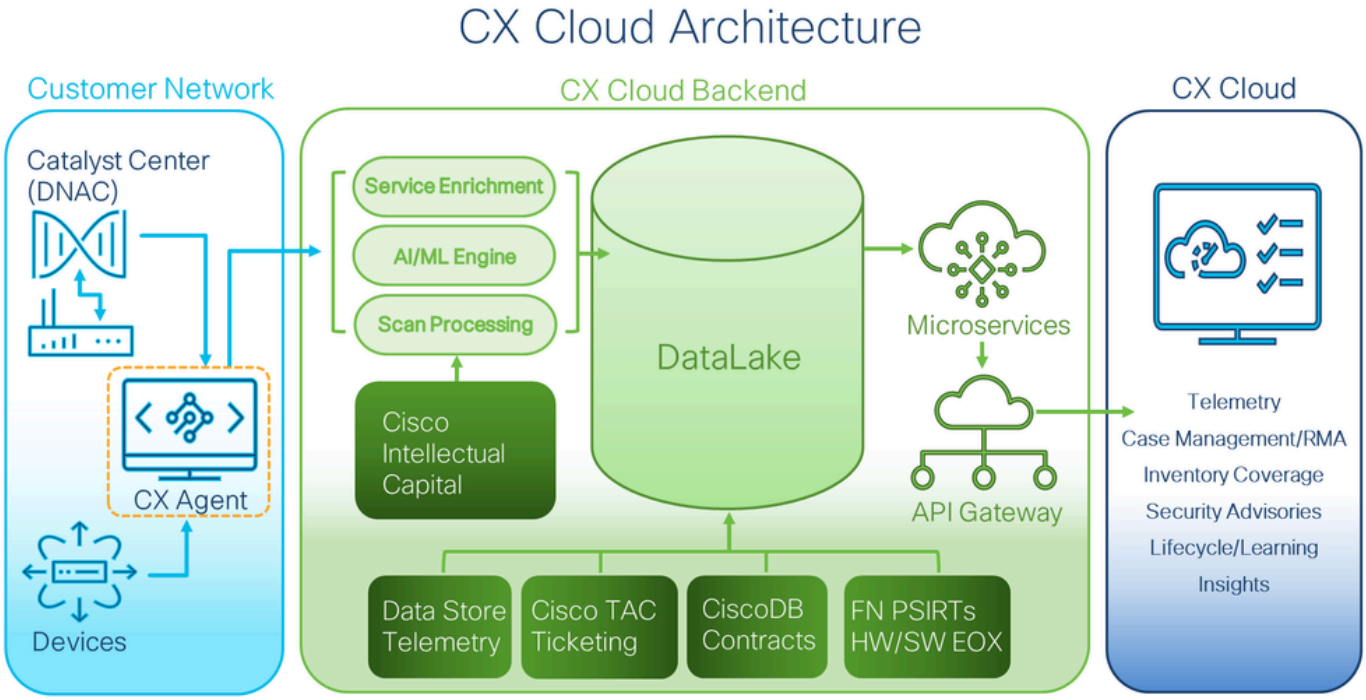
CXエージェント概要ガイドv3.1

内容

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)エージェントについて説明します。シスコのCX Agentは、お客様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、お客様に実用的な洞察を提供する、拡張性の高いプラットフォームです。CX Agentを使用すると、アクティブな実行コンフィグレーションデータを人工知能(AI)/機械学習(ML)に変換し、CX Cloudに表示される予防的かつ予測的な洞察を得ることができます(Success Tracks、Smart Net Total Care(SNTC)、Business Critical Services(BCS)、Lifecycle Services(LCS)など)。



CX Cloudアーキテクチャ

このマニュアルは、CX Cloudおよびパートナーアドミニストレータのみを対象としています。スーパーユーザ管理者(SUA)および管理者ロールを持つユーザは、このガイドで説明されているアクションを実行するために必要な権限を持ちます。

このガイドは、CXエージェントv3.1専用です。以前のバージョンにアクセスするには、「Cisco CX Agent」ページを参照してください。

✎ 注：このガイドの画像は参照用です。実際の内容はさまざまです。

前提条件

CX Agentは仮想マシン(VM)として実行され、Open Virtual Appliance(OVA)または仮想ハードディスク(VHD)としてダウンロードできます。

導入の要件

- 新しいインストールには、次のいずれかのハイパーバイザが必要です。
  - VMware ESXi v5.5以降
  - Oracle Virtual Box v5.2.30以降
  - Windows Hypervisorバージョン2012 ~ 2022およびバージョン2025

- VMを導入するには、次の表に示す設定が必要です。

CXエージェントの導入タイプ	CPUコアの数	RAM	ハード ディスク	* 直接資産の最大数 cxエージェントに接続	サポートされるハイパーバイザ
小さいOVA	8C	16 GB	200 GB	10,000	VMware ESXi、Oracle VirtualBox、および Windows Hyper-V
中OVA	16C	32 GB	600 GB	20,000	VMware ESXi
大きいOVA	32C	64 GB	1200 GB	50,000 :	VMware ESXi

* 各CX Cloud Agentインスタンスについて、20のCisco Catalyst Center(Catalyst Center)非クラスタまたは10のCatalyst Centerクラスタを接続することに加えて、

注：RADKitサービスは、中規模および大規模のOVAタイプのCXエージェントの導入でのみ利用できます。

- CX Cloudデータを格納するプライマリ・データ・リージョンとして米国の指定されたデータ・センターを使用しているお客様の場合、CX 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.csco.cloud
  - FQDN:ng.acs.agent.us.csco.cloud
  - FQDN:cloudsso.cisco.com
  - FQDN:api-cx.cisco.com
- CX Cloudのデータを格納するプライマリ・データ・リージョンとして指定のヨーロッパのデータ・センターを使用しているお客様の場合： CX Agentは、FQDNを使用し、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できる必要があります。
  - FQDN:agent.us.csco.cloud
  - FQDN:agent.emea.csco.cloud
  - FQDN:ng.acs.agent.emea.csco.cloud
  - FQDN:cloudsso.cisco.com
  - FQDN:api-cx.cisco.com
- 指定されたアジア太平洋地域のデータ・センターをプライマリ・データ・リージョンとして使用し、CX Cloud・ データを格納しているお客様の場合： CX Agentは、ここに示す両方のサーバに、FQDNを使用し、TCPポート443でHTTPSを使用して接続できる必要があります。
  - FQDN:agent.us.csco.cloud
  - FQDN:agent.apjc.csco.cloud

    - FQDN:ng.acs.agent.apjc.csco.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に登録する場合のみ、FQDN(agent.us.csco.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にアクセスできる必要があります。
- FQDNを使用するRADKitを使用し、TCPポート443でHTTPSを使用しているお客様向け：
    - 米国のFQDN:radkit.us.csco.cloud
    - EMEAのFQDN:radkit.emea.csco.cloud
    - APJC FQDN:radkit.apjc.csco.cloud
- RADKitが出力をサービス要求に添付できるようにするには、CXエージェントがFQDN cxd.cisco.comにアクセスできる必要があります。
- 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。

CX Cloud Agent Traffic

Source	Destination	Protocol	Port	Purpose	Type
CX Cloud Agent	All regions: cloudsso.cisco.com api-cx.cisco.com agent.us.csco.cloud radkit.emea.csco.cloud Catalyst Center AMER region: ng.acs.agent.us.csco.cloud EMEA region: agent.emea.csco.cloud ng.acs.agent.emea.csco.cloud APJC region: agent.apjc.csco.cloud ng.acs.agent.apjc.csco.cloud	HTTPS	TCP/443	Initial configuration Upgrades Inventory & telemetry transfers Access to RADKit Cloud	Outbound to Cisco AWS regional data centers and Catalyst Center
CX Cloud Agent	Network Devices	SNMP	UDP/161	Initial discovery Ongoing inventory collections	Outbound to LAN
CX Cloud Agent	Network Devices	SSH	TCP/22	Collection of telemetry from CLI commands	Outbound to LAN
CX Cloud Agent	Network Devices	Telnet	TCP/23	Collection of telemetry from CLI commands	Outbound to LAN
Network Devices	CX Cloud Agent	Syslog	UDP/514	Transfer syslogs for Alert Fault Management	Inbound from LAN
Workstation	CX Cloud Agent	SSH	TCP/22	CX Cloud Agent Maintenance	Inbound from LAN

- 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。それ以外の場合は、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アドレスを使用できる必要があります。
- IPv4のみがサポートされます。
- 認定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Catalyst Centerのバージョンは、2.1.2.x ~ 2.2.3.x、2.3.3.x、2.3.5.x、2.3.7.x、およびCatalyst Center仮想アプライアンスとCatalyst 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エージェントのIPアドレス。
- 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 ジャーニーを開始するには、次のドメインにアクセスする必要があります。提供されたホスト名のみを使用します。固定IPアドレスは使用しないでください。

CXエージェント・ポータルに固有のドメイン

主要なドメイン	その他のドメイン
csco.cloud	cloudfront.net
split.io	eum-appdynamics.com
	appdynamics.com
	tiqcdn.com
	jquery.com

CXエージェントOVAに固有のドメイン

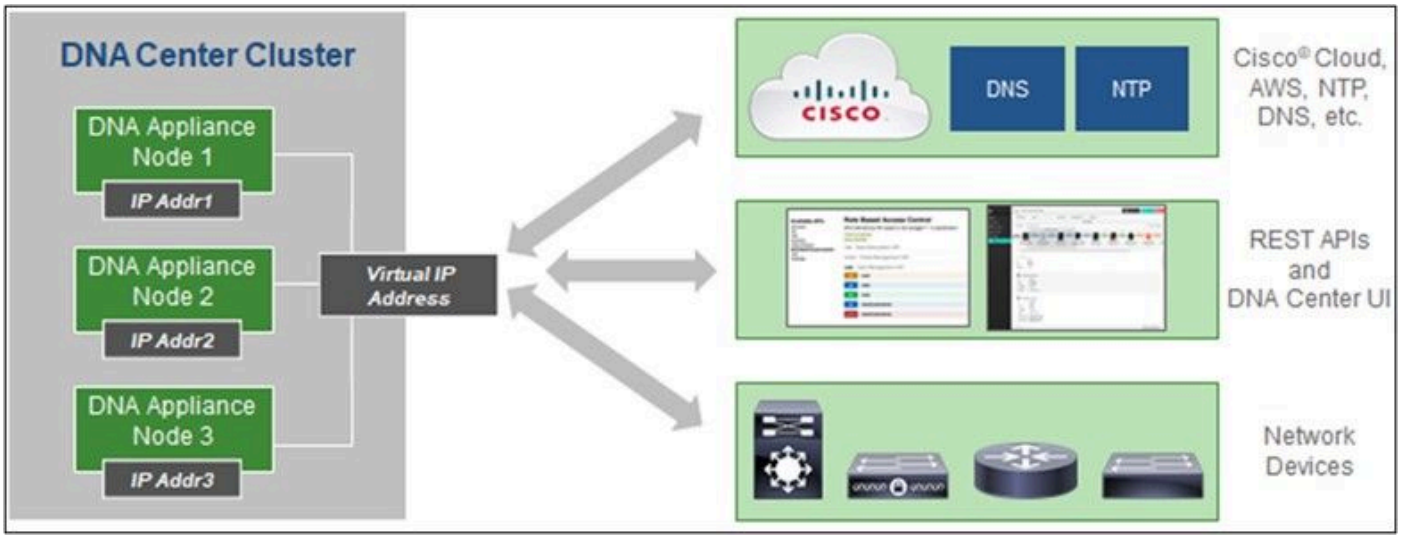
AMERICAS	EMEA	APJC
cloudsso.cisco.com	cloudsso.cisco.com	cloudsso.cisco.com
api-cx.cisco.com	api-cx.cisco.com	api-cx.cisco.com
agent.us.csco.cloud（クラウド）	agent.us.csco.cloud（クラウド）	agent.us.csco.cloud（クラウド）
ng.acs.agent.us.csco.cloud（クラウド）	エージェント.emea.csco.cloud	エージェント.apjc.csco.cloud
	ng.acs.agent.emea.csco.cloud	ng.acs.agent.apjc.csco.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。

Catalyst 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Catalyst Centerのバージョンは、2.1.2.x ~ 2.2.3.x、2.3.3.x、2.3.5.x、2.3.7.x、およびCatalyst Center仮想アプライアンスとCatalyst 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で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

サポート対象製品リスト

CXエージェントでサポートされている製品のリストを表示するには、「サポートされている製品のリスト」を参照してください。

CX Agent v3.1のアップグレード/インストール

- 新しいバージョンにアップグレードする既存のお客様は、「CX Agent v3.1のアップグレード」を参照してください。
- 新しく柔軟なOVA v3.1のインストールを実装する新規のお客様は、「CXエージェントの追加」を参照してください。

既存のVMの大規模構成および中規模構成へのアップグレード

お客様は、ネットワークのサイズと複雑さに基づいて、Flexible OVAオプションを使用して既存のVM構成を中規模または大規模にアップグレードできます。

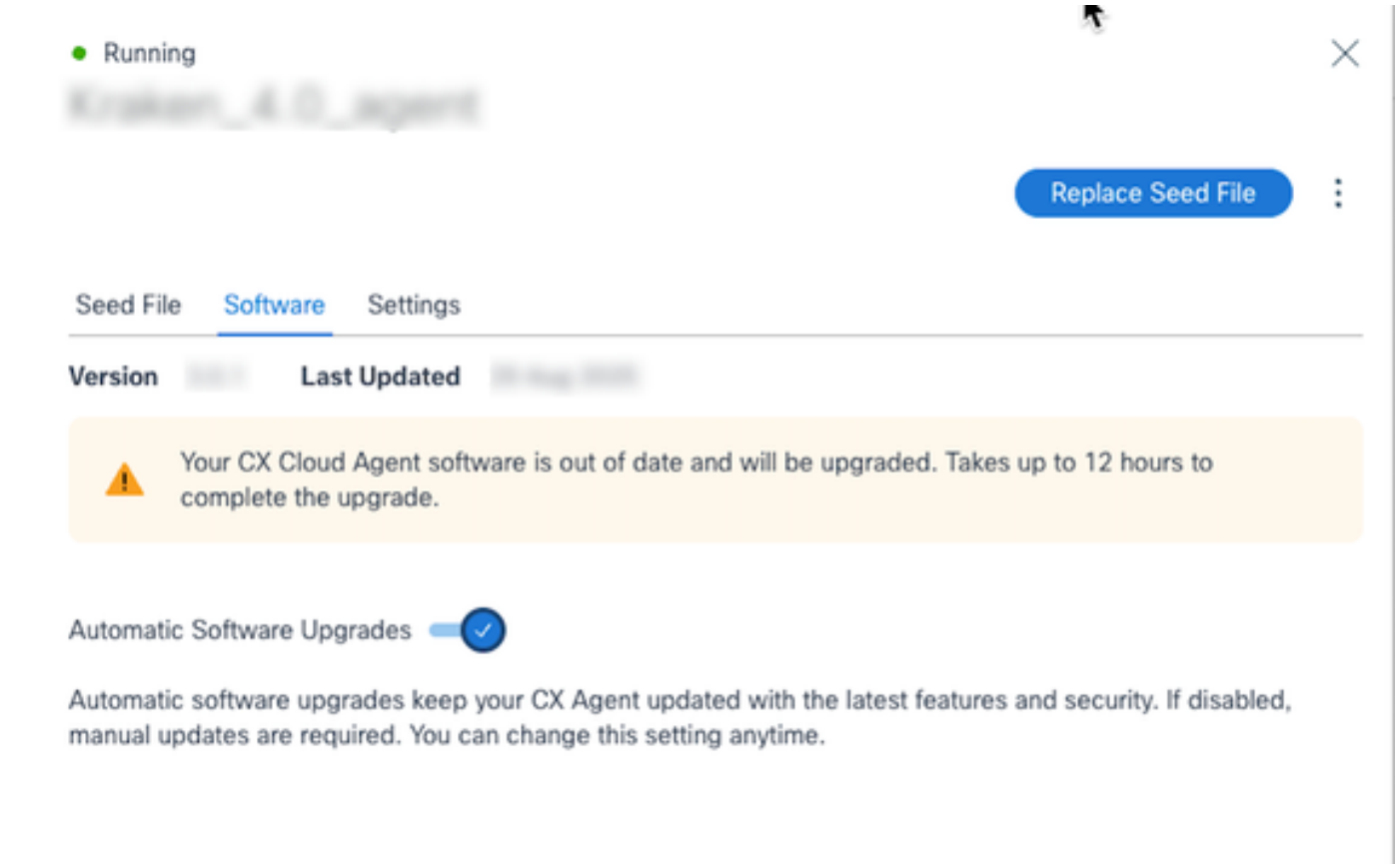
既存のVM構成を小規模から中規模または大規模にアップグレードする方法については、「CXエージェントVMの中規模および大規模構成へのアップグレード」のセクションを参照してください。

CX Agent v3.1へのアップグレード

既存のお客様は、自動アップグレードを有効にするか、既存のバージョンから手動でアップグレードすることにより、最新バージョンにアップグレードできます。

自動アップグレード

自動ソフトウェアアップグレード切り替えを有効にすると、新しいバージョンがリリースされたときにシステムが確実に更新されます。このオプションは、新規インストールではデフォルトで有効になっていますが、会社のポリシーに合わせるため、または予定されたメンテナンス期間中にアップグレードをスケジュールするために、いつでも変更できます。



自動アップグレード

注：既存のCXエージェントインスタンスの自動アップグレードはデフォルトで無効になっていますが、ユーザはいつでも有効にできます。

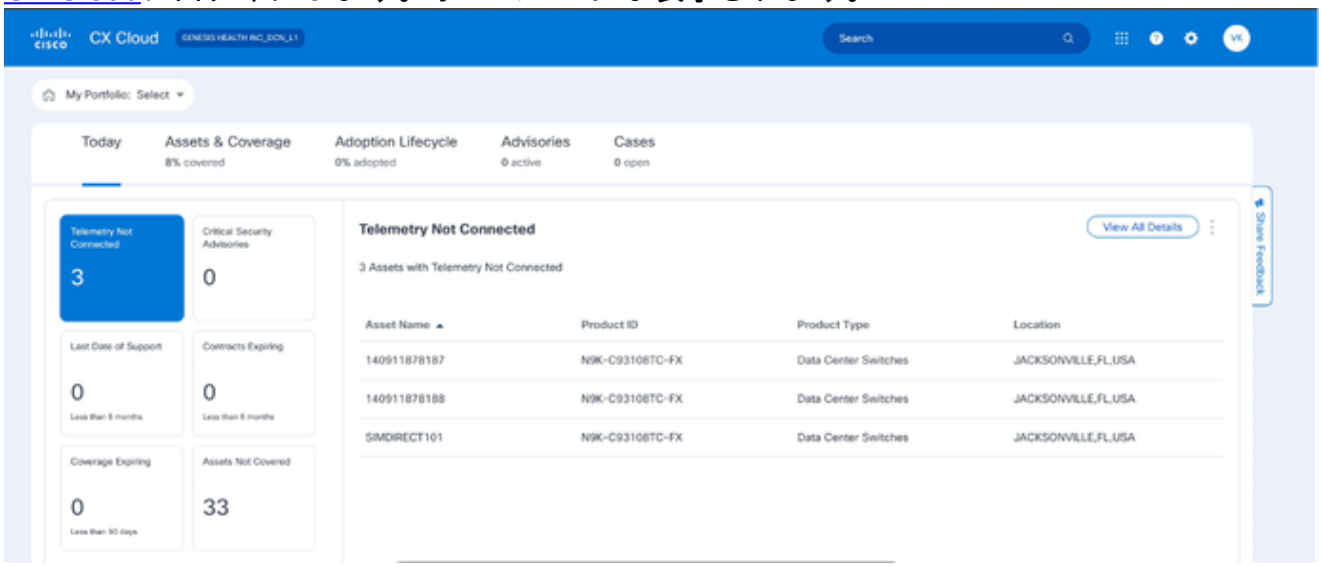
手動アップグレード

自動アップグレードを使用せず、自動ソフトウェアアップグレードをイネーブルにしていないお客様は、手動アップグレードを選択できます。CX Agent v2.4.x以降では、このセクションで説明する手順に従って、v3.1への直接アップグレードをサポートしています。

注:CXエージェントv2.3.x以前をご使用のお客様は、v3.1にアップグレードする前にv2.4.xに段階的にアップグレードするか、新規OVAインストールを実行する必要があります。

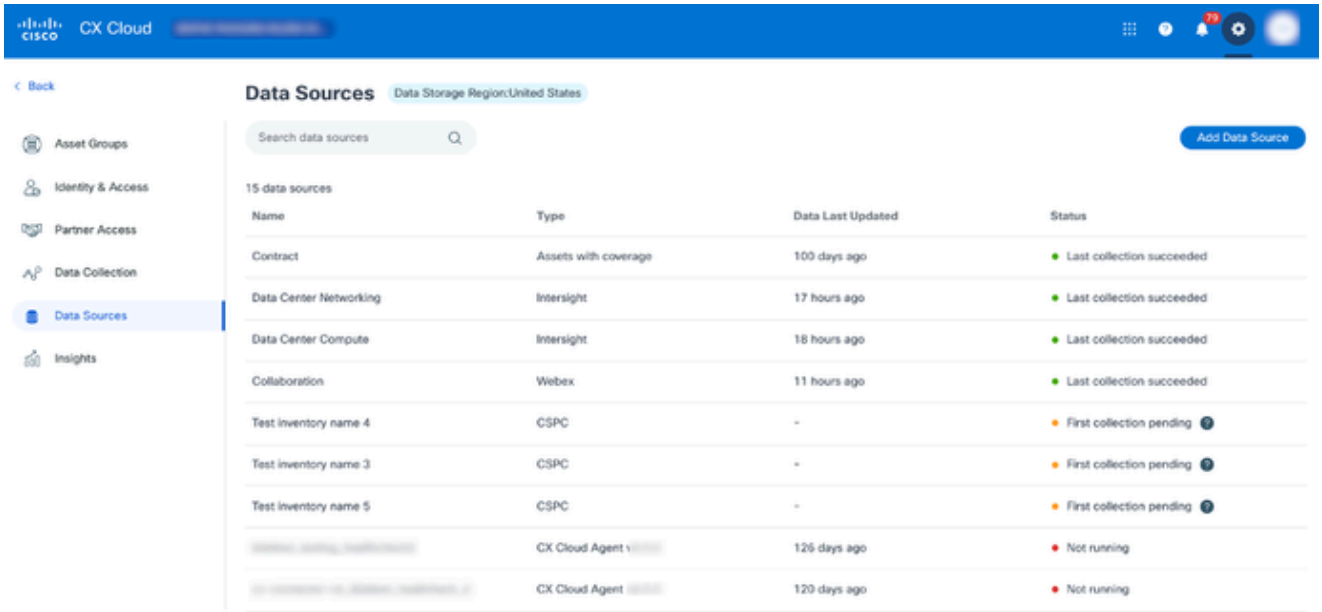
CX CloudからCX Agentアップグレードv3.1をインストールするには、以下の手順に従ってください。

1. CX Cloudにログインします。ホームページが表示されます。



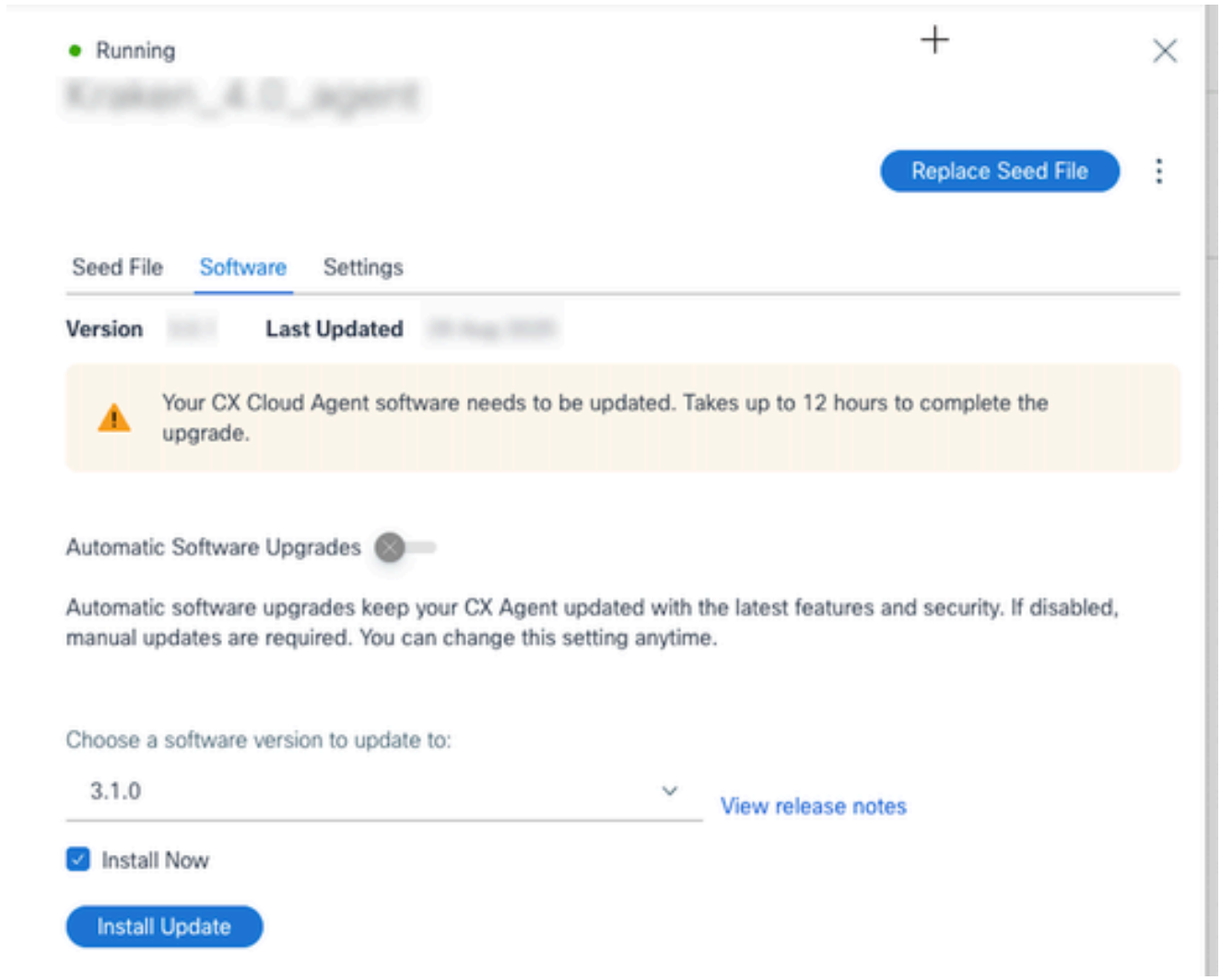
CX Cloudホームページ

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。



データソース

3. CX Agentのデータソースをクリックします。CXエージェントの詳細ウィンドウが開きます。



手動アップグレード

4. Choose a software version to update toドロップダウンリストから、ソフトウェアバージョン3.1.0を選択します。
5. Install Updateをクリックして CX Agent v3.1をインストールします。

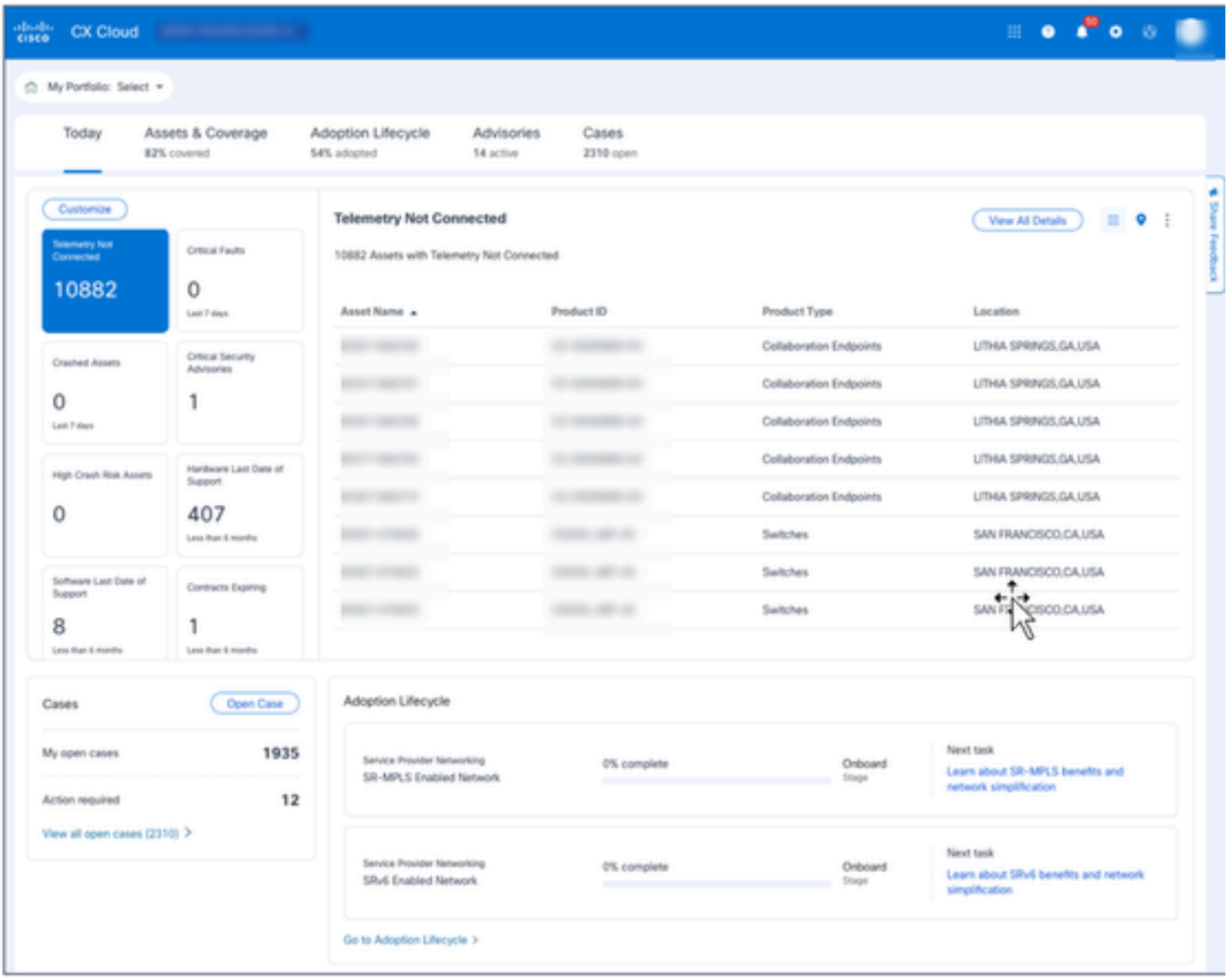
注：お客様は、スケジュールオプションを表示するInstall Nowチェックボックスをオフにすることで、後で更新するようにスケジュールできます。

CXエージェントの追加

お客様は、CX Cloudで最大20のCX Agentインスタンスを追加できます。

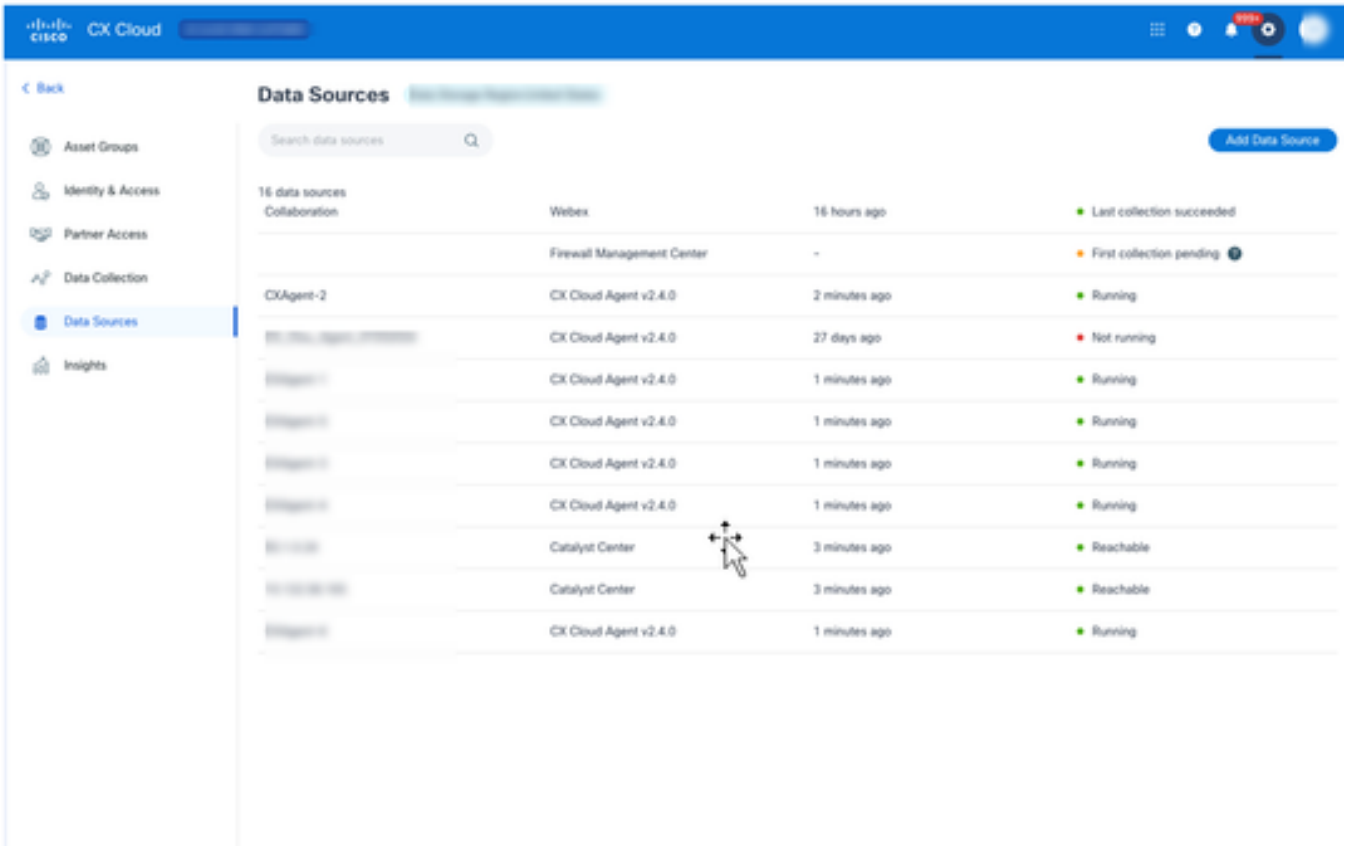
CXエージェントを追加するには、以下の手順に従ってください。

1. CX Cloudにログインします。ホームページが表示されます。



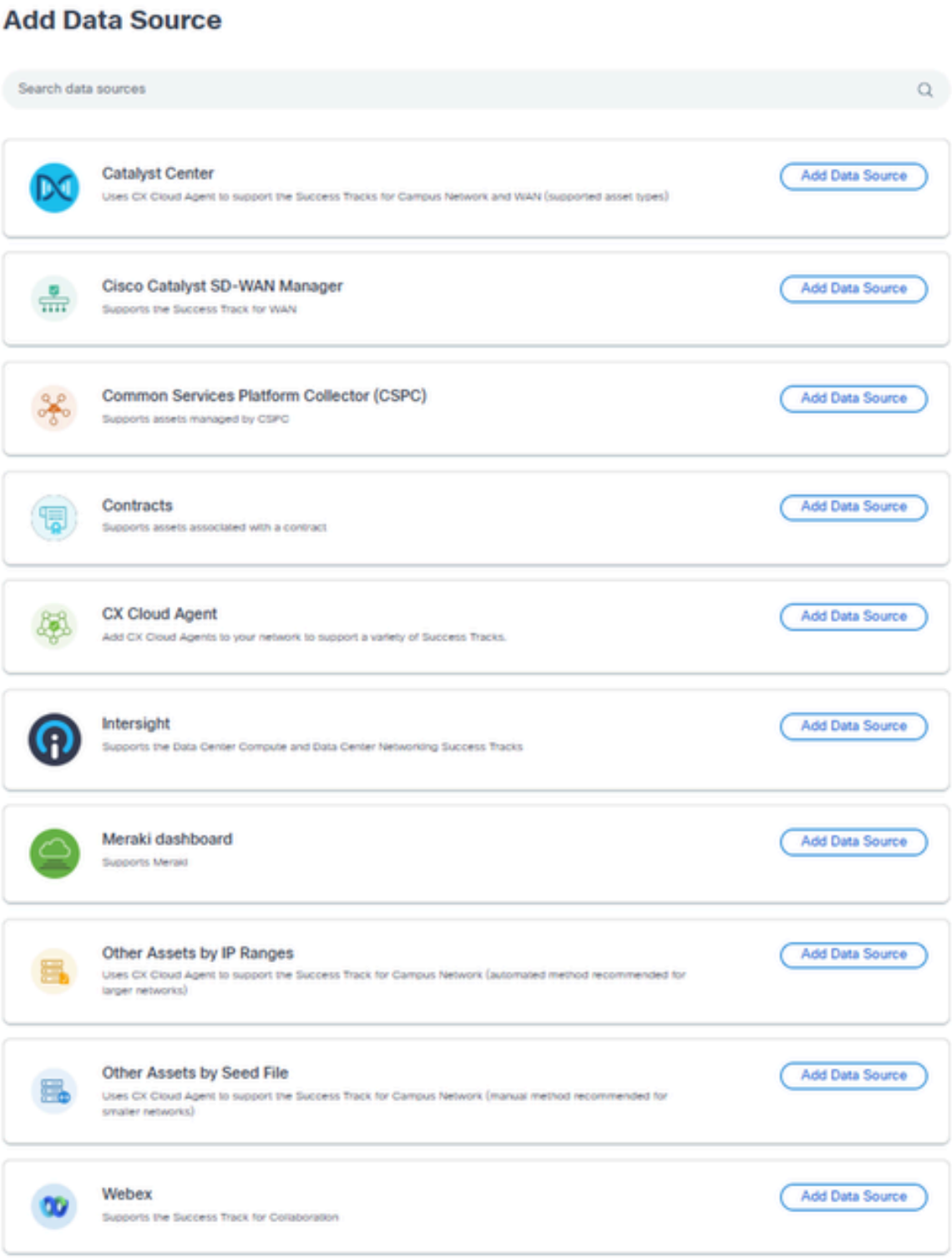
CX Cloudホームページ

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。



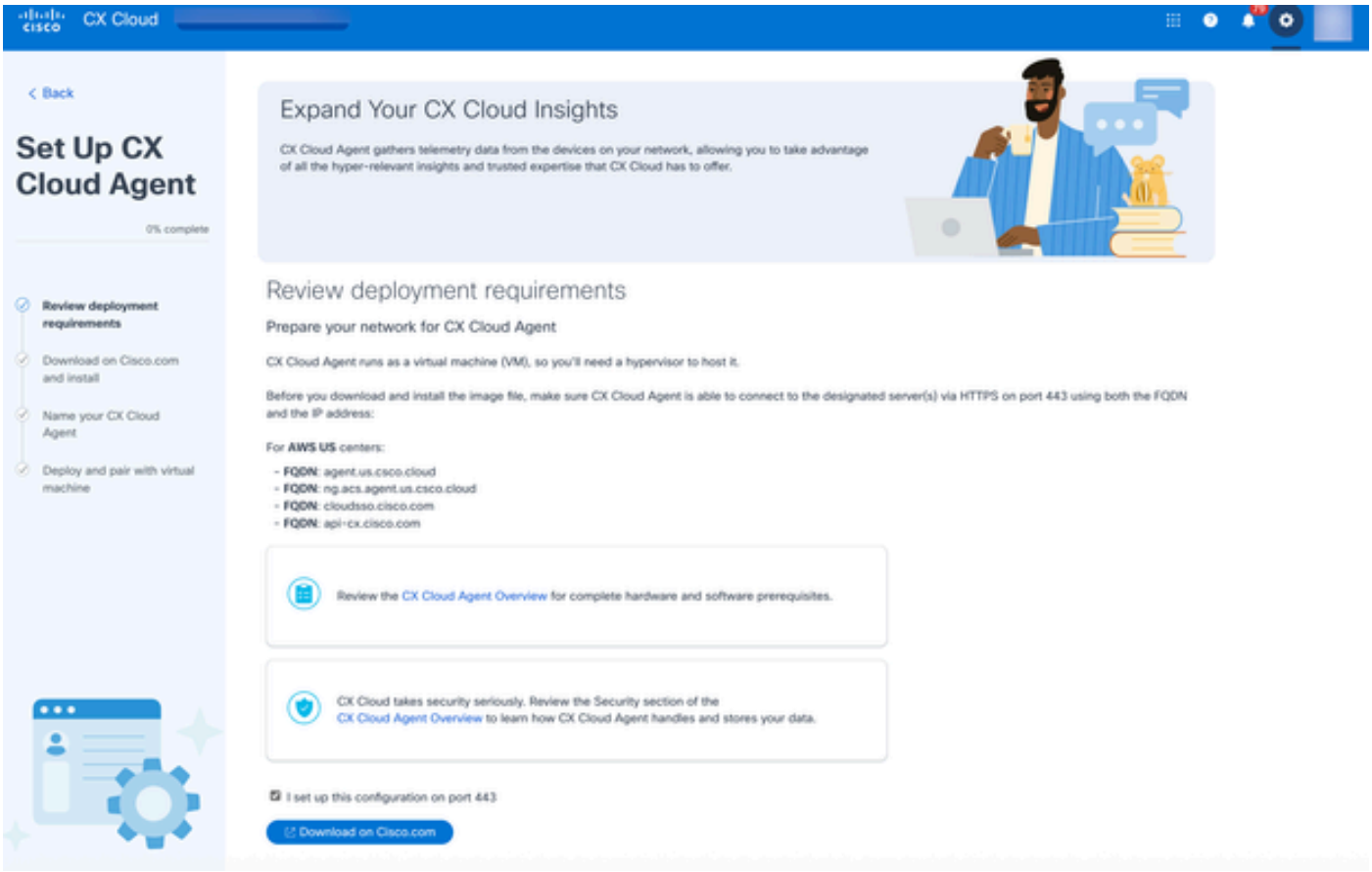
データソース

3. Add Data Sourceをクリックします。データソースの追加ページが開きます。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。



データソースの追加

4. CX AgentオプションからAdd Data Sourceをクリックします。Set Up CX Agentウィンドウが開きます。



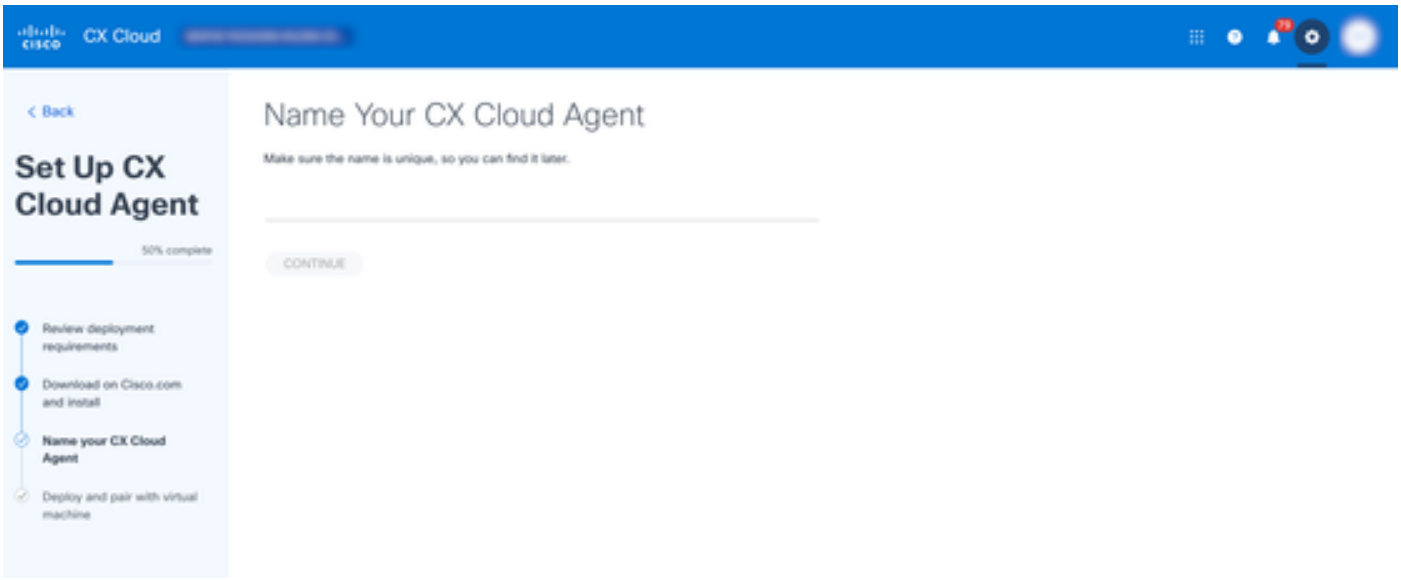
CXエージェントの追加

5. 「展開要件のレビュー」セクションを確認し、「I set up this configuration on port 443」チェックボックスをオンにします。
6. Cisco.comのDownloadをクリックします。Software Downloadウィンドウが別のタブで開きます。
7. 「CX Agent v3.1.0 OVA」ファイルをダウンロードします。

注:「OVA」ファイルを導入した後、CXエージェントのセットアップを完了するために必要なペアリングコードが生成されます。

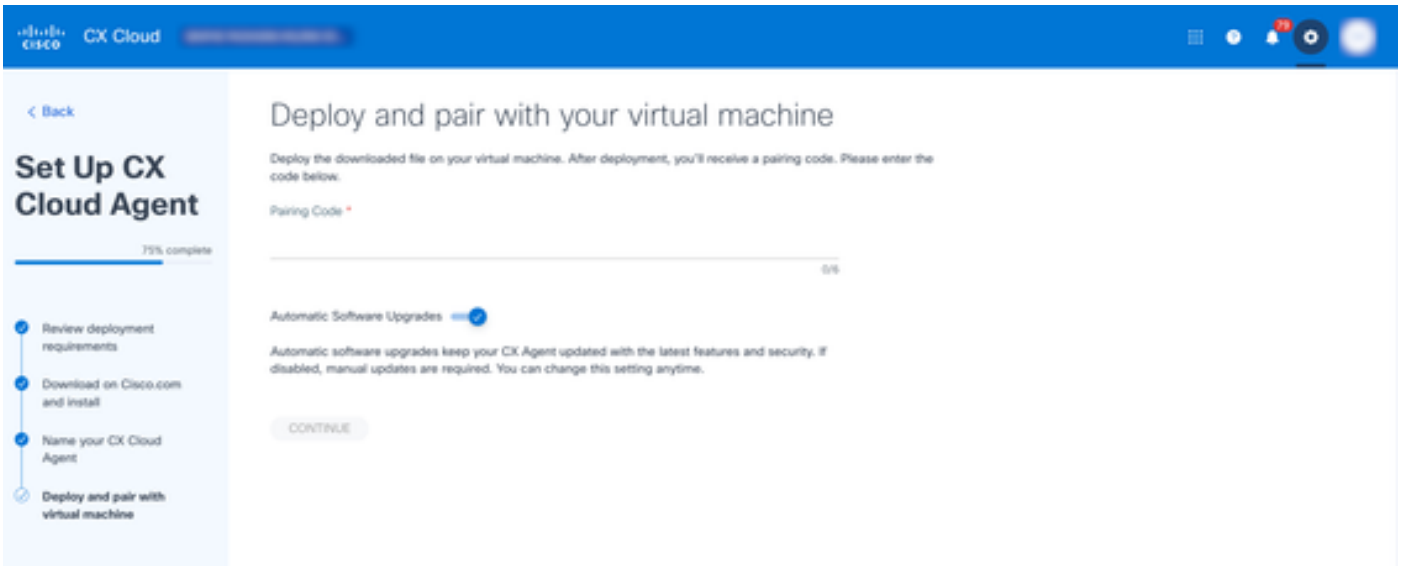
---

8. Name Your CX Cloud AgentフィールドにCX Agentの名前を入力します。



名前CXエージェント

9. Continueをクリックします。Deploy and pair with your virtual machineウィンドウが開きます。



ペアリングコード

10. ダウンロードした「OVA」ファイルの展開後に受信したペアコードを入力します。

11. Continueをクリックします。登録の進行状況が表示され、確認メッセージが表示されます。

注：データソースとしてCXエージェントインスタンスを追加するには、上記の手順を繰り返します。

CX Agent for BCS/LCSの構成

シスコの新しいConverged Collection機能は、BCS/LCS用のCX Agent v3.1の設定を合理化し、カスタマーエクスペリエンスを簡素化します。

注：この設定は、BCS/LCSのお客様のコレクタの設定を担当するシスコサポートエンジニアに固有のものです。

BCS/LCSをご利用のお客様は、CX Cloud Communityにアクセスして、ユーザのオンボーディングやその他の関連情報に関する詳細情報を確認できます。

前提条件

SUA(Super User Administrator)および管理者アクセス権を持つサポート・エンジニアは、BCS/LCSのCXエージェント構成のみを実行できます。

CXエージェントの構成

CX Agent for BCS/LCSを構成するには、シスコサポートにお問い合わせください。

RADKit機能の設定

CX Agent v3.1は、CX Cloudのシスコデバイスのリモート管理とトラブルシューティングを強化するために設計された、オプションのRADKit構成を提供します。有効にすると、認証されたユーザは、データのキャプチャ、設定、およびソフトウェアのアップグレードなどの操作をリモートで安全に実行できます。これらの設定は、お客様の運用要件に基づいて、いつでも有効または無効にすることができます。

RADKitの包括的な詳細については、『Cisco RADKit』を参照してください。

CLIによるRADKitクライアントの統合

RADKitクライアントサービスを統合するには、管理者アカウントを作成し、次の手順に従ってサービスを登録します。

注：次の手順では、CXエージェントVMへのルートアクセスが必要です。

1. 適切なクレデンシャルを使用して、端末とセキュアシェル(SSH)をVMに開きます。次に例を示します。

```
ssh your_username@your_vm_ip
```

2. 次のコマンドを実行して、ネットワーク接続を有効にします。

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

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

3. ローカルマシンで、管理者アカウントを作成するためにマネージャエンドポイントにPOST要求を送信します。リクエスト本文には以下を含める必要があります。

- admin_name（必須）：管理者アカウントのユーザ名
- email（オプション）：管理者アカウントの電子メールアドレス
- full_name（オプション）：管理者のフルネーム
- description（オプション）：管理者アカウントの説明。

次の例は、cURLを使用してこの要求を送信する方法を示しています。

```
curl -X POST \

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

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

  -d '{

        "admin_name": "admin_user123",

        "email": "admin@example.com",

        "full_name": "管理者ユーザー",

        「説明」:「システムを管理するための管理者アカウント」

      }'
```

管理者アカウントが正常に作成されると、サーバは管理者アカウントが正常に作成されたことを示す確認メッセージで応答します。この応答には、最初のログイン時に変更する必要がある一時的なパスワードも含まれています。ただし、管理者アカウントがすでに存在する場合、サーバは「Admin already created」というメッセージとともにステータスコード400を返します。

4. Webブラウザを開き、RADKit Web UI(https://<your_vm_ip>:30101/)に移動します。
5. 管理者ユーザ名(admin_name)と、応答で提供された一時パスワードを使用してログインします。

注：最初のログイン時に、ユーザはパスワードの変更を求められます。指示に従って、新しいパスワードを設定します。

---

6. ローカルマシンでRADKitクライアントを実行し、サービスを登録します。
7. 認証後、次のコマンドを実行してワンタイムパスワードを生成します。

参考`grant_service_otp()`

8. ローカルマシンで、マネージャエンドポイントにPOST要求を送信し、サービスを登録します。リクエスト本文には以下を含める必要があります。

- OTP（必須）：ワンタイムパスワード文字列

次の例は、cURLを使用してこの要求を送信する方法を示しています。

```
curl -X POST \
```

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

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

-d '{

        「one_time_password」:「PROD:1234-1234-1234」

    }'
```

登録に成功すると、確認メッセージが表示され、ユーザは管理者アカウントを使用してRADKitサービスを管理できます。

ネットワーク接続を無効にするには、次のコマンドを実行します。

kubectl適用 – f /home/cxcadmin/deny-from-other-namespaces.yaml

既存のCXエージェント用のVaultの構成

オプションのVault設定機能を使用すると、CX CloudはVaultサービスに安全に接続して、最新のクレデンシャルを使用してトークンやインベントリリストなどの機密データにアクセスできます。有効にすると、CX Cloudは設定されたアドレスとトークンを自動的に使用します。この設定はいつでも有効または無効にできます。現在、HashiCorpのVault構成のみがサポートされています。

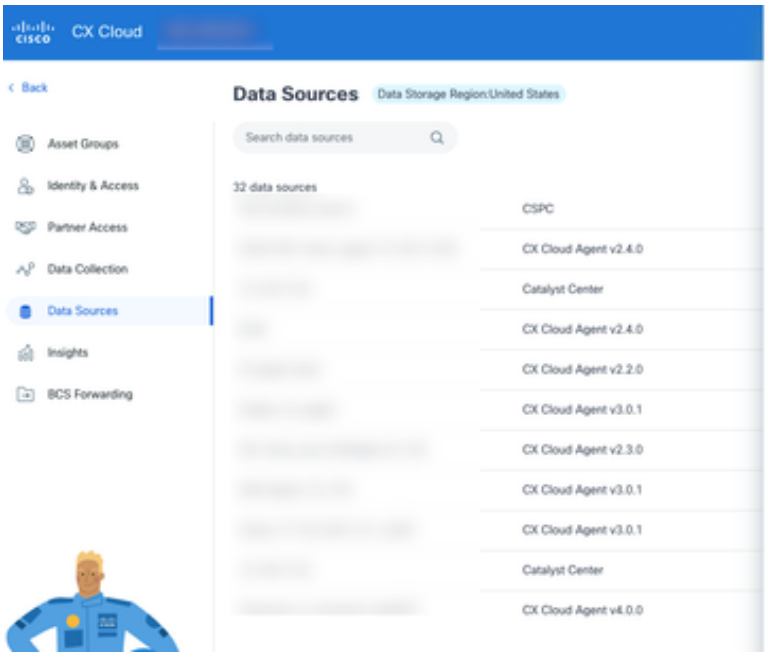
Vaultは、次の2つの方法で設定できます。

- CX Cloud UIを使用
- CLIを使用

CX Cloud UIでのHashiCorp Vaultの設定

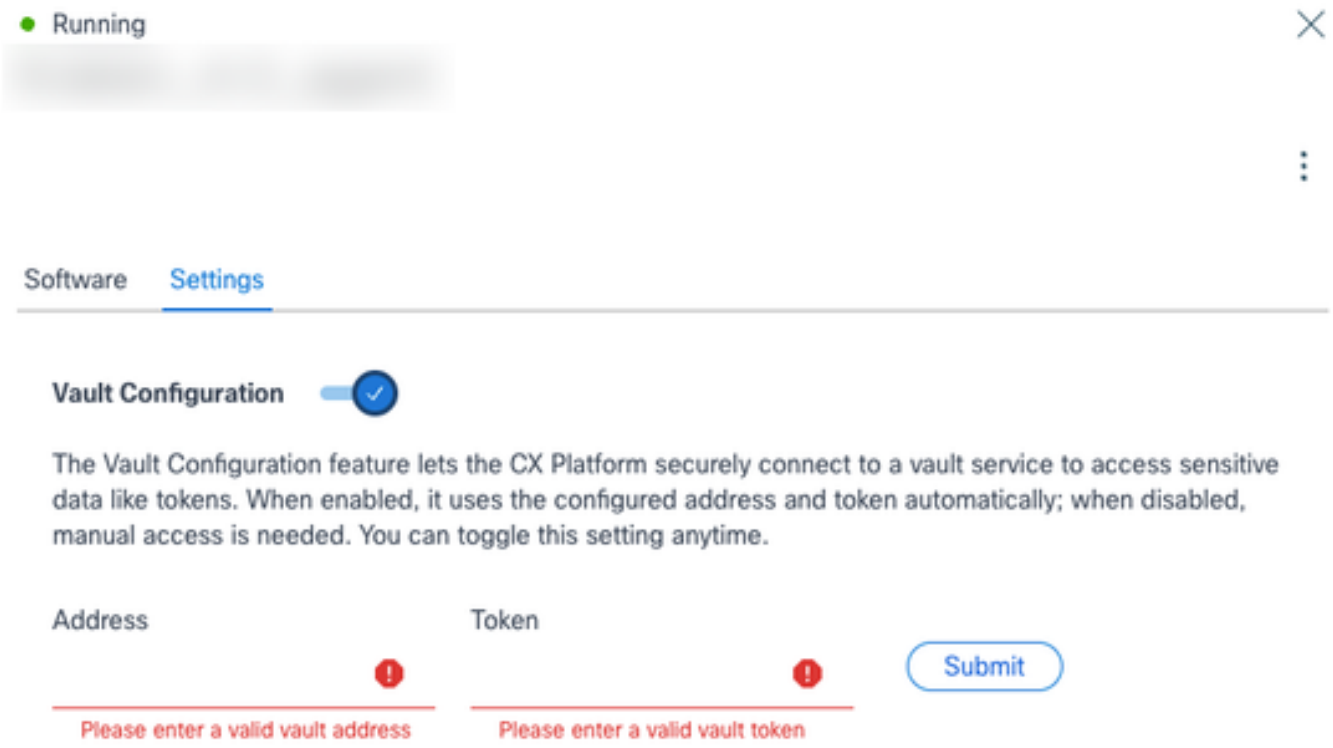
既存のCXエージェント用にHashiCorp資格情報コンテナーを構成するには、次の手順に従います。

1. 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。
2. CXエージェントのデータ・ソースをクリックします。CXエージェントの詳細ウィンドウが開きます。



Settings

3. Settingsタブをクリックします。
4. Vault Configuration切り替えを有効にします。



Vaultの設定

5. AddressフィールドとTokenフィールドに詳細を入力します。

6. Submitをクリックします。確認と追加したIPアドレスが表示されます。

Removeをクリックすると、設定済みのVaultを削除できます。

CLIを使用したCX AgentとHashiCorp Vaultの統合

このセクションでは、Cisco CX AgentとHashiCorp Vaultインスタンス間の接続を設定する手順の概要を説明します。この統合により、デバイスクレデンシャルの安全な保存と取得が可能になり、全体的なセキュリティポスチャが強化されます。

前提条件

- cxエージェントVMへのcxcrootアクセス
- 実行中でアクセス可能なVaultインスタンス

HashiCorp Vaultとの統合

- Vault統合を有効にするには、次のコマンドを実行します。

```
cxcli agent vaultオン
```

- Vaultの統合を無効にするには、次のコマンドを実行します。

```
cxcliエージェントボールトオフ
```

- 現在のボールト統合ステータスを確認するには、次のコマンドを実行します。

```
cxcliエージェントボールトステータス
```

HashiCorp Vault統合の有効化

Vault統合を有効にするには

1. cxcrootユーザアカウントを使用してSSH経由でCXエージェントにログインし、CXエージェントにアクセスします。
2. 次のコマンドを実行して、rootユーザに切り替え、権限を昇格させます。

```
sudo su ( スドス )
```

3. 次のコマンドを実行して、現在のボールト統合ステータスを確認します。

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

vault統合が無効

4. 次のコマンドを実行して、ボールト統合を有効にします。

```
cxcli agent vaultオン
```

5. 次のフィールドを更新します。

- Vaultアドレス
- Vaultルートトークン

6. 検証するには、Vaultとの統合のステータスを確認します。応答メッセージで、統合が有効になっていることを確認する必要があります。

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

```
HashiCorpのVaultアドレスを入力：
```

```
HashiCorp Vault Tokenを入力：
```

```
vault統合の有効化root@cxcloudagent:/home/cxcroot#
```

HashiCorp Vault統合の無効化

CXエージェントにアクセスするには、以下の手順に従ってください。

1. cxcrootユーザアカウントを使用して、SSH経由でCXエージェントにログインします。
2. 次のコマンドを実行して、rootユーザに切り替え、権限を昇格させます。

```
sudo su ( スドス )
```

3. 次のコマンドを実行して、HashiCorp Vault統合を無効にします。

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

```
vault統合が無効
```

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

HashiCorp Vaultデバイス資格情報スキーマ

Vault Credentials Schema：デバイスクレデンシャルの使用可能なオプションとサポートされるフィールドの詳細については、「Vault Credentials schema」ファイル(vault-credentials-schema.json)をダウンロードしてください。

例：スキーマに基づくJSONクレデンシャルの例を次に示します。

-

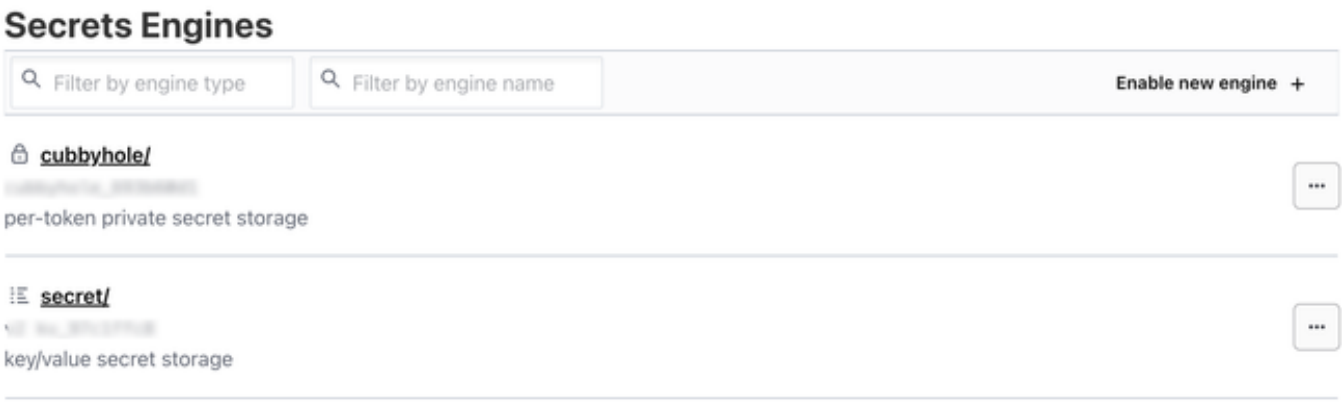
```
{
"targetIp": "5.0.1.*",
"credentials": {
"snmpv3": {
"user": "cisco",
"authPassword": "*******",
"authAlgorithm": "MD5",
"privacyPassword": "*******",
"privacyAlgorithm": "AES-256"
},
"telnet": {
"user": "cisco",
```

