Présentation de CX Cloud Agent v2.0

Table des matières

- Introduction
- Informations générales
  - Conditions préalables
  - Accès aux domaines critiques
    - Prérequis pour la mise à niveau vers CX Cloud Agent v2.0
  - Versions certifiées du centre Cisco DNA
  - Navigateurs pris en charge
- Déploiement de CX Cloud Agent
- Connexion de CX Cloud Agent au cloud CX
- Déploiement et configuration du réseau
  - Déploiement OVA
    - Installation du client lourd ESXi 5.5/6.0
    - Installation du client Web ESXi 6.0
    - Installation de client Web vCenter
    - Installation d'Oracle Virtual Box 5.2.30
    - Installation de Microsoft Hyper-V
  - Configuration du réseau
  - Autre approche pour générer un code de jumelage à l'aide de CLI
- Configurer Cisco DNA Center pour transférer Syslog vers CX Cloud Agent
  - Prérequis
  - Configurer le paramètre de transfert Syslog
  - Activer les paramètres Syslog au niveau des informations
- Sécurité
  - Sécurité physique
  - Accès utilisateur
  - Sécurité de compte
  - Sécurité du réseau
  - Authentification
  - Durcissement
  - Sécurité des données
  - Transmission de données
  - Connexions et surveillance
  - Résumé de la sécurité
- Forum aux questions
  - Agent CX Cloud
    - Déploiement
    - Versions et correctifs
    - Configuration de l'authentification et du proxy
    - Protocole SSH (Secure Shell)
    - Ports et services

Connexion de l’agent CX Cloud au centre Cisco DNA

Analyse de diagnostic utilisée par l’agent CX Cloud

Journaux du système de l’agent CX Cloud

Dépannage

Réponses aux échecs de collecte

Réponses aux échecs de l'analyse diagnostique

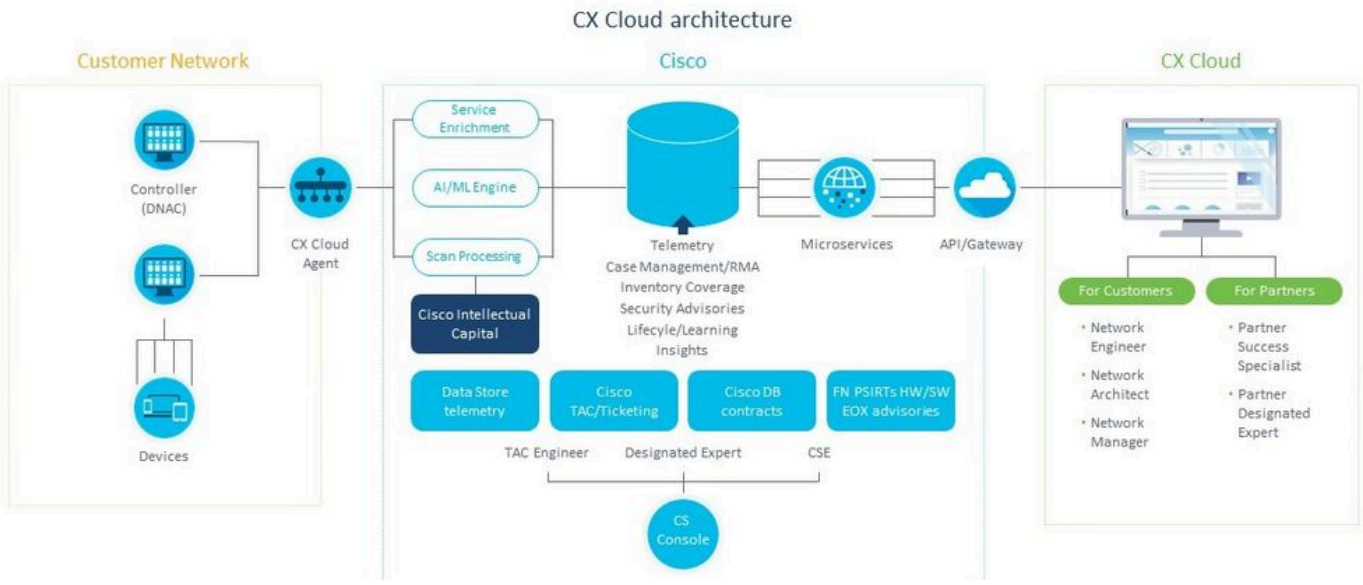
Introduction

Ce document décrit Cisco CX Cloud Agent, une plate-forme logicielle modulaire sur site qui héberge des fonctionnalités de microservice conteneurisé légères.

Informations générales

Les fonctionnalités de l'agent cloud Cisco Customer Experience (CX) peuvent être installées, configurées et gérées sur le site du client à partir du cloud. CX Cloud Agent accélère la monétisation de nouvelles offres, fait évoluer les fonctionnalités et aide à développer des services de nouvelle génération basés sur le Big Data, l'analytique, l'automatisation, l'apprentissage automatique/l'intelligence artificielle (ML/AI) et la diffusion en continu.

Remarque : Ce guide est destiné aux utilisateurs de CX Cloud Agent v2.0. Veuillez vous reporter à Cisco CX Cloud Agent pour d'autres informations connexes.



Architecture de l’agent CX Cloud

Architecture de l’agent CX Cloud

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

Conditions préalables

L’agent CX Cloud fonctionne comme une machine virtuelle (VM) et peut être téléchargé en tant qu’appliance virtuelle ouverte (OVA) ou disque dur virtuel (VHD).

Exigences de déploiement :

- Un de ces hyperviseurs :
  - VMware ESXi version 5.5 ou ultérieure
  - Oracle Virtual Box 5.2.30
  - Hyperviseur Windows version 2012 à 2016
- L'hyperviseur peut héberger une machine virtuelle qui nécessite :
  - CPU 8 cœurs
  - 16 Go mémoire/RAM
  - 200 Go d’espace disque
- Pour les clients qui utilisent des data centers Cisco US désignés comme principale région de données pour stocker les données du cloud CX :
  L'agent cloud CX doit pouvoir se connecter aux 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) : ng.acs.agent.us.csco.cloud
  Nom de domaine complet (FQDN) : cloudsso.cisco.com
  Nom de domaine complet (FQDN) : api-cx.cisco.com
- Pour les clients qui utilisent des data centers Cisco Europe désignés comme la principale région de données pour stocker les données du cloud CX :
  L'agent cloud 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
  Nom de domaine complet (FQDN) : cloudsso.cisco.com
  Nom de domaine complet (FQDN) : api-cx.cisco.com
- Pour les clients qui utilisent des data centers Cisco Asie-Pacifique désignés comme principale région de données pour stocker les données du cloud CX :
  L'agent cloud 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
  Nom de domaine complet (FQDN) : cloudsso.cisco.com
  Nom de domaine complet (FQDN) : api-cx.cisco.com

- Pour les clients qui utilisent les data centers désignés Cisco Europe et Cisco 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.

Autres remarques sur l’agent CX Cloud :

- 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, un masque de sous-réseau, une adresse IP de passerelle par défaut et une adresse IP de serveur DNS doivent être disponibles.
- Seul IPv4 est pris en charge, pas IPv6.
- Les versions certifiées de Cisco Digital Network Architecture (DNA) Center 1.2.8 à 1.3.3.9 et 2.1.2.0 à 2.2.3.5 à noeud unique et cluster haute disponibilité (HA) sont requises.
- Si le réseau dispose d'une interception SSL, indiquez l'adresse IP de l'agent cloud CX.

Accès aux domaines critiques

Pour démarrer le parcours vers le cloud CX, les utilisateurs doivent avoir accès à ces domaines.

Principaux domaines	Autres domaines
cisco.com	mixpanel.com
csco.cloud	cloudfront.net
split.io	eum-appdynamics.com
	appdynamics.com
	tiqcdn.com
	jquery.com

Domaines spécifiques à la région :

AMÉRIQUE	EMEA	APJC
cloudsso.cisco.com	cloudsso.cisco.com	cloudsso.cisco.com
api-cx.cisco.com	api-cx.cisco.com	api-cx.cisco.com

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

Conditions préalables à la mise à niveau vers CX Cloud Agent v2.0

Les conditions préalables décrites dans cette section doivent être remplies avant la mise à niveau vers CX Cloud Agent v2.0.

1. Assurez-vous que CX Cloud Agent v1.12.x et versions ultérieures doivent être installés avant le lancement de la mise à niveau.
2. Procédez comme suit pour configurer le serveur de noms de domaine s'il n'est pas déjà configuré :
    1. Connectez-vous à la console CLI (Command Line Interface) de la machine virtuelle CX Cloud Agent.
    2. Exécutez la commande cxcli agent configureDNS.
    3. Saisissez l'adresse IP DNS.
    4. Cliquez sur Exit.
3. Assurez-vous que le réseau du client autorise les noms de domaine dans Critical Domain Access à finaliser le réenregistrement de l'agent cloud lors de la migration. CX Cloud Agent doit être en mesure d'atteindre ces domaines et les domaines doivent également pouvoir être résolus à partir du serveur DNS. Contactez l'équipe réseau si un domaine est inaccessible.
4. Prenez un snapshot de machine virtuelle Cloud Agent avant de lancer la mise à niveau v2.0 (accès approprié requis).

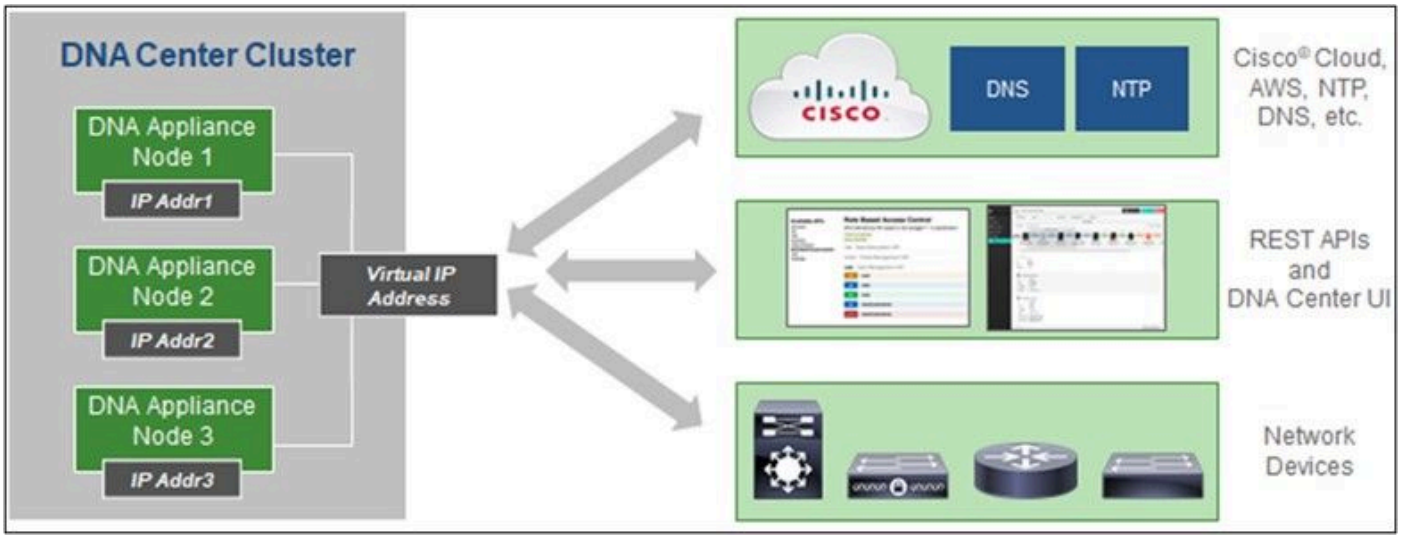
Remarque : Les versions antérieures à la version 1.10 doivent d'abord être mises à niveau vers la version 1.10, puis par mises à niveau incrémentielles vers la version 1.12.x, puis vers la version 2.0. Les utilisateurs peuvent effectuer une mise à niveau à partir de Paramètres d'administration > Sources de données dans le portail Cloud CX. Cliquez sur View Update pour terminer la mise à niveau.

Ces conditions doivent être remplies pour que la configuration réussisse :

1. Liste des DNAC et de leurs références
2. Utilisateur DNAC avec accès au rôle Admin ou Observer
3. Adresse IP virtuelle ou adresse IP physique/autonome pour le cluster DNAC
4. Accessibilité réussie entre l'agent cloud et DNAC
5. DNAC doit avoir au moins 1 (un) périphérique géré

Versions certifiées du centre Cisco DNA

Les versions certifiées de nœud unique et de grappe haute disponibilité du centre Cisco DNA sont les versions 1.2.8 à 1.3.3.9 et 2.1.2.0 à 2.2.3.5.



Grappe haute disponibilité multi-nœuds du centre Cisco DNA

Grappe haute disponibilité multi-nœuds du centre Cisco DNA

Navigateurs pris en charge

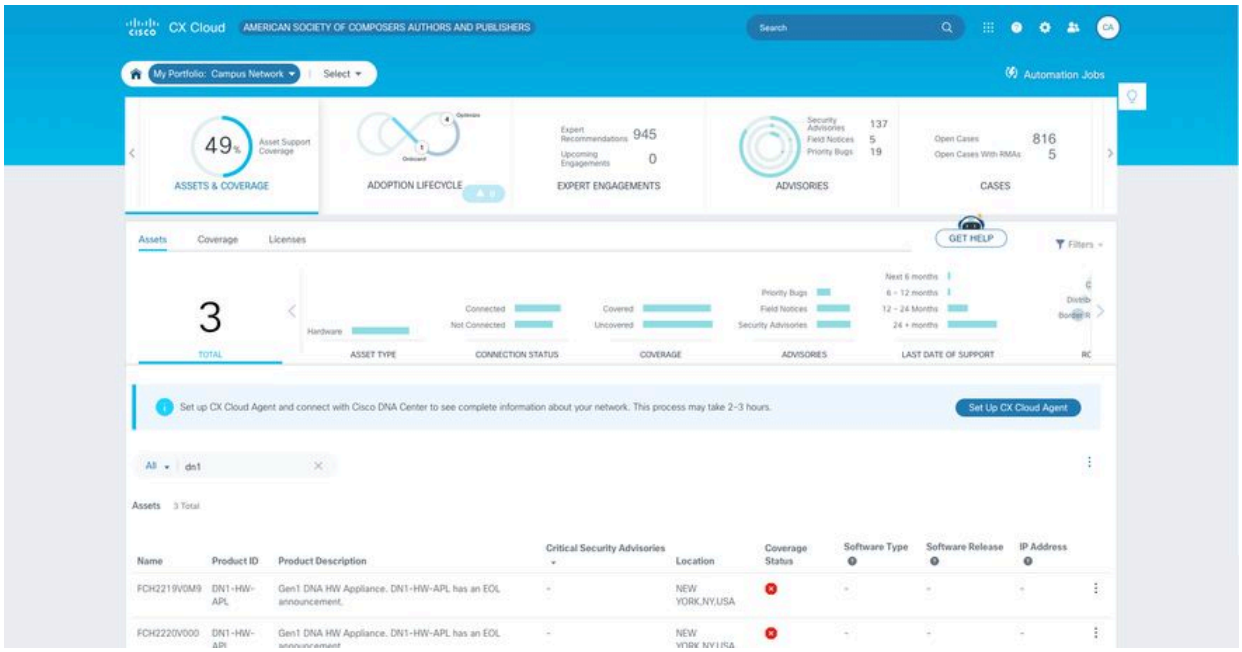
Pour une expérience optimale sur Cisco.com, nous vous recommandons la dernière version officielle des navigateurs suivants :

- Google Chrome
- Microsoft Edge
- Mozilla Firefox

Déploiement de CX Cloud Agent

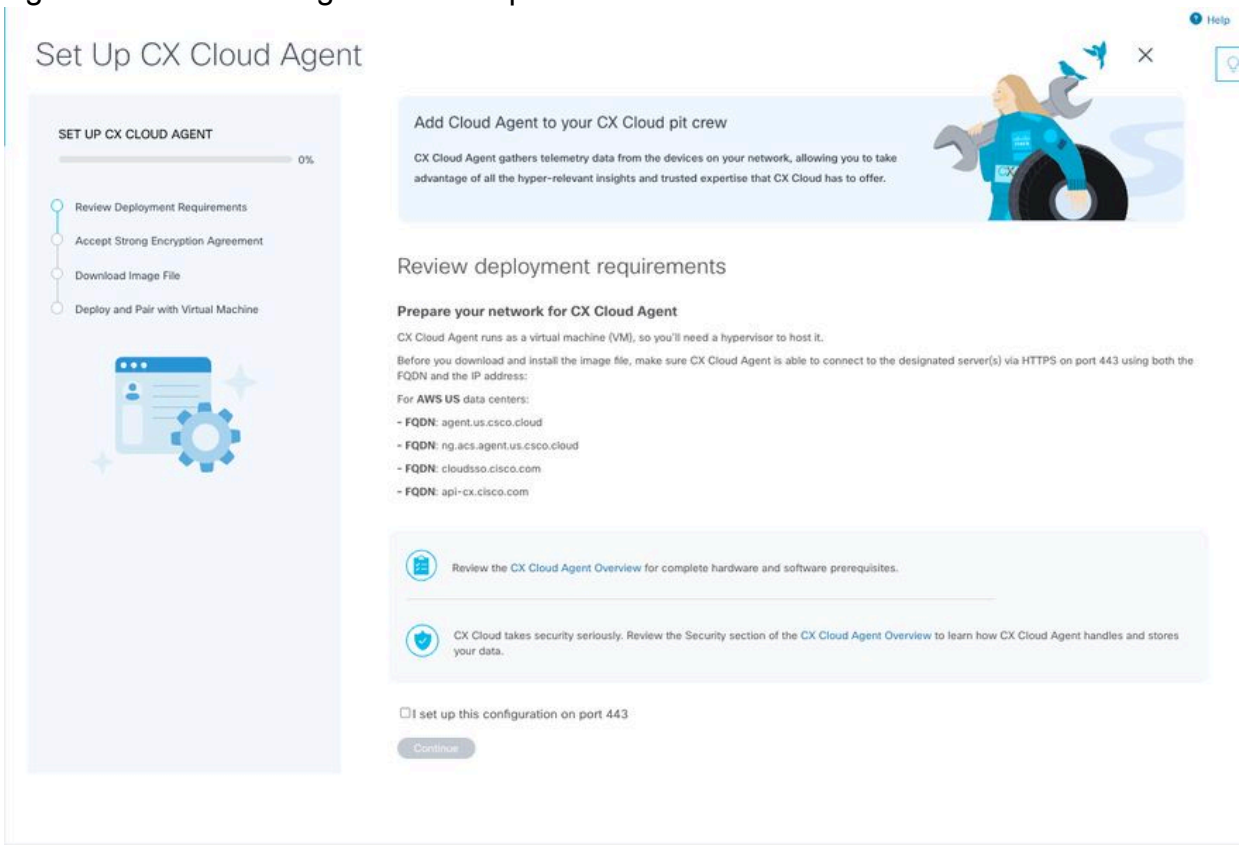
Pour déployer l'agent CX Cloud :

1. Cliquez sur cx.cisco.com pour vous connecter à CX Cloud.
2. Sélectionnez Campus Network et accédez à la vignette ASSETS & COVERAGE.



Page d'accueil

3. Cliquez sur Set Up CX Cloud Agent dans la bannière. La fenêtre Configurer CX Cloud Agent - Vérifier les exigences de déploiement s'ouvre.



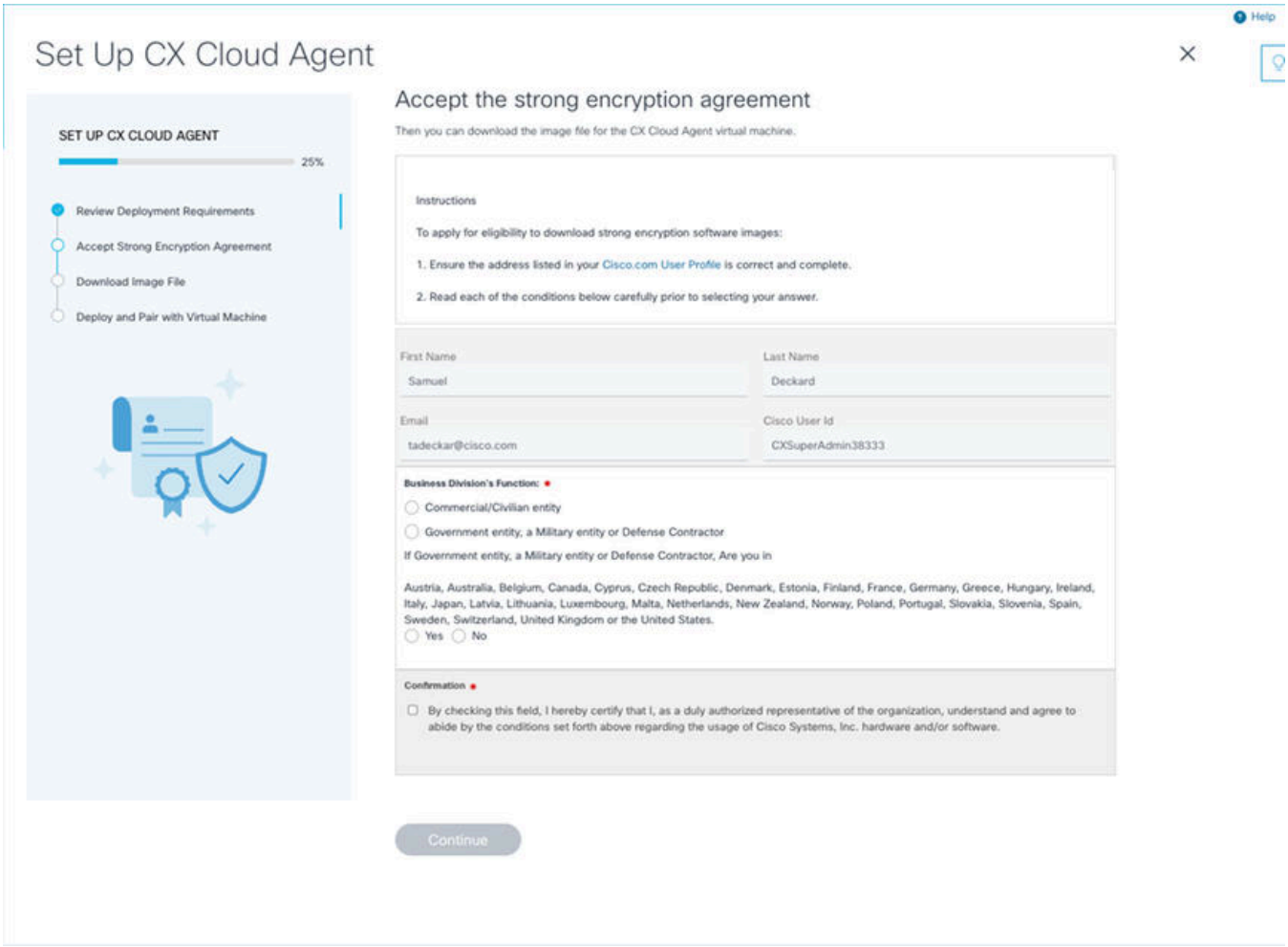
Examen des exigences de déploiement

4. Lisez les conditions préalables dans Vérifier les exigences de déploiement et activez la case à cocher Je configure cette configuration sur le port 443.

Remarque : Les images (et leur contenu) de ce guide sont fournies à titre de référence

uniquement. Le contenu réel peut varier.

5. Cliquez sur Continuer. La fenêtre Set Up CX Cloud Agent - Accept the strong encryption agreement s'affiche.



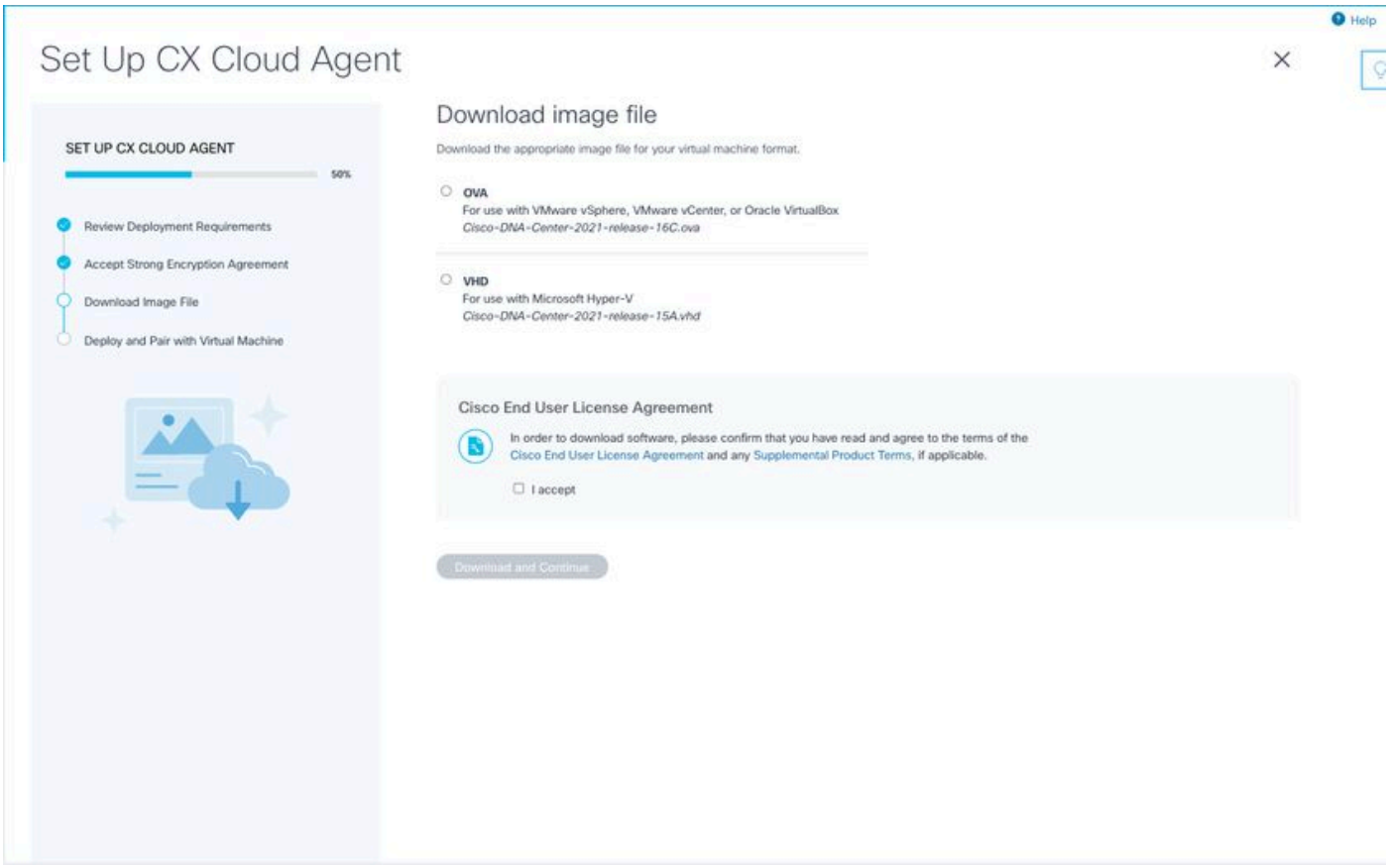
Contrat de chiffrement

6. Vérifiez les informations préremplies dans les champs Prénom, Nom, Courrier électronique et ID utilisateur CCO.

7. Sélectionnez le Business division’s function.

8. Cochez la case Confirmation pour accepter les conditions d'utilisation.

9. Cliquez sur Continuer. La fenêtre Set Up CX Cloud Agent - Download image file s'ouvre.



Télécharger l'image

10. Sélectionnez le format de fichier approprié pour télécharger le fichier image requis pour l'installation.

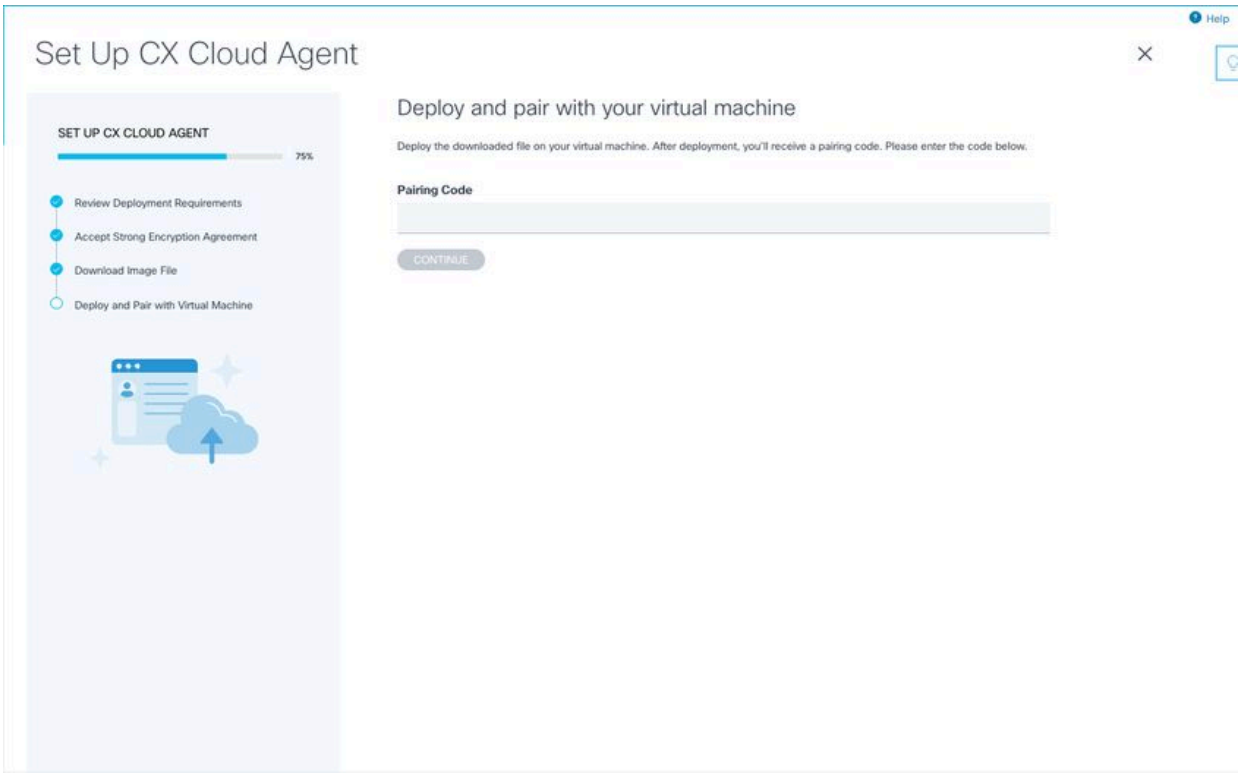
11. Cochez la case J'accepte pour accepter le Contrat de licence d'utilisateur final Cisco.

