Validation du problème prod de Présentation de CX Cloud Agent v2.2. Veuillez ignorer cet article

Table des matières

Introduction

Ce document décrit l'agent cloud Cisco Customer Experience (CX).

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

Exigences de déploiement :

- Un de ces hyperviseurs :
  - VMware ESXi version 5.5 ou ultérieure
  - Oracle Virtual Box 5.2.30 ou version ultérieure
  - Hyperviseur Windows version 2012 à 2022
- L'hyperviseur peut héberger une machine virtuelle qui nécessite :
  - CPU 8 cœurs
  - 16 Go mémoire/RAM
  - 200 Go d’espace disque
- Pour les clients utilisant des data centers américains désignés comme région de données principale pour stocker les données du cloud CX, l'agent cloud 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 : agent.us.csco.cloud
  - Nom de domaine complet : ng.acs.agent.us.csco.cloud
  - Nom de domaine complet : cloudsso.cisco.com
  - Nom de domaine complet : api-cx.cisco.com

- Pour les clients utilisant des data centers désignés en Europe comme principale région de données pour stocker des données Cloud CX : l'agent Cloud CX doit être en mesure de se connecter aux deux serveurs présentés ici, en utilisant le nom de domaine complet (FQDN) et HTTPS sur le port TCP 443 :
  - Nom de domaine complet : agent.us.csco.cloud
  - Nom de domaine complet : agent.emea.csco.cloud
  - Nom de domaine complet : ng.acs.agent.emea.csco.cloud
  - Nom de domaine complet : cloudsso.cisco.com
  - Nom de domaine complet : api-cx.cisco.com
- Pour les clients utilisant des data centers Asie-Pacifique désignés comme région de données principale pour stocker les données du cloud CX : l'agent cloud CX doit être en mesure de se connecter aux deux serveurs présentés ici, en utilisant le nom de domaine complet (FQDN) et HTTPS sur le port TCP 443 :
  - Nom de domaine complet : agent.us.csco.cloud
  - Nom de domaine complet : agent.apjc.csco.cloud
  - Nom de domaine complet : ng.acs.agent.apjc.csco.cloud
  - Nom de domaine complet : cloudsso.cisco.com
  - Nom de domaine complet : api-cx.cisco.com
- 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 requise 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.
- Ce tableau récapitule les ports et les protocoles qui doivent être ouverts et activés pour que CX Cloud Agent fonctionne correctement :

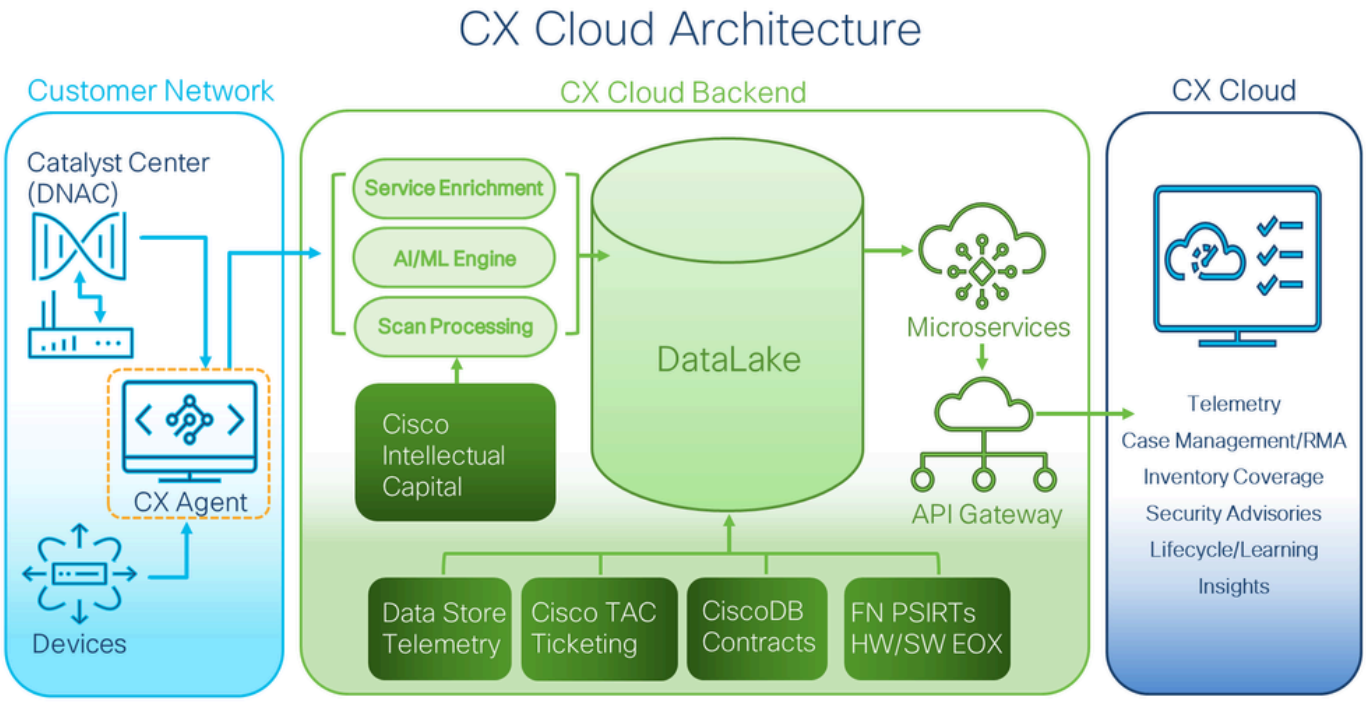
					Required for both Cisco DNA Center and Other Assets collected by CX Cloud Agent support	
					Mandatory TCP/7 Echo (ICMP) port must be combined with one of the other two ports (for device discovery process)	
CX Cloud Agent Traffic					Mandatory for other assets collected by CX Cloud Agent support	
Source	**Destination**		**Protocol**	**Port**	**Purpose**	**Type**
	IP Address	**Hostname**				
Data Collection and Transfer						
Agent IP	Dynamic IPs Cisco DNA Center Server IP	For All regions, FQDN: cloudsso.cisco.com FQDN: api-cx.cisco.com QDN: agent.us.csco.cloud DNAC Servers Additionally, For Americas region, FQDN: ng.acs.agent.us.csco.cloud For EMEA region, FQDN: agent.emea.csco.cloud, and FQDN: ng.acs.agent.emea.csco.cloud For APJC region, FQDN: agent.apjc.csco.cloud, and FQDN: ng.acs.agent.apjc.csco.cloud	HTTPS	TCP/ 443	Data collection via DNAC servers, Data transfer to CX Cloud, including upgrade functionality	Outbound connection to DNAC servers + Outbound to Cisco AWS regional data centers
Agent IP	Customer Device		SNMP	UDP/161	Collect OIDs and MIBs for other assets collected by CX Cloud Agent	Outbound to LAN
Devices	Agent IP		SYSLOG	UDP/514	Stream Syslog messages from Device to Agent	Inbound from LAN
Agent IP	Customer Device		SSH	TCP/22	Collect CLI commands	Outbound to LAN
Agent IP	Customer Device		Echo	TCP/7	Check the device reachability	Outbound to LAN
Agent IP	Customer Device		Telnet	TCP/23	Collect CLI commands	Outbound to LAN
Agent Administration Access						
Support VM	Agent IP		SSH	TCP/22	Agent Maintenance	Inbound from LAN

Informations générales

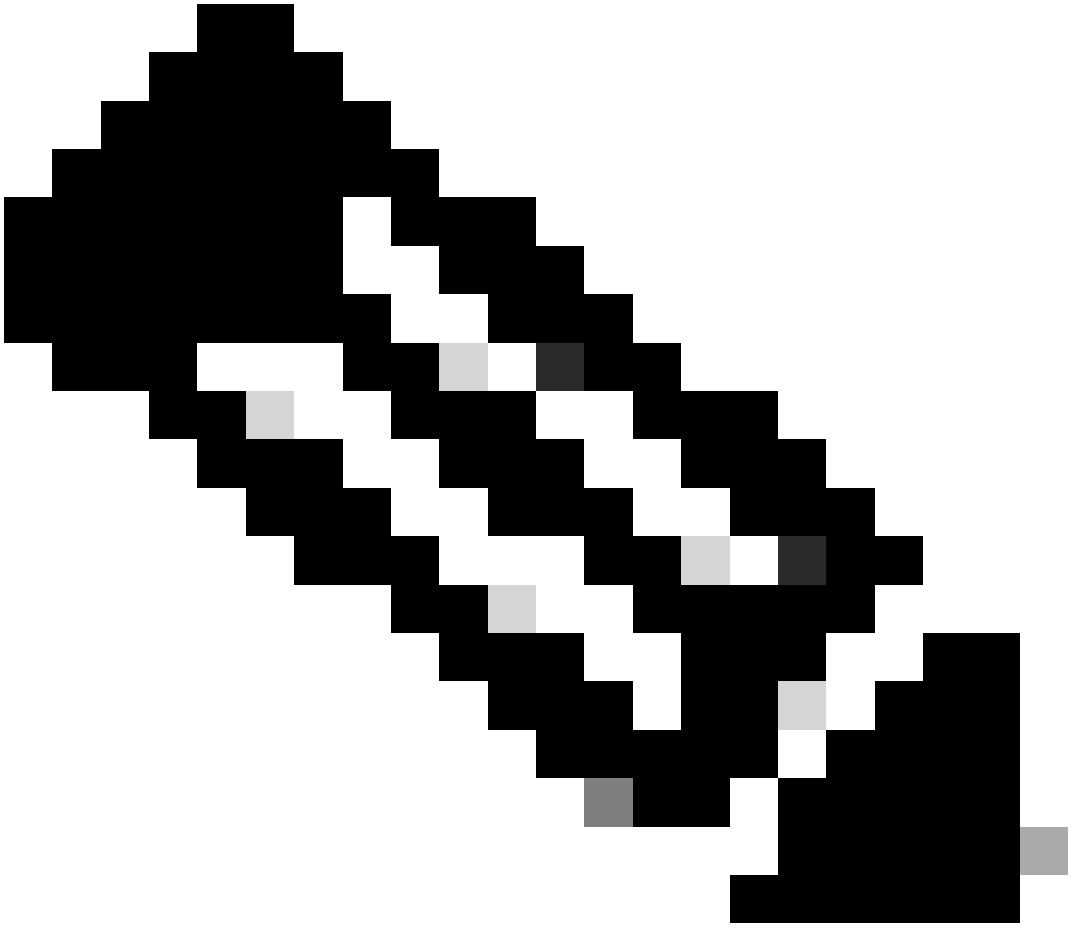
Cisco (CX) Cloud Agent est une plate-forme hautement évolutive qui collecte des données de télémétrie à partir des périphériques réseau des clients afin de fournir des informations exploitables aux clients. CX Cloud Agent permet la transformation de l'intelligence artificielle (IA)/apprentissage automatique (ML) des données de configuration en cours en informations

proactives et prédictives affichées dans CX Cloud.

Ce guide est spécifique à CX Cloud Agent v2.2 et ultérieures. Reportez-vous à la page Cisco CX Cloud Agent pour accéder aux versions antérieures.



Architecture cloud CX



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

- 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 (Domain Name Service) libres doivent être disponibles.
- Seul IPv4 est pris en charge.
- Les versions certifiées de Cisco DNA Center à noeud unique et cluster haute disponibilité (HA) sont les versions 2.1.2.x à 2.2.3.x, 2.3.3.x, 2.3.5.x et Cisco Catalyst Center Virtual Appliance et Cisco DNA Center Virtual Appliance.
- Si le réseau dispose d'une interception SSL, indiquez l'adresse IP de CX Cloud Agent.
- 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 peuvent pas être utilisées.

Accès aux domaines critiques

Pour démarrer le parcours vers le cloud CX, les utilisateurs doivent avoir accès à ces domaines. Utilisez uniquement les noms d'hôte fournis ; n'utilisez pas d'adresses IP statiques.

Domaines spécifiques au portail CX Cloud Agent

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

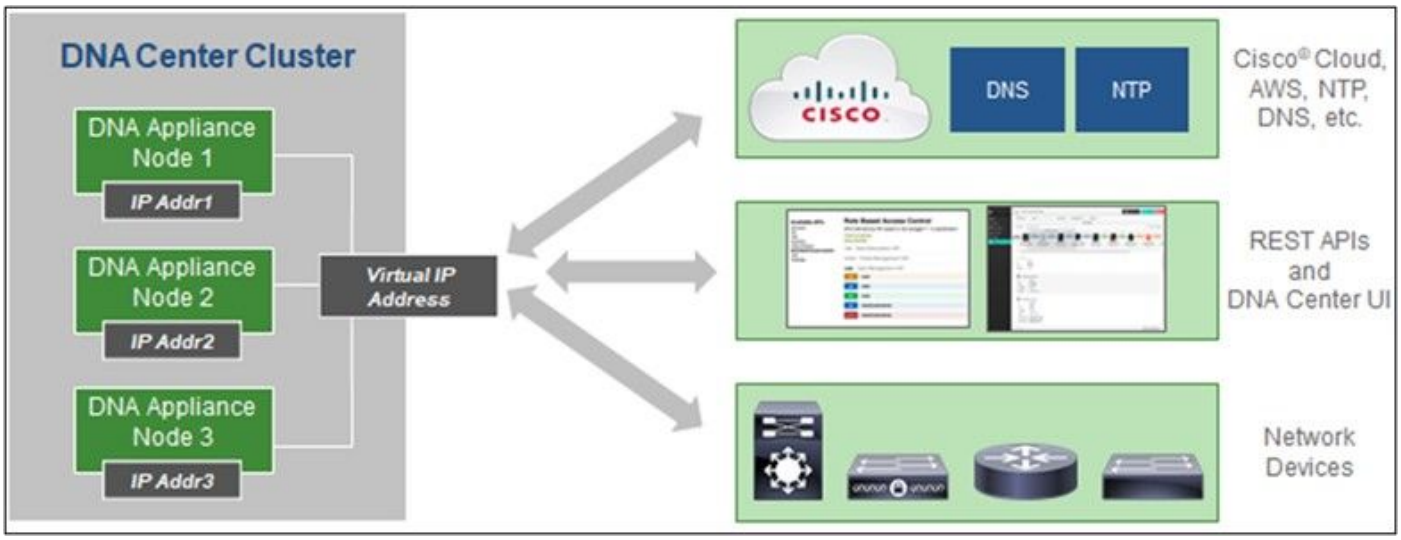
Domaines spécifiques à CX Cloud Agent OVA

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

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

Version prise en charge de Cisco DNA Center

Les versions 2.1.2.x à 2.2.3.x, 2.1.2.x, 2.3.3.x, 2.3.5.x, Cisco Catalyst Center Virtual Appliance et Cisco DNA Center Virtual Appliance sont prises en charge pour les noeuds uniques et les clusters haute disponibilité Cisco DNA Center.



Grappe haute disponibilité multi-nœuds du centre Cisco DNA

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

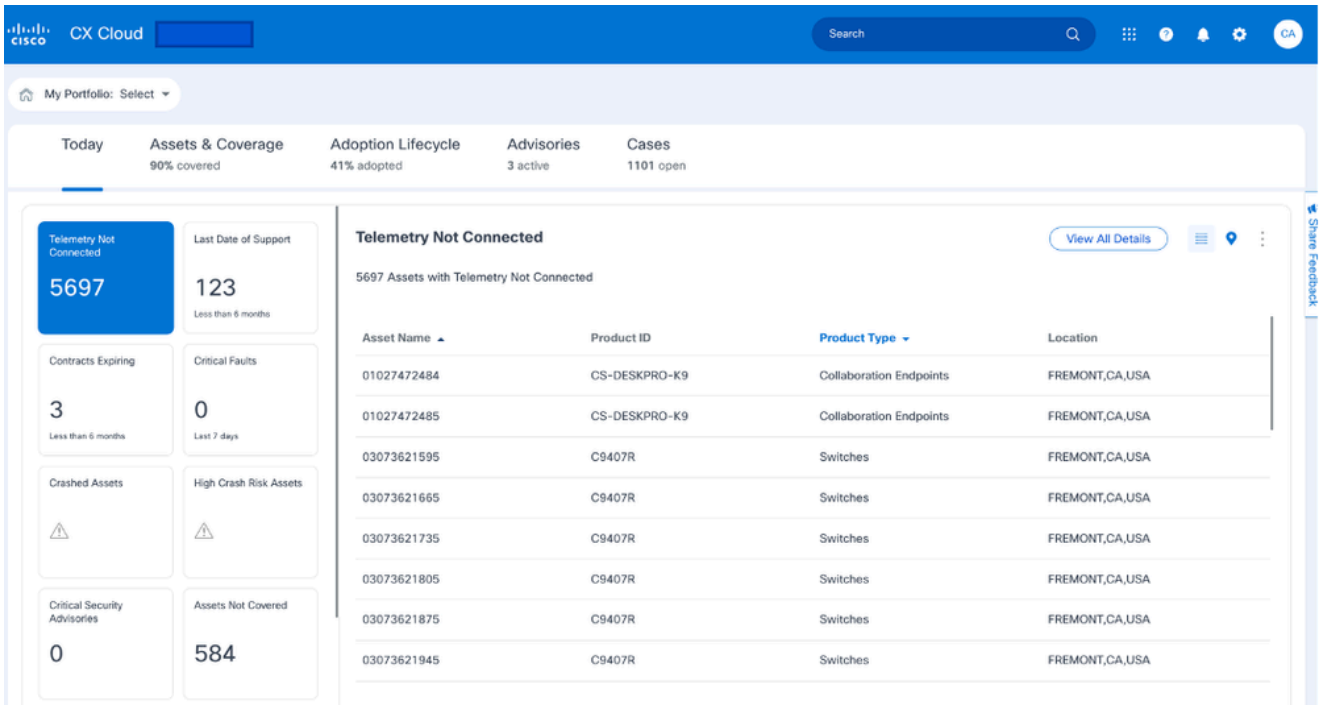
Liste des produits pris en charge

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

Connexion des sources de données

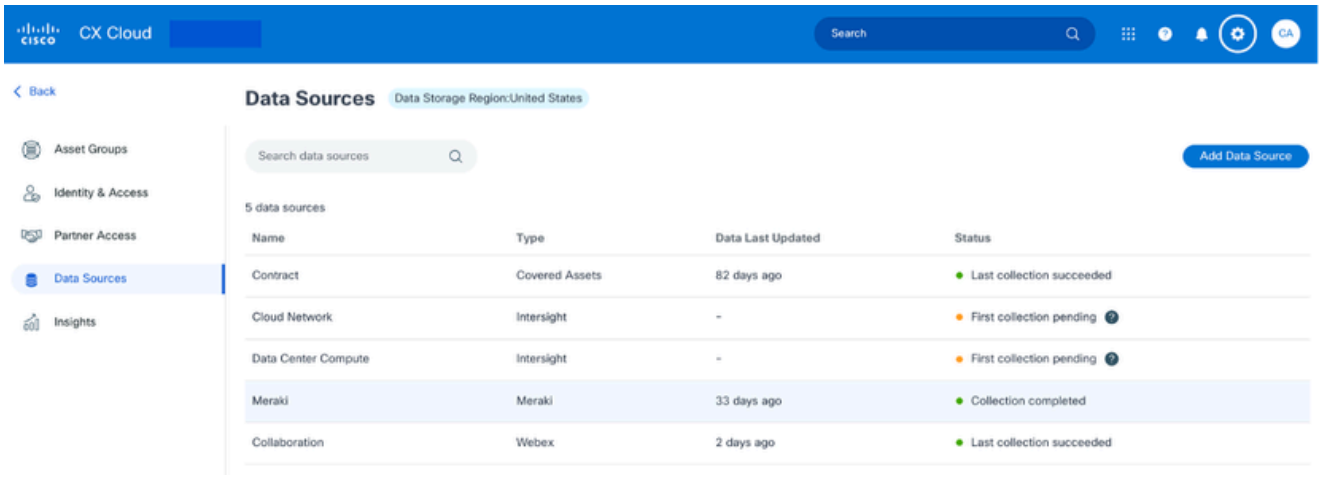
Pour connecter des sources de données :

1. Cliquez sur cx.cisco.com pour vous connecter à CX Cloud.



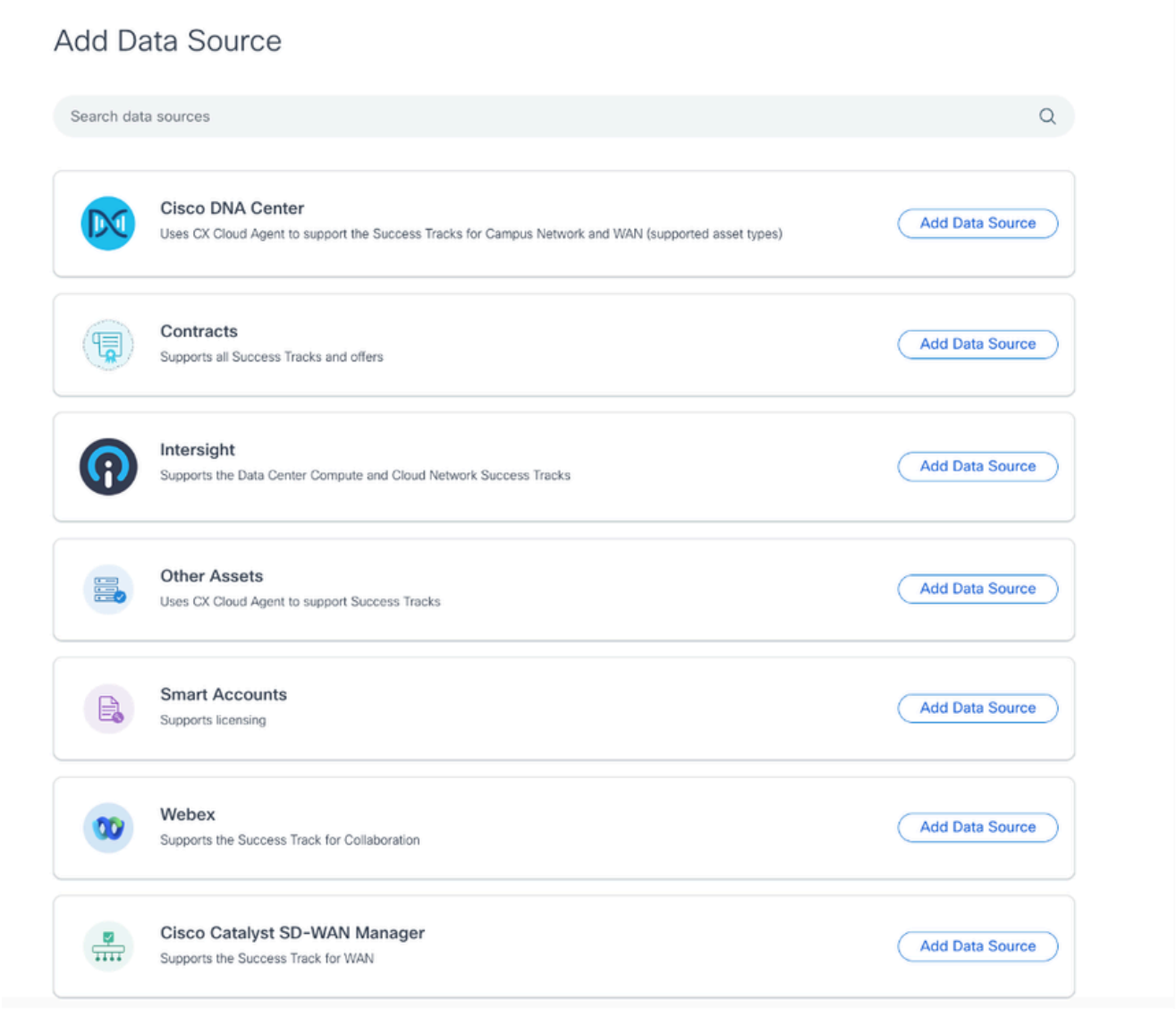
Page d'accueil de CX Cloud

2. Sélectionnez l'icône Admin Center. La fenêtre Sources de données s'ouvre.



Source de données

3. Cliquez sur Ajouter une source de données. La fenêtre Ajouter une source de données s'affiche. Les options affichées peuvent varier en fonction des abonnements des clients.



Ajouter une source de données

4. Cliquez sur Ajouter une source de données pour sélectionner la source de données applicable. Si CX Cloud Agent n'a pas été configuré précédemment, la fenêtre Setting Up CX Cloud Agent s'ouvre et vous devez y effectuer la configuration. Si la configuration est terminée, la connexion continue. Reportez-vous à l'une de ces sections pour continuer :

Configuration de CX Cloud Agent

Ajout de Cisco DNA Center comme source de données

Ajout d'autres ressources comme sources de données

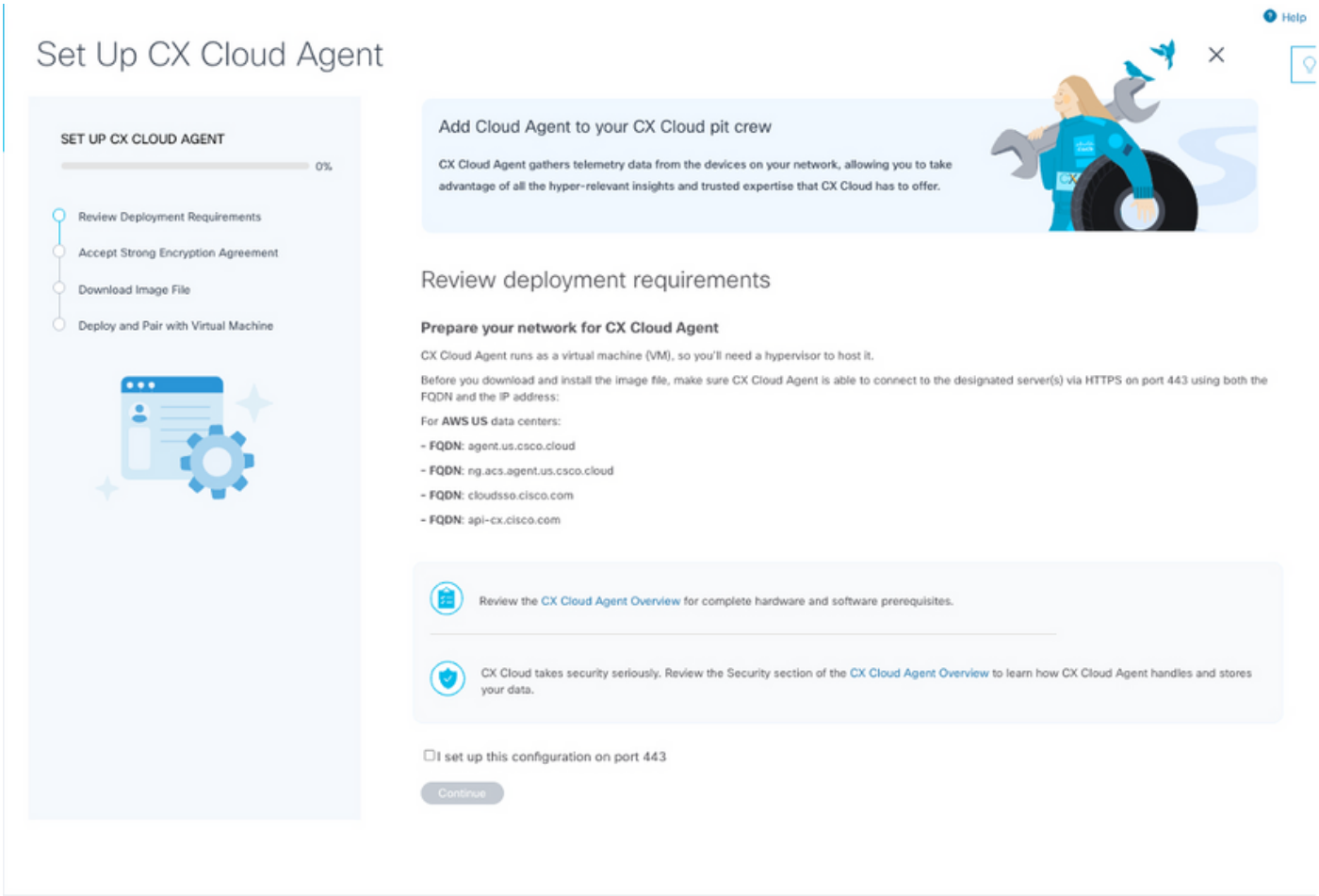
Remarque : l'option Autres ressources n'est disponible que si la connectivité des périphériques directs n'a pas été configurée précédemment.

Configuration de CX Cloud Agent

La configuration de CX Cloud Agent est demandée lors de la connexion de sources de données si

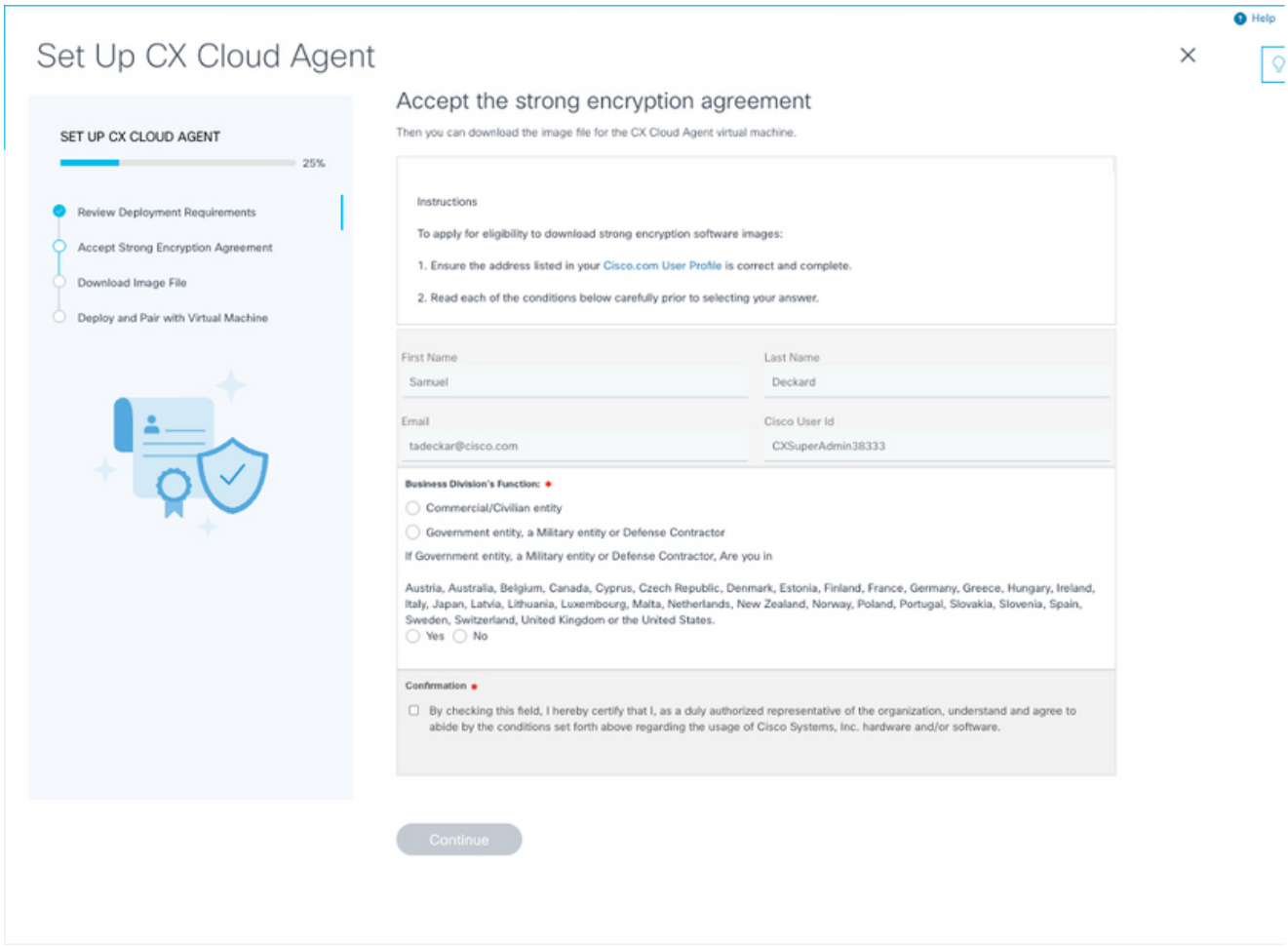
elle n'a pas déjà été effectuée.

Pour configurer CX Cloud Agent :



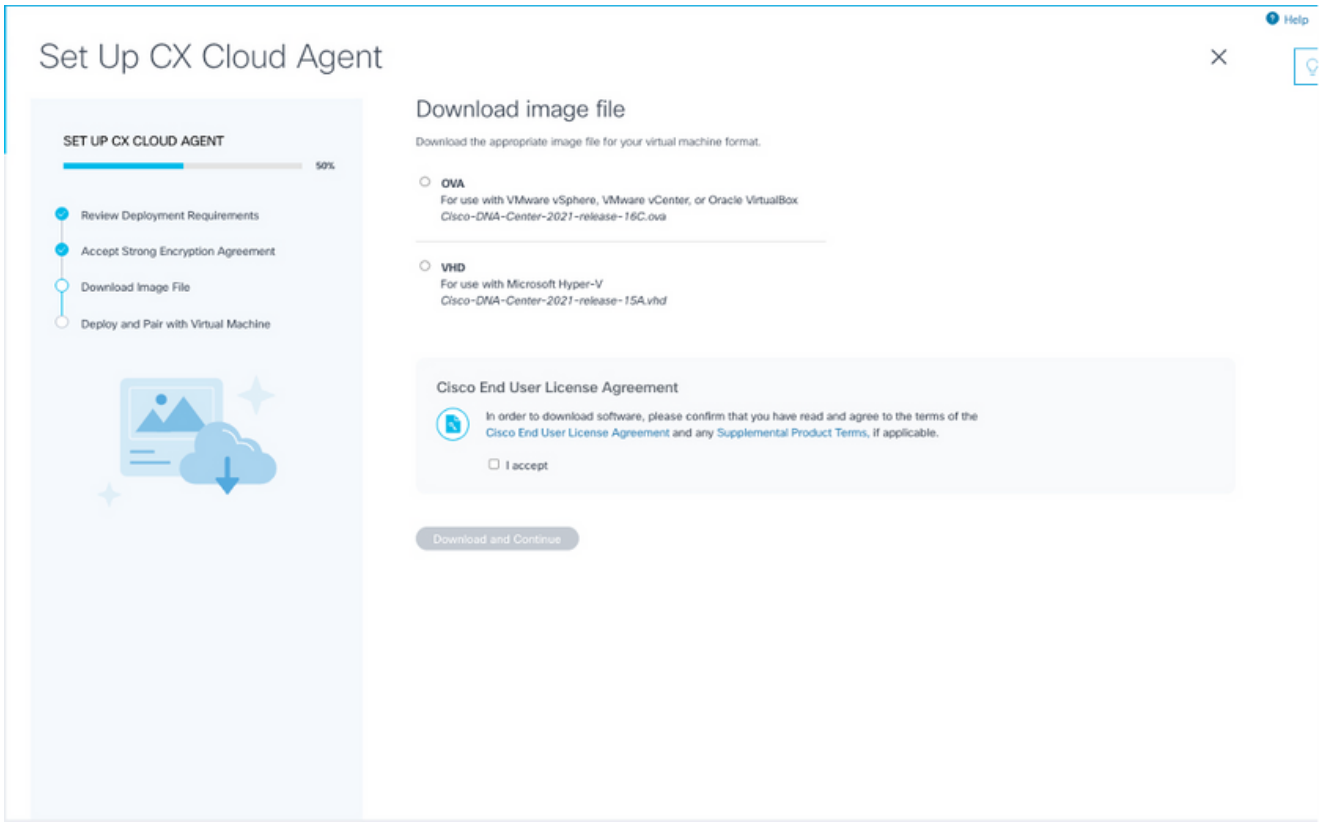
Examen des exigences de déploiement

1. Vérifiez les exigences de déploiement et activez la case à cocher I set up this configuration on port 443.
2. Cliquez sur Continue. La fenêtre Set Up CX Cloud Agent - Accept the strong encryption agreement s'affiche.



Contrat de chiffrement

3. Vérifiez les informations pré-remplies dans les champs Prénom, Nom, E-mail et ID d'utilisateur Cisco.
4. Sélectionnez la fonction de la division commerciale appropriée.
5. Cochez la case Confirmation pour accepter les conditions d’utilisation.
6. Cliquez sur Continue. La fenêtre Configurer CX Cloud Agent - Télécharger le fichier image s'affiche.



Télécharger l'image

7. Sélectionnez le format de fichier approprié pour télécharger le fichier image requis pour l'installation.
8. Cochez la case J'accepte pour accepter le Contrat de licence de l'utilisateur final Cisco.
9. Cliquez sur Download and Continue. La fenêtre Set Up CX Cloud Agent - Deploy and pair with your virtual machine s'affiche.
10. Référez-vous à Configuration du réseau pour obtenir le code d'appariement requis dans la section suivante.

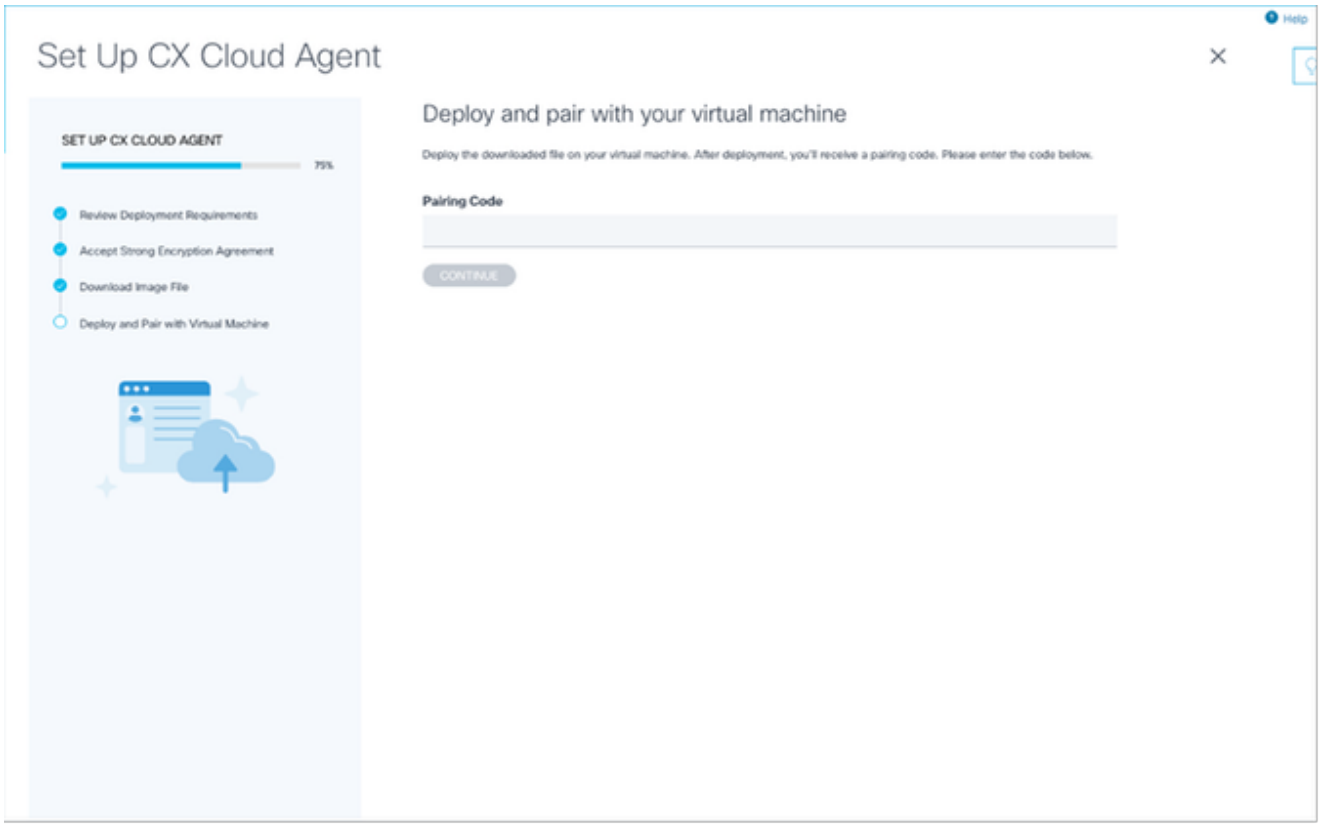
Connexion de l'agent CX Cloud au CX Cloud

La connexion de CX Cloud Agent à CX Cloud est nécessaire pour que la collecte de données télémétriques puisse commencer, afin que les informations de l'interface utilisateur puissent être mises à jour pour afficher les ressources et les informations actuelles. Cette section fournit des détails pour compléter les directives de connexion et de dépannage.

