CX Cloud Agentの概要v2.2

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)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.csco.cloud
  - FQDN:ng.acs.agent.us.csco.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

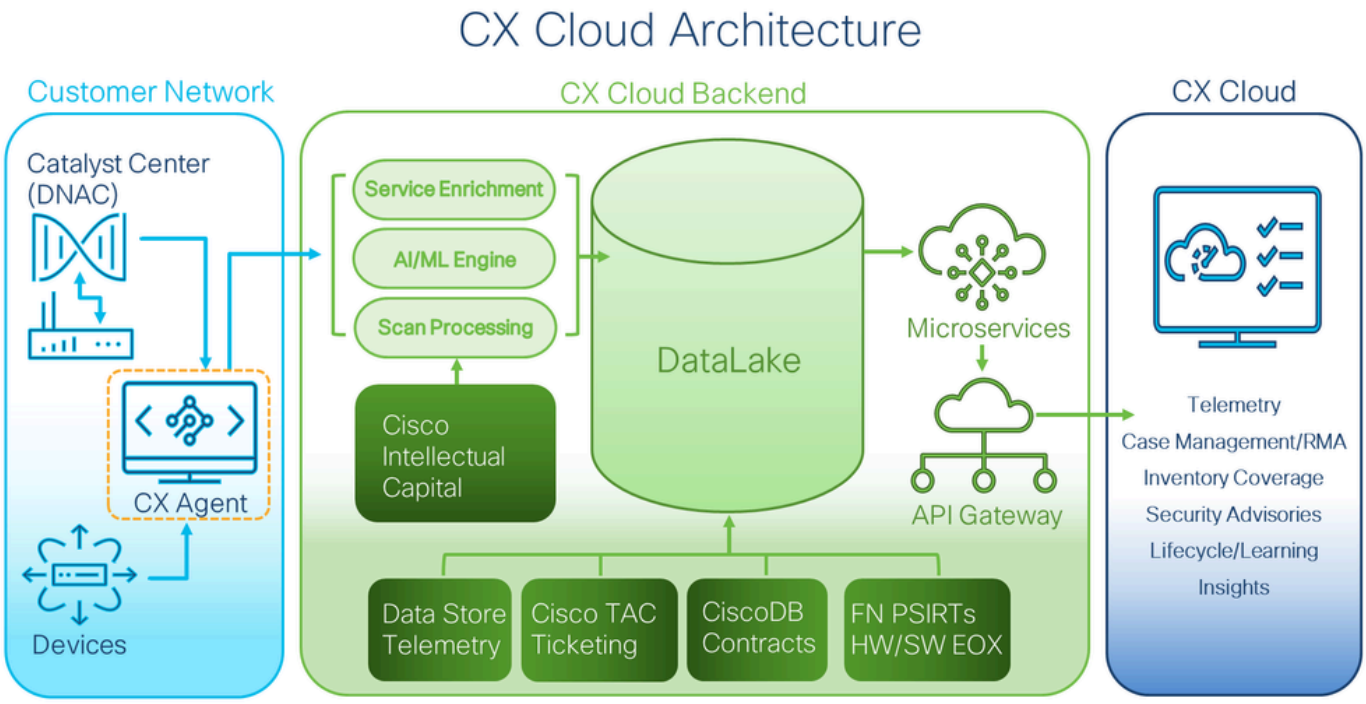
用して、ここに示す両方のサーバに接続できる必要があります。
    - FQDN:agent.us.csco.cloud
    - FQDN:agent.emea.csco.cloud
    - FQDN:ng.acs.agent.emea.csco.cloud
    - FQDN:cloudsso.cisco.com
    - FQDN:api-cx.cisco.com
- CX Cloudデータを格納する主要なデータリージョンとしてアジア太平洋地域の指定データセンターを使用しているお客様：CX Cloud Agentは、FQDNを使用して、およびTCPポート443のHTTPSを使用して、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に登録する場合にのみ、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。

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

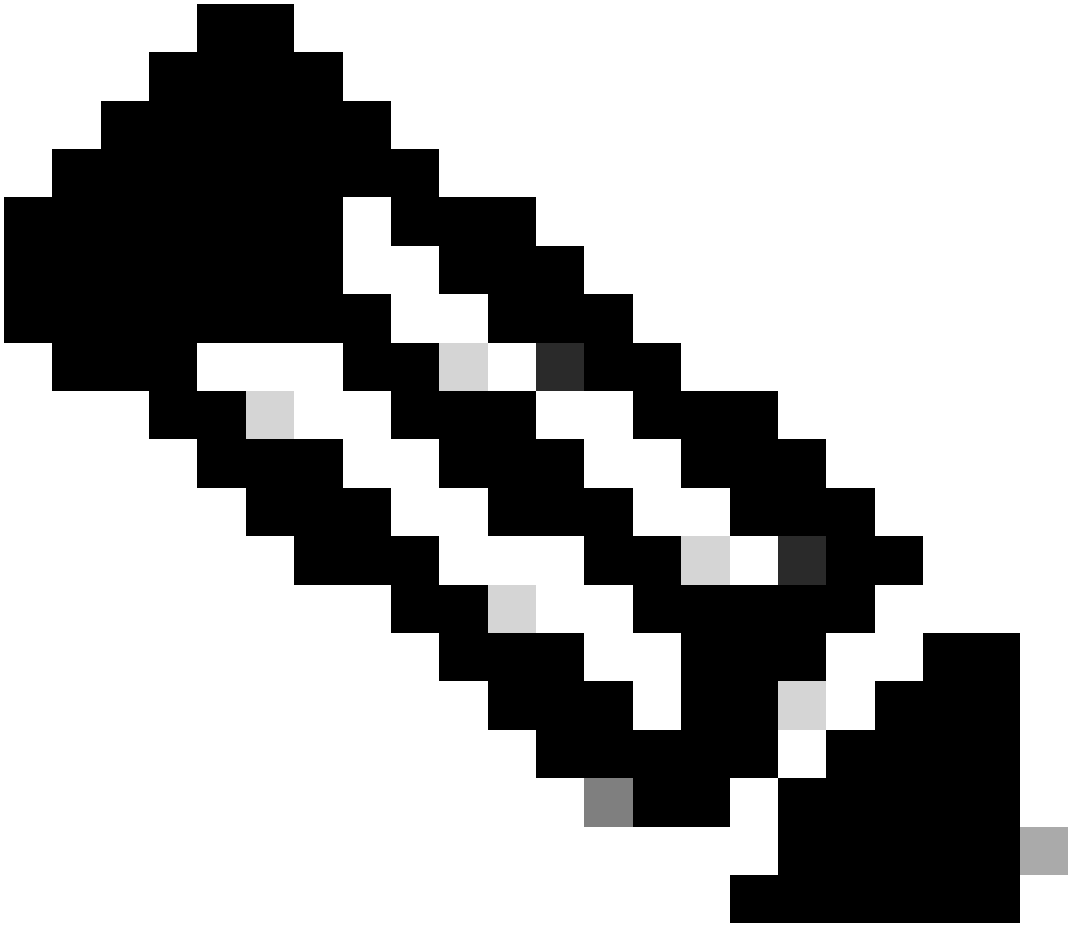
背景説明

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アドレスを使用できる必要があります。
- 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
csco.cloud	cloudfront.net
split.io	eum-appdynamics.com
	appdynamics.com
	tiqcdn.com
	jquery.com

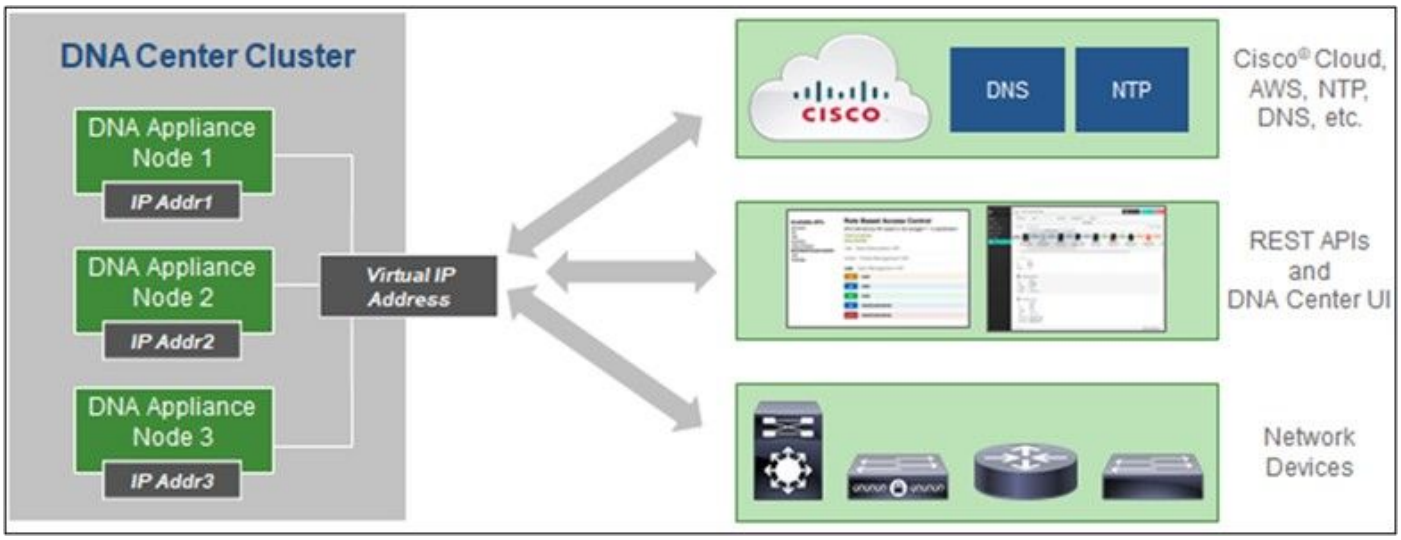
CX Cloud Agent OVAに固有のドメイン

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.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。

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

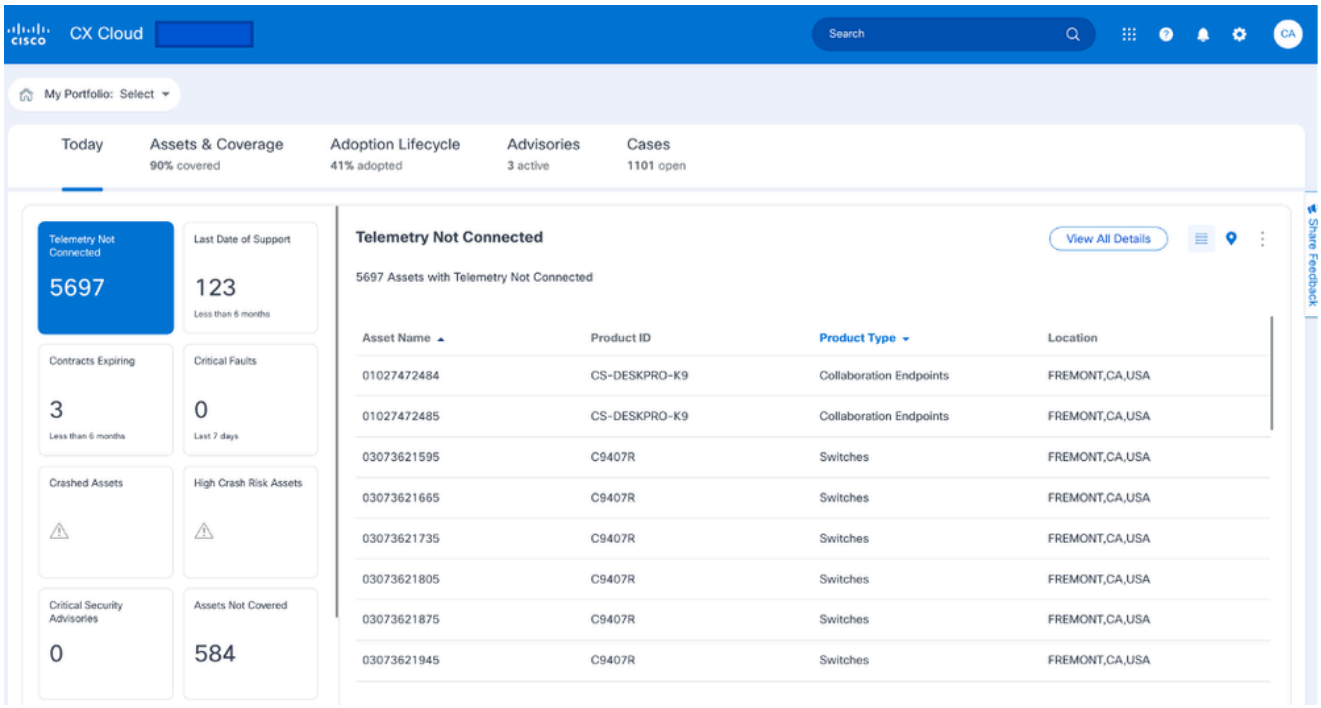
サポートされる製品リスト

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

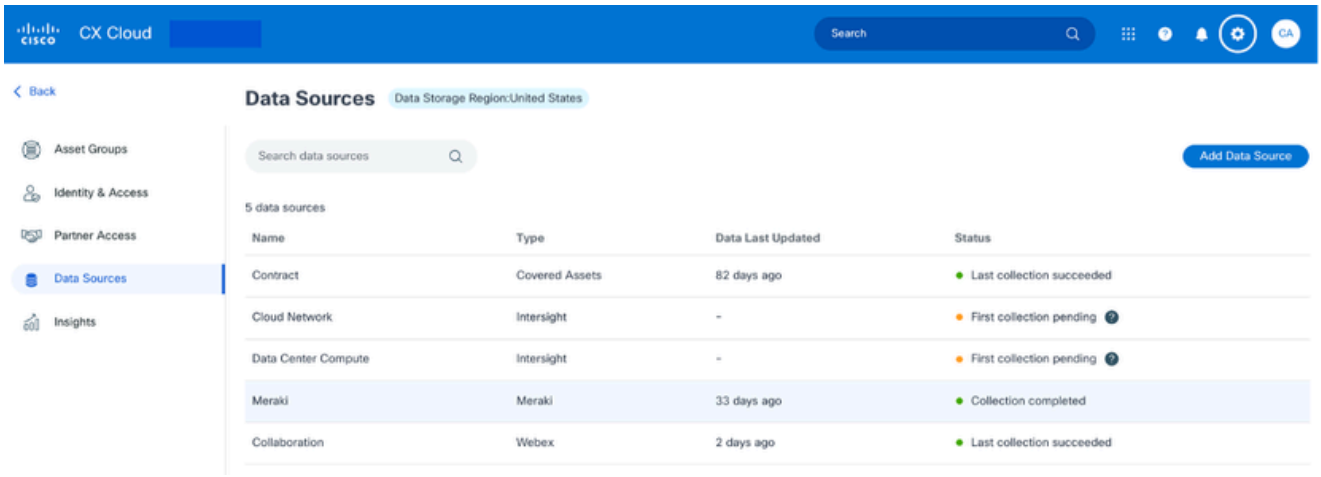
データ・ソースを接続するには、次の手順に従います：

1. cx.cisco.comをクリックして、CX Cloudに口グインします。



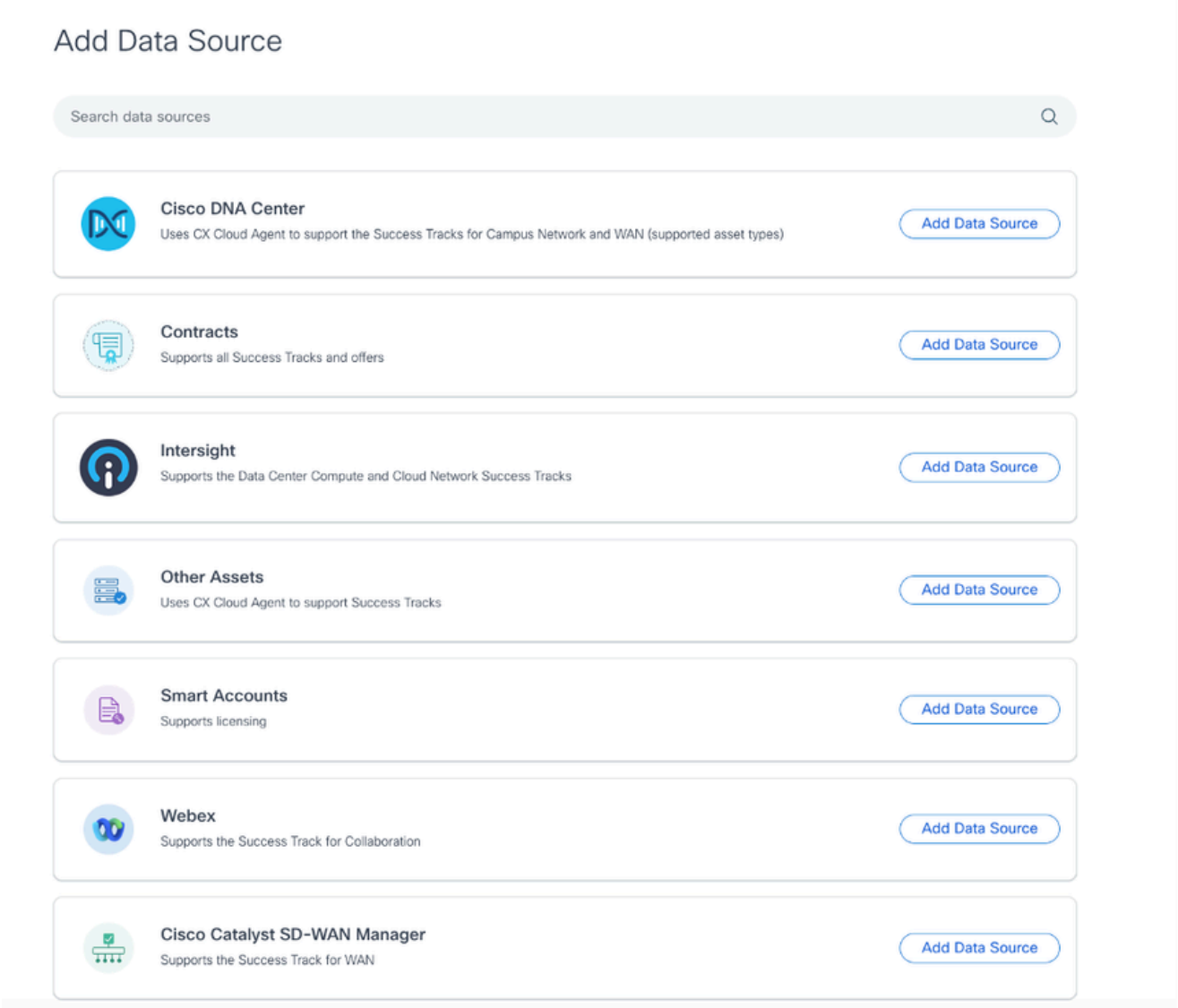
CX Cloudホームページ

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。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。



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]

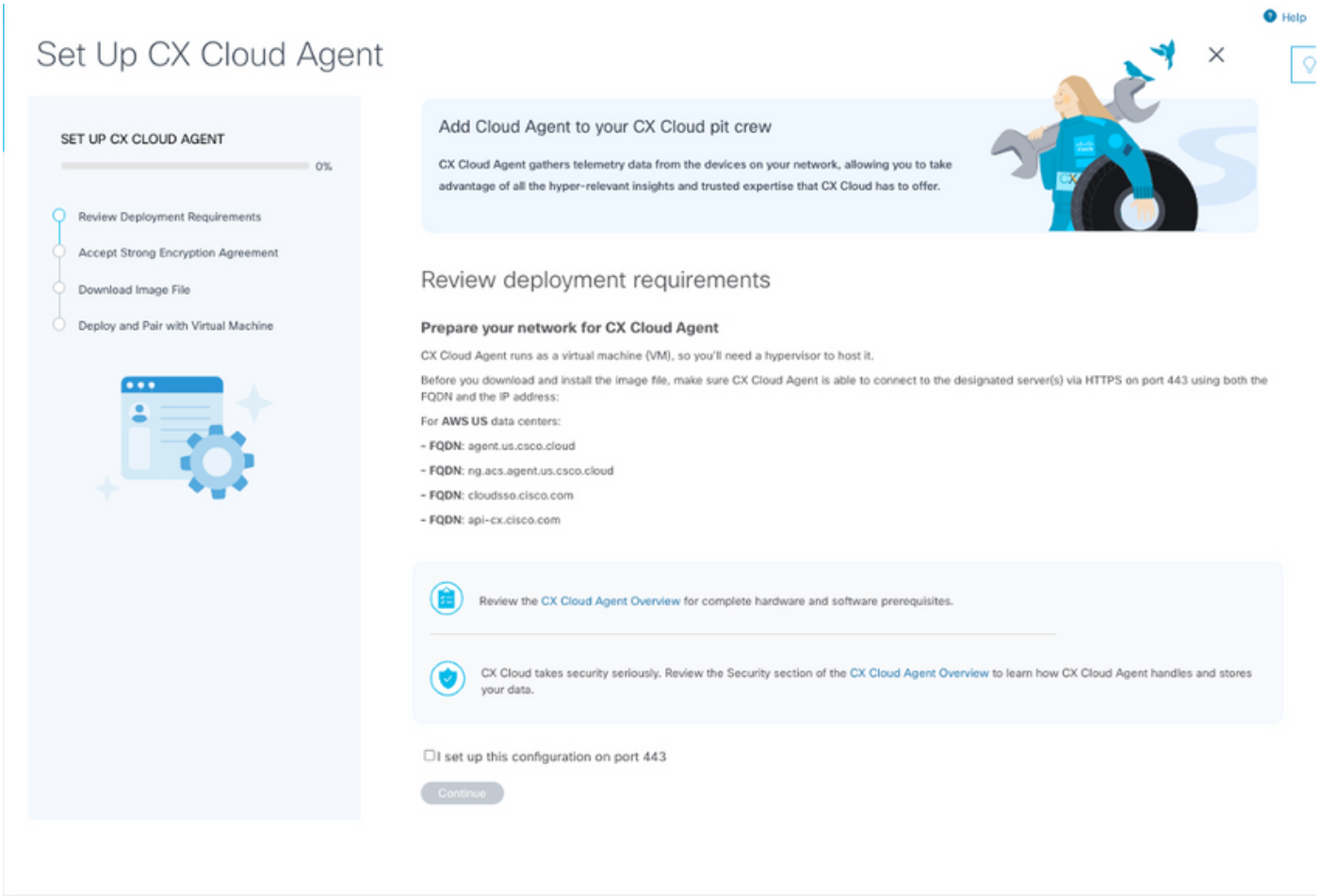
注:[その他のアセット]オプションは、ダイレクトデバイス接続が以前に設定されていない場合にのみ使用できます。