```
"password": "*******",
"enableUser": "cisco",
"enablePassword": "********"
}
}
}
```

注：ユーザは、1つのクレデンシャルJSONファイル内で複数のプロトコルを指定できます。ただし、同じファミリからの重複したプロトコルを含めないでください（たとえば、同じクレデンシャルファイルにSNMPv2cとSNMPv3の両方を含めないでください）。

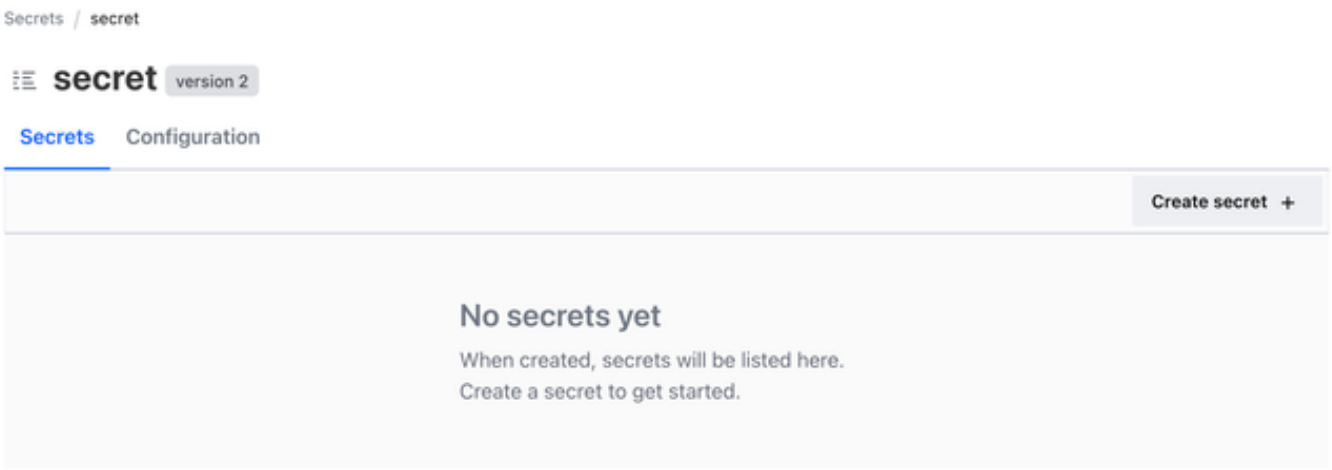
HashiCorp Vaultでのデバイス資格情報の設定(初回)

1. Vaultインスタンスにログインします。



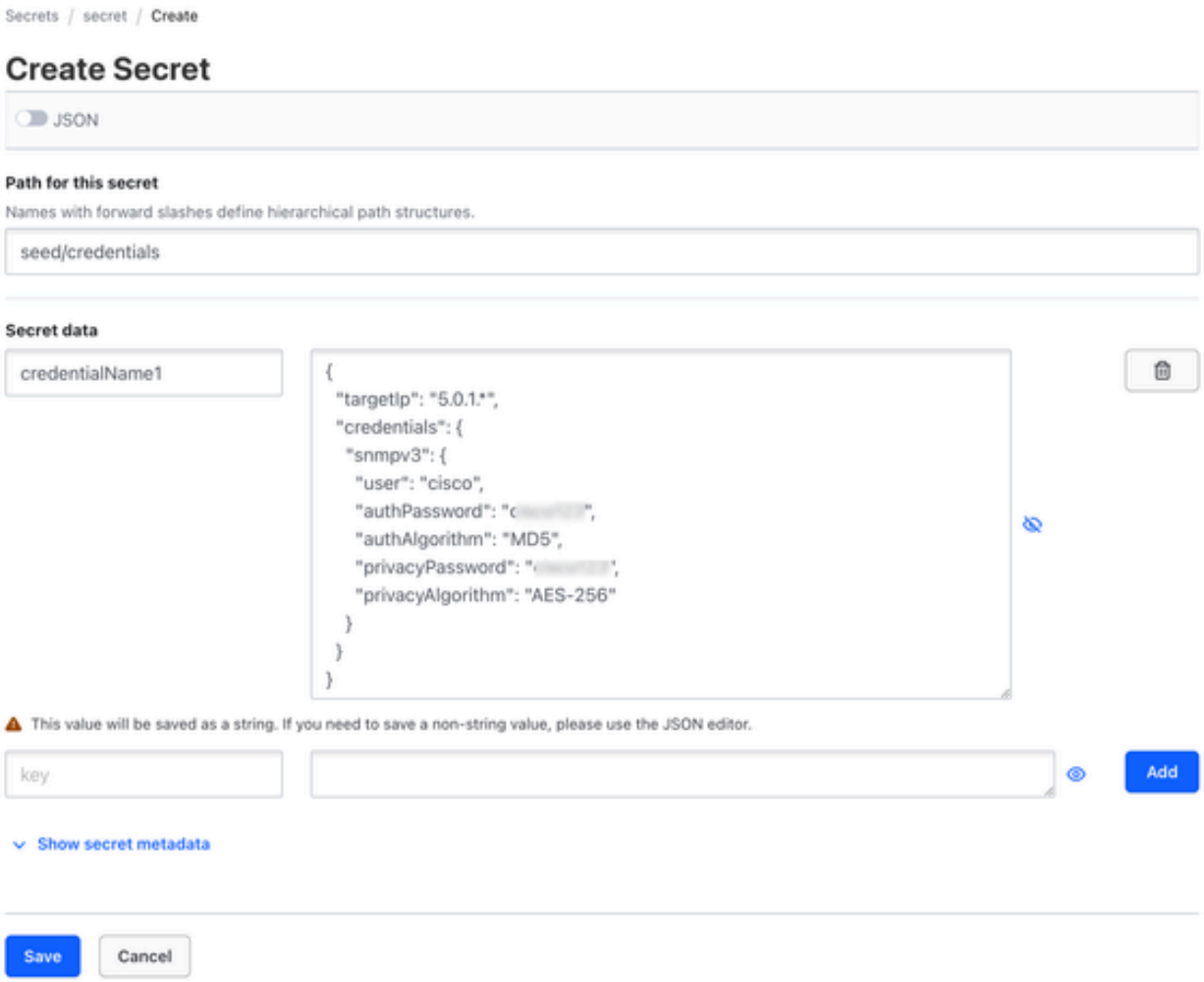
秘密鍵

2. secret/seed/credentialsのパスを使用して、新しいキー値のシークレットを作成します。
3. キーと値のシークレットストレージエンジン(secret/)を選択します。



キー値のシークレット

4. Create secretをクリックします。Create Secretウィンドウが開きます。

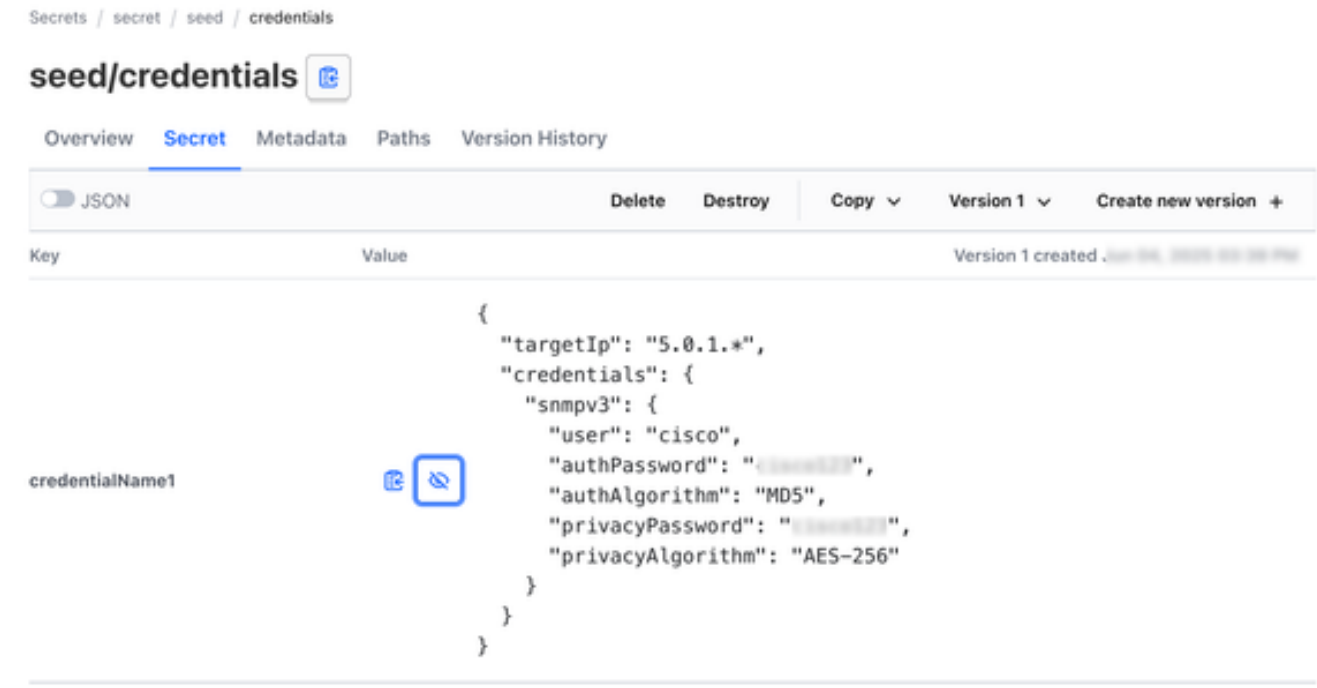


クライアントシークレット

5. 次のフィールドを更新します。

- シークレットのパス：シード/資格情報
- シークレットデータ：キーと値のシークレットのコレクション
- key：カスタムの一意のクレデンシャル名
- 値：クレデンシャルJSON

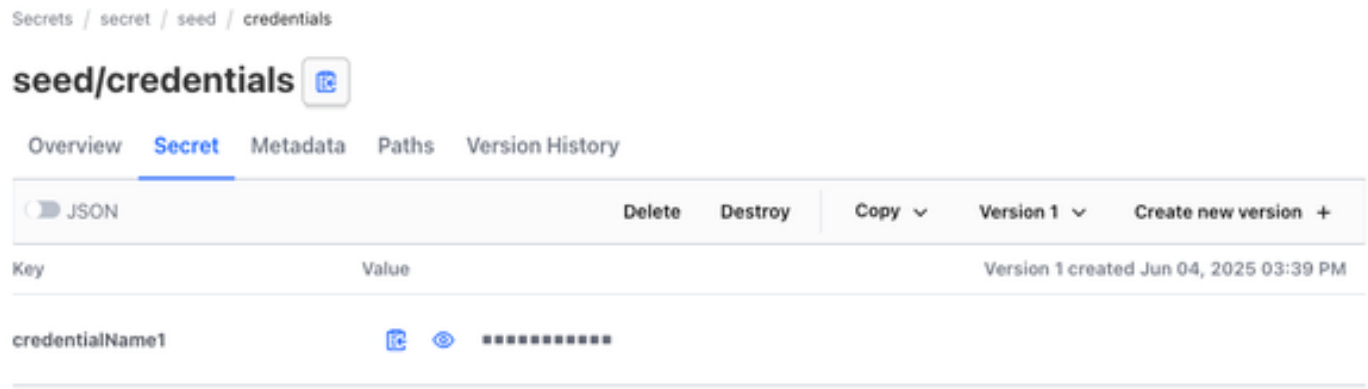
6. 「保存」をクリックします。これで、シークレットがHashiCorp Vaultに保存されます。



Credentials

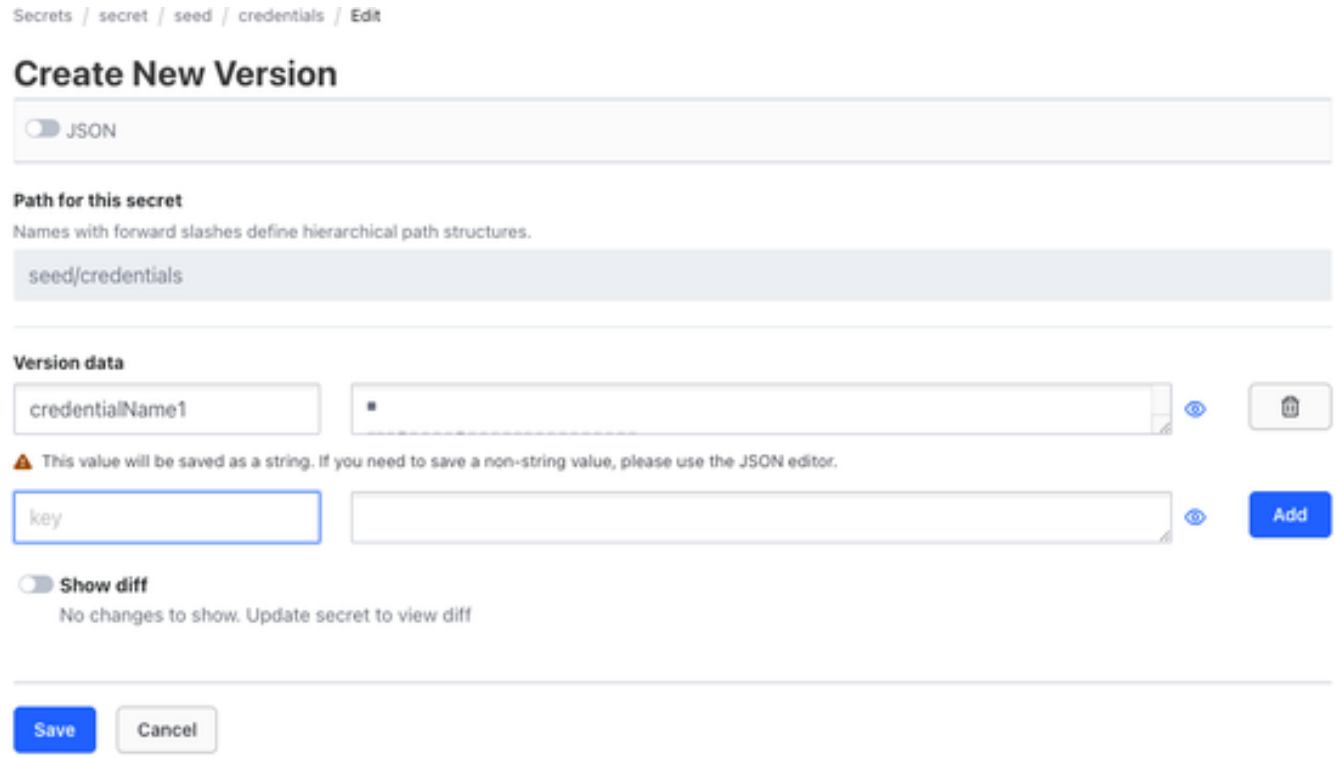
HashiCorp Vaultへの資格情報の追加

1. HashiCorp Vaultインスタンスにログインします。



資格情報の追加

2. すでに作成されているシークレット「シークレット/シード/クレデンシャル」に移動します。



バージョンの作成

3. 「新規バージョンの作成」をクリックします。

4. 必要に応じて任意の数のキーと値のペアを指定して、新しいシークレットを追加します。

5. Saveをクリックします。

デフォルトのクレデンシャルを使用したCX Cloudシードファイル

- シードファイルの簡素化:Hashicorp Vaultで設定されたクレデンシャルを使用する場合は、機密情報を省略してシードファイルを簡素化します
- IPアドレスまたはホスト名のみを指定する：ユーザはシードファイルでIPアドレスまたはホスト名のみを渡すことができ、他のフィールドは空白のままにします

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

IPまたはホスト名

- HashiCorpの資格情報とシードファイルの資格情報の両方を使用する：シードファイル内の一部のデバイスに対する資格情報を指定する一方で、他のデバイスに対する資格情報の管理はボールトに依存して行います

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

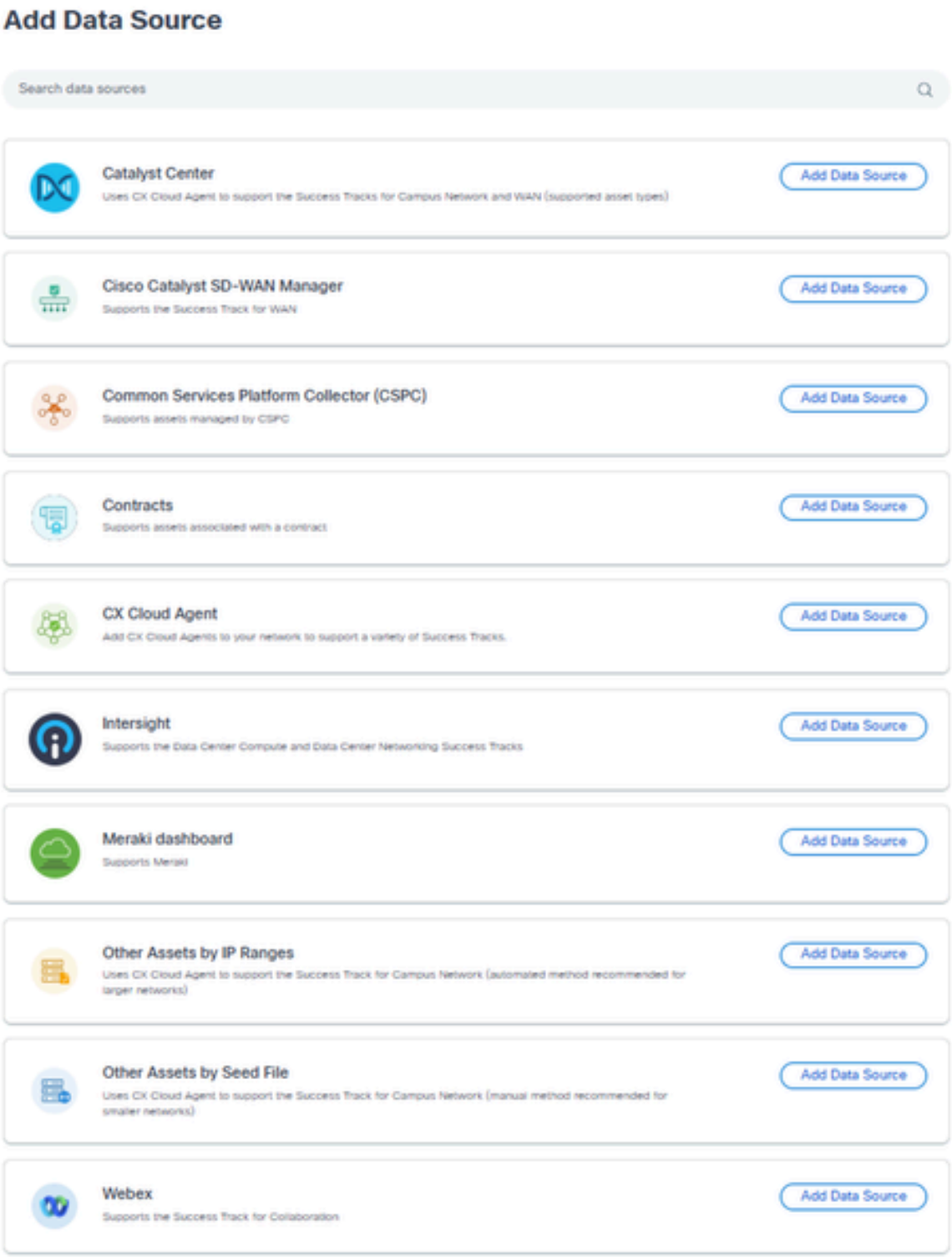
IPまたはホスト名

Catalyst Centerをデータソースとして追加

スーパー管理者ユーザロールを持つユーザは、Catalyst Centerデータソースを追加できます。

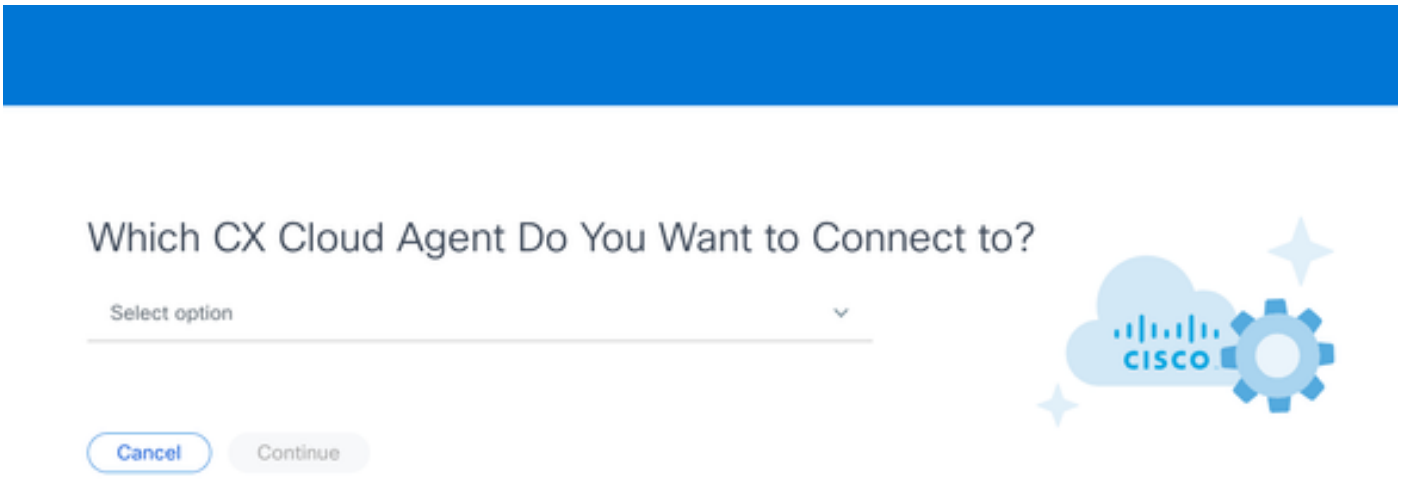
Catalyst Centerをデータソースとして追加するには、次の手順を実行します。

1. 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。
2. Add Data Sourceをクリックします。データソースの追加ページが表示されます。



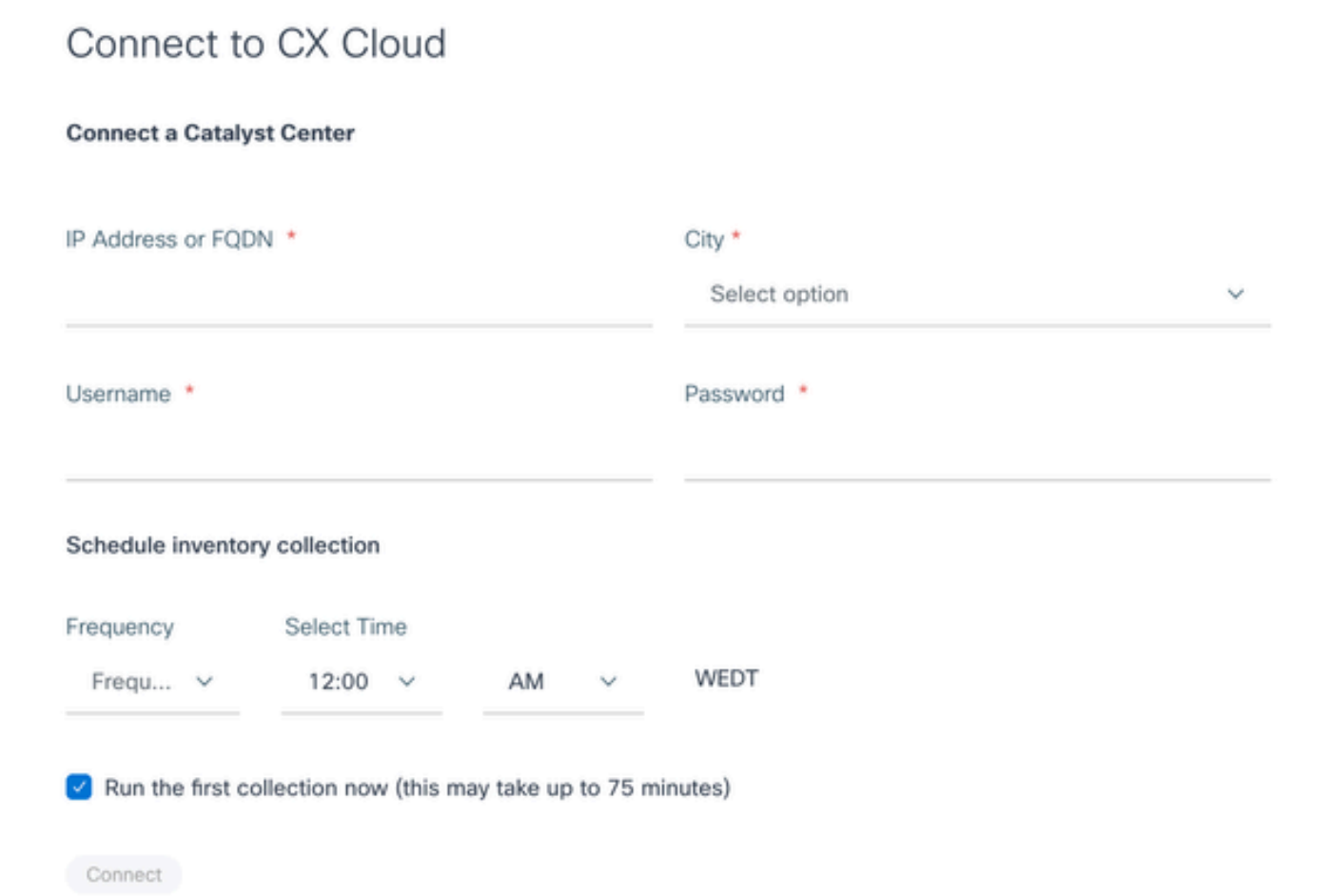
データソースの追加

3. Catalyst CenterオプションからAdd Data Sourceをクリックします。



CXエージェントの選択

4. Which CX Agent Do You Want to Connect toドロップダウンリストから、CXエージェントを選択します。
5. [Continue] をクリックします。Connect to CX Cloudウィンドウが開きます。



周波数

6. 次の詳細を入力します。

- 仮想IPアドレスまたはFQDN（Catalyst CenterのIPアドレス）
- 市（Catalystセンターの場所）
- ユーザ名
- Password
- [頻度]と[時間の選択]は、CXエージェントが[インベントリ収集のスケジュール]セクションでネットワークスキャンを実行する頻度を指定します

注意：コレクションを今すぐ実行するには、「最初のコレクションを今すぐ実行」チェック・ボックスを選択します。

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

データソースとしてのSolarWinds®の追加

注:SolarWinds®データソースを追加する必要がある場合は、シスコサポートにお問い合わせください。

BCS/LCSのお客様は、CX Agent機能を使用してSolarWinds®を外部統合できるようになりました。自動化の向上により、透過性の向上、管理性の向上、ユーザー・エクスペリエンスの向上が実現します。CX Agentは、インベントリやその他の必要なデータを収集し、Operational Insights Collectorによって生成された最新のレポートと形式、データの完全性、データの正確性に関して一貫性のある各種レポートを生成します。CX Agentは、BCS/LCSの顧客がSolarwinds®からデータを収集するためにOICをCX Agentに置きき換かせることによって、Solar®との統合をサポートできます。Solarwinds®データソースを含むこの機能は、BCS/LCSのお客様だけが利用できます。

最初の収集の前に、CXエージェントをBCS転送で設定する必要があります。設定しないと、ファイルは未処理のままになります。BCS転送の構成の詳細については、「CX Agent for BCS or LCSの構成」のセクションを参照してください。

注：

- 同じSolarWinds®インスタンスの複数のコレクションが前のファイルを上書きします（後のアップロードが優先）
- 複数のソースがサポートされていますが、各SolarWinds®インスタンスには一意のIPとアプライアンスIDが必要です

他のアセットをデータソースとして追加する

テレメトリの収集は、Catalyst Centerで管理されていないデバイスにも拡張され、ユーザはテレメトリに由来する洞察や分析を表示して、幅広いデバイスと対話できます。CXエージェントの初期設定後、CX Cloudが監視するインフラストラクチャ内の20の追加のCatalystセンターに接続するようにCXエージェントを構成できます。

CX Cloudに組み込むデバイスを識別するには、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エージェントでスキャンするIP範囲を指定します。どちらの方法も、ディスカバリの目的ではSimple Network Management Protocol(SNMP)を使用し、接続の目的ではSecure Shell(SSH)を使用します。適切に設定して、テレメトリ収集を正常に行う必要があります。

他のアセットをデータソースとして追加するには、次のいずれかのオプションを使用します。

- 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する
- IPアドレスの範囲を指定します

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が使用されます。SNMPにはさまざまなバージョンがありますが、CX AgentはSNMPv2cとSNMPv3をサポートし、一方または両方のバージョンを構成できます。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の間の接続を有効にするには、同じ情報をユーザが入力する必要があります。この情報の詳細については、次に説明します。

SNMPv2cとSNMPv3は、セキュリティとリモート設定モデルが異なります。SNMPV3では、SHA暗号化をサポートする拡張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いて、SNMPv2cではなくSNMPv3を設定することが推奨されます。両方のバージョンのSNMPがユーザーによって構成されている場合、CX AgentはデフォルトでSNMPv3を使用してそれぞれのデバイスと通信しようと試み、通信が正常にネゴシエートできない場合は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。 適切な組み込みサポートがない個別のレガシー資産の場合を除き、SSHv2を使用する必要があります。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い場合、テレメトリデータと基盤となる資産は、SSHv1に依存するとこれらの脆弱性のために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（ユーザ名やパスワードなど）は暗号化されないため、セキュリティが強化されていなくてもセキュリティ侵害に対して脆弱です。

デバイスのテレメトリ処理の制限

デバイスのテレメトリデータを処理する際には、次の制限事項があります。

- 一部のデバイスは、Collection Summaryで到達可能と表示されていても、CX Cloud Assetsページでは表示されません。
