateur virtuel. La page Assistant Nouvel ordinateur virtuel - Avant de commencer s'affiche.



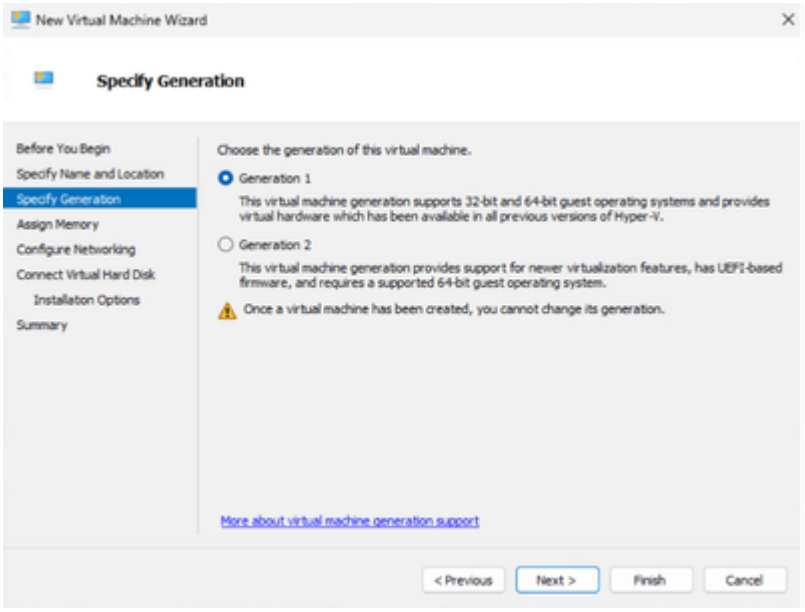
Assistant Nouvelle machine virtuelle

4. Cliquez sur Next (Suivant). La page Assistant Nouvel ordinateur virtuel - Spécifier le nom et l'emplacement s'affiche.



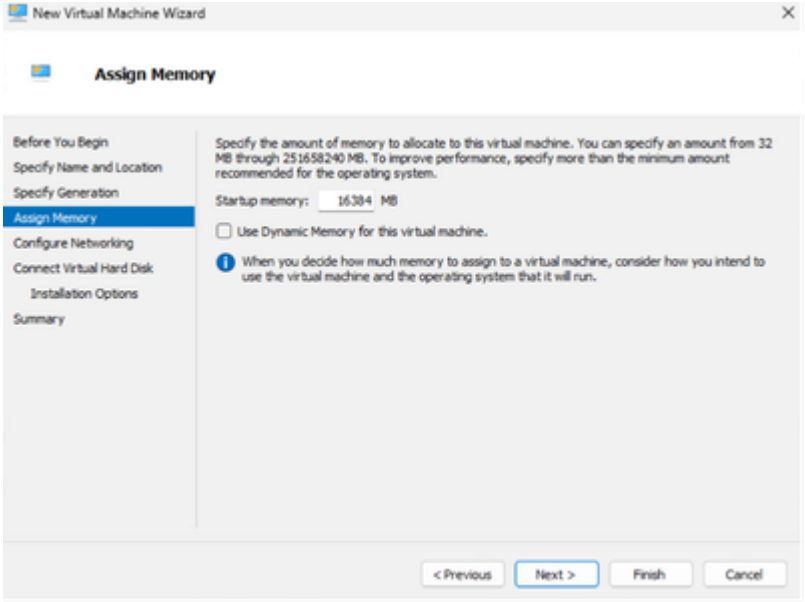
Nom et emplacement

5. Saisissez le nom et l'emplacement.
6. Cliquez sur Next (Suivant). La page Assistant Nouvel ordinateur virtuel - Spécifier la génération s'affiche.



Spécifier la génération

7. Cliquez sur la case d'option Generation 1.
8. Cliquez sur Next (Suivant). La page Assistant Nouvelle machine virtuelle - Attribuer de la mémoire s'affiche.

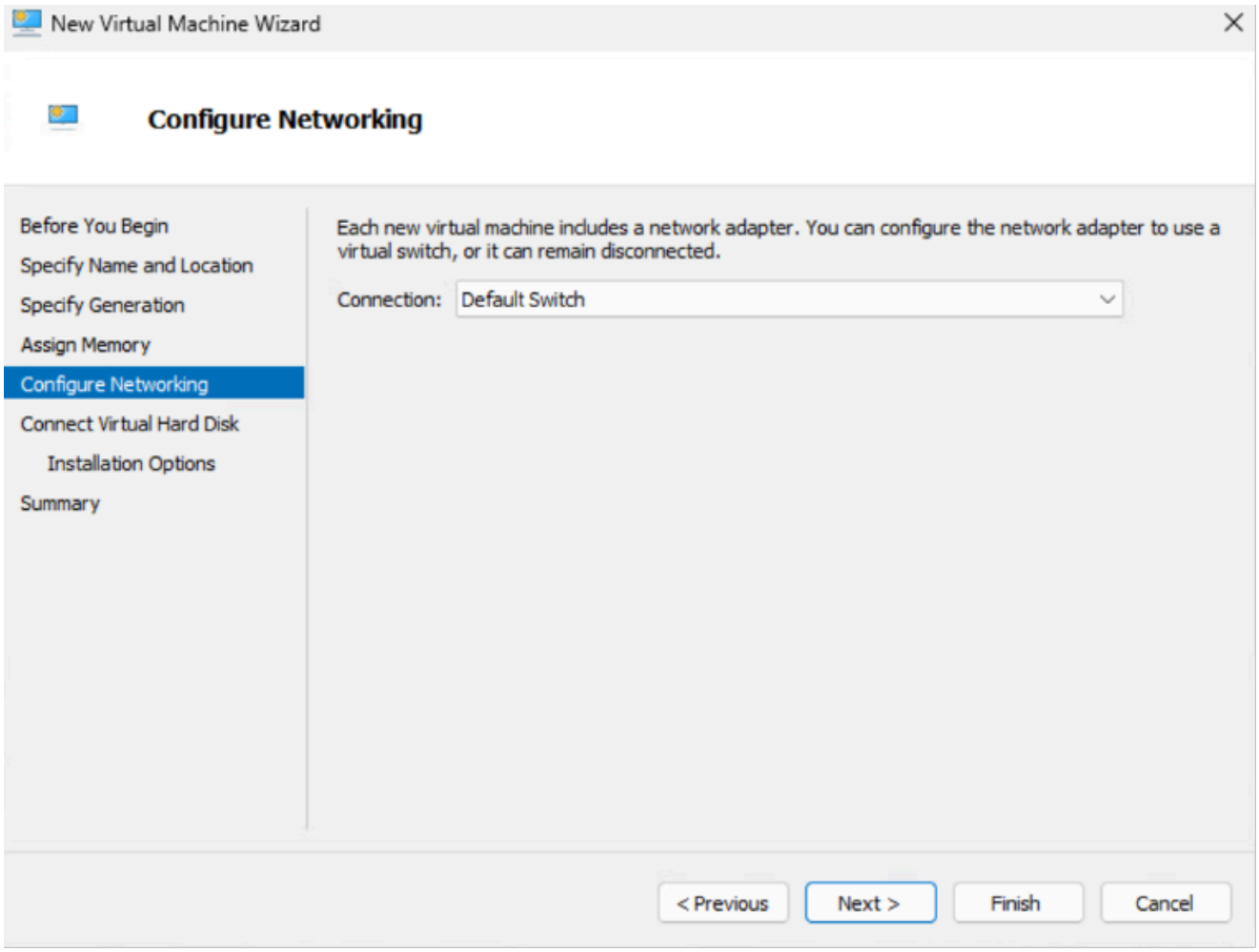


Mémoire

9. Saisissez la quantité de mémoire vive souhaitée dans le champ Mémoire de démarrage.
    - 16 Go pour un déploiement de petite envergure
    - 32 Go pour un déploiement moyen
    - 64 Go pour les déploiements de grande envergure

    Remarques :
    - Pour CX Agent, la mémoire allouée minimale doit être d'au moins 16 Go.
    - La case Utiliser la mémoire dynamique pour cet ordinateur virtuel ne doit pas être cochée.

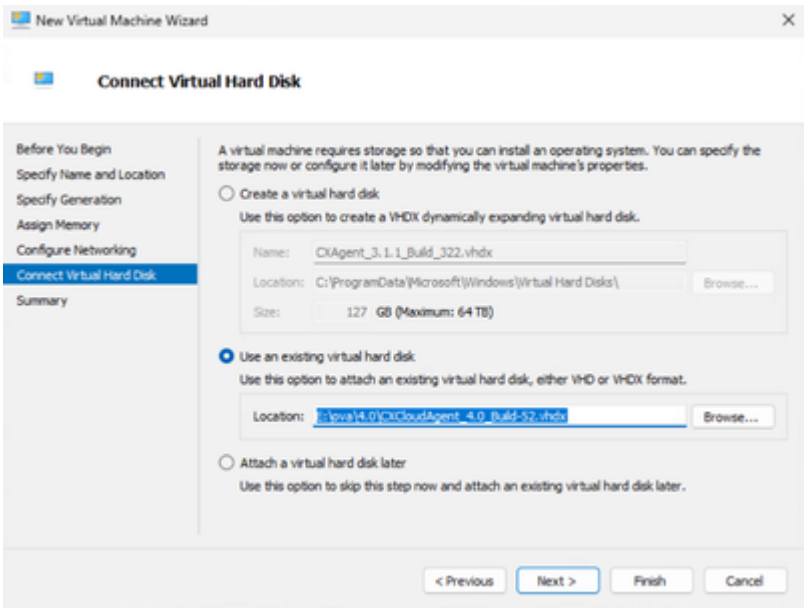
10. Cliquez sur Next (Suivant). La page Assistant Nouvel ordinateur virtuel - Configurer la mise en réseau s'affiche.



