

# CX Cloud Agent Overview v2.2の実稼働環境の問題の検証この記事は無視してください

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[背景説明](#)

[重要なドメインへのアクセス](#)

[CX Cloudエージェントポータルに固有のドメイン](#)

[CX Cloud Agent OVAに固有のドメイン](#)

[Cisco DNA Centerのサポート対象バージョン](#)

[サポートされるブラウザ](#)

[サポートされる製品リスト](#)

[データソースの接続](#)

[CX Cloud Agentのセットアップ](#)

[CX Cloud Agent と CX Cloud の接続](#)

[データソースとしてのCisco DNA Centerの追加](#)

[データソースとしての他のアセットの追加](#)

[概要](#)

[検出プロトコル](#)

[接続プロトコル](#)

[シードファイルを使用してデバイスを追加する](#)

[テレメトリデバイスの処理の制限](#)

[新しいシードファイルを使用してデバイスを追加する](#)

[変更したシードファイルを使用してデバイスを追加する](#)

[IP範囲を使用したデバイスの追加](#)

[IP範囲の編集](#)

[診断スキャンのスケジュール](#)

[導入とネットワーク設定](#)

[OVA の導入](#)

[ThickClient ESXi 5.5/6.0のインストール](#)

[WebClient ESXi 6.0のインストール](#)

[WebClient vCenterのインストール](#)

[OracleVirtual Box 5.2.30のインストール](#)

[MicrosoftHyper-Vのインストール](#)

[ネットワーク設定](#)

[CLIを使用してペアコードを生成する別の方法](#)

[SyslogをCX Cloud Agentに転送するためのCisco DNA Centerの設定](#)

[前提条件](#)

[Syslog転送設定の設定](#)

[SyslogをCX Cloud Agentに転送するための他のアセットの設定](#)

[転送機能を備えた既存のSyslogサーバ](#)

[転送機能のない、またはsyslogサーバのない既存のsyslogサーバ](#)

[情報レベルのsyslog設定を有効にする](#)

## [CX Cloud VMのバックアップと復元](#)

[バックアップ](#)

[復元](#)

## [セキュリティ](#)

[物理セキュリティ](#)

[アカウントのセキュリティ](#)

[ネットワーク セキュリティ](#)

[\[Authentication\]](#)

[強化](#)

[データセキュリティ](#)

[データの伝送](#)

[ログとモニタリング](#)

[Ciscoテレメトリコマンド](#)

[セキュリティ サマリ](#)

---

# はじめに

このドキュメントでは、シスコのカスタマーエクスペリエンス(CX)Cloud Agentについて説明します。

## 前提条件

CX Cloud Agent は仮想マシン ( VM ) として実行され、オープン仮想アプライアンス ( OVA ) または仮想ディスク ( VHD ) としてダウンロードできます。

## 要件

導入要件 :

- 次のハイパーバイザのいずれか :
  - VMware ESXi バージョン 5.5 以降
  - Oracle Virtual Box 5.2.30以降
  - Windows Hypervisorバージョン2012 ~ 2022
- ハイパーバイザはVMをホストでき、これには次のものがが必要です。
  - 8 コア CPU
  - 16GB メモリ/RAM
  - 200GB のディスク容量
- CX Cloudデータを格納する主要なデータリージョンとして米国の指定データセンターを使用しているお客様の場合、CX Cloud Agentは、完全修飾ドメイン名(FQDN)を使用し、TCPポート443でHTTPSを使用して、ここに示すサーバに接続できる必要があります。
  - FQDN:agent.us.cisco.cloud
  - FQDN:ng.acs.agent.us.cisco.cloud
  - FQDN:cloudsso.cisco.com
  - FQDN:api-cx.cisco.com

- CX Cloudデータを格納する主要なデータリージョンとして指定の欧州のデータセンターを使用しているお客様：CX Cloud Agentは、FQDNを使用して、TCPポート443でHTTPSを使用して、ここに示す両方のサーバに接続する必要があります。
  - FQDN:agent.us.cisco.cloud
  - FQDN:agent.emea.cisco.cloud
  - FQDN:ng.acs.agent.emea.cisco.cloud
  - FQDN:cloudsso.cisco.com
  - FQDN:api-cx.cisco.com
- CX Cloudデータを格納する主要なデータリージョンとしてアジア太平洋地域の指定データセンターを使用しているお客様：CX Cloud Agentは、FQDNを使用して、およびTCPポート443のHTTPSを使用して、ここに示す両方のサーバに接続する必要があります。
  - FQDN:agent.us.cisco.cloud
  - FQDN:agent.apjc.cisco.cloud
  - FQDN:ng.acs.agent.apjc.cisco.cloud
  - FQDN:cloudsso.cisco.com
  - FQDN:api-cx.cisco.com
- 主要なデータリージョンとして指定の欧州およびアジア太平洋のデータセンターを使用しているお客様は、初期設定時にCX Cloud AgentをCX Cloudに登録する場合にのみ、FQDN:agent.us.cisco.cloudへの接続が必要です。CX Cloud AgentがCX Cloudに正常に登録されると、この接続は不要になります。
- CX Cloud Agentのローカル管理では、ポート22がアクセス可能である必要があります。
- 次の表に、CX Cloud Agentが正しく動作するために開いて有効にする必要があるポートとプロトコルの概要を示します。

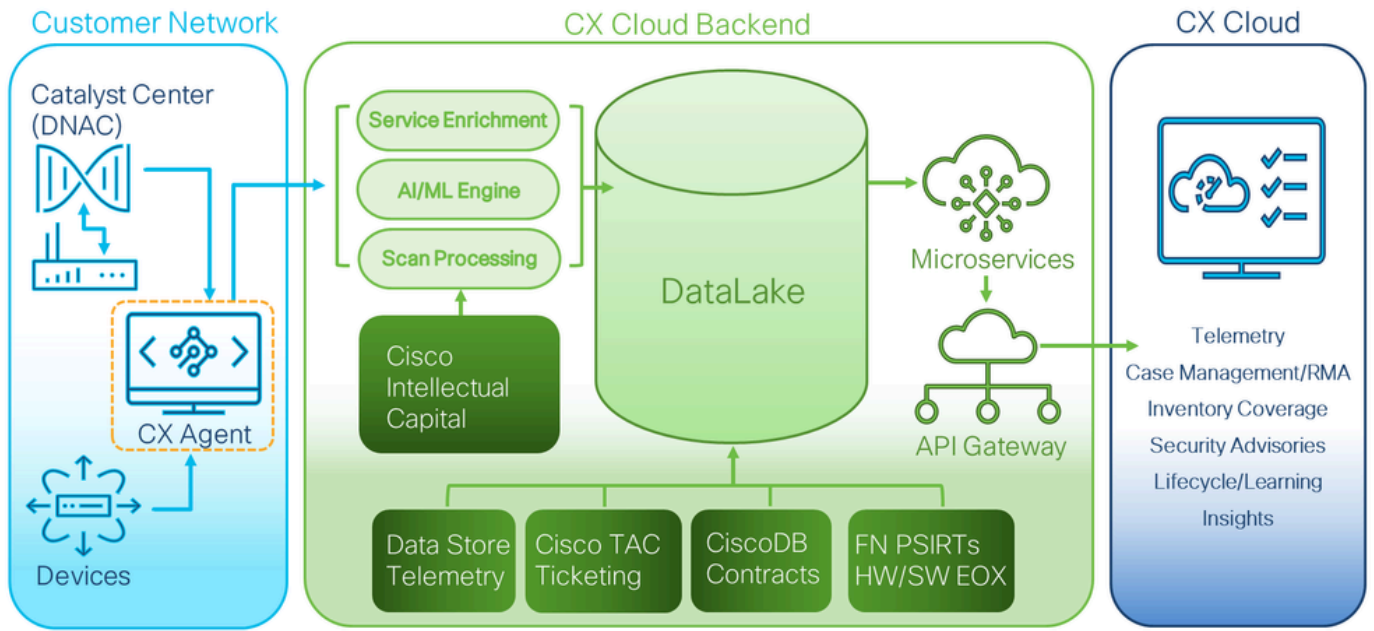
| Source                        |   | Destination  |  | Protocol | Port     | Purpose  | Type  |
|-------------------------------|---|--|--|----------|----------|--|---|
| IP Address                    | Hostname  |  |  |          |          |  |   |
| <b>CX Cloud Agent Traffic</b> |   |  |  |          |          |  |   |
| Data Collection and Transfer  |   |  |  |          |          |  |   |
| Agent IP                      | Dynamic IPs<br>Cisco DNA<br>Center Server<br>IP | For All regions,<br>FQDN: cloudsso.cisco.com<br>FQDN: api-cx.cisco.com<br>QDN: agent.us.cisco.cloud<br>DNAC Servers<br><br>Additionally,<br>For Americas region, FQDN: ng.acs.agent.us.cisco.cloud<br>For EMEA region, FQDN: agent.emea.cisco.cloud, and FQDN: ng.acs.agent.emea.cisco.cloud<br>For APJC region, FQDN: agent.apjc.cisco.cloud, and FQDN: ng.acs.agent.apjc.cisco.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  |

## 背景説明

Cisco(CX)Cloud Agentは、顧客のネットワークデバイスからテレメトリデータを収集し、顧客に実用的な洞察を提供する、スケーラビリティの高いプラットフォームです。CX Cloud Agentを使用すると、アクティブな実行コンフィギュレーションデータを、CX Cloudに表示される予防的で予測的な洞察に変換できます。

このマニュアルは、CX Cloud Agent v2.2以降に固有のものです。以前のバージョンにアクセスするには、『[Cisco CX Cloud Agent](#)』ページを参照してください。

# CX Cloud Architecture



CX Cloudアーキテクチャ

---

注：このガイドの画像（およびコンテンツ）は参照目的でのみ提供されています。実際の内容は異なることがあります。

- VM環境でDynamic Host Configuration Protocol(DHCP)が有効になっている場合は、IPが自動的に検出されます。そうでない場合は、空きIPv4アドレス、サブネットマスク、デフォルトゲートウェイIPアドレス、およびドメインネームサービス(DNS)サーバIPアドレスを使用する必要があります。
- IPv4のみサポートされます。
- 認定されたシングルノードおよびハイアベイラビリティ(HA)クラスタのCisco DNA Centerのバージョンは、2.1.2.xから2.2.3.x、2.3.3.x、2.3.5.x、およびCisco Catalyst Center仮想アプライアンスとCisco DNA Center仮想アプライアンスです。
- ネットワークにSSL代行受信がある場合は、permit-list CX Cloud AgentのIPアドレスを指定します。
- 直接接続されたすべてのアセットには、SSH特権レベル15が必要です。
- 指定されたホスト名のみを使用します。静的IPアドレスは使用できません。

## 重要なドメインへのアクセス


CX Cloudへの移行を開始するには、これらのドメインへのアクセスが必要です。指定されたホスト名のみを使用し、固定IPアドレスは使用しないでください。

### CX Cloudエージェントポータルに固有のドメイン

| 主要ドメイン      | その他のドメイン            |
|-------------|---------------------|
| cisco.com   | mixpanel.com        |
| cisco.cloud | cloudfront.net      |
| split.io    | eum-appdynamics.com |
|             | appdynamics.com     |
|             | tiqcdn.com          |
|             | jquery.com          |

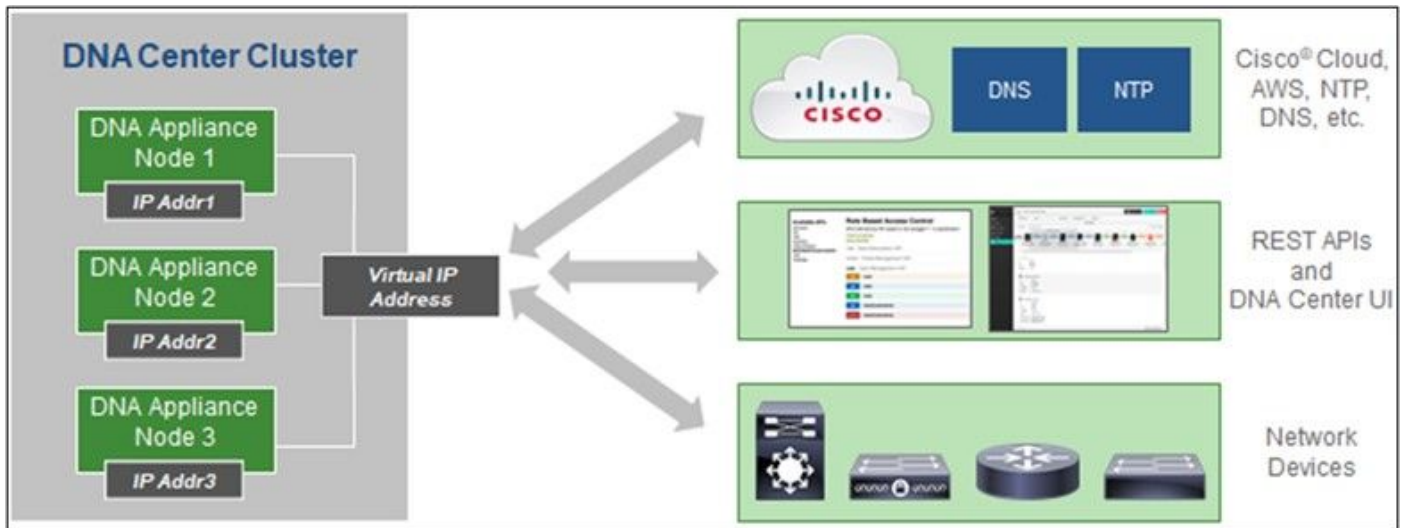
### CX Cloud Agent OVAに固有のドメイン

| AMERICAS                           | 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.cisco.cloud (クラウド)        | agent.us.cisco.cloud (クラウド)   | agent.us.cisco.cloud (クラウド)   |
| ng.acs.agent.us.cisco.cloud (クラウド) | エージェント.emea.cisco.cloud       | エージェント.apjc.cisco.cloud       |
|                                    | ng.acs.agent.emea.cisco.cloud | ng.acs.agent.apjc.cisco.cloud |

 注：指定したFQDNのポート443でリダイレクションを有効にして、発信アクセスを許可する必要があります。

## Cisco DNA Centerのサポート対象バージョン

サポートされるシングルノードおよびHAクラスタCisco DNA Centerのバージョンは、2.1.2.x ~ 2.2.3.x、2.3.3.x、2.3.5.x、Cisco Catalyst Center仮想アプライアンス、およびCisco DNA Center仮想アプライアンスです。



マルチノード HA クラスタ Cisco DNA Center

## サポートされるブラウザ

Cisco.comを快適にご利用いただくために、次のブラウザの最新の公式リリースをお勧めします。

- Google Chrome
- Microsoft Edge
- Mozilla Firefox

## サポートされる製品リスト

CX Cloud Agentがサポートする製品のリストについては、『[サポート対象製品リスト](#)』を参照してください。

## データソースの接続

データ・ソースを接続するには、次の手順に従います：

1. [cx.cisco.com](https://cx.cisco.com)をクリックして、CX Cloudにログインします。

The screenshot shows the Cisco CX Cloud dashboard. At the top, there's a navigation bar with the Cisco logo, 'CX Cloud', a search bar, and utility icons. Below the navigation bar, there's a 'My Portfolio: Select' dropdown and a summary row with categories: Today, Assets & Coverage (90% covered), Adoption Lifecycle (41% adopted), Advisories (3 active), and Cases (1101 open).

The main content area is divided into two sections. On the left, there are several summary cards:
 

- Telemetry Not Connected:** 5697 (Less than 6 months)
- Last Date of Support:** 123 (Less than 6 months)
- Contracts Expiring:** 3 (Less than 6 months)
- Critical Faults:** 0 (Last 7 days)
- Crashed Assets:** 0
- High Crash Risk Assets:** 0
- Critical Security Advisories:** 0
- Assets Not Covered:** 584

On the right, there's a section titled 'Telemetry Not Connected' with a 'View All Details' button. Below the title, it says '5697 Assets with Telemetry Not Connected'. A table lists these assets with columns: Asset Name, Product ID, Product Type, and Location.

| Asset Name  | Product ID    | Product Type            | Location       |
|-------------|---------------|-------------------------|----------------|
| 01027472484 | CS-DESKPRO-K9 | Collaboration Endpoints | FREMONT,CA,USA |
| 01027472485 | CS-DESKPRO-K9 | Collaboration Endpoints | FREMONT,CA,USA |
| 03073621595 | C9407R        | Switches                | FREMONT,CA,USA |
| 03073621665 | C9407R        | Switches                | FREMONT,CA,USA |
| 03073621735 | C9407R        | Switches                | FREMONT,CA,USA |
| 03073621805 | C9407R        | Switches                | FREMONT,CA,USA |
| 03073621875 | C9407R        | Switches                | FREMONT,CA,USA |
| 03073621945 | C9407R        | Switches                | FREMONT,CA,USA |

CX Cloudホームページ

2. Admin Centerアイコンを選択します。「データソース」ウィンドウが開きます。

The screenshot shows the Cisco Admin Center 'Data Sources' page. The top navigation bar is the same as the previous screenshot. The main content area has a left sidebar with navigation options: Asset Groups, Identity & Access, Partner Access, Data Sources (selected), and Insights.

The main content area is titled 'Data Sources' with a sub-header 'Data Storage Region: United States'. There's a search bar for data sources and an 'Add Data Source' button. Below this, a table lists 5 data sources:

| Name                | Type           | Data Last Updated | Status                    |
|---------------------|----------------|-------------------|---------------------------|
| Contract            | Covered Assets | 82 days ago       | Last collection succeeded |
| Cloud Network       | Intersight     | -                 | First collection pending  |
| Data Center Compute | Intersight     | -                 | First collection pending  |
| Meraki              | Meraki         | 33 days ago       | Collection completed      |
| Collaboration       | Webex          | 2 days ago        | Last collection succeeded |








データソース

3. Add Data Sourceをクリックします。Add Data Sourceウィンドウが開きます。表示されるオプションは、お客様のサブスクリプションによって異なります。



## Add Data Source

Search data sources Q

|   |                                 |
|---|---------------------------------|
|  <b>Cisco DNA Center</b><br>Uses CX Cloud Agent to support the Success Tracks for Campus Network and WAN (supported asset types) | <a href="#">Add Data Source</a> |
|  <b>Contracts</b><br>Supports all Success Tracks and offers  | <a href="#">Add Data Source</a> |
|  <b>Intersight</b><br>Supports the Data Center Compute and Cloud Network Success Tracks  | <a href="#">Add Data Source</a> |
|  <b>Other Assets</b><br>Uses CX Cloud Agent to support Success Tracks  | <a href="#">Add Data Source</a> |
|  <b>Smart Accounts</b><br>Supports licensing   | <a href="#">Add Data Source</a> |
|  <b>Webex</b><br>Supports the Success Track for Collaboration  | <a href="#">Add Data Source</a> |
|  <b>Cisco Catalyst SD-WAN Manager</b><br>Supports the Success Track for WAN  | <a href="#">Add Data Source</a> |


### データソースの追加

4. Add Data Sourceをクリックして、該当するデータソースを選択します。CX Cloud Agentがまだセットアップされていない場合は、セットアップを完了する必要がある[Setting Up CX Cloud Agent](#)ウィンドウが開きます。セットアップが完了すると、接続が継続されます。次のいずれかのセクションを参照して続行します。

### [CX Cloud Agentのセットアップ](#)

#### [データソースとしてのCisco DNA Centerの追加](#)

#### [データソースとしての他のアセットの追加](#)

 注:[その他のアセット]オプションは、ダイレクトデバイス接続が以前に設定されていない場合にのみ使用できます。

### CX Cloud Agentのセットアップ

データソースに接続する際に、CX Cloud Agentのセットアップが完了していない場合は、セット

アップのプロンプトが表示されます。

CX Cloud Agentをセットアップするには、次の手順を実行します。

SET UP CX CLOUD AGENT 0%

- Review Deployment Requirements
- Accept Strong Encryption Agreement
- Download Image File
- Deploy and Pair with Virtual Machine

### Add Cloud Agent to your CX Cloud pit crew

CX Cloud Agent gathers telemetry data from the devices on your network, allowing you to take advantage of all the hyper-relevant insights and trusted expertise that CX Cloud has to offer.

### Review deployment requirements

#### Prepare your network for CX Cloud Agent

CX Cloud Agent runs as a virtual machine (VM), so you'll need a hypervisor to host it. Before you download and install the image file, make sure CX Cloud Agent is able to connect to the designated server(s) via HTTPS on port 443 using both the FQDN and the IP address:

For AWS US data centers:

- FQDN: agent.us.cisco.cloud
- FQDN: ng.acs.agent.us.cisco.cloud
- FQDN: cloudss0.cisco.com
- FQDN: api-cx.cisco.com

Review the [CX Cloud Agent Overview](#) for complete hardware and software prerequisites.

CX Cloud takes security seriously. Review the Security section of the [CX Cloud Agent Overview](#) to learn how CX Cloud Agent handles and stores your data.

I set up this configuration on port 443

Continue

#### 導入要件の確認

1. Review deployment requirementsを確認し、I set up this configuration on port 443チェックボックスを選択します。
2. [Continue] をクリックします。[CX Cloud Agentのセットアップ – 強力な暗号化契約に同意する]ウィンドウが開きます。

# Set Up CX Cloud Agent

Help

×

SET UP CX CLOUD AGENT 25%

- Review Deployment Requirements
- Accept Strong Encryption Agreement
- Download Image File
- Deploy and Pair with Virtual Machine

## Accept the strong encryption agreement

Then you can download the image file for the CX Cloud Agent virtual machine.

Instructions

To apply for eligibility to download strong encryption software images:

1. Ensure the address listed in your Cisco.com User Profile is correct and complete.
2. Read each of the conditions below carefully prior to selecting your answer.

|                             |                                    |
|-----------------------------|------------------------------------|
| First Name<br>Samuel        | Last Name<br>Deckard               |
| Email<br>tadeckar@cisco.com | Cisco User Id<br>CXSuperAdmin38333 |

**Business Division's Function:**

- Commercial/Civilian entity
- Government entity, a Military entity or Defense Contractor

If Government entity, a Military entity or Defense Contractor, Are you in

Austria, Australia, Belgium, Canada, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Netherlands, New Zealand, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, Switzerland, United Kingdom or the United States.

- Yes
- No

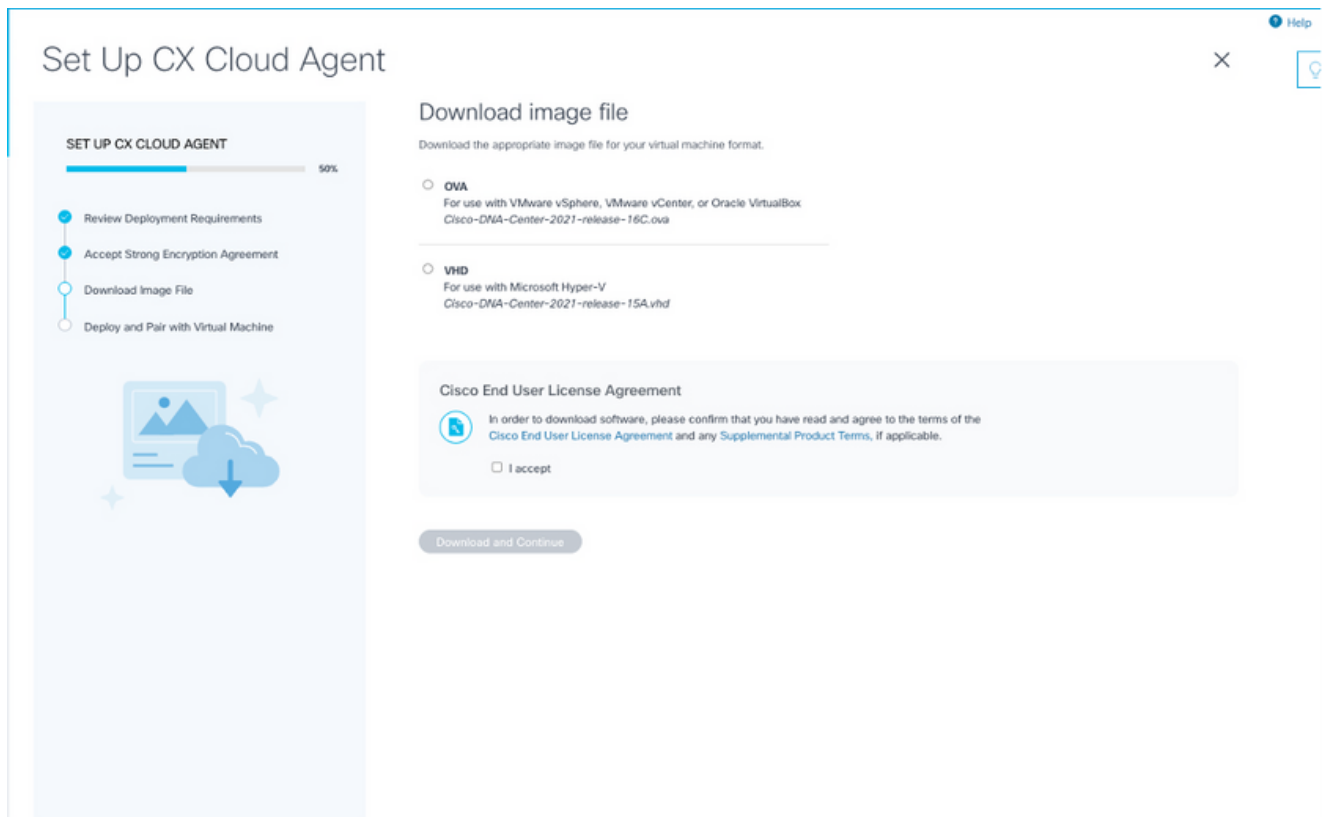
**Confirmation**

By checking this field, I hereby certify that I, as a duly authorized representative of the organization, understand and agree to abide by the conditions set forth above regarding the usage of Cisco Systems, Inc. hardware and/or software.

Continue

暗号化契約

3. First Name、Last Name、E-mail、およびCisco User Idフィールドに事前に入力された情報を確認します。
4. 該当する事業部の機能を選択します。
5. [確認 ( Confirmation ) ] チェックボックスをオンにして、使用条件に同意します。
6. [Continue] をクリックします。CX Cloud Agentのセットアップ – イメージファイルのダウンロードウィンドウが開きます。



ダウンロード イメージ

7. インストールに必要なイメージファイルをダウンロードするための適切なファイル形式を選択します。
8. I acceptチェックボックスをオンにして、Cisco End User License Agreement(EULA)に同意します。
9. Download and Continueをクリックします。[CX Cloud Agentのセットアップ – 導入して仮想マシンとペア設定]ウィンドウが開きます。
10. 次の項に必要なペアコードを取得するには、『[ネットワーク設定](#)』を参照してください。


## CX Cloud Agent と CX Cloud の接続

テレメトリの収集を開始するには、CX Cloud AgentをCX Cloudに接続する必要があります。これにより、UIの情報を更新して、現在のアセットとインサイトを表示できます。このセクションでは、接続とトラブルシューティングのガイドラインを完成させるための詳細を提供します。

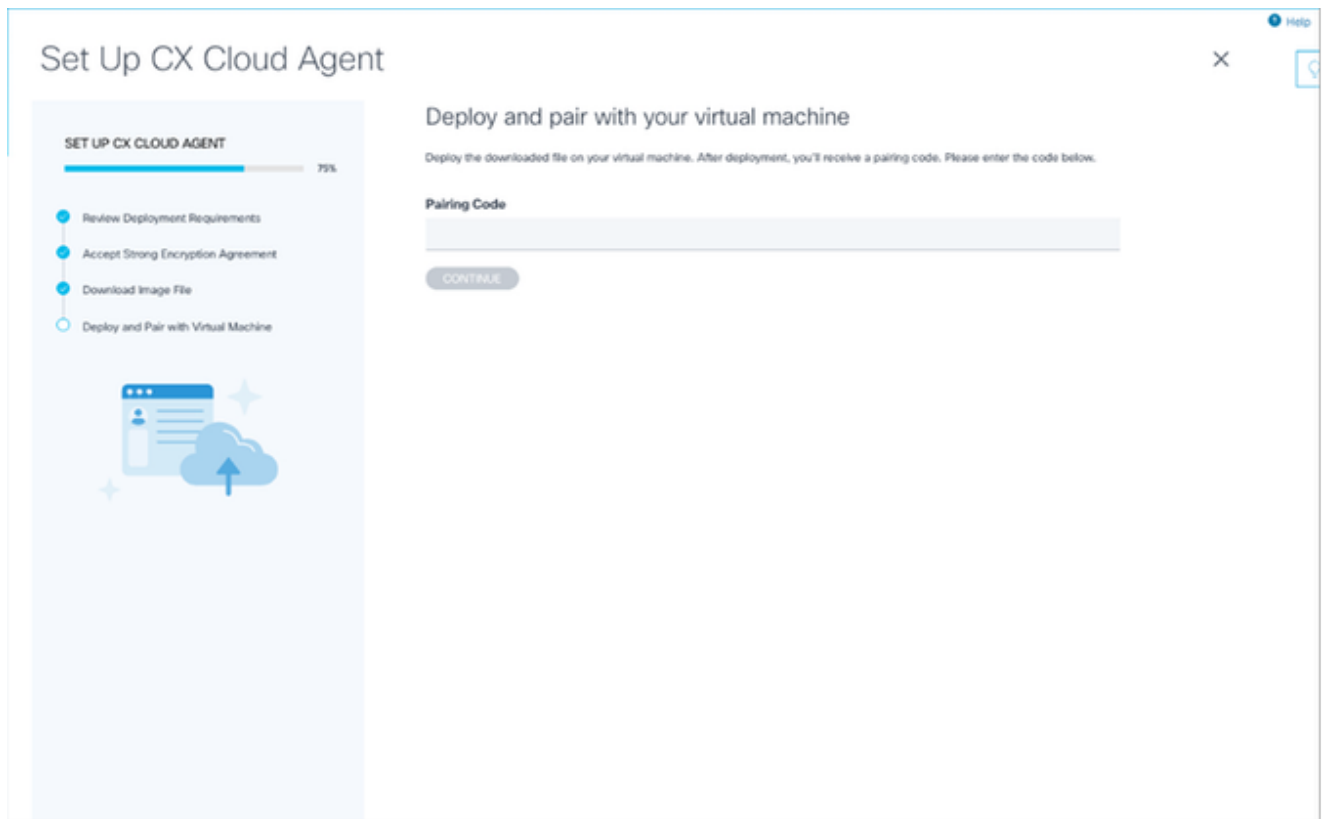
CX Cloud AgentをCX Cloudに接続するには、次の手順を実行します。

1. エージェントを介して接続された仮想マシンのコンソールダイアログまたはコマンドラインインターフェイス(CLI)に表示されるペアリングコードを入力します。

---

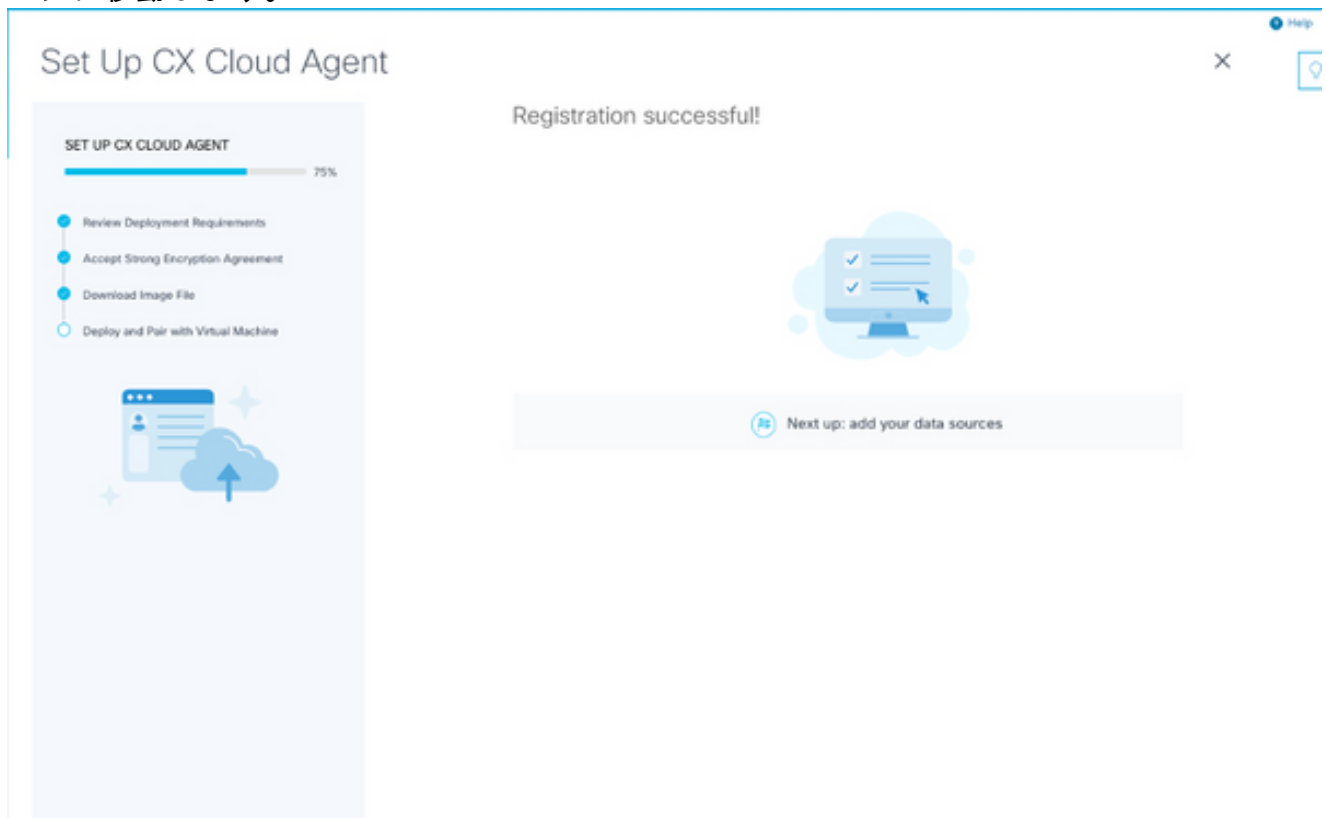
 注：ペアリングコードは、ダウンロードされたOVAファイルの導入後に受信されます。