Pour connecter CX Cloud Agent à CX Cloud :

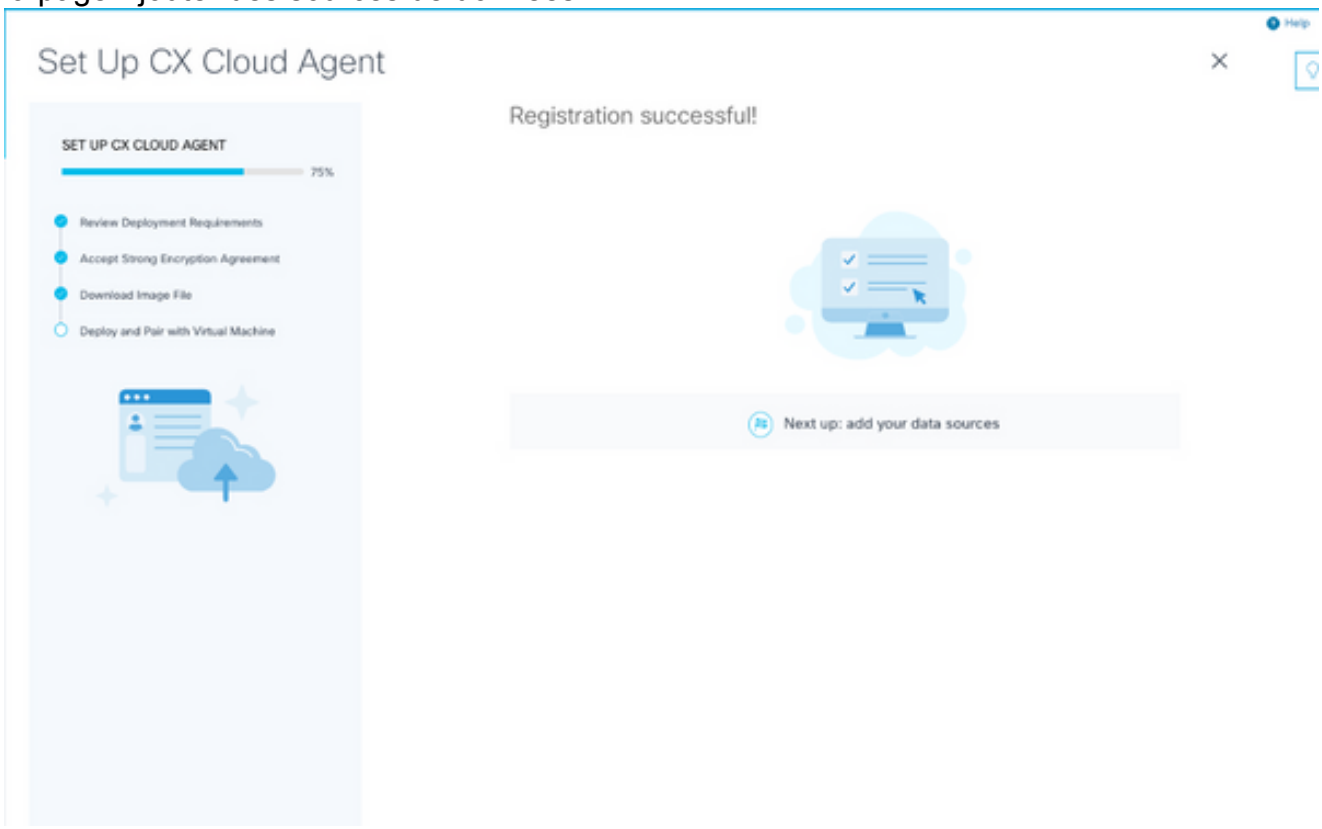
1. Entrez le code d'appariement fourni dans la boîte de dialogue de la console ou dans l'interface de ligne de commande (CLI) de la machine virtuelle connectée via l'agent.

Remarque : le code d'appariement est reçu après le déploiement du fichier OVA téléchargé.



Code de jumelage

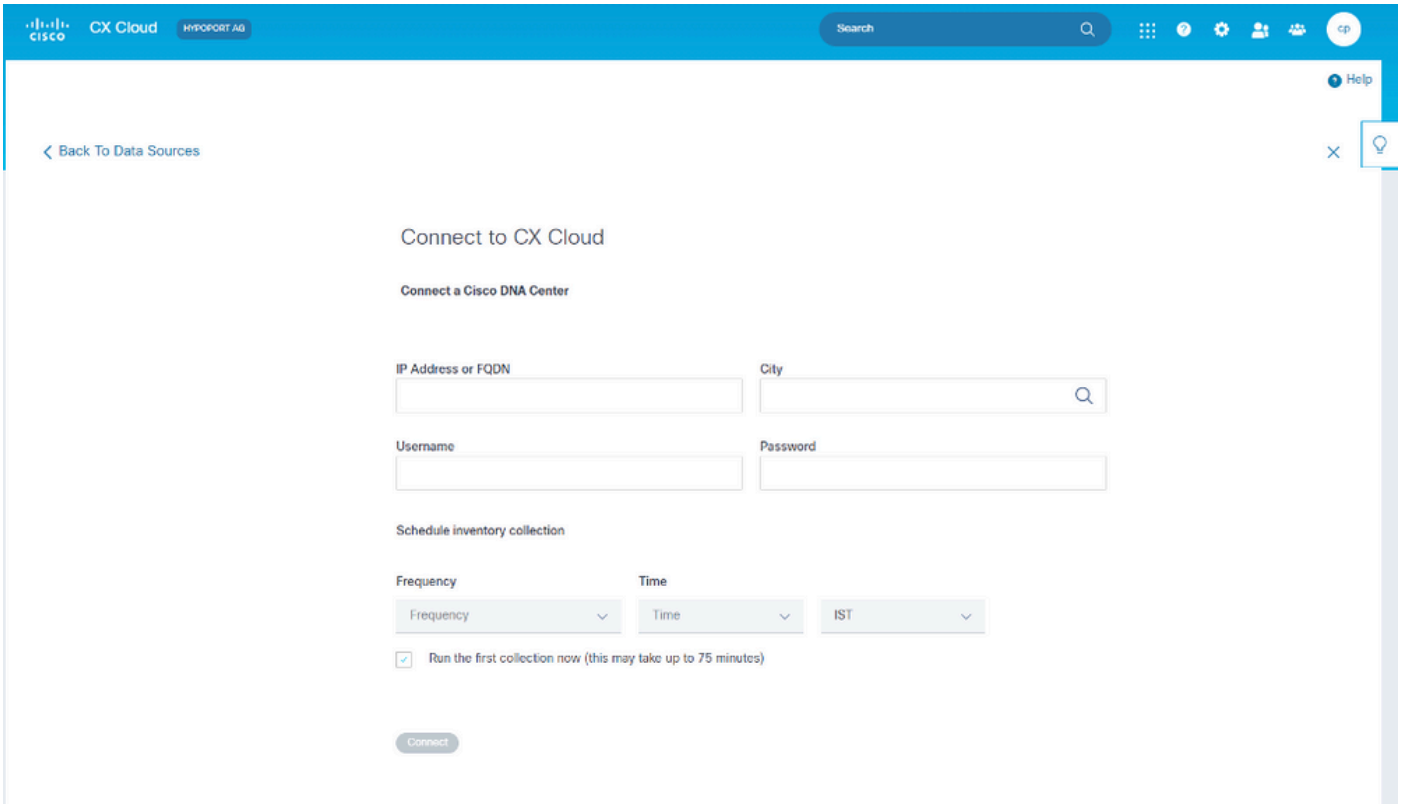
2. Cliquez sur Continue pour enregistrer l'agent cloud CX. La fenêtre Configurer CX Cloud Agent - Enregistrement réussi s'ouvre brièvement avant de naviguer automatiquement vers la page Ajouter des sources de données.



Inscription réussie

Ajout de Cisco DNA Center comme source de données

Lorsque Cisco DNA Center est sélectionné dans la fenêtre de connexion des sources de données (reportez-vous à l'image Connecter les sources de données dans la section Connexion des sources de données), cette fenêtre s'ouvre :



Connexion au cloud CX

Pour ajouter Cisco DNA Center en tant que source de données :

1. Saisissez l'adresse IP Cisco DNA Center ou l'adresse IP virtuelle ou le nom de domaine complet, la ville (emplacement de Cisco DNA Center), le nom d'utilisateur et le mot de passe.

   Remarque : n'utilisez pas une adresse IP de noeud de cluster individuelle.

2. Planifiez une collecte d'inventaire en saisissant une fréquence et une heure pour indiquer la fréquence à laquelle CX Cloud Agent peut effectuer des analyses du réseau et mettre à jour les informations sur les périphériques connectés.

   Remarque : la première collecte d'inventaire peut prendre jusqu'à 75 minutes.

3. Cliquez sur Connect. Une confirmation s'affiche avec l'adresse IP Cisco DNA Center.

Connexion réussie

4. Cliquez sur Add Another Cisco DNA Center, Done ou Back to Data Sources pour revenir à la fenêtre Data Sources.

Ajout d'autres ressources comme sources de données

Aperçu

La collecte de données télémétriques a été étendue aux périphériques non gérés par Cisco DNA Center, ce qui permet aux clients d'afficher et d'interagir avec des données et des analyses issues de la télémétrie pour un plus large éventail de périphériques. Après la configuration initiale de CX Cloud Agent, les utilisateurs ont la possibilité de configurer CX Cloud Agent pour se connecter à 20 centres Cisco DNA supplémentaires au sein de l'infrastructure surveillée par CX Cloud. Les utilisateurs peuvent également connecter CX Cloud Agent directement à d'autres ressources matérielles de leur environnement, jusqu'à 10 000 périphériques connectés directement.

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

Remarque :
Vous pouvez utiliser le fichier d'amorce ou la plage IP. Il n'est pas possible de modifier cette sélection après la configuration initiale.

Remarque :

Un fichier d'amorçage initial peut être remplacé par un autre fichier d'amorçage, tandis qu'une plage IP initiale peut être modifiée en une nouvelle plage IP.

Lorsque Autres immobilisations est sélectionné dans la fenêtre de connexion des sources de données, cette fenêtre s'ouvre :

Configuration de la connexion au cloud CX

Pour ajouter d'autres ressources en tant que sources de données :

- Téléchargez un fichier de départ à l'aide d'un modèle de fichier de départ.
- Indiquez 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 Cloud Agent prend en charge SNMP2c et SNMP V3 et l'une ou les deux versions peuvent être configurées. Les mêmes informations, décrites ensuite 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, à l'exception des périphériques hérités plus anciens qui ne prennent pas en charge SNMPv3. Si les deux versions de SNMP sont configurées par l'utilisateur, CX Cloud Agent peut, par défaut, tenter de communiquer avec chaque périphérique respectif à l'aide de SNMPv3 et

revenir 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 peut 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 (noms d'utilisateur et mots de passe) envoyées via Telnet ne sont pas chiffrées et sont donc vulnérables aux compromissions, en l'absence d'une sécurité supplémentaire.

Ajouter des périphériques à l'aide d'un fichier de démarrage

À propos du fichier de démarrage

Un fichier d'amorçage est un fichier de valeurs séparées par des virgules (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 peut être collectée par CX Cloud Agent. 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.

CX Cloud Agent peut tenter de se connecter aux périphériques, mais ne peut pas les traiter pour les afficher dans les pages Ressources dans les cas où il ne peut pas 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.

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. Cliquez sur le lien fourni pour afficher un fichier d'amorçage au format PDF. Ce fichier PDF est fourni à titre de référence uniquement et peut être utilisé pour créer un fichier de départ qui doit être enregistré au format .csv.

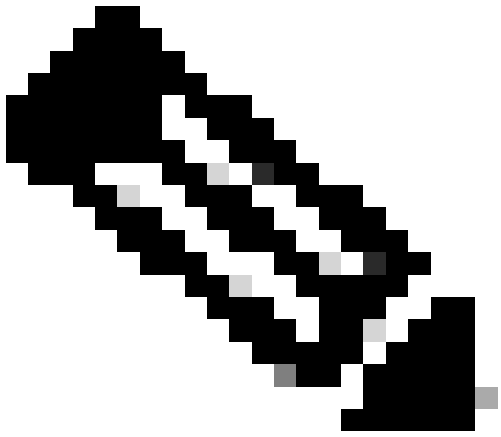
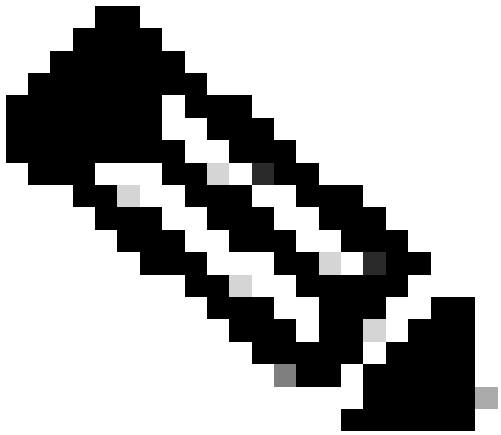
Cliquez sur ce lien pour afficher un fichier d'amorçage qui peut être utilisé pour créer un fichier d'amorçage au format .csv.

Remarque : ce fichier PDF est fourni à titre de référence uniquement et peut être utilisé pour créer un fichier d'amorçage qui doit être enregistré au format .csv.

Ce tableau 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 CX Cloud Agent 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	snmpv3UserName : obligatoire si col#=3 est sélectionné comme 'snmpv3'	Si SNMPv3 est sélectionné pour communiquer avec un périphérique spécifique, le nom d'utilisateur de connexion correspondant doit être fourni.
E	snmpv3AuthAlgorithm : les valeurs peuvent être MD5 ou SHA	Le protocole SNMPv3 autorise l'authentification via l'algorithme MD5 ou SHA. Si le périphérique est configuré avec l'authentification sécurisée, l'algorithme d'authentification correspondant doit être fourni.

Colonne du fichier de démarrage	En-tête / Identificateur de colonne	Objet de la colonne
		 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 peuvent être DES , 3DES	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. 

Colonne du fichier de démarrage	En-tête / Identificateur de colonne	Objet de la colonne
		Remarque : les clés 56 bits utilisées par DES sont considérées comme trop courtes pour fournir une sécurité cryptographique, et 3DES peut être utilisé sur tous les périphériques qui le 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 fourni pour la connexion du périphérique.
I	snmpv3EngineId : engineID, ID unique représentant le périphérique, spécifier l'ID du 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 CX Cloud Agent. 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 est conçue pour interagir directement avec le périphérique. CX Cloud 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.

Colonne du fichier de démarrage	En-tête / Identificateur de colonne	Objet de la colonne
L	cliUser : nom d'utilisateur CLI (le 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	cliPassword : mot de passe utilisateur CLI (le 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 mot de passe 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.
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

Limitations du traitement de télémétrie pour les périphériques

Il existe des limitations lors du 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 du cloud CX. Les limites de l'instrumentation des dispositifs empêchent le traitement de cette télémétrie.

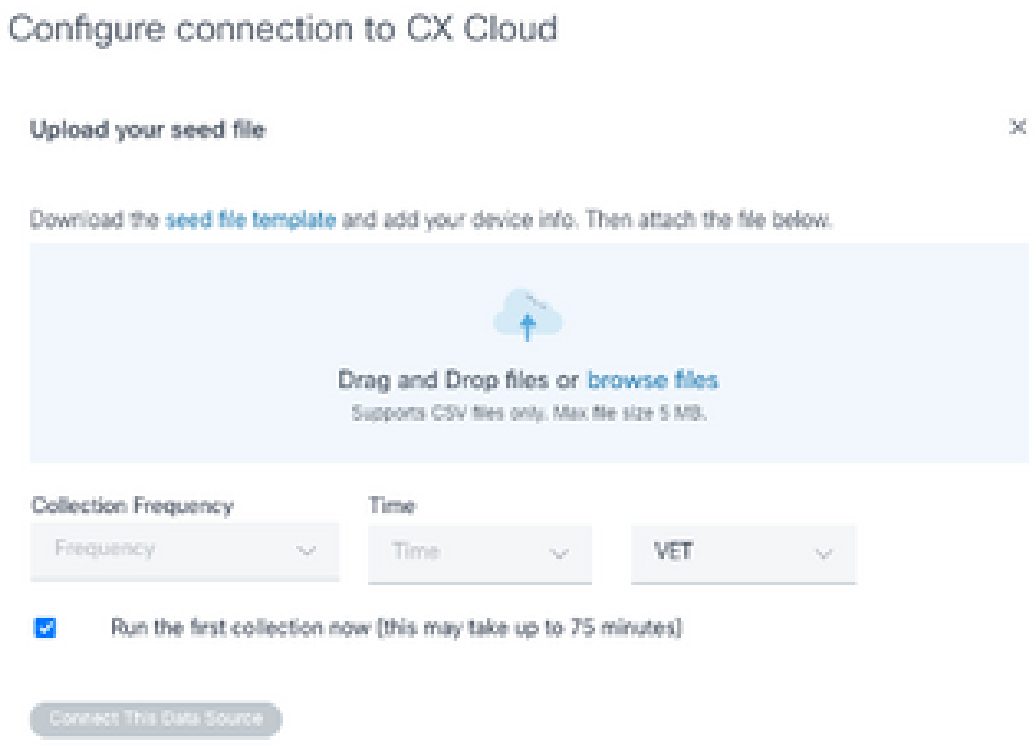
- Les attributs de télémétrie peuvent être inexacts ou manquants dans la page des ressources cloud CX pour les périphériques qui ne font pas partie du suivi de réussite du campus.
- Si un périphérique du fichier de départ ou des collections de plages IP fait également partie de l'inventaire Cisco DNA Center, le périphérique n'est signalé qu'une seule fois pour l'entrée Cisco DNA Center. L'entrée de plage IP/fichier d'amorce n'est pas collectée ou traitée pour éviter la duplication.

Ajouter des périphériques à l'aide d'un nouveau fichier de démarrage

Pour ajouter des périphériques à l'aide d'un nouveau fichier de départ :

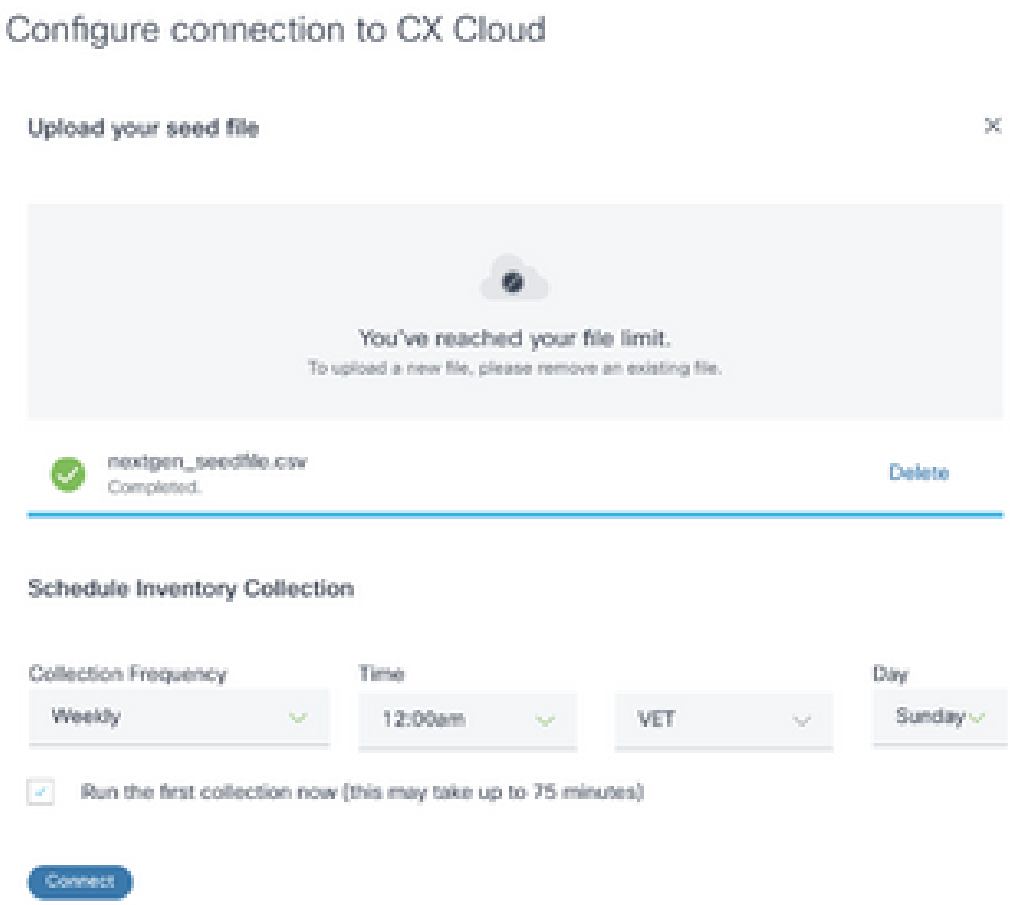
1. Téléchargez le modèle de fichier d'amorçage (PDF) à l'aide du lien intégré dans ce document (reportez-vous à A propos du fichier d'amorçage) ou via un lien dans la fenêtre Configurer la connexion au cloud CX.

Remarque : le lien de la fenêtre Configurer la connexion au cloud CX n'est plus disponible une fois le fichier d'amorçage initial téléchargé.



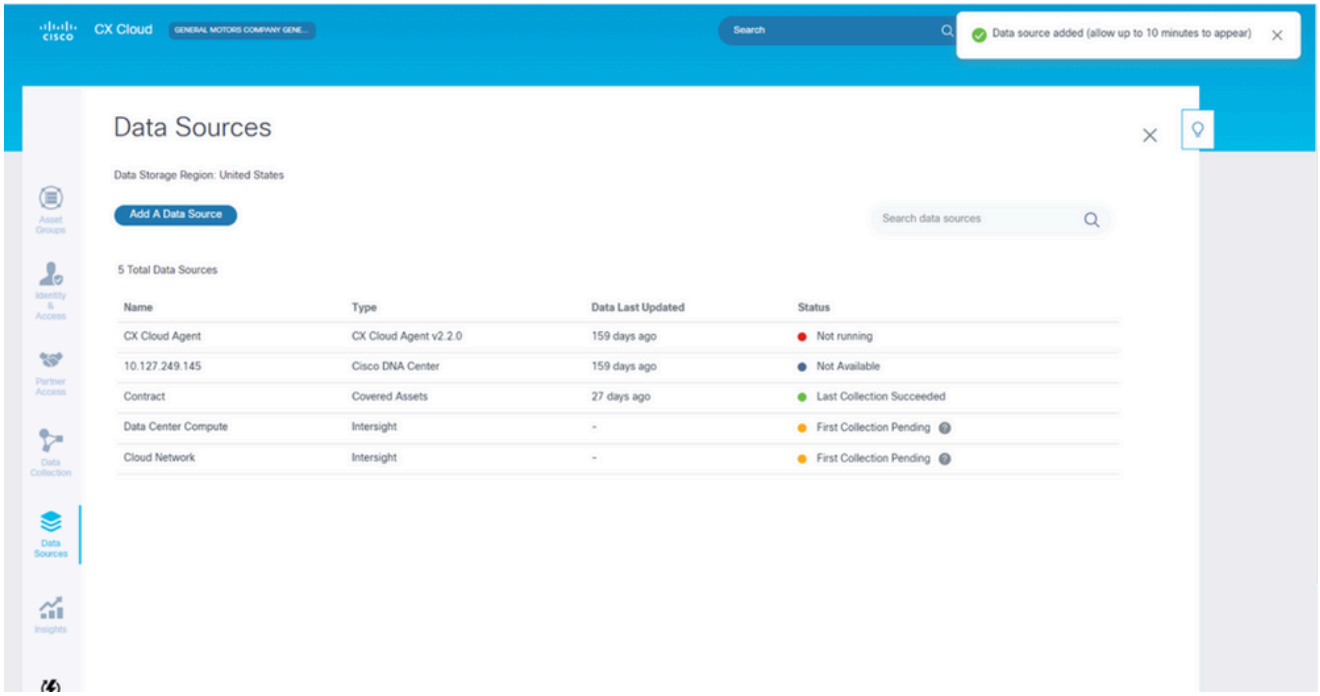
Fenêtre Configurer la connexion au cloud CX

2. Ouvrez une feuille de calcul Excel (ou toute autre feuille de calcul préférée) et entrez les en-têtes comme indiqué dans le modèle.
3. Saisissez les données manuellement ou importez-les dans le fichier.
4. Une fois terminé, enregistrez le modèle en tant que fichier .csv pour importer le fichier dans CX Cloud Agent.



Fenêtre Charger le fichier d'amorçage

5. Dans la fenêtre Upload your seed file, faites glisser et déposez le fichier .csv nouvellement créé ou cliquez sur browse files and navigate to the .csv file.
6. Renseignez la section Planifier la collecte d'inventaire et cliquez sur Connexion. La fenêtre Sources de données s'ouvre et affiche un message de confirmation.
7. 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.



Message de confirmation

Ajout de périphériques à l'aide d'un fichier de démarrage modifié

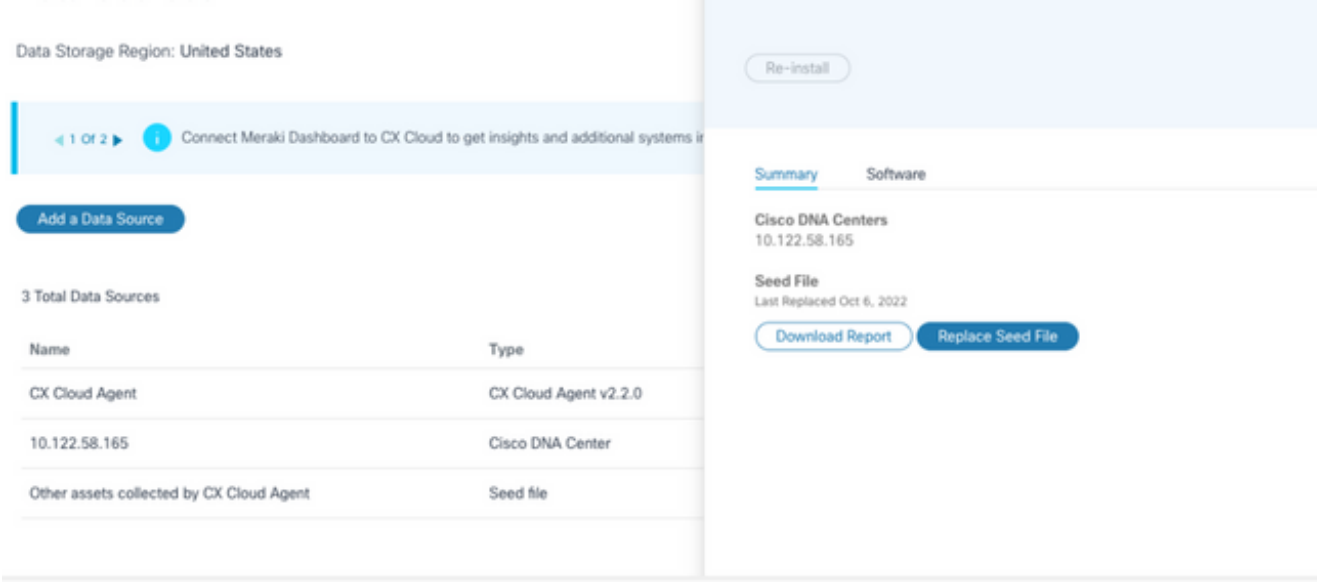
Pour ajouter, modifier ou supprimer des périphériques à l'aide du fichier de départ actuel :

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

Remarque : pour ajouter des ressources 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.

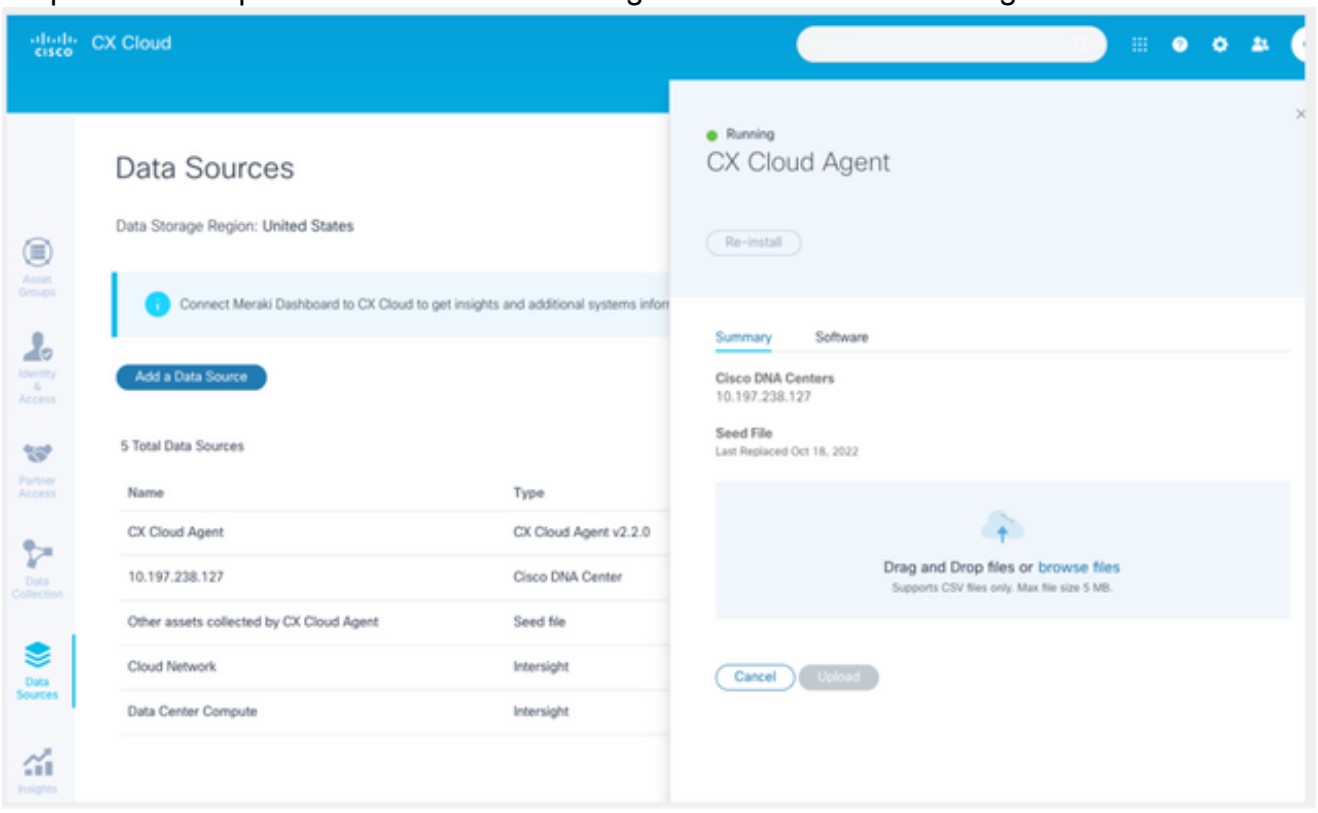
---

2. Dans la page Sources de données, sélectionnez une source de données qui a un type d'agent cloud CX. Une fenêtre de détails s'ouvre avec les onglets Summary et Software.



Fenêtre Détails

3. Cliquez sur Télécharger le rapport pour générer un rapport sur toutes les ressources pour la source de données sélectionnée. Le rapport fournit des informations sur l'adresse IP, le numéro de série, l'accessibilité, le type de commande, l'état de la commande et l'erreur de commande du périphérique, le cas échéant.
4. Cliquez sur Remplacer le fichier de démarrage. La fenêtre CX Cloud Agent s'ouvre.



Fenêtre CX Cloud Agent

5. Faites glisser et déposez le fichier de départ modifié dans la fenêtre ou accédez au fichier et ajoutez-le dans la fenêtre.
6. Cliquez sur Upload (charger).

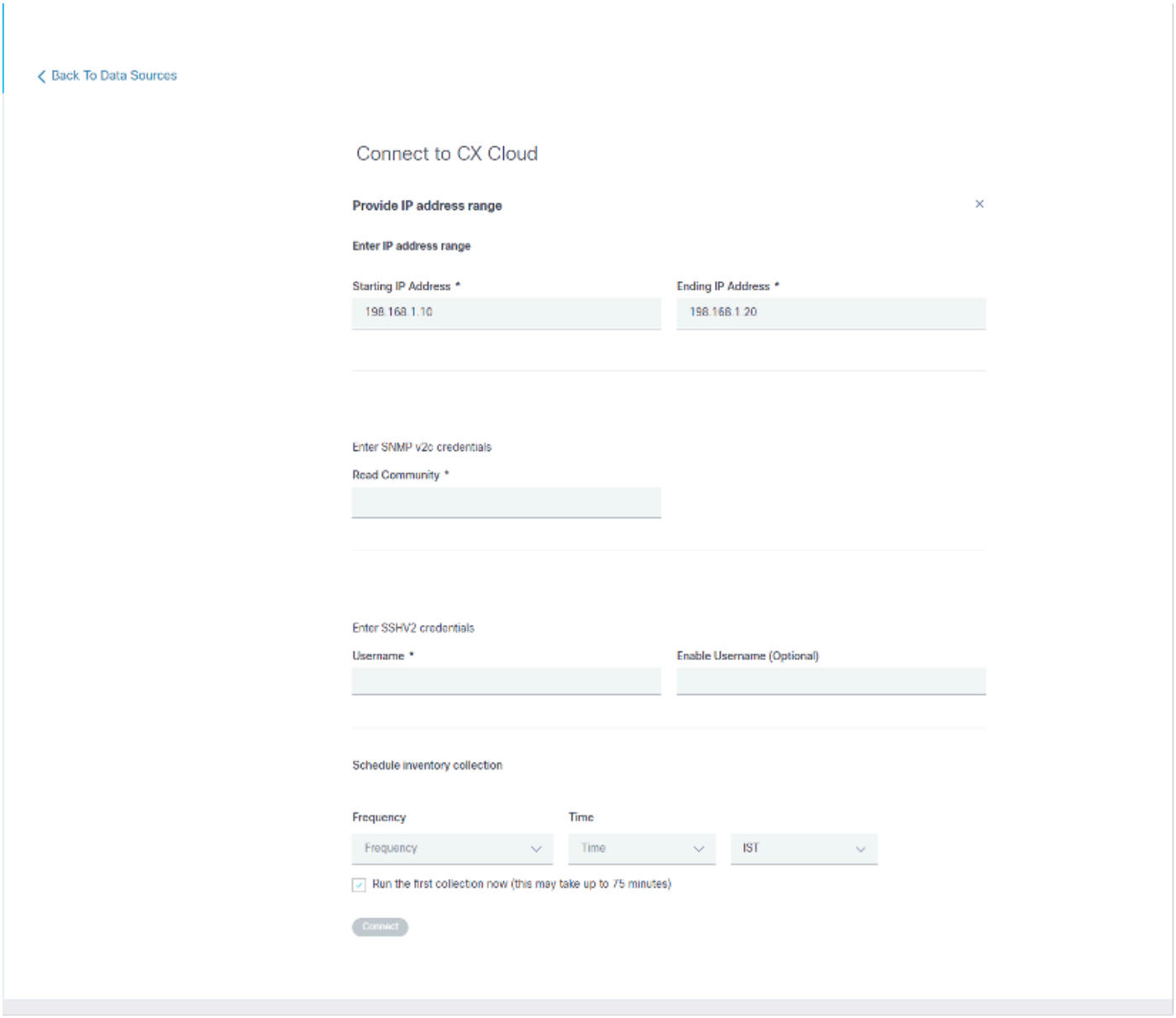
Ajout de périphériques utilisant des plages IP

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 Cloud 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 au cours de la configuration, CX Cloud Agent 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 CX Cloud Agent d'utiliser les informations d'identification fournies par l'utilisateur avec toute adresse IP. Par 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

CX Cloud Agent peut tenter de se connecter aux périphériques mais ne peut pas traiter chacun d'eux pour les afficher dans la vue Ressources dans les cas où il ne peut pas 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 périphériques à la demande afin d'inclure tout périphérique nouvellement ajouté à l'inventaire de collecte de CX Cloud Agent.



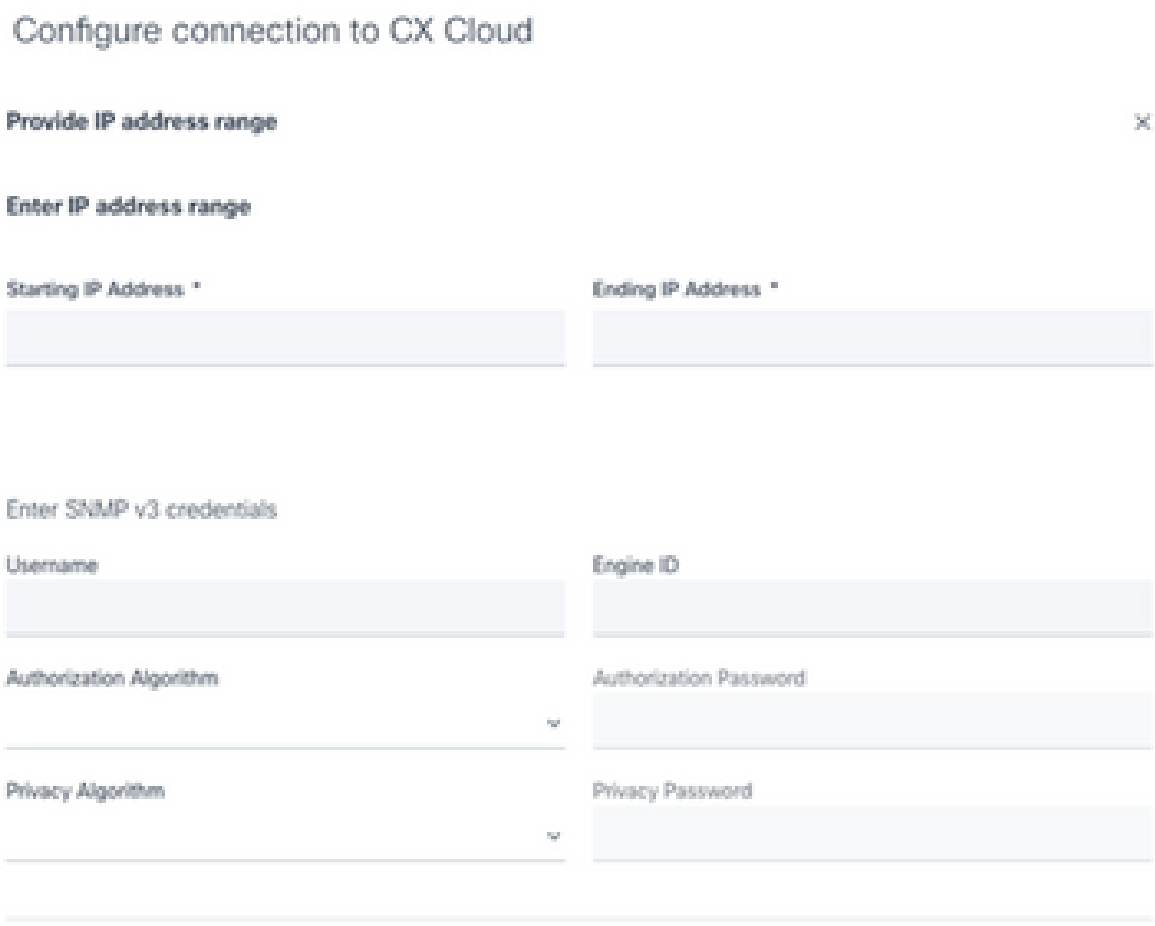
Fenêtre Plage d'adresses IP initiales

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 Cloud 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 peut s'assurer que tous les protocoles pertinents dans la plage IP, ainsi que les versions SSH et les informations d'identification Telnet sont valides ou que les connexions peuvent échouer.