Réseautage

11. Dans la liste déroulante Connection, sélectionnez un commutateur virtuel pour la connectivité réseau.
12. Cliquez sur Next (Suivant). La page Assistant Nouvelle machine virtuelle - Connexion du disque dur virtuel s'affiche.

Remarque : l'option « Utiliser un disque virtuel existant » est sélectionnée par défaut. N'apportez aucune modification.



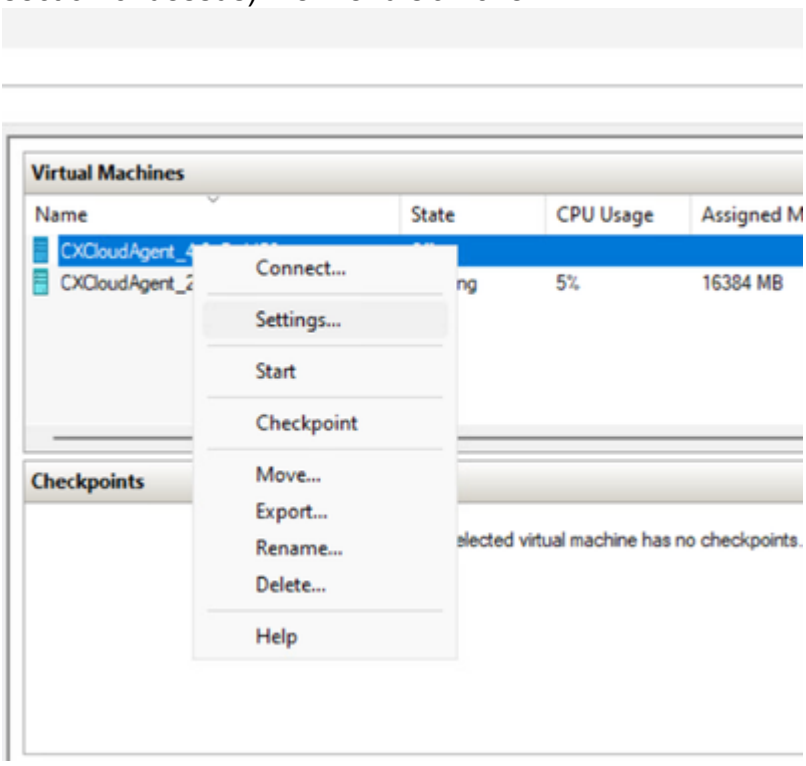
Connexion du disque dur virtuel

13. Vérifiez le résumé et cliquez sur Terminer.

Paramètres du processeur

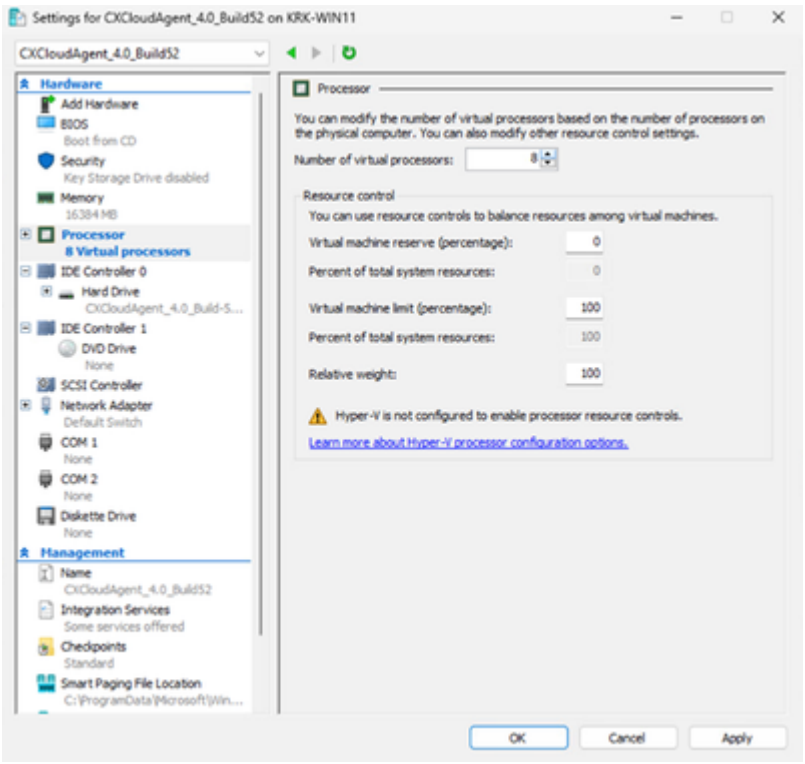
Pour vérifier les paramètres du processeur :

1. Cliquez avec le bouton droit sur la nouvelle machine virtuelle (comme indiqué dans la section ci-dessus). Le menu s'affiche.

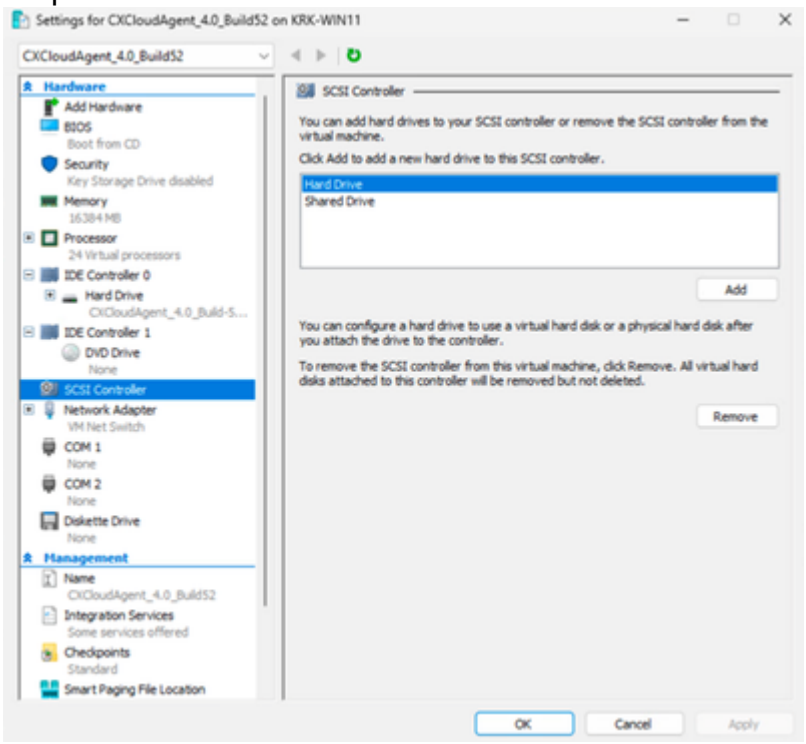


Paramètres VM

2. Sélectionnez Settings.
3. Cliquez sur Processeur dans le volet Matériel.

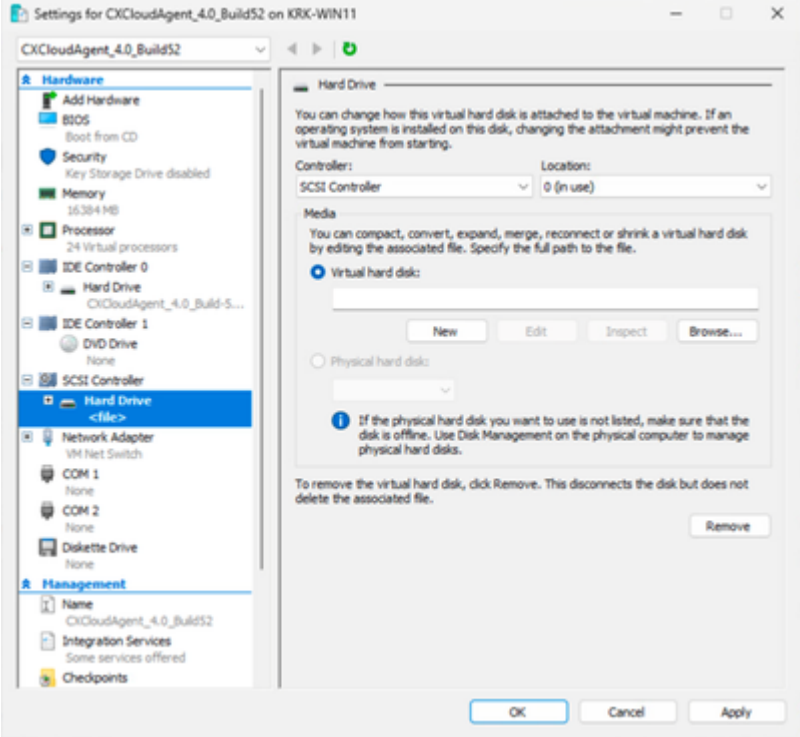


4. Mettez à jour le champ Nombre de processeurs virtuels comme indiqué ci-dessous :
    - Petit déploiement : 8
    - Déploiement moyen : 16
    - Déploiement étendu : Minimum 32
5. Cliquez sur Apply.
6. Click OK.
7. Mettez à jour les paramètres de stockage si vous créez un déploiement moyen ou important de l'agent CX. Pour mettre à jour :
    1. Cliquez sur Paramètres VM.