12. Cliquez sur Download and Continue. La fenêtre Set Up CX Cloud Agent - Deploy and pair with your virtual machine s'ouvre.

13. Reportez-vous à Configuration réseau pour l'installation d'OVA et passez à la section suivante pour installer l'agent cloud CX.

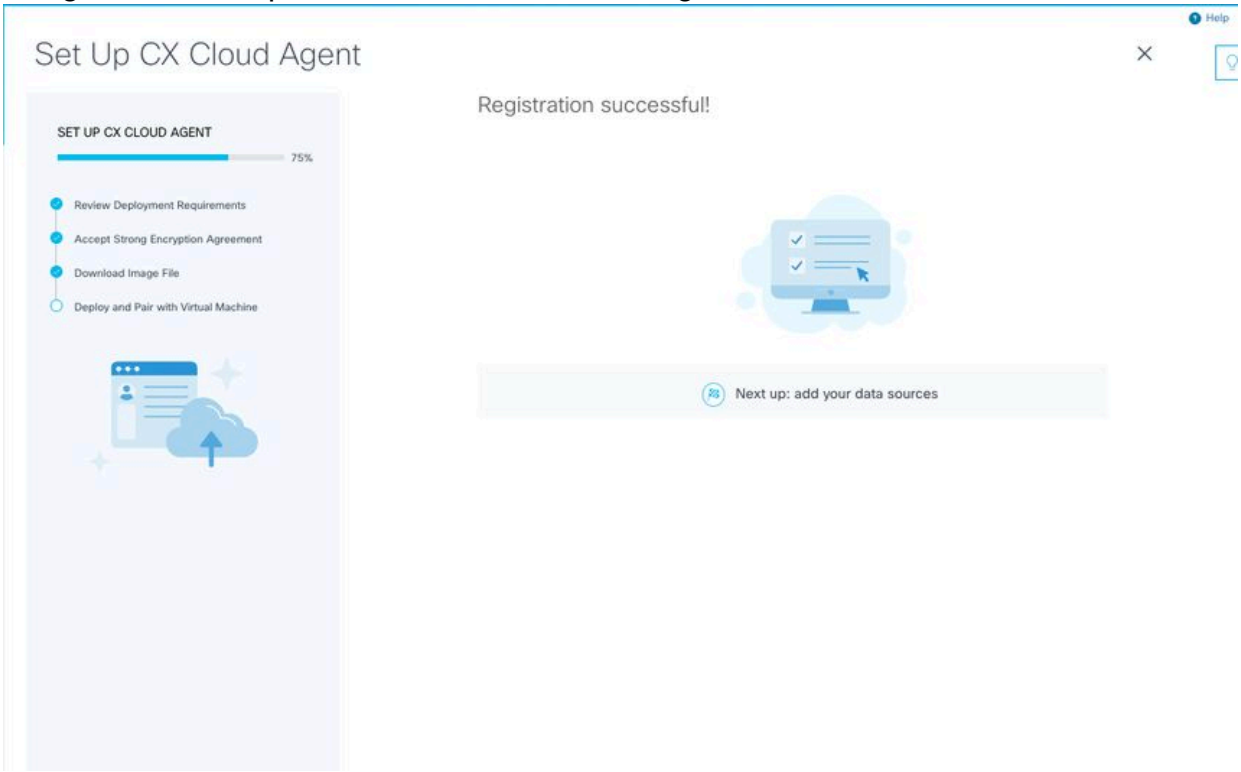
Connexion de CX Cloud Agent au cloud CX

1. Saisissez le code d'appariement fourni dans la boîte de dialogue de la console ou dans l'interface de ligne de commande (CLI).

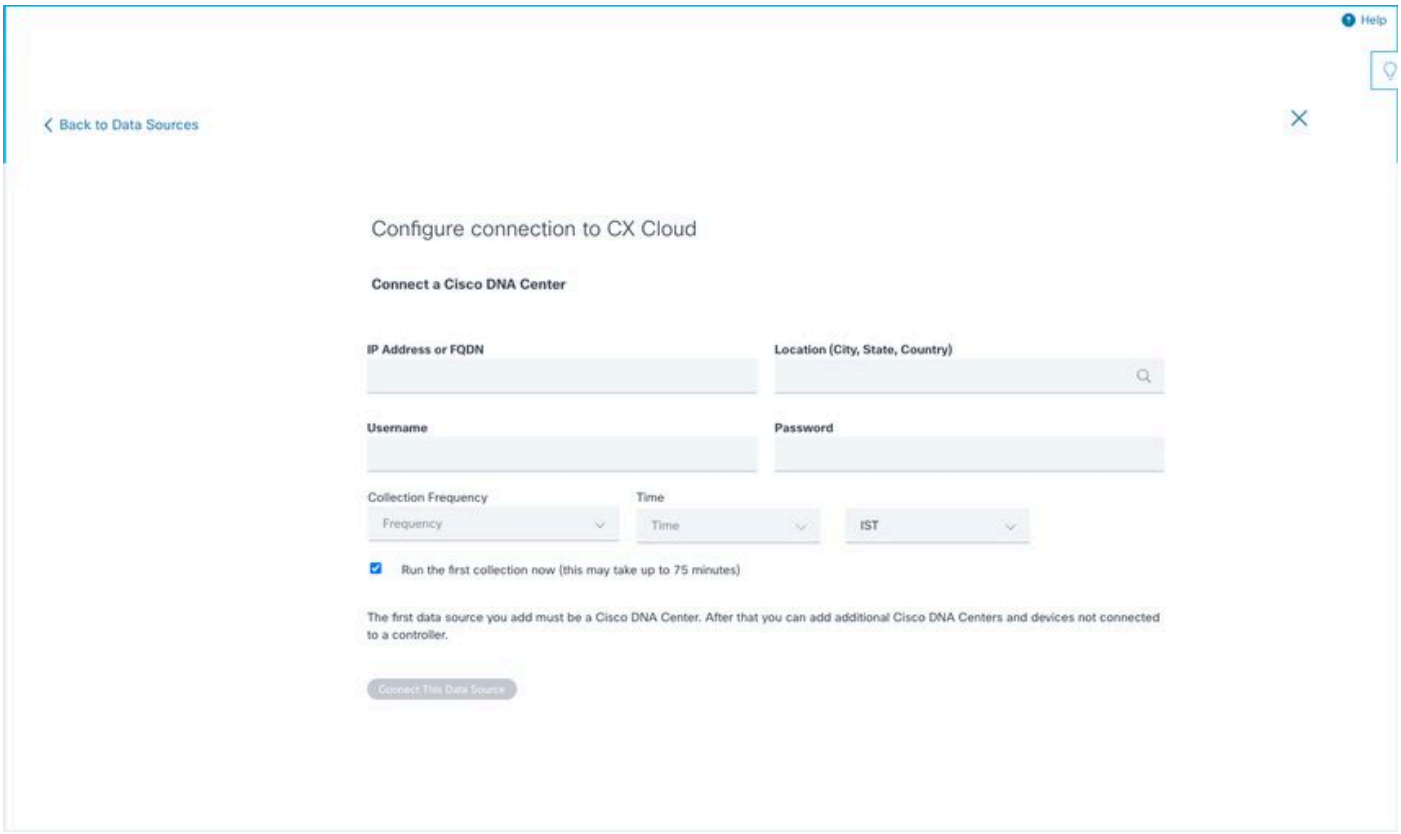


Code de jumelage

2. Cliquez sur Continue pour enregistrer l'agent cloud CX. La fenêtre Set Up CX Cloud Agent - Registration successful s'affiche pendant quelques secondes avant de naviguer automatiquement vers la fenêtre Configure Connection to CX Cloud

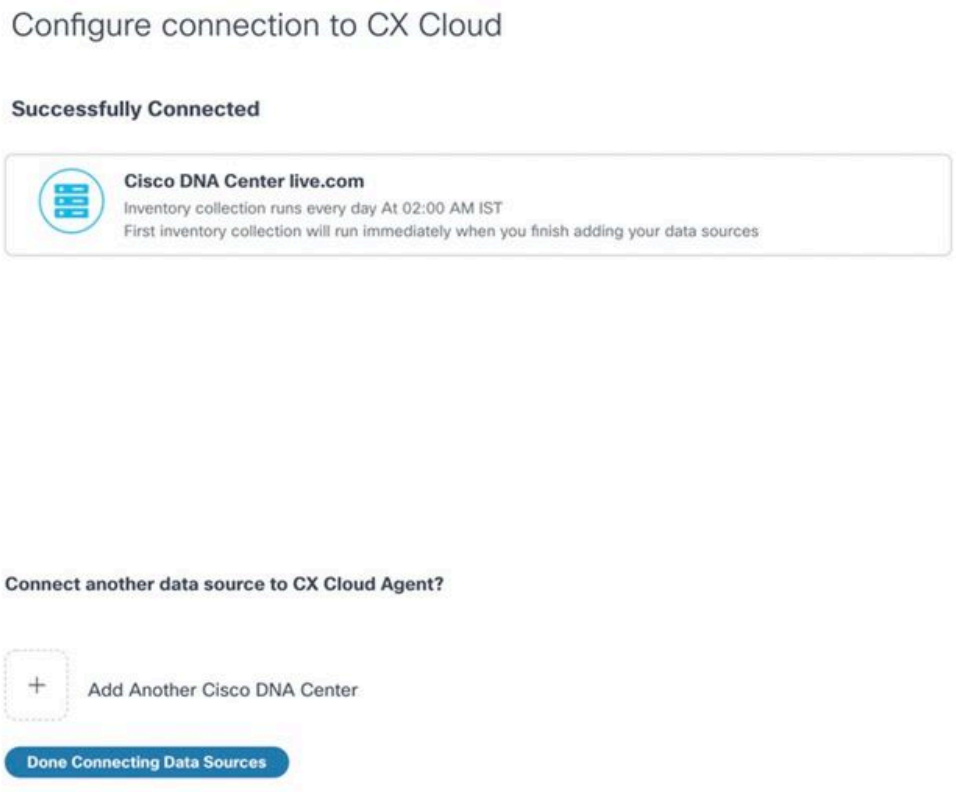


Inscription réussie



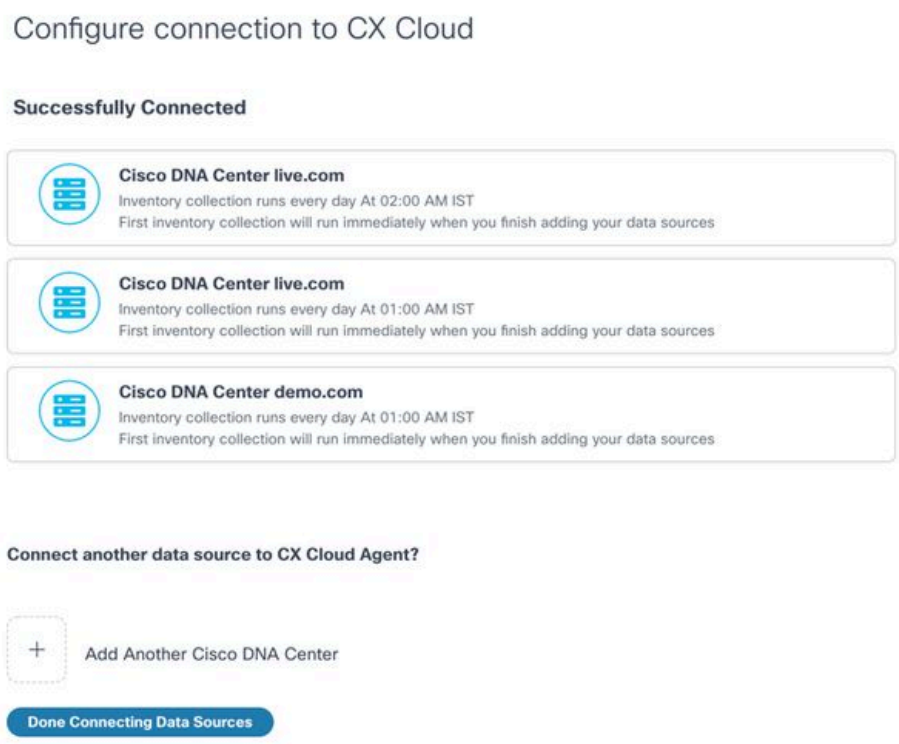
Configurer la connexion

3. Entrez les données et cliquez sur Connecter cette source de données. Le message de confirmation « Connexion réussie » s'affiche.



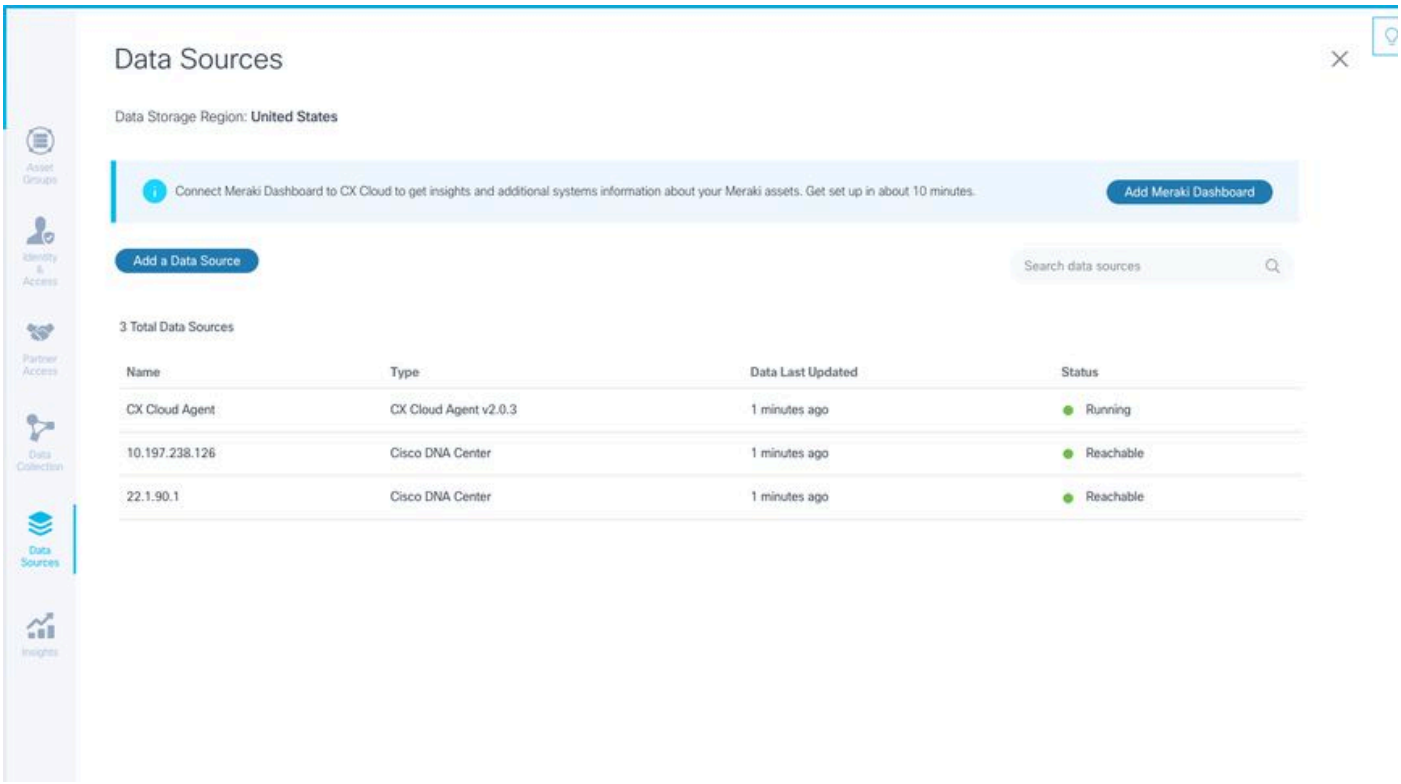
Ajout de DNAC réussi

Remarque : Cliquez sur Add Another Cisco DNA Centerpour ajouter plusieurs DNAC.



Ajout de plusieurs DNAC

4. Cliquez sur Terminé la connexion des sources de données. La fenêtre Sources de données s'ouvre.



Source de données

Déploiement et configuration du réseau

Vous pouvez sélectionner l'une des options suivantes pour déployer CX Cloud Agent :

- Si vous sélectionnez VMware vSphere/vCenter client lourd ESXi 5.5/6.0, allez au client lourd
- Si vous sélectionnez VMware vSphere/vCenter Web Client ESXi 6.0, allez au client Web vSphere ou au Centre
- Si vous sélectionnez Oracle Virtual Box 5.2.30, accédez à la machine virtuelle Oracle
- Si vous sélectionnez Microsoft Hyper-V, allez à Hyper-V

Déploiement OVA

Installation du client lourd ESXi 5.5/6.0

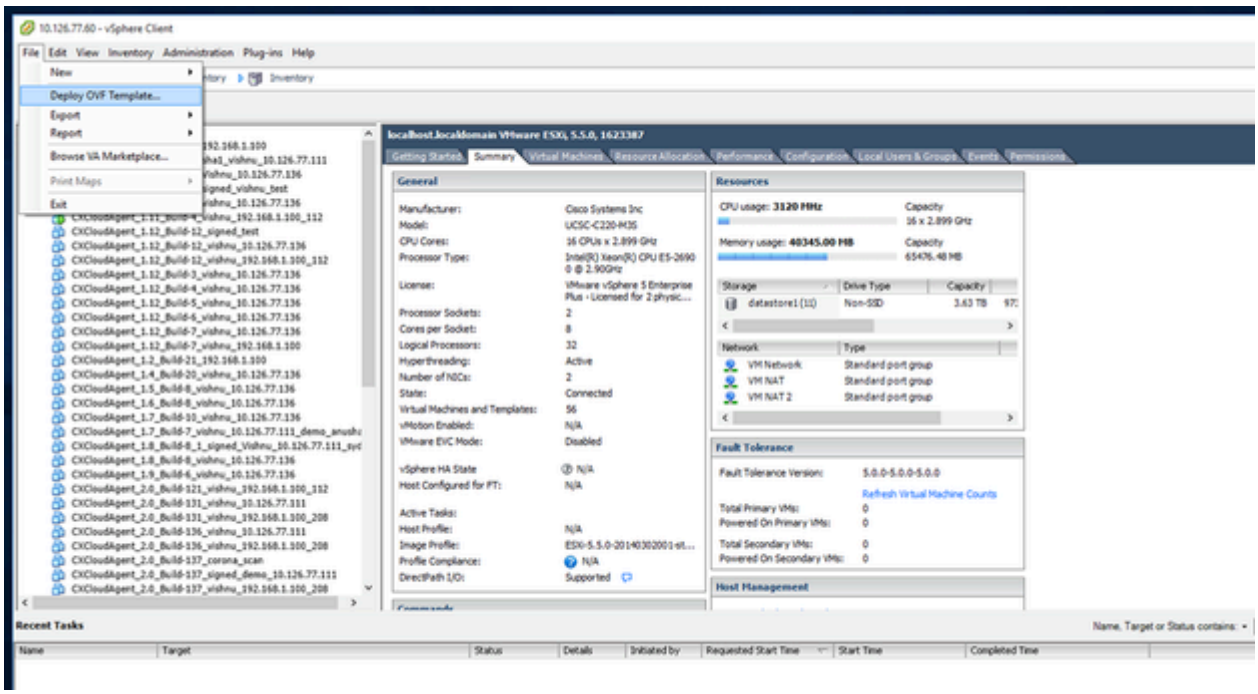
Ce client permet le déploiement de CX Cloud Agent OVA à l'aide du client vSphere épais.