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

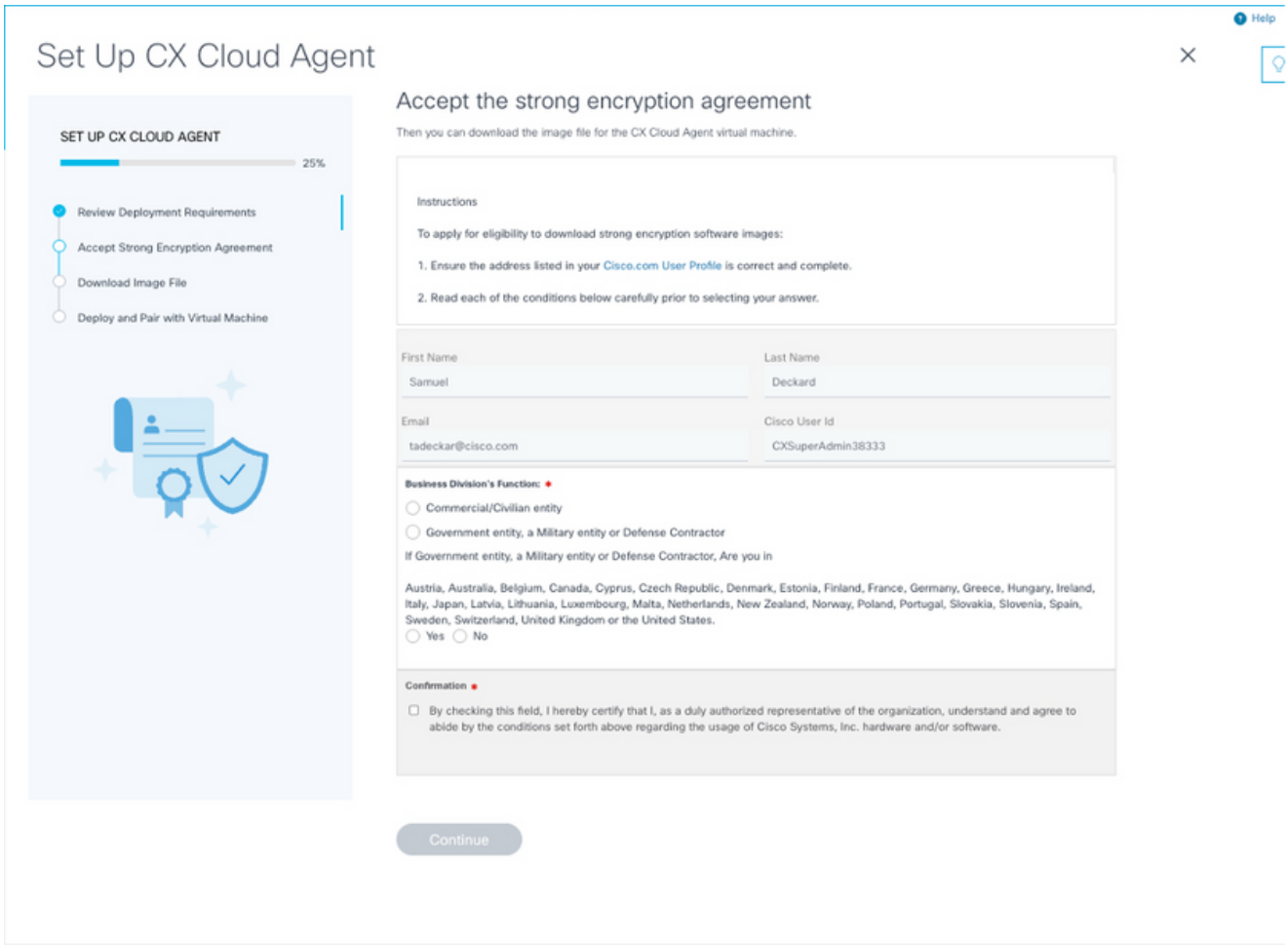
アップのプロンプトが表示されます。

CX Cloud Agentをセットアップするには、次の手順を実行します。



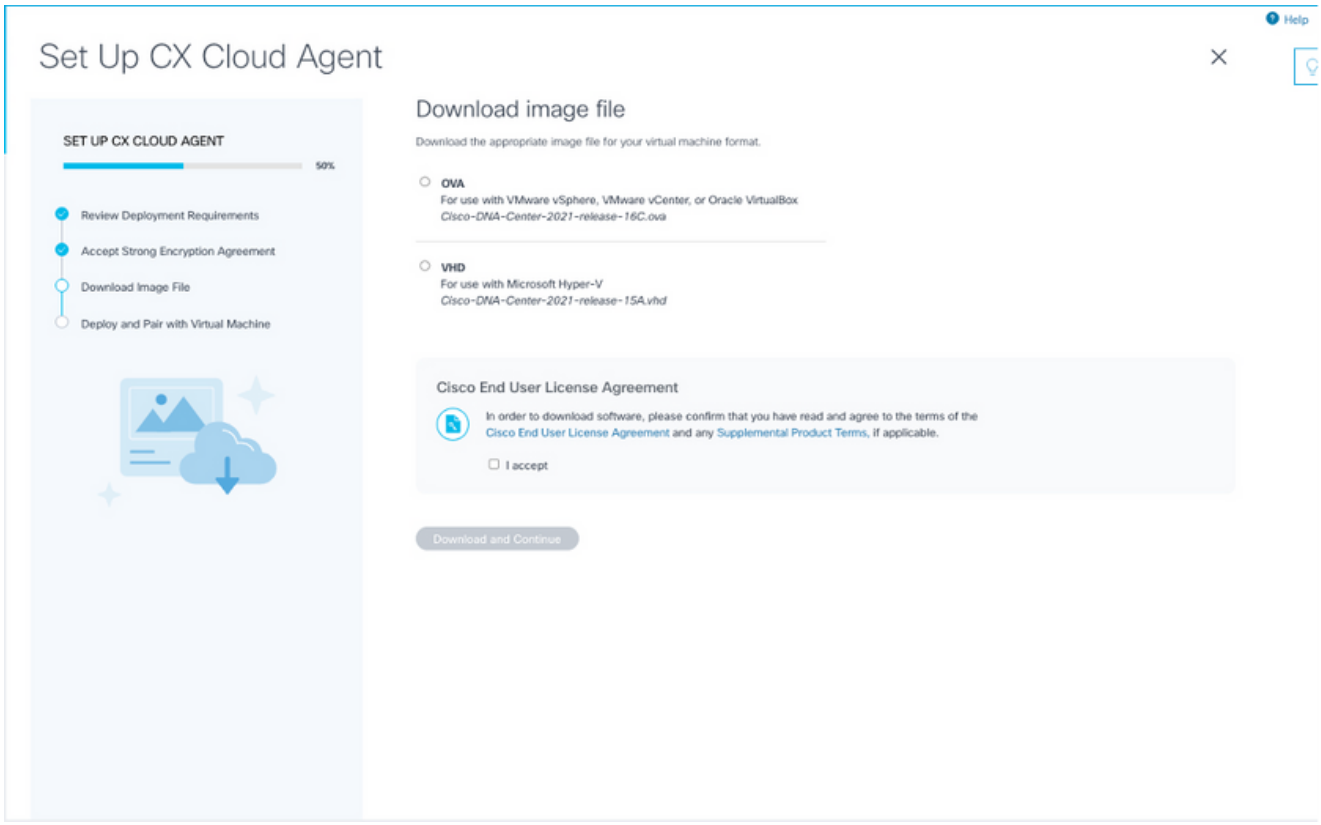
導入要件の確認

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。



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. 次の項で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。

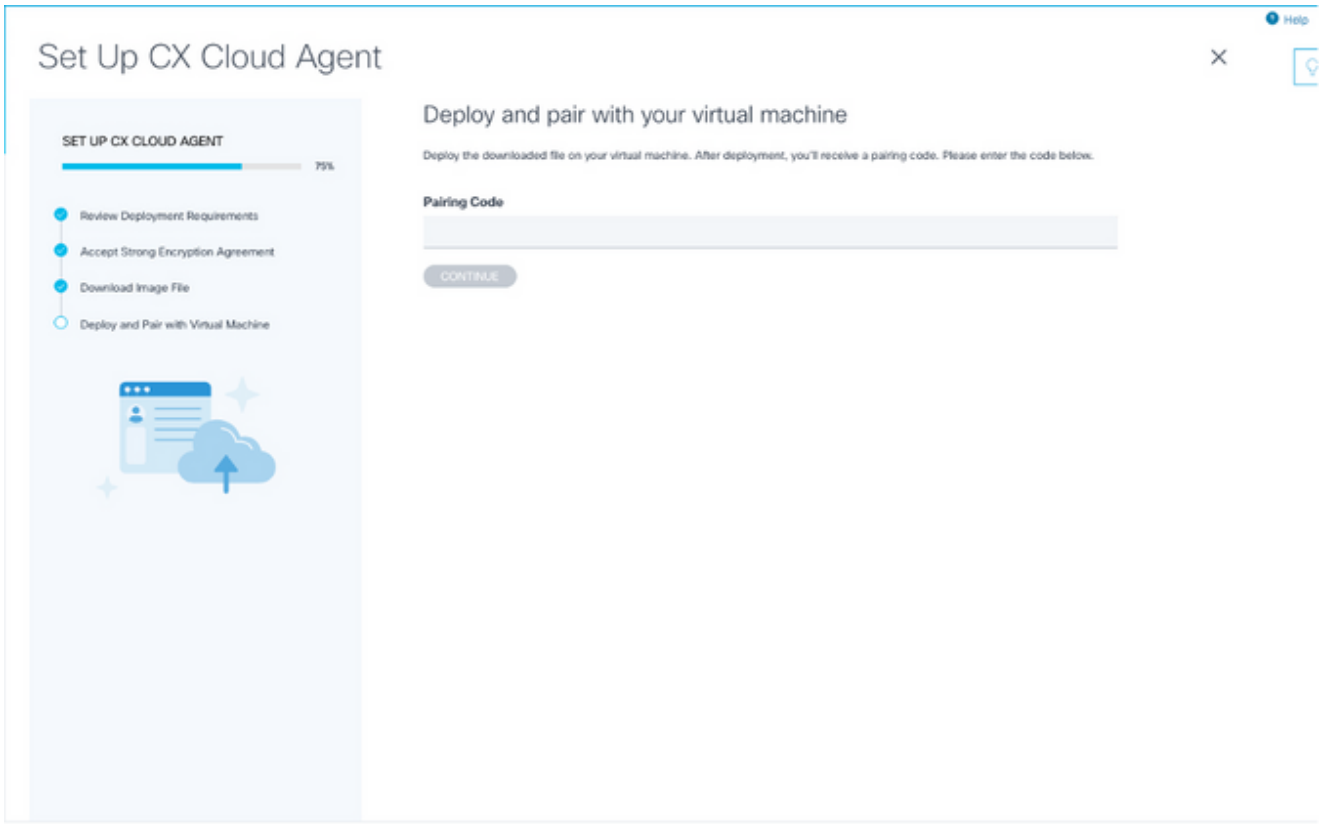
CX Cloud Agent と CX Cloud の接続

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。

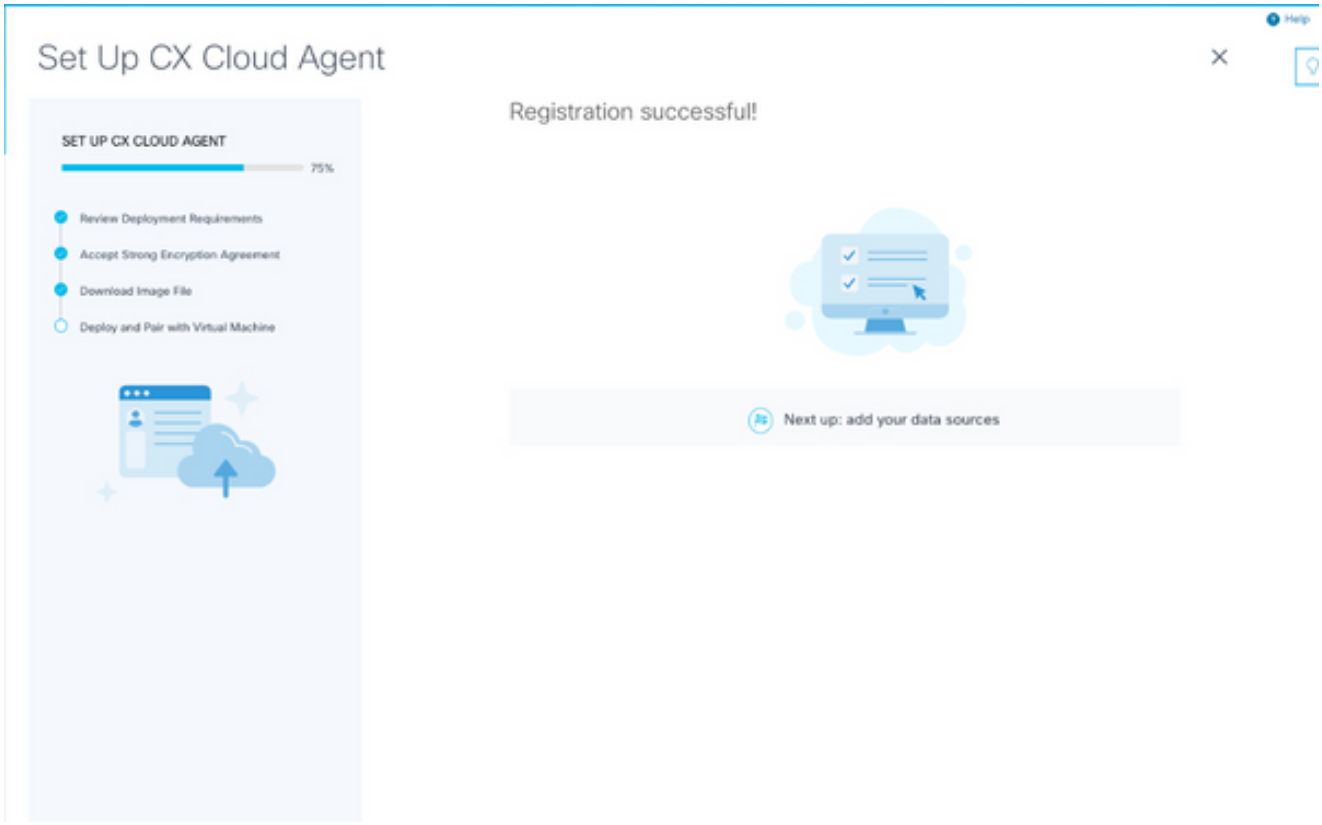
1. エージェントを介して接続された仮想マシンのコンソールダイアログまたはコマンドラインインターフェイス(CLI)に表示されるペアリングコードを入力します。

> 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

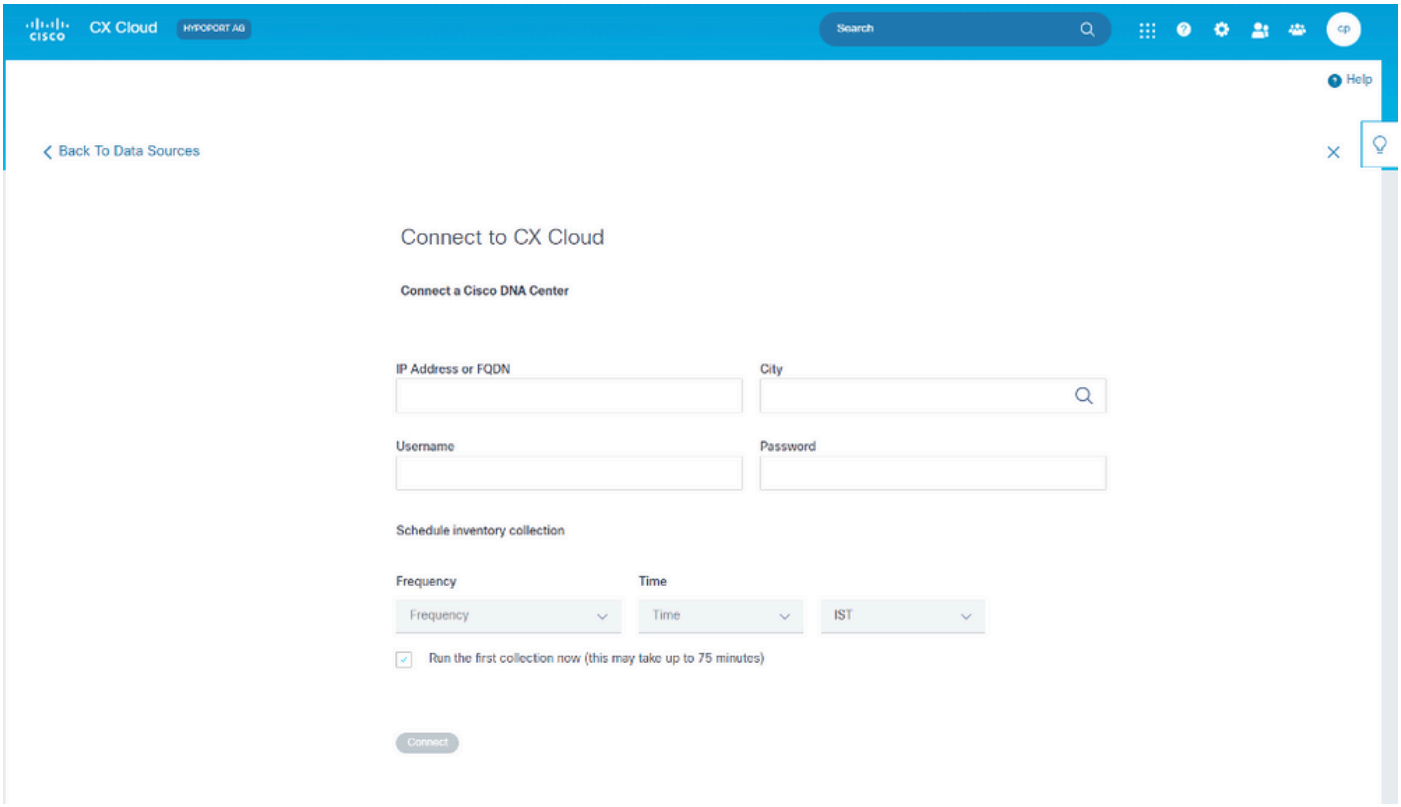
2. Continueをクリックして、CX Cloud Agentを登録します。CX Cloud Agentのセットアップ – 登録が正常に完了しましたウィンドウが短時間開いた後、自動的にデータソースの追加ページに移動します。



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。

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。

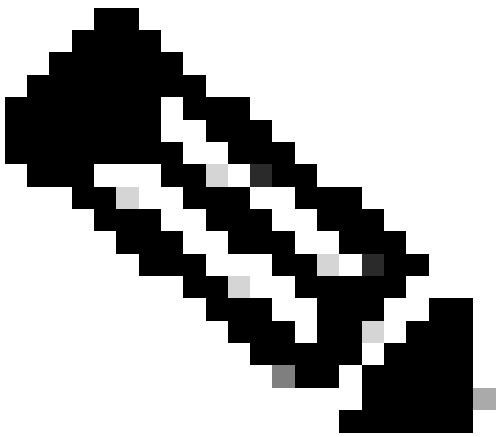
列ヘッダーを含むサンプルシードファイルの形式は、一切変更しないことが重要です。表示されたリンクをクリックして、PDF形式のシードファイルを表示します。このPDFは参照専用で、.csv形式で保存する必要があるシードファイルの作成に使用できます。