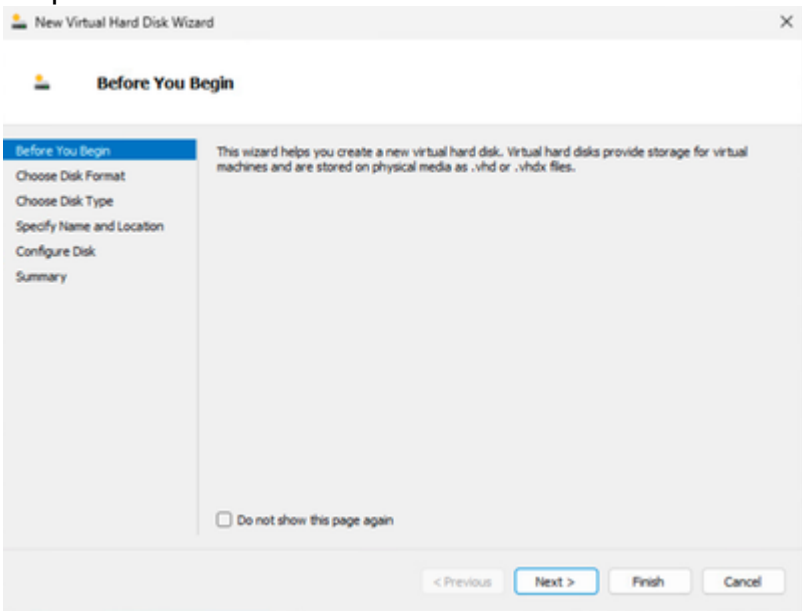
Contrôleur SCSI

2. Cliquez sur la section Contrôleur SCSI.
3. Cliquez sur Add avec l'option Hard Drive sélectionnée.



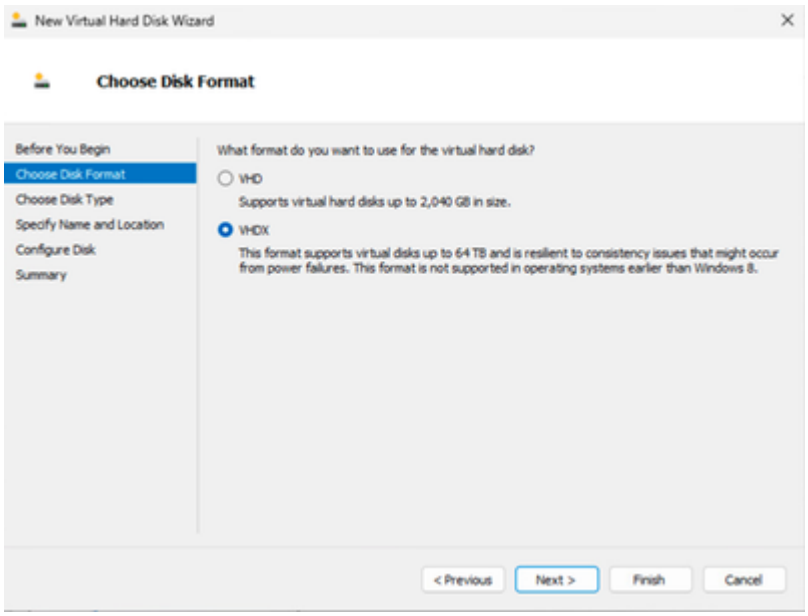
Disque dur

4. Cliquez sur New dans Media. Un nouvel assistant de disque dur virtuel s'ouvre.



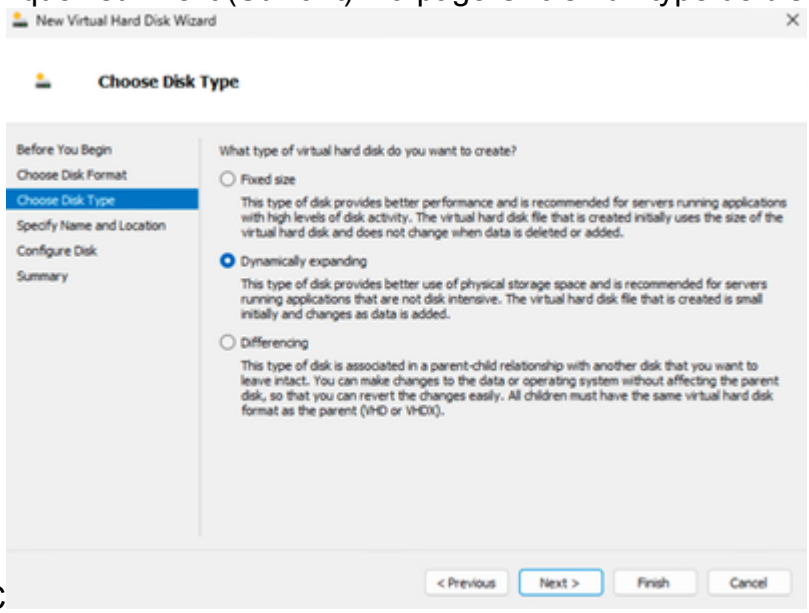
Assistant Nouveau disque dur

5. Cliquez sur Next (Suivant). La page Choisir le format de disque s'affiche.



Choisir le format de disque

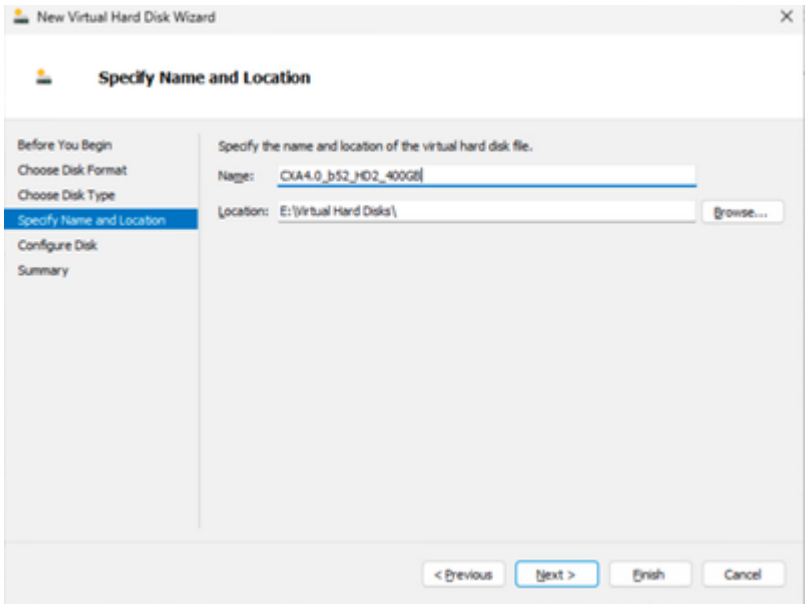
6. Cliquez sur la case d'option VHDX pour sélectionner le format de disque.
7. Cliquez sur Next (Suivant). La page Choisir un type de disque s'affiche.



C

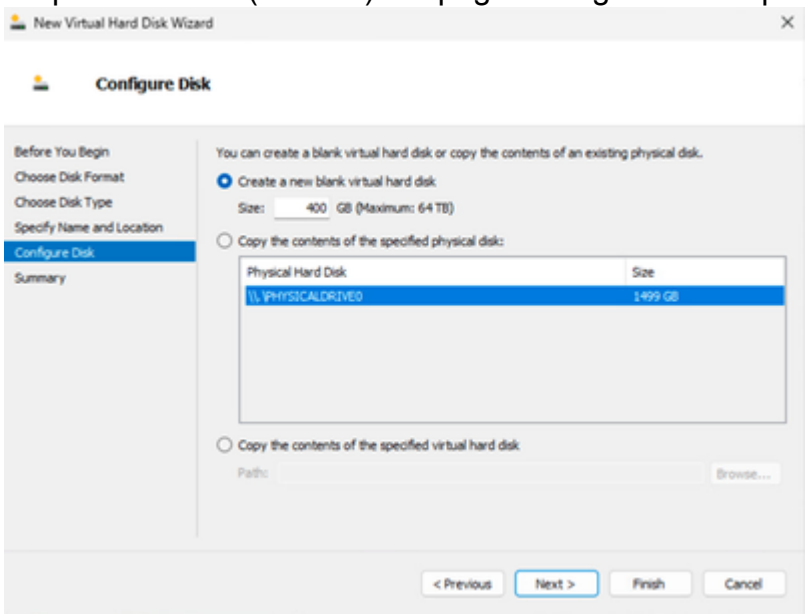
Choisir le type de disque

8. Cliquez sur la case d'option Développer dynamiquement.
9. Cliquez sur Next (Suivant). La page Spécifier le nom et l'emplacement s'affiche.



Spécifier le nom et l'emplacement

10. Saisissez le nom et l'emplacement du disque.
11. Cliquez sur Next (Suivant). La page Configurer le disque s'affiche.



Configurer le disque

12. Saisissez la taille du nouveau disque comme recommandé ci-dessous :
    - Déploiement moyen : 400 Go
    - Déploiement étendu : 1000 Go
13. Cliquez sur Finish (Terminer). La machine virtuelle Hyper-V est prête à l'emploi et peut être démarrée.

8. Référez-vous à Configuration du réseau pour passer aux étapes suivantes.

Validation des signatures d'image Microsoft Hyper-V

Pour garantir l'intégrité et l'authenticité des images Microsoft Hyper-V, la validation des signatures est effectuée dans le cadre du processus de sécurité.