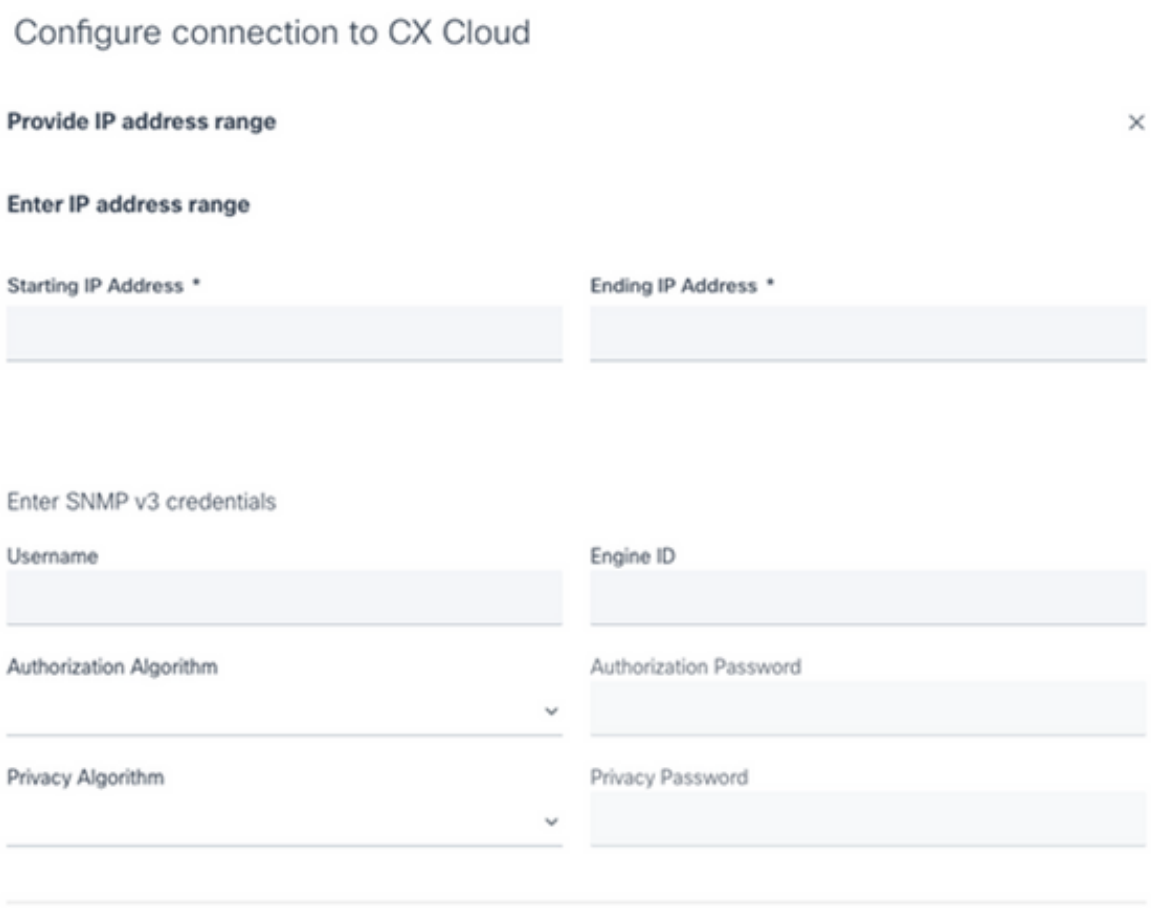
Pour ajouter des périphériques à l'aide de la plage IP :

1. Dans la fenêtre Configurer la connexion au cloud CX, sélectionnez l'option Fournir une plage d'adresses IP.

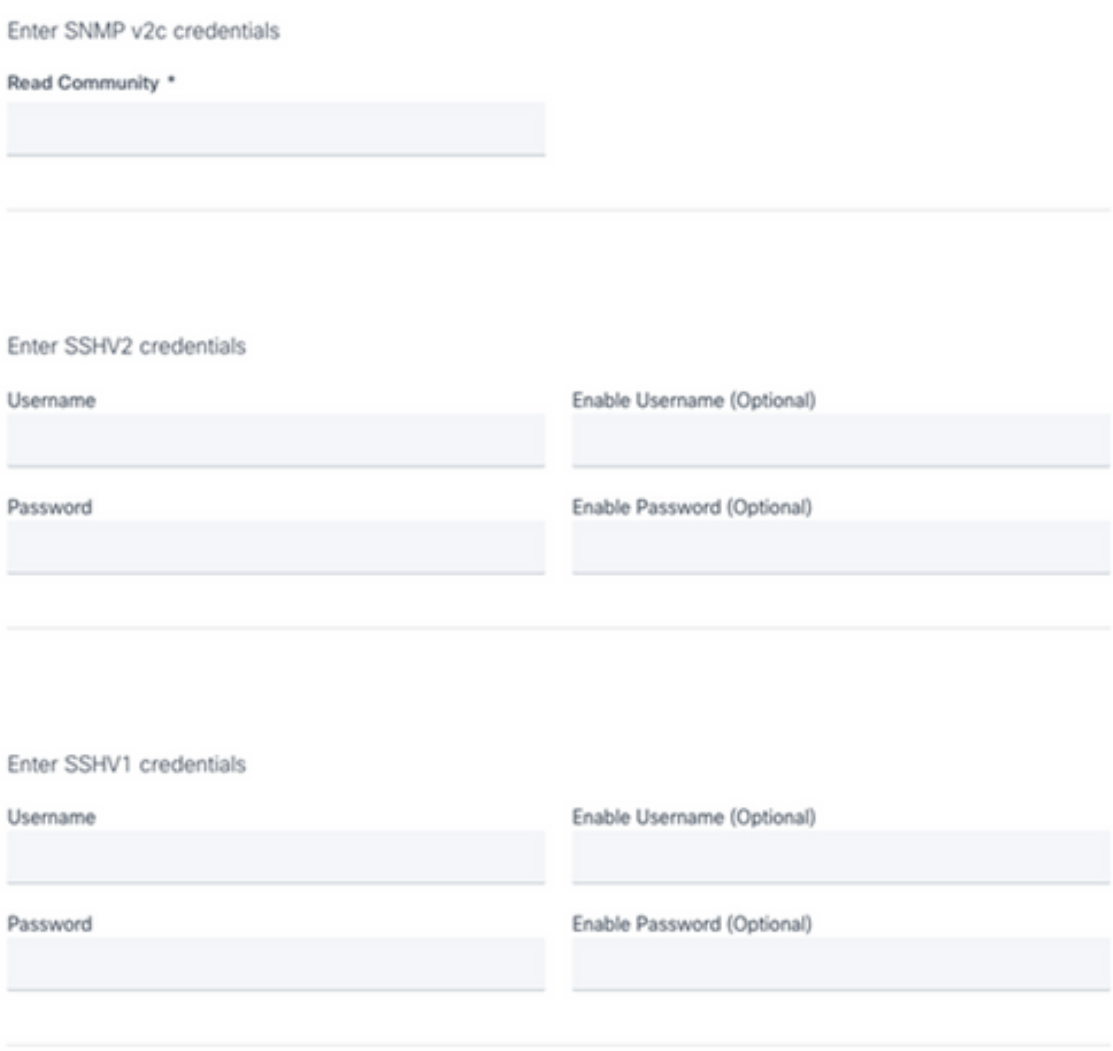


Formulaire d'ajout de périphériques utilisant des adresses IP

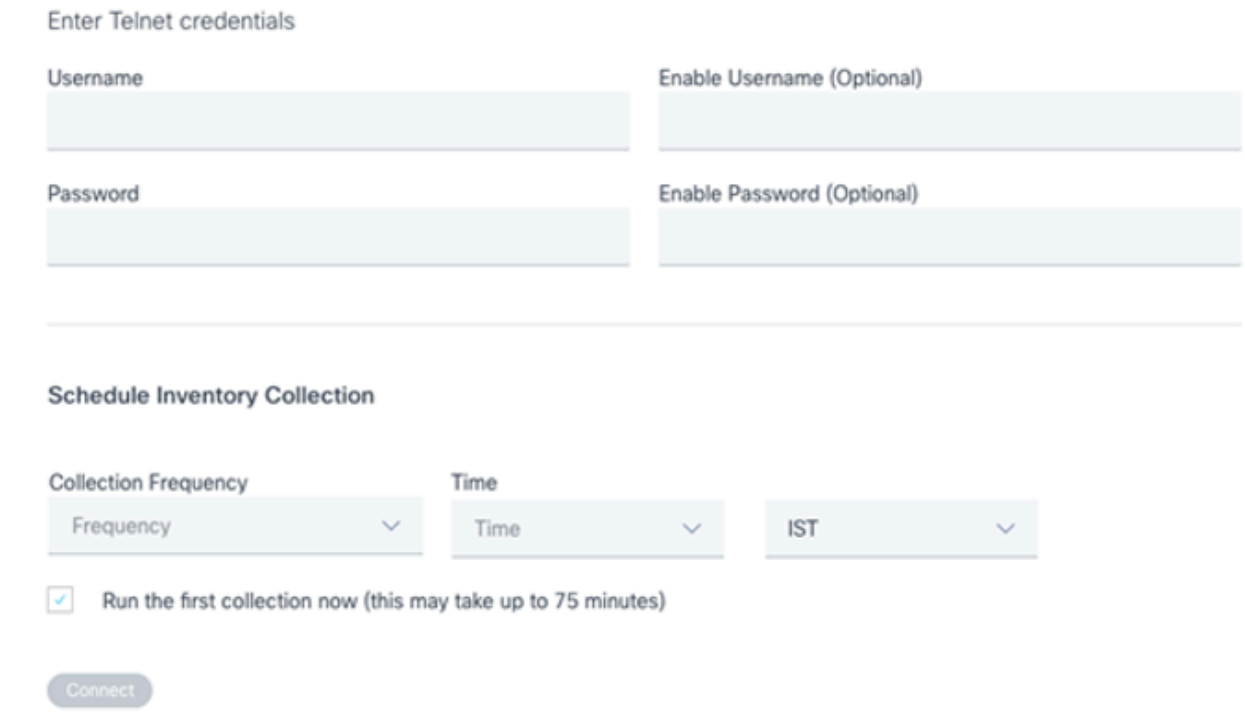
2. Remplissez le formulaire avec les informations pertinentes.
3. Plusieurs options de connexion peuvent être sélectionnées. Ces écrans affichent les informations d'identification de configuration des options. Reportez-vous à À propos du fichier de démarrage pour une description des champs d'informations d'identification pour chaque option de connexion.



Identifiants SNMP v3

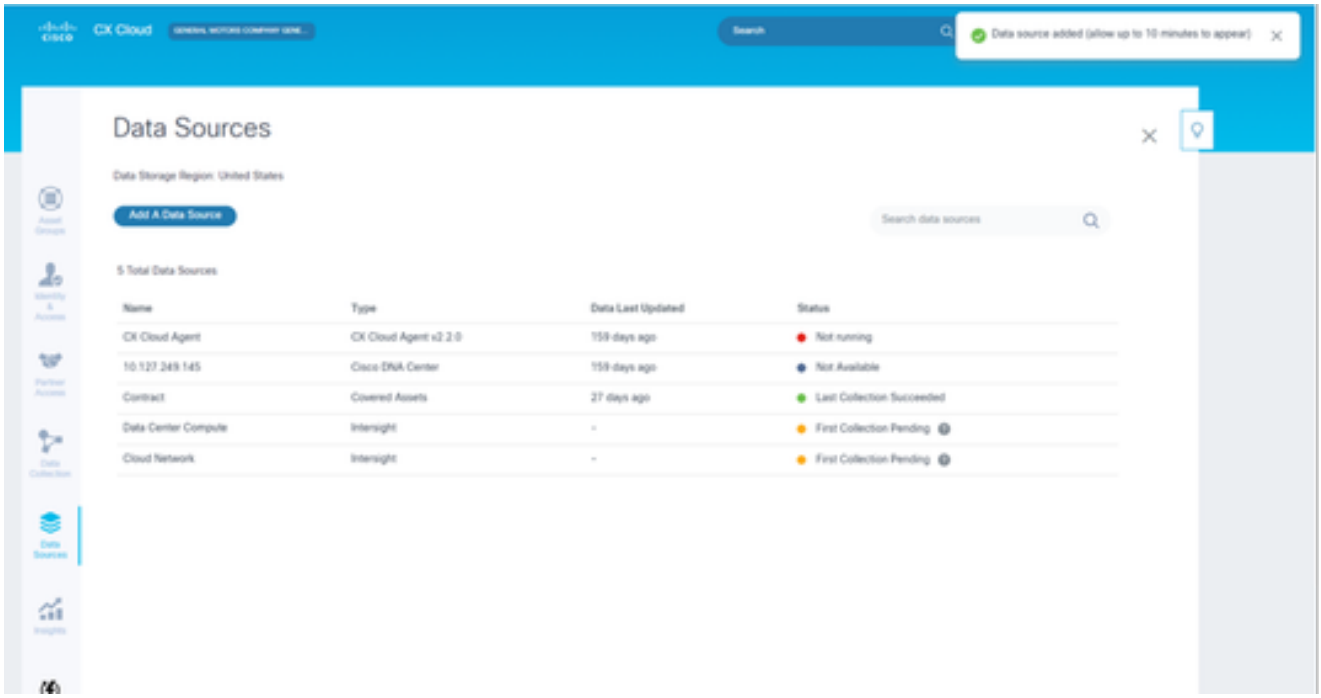


Identifiants SNMP v2, SSHV2 et SSHV1



Informations d'identification Telnet et planification d'analyse réseau

4. Cliquez sur Connect. La fenêtre Sources de données s'ouvre et affiche un message de confirmation.

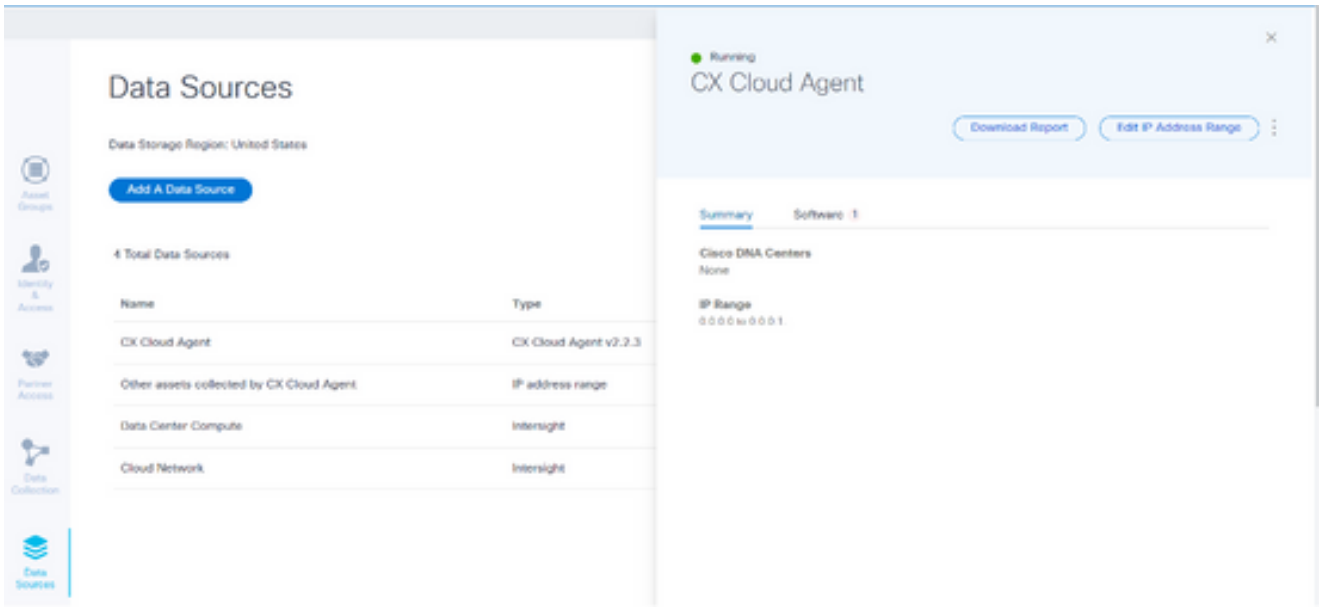


Confirmation

Modification des plages IP

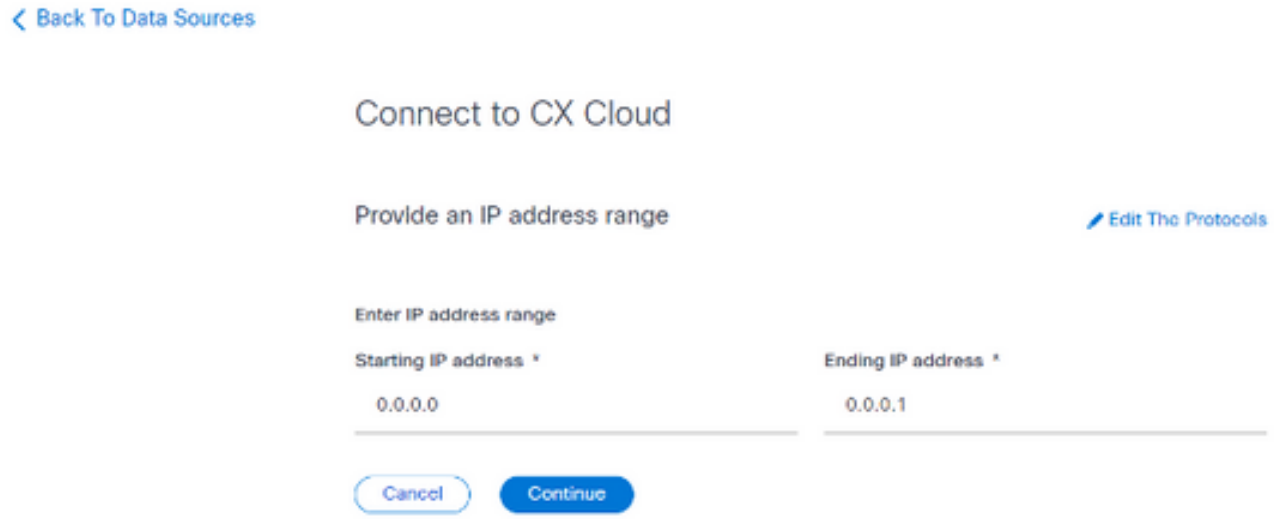
Pour modifier une plage d'adresses IP ;

1. Accédez à la fenêtre Sources de données.



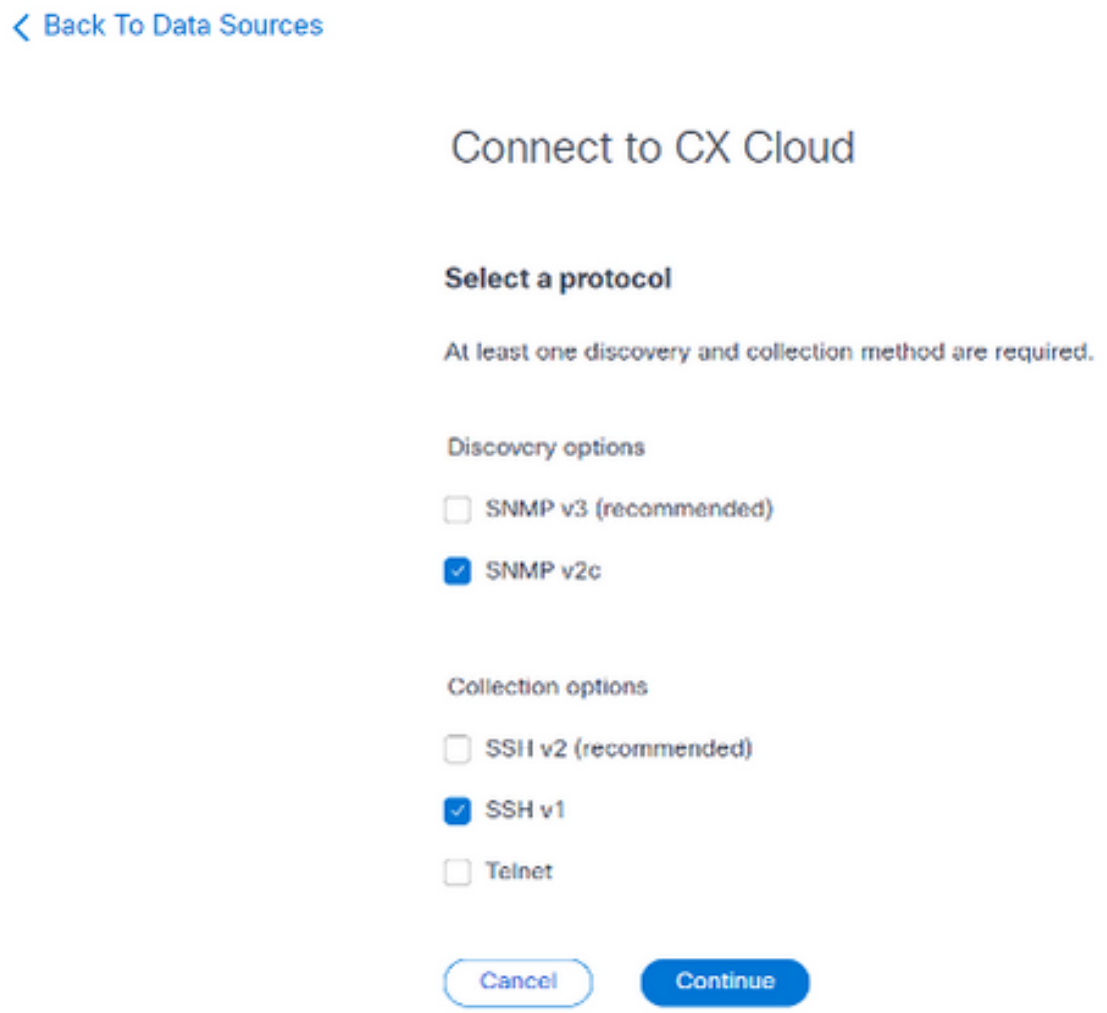
Source de données

2. Cliquez sur l'agent cloud CX qui nécessite une modification de plage d'adresses IP dans Sources de données. La fenêtre des détails s'ouvre.
3. Cliquez sur Edit IP Address Range. La fenêtre Connect to CX Cloud s'ouvre.



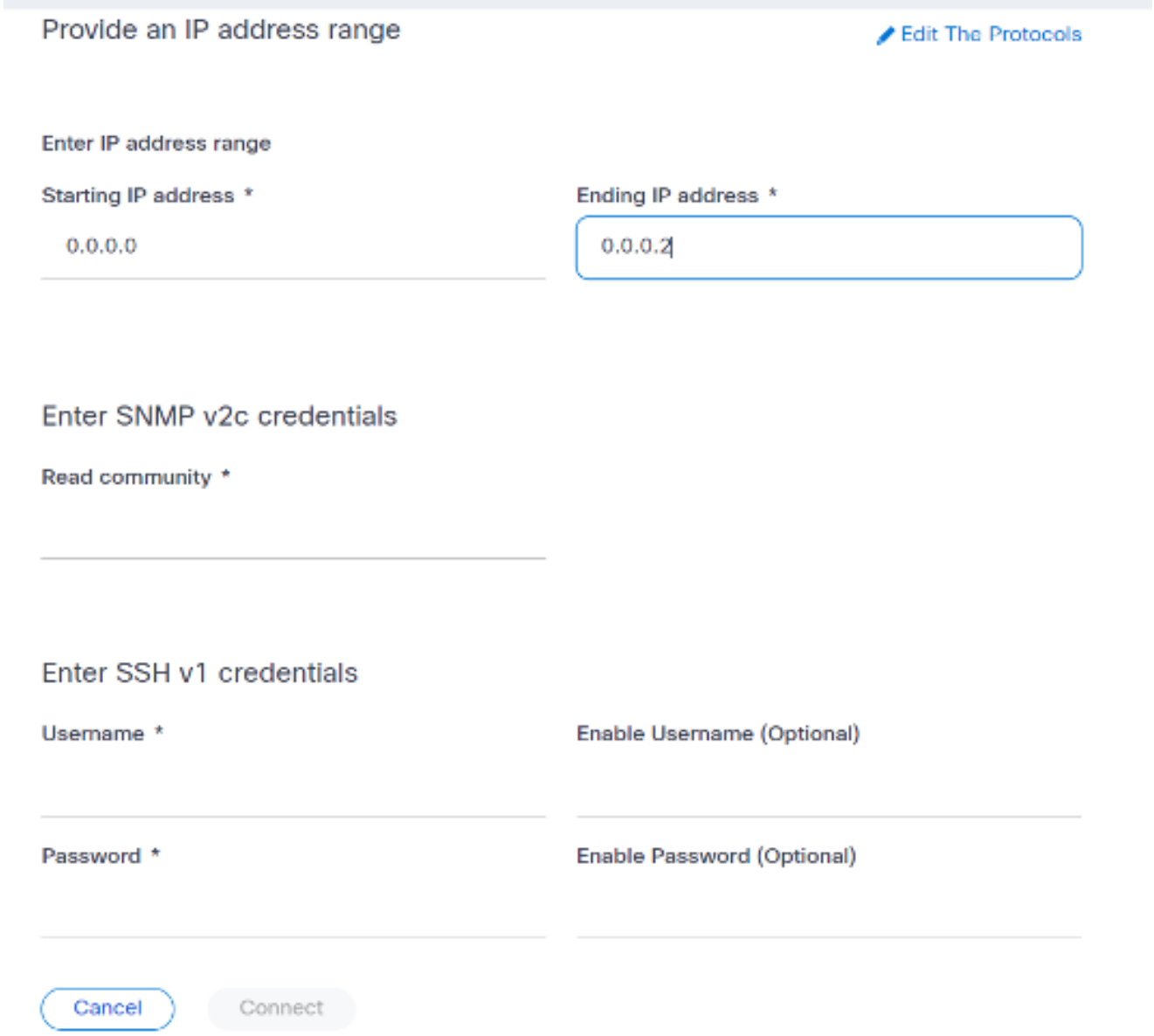
Fournir une plage IP

4. Mettez à jour les nouvelles adresses IP dans les champs Starting IP address et Ending IP address.
5. Cliquez sur le lien Edit the Protocols. La fenêtre Connect to CX Cloud - Select a protocol s'ouvre.



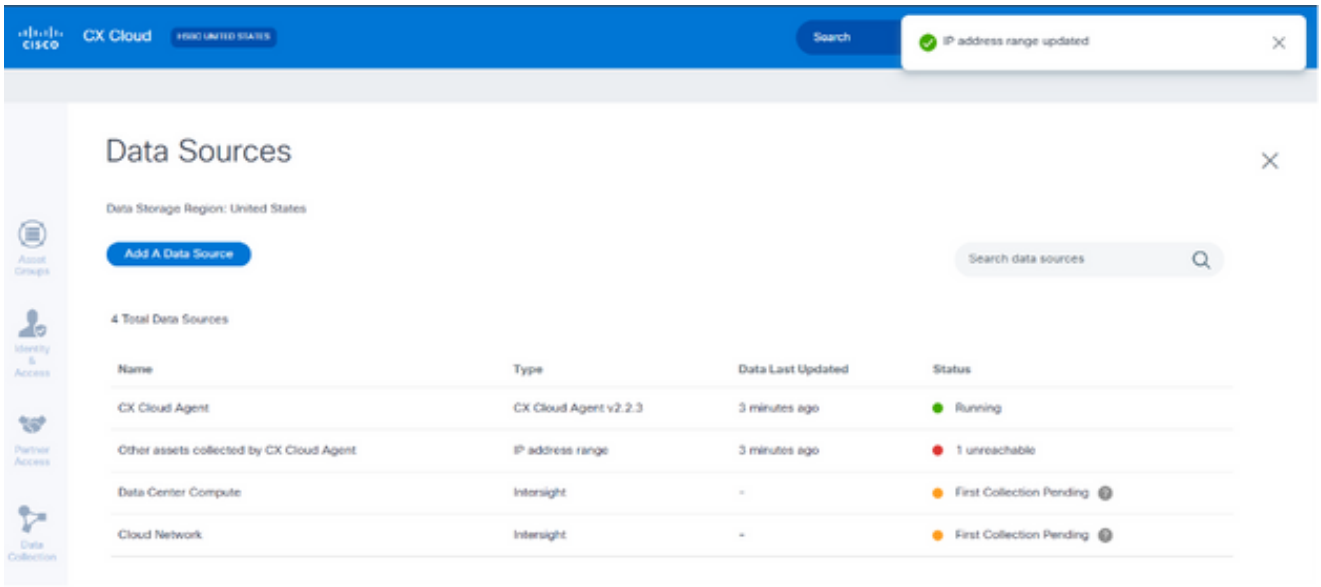
Sélectionner un protocole

6. Sélectionnez les protocoles applicables en cochant les cases appropriées.
7. Cliquez sur Continue. La fenêtre Fournir une plage d'adresses IP s'ouvre.



Entrer les identifiants

8. Saisissez les informations de configuration.
9. Cliquez sur Connect. La fenêtre Sources de données s'ouvre et affiche un message de confirmation.



Confirmation

Remarque : le message de confirmation ne garantit pas que les périphériques de la plage modifiée sont accessibles et que les informations d'identification ont été acceptées.

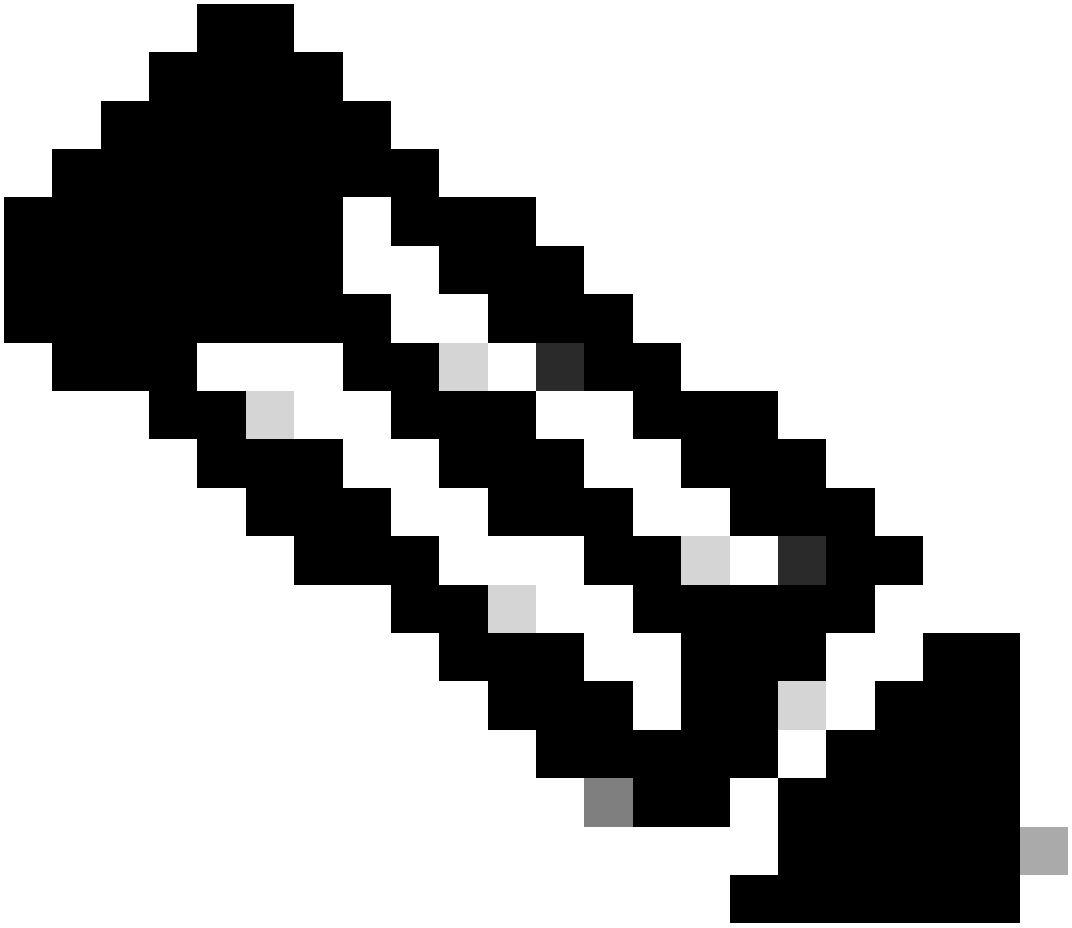
À propos des périphériques détectés à partir de plusieurs contrôleurs

Il est possible que certains périphériques soient détectés par Cisco DNA Center et que la connexion directe des périphériques à CX Cloud Agent entraîne la collecte de données dupliquées 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 Cloud Agent gère les périphériques.

- Si un périphérique est d'abord découvert par Cisco DNA Center, puis redécouvert par connexion directe du périphérique (à l'aide d'un fichier de départ ou d'une plage IP), Cisco DNA Center a la priorité pour le contrôle du périphérique.
- Si un périphérique est d'abord détecté par une connexion de périphérique directe à CX Cloud Agent, puis redécouvert par Cisco DNA Center, Cisco DNA Center est prioritaire pour le contrôle du périphérique.

Planification des analyses de diagnostic

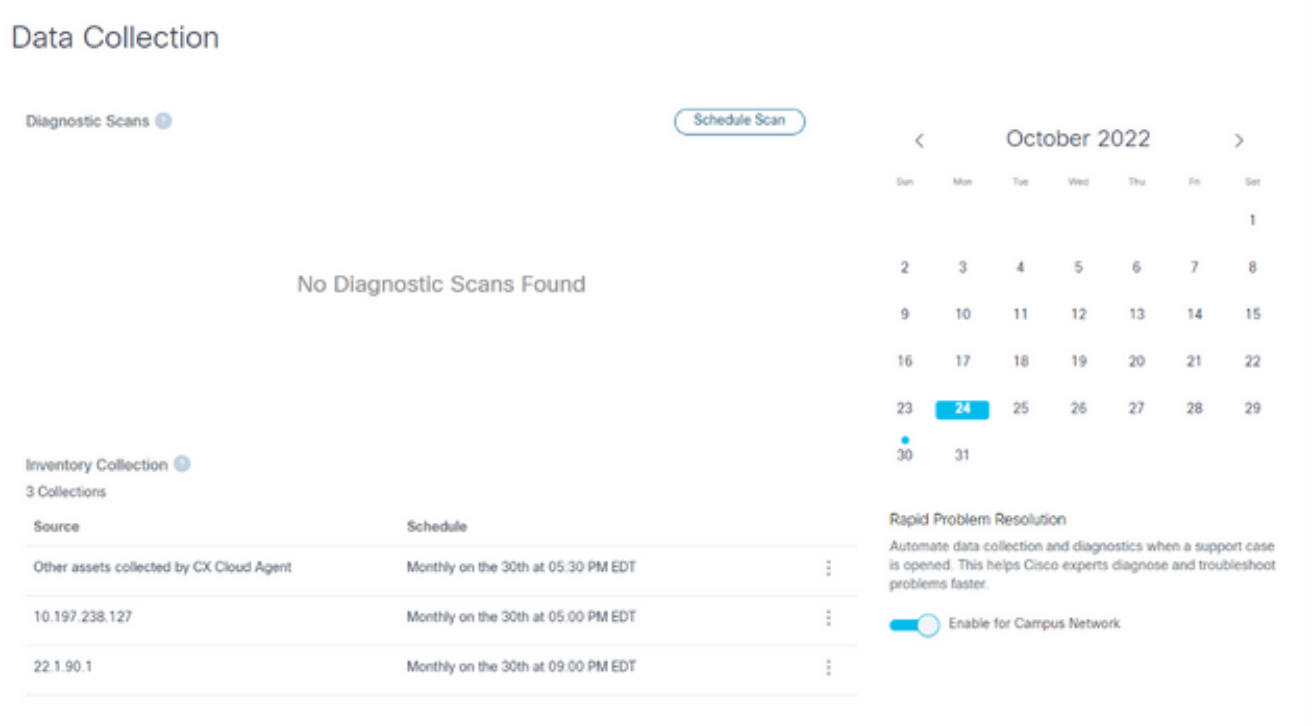
Les clients peuvent planifier des analyses de diagnostic à la demande dans le cloud CX.



Remarque : 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.

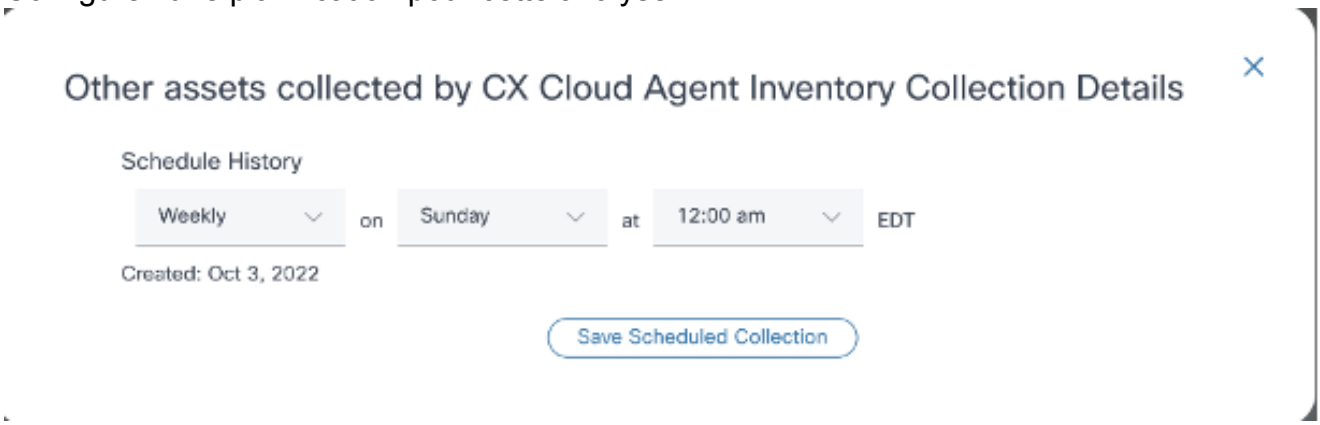
Pour planifier des analyses de diagnostic :

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.



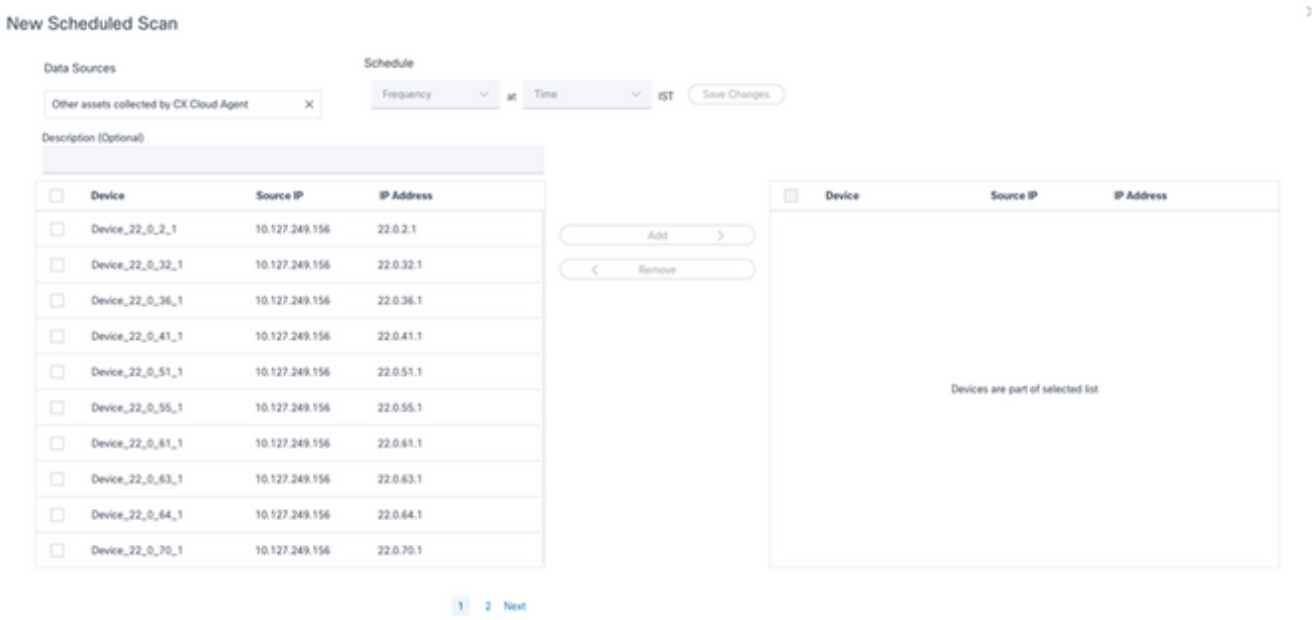
Collecte de données

4. Configurez une planification pour cette analyse.



Configurer la planification d'analyse

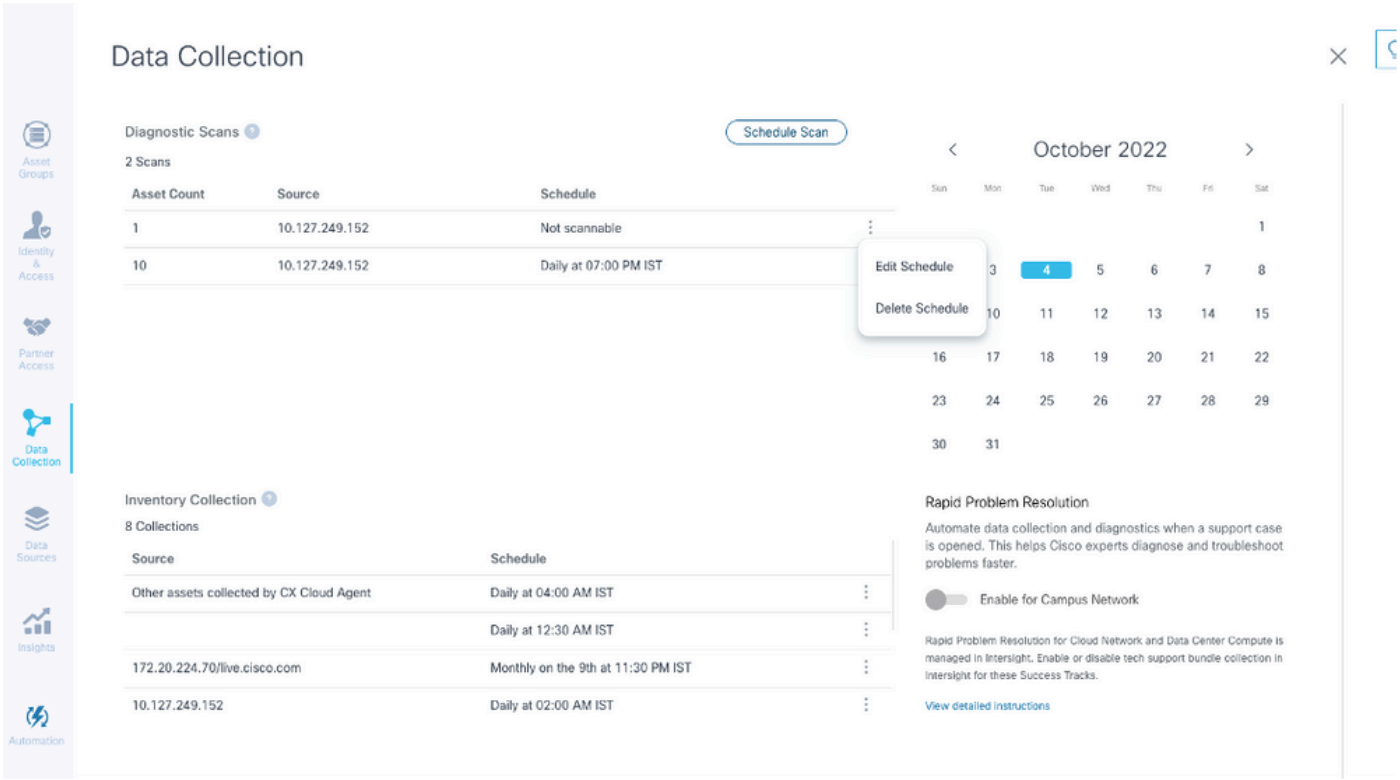
5. Dans la liste des périphériques, sélectionnez tous les périphériques pour l'analyse et cliquez sur Add.