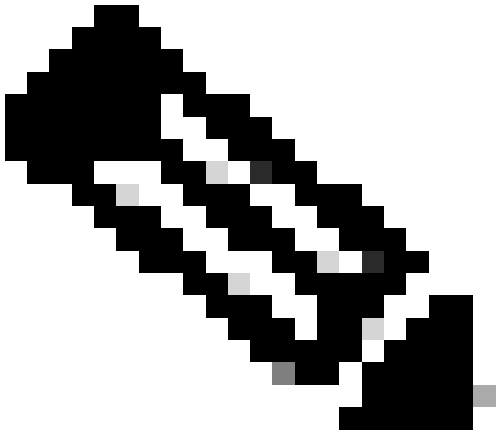
.csv形式のシードファイルの作成に使用できるシードファイルを表示するには、このリンクをクリックします。

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
		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。
C	snmpRo:col#=3が「snmpv2c」として選択されている場合は必須	特定のデバイスに対して従来のSNMPv2バ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にすることができます	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。  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。
F	snmpv3AuthPassword：パ	デバイスにMD5またはSHA暗号化アルゴリズ

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	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。  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。
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。

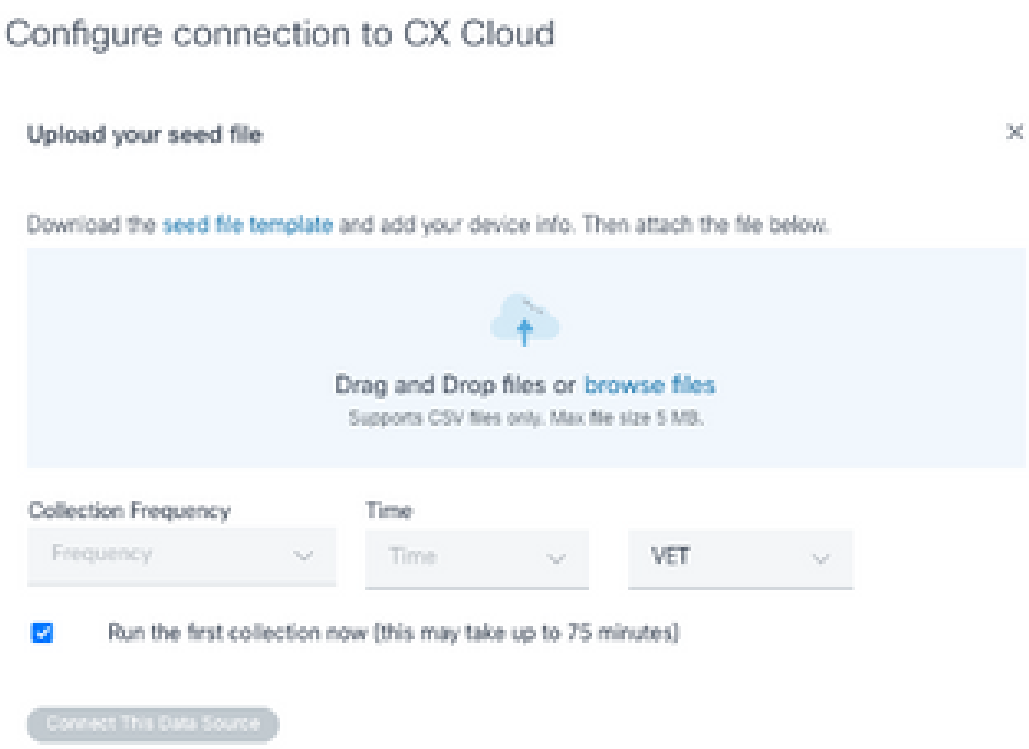
- Campus Successトラックに含まれないデバイスのテレメトリ属性が、CX Cloud Assetsページで不正確または欠落する可能性があります。
- シードファイルまたはIP範囲コレクションのデバイスがCisco DNA Centerインベントリの一部でもある場合、デバイスはCisco DNA Centerエントリに対して1回だけ報告されます。シードファイルまたはIP範囲のエントリは、重複を避けるために収集も処理もされません。

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。

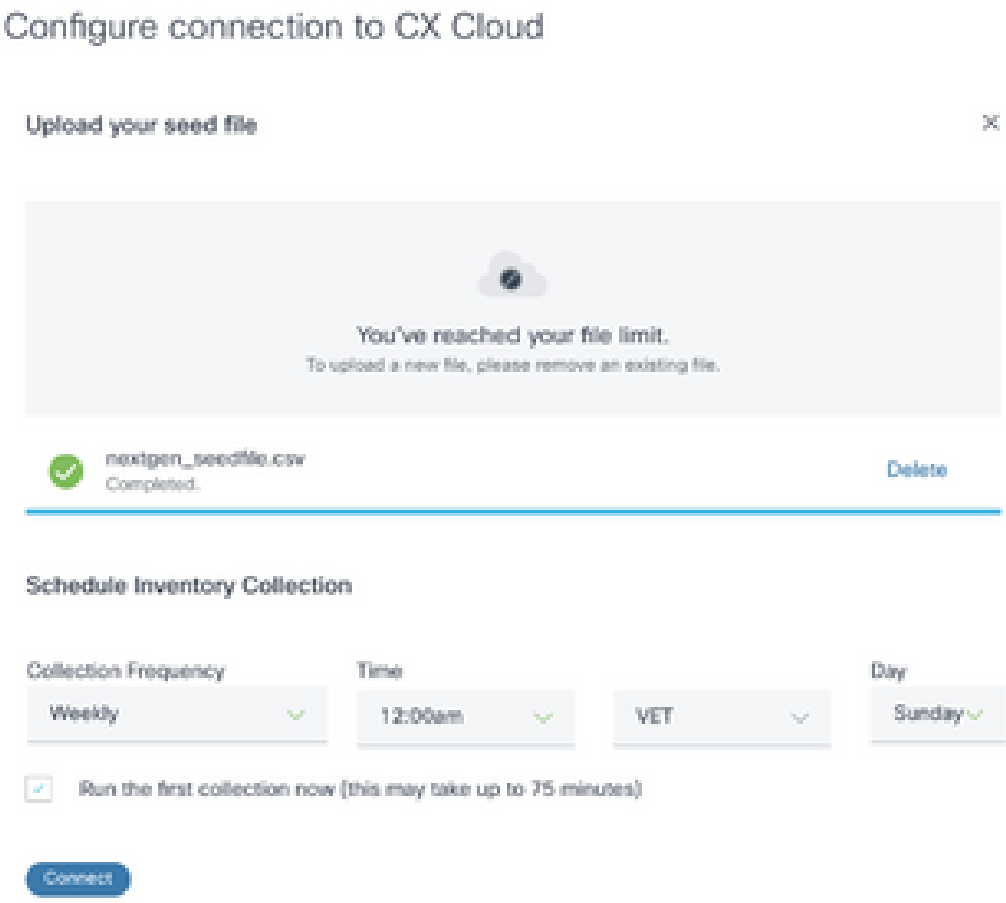
1. このドキュメントの埋め込みリンク（「シードファイルについて」を参照）を使用するか、「CX Cloudへの接続の設定」ウィンドウのリンクを使用して、シードファイルテンプレート(PDF)をダウンロードします。

   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。



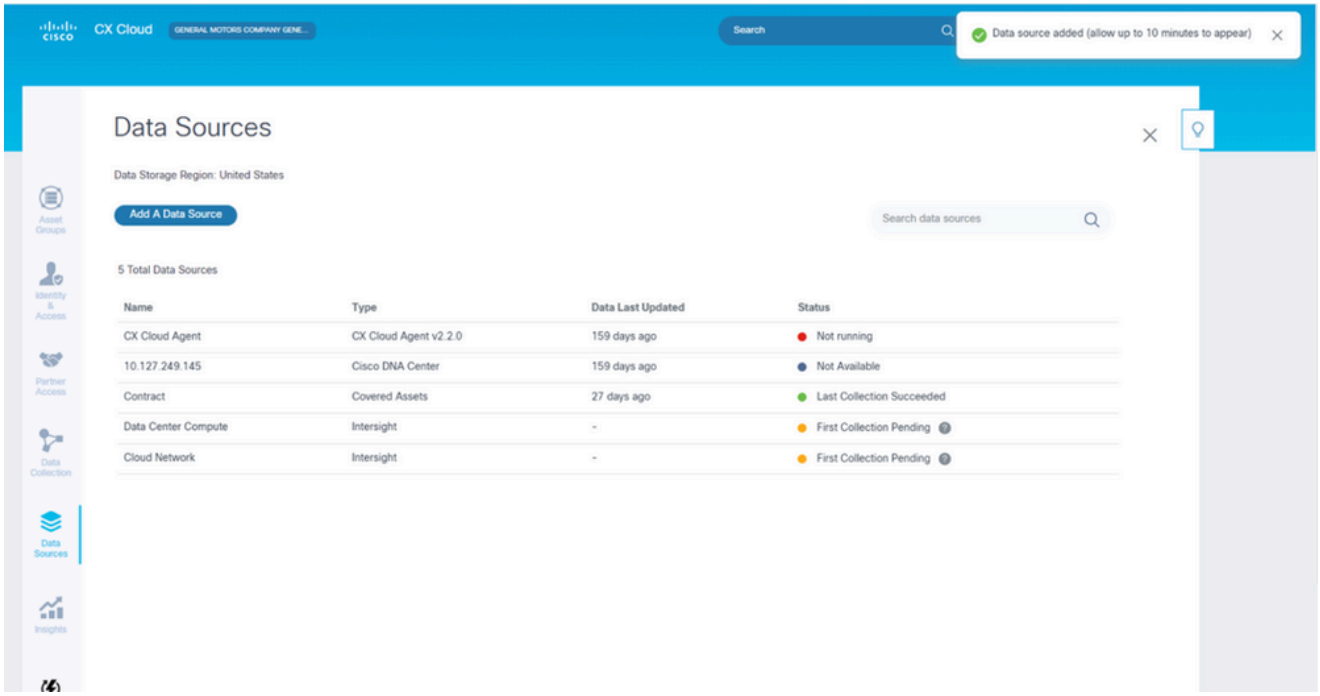
「CX Cloudへの接続の設定」ウィンドウ

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。



Upload Seed Fileウィンドウ

5. 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。
6. 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。
7. 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。



確認メッセージ

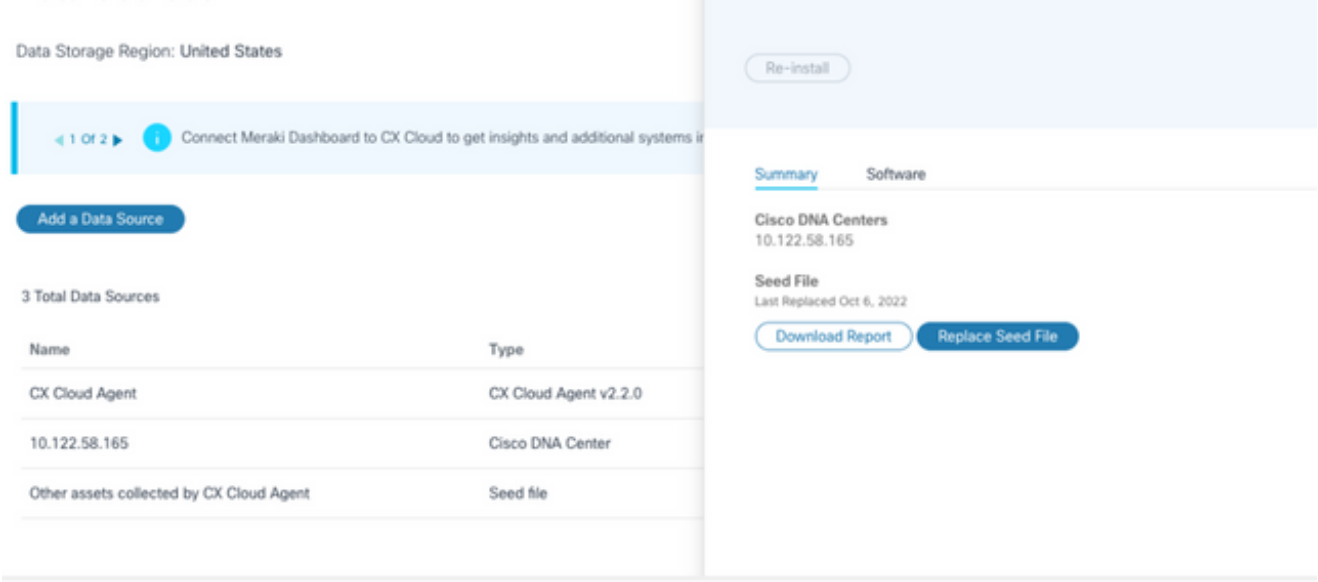
変更したシードファイルを使用してデバイスを追加する

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。

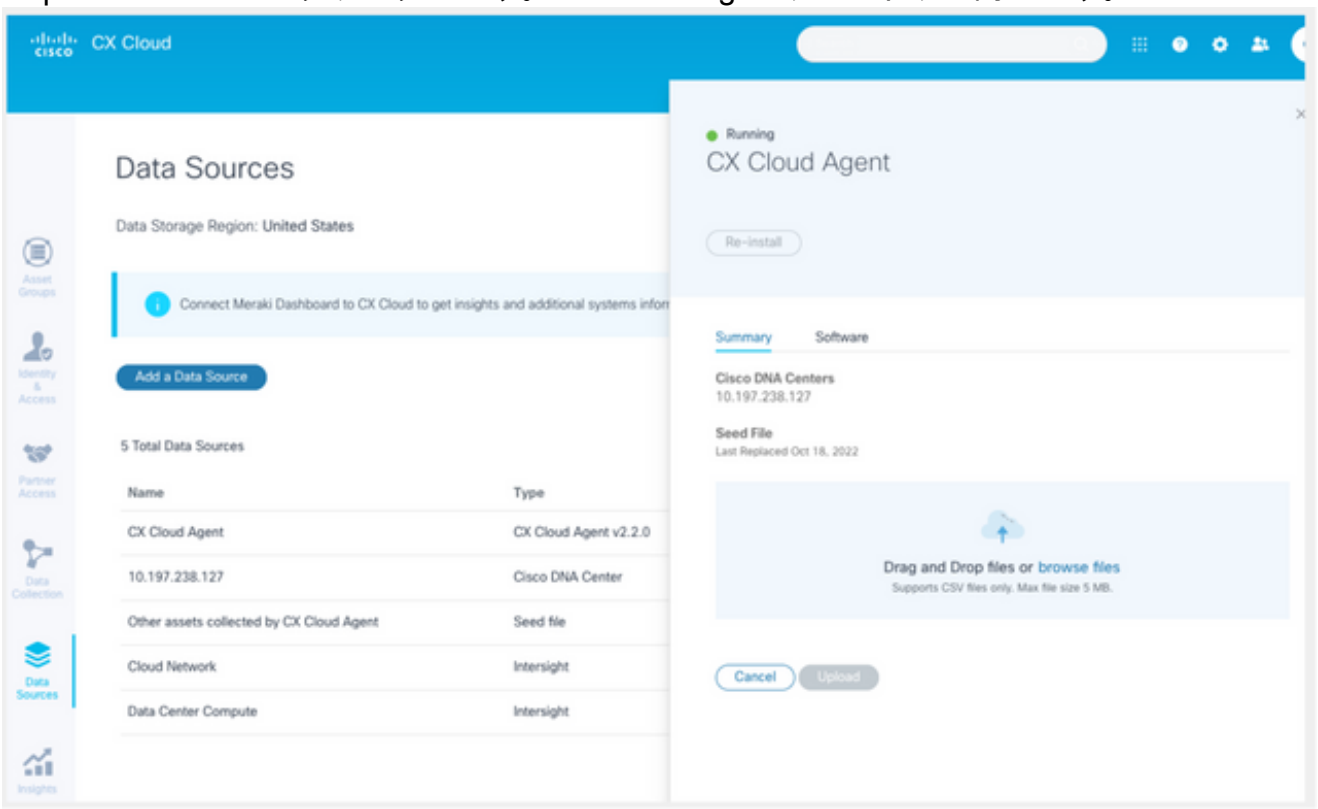
> 注：シードファイルにアセットを追加するには、以前に作成したシードファイルにアセットを追加し、ファイルをリロードします。新しいシードファイルをアップロードすると現在のシードファイルが置き換えられるため、これが必要になります。検出と収集には、アップロードされた最新のシードファイルのみが使用されます。

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

3. 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。
4. 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