Conditions préalables

- Possibilité d'exécuter des commandes OpenSSL via l'interface de ligne de commande
- Possibilité d'exécuter des commandes grep via l'interface de ligne de commande
- Image fournie par Cisco pour la vérification des signatures
- Certificat d'entité finale x.509 signé par Cisco contenant une clé publique utilisée pour la vérification de la signature ; ce certificat est émis par une autorité de certification subordonnée Cisco, qui est approuvée par l'autorité de certification racine Cisco
- Signature générée pour l'image
- Programme de vérification des signatures requis pour vérifier la chaîne de certificats x.509 à 3 niveaux et la signature ; la chaîne de certificats est d'abord validée, y compris le certificat de l'entité finale et les certificats bien connus de l'autorité de certification secondaire et de l'autorité de certification racine, puis l'autorité de certification secondaire et l'autorité de certification racine sont soit lues à partir d'un répertoire local spécifié, soit téléchargées à partir du site Web de l'ICP ; le certificat d'entité finale authentifié est utilisé pour vérifier la signature

Exécuter le package de vérification des signatures

Les clients peuvent vérifier que l'archive ZIP Cisco téléchargée a été signée avec un certificat de version Cisco. Exécutez les commandes des exemples ci-dessous pour vérifier les signatures.



Remarque : Assurez-vous que les attributs corrects sont référencés dans les exemples de commandes ci-dessous.

Commande 1 (signature sha512, Cisco rootCA & subCA téléchargé à partir de l'exemple du site Web PKI) :

```
./cisco_x509_verify_release.py3 -e CX_COLLECTOR_HYPER_REL_CERT.pem -i
CXCloudAgent__Build-348_SHA1.vhdx_RELEASE_signed.zip -s
CXCloudAgent_3.1_Build-348_SHA1.vhdx_RELEASE_signed.zip.signature -v
dgst –algo sha512 –failExpiredCerts
```

Sortie de commande

```
<messages d'erreur possibles, certains avec le mot de code
UNSAFE_LEGACY_RENEGOTIATION_DISABLED>

Récupération du certificat rootCA à partir de
https://www.cisco.com/security/pki/certs/csirca4096.cer...

Récupération et vérification réussies de csirca4096.cer.

Récupération du certificat de la sous-autorité de certification à partir
de https://www.cisco.com/security/pki/certs/cgsisca4096.cer...
```

```
Récupération et vérification de cgsisca4096.cer réussies.

Chaîne de certificats racine, sous-jacente et d'entité finale vérifiée.

Récupération réussie d'une clé publique de
CX_COLLECTOR_HYPER_REL_CERT.pem.

Vérification réussie de la signature de CXCloudAgent_3.1_Build-
348_SHA1.vhdx_RELEASE_signed.zip à l'aide de
CX_COLLECTOR_HYPER_REL_CERT.pem
```

Commande 2 (signature sha512, Cisco Virtual UEFI rootCA & subCA récupéré à partir du site Web PKI de Cisco, exemple) :

```
./cisco_x509_verify_release.py3 -e CX_COLLECTOR_HYPER_REL_CERT.pem -i
CXCloudAgent_3.1_Build-348_SHA1.vhdx_RELEASE_signed.zip -s
CXCloudAgent_3.1_Build-348_SHA1.vhdx_RELEASE_signed.zip.signature -v
dgst —algo sha512 -failExpiredCerts
```

Sortie de commande

```
<messages d'erreur possibles, certains avec le mot de code
UNSAFE_LEGACY_RENEGOTIATION_DISABLED>

Récupération du certificat d'autorité de certification à partir de
https://www.cisco.com/security/pki/certs/vuefirca.cer...

Récupération et vérification réussies de vuefirca.cer.

Récupération du certificat SubCA à partir de
https://www.cisco.com/security/pki/certs/vuefiscav2.cer...

Récupération et vérification de vuefiscav2.cer réussies.

Chaîne de certificats racine, sous-jacente et d'entité finale vérifiée.

Récupération réussie d'une clé publique de
CX_COLLECTOR_HYPER_REL_CERT.pem.

Vérification réussie de la signature de CXCloudAgent_3.1_Build-
348_SHA1.vhdx_RELEASE_signed.zip à l'aide de
CX_COLLECTOR_HYPER_REL_CERT.pem
```

Commande 3 (exemple local Cisco rootCA et subCA)

```
./cisco_x509_verify_release.py3 -e CX_COLLECTOR_HYPER_REL_CERT.pem -i
CXCloudAgent_3.1_Build-348_SHA1.vhdx_RELEASE_signed.zip -s
CXCloudAgent_3.1_Build-348_SHA1.vhdx_RELEASE_signed.zip.signature -c
/cert/store -v dgst —algo sha512 -failExpiredCerts
```

Sortie de commande

```
Utilisation du certificat rootCA fourni localement
/cert/store/vuefirca.cer

Utilisation du certificat subCA fourni localement
/cert/store/vuefiscav2.cer

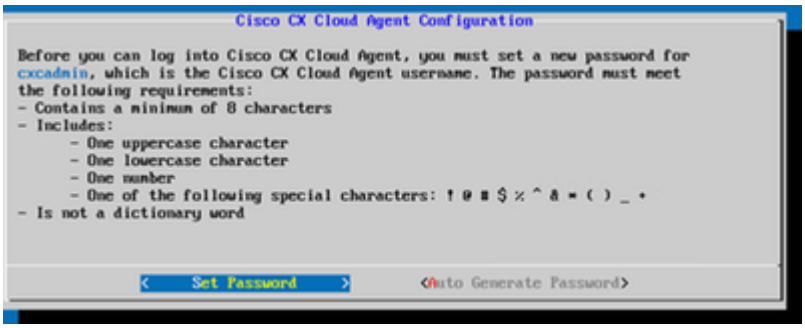
Chaîne de certificats racine, sous-jacente et d'entité finale vérifiée.

Récupération réussie d'une clé publique de
CX_COLLECTOR_HYPER_REL_CERT.pem.

Vérification réussie de la signature de CXCloudAgent_3.1_Build-
348_SHA1.vhdx_RELEASE_signed.zip à l'aide de
CX_COLLECTOR_HYPER_REL_CERT.pem
```

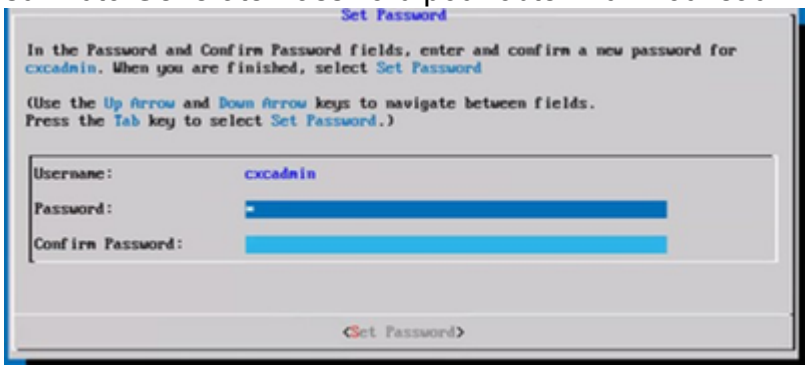
Configuration du réseau

Pour définir le mot de passe CX Cloud Agent pour le nom d'utilisateur cxcadmin :



Définir un mot de passe

1. Cliquez sur Set Password pour ajouter un nouveau mot de passe pour cxcadmin OU cliquez sur Auto Generate Password pour obtenir un nouveau mot de passe.



Nouveau mot de passe

2. Si Set Password est sélectionné, saisissez le mot de passe pour cxcadmin et confirmez-le. Cliquez sur Set Password et passez à l'étape 3.
   OU

Si Auto Generate Password est sélectionné, copiez le mot de passe généré et stockez-le pour une utilisation ultérieure. Cliquez sur Save Password et passez à l'étape 4.

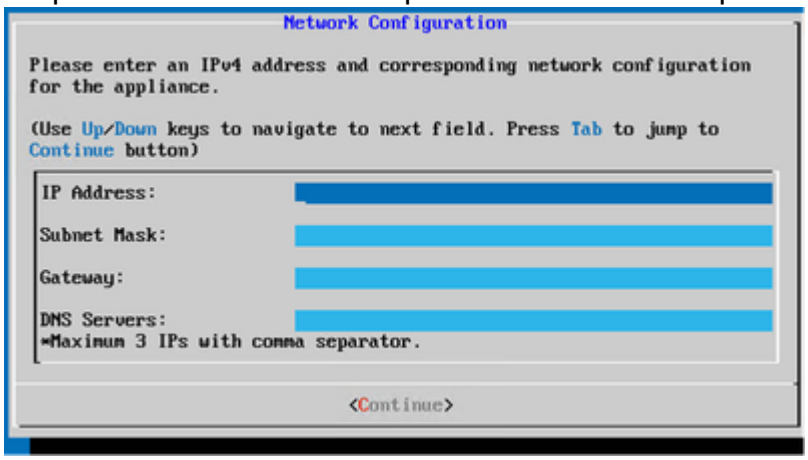


Mot de passe généré automatiquement



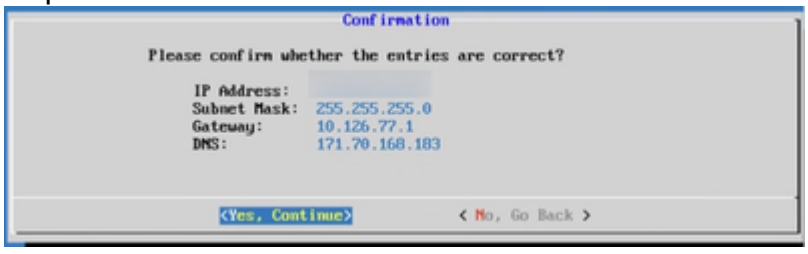
Enregistrez le mot de passe.