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



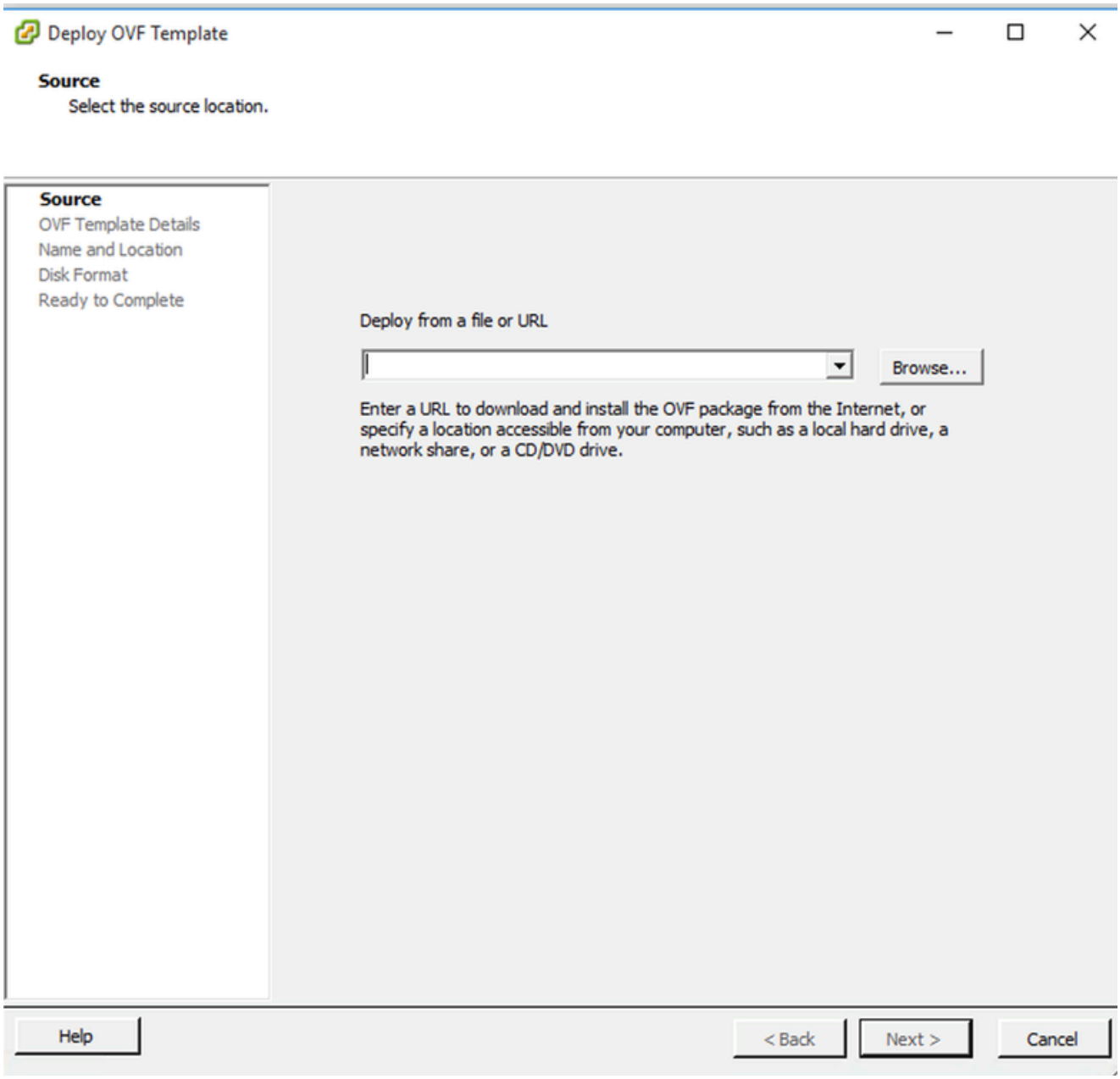
Connexion

2. Naviguez jusqu'à File > Deploy OVF Template.



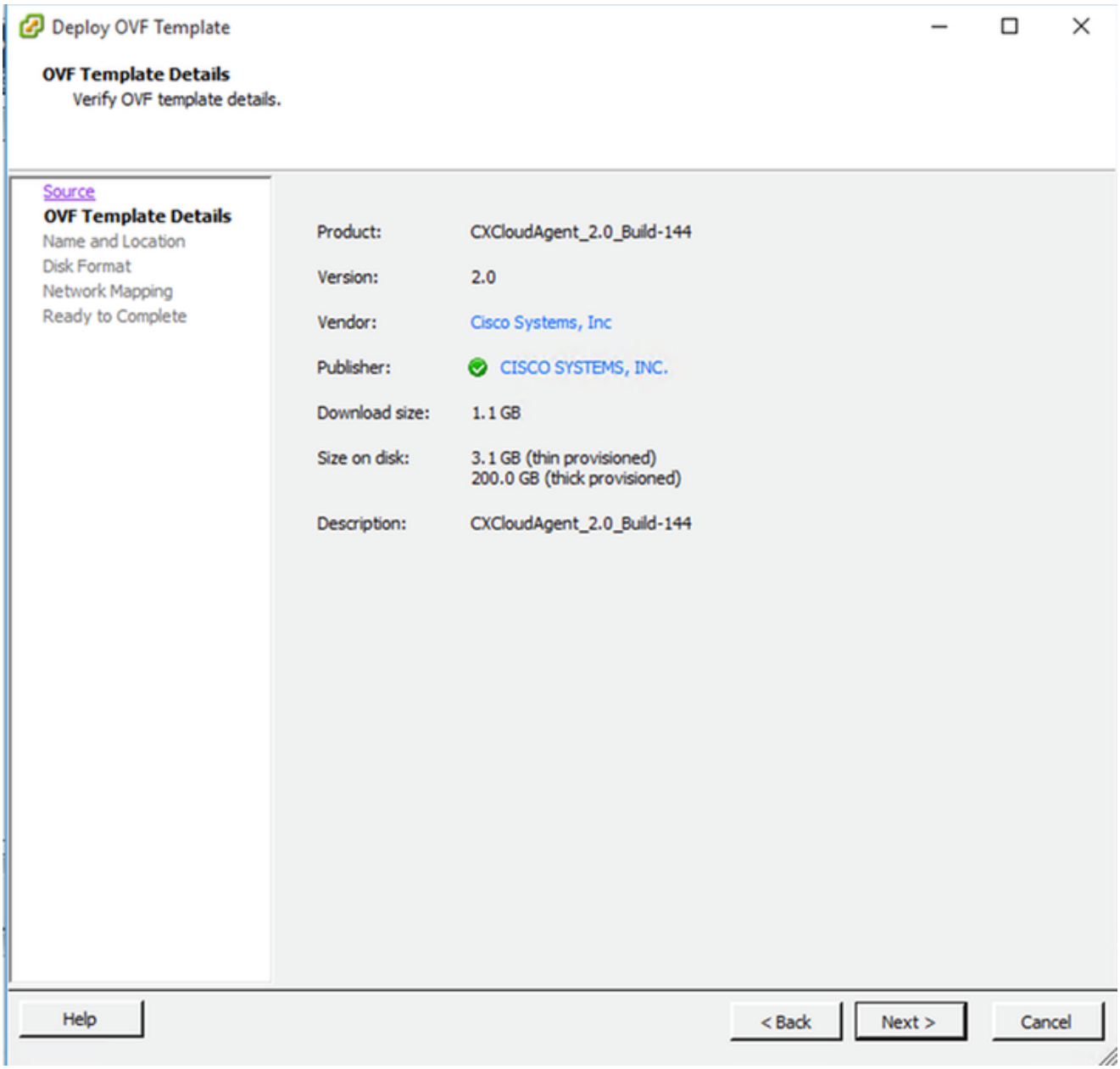
vSphere Client

3. Sélectionnez le fichier OVA, puis cliquez sur Next.



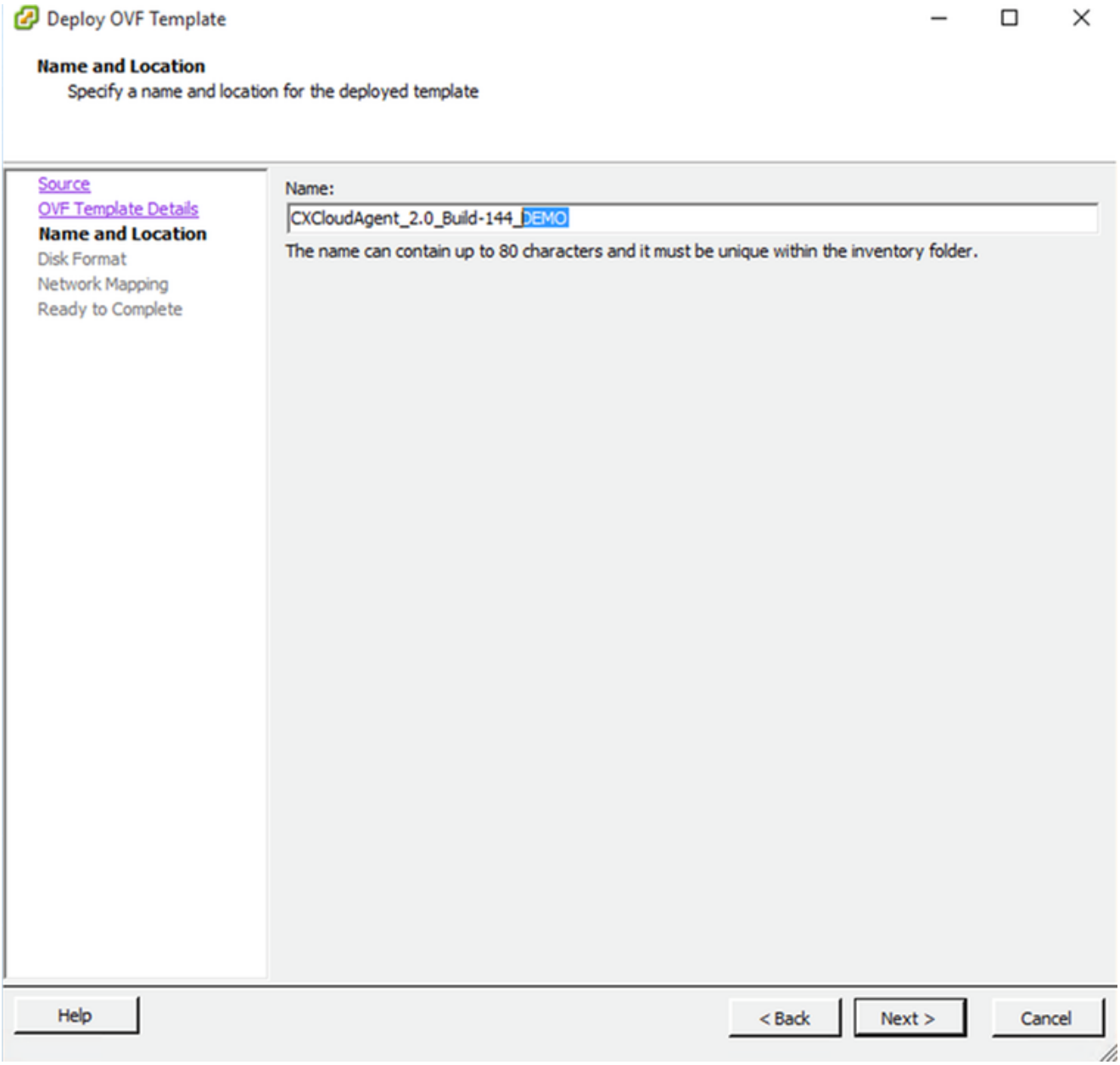
Chemin OVA

4. Vérifiez le OVF Details et cliquez sur Next.



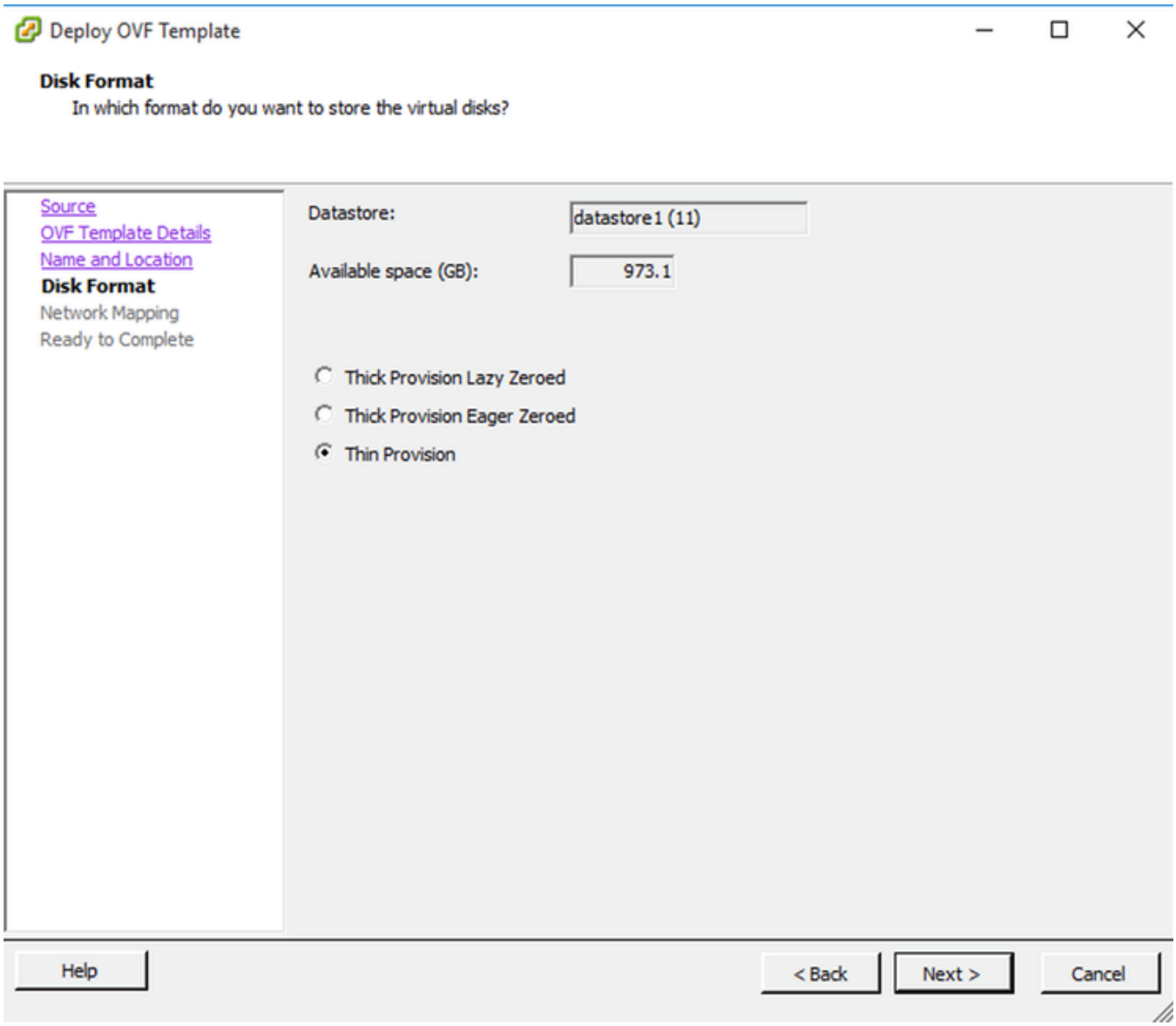
Détails du modèle

5. Saisissez une Unique Name réponse et cliquez sur Next.



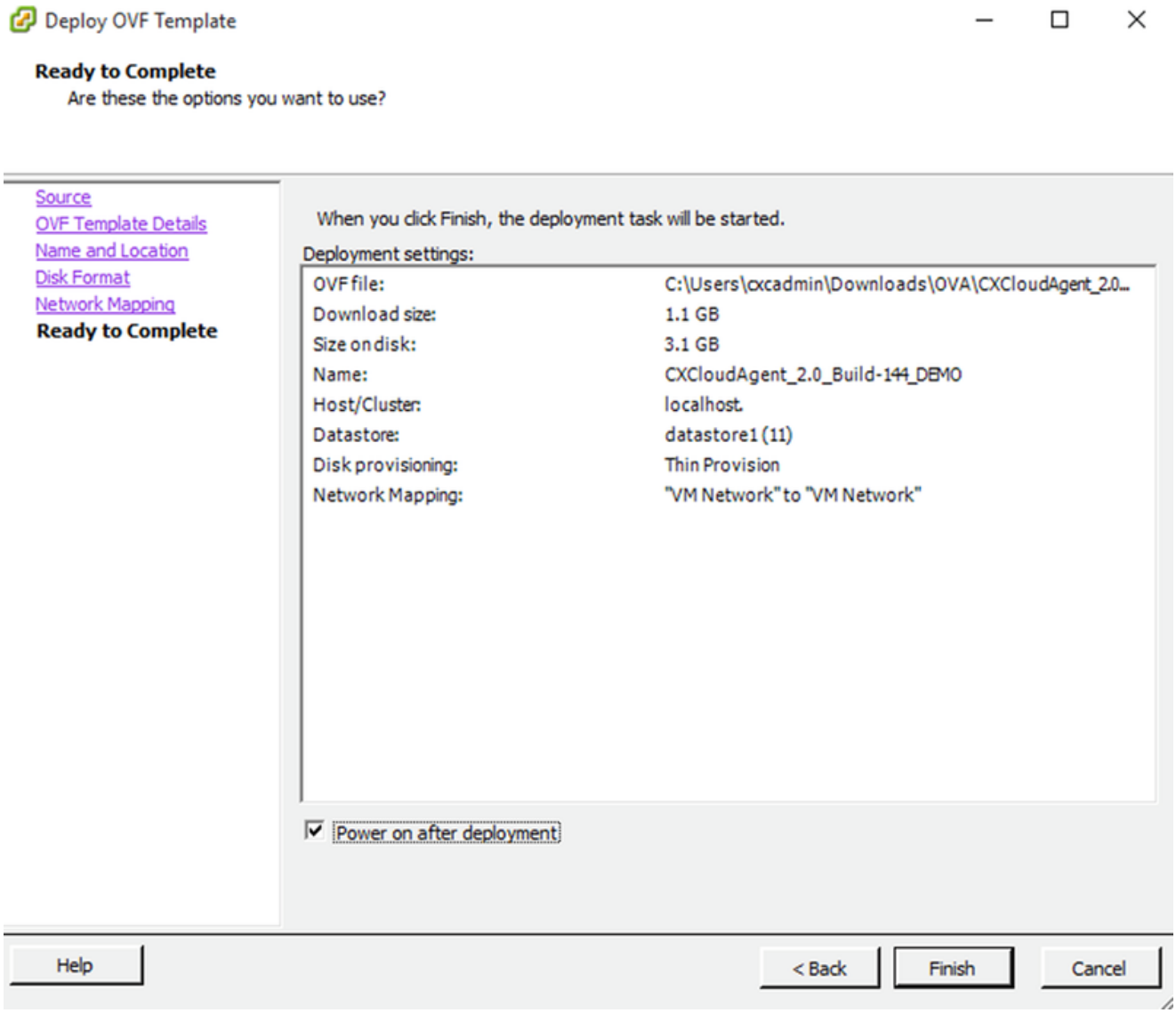
Nom et emplacement

6. Sélectionnez un Disk Format et cliquez sur Next (Thin Provision est recommandé).



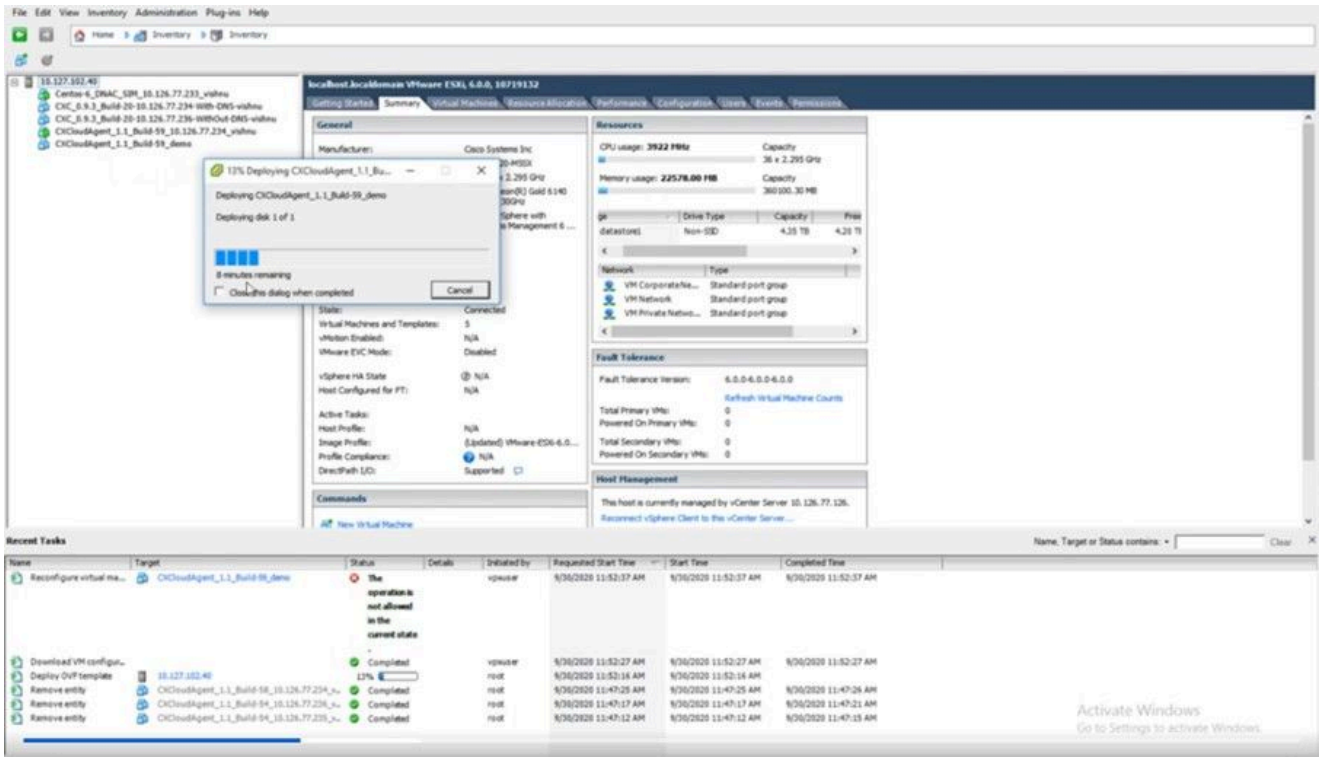
Format de disque

7. Cochez la case, Power on after deployment puis cliquez sur Finish.

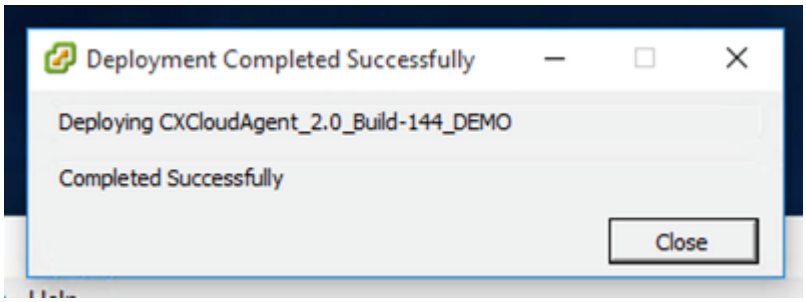


Prêt pour la confirmation

Le déploiement peut prendre plusieurs minutes. Attendez d’obtenir un message de réussite.



Déploiement en cours



Déploiement terminé

8. Sélectionnez la machine virtuelle qui vient d'être déployée, ouvrez la console et accédez à Configuration réseau.

Installation du client Web ESXi 6.0

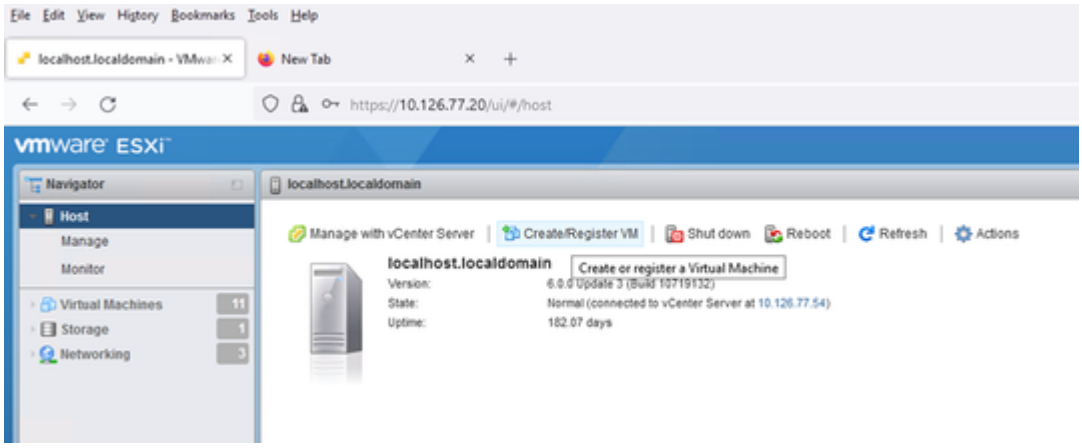
Ce client déploie CX Cloud Agent OVA en utilisant le Web vSphere.

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

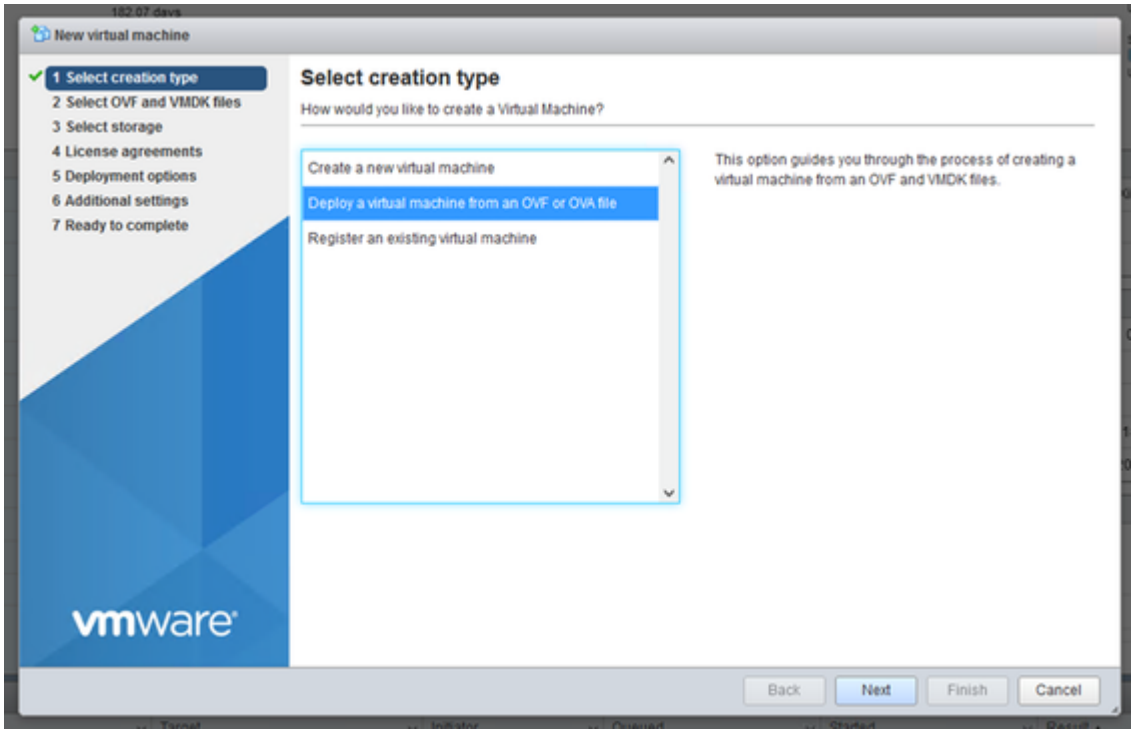


Connexion VMware ESXi

2. Sélectionnez Virtual Machine > Create / Register VM.

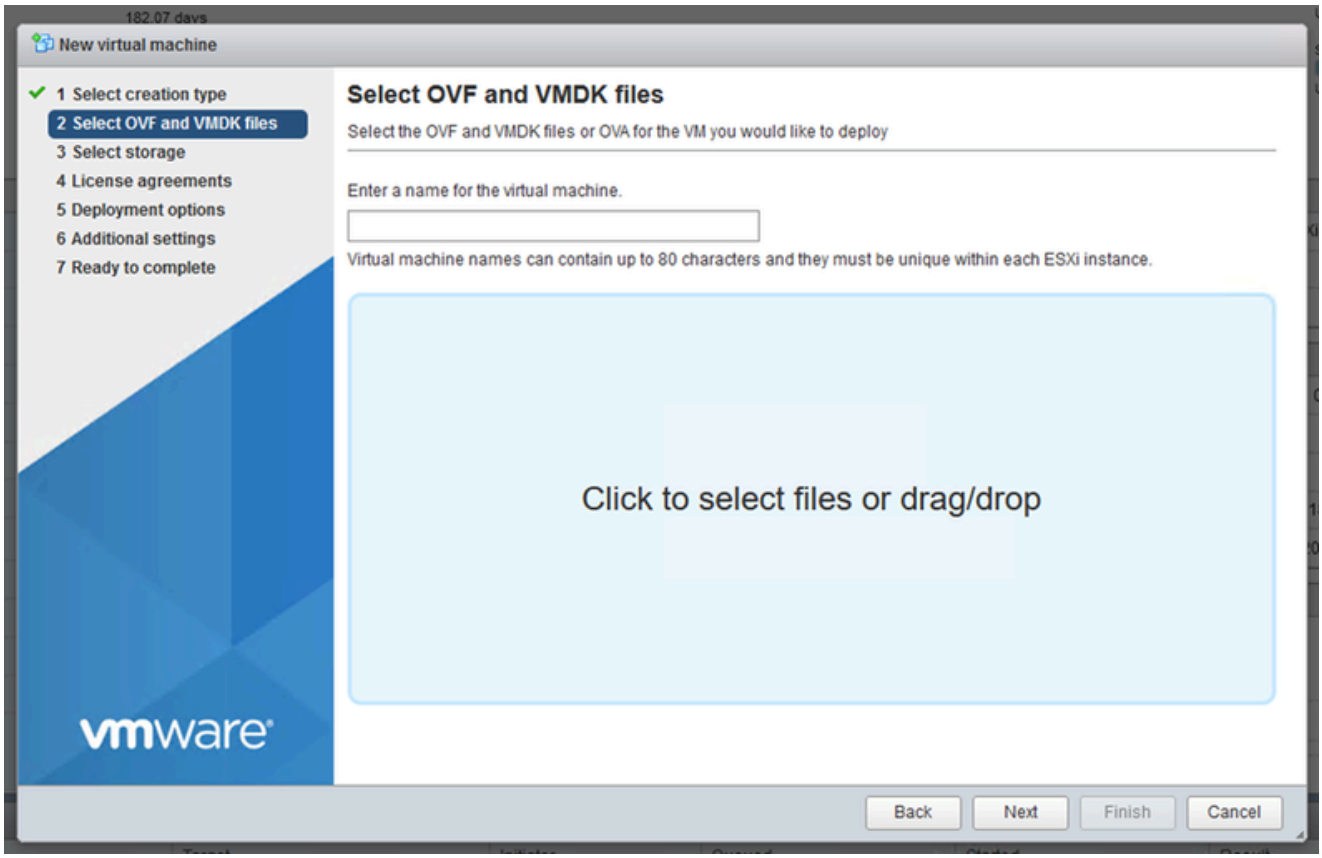


Créer une machine virtuelle



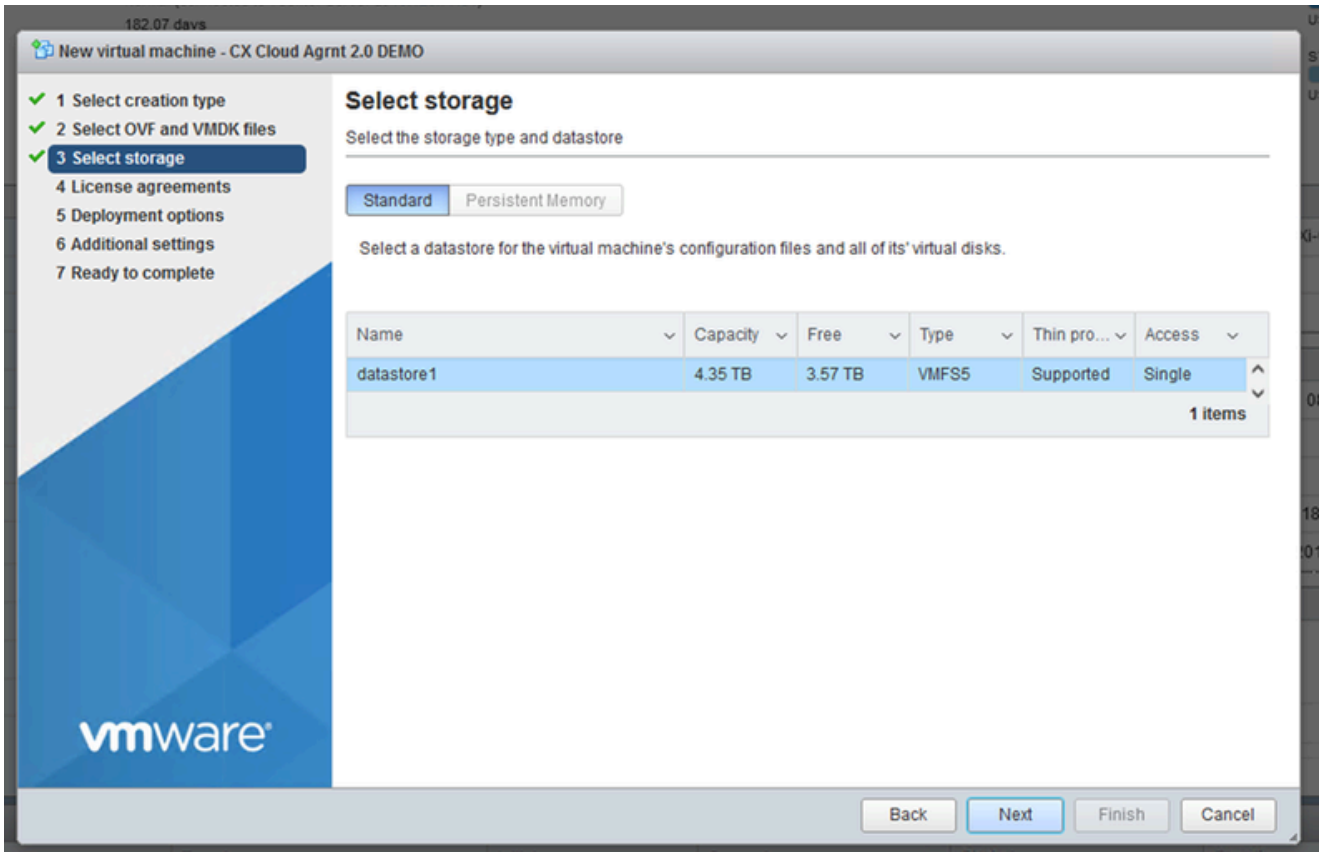
Déploiement OVA

3. Sélectionnez Deploy a virtual machine from an OVF or OVA file et cliquez sur Next.
4. Saisissez le nom de la machine virtuelle, recherchez le fichier ou faites glisser le fichier OVA téléchargé.
5. Cliquez sur Next.