5. 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。
6. [Upload] をクリックします。

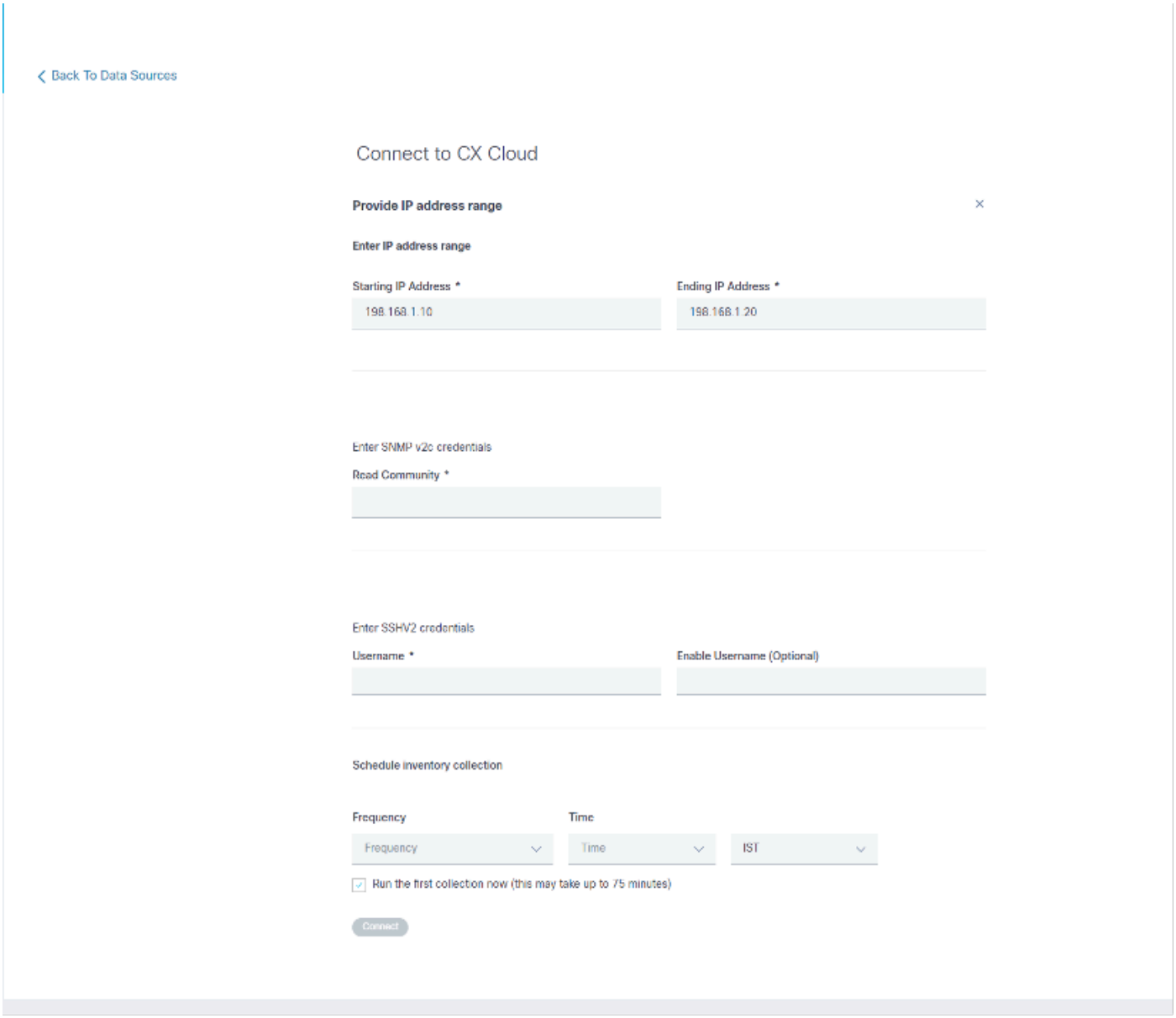
IP範囲を使用したデバイスの追加

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。



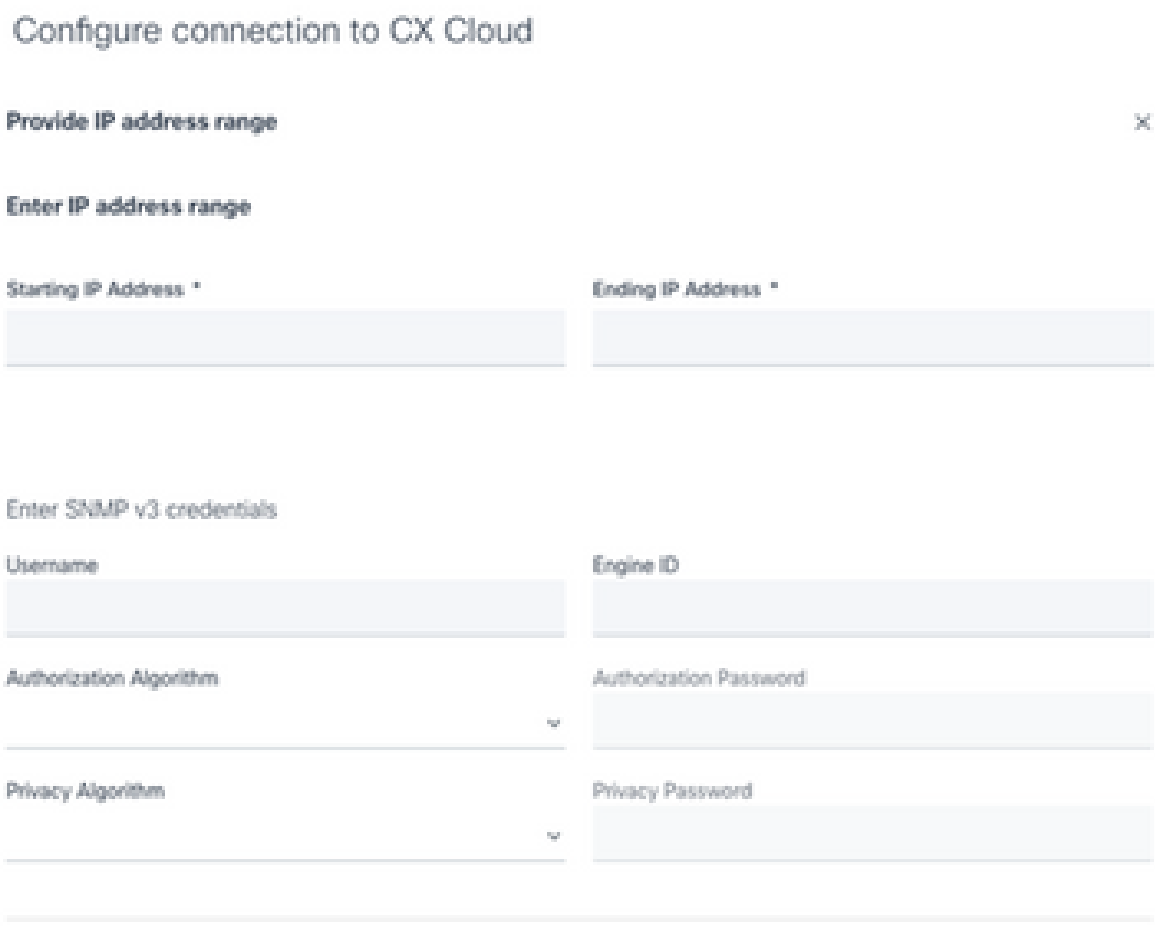
初期IPアドレス範囲ウィンドウ

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。

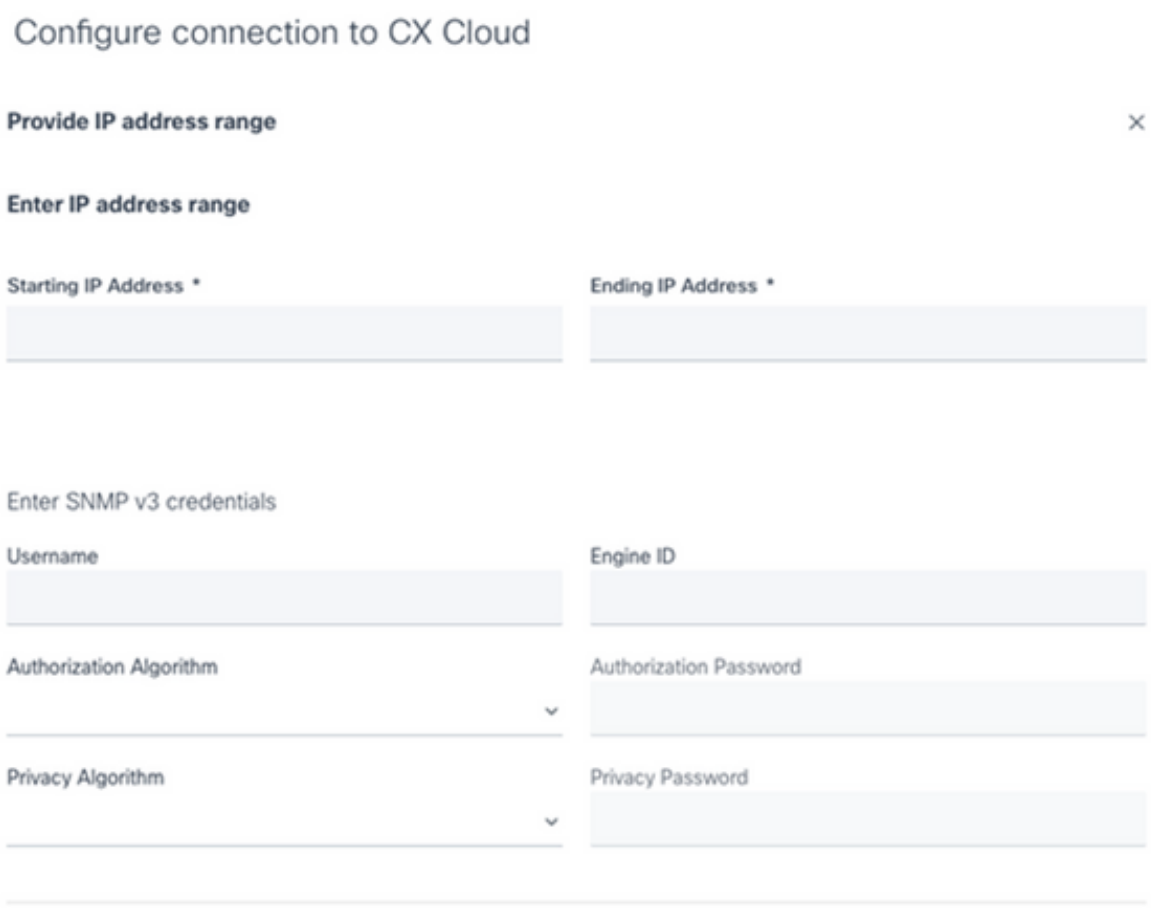
IP範囲を使用してデバイスを追加するには、次の手順を実行します。

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。

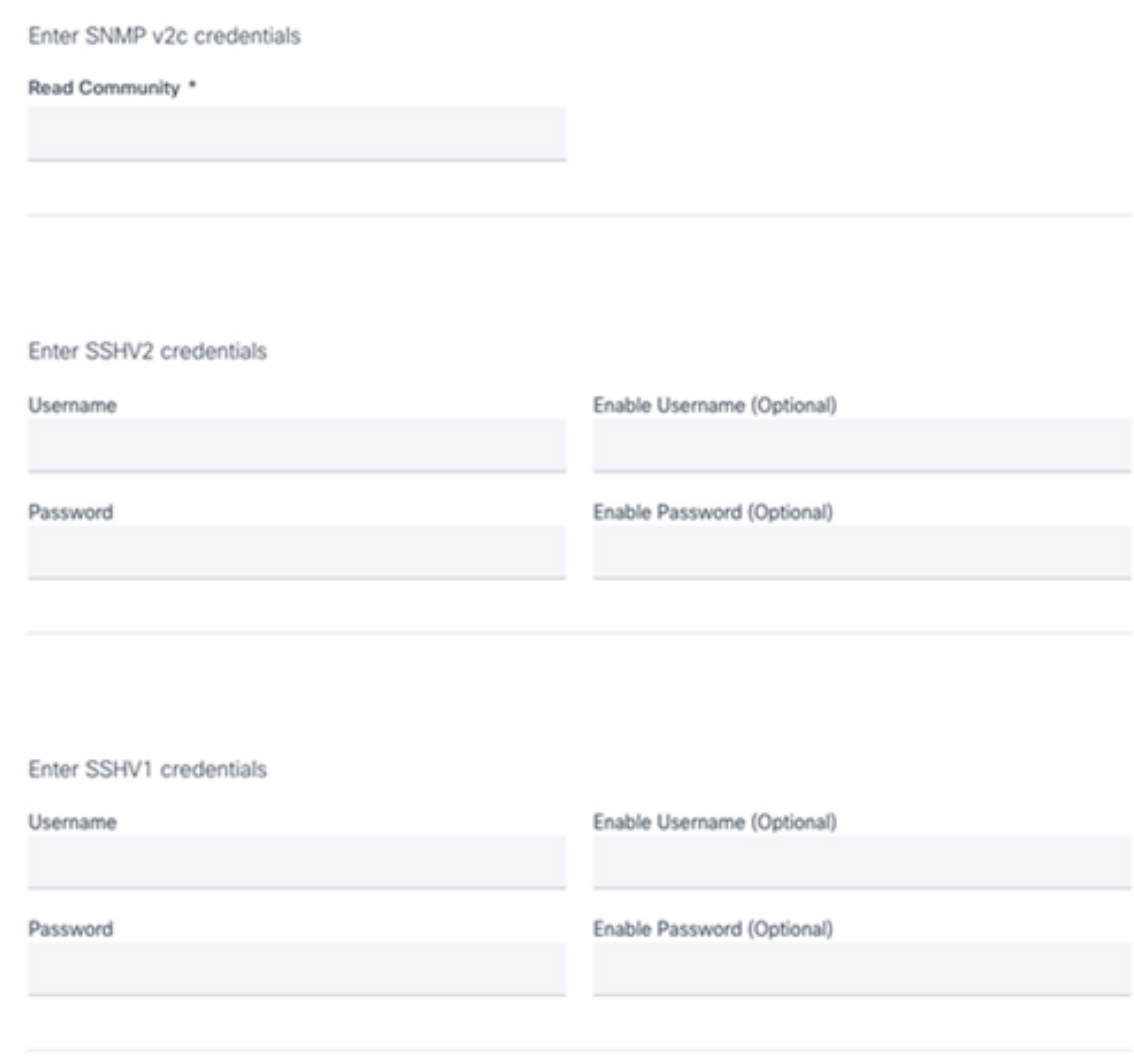


IPアドレスフォームを使用してデバイスを追加する

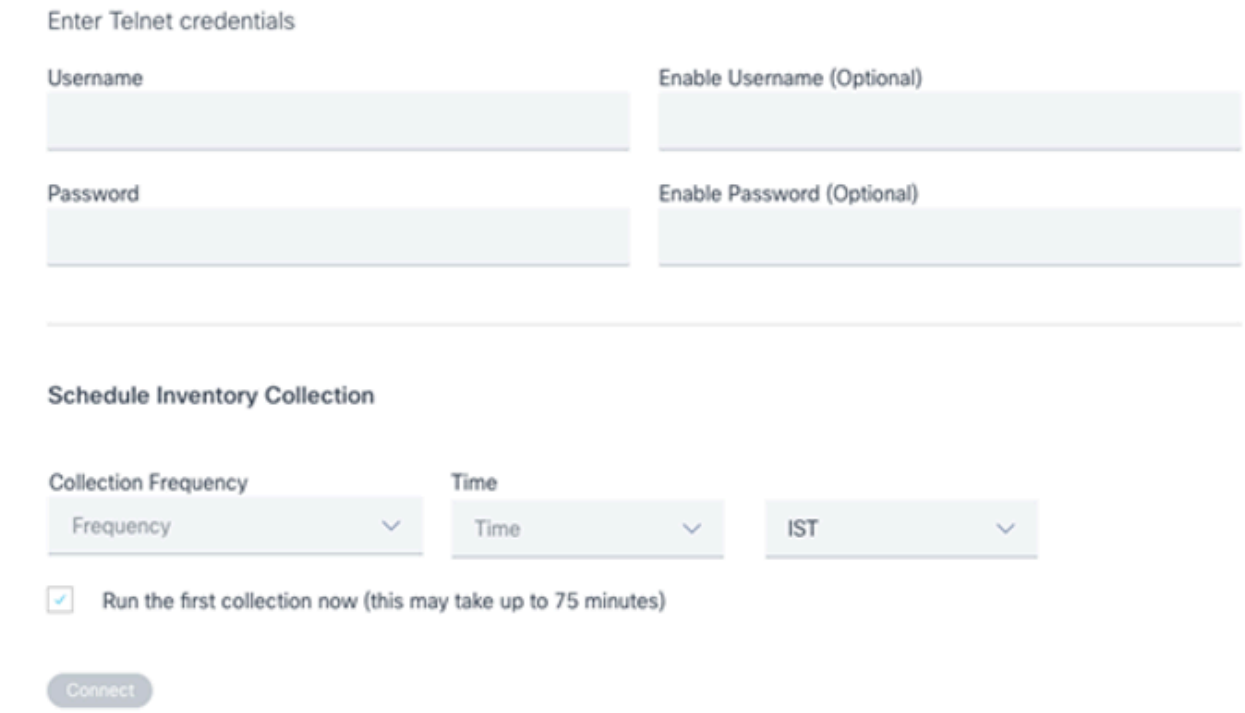
2. フォームに関連情報を入力します。
3. 複数の接続オプションを選択できます。これらの画面には、オプションの設定クレデンシャルが表示されます。各接続オプションのクレデンシャルフィールドの説明については、『シードファイルについて』を参照してください。