Planifier une analyse

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

Déploiement et configuration du réseau

Sélectionnez l'une des options suivantes pour déployer CX Cloud Agent :

- Pour sélectionner VMware vSphere/vCenter Thick Client ESXi 5.5/6.0, accédez à Thick Client
- Pour sélectionner VMware vSphere/vCenter Web Client ESXi 6.0, accédez à Web Client ou à vSphere Center
- Pour sélectionner Oracle Virtual Box 5.2.30, accédez à Oracle VM
- Pour sélectionner Microsoft Hyper-V, accédez à Hyper-V

Déploiement OVA

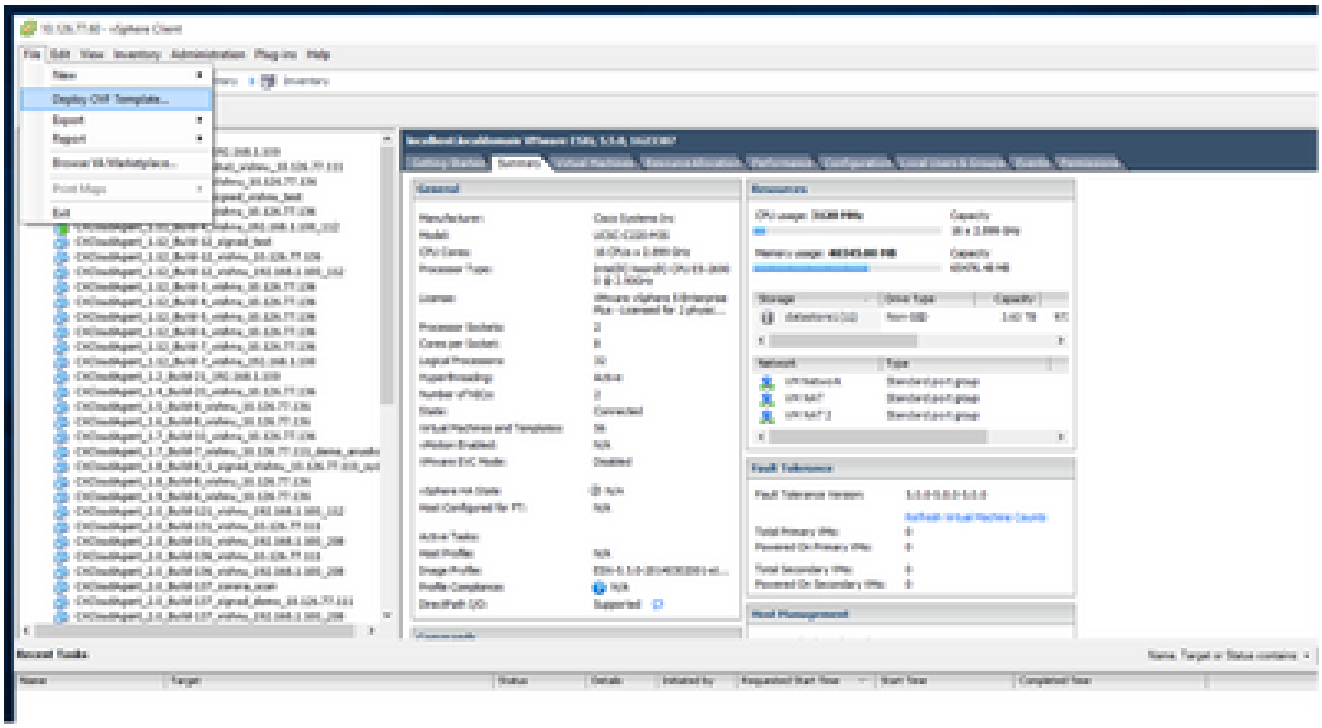
Installation du client lourd ESXi 5.5/6.0

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

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

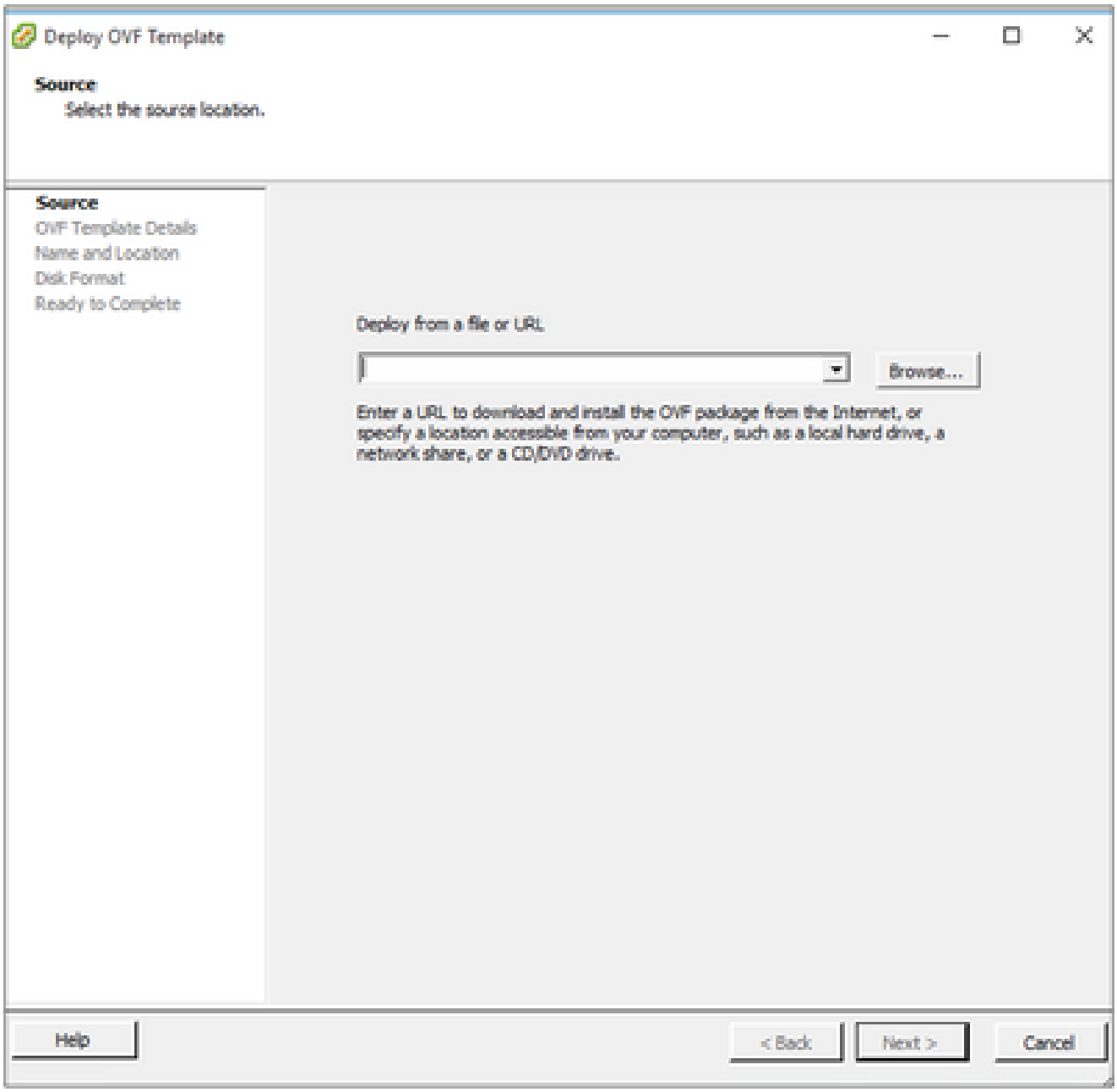
Connexion

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



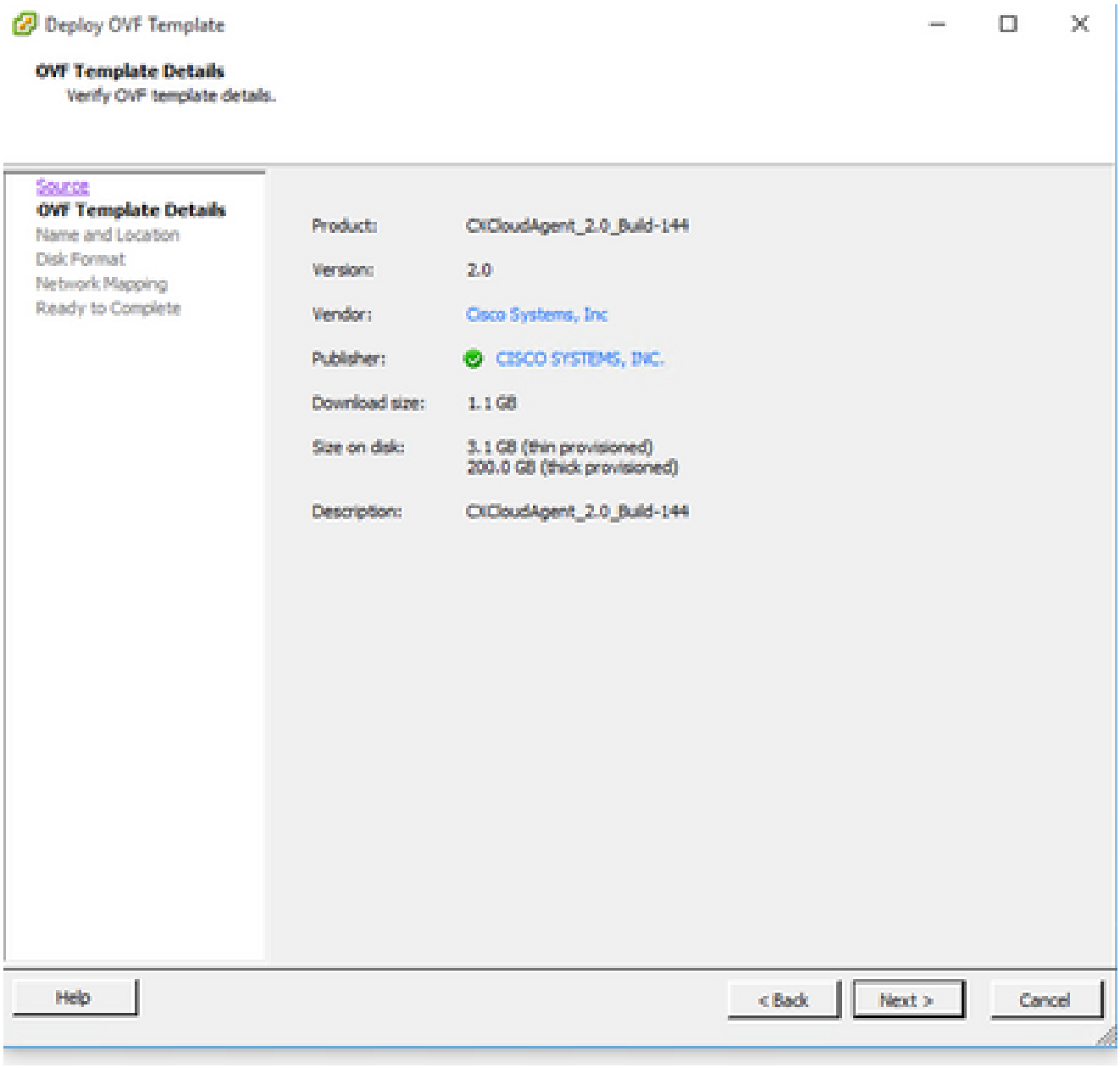
vSphere Client

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



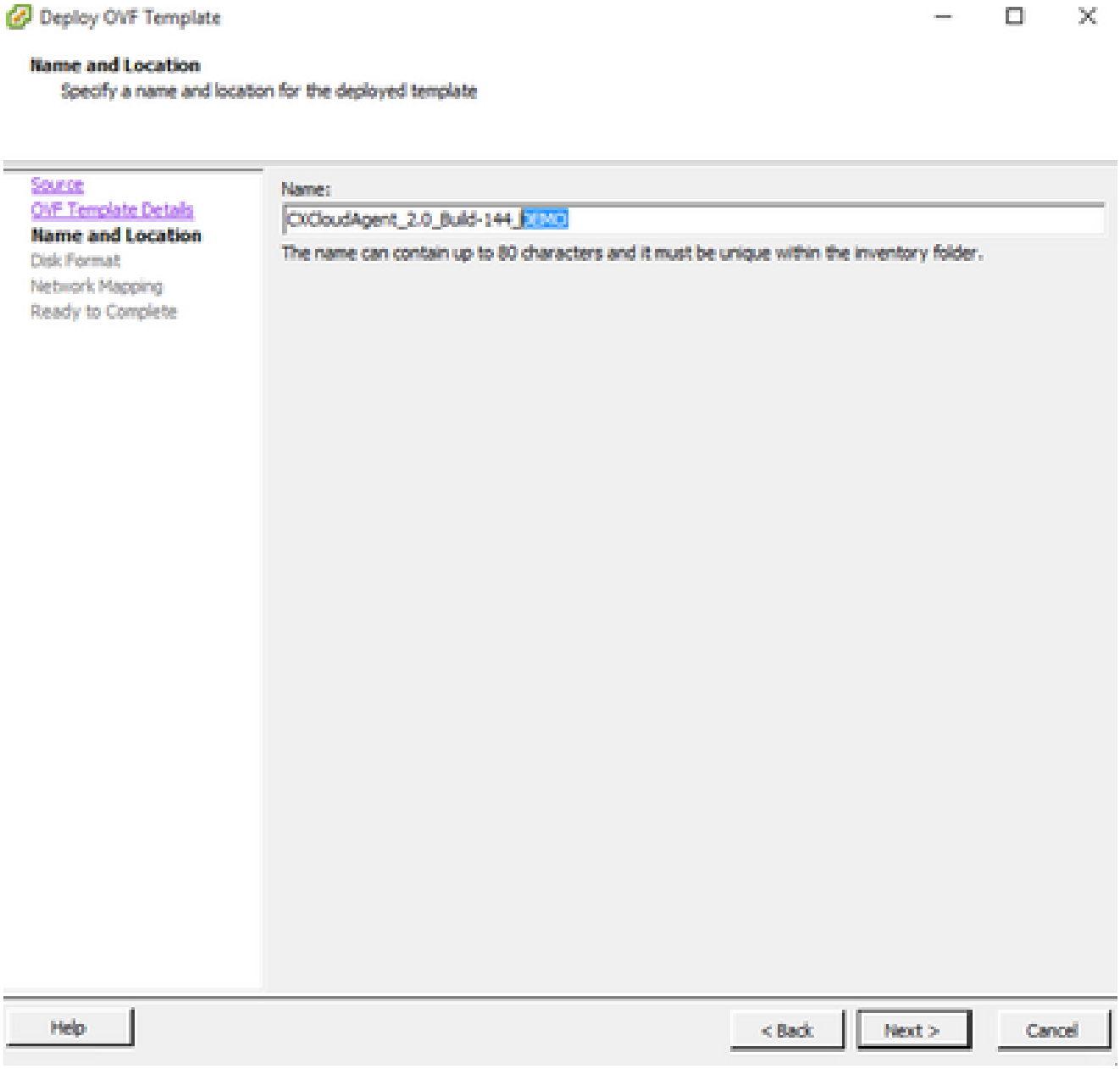
Chemin OVA

4. Vérifiez les détails OVF et cliquez sur Next.



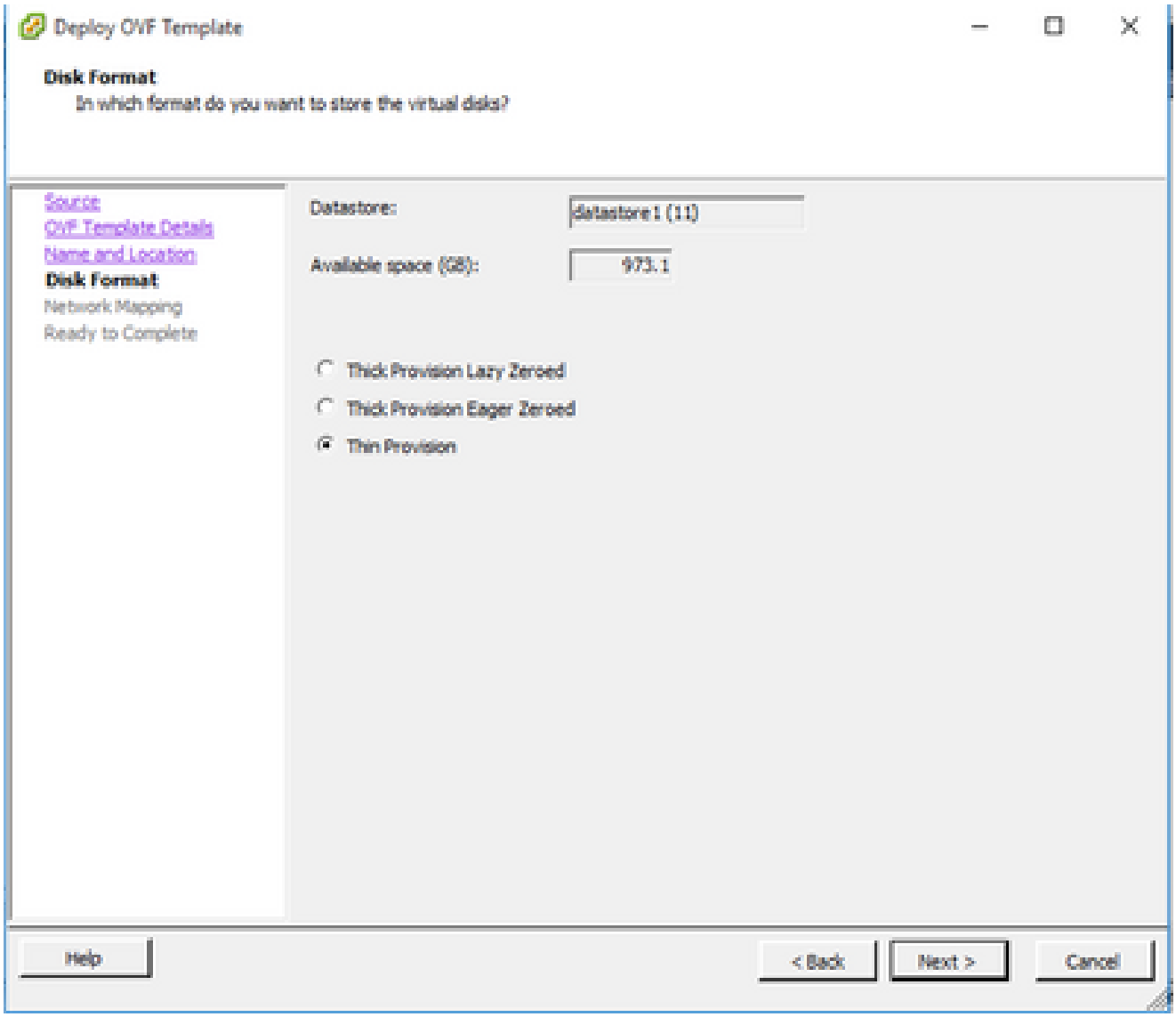
Détails du modèle

5. Entrez un nom unique et cliquez sur Suivant.



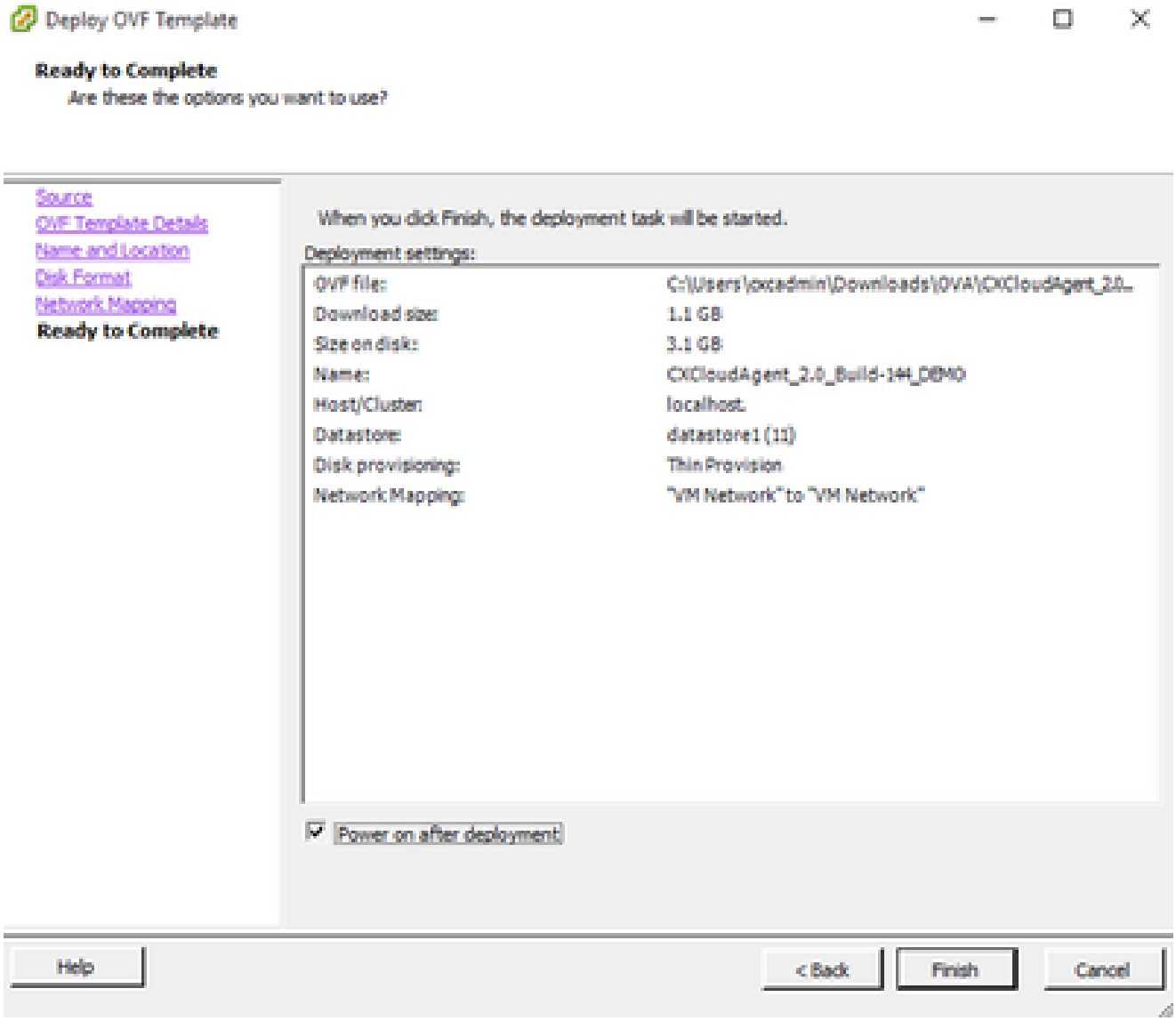
Nom et emplacement

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



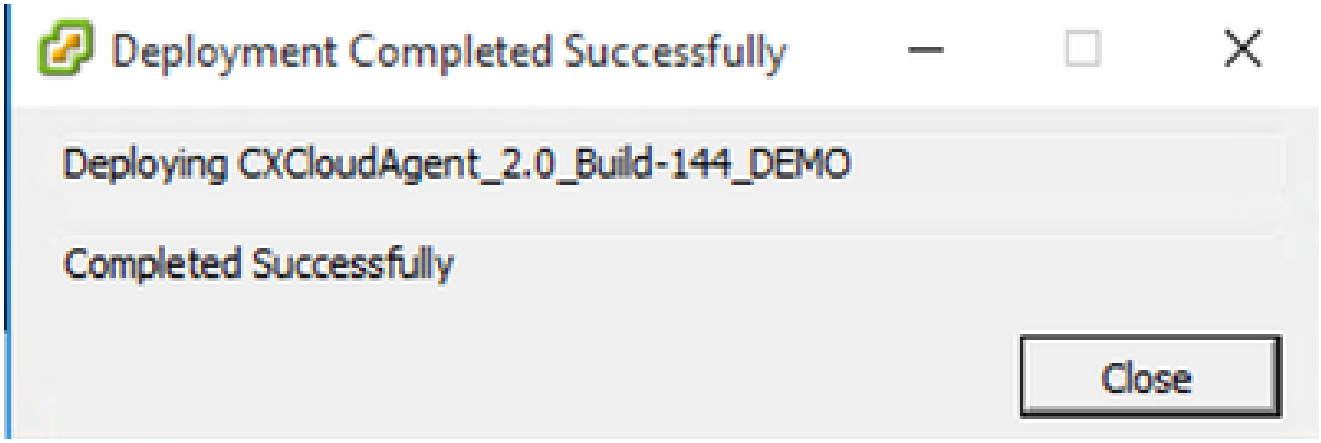
Format de disque

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

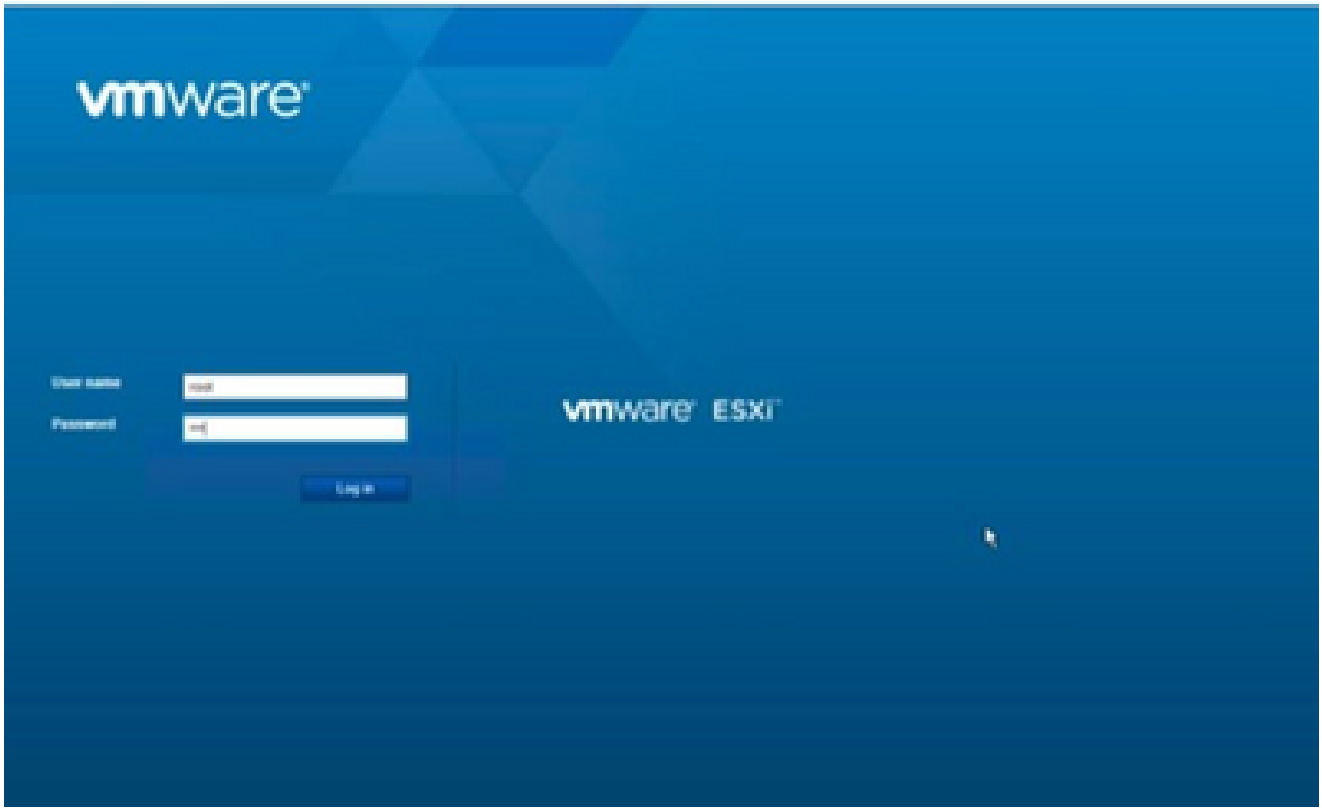
8. Sélectionnez la machine virtuelle déployée, ouvrez la console et accédez à Network

Configuration pour passer aux étapes suivantes.

Installation du client Web ESXi 6.0

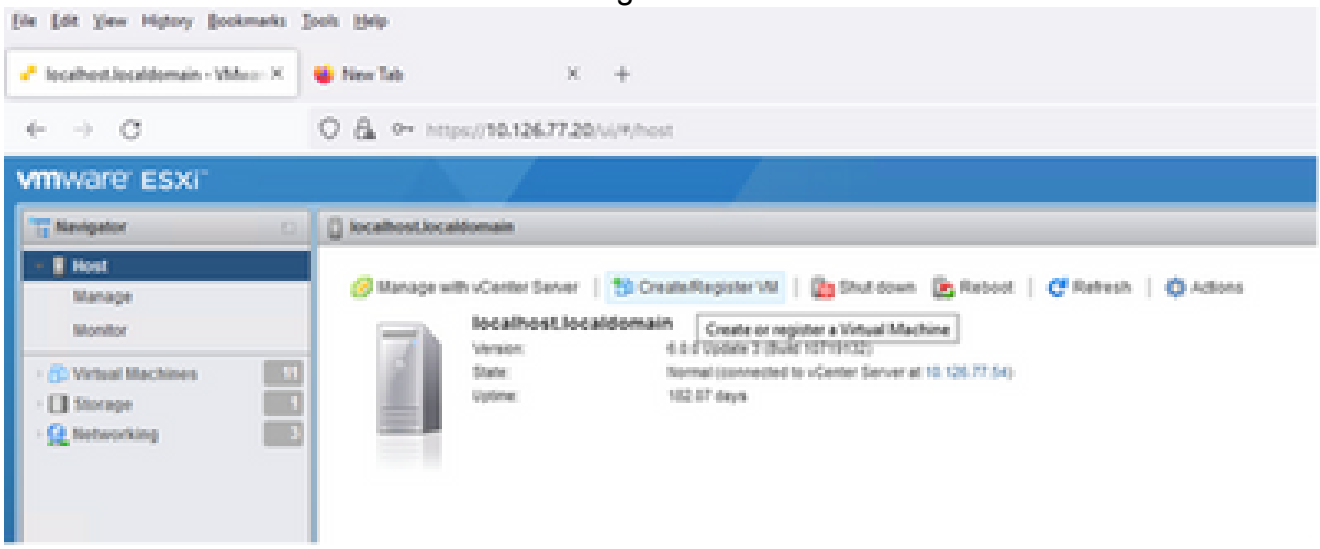
Ce client déploie CX Cloud Agent OVA en utilisant le Web vSphere.