---



ペアリングコード

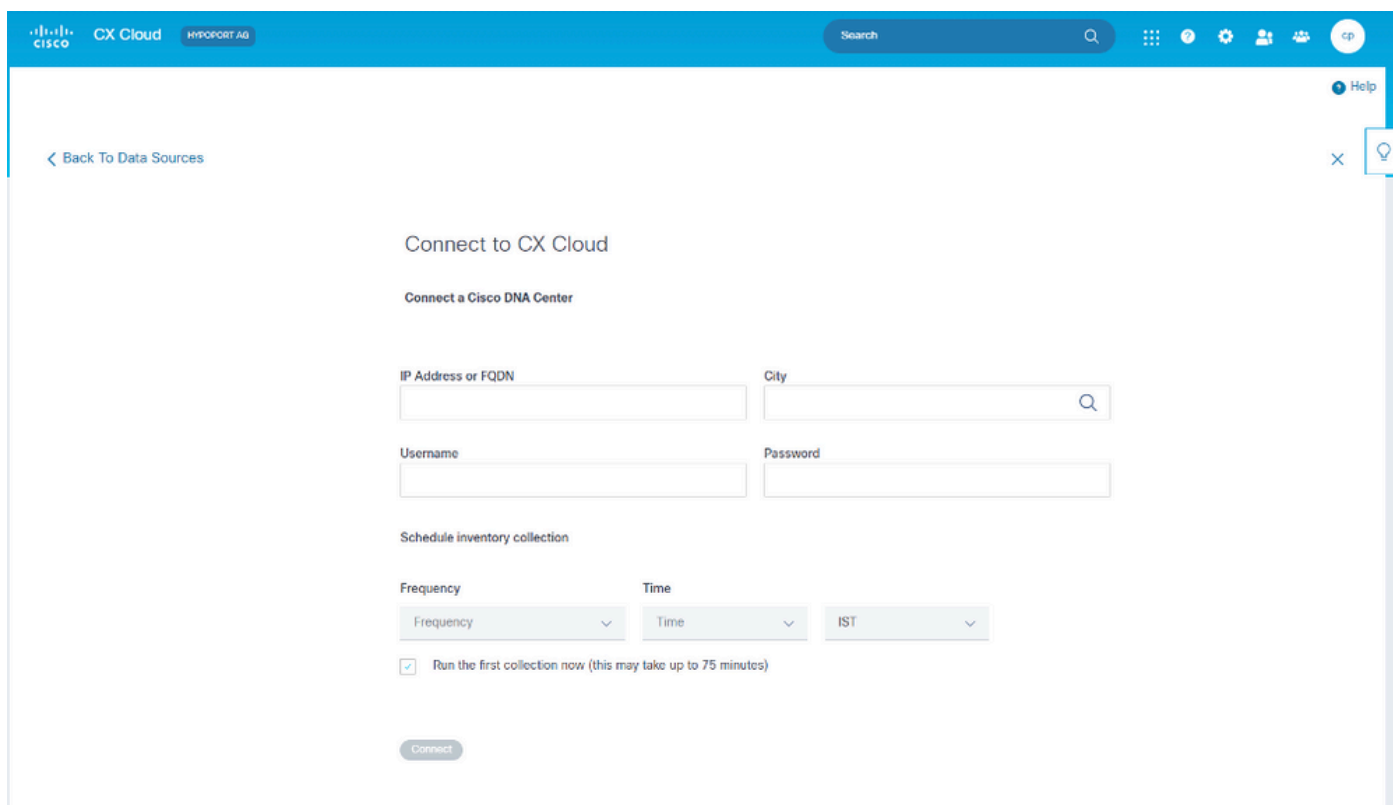
2. Continueをクリックして、CX Cloud Agentを登録します。CX Cloud Agentのセットアップ – 登録が正常に完了しましたウィンドウが短時間開いた後、自動的にデータソースの追加ページに移動します。



登録に成功しました

## データソースとしてのCisco DNA Centerの追加


データソース接続ウィンドウでCisco DNA Centerを選択すると（データソースの接続セクションのデータソースの接続の画像を参照）、次のウィンドウが開きます。




CX Cloudへの接続

Cisco DNA Centerをデータソースとして追加するには、次の手順を実行します。

1. Cisco DNA CenterのIPアドレスまたは仮想IPアドレスまたはFQDN、City（Cisco DNA Centerの場所）、Username、およびPasswordを入力します。

 注：個別のクラスタノードIPを使用しないでください。

2. 頻度と時間を入力してインベントリ収集のスケジュールを設定し、CX Cloud Agentが接続されたデバイスでネットワークスキャンと更新情報の取得を実行できる頻度を指定します。

 注：最初のインベントリ収集には最大75分かかることがあります。

3. [Connect] をクリックします。Cisco DNA CenterのIPアドレスを示す確認が表示されます。

### Connect to CX Cloud

Connected

**Cisco DNA Center 10.122.58.165**  
Inventory collector runs every day At 02:00 AM IST  
First collection will run immediately after data sources are added

Connect another data source to CX Cloud Agent?

+ Add Another Cisco DNA Center

Done

正常に接続しました

4. Add Another Cisco DNA Center、DoneまたはBack to Data Sourcesをクリックして、Data Sourcesウィンドウに戻ります。


## データソースとしての他のアセットの追加

### 概要


テレメトリの収集は、Cisco DNA Centerで管理されていないデバイスにも拡張されているため、お客様はテレメトリに由来する洞察や分析を参照し、より広範なデバイスと対話できます。CX Cloud Agentの初期セットアップ後、CX Cloudで監視されるインフラストラクチャ内の20の追加のCisco DNA Centerに接続するようにCX Cloud Agentを設定できます。また、CX Cloud Agentを環境内の他のハードウェア機器に直接接続することもできます。直接接続できるデバイスの数は最大10,000です。

シードファイルを使用してデバイスを一意に識別するか、CX Cloud AgentがスキャンできるIP範囲を指定することで、CX Cloudに組み込むデバイスを識別できます。どちらのアプローチも、ディスカバリではSimple Network Management Protocol(SNMP)を使用し、接続ではSecure Shell(SSH)を使用します。これらを正しく設定して、テレメトリ収集を正常に行う必要があります。

---

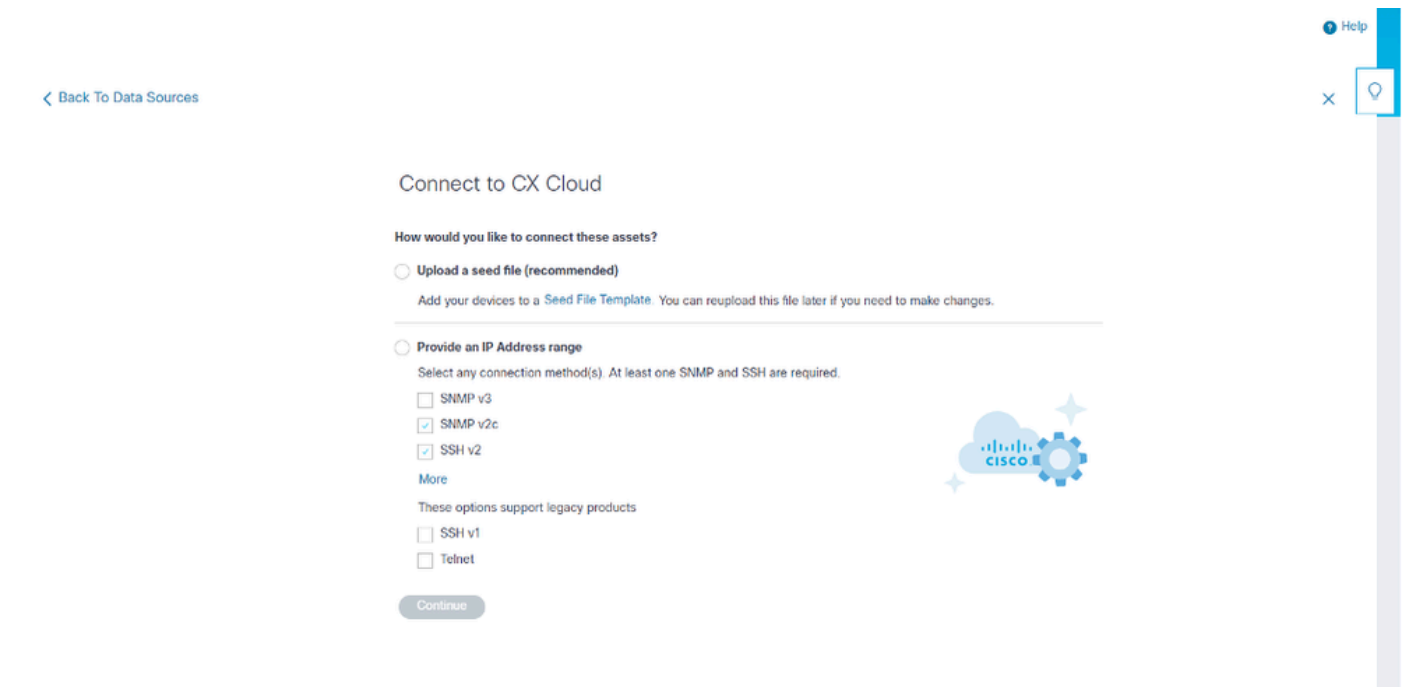
 **注：**  
シードファイルまたはIP範囲のいずれかを使用できます。初期設定後にこの選択を変更することはできません。

---

 **注：**  
初期シードファイルは別のシードファイルに置き換えることができ、初期IP範囲は新しいIP範囲に編集できます。

---

データソース接続ウィンドウでOther Assetsを選択すると、次のウィンドウが開きます。



## CX Cloudへの接続の設定

他のアセットをデータソースとして追加するには：

- ・ シードファイルテンプレートを使用してシードファイルをアップロードします。
- ・ IPアドレス範囲を指定します。

## 検出プロトコル

シードファイルベースの直接デバイス検出とIP範囲ベースの検出の両方で、検出プロトコルとしてSNMPを使用します。SNMPにはさまざまなバージョンがありますが、CX Cloud AgentはSNMPV2cとSNMP V3をサポートし、いずれか、または両方のバージョンを設定できます。設定を完了し、SNMP管理対象デバイスとSNMPサービスマネージャ間の接続を有効にするには、同じ情報（次に詳細を説明）をユーザが入力する必要があります。

SNMPV2cとSNMPV3は、セキュリティとリモート設定モデルの点で異なります。SNMPV3では、SHA暗号化をサポートする高度な暗号化セキュリティシステムを使用して、メッセージを認証し、メッセージのプライバシーを保護します。SNMPv3は、セキュリティリスクと脅威から保護するために、すべてのパブリックおよびインターネット側のネットワークでを使用することを推奨します。CX Cloudでは、SNMPv3のサポートが組み込まれていない古いレガシーデバイスを除き、SNMPv2cではなくSNMPv3を設定することをお勧めします。両方のバージョンのSNMPが設定されている場合、デフォルトでCX Cloud AgentはSNMPv3を使用して各デバイスとの通信を試み、通信が正常にネゴシエートされない場合はSNMPv2cに戻ります。

## 接続プロトコル

デバイスの直接接続のセットアップの一環として、ユーザはデバイス接続プロトコルの詳細を指定する必要があります。具体的には、SSH（またはtelnet）です。SSHv2は、適切な組み込みサ



ポートを備えていない個別のレガシー資産の場合を除き、使用できます。SSHv1プロトコルには基本的な脆弱性が含まれることに注意してください。追加のセキュリティがなければ、SSHv1に依存する際に、これらの脆弱性が原因でテレメトリデータと基盤となる資産が侵害される可能性があります。Telnetも安全ではありません。Telnet経由で送信されるクレデンシャル情報(ユーザー名とパスワード)は暗号化されないため、セキュリティが強化されていないことから、セキュリティが侵害される危険性があります。

## シードファイルを使用してデバイスを追加する


### シードファイルについて

シードファイルは、各行がシステムデータレコードを表すカンマ区切り値(csv)ファイルです。シードファイルでは、すべてのシードファイルレコードは、CX Cloud Agentがテレメトリを収集できる固有のデバイスに対応します。インポートされるシードファイルの各デバイスエントリのすべてのエラーメッセージまたは情報メッセージは、ジョブログの詳細の一部として取得されます。シードファイル内のすべてのデバイスは、初期設定時に到達不能であったとしても、管理対象デバイスと見なされます。新しいシードファイルをアップロードして以前のシードファイルと置き換える場合は、最後にアップロードした日付がCX Cloudに表示されます。

CX Cloud Agentはデバイスへの接続を試行できますが、PIDまたはシリアル番号を判別できない場合、Assetsページに表示するそれぞれのデバイスを処理できません。シードファイル内の、セミコロンで始まる行はすべて無視されます。シードファイルのヘッダ行はセミコロンで始まり、そのまま保持することも(推奨オプション)、顧客シードファイルの作成中に削除することもできます。

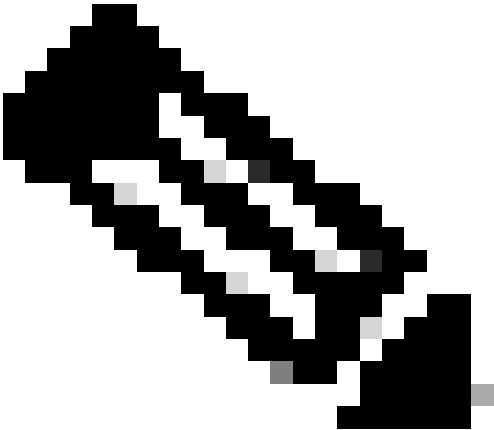
列ヘッダーを含むサンプルシードファイルの形式は、一切変更しないことが重要です。表示されたリンクをクリックして、PDF形式のシードファイルを表示します。このPDFは参照専用で、.csv形式で保存する必要があるシードファイルの作成に使用できます。

.csv形式のシードファイルの作成に使用できるシードファイルを表示するには、この[リンク](#)をクリックします。

 注：このPDFは参照専用で、.csv形式で保存する必要があるシードファイルを作成するために使用できます。

この表は、必要なすべてのシード・ファイル列と、各列に含める必要のあるデータを示しています。

| シードファイル列 | 列ヘッダー/識別子      | カラムの目的   |
|----------|----------------|--|
| A        | IPアドレスまたはホスト名  | デバイスの有効な一意のIPアドレスまたはホスト名を指定します。                  |
| B        | SNMPプロトコルバージョン | SNMPプロトコルは、CX Cloud Agentによって必要とされ、お客様のネットワーク内での |

| シードファイル列 | 列ヘッダー/識別子   | カラムの目的   |
|----------|---|--|
|          |   | <p>デバイス検出に使用されます。値には snmpv2c または snmpv3 を使用できますが、セキュリティ上の考慮事項から、snmpv3 の使用が推奨されます。</p>   |
| C        | <p>snmpRo:col#=3 が 「snmpv2c」 として選択されている場合は必須</p>        | <p>特定のデバイスに対して従来のSNMPv2バリエーションを選択した場合は、デバイスのSNMPコレクションに対してsnmpRO（読み取り専用）クレデンシャルを指定する必要があります。それ以外の場合は、空白を入力できます。</p>  |
| D        | <p>snmpv3UserName:col#=3 が 「snmpv3」 として選択されている場合は必須</p> | <p>特定のデバイスとの通信にSNMPv3を選択した場合は、それぞれのログインユーザ名を指定する必要があります。</p>   |
| E        | <p>snmpv3AuthAlgorithm : 値は MD5 または SHA にすることができます</p>  | <p>SNMPv3 プロトコルは、MD5 または SHA アルゴリズムによる認証を許可します。デバイスにセキュア認証が設定されている場合、それぞれの認証アルゴリズムを指定する必要があります。</p>  <p>注：MD5 は安全でないと見なされており、SHA はサポートしているすべてのデバイスで使用できます。</p> |
| F        | <p>snmpv3AuthPassword : パ</p>                           | <p>デバイスに MD5 または SHA 暗号化アルゴリズム</p>   |

| シードファイル列 | 列ヘッダー/識別子  | カラムの目的  |
|----------|--|---|
|          | スワード   | ムが設定されている場合は、デバイスアクセス用に関連する認証パスワードを指定する必要があります。   |
| G        | snmpv3PrivAlgorithm : 値はDES、3DES                                 | <p>デバイスにSNMPv3プライバシーアルゴリズムが設定されている場合 (このアルゴリズムは応答の暗号化に使用されます)、それぞれのアルゴリズムを指定する必要があります。</p>  <p>注:DESで使用される56ビットキーは、暗号化セキュリティを提供するには短すぎるとみなされ、3DESは、これをサポートするすべてのデバイスで使用できます。</p> |
| H        | snmpv3PrivPassword : パスワード                                       | デバイスでSNMPv3プライバシーアルゴリズムが設定されている場合は、デバイス接続に対応するプライバシーパスワードを提供する必要があります。  |
| I        | snmpv3EngineId:engineID、デバイスを表す一意のID、デバイスで手動で設定されている場合はエンジンIDを指定 | SNMPv3 EngineIDは、各デバイスを表す一意のIDです。このエンジンIDは、CX Cloud AgentがSNMPデータセットを収集する際に参照として送信されます。お客様がEngineIDを手動で設定する場合は、それぞれのEngineIDを指定する必要があります。   |

| シードファイル列 | 列ヘッダー/識別子   | カラムの目的  |
|----------|---|---|
| J        | cliProtocol: 値は'telnet'、'sshv1'、'sshv2'です。空の場合は、デフォルトで'sshv2'に設定できます                                      | CLIは、デバイスと直接やり取りすることを目的としています。CX Cloud Agentは、特定のデバイスのCLI収集にこのプロトコルを使用します。このCLI収集データは、CX Cloud内のAssetsおよびその他のInsightsレポートに使用されます。SSHv2が推奨されます。他のネットワークセキュリティ対策がない場合、それ自体では、SSHv1およびTelnetプロトコルは適切なトランスポートセキュリティを提供しません。 |
| K        | cliPort: CLIプロトコルポート番号  | CLIプロトコルを選択する場合は、それぞれのポート番号を指定する必要があります。たとえば、SSHの場合は22、Telnetの場合は23です。  |
| 起        | cliUser: CLIユーザ名 (CLIユーザ名/パスワードまたはBOTHのいずれかを指定できますが、両方のカラム ( col#=12および col#=13 ) を空にすることはできません)。         | デバイスのそれぞれのCLIユーザ名を指定する必要があります。これは、CLI収集時にデバイスに接続するときにCX Cloud Agentによって使用されます。  |
| M        | cliPassword: CLIユーザパスワード (CLIユーザ名/パスワードまたはBOTHのいずれかを指定できますが、両方のカラム ( col#=12および col#=13 ) を空にすることはできません)。 | デバイスの各CLIパスワードを入力する必要があります。これは、CLI収集時にデバイスに接続するときにCX Cloud Agentによって使用されます。   |
| N        | cliEnableUser   | デバイスでenableが設定されている場合は、デバイスのenableUsername値を指定する必要があります。  |
| O        | cliEnablePassword   | デバイスでenableが設定されている場合、デバイスのenablePassword値を指定する必要があります。   |

| シードファイル列 | 列ヘッダー/識別子      | カラムの目的        |
|----------|----------------|---------------|
| P        | 将来のサポート（入力は不要） | 将来の使用のために予約済み |
| Q        | 将来のサポート（入力は不要） | 将来の使用のために予約済み |
| R        | 将来のサポート（入力は不要） | 将来の使用のために予約済み |
| S        | 将来のサポート（入力は不要） | 将来の使用のために予約済み |

#### デバイスのテレメトリ処理に関する制限事項

デバイスのテレメトリデータを処理する際の制限事項は次のとおりです。


- 一部のデバイスは、Collection Summaryに到達可能として表示されますが、CX Cloud Assetsページには表示されません。デバイス機器の制限により、このようなデバイステレメトリの処理が妨げられます。
- Campus Successトラックに含まれないデバイスのテレメトリ属性が、CX Cloud Assetsページで不正確または欠落する可能性があります。
- シードファイルまたはIP範囲コレクションのデバイスがCisco DNA Centerインベントリの一部でもある場合、デバイスはCisco DNA Centerエントリに対して1回だけ報告されます。シードファイルまたはIP範囲のエントリは、重複を避けるために収集も処理もされません。

#### 新しいシードファイルを使用してデバイスを追加する

新しいシードファイルを使用してデバイスを追加するには、次の手順を実行します。

- このドキュメントの埋め込みリンク（「シードファイルについて」を参照）を使用するか、「CX Cloudへの接続の設定」ウィンドウのリンクを使用して、シードファイルテンプレート(PDF)をダウンロードします。

---

 注：初期シードファイルのダウンロードが完了すると、Configure Connection to CX Cloudウィンドウのリンクは使用できなくなります。

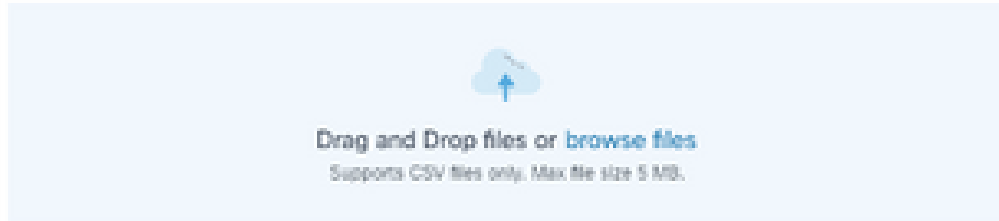
---

## Configure connection to CX Cloud

Upload your seed file

✕

Download the [seed file template](#) and add your device info. Then attach the file below.



Collection Frequency

Frequency



Time

Time



VET



Run the first collection now (this may take up to 75 minutes)


Connect This Data Source

「CX Cloudへの接続の設定」ウィンドウ


2. Excelスプレッドシート（または任意の推奨スプレッドシート）を開き、テンプレートに示すように見出しを入力します。
3. データを手動で入力するか、ファイルにデータをインポートします。
4. 完了したら、テンプレートを.csvファイルとして保存し、CX Cloud Agentにインポートします。

## Configure connection to CX Cloud

Upload your seed file ✕







You've reached your file limit.  
To upload a new file, please remove an existing file.

|   |                                    |                        |
|---|------------------------------------|------------------------|
|  | nextgen_seedfile.csv<br>Completed. | <a href="#">Delete</a> |
|---|------------------------------------|------------------------|

---

### Schedule Inventory Collection

|  |   |  |
|--|---|--|
| Collection Frequency   | Time  | Day  |
| Weekly  | 12:00am  | VET     |
|  |   | Sunday  |

Run the first collection now (this may take up to 75 minutes)

[Connect](#)

### Upload Seed Fileウィンドウ

- シードファイルのアップロードウィンドウで、新しく作成した.csvファイルをドラッグアンドドロップするか、ファイルの参照をクリックして.csvファイルに移動します。
- Schedule Inventory Collectionセクションを完了し、Connectをクリックします。「データ・ソース」ウィンドウが開き、確認メッセージが表示されます。
- CX Cloudの初期設定が完了する前に、CX Cloud Agentはシードファイルを処理し、特定されたすべてのデバイスとの接続を確立して、最初のテレメトリ収集を実行する必要があります。収集は、オンデマンドで開始することも、ここで定義したスケジュールに従って実行することもできます。ユーザは、Run the first collection nowチェックボックスを選択して、最初のテレメトリ接続を実行できます。シードファイルで指定されているエントリの数やその他の要因によっては、このプロセスにかなりの時間がかかる場合があります。


| Name                | Type                  | Data Last Updated | Status                    |
|---------------------|-----------------------|-------------------|---------------------------|
| CX Cloud Agent      | CX Cloud Agent v2.2.0 | 159 days ago      | Not running               |
| 10.127.249.145      | Cisco DNA Center      | 159 days ago      | Not Available             |
| Contract            | Covered Assets        | 27 days ago       | Last Collection Succeeded |
| Data Center Compute | Intersight            | -                 | First Collection Pending  |
| Cloud Network       | Intersight            | -                 | First Collection Pending  |

確認メッセージ

## 変更したシードファイルを使用してデバイスを追加する

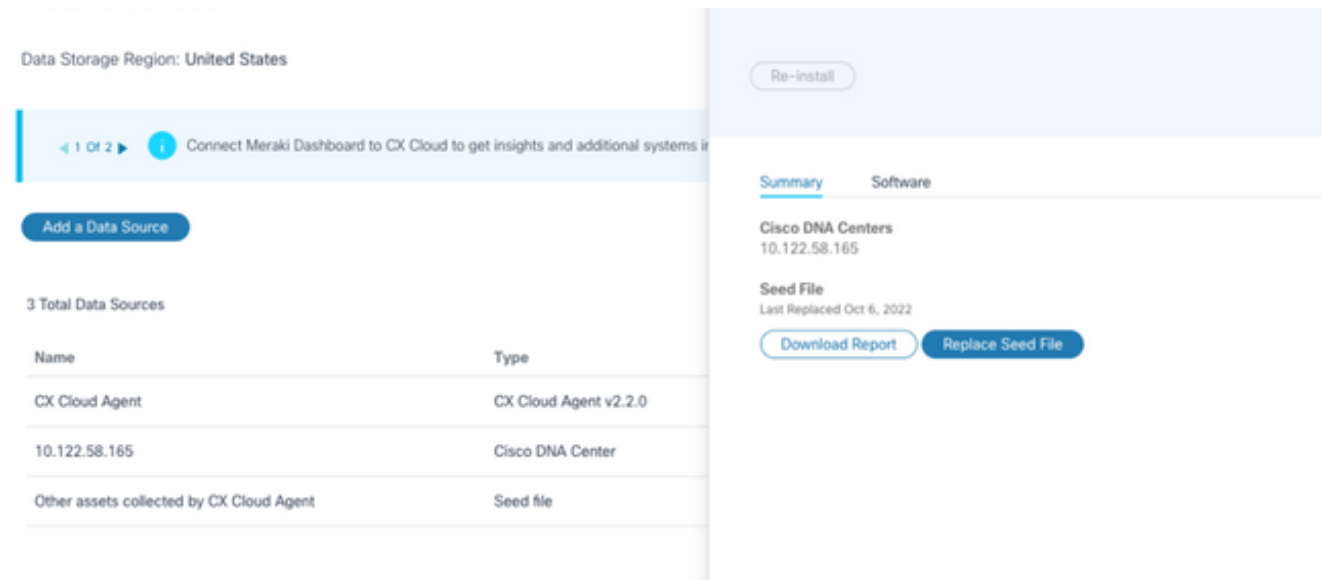
現在のシードファイルを使用してデバイスを追加、変更、または削除するには、次の手順を実行します。

1. 前に作成したシードファイルを開き、必要な変更を行ってファイルを保存します。

 注：シードファイルにアセットを追加するには、以前に作成したシードファイルにアセットを追加し、ファイルをリロードします。新しいシードファイルをアップロードすると現在のシードファイルが置き換えられるため、これが必要になります。検出と収集には、アップロードされた最新のシードファイルのみが使用されます。

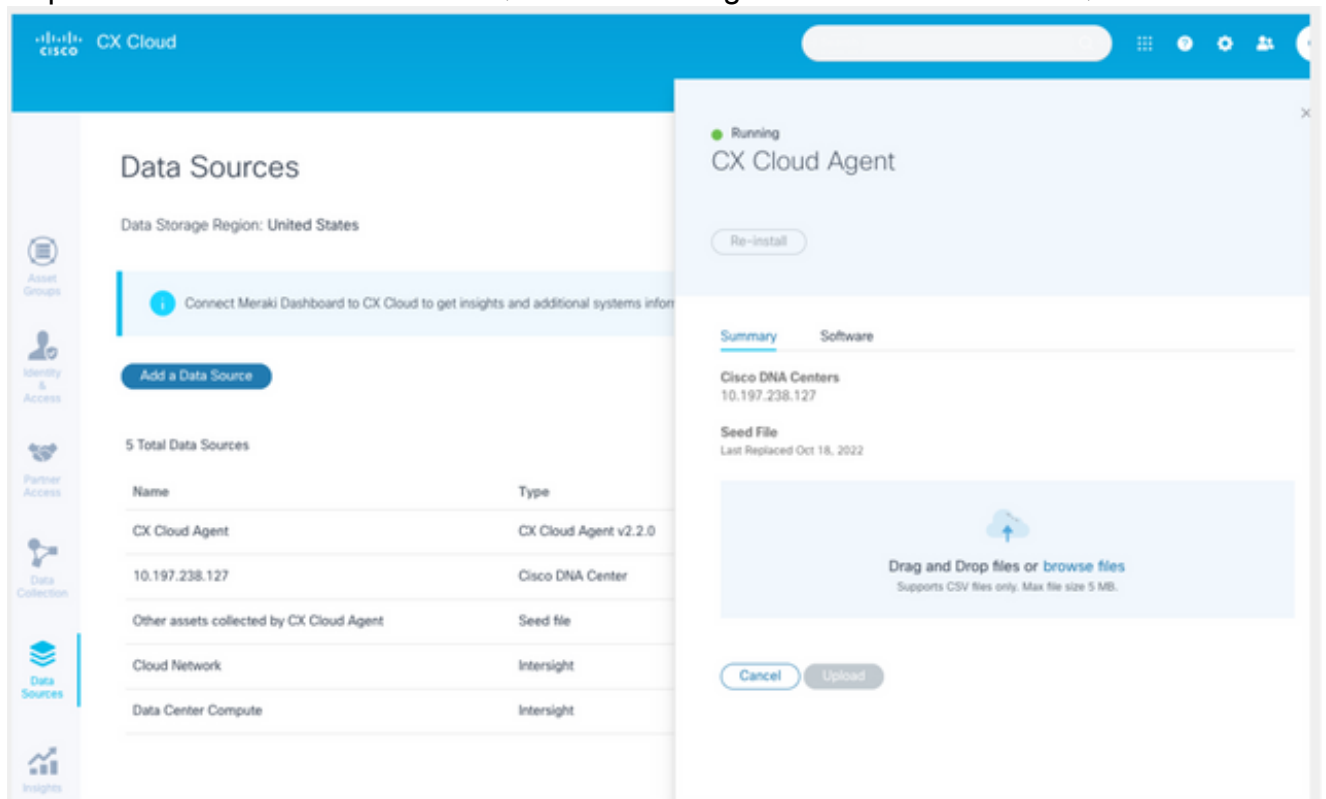
2. データソースページで、CX Cloud Agentのタイプを持つデータソースを選択します。詳細ウィンドウが開き、要約タブとソフトウェアタブが表示されます。





詳細ウィンドウ

- Download Reportをクリックして、選択したデータソースのすべてのアセットに関するレポートを生成します。レポートには、デバイスのIPアドレス、シリアル番号、到達可能性、コマンドタイプ、コマンドステータス、およびコマンドエラー（該当する場合）に関する情報が表示されます。
- Replace Seed Fileをクリックします。CX Cloud Agentウィンドウが開きます。



CX Cloud Agentウィンドウ

- 変更したシードファイルをウィンドウにドラッグアンドドロップするか、ファイルを参照してウィンドウに追加します。
- [Upload] をクリックします。

## IP範囲を使用したデバイスの追加

IP範囲を使用すると、ユーザはハードウェア資産を特定し、その後IPアドレスに基づいてそれらのデバイスからテレメトリを収集できます。テレメトリ収集用のデバイスは、1つのネットワークレベルのIP範囲を指定することで一意に識別できます。この範囲は、CX Cloud AgentがSNMPプロトコルを使用してスキャンできます。直接接続されたデバイスを識別するためにIP範囲を選択する場合、参照されるIPアドレスは可能な限り制限され、必要なすべての資産をカバーできます。