SNMP v3クレデンシャル

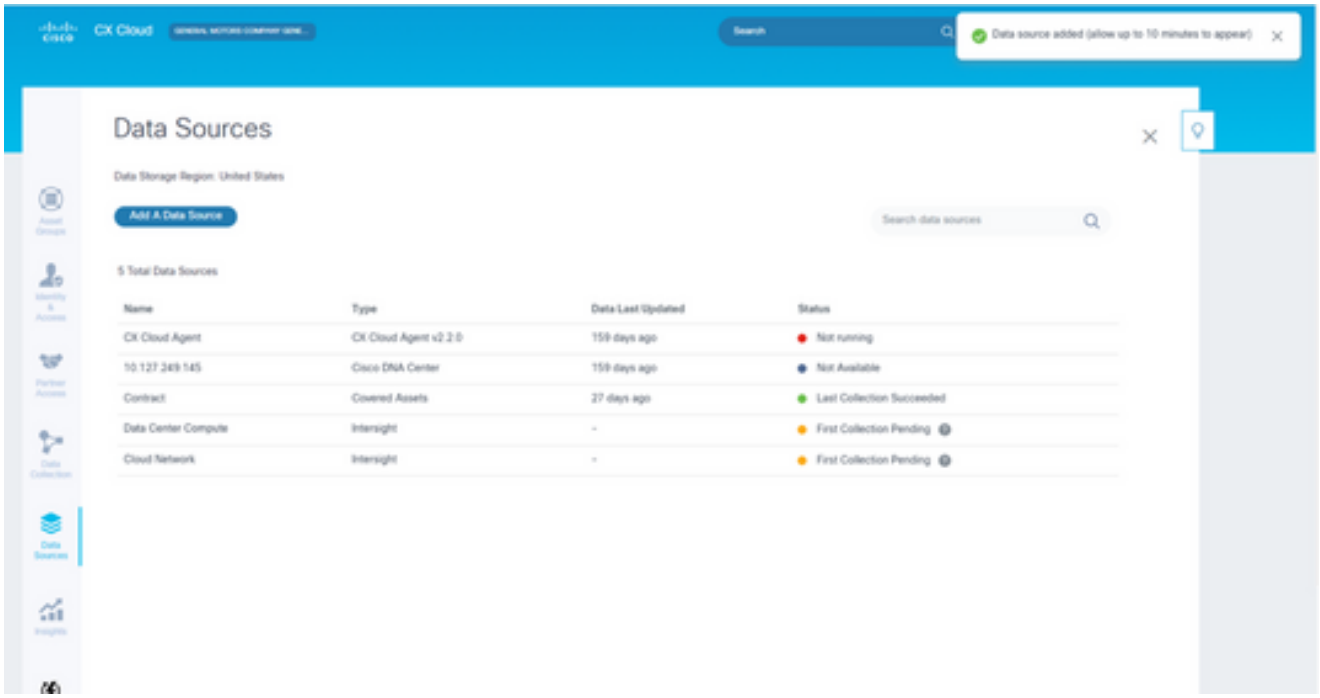


SNMP v2、SSHV2、およびSSHV1クレデンシャル



Telnetクレデンシャ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。

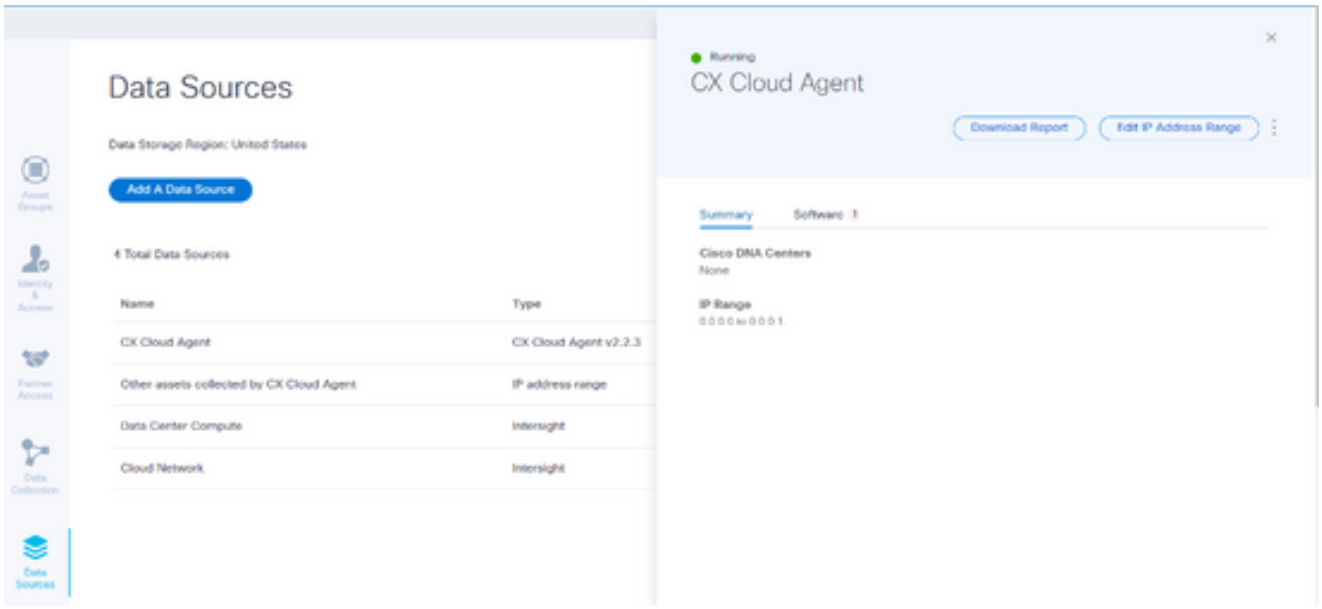


確認

IP範囲の編集

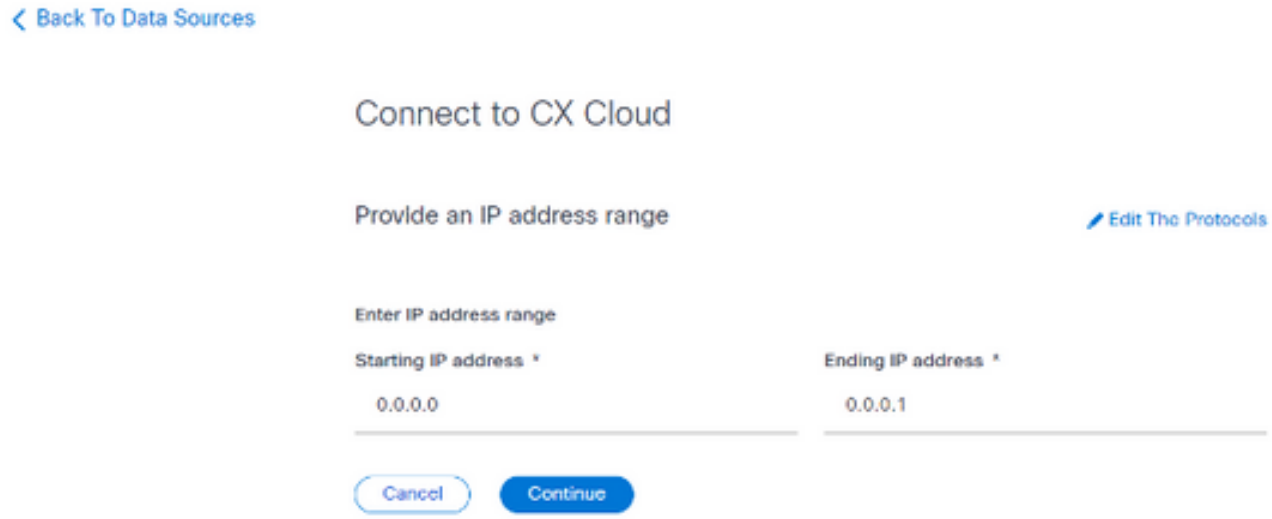
IP範囲を編集するには、

1. Data Sourcesウィンドウに移動します。



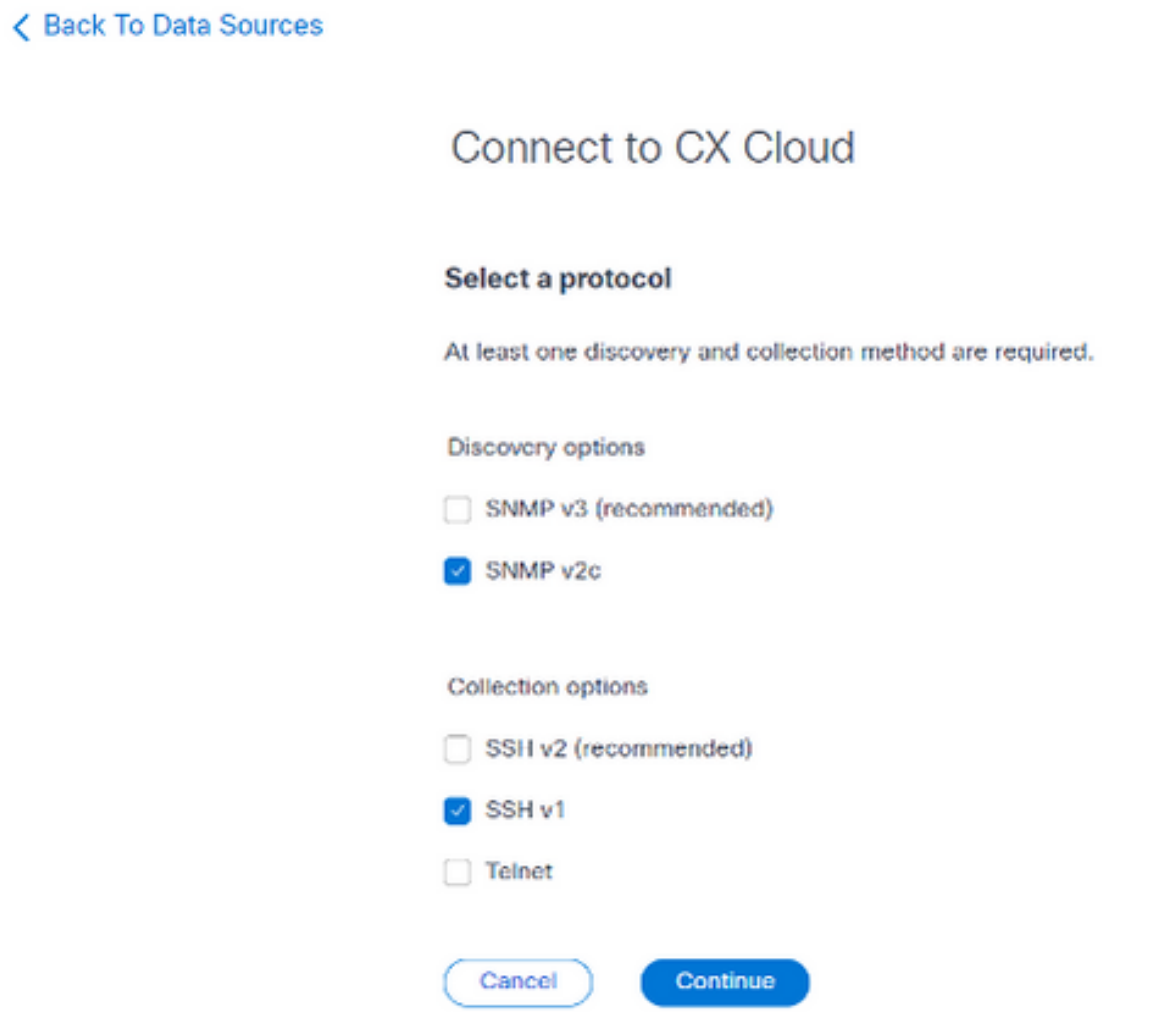
データソース

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。



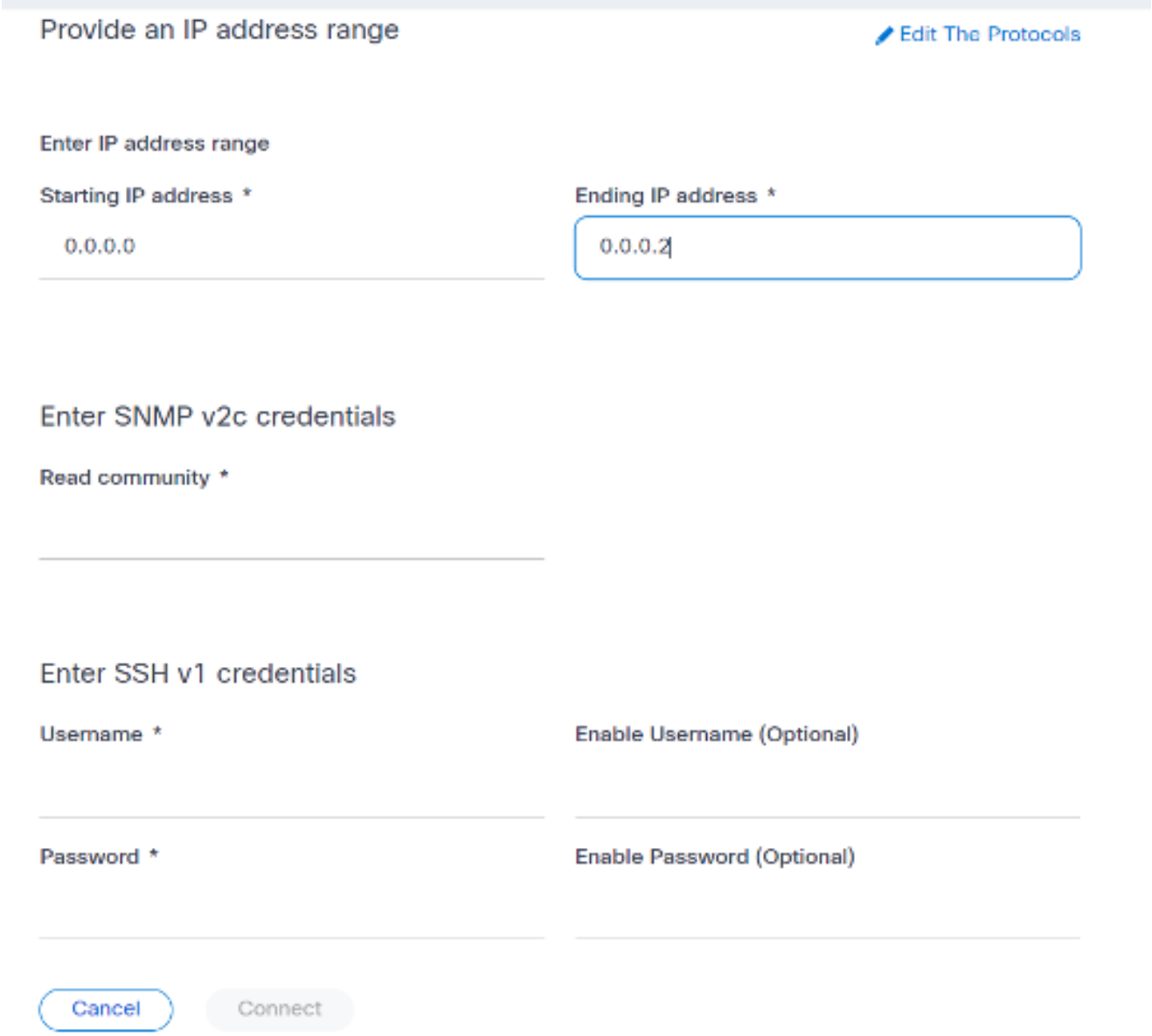
IP範囲の指定

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。



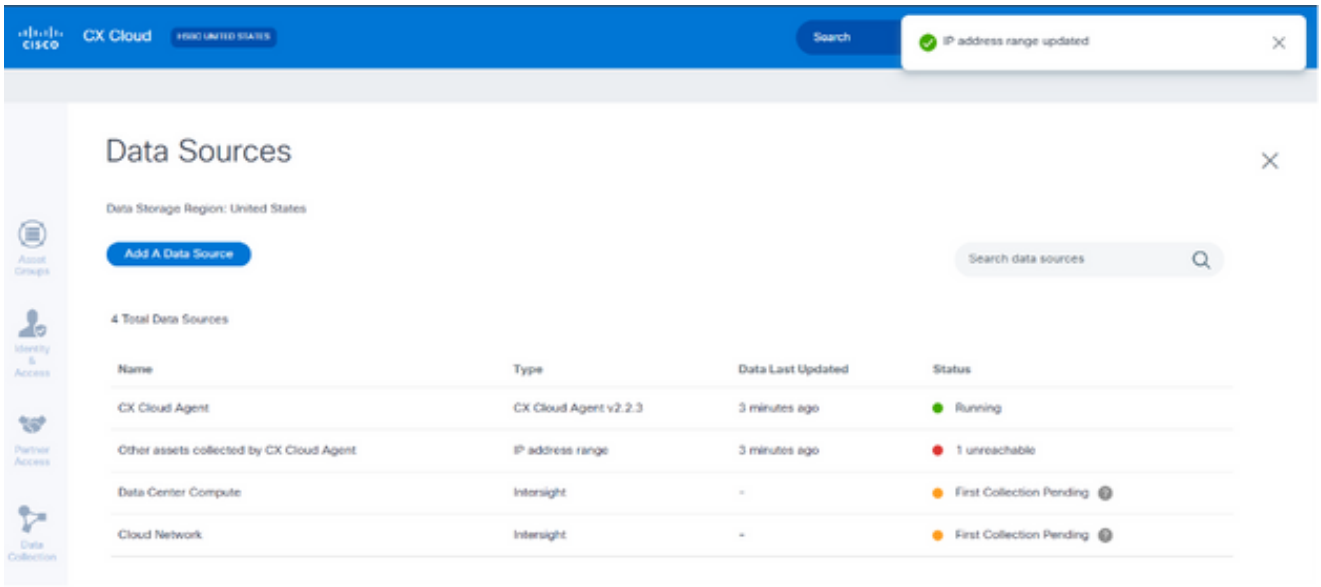
プロトコルの選択

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。



クレデンシャルの入力

8. 設定クレデンシャルを入力します。