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



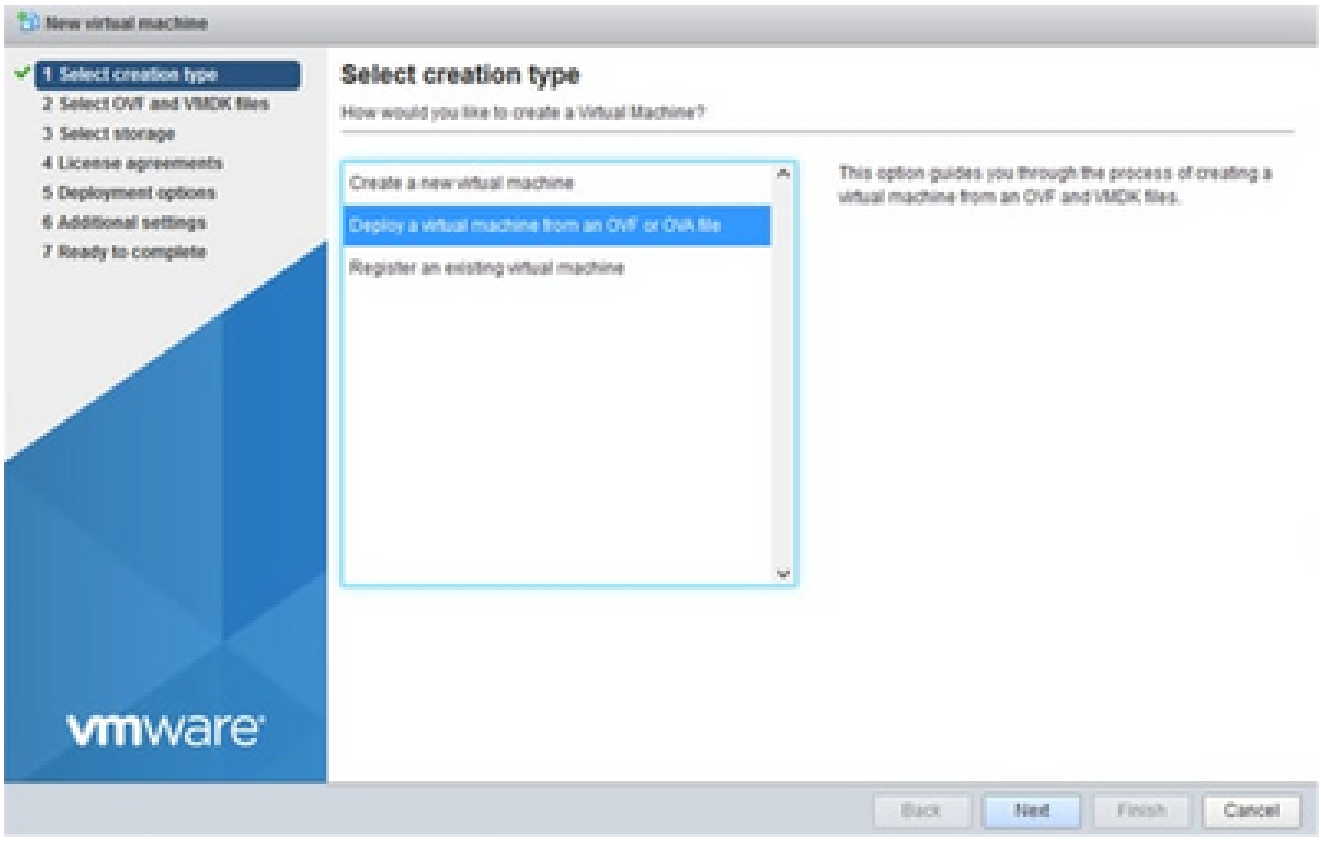
Connexion VMware ESXi

2. Sélectionnez Virtual Machine > Create / Register VM.



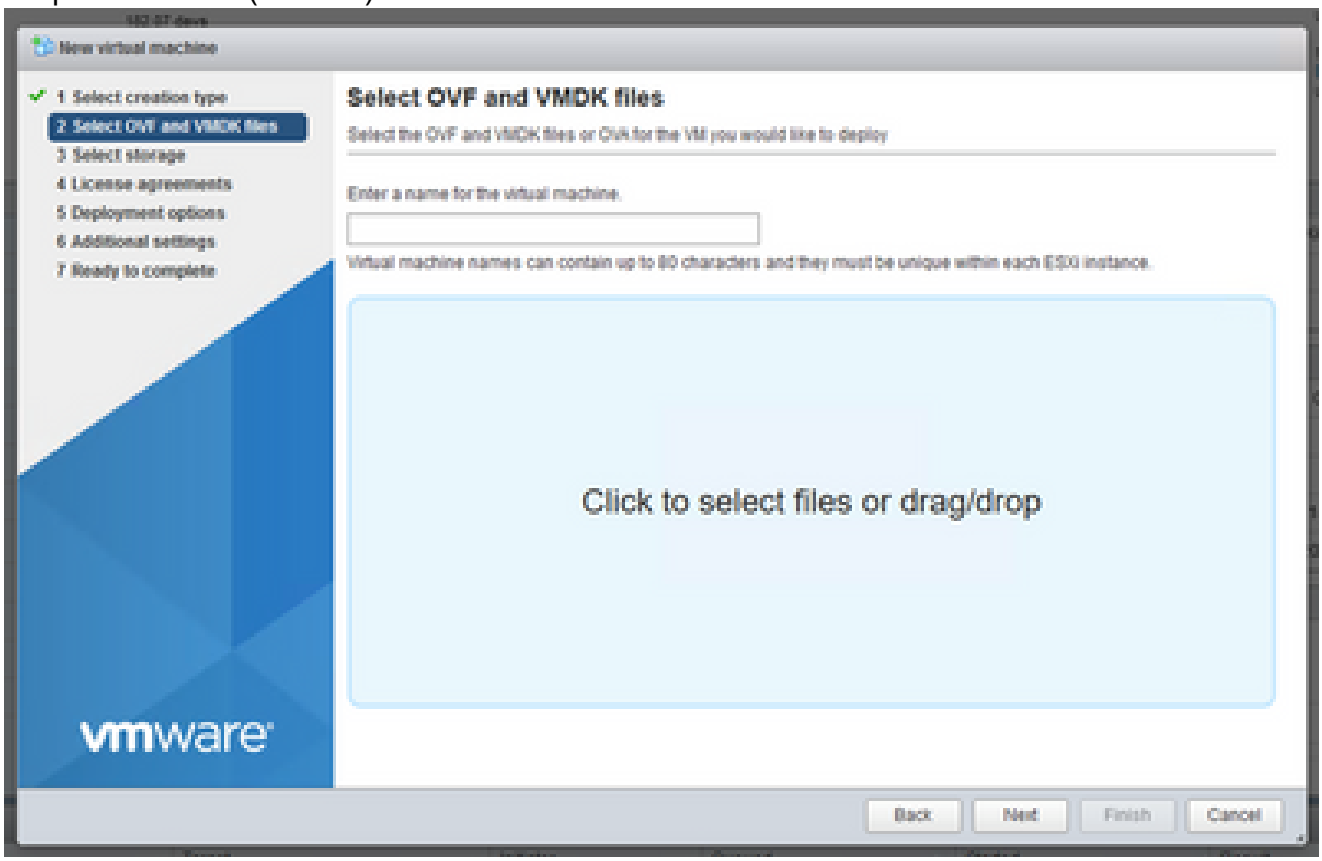
Créer une machine virtuelle

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



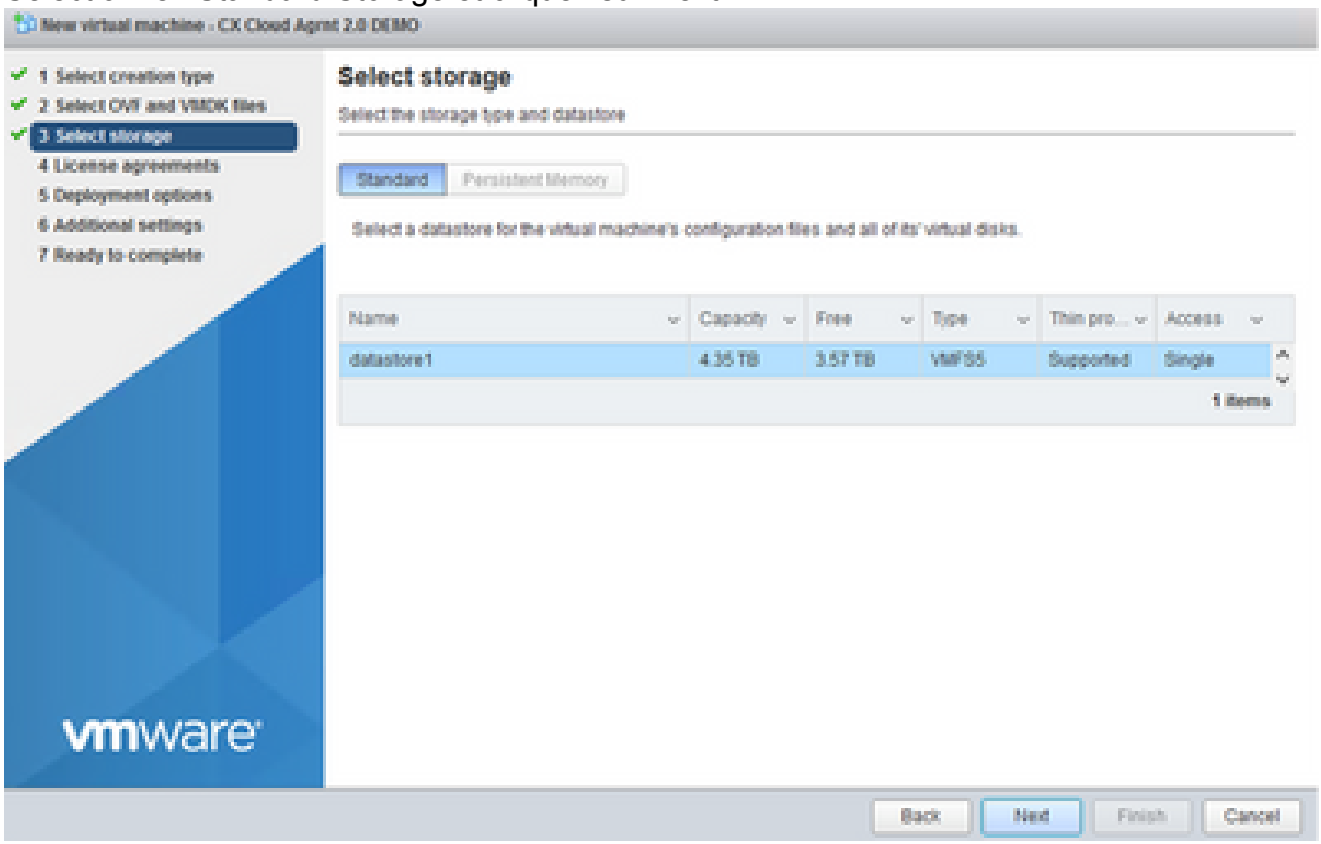
Sélectionner le type de création

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



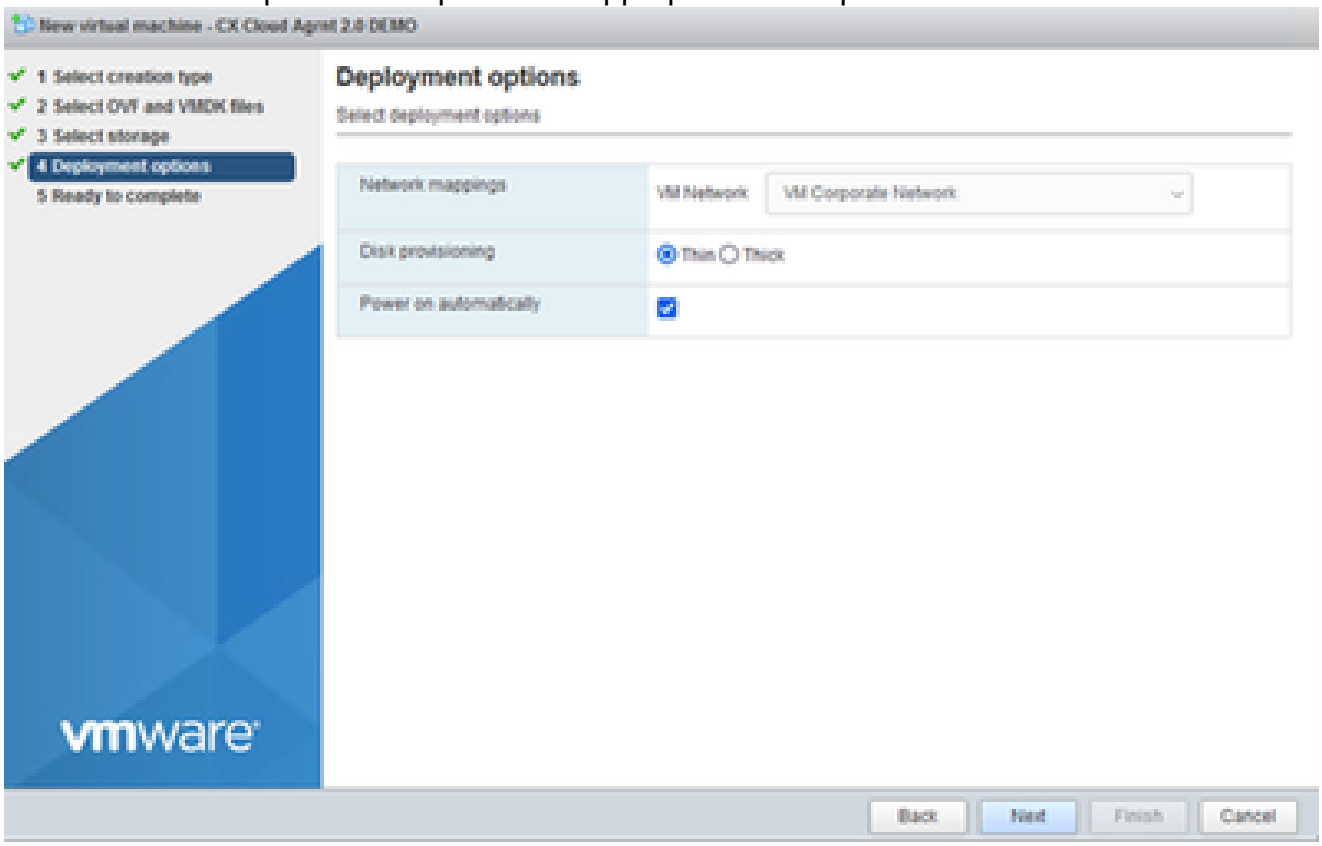
Sélection OVA

6. Sélectionnez Standard Storage et cliquez sur Next.



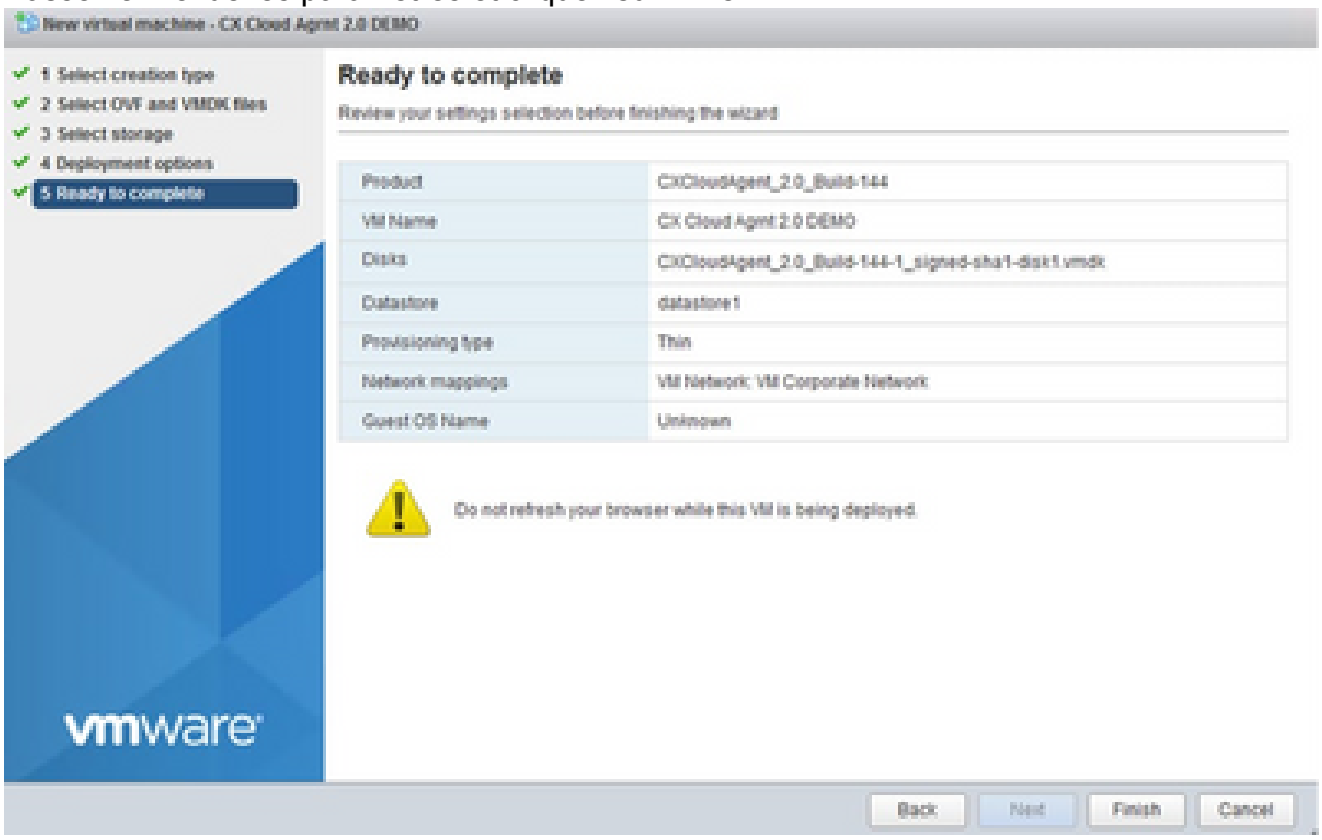
Sélectionner le stockage

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

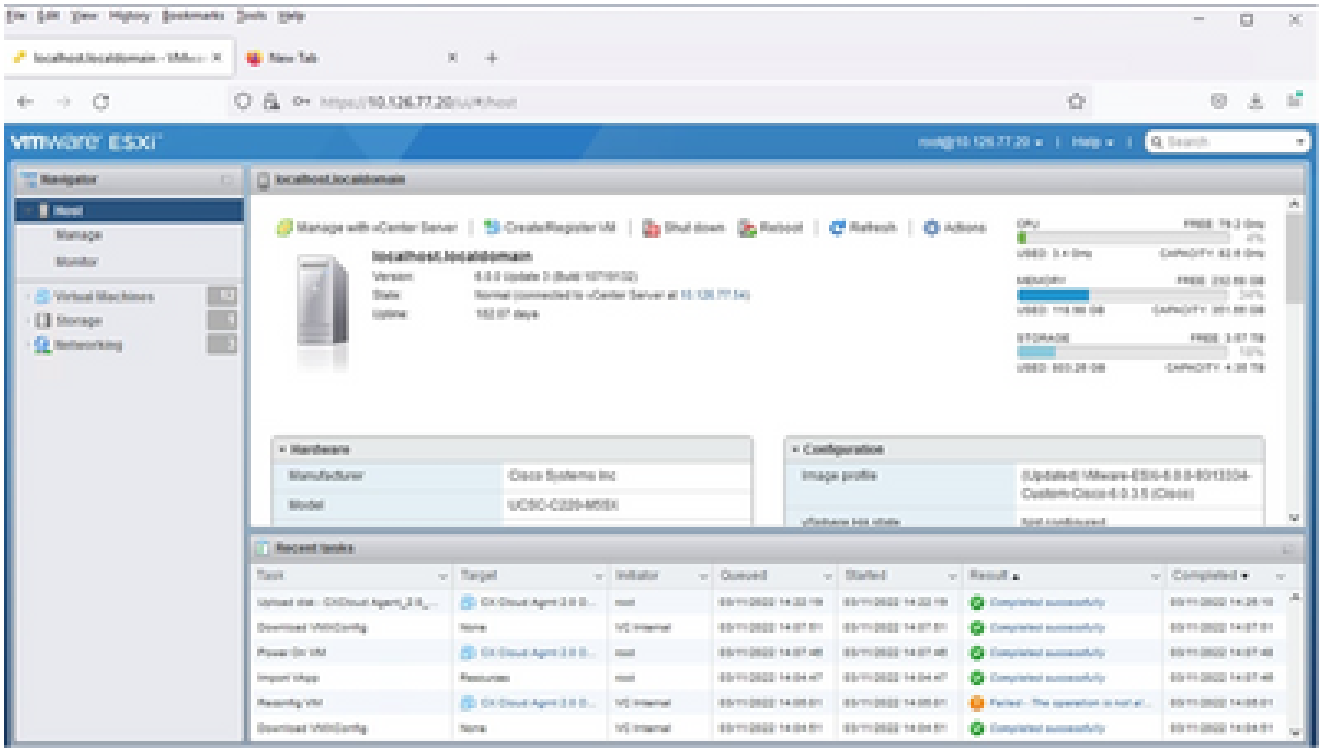


Options de déploiement

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

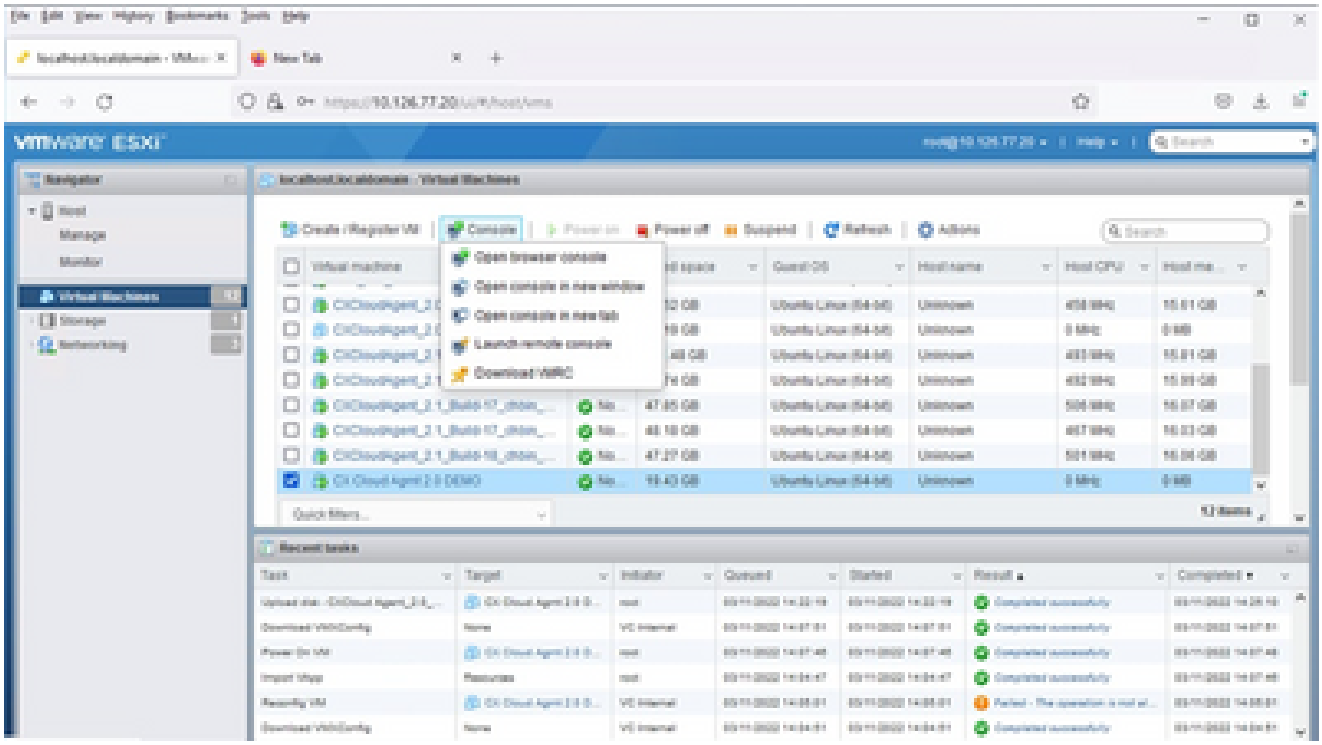


Prêt pour la confirmation



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.

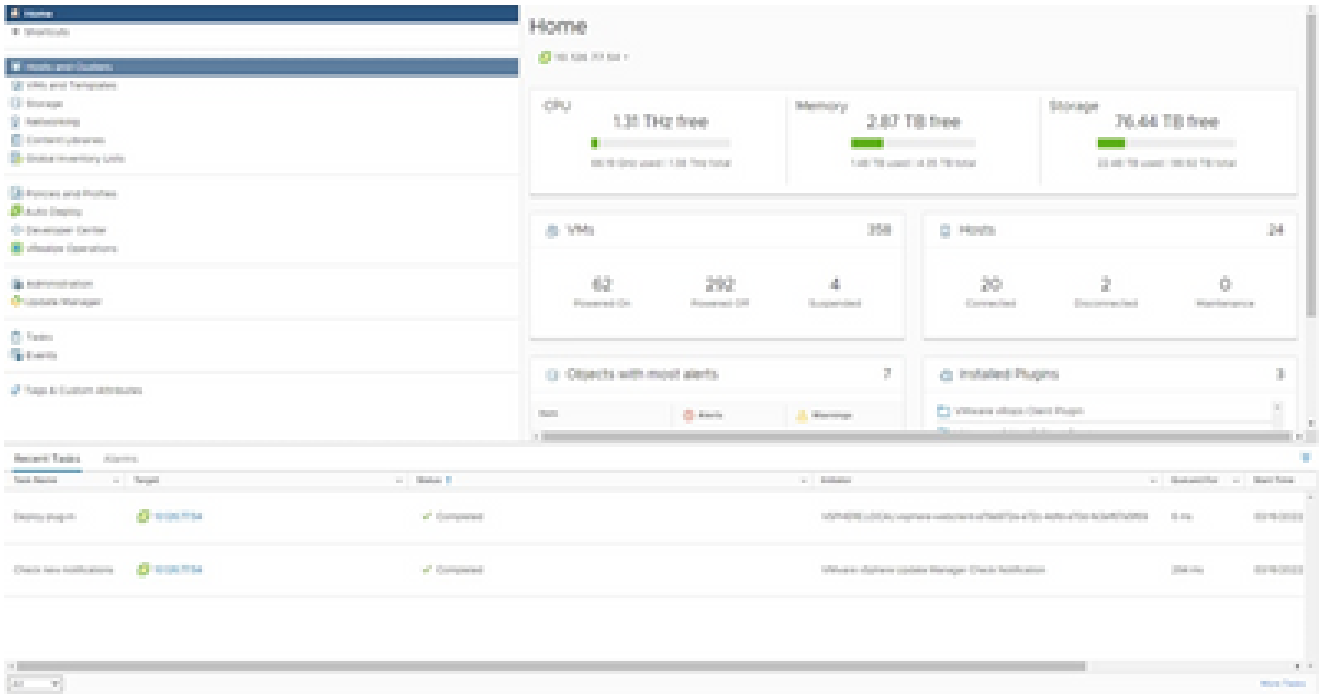
Installation de client Web vCenter

Effectuez les étapes suivantes :

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

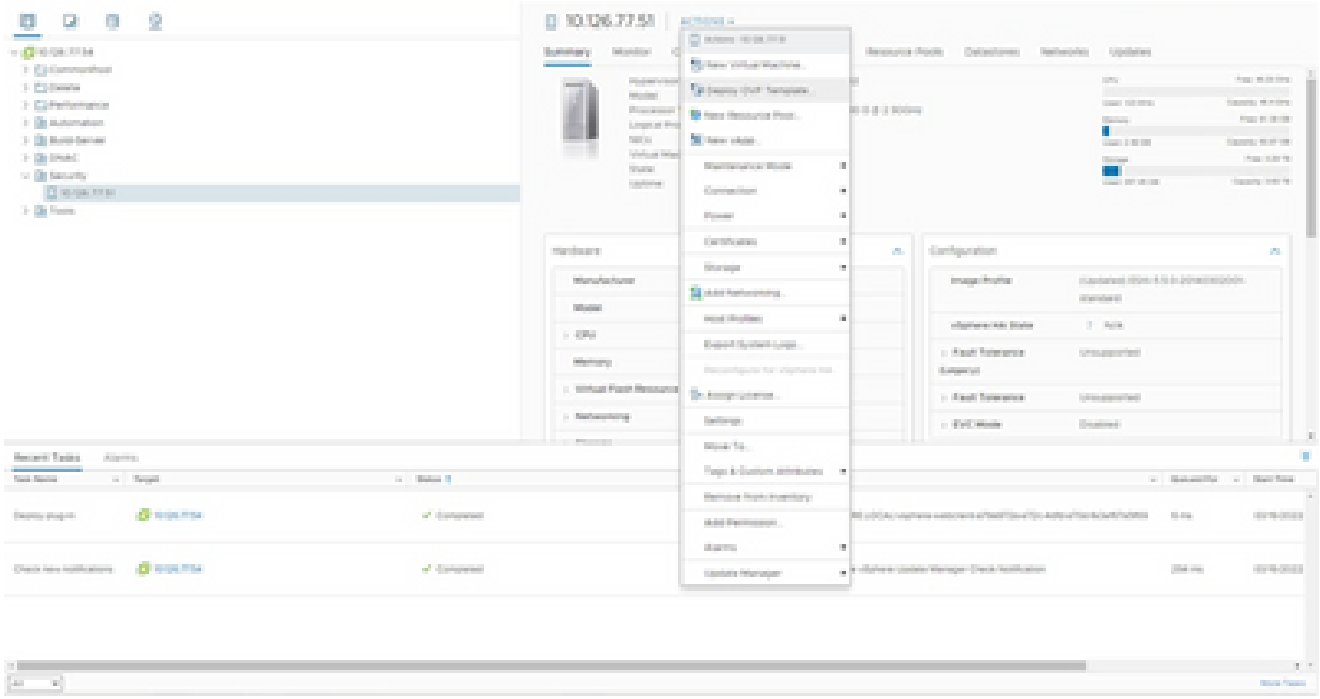
Ouvrir une session

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

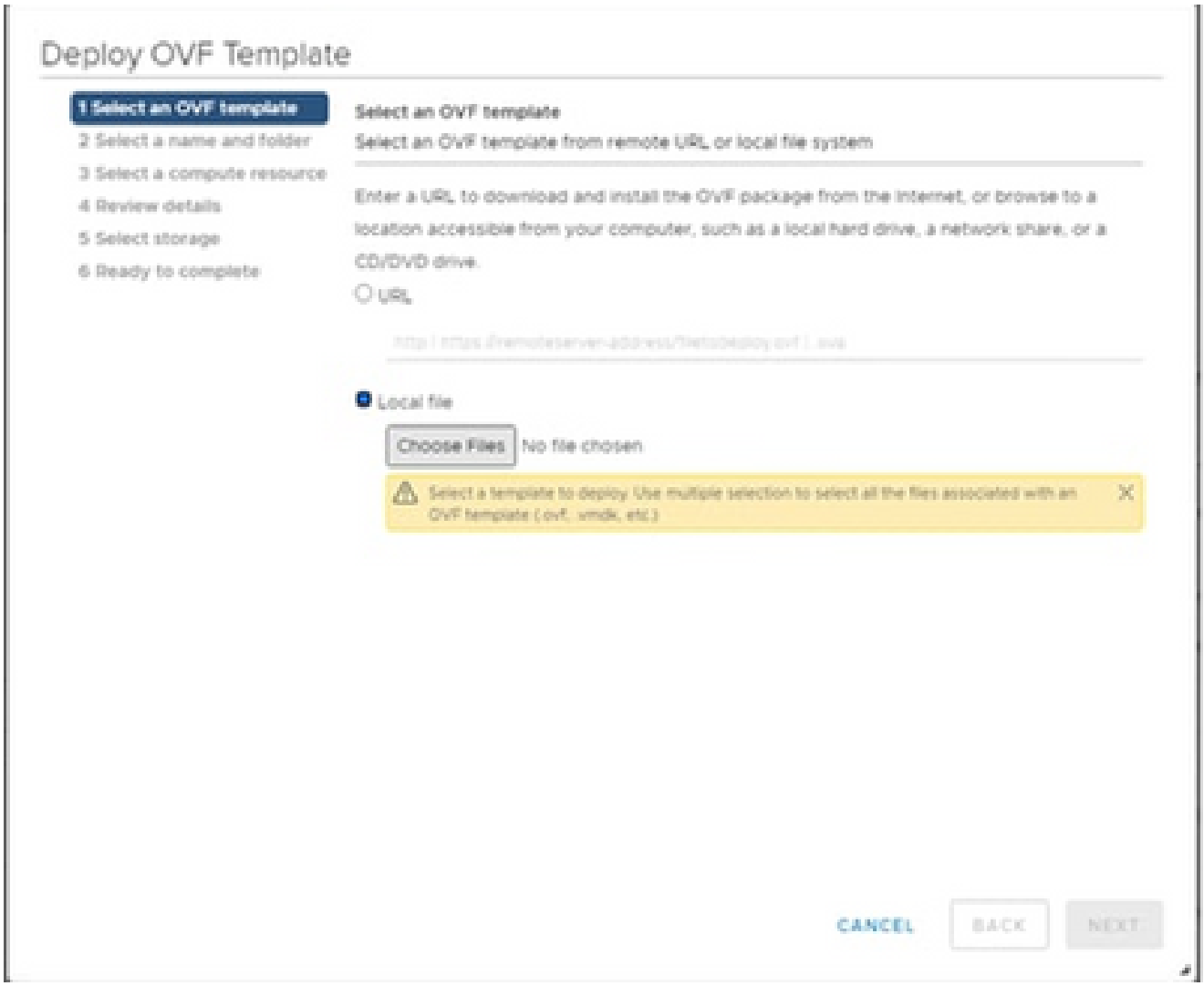


Page d’accueil

3. Sélectionnez la machine virtuelle et cliquez sur Action > Deploy OVF Template.

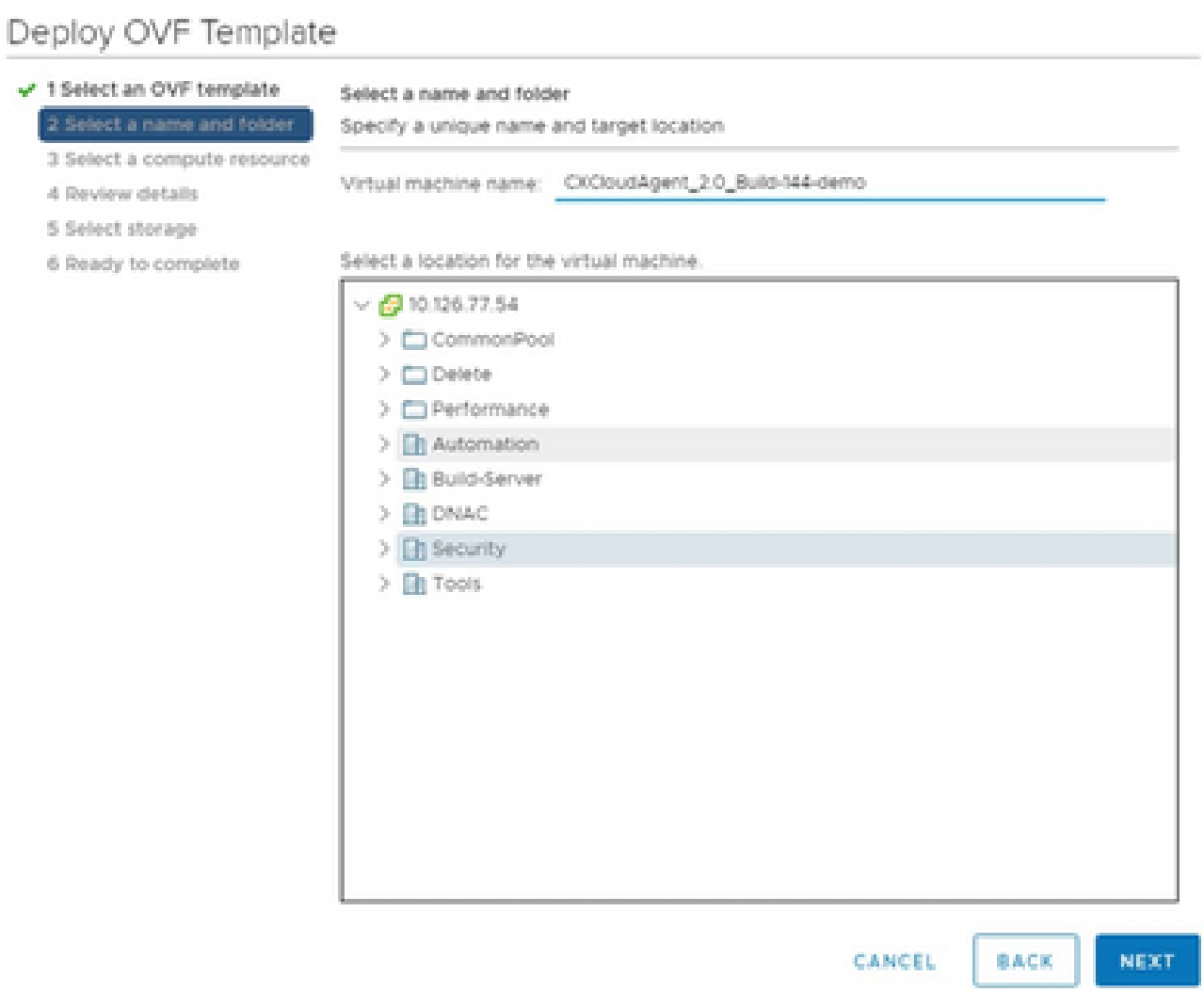


Actions



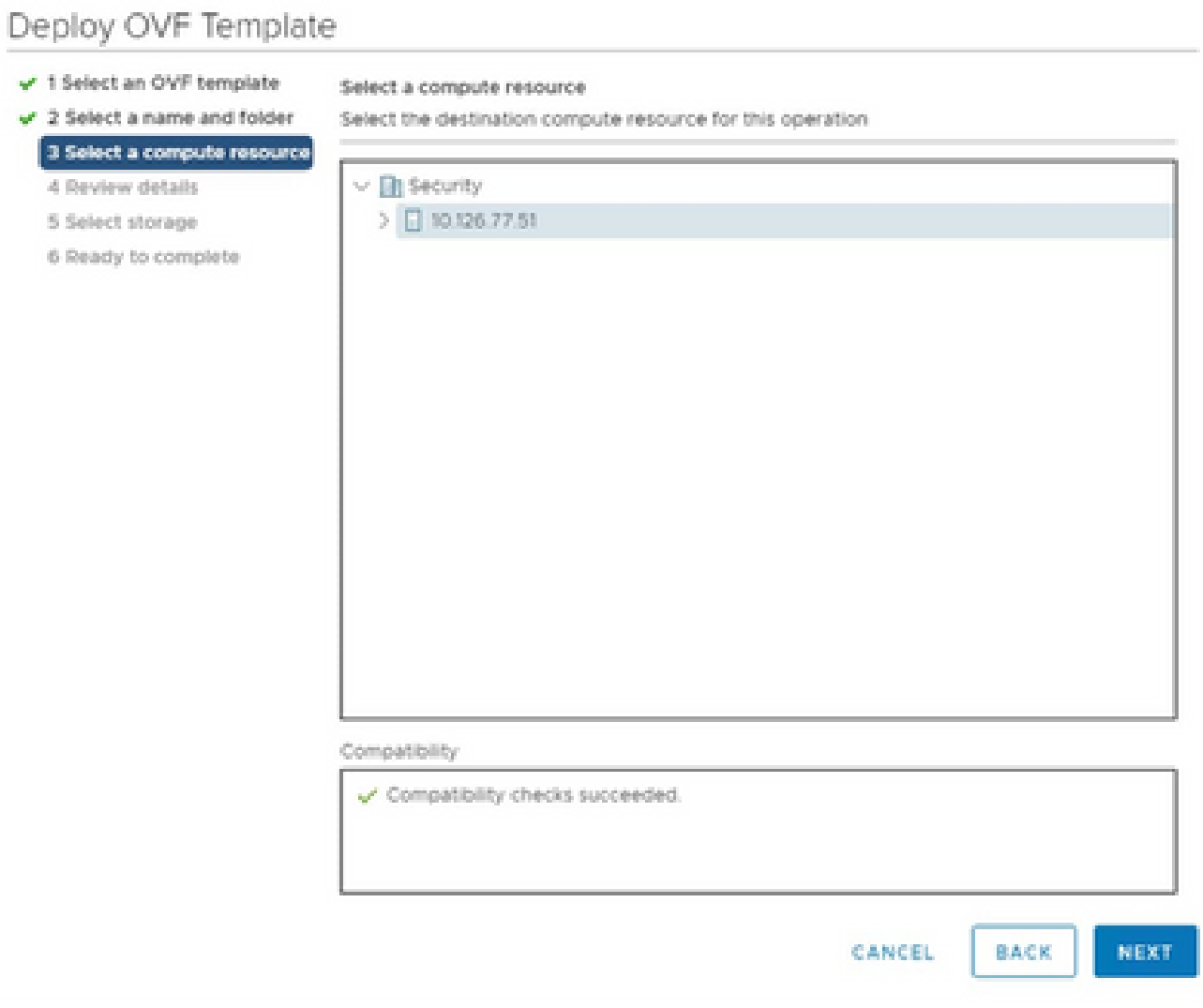
Sélectionner le modèle

4. Ajoutez directement l'URL ou parcourez pour sélectionner le fichier OVA et cliquez sur Next.
5. Entrez un nom unique et accédez à l'emplacement si nécessaire.
6. Cliquez sur Next (Suivant).