3. Cliquez sur Save Password pour utiliser le mot de passe pour l'authentification.



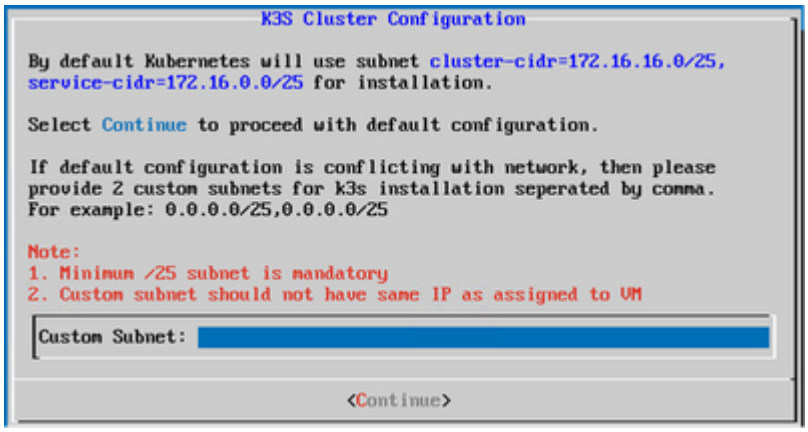
Configuration du réseau

4. Saisissez l'adresse IP, le masque de sous-réseau, la passerelle et le serveur DNS, puis cliquez sur Continuer.



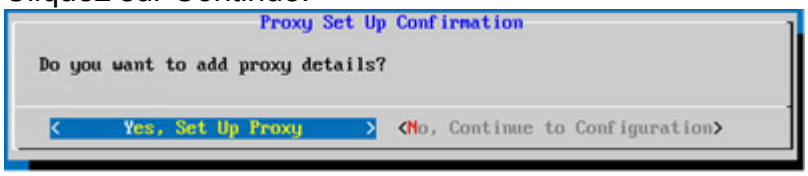
Confirmation

5. Confirmez les entrées et cliquez sur Yes, Continue.



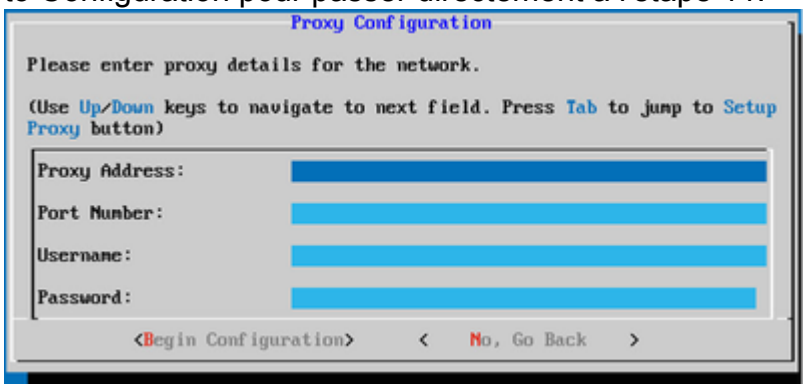
Sous-réseau personnalisé

6. Entrez l'adresse IP de sous-réseau personnalisé pour la configuration de cluster K3S (si le sous-réseau par défaut d'un client est en conflit avec le réseau de ses périphériques, sélectionnez un autre sous-réseau personnalisé).
7. Cliquez sur Continue.



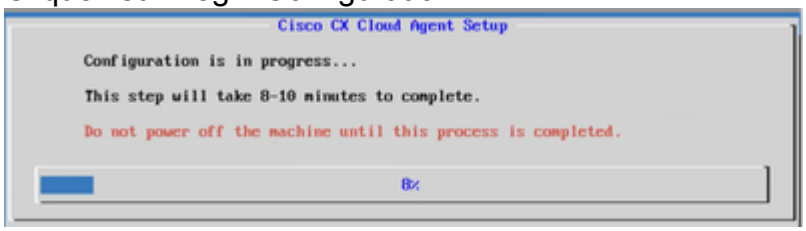
Configuration du proxy

8. Cliquez sur Yes, Set Up Proxy pour définir les détails du proxy ou cliquez sur No, Continue to Configuration pour passer directement à l'étape 11.

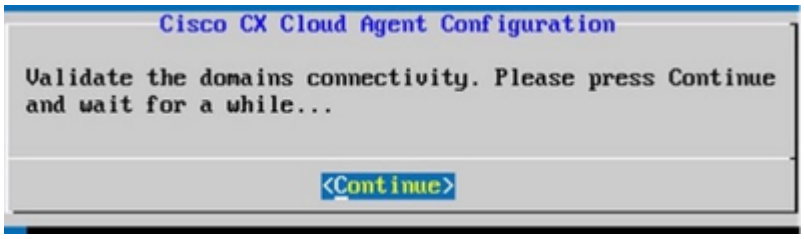


Configuration du proxy

9. Saisissez l’adresse proxy, le numéro de port, le nom d’utilisateur et le mot de passe.
10. Cliquez sur Begin Configuration.

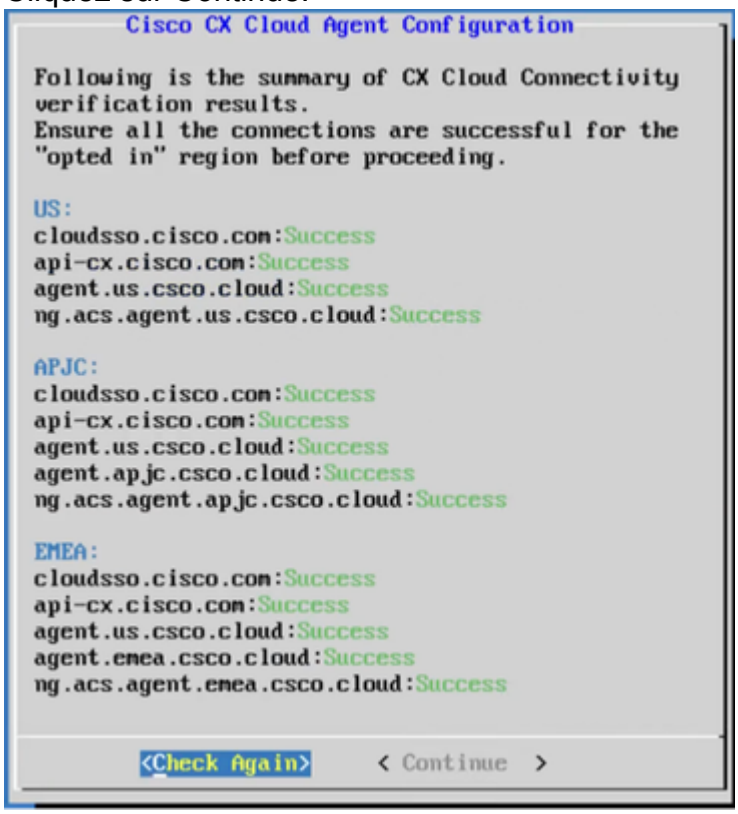


Configuration de CX Cloud Agent



Configuration de CX Cloud Agent

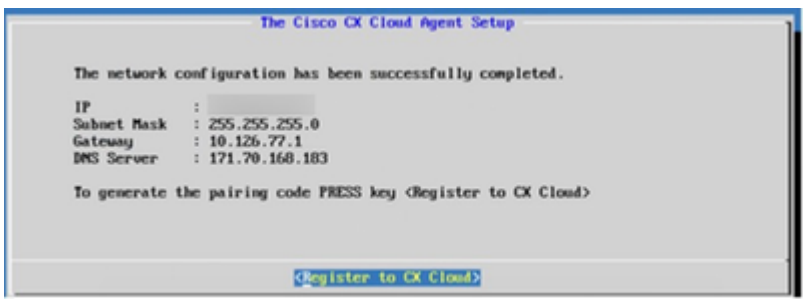
11. Cliquez sur Continue.



La configuration continue

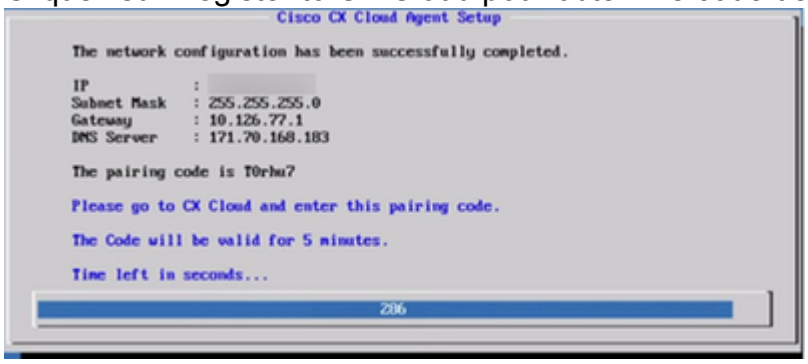
12. Cliquez sur Continue pour poursuivre la configuration pour atteindre le domaine avec succès. La configuration peut prendre plusieurs minutes.

Remarque : Si les domaines ne peuvent pas être atteints correctement, le client doit corriger l'accessibilité des domaines en apportant des modifications à son pare-feu pour s'assurer que les domaines sont accessibles. Cliquez sur Check Again une fois que le problème d'accessibilité des domaines est résolu.



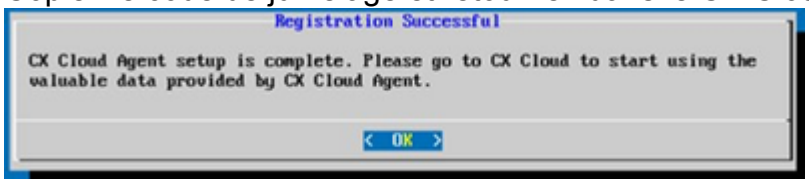
S'inscrire au CX Cloud

13. Cliquez sur Register to CX Cloud pour obtenir le code de jumelage.



Code de jumelage

14. Copiez le code de jumelage et retournez dans le CX Cloud pour continuer la configuration.



Inscription réussie

Remarque : Si le code d'appariement expire, cliquez sur Register to CX Cloud pour générer un nouveau code d'appariement (Étape 13).