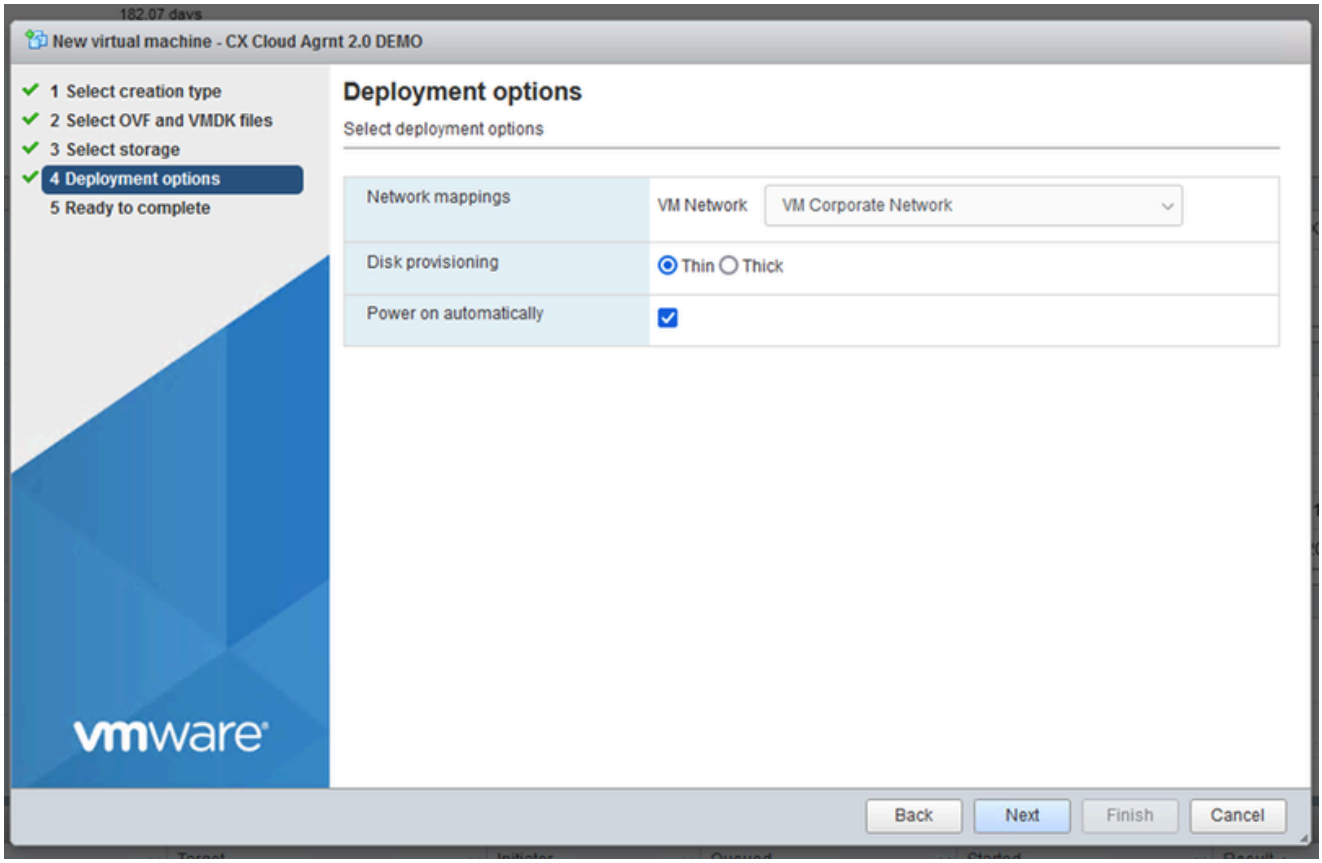


Sélection OVA

6. Sélectionnez Standard Storage et cliquez sur Next.

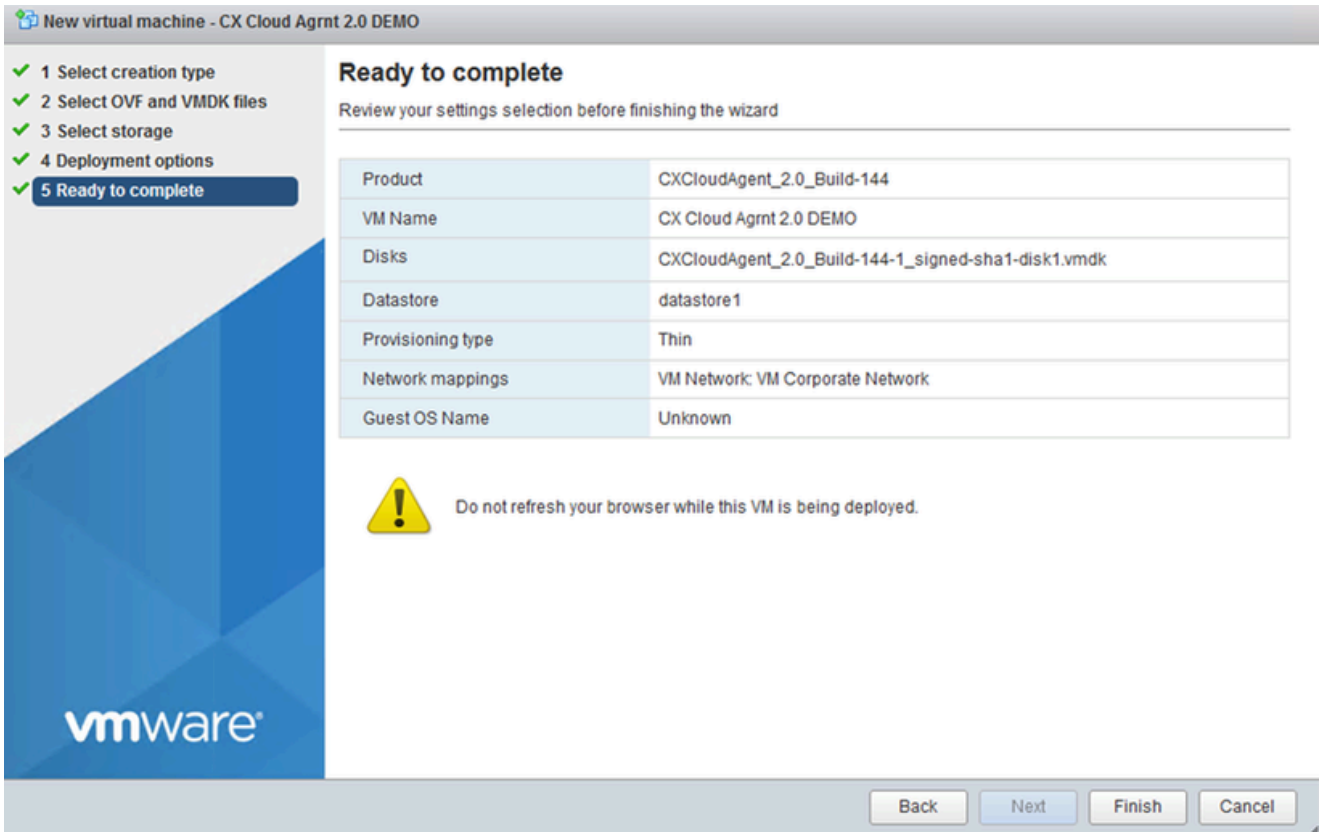


Sélectionner le stockage

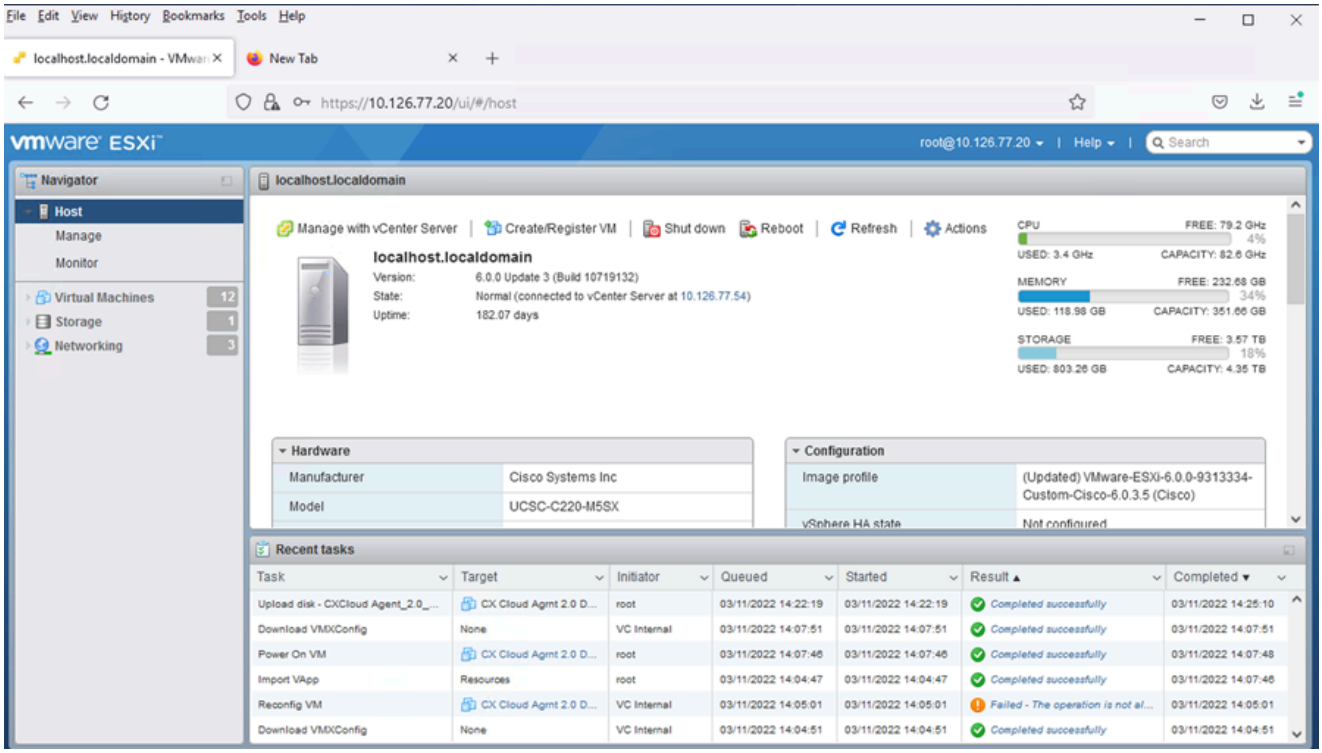


Options de déploiement

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

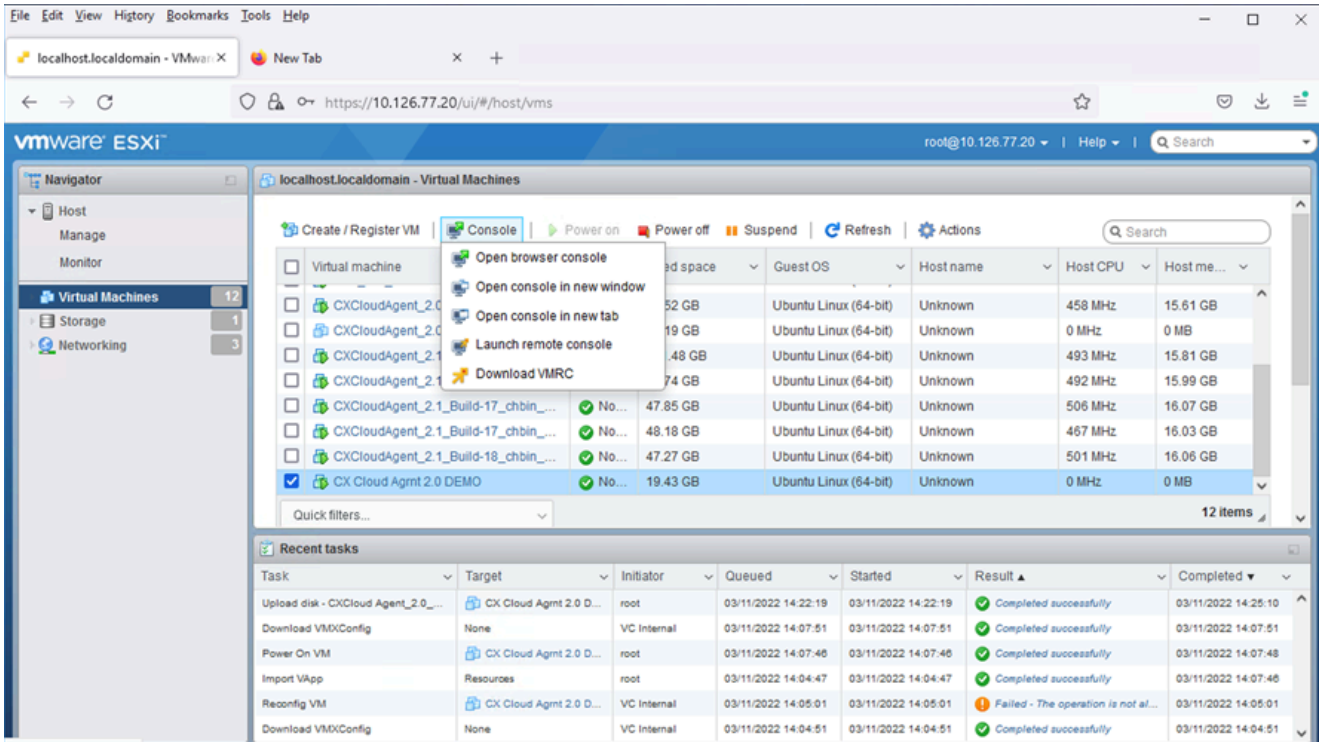


Prêt pour la confirmation



Confirmation réussie

8. Vérifiez les paramètres et cliquez sur Finish.
9. Sélectionnez la machine virtuelle qui vient d'être déployée, puis Console > Open browser console.



Ouvrir la console

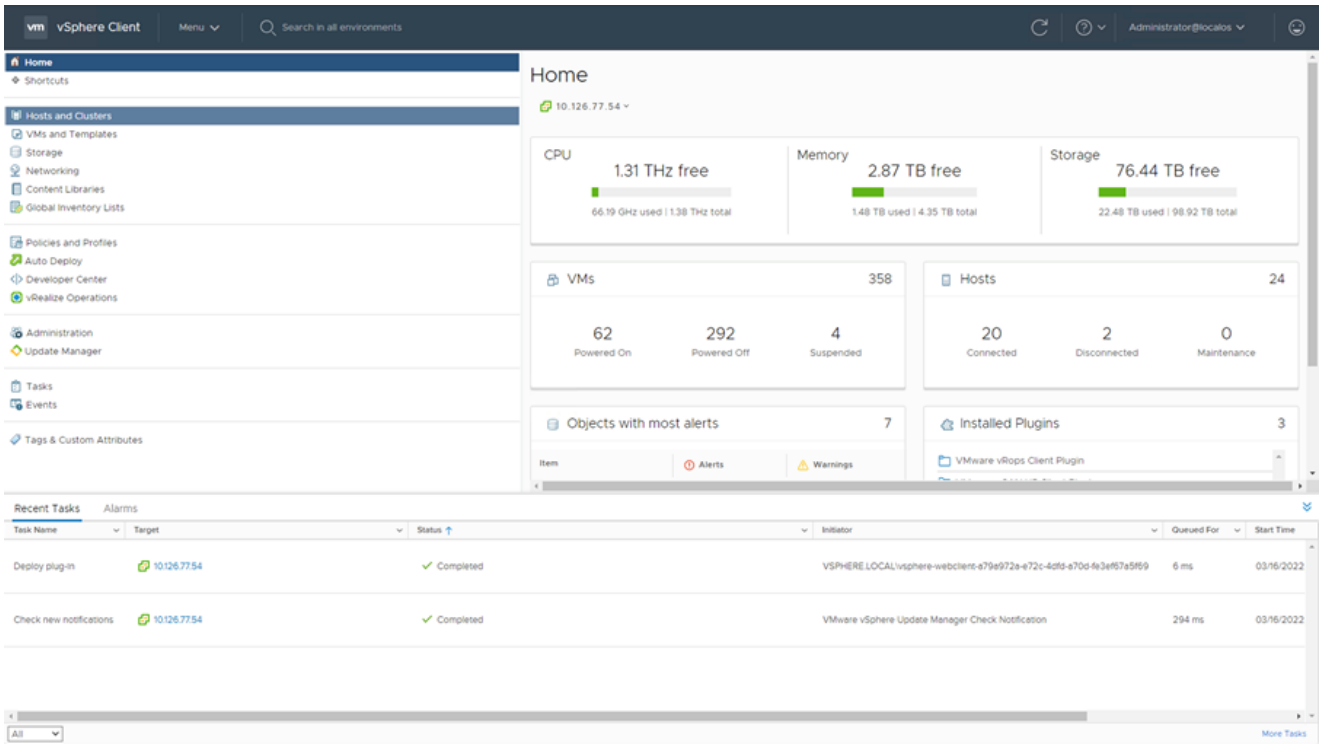
10. Naviguez vers Import Appliance.

Installation de client Web vCenter

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

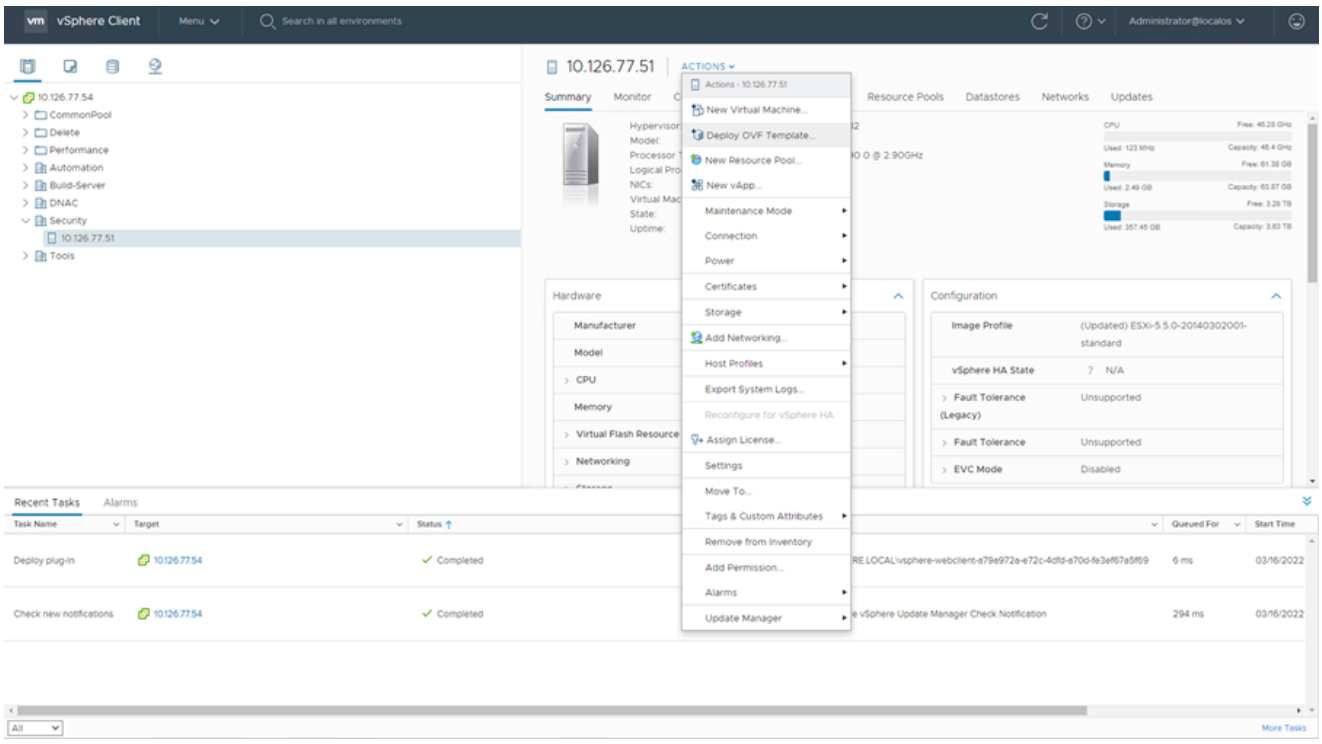


Connexion

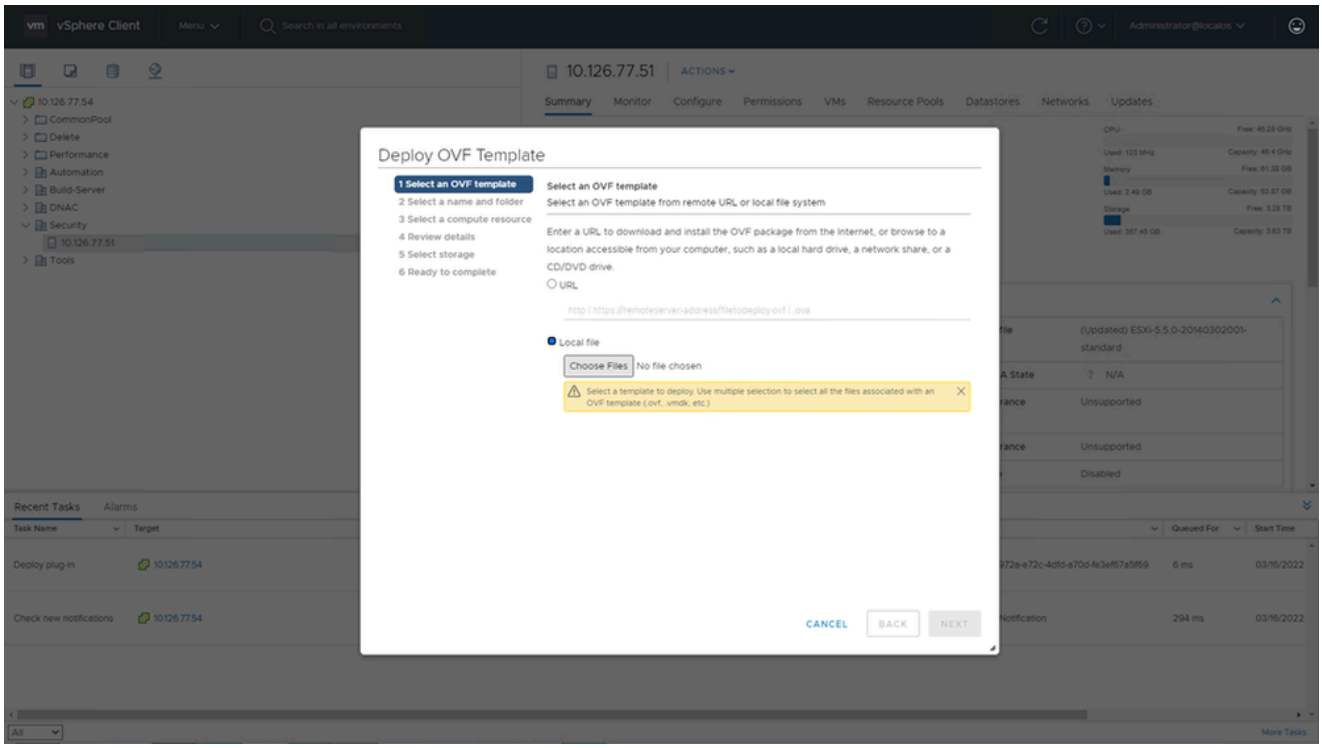


Écran d’accueil

2. Sur la page d'accueil, cliquez sur Hosts and Clusters.
3. Sélectionnez la machine virtuelle et cliquez sur Action > Deploy OVF Template.

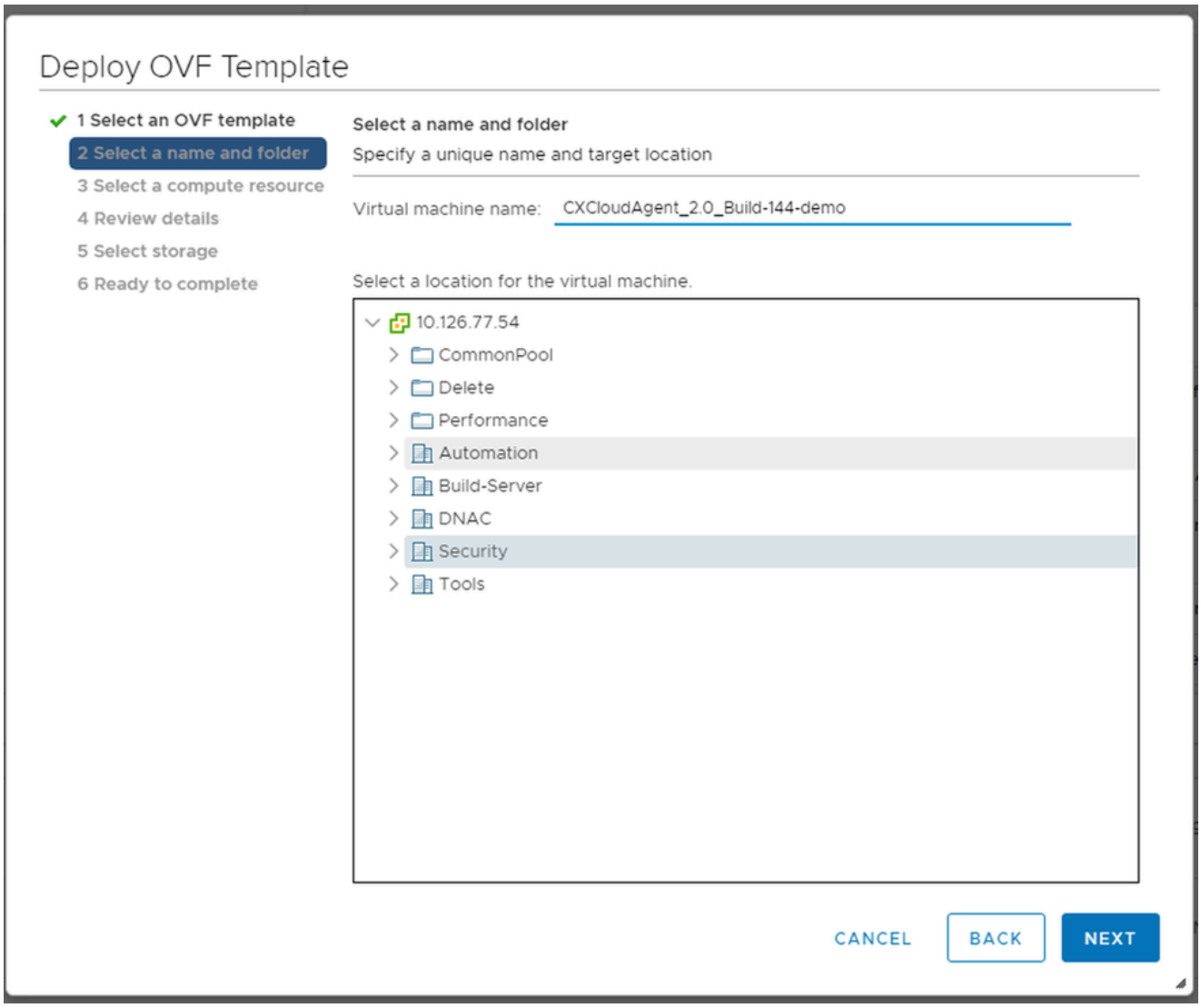


Actions



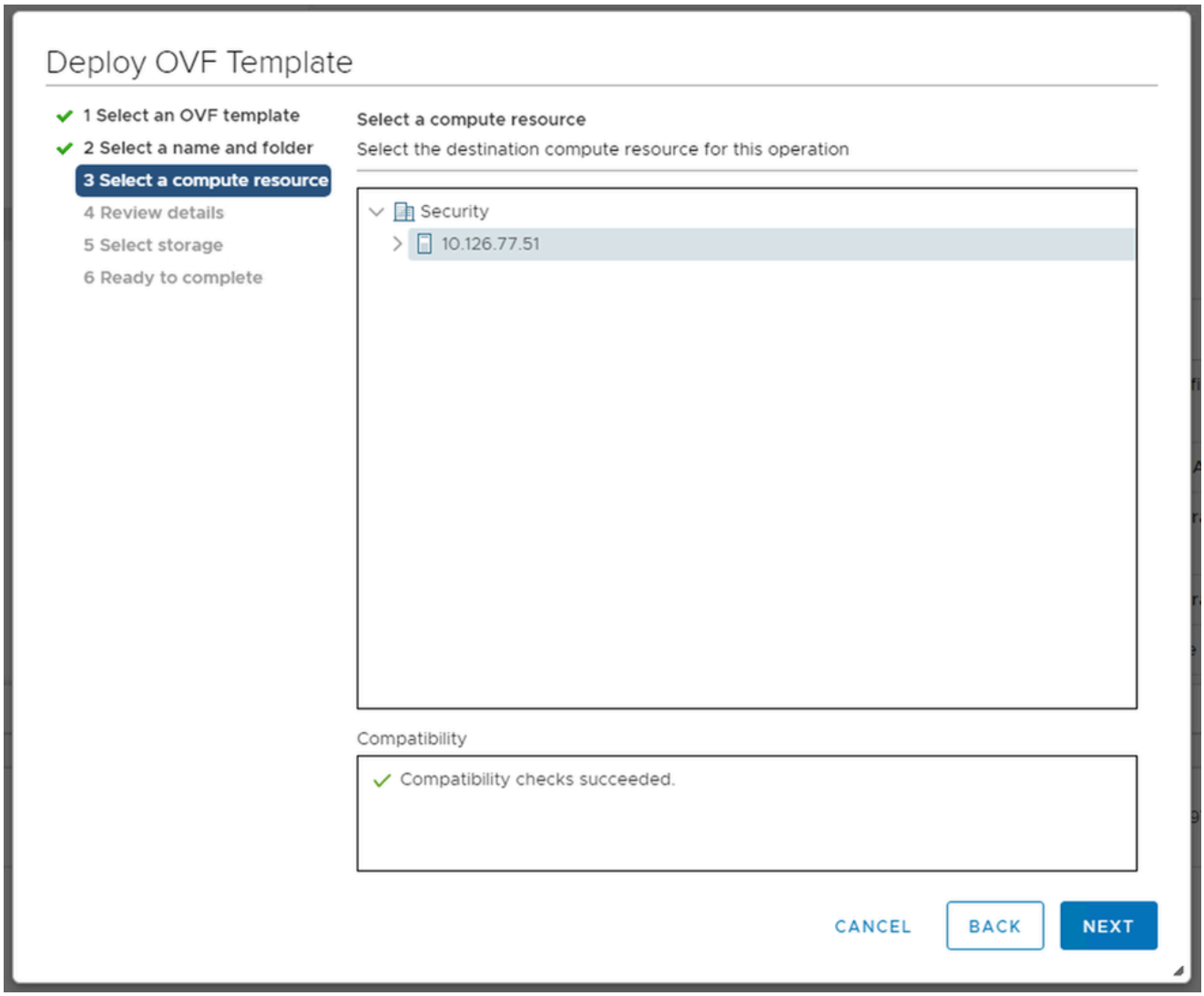
Sélectionner le modèle

4. Ajoutez l'URL directement ou recherchez le fichier OVA et cliquez sur Next.
5. Entrez un nom unique et accédez à l'emplacement si nécessaire .
6. Cliquez sur Next.