- 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Catalyst Centerインベントリにも含まれている場合、そのデバイスはCatalyst 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範囲エントリ内の各デバイスは、重複を避けるためにスキップされます。

- Cisco IP Phoneは、CX AgentによるデータCX Cloudでサポートされていません。その結果、Cisco IP Phoneは資産リストに表示されません。

シードファイルを使用して他のアセットを追加する

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.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、テレメトリがCXエージェントによって収集される必要があ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キャプチャされます。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エージェントはデバイスへの接続を試みますが、PIDまたはシリアル番号を特定できない場合は、各デバイスを処理して資産ページに表示できない可能性があります。

セミコロンで始まるシードファイルの行はすべて無視されます。シードファイルのヘッダー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。

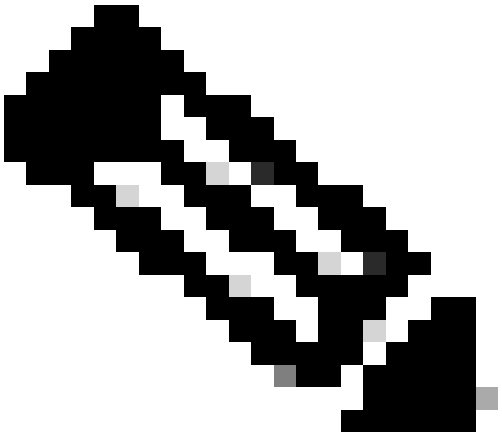
Common Services Platform Collector(CSPC)シードファイルは、標準のCX Cloudシードファイルと同じ方法でアップロードできます。また、必要な再フォーマットはすべてCX Cloudで管理されます。

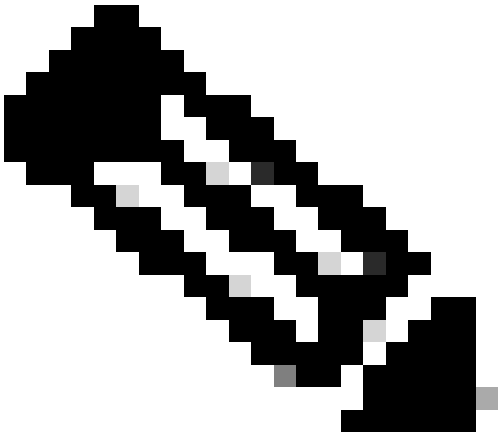
CX Agent v3.1以降では、CSPC形式またはCX形式のいずれかでシードファイルをアップロードできます。以前のバージョンのCX Agentでは、CX形式のシードファイルのみがサポートされています。

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。

次の表に、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ます。

シードファイル列	列ヘッダー/識別子	柱の目的
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エージェントで必要とされ、お客様のネットワーク内の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、セキュリティ上の理由からsnmpv3を使用することを推奨します。
C	snmpRo: col#=3が「	特定のデバイスに対してSNMPv2の従来のバ

シードファイル列	列ヘッダー/識別子	柱の目的
	snmpv2c」として選択されている場合は必須	リアントを選択した場合は、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。
D	snmpv3UserName:col#=3が「snmpv3」として選択されている場合は必須	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。
E	snmpv3AuthAlgorithm：値はMD5またはSHAです。	SNMPv3プロトコルでは、メッセージダイジェスト(MD5)またはセキュアハッシュアルゴリズム(SHA)による認証が許可されます。 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。  注:MD5は安全でないと見なされており、SHAはMD5をサポートするすべてのデバイスで使用できます。
F	snmpv3AuthPassword：パスワード	デバイスにMD5またはSHA暗号化アルゴリズムが設定されている場合、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	デバイスにSNMPv3プライバシーアルゴリズ

シードファイル列	列ヘッダー/識別子	柱の目的
	DES、3DES	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。  注:Data Encryption Standard（DES；データ暗号規格）で使用されている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ており、Triple Data Encryption Standard（3DES；トリプルデータ暗号規格）は、それをサポートするすべてのデバイスで使用できます。
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、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エージェントがSNMPデータセットを収集するとき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。
J	cliProtocol：値は'telnet'、'sshv1'、'sshv2'です。 空の	コマンドラインインターフェイス(CLI)は、デバイスと直接やり取りすることを目的として

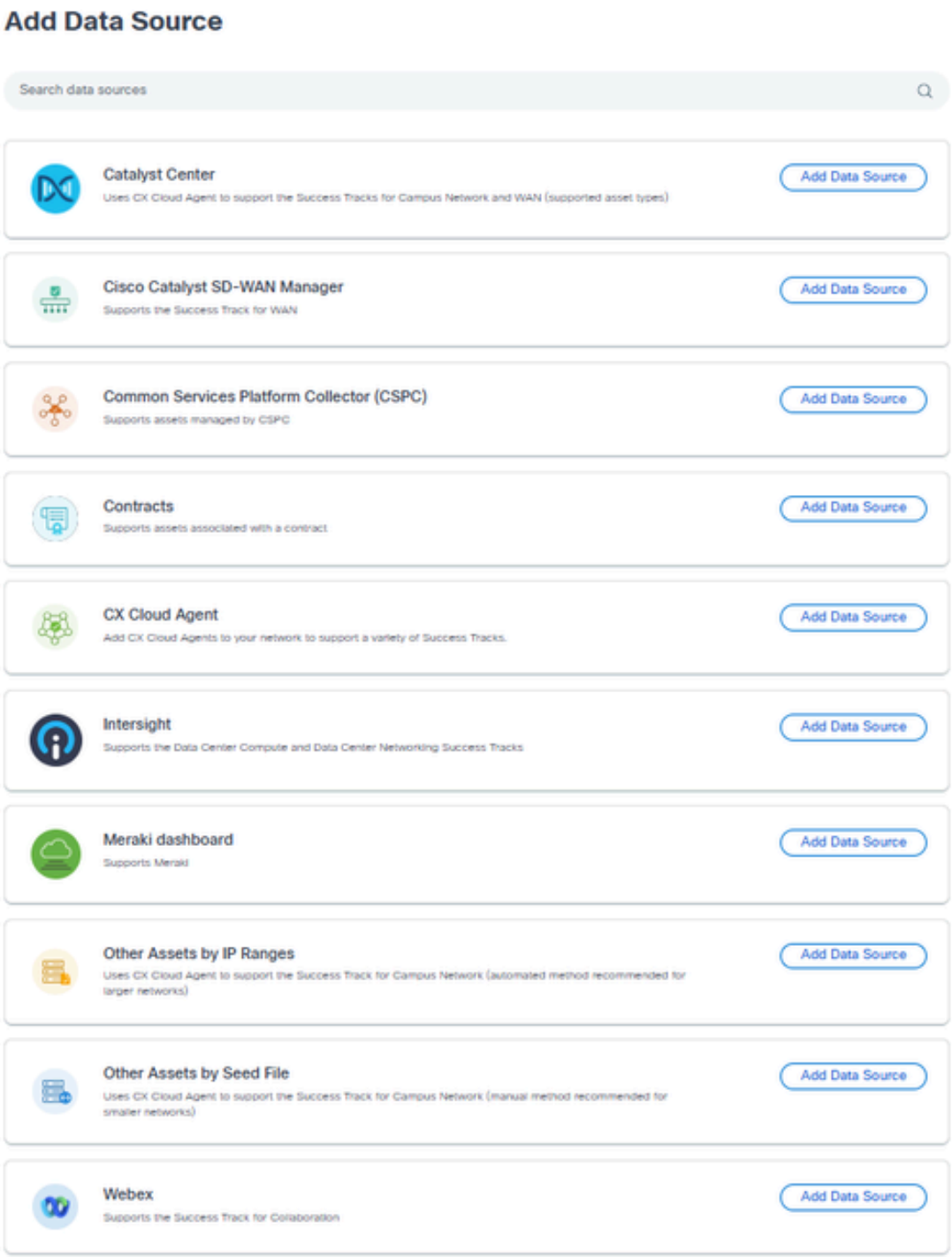
シードファイル列	列ヘッダー/識別子	柱の目的
	場合は、デフォルトで'sshv2'に設定できます	います。CXエージェントは、特定のデバイスのCLI収集にこのプロトコルを使用します。このCLI収集データは、CX Cloud内のアセットおよびその他のインサイトレポートに使用されます。SSHv2が推奨されます。他のネットワークセキュリティ対策がない場合、それ自体では、SSHv1およびTelnetプロトコルは十分なトランスポートセキュリティを提供しません。
K	cliPort:CLIプロトコルポート番号	いずれかのCLIプロトコルを選択した場合は、対応するポート番号を指定する必要があります。たとえば、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収集中のデバイスへの接続時に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)。	デバイスのそれぞれのCLIパスワード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エージェント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	柱の目的
P	将来のサポート（入力は不要）	将来の使用のために予約
Q	将来のサポート（入力は不要）	将来の使用のために予約
R	将来のサポート（入力は不要）	将来の使用のために予約
S	将来のサポート（入力は不要）	将来の使用のために予約

新しいシードファイルを使用してほかのアセットを追加する

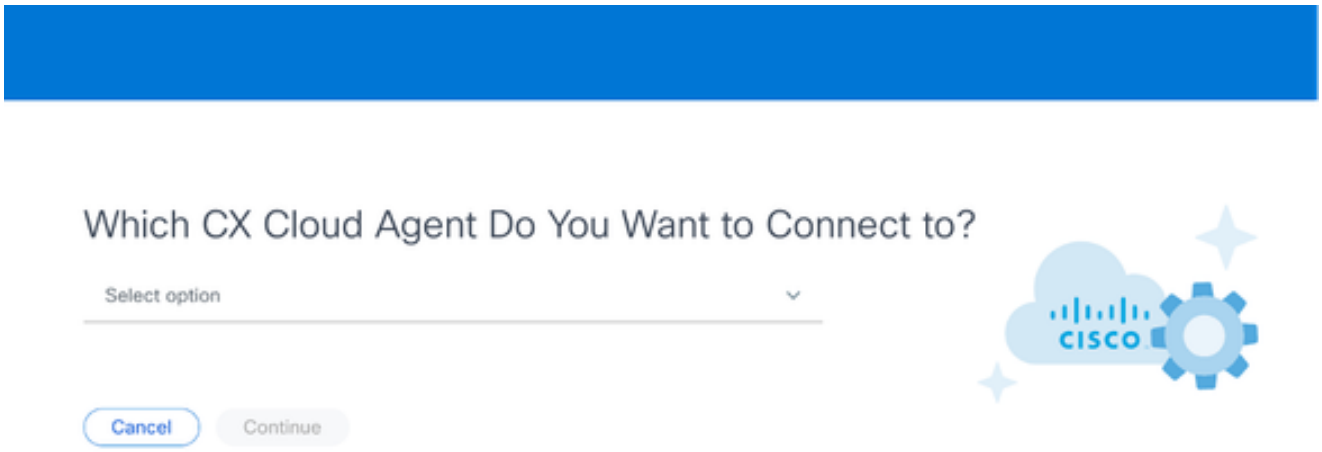
新規シードファイルを使用して他のアセットを追加するには：

1. Admin Center > Data Sourcesウィンドウで、Add Data Sourceをクリックします。



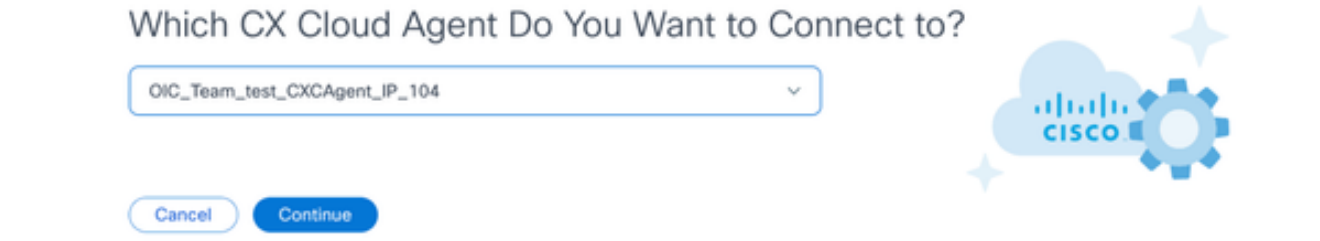
データソースの追加

2. Other Assets by Seed FileオプションからAdd Data Sourceをクリックします。



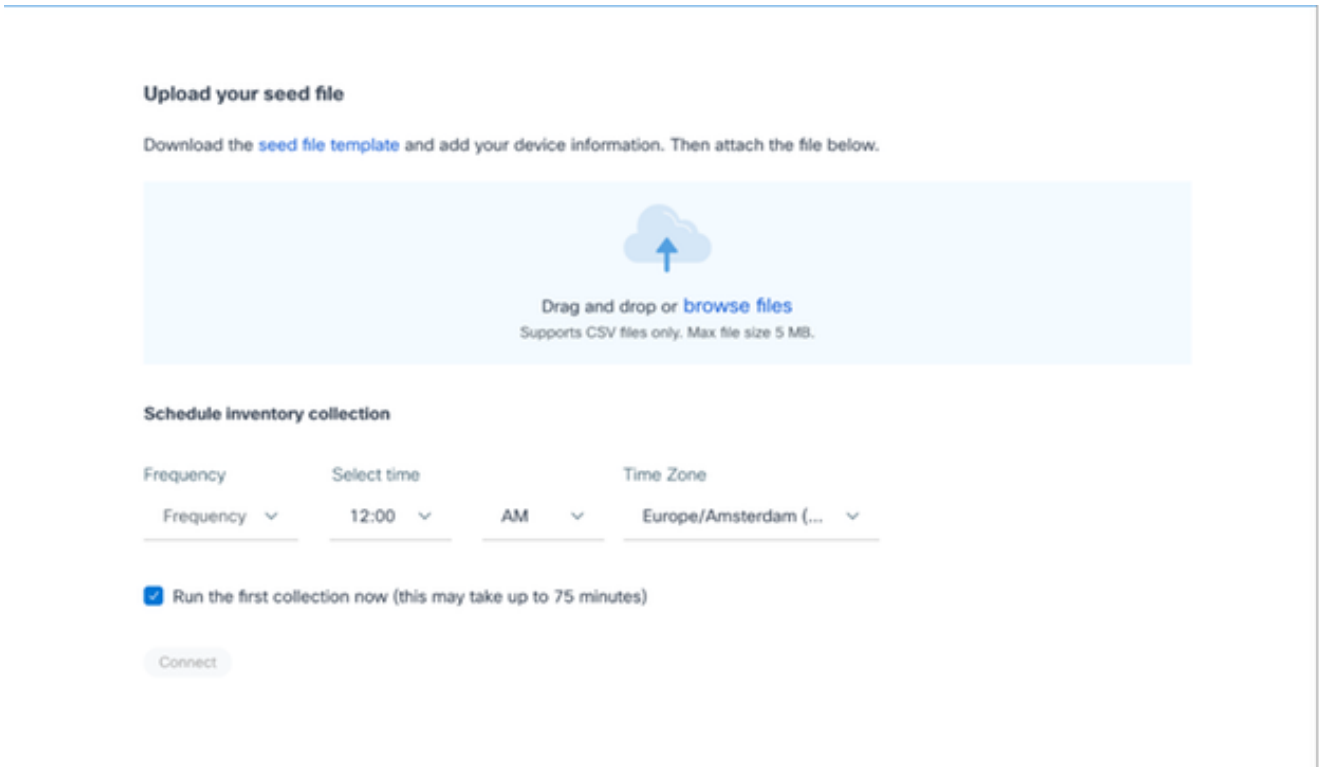
CXエージェントの選択

3. Which CX Cloud Agent Do You Want to Connect toドロップダウンリストから、CX Agentを選択します。



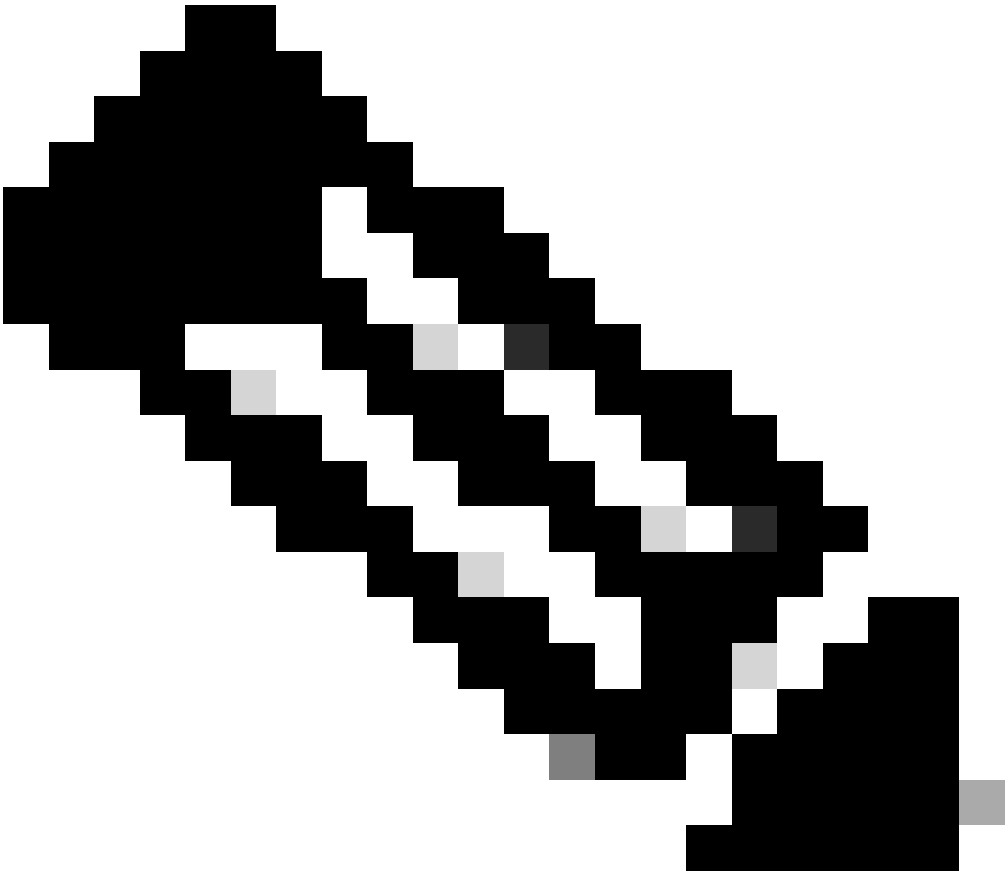
[Continue]

4. [Continue] をクリックします。シードファイルのアップロードページが表示されます。



シードファイルのアップロード

5. ハイパーリンクされたシードファイルテンプレートをクリックして、テンプレートをダウンロードします。
6. ファイルにデータを手動で入力またはインポートします。完了したら、テンプレートを.csvファイルとして保存し、ファイルをCXエージェントにインポートします。
7. .csvファイルをアップロードするには、ファイルの参照をドラッグアンドドロップするかクリックします。
8. 「インベントリ収集のスケジュール設定」セクションに入力します。



注: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、最初のテレメトリコレクション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。最初のテレメトリ接続を実行するには、[最初のコレクションを今すぐ実行する]チェックボックスをオンにします。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。

9. [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。

変更したシードファイルを使用して他のアセットを追加する

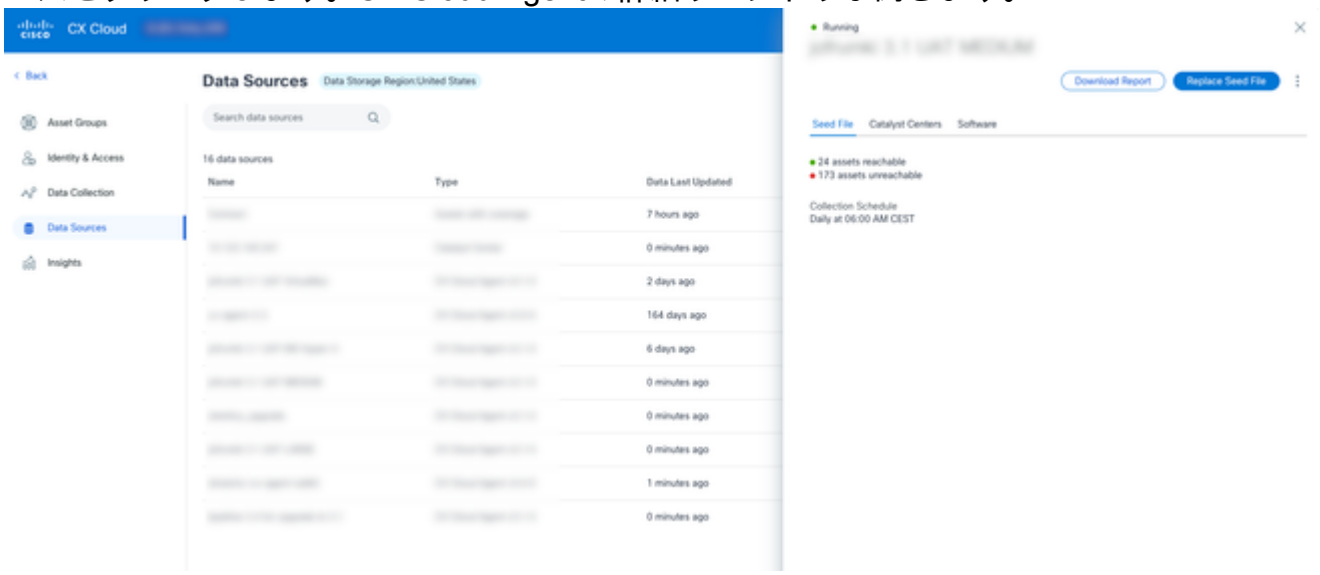
現在のシードファイルを使用してデバイスを追加、変更、または削除するには、次の手順に従います。

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

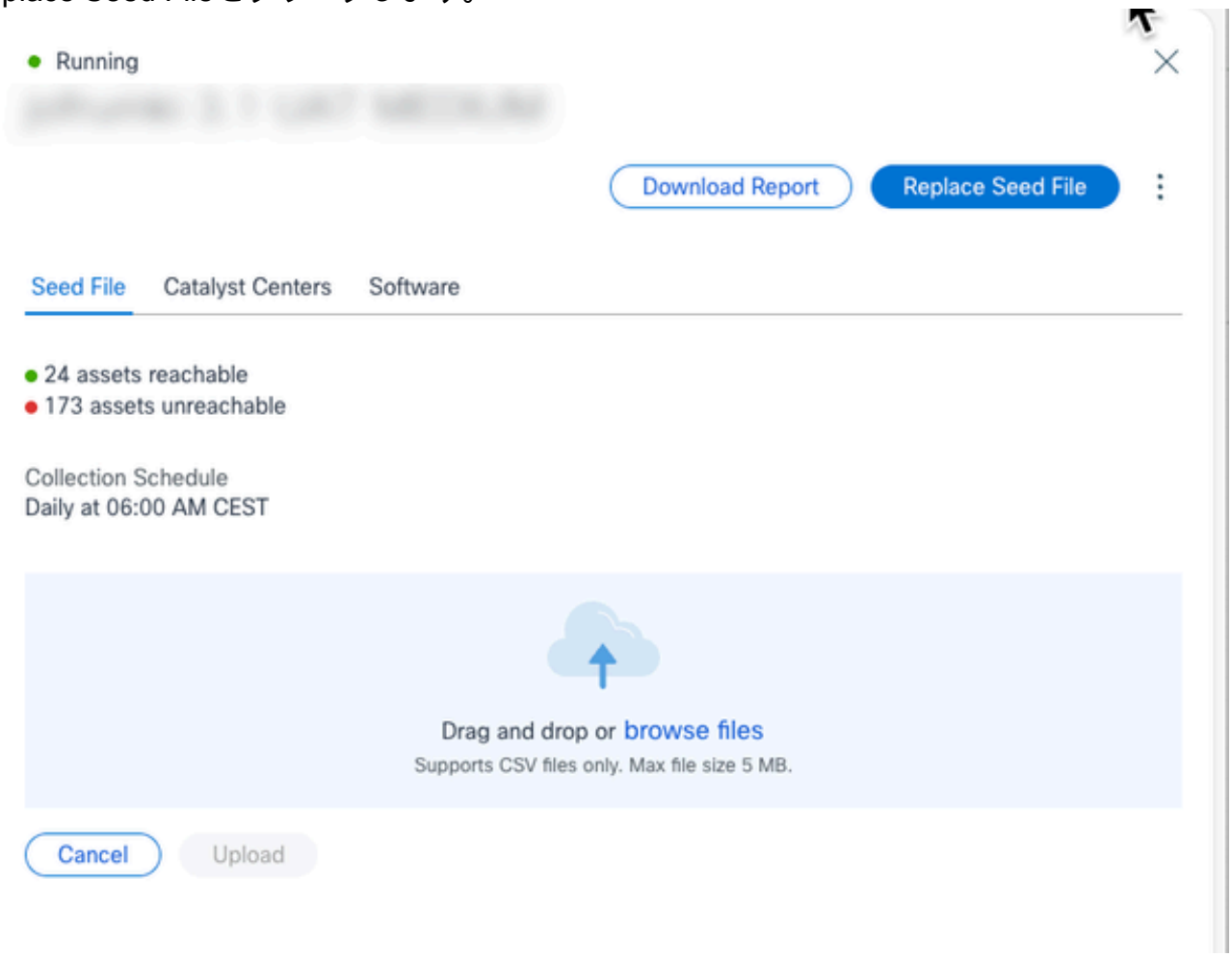
セットを追加してから、ファイルを再ロードします。現在のシードファイルが新しいシードファイルに置き換えられるため、これが必要になります。検出と収集には、アップロードされた最新のシードファイルのみが使用されます。

2. [データソース]ページで、更新されたシードファイルを必要とするCXエージェントデータソースをクリックします。CX Cloud Agentの詳細ウィンドウが開きます。