---

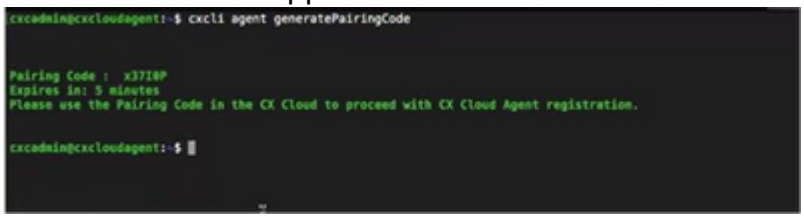
15. Cliquez sur OK.

Autre approche pour générer un code de jumelage à l'aide de CLI

Les utilisateurs peuvent également générer un code de jumelage à l'aide des options CLI.

Pour générer un code de jumelage à l'aide de CLI :

1. Connectez-vous à l'agent cloud via SSH à l'aide des informations d'identification utilisateur cxcadmin.
2. Générez le code d'appariement à l'aide de la commande cxcli agent generatePairingCode.



Générer le code de jumelage de la CLI

3. Copiez le code de jumelage et retournez dans le CX Cloud pour continuer la configuration.

Configuration des périphériques pour transférer Syslog vers CX Cloud Agent

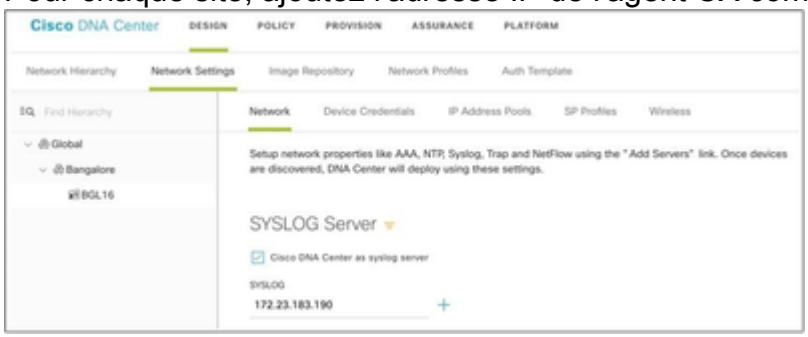
Conditions préalables

Les versions 2.1.2.0 à 2.2.3.5, 2.3.3.4 à 2.3.3.6, 2.3.5.0 et Cisco Catalyst Center Virtual Appliance sont prises en charge par Cisco Catalyst Center

Configuration du paramètre Syslog Forward

Pour configurer Syslog Forwarding to CX Agent dans Cisco Catalyst Center, procédez comme suit :

1. Lancez Cisco Catalyst Center.
2. Accédez à Design > Network Settings > Network.
3. Pour chaque site, ajoutez l'adresse IP de l'agent CX comme serveur Syslog.



Syslog Server (Serveur de journal système)

Remarque : Une fois configurés, tous les périphériques associés à ce site sont configurés pour envoyer le journal système avec le niveau critique à l'agent CX. Les périphériques doivent être associés à un site pour permettre le transfert syslog du périphérique vers CX Cloud Agent. Lorsqu'un paramètre de serveur syslog est mis à jour, tous les périphériques associés à ce site sont automatiquement définis sur le niveau critique par défaut.

Configuration d'autres ressources (collecte directe des périphériques) pour transférer Syslog à l'agent CX

Les périphériques doivent être configurés pour envoyer des messages Syslog à l'agent CX afin d'utiliser la fonctionnalité Fault Management de CX Cloud.

Remarque : L'agent CX signale uniquement les informations syslog des ressources Campus Success Track de niveau 2 vers CX Cloud. Les autres ressources ne peuvent pas configurer leur syslog sur CX Agent et leurs données syslog ne sont pas consignées dans CX Cloud.

Serveurs Syslog existants avec fonctionnalité de transfert

Suivez les instructions de configuration du logiciel serveur syslog et ajoutez l'adresse IP de l'agent CX comme nouvelle destination.

Remarque : Lors du transfert des syslogs, assurez-vous que l'adresse IP source du message syslog d'origine est conservée.

Serveurs Syslog existants sans fonctionnalité de transfert OU sans serveur Syslog

Configurez chaque périphérique pour qu'il envoie les syslogs directement à l'adresse IP de l'agent CX. Reportez-vous à cette documentation pour connaître les étapes de configuration spécifiques.

Guide de configuration de Cisco IOS® XE

Guide de configuration du contrôleur sans fil AireOS

Activation des paramètres Syslog au niveau des informations pour Cisco Catalyst Center

Pour rendre le niveau d'informations Syslog visible, procédez comme suit :

1. Accédez à Outils>Télémétrie.



Menu Outils

2. Sélectionnez et développez la vue Site et sélectionnez un site dans la hiérarchie des sites.



Vue du site

3. Sélectionnez le site requis et activez la case à cocher Device name pour tous les périphériques.
4. Sélectionnez Visibilité optimale dans la liste déroulante Actions.



Actions

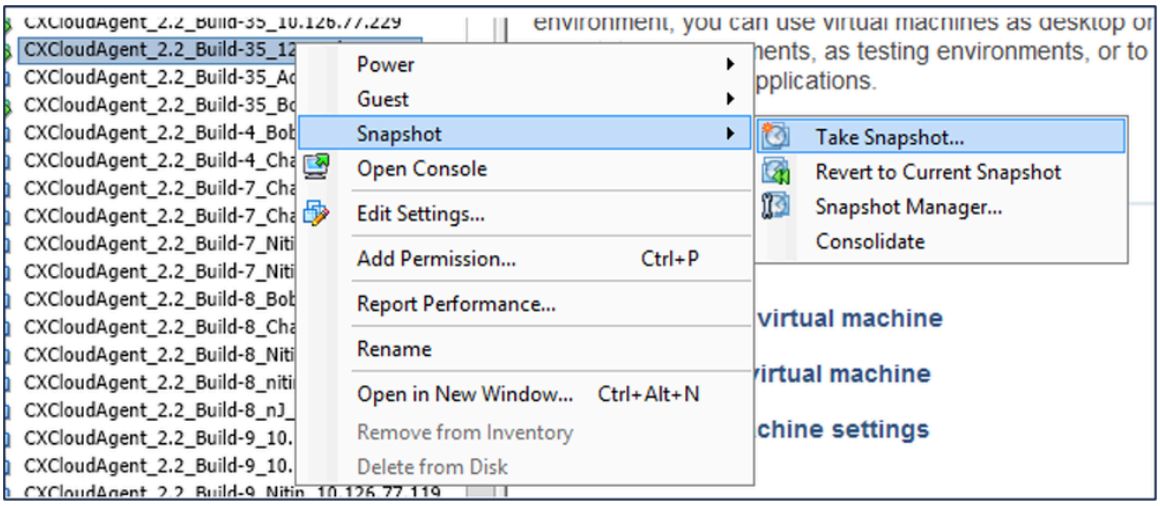
Sauvegarde et restauration de la machine virtuelle cloud CX

Il est recommandé de préserver l'état et les données d'une machine virtuelle CX Agent à un moment spécifique à l'aide de la fonction de snapshot. Cette fonction facilite la restauration de la VM du cloud CX à l'heure spécifique à laquelle le snapshot est pris.

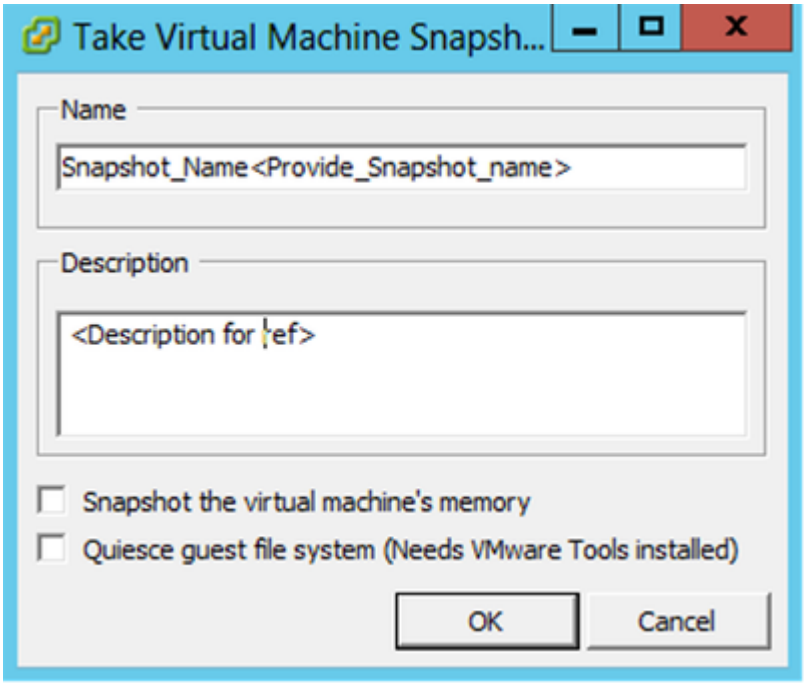
Sauvegarde de la machine virtuelle cloud CX

Pour sauvegarder la machine virtuelle CX Cloud :

1. Cliquez avec le bouton droit sur la VM et sélectionnez Snapshot > Take Snapshot. La fenêtre Take Virtual Machine Snapshot s'ouvre.