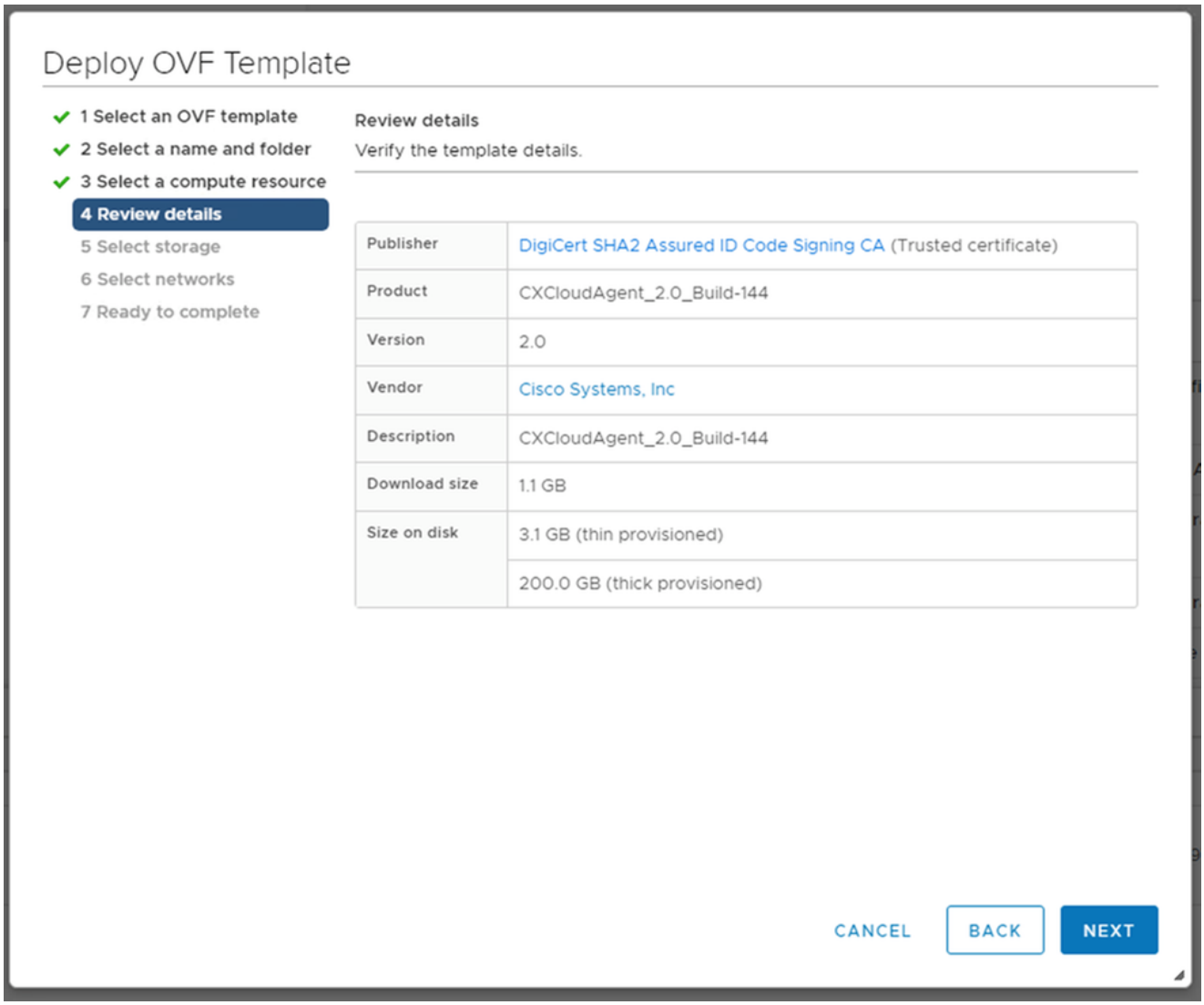
Nom et dossier

7. Sélectionnez une ressource de calcul et cliquez sur Next.



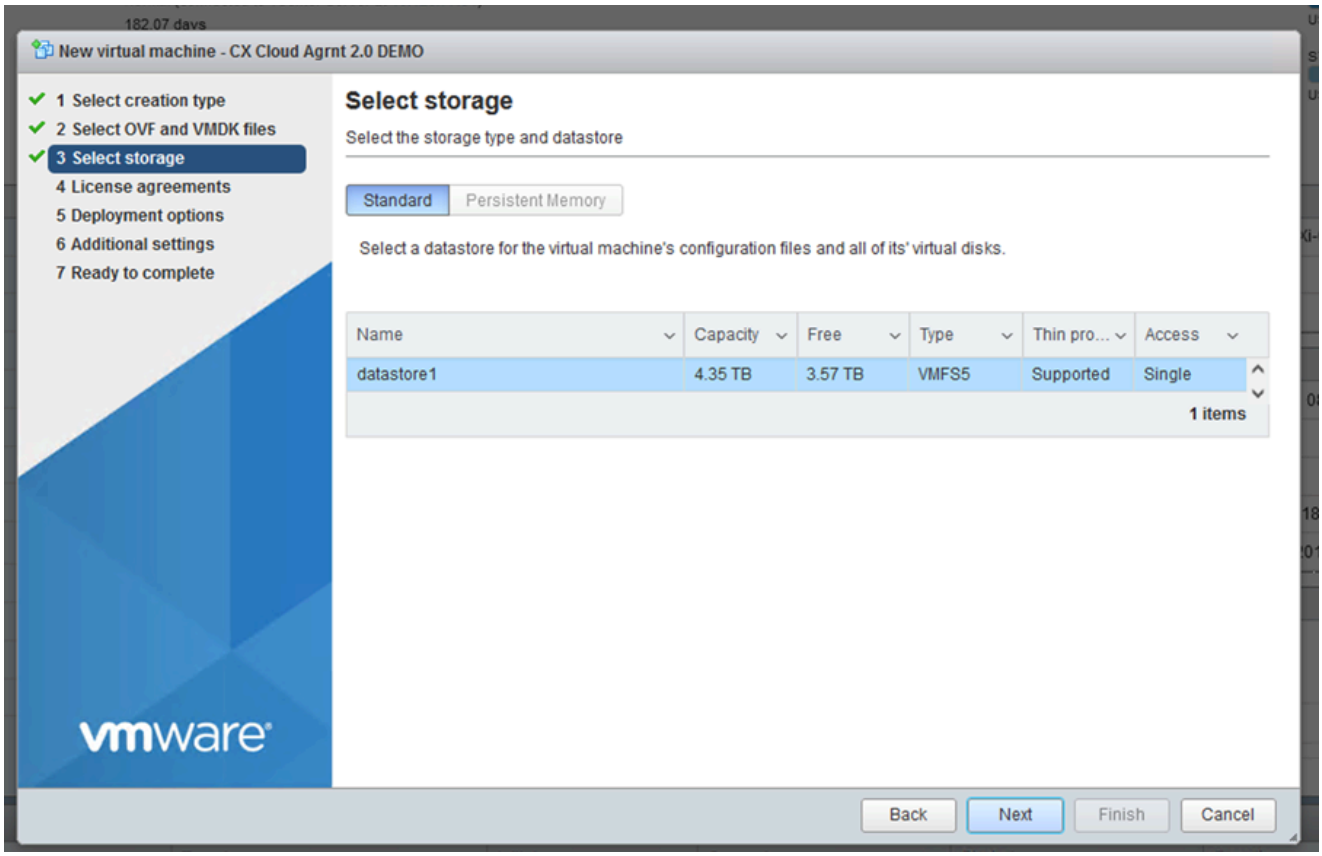
Sélectionner une ressource de calcul

8. Vérifiez les détails et cliquez sur Next.



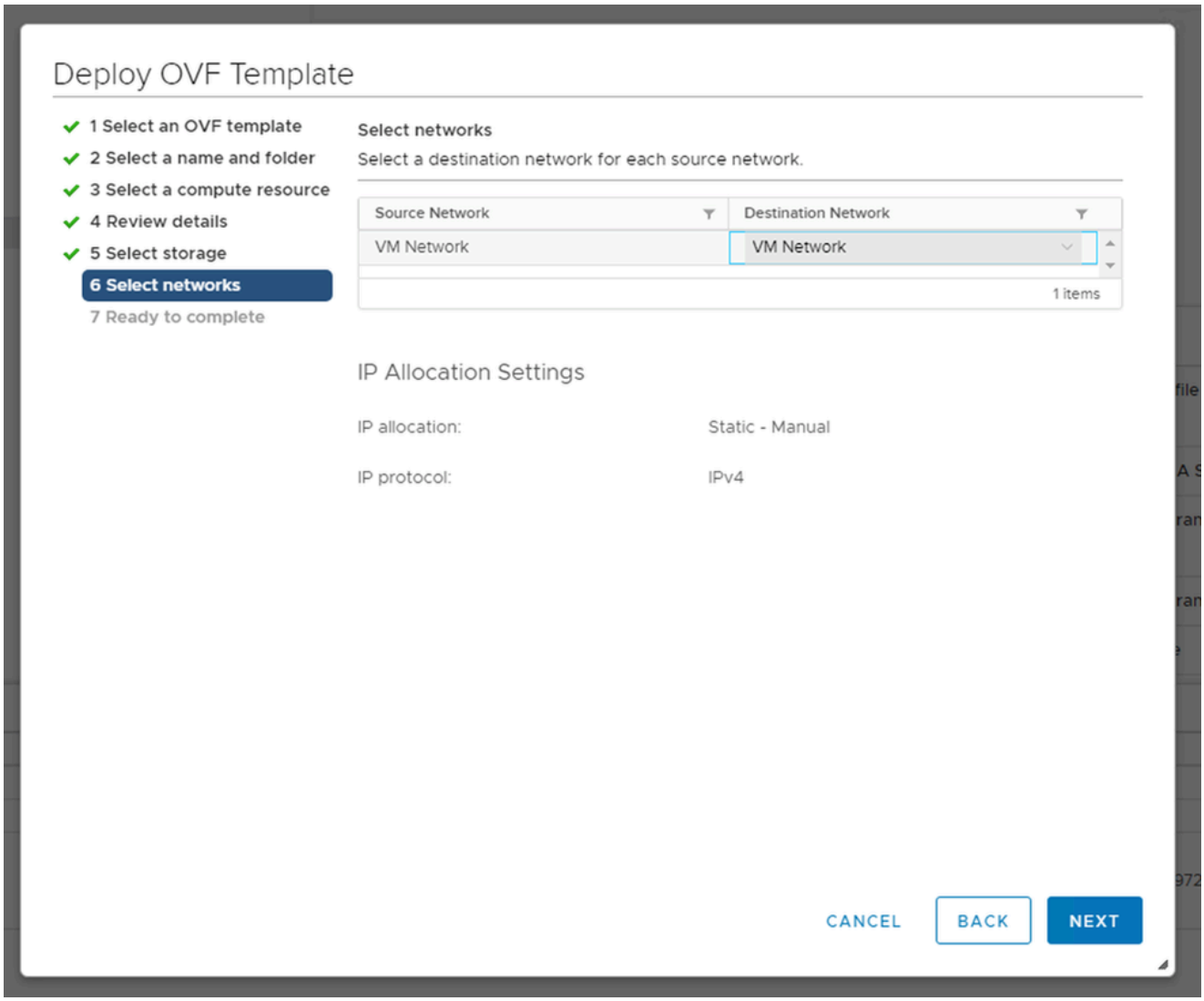
Examiner les détails

9. Sélectionnez le format du disque virtuel et cliquez sur Next.



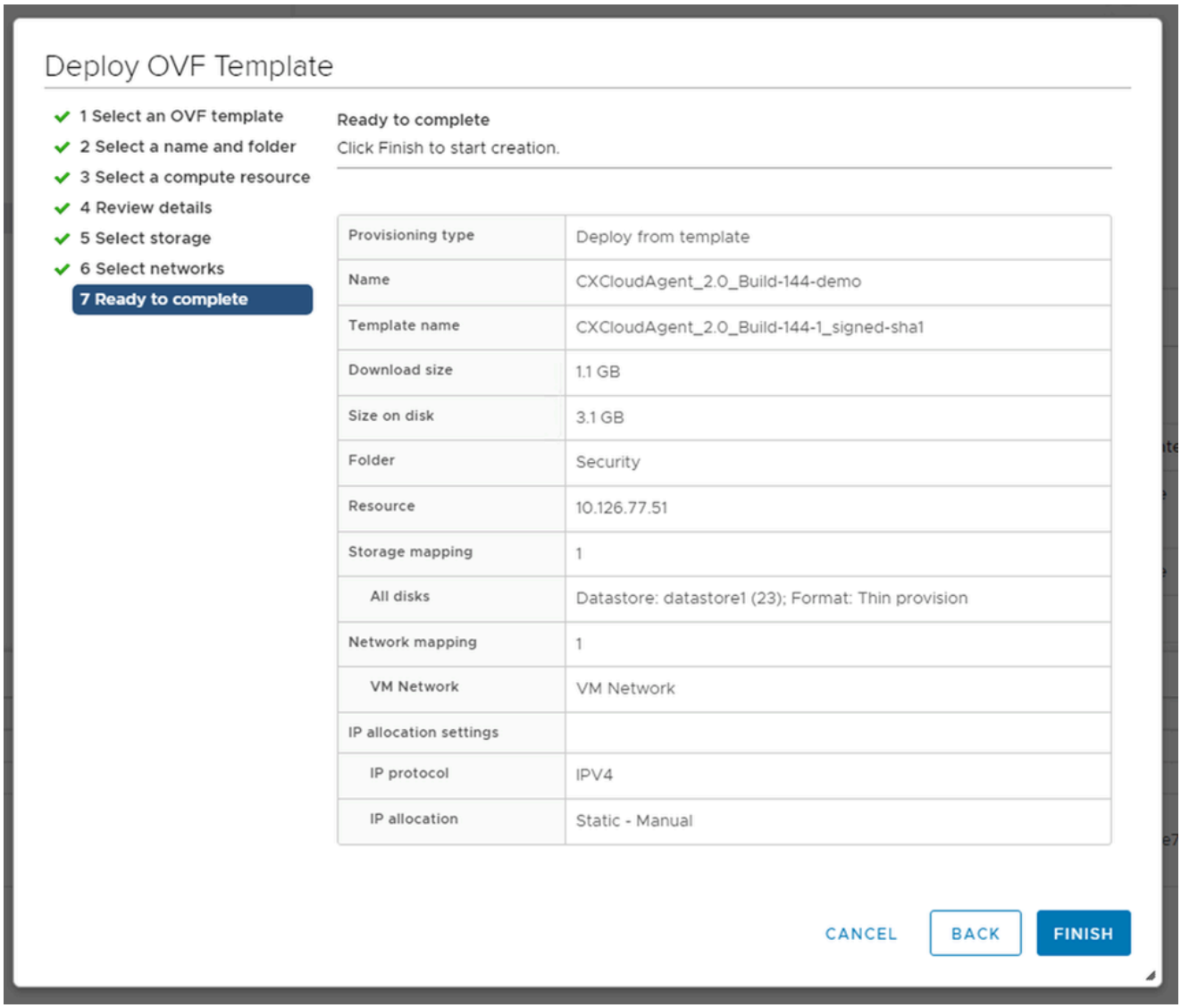
Sélectionner le stockage

10. Cliquez sur Next.



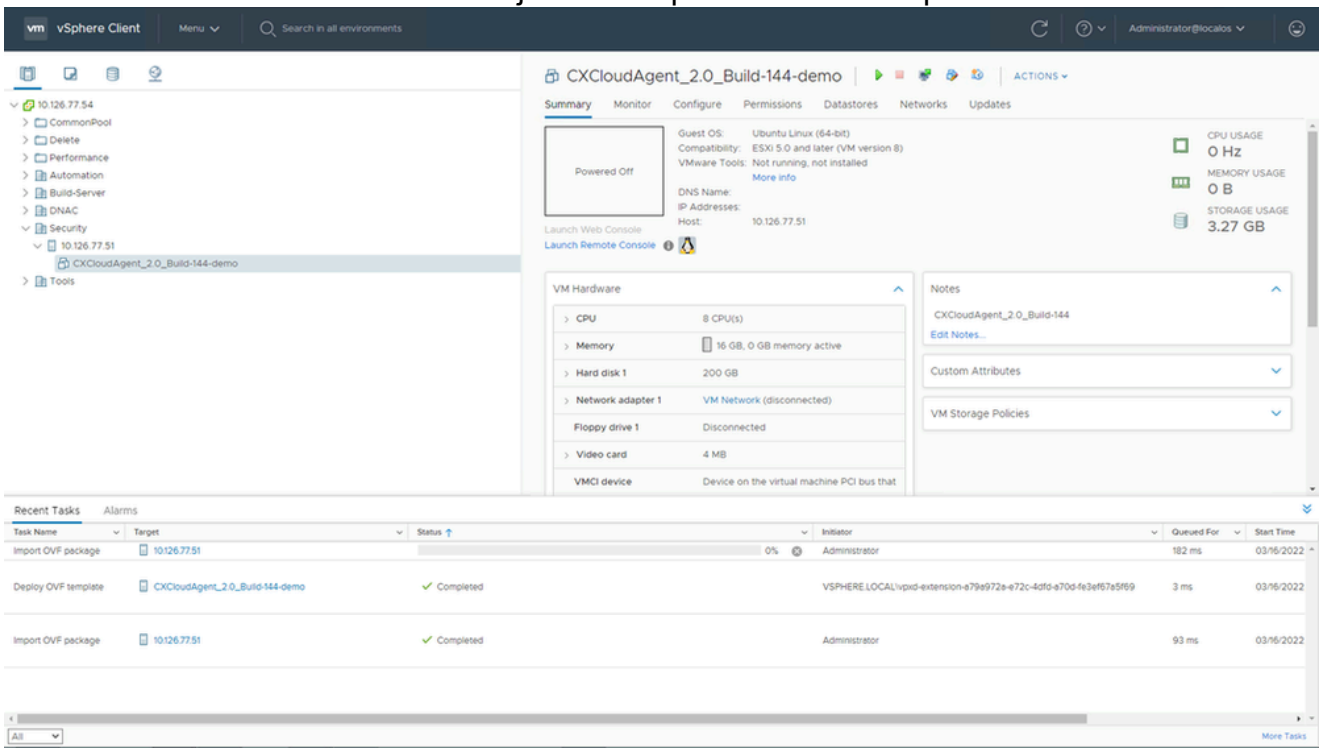
Sélectionner les réseaux

11. Cliquez sur Finish.



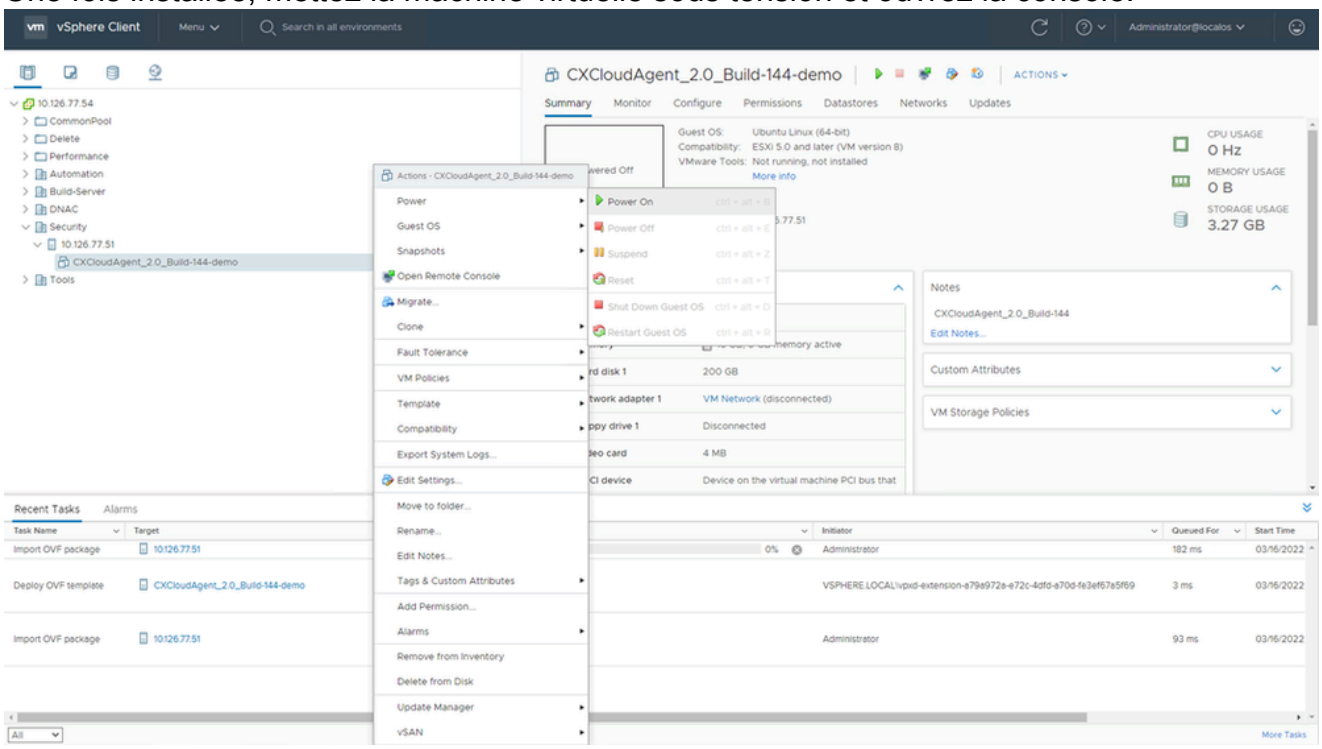
Prêt pour la confirmation

12. Une nouvelle machine virtuelle est ajoutée. Cliquez sur son nom pour afficher l'état.



VM ajoutée

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



Ouvrir la console

14. Naviguez vers Import Appliance.

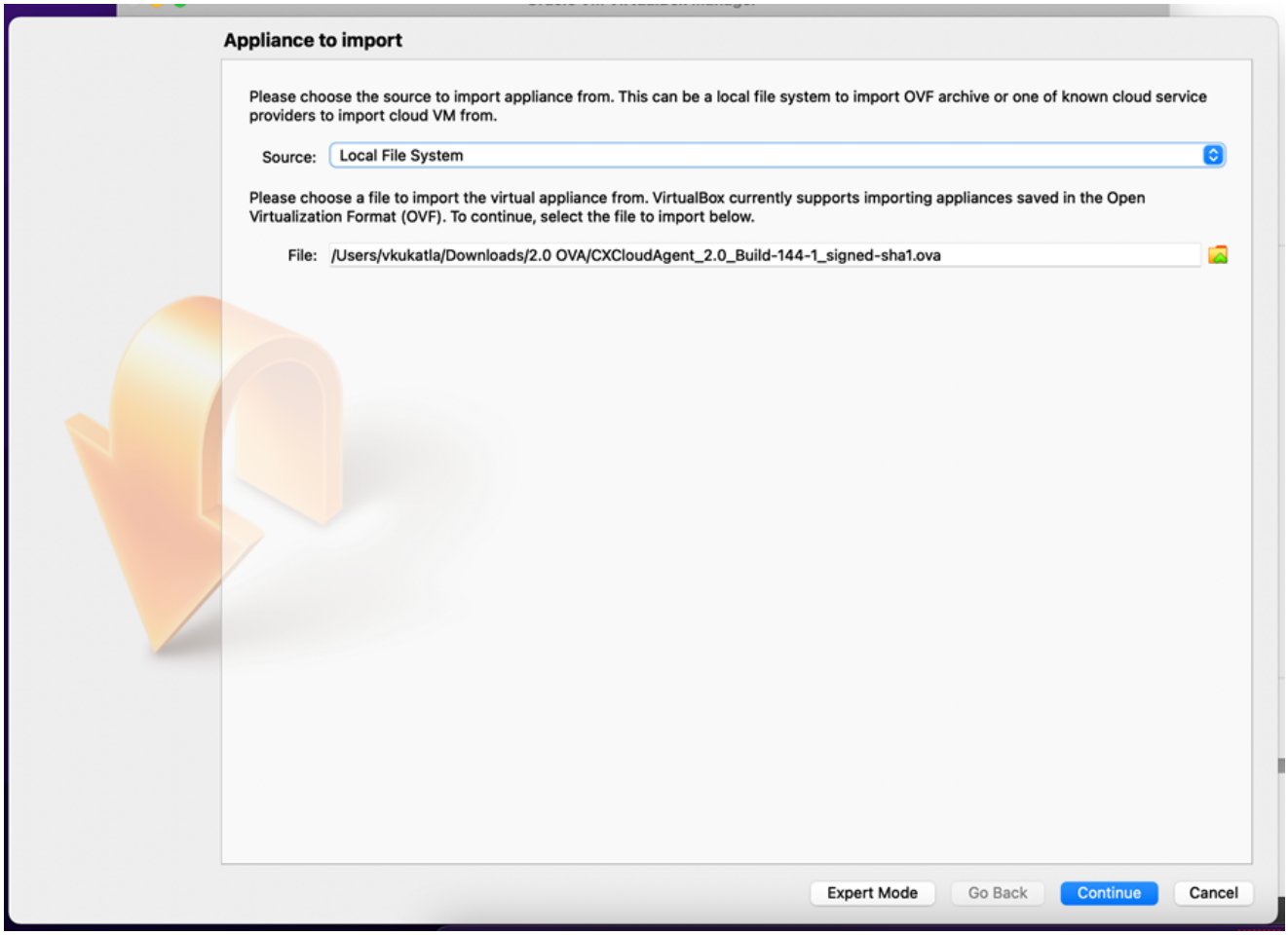
Installation d'Oracle Virtual Box 5.2.30

Ce client déploie CX Cloud Agent OVA via Oracle Virtual Box.



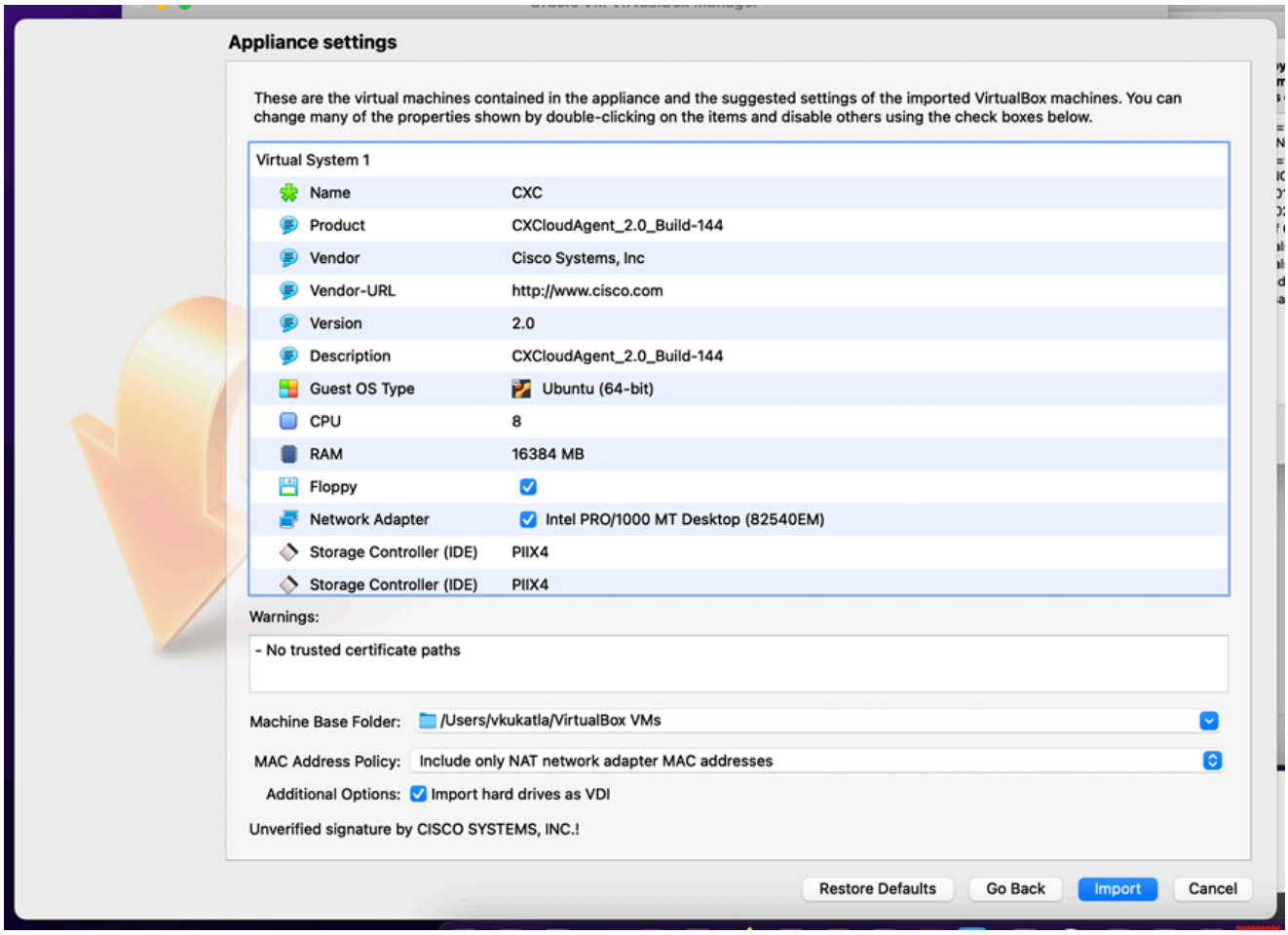
Machine virtuelle Oracle

1. Ouvrez l'interface utilisateur d'Oracle VM et sélectionnez File > Import Appliance.
2. Naviguez pour importer le fichier OVA.