- 特定のIPを指定したり、ワイルドカードを使用してIPのオクテットを置き換えて範囲を作成したりできます。
- セットアップ中に特定のIPアドレスが、特定のIPアドレスの範囲に含まれない場合、CX Cloud Agentは、そのようなIPアドレスを持つデバイスとの通信を試行せず、そのようなデバイスからテレメトリを収集しません。
- \*.\*.\*と入力すると、CX Cloud Agentはユーザが指定したクレデンシャルを任意のIPで使用できます。たとえば、172.16.\*.\*では、172.16.0.0/16サブネット内のすべてのデバイスにクレデンシャルを使用できます。
- ネットワークまたはInstalled Base(IB)に変更があれば、IP範囲を変更できます。「[IP範囲の編集](#)」の項を参照してください。

CX Cloud Agentはデバイスへの接続を試行できますが、PIDまたはシリアル番号を判別できない場合、各デバイスを処理してAssetsビューに表示できません。

---

### 注：

Edit IP Address Rangeをクリックすると、オンデマンドデバイス検出が開始されます。新しいデバイスを特定のIP範囲に追加または削除（内外）する場合は、必ずEdit IP Address Range（IPアドレス範囲の編集）をクリックし（「[IP範囲の編集](#)」の項を参照）、オンデマンドでのデバイスディスカバリを開始するために必要な手順を実行して、新しく追加されたデバイスをCX Cloud Agentの収集インベントリに含める必要があります。

---

### Connect to CX Cloud

#### Provide IP address range ×

Enter IP address range

Starting IP Address \*

198.168.1.10

Ending IP Address \*

198.168.1.20

Enter SNMP v2c credentials

Read Community \*

Enter SSHv2 credentials

Username \*

Enable Username (Optional)

Schedule inventory collection

Frequency

Frequency

Time

Time

IST

Run the first collection now (this may take up to 75 minutes)

Connect

#### 初期IPアドレス範囲ウィンドウ

IP範囲を使用してデバイスを追加するには、ユーザが設定UIを使用して適用可能なすべてのクレデンシャルを指定する必要があります。表示されるフィールドは、前のウィンドウで選択したプロトコルによって異なります。SNMPv2cとSNMPv3の両方を選択したり、SSHv2とSSHv1の両方を選択するなど、同じプロトコルを複数選択すると、個々のデバイスの機能に基づいて、CX Cloud Agentによって自動的にプロトコルの選択がネゴシエートされます。

IPアドレスを使用してデバイスを接続する場合、お客様はSSHバージョンおよびTelnetクレデンシャルとともにIP範囲内のすべての関連プロトコルが有効であることを確認できます。有効でない場合、接続が失敗する可能性があります。

IP範囲を使用してデバイスを追加するには、次の手順を実行します。

1. Configure connection to CX Cloudウィンドウで、Provide an IP Address rangeオプションを選択します。

## Configure connection to CX Cloud

Provide IP address range

×

Enter IP address range

Starting IP Address \*

Ending IP Address \*

Enter SNMP v3 credentials

Username

Engine ID

Authorization Algorithm

Authorization Password

Privacy Algorithm

Privacy Password

IPアドレスフォームを使用してデバイスを追加する

2. フォームに関連情報を入力します。
3. 複数の接続オプションを選択できます。これらの画面には、オプションの設定クレデンシャルが表示されます。各接続オプションのクレデンシャルフィールドの説明については、『[シードファイルについて](#)』を参照してください。

## Configure connection to CX Cloud

Provide IP address range

×

Enter IP address range

Starting IP Address \*

Ending IP Address \*

Enter SNMP v3 credentials

Username

Engine ID

Authorization Algorithm

Authorization Password

Privacy Algorithm

Privacy Password

SNMP v3クレデンシャル

Enter SNMP v2c credentials

Read Community \*

Enter SSHV2 credentials

Username

Enable Username (Optional)

Password

Enable Password (Optional)

Enter SSHV1 credentials

Username

Enable Username (Optional)

Password

Enable Password (Optional)

SNMP v2、SSHV2、およびSSHV1クレデンシャル

### Enter Telnet credentials

Username

Enable Username (Optional)

Password

Enable Password (Optional)

### Schedule Inventory Collection

Collection Frequency

Time

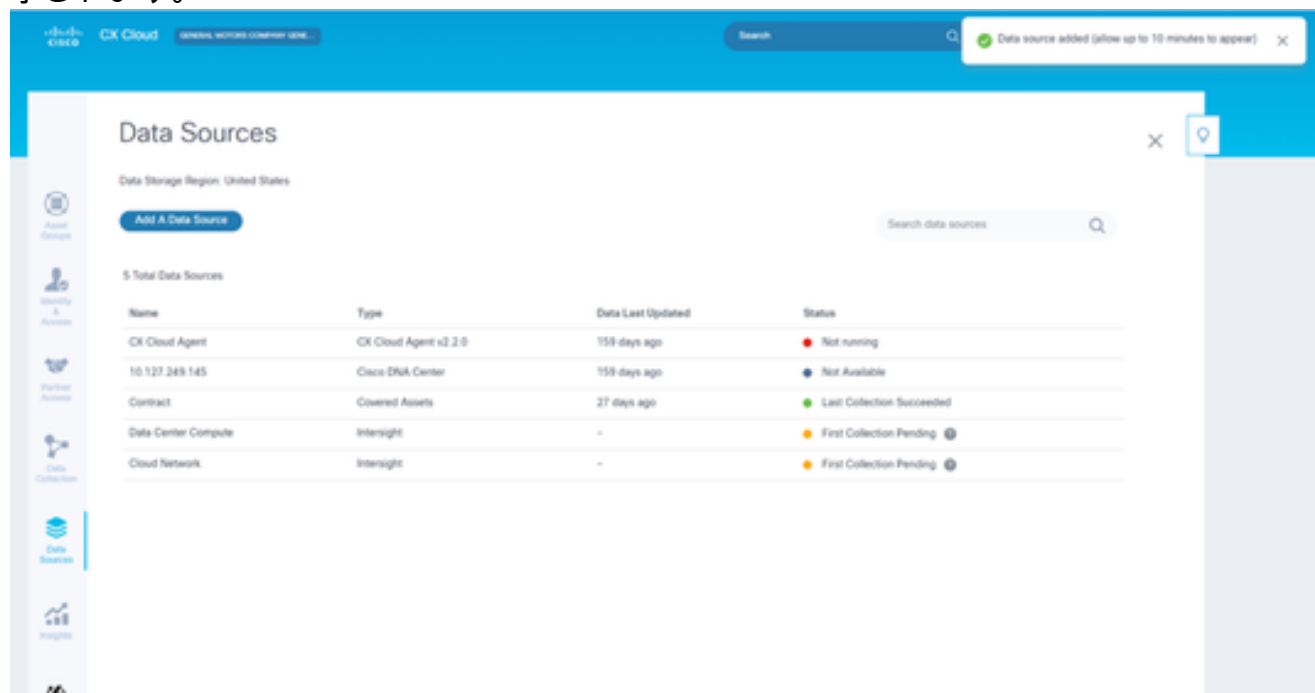
IST

Run the first collection now (this may take up to 75 minutes)

Connect

Telnetクレデンシヤルとネットワークスキャンスケジューリング

4. [Connect] をクリックします。「データ・ソース」ウィンドウが開き、確認メッセージが表示されます。

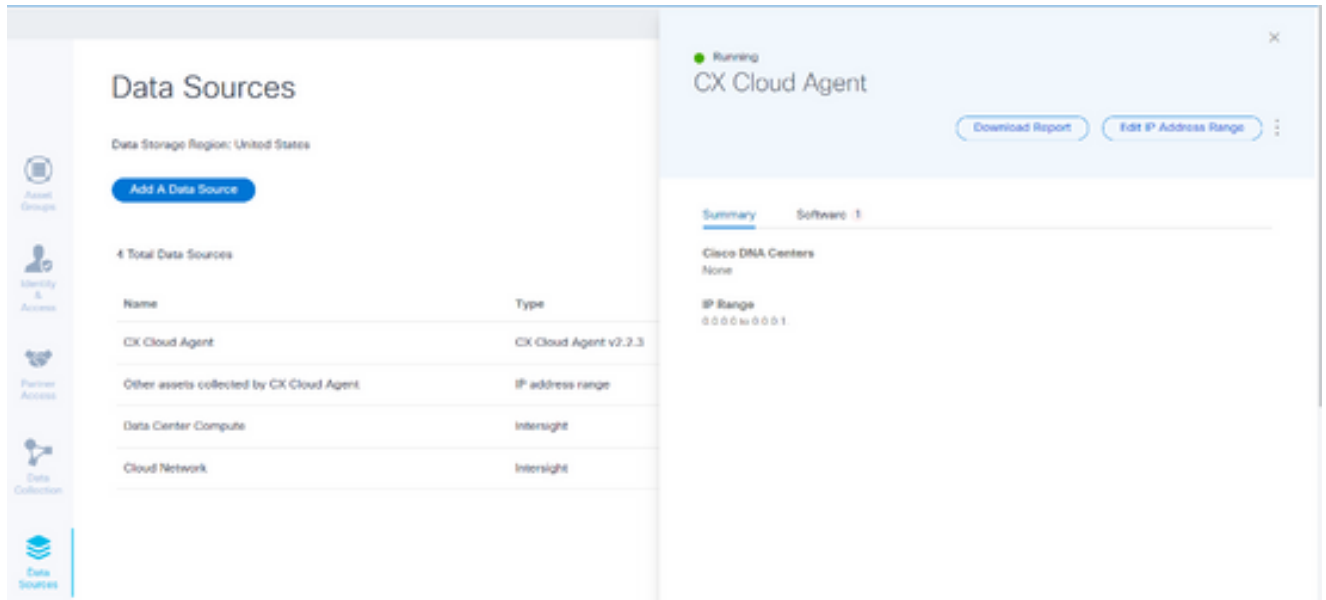


確認

### IP範囲の編集

IP範囲を編集するには、

1. Data Sourcesウィンドウに移動します。



データソース

2. データソースでIP範囲の編集が必要なCX Cloud Agentをクリックします。詳細ウィンドウが開きます。
3. Edit IP Address Rangeをクリックします。「CX Cloudに接続」ウィンドウが開きます。

[← Back To Data Sources](#)

## Connect to CX Cloud

Provide an IP address range

[Edit The Protocols](#)

Enter IP address range

Starting IP address \*

0.0.0.0

Ending IP address \*

0.0.0.1

Cancel

Continue

IP範囲の指定

4. Starting IP addressフィールドとEnding IP addressフィールドの新しいIPを更新します。
5. Edit the Protocolsリンクをクリックします。[CX Cloudに接続 – プロトコルの選択]ウィンドウが開きます。



## Connect to CX Cloud

### Select a protocol

At least one discovery and collection method are required.

#### Discovery options

SNMP v3 (recommended)

SNMP v2c

#### Collection options

SSH v2 (recommended)

SSH v1

Telnet

Cancel

Continue

プロトコルの選択

6. 該当するチェックボックスをクリックして、該当するプロトコルを選択します。
7. [Continue] をクリックします。Provide an IP address rangeウィンドウが開きます。

## Provide an IP address range

[Edit The Protocols](#)

### Enter IP address range

Starting IP address \*

0.0.0.0

Ending IP address \*

0.0.0.2

### Enter SNMP v2c credentials

Read community \*

### Enter SSH v1 credentials

Username \*

Enable Username (Optional)

Password \*

Enable Password (Optional)

Cancel

Connect


クレデンシャルの入力

- 設定クレデンシャルを入力します。
- [Connect] をクリックします。「データ・ソース」ウィンドウが開き、確認メッセージが表示されます。

The screenshot shows the Cisco CX Cloud interface. At the top, there's a navigation bar with 'CX Cloud' and 'F500 UNITED STATES'. A search bar is on the right, and a notification says 'IP address range updated'. The main content area is titled 'Data Sources' and shows 'Data Storage Region: United States'. There's a button 'Add A Data Source' and a search bar 'Search data sources'. Below that, it says '4 Total Data Sources' and displays a table:

| Name                                     | Type                  | Data Last Updated | Status                   |
|--|-----------------------|-------------------|--------------------------|
| CX Cloud Agent                           | CX Cloud Agent v2.2.3 | 3 minutes ago     | Running                  |
| Other assets collected by CX Cloud Agent | IP address range      | 3 minutes ago     | 1 unreachable            |
| Data Center Compute                      | Intersight            | -                 | First Collection Pending |
| Cloud Network                            | Intersight            | -                 | First Collection Pending |

確認

 注：確認メッセージでは、編集した範囲のデバイスが到達可能であることと、クレデンシャルが受け入れられたことは確認されません。

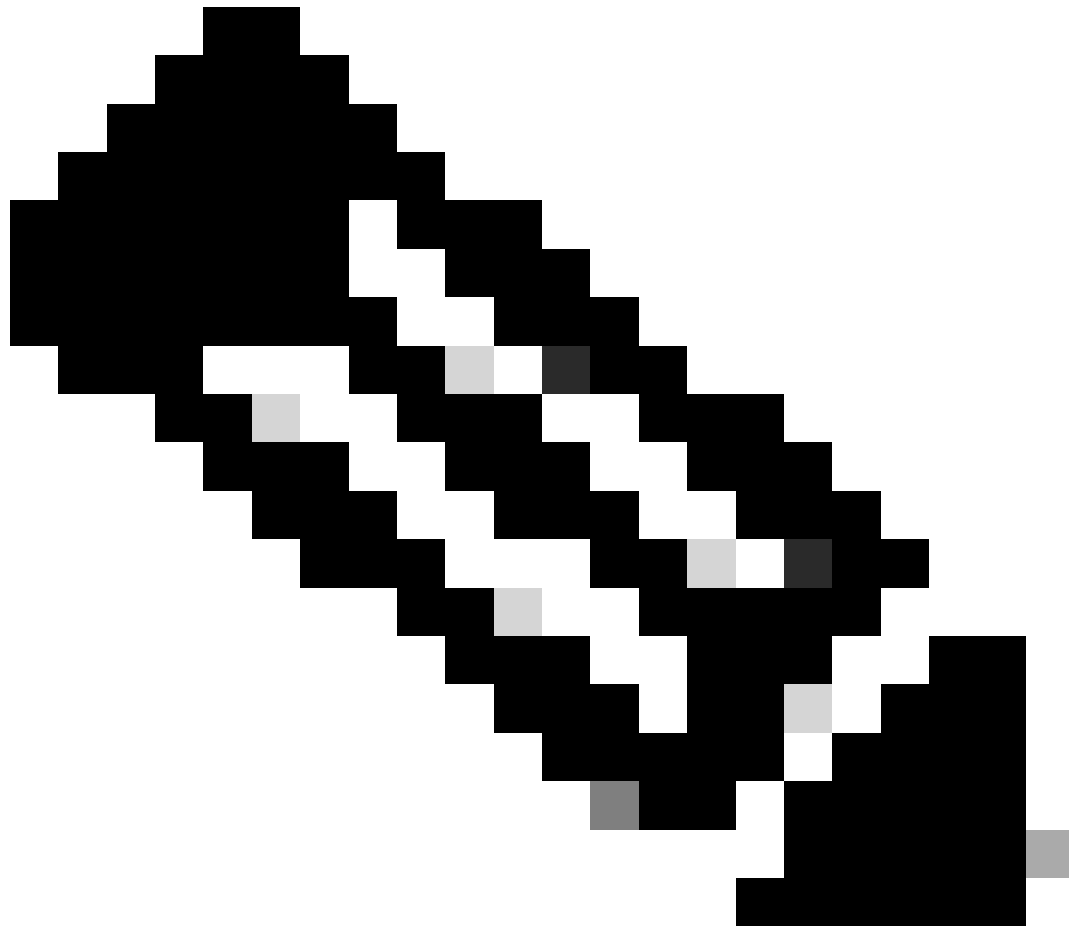
## 複数のコントローラから検出されたデバイスについて

一部のデバイスは、Cisco DNA CenterとCX Cloud Agentへの直接接続の両方で検出され、それらのデバイスから重複データが収集される可能性があります。重複データの収集を避け、1つのコントローラだけでデバイスを管理するには、CX Cloud Agentがデバイスを管理する優先順位を決定する必要があります。

- デバイスが最初にCisco DNA Centerによって検出され、次に直接デバイス接続 ( シードファイルまたはIP範囲を使用 ) によって再検出された場合、デバイスの制御ではCisco DNA Centerが優先されます。
- デバイスが最初にCX Cloud Agentへの直接接続によって検出され、次にCisco DNA Centerによって再検出される場合、デバイスの制御ではCisco DNA Centerが優先されます。

## 診断スキンのスケジュール

お客様は、CX Cloudでオンデマンドの診断スキンをスケジュールできます。



注：診断スキャンをスケジュールするか、インベントリ収集スケジュールとは少なくとも6～7時間の間隔を空けてオンデマンドスキャンを開始して、重複しないようにすることをお勧めします。複数の診断スキャンを同時に実行すると、スキャンプロセスが遅くなり、スキャンが失敗する可能性があります。

---

診断スキャンをスケジュールする手順は、次のとおりです。

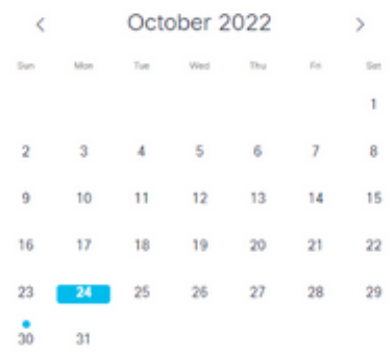
1. ホームページで設定（歯車）アイコンをクリックします。
2. Data Sourcesページで、左ペインからData Collectionを選択します。
3. Schedule Scanをクリックします。

## Data Collection

Diagnostic Scans ③

Schedule Scan

No Diagnostic Scans Found



Inventory Collection ③

3 Collections

| Source                                   | Schedule                            |   |
|--|-------------------------------------|---|
| Other assets collected by CX Cloud Agent | Monthly on the 30th at 05:30 PM EDT | ⋮ |
| 10.197.238.127                           | Monthly on the 30th at 05:00 PM EDT | ⋮ |
| 22.1.90.1                                | Monthly on the 30th at 09:00 PM EDT | ⋮ |

Rapid Problem Resolution

Automate data collection and diagnostics when a support case is opened. This helps Cisco experts diagnose and troubleshoot problems faster.

Enable for Campus Network

データ収集

4. このスキャンのスケジュールを構成します。

### Other assets collected by CX Cloud Agent Inventory Collection Details

Schedule History

Weekly on Sunday at 12:00 am EDT  
Created: Oct 3, 2022

Save Scheduled Collection

スキャンスケジュールの構成

5. デバイスリストで、スキャンするすべてのデバイスを選択し、Addをクリックします。

## New Scheduled Scan

Data Sources: Other assets collected by CX Cloud Agent

Schedule: Frequency at Time IST Save Changes

Description (Optional)

| Device                                    | Source IP      | IP Address |
|---|----------------|------------|
| <input type="checkbox"/> Device_22_0_2_1  | 10.127.249.156 | 22.0.2.1   |
| <input type="checkbox"/> Device_22_0_32_1 | 10.127.249.156 | 22.0.32.1  |
| <input type="checkbox"/> Device_22_0_36_1 | 10.127.249.156 | 22.0.36.1  |
| <input type="checkbox"/> Device_22_0_41_1 | 10.127.249.156 | 22.0.41.1  |
| <input type="checkbox"/> Device_22_0_51_1 | 10.127.249.156 | 22.0.51.1  |
| <input type="checkbox"/> Device_22_0_55_1 | 10.127.249.156 | 22.0.55.1  |
| <input type="checkbox"/> Device_22_0_61_1 | 10.127.249.156 | 22.0.61.1  |
| <input type="checkbox"/> Device_22_0_63_1 | 10.127.249.156 | 22.0.63.1  |
| <input type="checkbox"/> Device_22_0_64_1 | 10.127.249.156 | 22.0.64.1  |
| <input type="checkbox"/> Device_22_0_70_1 | 10.127.249.156 | 22.0.70.1  |

Add >

< Remove

| Device                            | Source IP | IP Address |
|-----------------------------------|-----------|------------|
| Devices are part of selected list |           |            |

1 2 Next

### スキャンのスケジュール

6. スケジュールが完了したら、Save Changesをクリックします。

診断スキャンとインベントリ収集のスケジュールは、[データ収集]ページで編集および削除できません。

The screenshot shows the 'Data Collection' page with a sidebar on the left containing navigation icons for Asset Groups, Identity & Access, Partner Access, Data Collection, Data Sources, Insights, and Automation. The main content area is divided into 'Diagnostic Scans' and 'Inventory Collection'.

**Diagnostic Scans**

| Asset Count | Source         | Schedule              |
|-------------|----------------|-----------------------|
| 1           | 10.127.249.152 | Not scannable         |
| 10          | 10.127.249.152 | Daily at 07:00 PM IST |

A 'Schedule Scan' button is visible above the table. A calendar for October 2022 is shown on the right, with a tooltip for the 4th containing 'Edit Schedule' and 'Delete Schedule' options.

**Inventory Collection**

| Source                                   | Schedule                           |
|--|------------------------------------|
| Other assets collected by CX Cloud Agent | Daily at 04:00 AM IST              |
|  | Daily at 12:30 AM IST              |
| 172.20.224.70/live.cisco.com             | Monthly on the 9th at 11:30 PM IST |
| 10.127.249.152                           | Daily at 02:00 AM IST              |

Below the table, there is a section for 'Rapid Problem Resolution' with a toggle for 'Enable for Campus Network' and a link to 'View detailed instructions'.

スケジュールの編集および削除オプションを使用したデータ収集

## 導入とネットワーク設定

CX Cloud Agentを導入するには、次のいずれかのオプションを選択します。

- VMware vSphere/vCenter Thick Client ESXi 5.5/6.0を選択するには、[Thick Client](#)に移動します。
- VMware vSphere/vCenter Web Client ESXi 6.0を選択するには、[Web Client](#)または[vSphere Center](#)に移動します。
- Oracle Virtual Box 5.2.30を選択するには、[Oracle VM](#)に移動します。
- Microsoft Hyper-Vを選択するには、[Hyper-V](#)

## OVA の導入

### シッククライアント ESXi 5.5/6.0 のインストール

このクライアントでは、vSphereシッククライアントを使用してCX Cloud Agent OVAを導入できません。

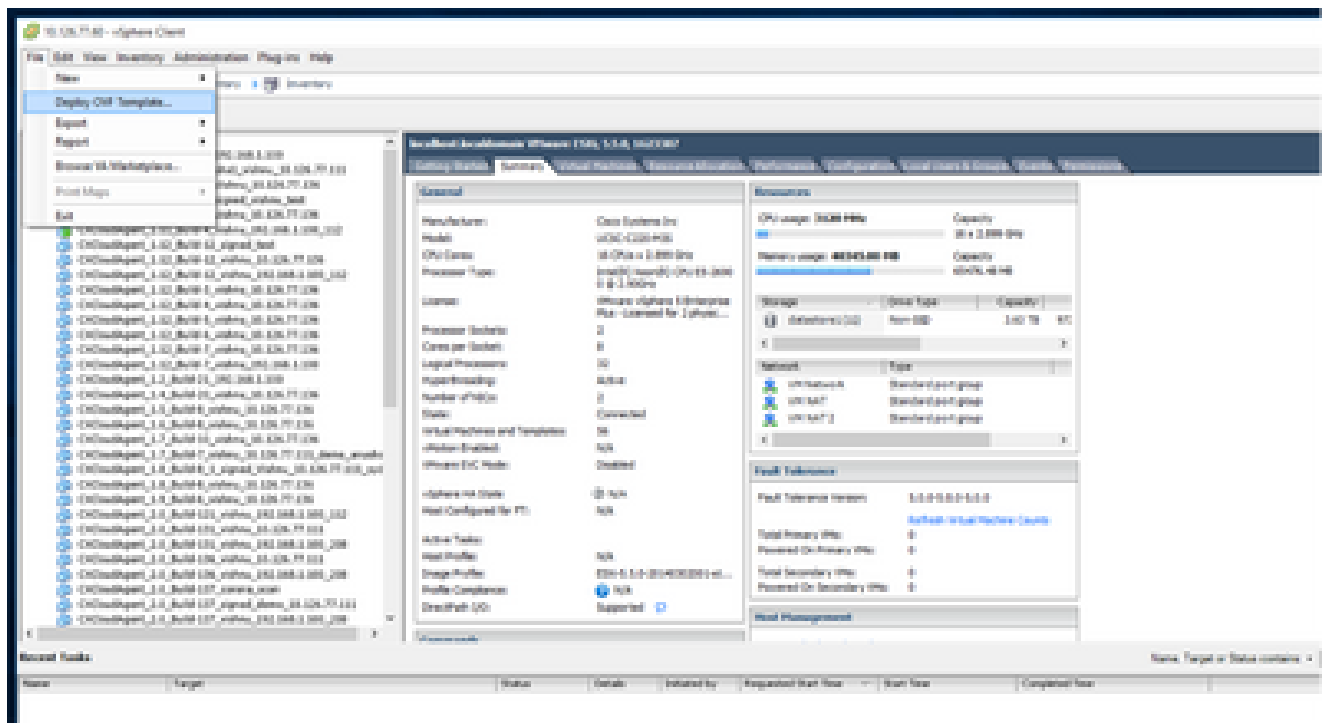
1. イメージをダウンロードしたら、VMware vSphere Clientを起動してログインします。



ログイン

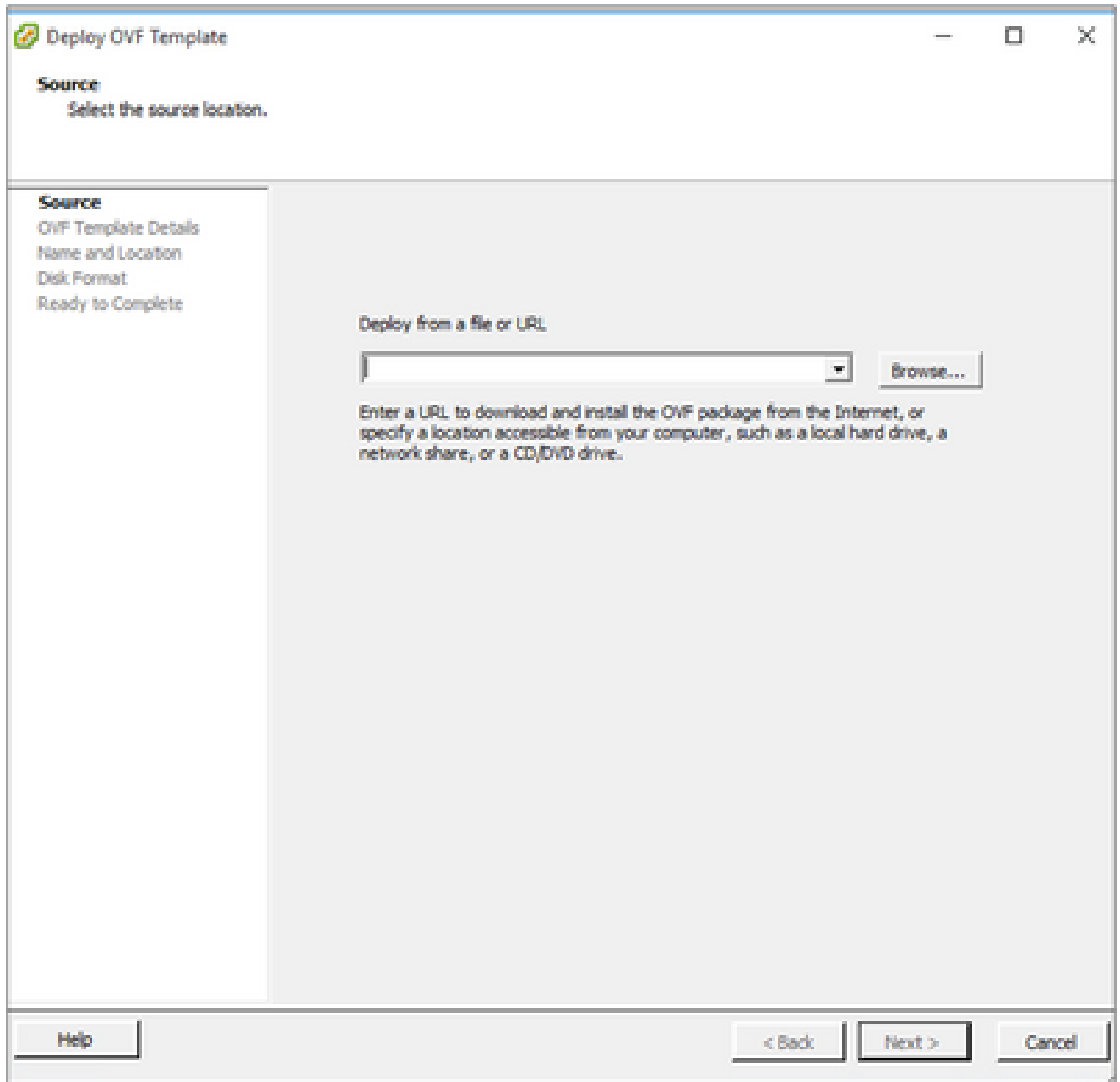
- メニューから、File > Deploy OVF Templateの順に選択します。





vSphere クライアント

3. OVAファイルを参照して選択し、Nextをクリックします。



OVA バス

4. OVF Detailsを確認し、Nextをクリックします。

**OVF Template Details**

Verify OVF template details.

**SOURCE**  
**OVF Template Details**  
Name and Location  
Disk Format  
Network Mapping  
Ready to Complete

|                |   |
|----------------|---|
| Product:       | CXCloudAgent_2.0_Build-144                                |
| Version:       | 2.0   |
| Vendor:        | Cisco Systems, Inc  |
| Publisher:     | <input checked="" type="checkbox"/> CISCO SYSTEMS, INC.   |
| Download size: | 1.1 GB  |
| Size on disk:  | 3.1 GB (thin provisioned)<br>200.0 GB (thick provisioned) |
| Description:   | CXCloudAgent_2.0_Build-144                                |

Help      < Back      Next >      Cancel

テンプレートの詳細

5. 一意の名前を入力して、Nextをクリックします。

**Name and Location**

Specify a name and location for the deployed template

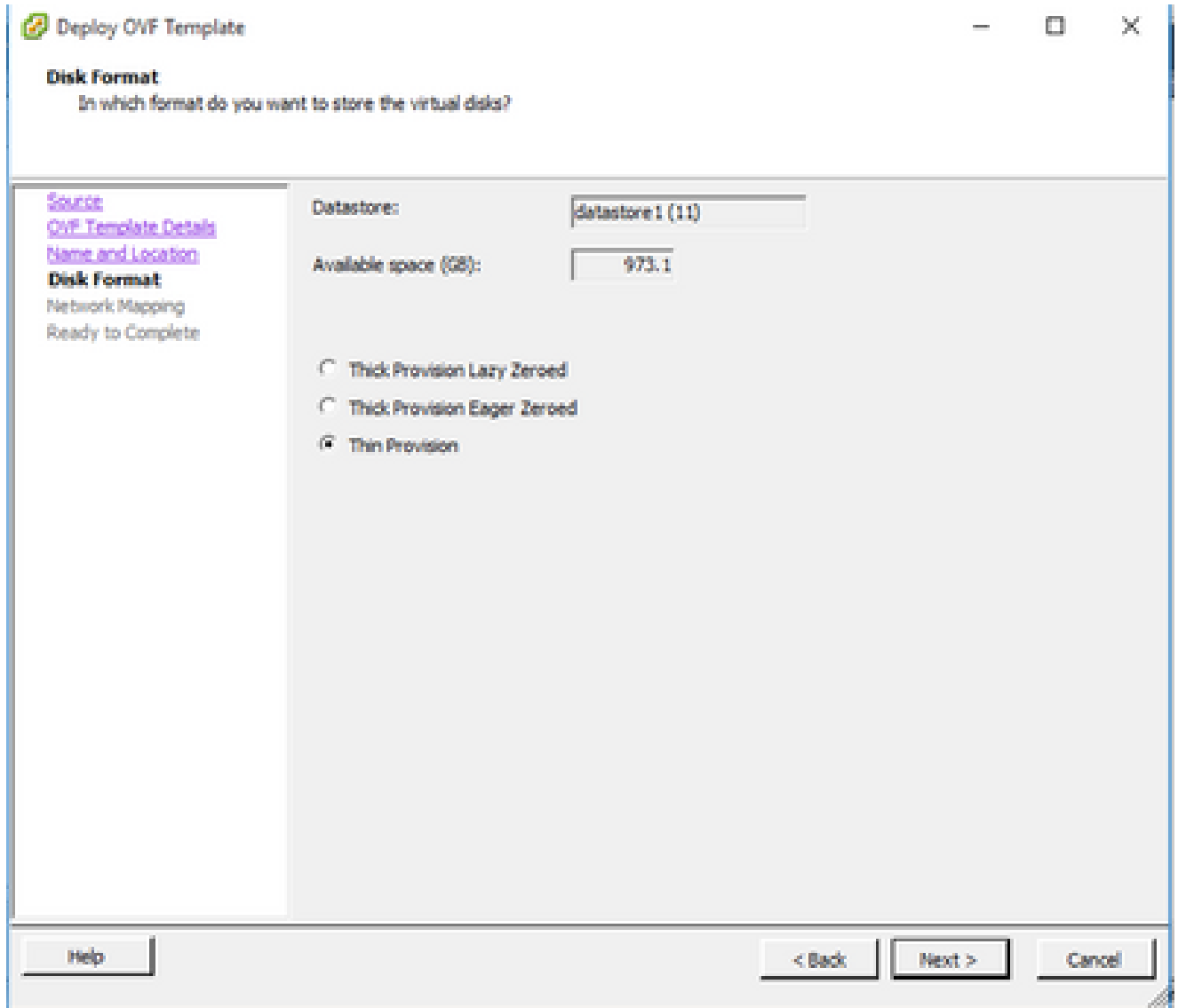
**Source**  
[OVF Template Details](#)  
**Name and Location**  
Disk Format  
Network Mapping  
Ready to Complete

Name:  
CxCloudAgent\_2.0\_Build-144\_0000  
The name can contain up to 80 characters and it must be unique within the inventory folder.