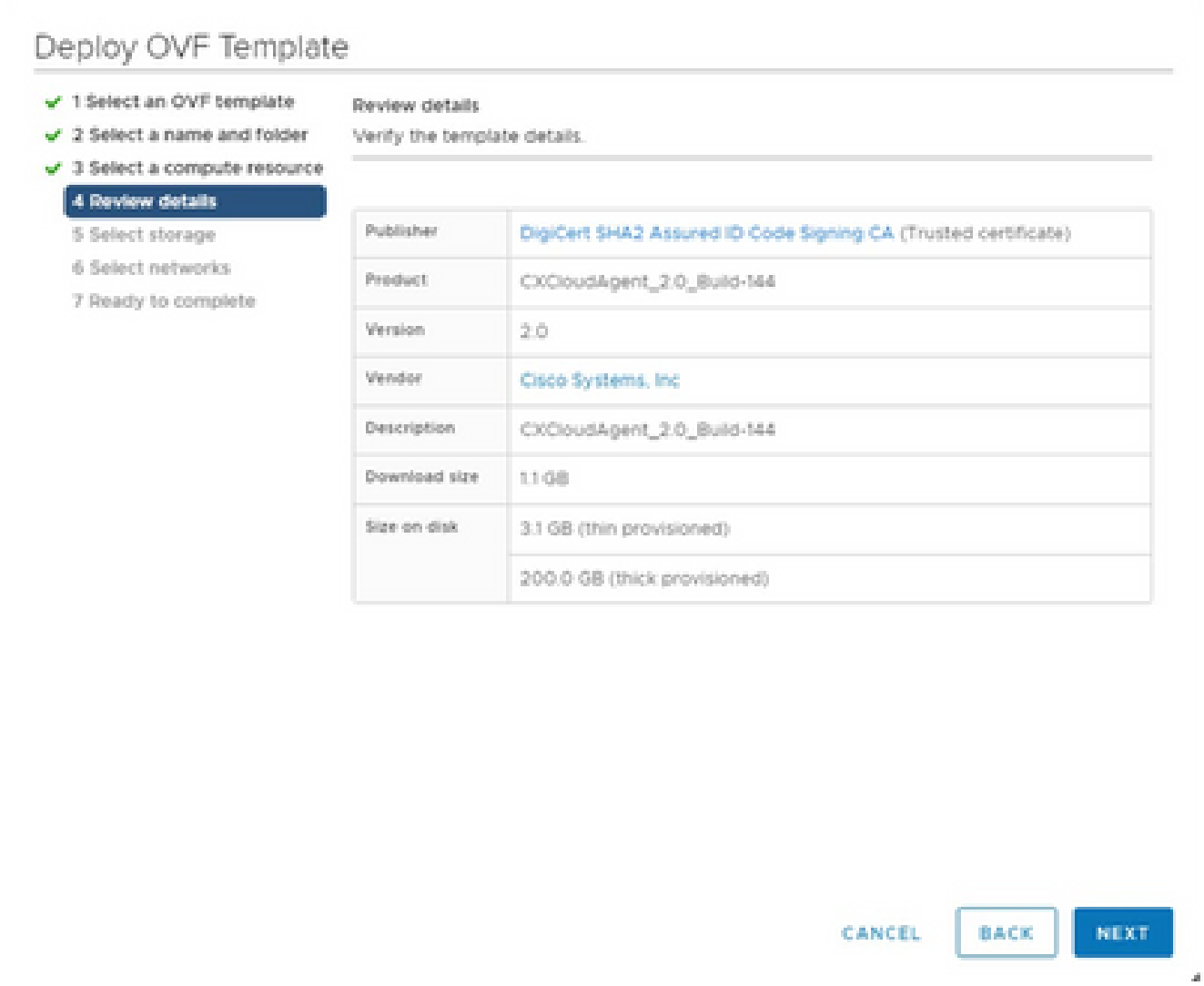
Nom et dossier

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



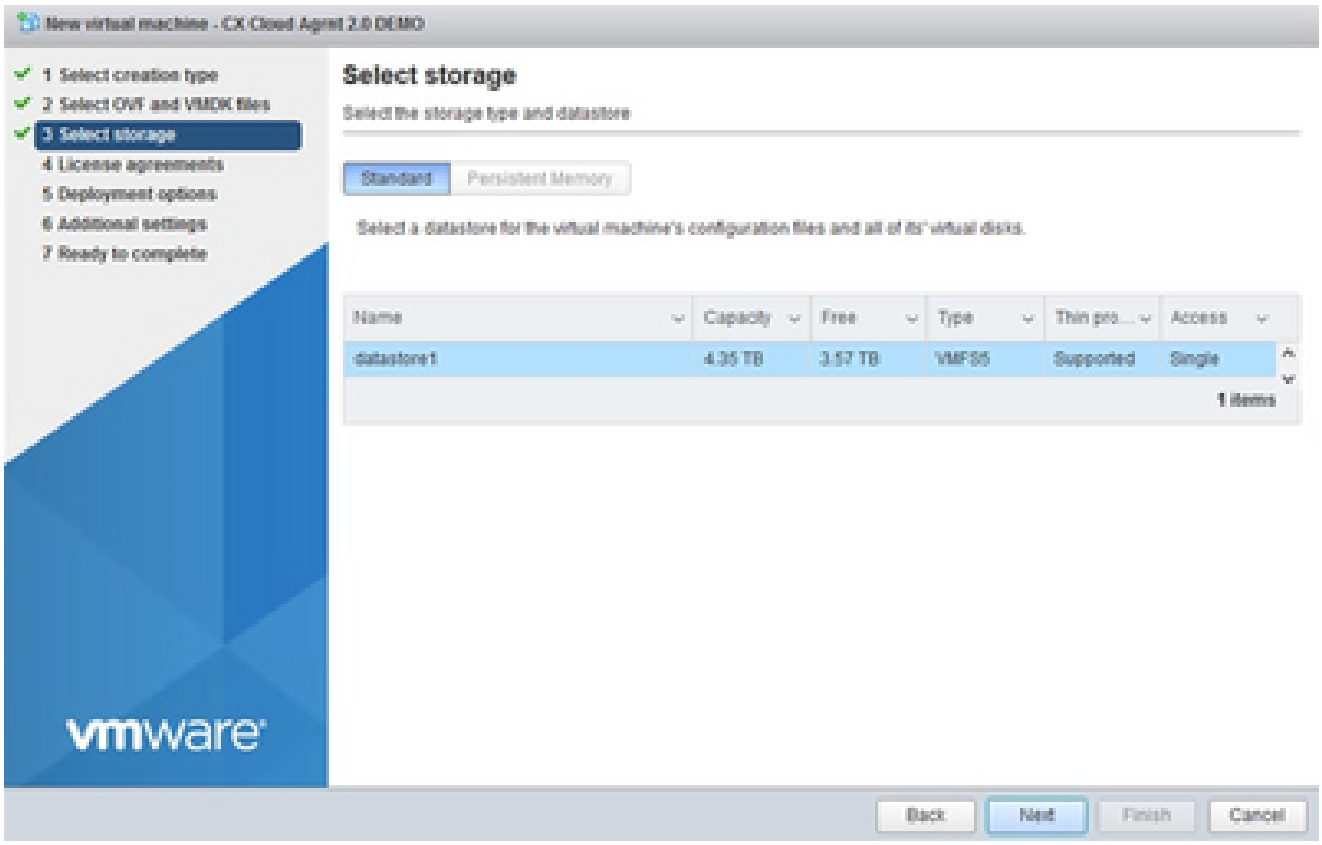
Sélectionner une ressource informatique

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



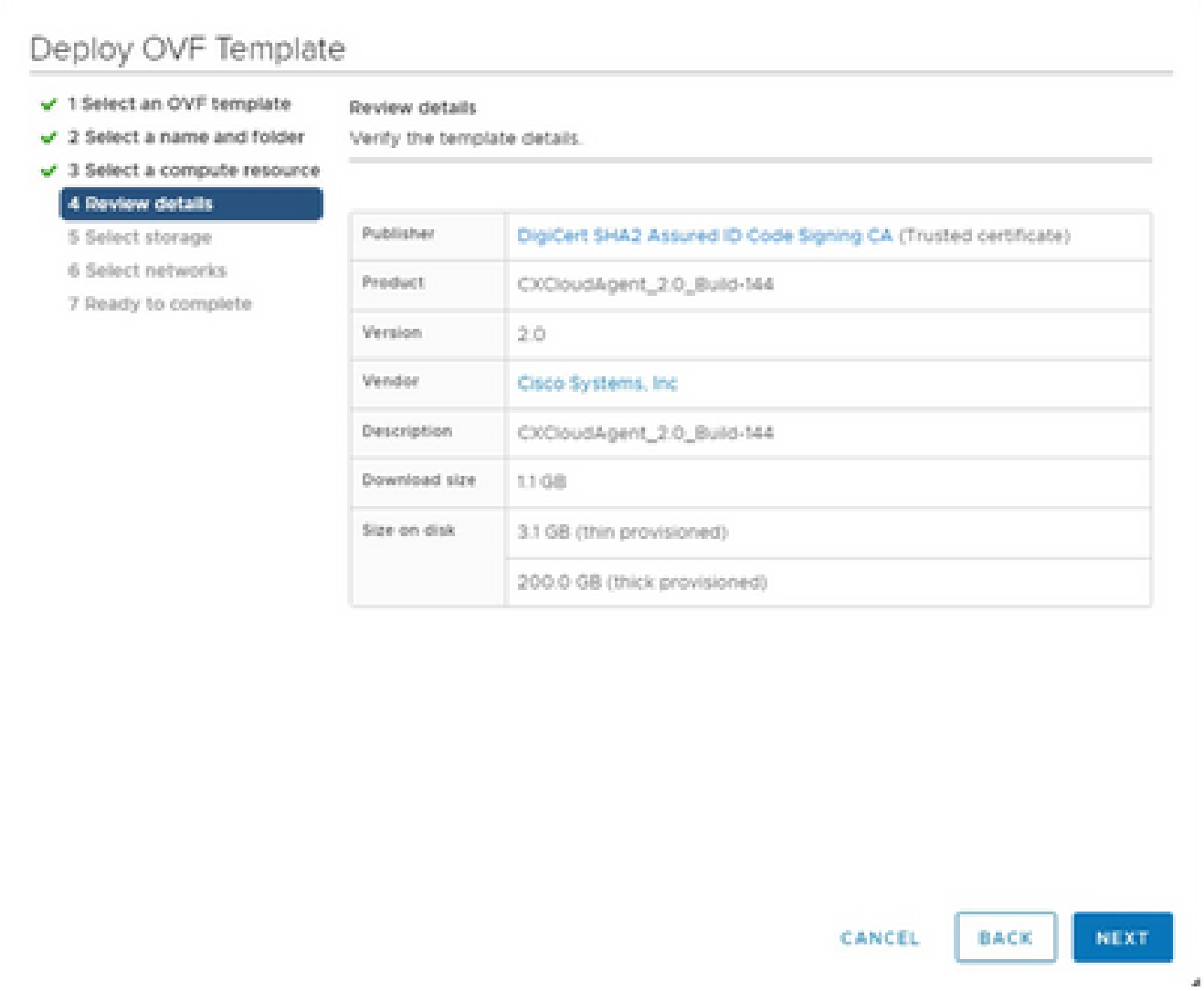
Examiner les détails

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



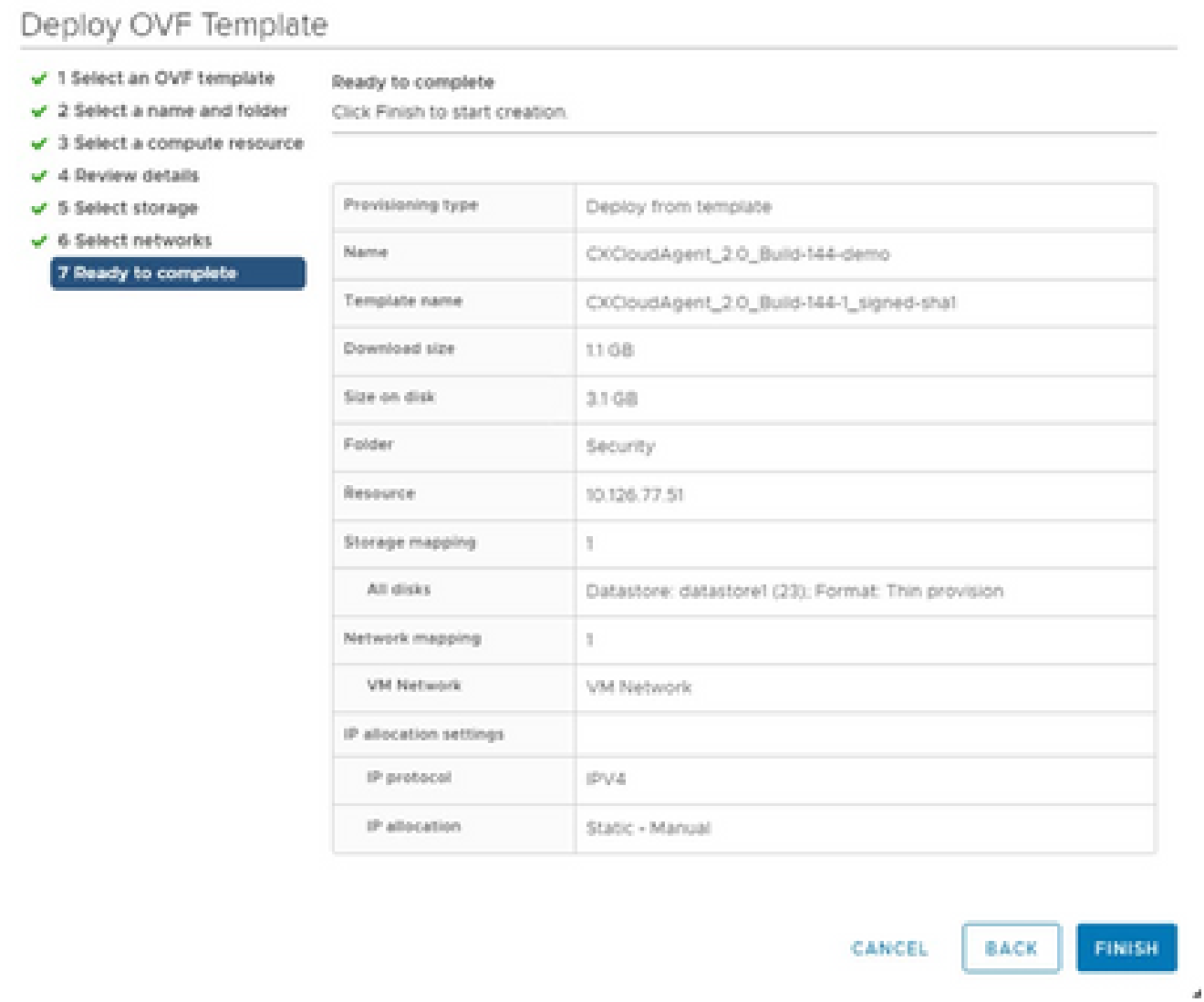
Sélectionner le stockage

10. Cliquez sur Next (Suivant).



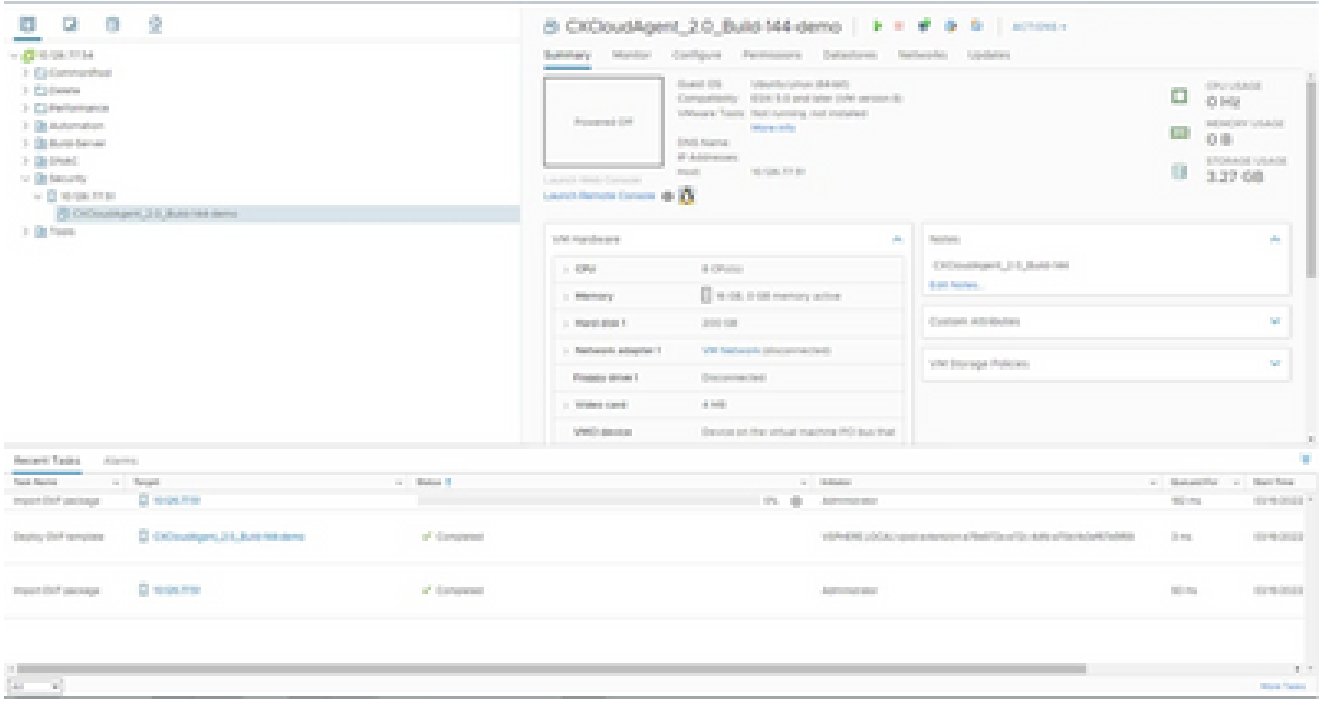
Sélectionner le réseau

11. Cliquez sur Finish (Terminer).



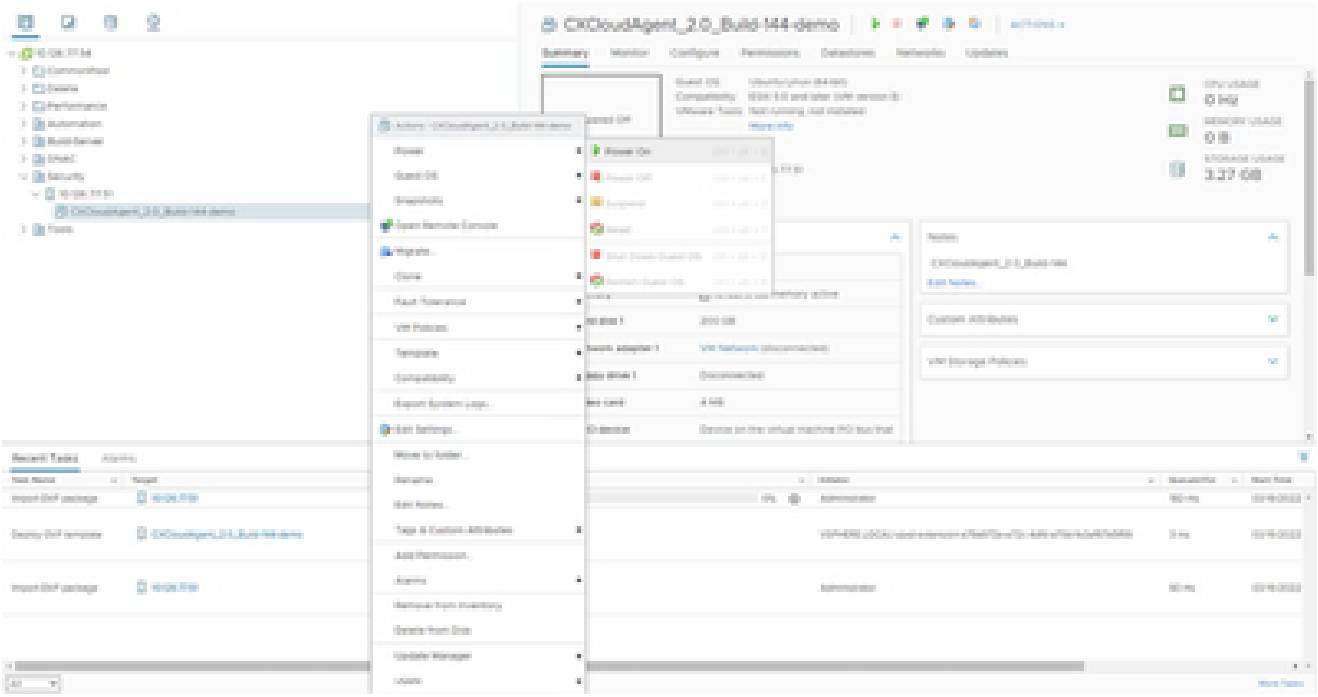
Prêt pour la confirmation

12. Cliquez sur le nom de la VM nouvellement ajoutée pour afficher son état.



VM ajoutée

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



Ouvrir la console

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

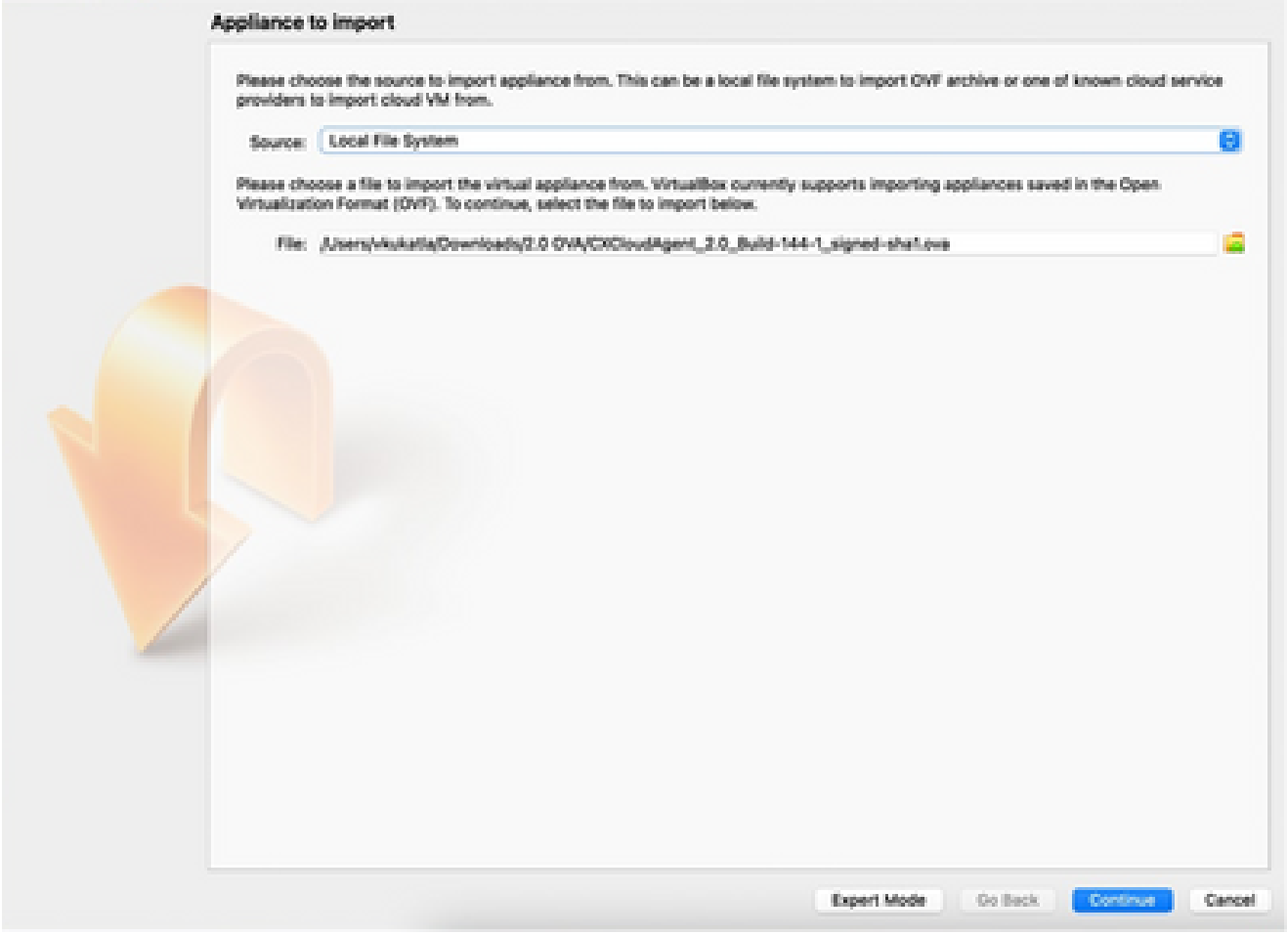
Installation d'Oracle Virtual Box 5.2.30

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

1. Ouvrez l'interface utilisateur d'Oracle VM et sélectionnez Fichier> Importer l'appliance.

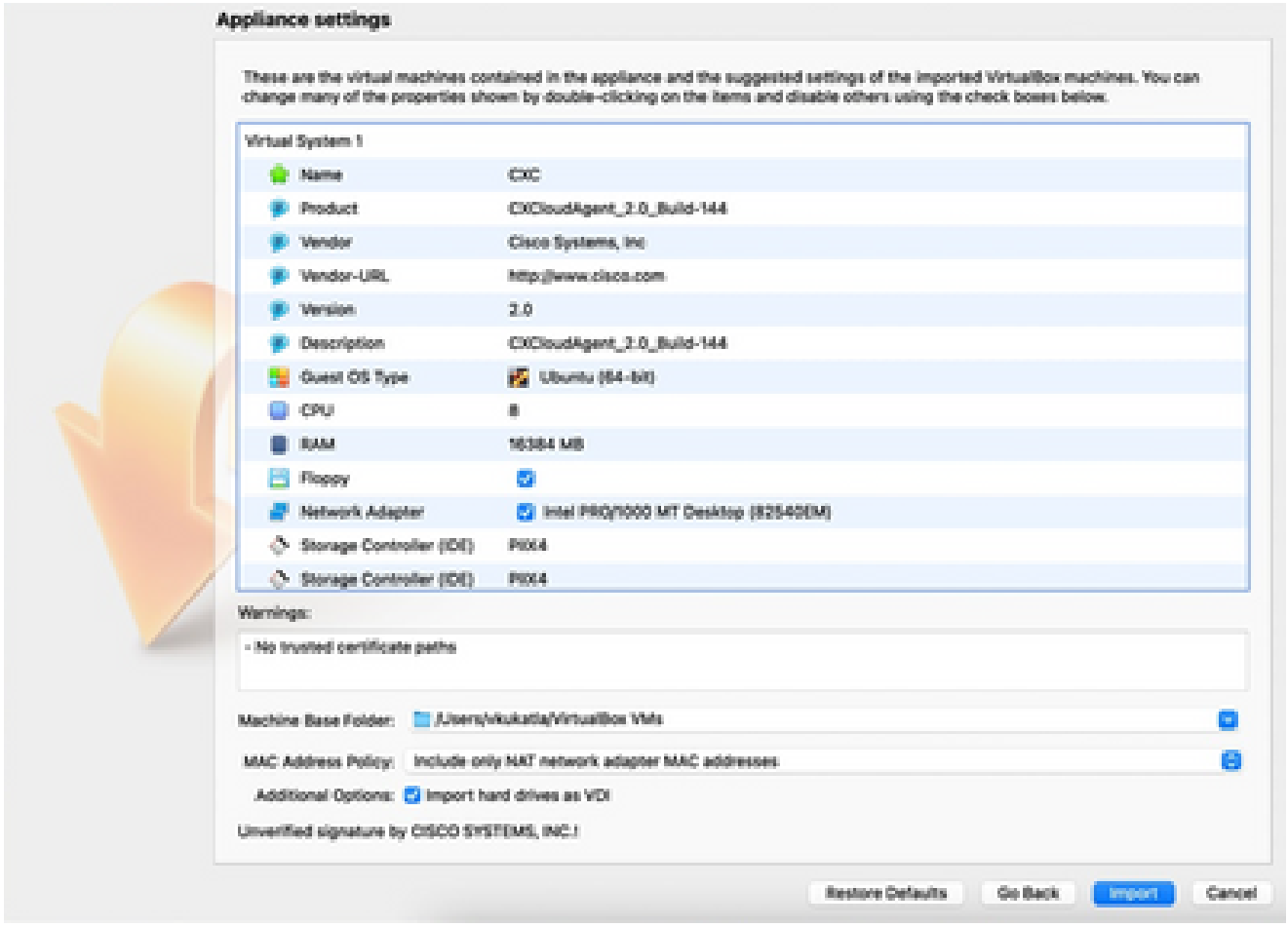
Machine virtuelle Oracle

2. Naviguez pour importer le fichier OVA.



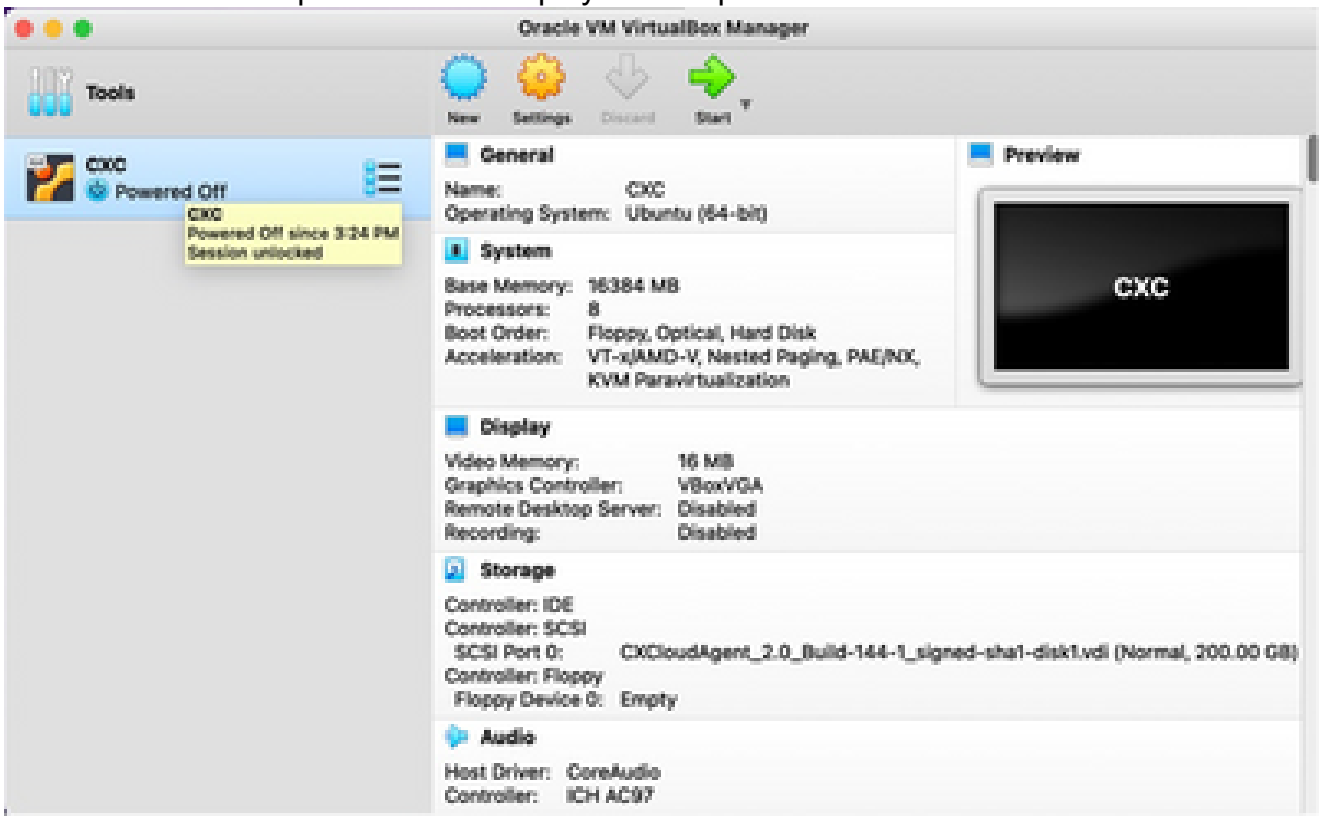
Sélectionner le fichier

3. Cliquez sur Import.

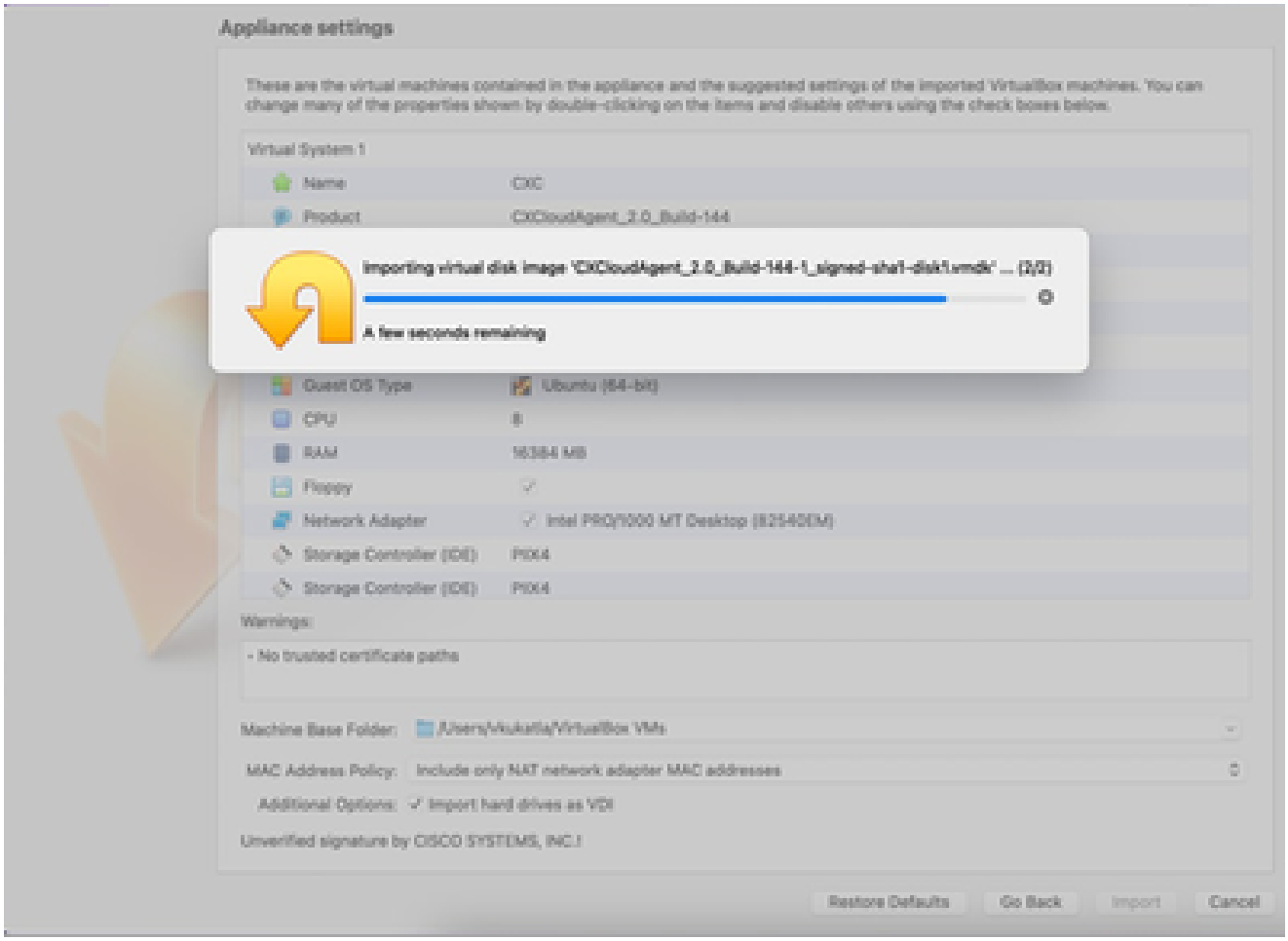


Fichier d'importation

4. Sélectionnez la VM qui vient d'être déployée et cliquez sur Démarrer.

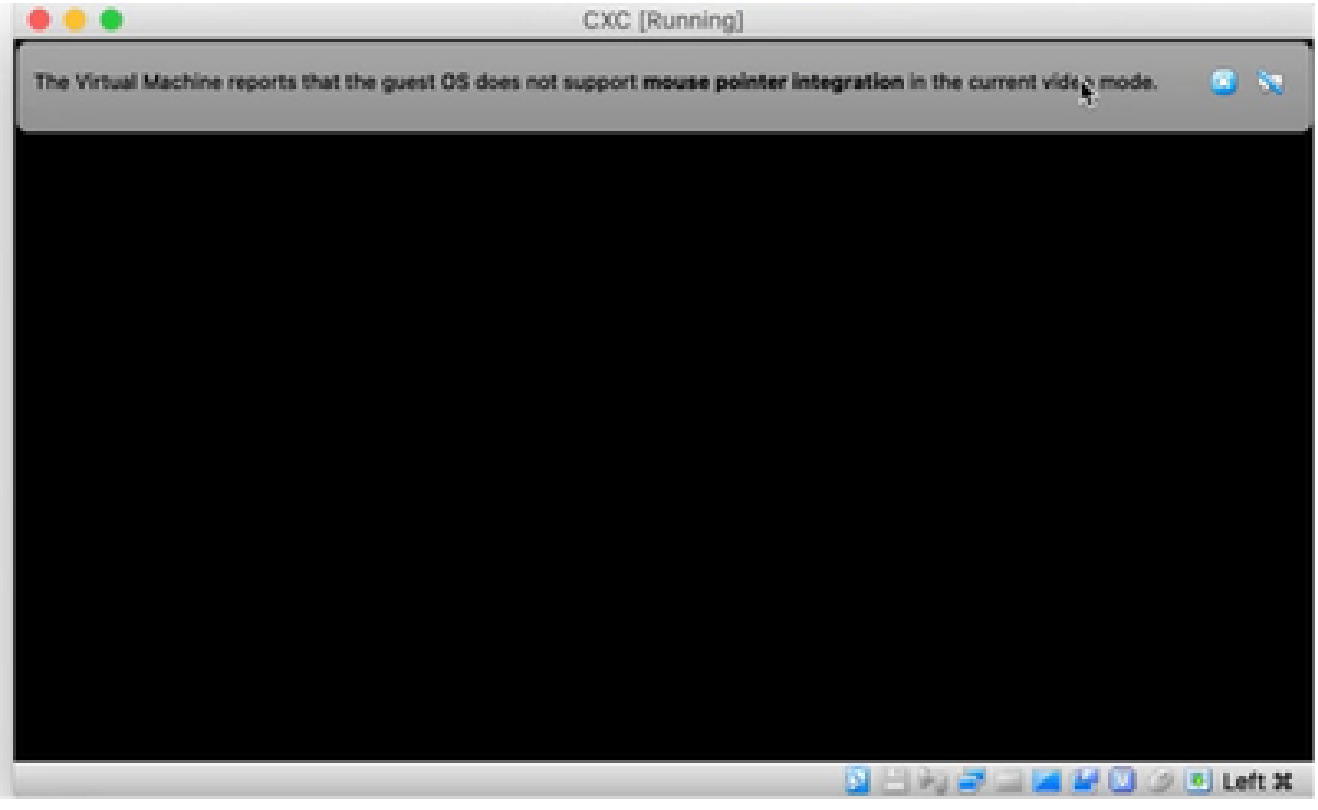


Démarrage de la console de machine virtuelle



Importation en cours

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



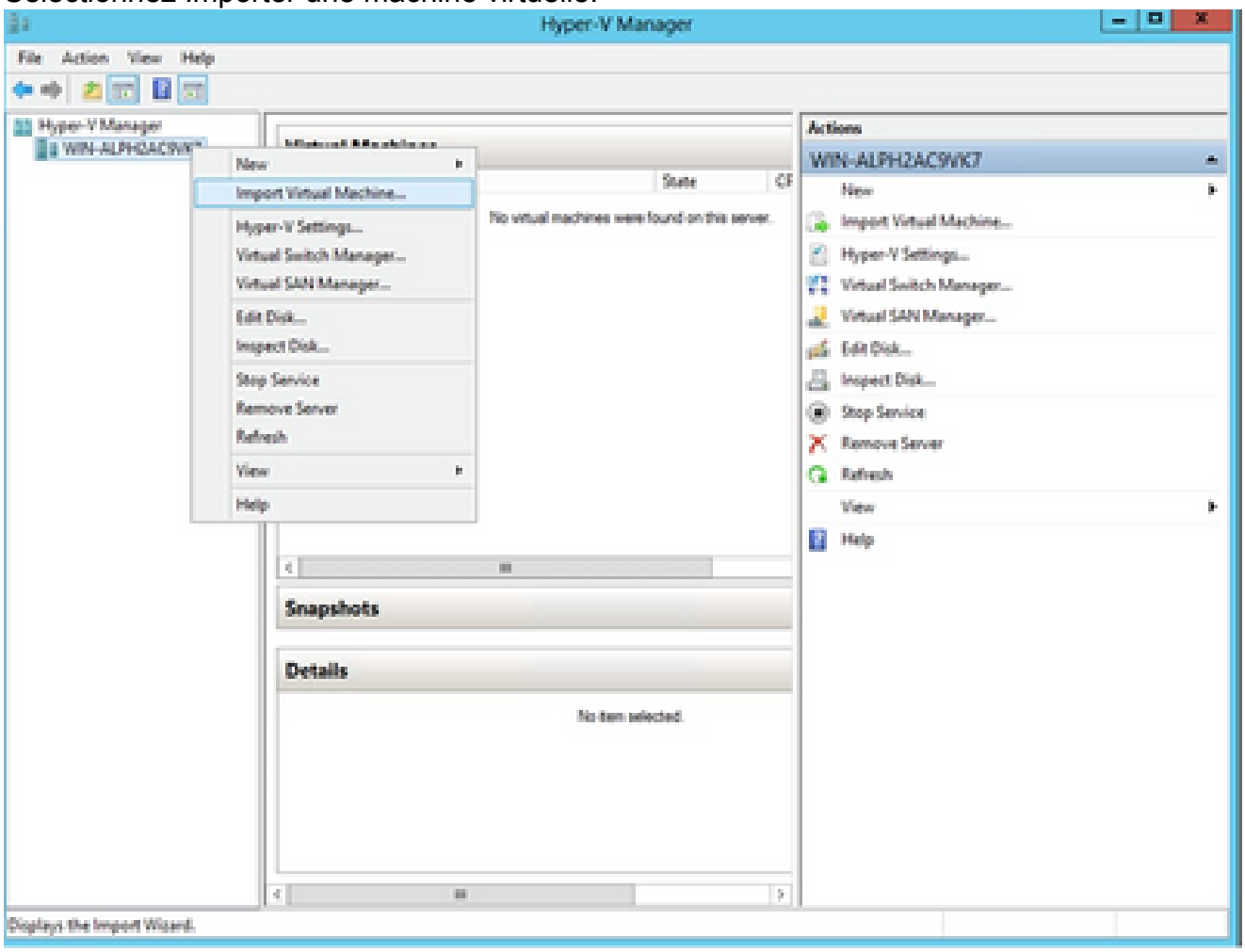
Ouvrir la console

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

Installation de Microsoft Hyper-V

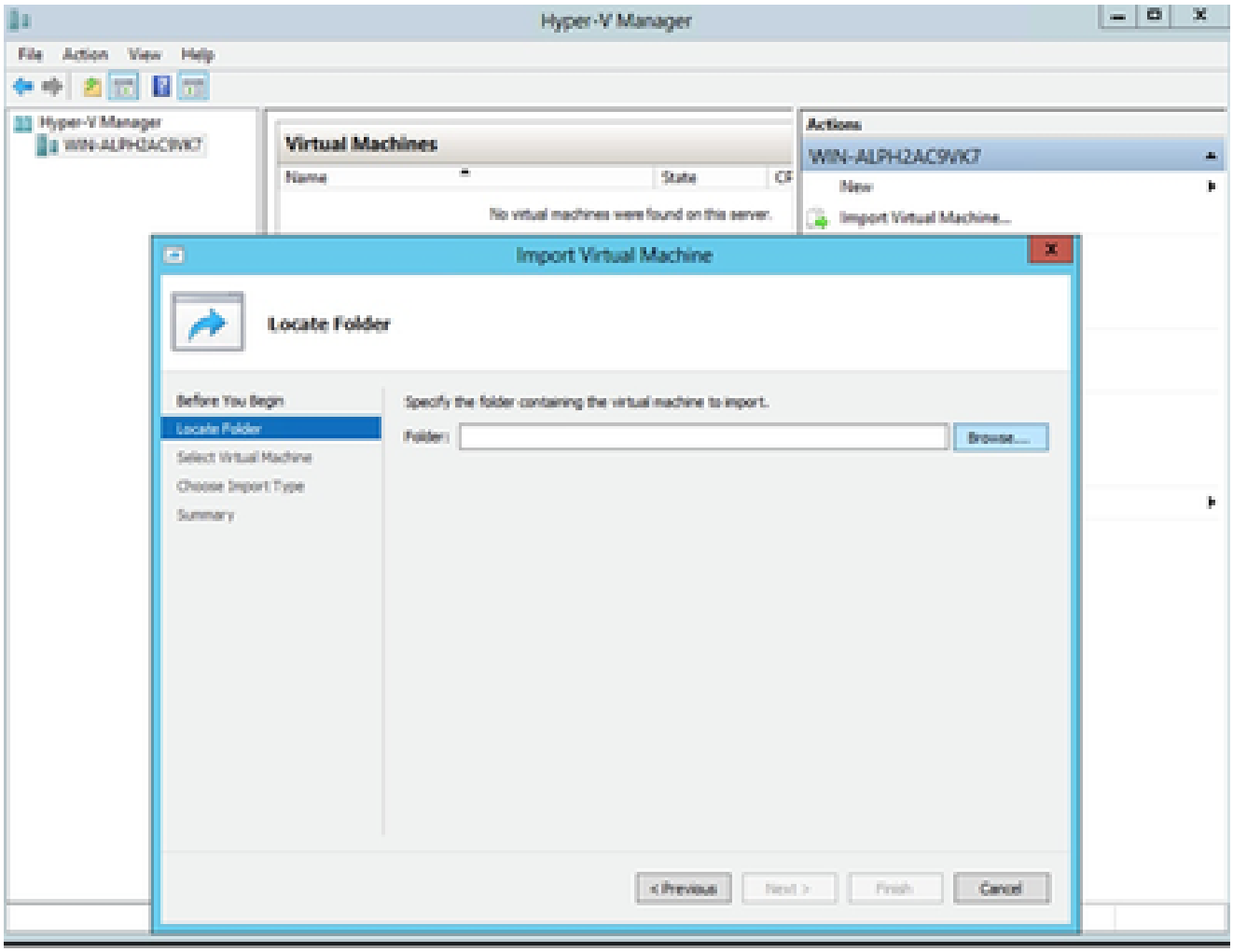
Effectuez les étapes suivantes :