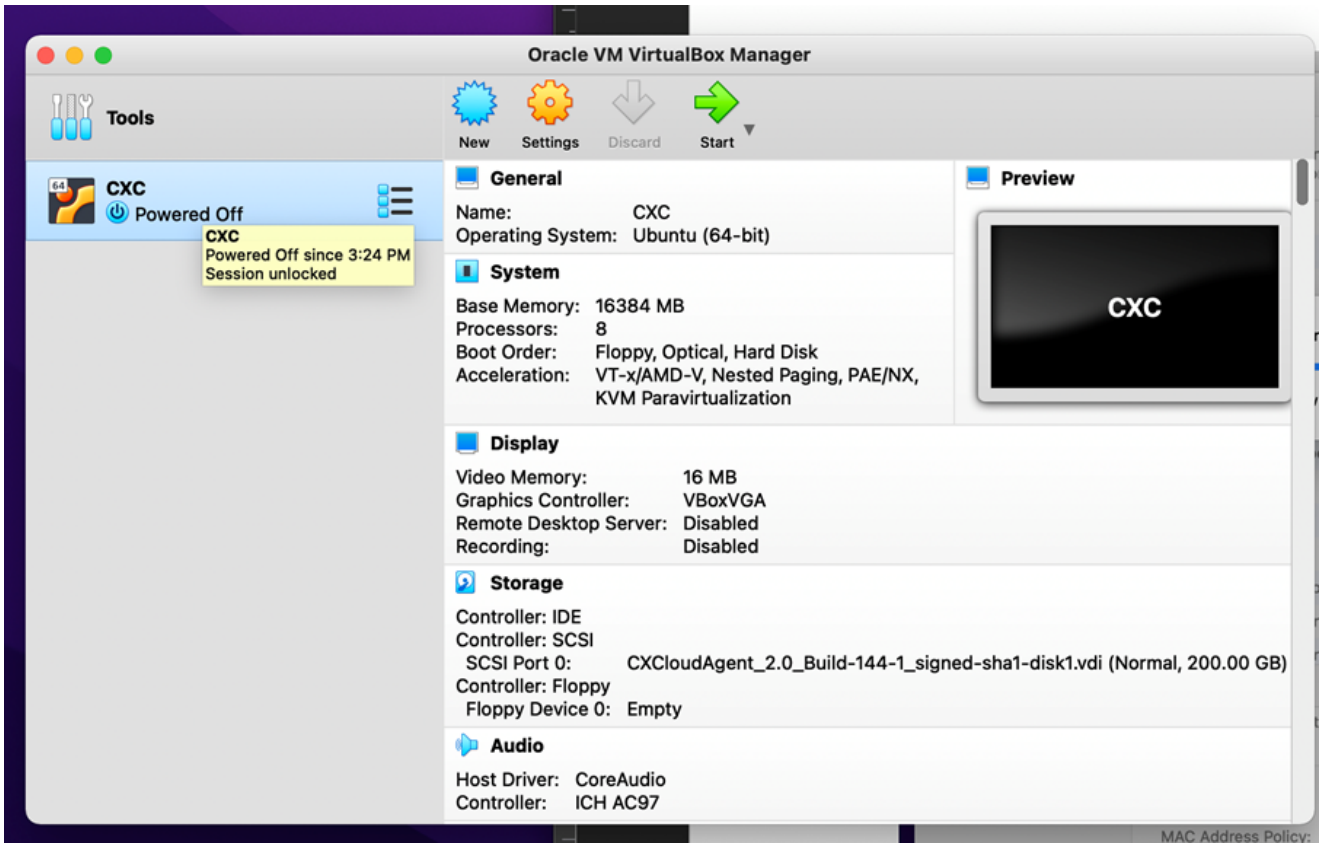
Sélectionner le fichier

3. Cliquez sur Import.

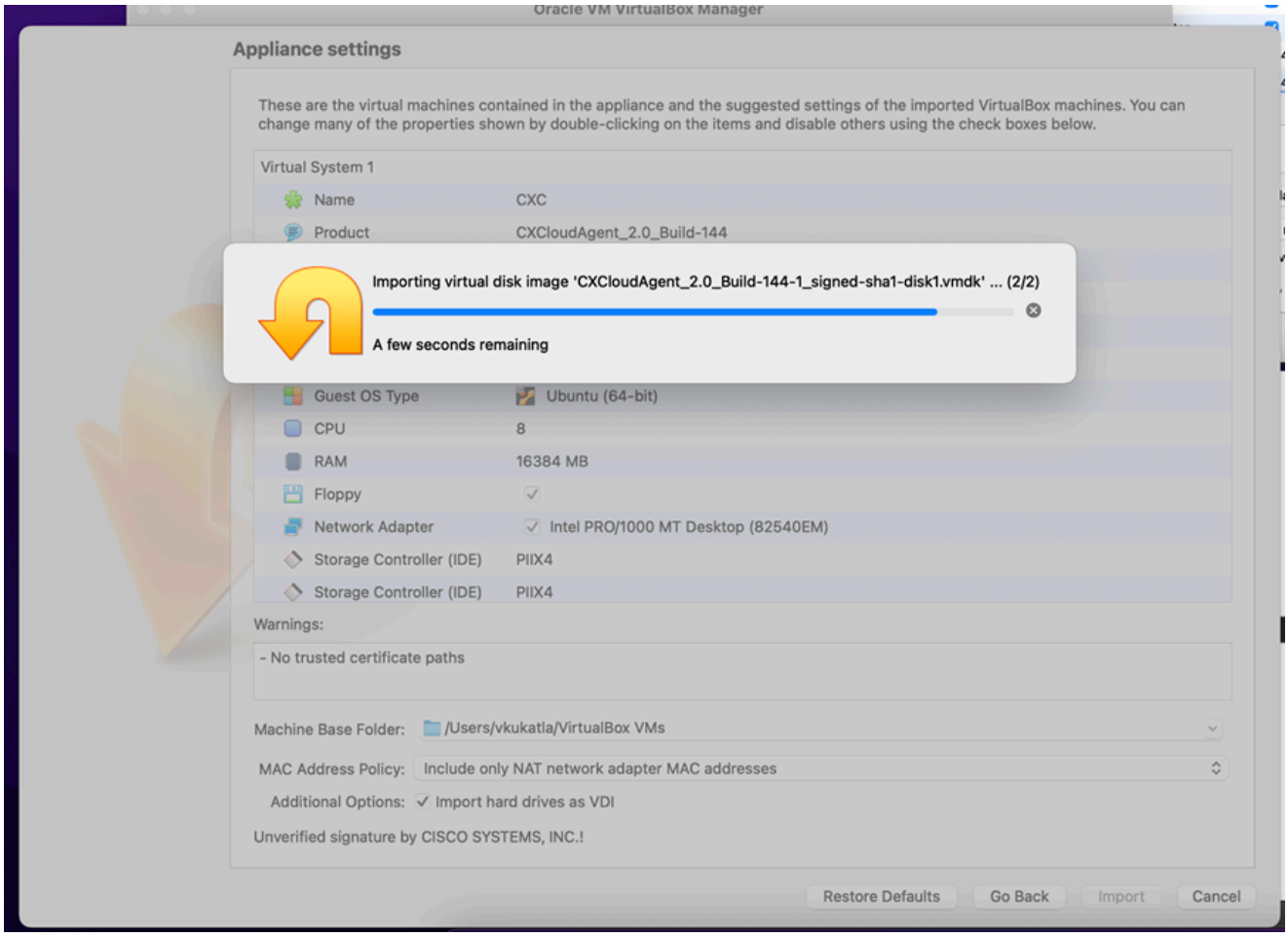


Fichier d'importation

4. Sélectionnez la VM que vous venez de déployer et cliquez sur Start.

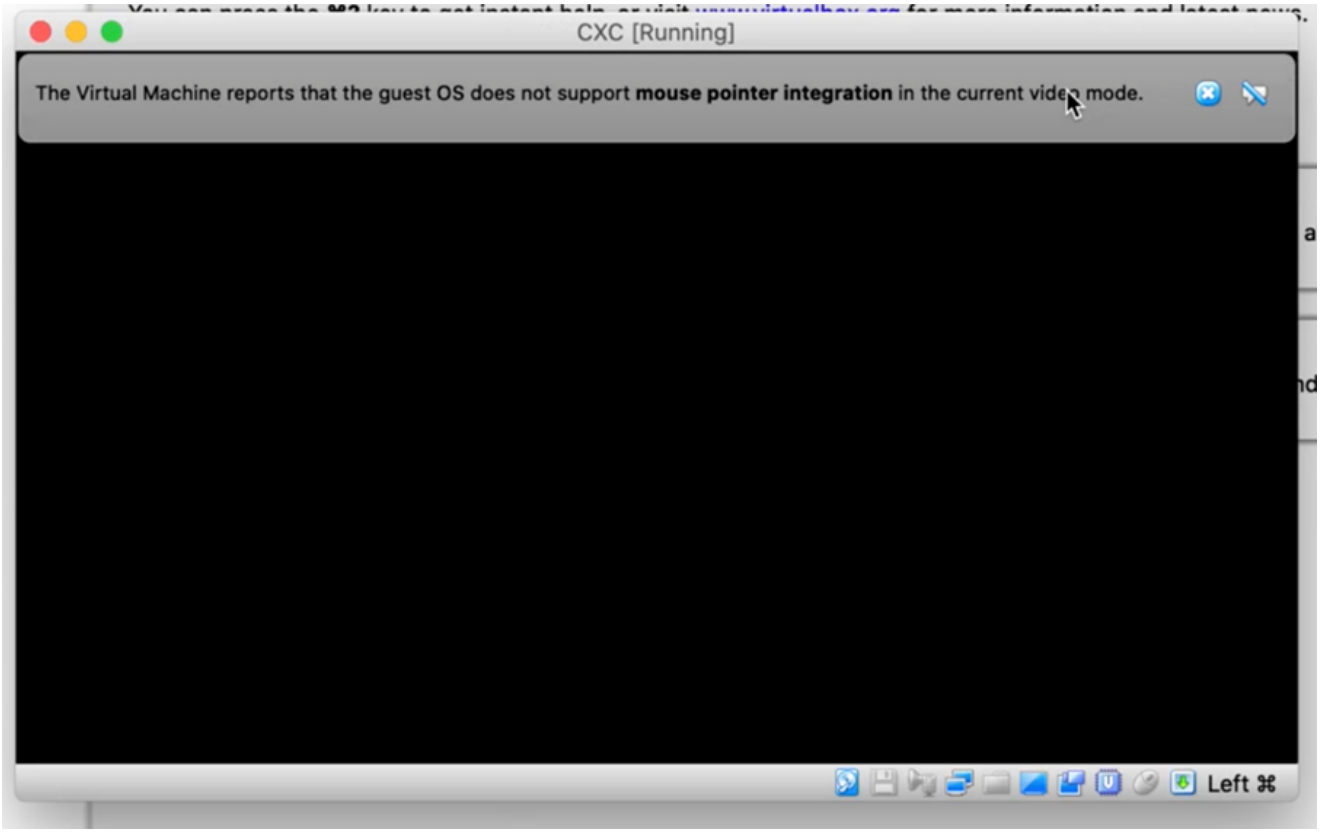


Démarrage de la console de machine virtuelle



Importation en cours

5. Mettez la machine virtuelle sous tension. La console affiche .

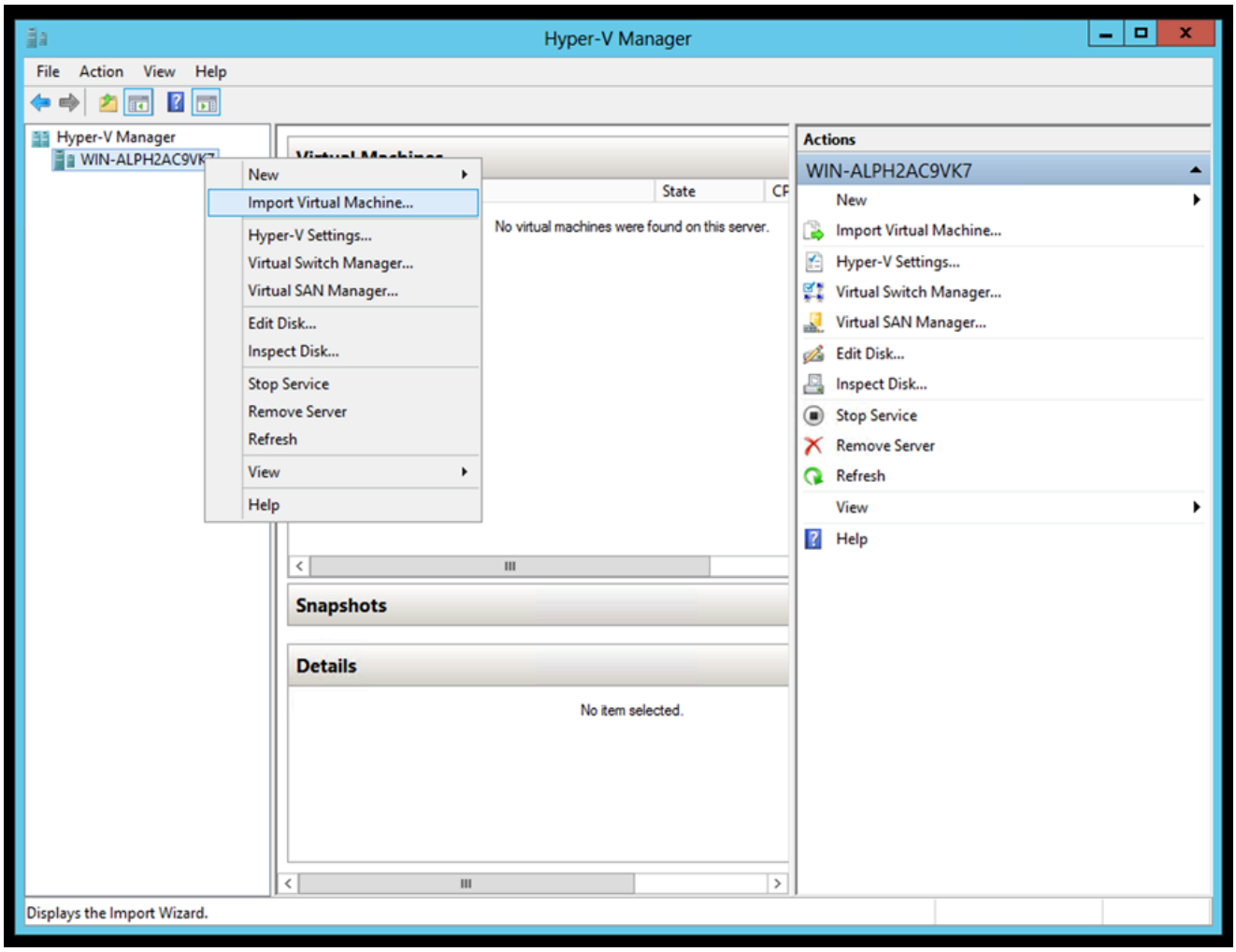


Ouvrir la console

6. Naviguez vers Import Appliance.

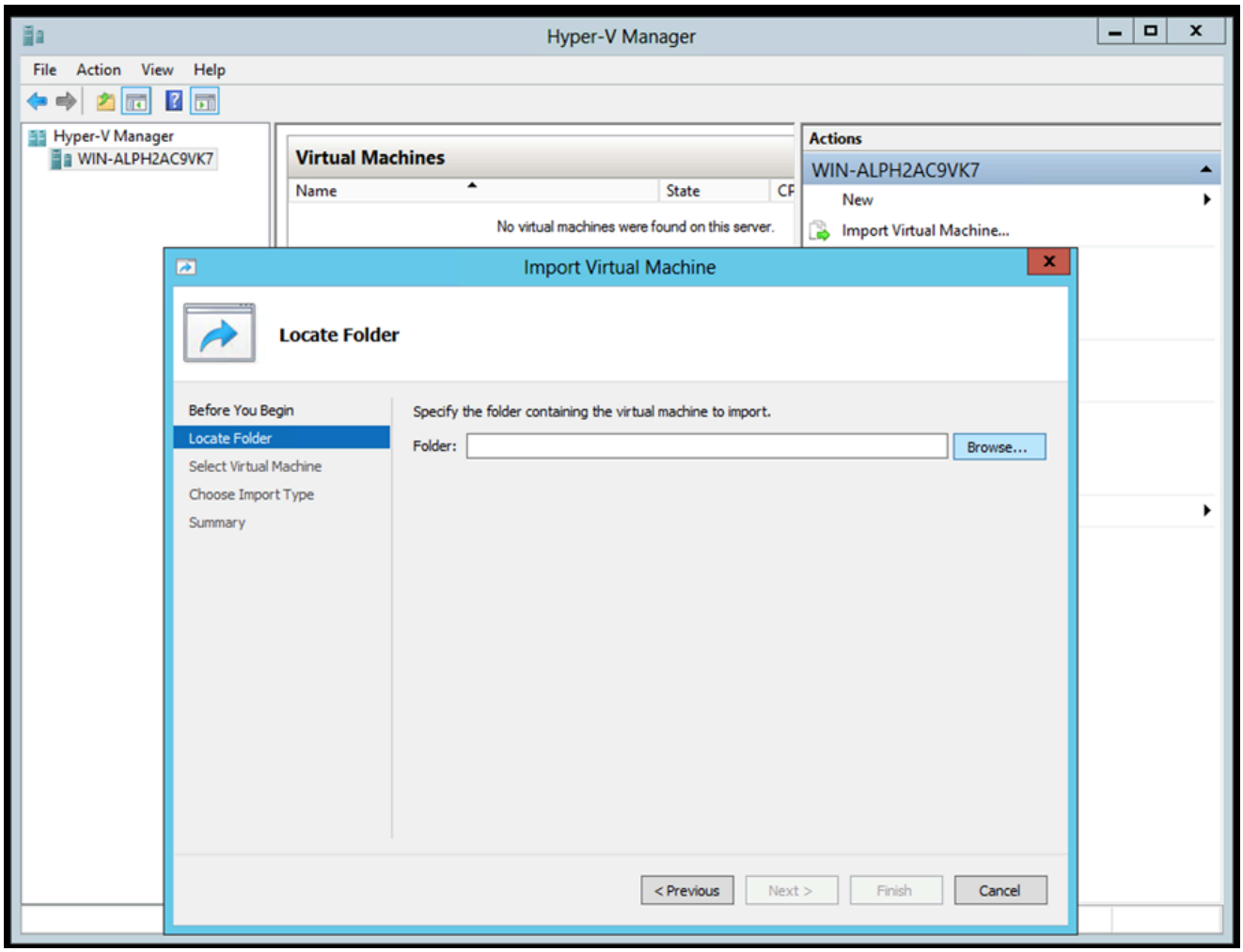
Installation de Microsoft Hyper-V

1. Sélectionnez Import Virtual Machine.



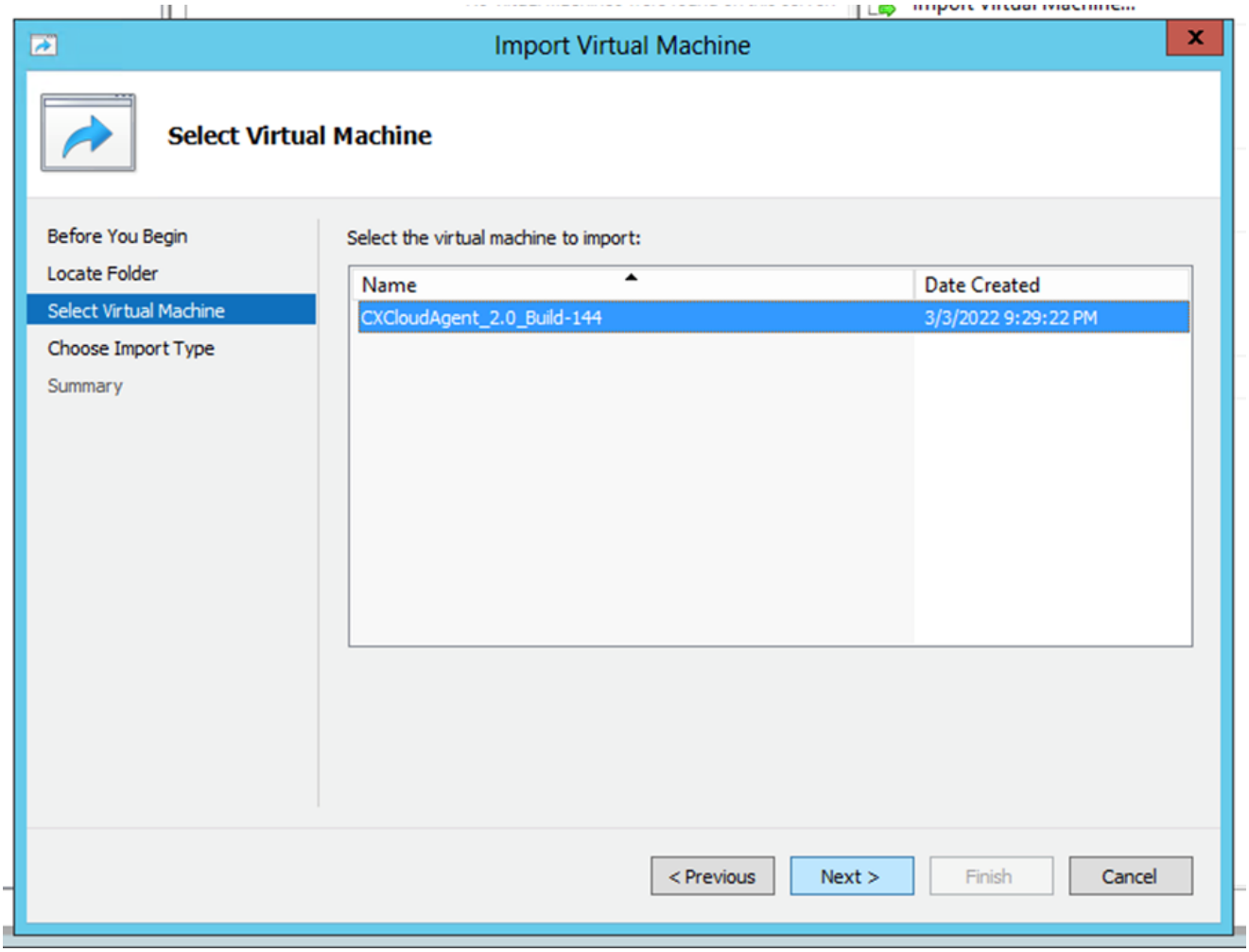
Gestionnaire Hyper-V

2. Recherchez et sélectionnez le dossier de téléchargement.
3. Cliquez sur Next.



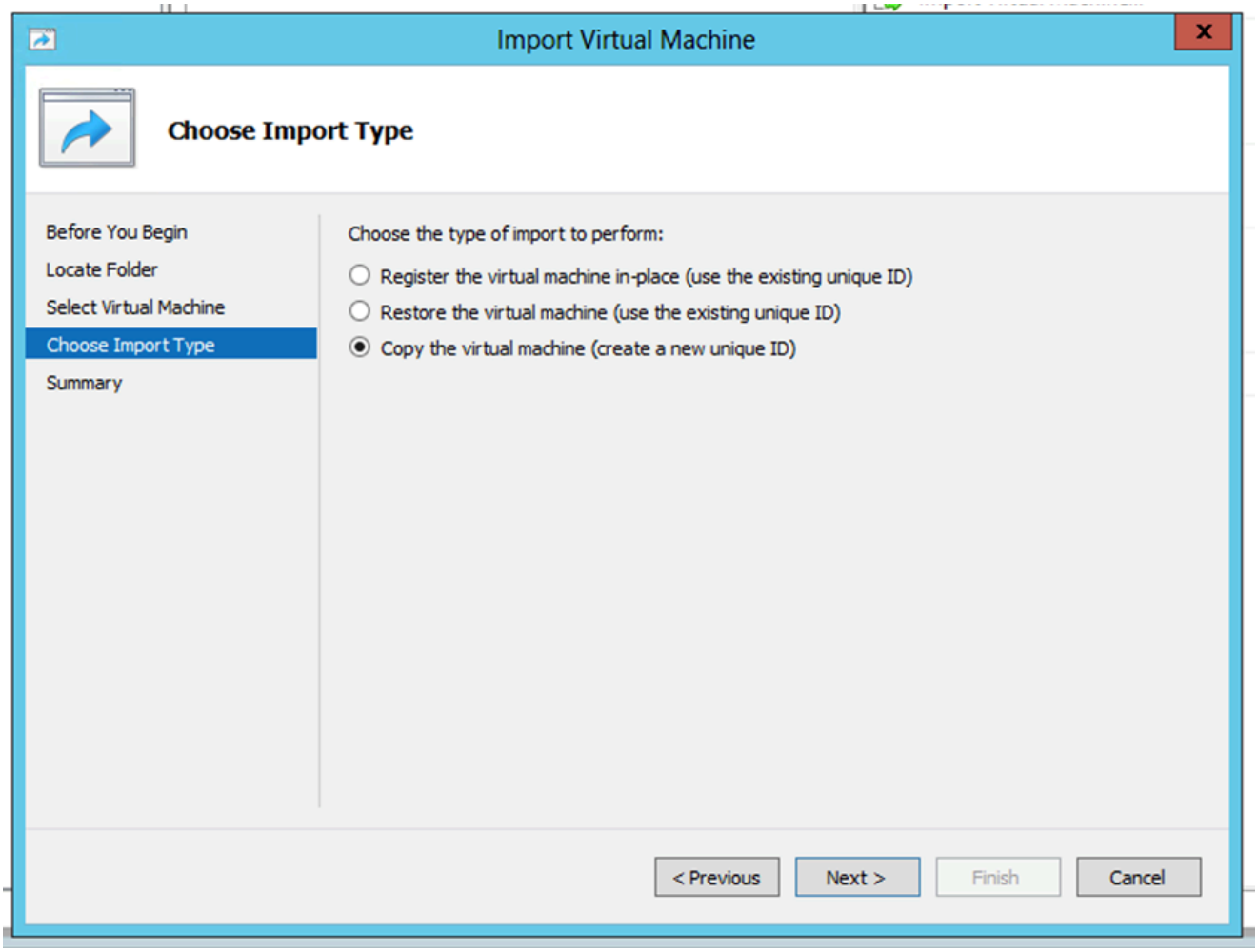
Dossier à importer

4. Sélectionnez la machine virtuelle et cliquez sur Next.



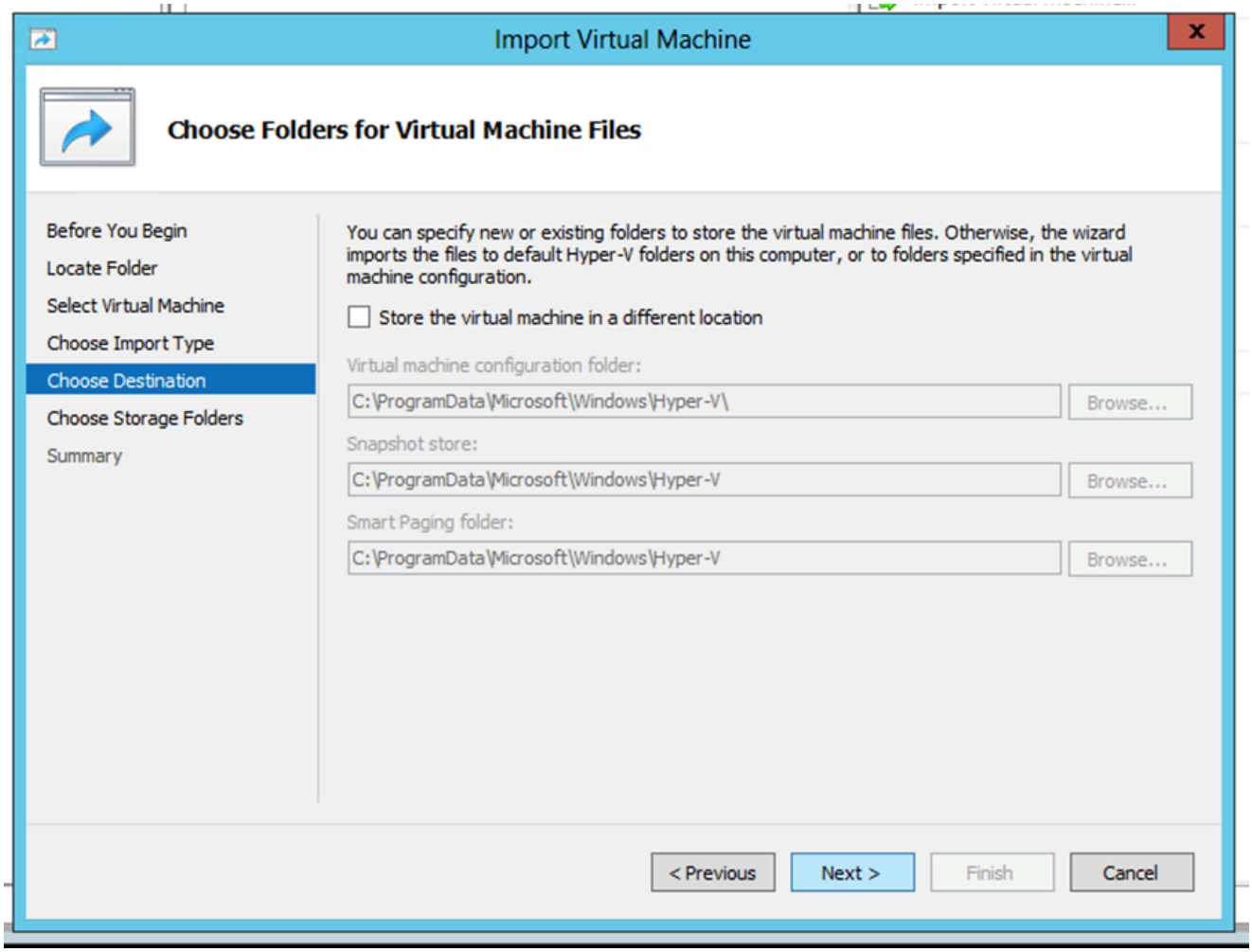
Sélectionner une machine virtuelle

5. Sélectionnez la Copy the virtual machine (create a new unique ID) case d'option et cliquez sur Next.



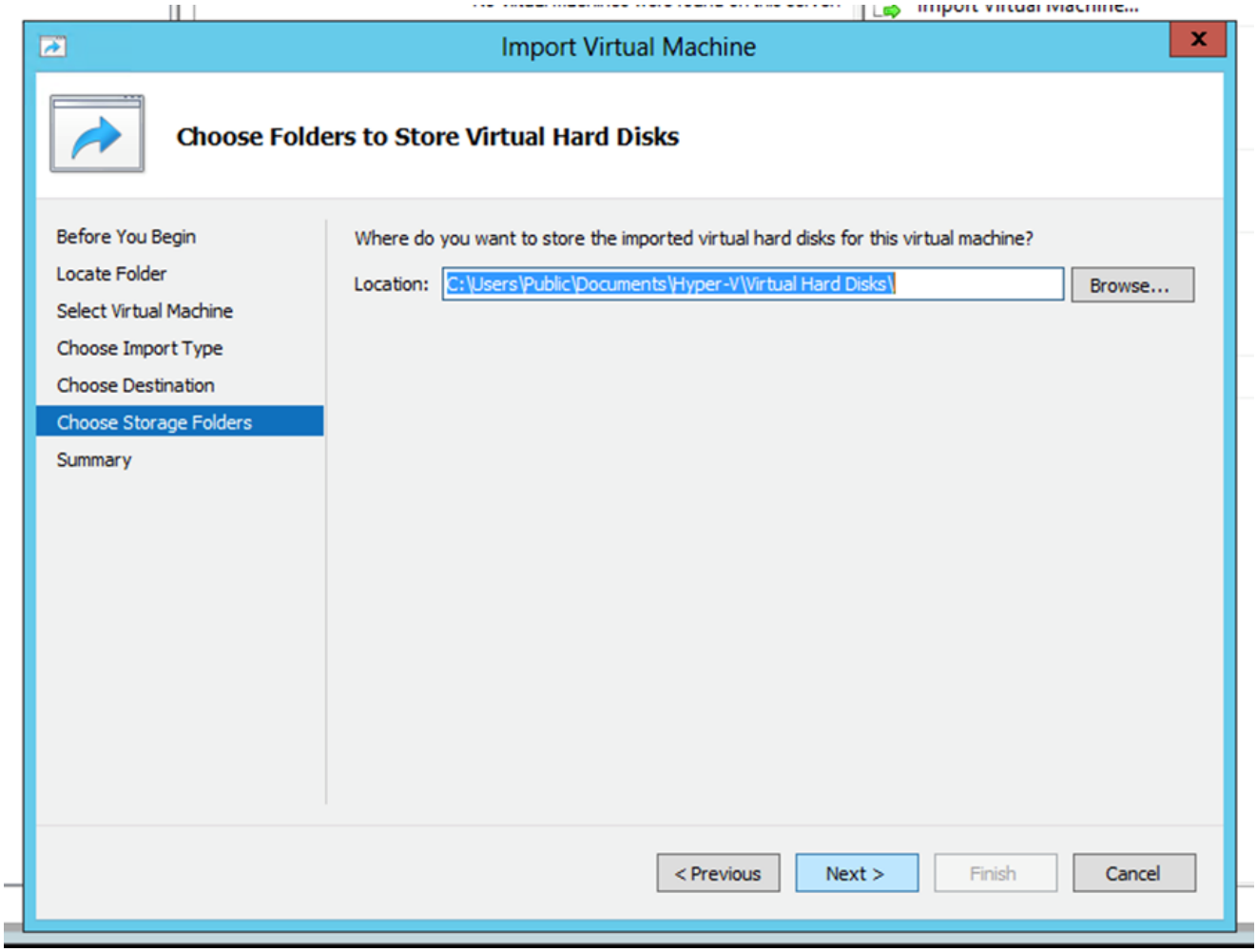
Type d’importation

6. Naviguez pour sélectionner le dossier pour les fichiers de machine virtuelle. Il est recommandé d'utiliser les chemins par défaut.
7. Cliquez sur Next.