Help < Back Next > Cancel

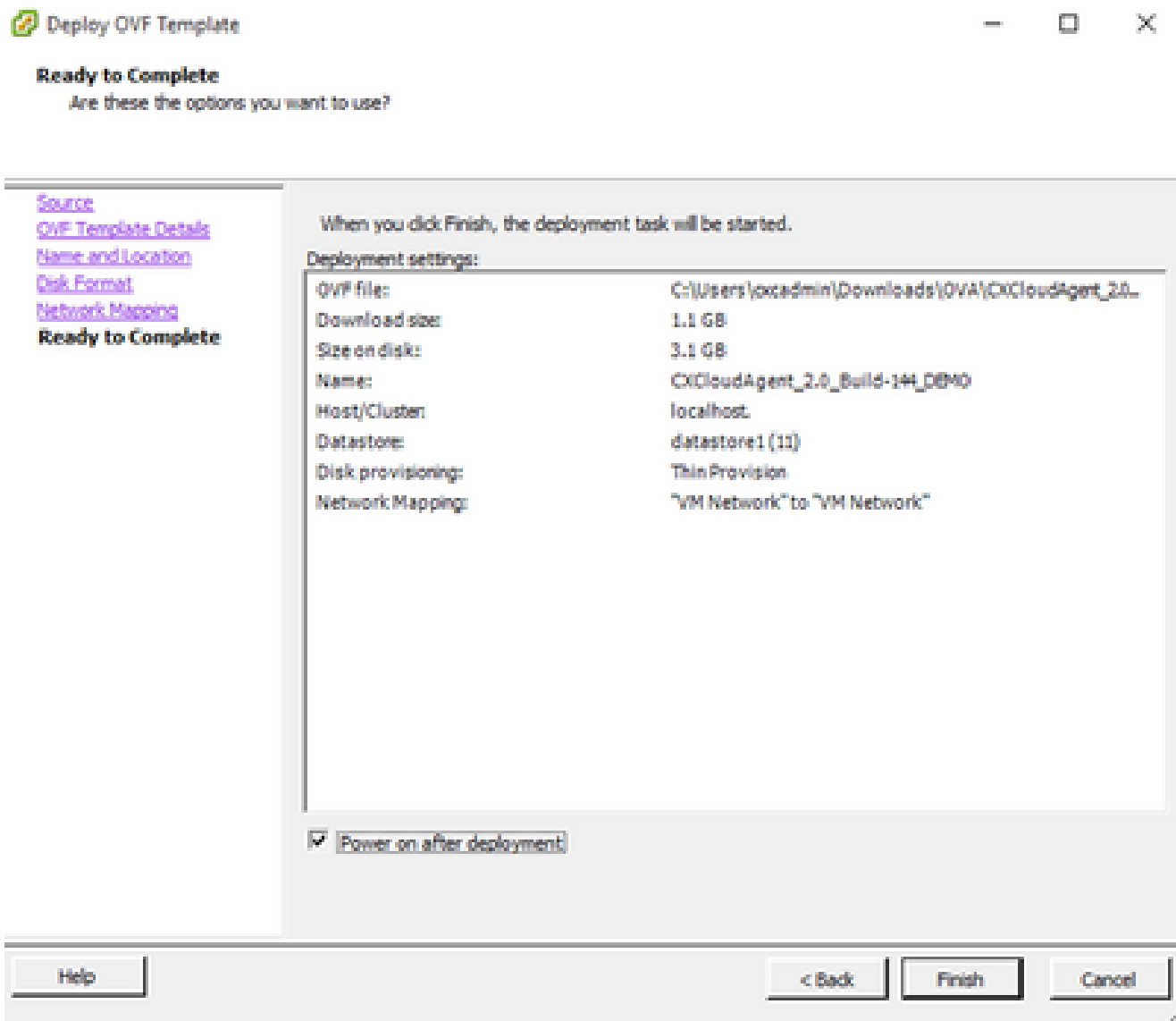
名前と場所

6. Disk Formatを選択し、Nextをクリックします（Thin Provisionを推奨）。



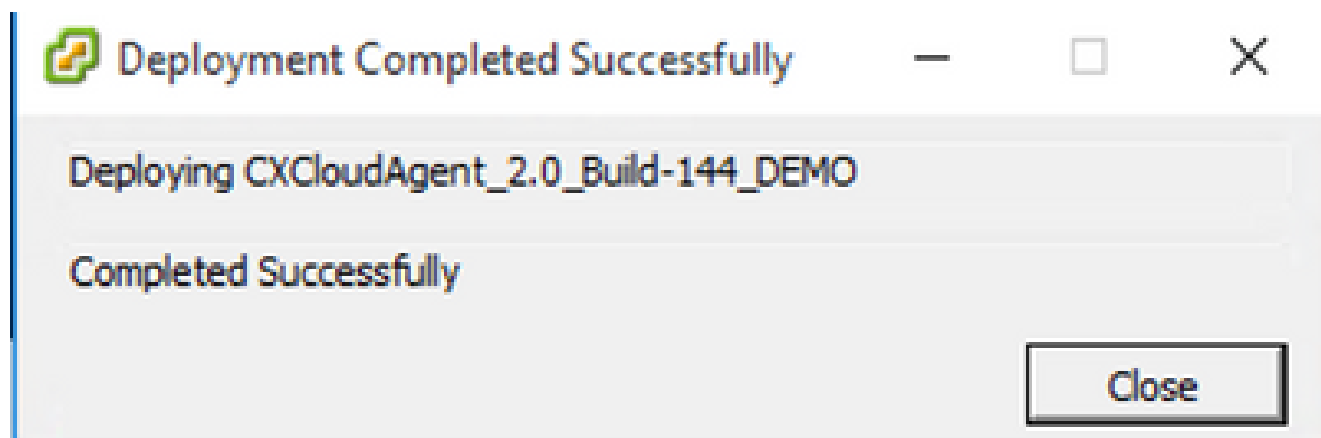
ディスクの書式設定

7. Power on after deployment チェックボックスを選択して、Closeをクリックします。



終了準備の完了 ( Ready to Complete )

導入には数分かかる場合があります。展開が成功すると、確認の表示が行われます。



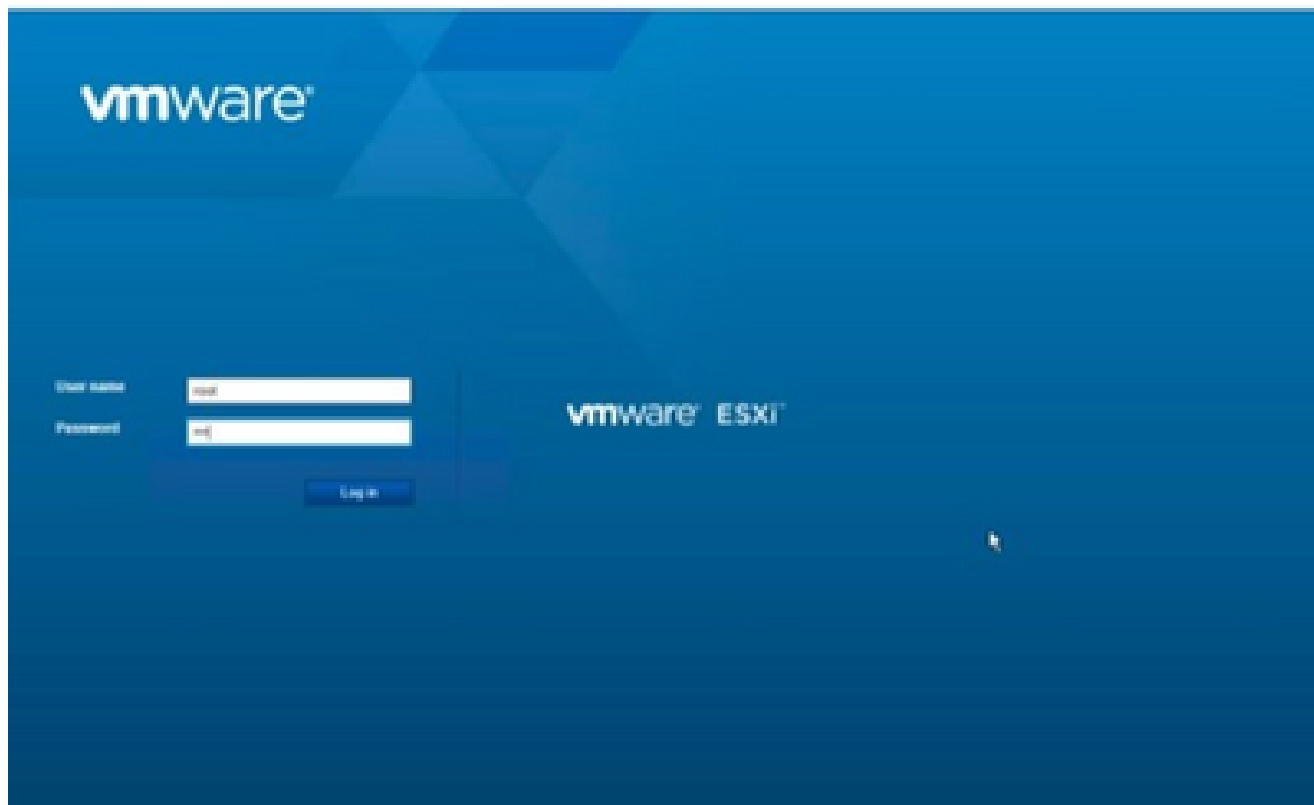
導入の完了

- 導入したVMを選択し、コンソールを開いて [Network Configuration](#) に移動し、次の手順に進みます。

## Web クライアント ESXi 6.0 のインストール

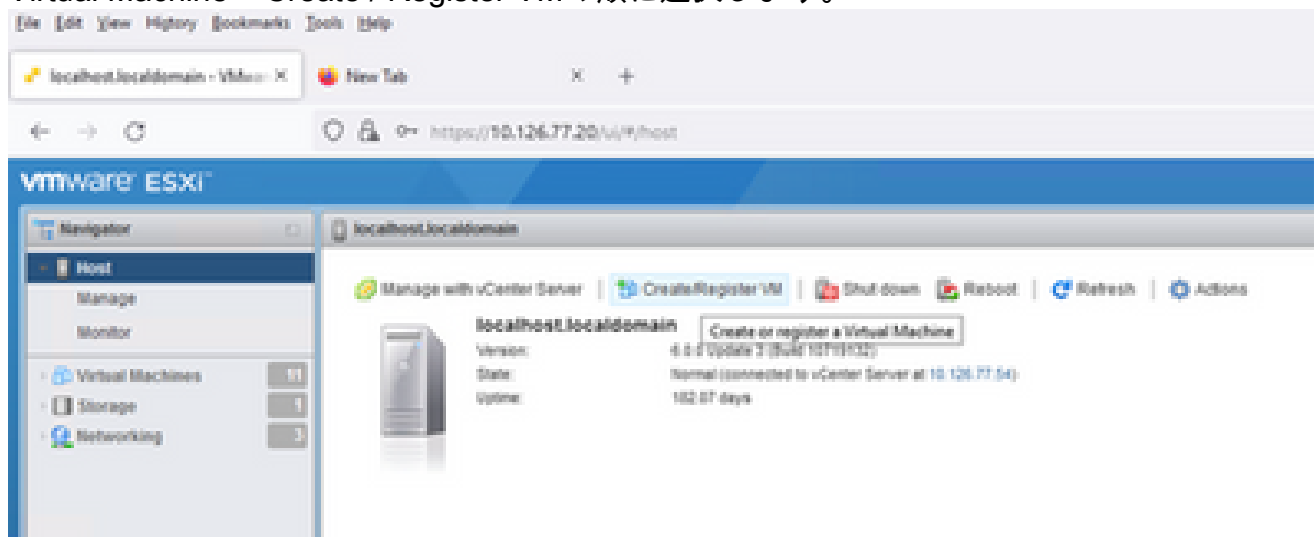
このクライアントは、vSphere Webを使用してCX Cloud Agent OVAを導入します。

1. VMの導入に使用するESXi/ハイパーバイザクレデンシャルを使用して、VMWare UIにログインします。



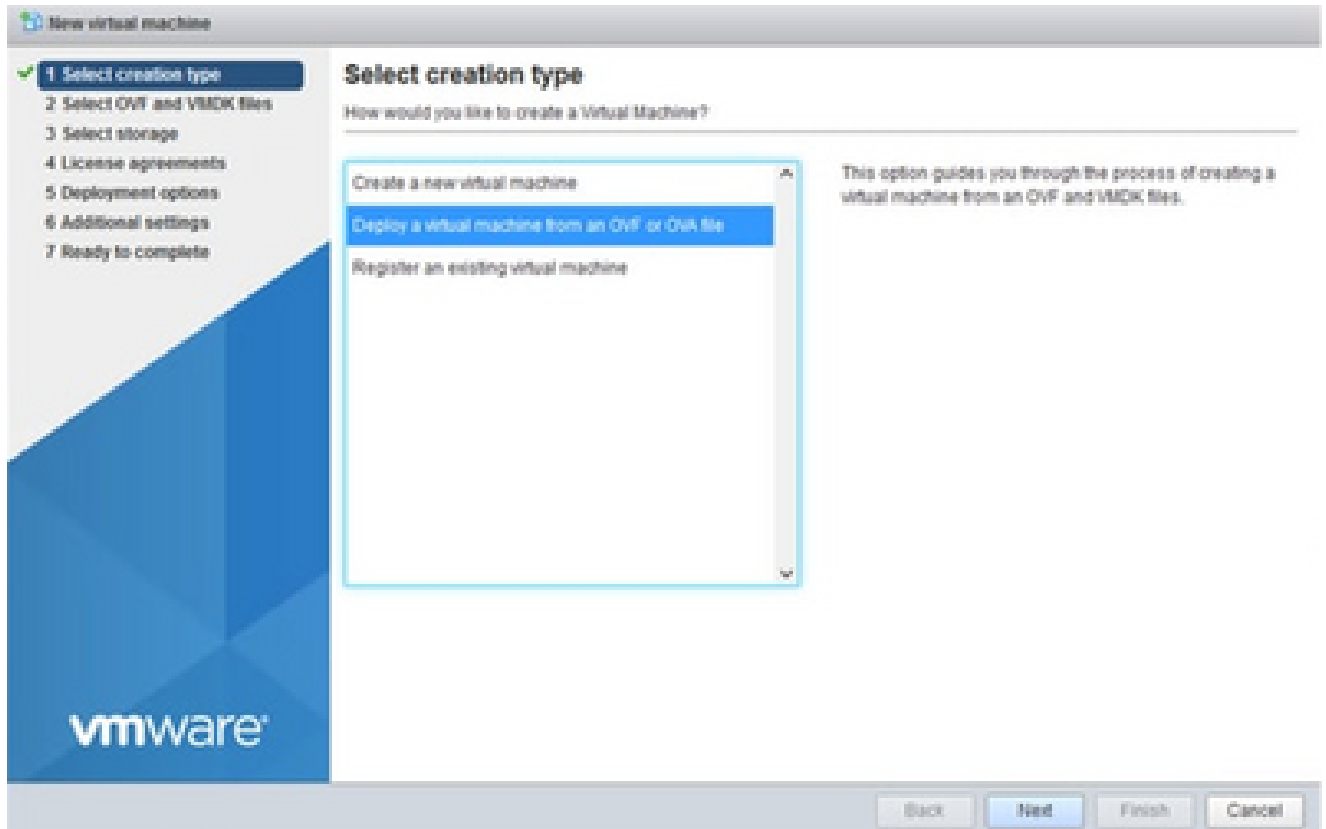
VMware ESXi のログイン

2. Virtual Machine > Create / Register VMの順に選択します。



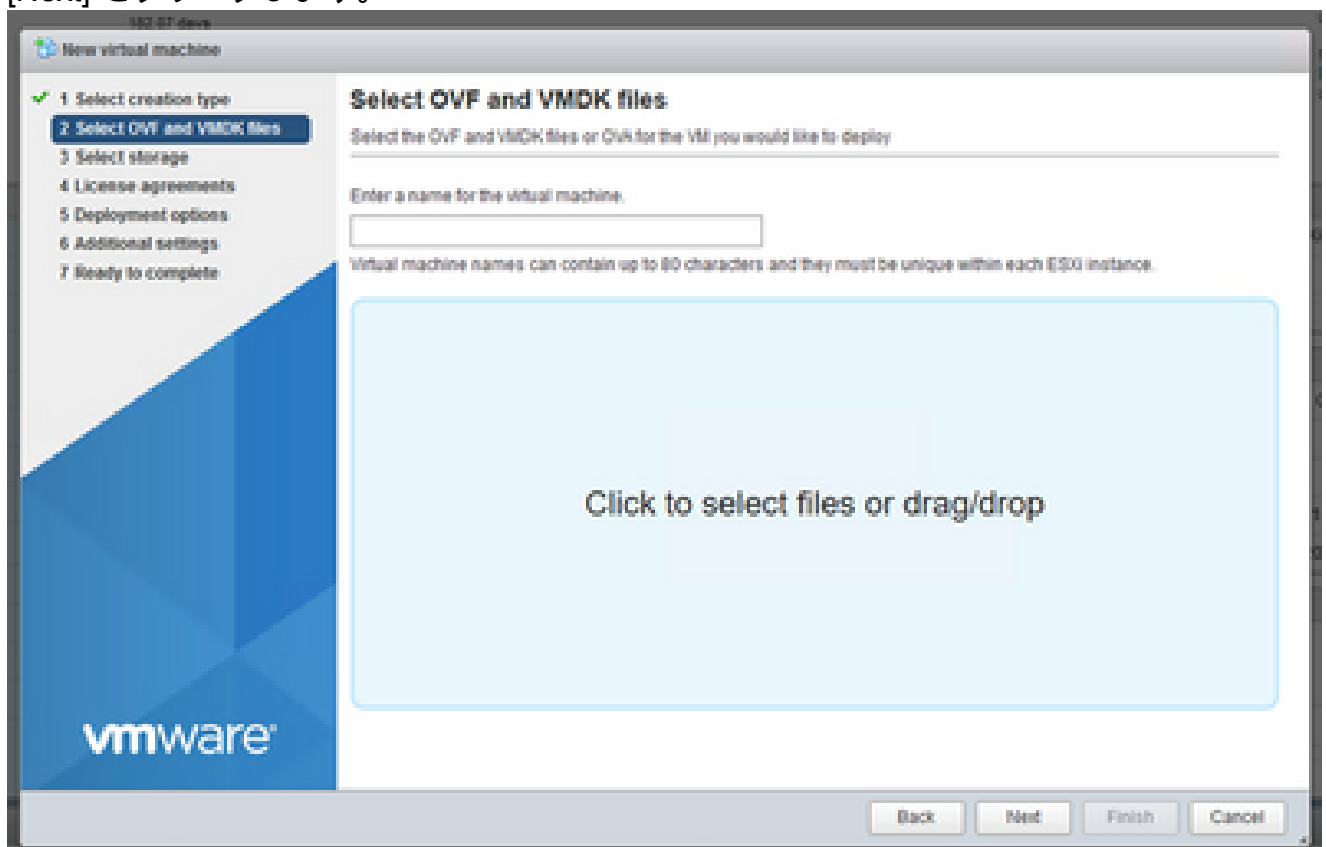
VM の作成

3. [OVF または OVA ファイルから仮想マシンを導入 ( Deploy a virtual machine from OVF or OVA file ) ] を選択して、[次へ ( Next ) ] をクリックします。



作成タイプの選択

4. VMの名前を入力し、ファイルを参照して選択するか、ダウンロードしたOVAファイルをドラッグアンドドロップします。
5. [Next] をクリックします。



OVA の選択



6. [標準ストレージ ( Standard Storage ) ] を選択し、[次へ ( Next ) ] をクリックします。

| Name       | Capacity | Free    | Type  | Thin pro... | Access |
|------------|----------|---------|-------|-------------|--------|
| datastore1 | 4.35 TB  | 3.57 TB | VMFS5 | Supported   | Single |

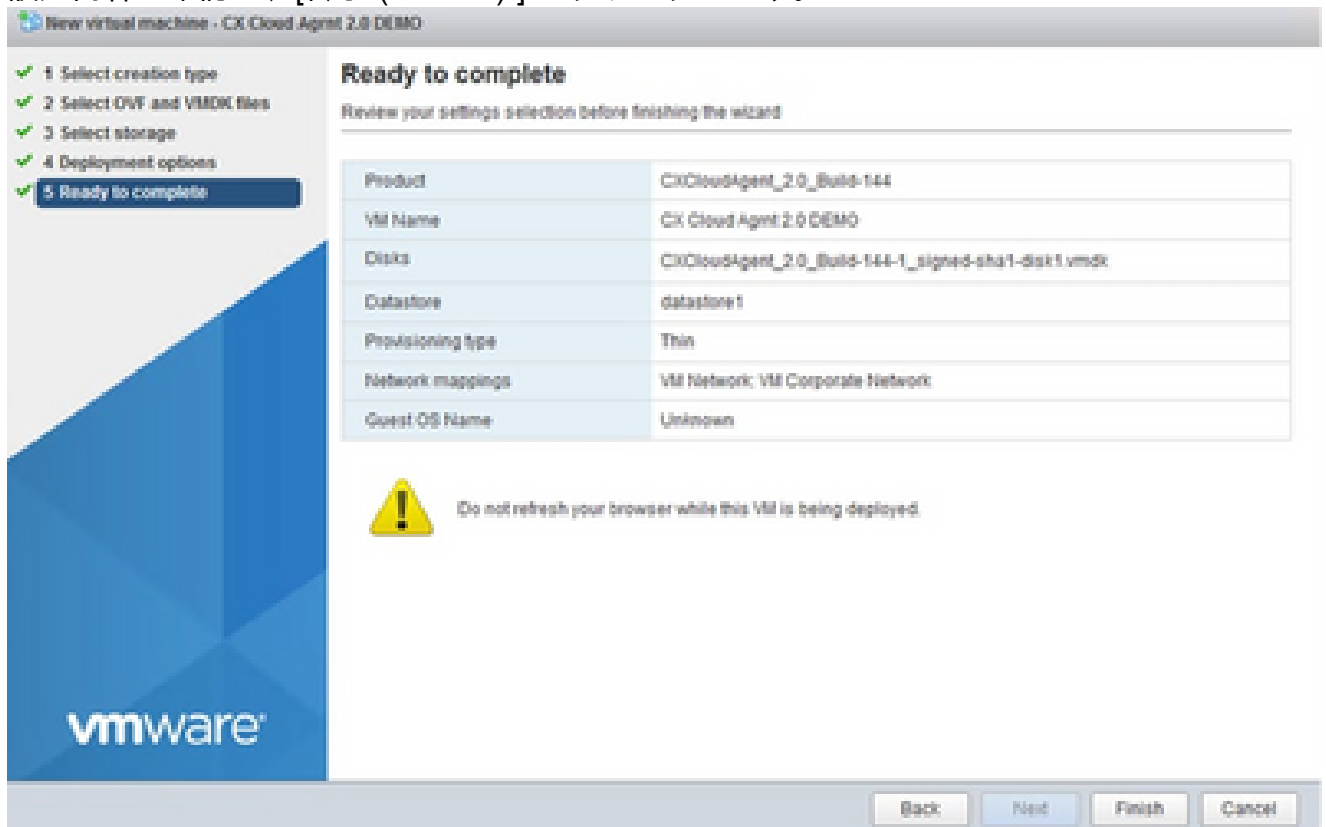
ストレージの選択

7. 適切なDeploymentオプションを選択し、Nextをクリックします。

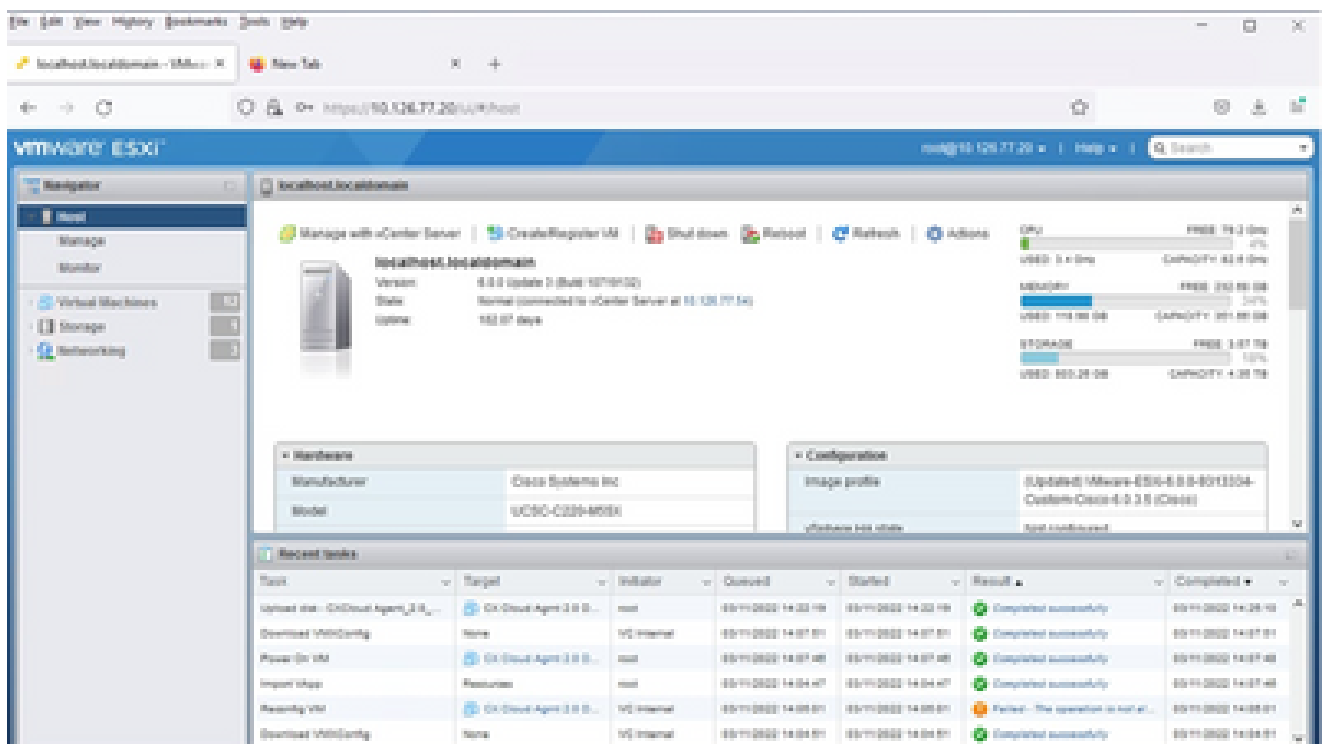
|                        |   |                      |
|------------------------|---|----------------------|
| Network mappings       | VM Network  | VM Corporate Network |
| Disk provisioning      | <input checked="" type="radio"/> Thin <input type="radio"/> Thick |                      |
| Power on automatically | <input checked="" type="checkbox"/>                               |                      |

導入オプション

8. 設定内容を確認し、[終了 ( Finish ) ] をクリックします。

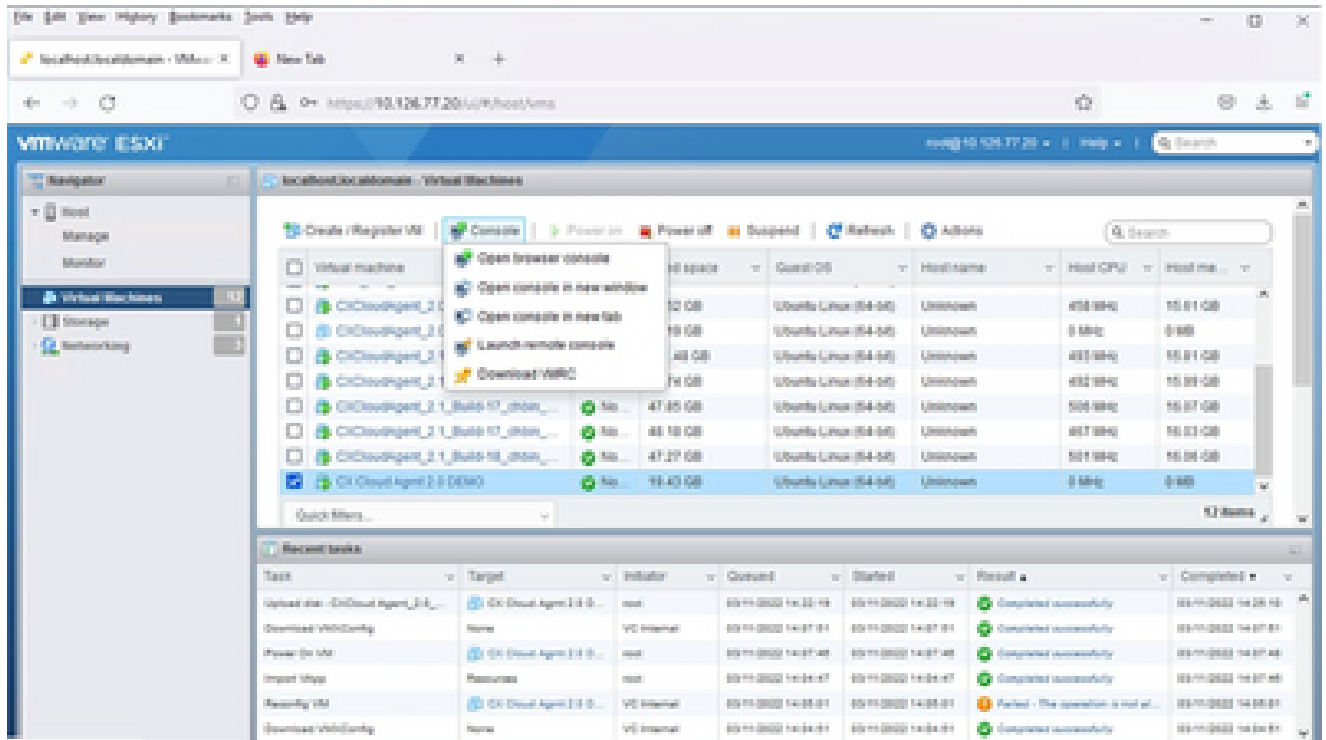


終了準備の完了 ( Ready to Complete )



正常終了

9. 導入したばかりのVMを選択し、Console > Open browser consoleの順に選択します。



コンソール

10. [Network Configuration](#)に移動して、次の手順に進みます。

Web クライアント vCenter のインストール

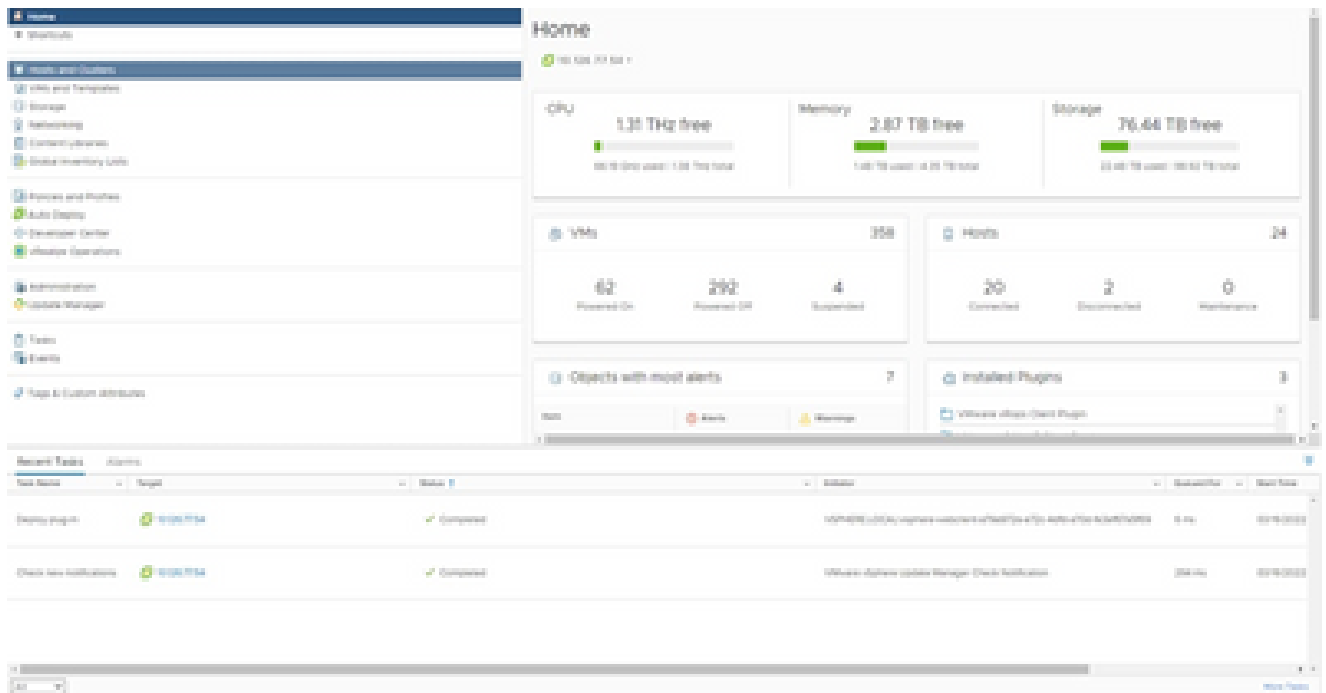
次の手順を実行します。

1. ESXi/ハイパーバイザのクレデンシャルを使用してvCenterクライアントにログインします。



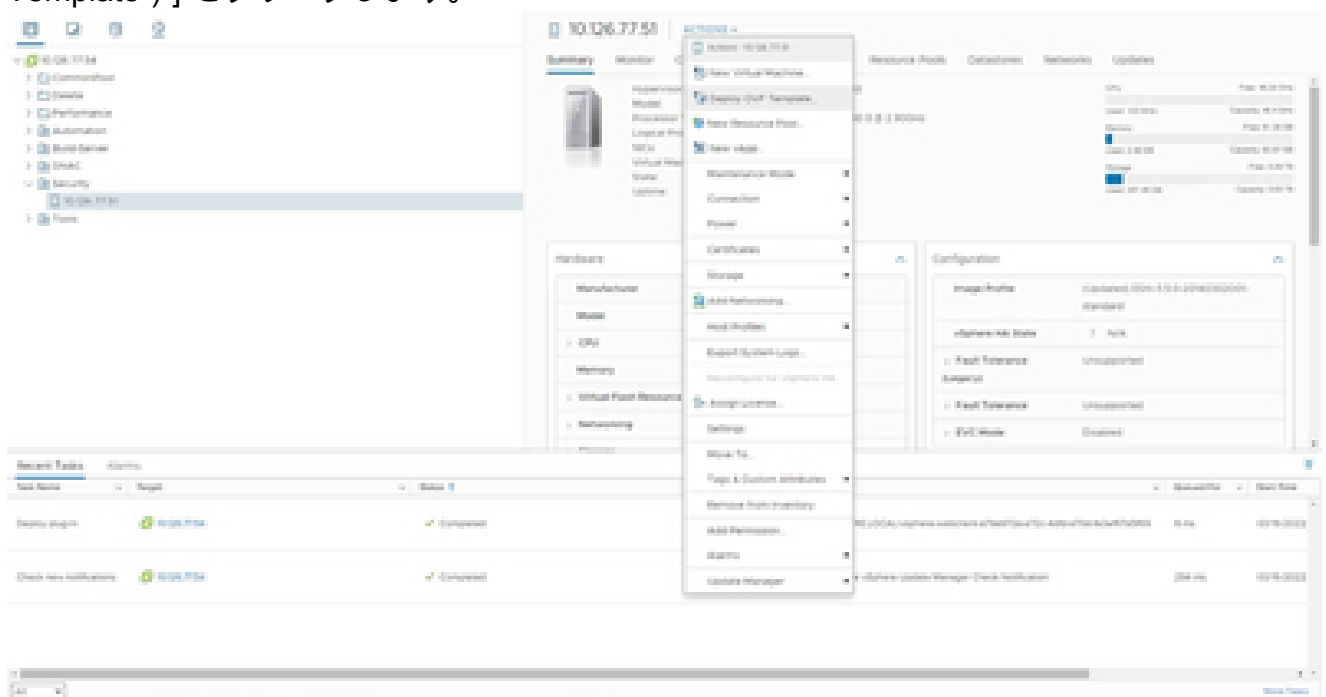
ログイン

2. Homeページから、Hosts and Clustersをクリックします。



ホームページ

3. VM を選択し、[アクション ( Action ) ] > [OVF テンプレートの導入 ( Deploy OVF Template ) ] をクリックします。



[アクション ( Actions ) ]

## Deploy OVF Template

### 1 Select an OVF template

- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 Select storage
- 6 Ready to complete

### Select an OVF template

Select an OVF template from remote URL, or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

URL

Local file

No file chosen

 Select a template to deploy. Use multiple selection to select all the files associated with an OVF template (.ovf, .vmdk, etc.)