シード ファイル

3. Replace Seed Fileをクリックします。



4. 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、変更したシードファイルをアップロードします。
5. [Upload] をクリックします。

シードファイルのデフォルトのクレデンシャル

CXエージェントは、お客様がエージェント内でローカルに設定できるデフォルトの認証情報を提供するため、シードファイルに機密パスワードを直接含める必要がなくなります。これにより、機密情報の漏えいが減り、お客様の主な懸念事項に対処することで、セキュリティが強化されます。

IP範囲を使用した他のアセットの追加

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、単一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、SNMPプロトコルを使用してCXエージェントによっ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範囲を選択した場合、参照されるIPアドレスはできるだけ制限され、必要なすべての資産をカバーできます。

- 特定のIPを指定することも、IPのオクテットをワイルドカードで置き換えて範囲を作成することもできます。
- セットアップ時に特定のIPアドレスが、指定したIP範囲に含まれない場合、CXエージェントは、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エージェントはユーザーが指定した認証情報を任意の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エージェントはデバイスに接続を試みますが、PIDまたはシリアル番号を特定できない場合は、各デバイスを処理してAssetsビューに表示できない可能性があります。

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。指定したIP範囲に新しいデバイスを追加または削除する場合、お客様は必ずEdit IP Address Rangeをクリックし(「IP範囲の編集」の項を参照)、オンデマンド· デバイス検出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エージェントの収集インベントリに含める必要があります。

IP範囲を使用してデバイスを追加するには、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

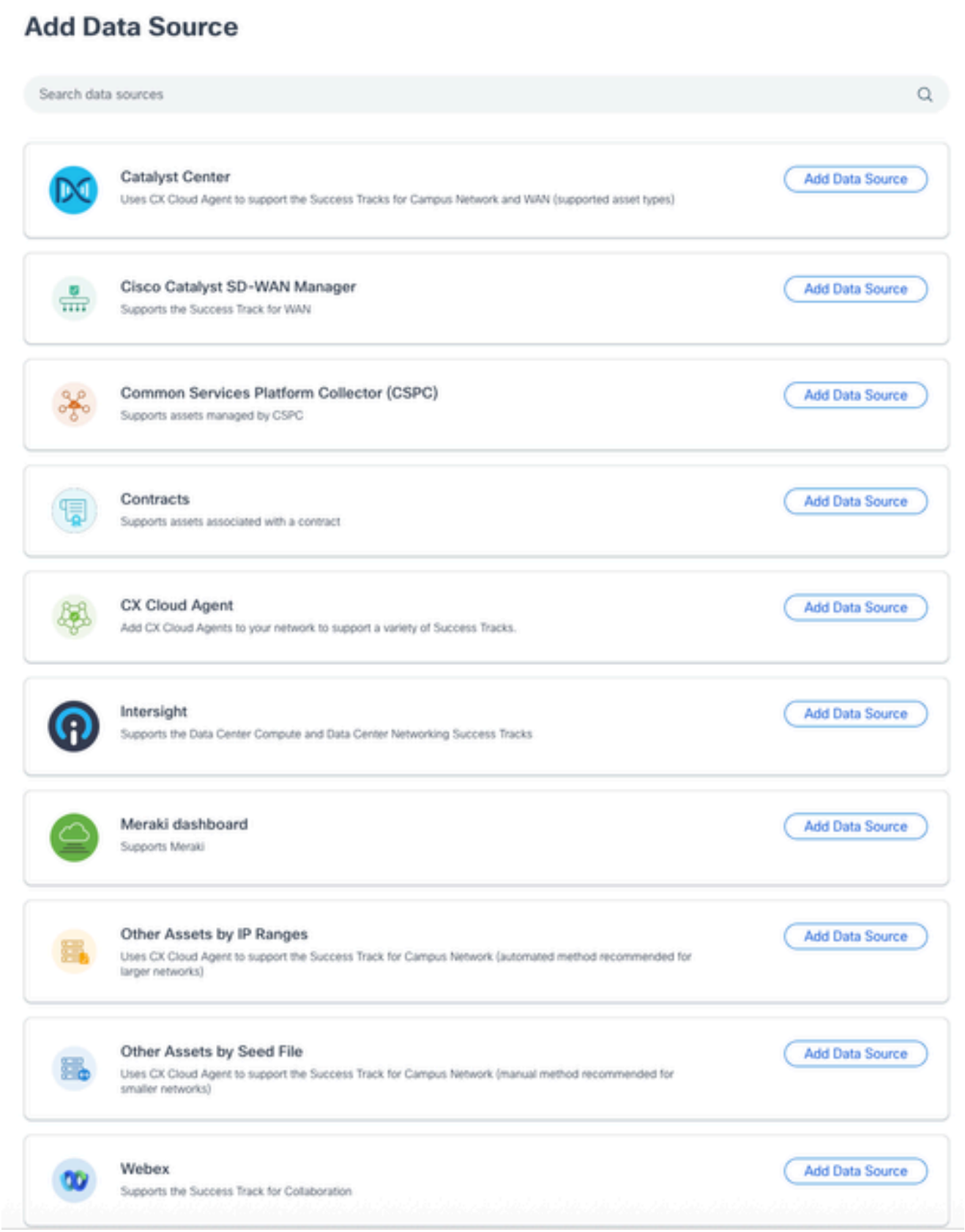
するなど、同じプロトコルに対して複数の選択を行った場合、CX Agentは個々のデバイスの機能に基づいてプロトコルの選択を自動的に自動ネゴシエートします。

IPアドレスを使用してデバイスを接続する際は、SSHバージョンおよびTelnetクレデンシャルとともに、IP範囲内の関連プロトコルがすべて有効であることを確認する必要があります。有効でない場合、接続は失敗します。

IP範囲による他のアセットの追加

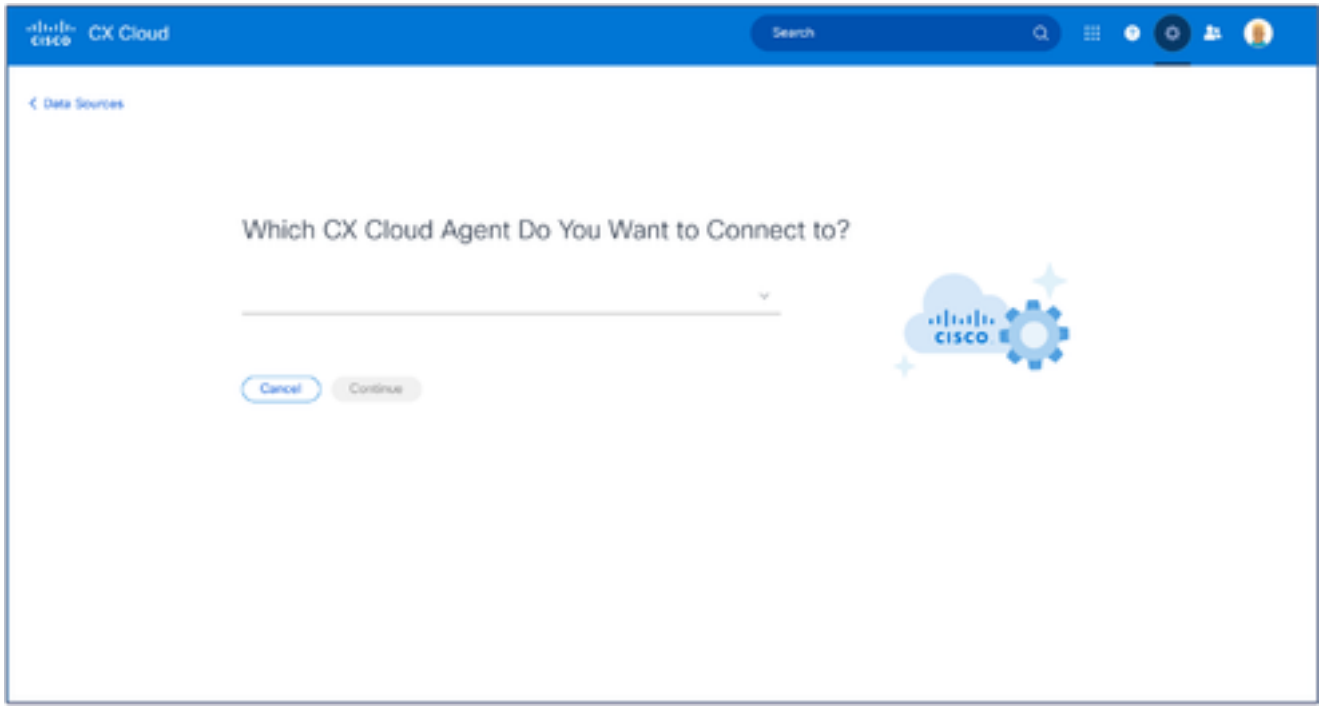
IP範囲を使用してデバイスを追加するには、次の手順に従います。

1. 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。
2. Admin Center > Data Sourcesウィンドウで、Add Data Sourceをクリックします。



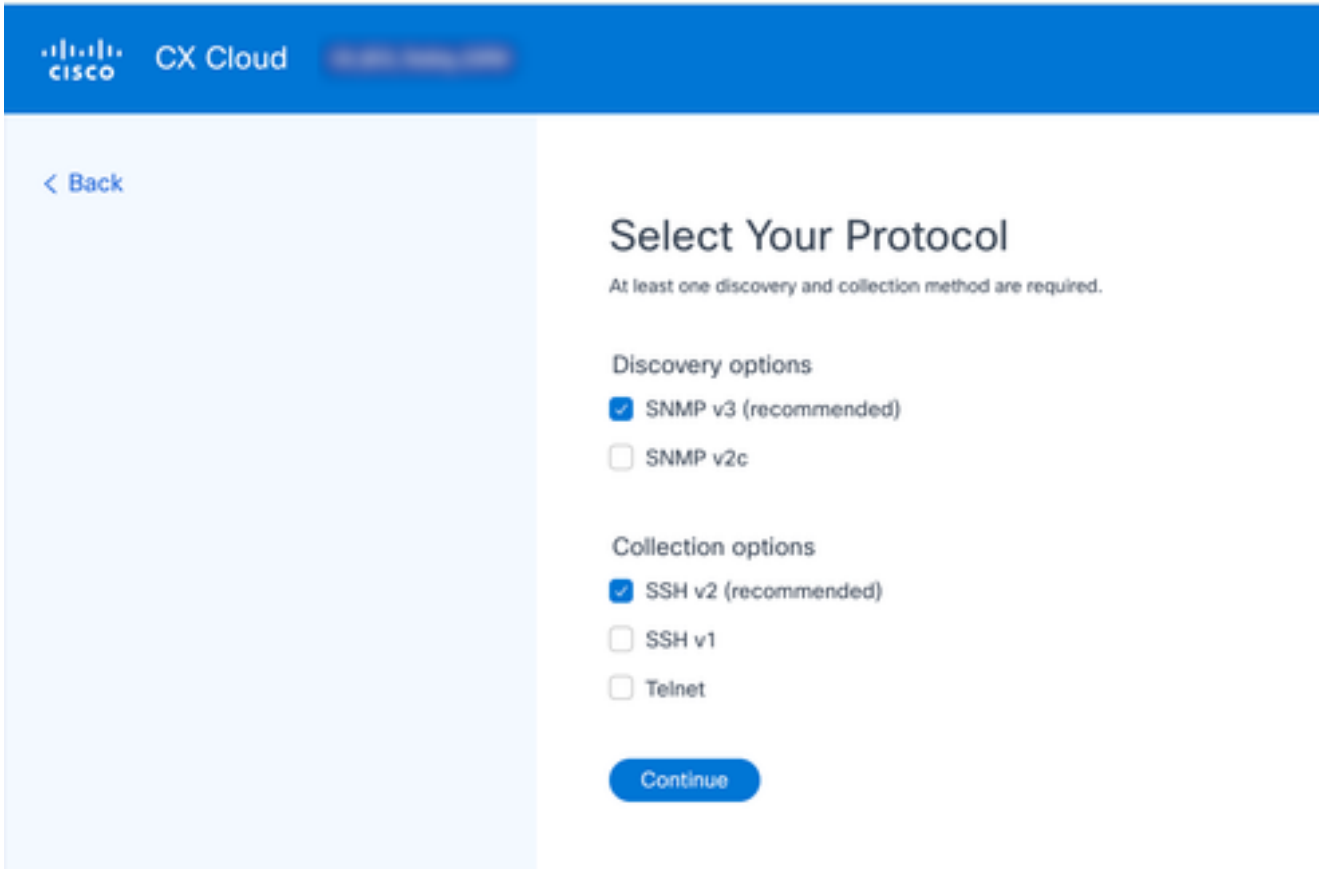
データソースの追加

3. Other Assets by IP RangesオプションでAdd Data Sourceをクリックします。



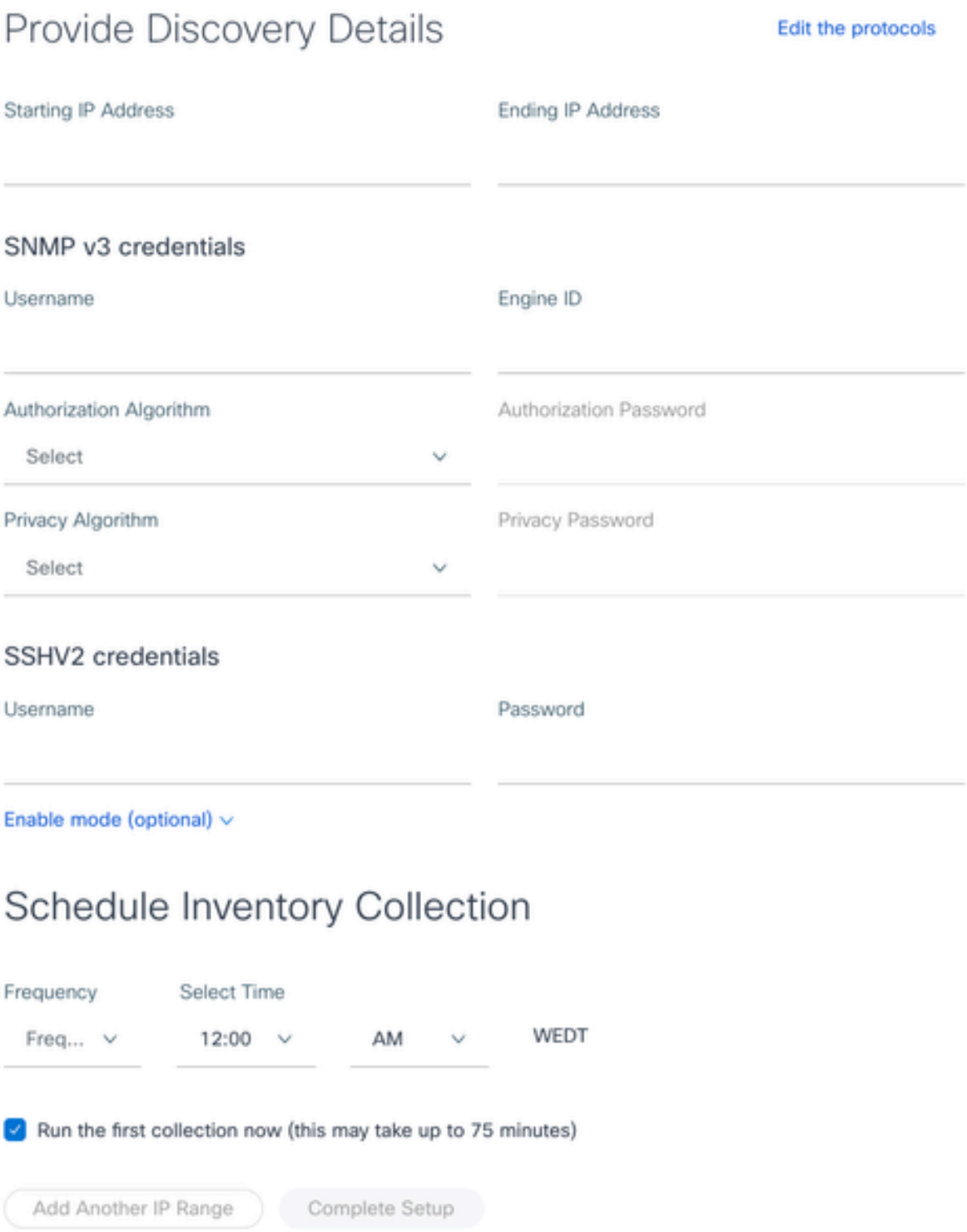
CX Cloud Agentの選択

4. Which CX Cloud Agent Do You Want to Connect toドロップダウンリストから、CX Agentを選択します。
5. [Continue] をクリックします。Select Your Protocolウィンドウが開きます。



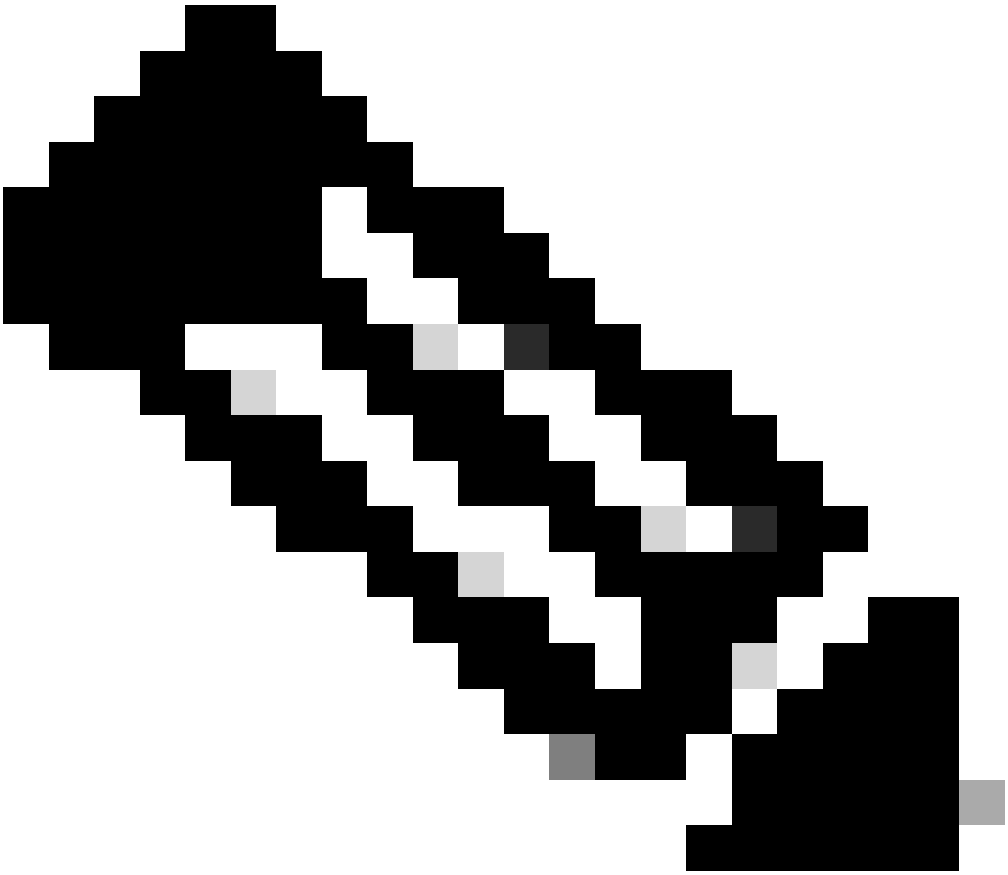
プロトコルの選択

6. Discovery optionsとCollection optionsの適切なチェックボックスをオンにします。
7. [Continue] をクリックします。



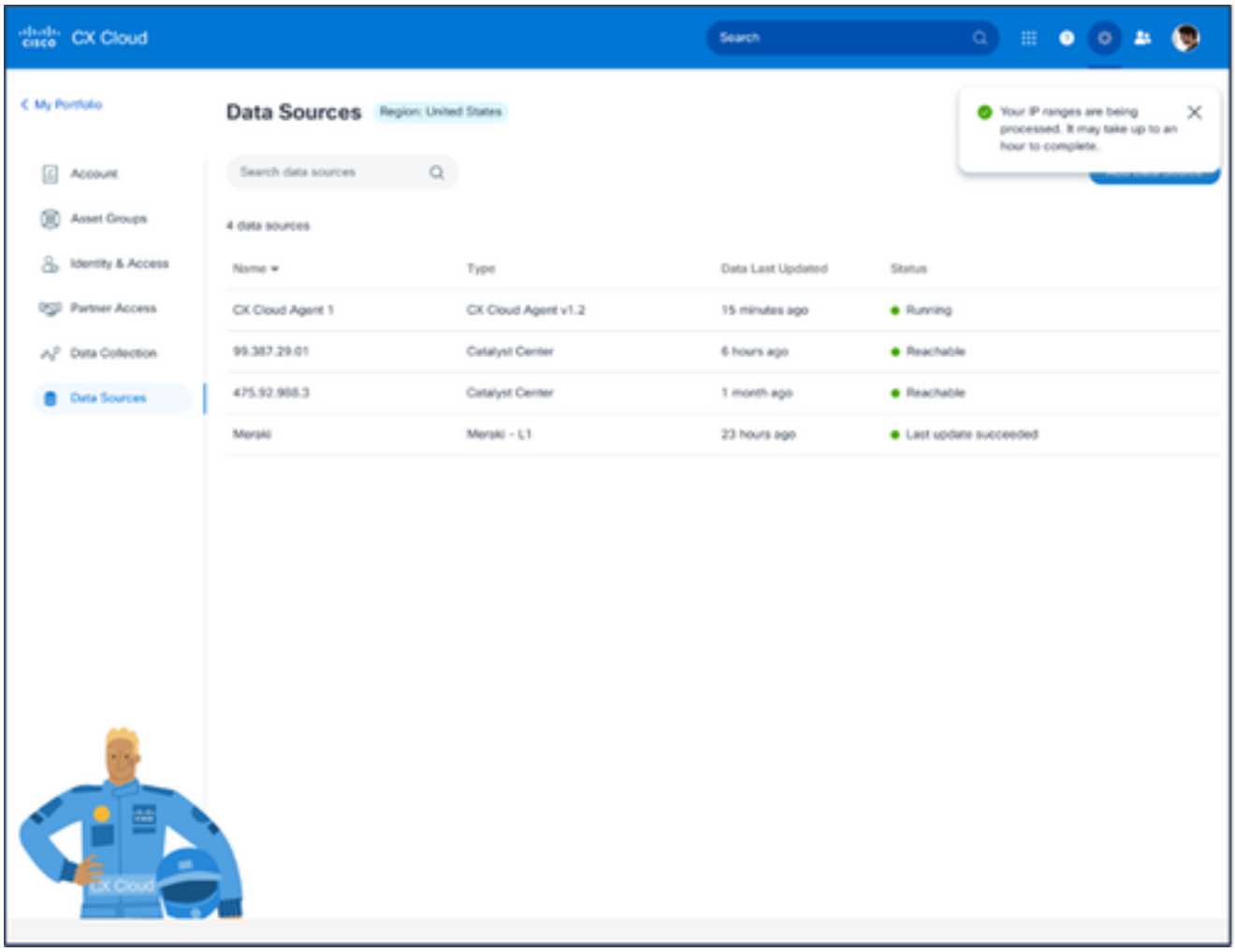
検出の詳細

8. 必要な詳細を「検出の詳細の指定」および「インベントリ収集のスケジュール設定」セクションに入力します。



注：選択したCXエージェントに別のIP範囲を追加するには、[Add Another IP Range]をクリックして[Set Your Protocol]ウィンドウに戻り、このセクションの手順を繰り返します。

9. Complete Setupをクリックします。展開が正常に完了すると、確認が表示されます。

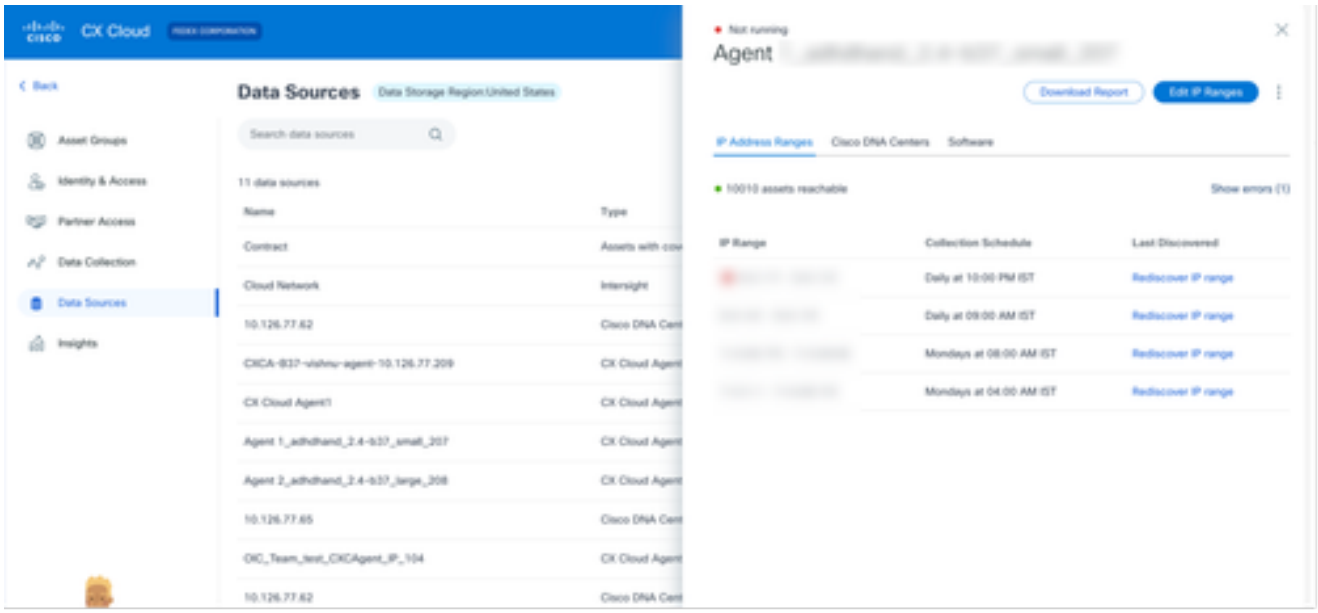


確認メッセージ

IP範囲の編集

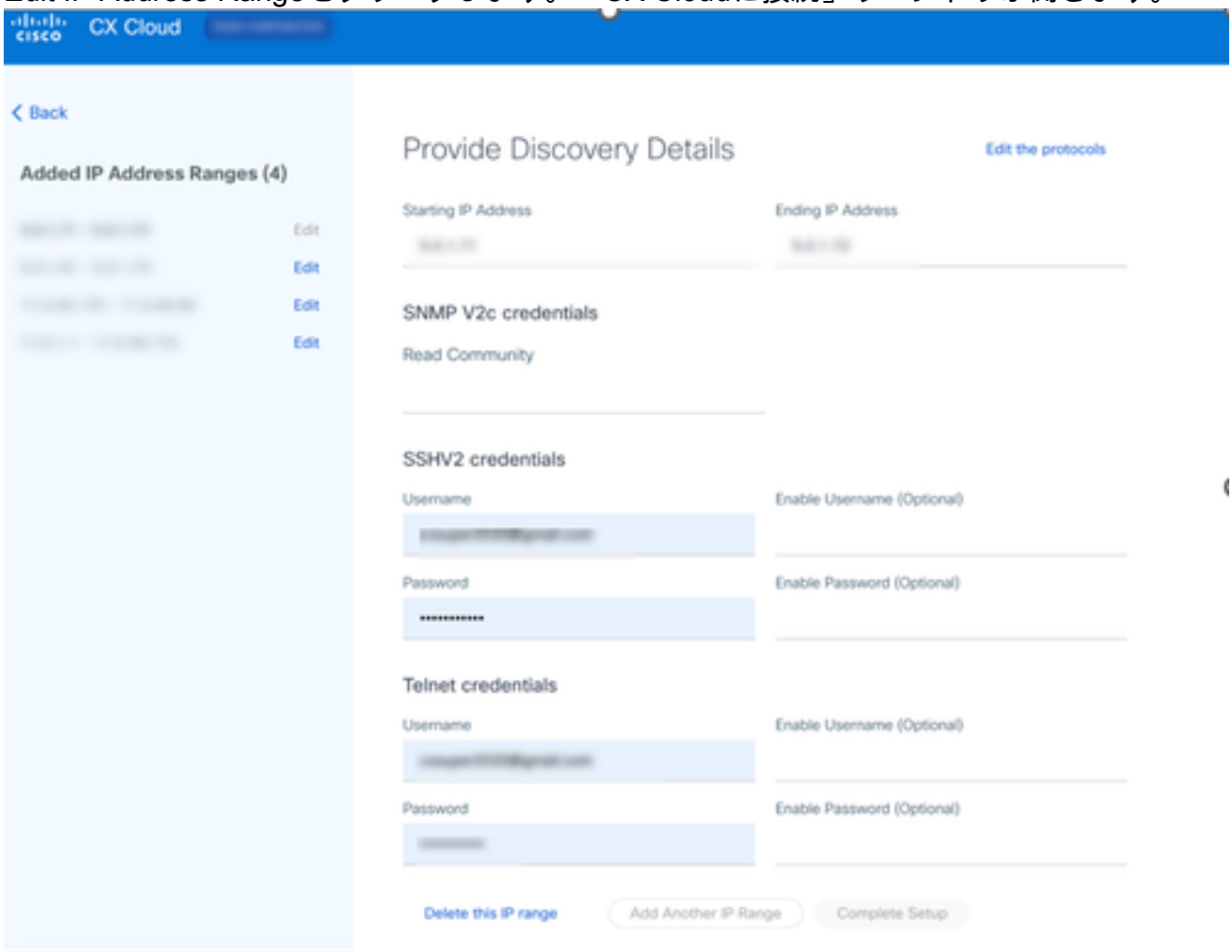
IP範囲を編集するには、次の手順に従います。

1. Data Sourcesウィンドウに移動します。
2. データソースでIP範囲の編集を必要とするCXエージェントをクリックします。詳細ウィンドウが開きます。

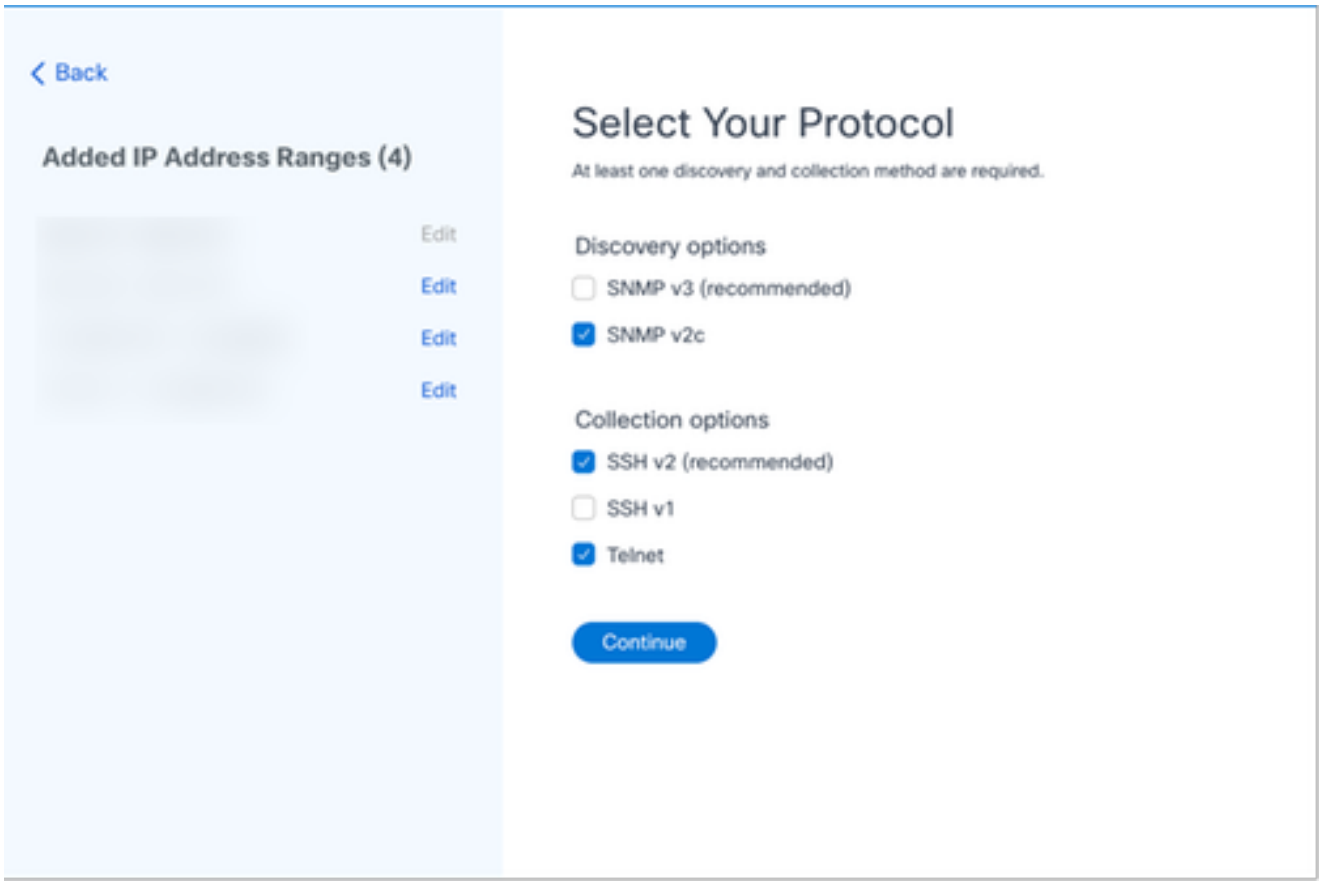


データソース

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。

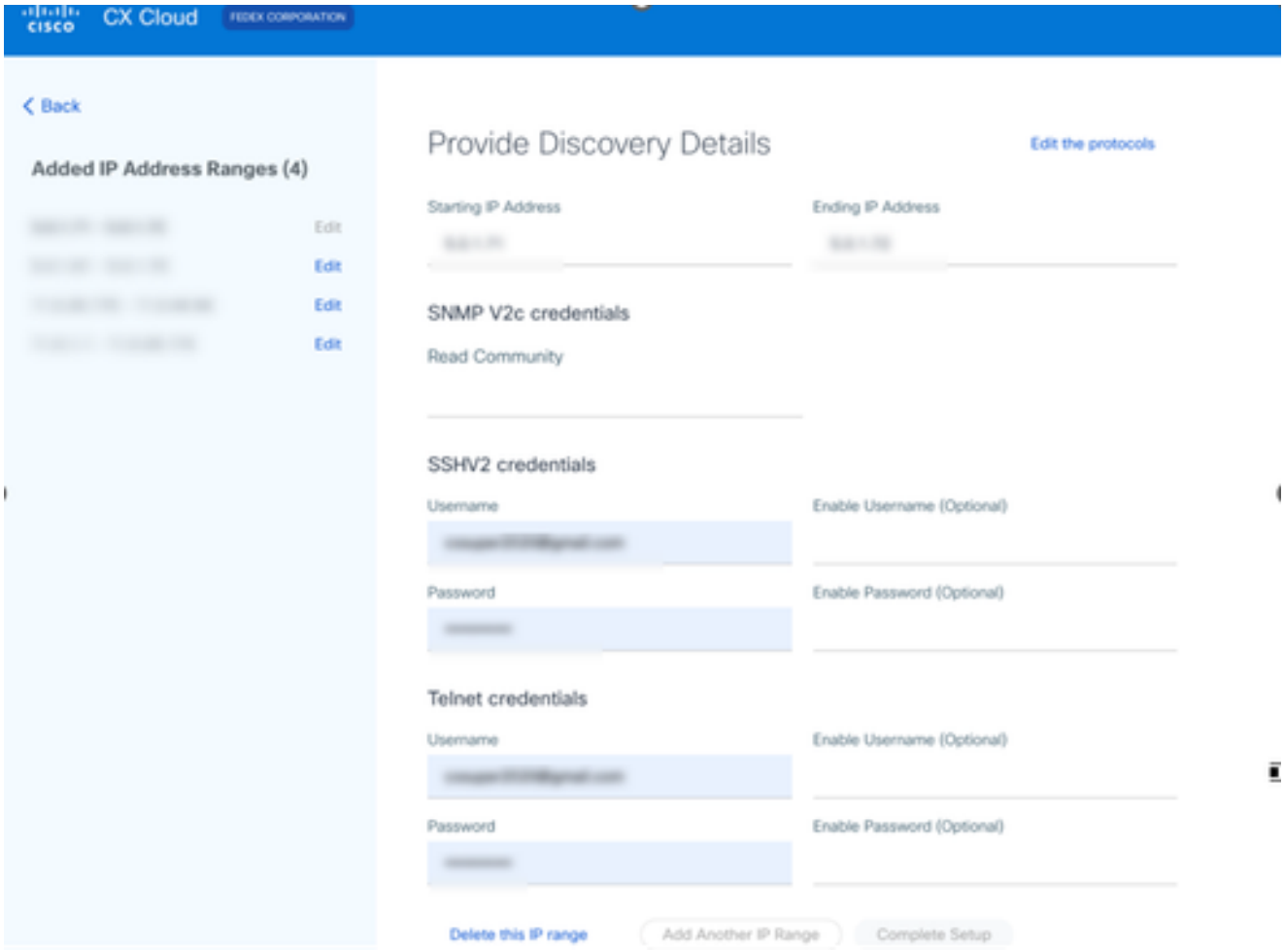


4. Edit the protocolsをクリックします。Select Your Protocolウィンドウが開きます。



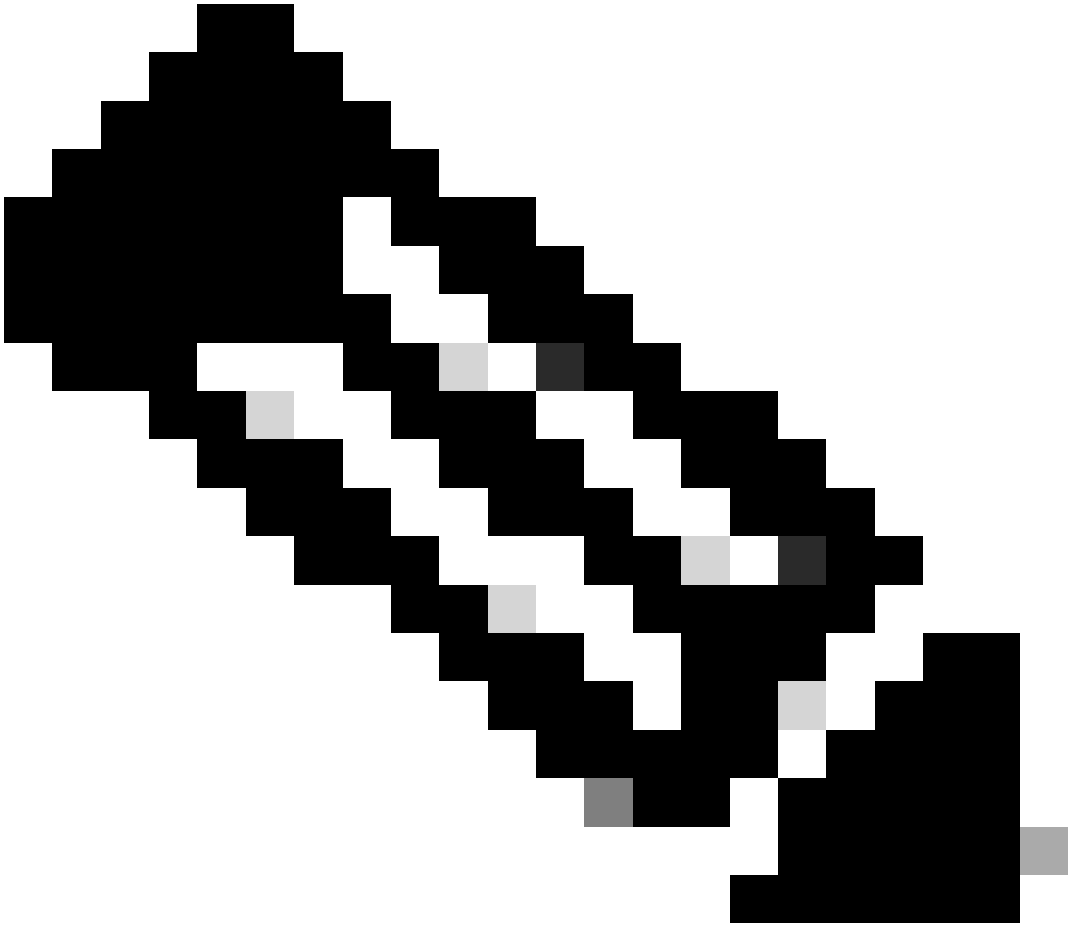
プロトコルの選択

5. 該当するチェックボックスをオンにして該当するプロトコルを選択し、Continueをクリックして、Provide Discovery Detailsウィンドウに戻ります。

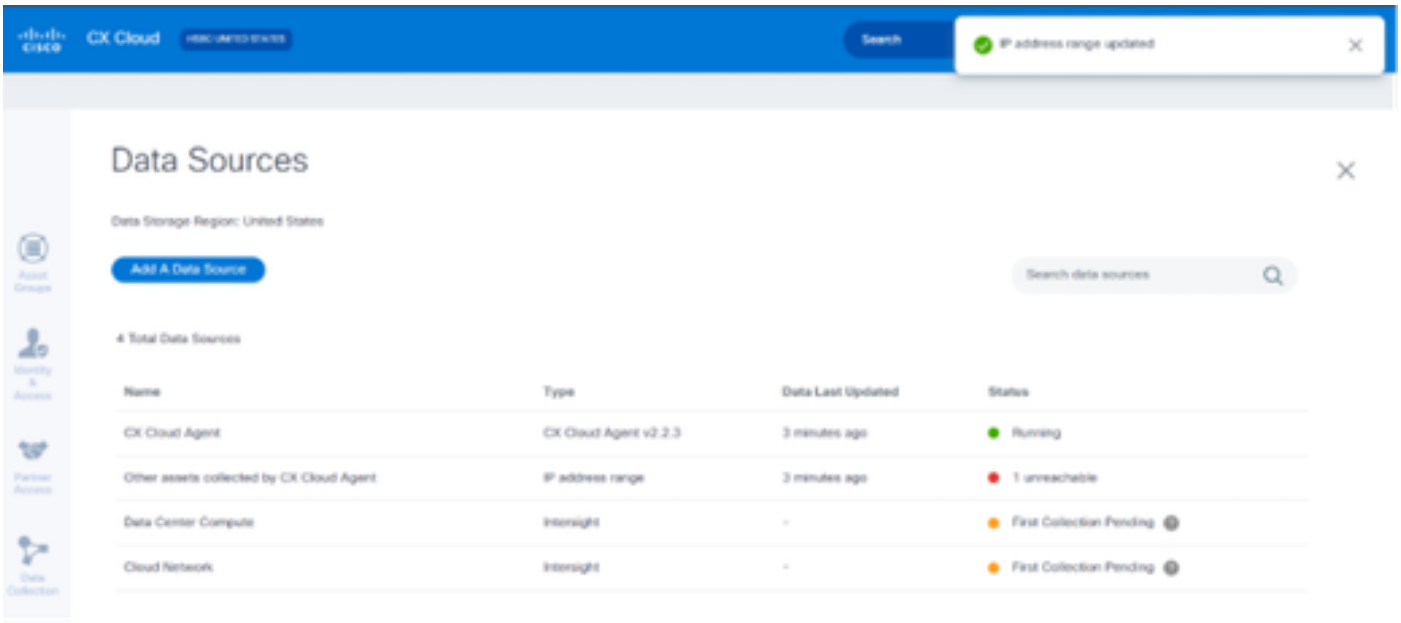


ディスカバリの詳細の提供

6. 必要に応じて詳細を編集し、Complete Setupをクリックします。Data Sourcesウィンドウが開き、新しく追加したIPアドレス範囲の追加を確認するメッセージが表示されます。



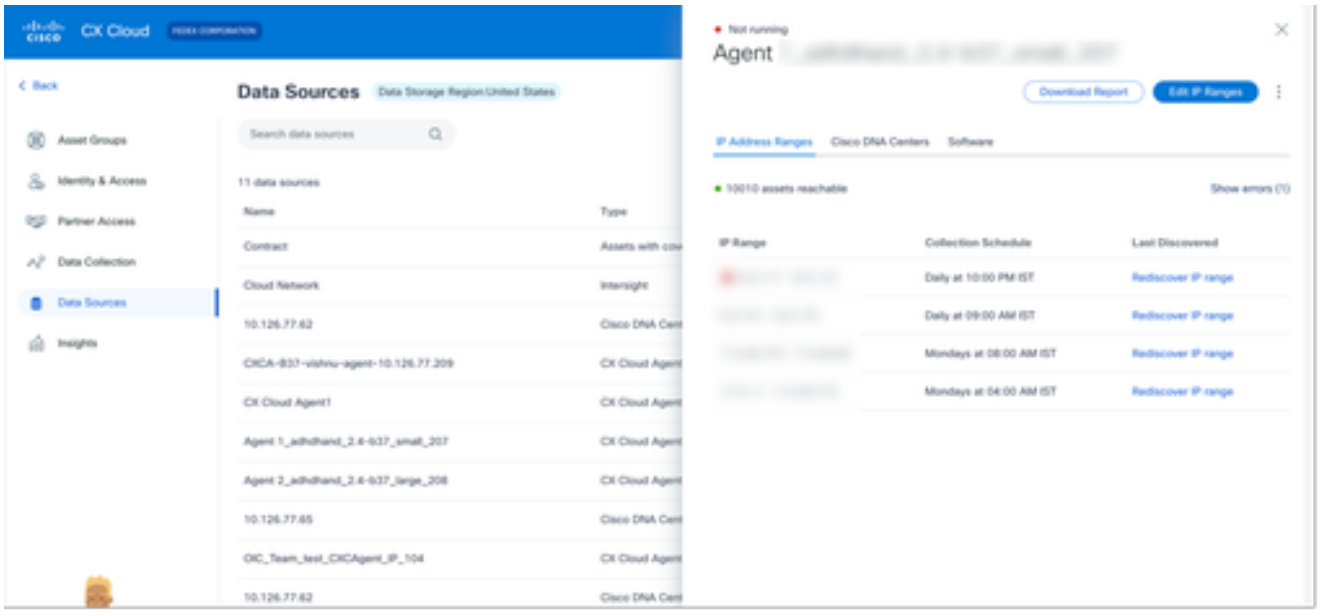
注：この確認メッセージでは、変更された範囲内のデバイスが到達可能かどうか、またはそのクレデンシャルが受け入れられているかどうかは確認されません。この確認は、お客様がディスカバリプロセスを開始したときに行われます。



IP範囲の削除

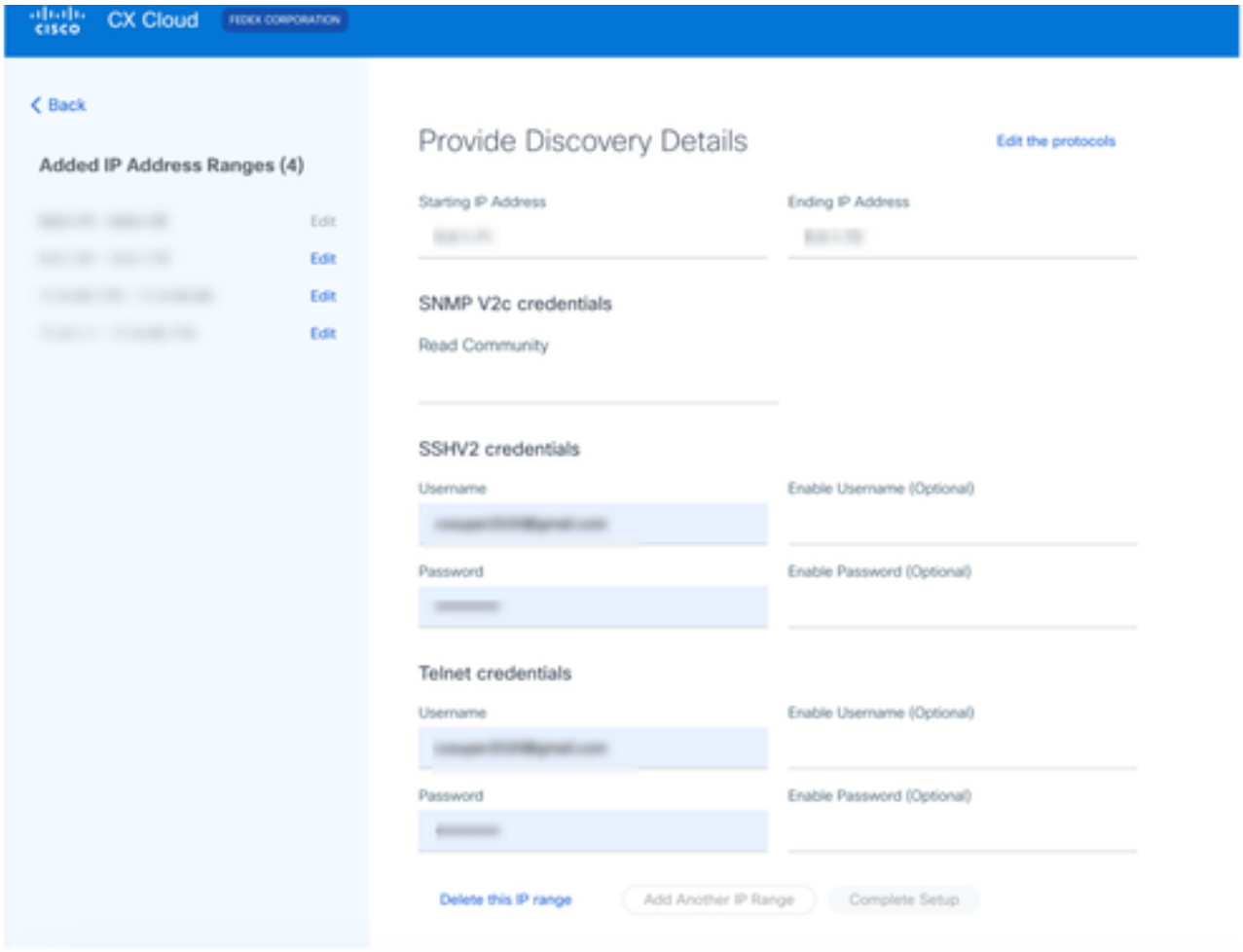
IP範囲を削除するには、次の手順に従います。

1. Data Sourcesウィンドウに移動します。
2. 削除する必要があるIP範囲のCXエージェントを選択します。詳細ウィンドウが開きます。



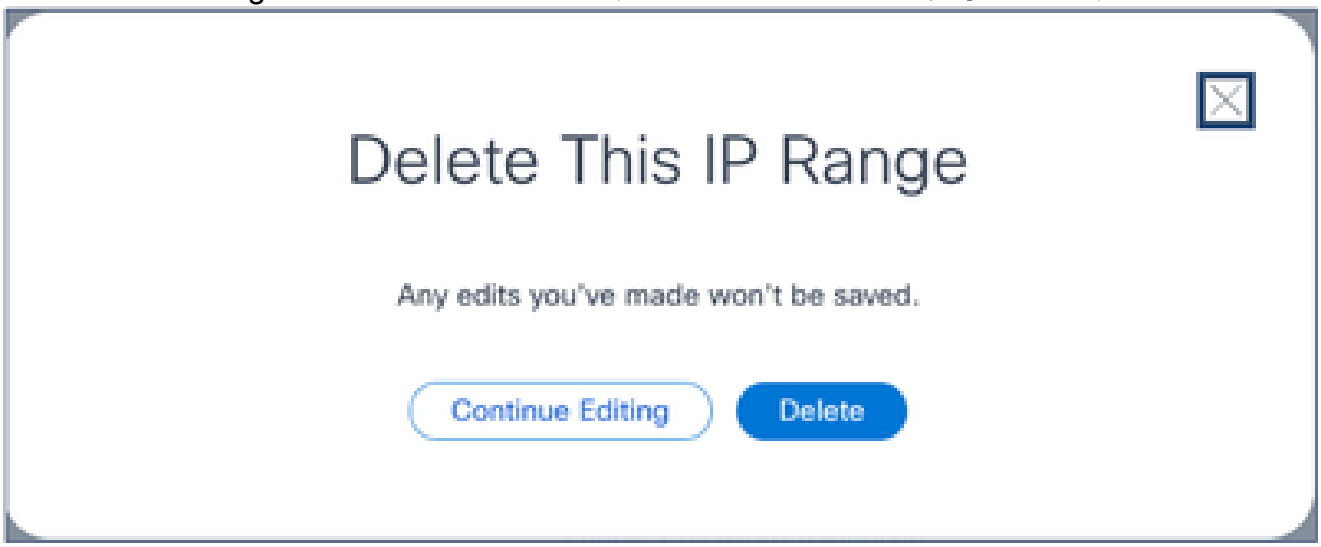
データソース

3. Edit IP Rangesをクリックします。Provide Discovery Detailsウィンドウが開きます。



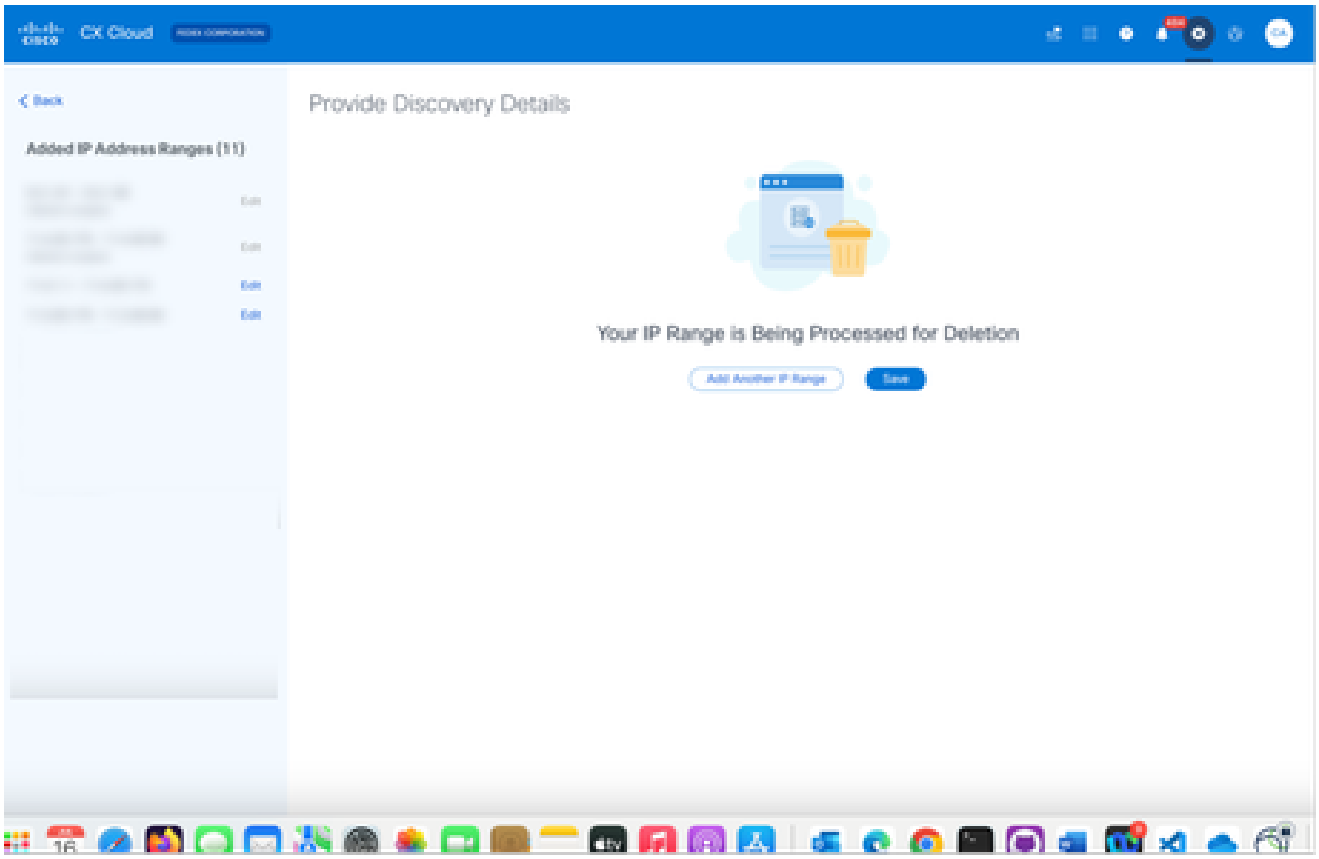
ディスカバリの詳細の提供

4. Delete this IP rangeリンクをクリックします。確認メッセージが表示されます。



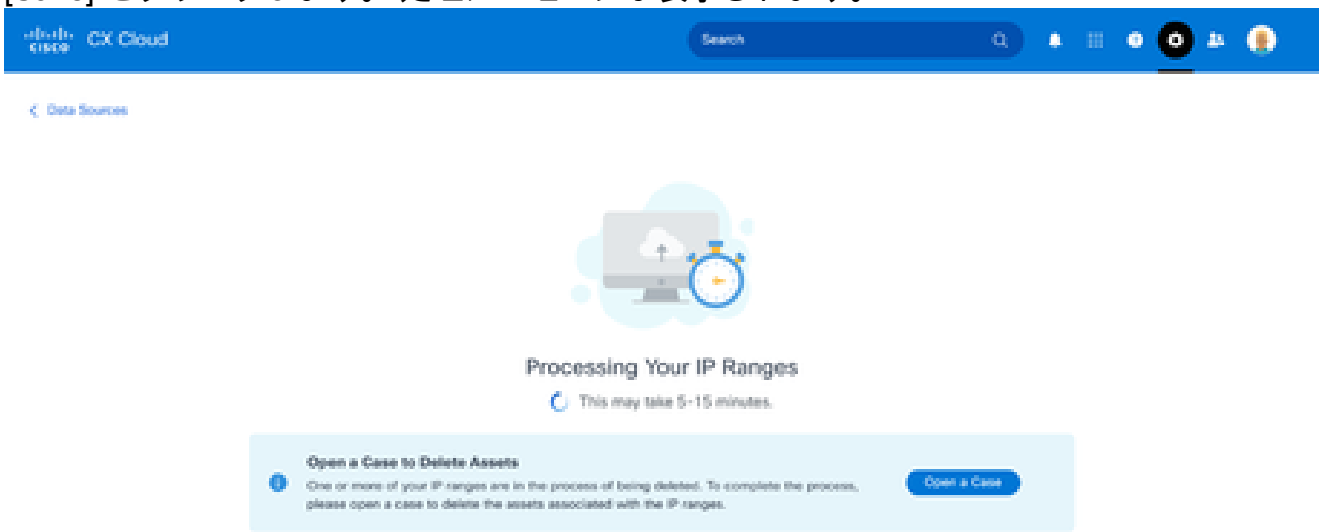
確認削除メッセージ

5. [Delete] をクリックします。



IP範囲の削除

6. [Save] をクリックします。.処理メッセージが表示されます。



7. Open a Caseをクリックしてケースを作成し、IP範囲に関連付けられているアセットを削除します。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。

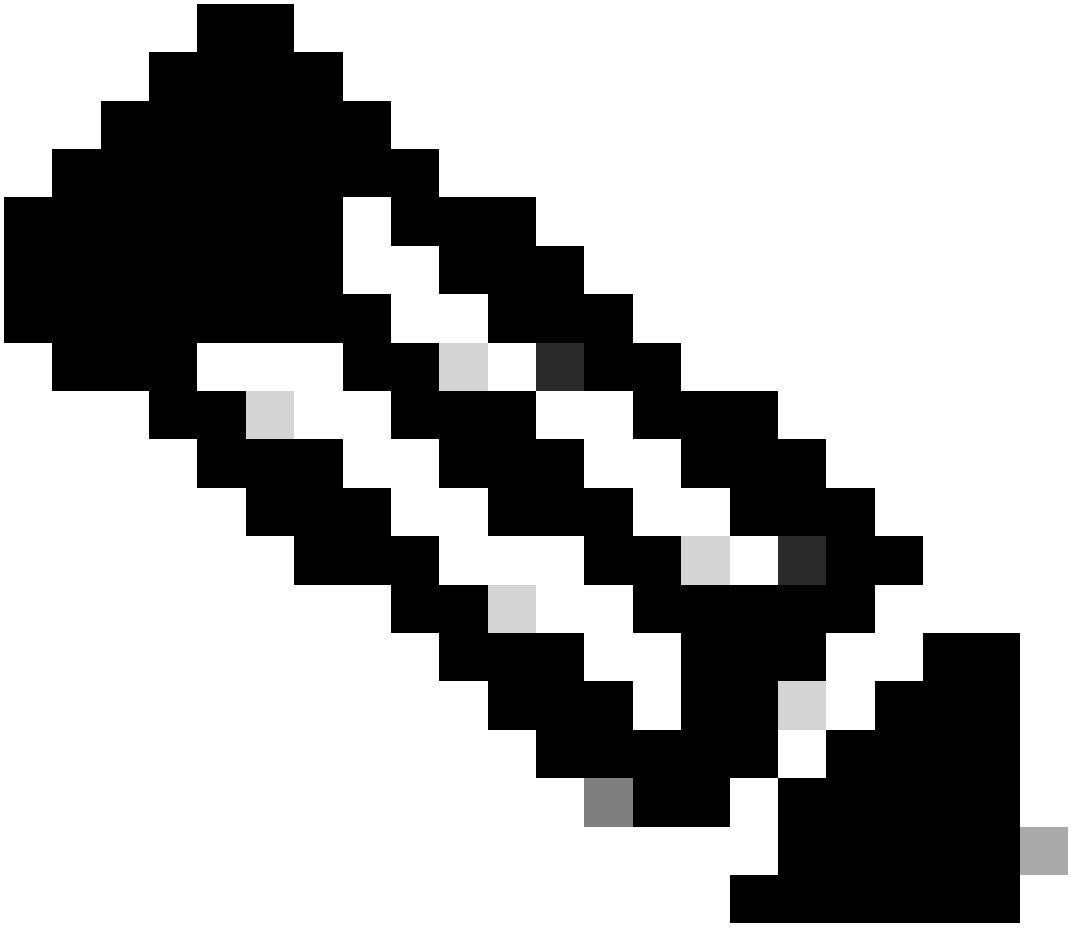
複数のコントローラから検出されたデバイスについて

Catalyst CenterとCXエージェントが収集するその他の資産（ダイレクト・デバイス接続）が同じCXエージェント上にある場合は、Cisco Catalyst CenterとCXエージェントへのダイレクト・デバイス接続の両方がデバイスを検出し、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。重複したデータを収集し、1つのコントローラのみがデバイスを管理するようにするには、CXエージェント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 Catalyst Centerで検出され、（シードファイルまたはIP範囲を使用して）直接デバイス接続で再検出された場合は、デバイスの制御においてCisco Catalyst Centerが優先されます。
- デバイスが最初にCXエージェントへの直接デバイス接続によって検出され、次にCisco Catalyst Centerによって再検出された場合、デバイスの制御ではCisco Catalyst Centerが優先されます。

診断スキャンのスケジュール

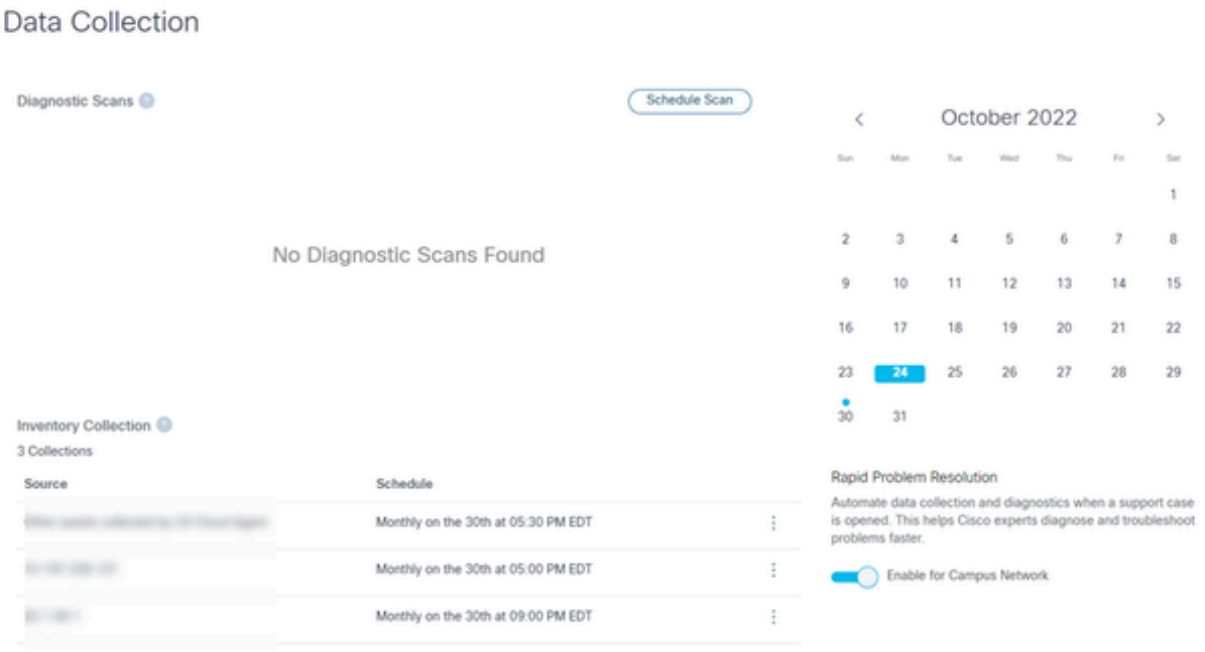
お客様は、該当するSuccess Tracksとその対象デバイスに関してCX Cloudでオンデマンド診断スキャンをスケジュールし、アドバイザリのPriority Bugsに情報を入力できます。