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。



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。

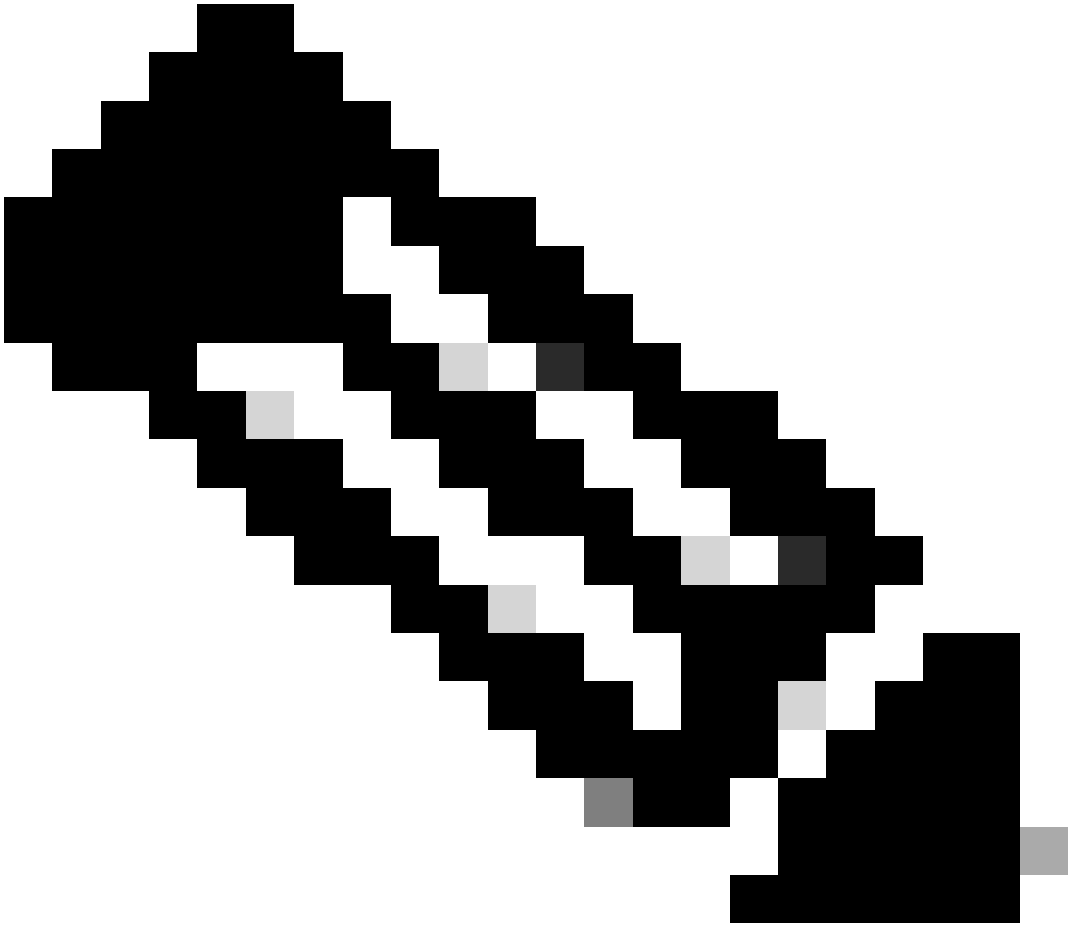
複数のコントローラから検出されたデバイスについて

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。

診断スキャンのスケジュール

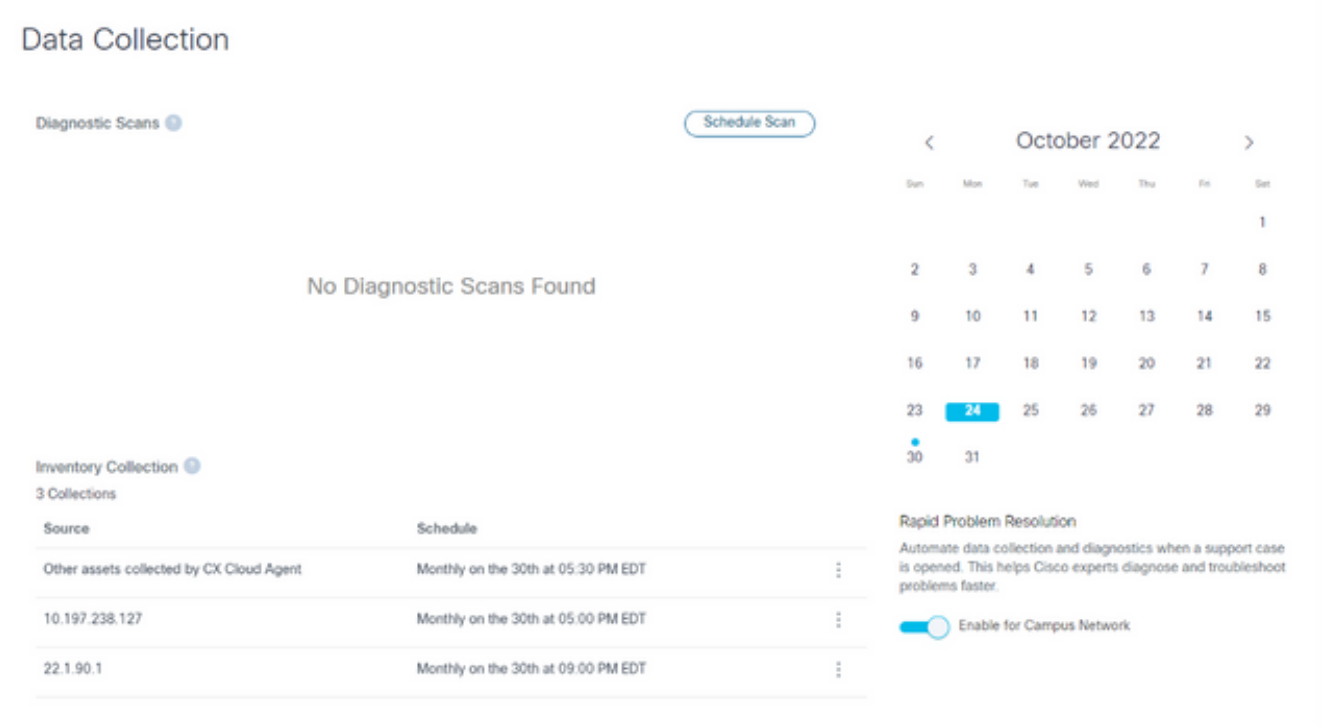
お客様は、CX Cloudでオンデマンドの診断スキャンをスケジュールできます。



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。

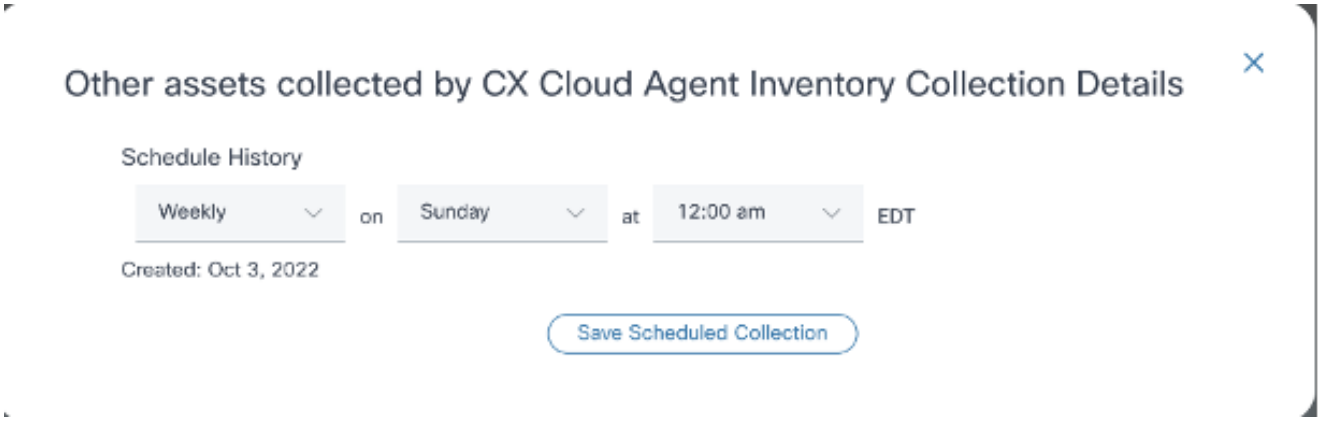
診断スキャンをスケジュールする手順は、次のとおりです。

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。



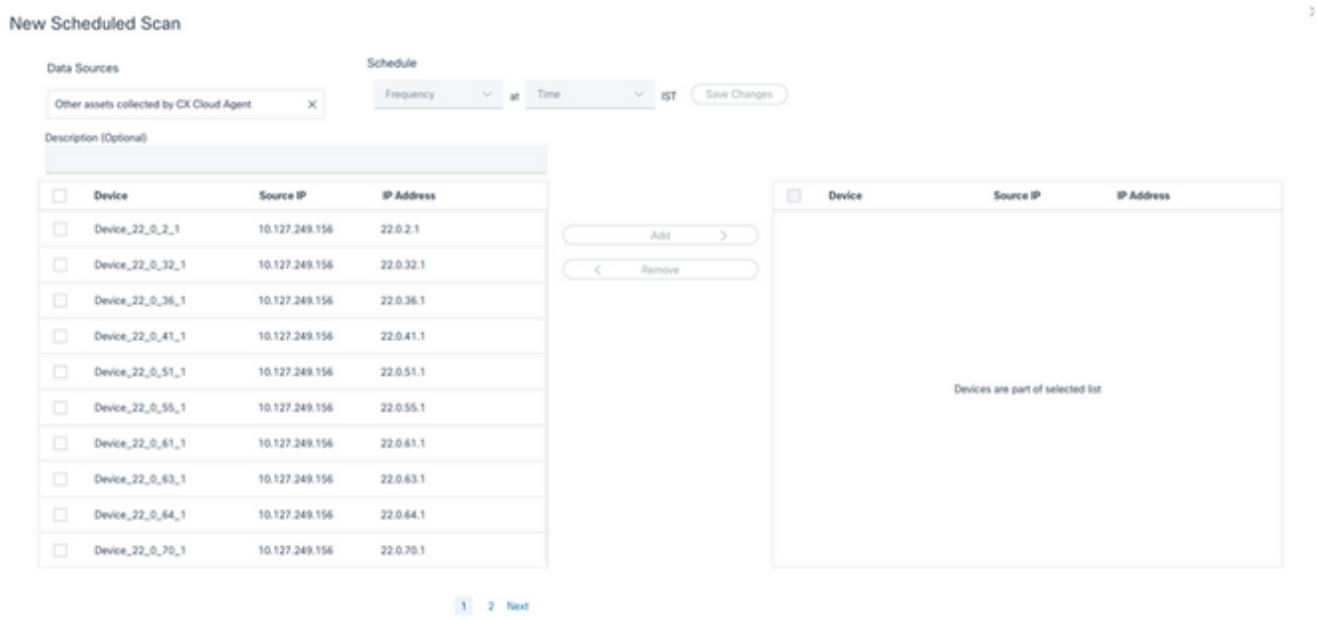
データ収集

4. このスキャンのスケジュールを構成します。



スキャンスケジュールの構成

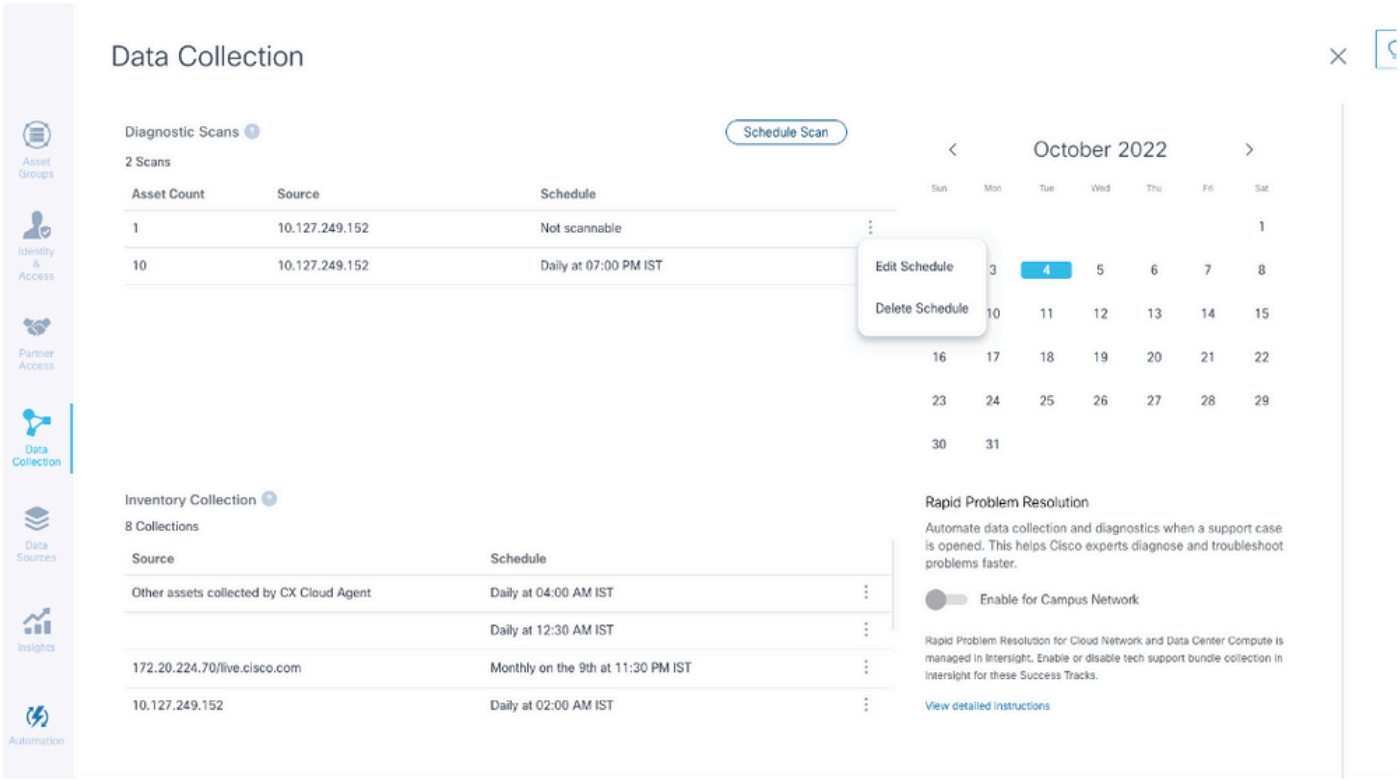
5. デバイスリストで、スキャンするすべてのデバイスを選択し、Addをクリックします。