テンプレートの選択(Select Template)

4. URLを直接追加するか、参照してOVAファイルを選択し、Nextをクリックします。
5. 一意の名前を入力し、必要に応じて場所を参照します。
6. [Next] をクリックします。

# Deploy OVF Template

✓ 1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

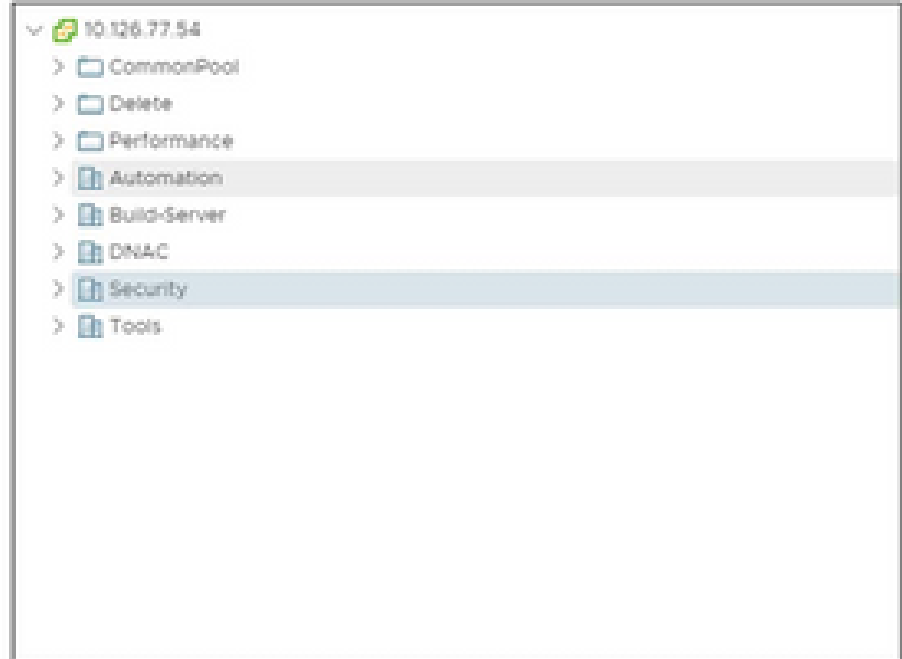
6 Ready to complete

Select a name and folder

Specify a unique name and target location

Virtual machine name: CXCloudAgent\_2.0\_Build-144-demo

Select a location for the virtual machine.



CANCEL

BACK

NEXT

名前とフォルダ

7. コンピューティングリソースを選択し、Nextをクリックします。

## Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- 3 Select a compute resource**
- 4 Review details
- 5 Select storage
- 6 Ready to complete

Select a compute resource

Select the destination compute resource for this operation

▼ Security

> 10.126.77.51

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

コンピュータリソースの選択

8. 詳細を確認し、[次へ ( Next ) ] をクリックします。

## Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- 4 Review details**
- 5 Select storage
- 6 Select networks
- 7 Ready to complete

### Review details

Verify the template details.

|               |  |
|---------------|--|
| Publisher     | DigiCert SHA2 Assured ID Code Signing CA (Trusted certificate) |
| Product       | CxCloudAgent_3.0_Build-144                                     |
| Version       | 2.0  |
| Vendor        | Cisco Systems, Inc   |
| Description   | CxCloudAgent_3.0_Build-144                                     |
| Download size | 1.1 GB   |
| Size on disk  | 3.1 GB (thin provisioned)                                      |
|               | 200.0 GB (thick provisioned)                                   |

CANCEL

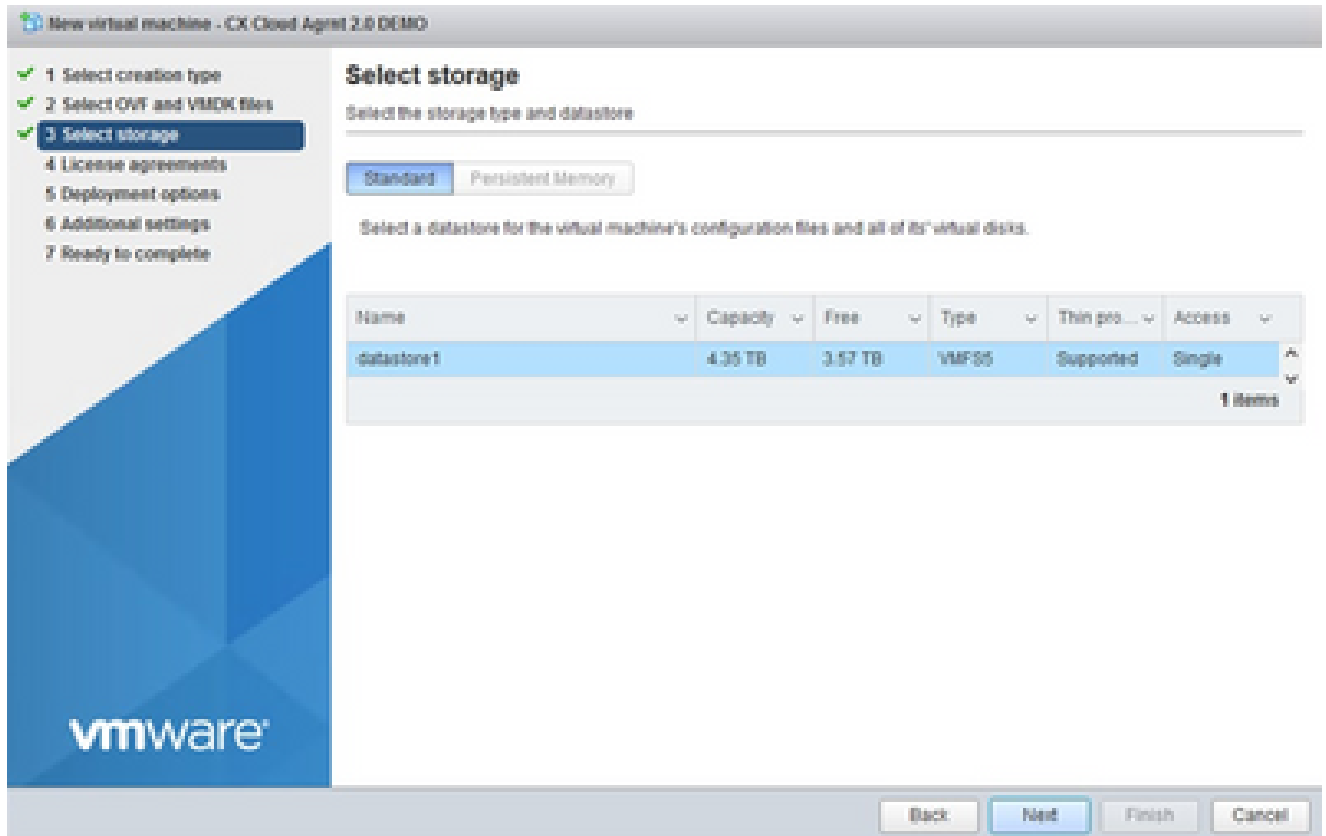
BACK

NEXT

詳細の確認

9. 仮想ディスク形式を選択し、[次へ ( Next ) ] をクリックします。





ストレージの選択

10. [Next] をクリックします。

## Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- 4 Review details**
- 5 Select storage
- 6 Select networks
- 7 Ready to complete

### Review details

Verify the template details.

|               |  |
|---------------|--|
| Publisher     | DigiCert SHA2 Assured ID Code Signing CA (Trusted certificate) |
| Product       | CxCloudAgent_3.0_Build-144                                     |
| Version       | 2.0  |
| Vendor        | Cisco Systems, Inc   |
| Description   | CxCloudAgent_3.0_Build-144                                     |
| Download size | 1.1 GB   |
| Size on disk  | 3.1 GB (thin provisioned)                                      |
|               | 200.0 GB (thick provisioned)                                   |

CANCEL

BACK

NEXT

ネットワークの選択

11. [Finish] をクリックします。

# Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 Select storage
- ✓ 6 Select networks
- 7 Ready to complete**

Ready to complete  
Click Finish to start creation.

|                        |  |
|------------------------|--|
| Provisioning type      | Deploy from template                               |
| Name                   | CxCloudAgent_2.0_Build-144-demo                    |
| Template name          | CxCloudAgent_2.0_Build-144-1_signed-sha1           |
| Download size          | 11 GB  |
| Size on disk           | 3.1 GB   |
| Folder                 | Security   |
| Resource               | 10.126.77.51                                       |
| Storage mapping        | 1  |
| All disks              | Datastore: datastore1 (23); Format: Thin provision |
| Network mapping        | 1  |
| VM Network             | VM Network   |
| IP allocation settings |  |
| IP protocol            | IPv4   |
| IP allocation          | Static - Manual                                    |

CANCEL BACK FINISH

終了準備の完了 ( Ready to Complete )

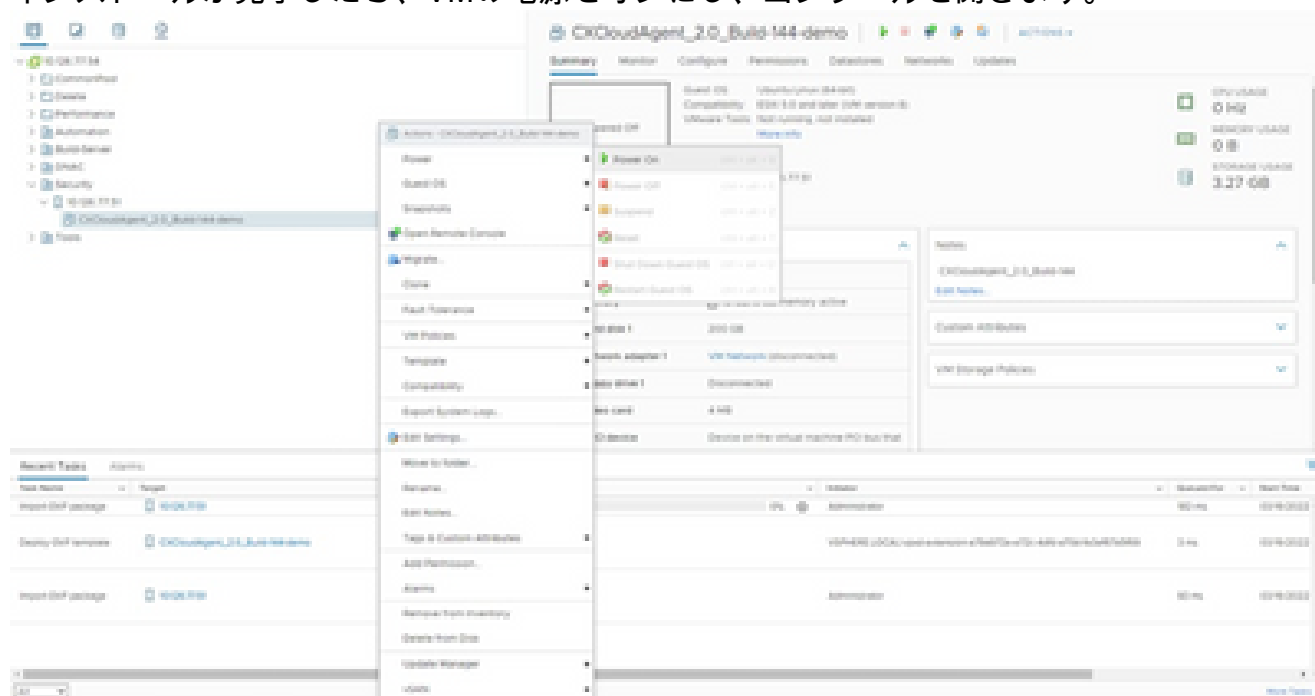
## 12. 新しく追加されたVMの名前をクリックして、ステータスを表示します。

The screenshot shows the vSphere interface. The top part displays the details for the VM 'CxCloudAgent\_2.0\_Build-144-demo', including its status (Powered Off), hardware specifications (CPU, Memory, Hard disk, Network adapter, Floppy disk, Video card, VMX device), and storage/network settings. Below this, the 'Recent Tasks' table is visible, showing the deployment of this VM as a completed task.

| Task Name           | Progress | Status    | Owner         | Start Time | End Time   |
|---------------------|----------|-----------|---------------|------------|------------|
| Import OVF template | 100%     | Completed | Administrator | 12/19/2022 | 12/19/2022 |
| Deploy OVF template | 100%     | Completed | Administrator | 12/19/2022 | 12/19/2022 |
| Import OVF template | 100%     | Completed | Administrator | 12/19/2022 | 12/19/2022 |

追加されたVM

### 13. インストールが完了したら、VMの電源をオンにし、コンソールを開きます。



[コンソールを開く ( Open Console )]

### 14. [ネットワーク設定](#)に移動し、次の手順に進みます。

## Oracle Virtual Box 5.2.30 のインストール

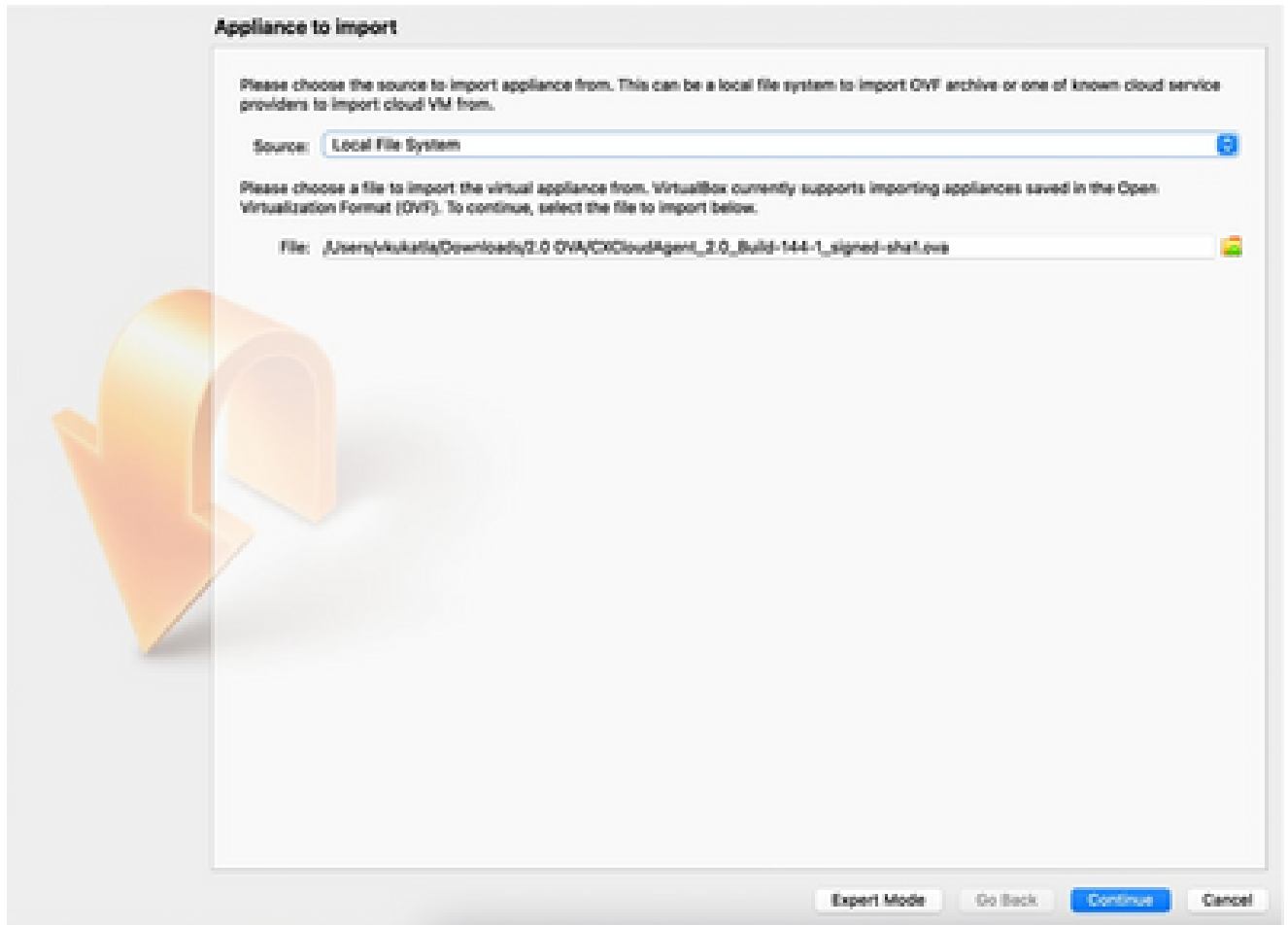
このクライアントは、Oracle Virtual Boxを介してCX Cloud Agent OVAを導入します。

### 1. Oracle VM UIを開き、File> Import Applianceを選択します。



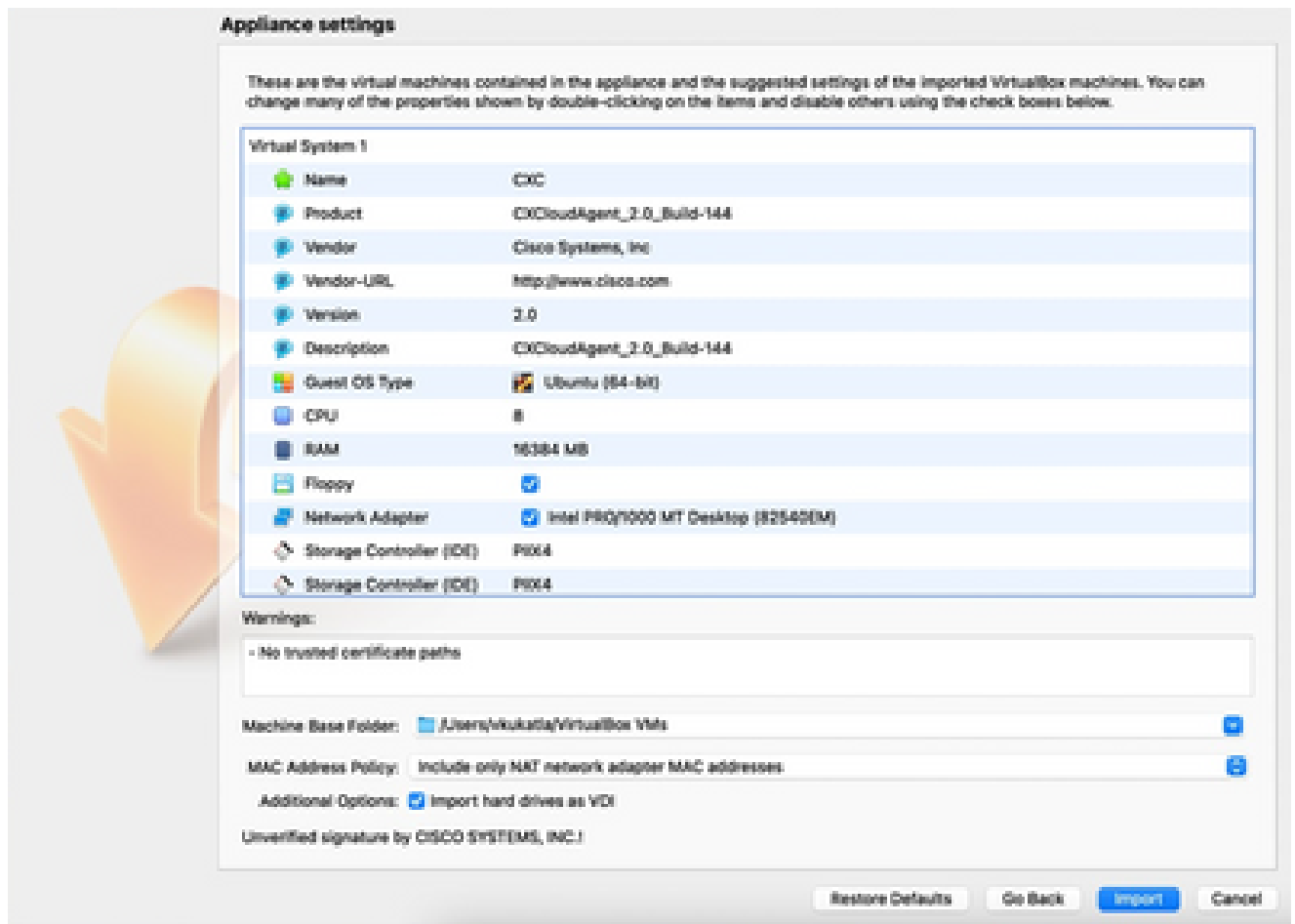
Oracle VM

### 2. インポートする OVA ファイルを参照します。



ファイルの選択

3. [Import] をクリックします。

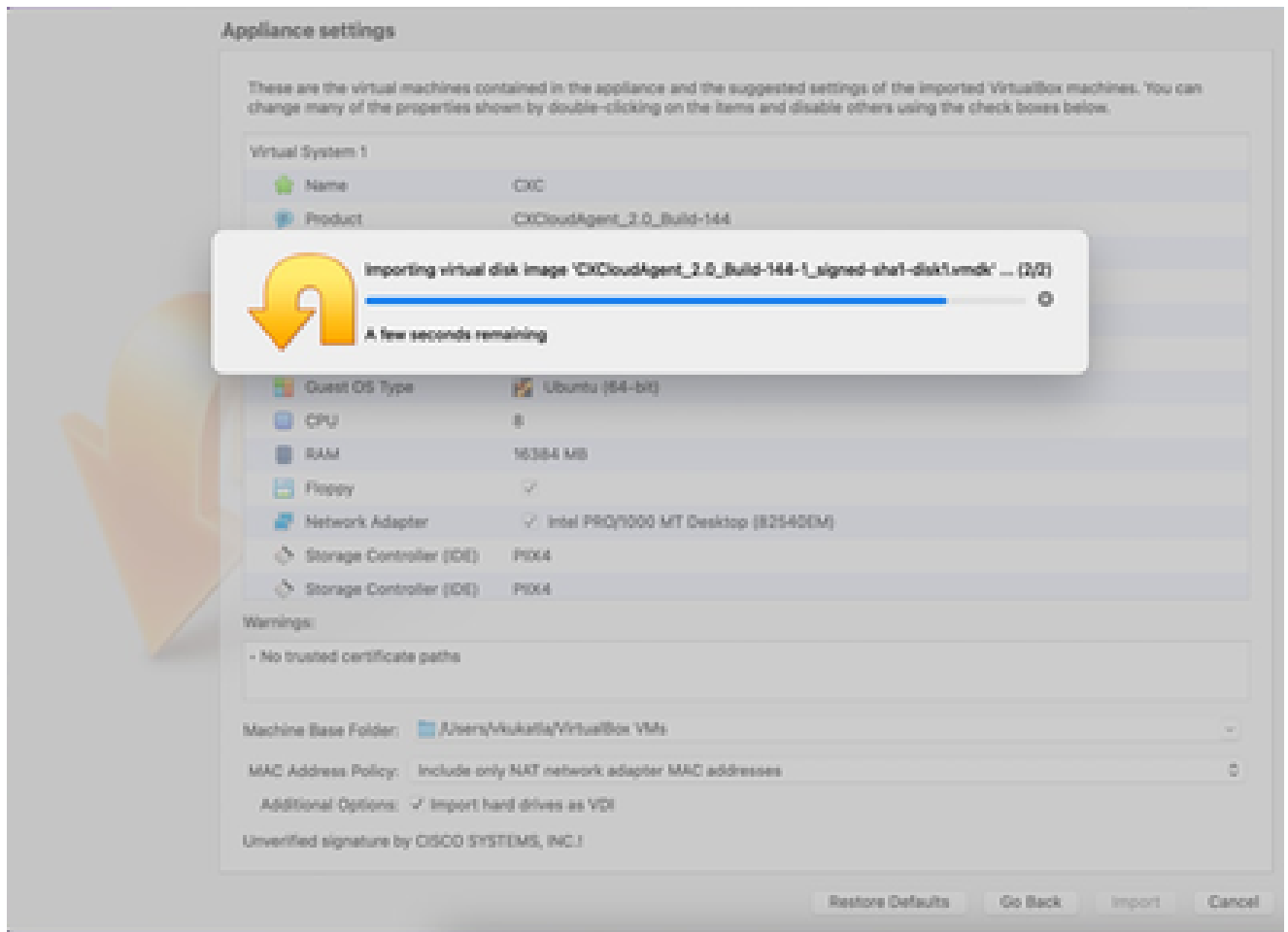


ファイルのインポート

#### 4. 導入したばかりのVMを選択し、Startをクリックします。



VM コンソールの起動



インポートしています

## 5. VMの電源をオンにします。コンソールが表示されます。



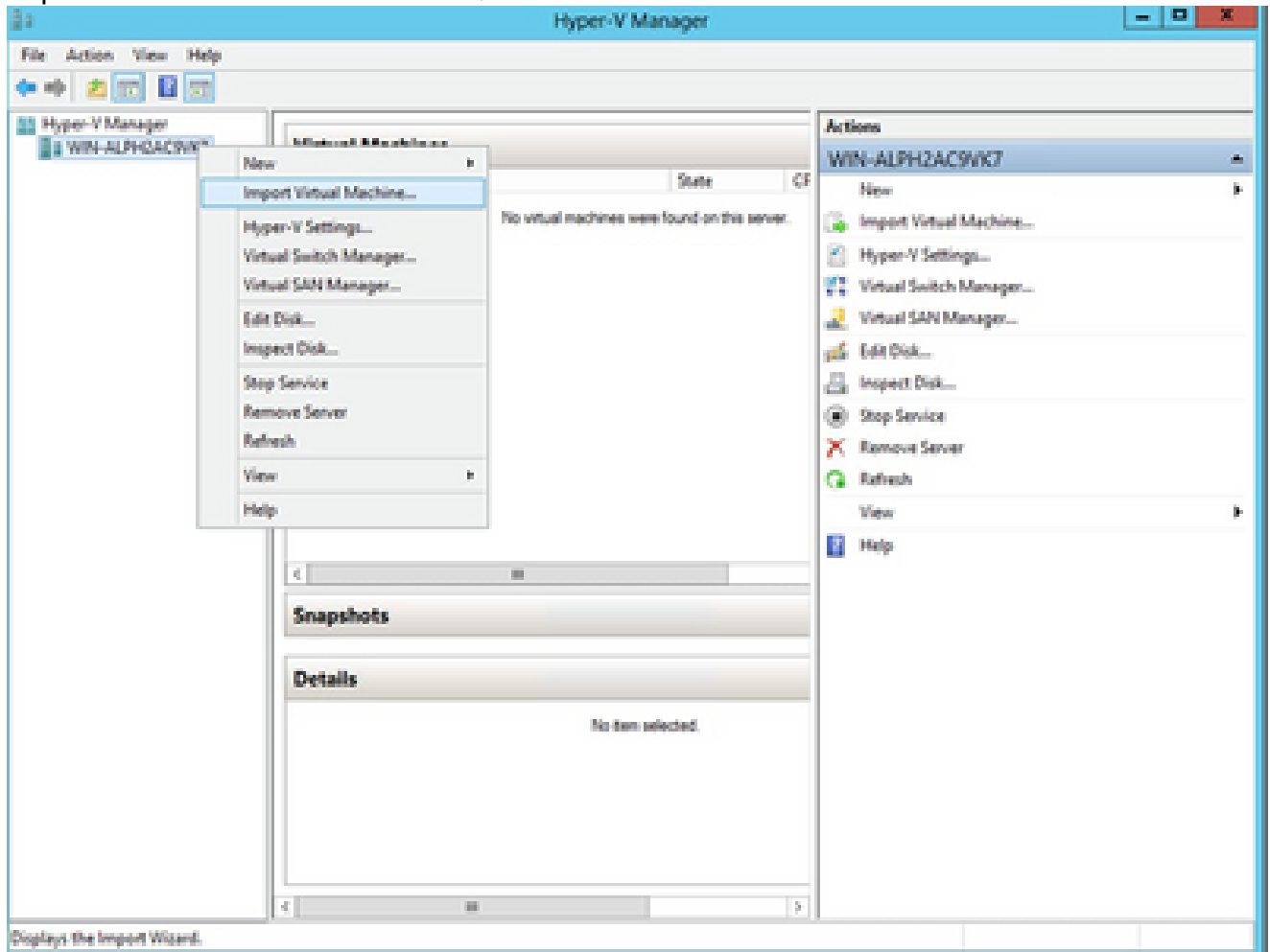
[コンソールを開く ( Open Console )]