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時間離れた場所でオンデマンドスキャンを開始して、それらが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、スキャンプロセスの速度が低下し、スキャンが失敗する可能性があります。

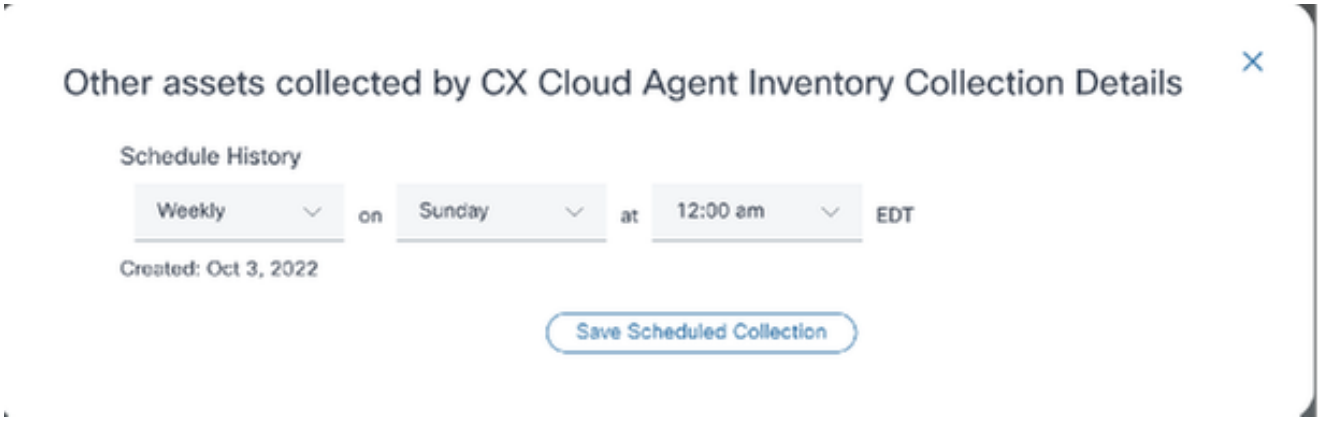
診断スキャンをスケジュールするには、次の手順に従います。

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ページの左側のペインでData Collectionを選択します。
3. Schedule Scanをクリックします。



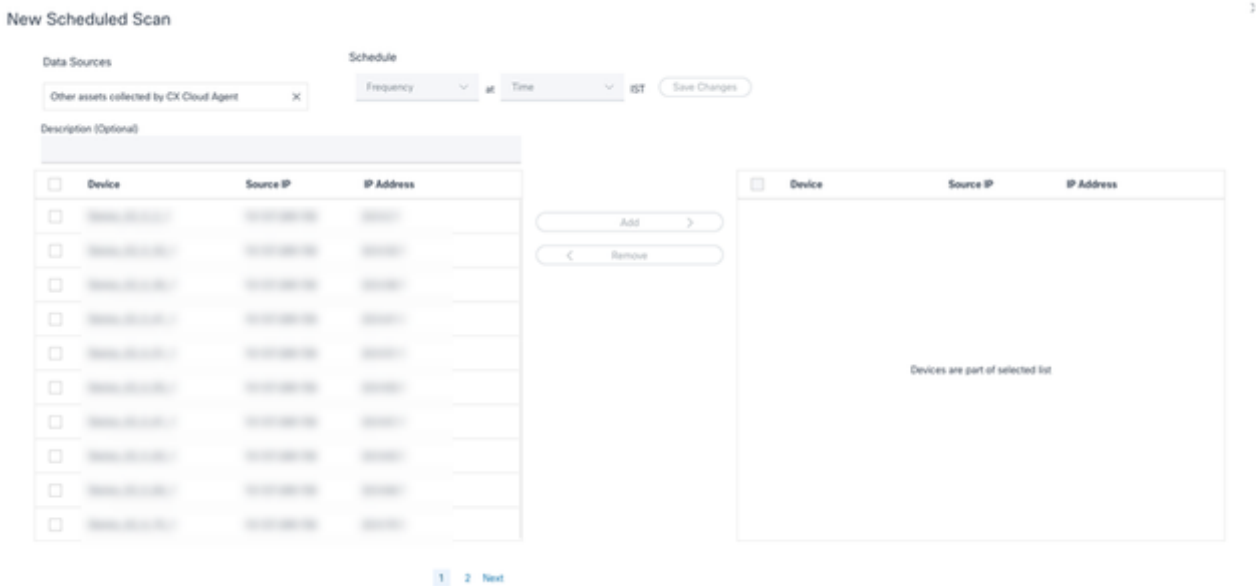
スキャンのスケジュール

4. このスキャンのスケジュールを構成します。



スキャンスケジュールの構成

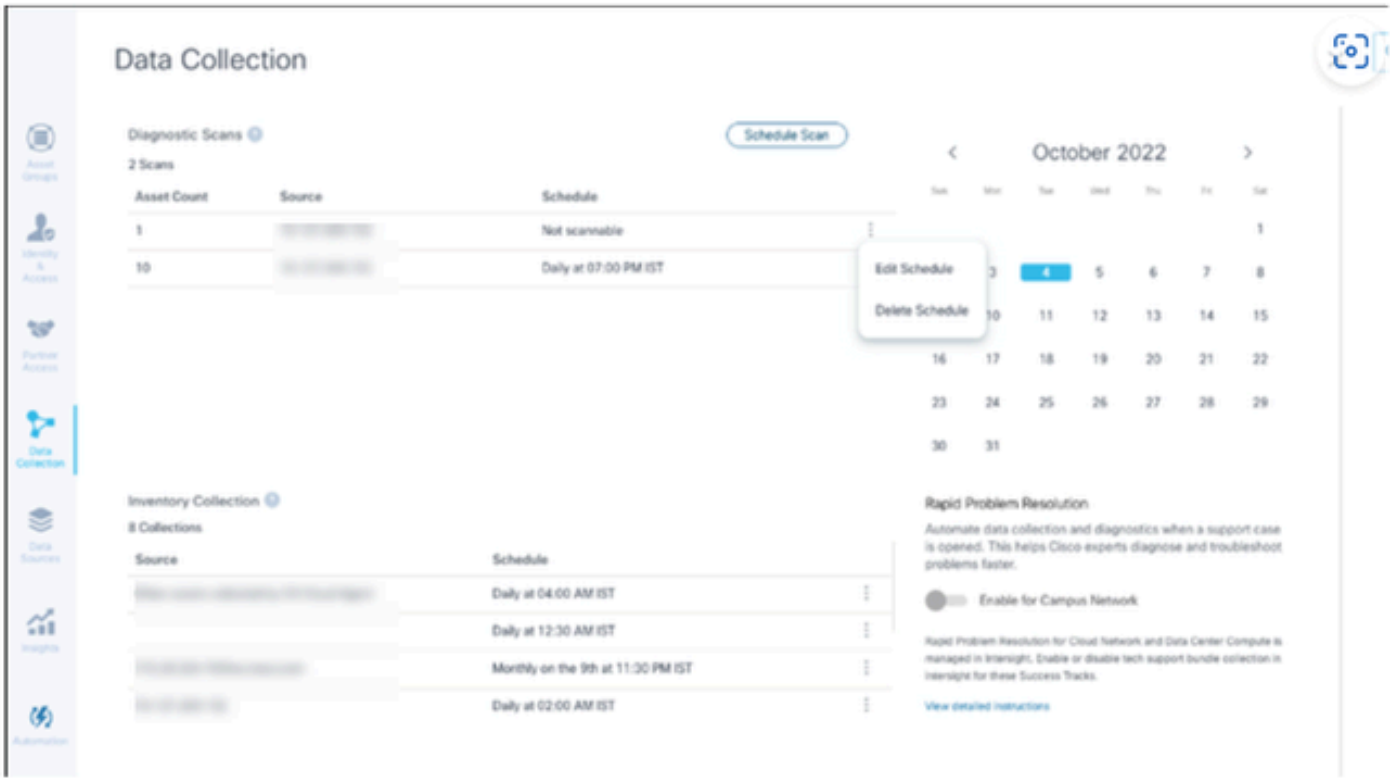
5. デバイスリストで、スキャンするすべてのデバイスを選択し、Addをクリックします。



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す。



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・コレクション

CXエージェントVMの中規模および大規模構成へのアップグレード

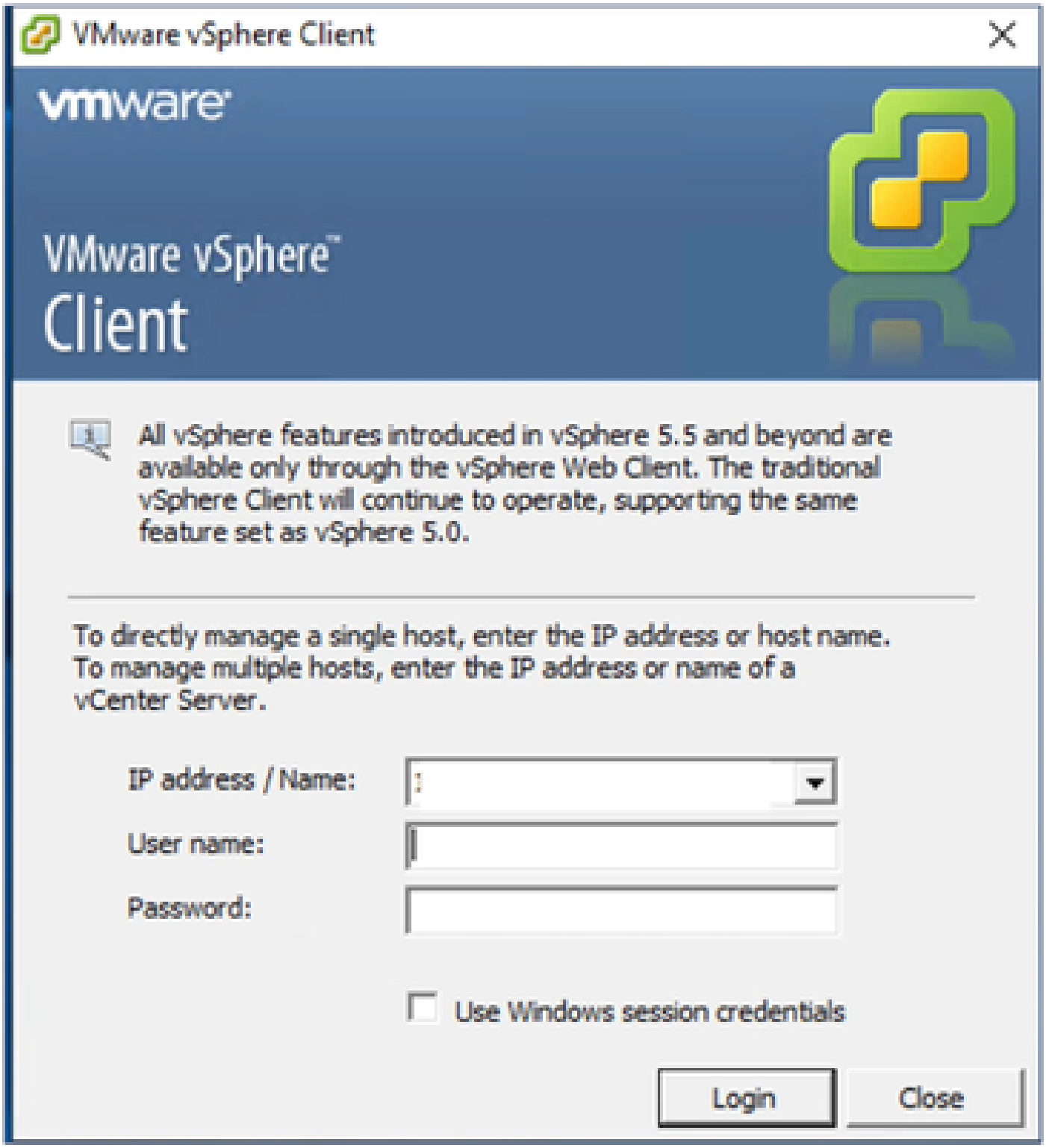
VMをアップグレードした後は、次の操作を実行できません。

- 大規模または中規模の構成から小規模の構成への縮小
- 大規模な構成から中規模な構成への縮小
- 中規模から大規模の構成へのアップグレード

VMをアップグレードする前に、障害発生時のリカバリのためにスナップショットを作成することをお勧めします。詳細については、『CX Cloud VMのバックアップおよび復元』を参照してください。

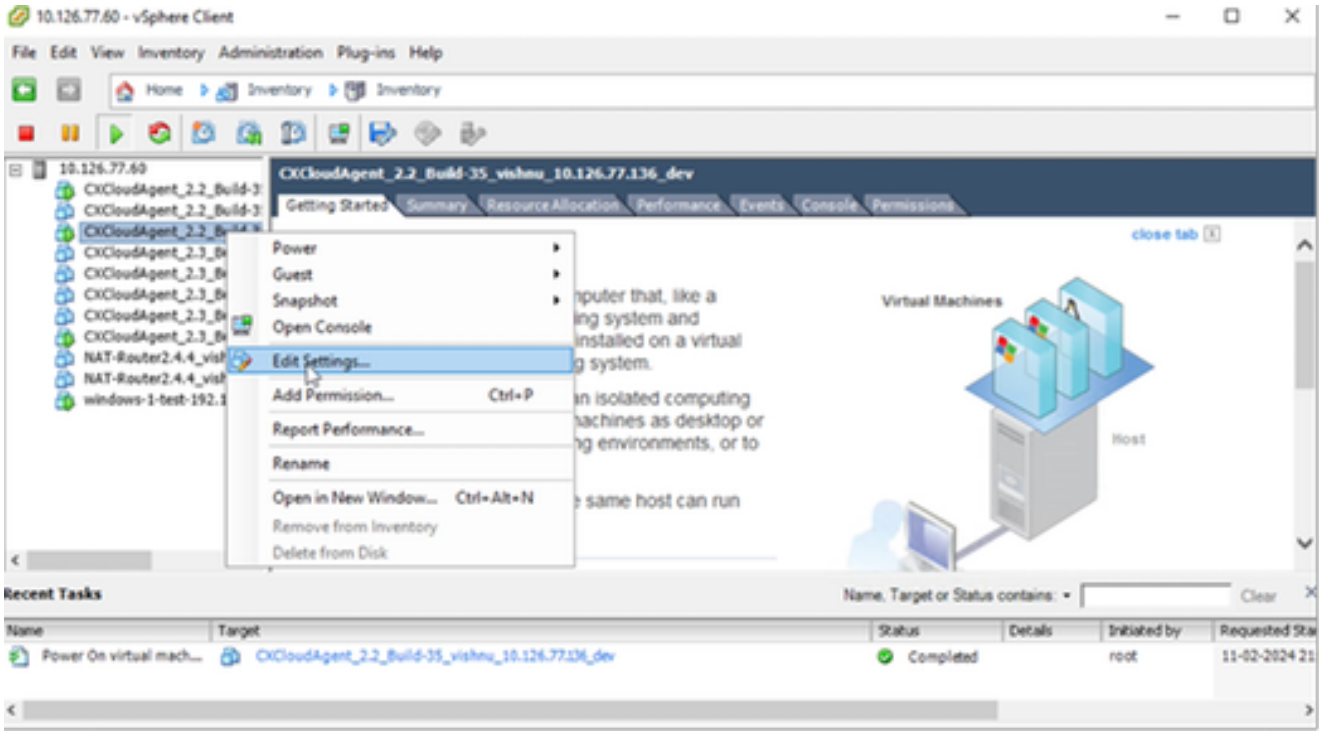
VMware vSphere Thick Clientを使用した再設定

既存のVMware vSphere Thick Clientを使用してVM設定をアップグレードするには、次の手順を実行します。



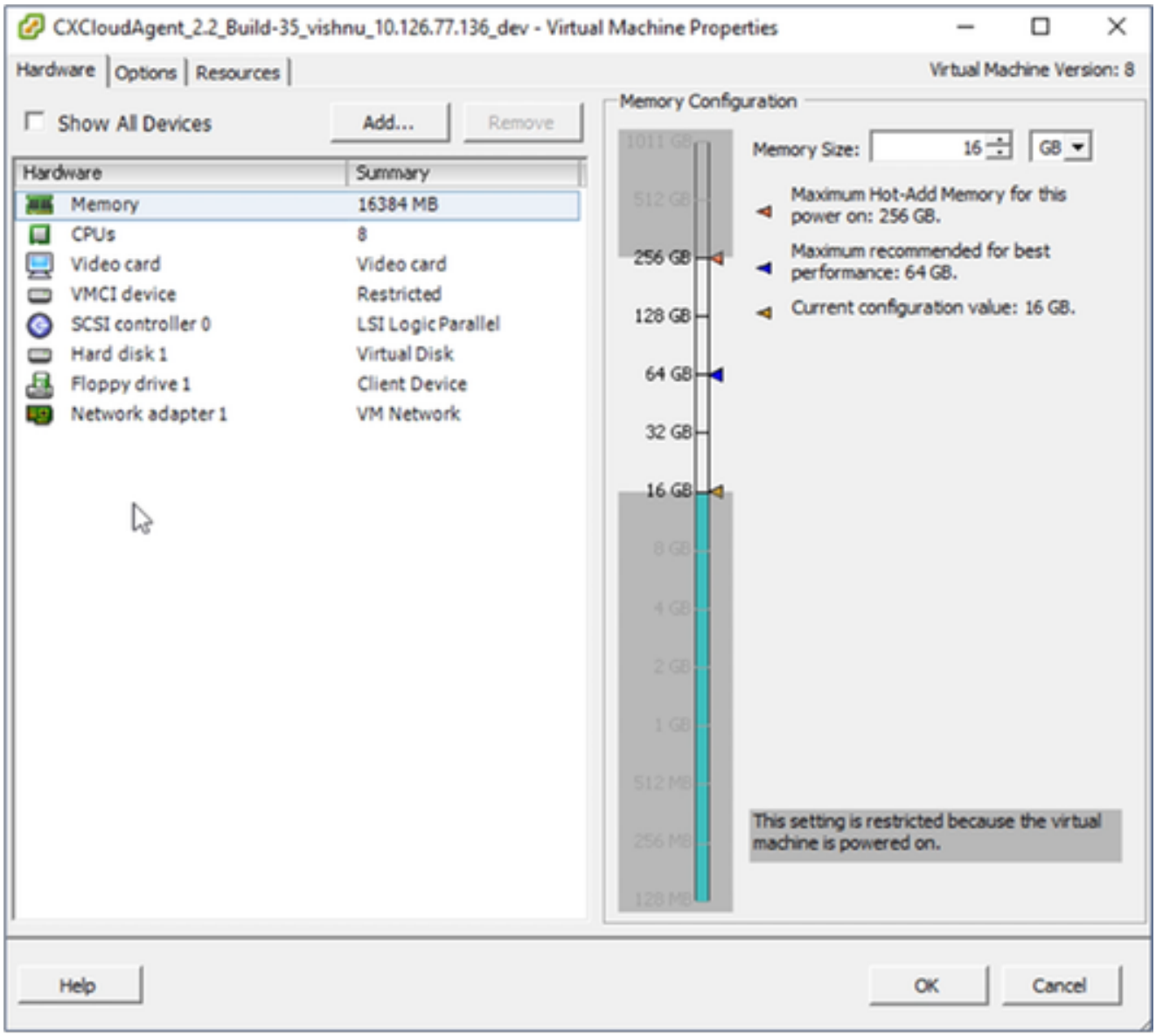
vSphere クライアント

1. VMware vSphere Clientにログインします。ホームページにVMのリストが表示されます。



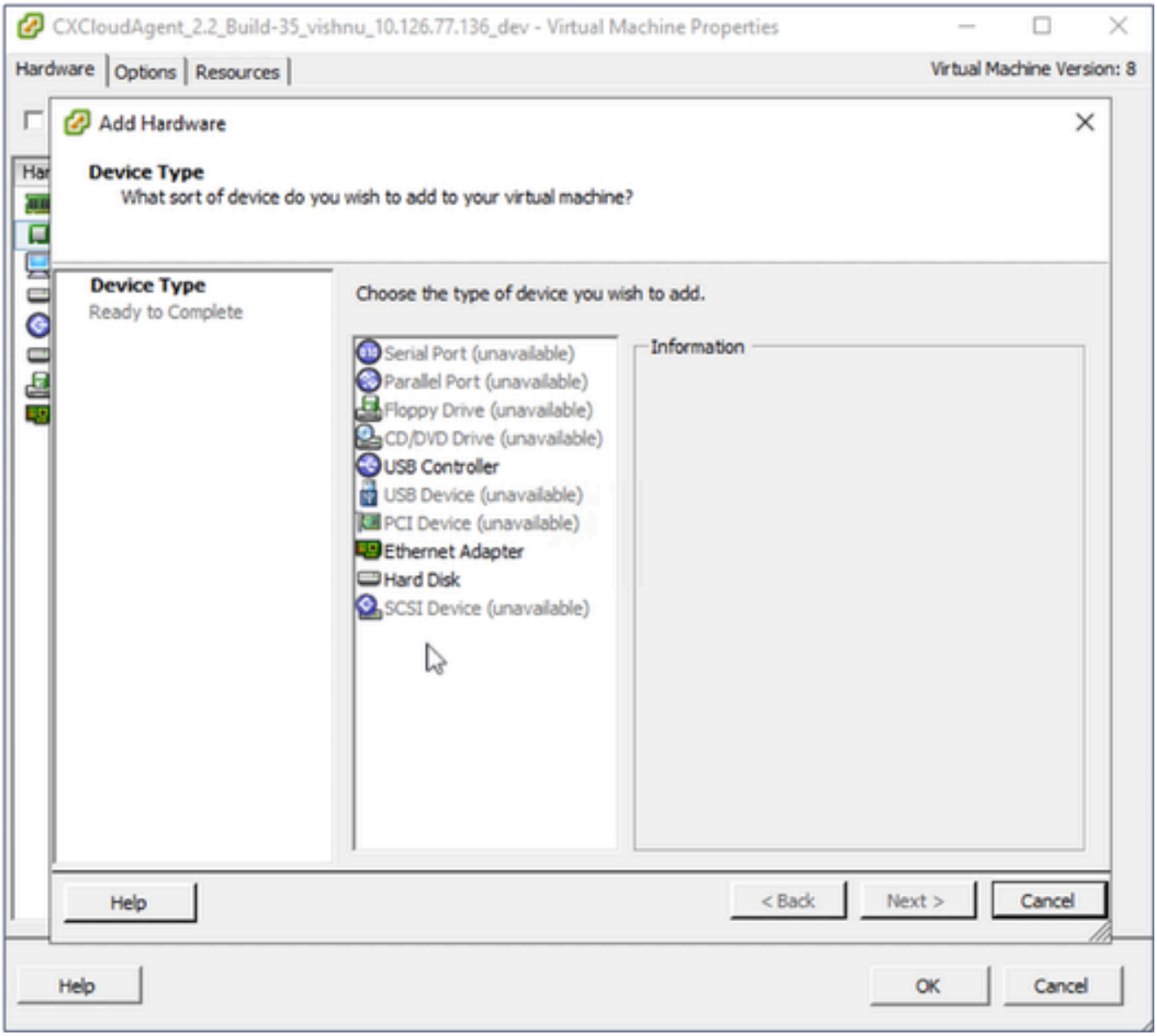
設定の編集

2. ターゲットVMを右クリックし、メニューからEdit Settingsを選択します。VM Propertiesウィンドウが開きます。



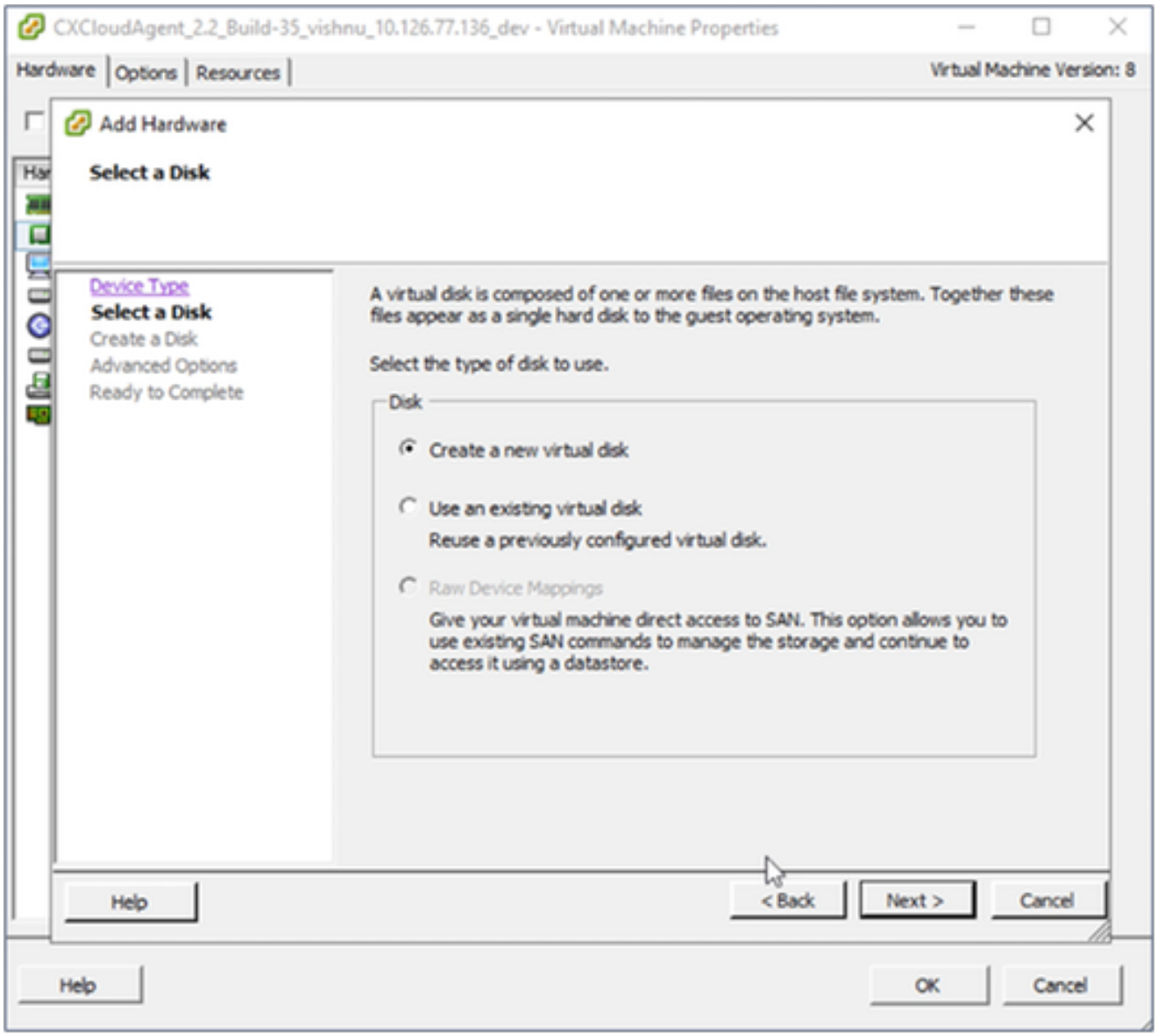
VMのプロパティ

3. 指定に従って、Memory Sizeの値を更新します。
   中：32 GB(32768 MB)
   大：64 GB(65536 MB)
4. CPUを選択し、指定どおりに値を更新します。
   中：16コア（8ソケット*2コア/ソケット）
   大：32コア（16ソケット*2コア/ソケット）
5. [Add] をクリックします。Add Hardwareウィンドウが開きます。



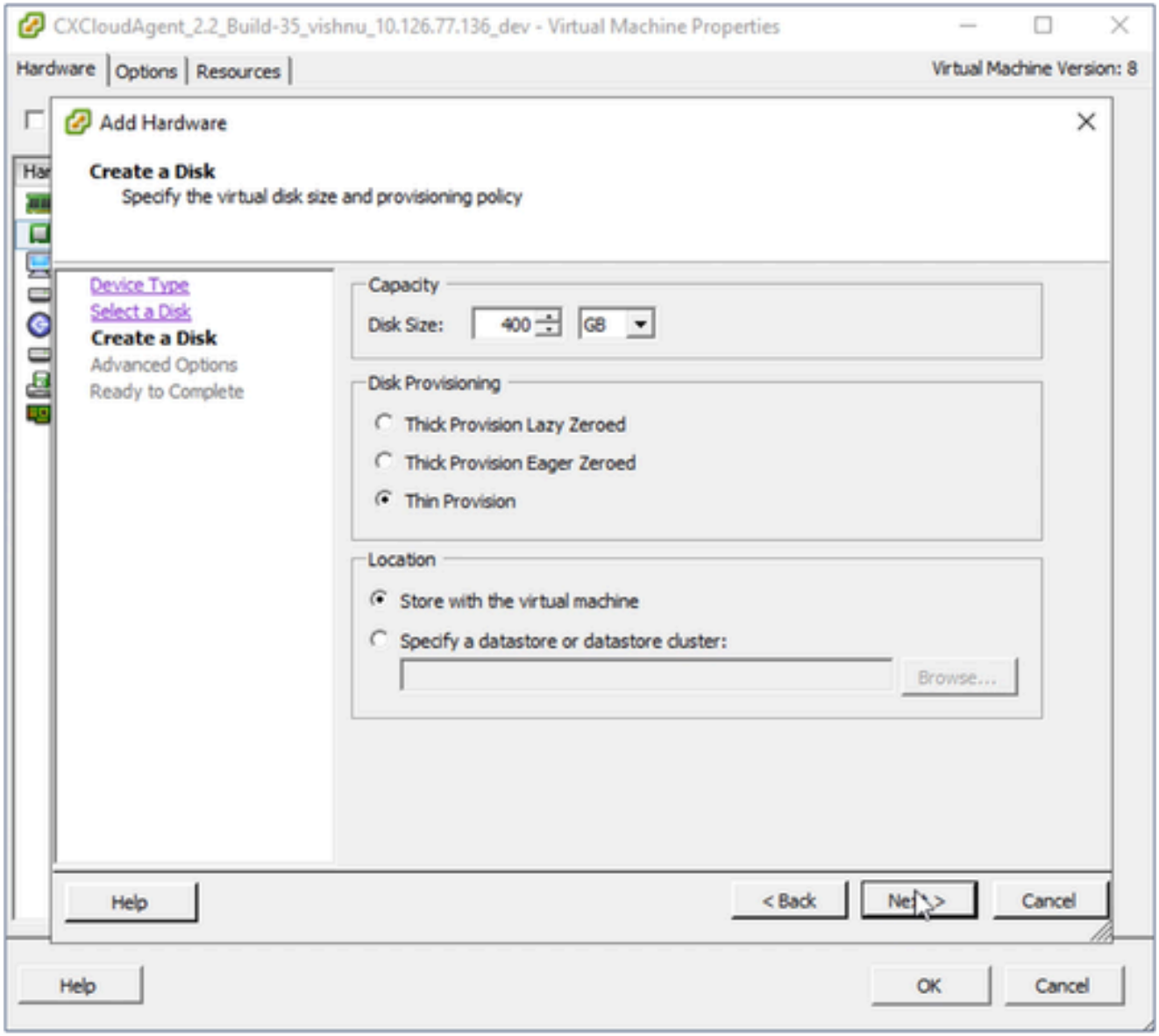
デバイスタイプ

6. Device TypeとしてHard Diskを選択します。
7. [Next] をクリックします。



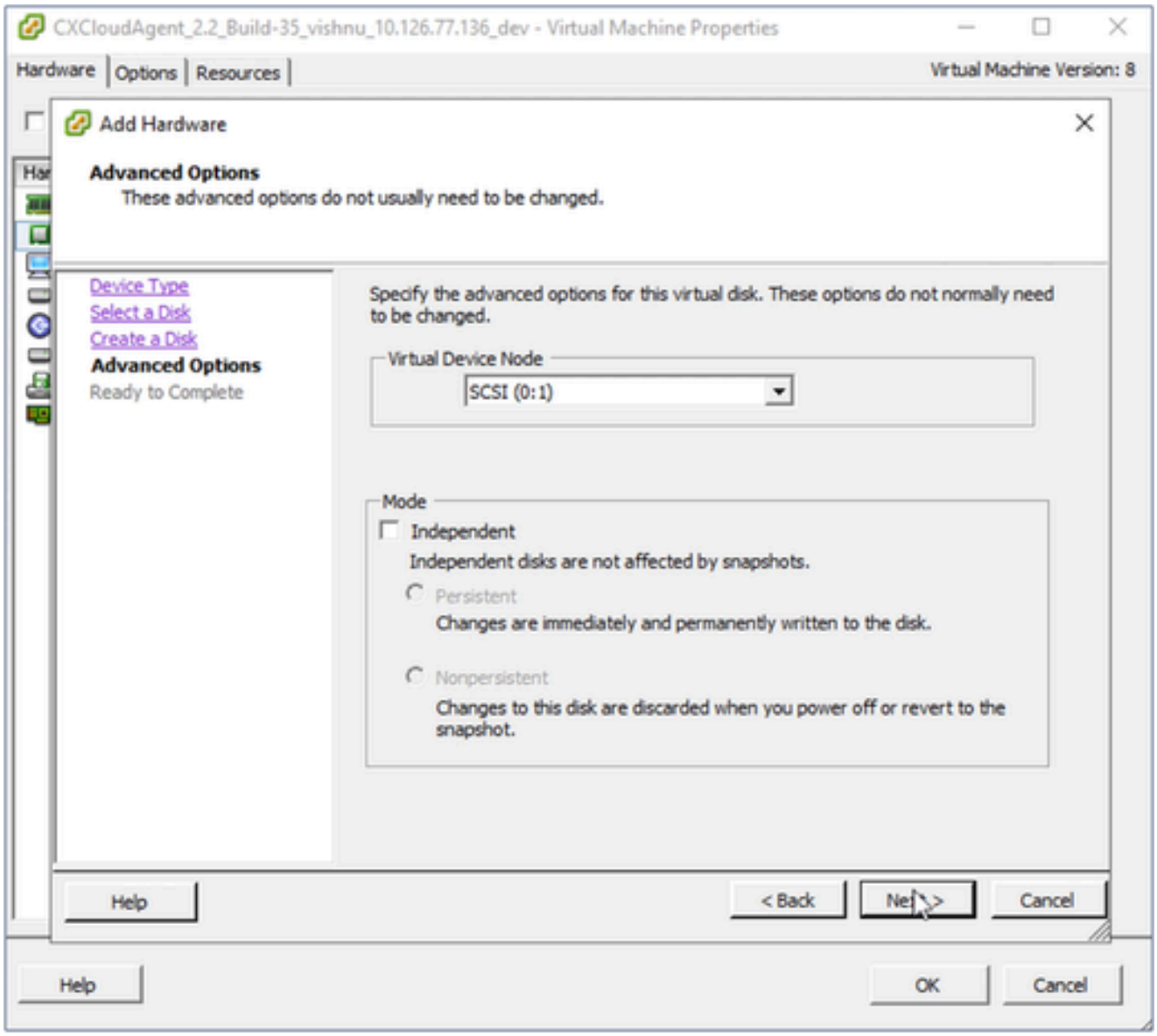
ディスクの選択

8. Create a new virtual diskオプションボタンを選択し、Nextをクリックします。



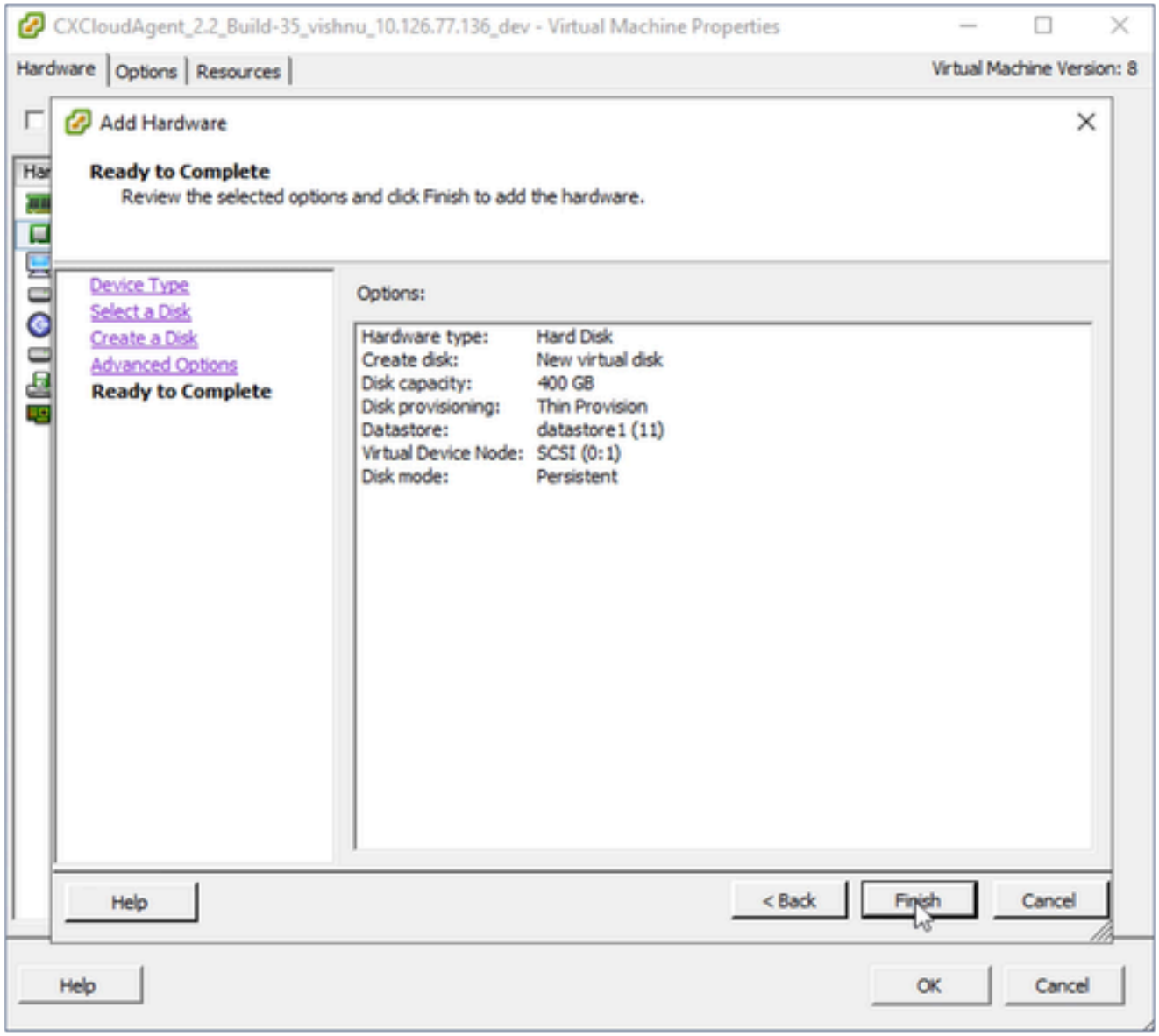
ディスクの作成

9. Capacity > Disk Sizeを指定どおりに更新します。
   小規模から中規模：400 GB（初期サイズは200 GB、総容量は600 GBに増加）
   小規模から大規模：1000 GB（初期サイズは200 GB、総容量は1200 GBに増加）
10. Disk ProvisioningのThin Provisionオプションボタンを選択します。
11. [Next] をクリックします。Advanced Optionsウィンドウが表示されます。



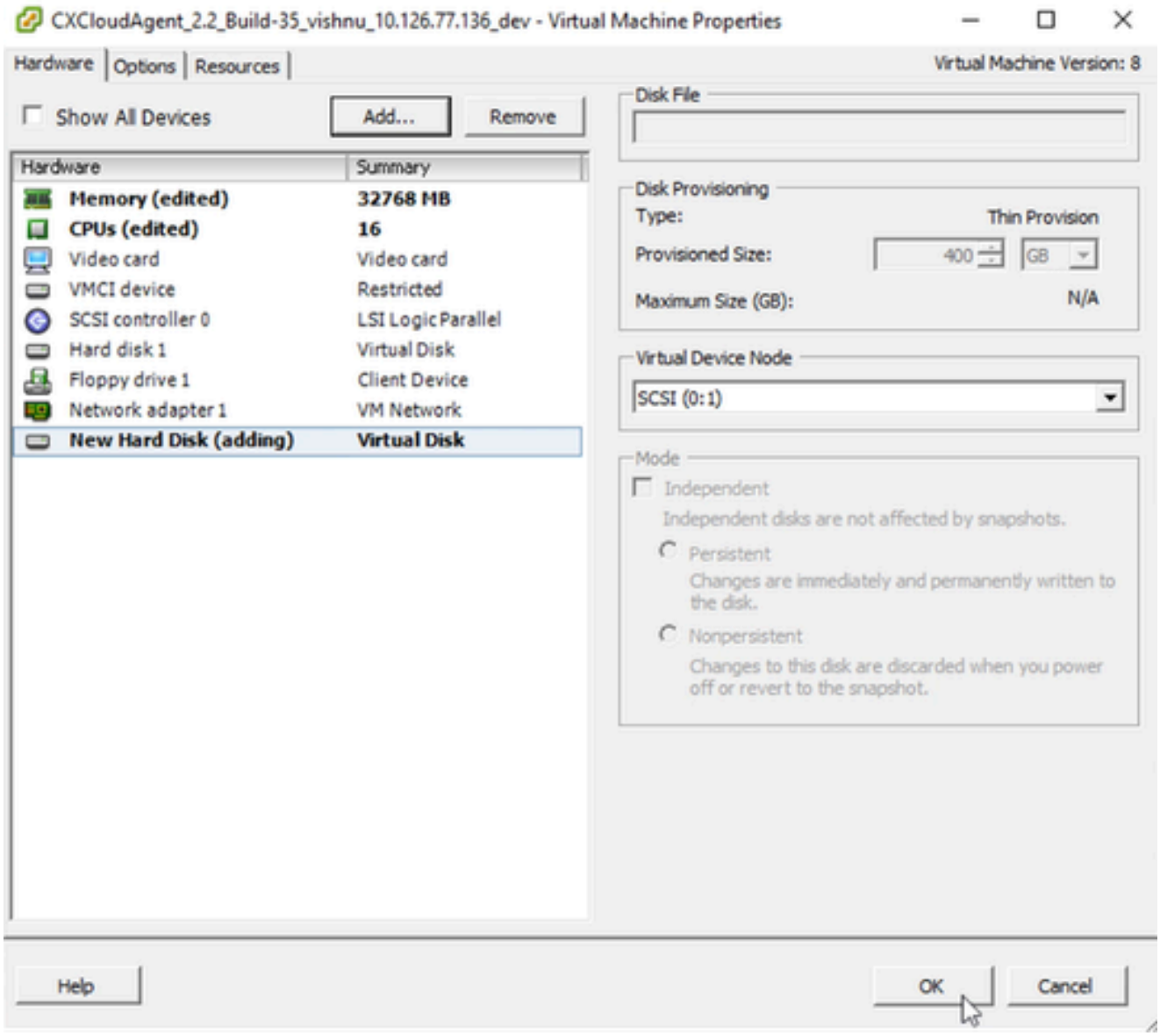
詳細オプション

12. 変更しないでください。[Next] をクリックして次に進みます。



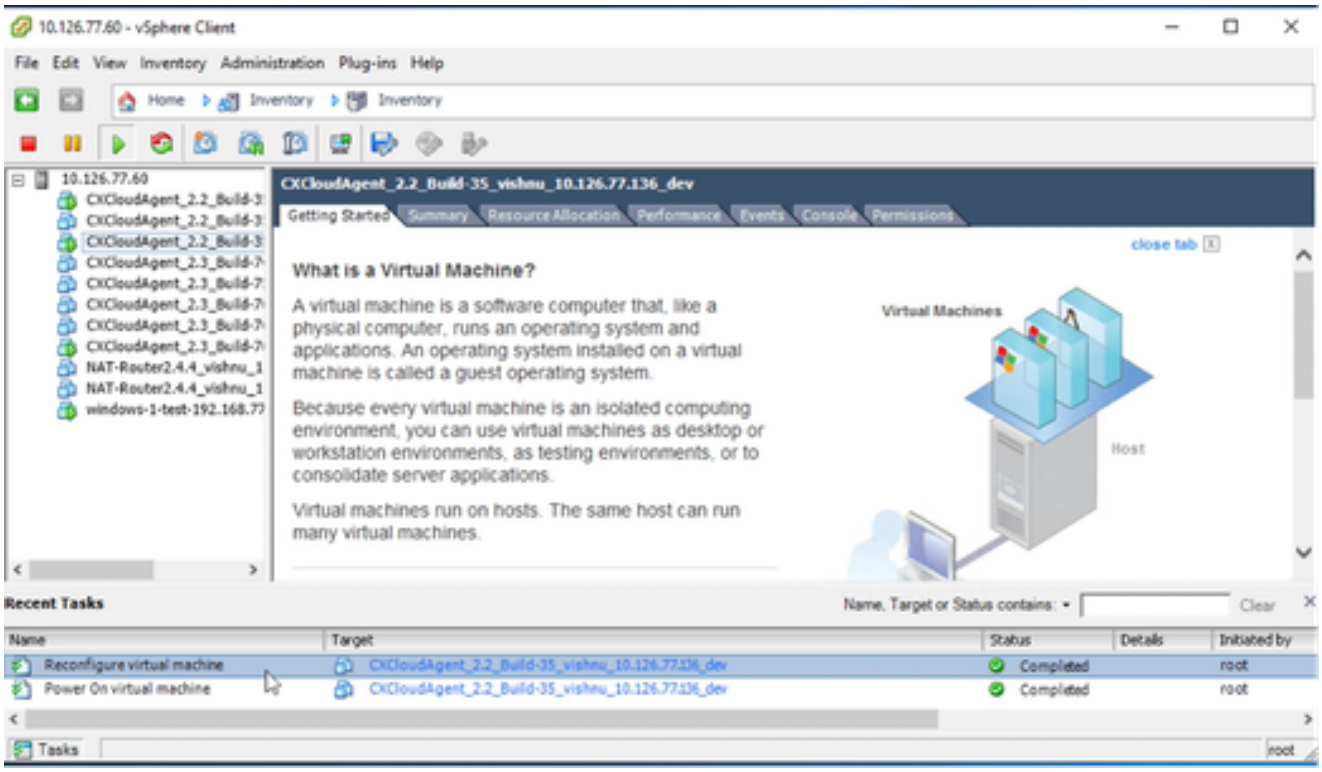
終了準備の完了（Ready to Complete）

13. [Finish] をクリックします。

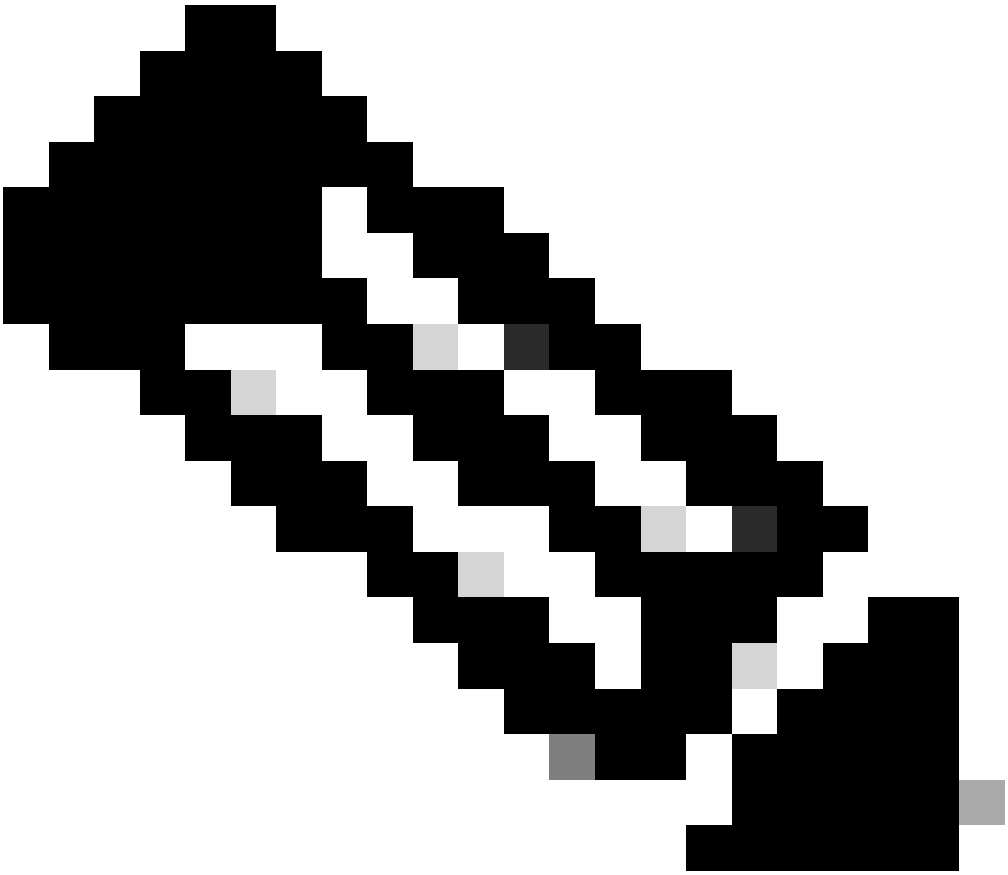


ハードウェア

14. OKをクリックして、再設定を完了します。完了した再設定が、[最近のタスク]パネルに表示されます。


10.126.77.60 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Inventory
10.126.77.60
CXCloudAgent_2.2_Build-35_vishnu_10.126.77.136_dev
Getting Started Summary Resource Allocation Performance Events Console Permissions
close tab
What is a Virtual Machine?
A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.
Because every virtual machine is an isolated computing environment, you can use virtual machines as desktop or workstation environments, as testing environments, or to consolidate server applications.
Virtual machines run on hosts. The same host can run many virtual machines.
Virtual Machines
Host
Recent Tasks
Name, Target or Status contains:
Clear
Name
Target
Status
Details
Initiated by
Reconfigure virtual machine
CXCloudAgent_2.2_Build-35_vishnu_10.126.77.136_dev
Completed
root
Power On virtual machine
CXCloudAgent_2.2_Build-35_vishnu_10.126.77.136_dev
Completed
root
Tasks
root

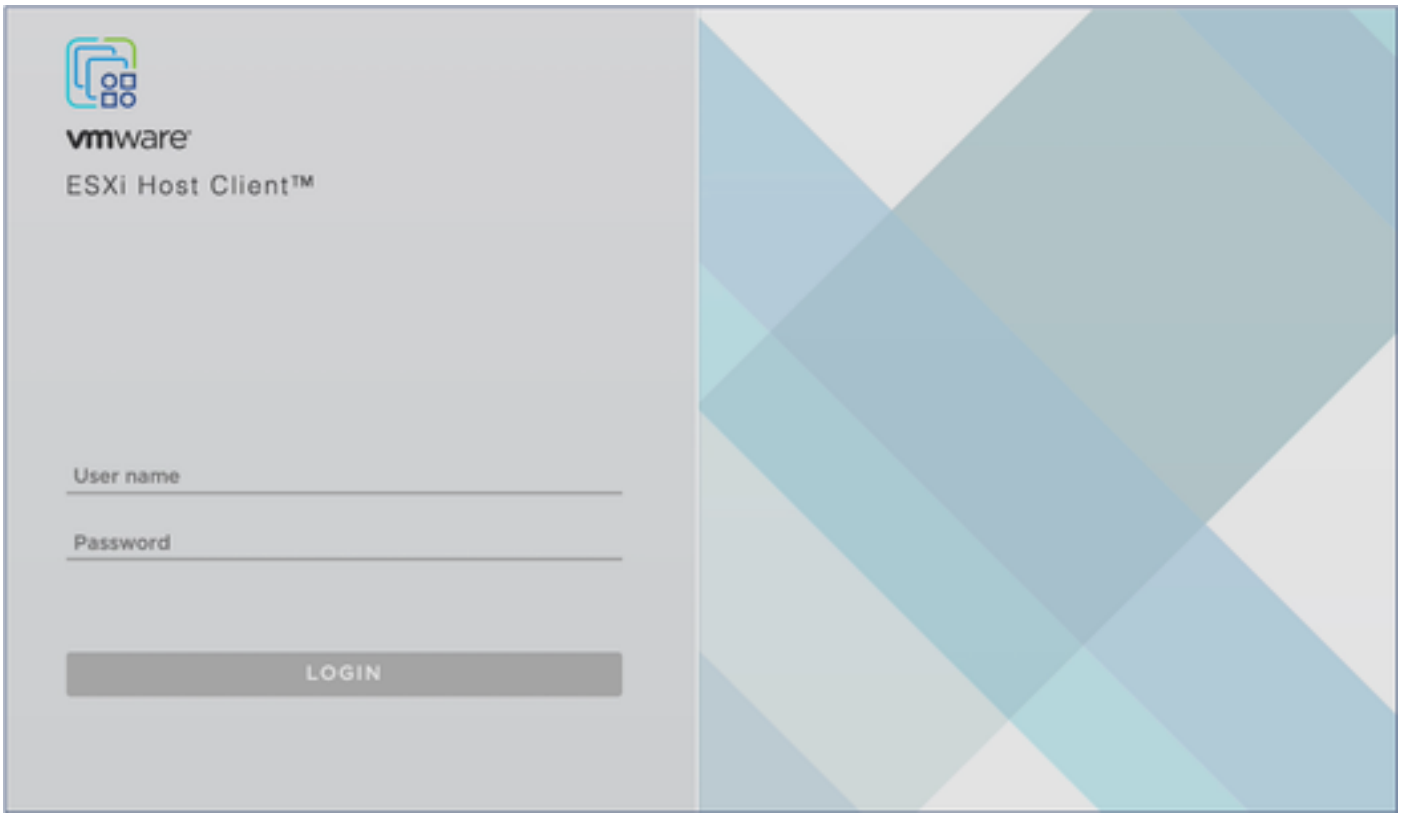
最近のタスク



注：設定の変更は、完了するまで約5分かかります。

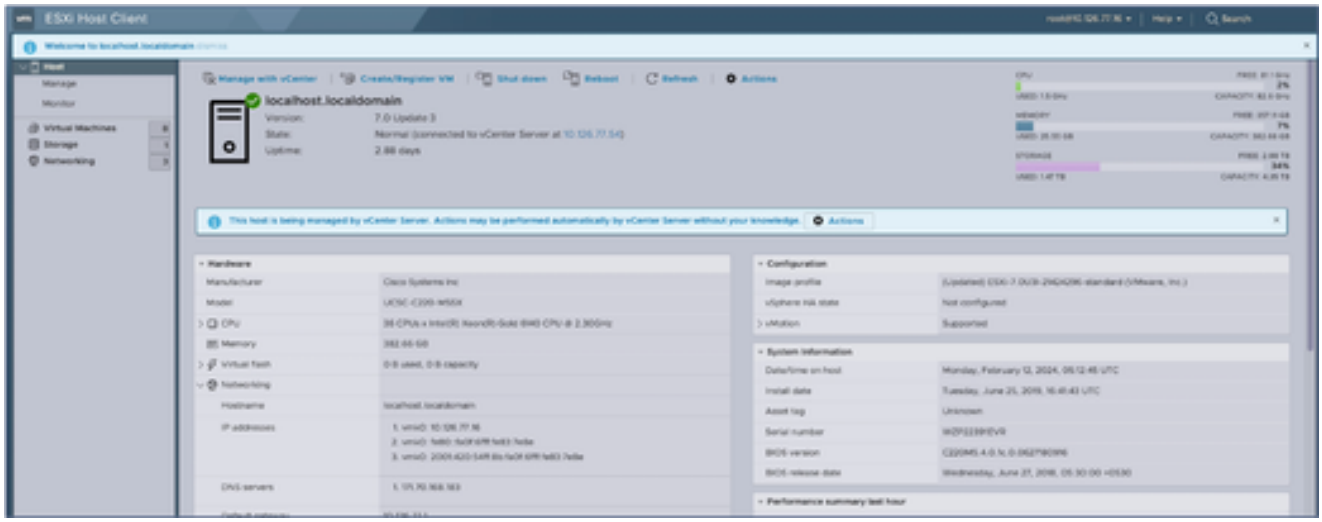
WebクライアントESXi v6.0を使用した再設定

Web Client ESXi v6.0を使用してVM構成を更新するには、次の手順を実行します。



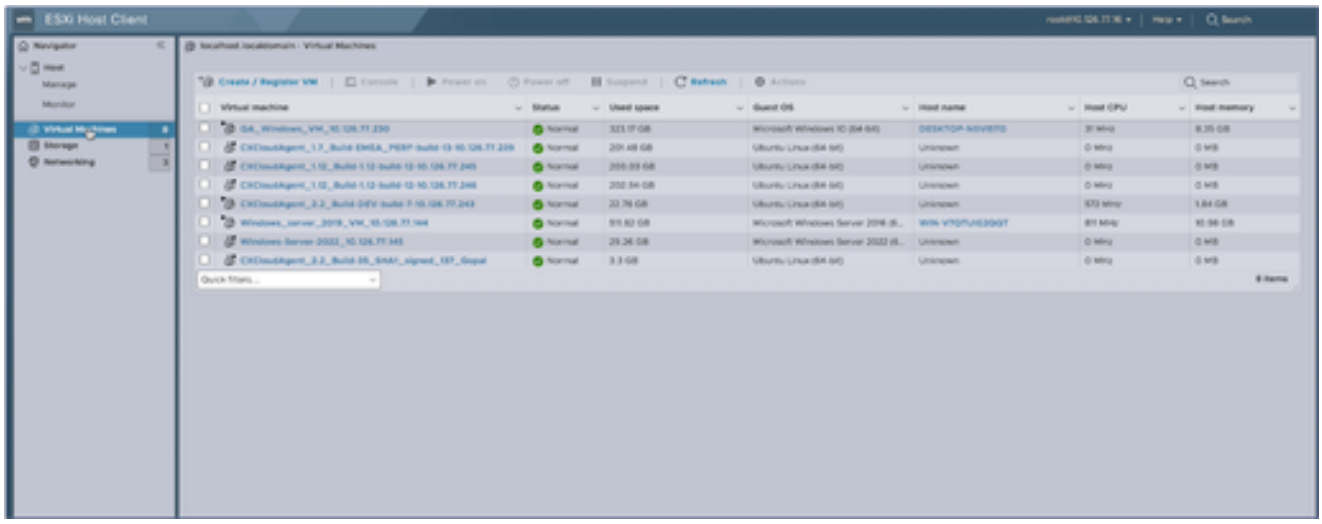
ESXiクライアント

1. VMware ESXiクライアントにログインします。ホームページが表示されます。



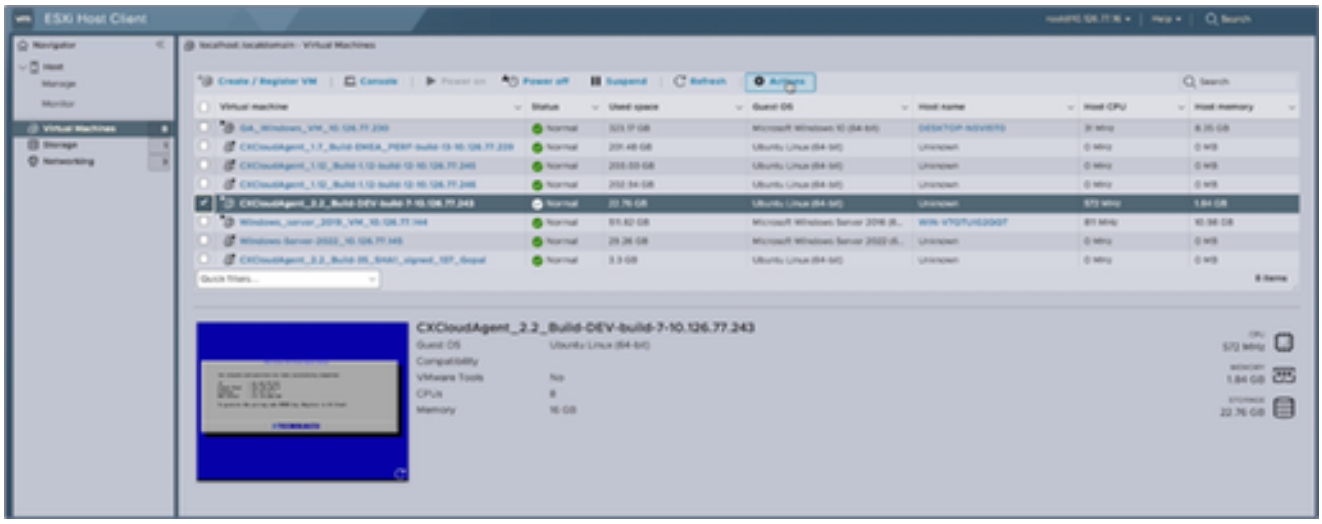
ESXiホームページ

2. Virtual Machineをクリックして、VMのリストを表示します。



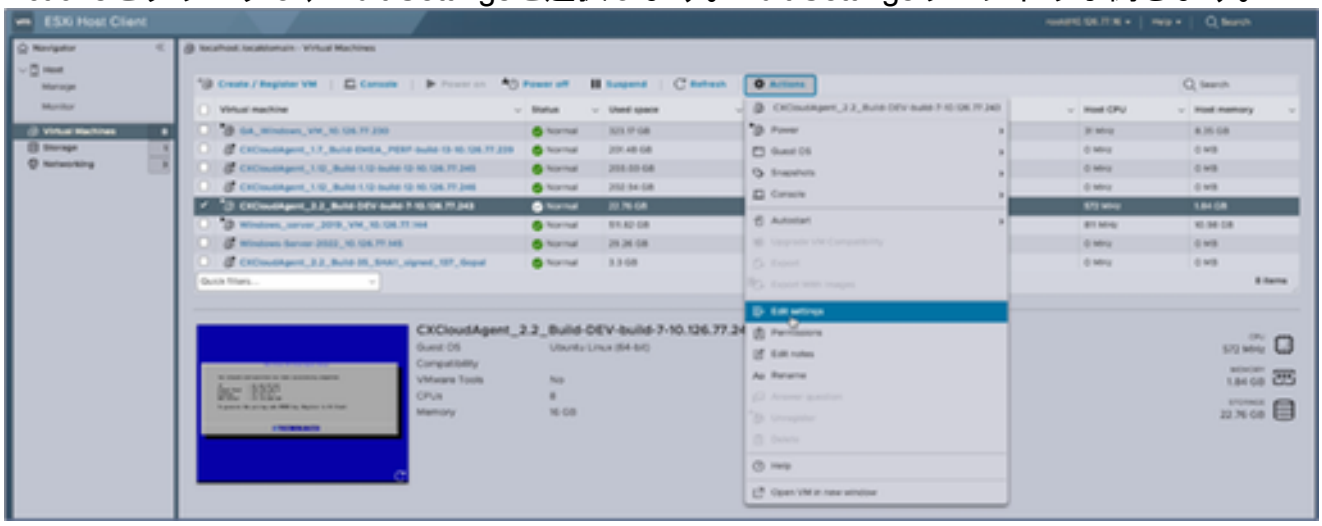
VMのリスト

3. ターゲットVMを選択します。

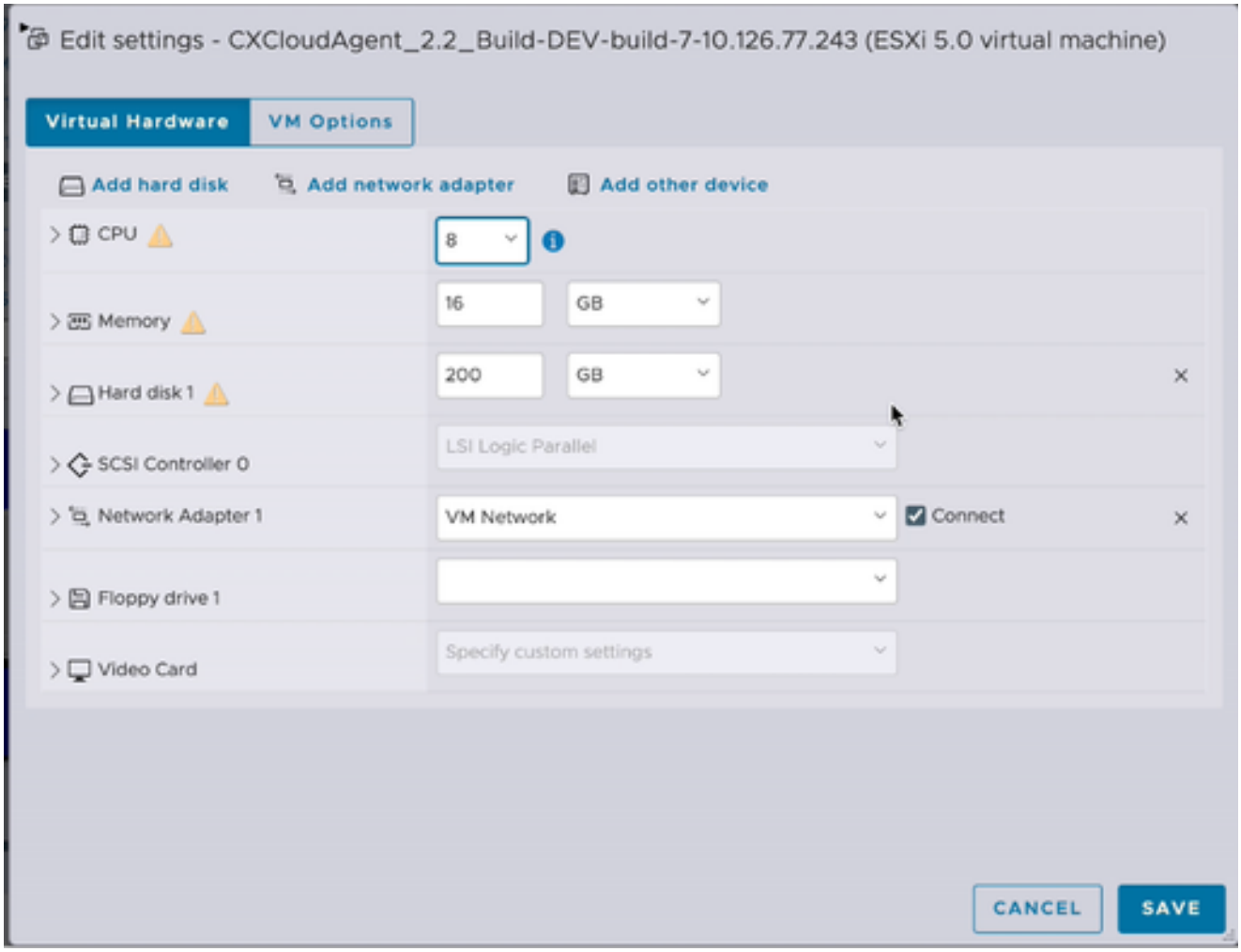


ターゲットVM

4. Actionsをクリックし、Edit Settingsを選択します。Edit Settingsウィンドウが開きます。

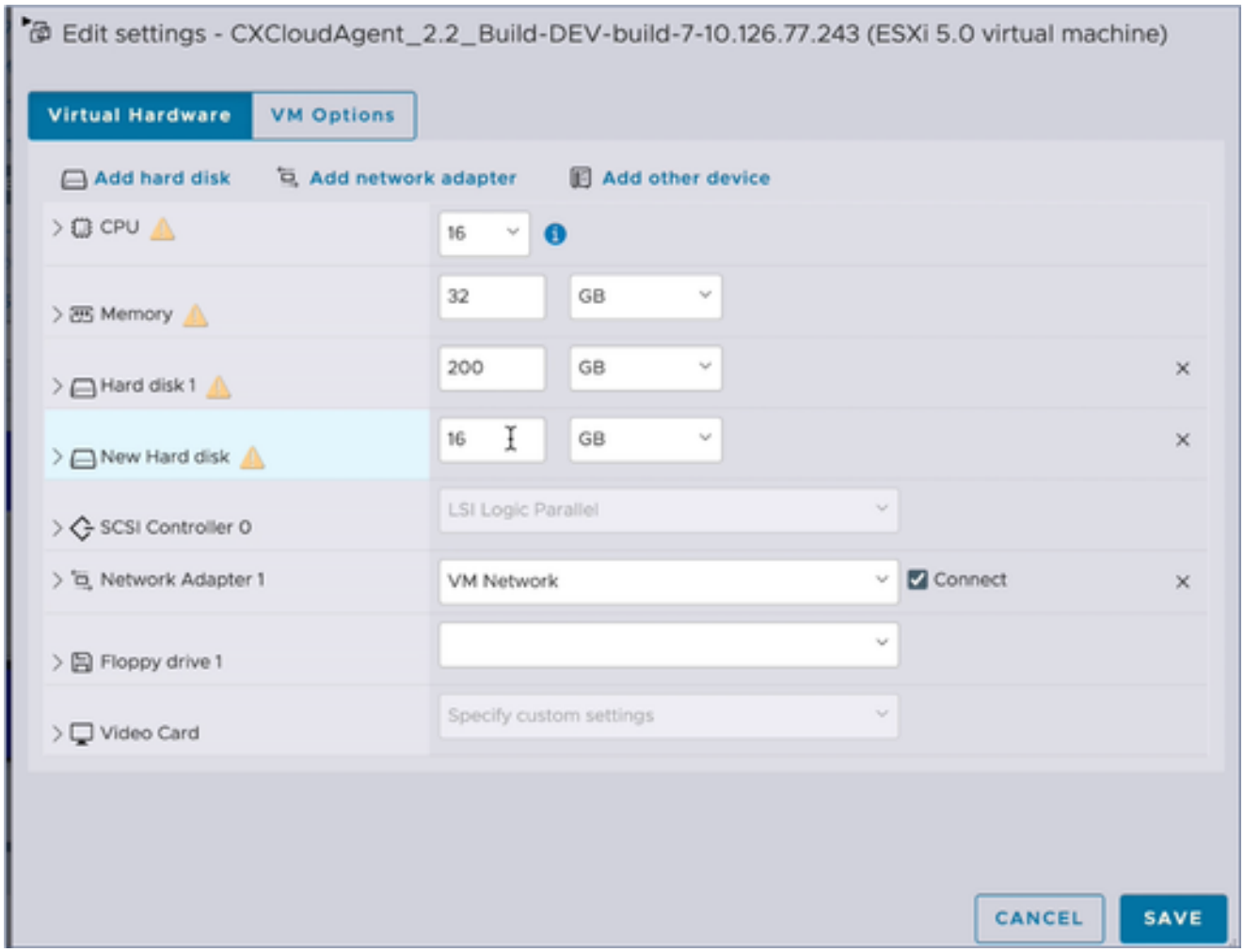


[アクション（ Actions ）]



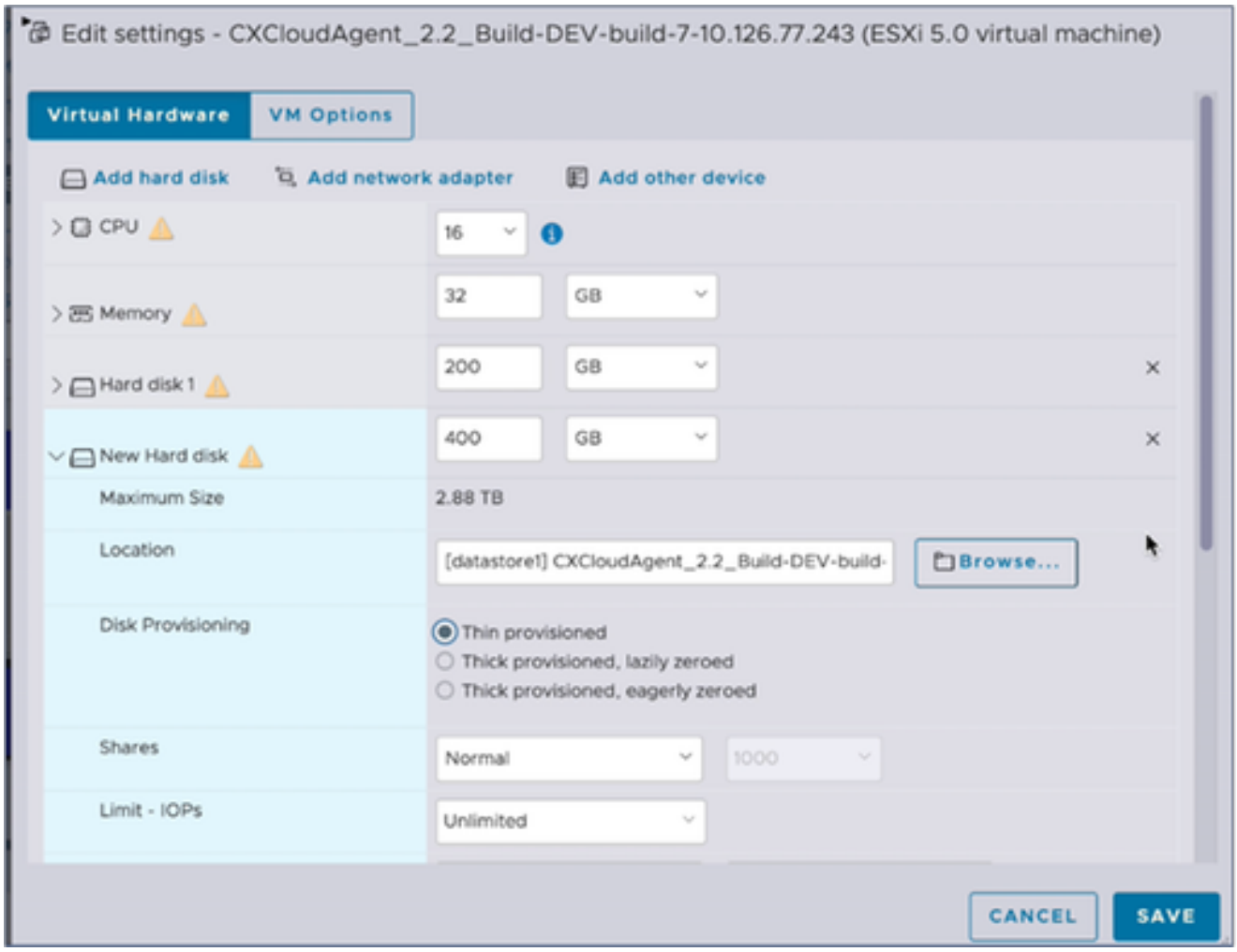
設定の編集

5. 指定に従ってCPU値を更新します。
   中：16コア（8ソケット*2コア/ソケット）
   大：32コア（16ソケット*2コア/ソケット）
6. 指定に従ってMemoryの値を更新します。
   中：32 GB
   大：64 GB
7. Add hard disk > New standard hard diskの順にクリックします。新しいハードディスクエントリがEdit settingsウィンドウに表示されます。



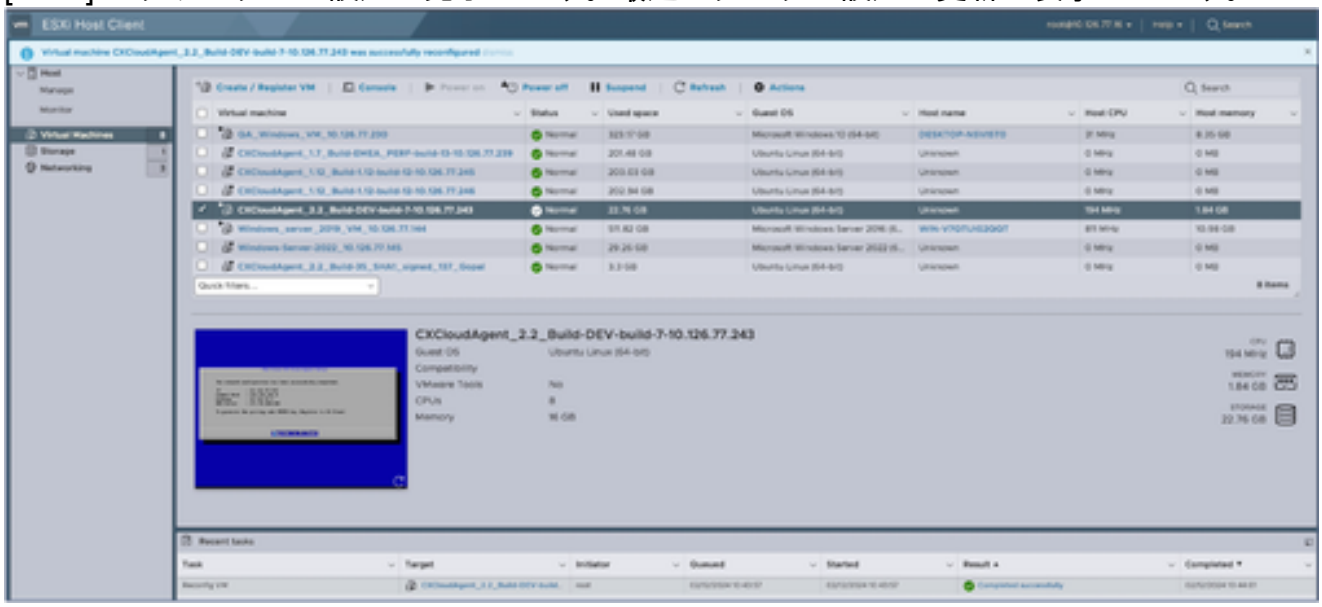
設定の編集

8. 指定に従って新しいハードディスクの値を更新します。
   小規模から中規模：400 GB（初期サイズは200 GB、総容量は600 GBに増加）
   小規模から大規模：1000 GB（初期サイズは200 GB、総容量は1200 GBに増加）
9. 矢印をクリックしてNew Hard diskを展開します。プロパティが表示されます。



設定の編集

10. Thin provisionedオプションボタンを選択します。
11. [Save] をクリックして設定を完了します。最近のタスクに設定の更新が表示されます。



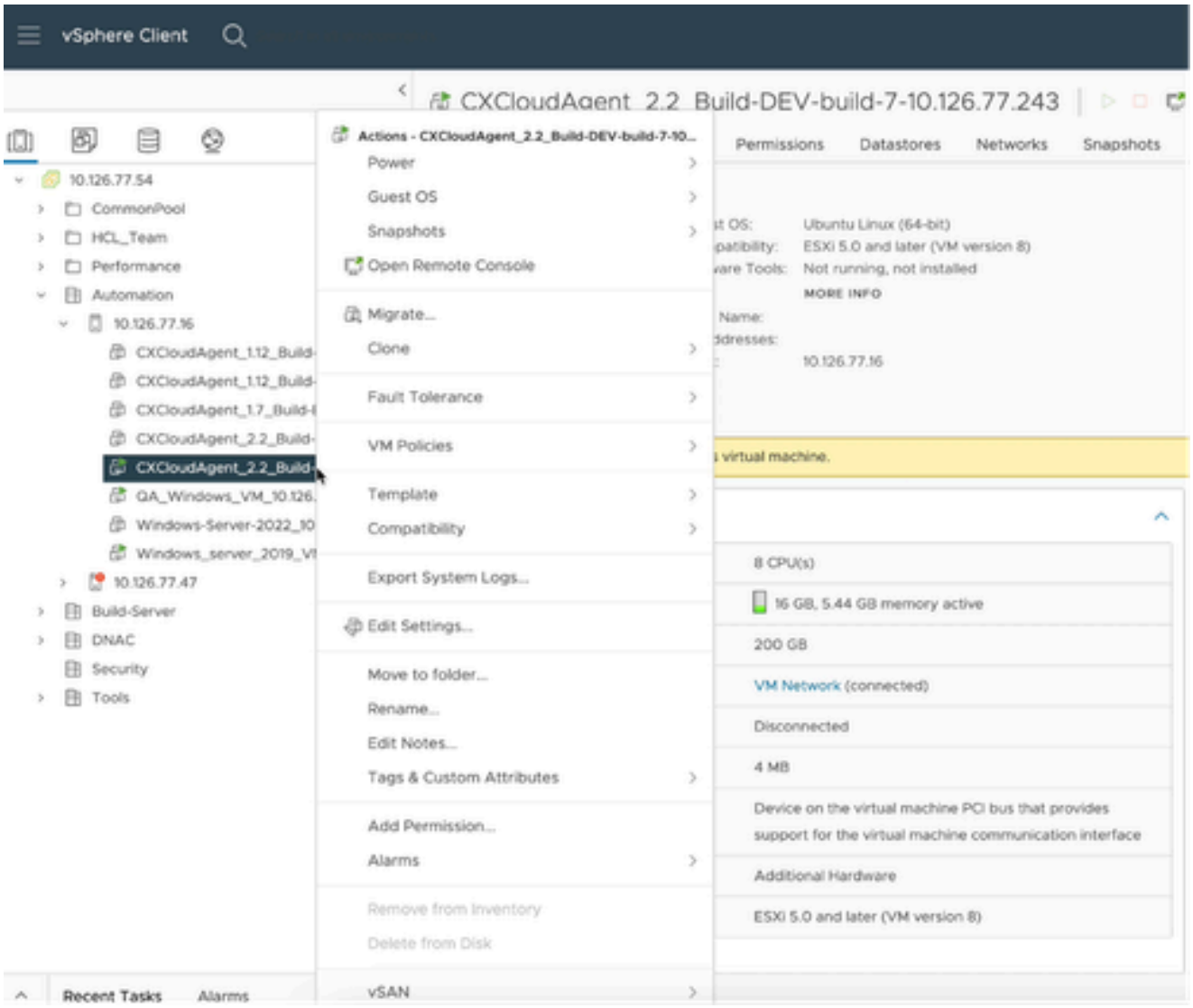
最近のタスク

Webクライアントvcenterを使用した再設定

WebクライアントvCenterを使用してVM設定を更新するには、次の手順を実行します。

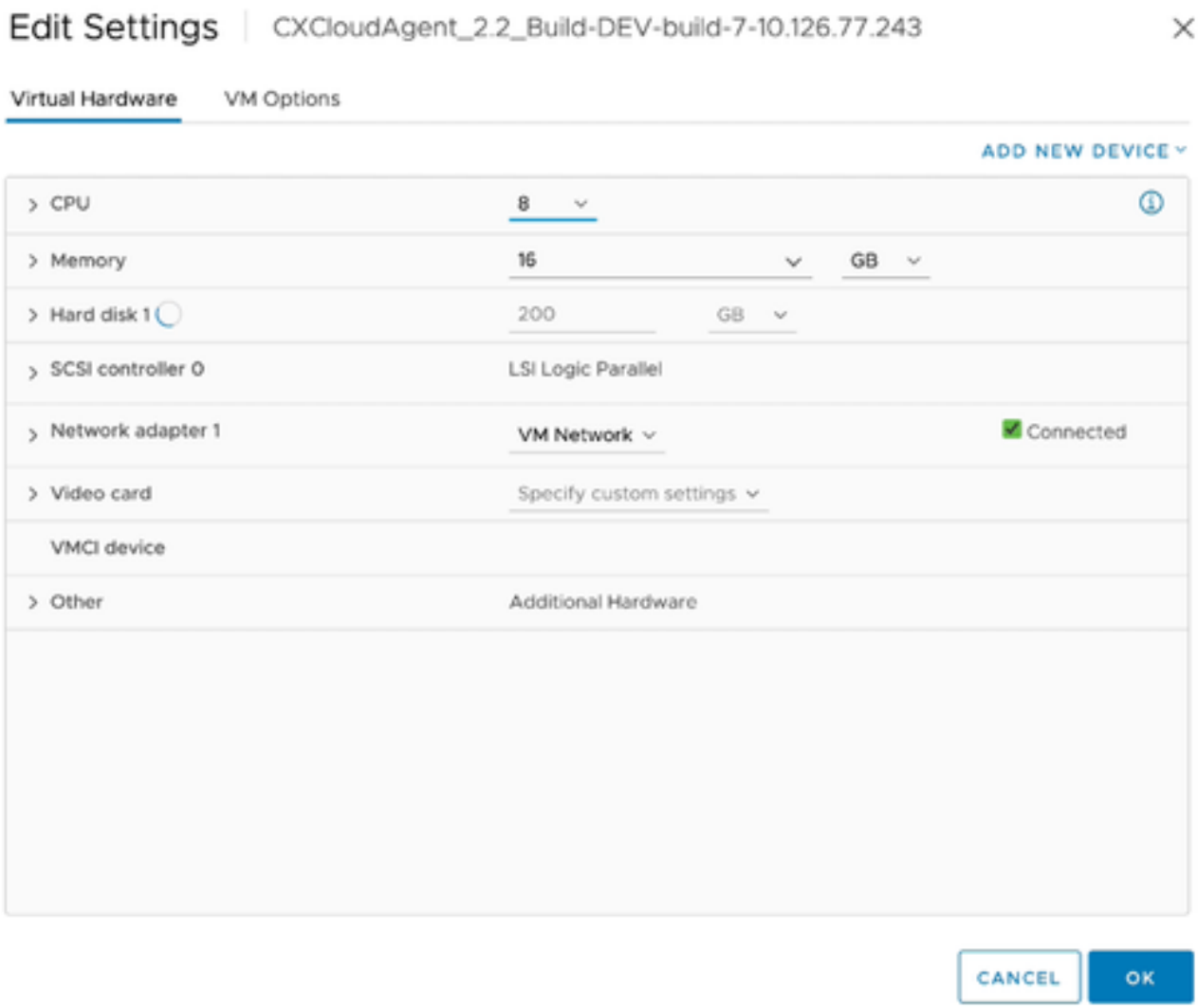
vCenter