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

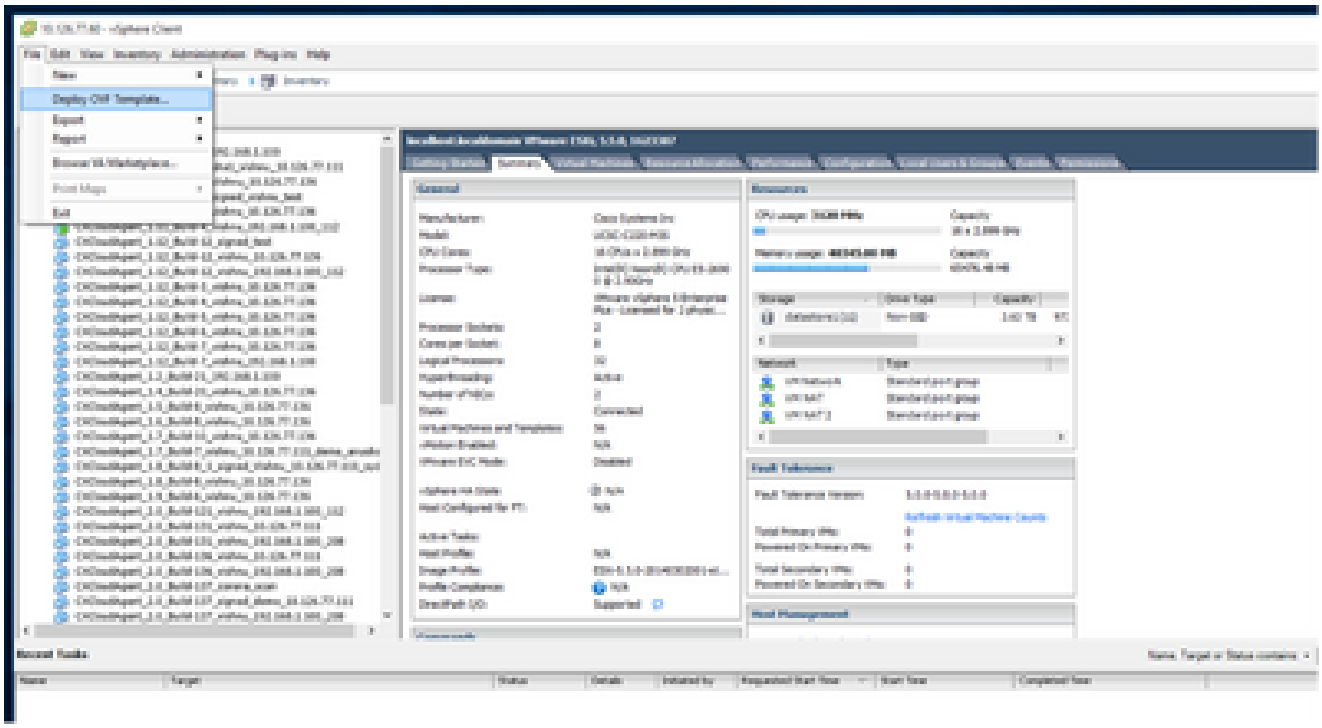
シッククライアント ESXi 5.5/6.0 のインストール

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。

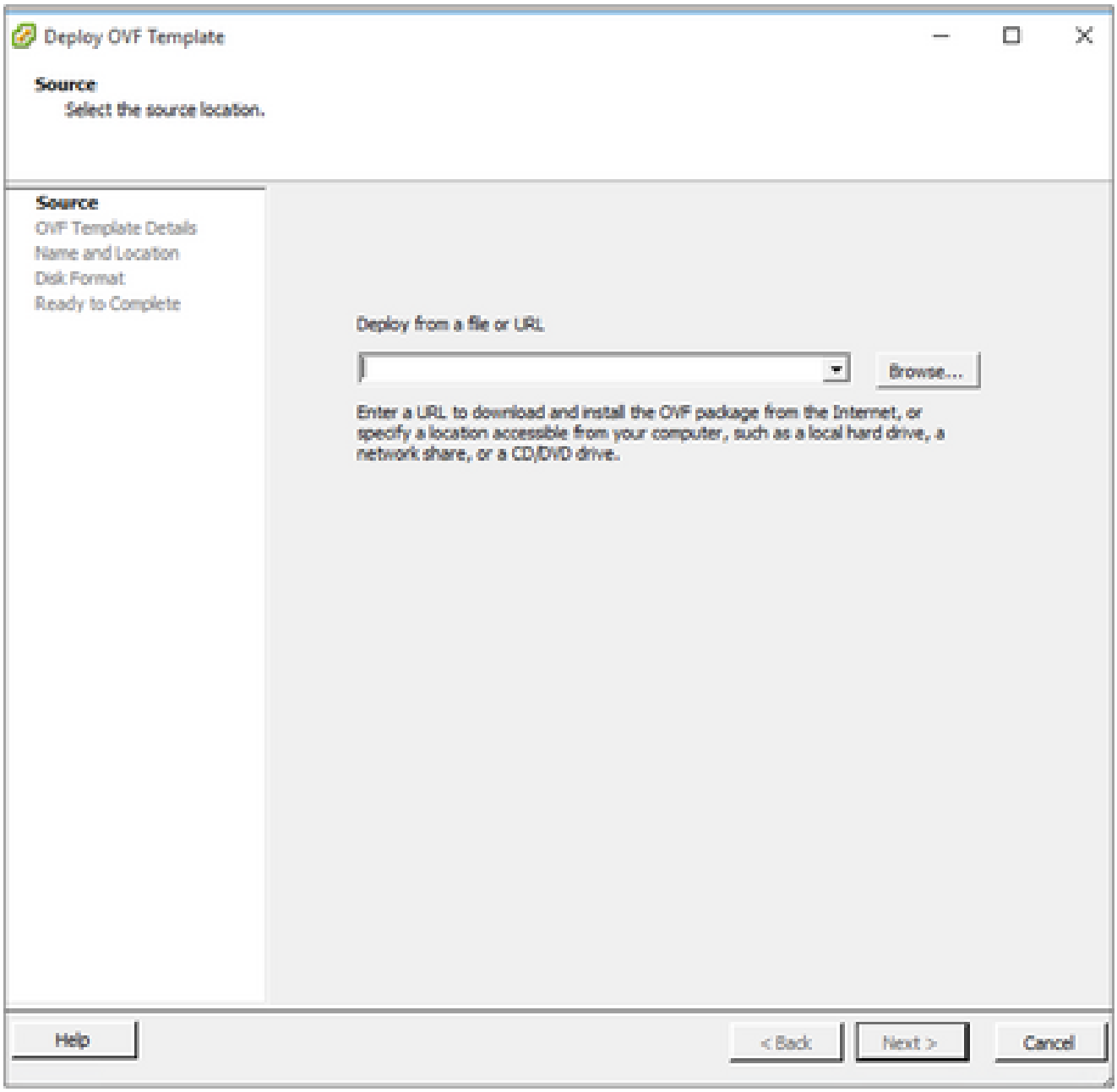
ログイン

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



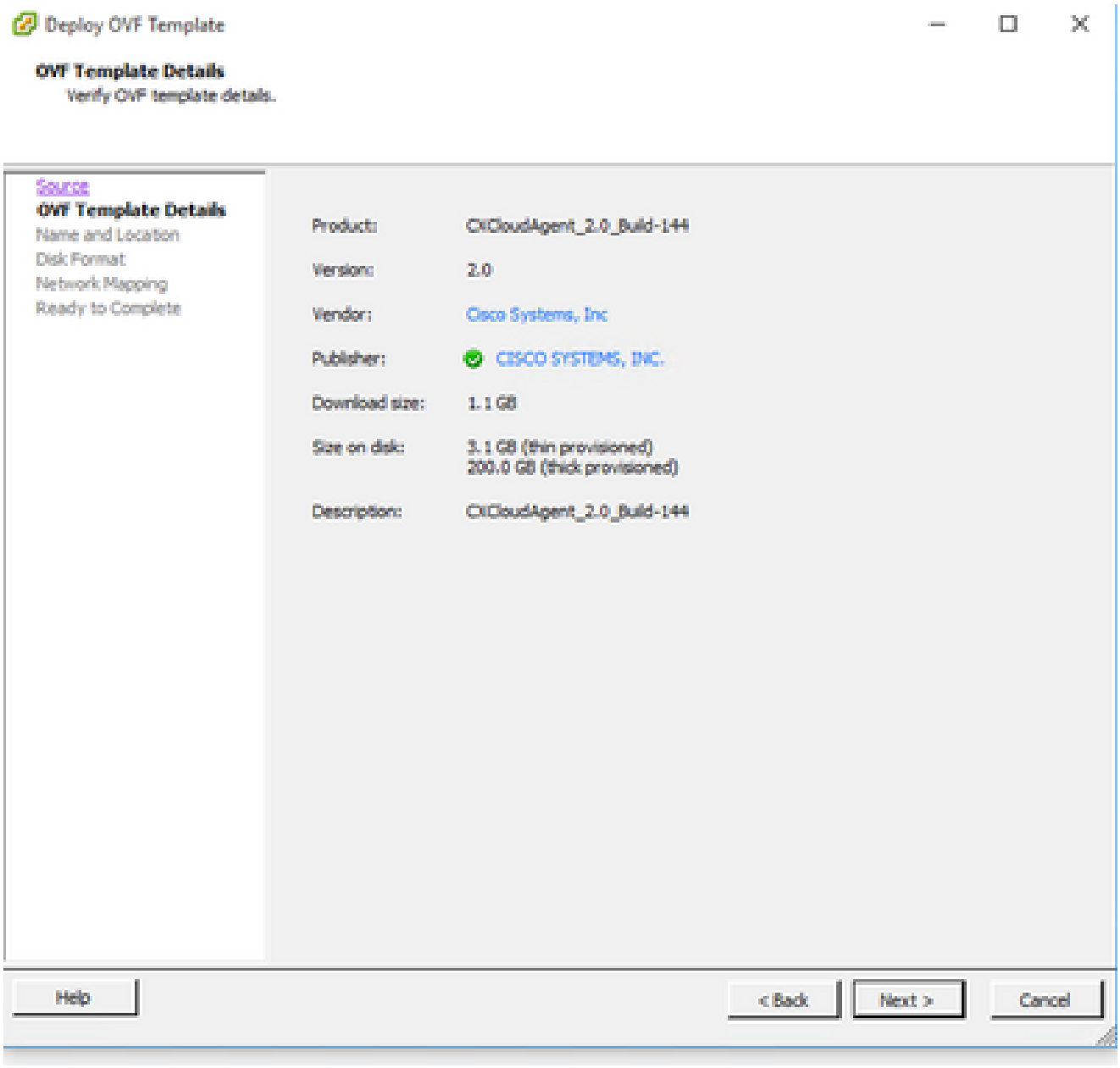
vSphere クライアント

3. OVAファイルを参照して選択し、Nextをクリックします。



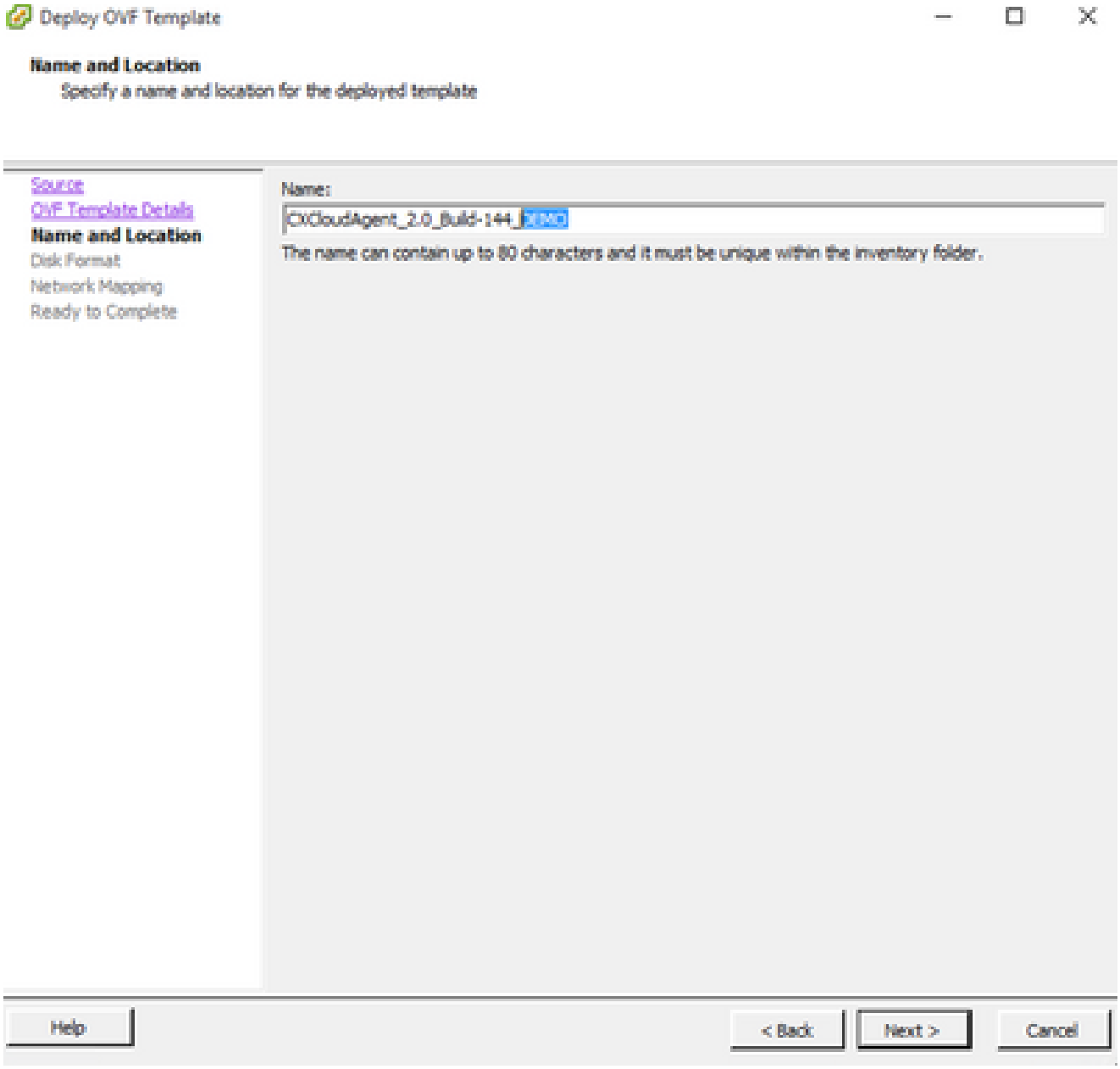
OVA パス

4. OVF Detailsを確認し、Nextをクリックします。



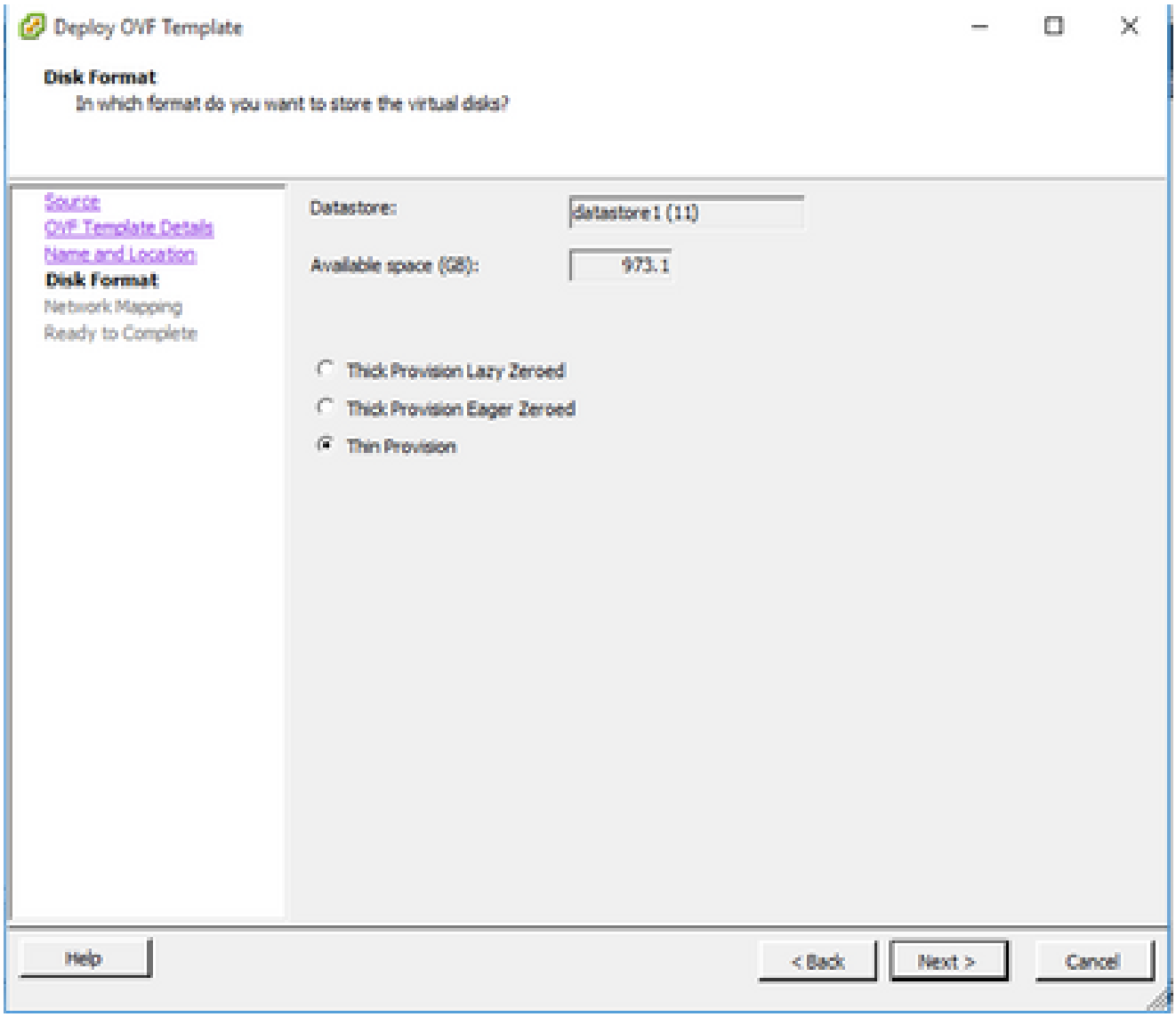
テンプレートの詳細

5. 一意の名前を入力して、Nextをクリックします。



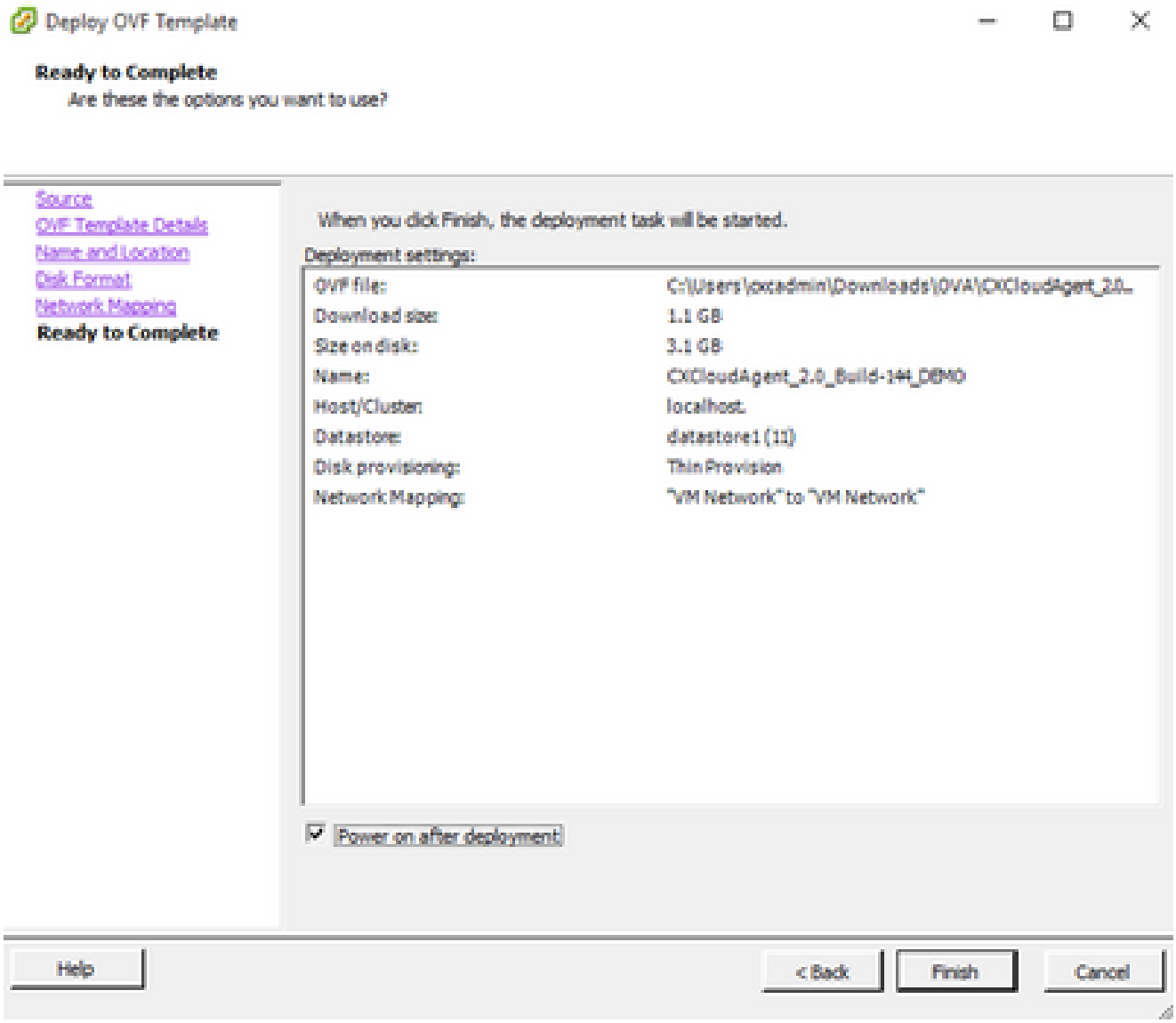
名前と場所

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



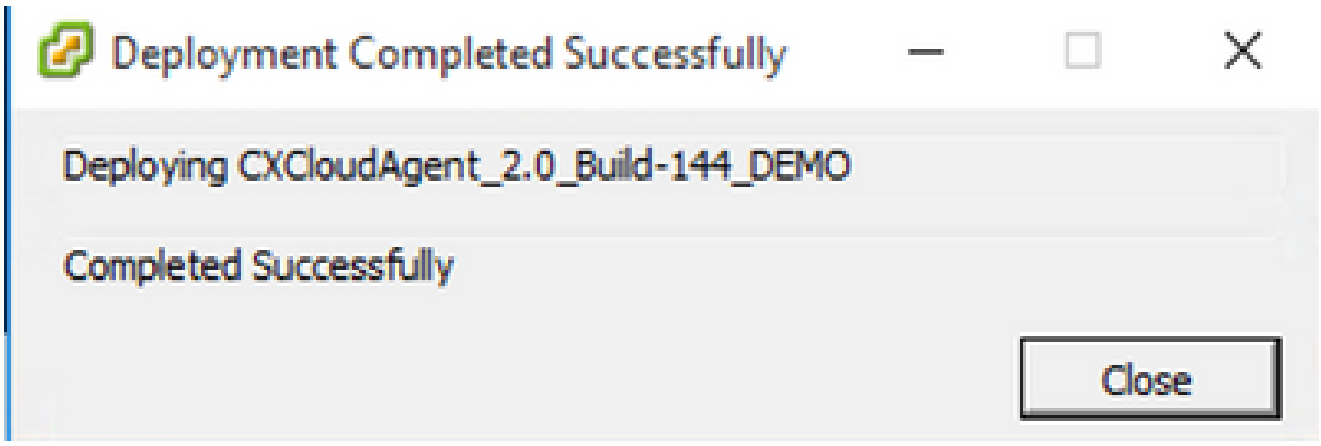
ディスクの書式設定

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。展開が成功すると、確認の表示が行われます。



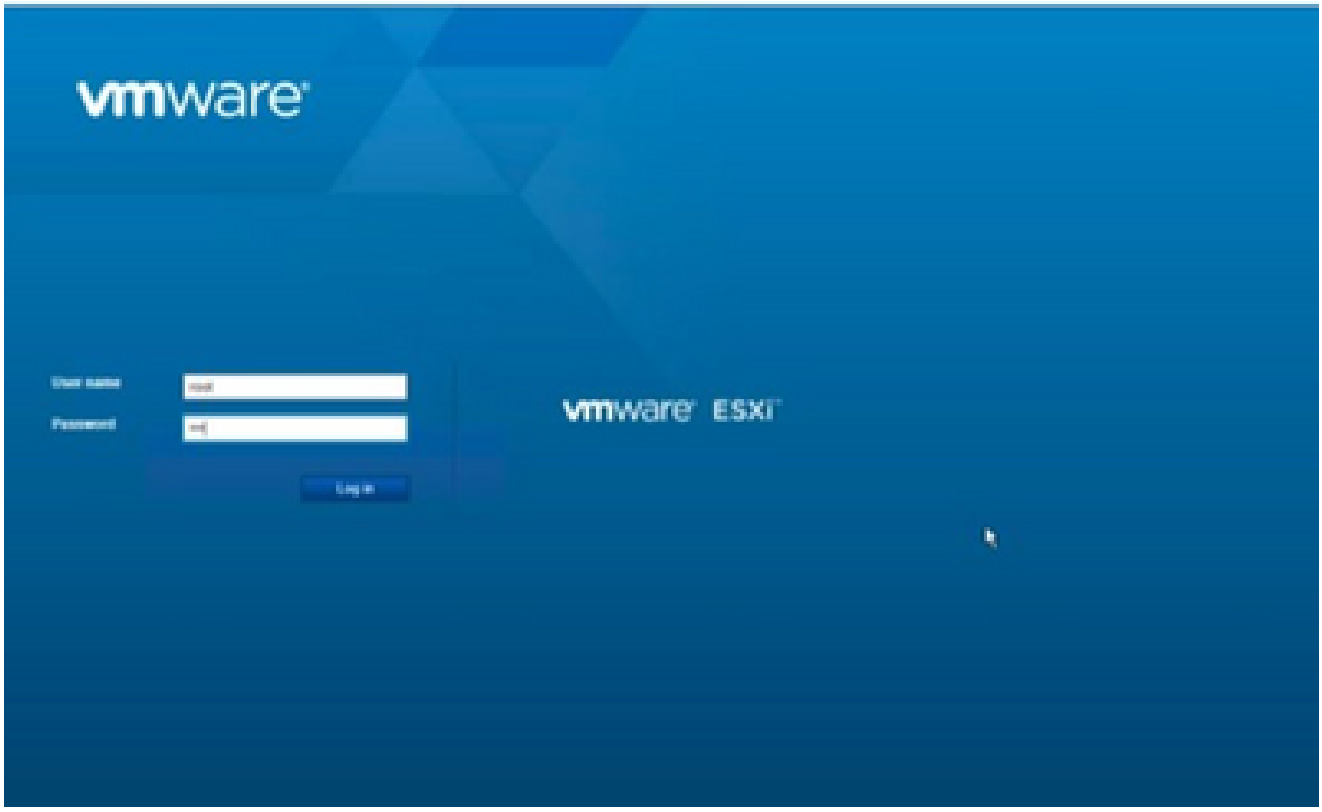
導入の完了

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

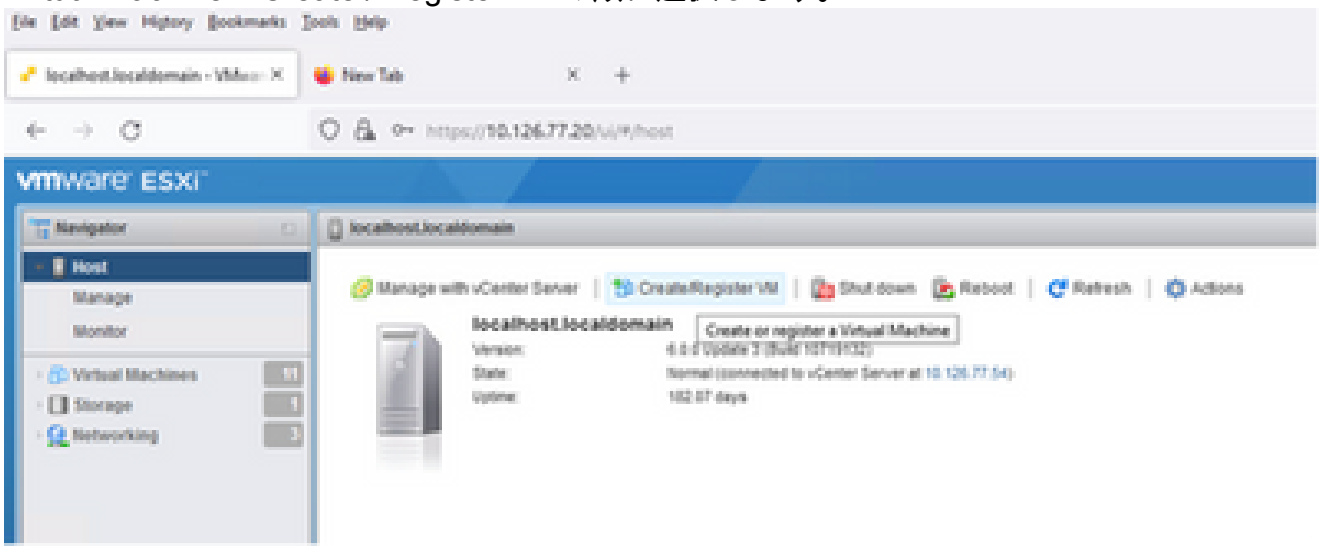
このクライアントは、vSphere Webを使用してCX Cloud Agent OVAを導入します。