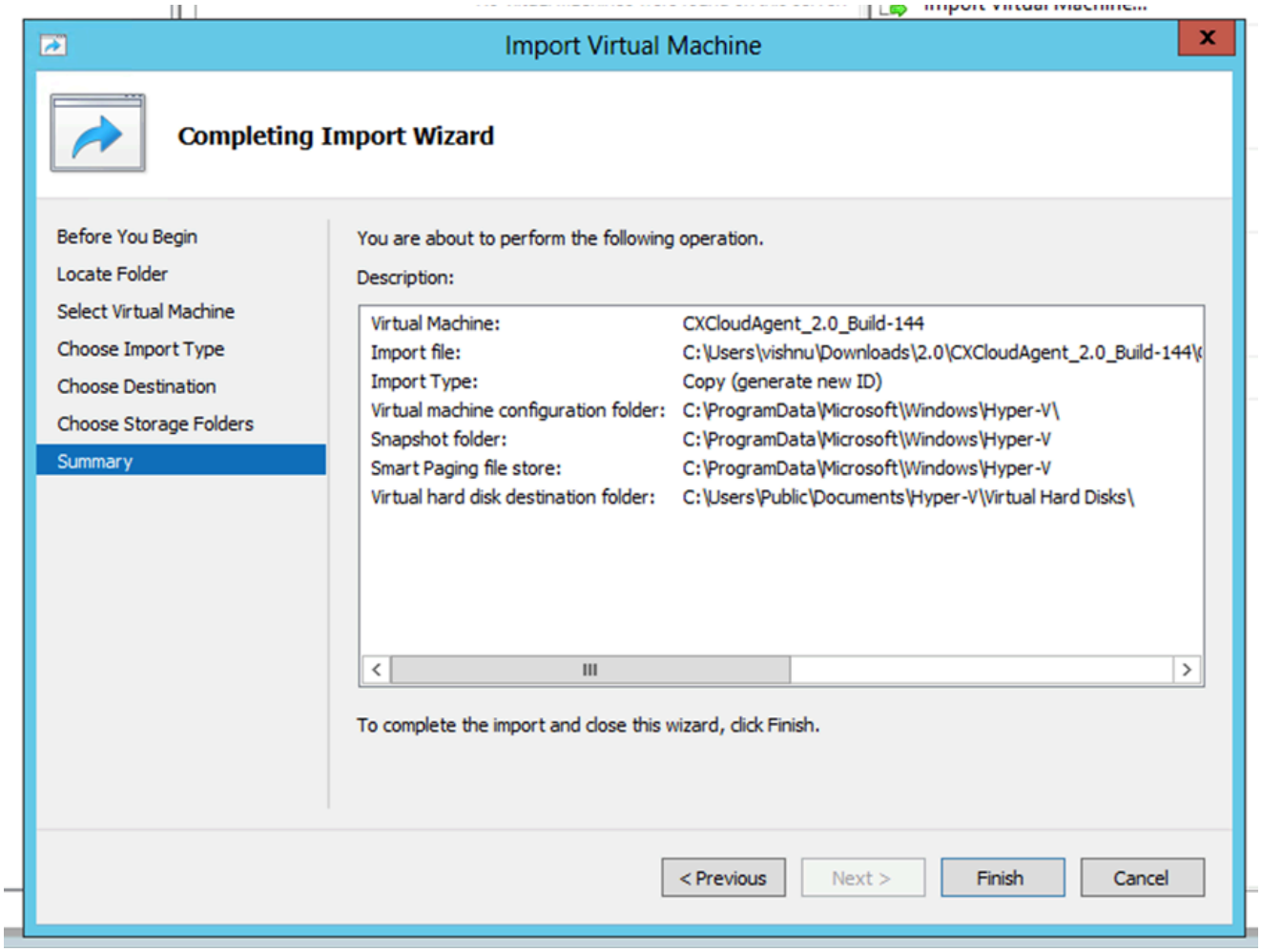
Choisir un dossier

8. Recherchez et sélectionnez le dossier dans lequel stocker le disque dur de la machine virtuelle. Il est recommandé d'utiliser les chemins par défaut.
9. Cliquez sur Next.



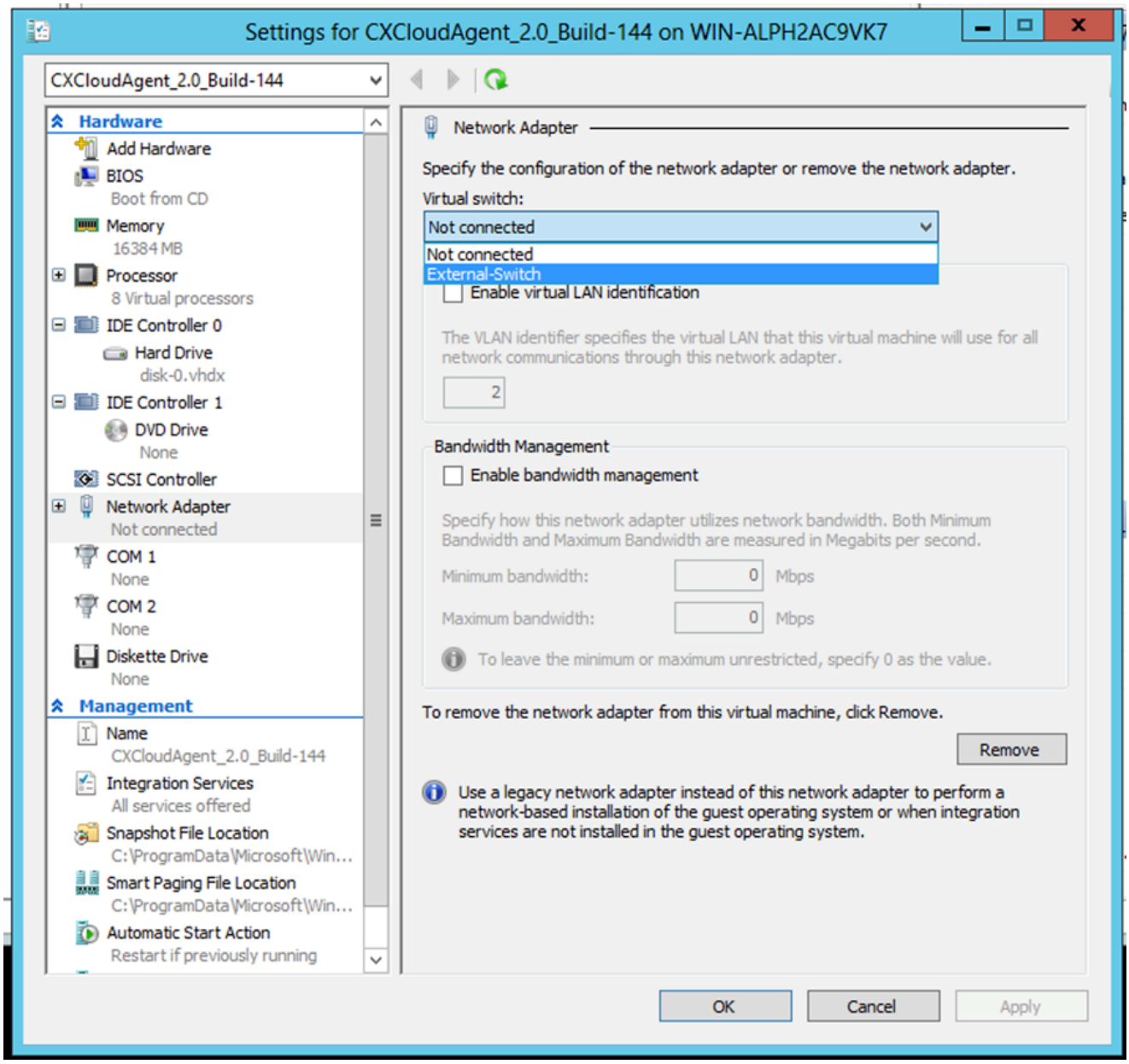
Dossier de stockage des disques durs virtuels

10. Le récapitulatif des VM s'affiche. Vérifiez toutes les entrées et cliquez sur Finish.



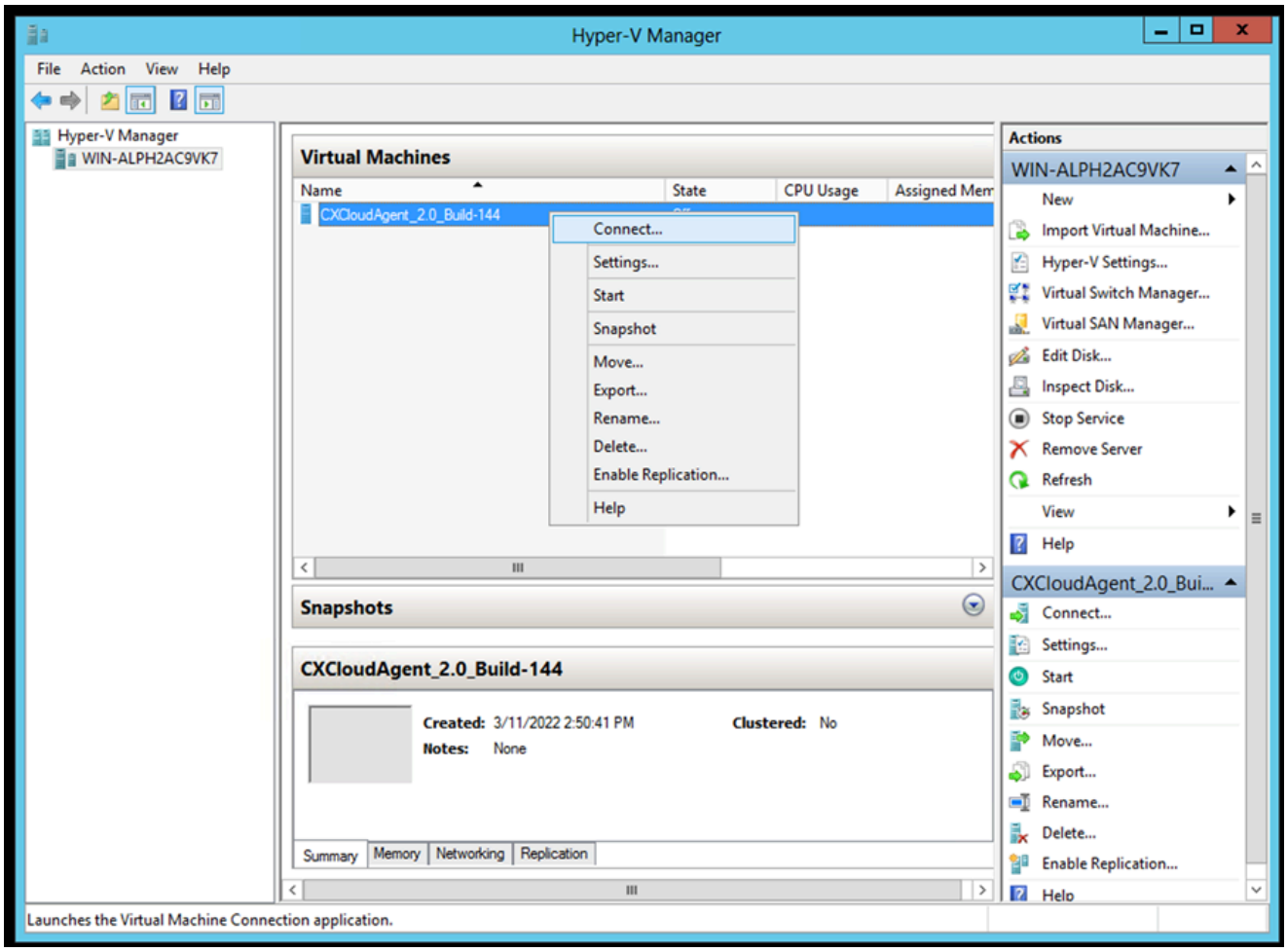
Résumé

11. Une fois l'importation terminée, une nouvelle machine virtuelle est créée sur Hyper-V. Ouvrez le paramètre de la machine virtuelle.
12. Sélectionnez l'adaptateur réseau dans le volet gauche et choisissez la carte disponible Virtual Switch dans la liste déroulante.



Commutateur virtuel

13. Sélectionnez Connect pour démarrer la machine virtuelle.



Démarrage de la machine virtuelle

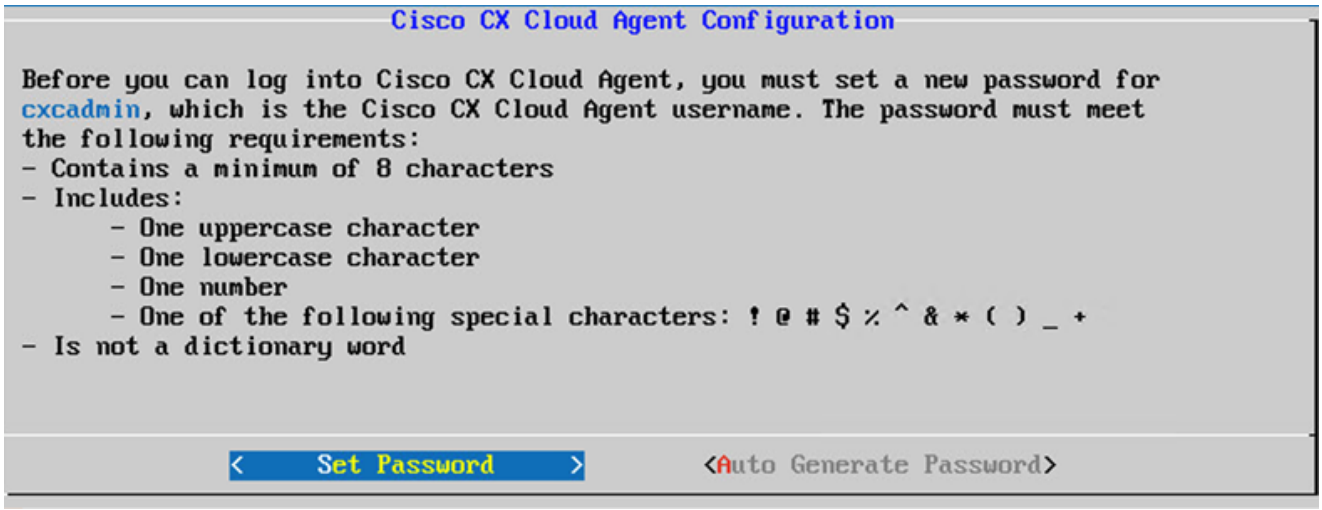
14. Naviguez vers Import Appliance.

Configuration du réseau



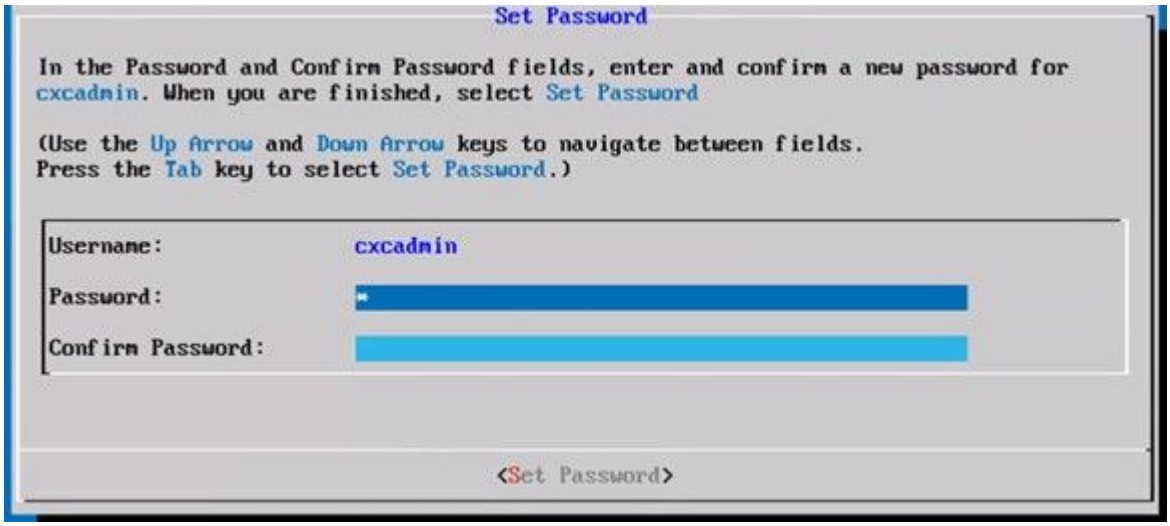
Console de machine virtuelle

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



Définir un mot de passe

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



Nouveau mot de passe

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



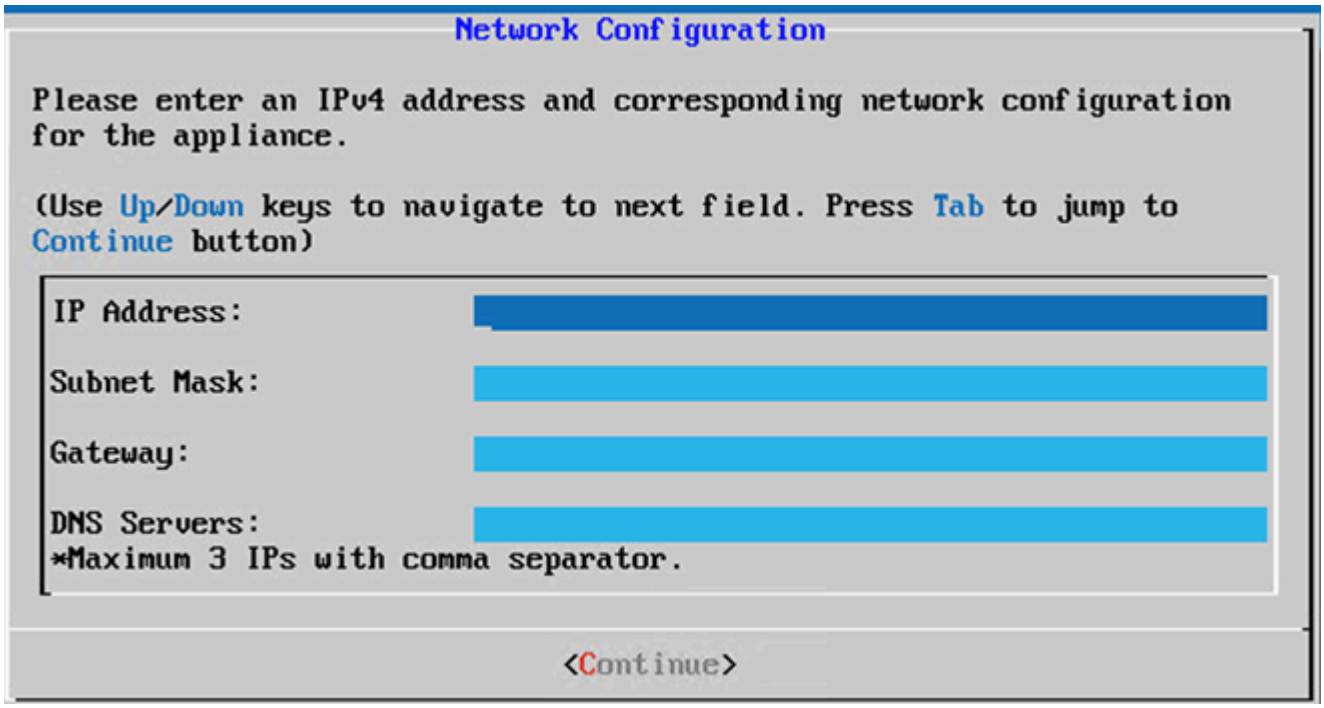
Mot de passe généré automatiquement

3. Cliquez sur Save Password pour l'utiliser pour l'authentification.



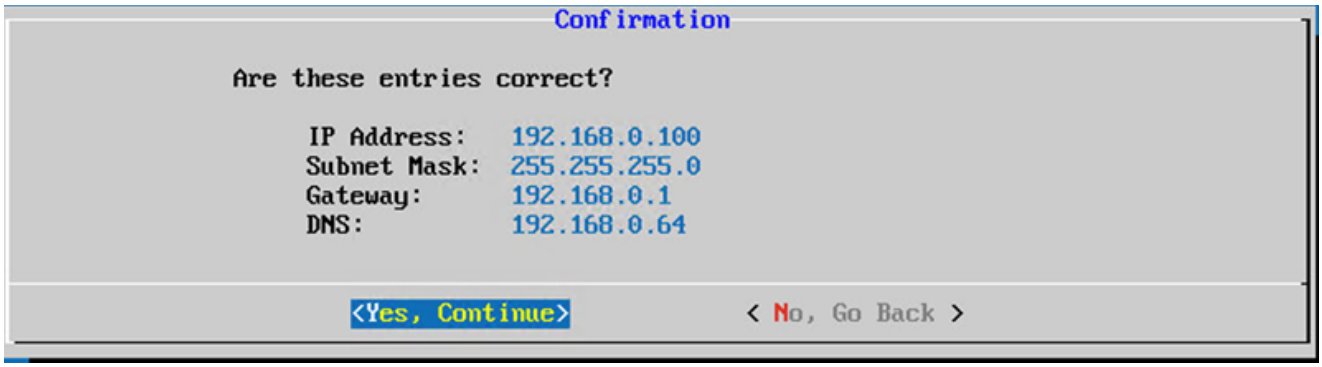
Enregistrez le mot de passe.

4. Saisissez les IP Address, Subnet Mask, Gatewayet DNS Server et cliquez sur Continue.



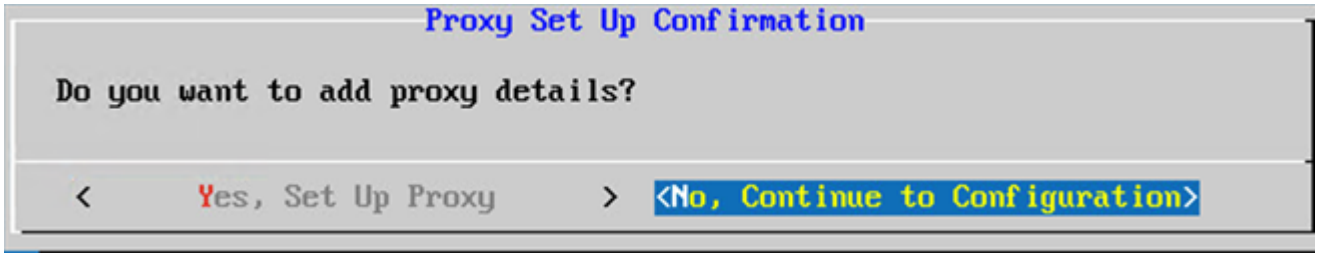
Configuration du réseau

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



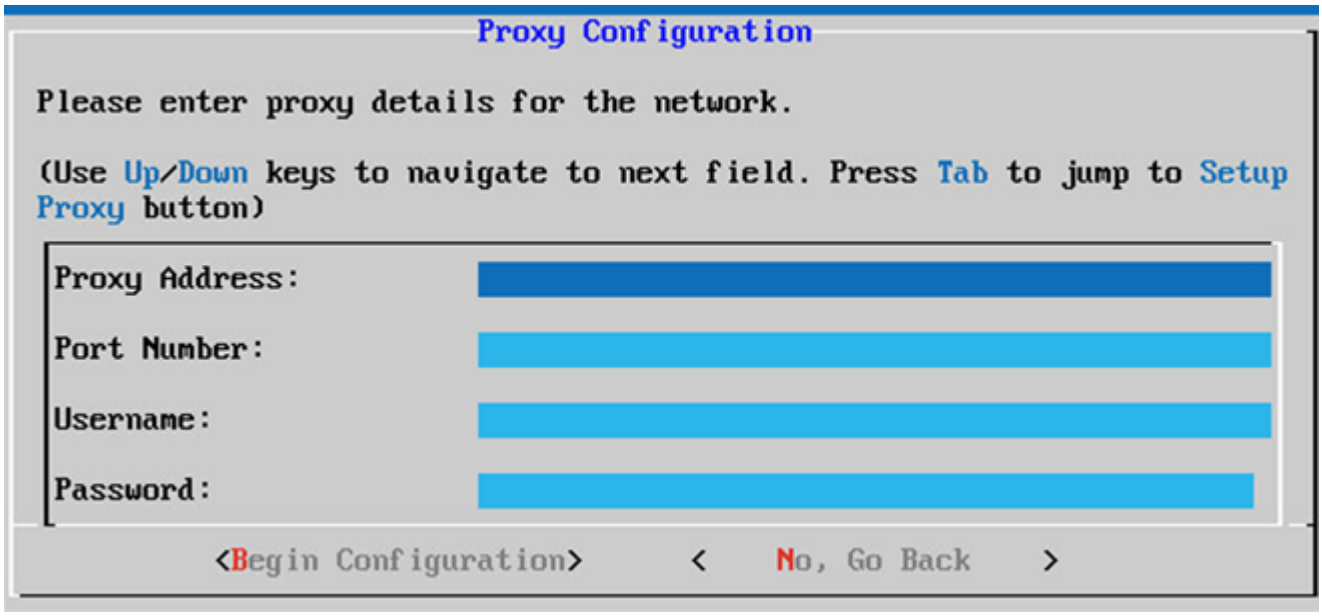
Confirmation

6. Pour définir les détails du proxy, cliquez sur Yes,Set Up Proxy ou cliquez sur No, Continue to Configuration pour terminer la configuration et passez à l'étape 8.



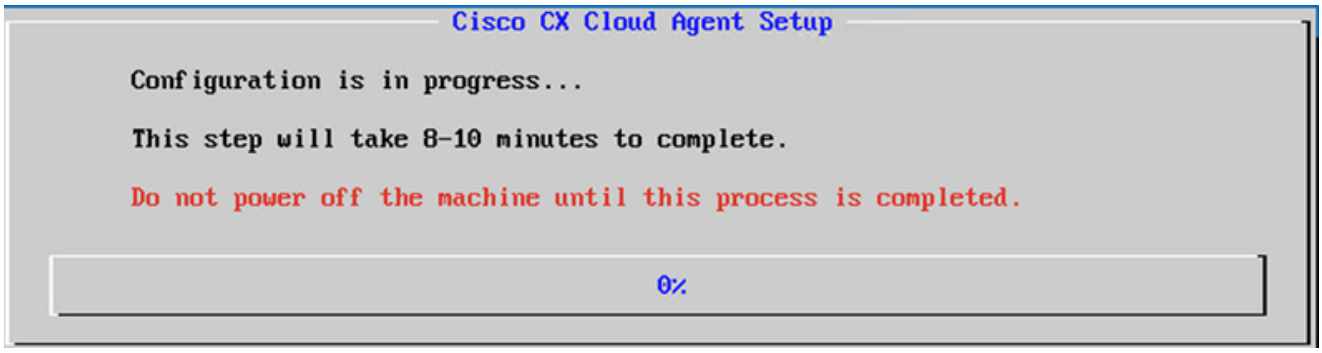
Mise à disposition du proxy

7. Saisissez les Proxy Address, Port Number, Usernameet Password.



Configuration du proxy

8. Cliquez sur Begin Configuration. La configuration peut prendre plusieurs minutes.



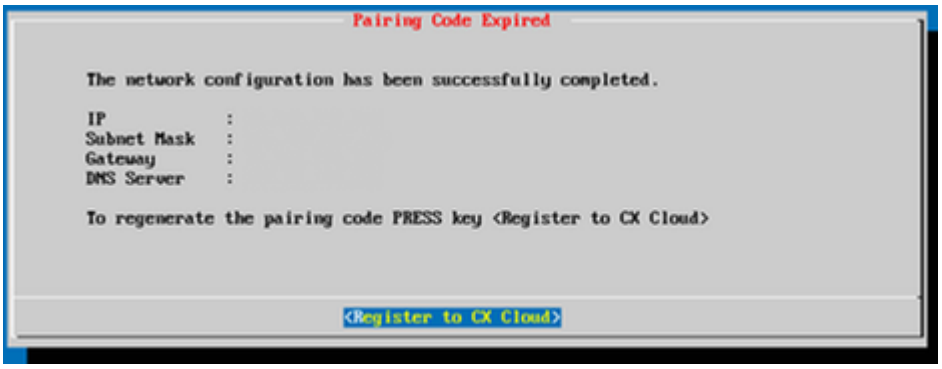
Configuration en cours

9. Copiez le Pairing Code et revenez au cloud CX pour poursuivre la configuration.



Code de jumelage

10. Si le code d'appariement expire, cliquez sur Register to CX Cloud pour obtenir à nouveau le code.



Code expiré

11. Cliquez sur OK.



Inscription réussie

12. Revenez à la section Connexion de CX Cloud Agent à CX Cloud et effectuez les étapes répertoriées.

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 l'interface de ligne de commande :

1. Connectez-vous à l'agent cloud via SSH à l'aide des informations d'identification utilisateur cxcadmin.

2. Générez le code de jumelage à l'aide de la commande cxcli agent generatePairingCode.



Générer le code de jumelage de la CLI

3. Copiez le Pairing Code et revenez au cloud CX pour poursuivre la configuration. Pour plus d'informations, reportez-vous à Connexion au portail client.

Configurer Cisco DNA Center pour transférer Syslog vers CX Cloud Agent

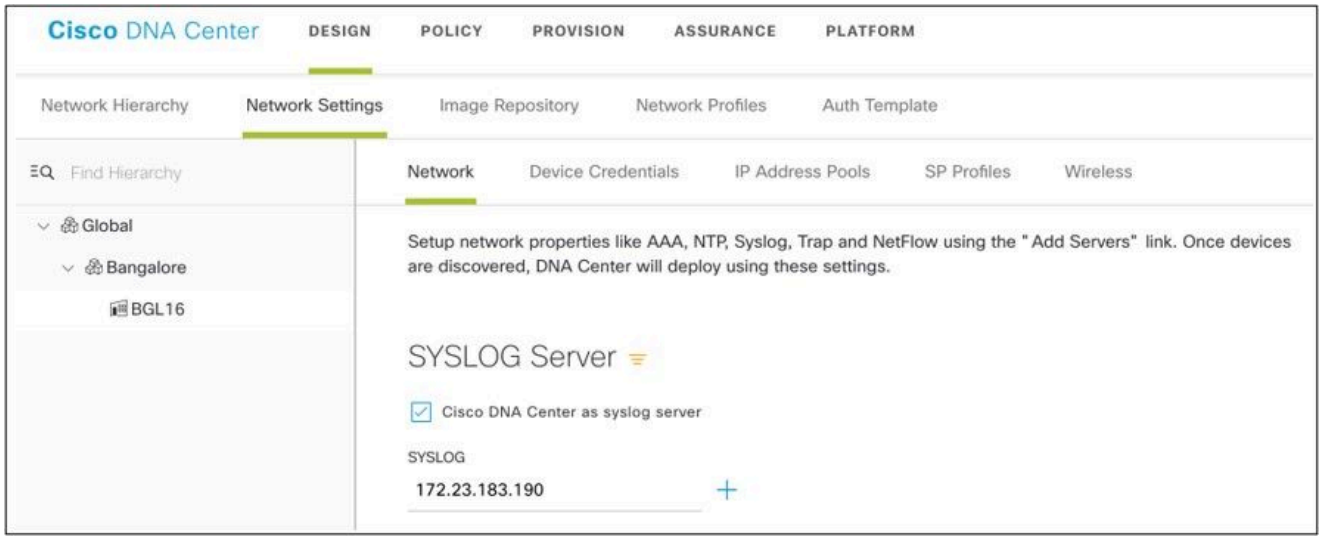
Prérequis

Les versions de Cisco DNA Center prises en charge vont de 1.2.8 à 1.3.3.9 et de 2.1.2.0 à 2.2.3.5.