1. vCenterにログインします。ホームページが表示されます。



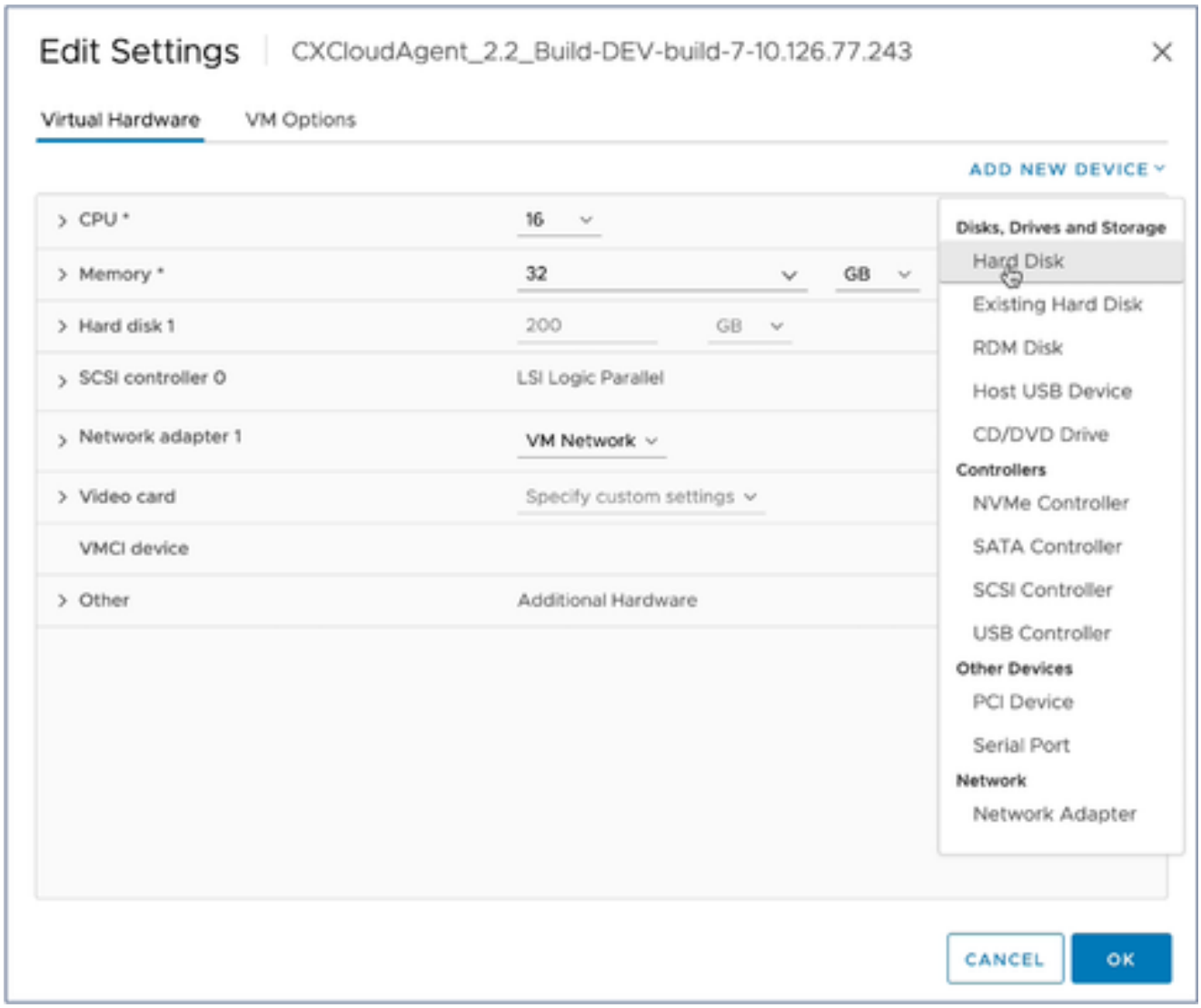
VMのリスト

2. ターゲットVMを右クリックし、メニューからEdit Settingsを選択します。Edit Settingsウィンドウが開きます。



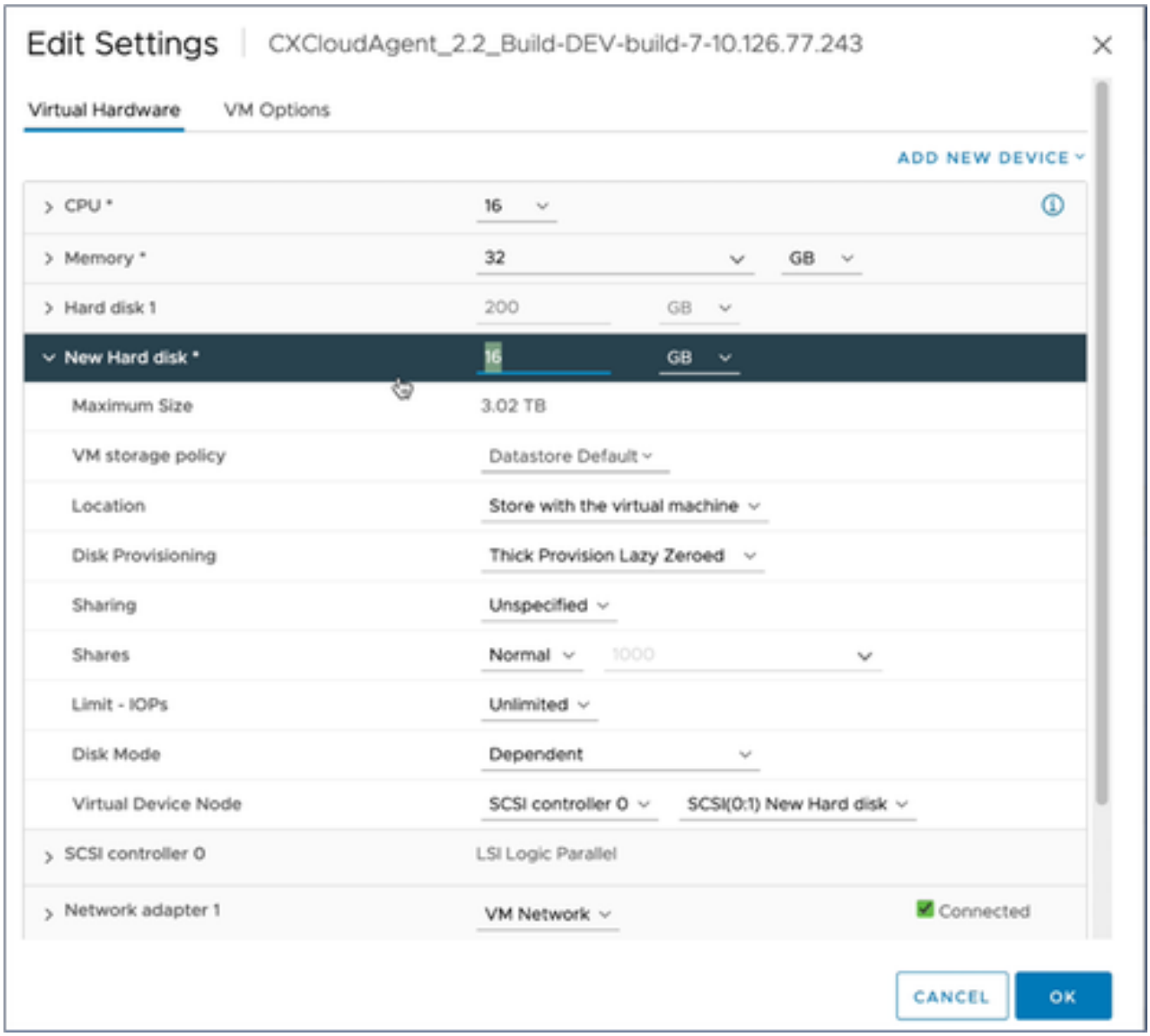
設定の編集

3. 指定に従ってCPU値を更新します:
   中：16コア（8ソケット*2コア/ソケット）
   大：32コア（16ソケット*2コア/ソケット）
4. 指定に従ってMemoryの値を更新します。
   中：32 GB
   大：64 GB



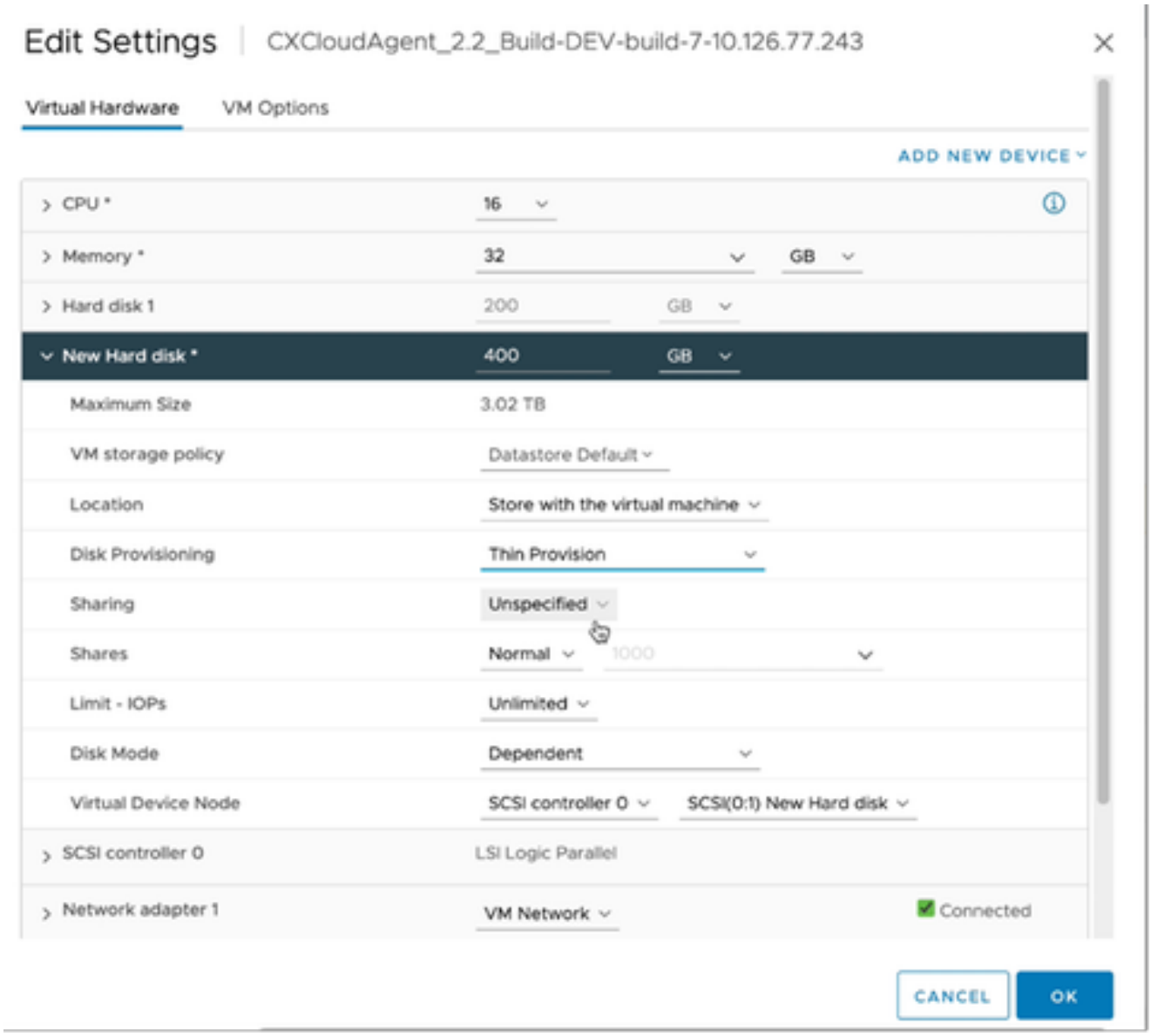
設定の編集

5. Add New Deviceをクリックして、Hard Diskを選択します。New Hard diskエントリが追加されます。



設定の編集

6. 指定に従って新しいハードディスクメモリをアップデートします。
   小規模から中規模：400 GB（初期サイズは200 GB、総容量は600 GBに増加）
   小規模から大規模：1000 GB（初期サイズは200 GB、総容量は1200 GBに増加）



設定の編集

7. Disk Provisioningドロップダウンリストから、Thin Provisioningを選択します。
8. OKをクリックして、アップグレードを完了します。

導入とネットワーク設定

CXエージェントを導入するには、次のいずれかのオプションを選択します。

- VMware vSphere/vCenterシッククライアントESXi 5.5/6.0
- VMware vSphere/vCenter Web Client ESXi 6.0またはWeb Client vCenterのインストール
- Oracle Virtual Box 7.0.12
- Microsoft Hyper-V のインストール

OVA の導入

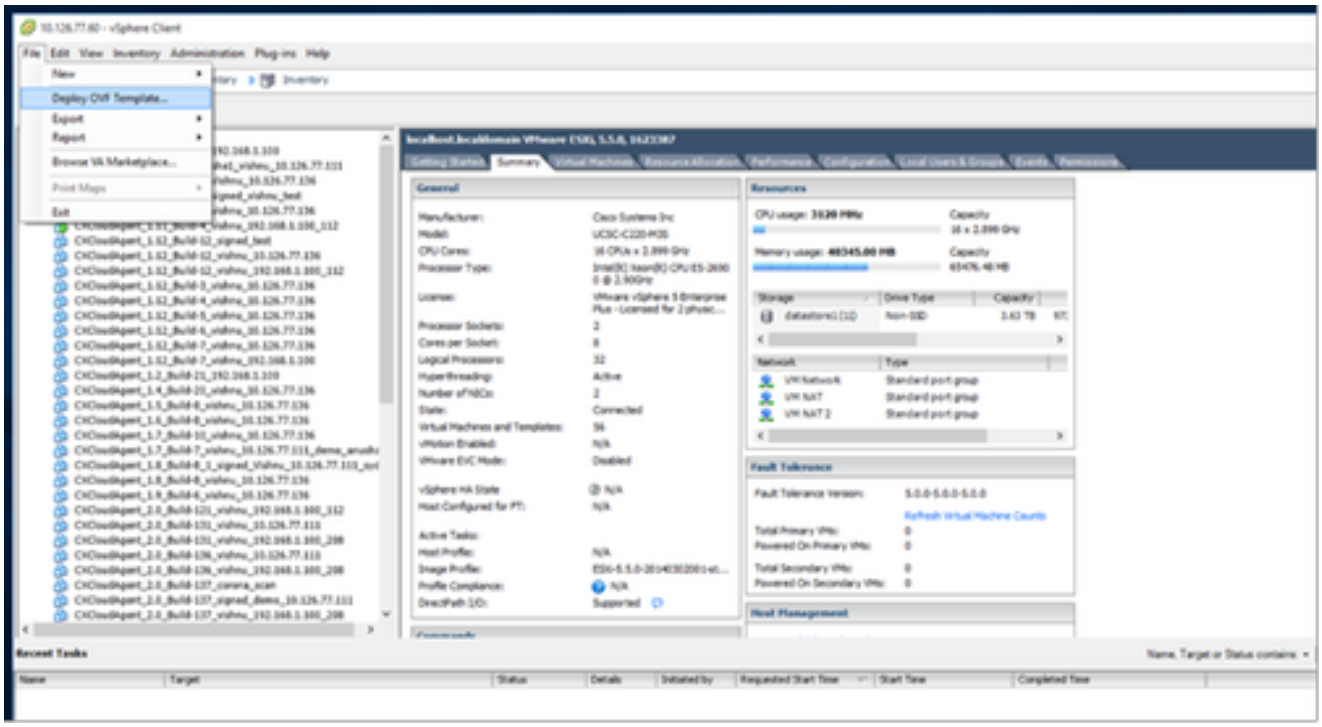
シッククライアント ESXi 5.5/6.0 のインストール

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エージェントOVAを導入できます。

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。

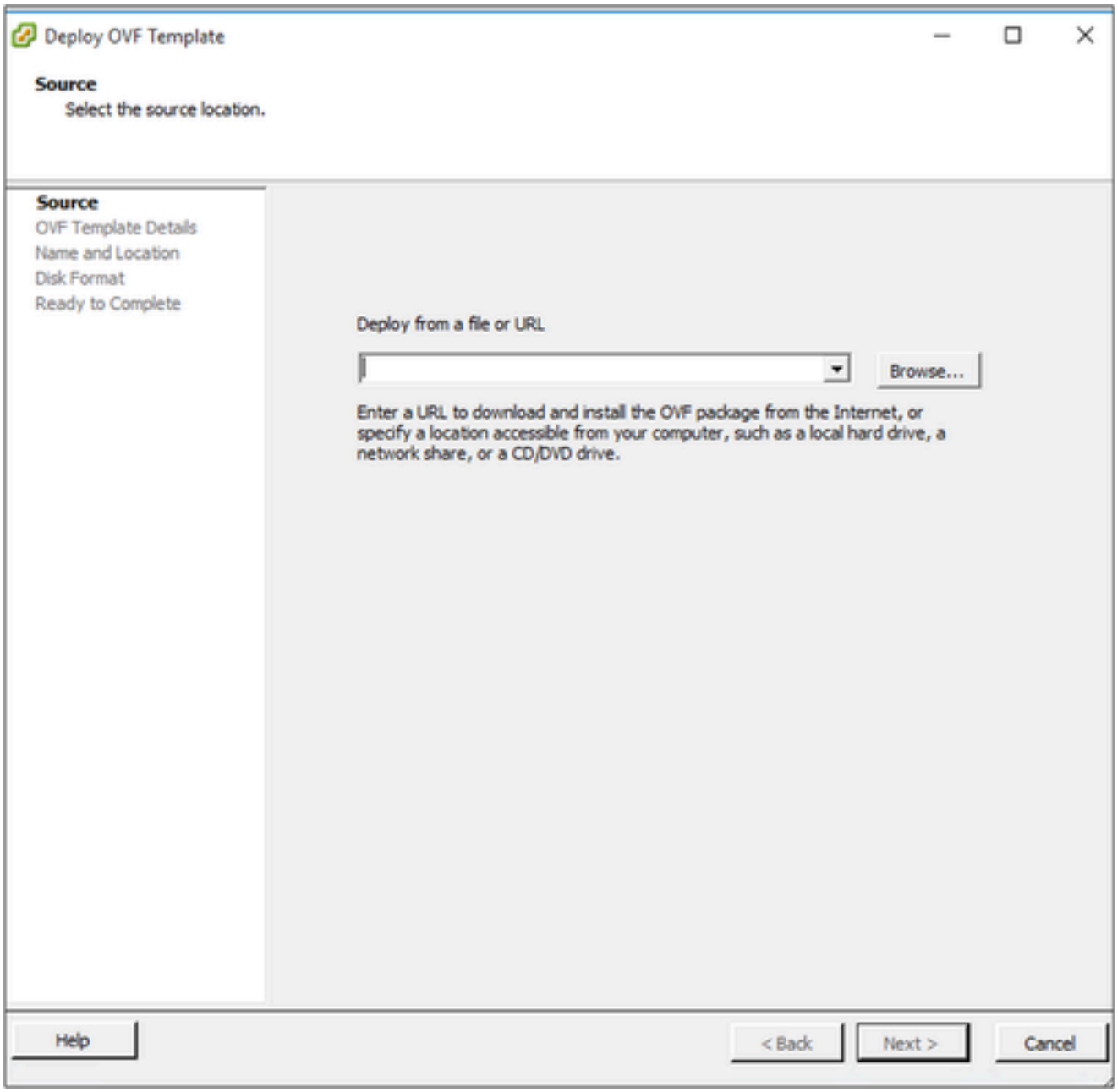
ログイン

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



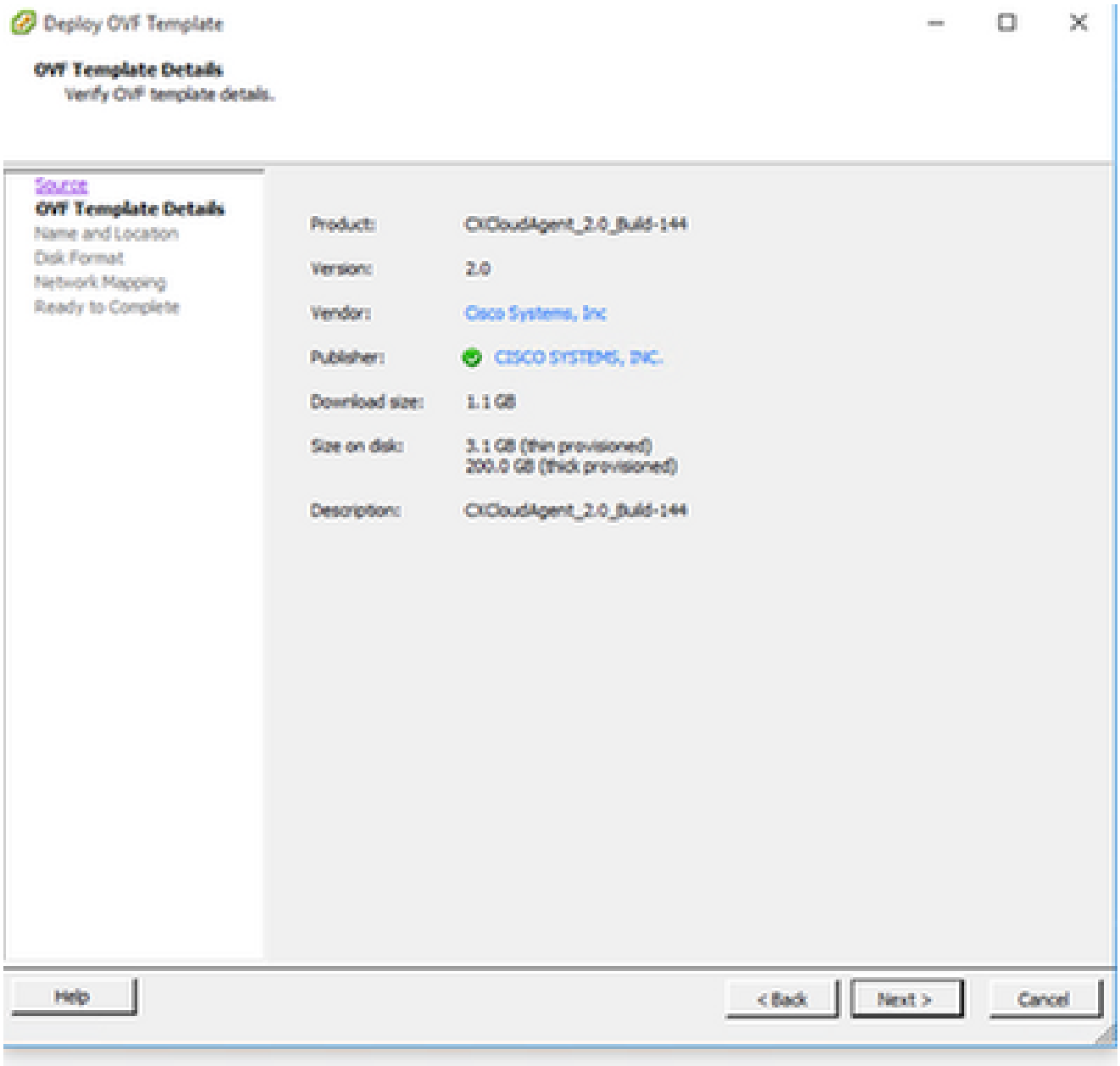
vSphere クライアント

3. OVAファイルを参照して選択し、Nextをクリックします。



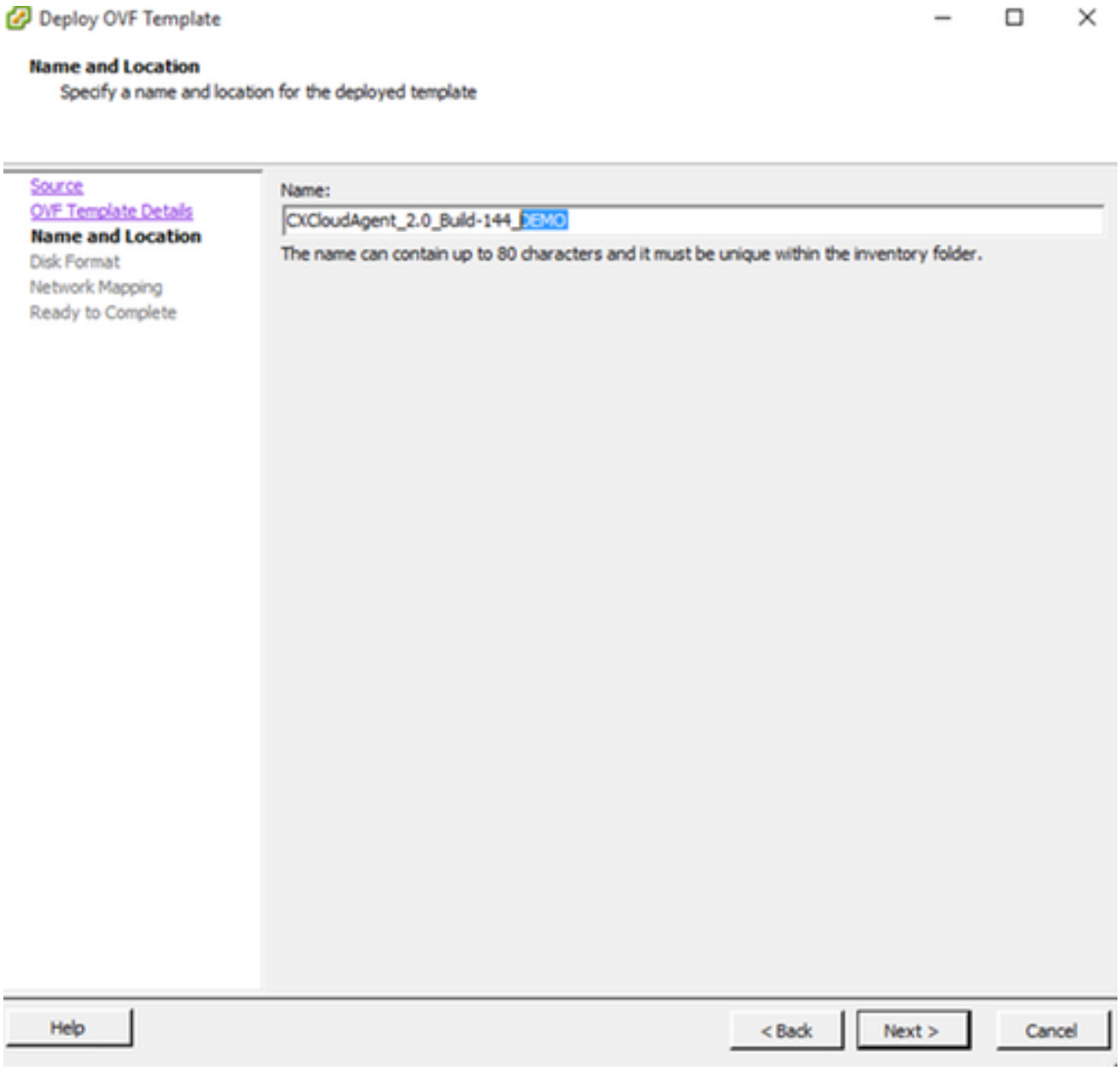
OVA パス

4. OVF Detailsを確認し、Nextをクリックします。



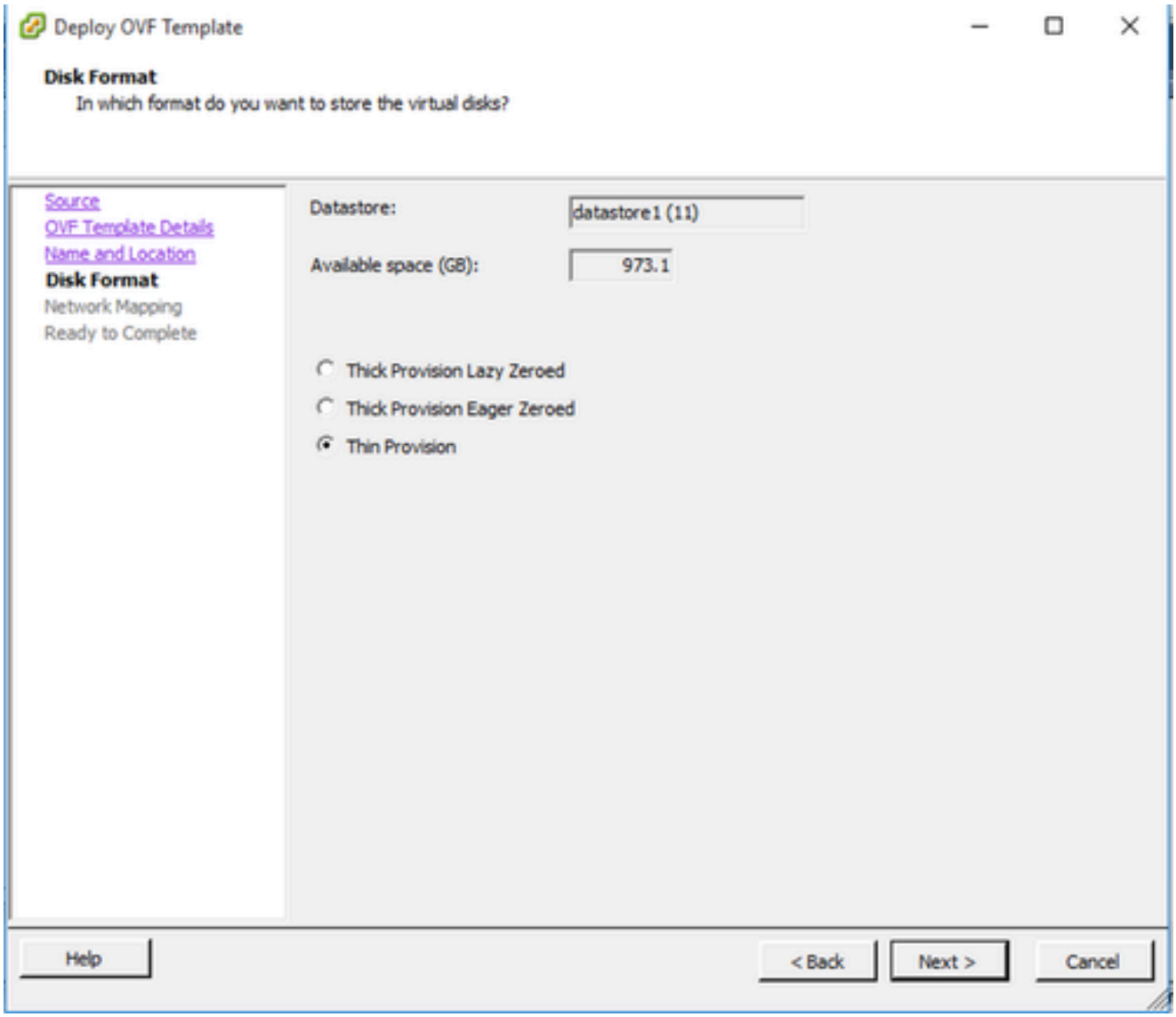
テンプレートの詳細

5. 一意の名前を入力して、Nextをクリックします。



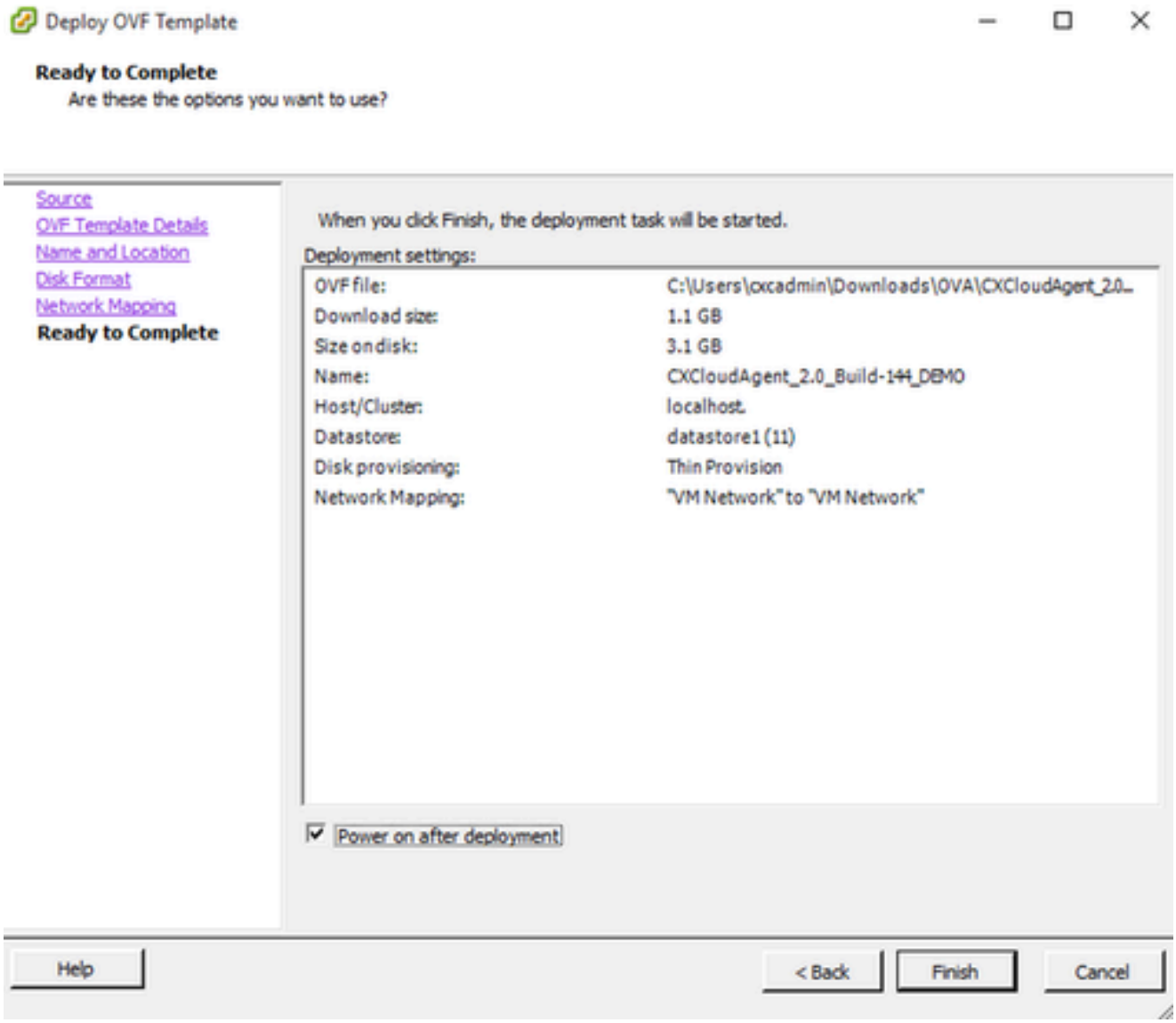
名前と場所

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



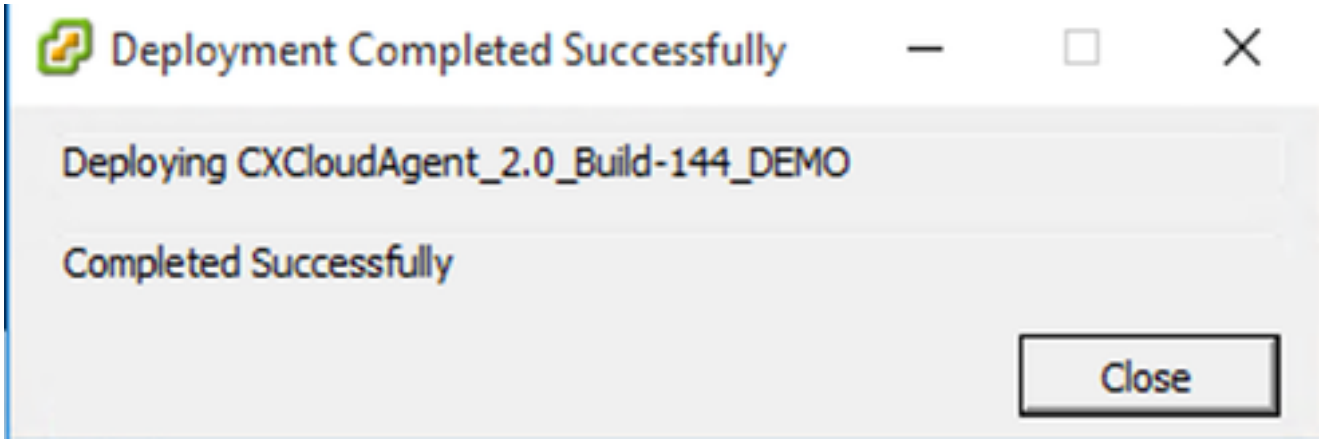
ディスクの書式設定

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。導入が成功すると、確認の画面が表示されます。



導入の完了

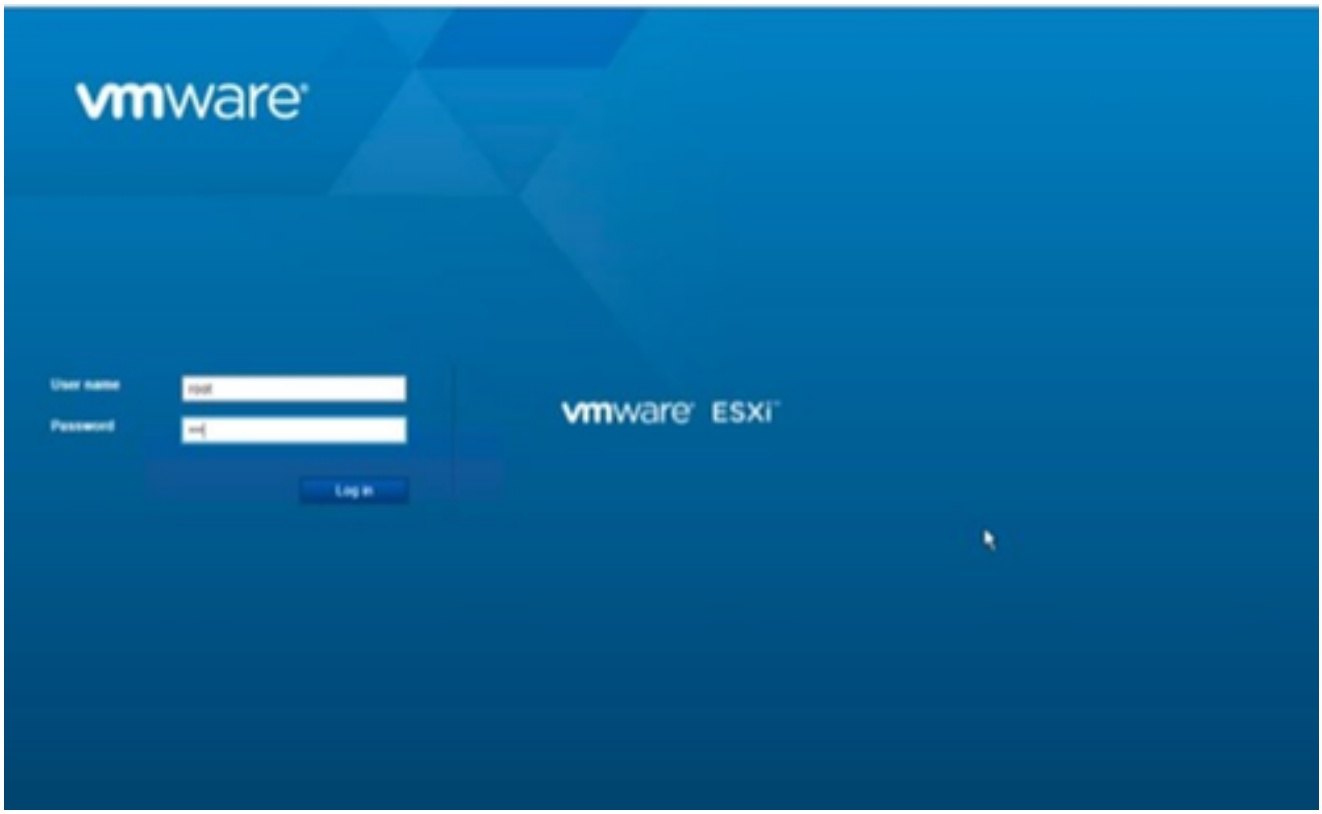
8. 導入したVMを選択し、コンソールを開いてNetwork Configurationに移動し、次の手順に進

みます。

Web クライアント ESXi 6.0 のインストール

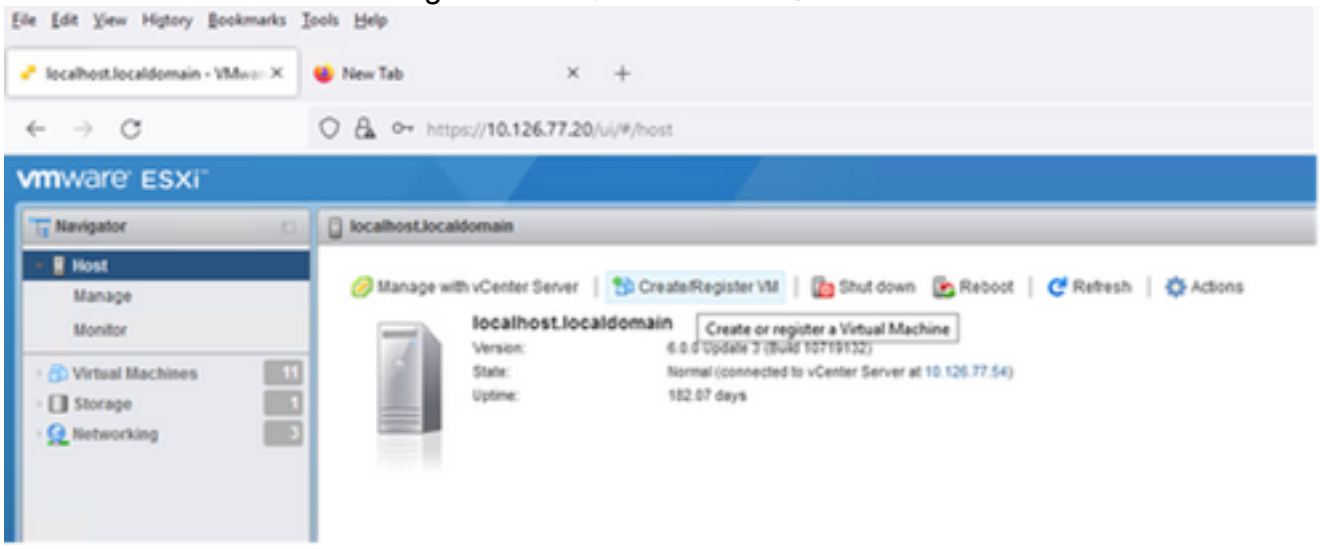
このクライアントは、vSphere Webを使用してCX Cloud OVAを導入します。

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。



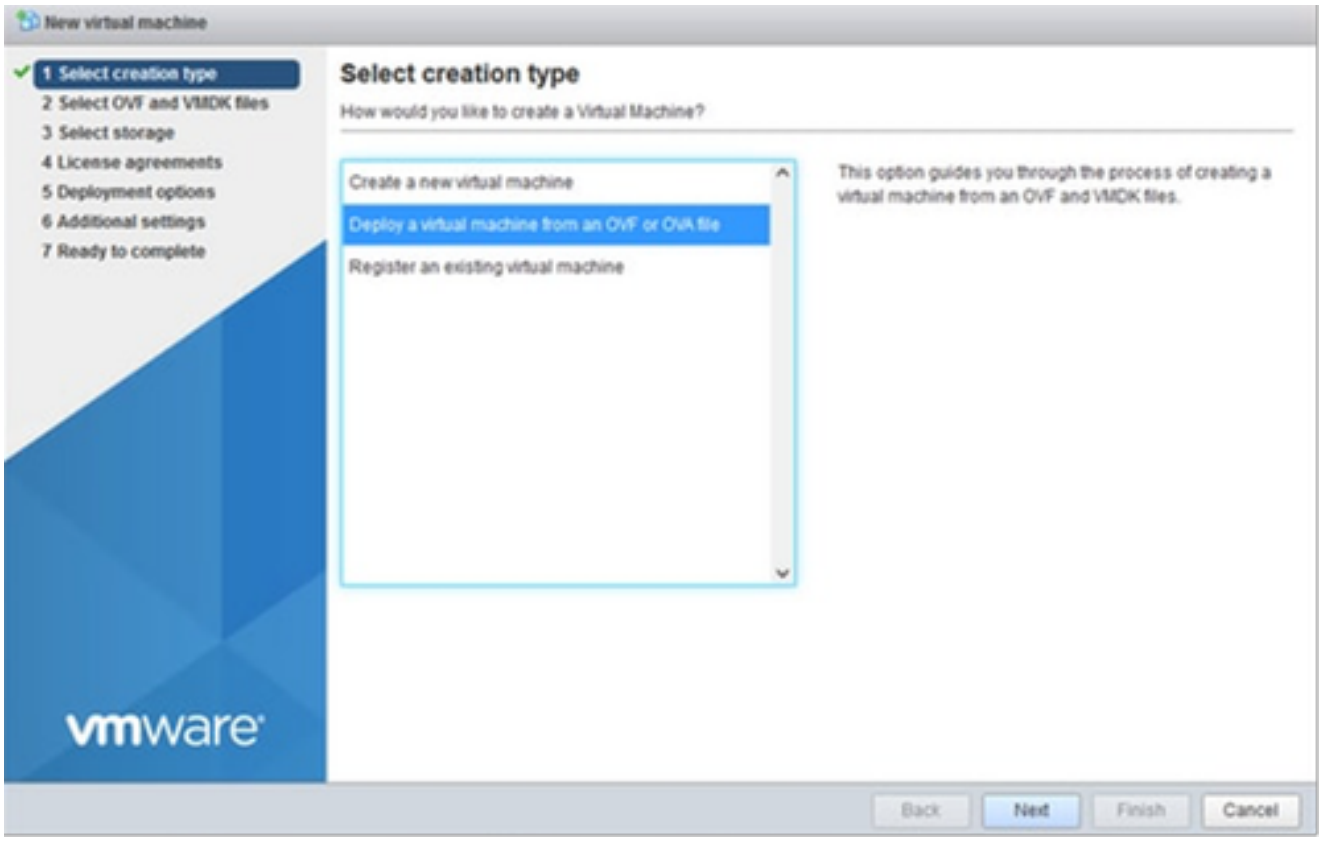
VMware ESXi のログイン

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



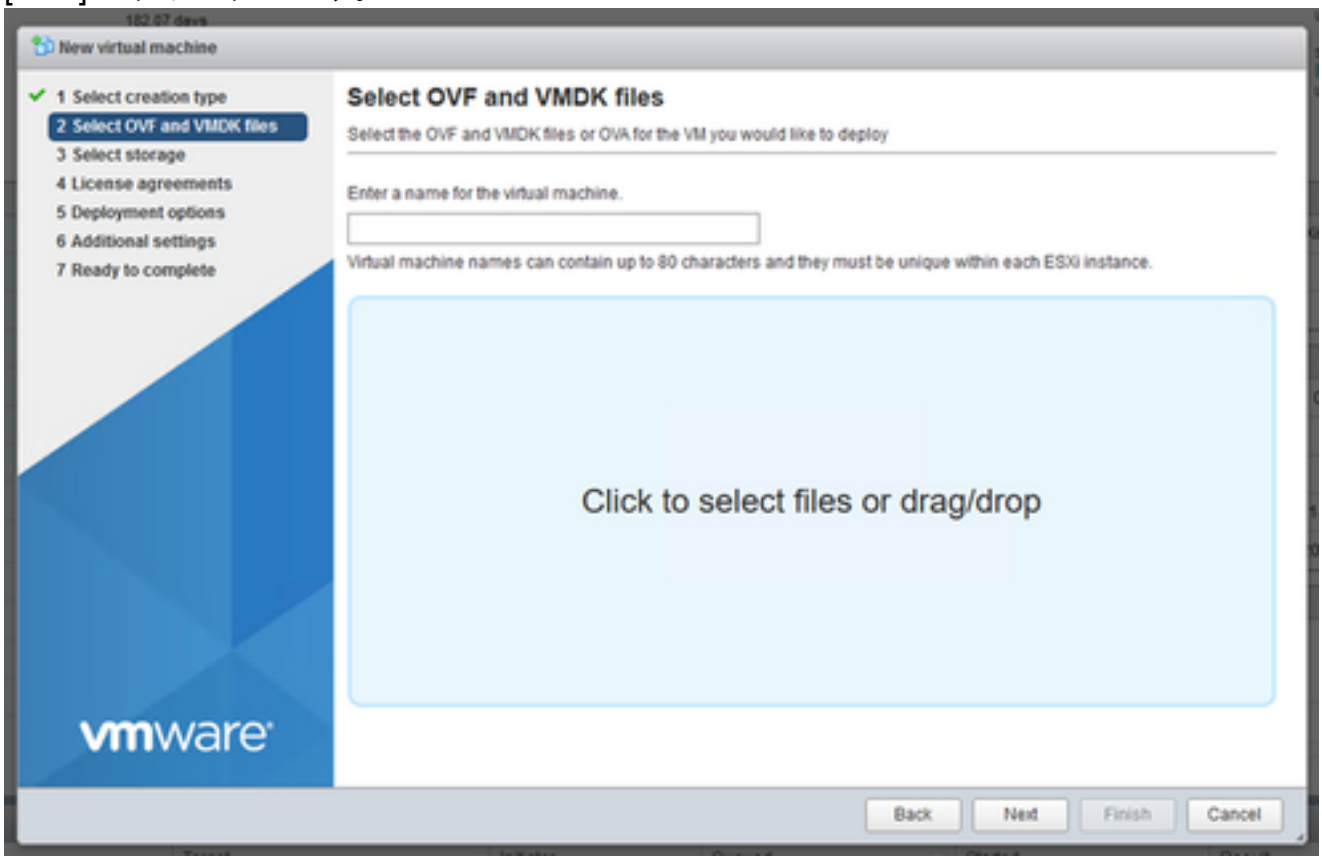
VM の作成

3. Deploy a virtual machine from an OVF or OVA fileを選択し、Nextをクリックします。



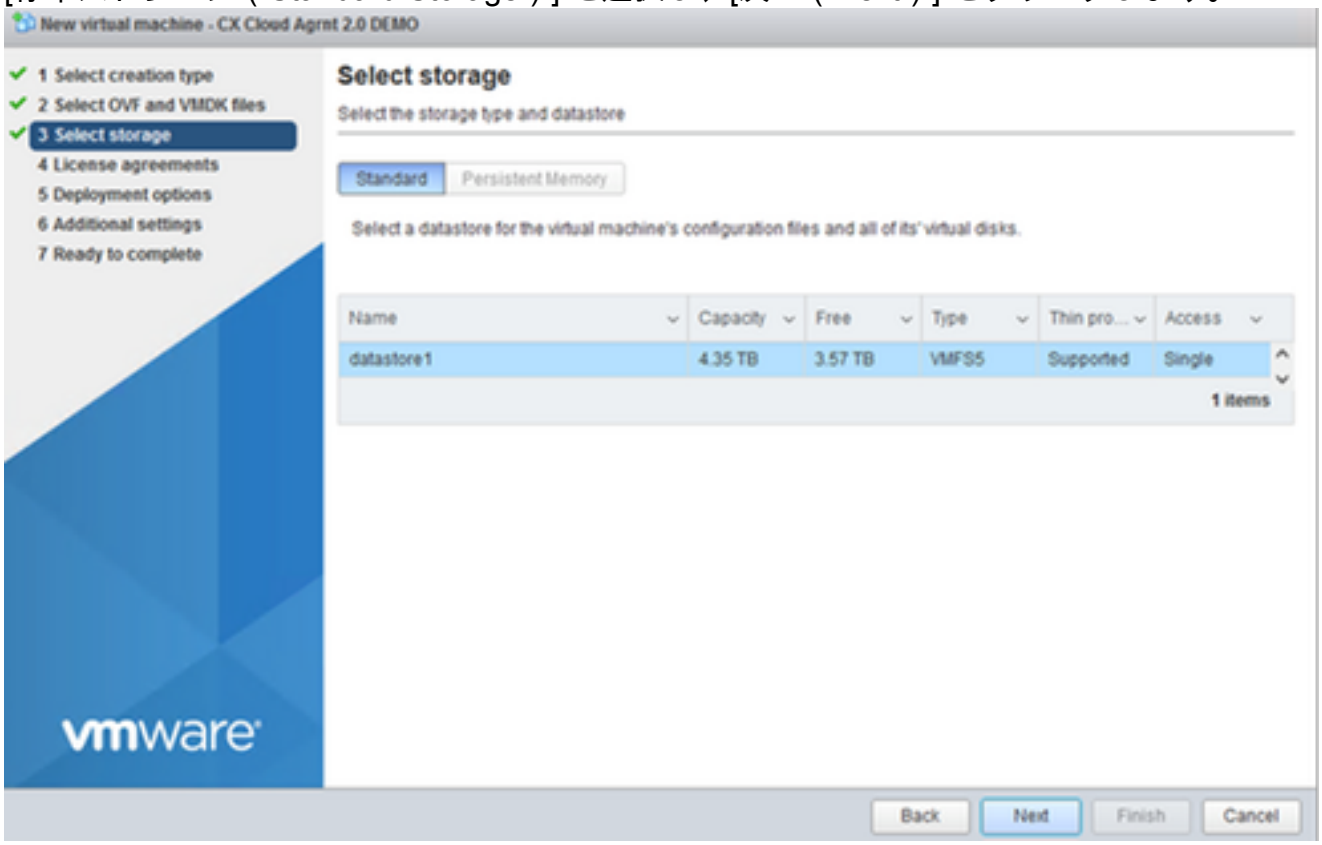
作成タイプの選択

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。



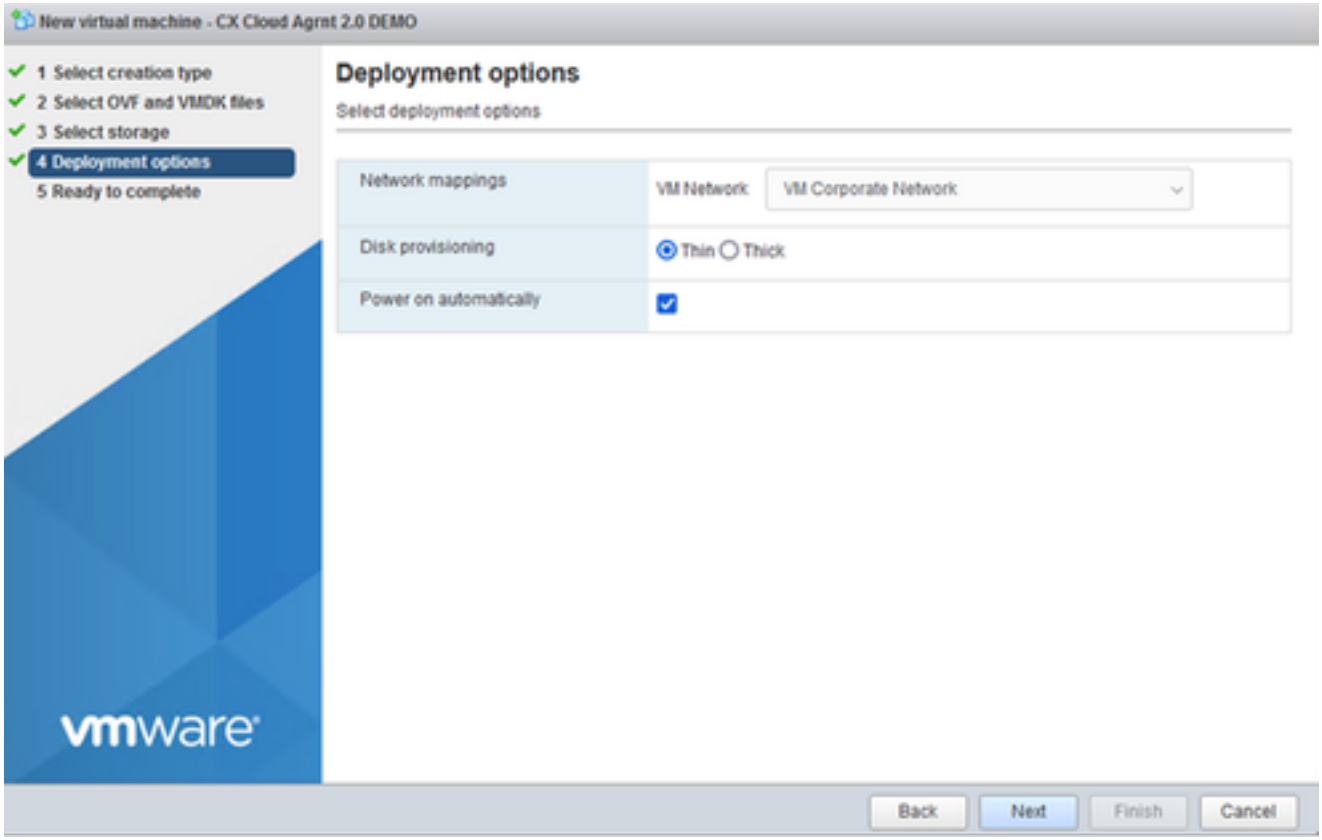
OVA の選択

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。



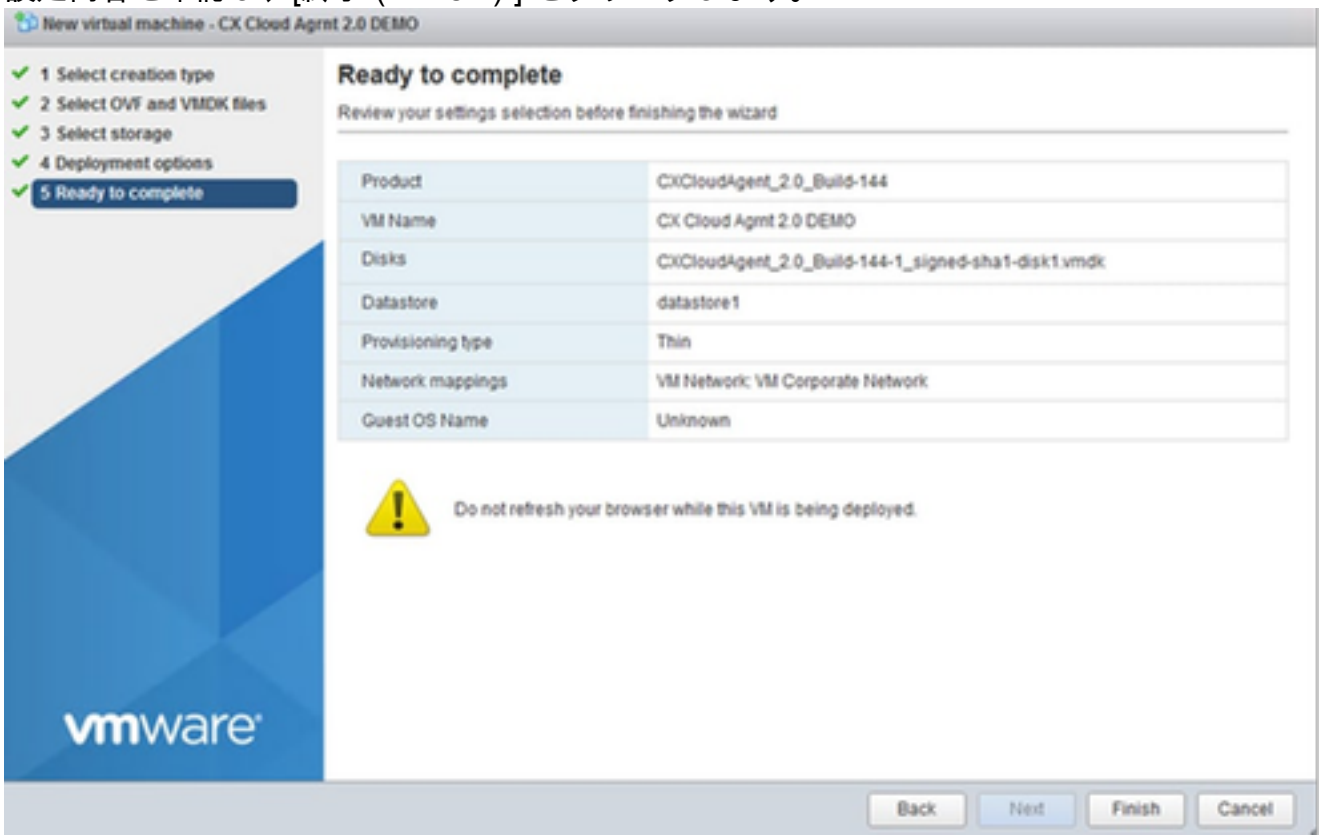
ストレージの選択

7. 適切な導入オプションを選択し、Nextをクリックします。

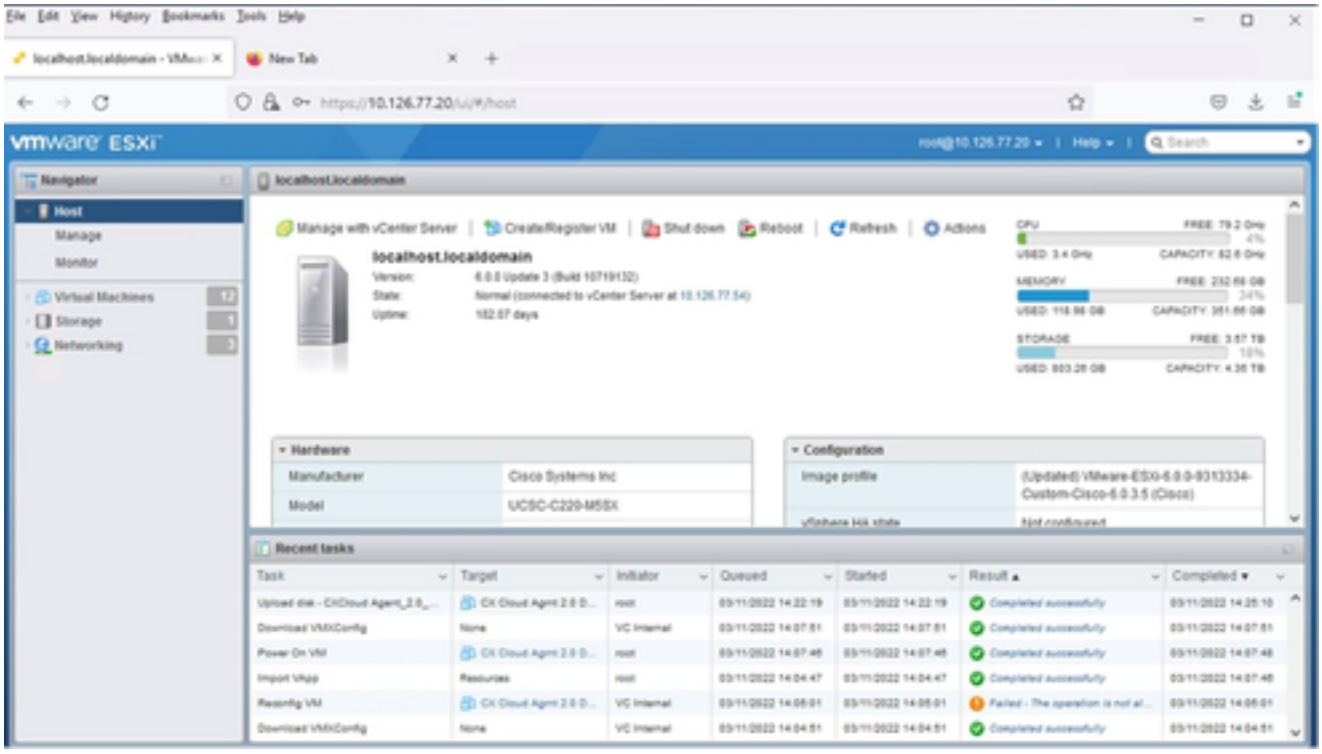


導入オプション

8. 設定内容を確認し、[終了（Finish）] をクリックします。

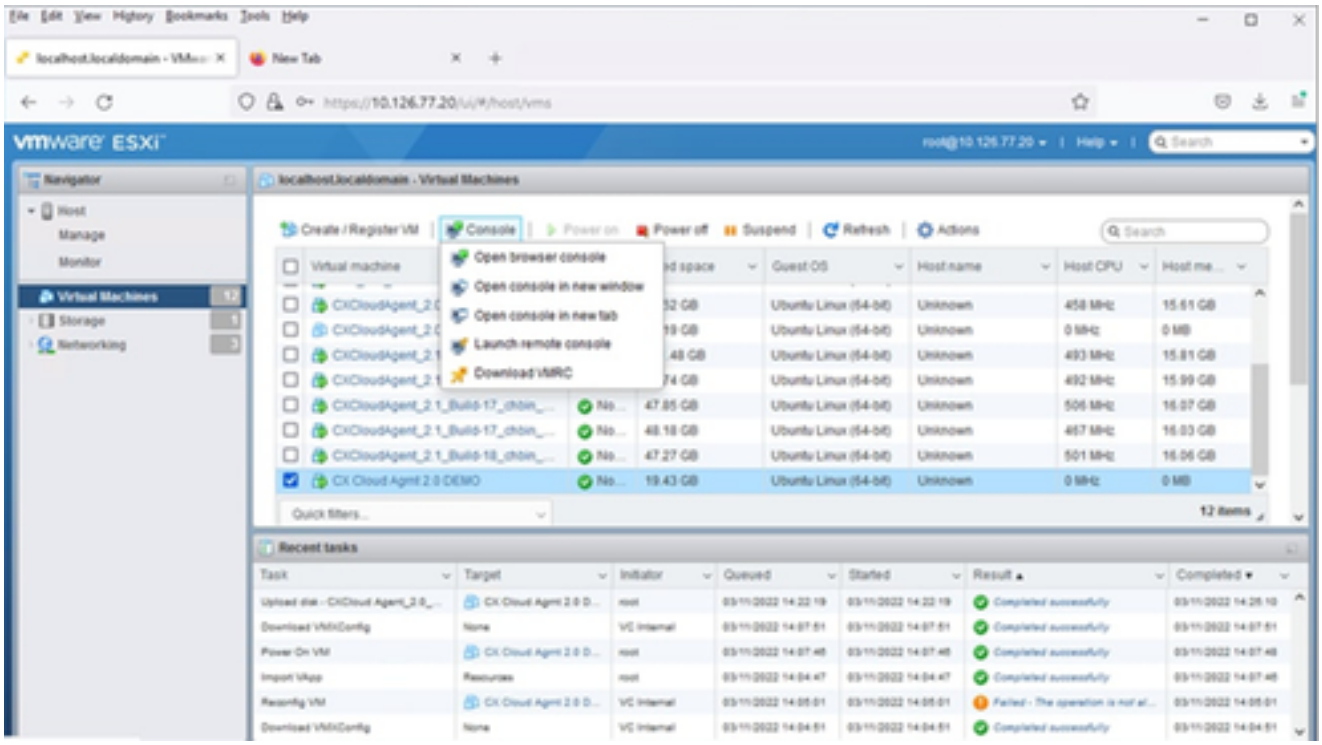


終了準備の完了（Ready to Complete）



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。



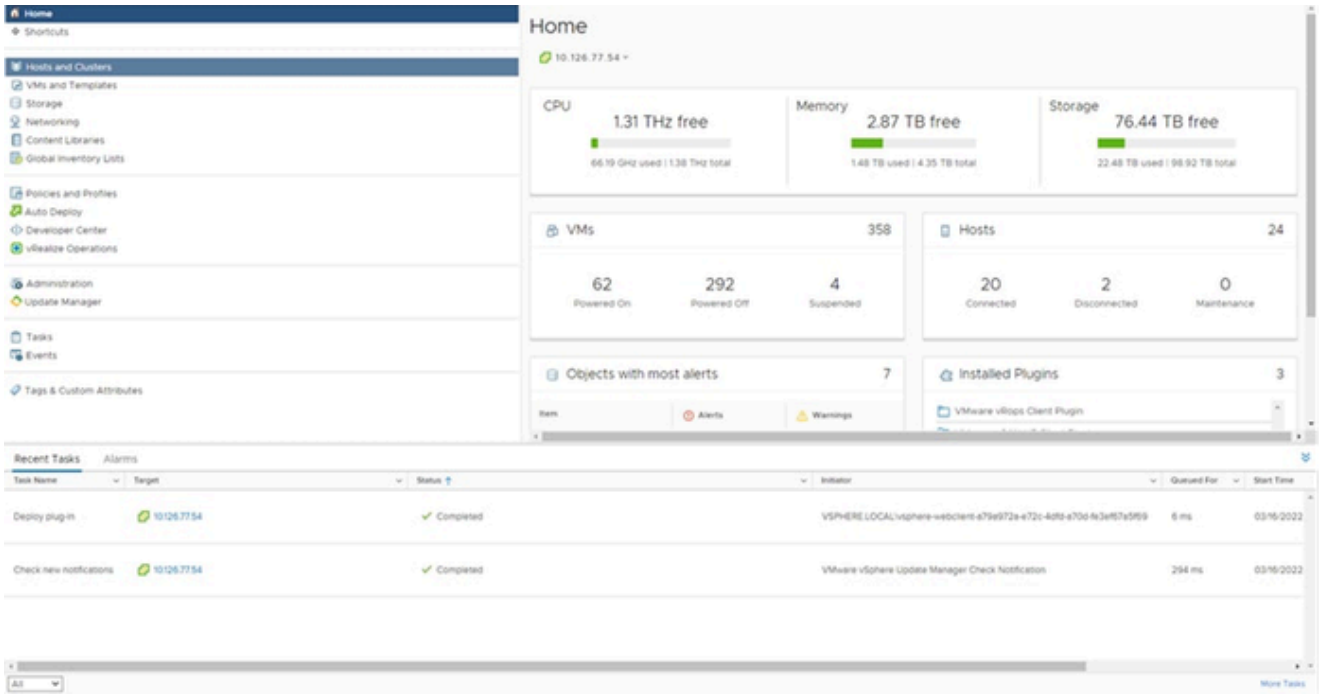
コンソール

10. Network Configurationの順に移動して、次のステップに進みます。

Web クライアント vCenter のインストール

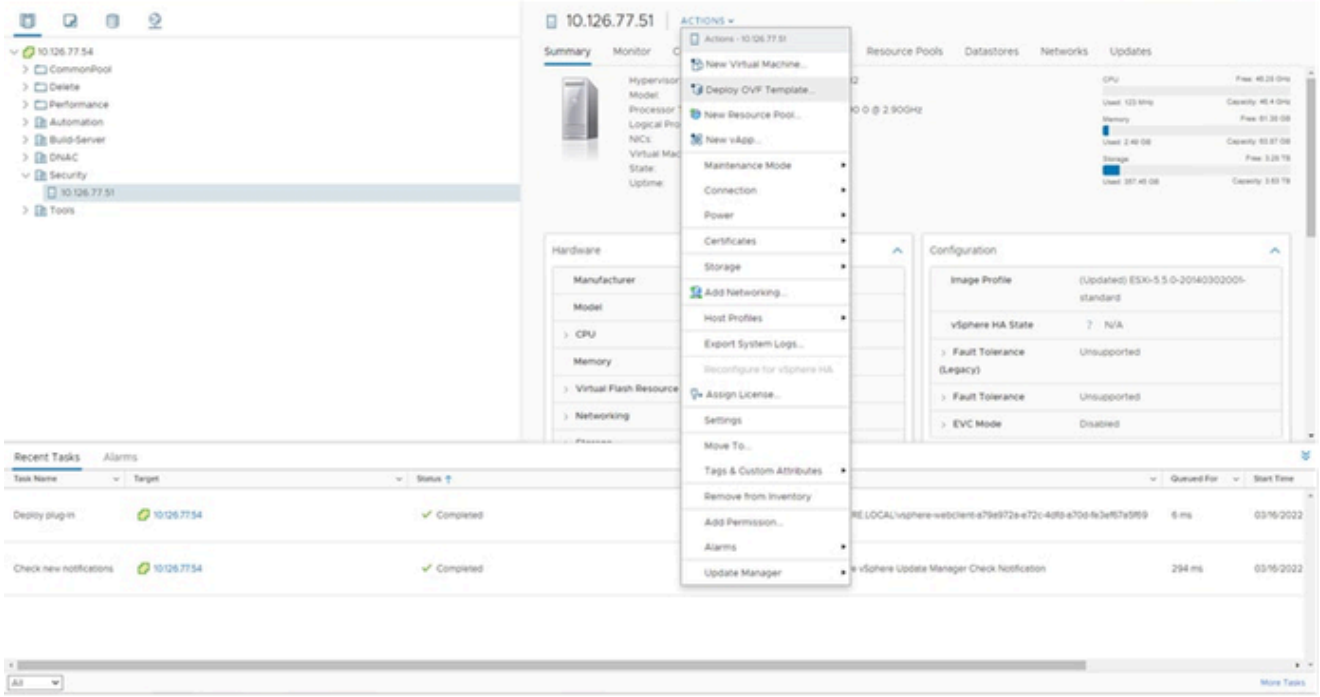
このクライアントでは、WebクライアントvCenterを使用してCXエージェントOVAを導入できます。

1. ESXi/ハイパーバイザ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。



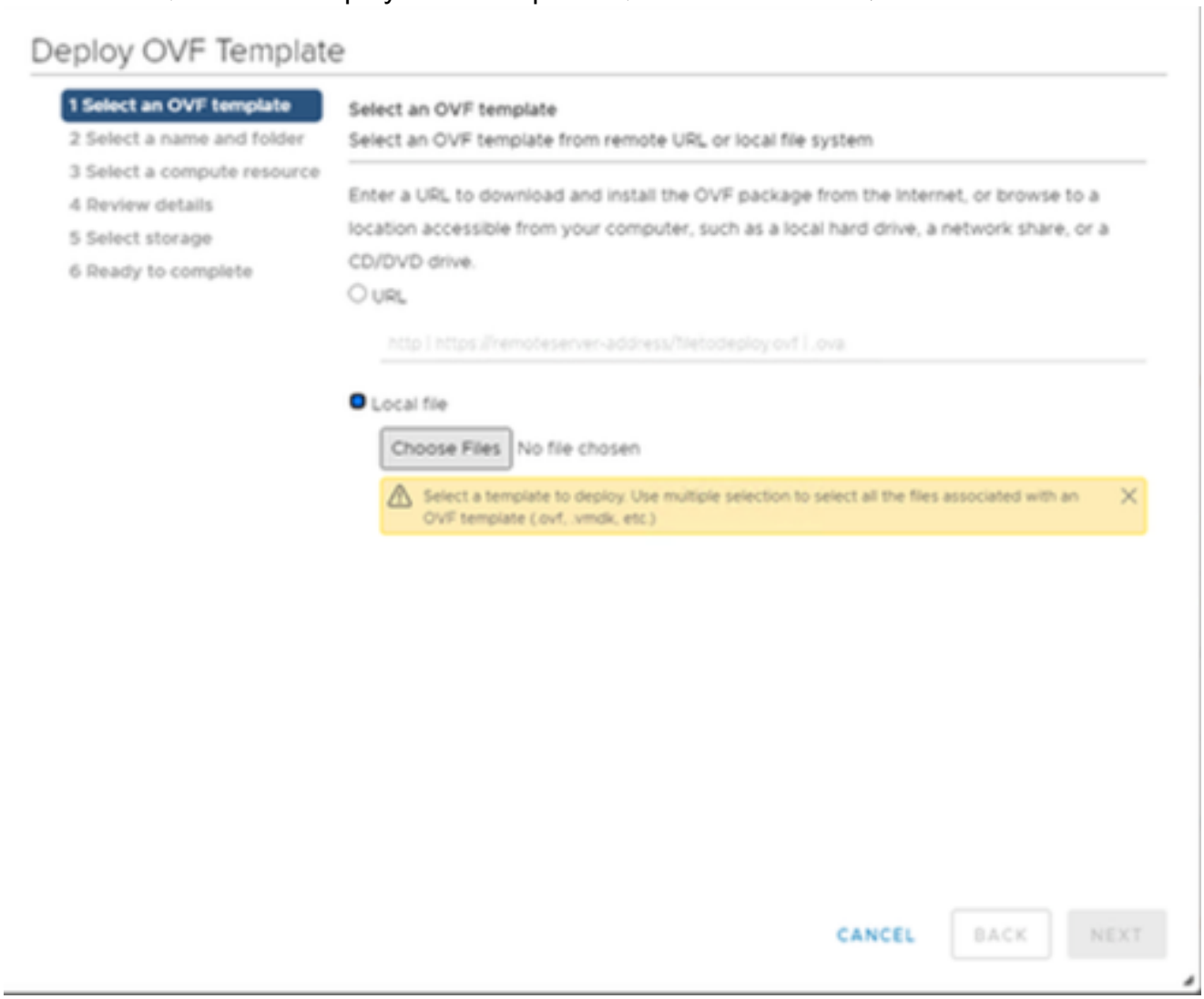
ホームページ

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

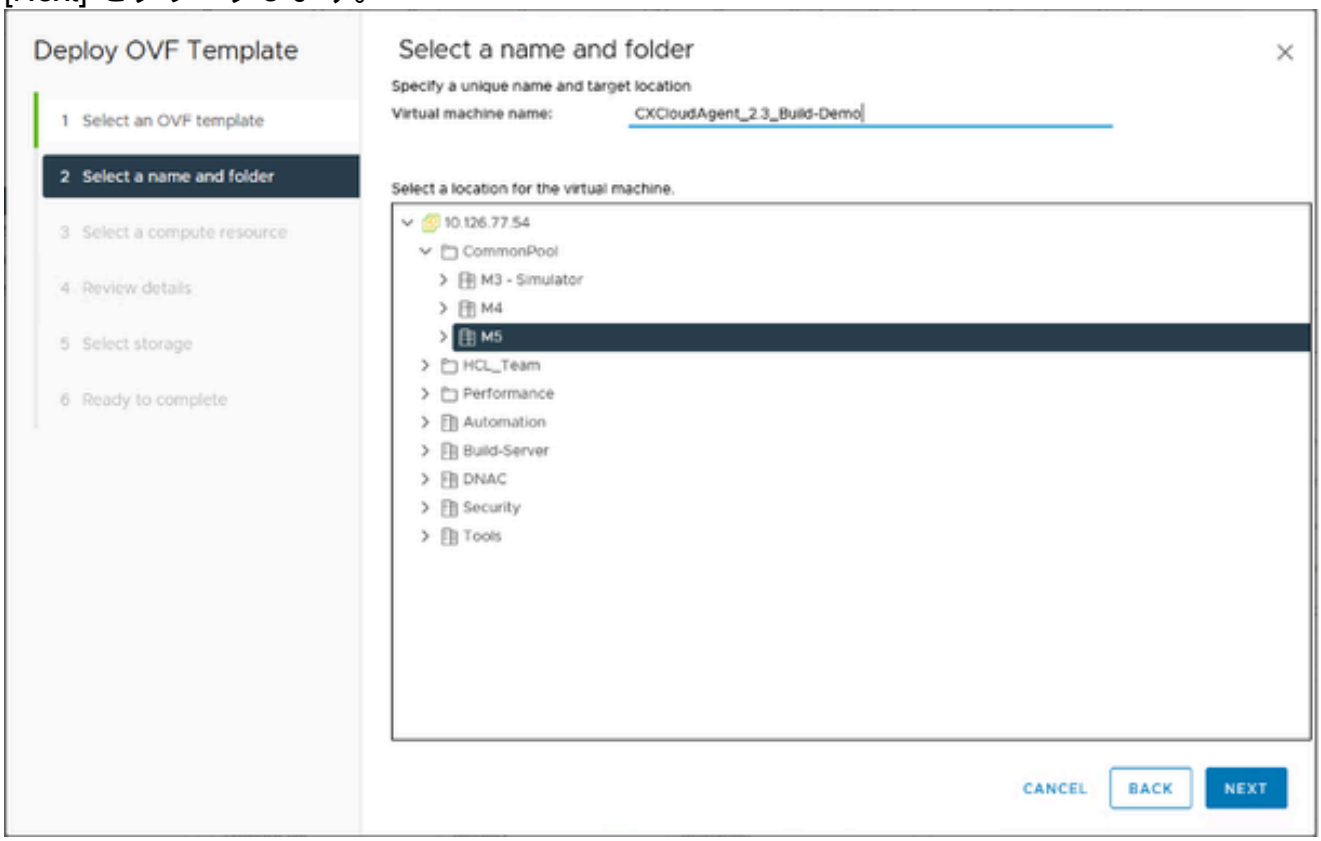


ホストとクラスタ

3. VMを選択し、Action > Deploy OVF Templateの順にクリックします。

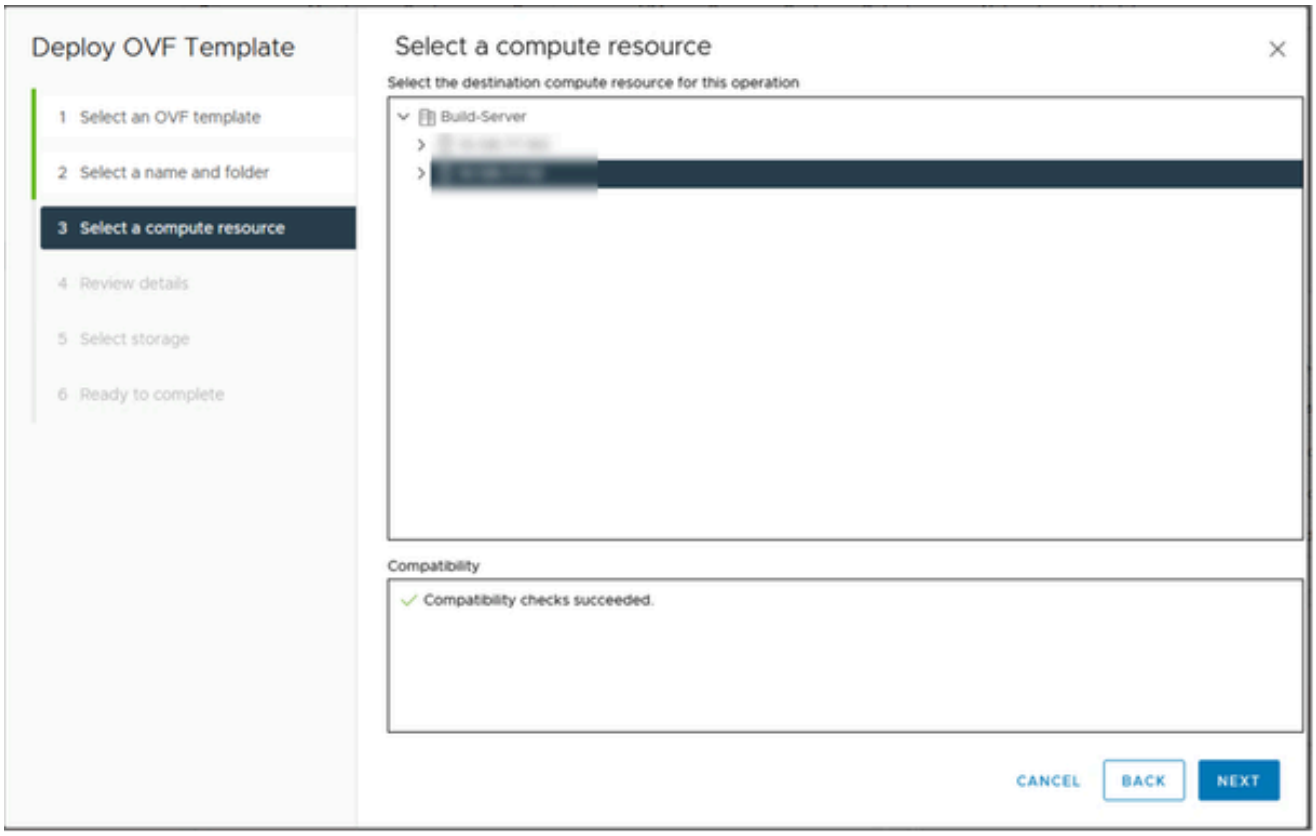


4. URLを直接追加するか、ブラウズしてOVAファイルを選択します。
5. [Next] をクリックします。



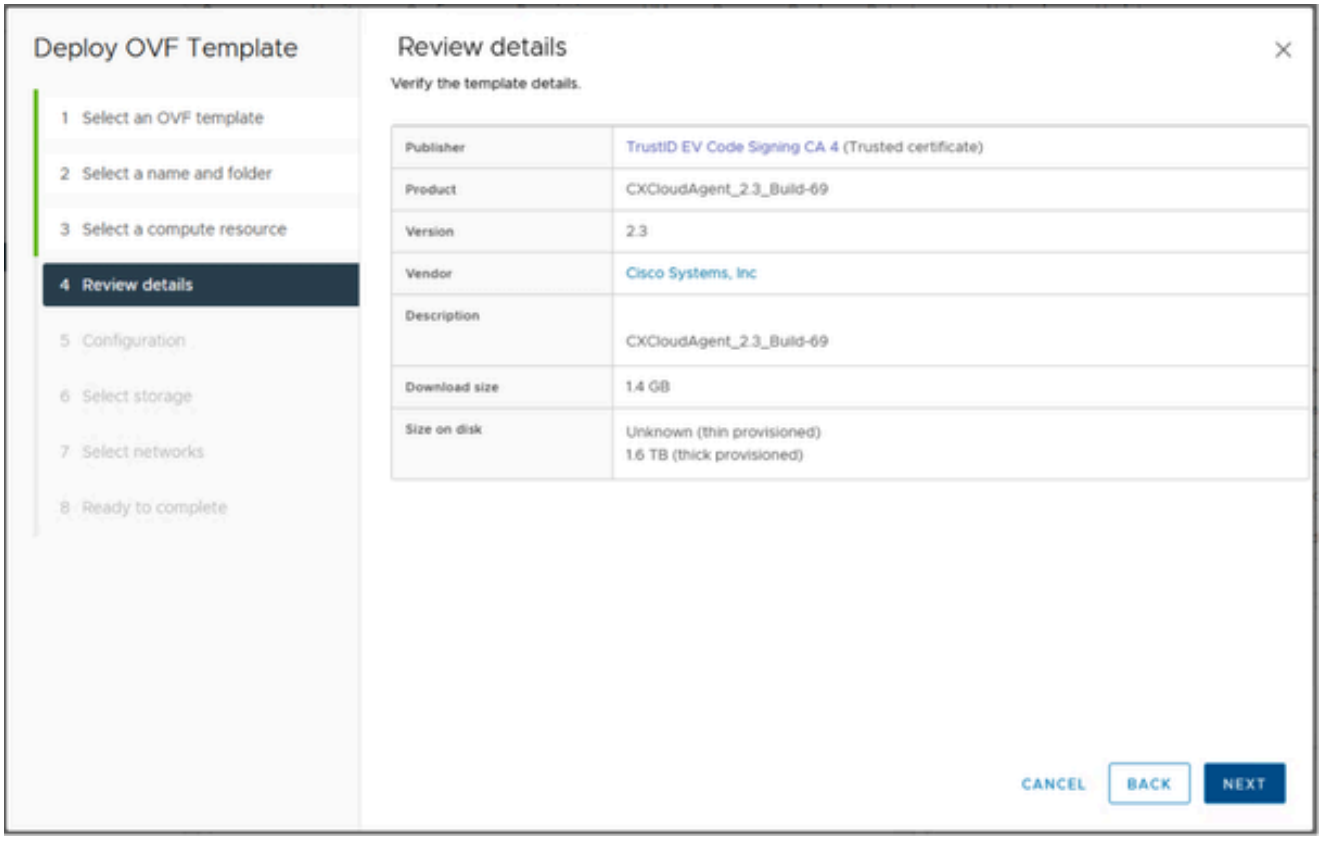
名前とフォルダ

6. 一意の名前を入力し、必要に応じて場所を参照します。
7. [Next] をクリックします。



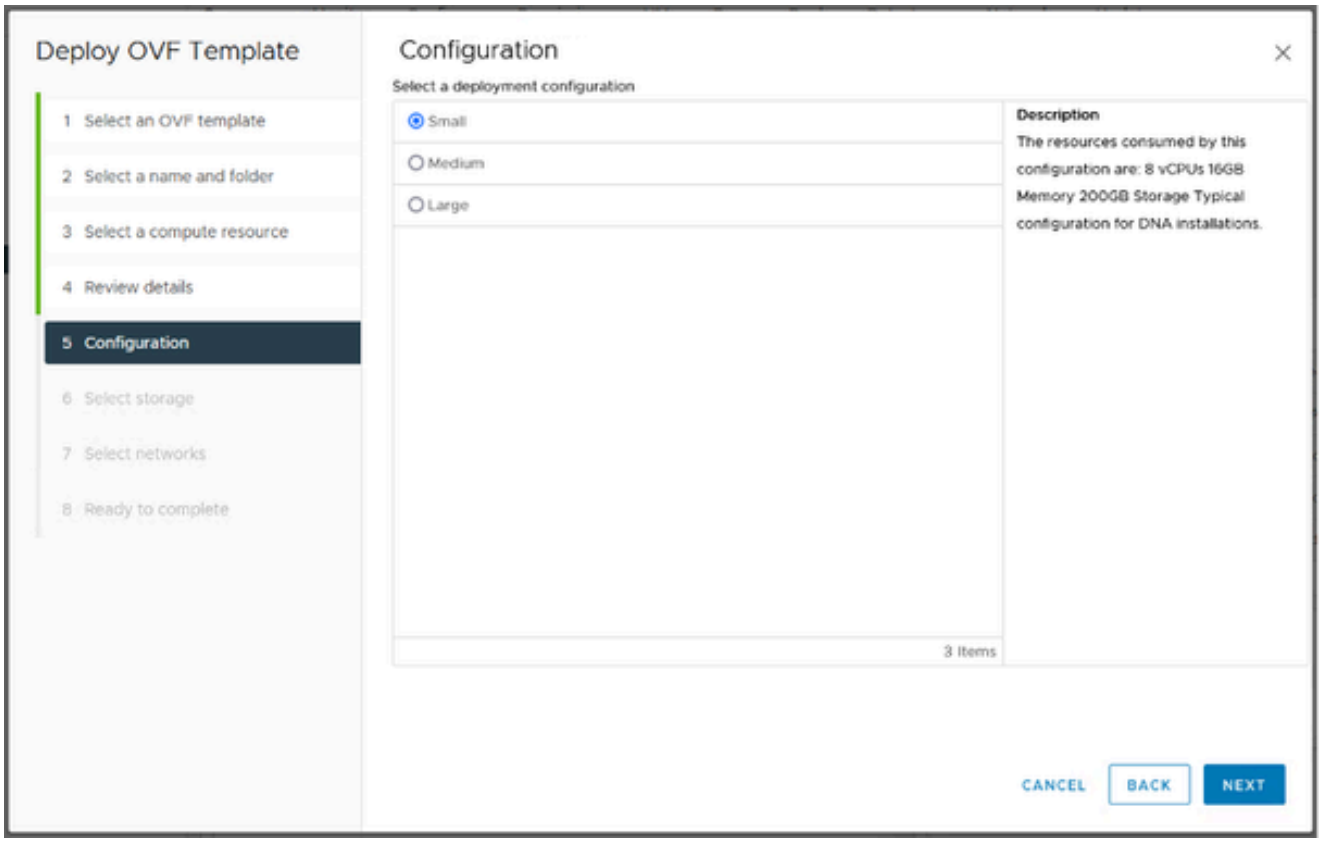
コンピューティングリソースの選択

8. 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。



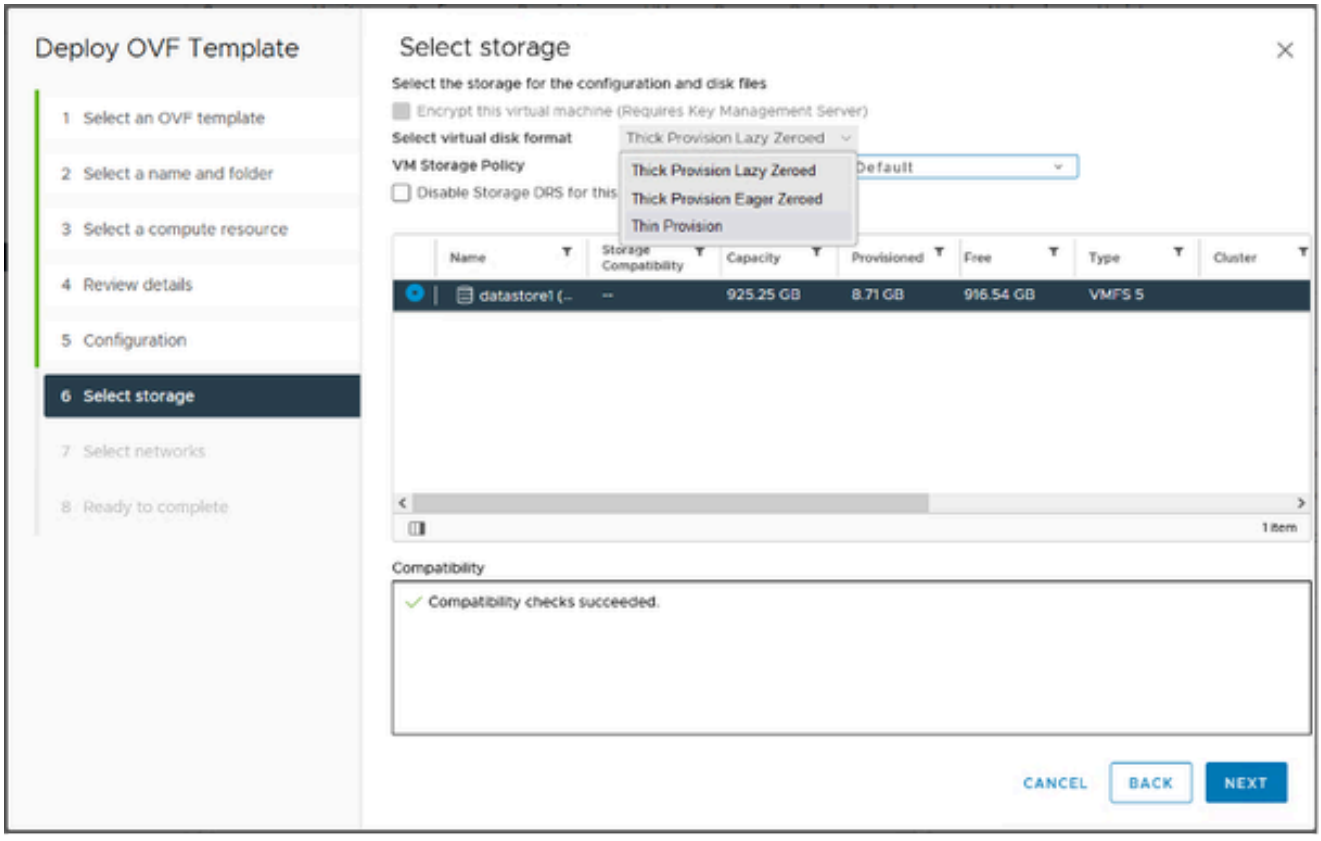
詳細の確認

9. 詳細を確認し、[次へ (Next)] をクリックします。



コンフィギュレーション

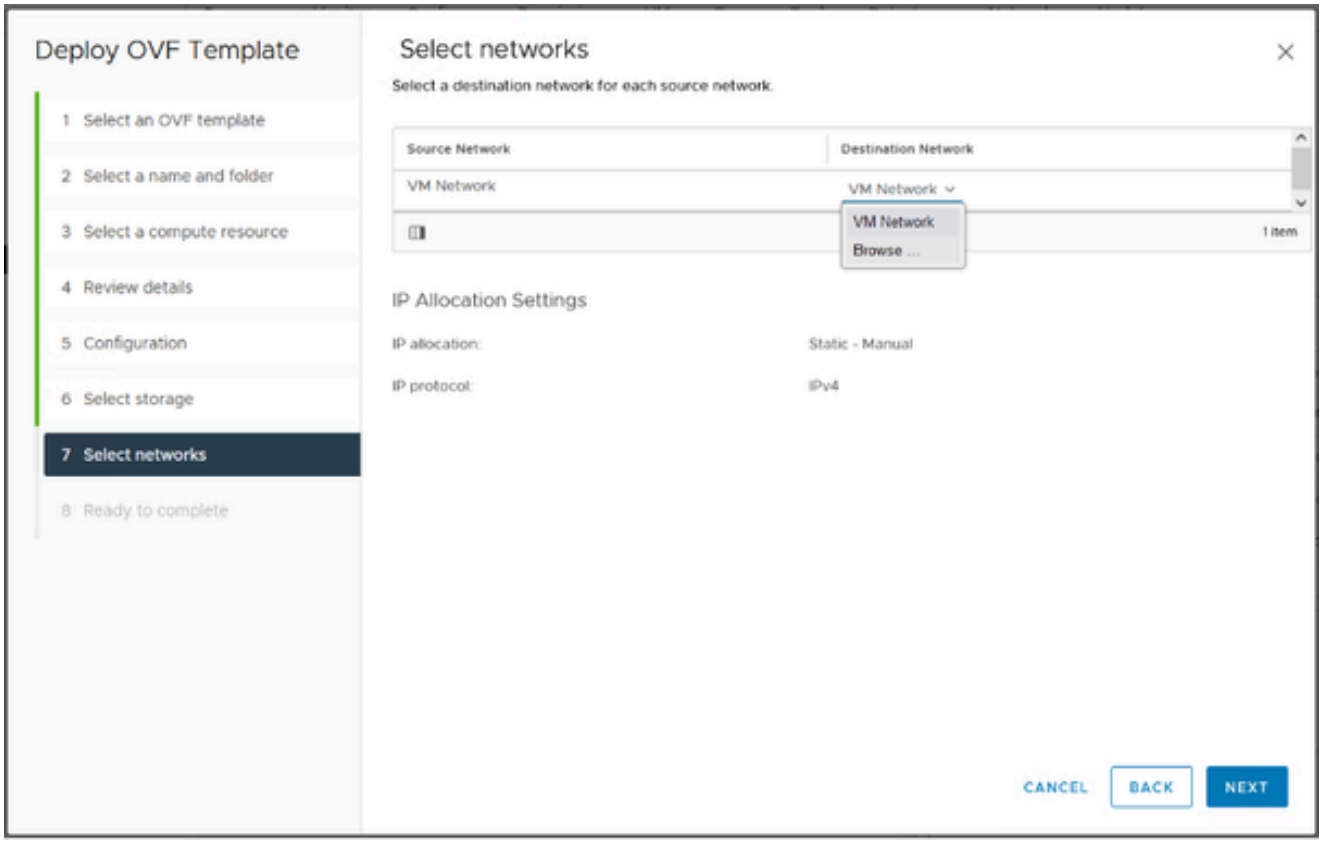
10. 導入設定を選択し、Nextをクリックします。



コンフィギュレーション

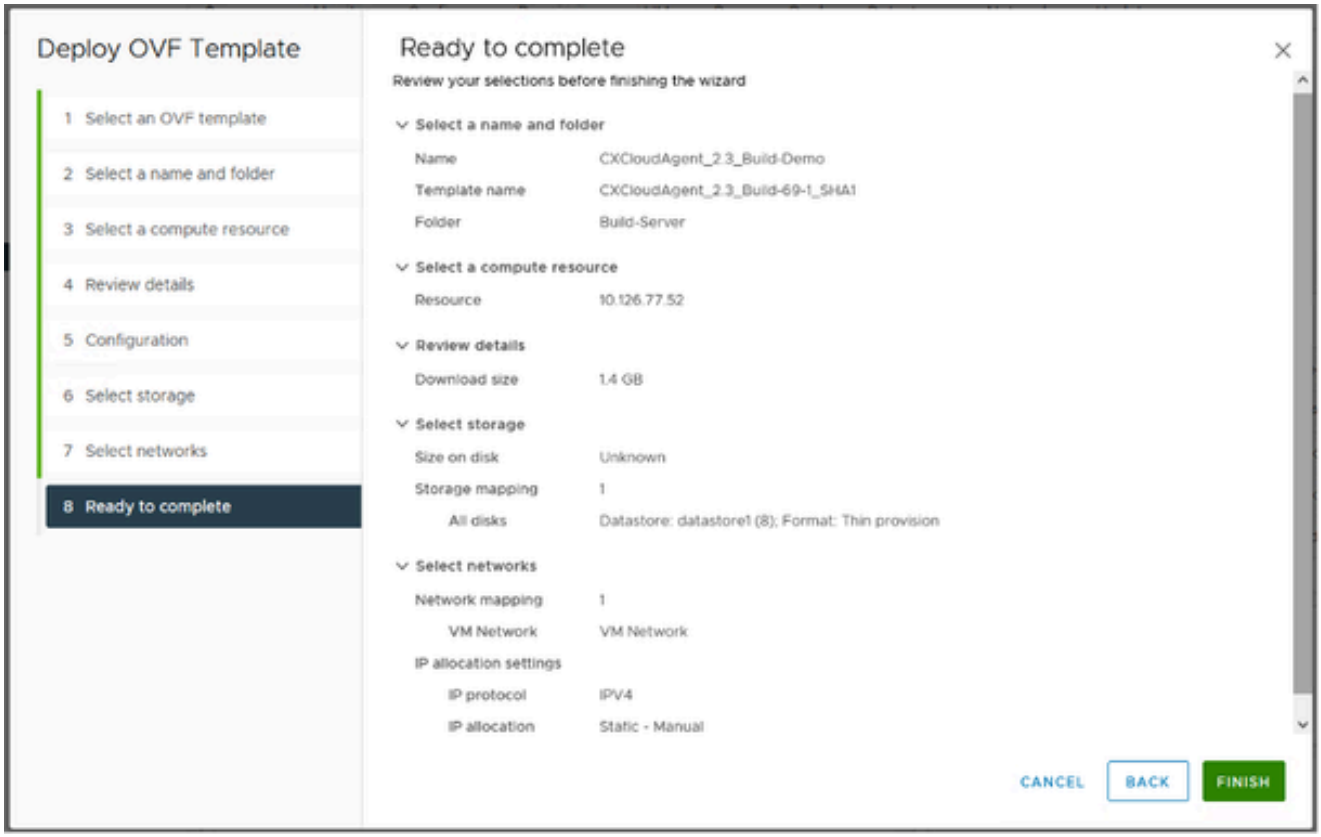
11. ドロップダウンリストからStorage > Select virtual disk formatを選択し、Nextをクリックし

ます。



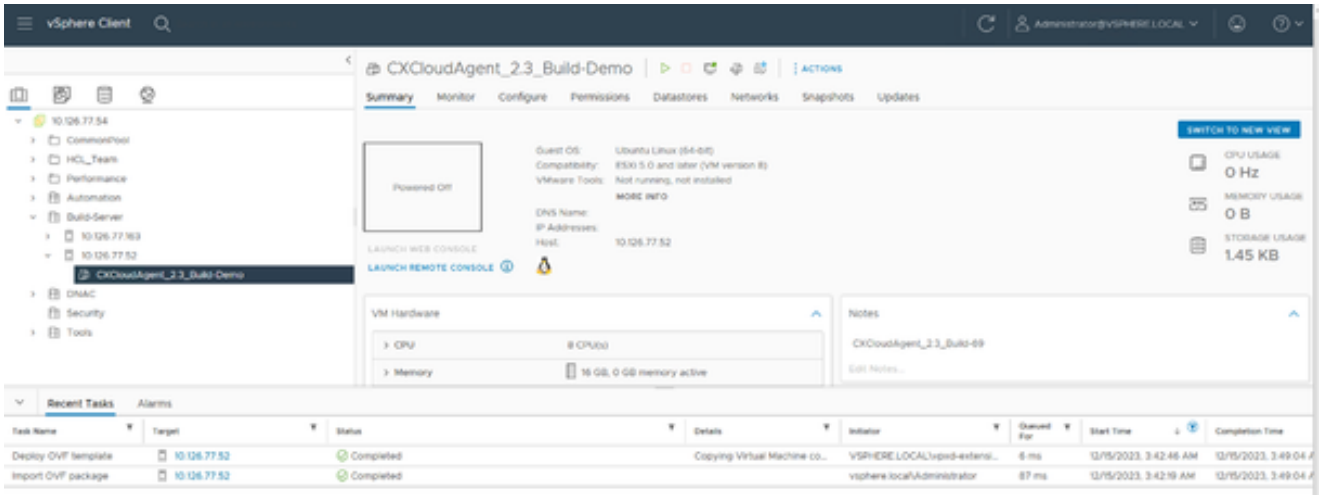
ネットワークの選択

12. Select networksで適切な選択を行い、Nextをクリックします。



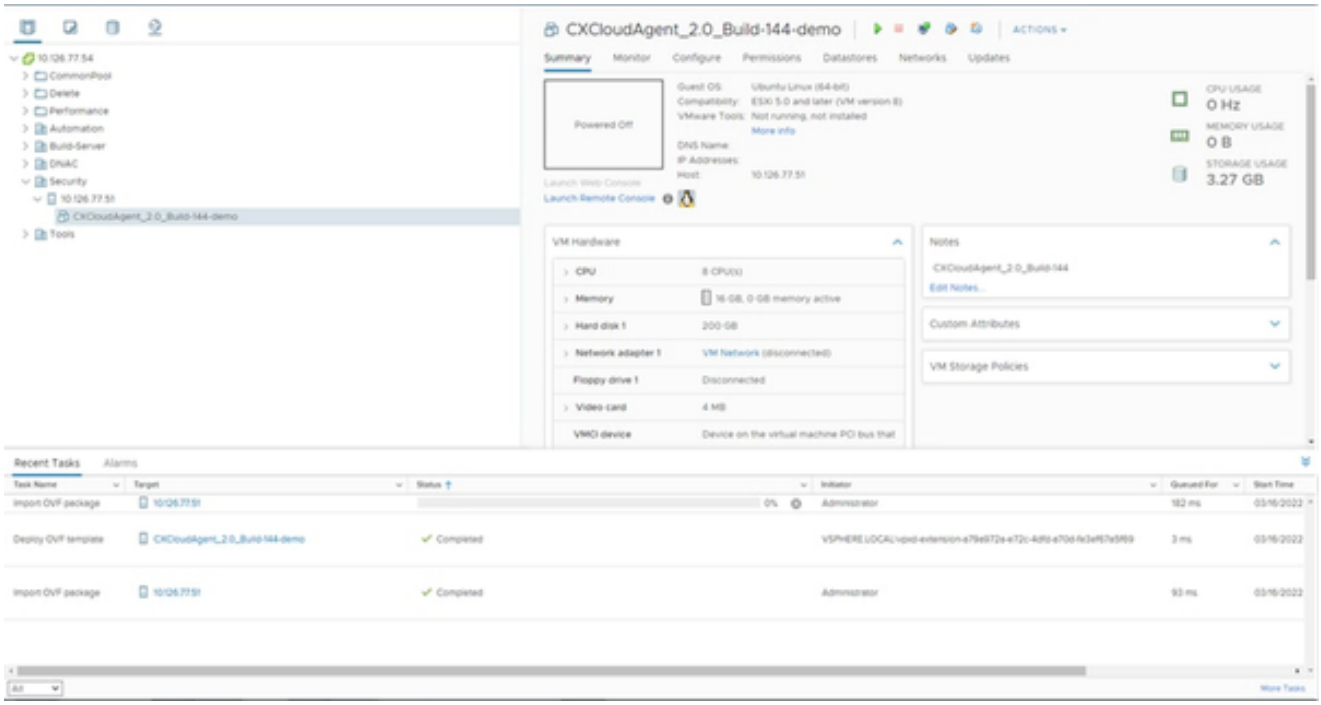
終了準備の完了（Ready to Complete）

13. 選択内容を確認し、Finishをクリックします。ホームページが表示されます。



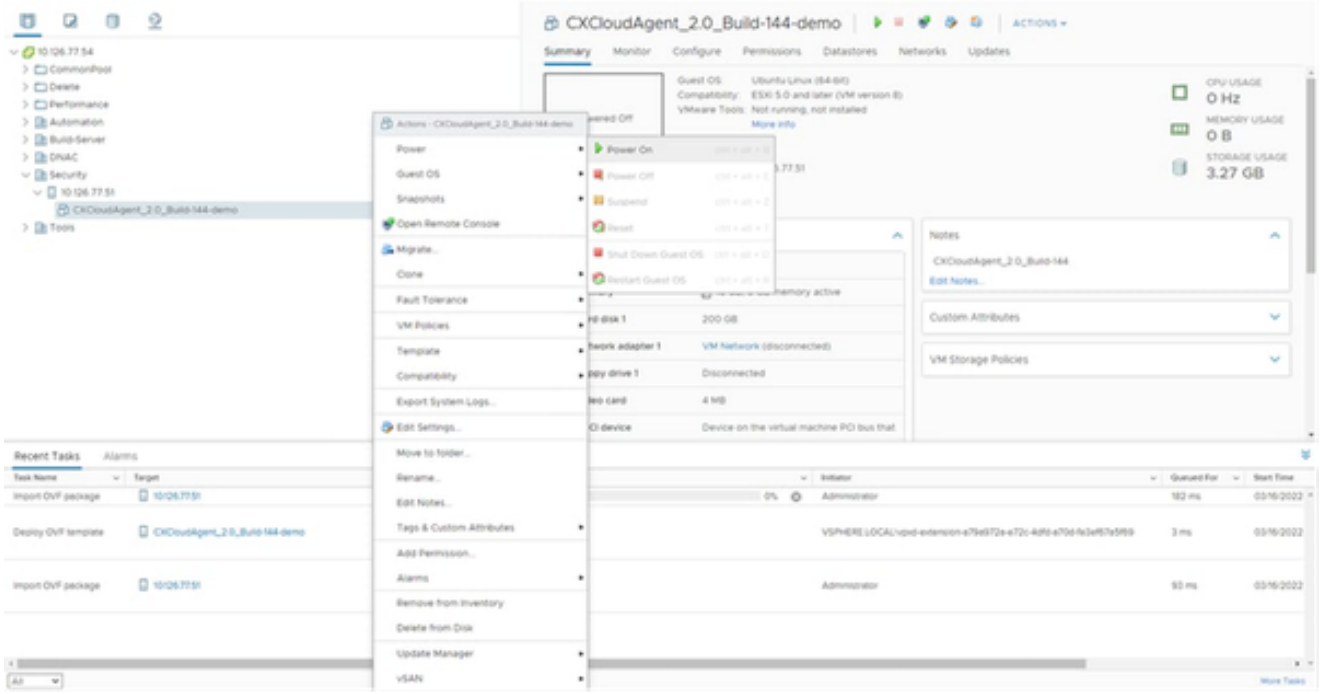
追加されたVM

14. 新しく追加されたVMをクリックすると、ステータスが表示されます。



追加されたVM

15. 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）]

16. ネットワーク設定に移動し、次の手順に進みます。

Oracle Virtual Box 7.0.12 のインストール

このクライアントは、Oracle Virtual Boxを介してCXエージェントOVAを導入します。

1. Windowsボックスの任意のフォルダに、CXCloudAgent_3.1 OVAをダウンロードします。
2. コマンドラインインターフェイスを使用してフォルダを参照します。
3. tar -xvf D:\CXCloudAgent_3.1_Build-xx.ovaコマンドを使用して、OVAファイルを解凍します。

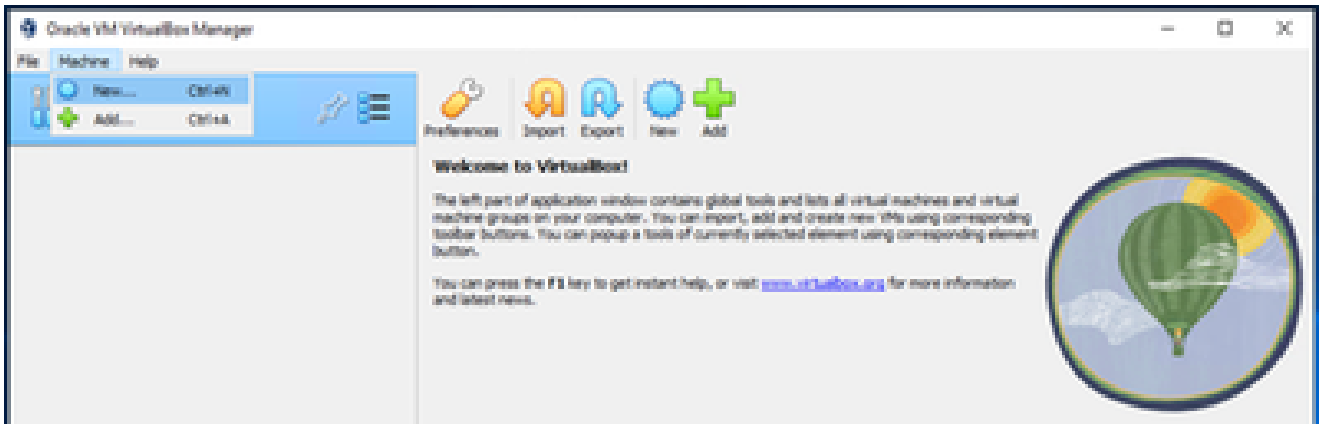
```
D:\>cd CXCAGENT