6. [Network Configuration](#)に移動して、次の手順に進みます。

## Microsoft Hyper-V のインストール

次の手順を実行します。

1. Import Virtual Machineを選択します。

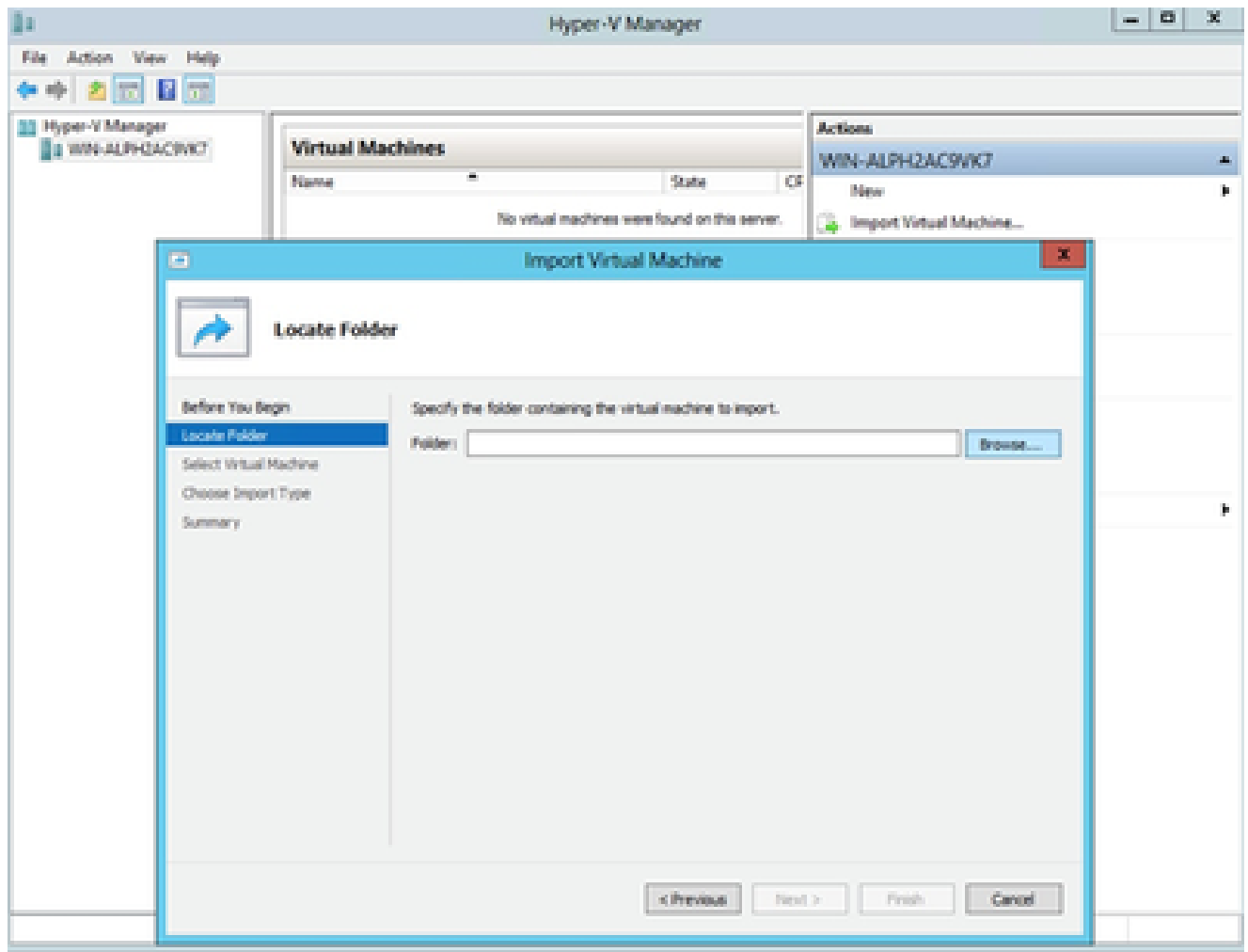


Hyper Vマネージャー

2. 参照してダウンロードフォルダを選択します。

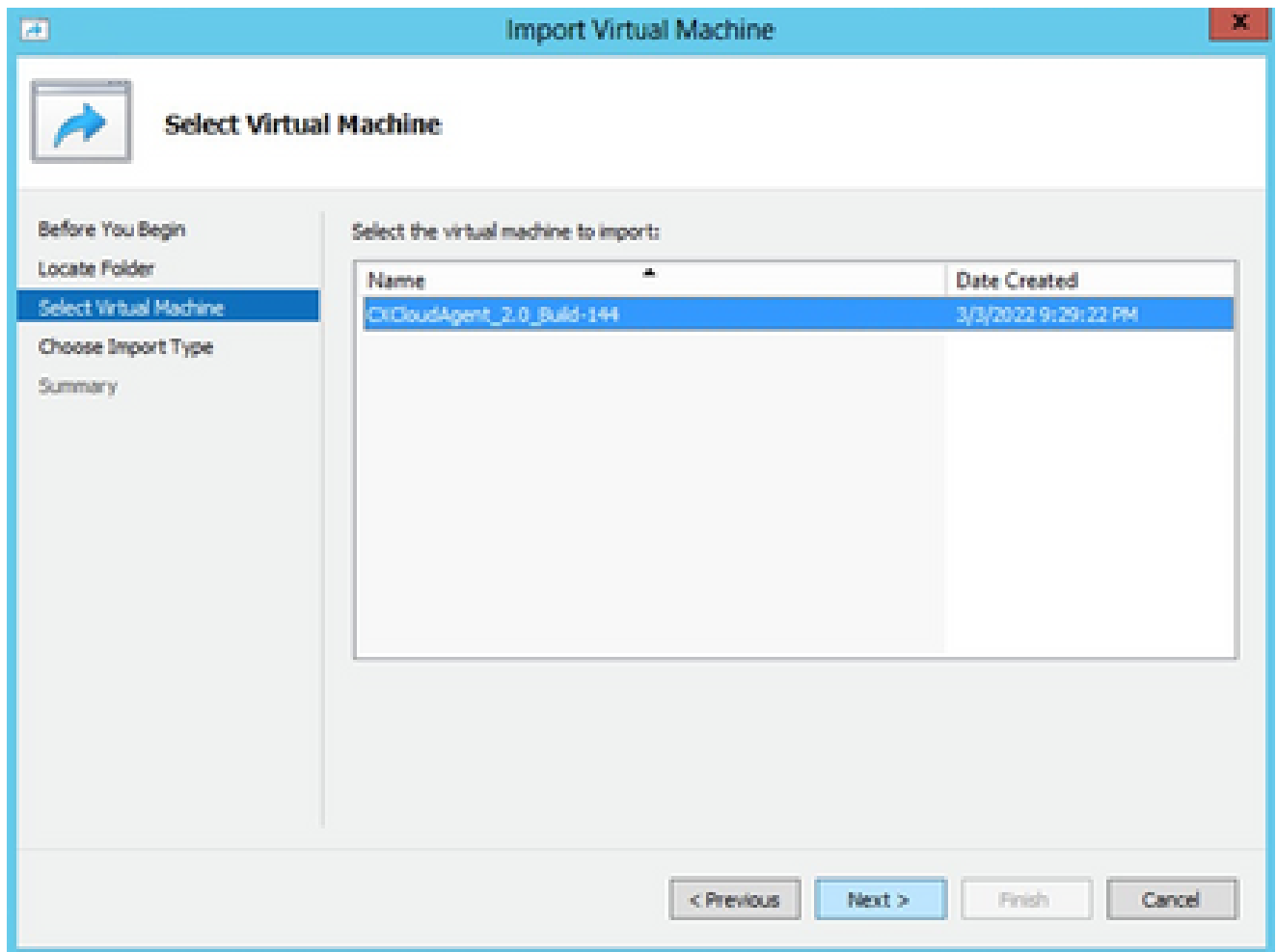
3. [Next] をクリックします。





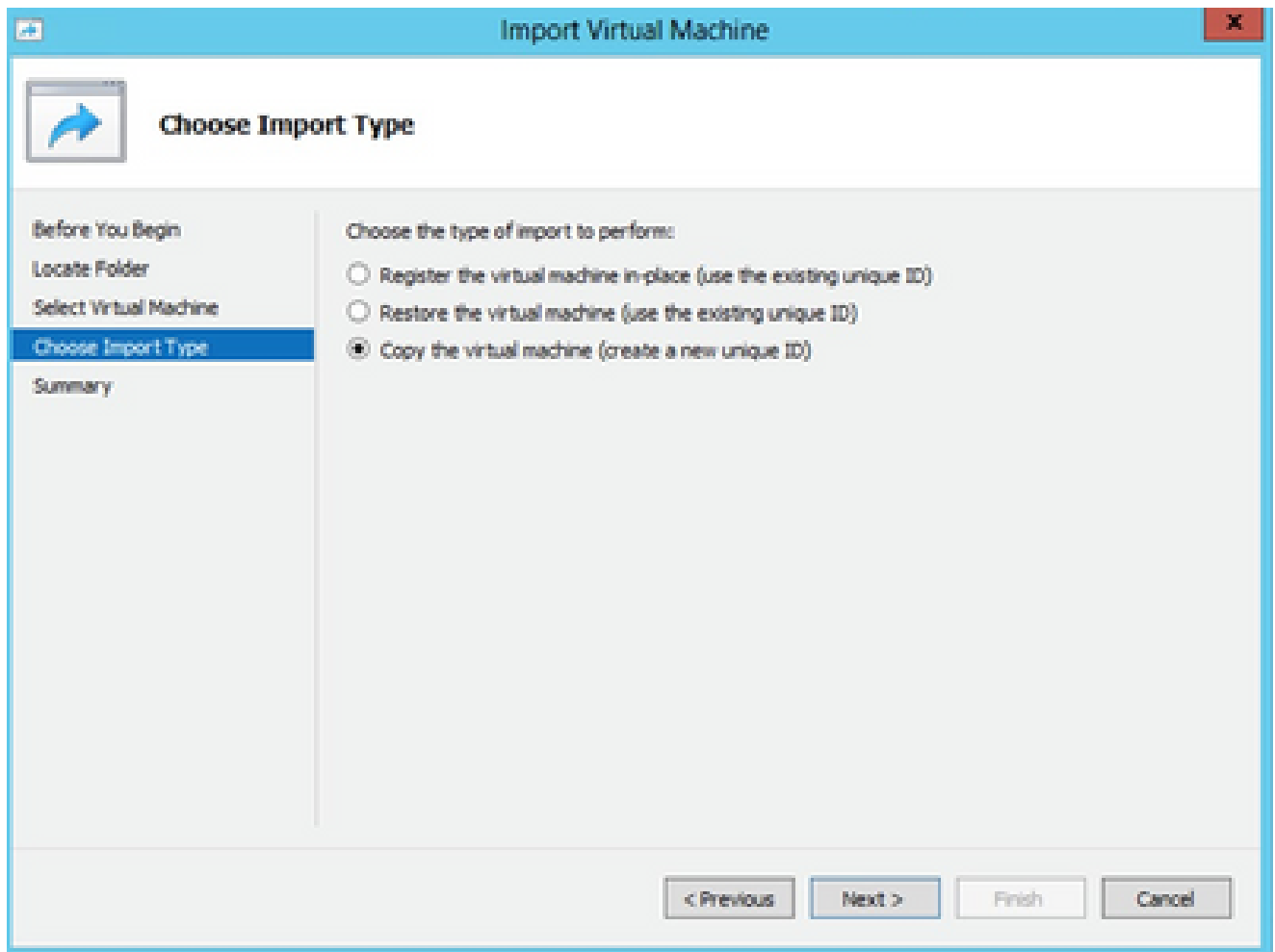
インポートするフォルダ

4. VMを選択し、Nextをクリックします。



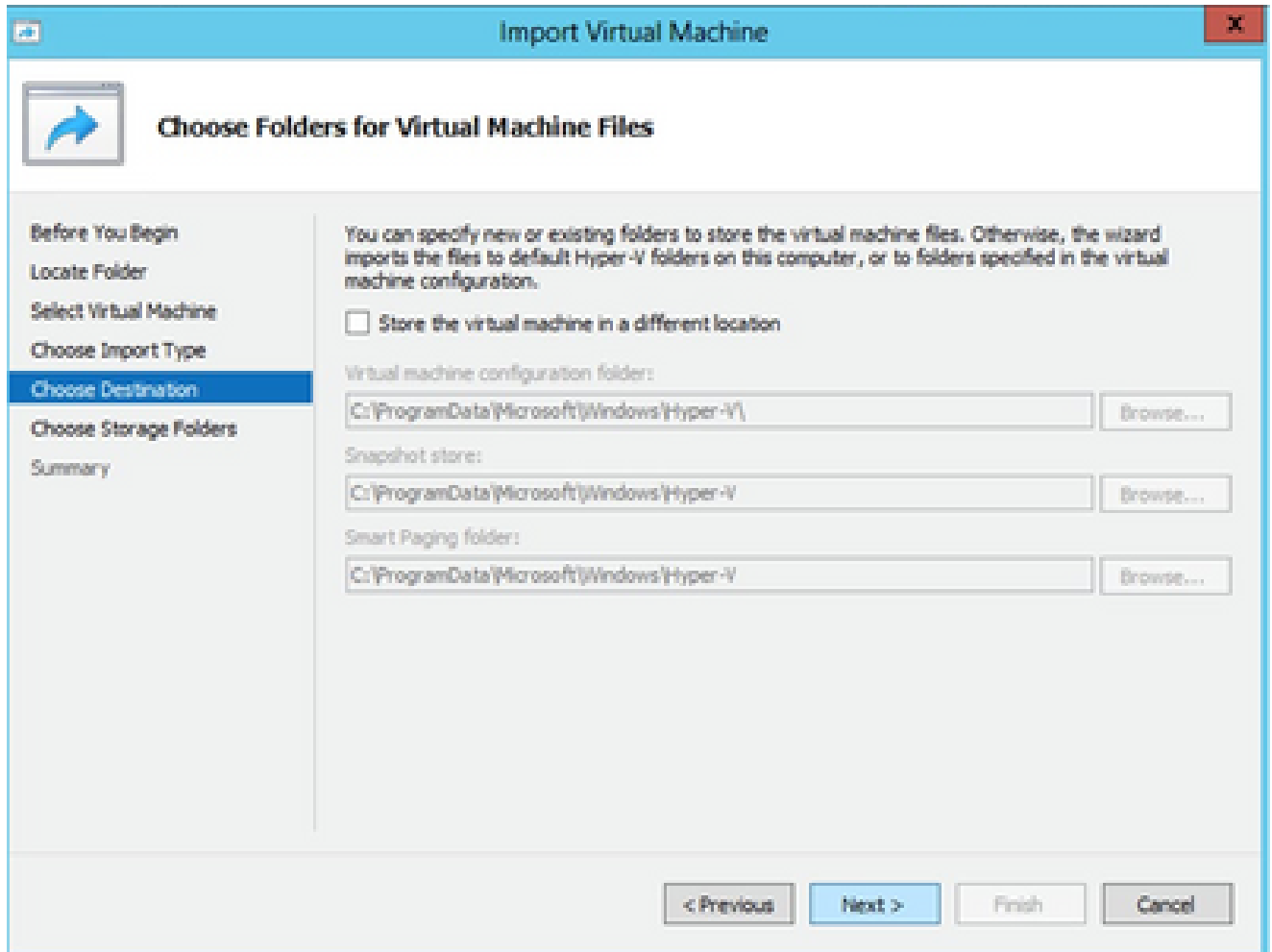
[VMの選択 ( Select VM ) ]

5. Copy the virtual machine (create a new unique ID)オプションボタンを選択し、Nextをクリックします。



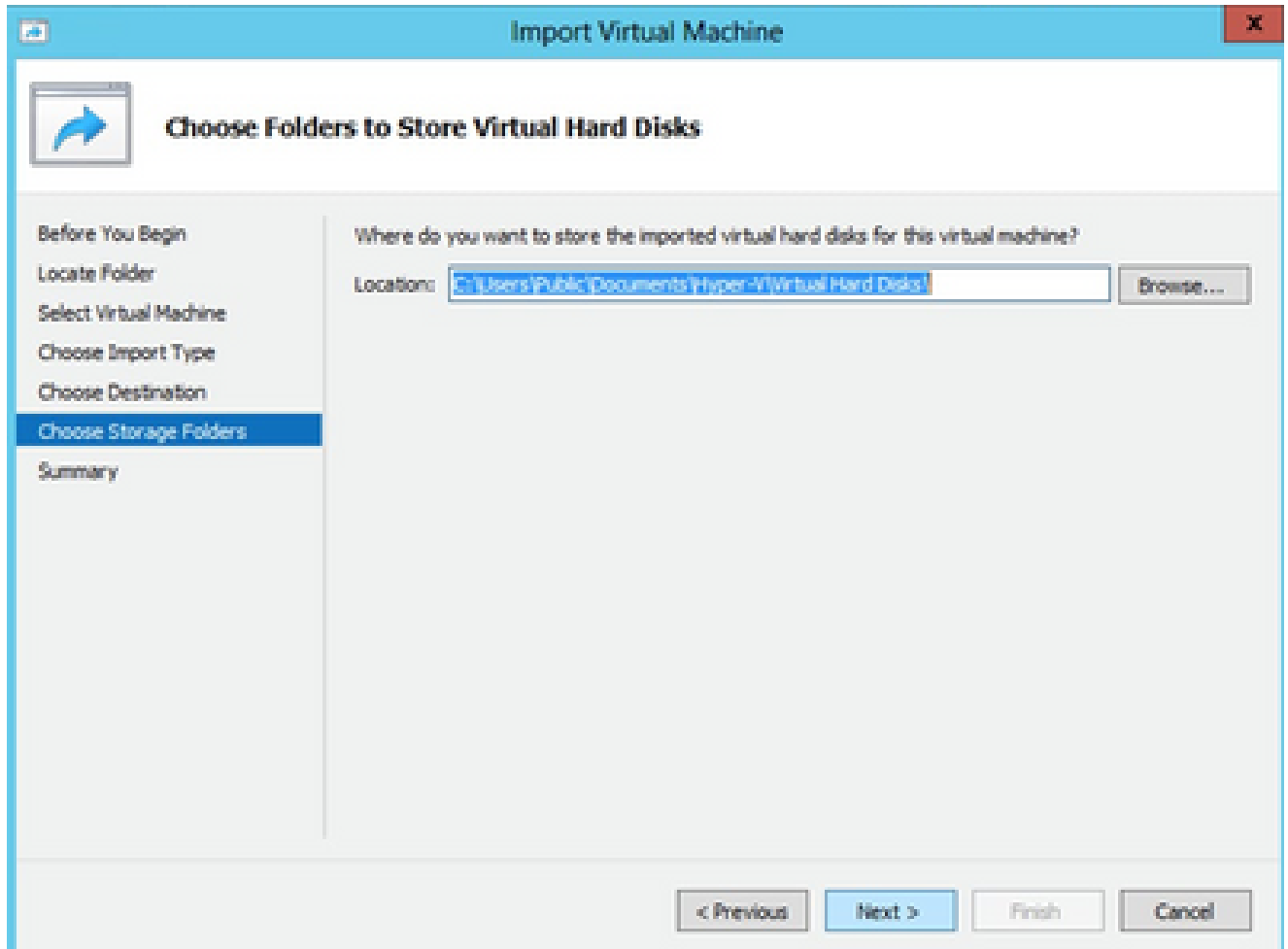
インポート タイプ

6. VM ファイルのフォルダを参照して選択します。デフォルトのパスを使用することを推奨します。
7. [Next] をクリックします。



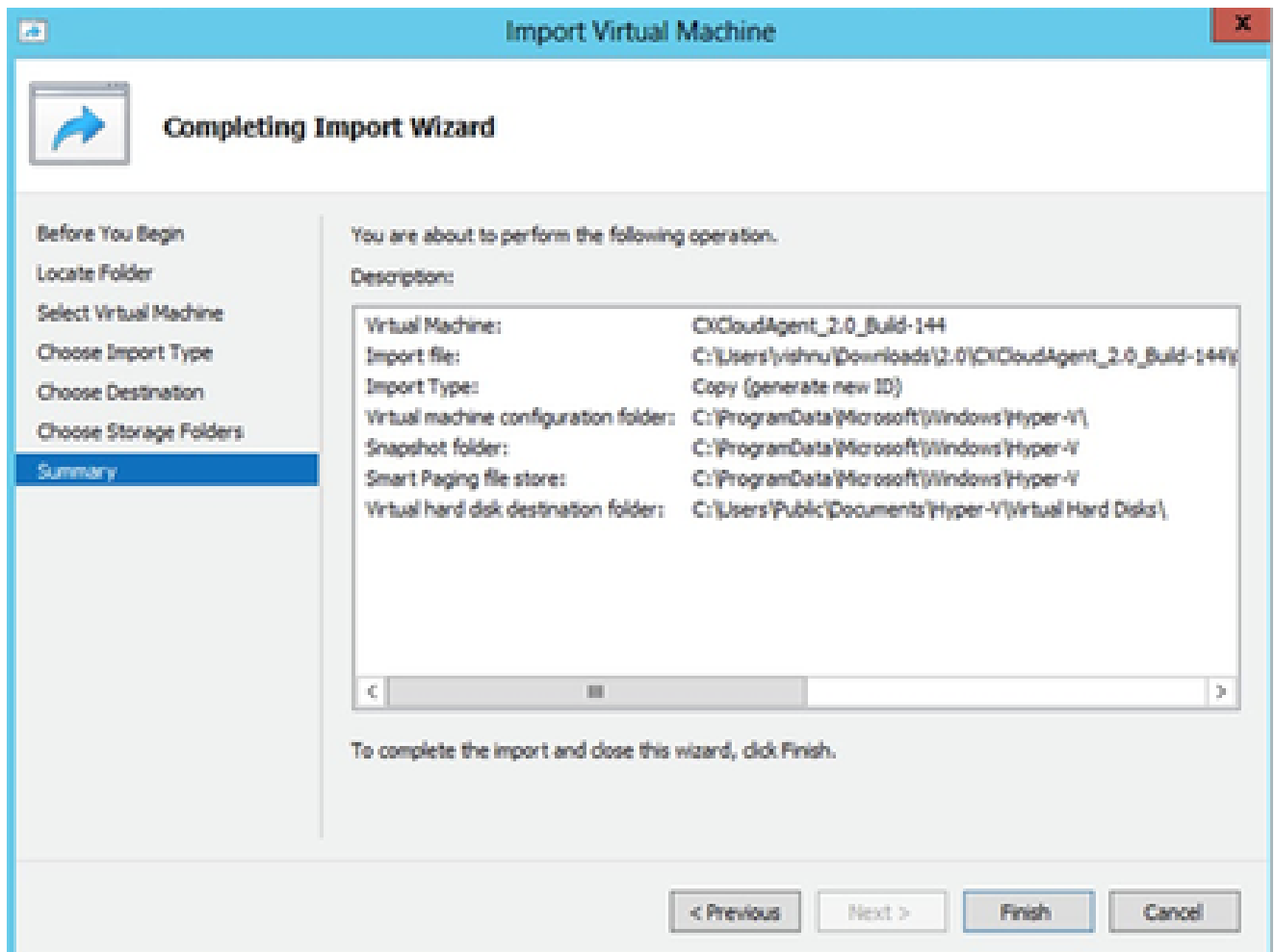
仮想マシンファイルのフォルダの選択

8. VM ディスクを保存するフォルダを参照して選択します。デフォルトパスを使用することをお勧めします。
9. [Next] をクリックします。



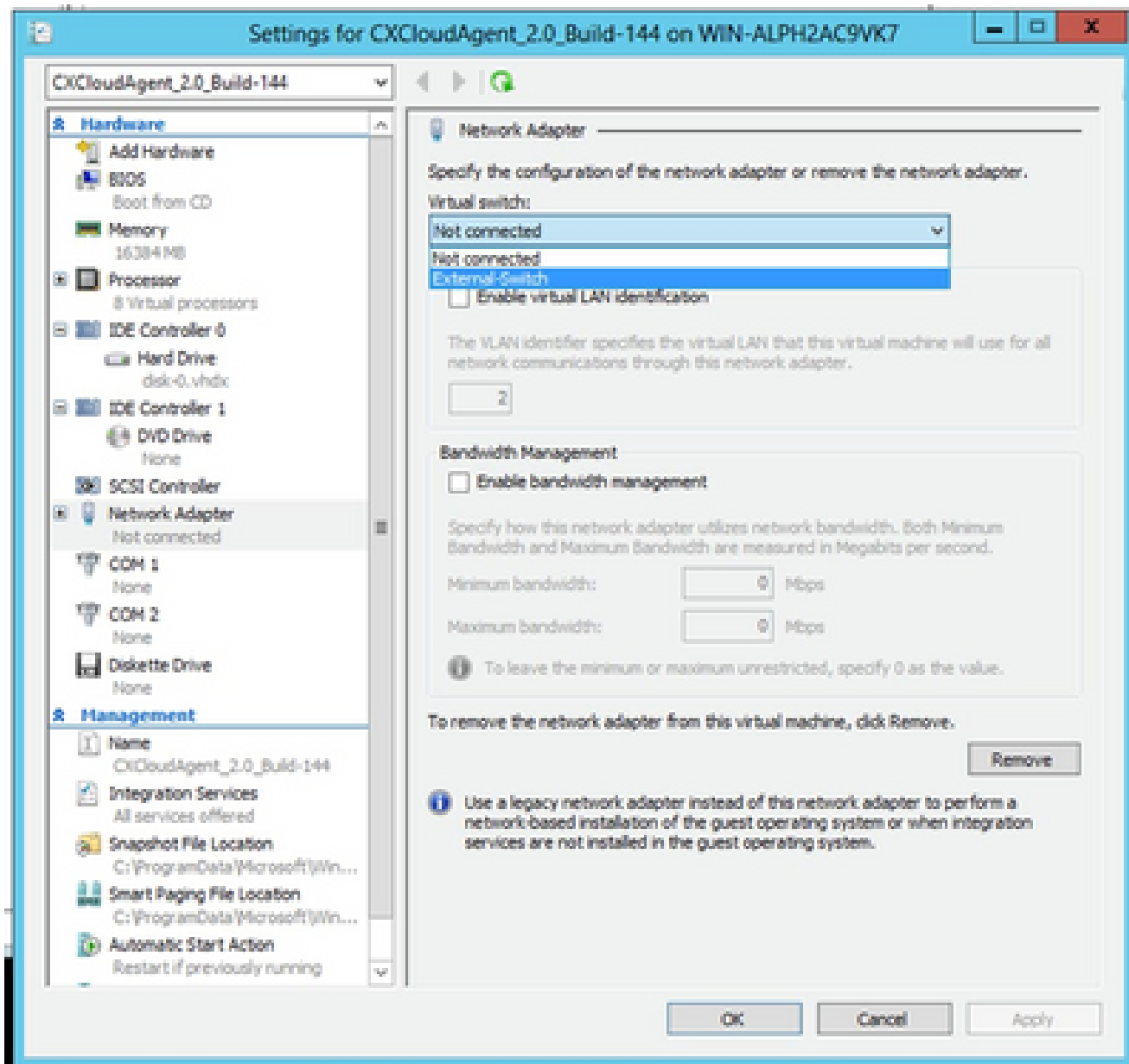
仮想ハードディスクを格納するフォルダ

10. VMサマリーが表示されます。すべての入力を確認し、Finishをクリックします。



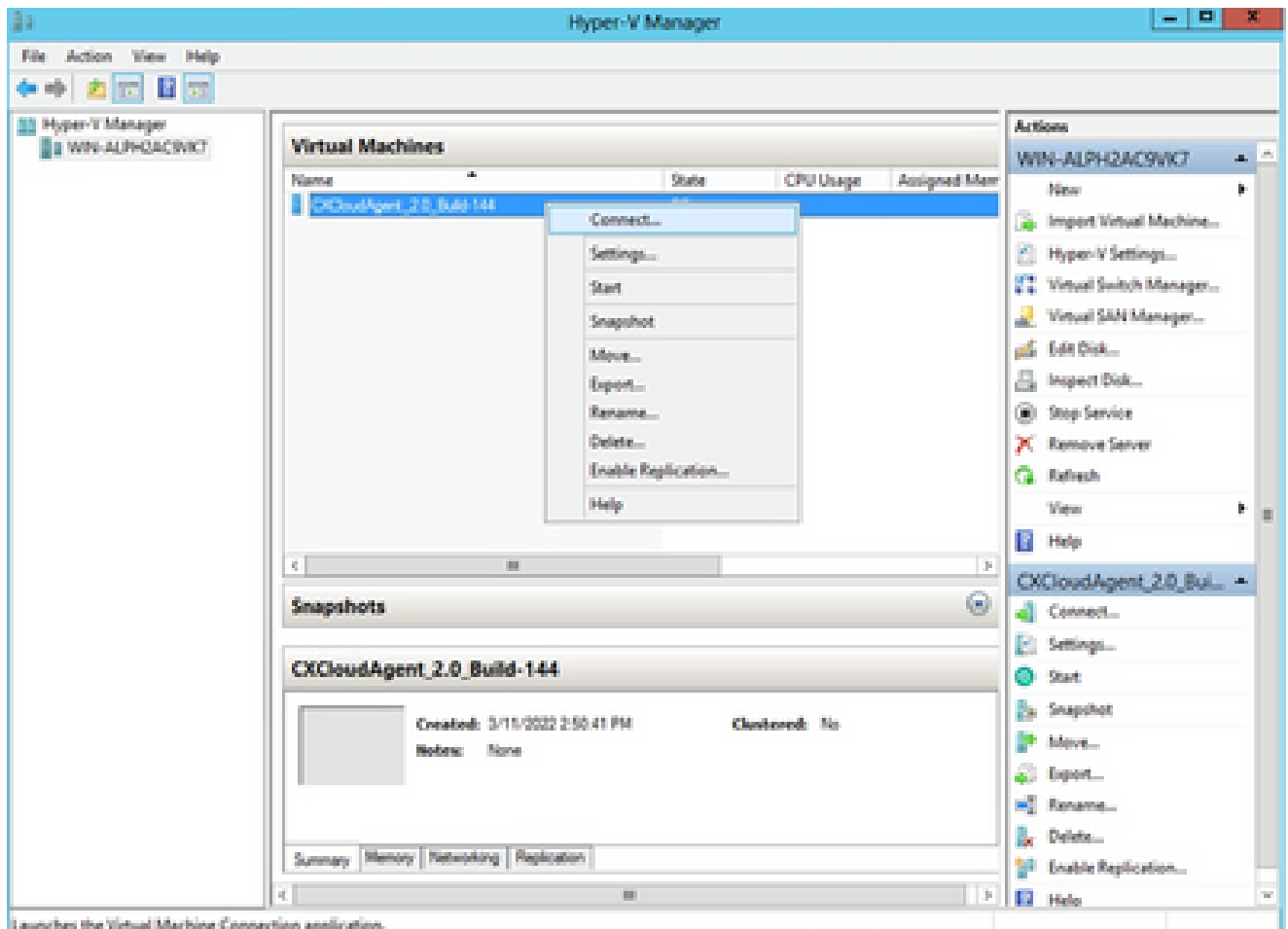
要約

11. インポートが正常に完了すると、新しいVMがHyper-Vに作成されます。VM設定を開きます。
12. 左側のペインでネットワークアダプタを選択し、使用可能な [仮想スイッチ (Virtual Switch)] をドロップダウンから選択します。



仮想スイッチ

13. Connectを選択してVMを起動します。



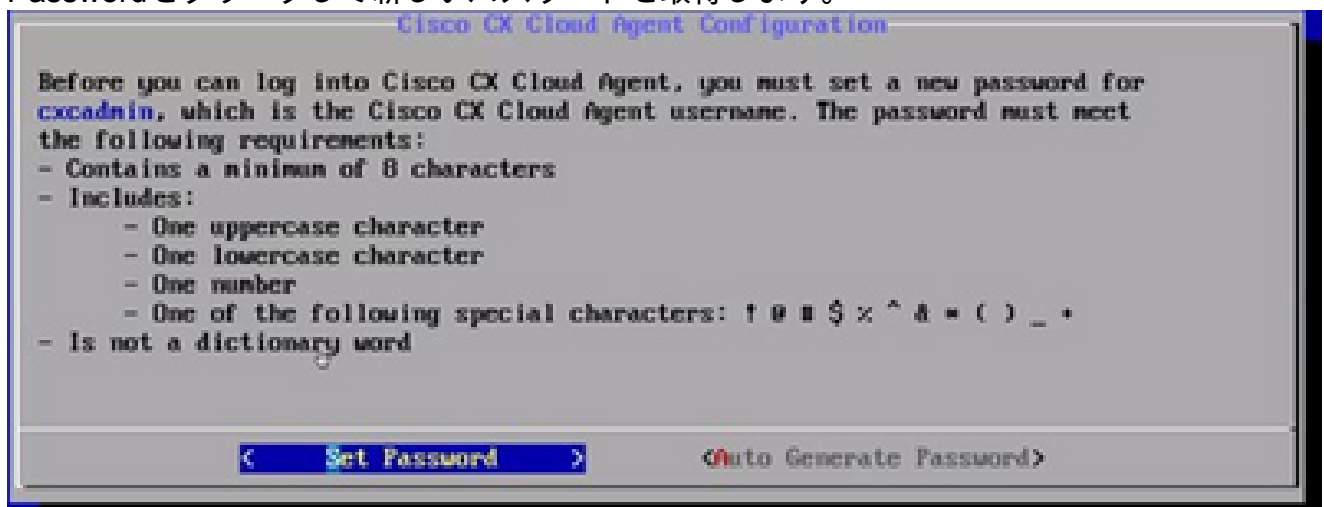
Launches the Virtual Machine Connection application.