Configurer le paramètre de transfert Syslog

Pour configurer Syslog Forwarding to CX Cloud Agent dans Cisco DNA Center à l'aide de l'interface utilisateur, procédez comme suit :

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



Syslog Server (Serveur de journal système)

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

Activer les paramètres Syslog au niveau des informations

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

1. Accédez à Tools>Telemetry.



Menu Outils

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



Vue du site

3. Sélectionnez le site requis et sélectionnez tous les périphériques à l'aide de la case à cocher Device name.

4. Dans la liste Actions déroulante, sélectionnez Optimal Visibility.



Actions

Sécurité

CX Cloud Agent garantit au client une sécurité de bout en bout. La connexion entre CX Cloud et CX Cloud Agent est chiffrée. SSH (Secure Socket Shell) de CX Cloud Agent prend en charge 11 algorithmes de chiffrement différents.

Sécurité physique

Déployez l'image OVA de CX Cloud Agent 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 consulter la FAQ pour définir ce mot de passe du chargeur de démarrage (mode utilisateur unique).

Accès utilisateur

Les utilisateurs de CX Cloud peuvent uniquement obtenir l'authentification et accéder aux API de Cloud Agent.

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. L'utilisateur et les informations d'authentification cxcadmin sont utilisés pour accéder à la fois aux API de l'agent CX Cloud et pour connecter l'appliance par ssh.

L'utilisateur cxcadmin dispose d'un accès restreint avec les privilèges les plus faibles. Le mot de passe cxcadmin respecte la stratégie de sécurité et est haché à sens unique avec une période d'expiration de 90 jours. L'utilisateur cxcadmin peut créer un utilisateur cxcroot à l'aide de l'utilitaire appelé remoteaccount. L'utilisateur cxcroot peut obtenir les privilèges racine. La phrase de passe expire dans deux jours.

Sécurité du réseau

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

Authentification

Authentification par mot de passe : L'appliance gère un seul utilisateur, « cxcadmin », qui permet à l'utilisateur de s'authentifier et de communiquer avec l'agent CX Cloud.

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

  l'utilisateur cxcadmin peut 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 peut être déchiffré uniquement à partir du portail SWIM (https://swims.cisco.com/abraxas/decrypt). Seul le personnel autorisé a accès à ce portail. L'utilisateur de cxcroot peut obtenir les privilèges racines en utilisant ce mot de passe déchiffré. La phrase secrète n'est valide que pour deux jours. L'utilisateur de cxcadmin doit recréer le compte et obtenir le mot de passe du portail SWIM après l'expiration du mot de passe.

Durcissement

L'appliance CX Cloud Agent est conforme aux normes de durcissement CIS.

Sécurité des données

L'appliance de l'agent CX Cloud ne stocke aucune information personnelle du client.

L'application d'authentification du périphérique (qui s'exécute comme l'un des modules) stocke les informations d'authentification chiffrées du serveur du centre Cisco DNA dans la base de données sécurisée. Les données recueillies par le centre Cisco DNA ne sont stockées sous aucune forme à l'intérieur de l'appliance. Les données recueillies sont téléversées sur le support peu de temps après la fin de la collecte, et les données sont purgées de l'agent.

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 établit une connexion sécurisée à l'aide de MQTT sur TLS v1.2

Connexions et surveillance

Les journaux ne contiennent aucune information sensible. Les journaux d'audit capturent toutes les actions sensibles à la sécurité effectuées sur l'appliance CX Cloud 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. L'utilisateur doit consulter la FAQ pour définir son mot de passe 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 via l'utilisateur cxcroot nécessite que les informations d'identification soient déchiffrées via le portail SWIM par le personnel autorisé.
Comptes utilisateurs	• cxcadmin : Ceci est un compte utilisateur créé par défaut. L'utilisateur peut exécuter les commandes de l'application de l'agent CX Cloud à l'aide de cxcli et dispose des privilèges les moins élevés 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, qui contiennent trois de ces catégories : majuscules, minuscules, caractères numériques 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 maximum et peuvent être régénérés à l'aide de l'utilisateur cxcadmin.
politique de mot de passe de connexion ssh	• Au moins huit (8) caractères, qui contiennent trois de ces catégories : majuscules, minuscules, caractères numériques et caractères spéciaux • 5 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 informations d'authentification du serveur du centre Cisco DNA sont chiffrées et stockées dans la base de données.

Forum aux questions

Agent CX Cloud

Déploiement

Q – Avec l'option « Re-install », l'utilisateur peut-il déployer le nouvel agent Cloud avec une nouvelle adresse IP?

R – Oui

Q - Quels sont les formats de fichiers disponibles pour l'installation ?

R – OVA et VHD

Q – Quel est l'environnement dans lequel l'installable peut être déployé?

R – OVA

VMware ESXi version 5.5 ou ultérieure

Oracle Virtual Box 5.2.30 ou version ultérieure

VHD

Hyperviseur Windows 2012 à 2016

Q – L'agent CX Cloud peut-il détecter une adresse IP dans un environnement DHCP?

R – Oui, dans le cas d'un environnement DHCP, l'affectation de l'adresse IP lors de la configuration IP est prise en compte. Cependant, la modification d'adresse IP attendue pour l'agent CX Cloud à un moment donné n'est pas prise en charge. En outre, on recommande au client de réserver l'adresse IP de l'agent cloud dans son environnement DHCP.

Q – L'agent CX Cloud prend-il en charge la configuration IPv4 et IPv6?

R – Non, seul IPV4 est pris en charge.

Q – Lors de la configuration IP, l'adresse IP est-elle validée?

R - Oui, la syntaxe des adresses IP et l'attribution d'adresses IP en double sont validées.

Q – Quel est le temps approximatif de déploiement OVA et de configuration IP?

R – Le déploiement d'OVA dépend de la vitesse à laquelle le réseau copie les données. La configuration de l'IP prend environ 8 à 10 minutes, ce qui comprend les créations de Kubernetes et de conteneurs.

Q – Existe-t-il une limitation concernant un type de matériel?

A - La machine hôte sur laquelle OVA est déployé doit répondre aux exigences fournies dans le cadre de la configuration du portail CX. Le CX Cloud Agent est testé avec VMware/Virtual box exécuté sur un matériel équipé de processeurs Intel Xeon E5 avec un rapport vCPU/CPU défini à 2:1. Si un processeur moins puissant ou un rapport plus important est utilisé, les performances peuvent se dégrader.

Q – Pouvons-nous générer le code de jumelage à tout moment?

R – Non, le code de jumelage ne peut être généré que si l'agent cloud n'est pas enregistré.

Q - Quelles sont les exigences en matière de bande passante entre les DNAC (jusqu'à 10 clusters ou 20 non-clusters) et l'agent ?

R - La bande passante n'est pas une contrainte lorsque l'agent et le DNAC se trouvent sur le même réseau LAN/WAN dans l'environnement du client. La bande passante réseau minimale requise est de 2,7 Mbits/s pour les collections d'inventaire de 5 000 périphériques +13000 points d'accès pour une connexion agent-DNAC. Si les syslogs sont collectés pour les analyses de couche 2, la bande passante minimale requise est de 3,5 Mbits/s pour 5 000 périphériques +13000 points d'accès pour l'inventaire, 5 000 syslogs et 2 000 périphériques pour les analyses, tous exécutés en parallèle à partir de l'agent.

Versions et correctifs

Q – Quels sont les différents types de versions répertoriées pour la mise à niveau de l'agent CX Cloud?

R - Vous trouverez ci-dessous l'ensemble des versions de CX Cloud Agent qui sont répertoriées :

- Ax0 (où x est la plus récente version majeure des fonctionnalités de production, exemple : 1.3.0)
- A.x.y (où A.x.0 est obligatoire et une mise à niveau incrémentielle doit être lancée, x est la dernière version de la fonctionnalité majeure de production et y est le dernier correctif de mise à niveau actif, par exemple : 1.3.1).
- A.x.y-z (où A.x.0 est obligatoire et une mise à niveau incrémentielle doit être initiée, x est la dernière version majeure de la fonctionnalité de production, et y est le dernier correctif de mise à niveau actif, et z est le correctif ponctuel qui est un correctif instantané pour une très courte période de temps, par exemple : 1.3.1-1)

où A est une version à long terme répartie sur une période de 3 à 5 ans.

Q - Où trouver la dernière version de CX Cloud Agent et comment mettre à niveau CX Cloud Agent existant ?

A - Accédez à Admin Settings > Data Sources. Cliquez sur le View Update et suivez les instructions affichées à l'écran.

Configuration de l'authentification et du proxy

Q – Quel est l'utilisateur par défaut de l'application d'agent CX Cloud?

R – cxcadmin

Q - Comment le mot de passe est-il défini pour l'utilisateur par défaut ?

R – Le mot de passe est défini lors de la configuration du réseau.

Q – Existe-t-il une option permettant de réinitialiser le mot de passe après le jour 0?

R – Aucune option particulière n'est fournie par l'agent pour réinitialiser le mot de passe, mais vous pouvez utiliser les commandes linux pour réinitialiser le mot de passe pour cxcadmin.

Q – Quelles sont les politiques de mot de passe pour configurer l'agent CX Cloud?

R – Les politiques de mot de passe sont les suivantes :

- L'âge maximal du mot de passe (longueur) est de 90 jours
- L'âge minimal du mot de passe (longueur) est de 8
- La longueur maximale du mot de passe est de 127 caractères.
- Au moins un majuscule et un minuscule doivent être fournis.
- Doit contenir au moins un caractère spécial (par exemple, !$%^&*()_+|~-=\`{}[]:";'<>?,/).
- Ces caractères ne sont pas autorisés
    - Caractères spéciaux de 8 bit (par exemple, ¬£, √Å √´, √¥, √ë, ¬ø, √ü)
    - Espaces
- Le mot de passe ne doit pas être le dernier mot de passe utilisé depuis 10 ans.
- Ne doit pas contenir d'expression régulière i.e.
- Ne doit pas contenir les termes suivants ou leurs dérivés : cisco, sanjose et sanfran

Q – Comment définir le mot de passe Grub?

A - Pour définir le mot de passe Grub, procédez comme suit :

1. Exécutez ssh comme cxcroot et fournissez le jeton [Contactez l'équipe d'assistance pour obtenir le jeton cxcroot]
2. Exécuter sudo su; fournir le même jeton
3. Exécutez la commande grub-mkpasswd-pbkdf2 et définissez le mot de passe GRUB. Le hachage du mot de passe fourni est imprimé, copiez le contenu.
4. vi dans le fichier /etc/grub.d/00_header. Accédez à la fin du fichier et remplacez la sortie de hachage précédant le contenu password_pbkdf2 root ***** par le hachage obtenu pour le mot de passe obtenu à l'étape 3
5. Enregistrez le fichier avec la commande : wq!
6. Exécutez la commande update-grub

Q - Quel est le délai d'expiration du mot de passe cxcadmin?

R – Le mot de passe expire dans 90 jours.

Q – Le système désactive-t-il le compte après plusieurs tentatives infructueuses de connexion?

R – Oui, le compte est désactivé après cinq tentatives infructueuses consécutives. La période de verrouillage est de 30 minutes.

Q – Comment générer une phrase secrète?

A - Effectuez ces étapes,

1. Exécutez ssh et connectez-vous en tant qu'utilisateur cxcadmin
2. Exécutez la commande remoteaccount cleanup -f
3. Exécutez la commande remoteaccount create

Q – L'hôte proxy prend-il en charge à la fois le nom d'hôte et l'adresse IP?

R - Oui, mais pour utiliser le nom d'hôte, l'utilisateur doit fournir l'adresse IP DNS lors de la configuration du réseau.

Protocole SSH (Secure Shell)

Q – Quels sont les chiffres pris en charge par le protocole SSH?

R – chacha20-poly1305@openssh.com, aes256-gcm@openssh.com, aes128-gcm@openssh.com, aes256-ctr, aes192-ctr, aes128-ctr

Q – Comment se connecter à la console?

A - Procédez comme suit pour vous connecter :

1. Connectez-vous en tant qu'utilisateur cxcadmin.
2. Entrez le mot de passe cxcadmin.

Q – Les connexions ssh sont-elles enregistrées?

R - Oui, ils sont consignés dans le fichier var/logs/audit/audit.log.

Q – Quelle est la durée d'inactivité de la session?

A - Le délai d'expiration de la session SSH se produit si l'agent cloud est inactif pendant cinq (5) minutes.

Ports et services

Q – Quels sont les ports ouverts par défaut sur CX Cloud Agent?

A - Ces ports sont disponibles :

- Outbound port: L'agent cloud CX déployé peut se connecter au back-end Cisco comme indiqué dans le tableau sur le port HTTPS 443 ou via un proxy pour envoyer des données à Cisco. L'agent CX Cloud déployé peut se connecter au centre Cisco DNA sur le port HTTPS 443.

.

AMÉRIQUE	EMEA	APJC
cloudsso.cisco.com	cloudsso.cisco.com	cloudsso.cisco.com

api-cx.cisco.com	api-cx.cisco.com	api-cx.cisco.com
agent.us.csco.cloud	agent.emea.csco.cloud	agent.apjc.csco.cloud
ng.acs.agent.us.csco.cloud	ng.acs.agent.emea.csco.cloud	ng.acs.agent.apjc.csco.cloud

Remarque : Outre les domaines répertoriés, lorsque les clients EMEA ou APJC réinstallent l'agent cloud, le domaine agent.us.csco.cloud doit être autorisé dans le pare-feu du client.

Le domaine agent.us.csco.cloud n'est plus nécessaire après une réinstallation réussie.

Remarque : Vérifiez que le trafic de retour doit être autorisé sur le port 443.

- Inbound port: Pour la gestion locale de CX Cloud Agent, 514 (Syslog) et 22 (ssh) doivent être accessibles. Le client doit autoriser le port 443 de son pare-feu à recevoir des données du cloud CX.

Connexion de l'agent CX Cloud au centre Cisco DNA

Q – Quel est le but et la relation du centre Cisco DNA avec l'agent CX Cloud r?

R - Cisco DNA Center est l'agent cloud qui gère les périphériques réseau des locaux du client. L'agent CX Cloud recueille les informations d'inventaire des périphériques à partir du centre Cisco DNA configuré et télécharge les informations d'inventaire accessibles en tant qu'« Affichage des actifs » dans CX Cloud.

Q – Où l'utilisateur peut-il fournir les détails du centre Cisco DNA sur l'agent CX Cloud?

R - Au cours de la configuration de CX Cloud Agent, l'utilisateur peut ajouter les détails de Cisco DNA Center à partir du portail CX Cloud. En outre, pendant les opérations de jour N, les utilisateurs peuvent ajouter des centres DNA supplémentaires à partir de Admin Settings > Data source.

Q – Combien de centres Cisco DNA peuvent être ajoutés?

A - 10 clusters DNAC Cisco ou 20 non-clusters DNAC.

Q - Quel rôle l'utilisateur de Cisco DNA Center peut-il jouer ?

A - Le rôle d'utilisateur peut être admin ou observer.

Q - Comment refléter les modifications apportées à CX Agent suite à des modifications apportées aux identifiants DNA Center connectés ?

R - Exécutez ces commandes à partir de la console CX Cloud Agent :

```
cxcli agent modifyController
```

Contactez le support pour tout problème lors de la mise à jour des identifiants DNAC.

Q – Comment les détails du centre Cisco DNA sont-ils stockés dans l'agent CX Cloud?

R – Les identifiants du centre Cisco DNA sont chiffrés à l'aide d'AES-256 et stockés dans la base de données de l'agent CX Cloud. La base de données de l'agent CX Cloud est protégée par un ID utilisateur et un mot de passe sécurisés.

Q - Quel type de cryptage sont utilisés lors de l'accès à l'API Cisco DNA Center à partir de CX Cloud Agent ?

R – HTTPS sur TLS 1.2 est utilisé pour la communication entre le centre Cisco DNA et l'agent CX Cloud.

Q – Quelles sont les opérations effectuées par l'agent CX Cloud sur l'agent Cloud intégré du centre Cisco DNA?

R - CX Cloud Agent collecte les données dont dispose Cisco DNA Center sur les périphériques réseau et utilise l'interface du canal d'exécution des commandes Cisco DNA Center pour communiquer avec les périphériques finaux et exécuter les commandes CLI (commande show). Aucune commande de modification de configuration n'est exécutée

Q – Quelles sont les données par défaut recueillies à partir du centre Cisco DNA et téléversées vers le serveur principal?

A-

- Entité de réseau
- Modules
- show version
- configuration
- Informations sur l'image du périphérique
- Étiquettes

Q – Quelles sont les données supplémentaires recueillies à partir du centre Cisco DNA et téléversées vers le serveur principal de Cisco?

R – Vous obtiendrez toute l'information ici.

Q – Comment les données d'inventaire sont-elles téléchargées dans le serveur principal?

R – L'agent CX Cloud télécharge les données à partir du protocole TLS 1.2 vers le serveur principal de Cisco.

Q – Quelle est la fréquence de téléversement de l'inventaire?

A - La collecte est déclenchée selon le planning défini par l'utilisateur et est téléchargée vers le serveur principal Cisco.

Q – L'utilisateur peut-il reprogrammer l'inventaire?

R - Oui, une option est disponible pour modifier les informations de planification à partir de Admin Settings> Data Sources.

Q – Quand l’expiration délai de connexion se produit-elle entre le centre Cisco DNA et l’agent Cloud?

A - Les délais d'attente sont classés en conséquence :

- Pour la connexion initiale, l’expiration délai est de 300 secondes maximum. Si la connexion n’est pas établie entre le centre Cisco DNA et l’agent Cloud dans un délai maximum de cinq minutes, la connexion est alors interrompue.
- Pour les connexions récurrentes, habituelles ou les mises à jour: le délai de réponse est de 1 800 secondes. Si la réponse n’est pas reçue ou ne peut pas être lue dans les 30 minutes, la connexion est interrompue.

Analyse de diagnostic utilisée par l’agent CX Cloud

Q – Quelles sont les commandes exécutées sur le périphérique pour l’analyse?

A - Les commandes qui doivent être exécutées sur le périphérique pour l'analyse sont déterminées dynamiquement pendant le processus d'analyse. L'ensemble de commandes peut changer au fil du temps, même pour le même périphérique (et ne contrôle pas l'analyse diagnostique).

Q – Où sont stockés et profilés les résultats de l’analyse?

R – Les résultats analysés sont stockés et profilés dans le serveur principal de Cisco.

Q – Les doublons (par nom d’hôte ou IP) dans le centre Cisco DNA ont-ils été ajoutés à l’analyse de diagnostic lorsque la source du centre Cisco DNA est branchée?

A - Non, les doublons sont filtrés et seuls les périphériques uniques sont extraits.

Q – Que se passe-t-il lorsqu’une des analyses de commandes échoue?

A - L'analyse du périphérique est complètement arrêtée et est marquée comme ayant échoué.

Journaux du système de l’agent CX Cloud

Q - Quelles informations de santé sont envoyées au cloud CX ?

R – Journaux d’application, état du module, détails du centre Cisco DNA, journaux d’audit, détails du système et détails du matériel.

Q – Quels détails système et matériel sont collectés?

R – Sortie d’échantillon :

system_details":{
"os_details":{

"containerRuntimeVersion":"docker://19.3.12",
"kernelVersion":"5.4.0-47-generic",
"kubeProxyVersion":"v1.15.12",
"kubeletVersion":"v1.15.12",
"machineID":"81edd7df1c1145e7bcc1ab4fe778615f",
"operatingSystem":"linux",
"osImage" :"Ubuntu 20.04.1 LTS",
"systemUID" :"42002151-4131-2ad8-4443-8682911bdadb"
},
"hardware_details":{
"total_cpu":"8",
"cpu_used":"12.5%",
"total_memory":"16007MB",
"free_memory" :"994 Mo",
"hdd_size":"214G",
"free_hdd_size":"202G"
}
}
}

Q – Comment les données de santé sont-elles envoyées au serveur principal?

R - Avec CX Cloud Agent, le service d'intégrité (facilité de maintenance) transmet les données au back-end Cisco.

Q – Quelle est la politique de conservation du journal des données de santé de l'agent CX Cloud dans le serveur principal?

R – La politique de conservation des journaux de santé de l'agent CX Cloud dans le serveur principal est de 120 jours.

Q – Quels sont les types de téléversements offerts?

A - Trois types de téléchargements disponibles,

1. Chargement des stocks
2. Téléchargement Syslog
3. Chargement de l'état des agents : 3 choses dans le cadre de la santé upload
    1. Santé des services - toutes les 5 minutes
    2. Podlog - toutes les 1 heure
    3. Journal d'audit - toutes les 1 heure

Dépannage

Problème : Impossible d'accéder à l'adresse IP configurée.

Solution : Exécutez ssh en utilisant l'IP configurée. Si la connexion expire, la raison possible est une mauvaise configuration IP. Dans ce cas, procédez à une réinstallation en configurant une

adresse IP valide. Cela peut être fait via le portail avec l'option de réinstallation fournie dans la page Admin Setting.

Problème : Comment vérifier si les services sont opérationnels après l'enregistrement?

Solution : Exécutez la commande présentée ici et vérifiez si les pods sont opérationnels.

1. ssh à l'adresse IP configurée comme cxcadmin.
2. Indiquez le mot de passe.
3. Exécutez la commande kubectl get pods.

Les pods peuvent être dans n'importe quel état, tel que l'exécution, l'initialisation ou la création du conteneur, mais après 20 minutes, les pods doivent être dans l'état d'exécution.

Si l'état n'est pas en cours d'exécution ou Initialisation du pod, vérifiez la description du pod avec la commande indiquée ici

kubectl description pod <podname>

Le résultat contient les informations sur l'état du pod.

Problème : Comment vérifier si l'intercepteur SSL est désactivé au niveau du proxy client ?
Solution : Exécutez la commande curl présentée ici pour vérifier la section du certificat du serveur. La réponse contient les détails du certificat du serveur Web de console.

curl -v —header 'Autorisation : Base xxxxxx' https://concsoweb-prd.cisco.com/

* Certificat de serveur :

* objet : C=US ; ST=Californie ; L=San José ; O=Cisco Systems, Inc.; CN=concsoweb-prd.cisco.com

* date de début : 16 février 11:55:11 2021 GMT

* date d'expiration : 16 février 12:05:00 2022 GMT

* subjectAltName : l'hôte « concsoweb-prd.cisco.com » correspond au certificat « concsoweb-prd.cisco.com »

* émetteur : C=US ; O=HydrantID (Avalanche Cloud Corporation); CN=AC G3 SSL HydrantID

* Vérification du certificat SSL OK.

> GET / HTTP/1.1

Problème : Les commandes kubectl ont échoué et affichent l'erreur comme suit : « La connexion au serveur X.X.X.X:6443 a été refusée - avez-vous spécifié le bon hôte ou port »
Solution :

- Vérifiez la disponibilité des ressources. [exemple : CPU, Mémoire]
- Attendez que le service Kubernetes démarre

Problème : Comment obtenir les détails de l'échec de collecte pour une commande ou un périphérique

Solution :

- Exécutez `kubectl get pods` et obtenez le nom de la zone de collecte.
- Exécutez `kubectl logs` pour obtenir les détails spécifiques à la commande/au périphérique.

Problème : La commande kubectl ne fonctionne pas avec l'erreur « [authentication.go: 64] Impossible d'authentifier la demande en raison d'une erreur : [x509: Le certificat est expiré ou n'est pas encore valide, x509: Le certificat est expiré ou n'est pas encore valide]"

Solution : exécutez les commandes indiquées ici en tant qu'utilisateur cxcroot

rm /var/lib/rancher/k3s/server/tls/dynamic-cert.json
systemctl restart k3s
kubectl —insecure-skip-tls-verify=true delete secret -n kube-system k3s-service
systemctl restart k3s

Réponses aux échecs de collecte

La collecte peut avoir échoué en raison de toute contrainte ou de tout problème rencontré avec le contrôleur ajouté ou les périphériques présents dans le contrôleur.

Le tableau ci-dessous contient l'extrait d'erreur pour les cas d'utilisation observés sous le microservice Collection pendant le processus de collecte.

Scénario	Extrait de journal dans le micro-service de collecte
Si le périphérique demandé est introuvable dans le centre Cisco DNA	{ "command": "show version", "status": "Failed",

Scénario	Extrait de journal dans le micro-service de collecte
	"commandResponse": "", "errorMessage": " No device found with id 02eb08be-b13f-4d25-9d63-eaf4e882f71a " }

Si le périphérique demandé n'est pas accessible à partir du centre Cisco DNA	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "Error occurred while executing command: show version\nError connecting to device [Host: 172.21.137.221:22]No route to host : No route to host "
	}

Si le périphérique demandé n'est pas accessible à partir du centre Cisco DNA	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "Error occured while executing command : show version\nError connecting to device [Host: X.X.X.X]Connection timed out: /X.X.X.X:22 : Connection timed out: /X.X.X.X:22"
	}

Si la commande demandée n'est pas accessible dans le périphérique	{
	"command": "show run-config",
	"status": "Success",
	"commandResponse": " Error occured while executing command : show run-config\n\nshow run-config\n ^\n% Invalid input detected at \u0027^\u0027 marker.\n\nXXCT5760#",
	"errorMessage": ""
	}

Si le périphérique demandé ne dispose pas de SSHv2 et que Cisco DNA Center tente de le connecter à SSHv2	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "Error occured while executing command : show version\nSSH2 channel closed : Remote party uses incompatible protocol, it is not SSH-2 compatible."
	}

Scénario	Extrait de journal dans le micro-service de collecte

Si la commande est désactivée dans le micro-service de collecte	{
	"command": "config paging disable",
	"status": "Command_Disabled",
	"commandResponse": "Command collection is disabled",
	"errorMessage": ""
	}

Si la tâche du gestionnaire de commandes échoue, et que l'URL de tâche n'est pas renvoyée par le centre Cisco DNA	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "The command runner task failed for device %s. Task URL is empty."
	}

Si la tâche de gestionnaire de commandes n'a pas pu être créée dans le centre Cisco DNA	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "The command runner task failed for device %s, RequestURL: %s. No task details."
	}

Si le micro-service de collecte ne reçoit pas de réponse à une demande de gestionnaire de commandes du centre Cisco DNA	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "The command runner task failed for device %s, RequestURL: %s."
	}

Si le centre Cisco DNA ne termine pas la tâche dans le délai imparti configuré (cinq minutes par commande dans le micro-service de collecte)	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "Operation Timedout. The command runner task failed for device %s, RequestURL: %s. No progress details."
	}

Si la tâche de gestionnaire de commandes a	{

Scénario	Extrait de journal dans le micro-service de collecte
échoué et que l’ID de fichier est vide pour la tâche soumise par le centre Cisco DNA	"command": "show version", "status": "Failed", "commandResponse": "", "errorMessage": "The command runner task failed for device %s, RequestURL: %s. File id is empty." }

Si la tâche du gestionnaire de commandes échoue, et que l’ID de fichier n’est pas renvoyé par le centre Cisco DNA	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "The command runner task failed for device %s, RequestURL: %s. No file id details."
	}

Si l’appareil n’est pas admissible à l’exécution du gestionnaire de commandes	{
	"command": "config paging disable",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "Requested devices are not in inventory,try with other devices available in inventory"
	}

Si le gestionnaire de commandes est désactivé pour l’utilisateur	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "{\"message\":\"Role does not have valid permissions to access the API\"}\n"
	}

Réponses aux échecs de l'analyse diagnostique

Échec de l’analyse. Cela pourrait être dû à l’un des composants répertoriés

Lorsque l’utilisateur lance une analyse à partir du portail, elle se solde parfois par « échec : erreur de serveur interne »

La cause du problème peut être l'un des composants répertoriés

- Point de contrôle

- Passerelle de données de réseau
- Connecteur
- Analyse de diagnostic
- Micro-service d'agent CX Cloud [devicemanager, collection]
- Centre Cisco DNA
- APIX
- Mashery
- Accès Ping
- IRONBANK
- IRONBANK GW
- Broker Big Data (BDB)

Pour afficher les journaux :

1. Connexion à la console CX Cloud Agent
2. ssh à cxcadmin et fournir le mot de passe
3. Exécuter `kubectl get pods`
4. Obtenez le nom du pod de la collection, du connecteur et de la facilité de maintenance.
5. Pour vérifier les journaux de microservice de collecte, de connexion et de maintenance

- Exécuter `kubectl logs`
- Exécuter `kubectl logs`
- Exécuter `kubectl logs`

Le tableau ci-dessous affiche l'extrait d'erreur détecté dans les journaux du microservice de collecte et du microservice de servicabilité en raison des problèmes/contraintes liés aux composants.

Scénario	Extrait de journal dans le micro-service de collecte

Le périphérique peut être accessible et pris en charge, mais les commandes à exécuter sur ce périphérique sont répertoriées en bloc dans le microservice Collection	{
	"command": "config paging disable",
	"status": "Command_Disabled",
	"commandResponse": "Command collection is disabled",
	}

Si le périphérique à analyser n'est pas accessible Se produit dans un scénario, lorsqu'il y a un problème de synchronisation entre les composants tels que le portail, l'analyse de diagnostic, le composant CX et le centre Cisco DNA	No device found with id 02eb08be-b13f-4d25-9d63-eaf4e882f71a

Scénario	Extrait de journal dans le micro-service de collecte
Si le périphérique qui doit être analysé est occupé (dans un scénario), le même périphérique fait partie d'un autre travail, et aucune demande parallèle du centre Cisco DNA n'est traitée pour le périphérique.	All requested devices are already being queried by command runner in another session. Please try other devices".
Si le périphérique n'est pas pris en charge pour l'analyse	Requested devices are not in inventory, try with other devices available in inventory
Si le périphérique tenté pour l'analyse est inaccessible	"Error occurred while executing command: show udi\nError connecting to device [Host: x.x.x.x:22] No route to host : No route to host
Si le centre Cisco DNA n'est pas joignable à partir de l'agent Cloud ou si le microservice de collecte de l'agent Cloud ne reçoit pas de réponse à une demande du gestionnaire de commandes du centre Cisco DNA	{ "command": "show version", "status": "Failed", "commandResponse": "", "errorMessage": "The command runner task failed for device %s, RequestURL: %s." }

Scénario	Extrait de journal dans le micro-service de l'agent de point de contrôle
Si des détails de planification sont manquants dans la demande d'analyse	Failed to execute request {"message":"23502: null value in column \"schedule\" violates not-null constraint"}
Si les détails du périphérique sont manquants dans la demande d'analyse	Failed to create scan policy. No valid devices in the request
Si la connexion entre le CPA et la connectivité est interrompue	Failed to execute request.
Si le périphérique qui doit être analysé n'est pas disponible dans les analyses de diagnostic	Failed to submit the request to scan. Reason = {\"message\":\"Device with Hostname=x.x.x.x' was not found\"}

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.