Sélectionner une machine virtuelle



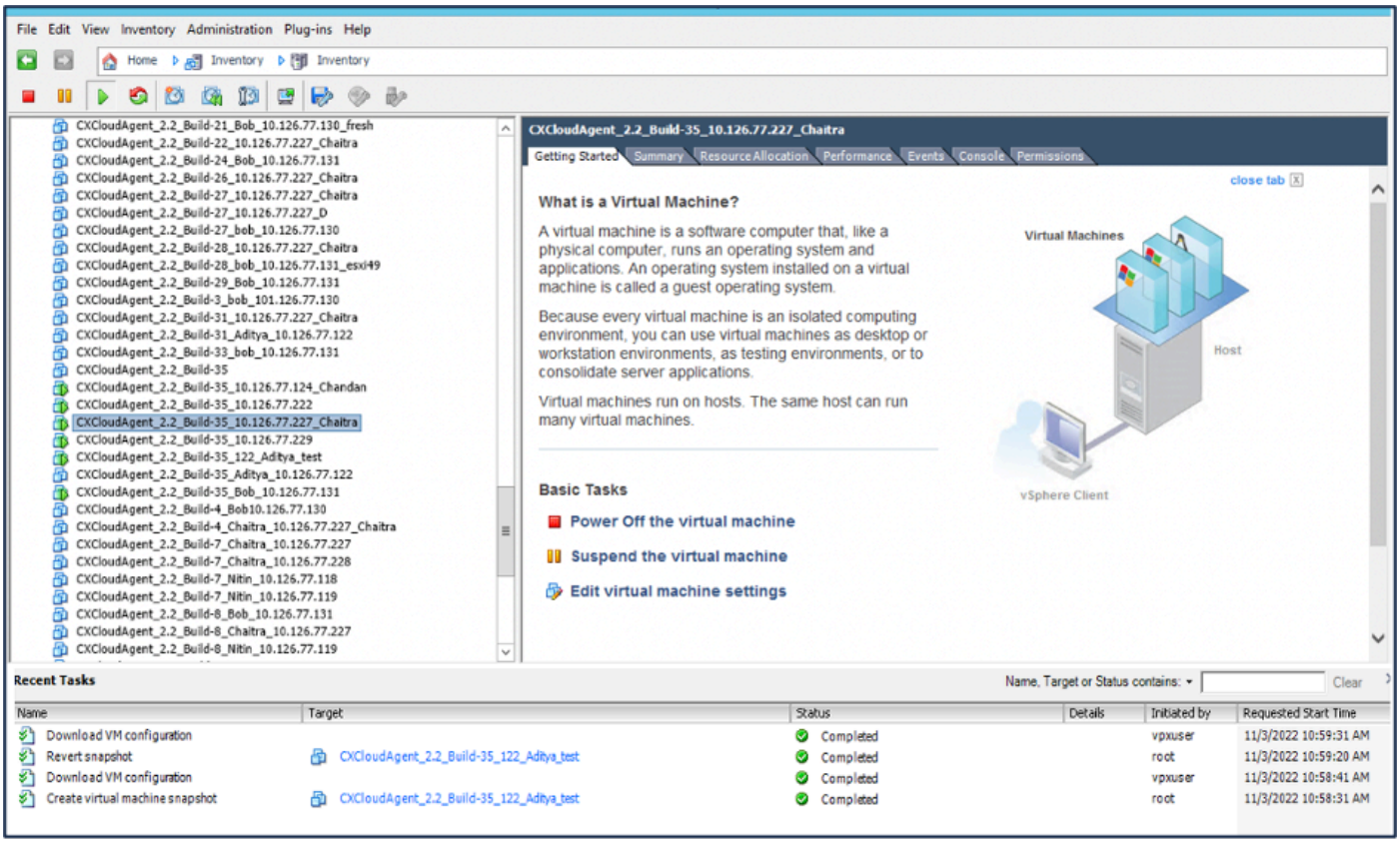
Prendre un snapshot de machine virtuelle

2. Saisissez le nom et la description.

Remarque : Vérifiez que la case à cocher Snapshot the virtual machine's memory (Instantané de la mémoire de la machine virtuelle) est désactivée.

---

3. Cliquez sur OK. L'état Créer un snapshot de machine virtuelle s'affiche comme Terminé dans la liste Tâches récentes.

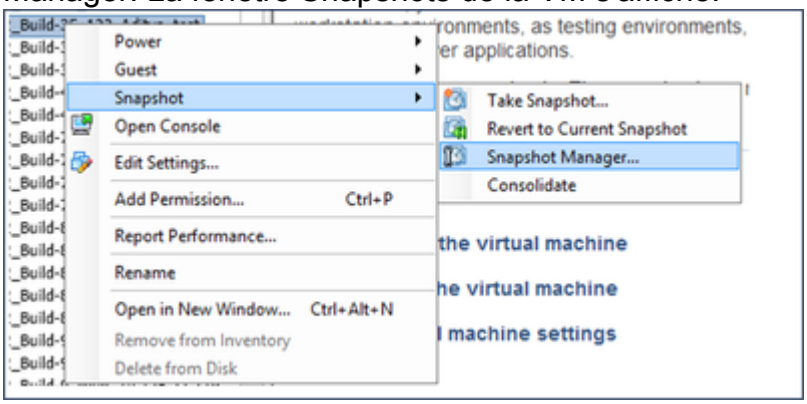


Tâches récentes

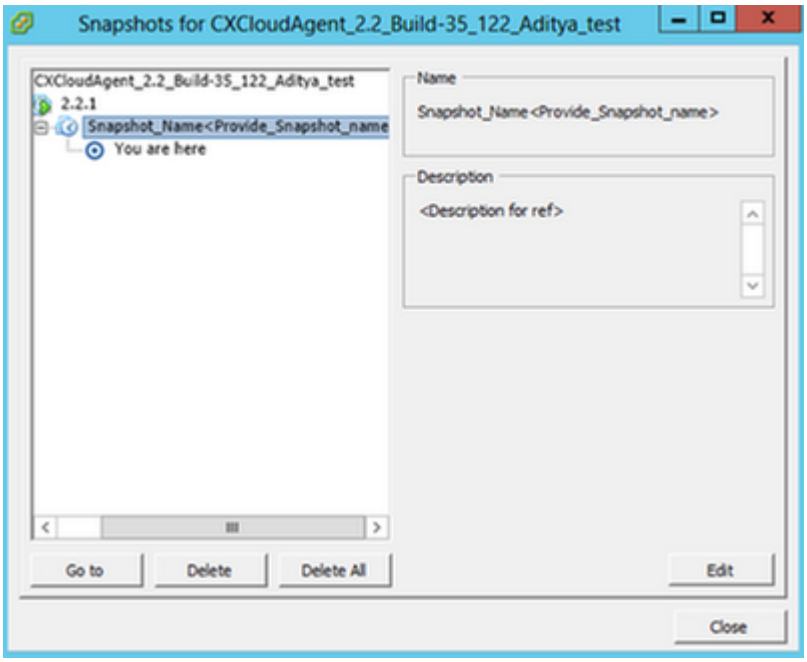
Restauration de la machine virtuelle du cloud CX

Pour restaurer la machine virtuelle CX Cloud :

1. Cliquez avec le bouton droit sur la VM et sélectionnez Snapshot > Snapshot Manager. La fenêtre Snapshots de la VM s'affiche.