VM の起動

14. [Network Configuration](#)に移動して、次の手順に進みます。

## ネットワーク設定

1. Set Passwordをクリックしてcxcadminの新しいパスワードを追加するか、Auto Generate Passwordをクリックして新しいパスワードを取得します。

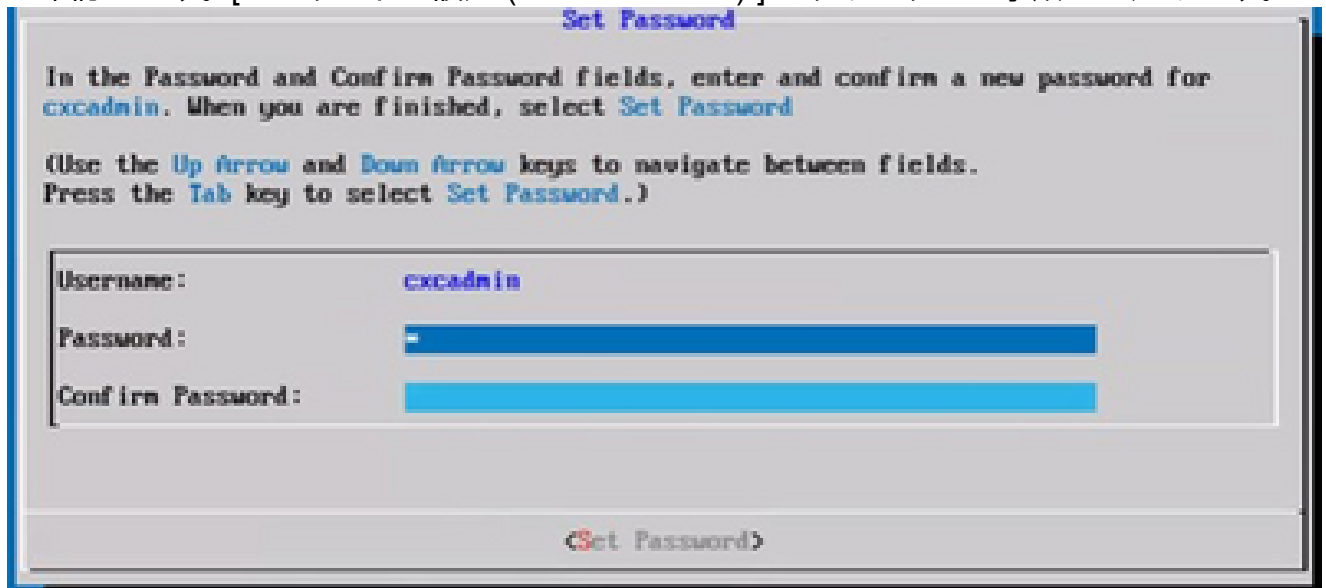


パスワードの設定

2. [パスワードの設定 ( Set Password ) ] を選択した場合は、cxcadmin のパスワードを入力し



て確認します。[パスワードの設定 ( Set Password ) ] をクリックして手順 3 に進みます。



新しいパスワード

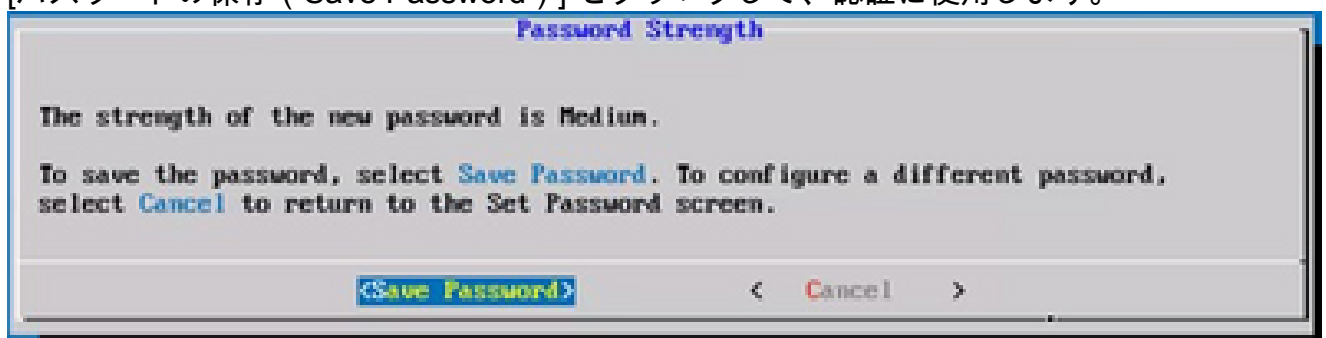
または

Auto Generate Passwordを選択した場合は、生成されたパスワードをコピーし、後で使用するために保存します。[パスワードの保存 ( Save Password ) ] をクリックして手順 4 に進みます。



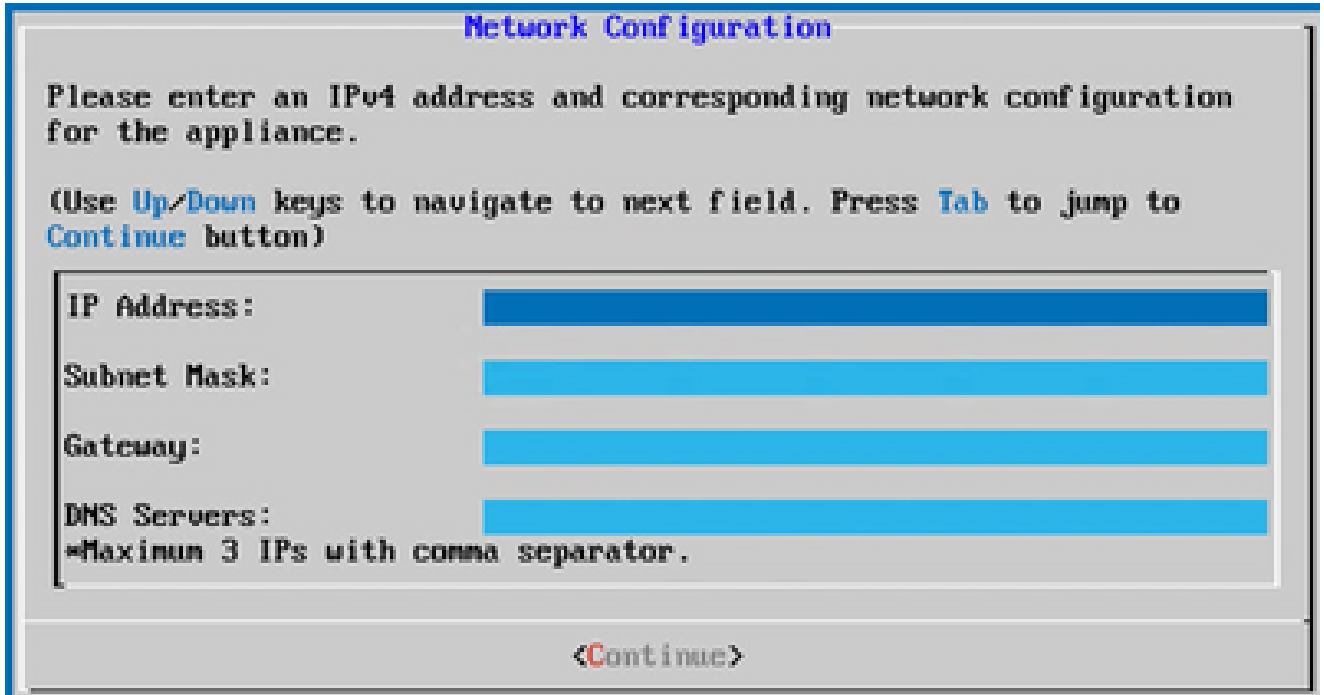
自動生成パスワード

3. [パスワードの保存 ( Save Password ) ] をクリックして、認証に使用します。



パスワードの保存 ( Save Password )

4. IP Address、Subnet Mask、Gateway、およびDNS Serverを入力し、Continueをクリックします。



The screenshot shows a terminal window titled "Network Configuration". The text inside reads: "Please enter an IPv4 address and corresponding network configuration for the appliance." followed by "(Use Up/Down keys to navigate to next field. Press Tab to jump to Continue button)". Below this are four input fields: "IP Address:", "Subnet Mask:", "Gateway:", and "DNS Servers:". The "DNS Servers:" field has a note below it: "Maximum 3 IPs with comma separator." At the bottom of the window is a button labeled "<Continue>".

ネットワーク設定

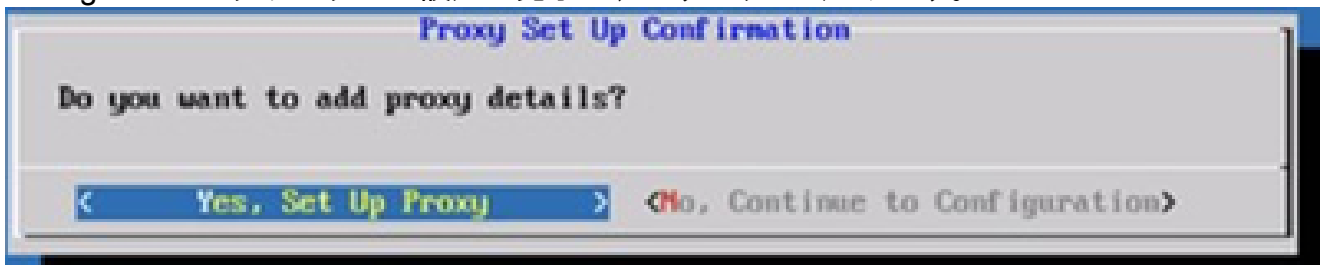
5. エントリを確認し、[はい、続行する ( Yes, Continue ) ] をクリックします。



The screenshot shows a terminal window titled "Confirmation". The text inside reads: "Are these entries correct?". Below this are the labels for the fields: "IP Address:", "Subnet Mask:", "Gateway:", and "DNS:". At the bottom of the window are two buttons: "<Yes, Continue>" and "<No, Go Back >".

コンフィギュレーション

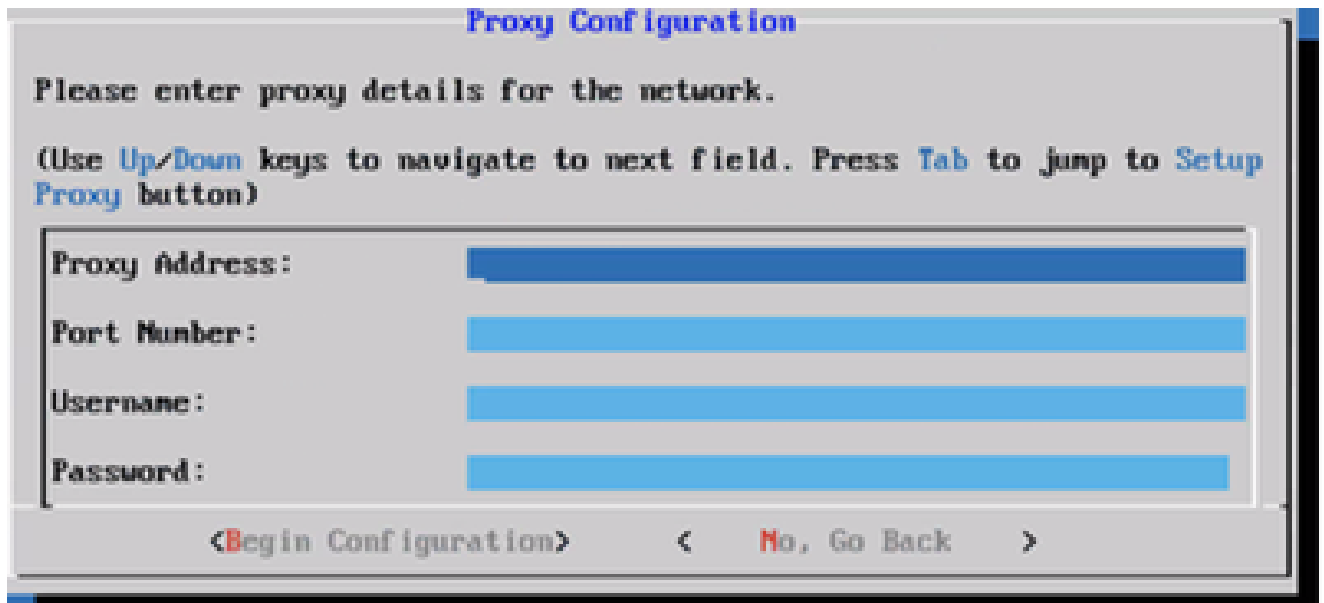
6. プロキシの詳細を設定するには、Yes, Set Up Proxyをクリックするか、No, Continue to Configurationをクリックして設定を完了し、ステップ8に進みます。



The screenshot shows a terminal window titled "Proxy Set Up Confirmation". The text inside reads: "Do you want to add proxy details?". At the bottom of the window are two buttons: "< Yes, Set Up Proxy >" and "<No, Continue to Configuration>".

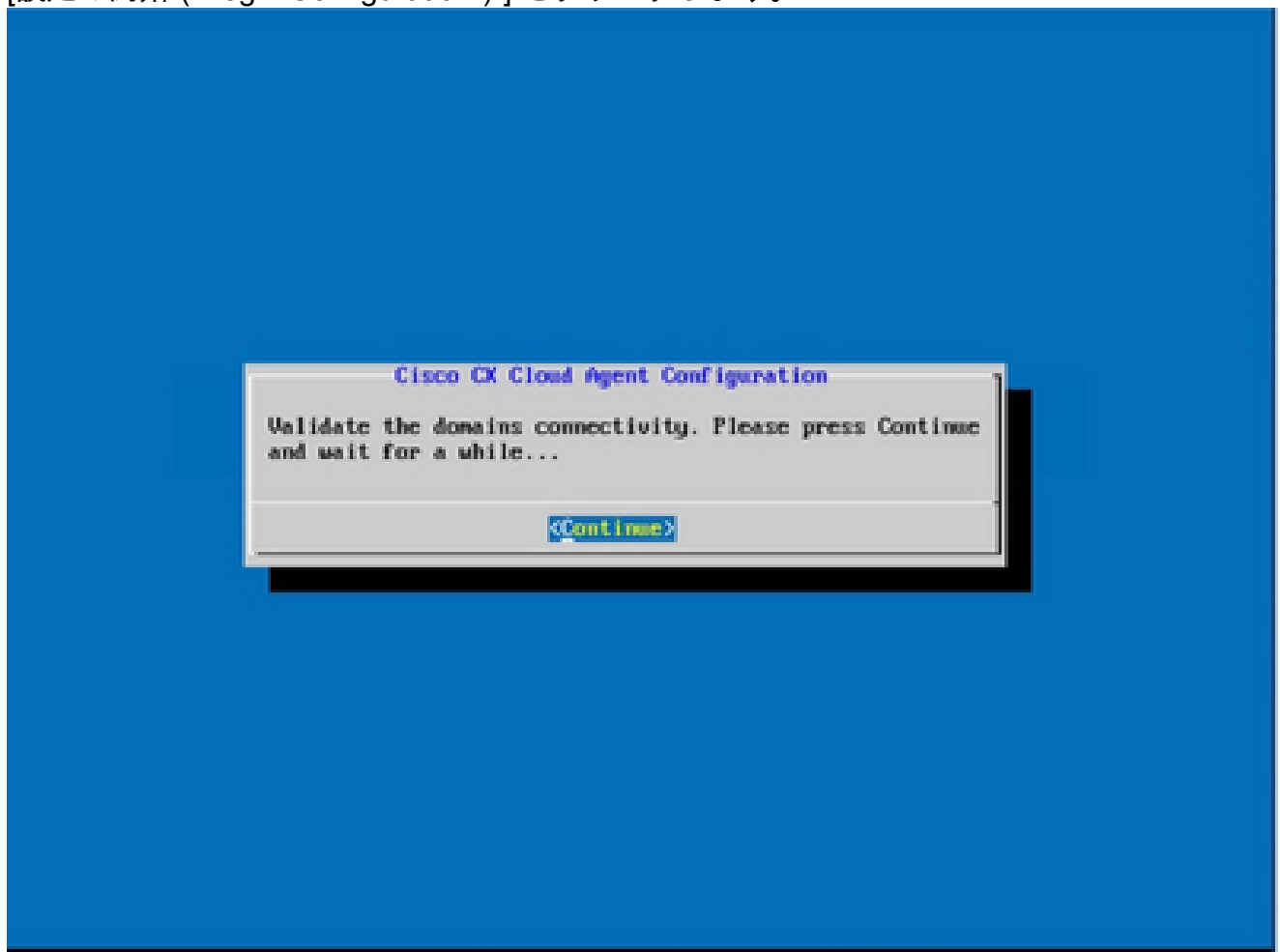
プロキシ設定

7. [プロキシアドレス ( Proxy Address ) ]、[ポート番号 ( Port Number ) ]、[ユーザー名 ( Username ) ]、[パスワード ( Password ) ] を入力します。



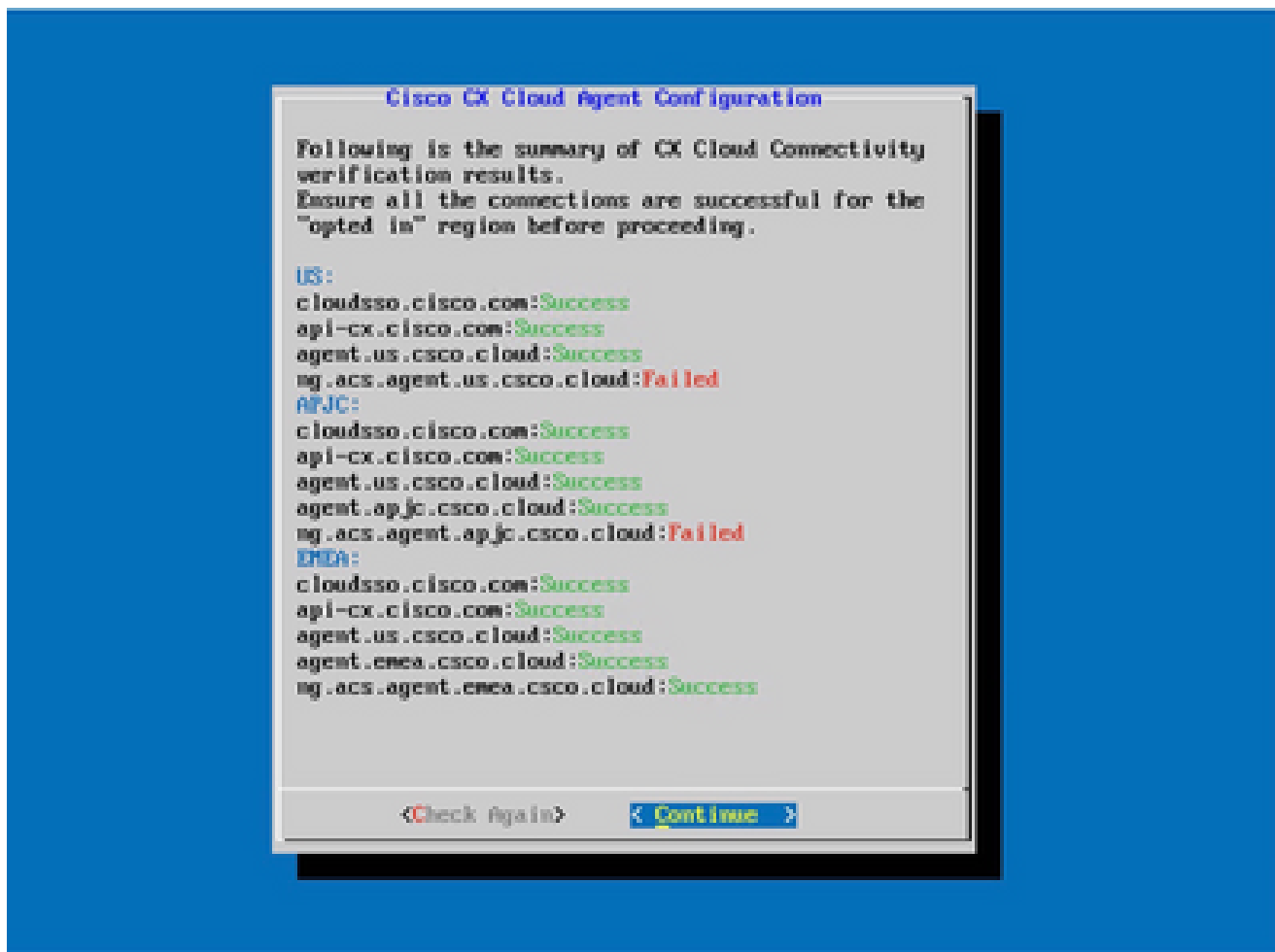
プロキシ設定

8. [設定の開始 ( Begin Configuration ) ] をクリックします。




Begin configuration

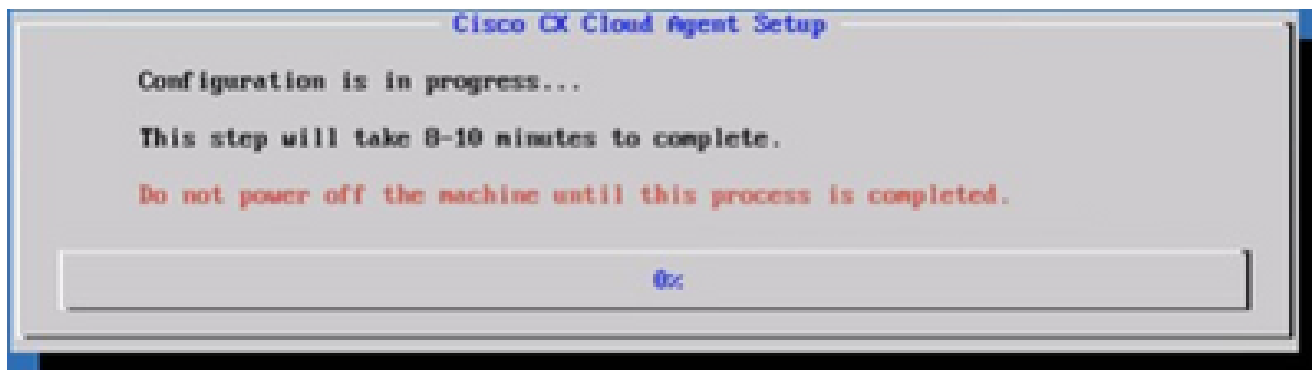
9. [Continue] をクリックします。



設定を続行

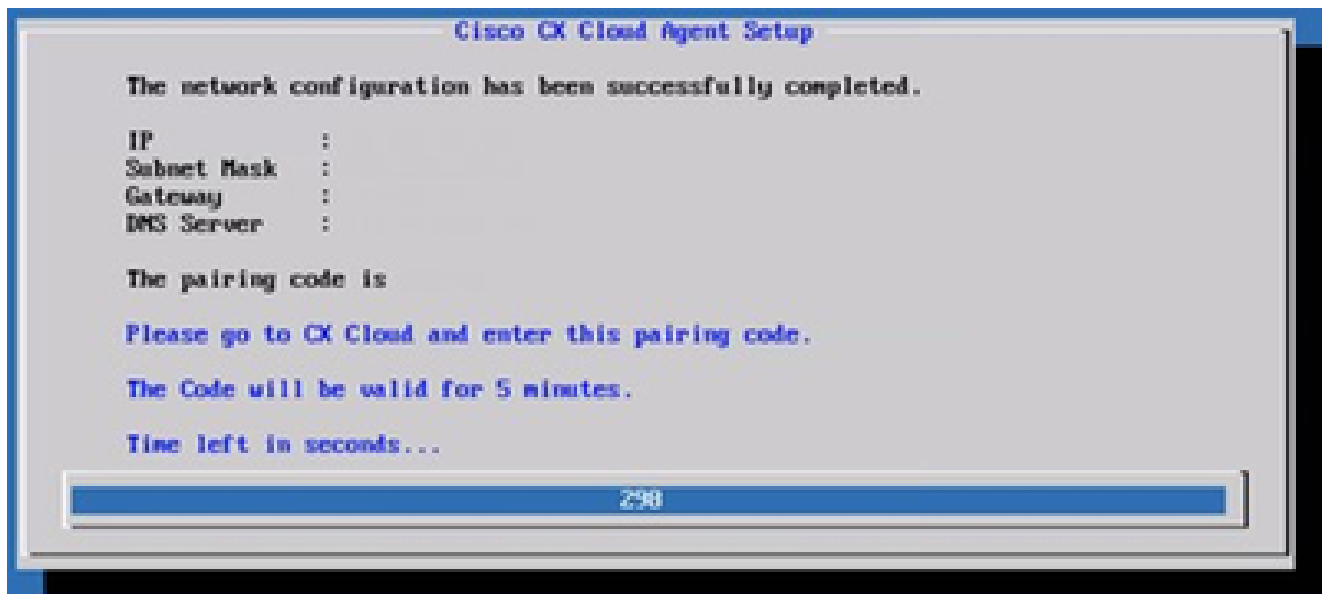
10. Continueをクリックして、ドメインに正常に到達するための設定を続行します。設定が完了するまでに数分かかる場合があります。

 注：ドメインに正常に到達できない場合、顧客はドメインが到達可能であることを確認するためにファイアウォールを変更して、ドメインの到達可能性を修正する必要があります。ドメインの到達可能性の問題を解決したら、Check Againをクリックします。



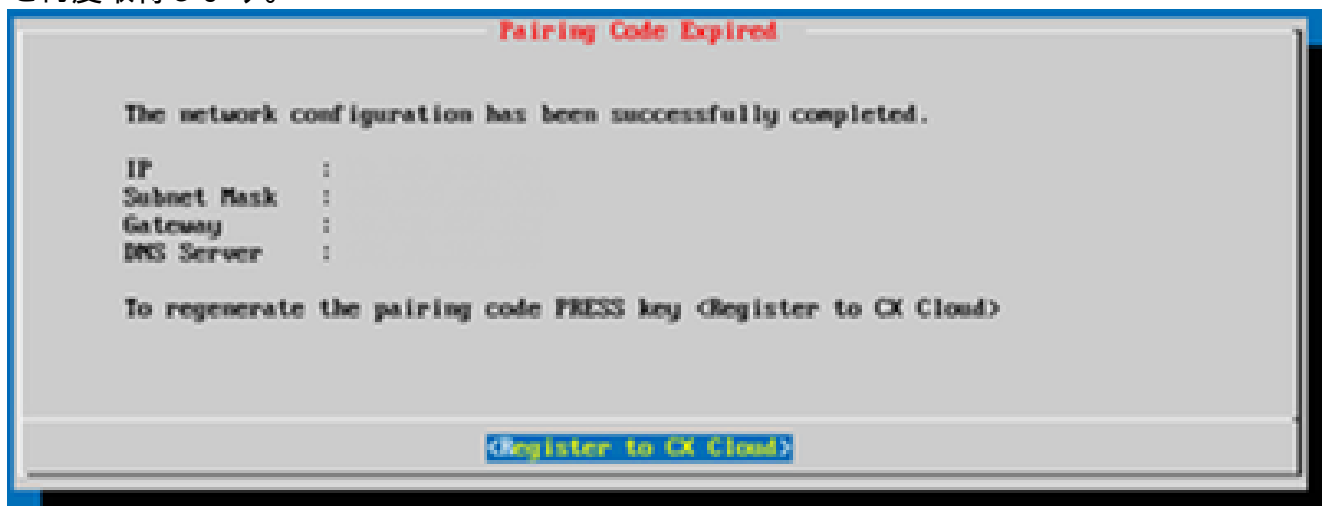
設定が進行中です

11. [ペアリングコード ( Pairing Code ) ] をコピーして CX Cloud に戻り、設定を続行します。



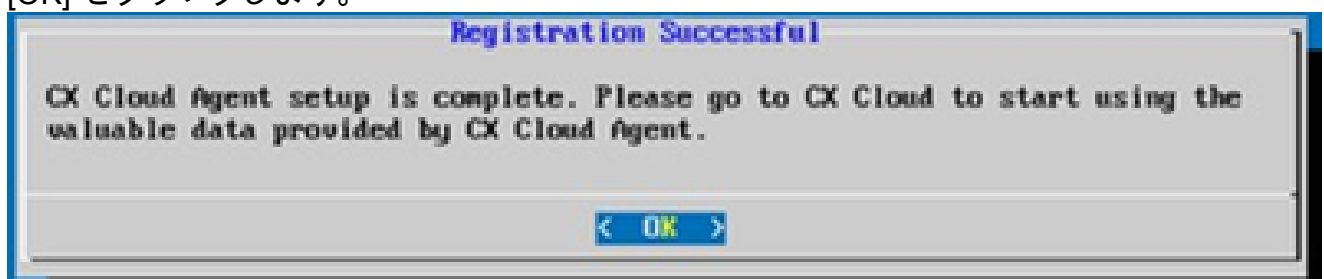
ペアリングコード

12. ペアリングコードの有効期限が切れた場合は、Register to CX Cloudをクリックしてコードを再度取得します。



コードが期限切れです

13. [OK] をクリックします。



登録に成功しました

CLIを使用してペアコードを生成する別の方法

ユーザは、CLIオプションを使用してペアリングコードを生成することもできます。

CLIを使用してペアリングコードを生成するには、次の手順に従います。

1. cxcadminユーザクレデンシャルを使用して、SSH経由でCloud Agentにログインします。
2. cxcli agent generatePairingCode コマンドを使用してペアリングコードを生成します。

```
cxcadmin@cxcloudagent:~$ cxcli agent generatePairingCode

Pairing Code : xJ7I8P
Expires in: 5 minutes
Please use the Pairing Code in the CX Cloud to proceed with CX Cloud Agent registration.

cxcadmin@cxcloudagent:~$
```

ペアリングコード CLI の生成

3. [ペアリングコード ( Pairing Code ) ] をコピーして CX Cloud に戻り、設定を続行します。

## SyslogをCX Cloud Agentに転送するためのCisco DNA Centerの設定

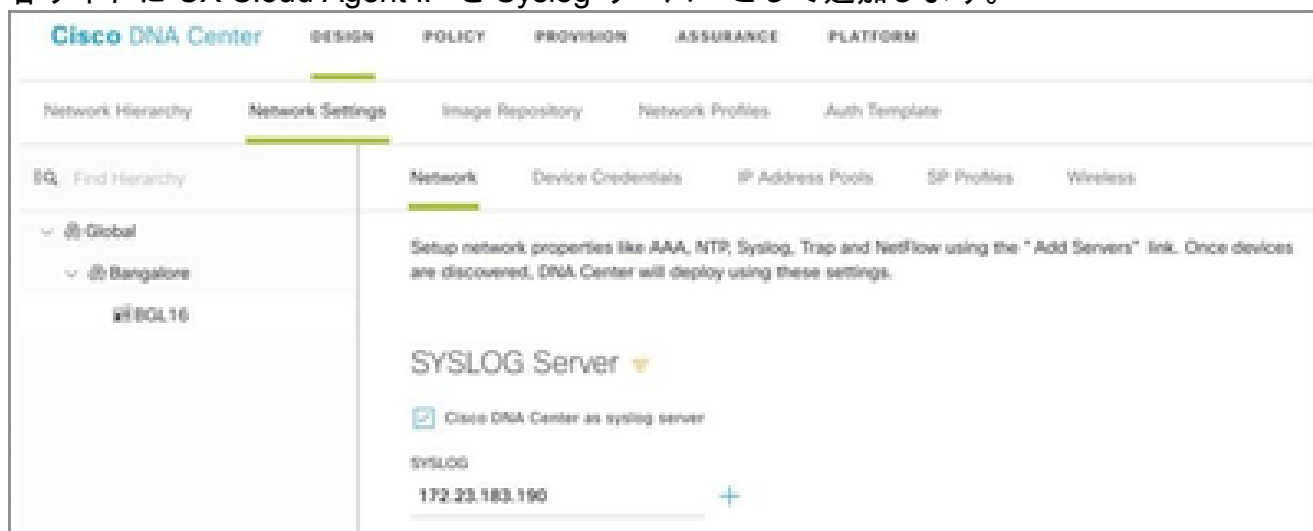
### 前提条件

サポートされるCisco DNA Centerのバージョンは、2.1.2.0 ~ 2.2.3.5、2.3.3.4 ~ 2.3.3.6、2.3.5.0、およびCisco DNA Center仮想アプライアンスです

### Syslog転送設定の設定


Cisco DNA CenterでCX Cloud AgentへのSyslog転送を設定するには、次の手順を実行します。

1. Cisco DNA Center を起動します。
2. [設計 ( Design ) ] > [ネットワーク設定 ( Network Settings ) ] > [ネットワーク ( Network ) ] に移動します。
3. 各サイトに CX Cloud Agent IP を Syslog サーバーとして追加します。