1. Sélectionnez Importer une machine virtuelle.



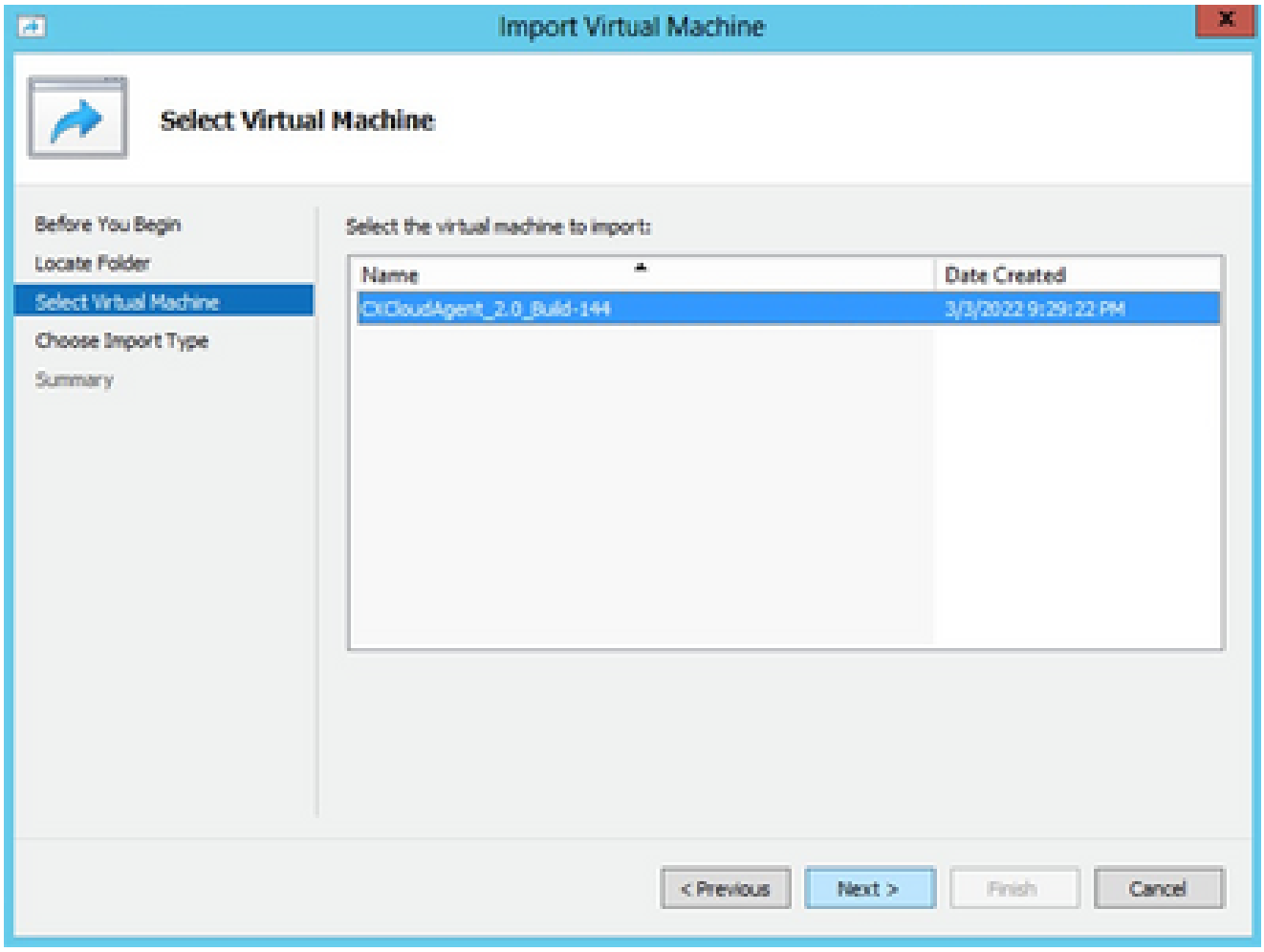
Gestionnaire Hyper-V

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



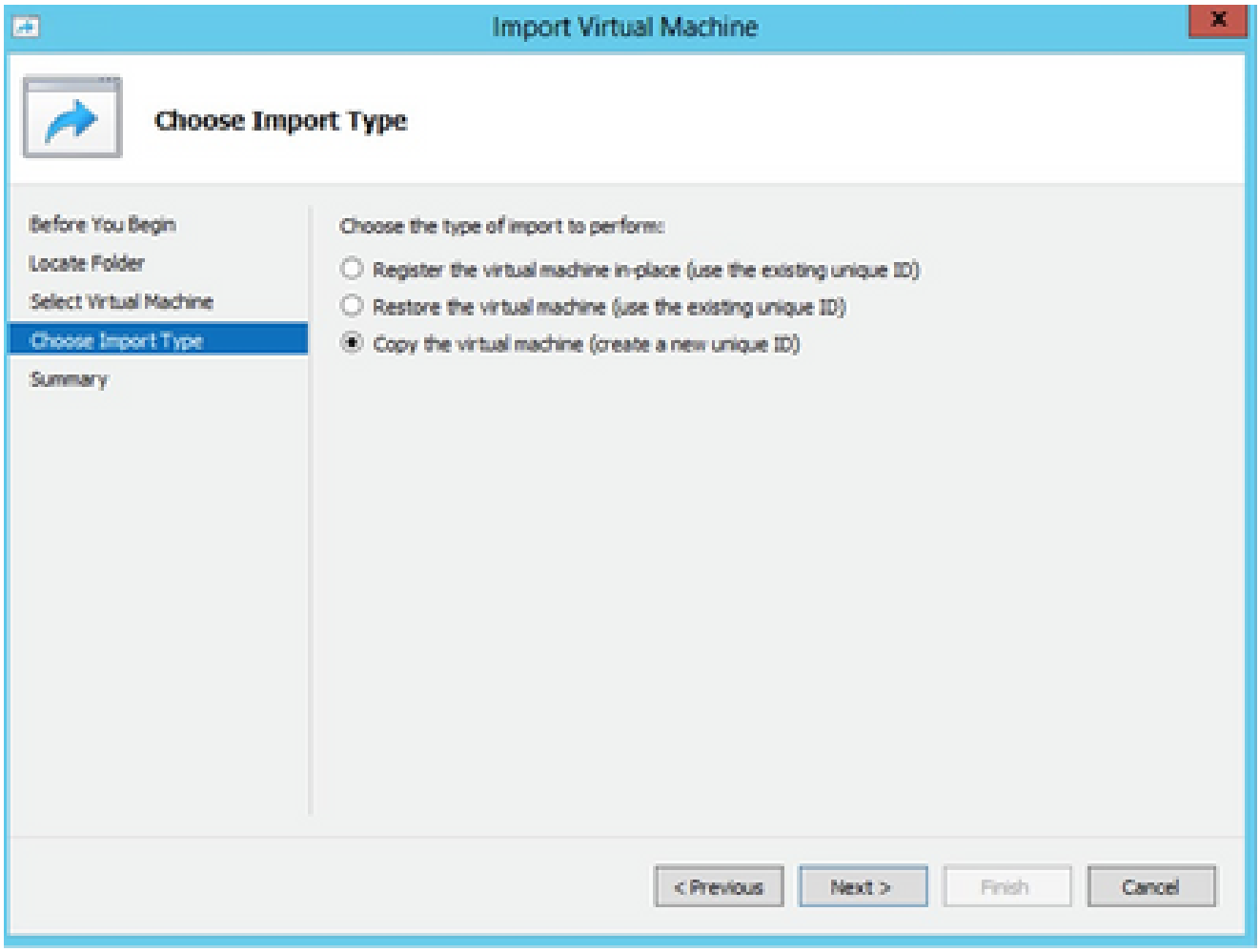
Dossier à importer

4. Sélectionnez la VM et cliquez sur Next (Suivant).



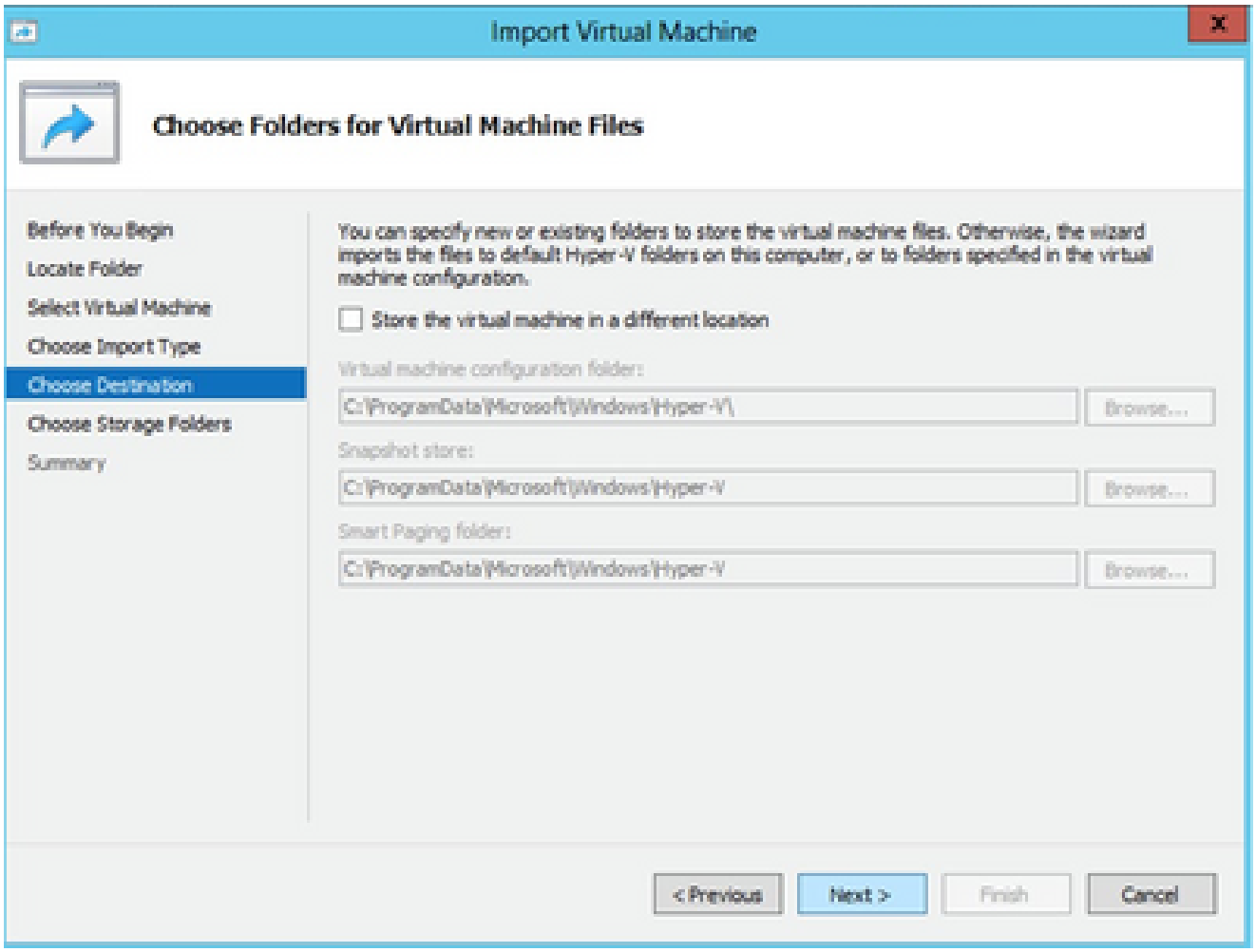
Sélectionner une machine virtuelle

5. Sélectionnez la case d'option Copier la machine virtuelle (créer un nouvel ID unique) et cliquez sur Suivant.



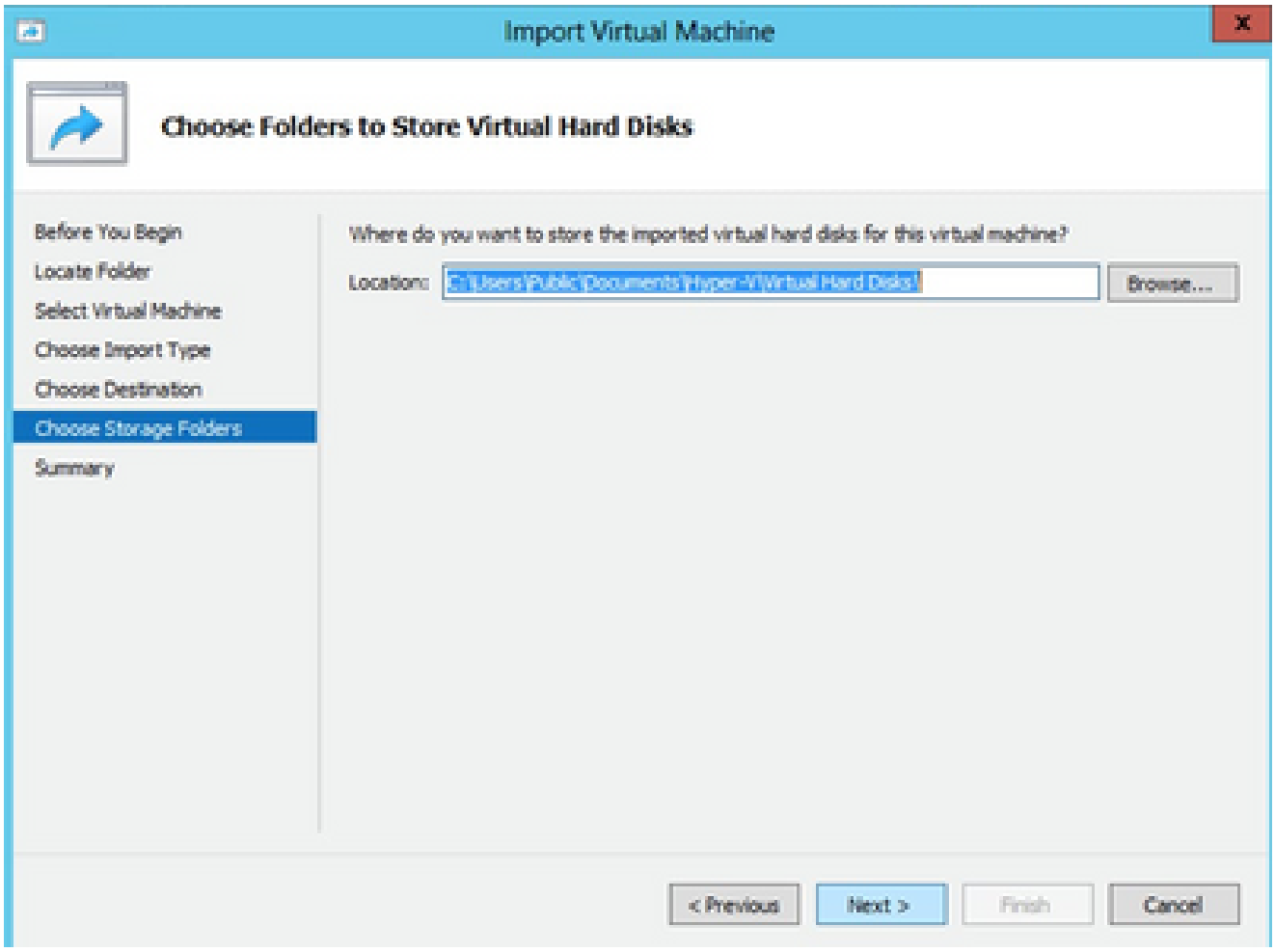
Type d’importation

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 (Suivant).



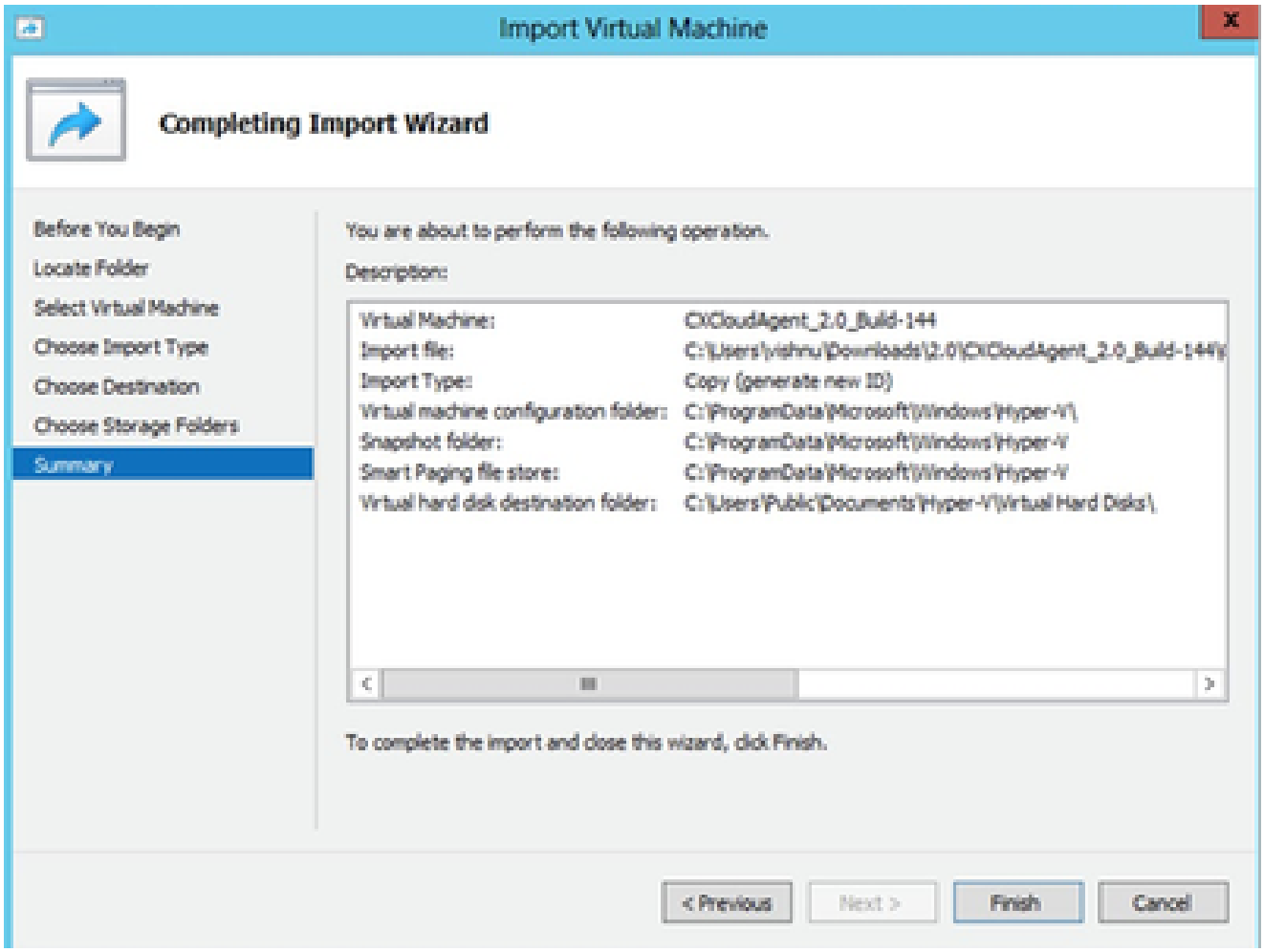
Choisir des dossiers pour les fichiers de machine virtuelle

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 (Suivant).



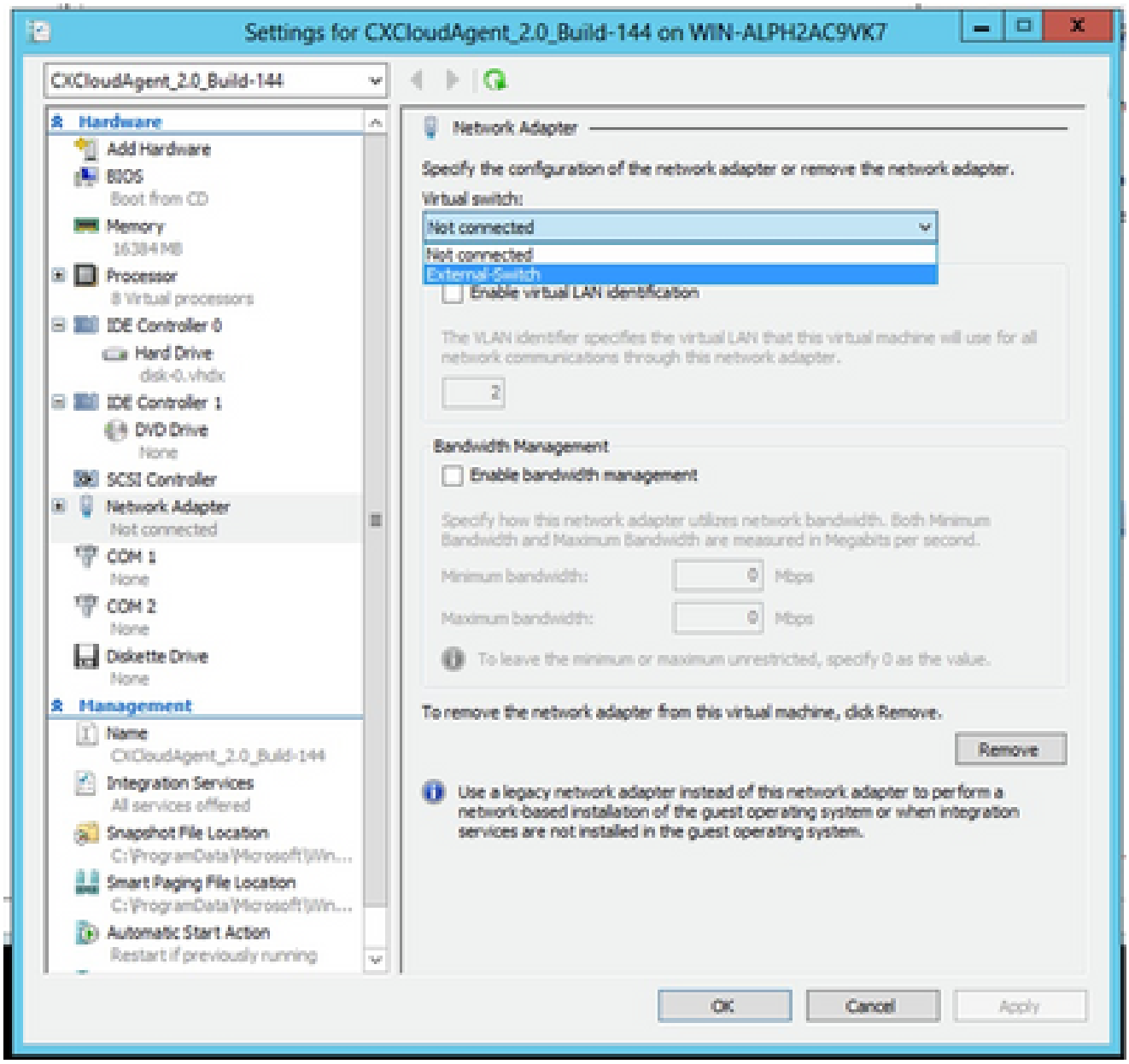
Dossier de stockage des disques durs virtuels

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



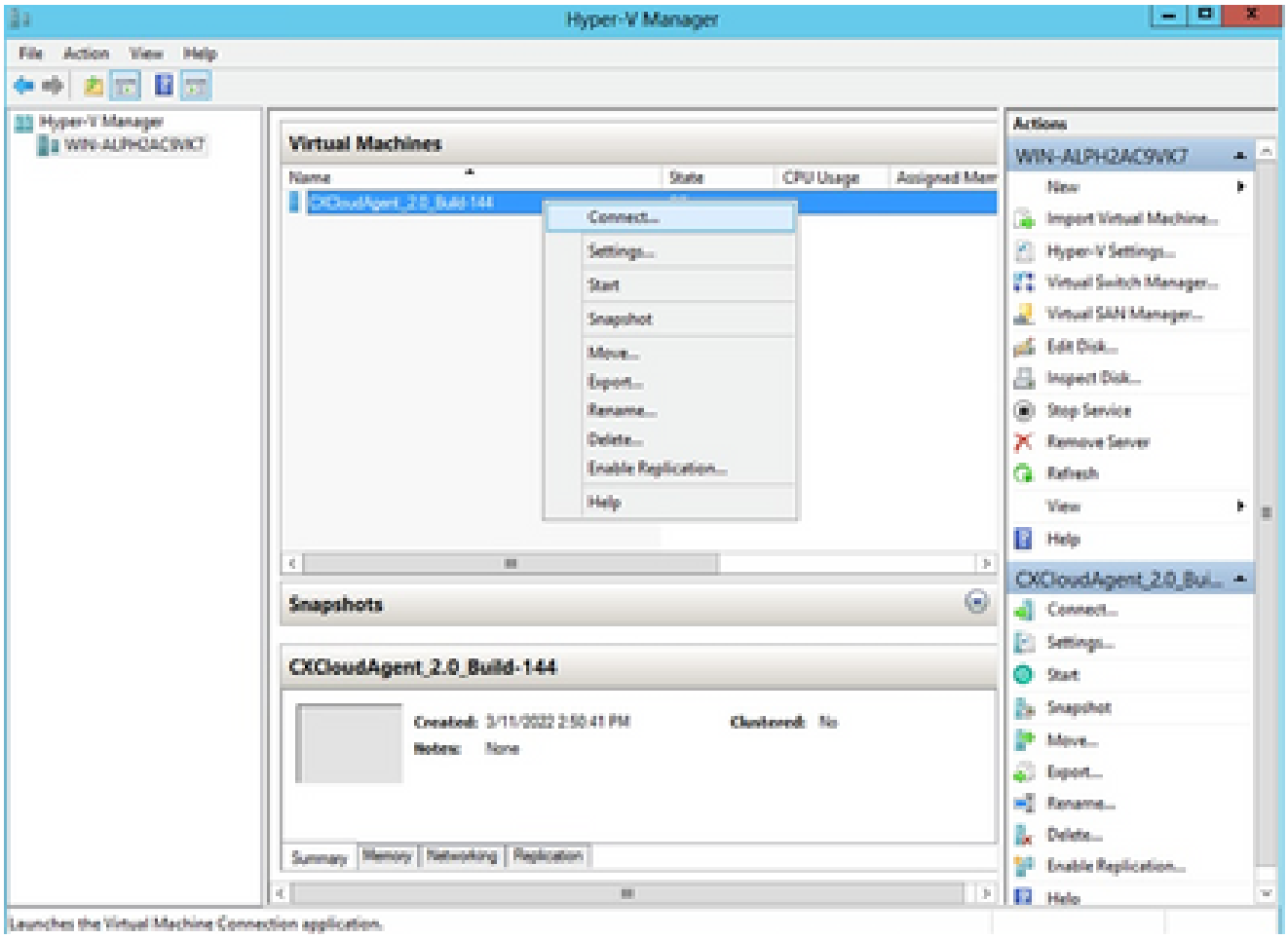
Résumé

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



Commutateur virtuel

13. Sélectionnez Connect pour démarrer la machine virtuelle.

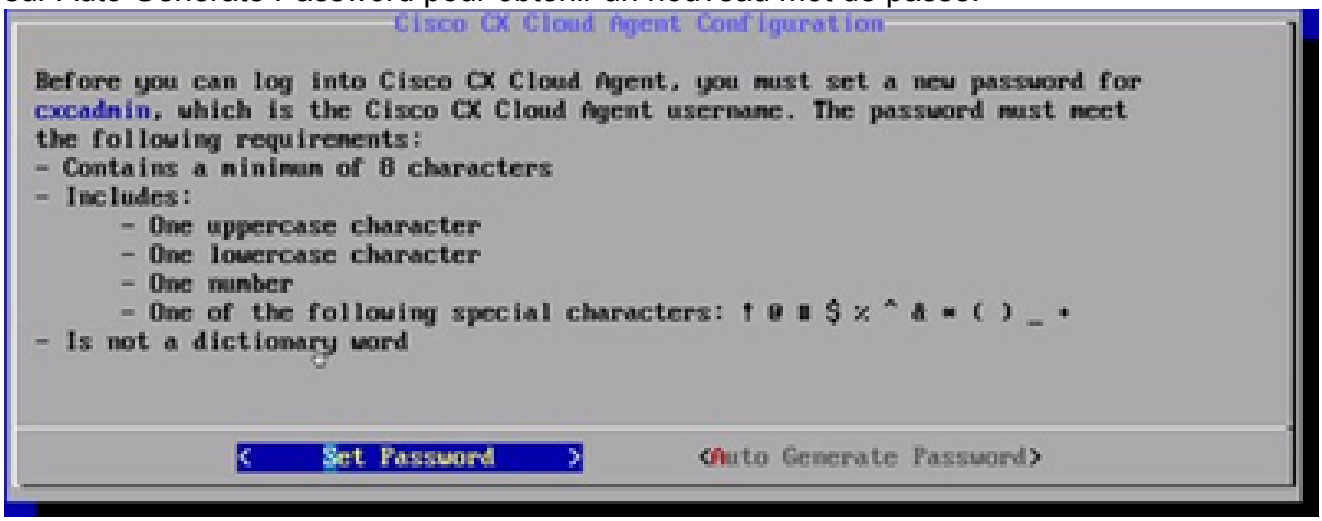


Démarrage de la machine virtuelle

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

Configuration du réseau

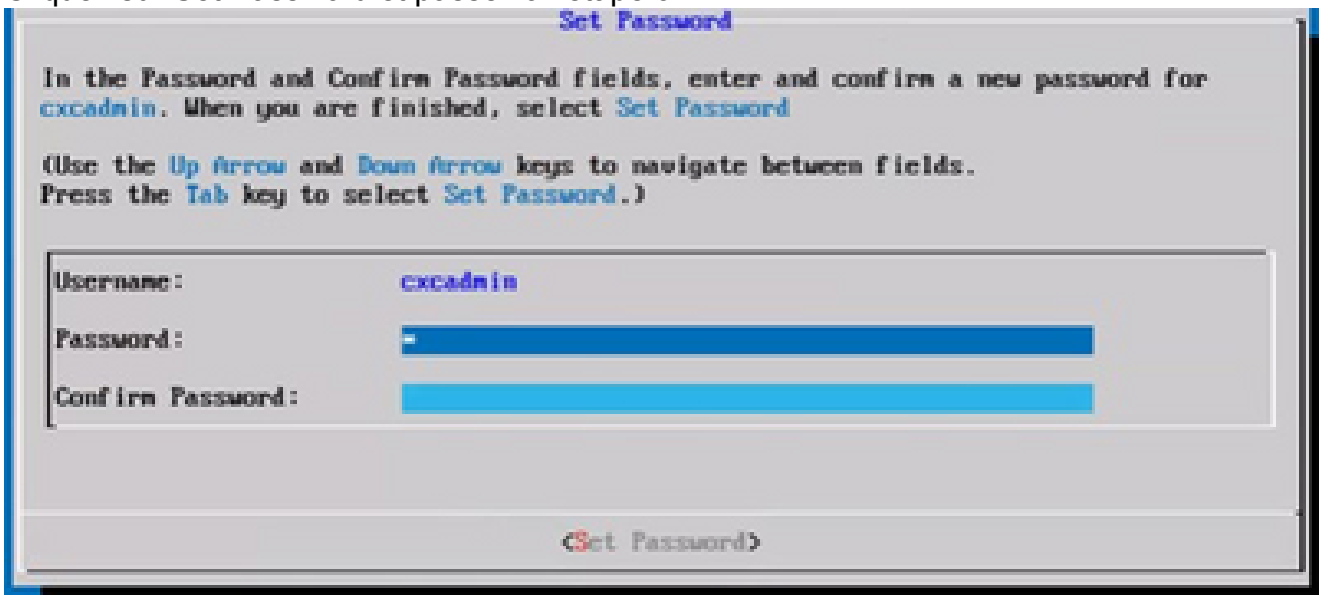
1. Cliquez sur Set Password pour ajouter un nouveau mot de passe pour cxcadmin OU cliquez sur Auto Generate Password pour obtenir un nouveau mot de passe.



Définir un 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.



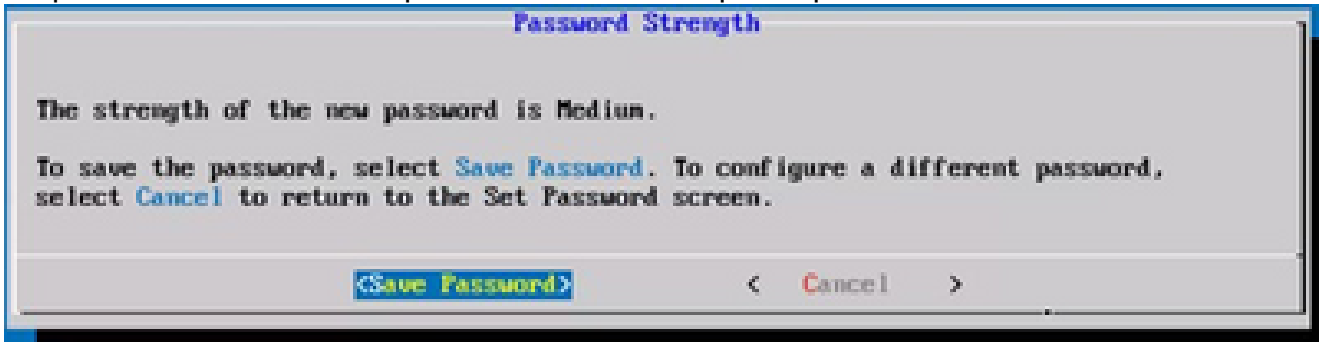
Nouveau mot de passe

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

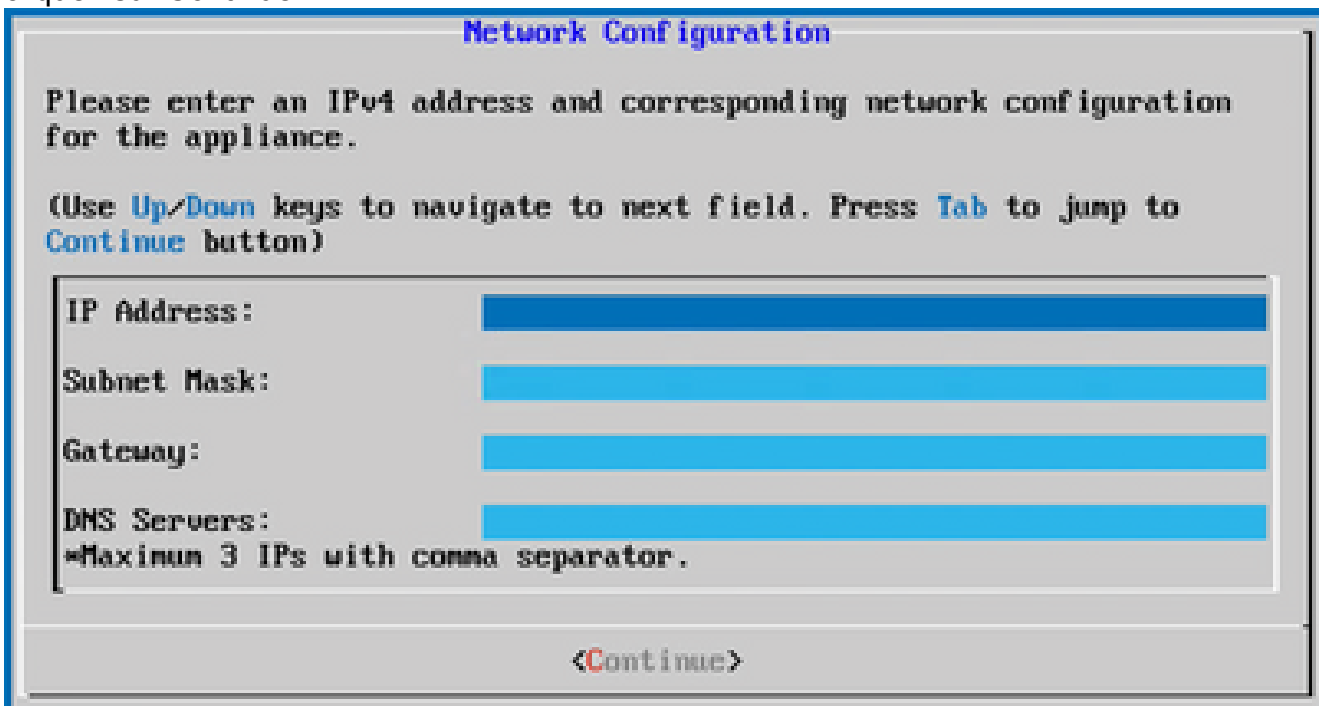
3. Cliquez sur Save Password pour utiliser le mot de passe pour l'authentification.



Enregistrez le mot de passe.

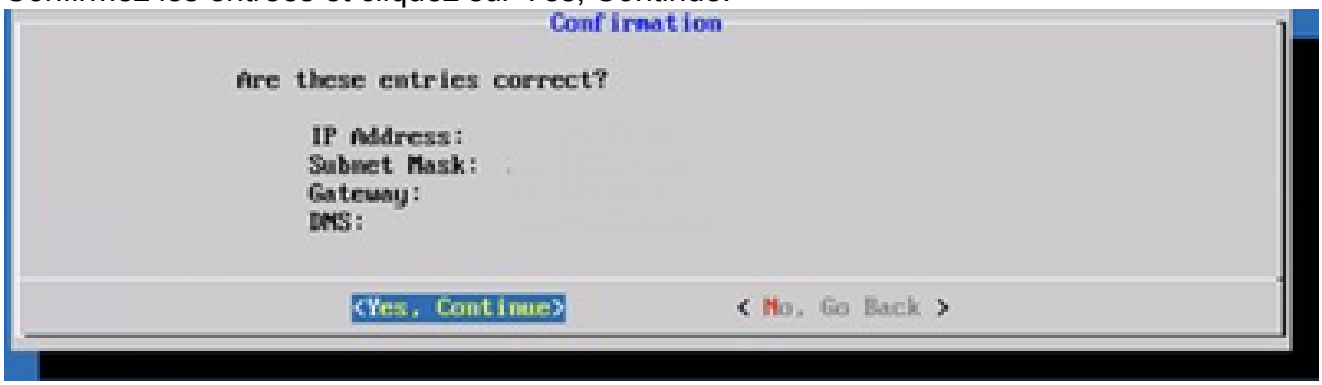
4. Saisissez l'adresse IP, le masque de sous-réseau, la passerelle et le serveur DNS, puis

cliquez sur Continuer.



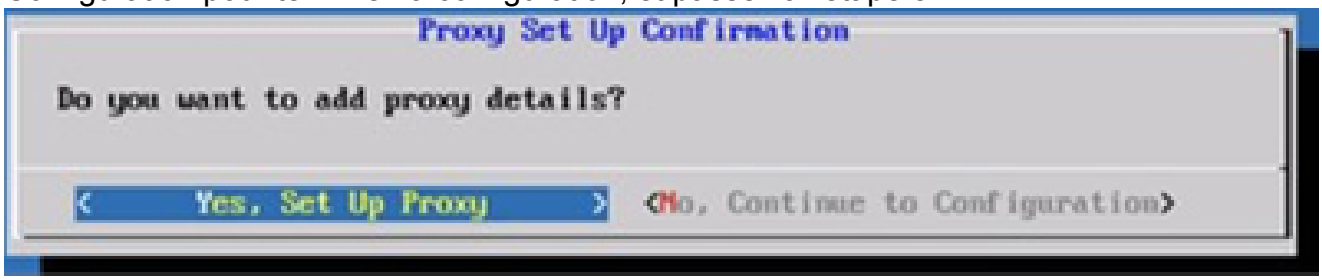
Configuration du réseau

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



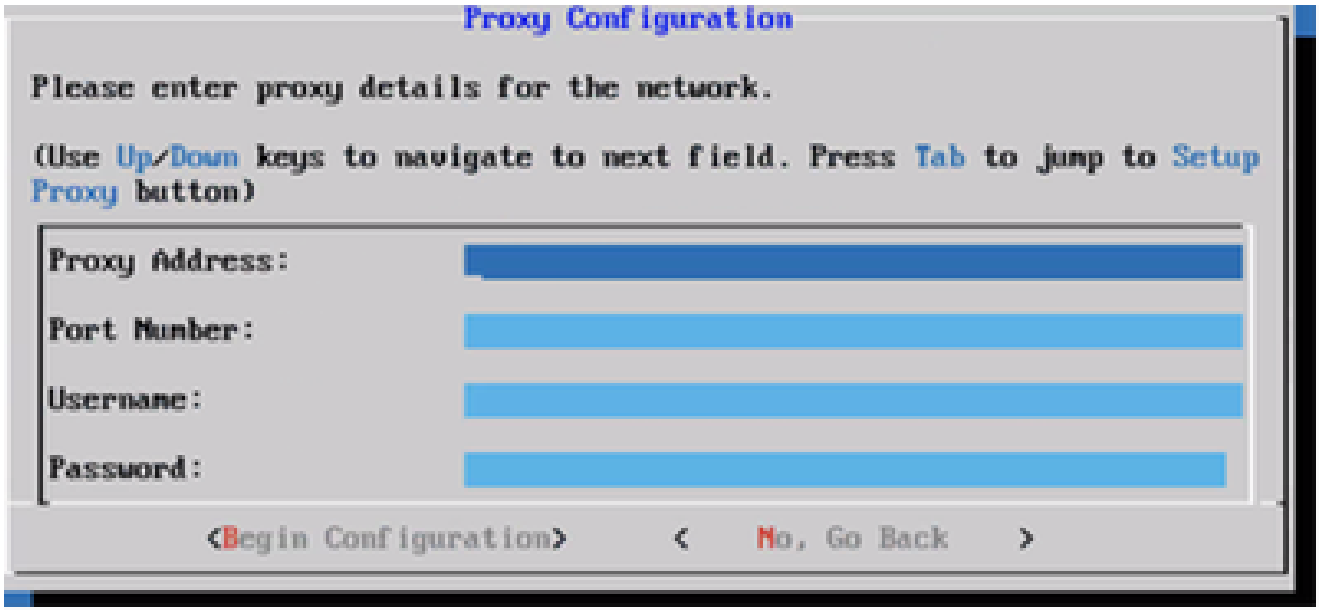
Configuration

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



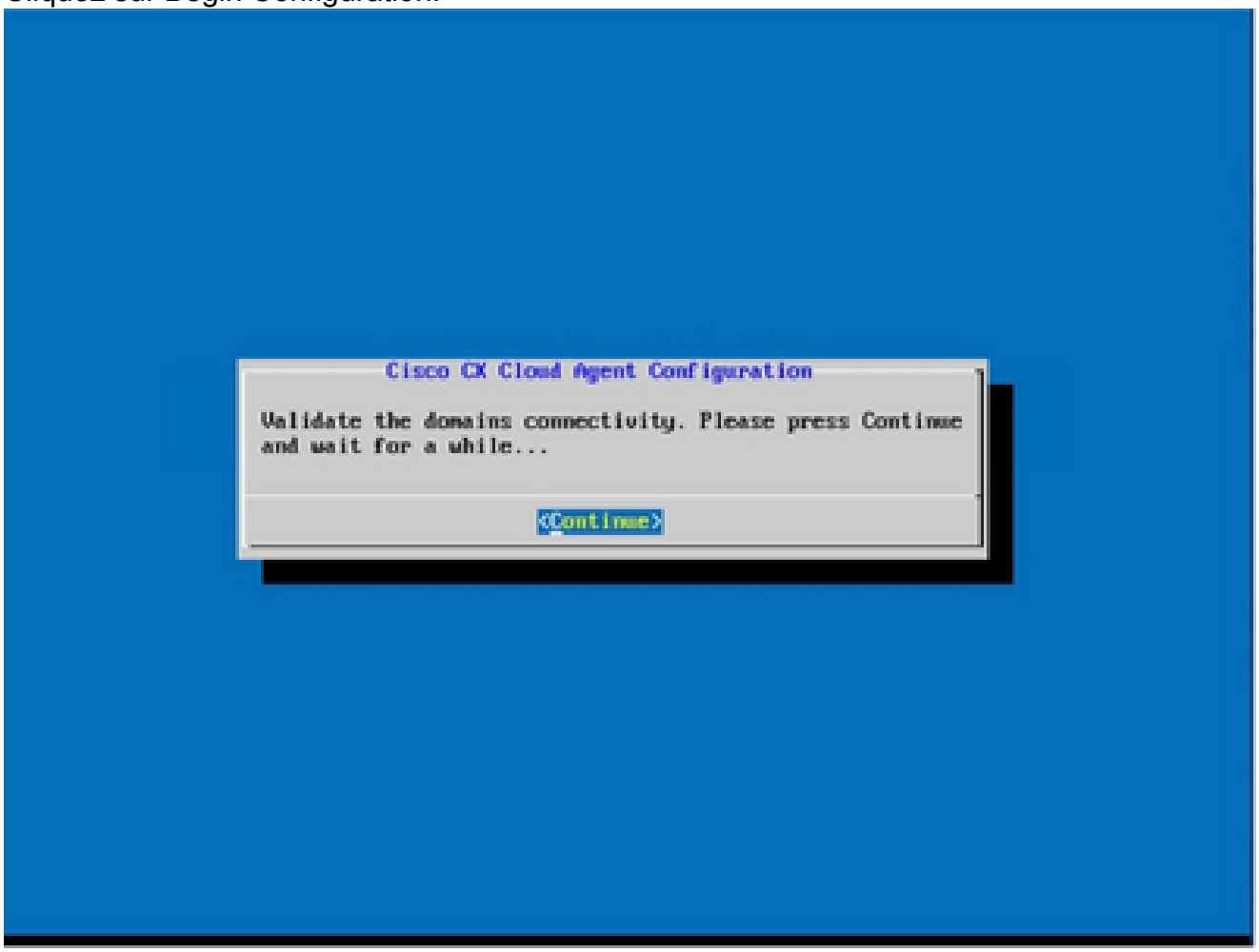
Mise à disposition du proxy

7. Saisissez l’adresse proxy, le numéro de port, le nom d’utilisateur et le mot de passe.



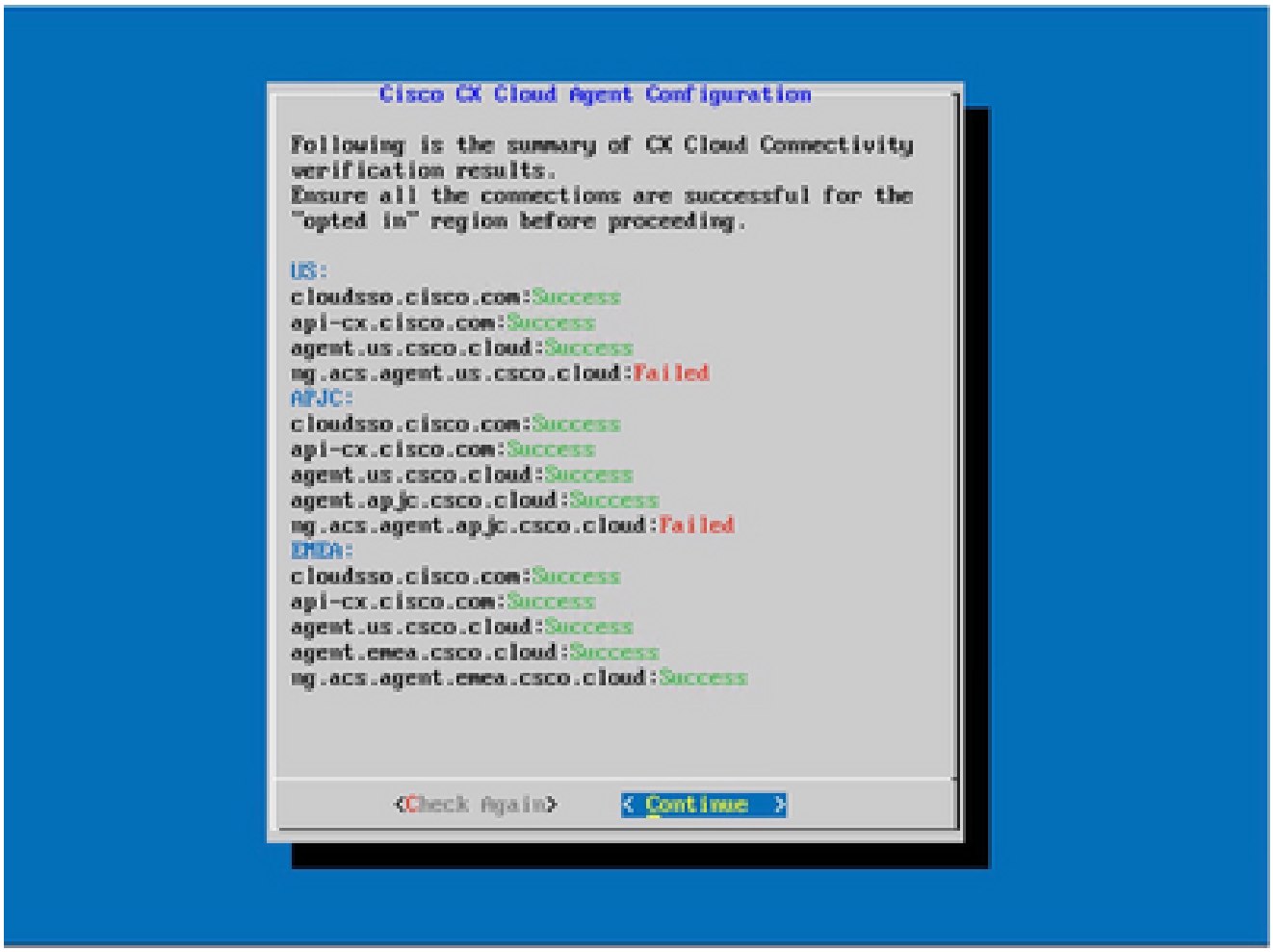
Configuration du proxy

8. Cliquez sur Begin Configuration.



Commencer la configuration

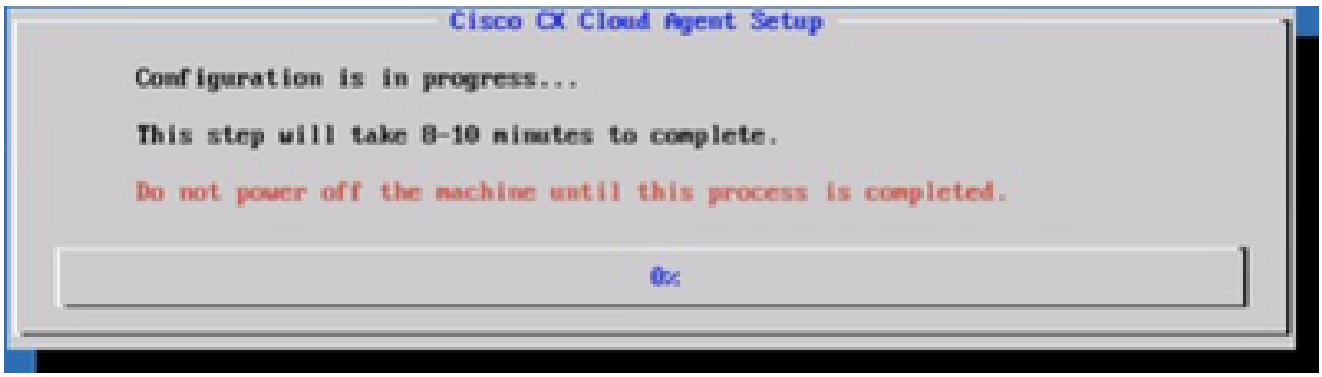
9. Cliquez sur Continue.