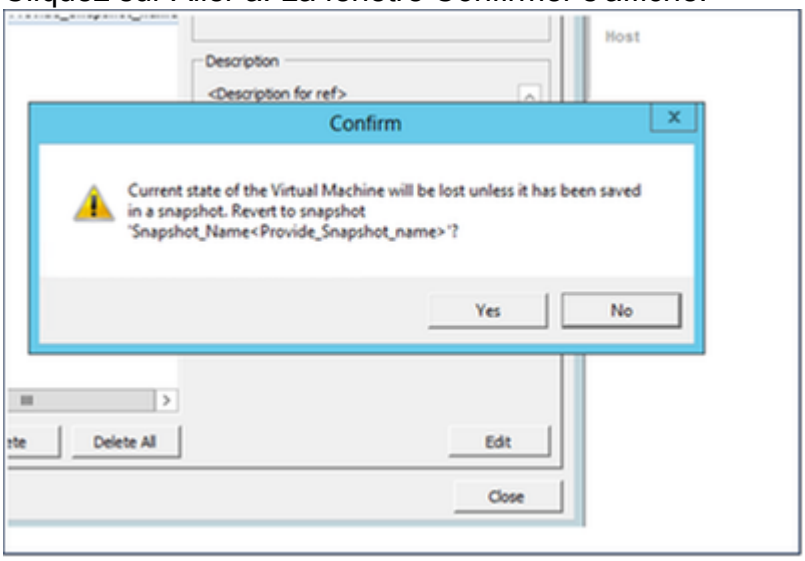


Fenêtre Sélectionner une VM



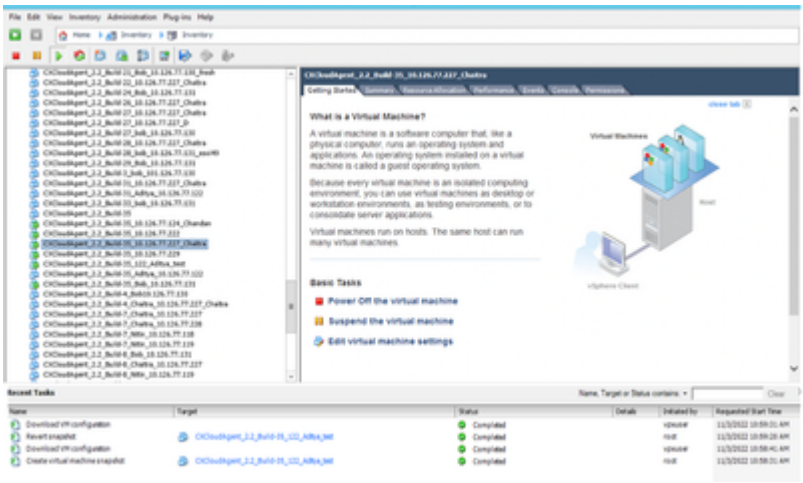
Fenêtre Clichés

2. Cliquez sur Aller à. La fenêtre Confirmer s'affiche.



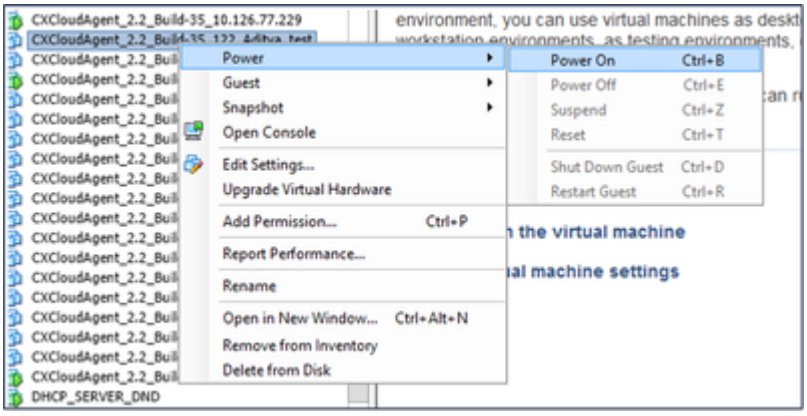
Fenêtre de confirmation

3. Cliquez sur Yes. L'état Rétablir le snapshot s'affiche comme Terminé dans la liste Tâches récentes.



Tâches récentes

4. Cliquez avec le bouton droit sur la VM et sélectionnez Power > Power On pour mettre la VM sous tension.



Sécurité

CX Agent garantit au client une sécurité de bout en bout. La connexion entre CX Cloud et CX Agent est sécurisée par TLS. L'utilisateur SSH par défaut de Cloud Agent est limité aux opérations de base.

Sécurité physique

Déployez l'image OVA de l'agent CX dans une entreprise de serveurs VMware sécurisée. L'OVA est partagé en toute sécurité par l'intermédiaire du centre de téléchargement de logiciels Cisco. Le mot de passe du chargeur de démarrage (mode utilisateur unique) est défini avec un mot de passe unique au hasard. Les utilisateurs doivent se référer à cette FAQ pour définir ce mot de passe du chargeur de démarrage (mode mono-utilisateur).

Sécurité de compte

Lors du déploiement, le compte utilisateur cxcadmin est créé. Les utilisateurs sont forcés de définir un mot de passe lors de la configuration initiale. Les identifiants/utilisateurs cxcadmin sont utilisés pour accéder aux API de l'agent CX et pour se connecter à l'appliance via SSH.

les utilisateurs cxcadmin ont un accès restreint avec les privilèges les plus bas. Le mot de passe cxcadmin suit la stratégie de sécurité et est haché dans un sens avec une période d'expiration de 90 jours. les utilisateurs cxcadmin peuvent créer un utilisateur cxcroot à l'aide de l'utilitaire appelé remoteaccount. les utilisateurs cxcroot peuvent obtenir des privilèges root.

Sécurité du réseau

La machine virtuelle CX Agent est accessible via SSH avec les informations d'identification de l'utilisateur cxcadmin. Les ports entrants sont limités à 22 (ssh) et à 514 (Syslog).

Authentification

Authentification par mot de passe : L'appliance gère un utilisateur unique (cxcadmin) qui permet à l'utilisateur de s'authentifier et de communiquer avec l'agent CX.

- Racine des actions privilégiées sur l’appliance à l’aide de ssh.

les utilisateurs cxcadmin peuvent créer un utilisateur cxcroot à l'aide d'un utilitaire appelé remoteaccount. Cet utilitaire affiche un mot de passe chiffré RSA/ECB/PKCS1v1_5 qui ne peut être déchiffré qu'à partir du portail SWIM (formulaire de demande DECRYPT). Seul le personnel autorisé a accès à ce portail. les utilisateurs cxcroot peuvent obtenir des privilèges root en utilisant ce mot de passe déchiffré. La phrase secrète n’est valide que pour deux jours. Les utilisateurs cxcadmin doivent recréer le compte et obtenir le mot de passe à partir du portail SWIM après expiration du mot de passe.

Durcissement

L'appliance CX Agent respecte les normes de renforcement du Centre de sécurité Internet.

Sécurité des données

L'appliance CX Agent ne stocke aucune information personnelle du client. L'application d'informations d'identification du périphérique (exécutée en tant que l'un des pods) stocke les informations d'identification du serveur chiffrées dans une base de données sécurisée. Les données collectées ne sont stockées sous aucune forme à l'intérieur de l'appareil, sauf temporairement lorsqu'elles sont en cours de traitement. Les données de télémétrie sont téléchargées sur le cloud CX dès que possible après la collecte et sont rapidement supprimées du stockage local après confirmation du succès du téléchargement.

Transmission de données

Le package d'enregistrement contient le certificat et les clés du périphérique X.509 uniques requis pour établir une connexion sécurisée avec Iot Core. L'utilisation de cet agent permet d'établir une connexion sécurisée à l'aide de MQTT (Message Queuing Telemetry Transport) sur TLS (Transport Layer Security) v1.2

Connexions et surveillance

Les journaux ne contiennent aucune forme de données d'informations personnelles identifiables (PII). Les journaux d'audit capturent toutes les actions sensibles à la sécurité effectuées sur l'appliance CX Cloud Agent.

Commandes de télémétrie Cisco

CX Cloud récupère la télémétrie des ressources à l'aide des API et des commandes répertoriées dans les commandes de télémétrie Cisco. Ce document classe les commandes en fonction de leur applicabilité à l'inventaire Cisco Catalyst Center, à Diagnostic Bridge, à Intersight, à Compliance Insights, à Faults et à toutes les autres sources de télémétrie collectées par l'agent CX.

Les informations sensibles de la télémétrie des ressources sont masquées avant d'être transmises au cloud. L'agent CX masque les données sensibles pour toutes les ressources collectées qui envoient des données de télémétrie directement à l'agent CX. Cela inclut les mots de passe, les clés, les chaînes de communauté, les noms d'utilisateur, etc. Les contrôleurs fournissent un masquage des données pour toutes les ressources gérées par les contrôleurs avant de transférer ces informations à l'agent CX. Dans certains cas, la télémétrie des ressources gérées par le contrôleur peut être rendue plus anonyme. Reportez-vous à la documentation d'assistance produit correspondante pour en savoir plus sur l'anonymisation de la télémétrie (par exemple, la section Anonymize Data du Guide de l'administrateur de Cisco Catalyst Center).

Bien que la liste des commandes de télémétrie ne puisse pas être personnalisée et que les règles de masquage des données ne puissent pas être modifiées, les clients peuvent contrôler les ressources auxquelles CX Cloud accède en spécifiant les sources de données, comme indiqué dans la documentation de support produit pour les périphériques gérés par contrôleur ou dans la section Connexions des sources de données de ce document (pour les autres ressources collectées par CX Agent).

Résumé de la sécurité

Fonctions de sécurité	Description
Mot de passe du chargeur de démarrage	Le mot de passe du chargeur de démarrage (mode utilisateur unique) est défini avec un mot de passe unique au hasard. Les utilisateurs doivent se référer à la FAQ pour définir son mot de passe du chargeur de démarrage (mode utilisateur unique).
Accès utilisateur	SSH : ·L'accès à l'appliance à l'aide de l'utilisateur cxcadmin nécessite des informations d'authentification créées lors de l'installation. · L'accès à l'appliance par l'utilisateur cxcroot nécessite que les identifiants

	soient décryptés par le personnel autorisé à l'aide du portail SWIM.
Comptes utilisateurs	·cxcadmin : compte d'utilisateur par défaut créé ; L'utilisateur peut exécuter les commandes de l'application Agent CX à l'aide de cxcli et dispose des privilèges les plus faibles sur l'appliance ; L'utilisateur cxcroot et son mot de passe chiffré sont générés à l'aide de l'utilisateur cxcadmin. ·cxcroot : cxcadmin peut créer cet utilisateur à l'aide de l'utilitaire remoteaccount ; L'utilisateur peut obtenir les privilèges racine avec ce compte.
politique de mot de passe cxcadmin	·Le mot de passe est haché de manière unidirectionnelle à l'aide de SHA-256 et stocké en toute sécurité. · Au moins huit (8) caractères, contenant trois de ces catégories : majuscules, minuscules, chiffres et caractères spéciaux.
politique de mot de passe cxcroot	·Le mot de passe cxcroot est chiffré RSA/ECB/PKCS1v1_5 ·La phrase secrète générée doit être déchiffrée dans le portail SWIM. · L'utilisateur et le mot de passe cxcroot sont valides pendant deux jours et peuvent être régénérés à l'aide de cxcadmin user.
politique de mot de passe de connexion ssh	· Au moins huit caractères qui contiennent trois de ces catégories : majuscules, minuscules, chiffres et caractères spéciaux. · Cinq tentatives de connexion infructueuses verrouillent la boîte pendant 30 minutes ; Le mot de passe expire dans 90 jours.
Ports	Ports entrants ouverts – 514 (Syslog) et 22 (ssh)
Sécurité des données	·Aucune information client enregistrée. ·Aucune donnée de périphérique enregistrée. · Les identifiants du serveur Cisco Catalyst Center sont chiffrés et stockés dans la base de données.

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.