Syslog サーバー

---


 注：  
設定が完了すると、そのサイトに関連付けられたすべてのデバイスが、レベルcriticalのsyslogをCX Cloud Agentに送信するように設定されます。デバイスからCX Cloud Agentへのsyslog転送を有効にするには、デバイスをサイトに関連付ける必要があります。syslogサーバの設定が更新されると、そのサイトに関連付けられたすべてのデバイスがデフォルトの重大レベルに自動的に設定されます。

---

## SyslogをCX Cloud Agentに転送するための他のアセットの設定

CX CloudのFault Management機能を使用するには、CX Cloud Agentにsyslogメッセージを送信するようにデバイスを設定する必要があります。

---


 注:syslogを転送するように他のアセットを設定できるのは、Campus Success Trackレベル2のデバイスだけです。

---

### 転送機能を備えた既存のSyslogサーバ

syslogサーバソフトウェアの設定手順を実行し、CX CloudエージェントのIPアドレスを新しい宛先として追加します。

---

 注：syslogを転送するときは、元のsyslogメッセージの送信元IPアドレスが保持されていることを確認してください。

---

### 転送機能のない、またはsyslogサーバのない既存のsyslogサーバ

syslogをCX Cloud AgentのIPアドレスに直接送信するように各デバイスを設定します。特定の設定手順については、次のドキュメントを参照してください。

[Cisco IOS® XEコンフィギュレーションガイド](#)

[AireOSワイヤレスコントローラコンフィギュレーションガイド](#)

### 情報レベルのsyslog設定の有効化

Syslog情報レベルを表示するには、次の手順を実行します。

1. Tools> Telemetryの順に移動します。



## TOOLS

**Discovery**

**Inventory**

**Topology**

**Image Repository**

**Command Runner**

**License Manager**

**Template Editor**

**Telemetry**

**Data and Reports**



[ツール]メニュー

2. サイトビューを選択して展開し、サイト階層からサイトを選択します。



サイト ビュー

3. 必要なサイトを選択し、Device nameチェックボックスを使用してすべてのデバイスを選択します。
4. ActionsドロップダウンからOptimal Visibilityを選択します。



[アクション ( Actions ) ]

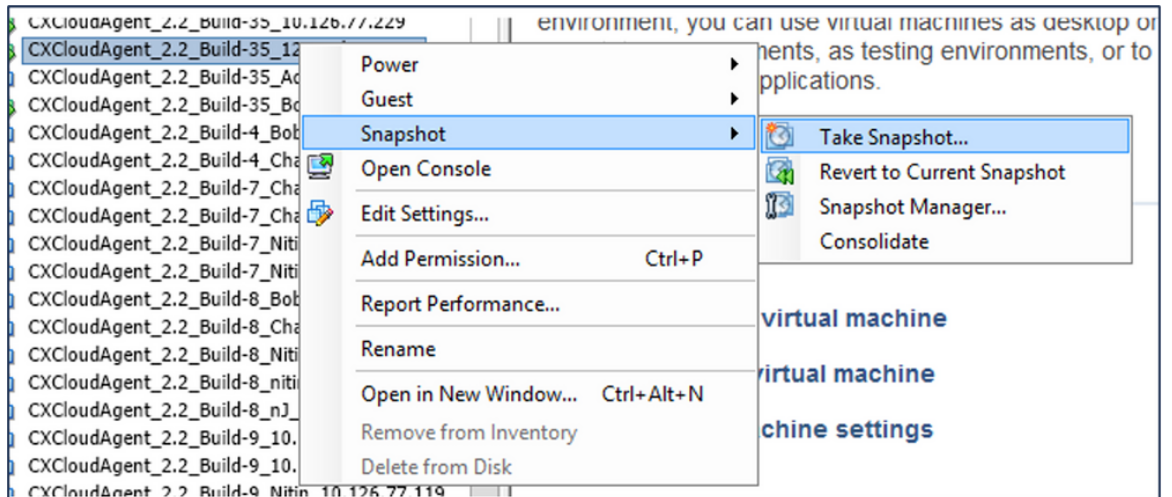
## CX Cloud VMのバックアップと復元

スナップショット機能を使用して、CX Cloud Agent VMの状態とデータを特定の時点で保持することを推奨します。この機能により、CX Cloud VMをスナップショットが作成された特定の時刻に簡単に復元できます。

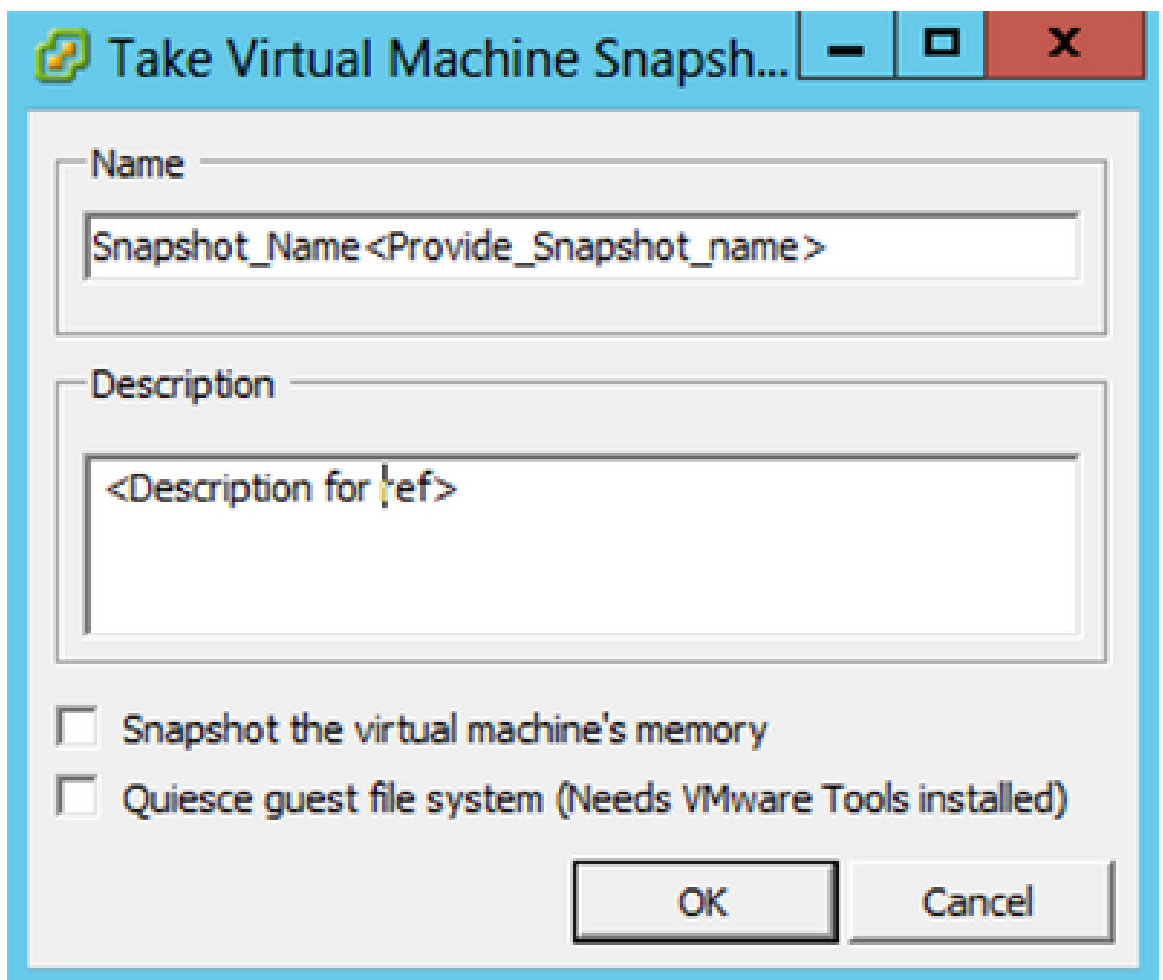
### バックアップ

CX Cloud VMをバックアップするには、次の手順を実行します。

1. VMを右クリックし、Snapshot > Take Snapshotの順に選択します。Take Virtual Machine Snapshotウィンドウが開きます。




[VMの選択 ( Select VM ) ]

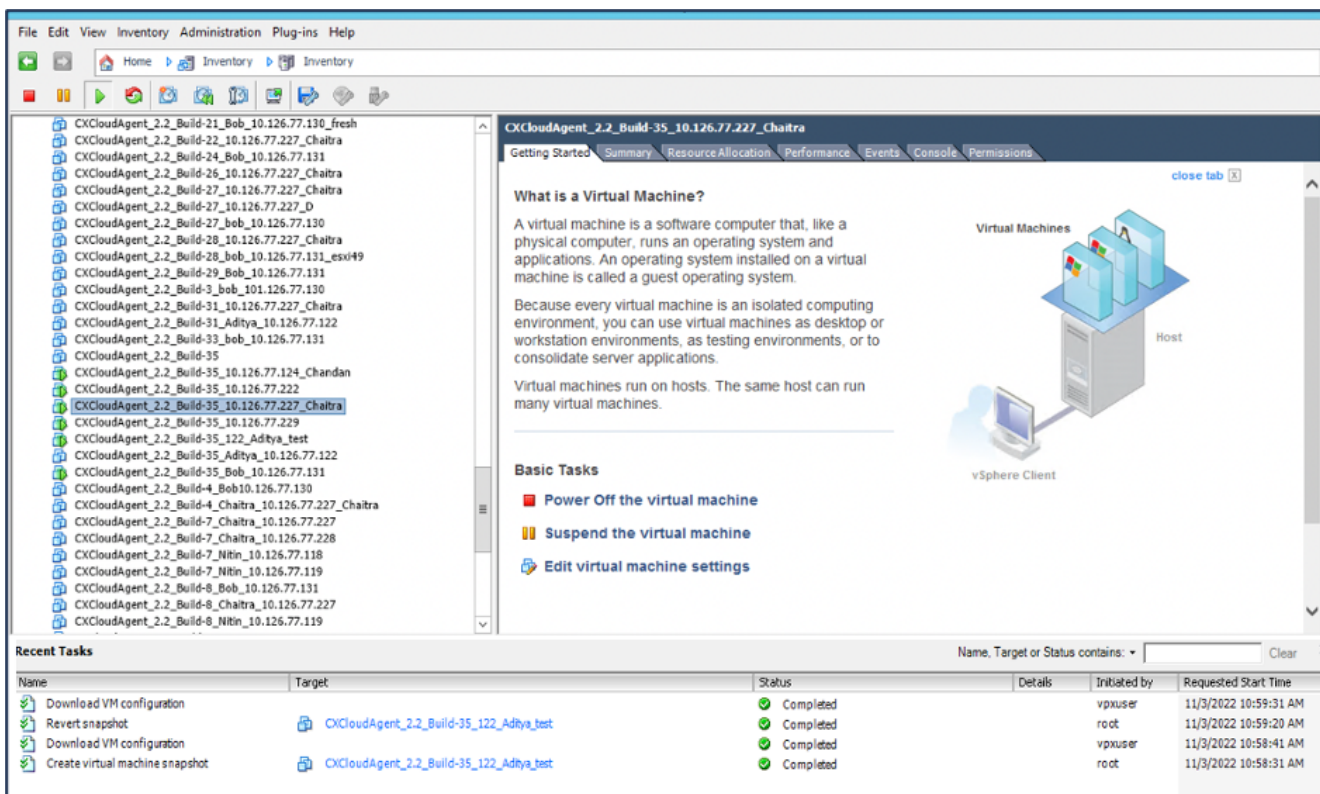


仮想マシンのスナップショットの作成

2. NameとDescriptionを入力します。

 注: [仮想マシンのメモリのスナップショットを作成する]チェックボックスがオフになっていることを確認します。

3. OKをクリックします。[最近のタスク]の一覧で、[仮想マシンスナップショットの作成]ステータスが[完了]と表示されます。

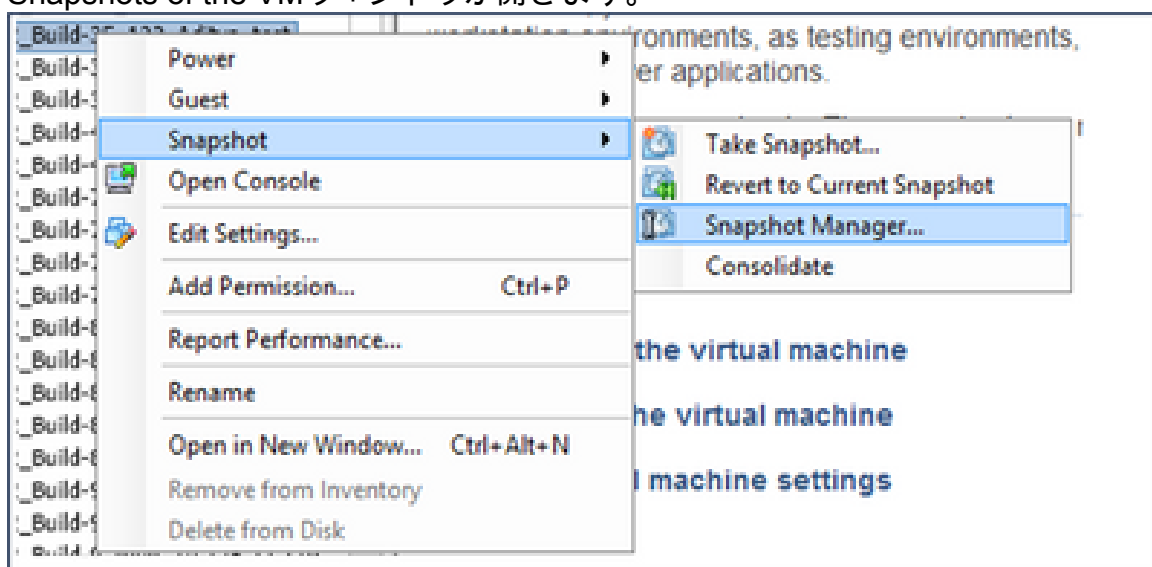


最近のタスク

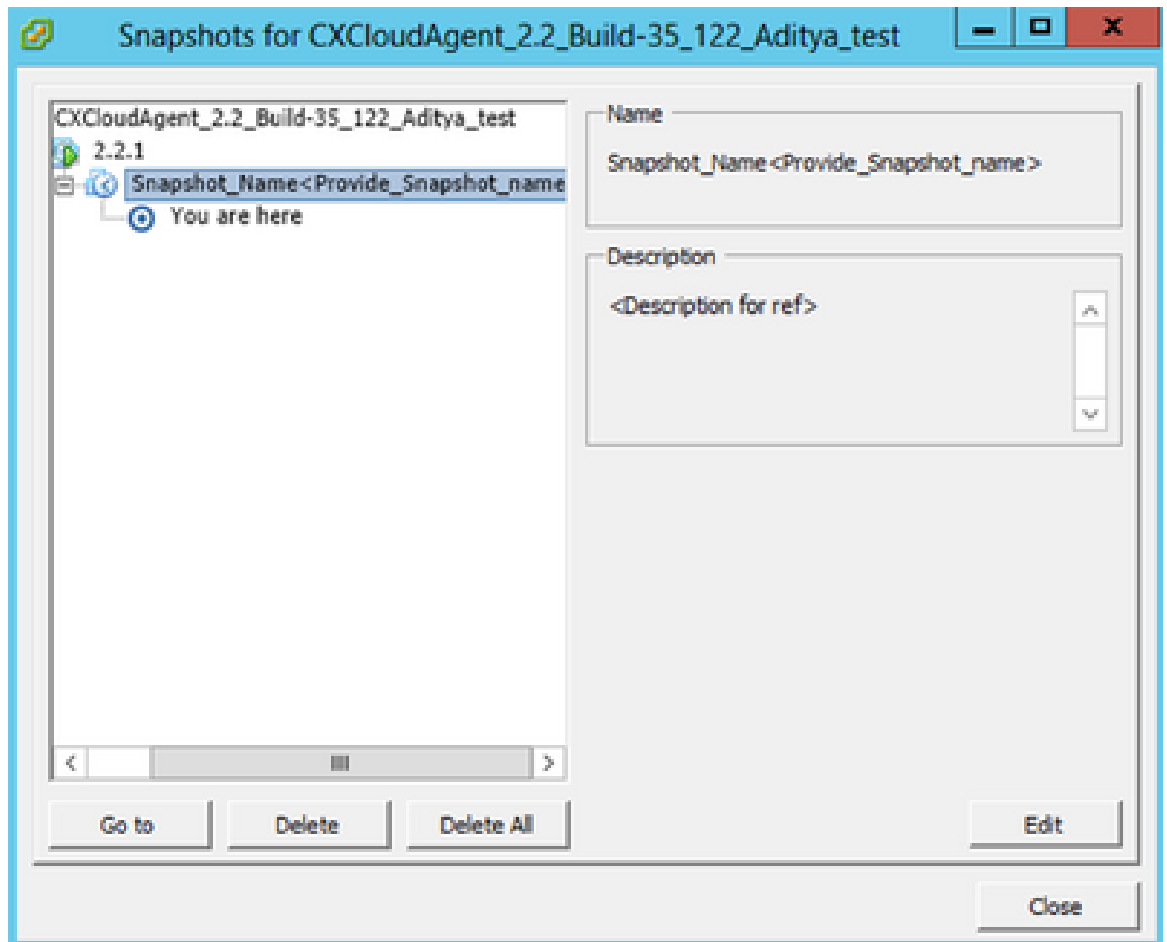
## 復元

CX Cloud VMを復元するには、次の手順を実行します。

1. VMを右クリックし、Snapshot > Snapshot Managerの順に選択します。Snapshots of the VMウィンドウが開きます。

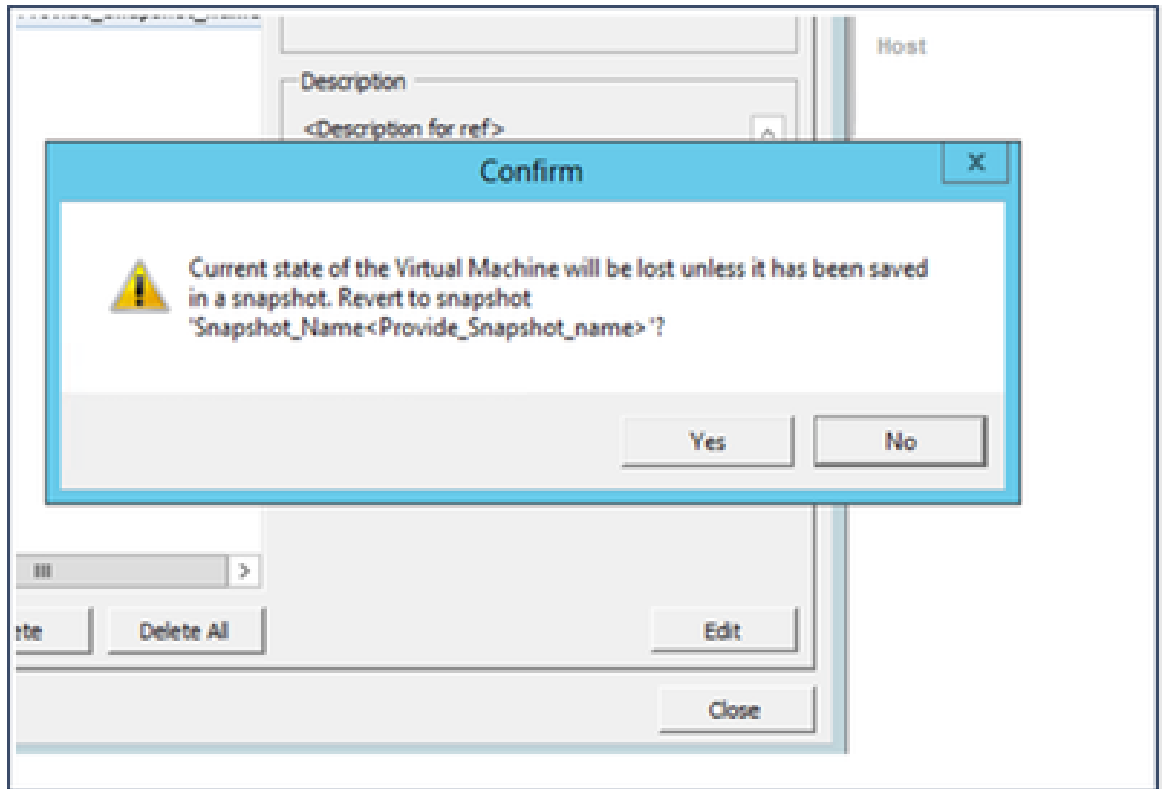


Select VMウィンドウ



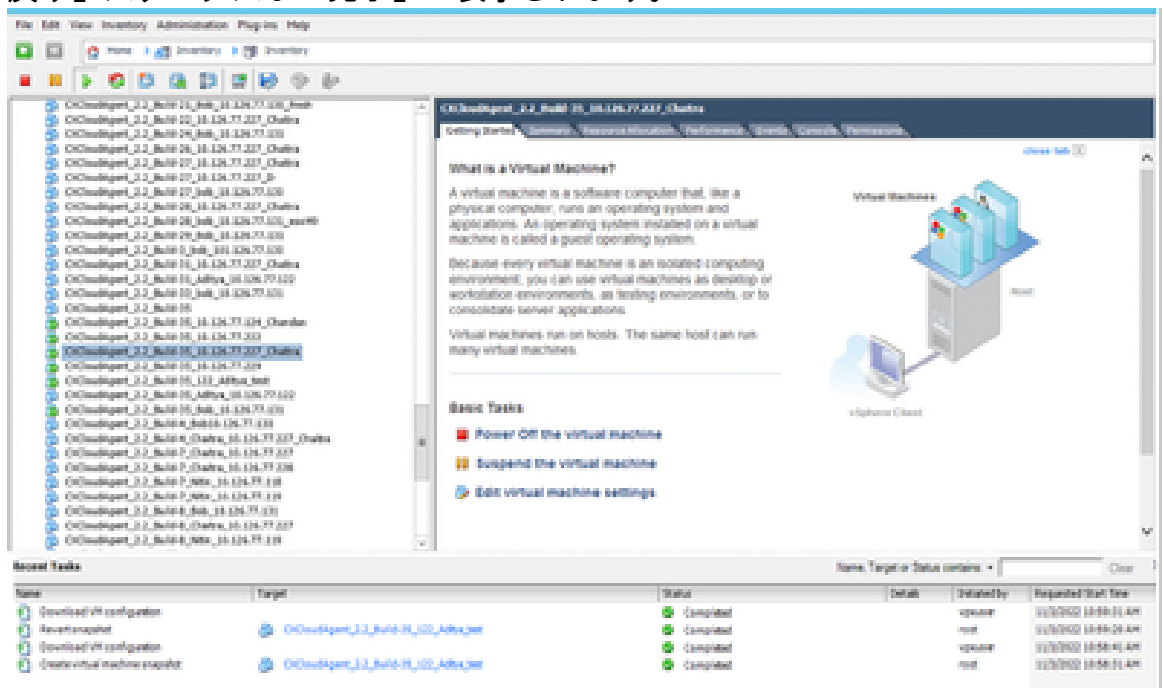
「スナップショット」ウィンドウ

2. Go toをクリックします。Confirmウィンドウが開きます。



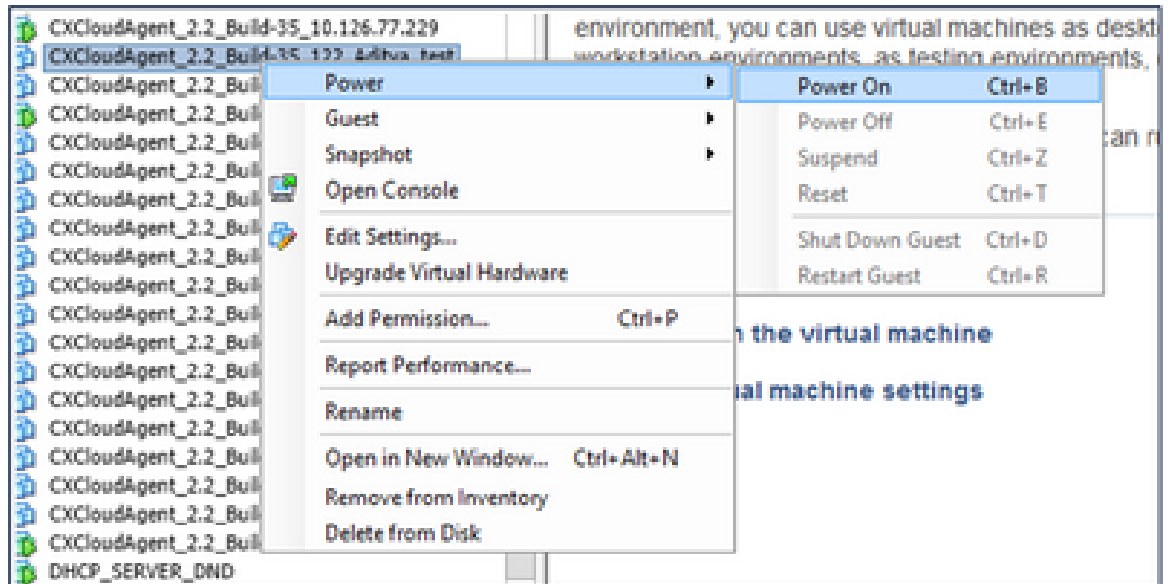
確認ウィンドウ

3. [Yes] をクリックします。「最近のタスク」リストに「スナップショットを元に戻す」ステータスが「完了」と表示されます。



最近のタスク

4. VMを右クリックし、Power > Power Onの順に選択してVMの電源をオンにします。



## セキュリティ

CX Cloud Agentは、エンドツーエンドセキュリティをお客様に保証します。CX CloudとCX Cloud Agent間の接続はTLSで保護されます。Cloud AgentのデフォルトのSSHユーザは、基本操作のみを実行するように制限されています。

### 物理セキュリティ

CX Cloud Agent OVAイメージを、セキュリティ保護されたVMwareサーバ会社に導入します。OVAは、シスコソフトウェアダウンロードセンターを通じて安全に共有されます。ブートローダー（シングルユーザーモード）には、一意のパスワードがランダムに設定されます。このブートローダ（シングルユーザーモード）パスワードを設定するには、ユーザはこの[FAQ](#)を参照する必要があります。

### アカウントのセキュリティ

導入時に、cxcadminユーザアカウントが作成されます。初期設定時にパスワードを設定する必要があります。cxcadminユーザ/クレデンシャルは、CX Cloud Agent APIの両方にアクセスし、SSH経由でアプライアンスに接続するために使用されます。

cxcadminユーザは、最小限の権限でアクセスが制限されています。cxcadminパスワードはセキュリティ・ポリシーに従い、90日間の期限切れで一方向ハッシュされます。cxcadminユーザは、remoteaccountというユーティリティを使用してcxcrootユーザを作成できます。cxcrootユーザはroot権限を取得できます。

### ネットワーク セキュリティ

CX Cloud Agent VMには、cxcadminユーザクレデンシャルを使用してSSHを使用してアクセスできます。着信ポートは22（SSH）、514（Syslog）に制限されます。

[Authentication]

パスワードベースの認証：アプライアンスは、単一のユーザ(cxcadmin)を管理します。このユーザは、このユーザを使用してCX Cloud Agentの認証と通信を実行できます。

- ssh を使用したアプライアンスでのルート権限アクション。

cxcadminユーザは、remoteaccountというユーティリティを使用してcxcroutユーザを作成できます。このユーティリティは、SWIMポータル([DECRYPT Request Form](#))からのみ復号できる、RSA/ECB/PKCS1v1\_5暗号化パスワードを表示します。このポータルへのアクセス権を持つのは、承認されたユーザーのみです。cxcroutユーザーは、この復号化されたパスワードを使用してルート権限を取得できます。パスフレーズは2日間だけ有効です。cxcadminユーザは、パスワードの有効期限が切れた後にアカウントを再作成し、SWIMポータルからパスワードを取得する必要があります。

## 強化

CX Cloud Agentアプライアンスは、Center of Internet Securityの強化標準に準拠しています。

## データセキュリティ

CX Cloud Agent アプライアンスには、お客様の個人情報は保存されません。デバイスクレデンシャルアプリケーション (ポッドの1つとして実行) は、暗号化されたサーバクレデンシャルをセキュアなデータベース内に保存します。収集されたデータは、処理時以外は一時的にアプライアンス内に保存されません。テレメトリデータは、収集が完了するとすぐにCX Cloudにアップロードされ、アップロードが成功したことを確認した後、ローカルストレージからすぐに削除されます。

## データの伝送

登録パッケージには、lot Coreとのセキュアな接続を確立するために必要な、一意の[X.509](#)デバイス証明書とキーが含まれています。このエージェントを使用して、Transport Layer Security(TLS)v1.2上でメッセージキューテレメトリトランスポート(MQTT)を使用してセキュアな接続を確立します

## ログとモニタリング

ログには、個人識別情報(PII)データの形式は含まれません。監査ログには、CX Cloud Agentアプライアンスで実行されたセキュリティの影響を受けるすべてのアクションが記録されます。

## Ciscoテレメトリコマンド

CX Cloudは、「[シスコテレメトリコマンド](#)」に記載されているAPIおよびコマンドを使用して、資産テレメトリを取得します。このドキュメントでは、Cisco DNA Centerインベントリ、Diagnostic Bridge、Intersight、Compliance Insights、Faults、およびCX Cloud Agentによって収集されたその他すべてのテレメトリ源への適用可能性に基づいてコマンドを分類しています。

資産テレメトリ内の機密情報は、クラウドに送信される前にマスクされます。CX Cloud Agentは、CX Cloud Agentにテレメトリを直接送信するすべての収集アセットの機密データをマスクしま

す。これには、パスワード、キー、コミュニティストリング、ユーザ名などが含まれます。コントローラは、すべてのコントローラ管理アセットのデータマスキングを行ってから、この情報をCX Cloud Agentに転送します。場合によっては、コントローラ管理資産のテレメトリをさらに匿名化できます。テレメトリの匿名化の詳細については、対応する[製品サポートドキュメント](#)を参照してください(たとえば、『Cisco DNA Center管理者ガイド』の「[データの匿名化](#)」セクションなど)。

テレメトリコマンドのリストはカスタマイズできず、データマスキングルールは変更できませんが、コントローラ管理デバイスの[製品サポートドキュメント](#)またはこのドキュメントの「データソースの接続」セクション(CX Cloud Agentが収集したその他の資産の場合)の説明に従ってデータソースを指定することで、お客様はテレメトリCX Cloudでアクセスする資産を制御できます。

## セキュリティ サマリ

| セキュリティ機能           | 説明  |
|--------------------|---|
| ブートローダーのパスワード      | ブートローダー ( シングルユーザーモード ) には、一意のパスワードがランダムに設定されます。ユーザは <a href="#">FAQ</a> を参照して、ブートローダ ( シングルユーザーモード ) のパスワードを設定する必要があります。   |
| ユーザーアクセス           | SSH :<br><ul style="list-style-type: none"> <li>・cxcadmin ユーザーを使用してアプライアンスにアクセスするには、インストール時に作成されたログイン情報が必要です。</li> <li>・ cxcrootユーザを使用してアプライアンスにアクセスするには、権限のあるユーザがSWIMポータルを使用してクレデンシャルを復号化する必要があります。</li> </ul>   |
| ユーザアカウント           | <ul style="list-style-type: none"> <li>・ cxcadmin : デフォルトのユーザー・ アカウントが作成されます。ユーザーはcxcliを使用してCX Cloud Agentアプリケーション・ コマンドを実行でき、アプライアンスに対する最小限の権限を持ちます。cxcrootユーザーとその暗号化されたパスワードはcxcadminユーザーを使用して生成されます。</li> <li>・ cxcroot: cxcadminは、ユーティリティremoteaccountを使用してこのユーザーを作成できます。ユーザーは、このアカウントでルート権限を取得できます。</li> </ul> |
| cxcadmin パスワードポリシー | <ul style="list-style-type: none"> <li>・パスワードは SHA-256 を使用して一方向ハッシュされ、安全に保存されます。</li> <li>・ 大文字、小文字、数字、特殊文字のうち3種類を含む、8文字以上。</li> </ul>  |



|                          |   |
|--------------------------|---|
| <p>cxcroot パスワードポリシー</p> | <ul style="list-style-type: none"> <li>・ cxcrootのパスワードはRSA/ECB/PKCS1v1_5で暗号化</li> <li>・生成されたパスワードは、SWIM ポータルで復号する必要があります。</li> <li>・ cxcrootのユーザとパスワードは2日間有効で、cxcadminユーザを使用して再生成できます。</li> </ul> |
| <p>ssh ログインパスワードポリシー</p> | <ul style="list-style-type: none"> <li>・ 8文字以上で、大文字、小文字、数字、特殊文字の3つのカテゴリを含む。</li> <li>・ ログイン試行に5回失敗すると、ボックスが30分間ロックされます。パスワードの有効期限は90日です。</li> </ul>   |
| <p>ポート</p>               | <p>オープンな着信ポート - 514 ( Syslog ) と 22 ( SSH )</p>   |
| <p>データセキュリティ</p>         | <ul style="list-style-type: none"> <li>・顧客情報は保存されません。</li> <li>・デバイスデータは保存されません。</li> <li>・Cisco DNA Center サーバーのログイン情報が暗号化され、データベースに保存されます。</li> </ul>   |

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。