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

D:\CXCAGENT>_
```

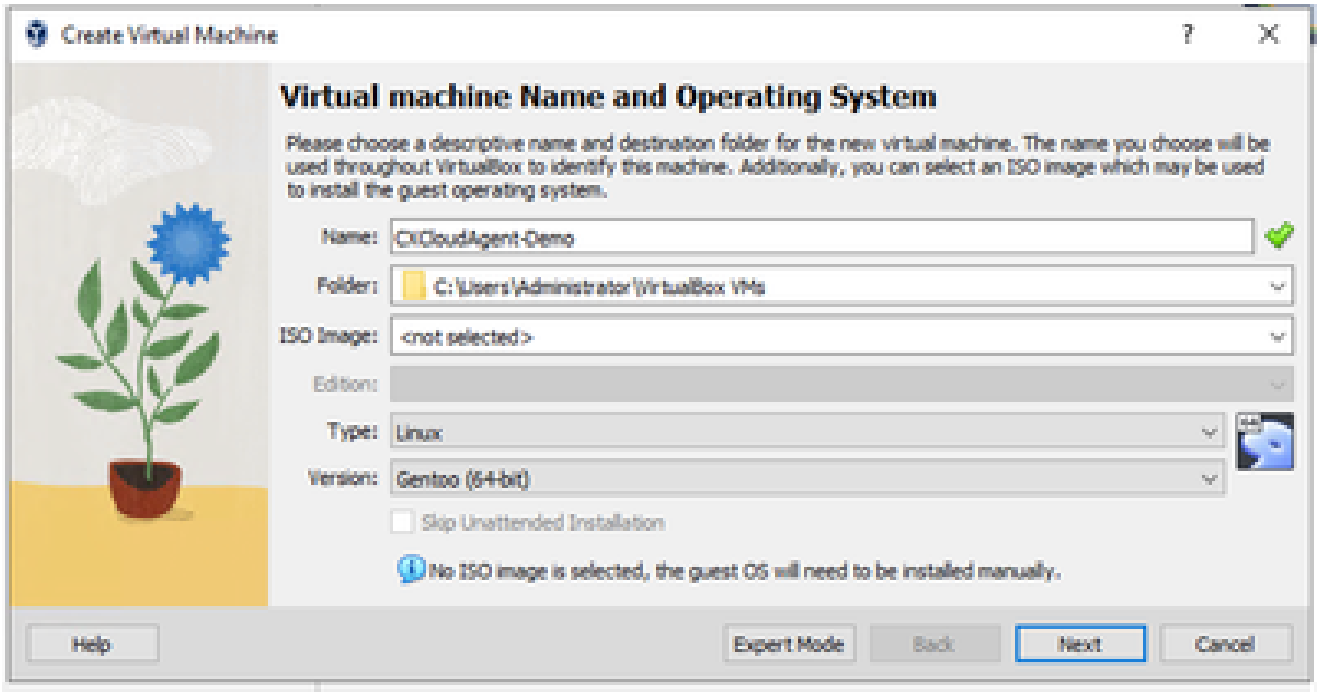
OVAファイルの解凍

4. Oracle VM UIを開きます。



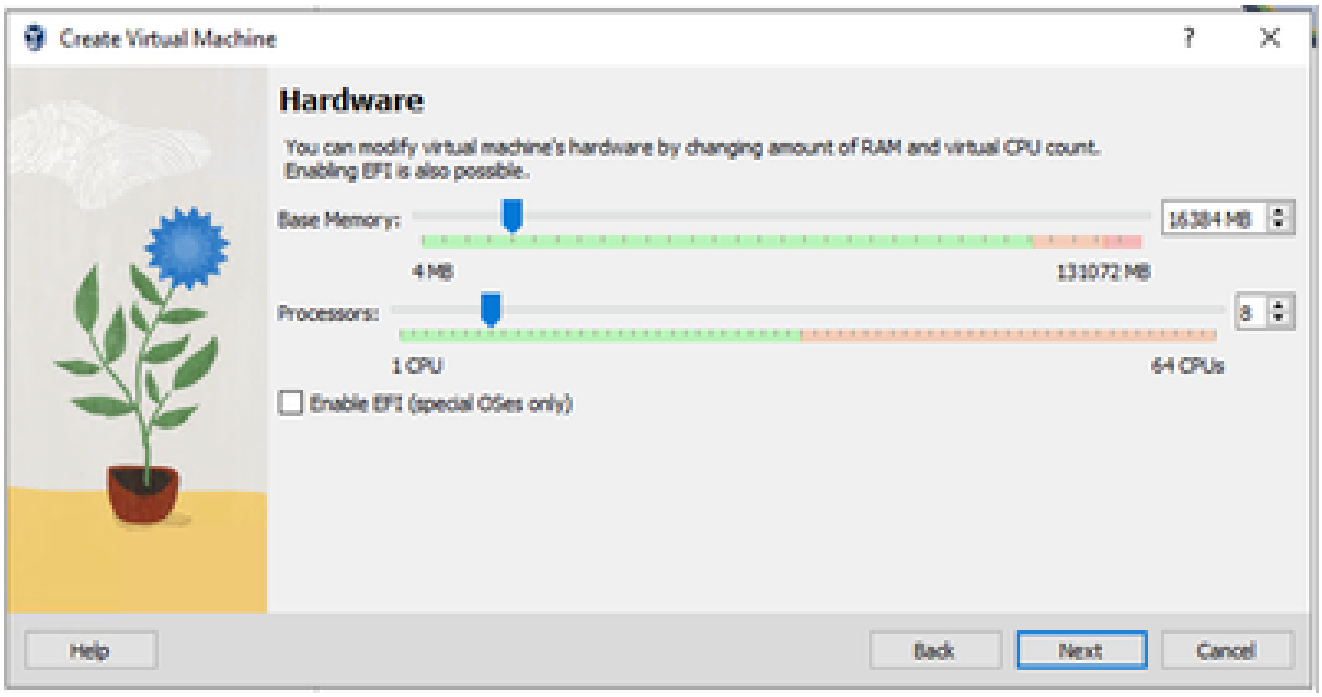
Oracle VM

5. メニューからMachine>Newの順に選択します。Create Virtual Machineウィンドウが開きます。



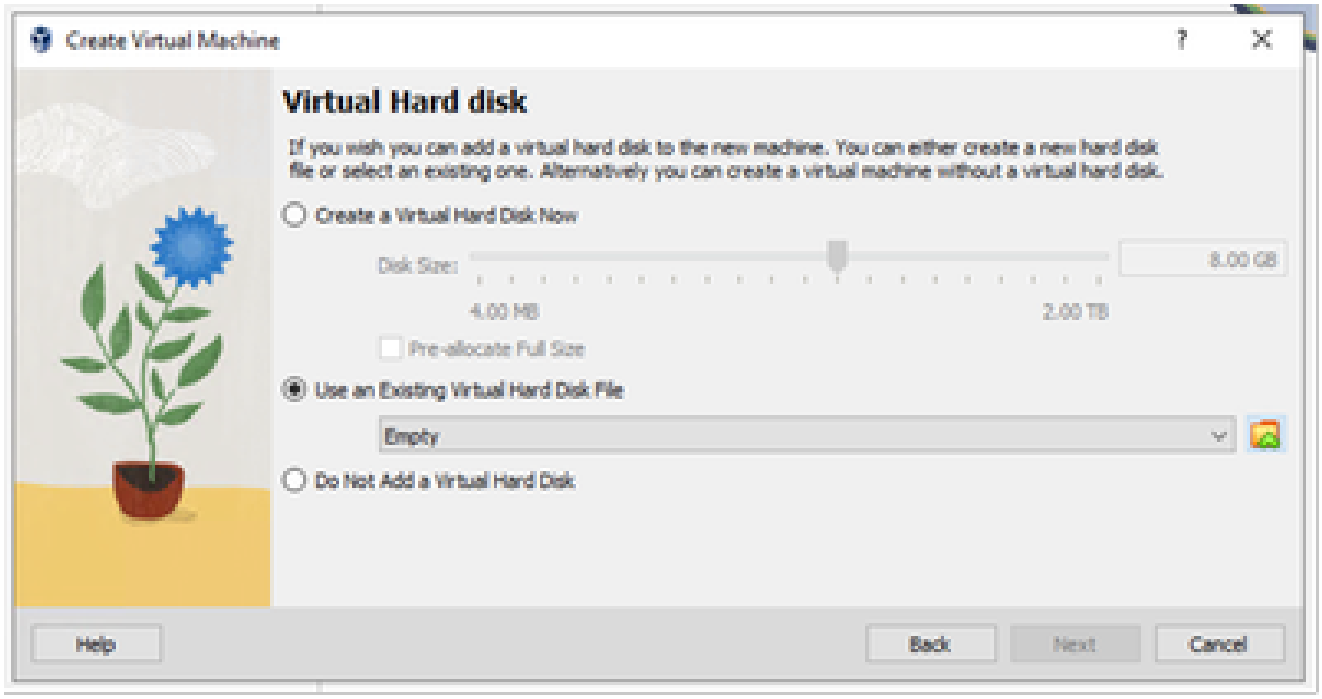
仮想マシンの作成

6. Virtual Machine Name and Operating Systemウィンドウで、次の詳細情報を入力します。
   名前:VM名
   フォルダ:VMデータの格納場所
   ISOイメージ：なし
   タイプ: Linux
   バージョン: Gentoo（64ビット）
7. [Next] をクリックします。Hardwareウィンドウが開きます。



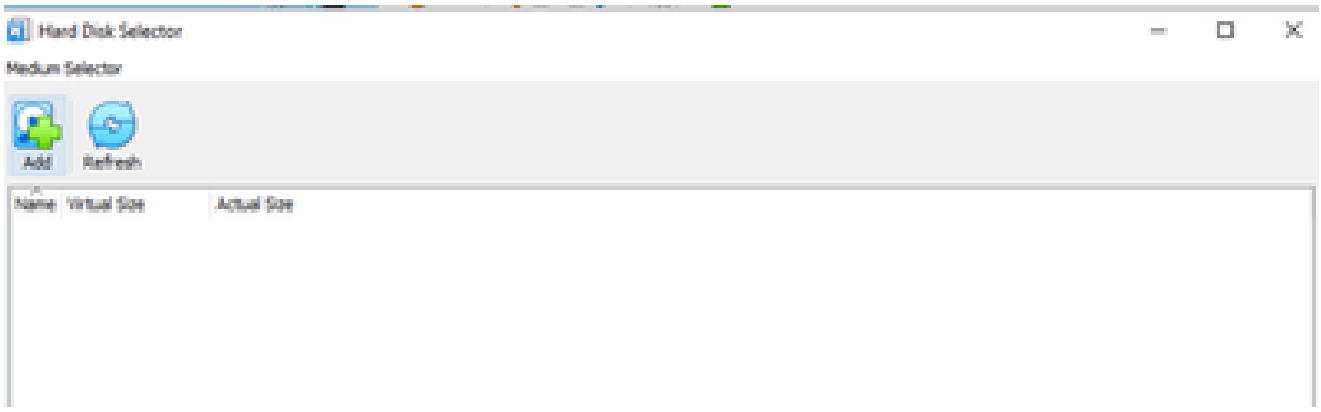
ハードウェア

8. Base Memory(16384 MB)およびProcessors(8 CPU)を入力し、Nextをクリックします。Virtual Hard Diskウィンドウが開きます。



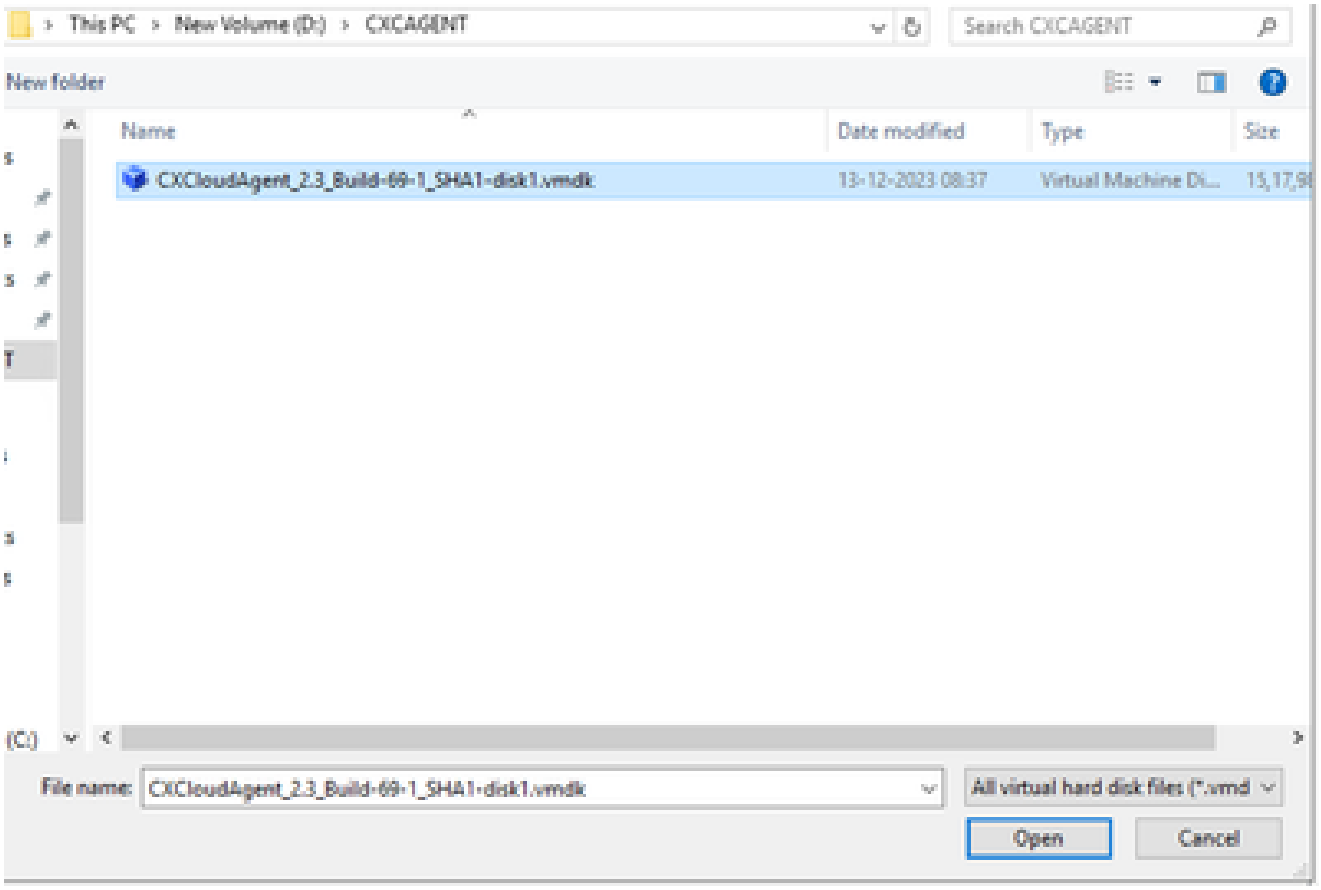
仮想ハードディスク

9. Use an Existing Virtual Hard Disk Fileオプションボタンを選択し、Browseアイコンを選択します。Hard Disk Selectorウィンドウが開きます。



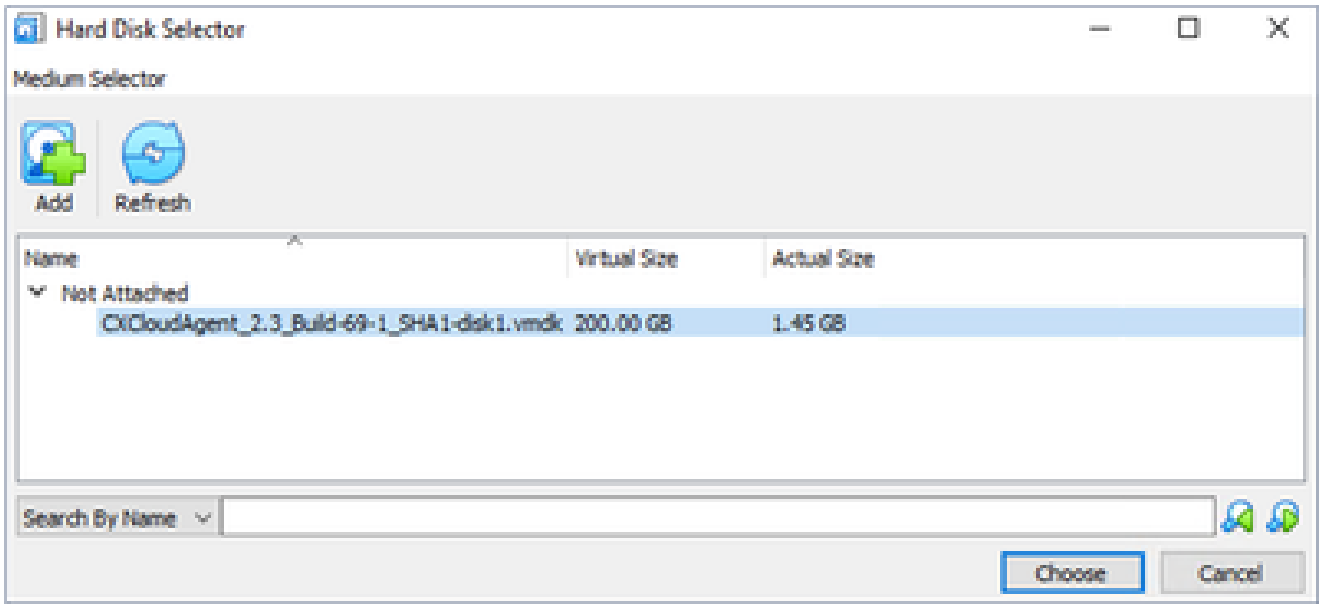
ハードディスクセレクタ

10. OVAフォルダを参照し、VMDKファイルを選択します。



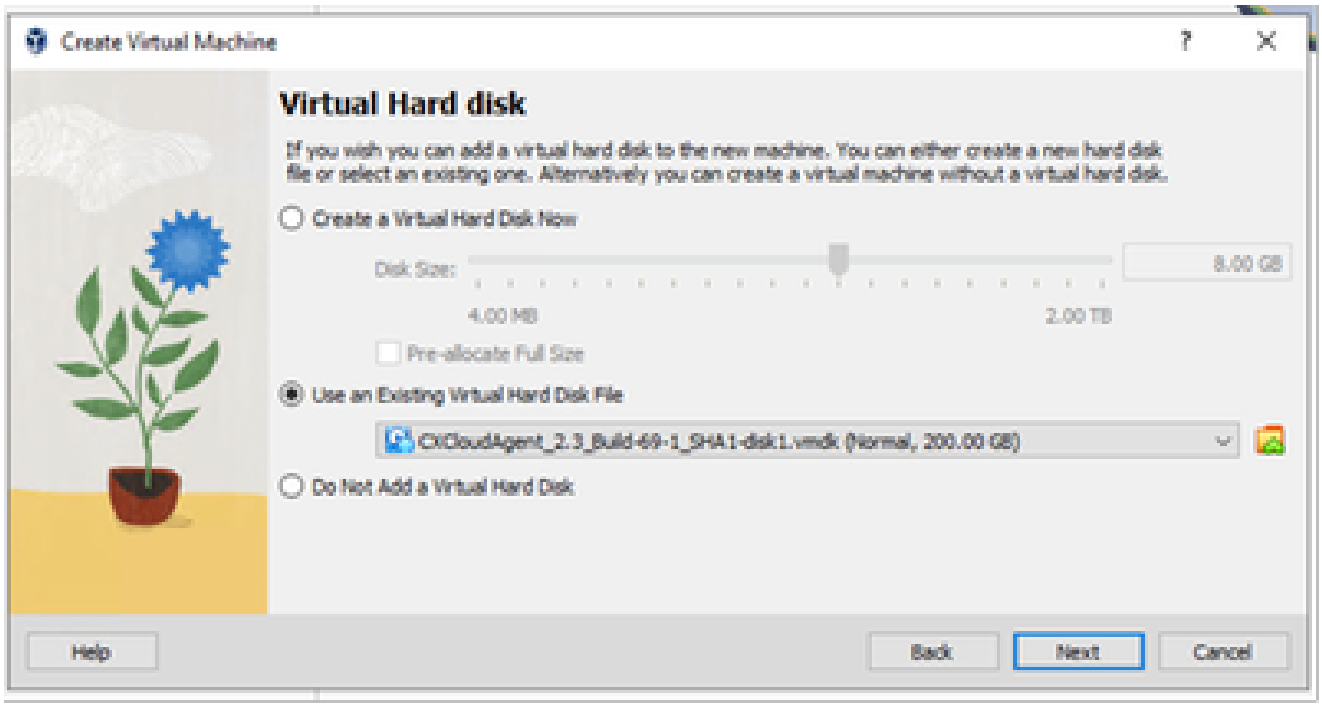
OVAフォルダ

11. [Open] をクリックします。ファイルがHardware Disk Selectorウィンドウに表示されます。



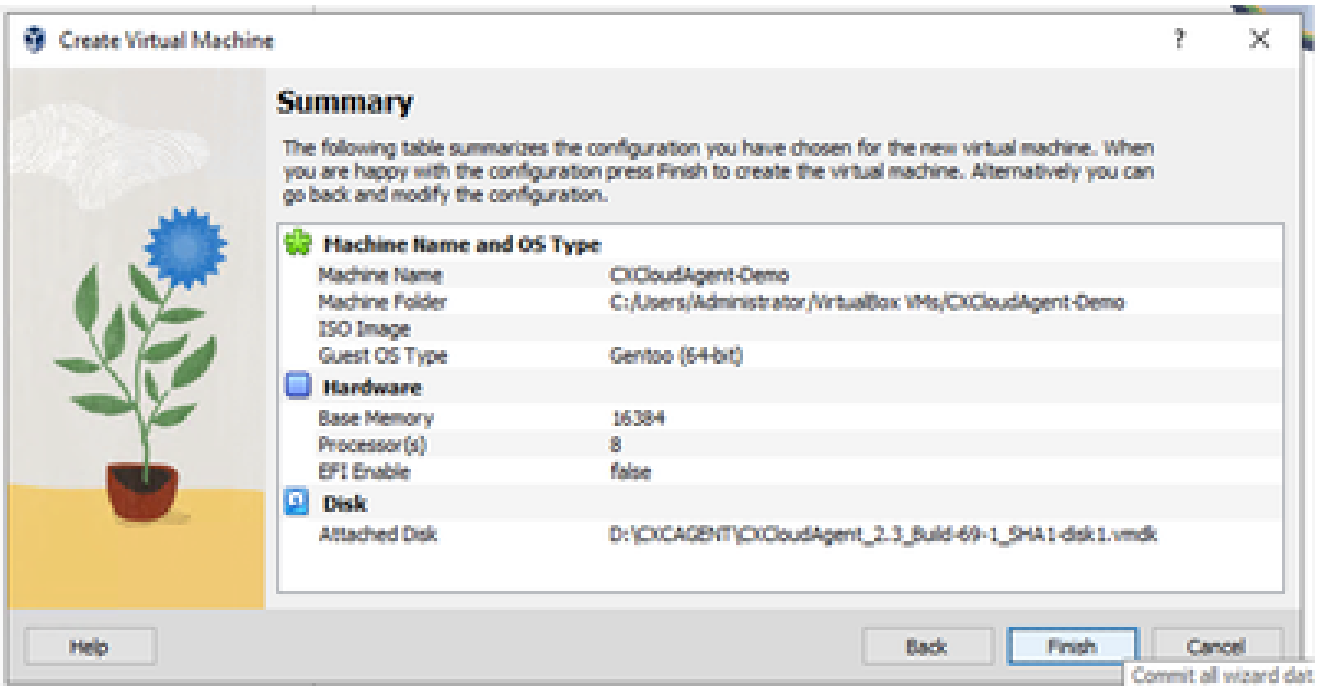
ハードディスクセレクタ

12. Chooseをクリックします。Virtual Hard Diskウィンドウが開きます。表示されたオプションが選択されていることを確認します。



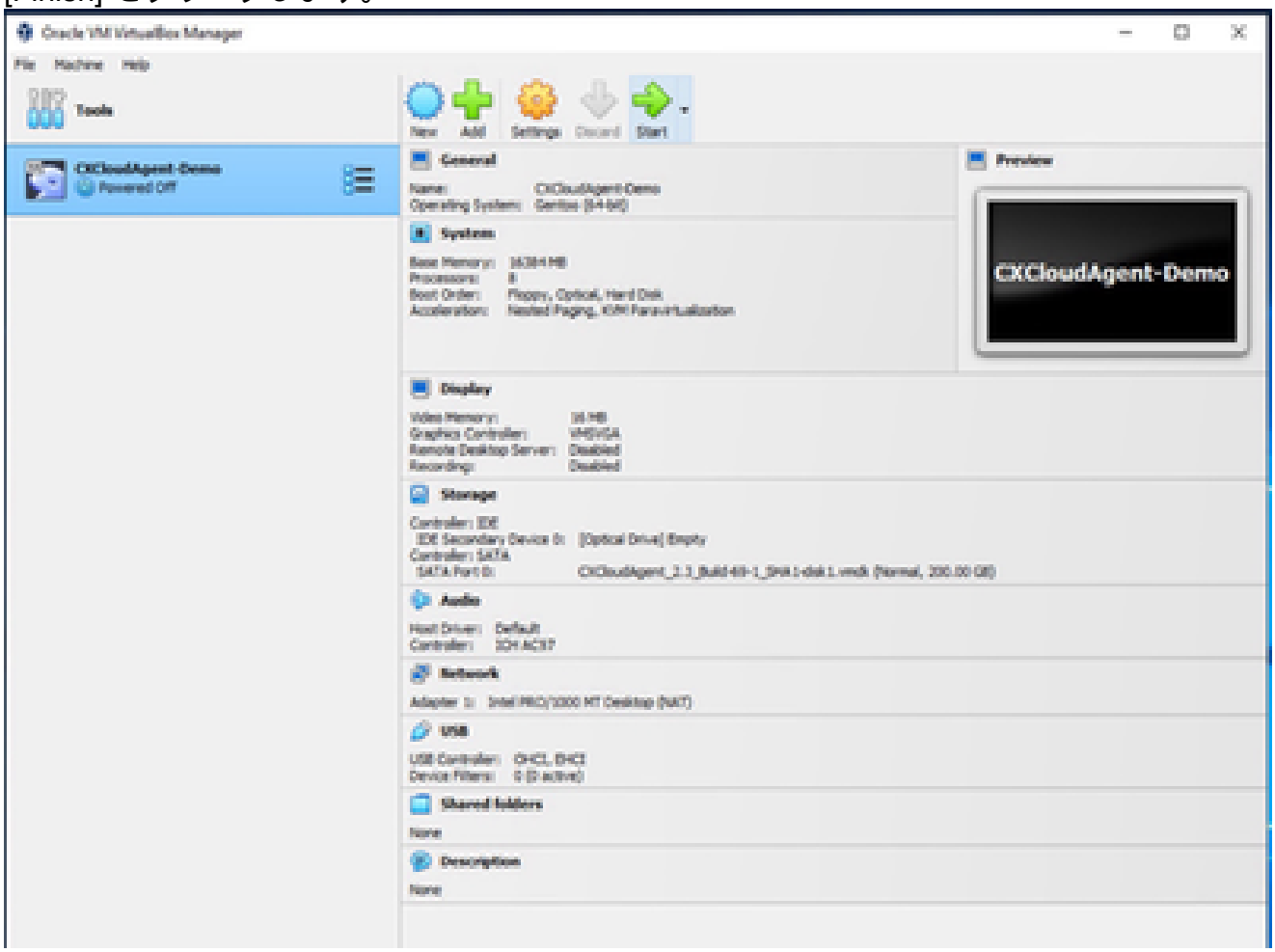
ファイルの選択

13. [Next] をクリックします。Summaryウィンドウが開きます。



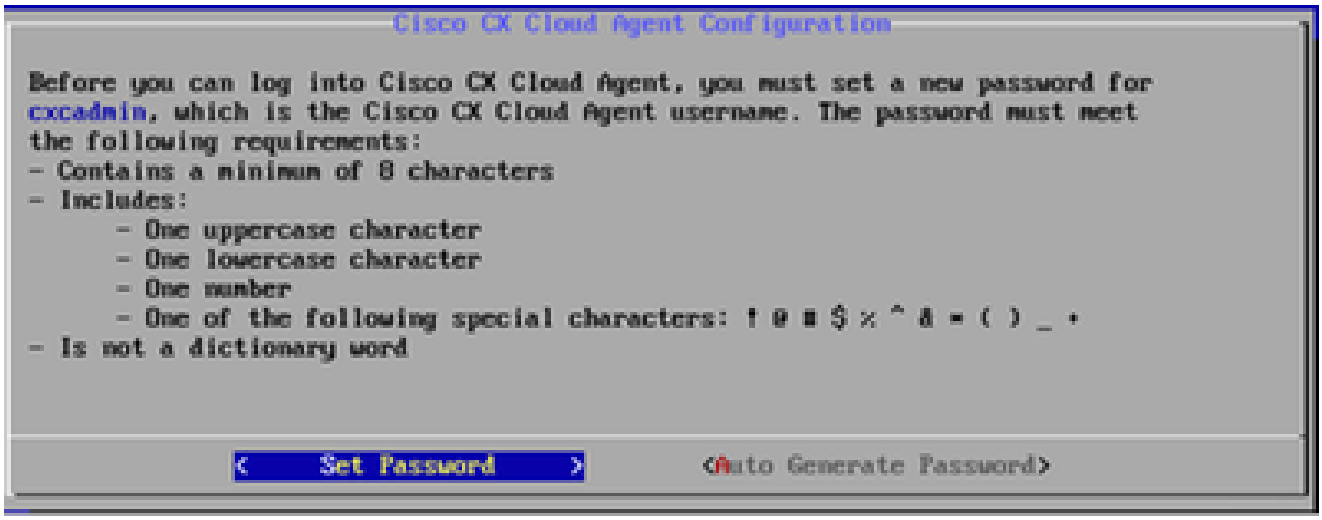
要約

14. [Finish] をクリックします。



VM コンソールの起動

15. 導入したVMを選択し、Startをクリックします。VMの電源が入り、コンソール画面にセットアップが表示されます。



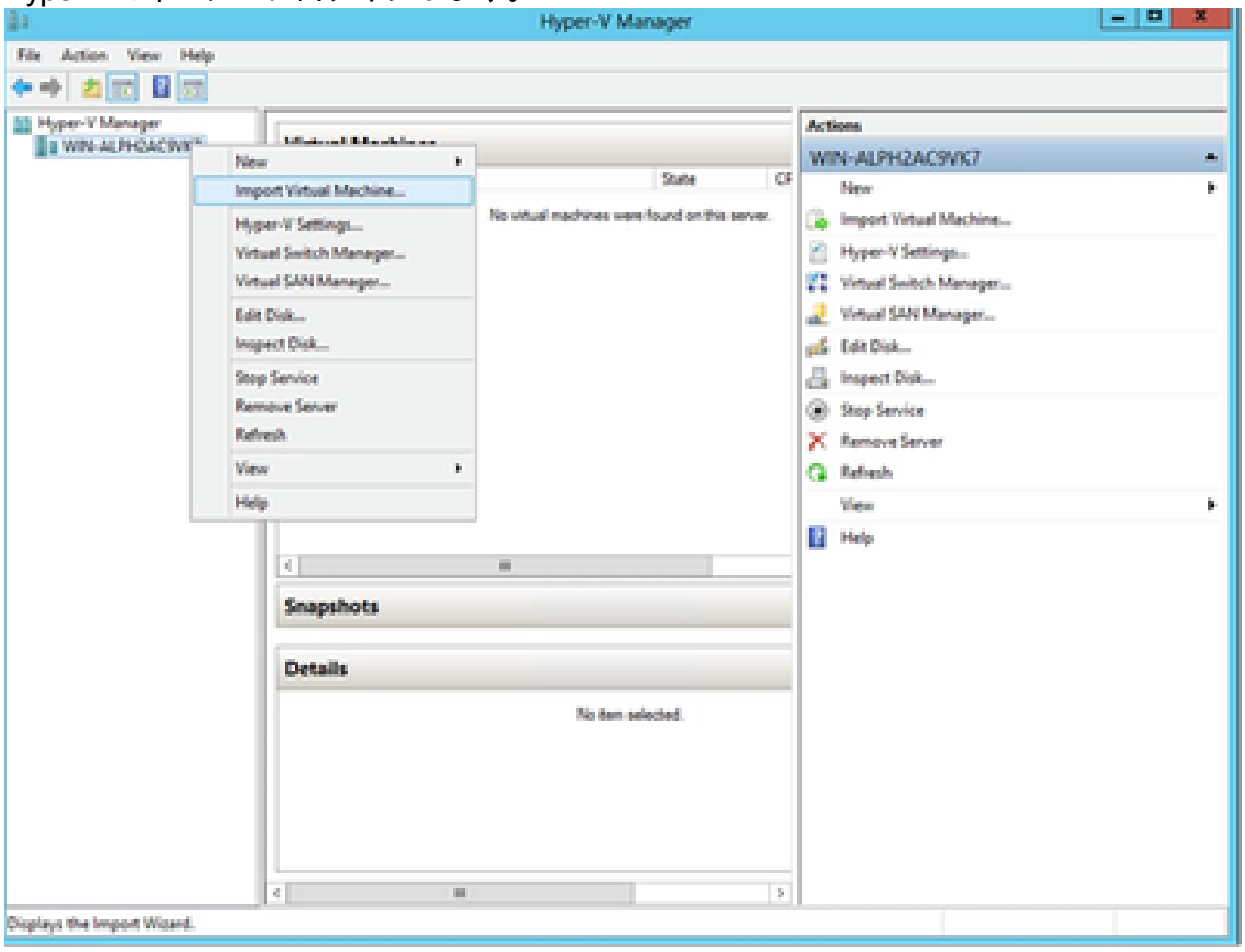
コンソールを開く

16. Network Configurationの順に移動して、次のステップに進みます。

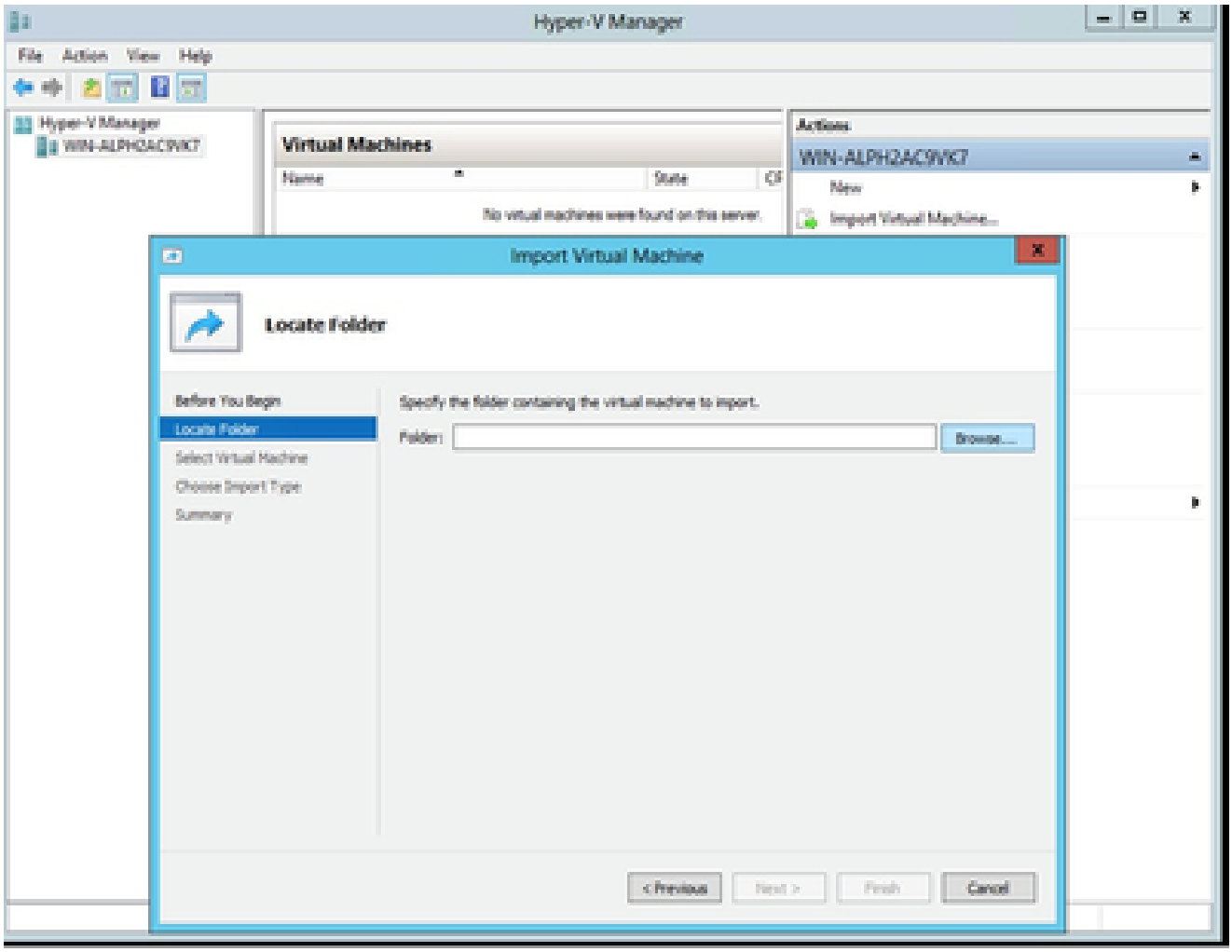
Microsoft Hyper-V のインストール

このクライアントは、Microsoft Hyper-Vのインストールを通じてCXエージェントOVAを導入します。

1. Hyper-Vマネージャにログインします。

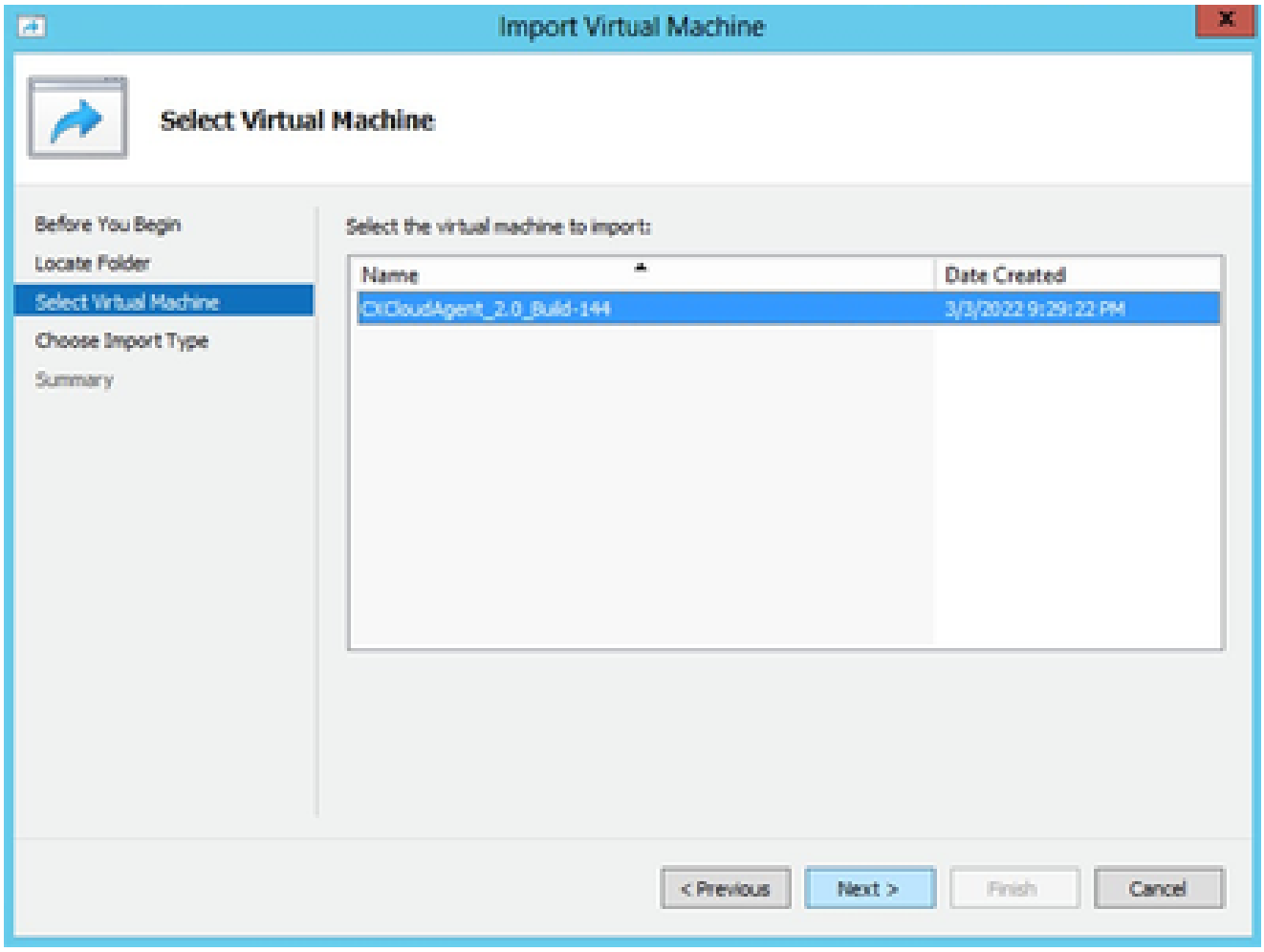


2. ターゲットVMを選択し、右クリックしてメニューを開き、Import Virtual Machineを選択します。



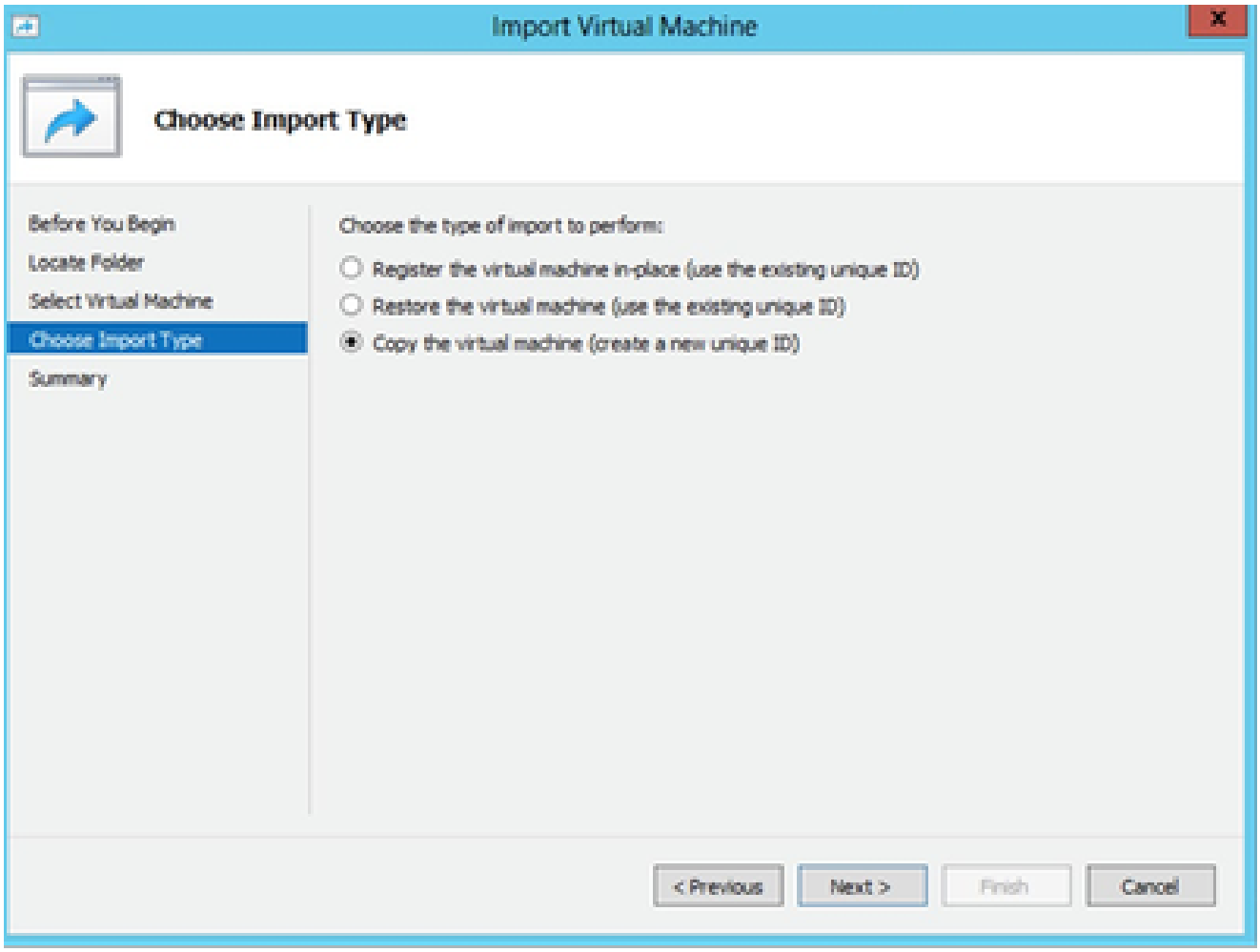
インポートするフォルダ

3. ダウンロードフォルダを参照して選択し、Nextをクリックします。



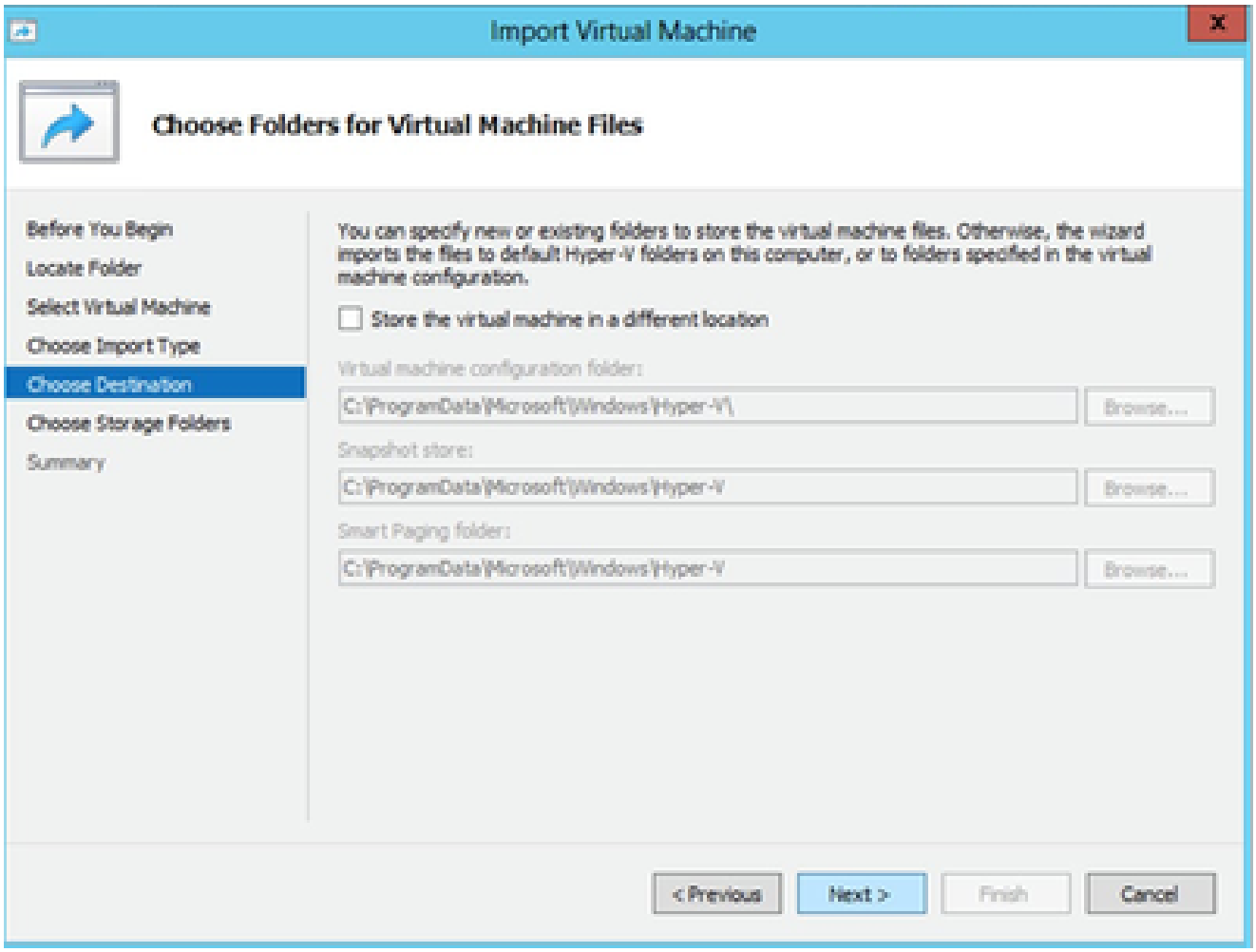
[VMの選択（Select VM）]

4. VMを選択し、Nextをクリックします。



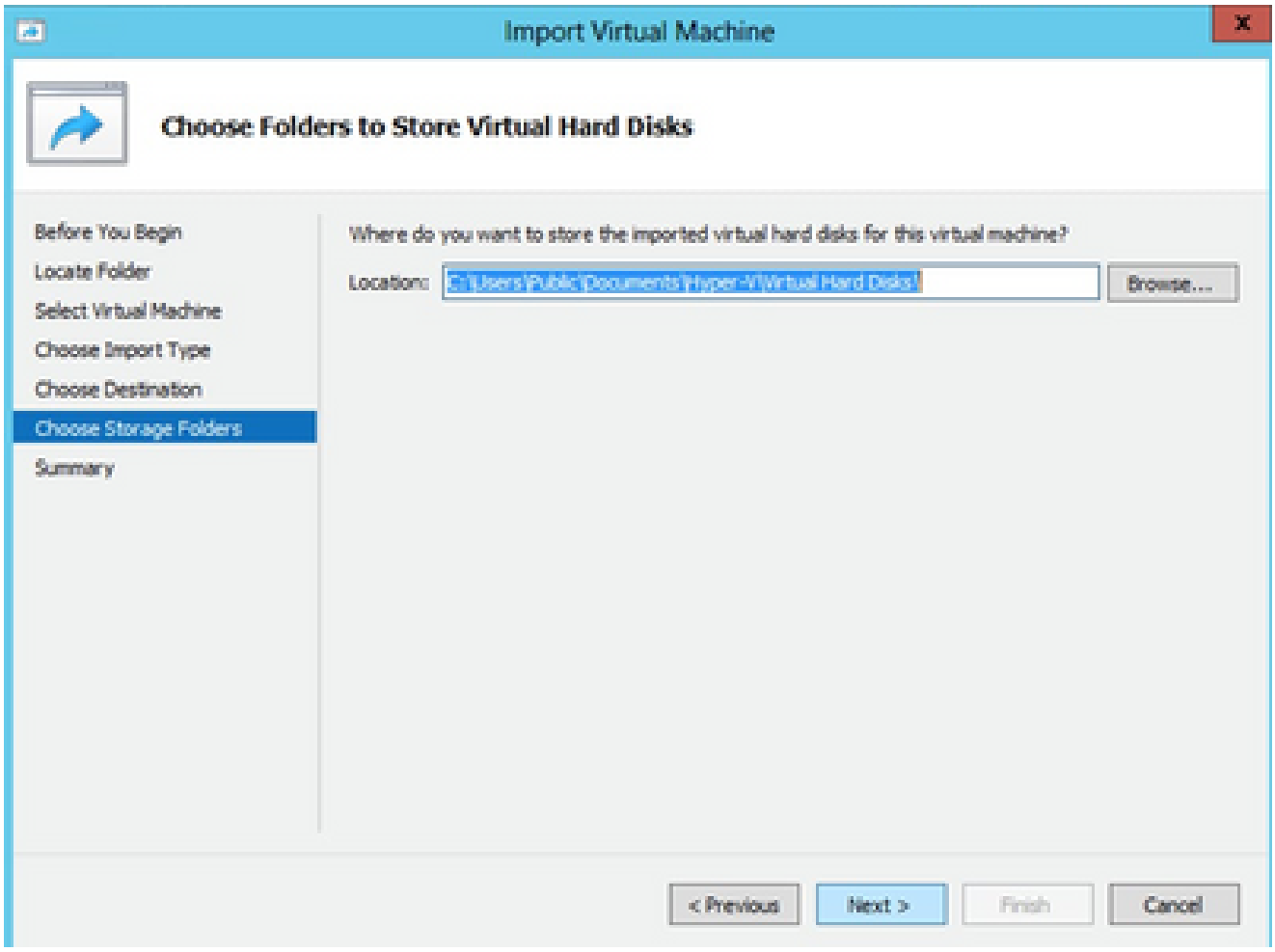
インポート タイプ

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。



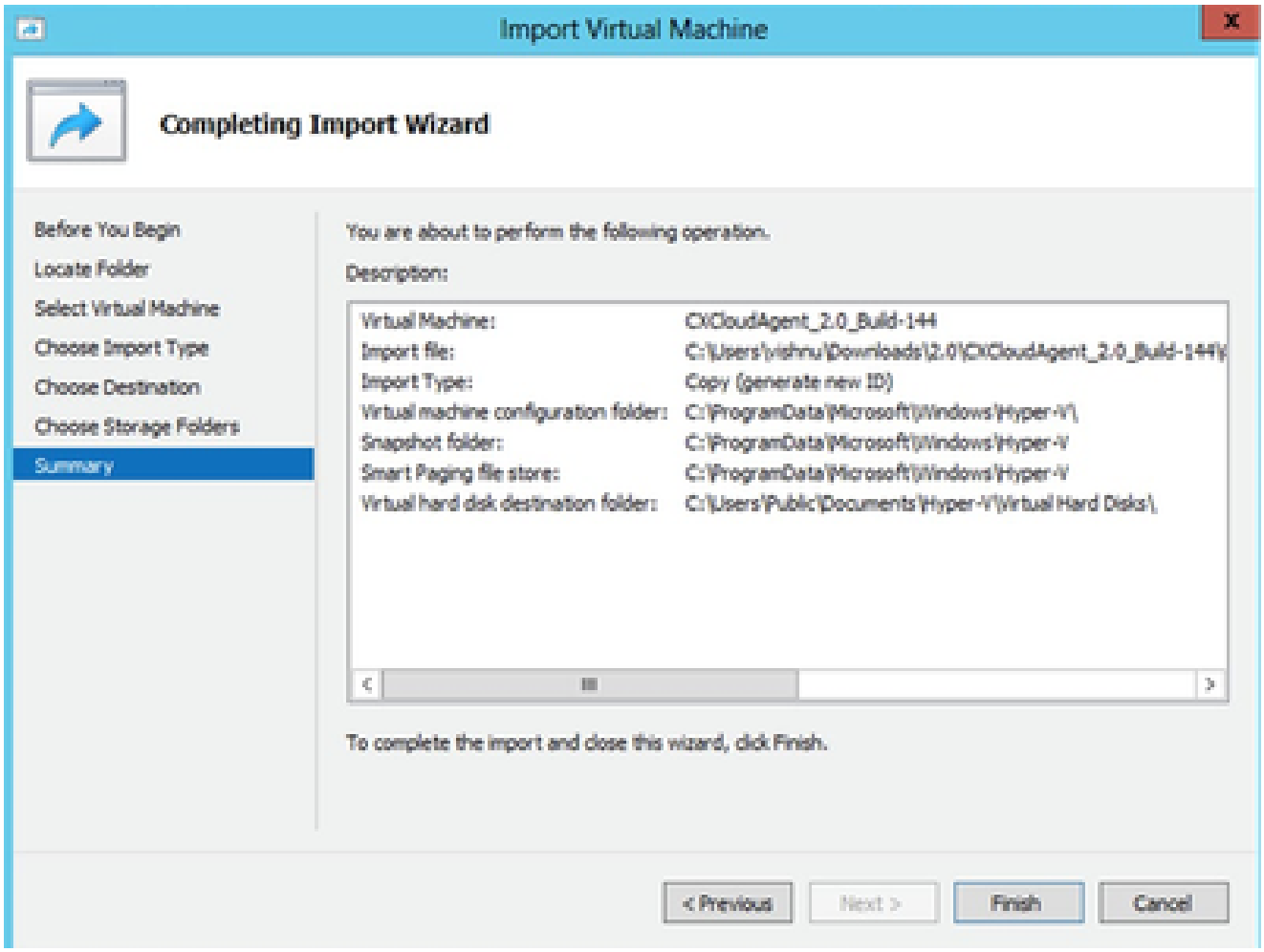
仮想マシンファイルのフォルダーの選択

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お勧めします。
7. [Next] をクリックします。



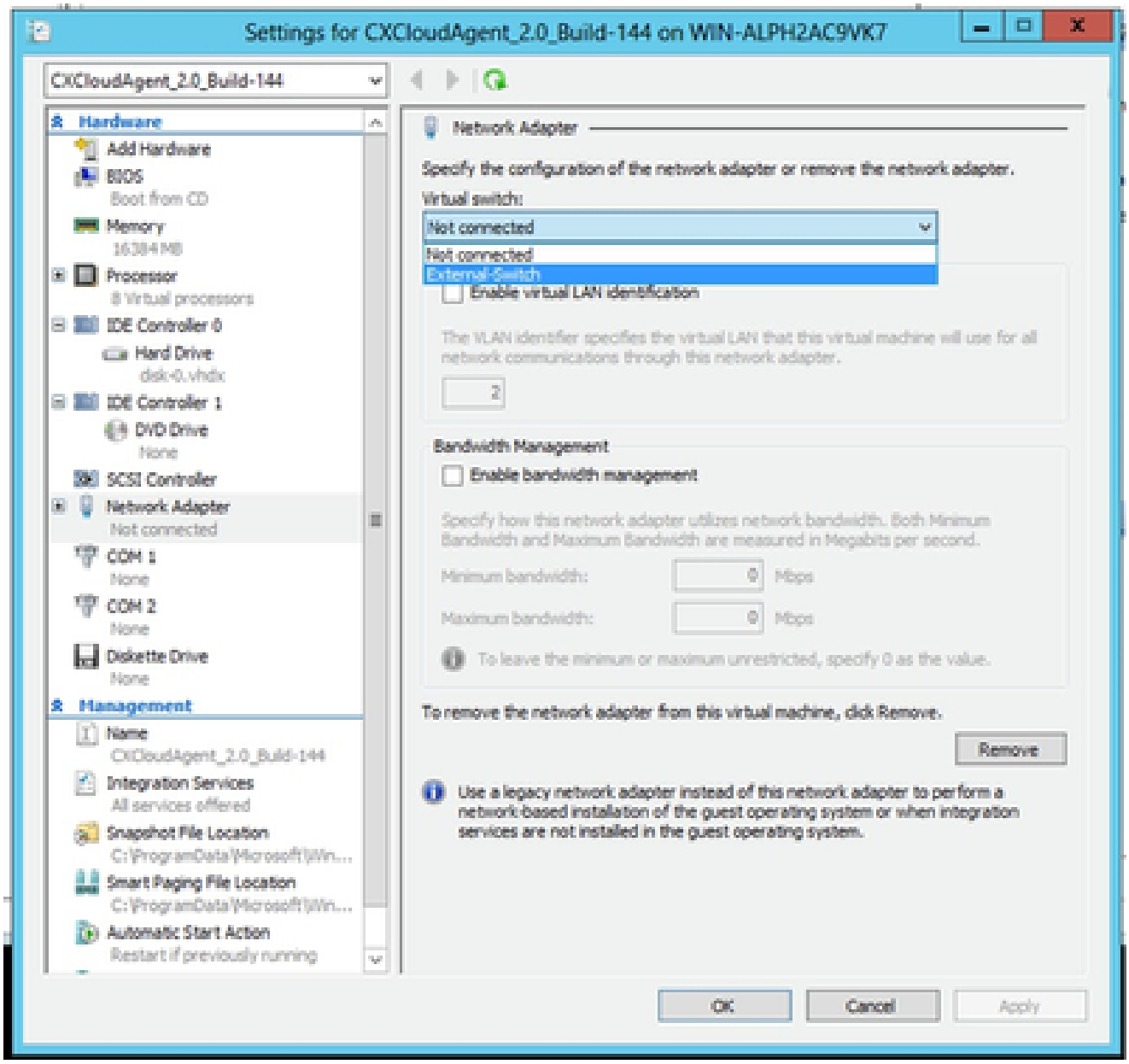
仮想ハードディスクを格納するフォルダー

8. VMハードディスクを保存するフォルダを参照して選択します。デフォルトの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。VMサマリーが表示されます。



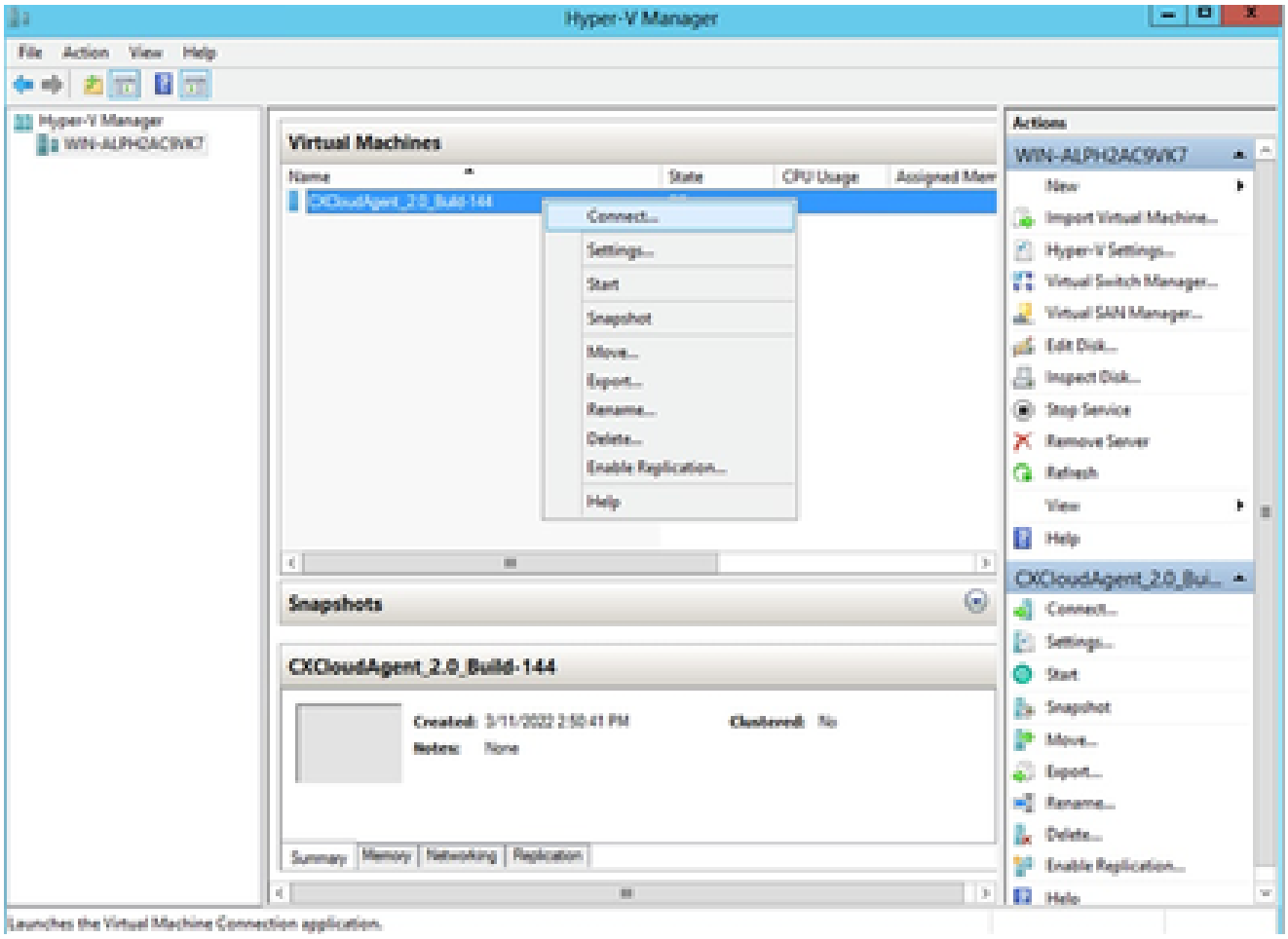
要約

10. すべての入力を確認し、Finishをクリックします。
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。



仮想スイッチ

12. 左側のパネルからNetwork Adaptorを選択し、ドロップダウンリストから使用可能な仮想スイッチを選択します。

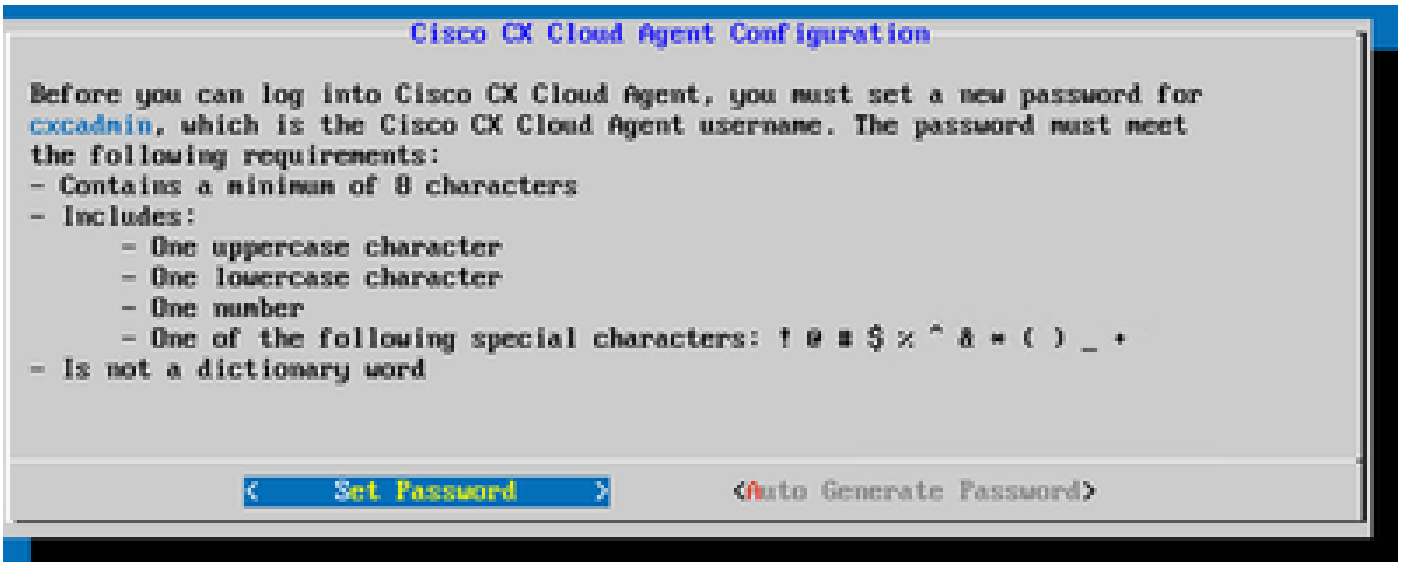


VM の起動

13. Connectを選択してVMを起動します。
14. Network Configurationの順に移動して、次のステップに進みます。

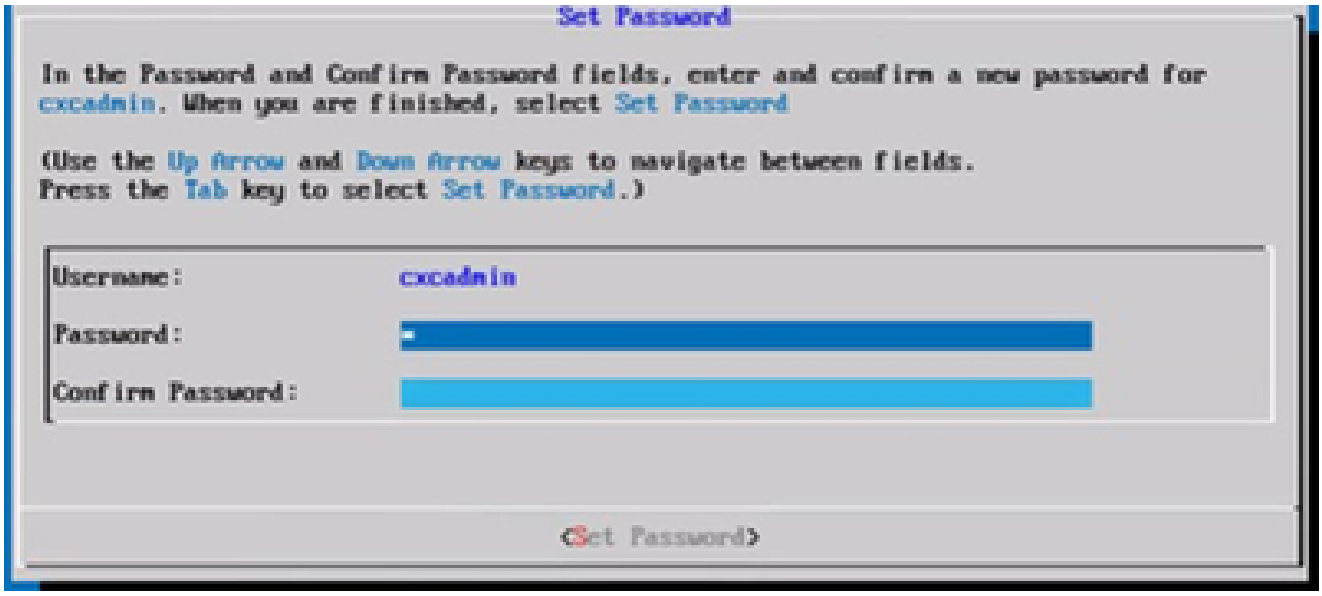
ネットワーク設定

cxcadminユーザ名のCX Cloud Agentパスワードを設定するには、次のコマンドを実行します。



パスワードの設定

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。



新しいパスワード

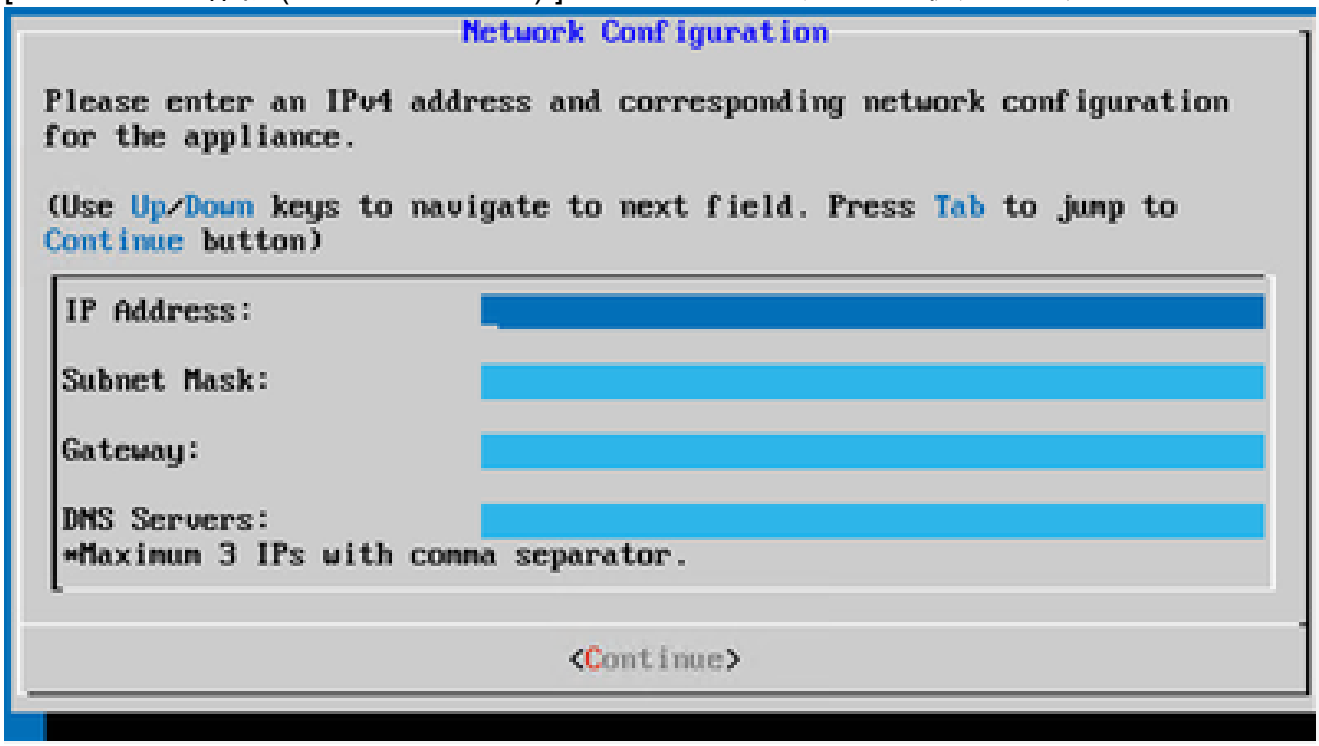
2. [パスワードの設定（Set Password）] を選択した場合は、cxcadmin のパスワードを入力して確認します。[パスワードの設定（Set Password）] をクリックして手順 3 に進みます。
または

Auto Generate Passwordが選択されている場合、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

パスワードの保存（Save Password）

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。

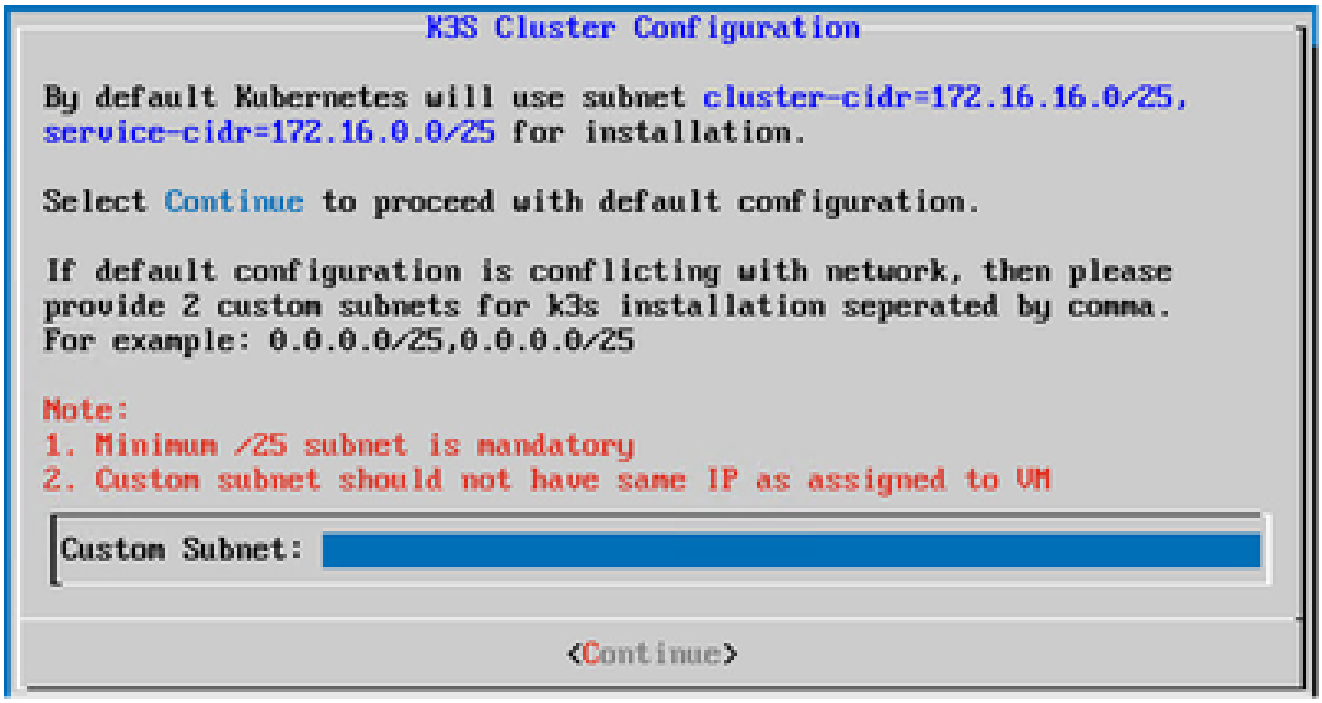


ネットワーク設定

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

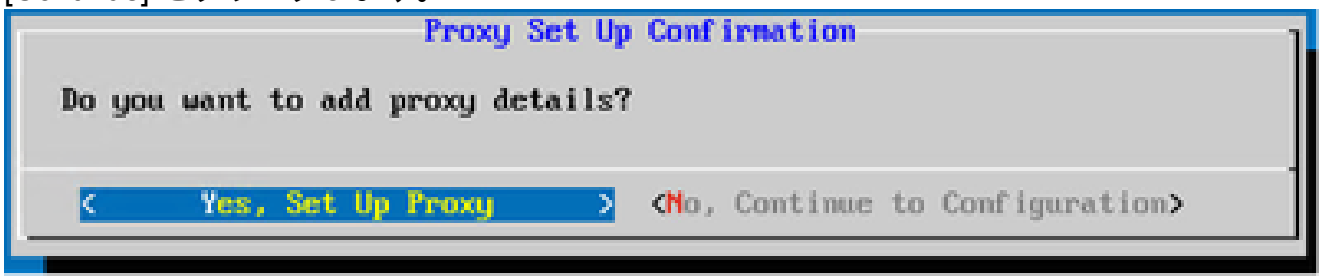
確認

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。



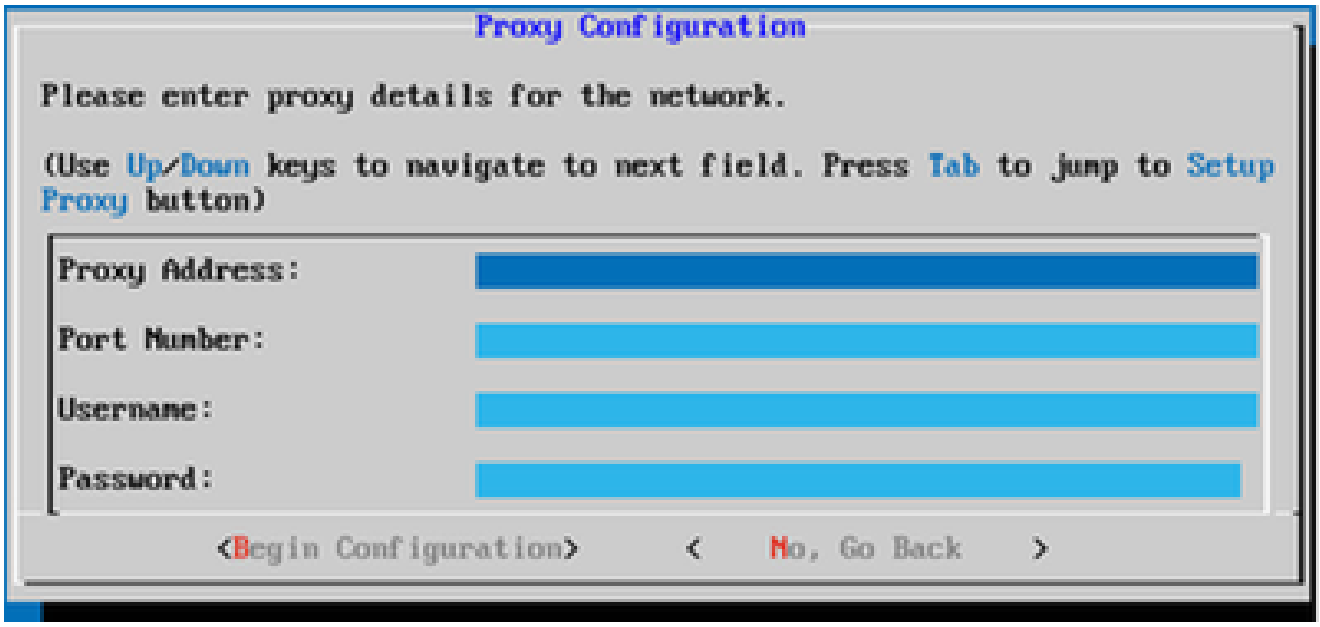
カスタムサブネット

6. K3Sクラスタ設定のカスタムサブネット IPを入力します（お客様のデフォルトサブネットがデバイスネットワークと競合する場合は、別のカスタムサブネットを選択します）。
7. [Continue] をクリックします。



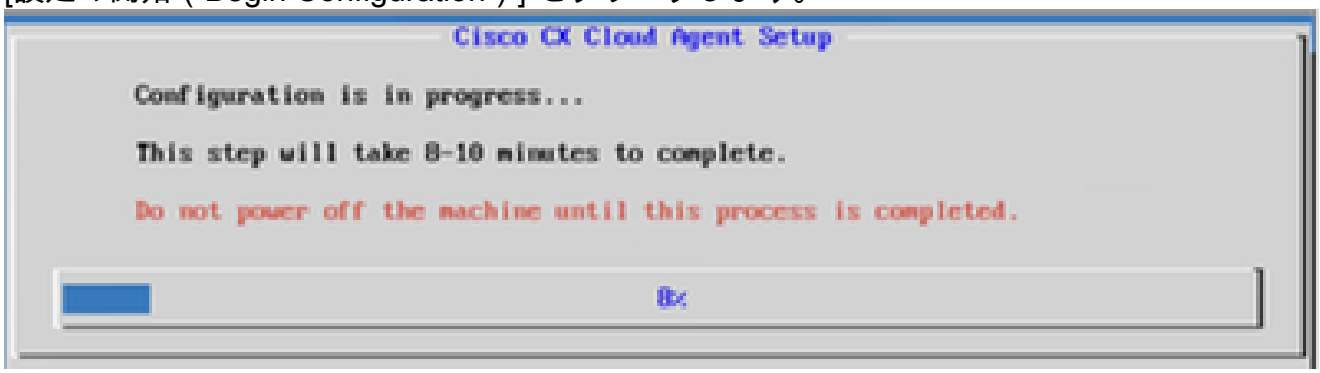
プロキシの設定

8. Yes, Set Up Proxyをクリックしてプロキシの詳細を設定するか、No, Continue to Configurationをクリックして直接ステップ11に進みます。

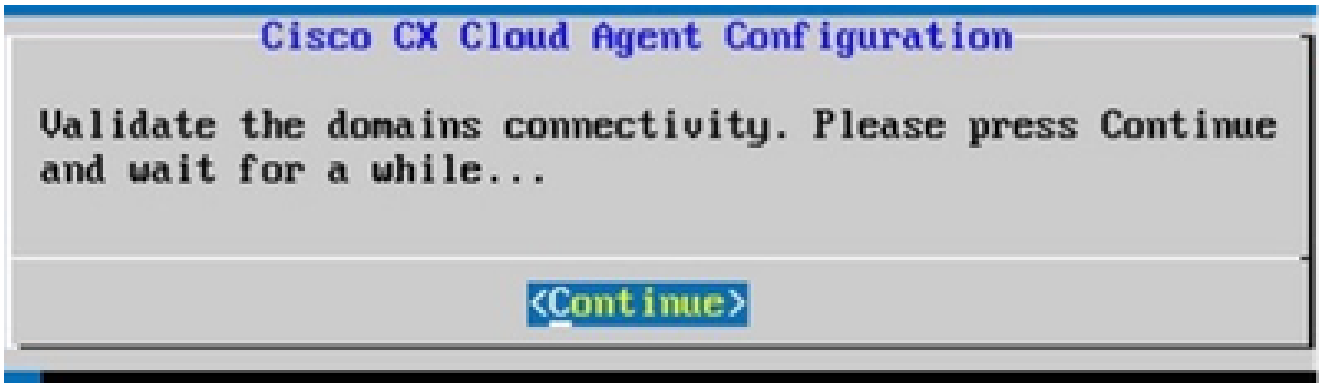


プロキシ設定

9. [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。
10. [設定の開始（Begin Configuration）] をクリックします。

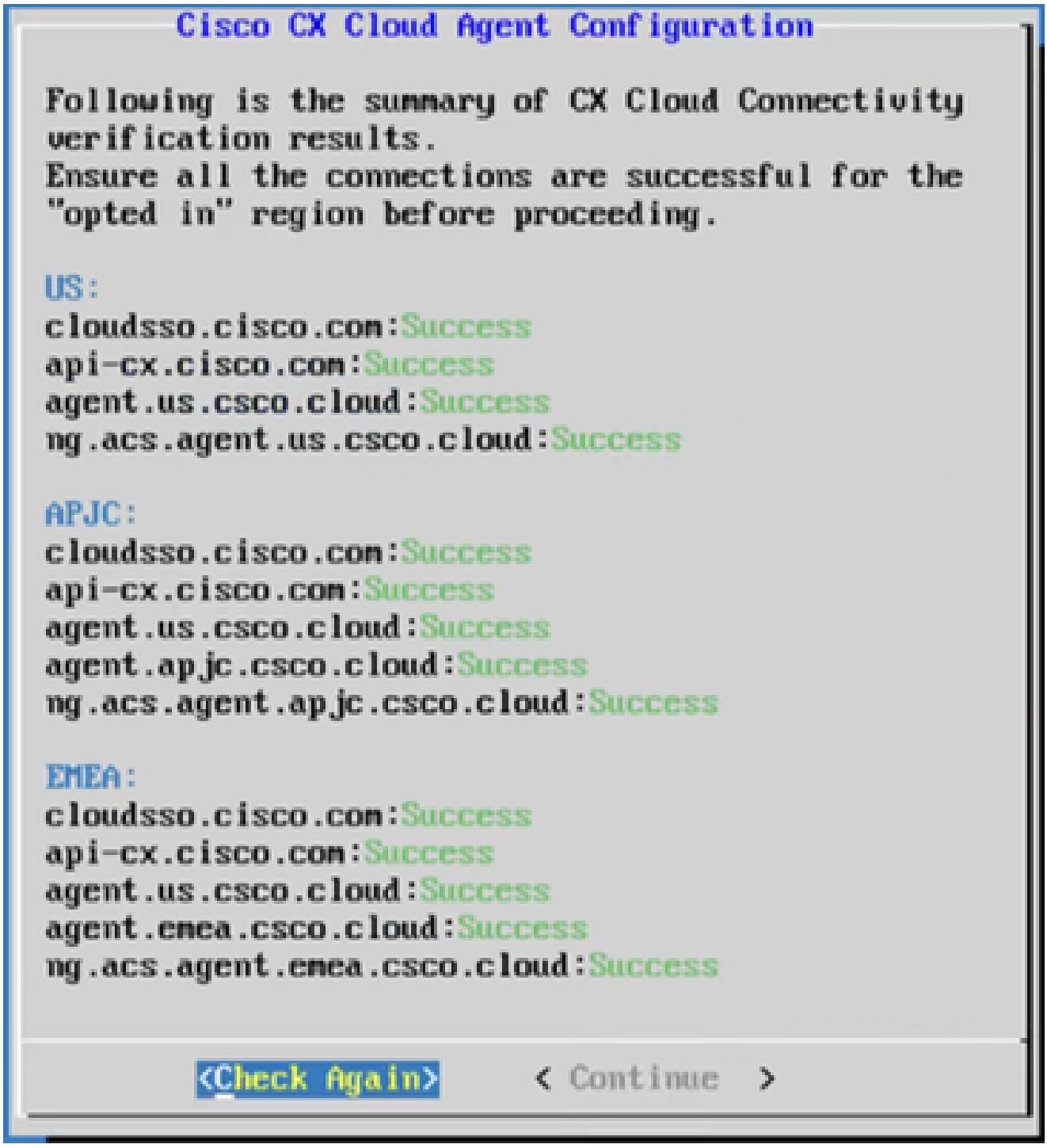


CX Cloudエージェントセットアップ



CX Cloud Agentの設定

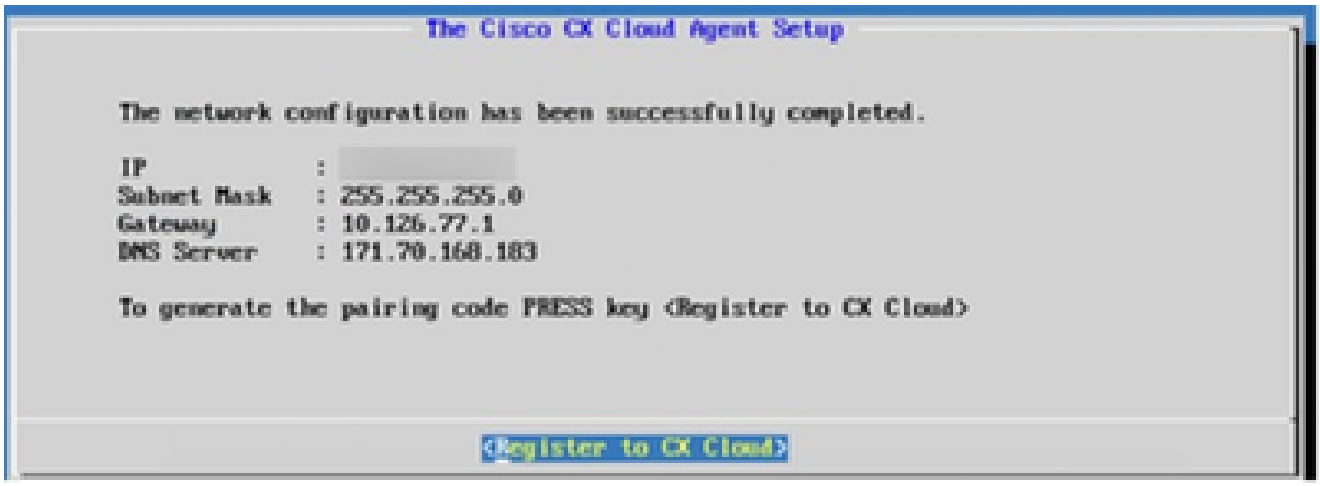
11. [Continue] をクリックします。



設定を続行

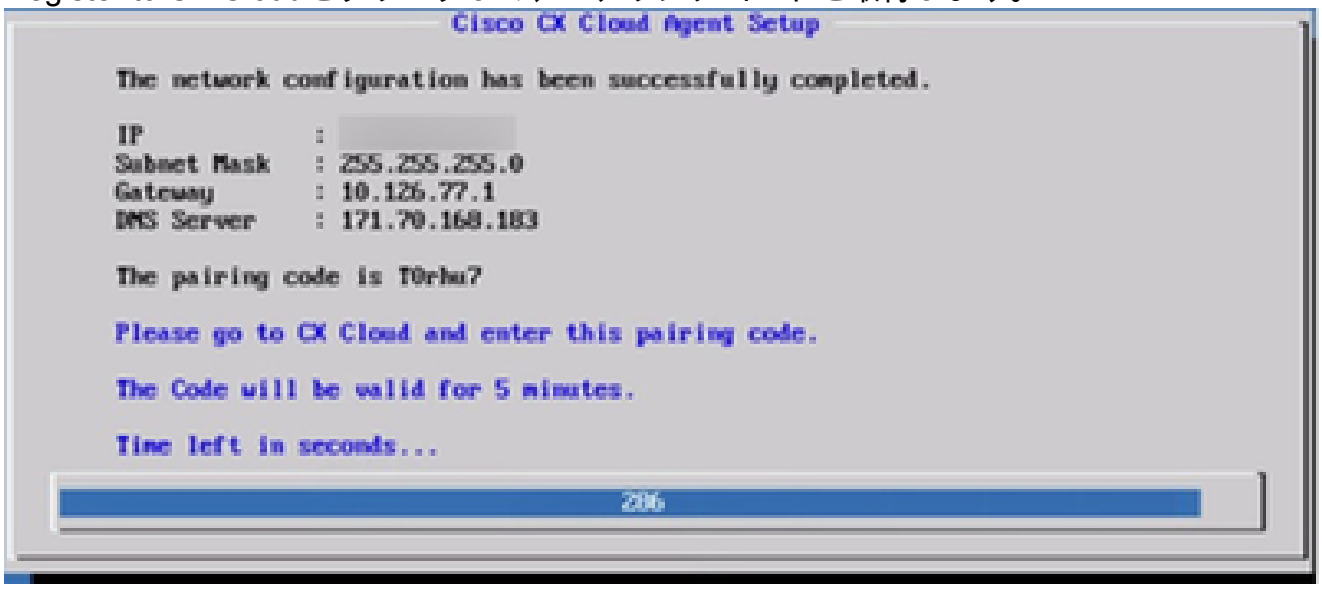
12. Continueをクリックして、ドメインに正常に到達するための設定を続行します。設定が完了するまでに数分かかる場合があります。

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になるよう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。



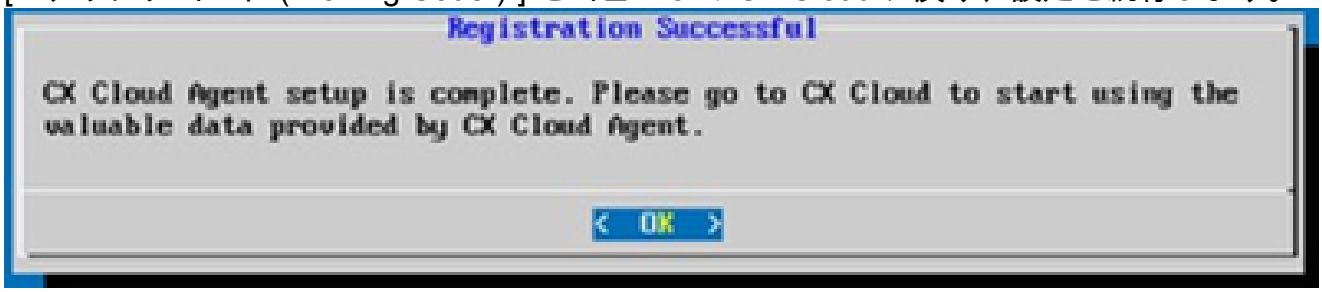
CX Cloud に登録

13. Register to CX Cloudをクリックして、ペアリングコードを取得します。



ペアリングコード

14. [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。



登録に成功しました

注：ペアリングコードの有効期限が切れた場合は、CX Cloudに登録するをクリックして新しいペアリングコードを生成します（ステップ13）。

---

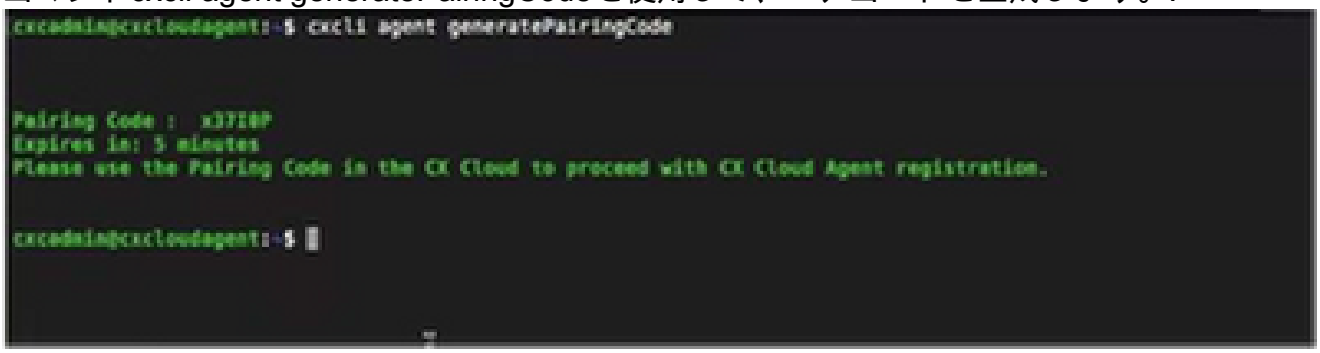
15. OKをクリックします。

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経由でクラウドエージェントにログインします。
2. コマンドcxcli agent generatePairingCodeを使用して、ペアコードを生成します。.



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。

CX Cloud Agentにsyslogを転送するためのデバイスの設定

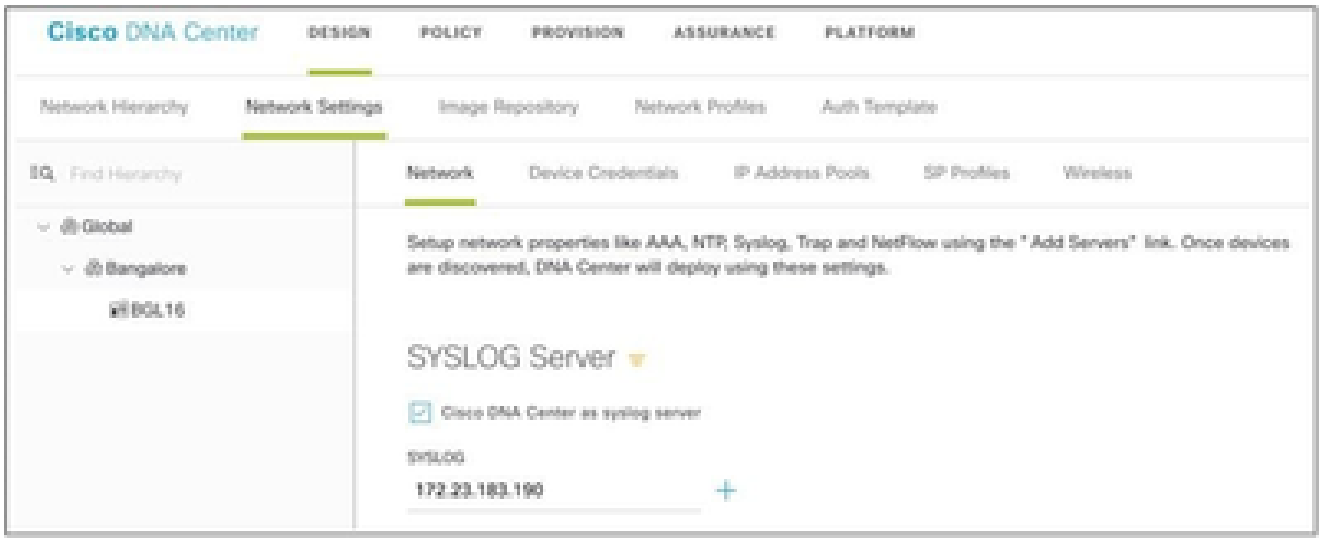
前提条件

サポートされるCisco Catalyst 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 Catalyst Center仮想アプライアンスです

Syslog転送設定の設定

Cisco Catalyst CenterでCXエージェントへのSyslog転送を設定するには、次の手順を実行します。