La configuration continue

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

Remarque : si les domaines ne sont pas accessibles, le client doit corriger l'accessibilité des domaines en modifiant 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.

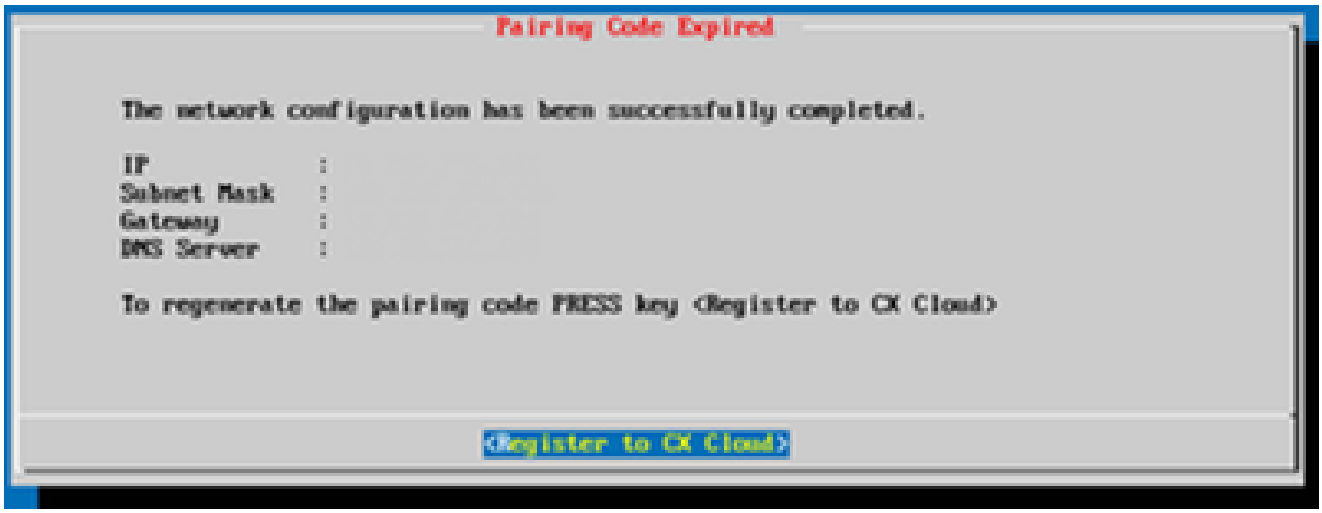


Configuration en cours

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

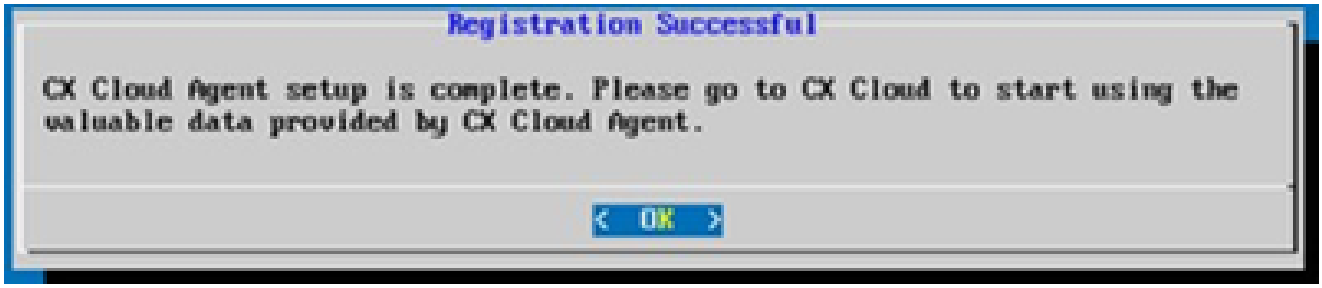
Code de jumelage

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



Code expiré

13. Click OK.



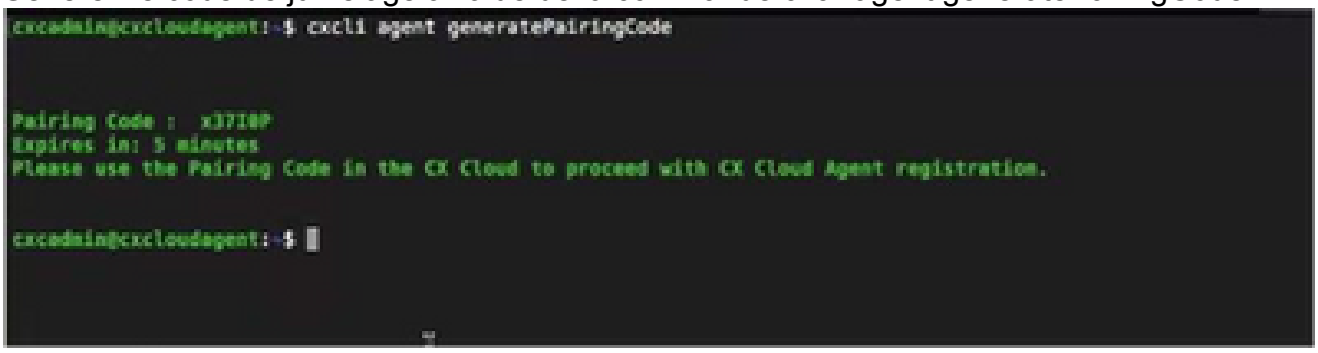
Inscription réussie

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 de jumelage 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.

Configurer Cisco DNA Center pour transférer Syslog vers CX Cloud Agent

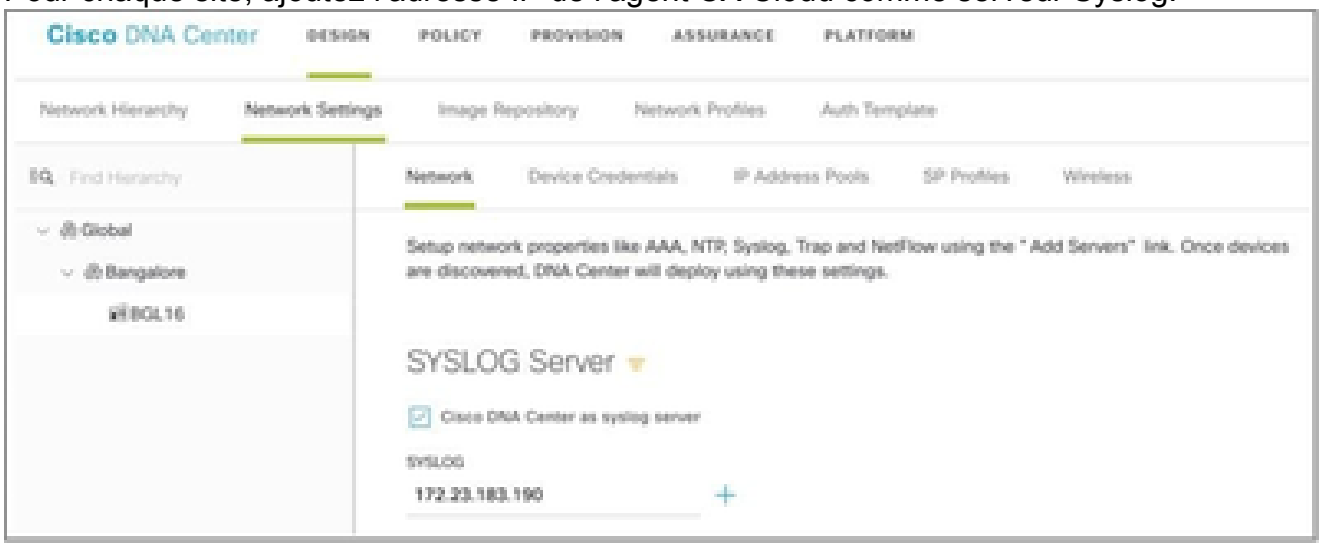
Conditions préalables

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 DNA Center Virtual Appliance sont prises en charge par Cisco DNA Center

Configuration du paramètre Syslog Forward

Pour configurer le transfert Syslog vers CX Cloud Agent dans Cisco DNA Center, 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.



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.

Configurer d'autres ressources pour transférer Syslog à CX Cloud Agent

Les périphériques doivent être configurés pour envoyer des messages Syslog à CX Cloud Agent afin d'utiliser la fonctionnalité de gestion des pannes de CX Cloud.

Remarque : seuls les périphériques Campus Success Track de niveau 2 peuvent configurer d'autres ressources pour transférer Syslog.

Serveurs Syslog existants avec fonctionnalité de transfert

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

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

Serveurs Syslog existants sans fonction de transfert OU sans serveur Syslog

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

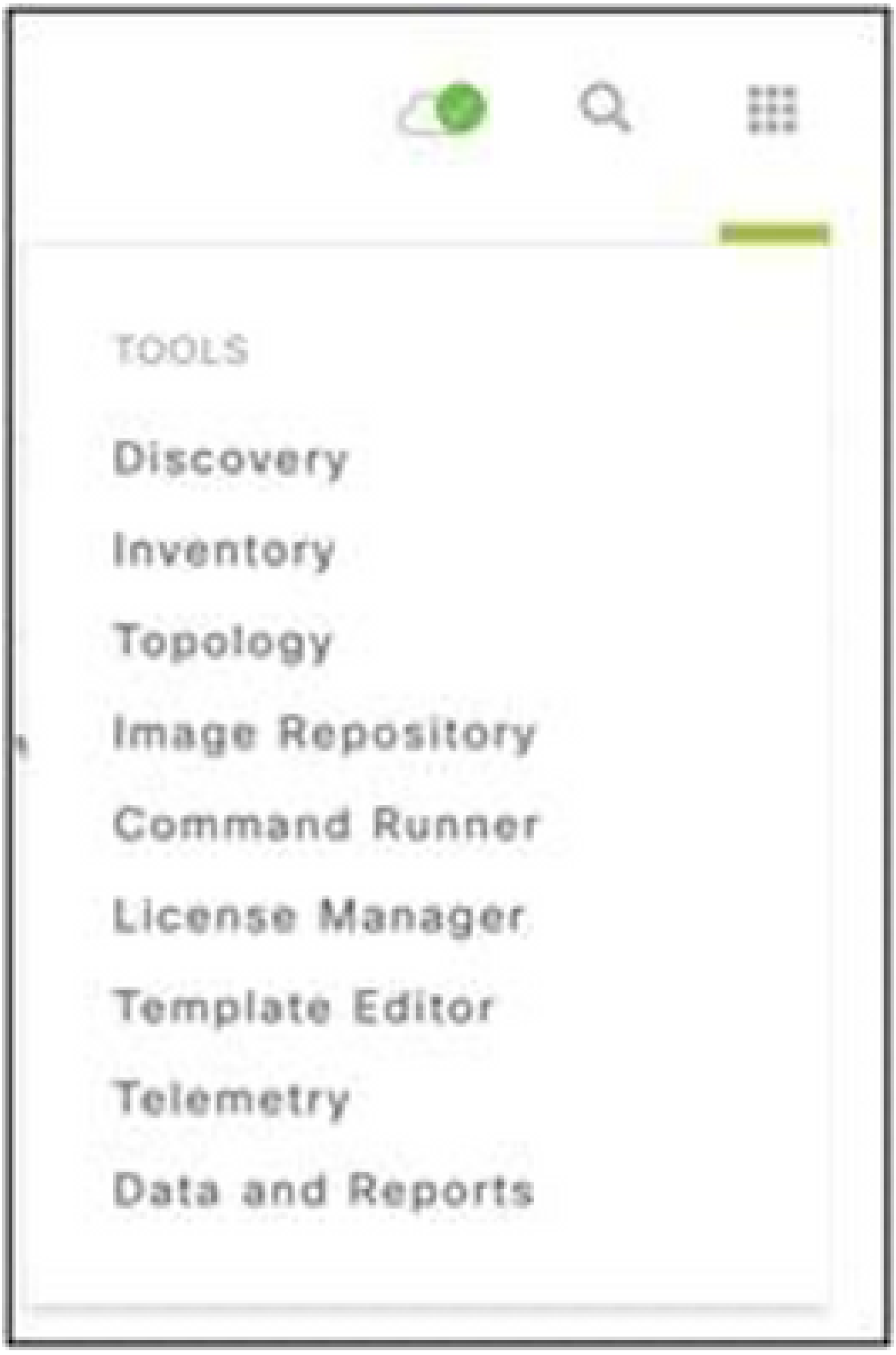
Guide de configuration de Cisco IOS® XE

Guide de configuration du contrôleur sans fil AireOS

Activer les paramètres Syslog au niveau des informations

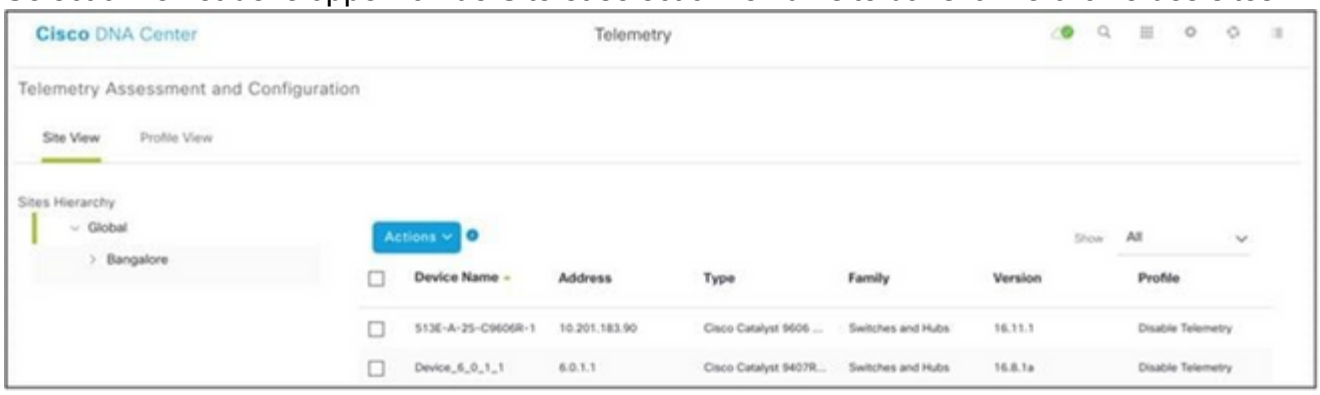
Pour rendre le niveau d'informations Syslog visible, procédez comme suit :

1. Accédez à Outils>Télémétrie.


TOOLS
Discovery
Inventory
Topology
Image Repository
Command Runner
License Manager
Template Editor
Telemetry
Data and Reports

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

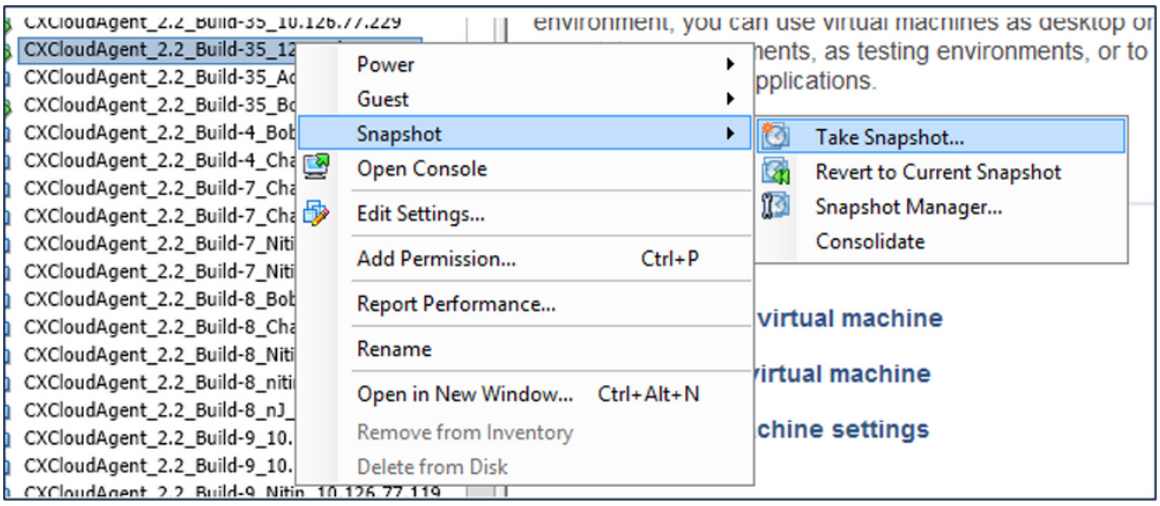
Sauvegarde et restauration de la machine virtuelle du cloud CX

Il est recommandé de préserver l'état et les données d'une machine virtuelle CX Cloud 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.

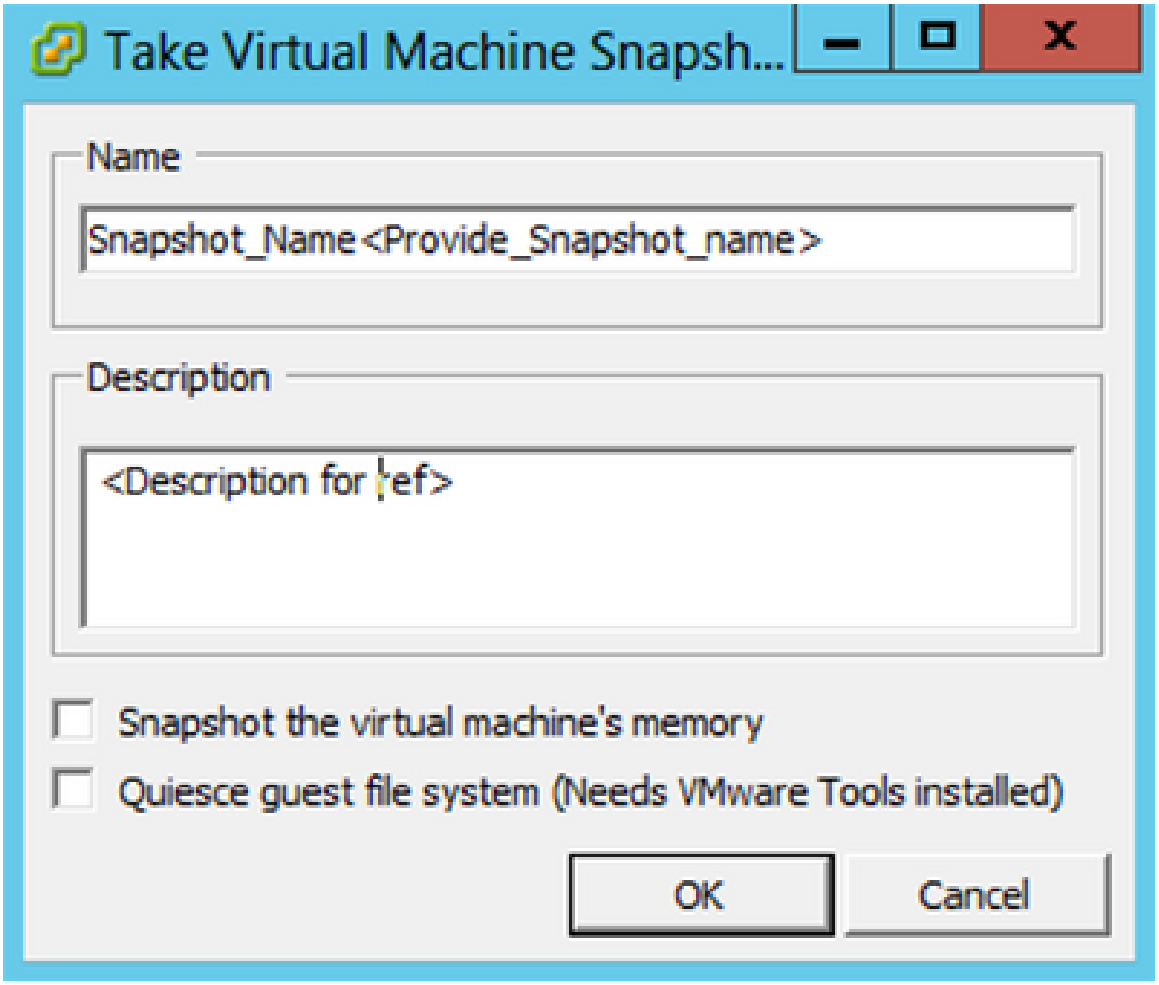
Sauvegarder

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



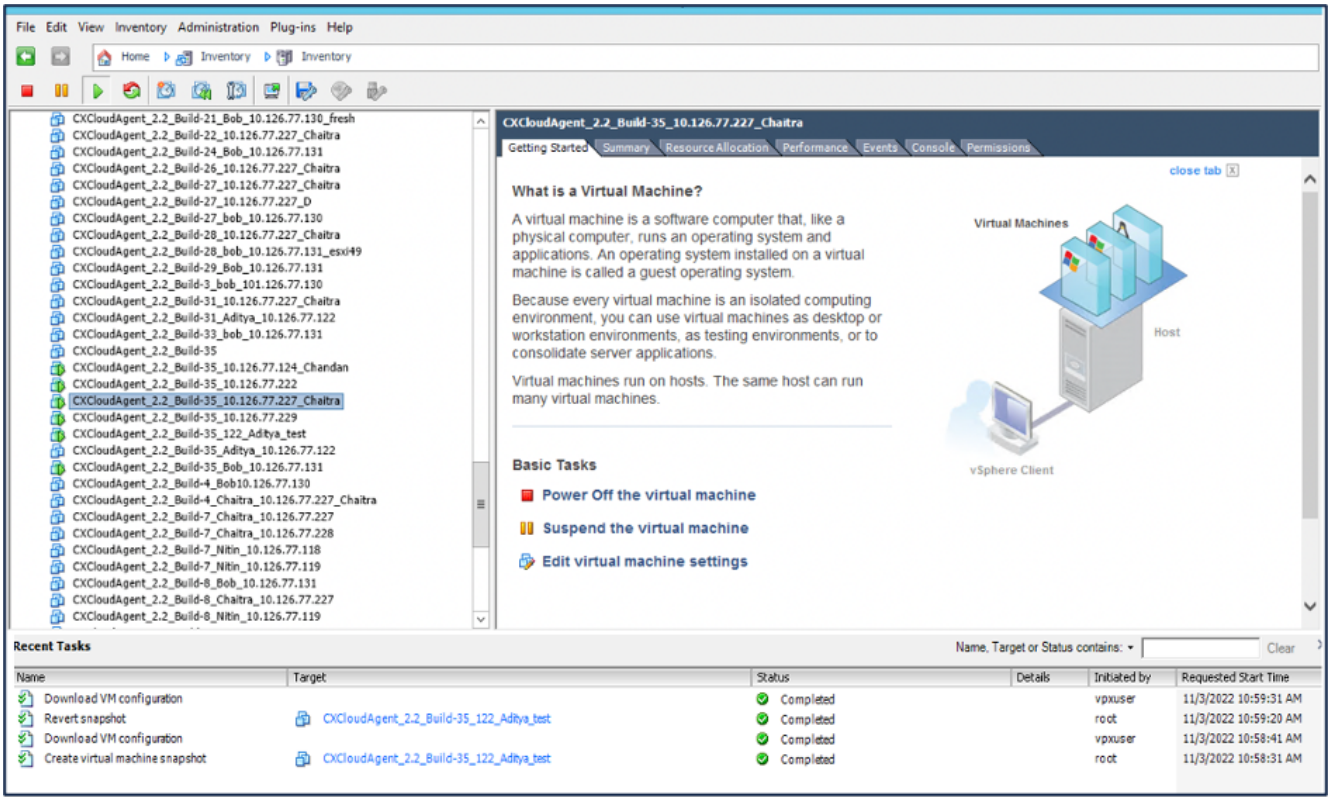
Prendre un snapshot de machine virtuelle

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.

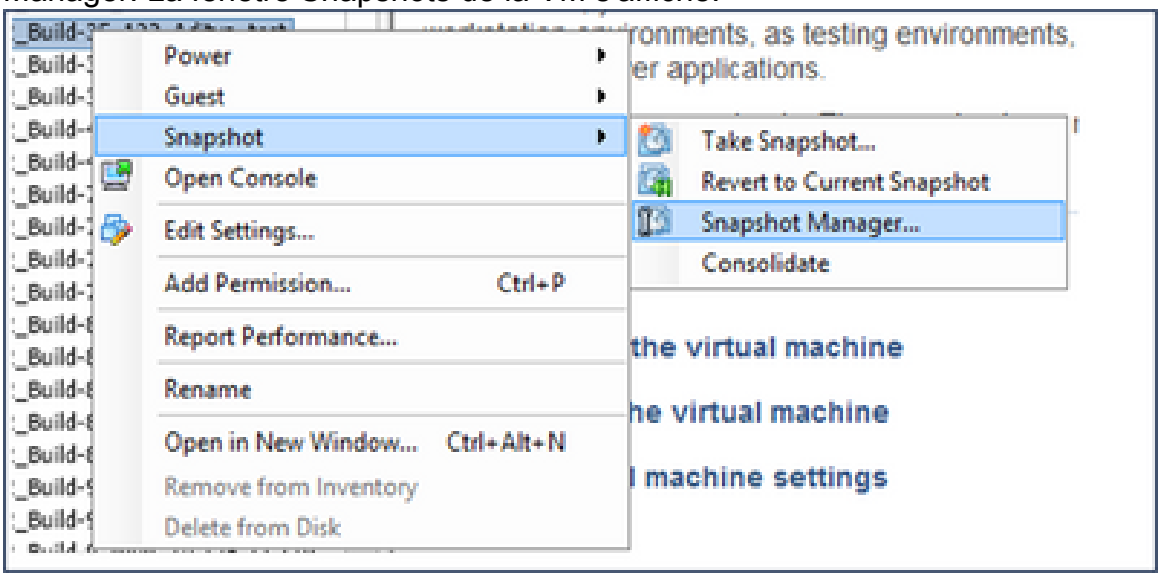


Tâches récentes

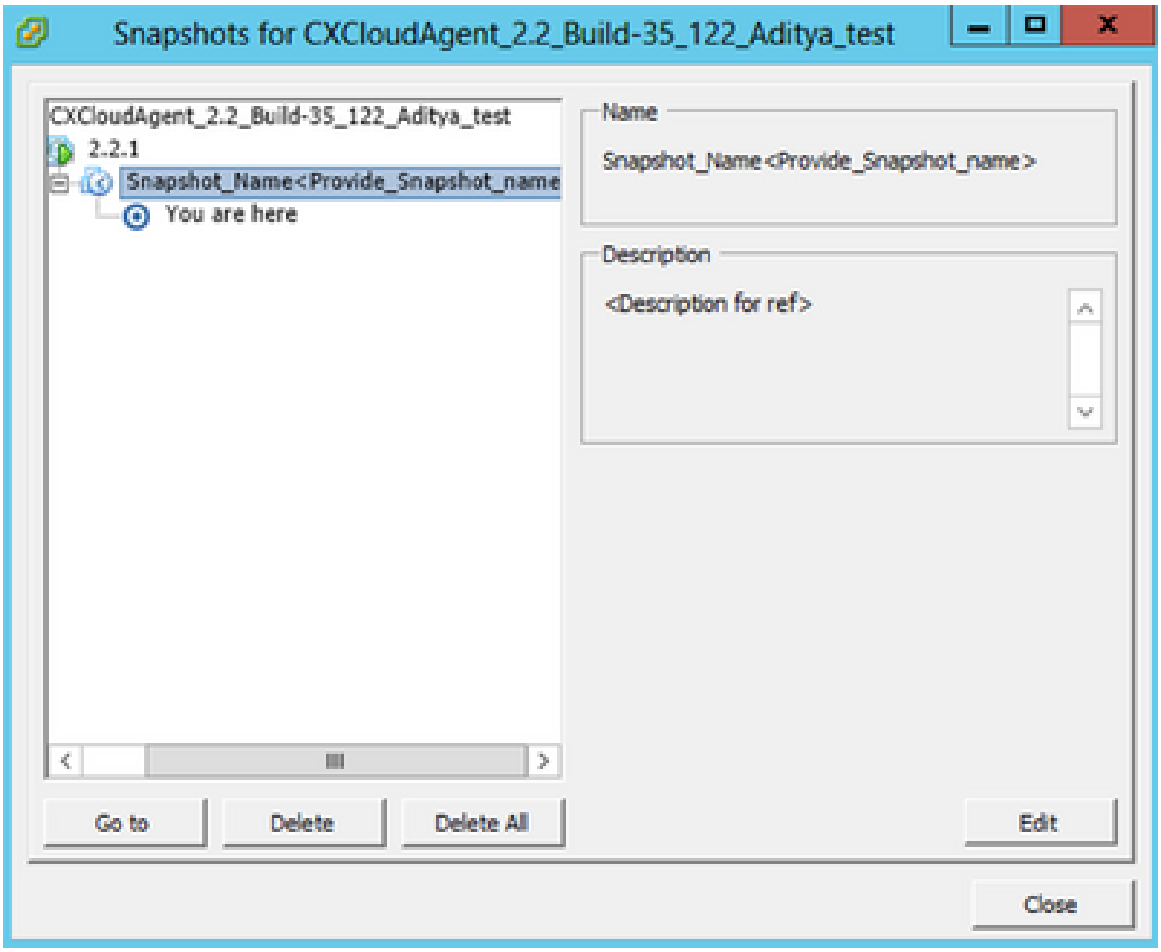
Restaurer

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.

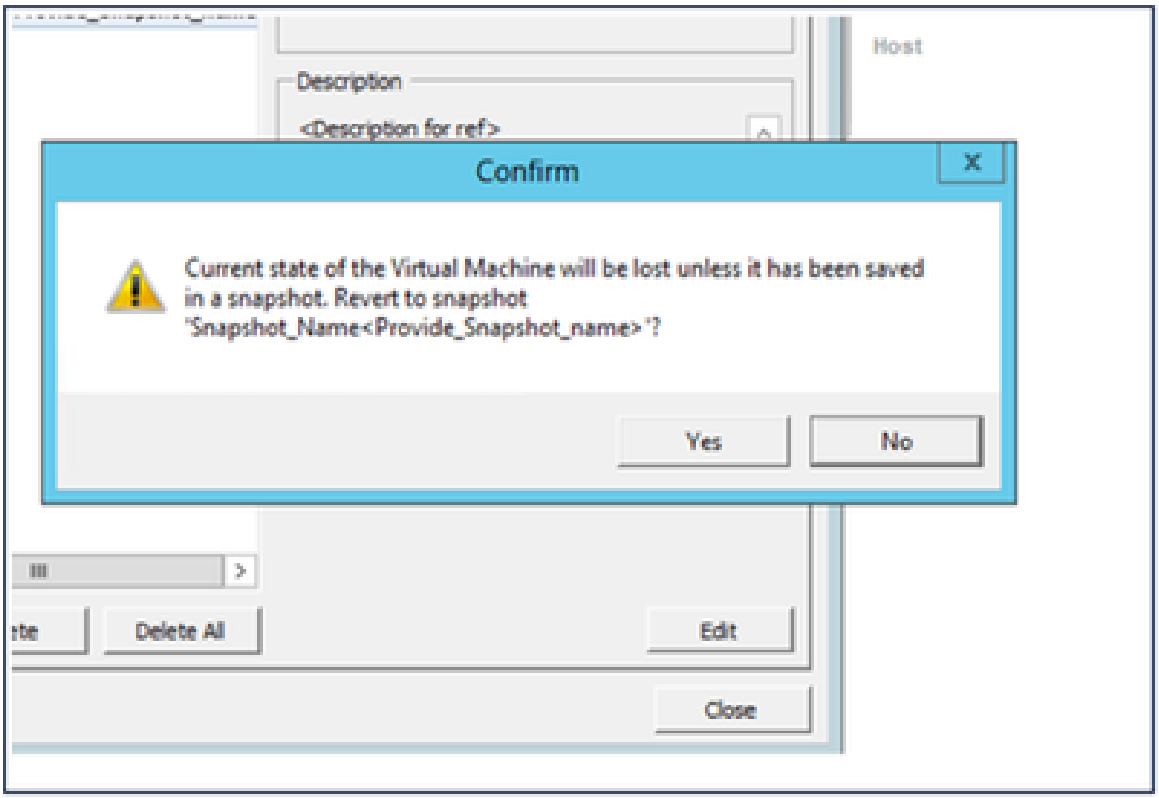


Fenêtre Sélectionner une VM



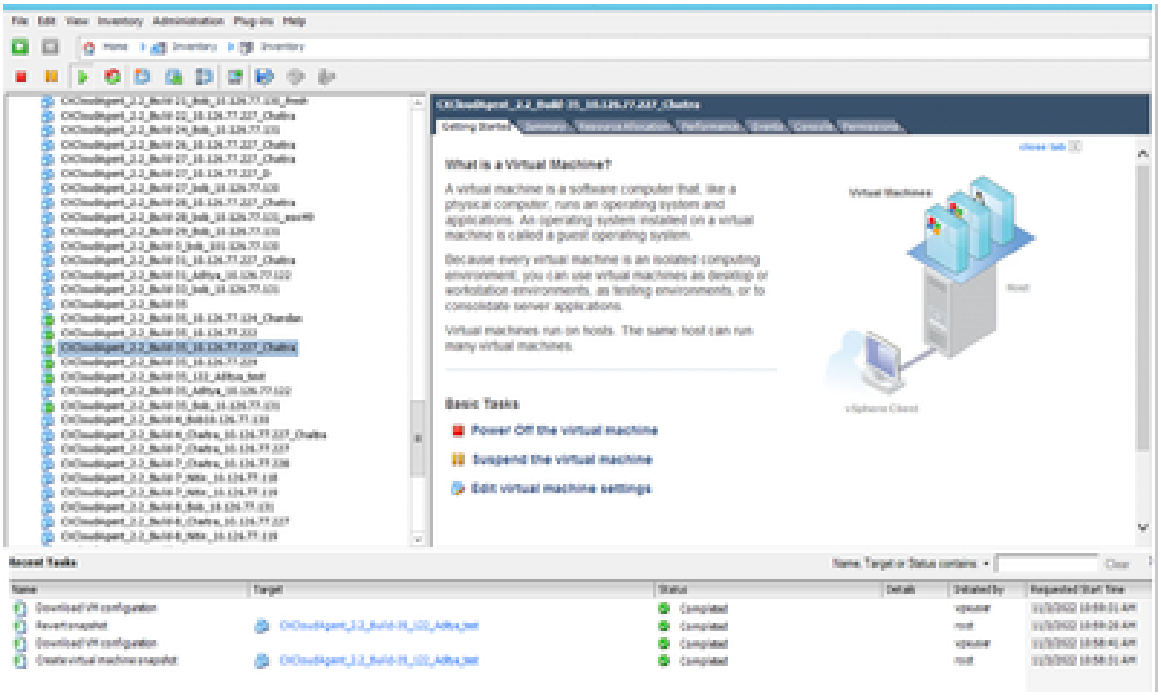
Fenêtre Clichés

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



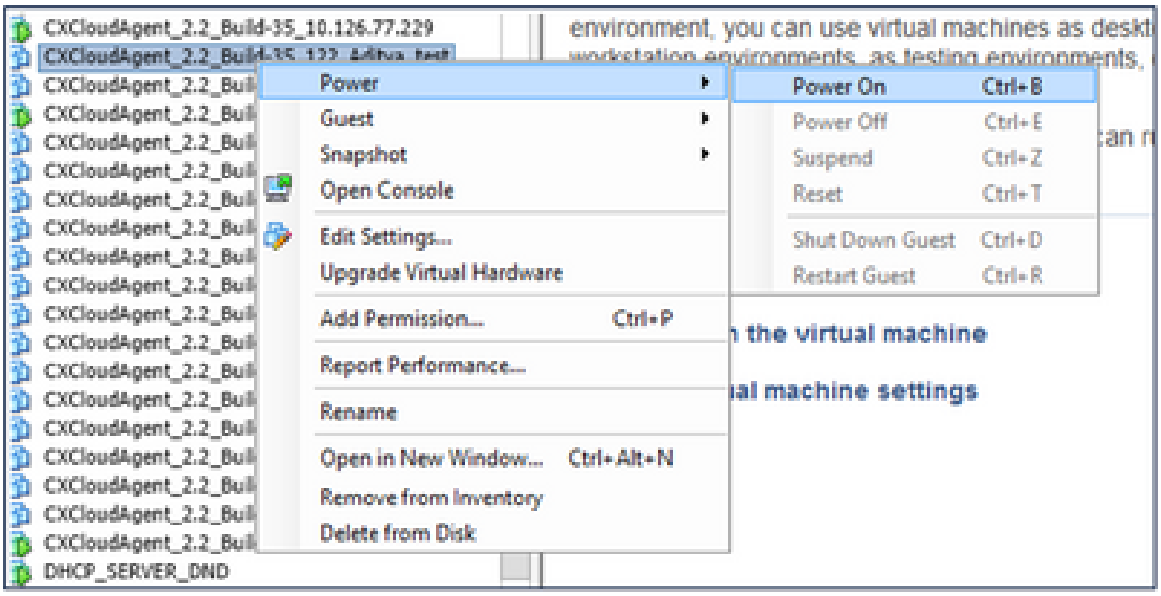
Fenêtre de confirmation

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 Cloud Agent garantit au client une sécurité de bout en bout. La connexion entre CX Cloud et CX Cloud 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 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 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 informations d'identification et d'utilisateur cxcadmin sont utilisées pour accéder aux API de CX Cloud Agent 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 à sens unique 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 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 basée sur mot de passe : l'appliance gère un seul utilisateur (cxcadmin) qui permet à l'utilisateur de s'authentifier et de communiquer avec l'agent cloud 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 de passe n'est valide que pendant deux jours. Les utilisateurs de 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 Cloud Agent respecte les normes de renforcement du Centre de sécurité Internet.

Sécurité des données

L’appliance de l’agent CX Cloud ne stocke aucune information personnelle du client. L'application Device Credential (exécutée en tant que l'un des pods) stocke les informations d'identification chiffrées du serveur 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 DNA Center, à Diagnostic Bridge, à Intersight, à Compliance

Insights, à Faults et à toutes les autres sources de télémétrie collectées par CX Cloud Agent.

Les informations sensibles de la télémétrie des ressources sont masquées avant d'être transmises au cloud. CX Cloud Agent masque les données sensibles pour toutes les ressources collectées qui envoient des données de télémétrie directement à CX Cloud Agent. 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 CX Cloud Agent. 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 DNA 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 d'assistance produit pour les périphériques gérés par un contrôleur ou dans la section Connexions des sources de données de ce document (pour les autres ressources collectées par 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. 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 CX Cloud Agent 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 cxcadmin user. · cxcroot : cxcadmin peut créer cet utilisateur à l'aide de l'utilitaire

	remoteaccount ; l'utilisateur peut obtenir des privilèges root 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 informations d'authentification du serveur du centre Cisco DNA sont chiffrées et stockées 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.