1. Cisco Catalyst 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. サイトごとに、CXエージェントのIPをSyslogサーバとして追加します。



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、CXエージェントに対してクリティカルなレベルでsyslogを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ているすべてのデバイスは、デフォルトの重大レベルに自動的に設定されます。

CXエージェントにsyslogを転送するための他のアセット（ダイレクトデバイスコレクション）の設定

CX Cloudの障害管理機能を使用するには、CXエージェントにsyslogメッセージを送信するようにデバイスを構成する必要があります。

注:CXエージェントは、Campus Success Trackレベル2アセットからの CX Cloudへのsyslog情報のみを報告します。その他の資産では、syslogがCX Agentに設定されず、CX Cloudでsyslogデータが報告されません。

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、新しい宛先としてCXエージェントのIPアドレスを追加します。

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

CXエージェントのIPアドレスにsyslogを直接送信するように各デバイスを構成します。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。

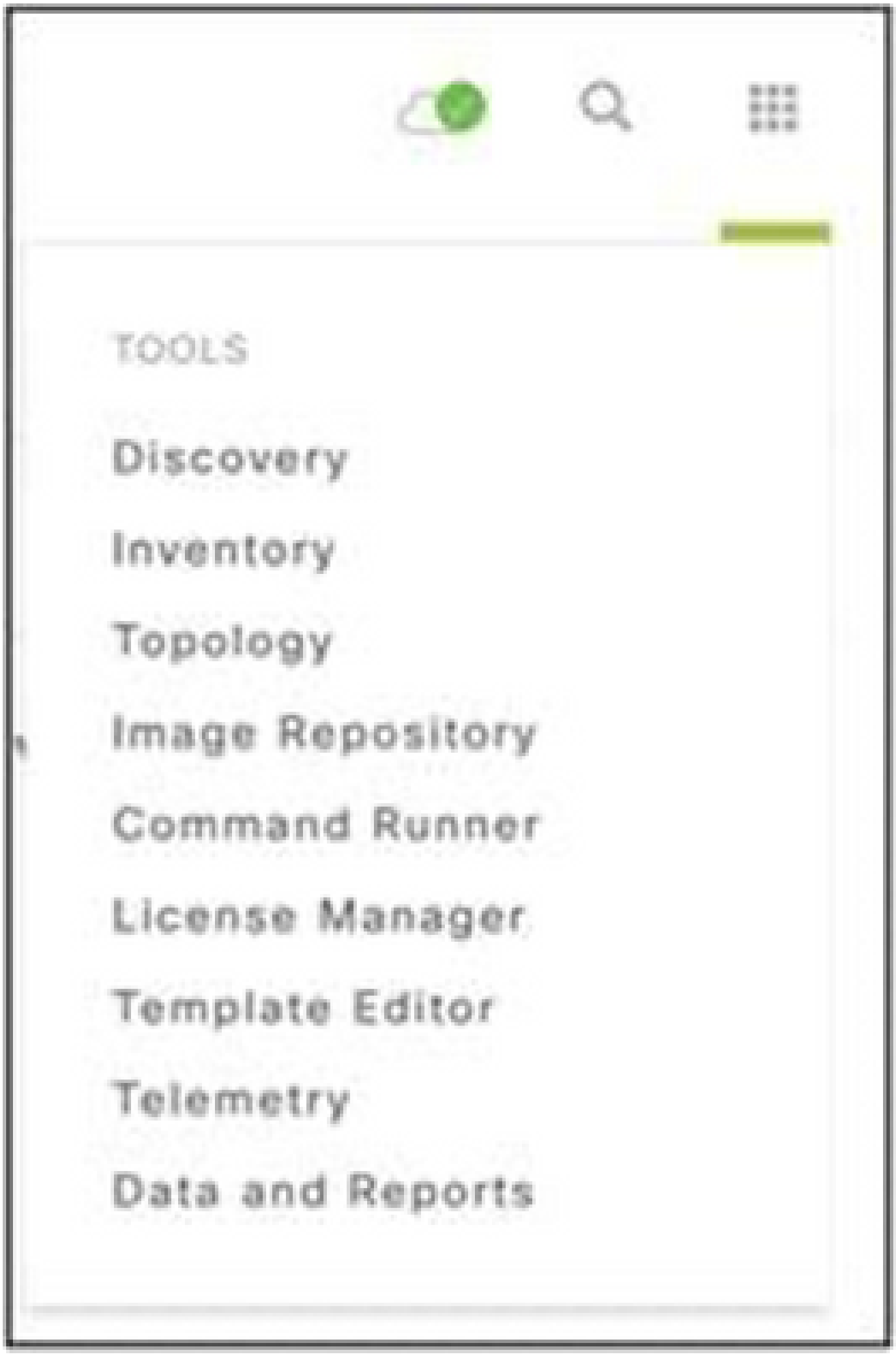
Cisco IOS® XEコンフィギュレーションガイド

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

Cisco Catalyst Centerの情報レベル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）]

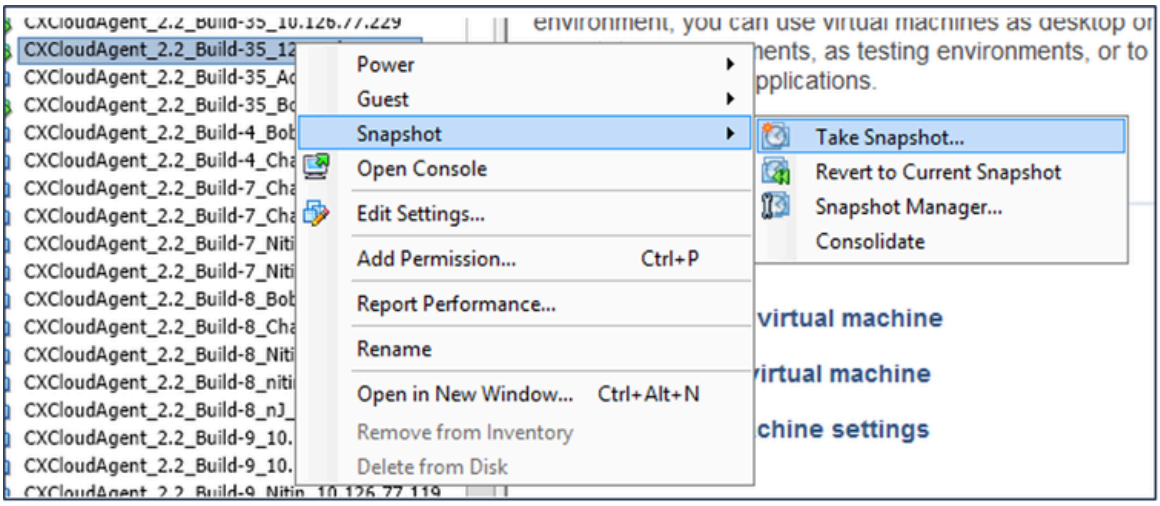
CX Cloud VMのバックアップと復元

スナップショット機能を使用して、CXエージェント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復元できます。

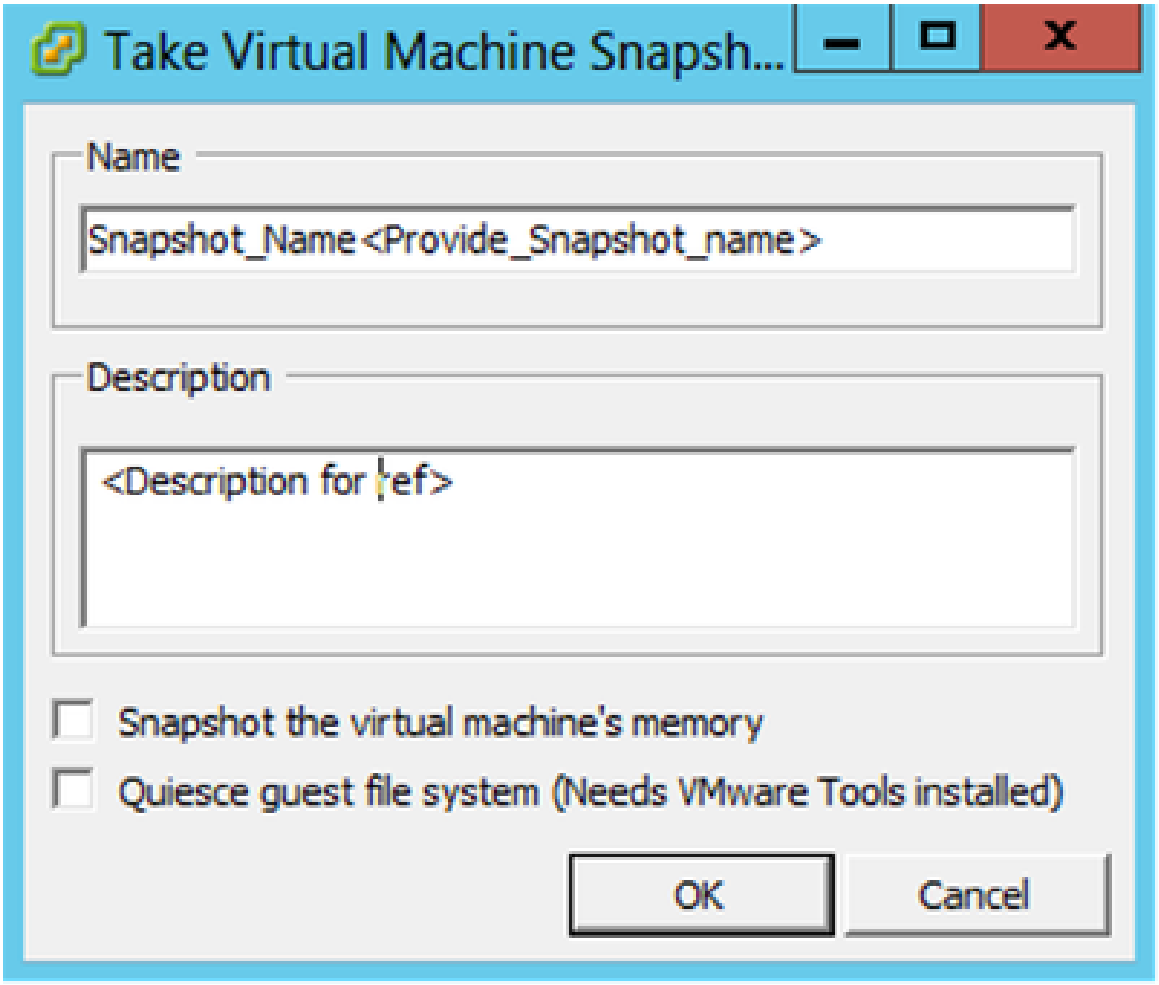
CX Cloud VMのバックアップ

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）]

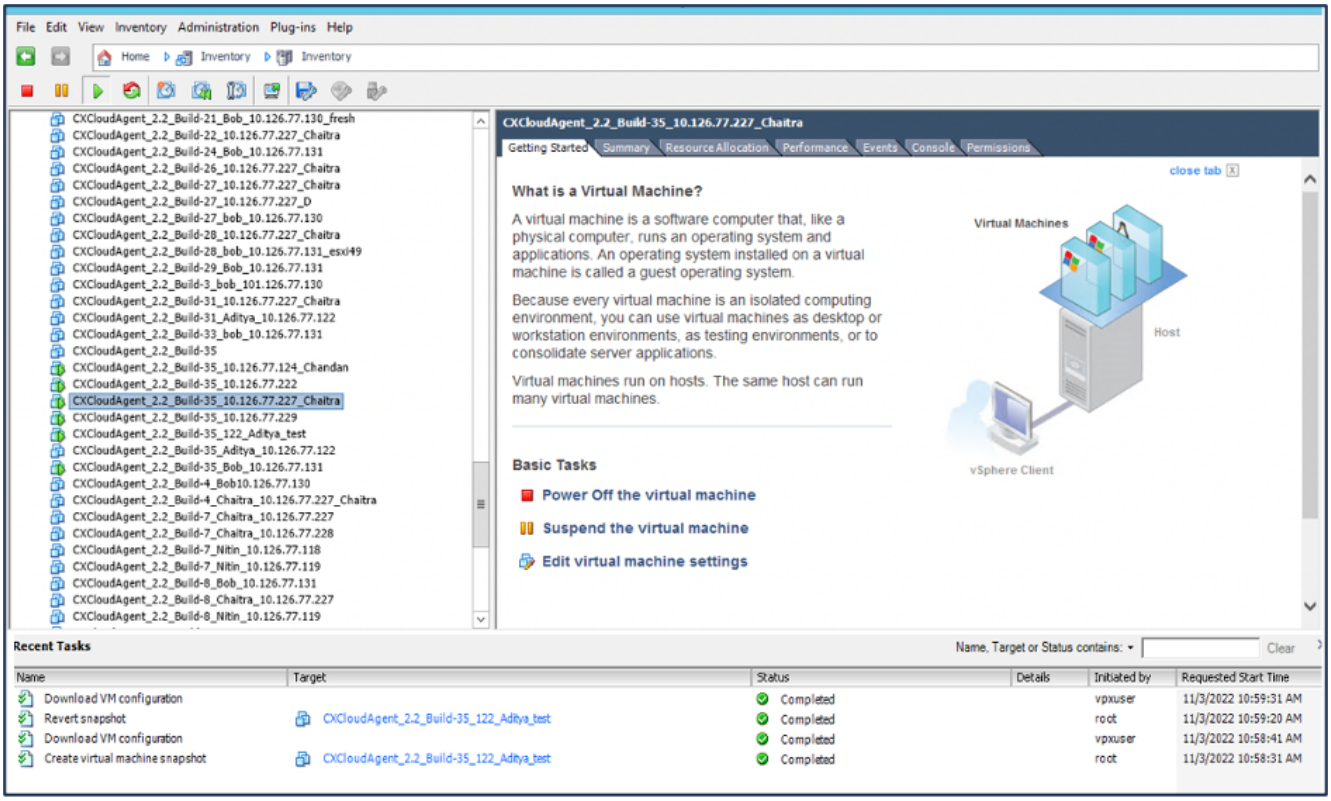


仮想マシンのスナップショットの作成

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。最近使ったタスクの一覧で、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。

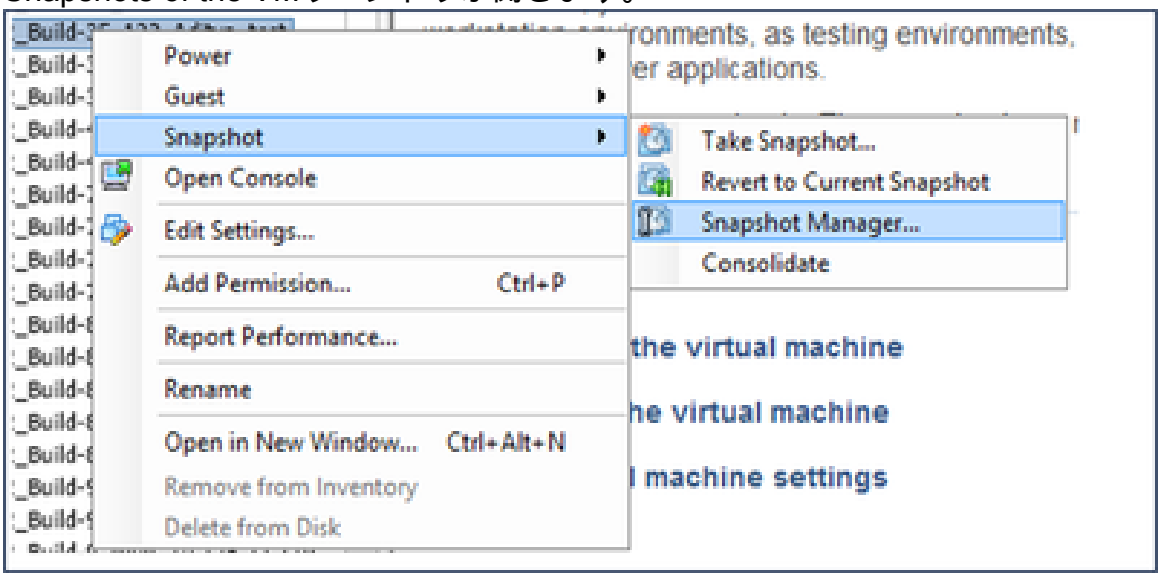


最近のタスク

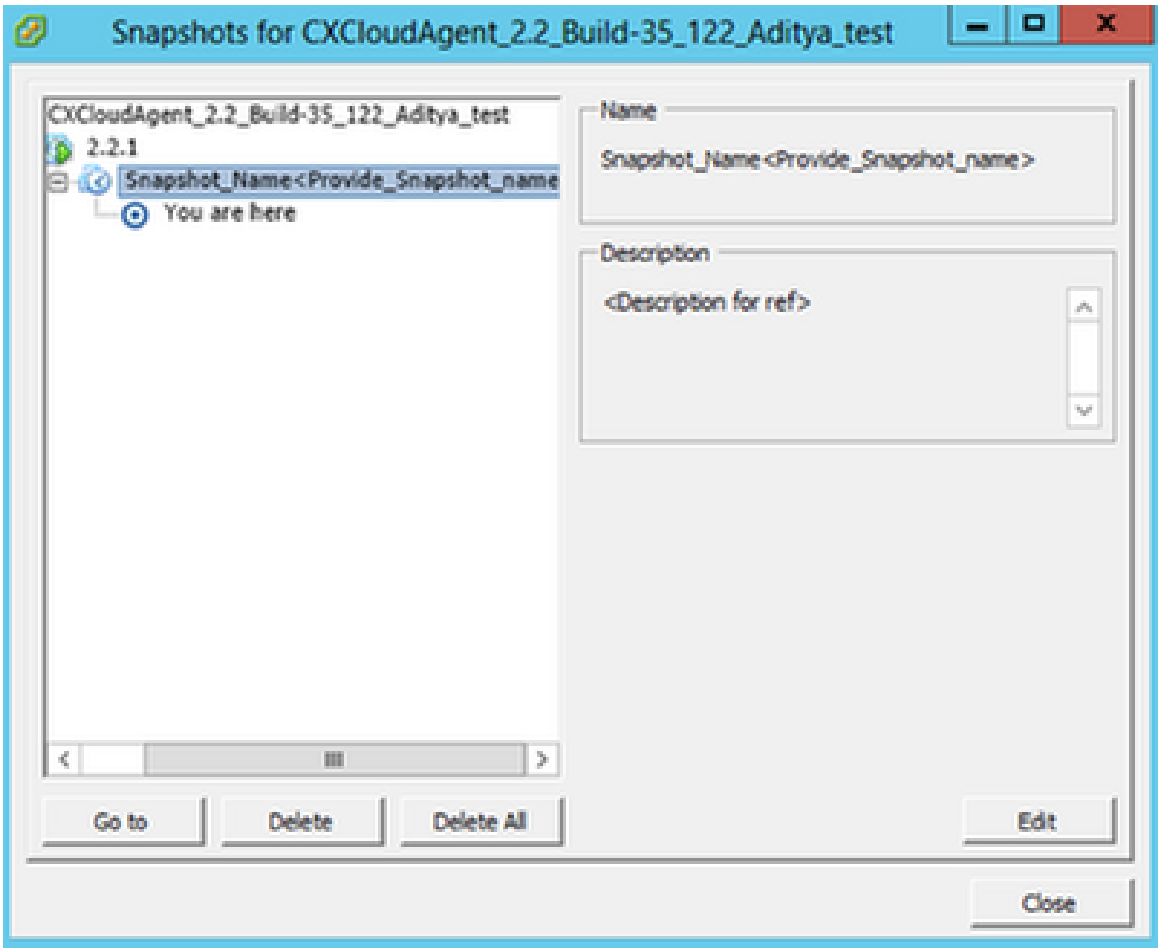
CX Cloud VMの復元

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。

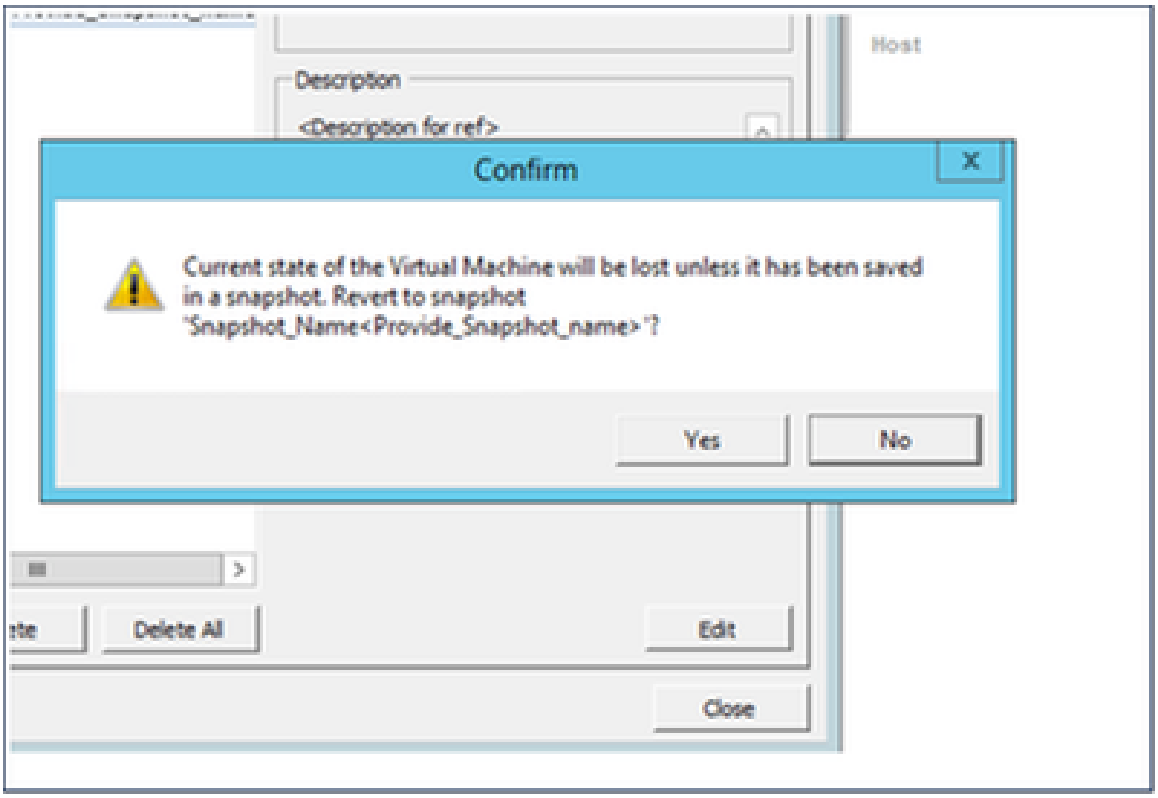


Select VMウィンドウ



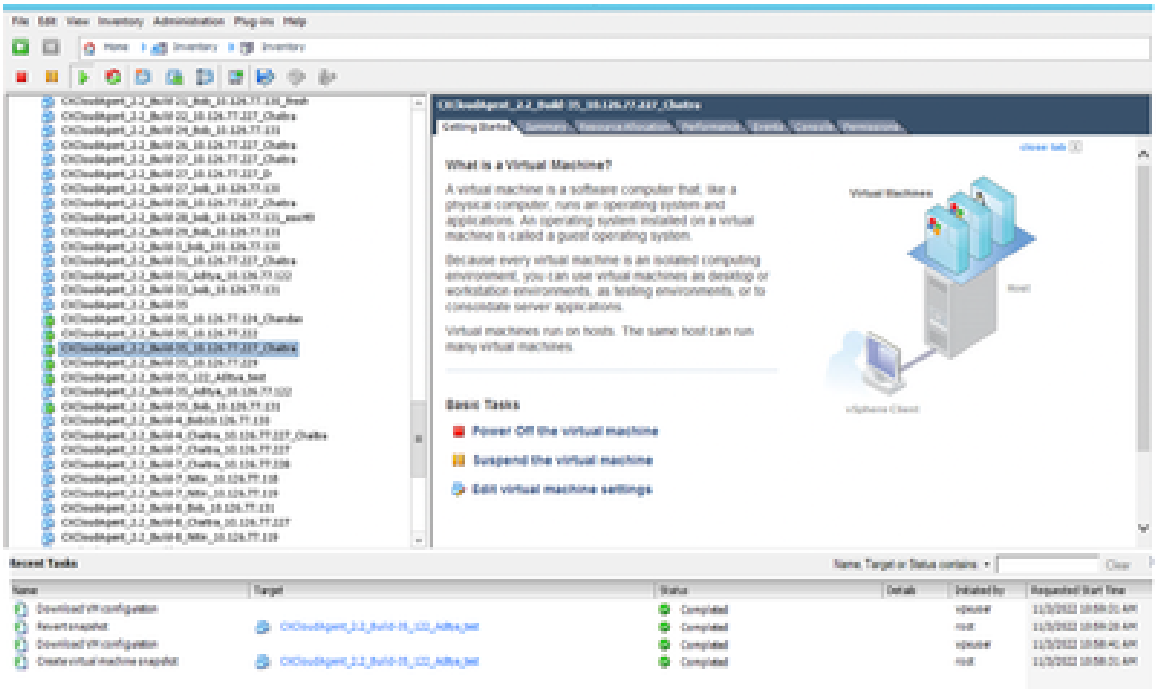
スナップショットウィンドウ

2. Go toをクリックします。Confirmウィンドウが開きます。



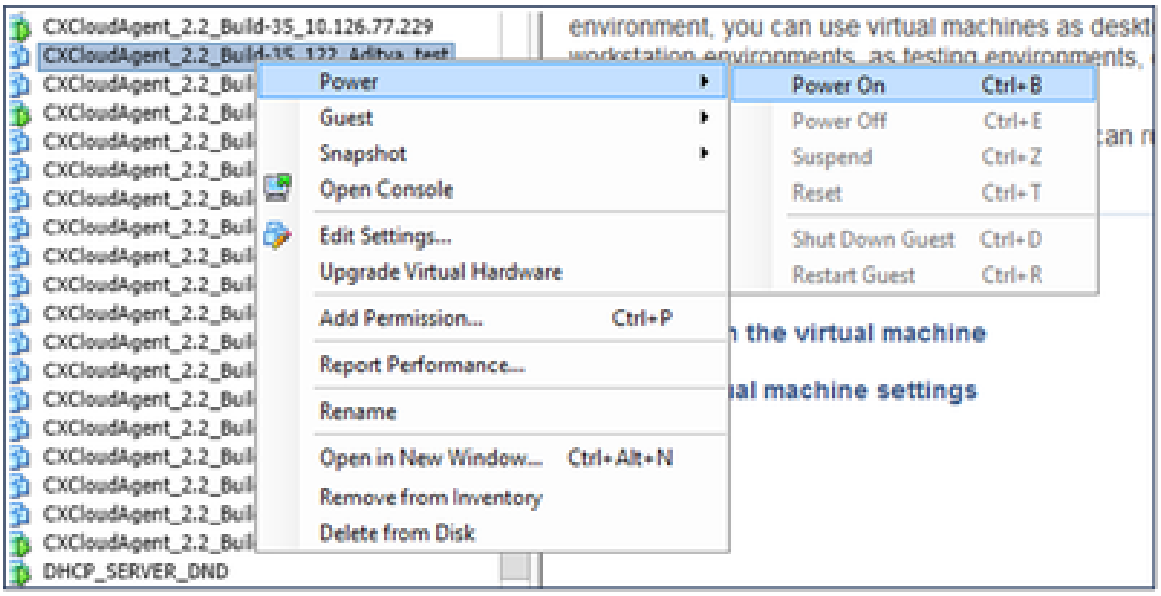
確認ウィンドウ

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 Agentは、お客様のエンド・ツー・エンドのセキュリティを確保します。CX CloudとCX Agent間の接続はTLSで保護されます。Cloud Agentのデフォルト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

セキュリティ保護されたVMwareサーバ会社にCXエージェントOVAイメージを導入します。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。ユーザーは初期設定時にパスワードを設定する必要があります。cxcadminユーザー/認証情報は、CXエージェントAPIへのアクセスとSSH経由でのアプライアンスへの接続に使用されます。

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日間の有効期限で一方向ハッシュされます。cxcadminユーザーは、remoteaccountというユーティリティを使用してcxcrootユーザーを作成できます。cxcrootユーザーはroot権限を取得できます。

ネットワーク セキュリティ

CXエージェント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。

認証

パスワード・ベースの認証：アプライアンスは、単一のユーザー(cxcadmin)を維持します。このユーザーは、このユーザーを使用してCXエージェントの認証と通信を行うことができます。

- 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cxcrootユーザを作成できます。このユーティリティは、RSA/ECB/PKCS1v1_5暗号化パスワードを表示します。このパスワードは、SWIMポータル(DECRYPT Request Form)からのみ復号できます。 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。cxcroot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ユーザはアカウントを再作成し、パスワードの有効期限が切れた後に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 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 Agentアプライアンスは、お客様の個人情報を保存しません。 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、アプライアンスの処理中を除き、アプライアンス内に一時的に保存されることはありません。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が確認された後、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、Iot Coreとのセキュアな接続を確立するために必要な固有のX.509デバイス証明書とキーが含まれています。そ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、セキュリティに影響を受けるすべてのアクションが記録されます。

Cisco Telemetry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 Catalyst Centerインベントリ、Diagnostic Bridge、Intersight、Compliance Insights、Faults、およびCXエージェントによって収集されたその他すべてのテレメトリ源へのコマンドの適用性に基づいて、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エージェントは

、テレメトリをCXエージェントに直接送信するすべての収集されたアセットの機密データをマスキングします。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資産に対してデータ・マスキングを行ってから、この情報をCXエージェントに転送します。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(例：『Cisco Catalyst Centerアドミニストレータガイド』の「データの匿名化」セクション)。

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、お客様は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エージェントが収集するその他の資産の場合）で説明されているように、データソースを指定することで、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FAQを参照して、ブートローダ（シングルユーザモード）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： ·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。 · 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。
ユーザアカウント	· 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エージェントのアプリケーション・コマンドを実行でき、アプライアンスに対して最小限の権限を持ちます。 cxcrootユーザーとその暗号化パスワードはcxcadminユーザーを使用して生成されます。 · 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。
cxcadmin パスワードポリシー	·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。 · 大文字、小文字、数字、特殊文字のうち3つのカテゴリを含む、8文字以上

cxcroot パスワードポリシー	· cxcrootのパスワードはRSA/ECB/PKCS1v1_5で暗号化 ·生成されたパスフレーズは、SWIM ポータルで復号する必要があります。 · 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。
ssh ログインパスワードポリシー	· 8文字以上で、大文字、小文字、数字、特殊文字の3つのカテゴリを含みます。 · 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。パスワードは90日で期限切れになります。
ポート	オープンな着信ポート - 514（Syslog）と 22（SSH）
データセキュリティ	·顧客情報は保存されません。 ·デバイスデータは保存されません。 · Cisco Catalyst Centerサーバのクレデンシャルは暗号化され、データベースに保存されます。

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。