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。



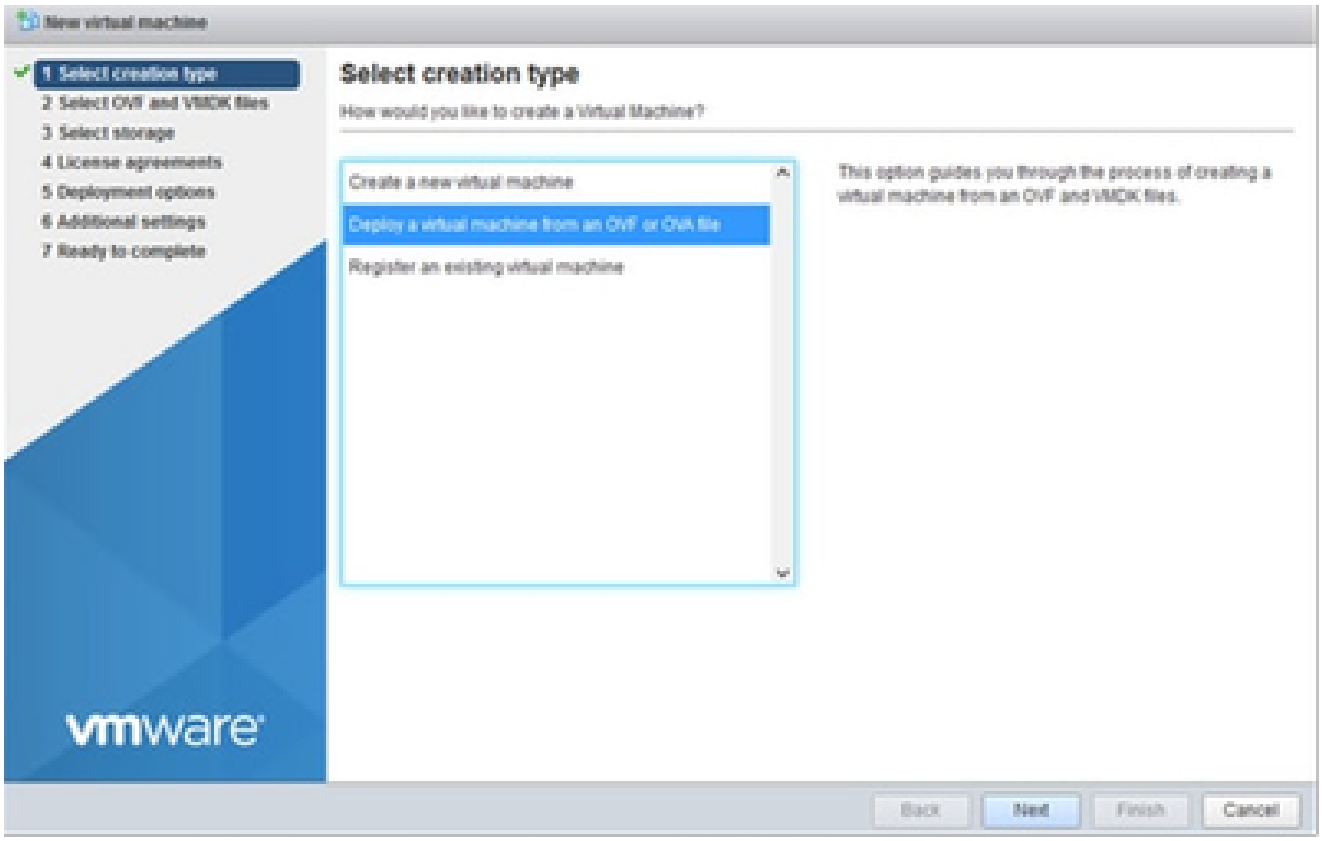
VMware ESXi のログイン

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



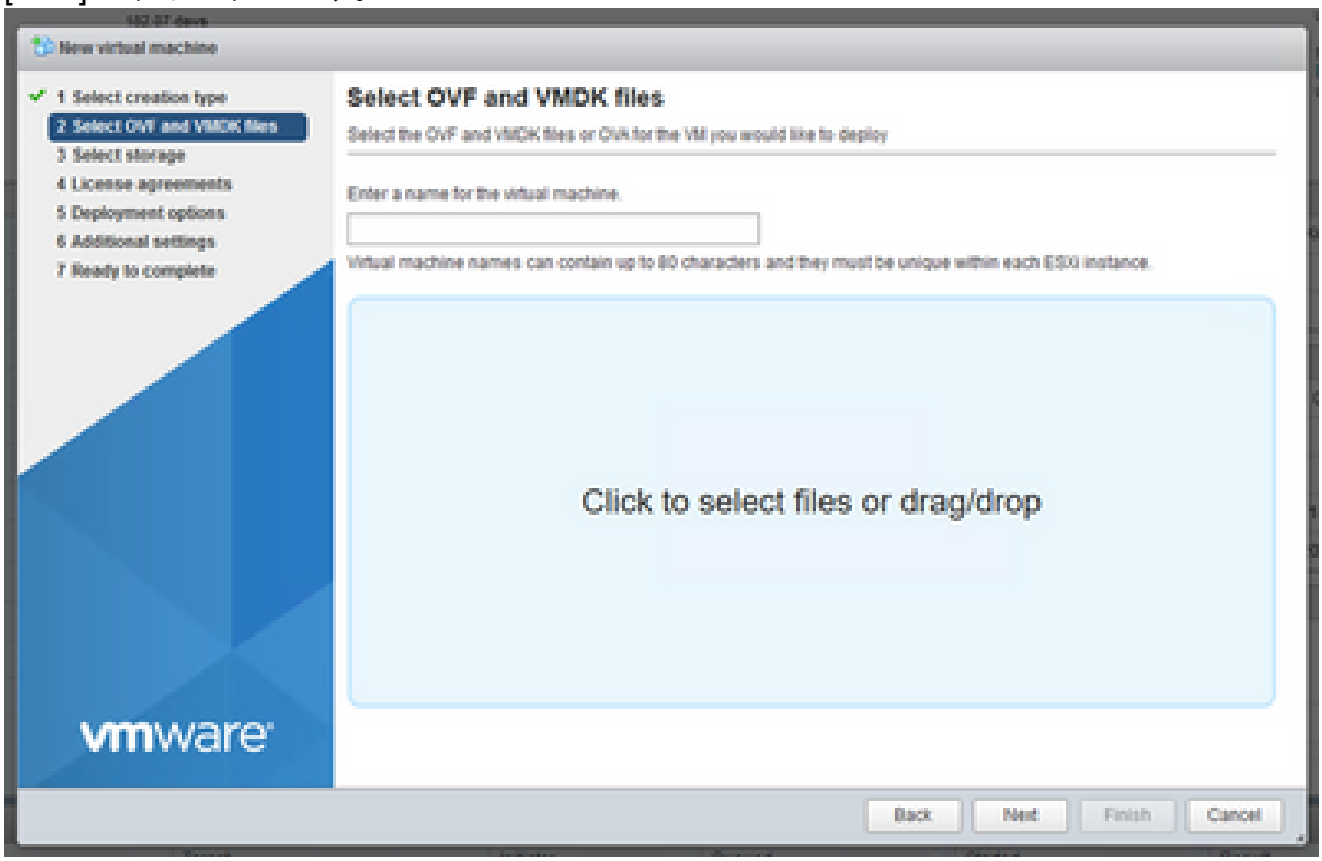
VM の作成

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。



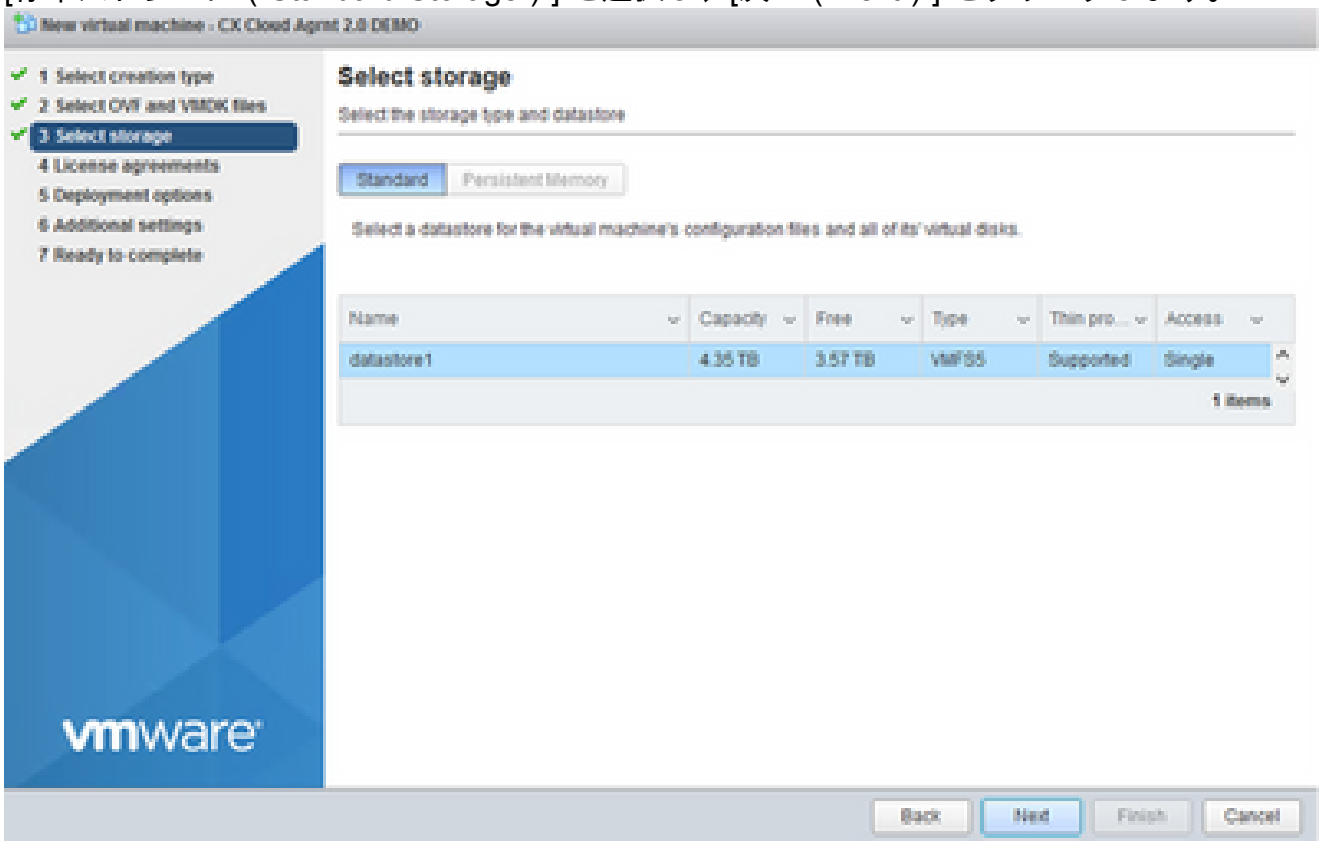
作成タイプの選択

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。



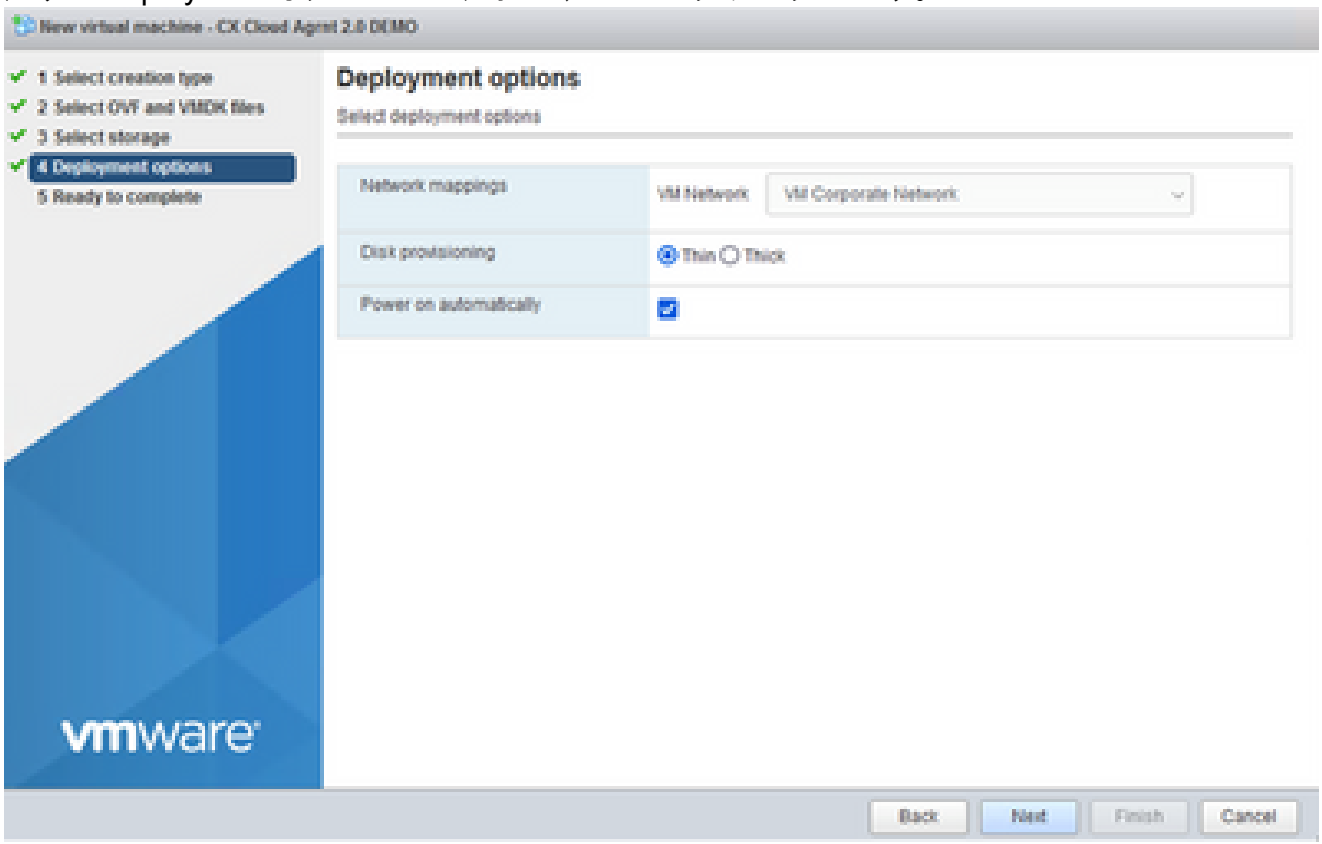
OVA の選択

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。



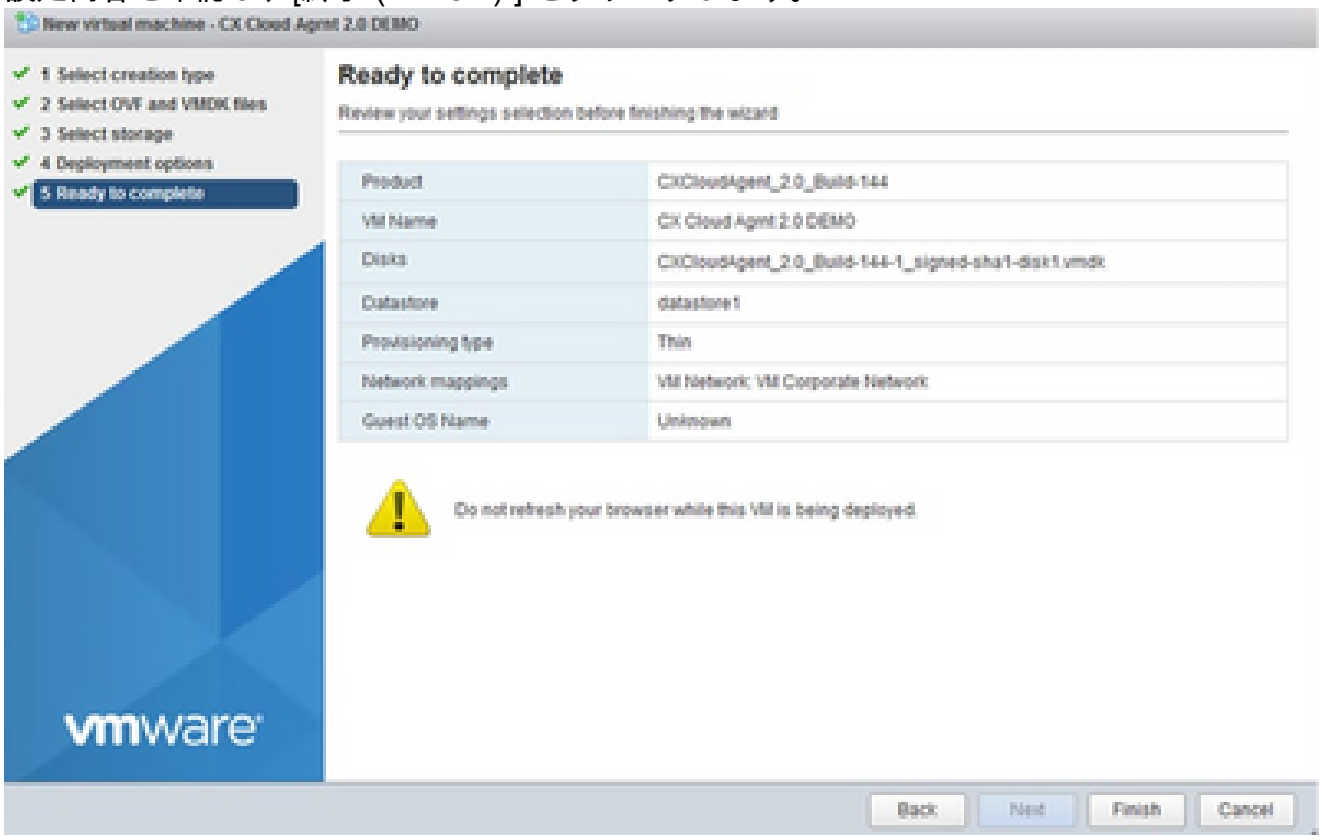
ストレージの選択

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

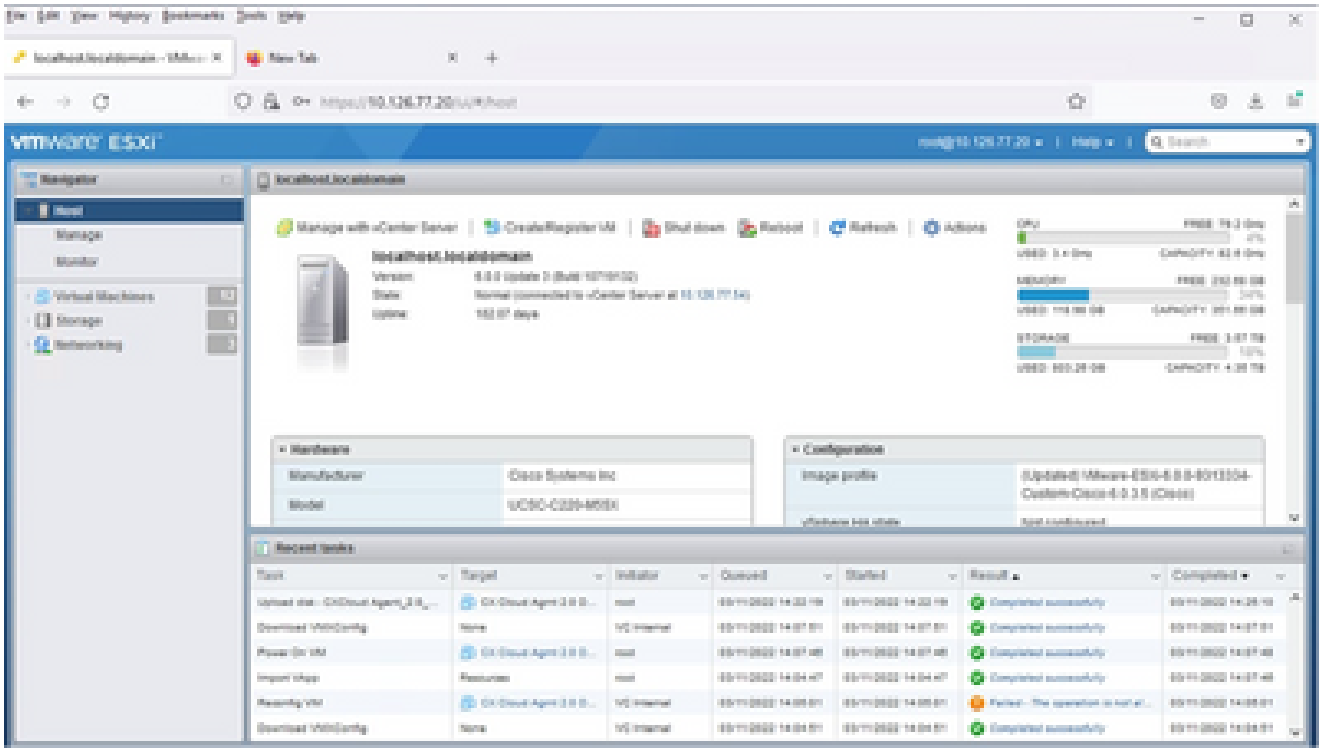


導入オプション

8. 設定内容を確認し、[終了（Finish）] をクリックします。

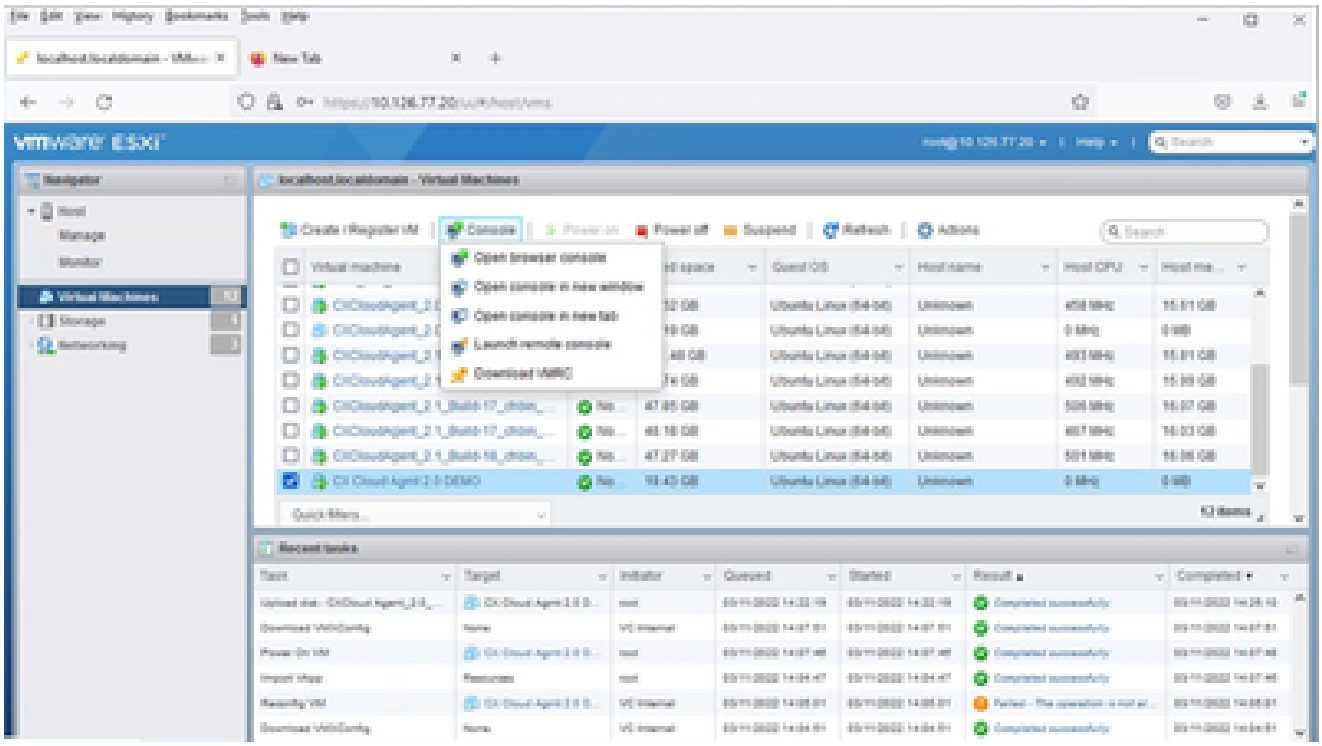


終了準備の完了（Ready to Complete）



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。

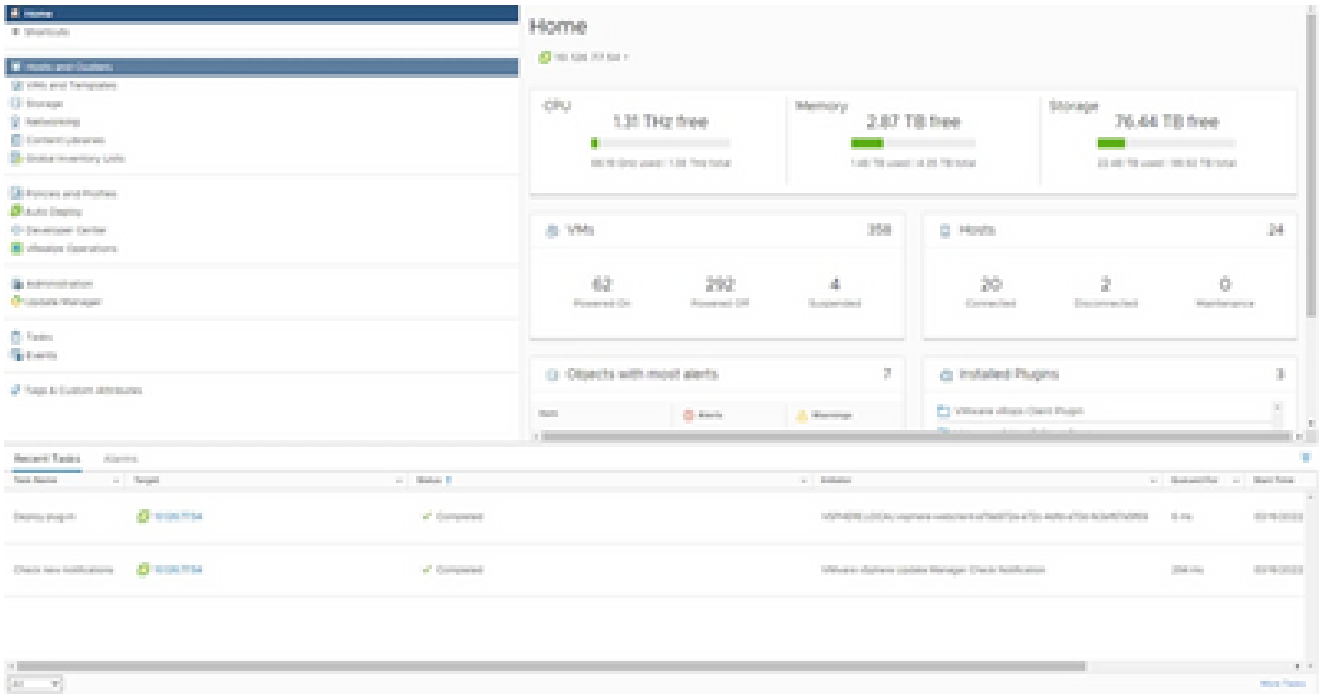
Web クライアント vCenter のインストール

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。

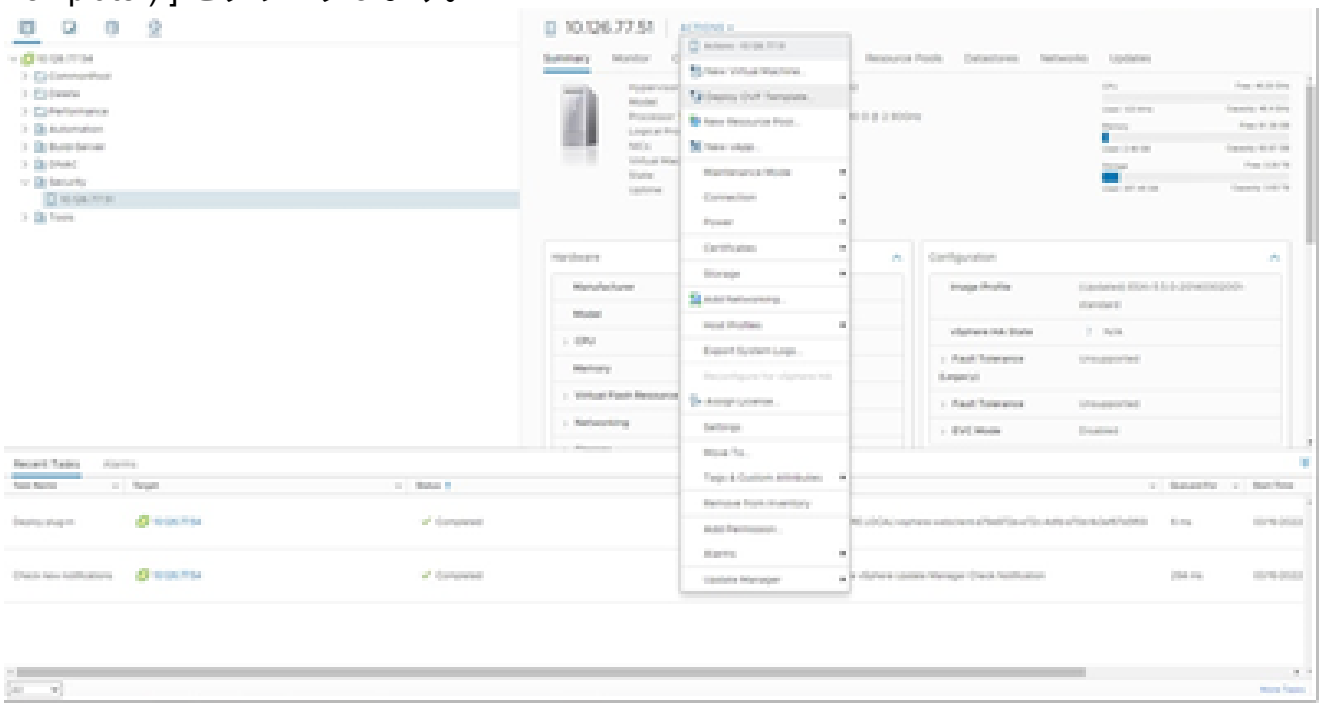
ログイン

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

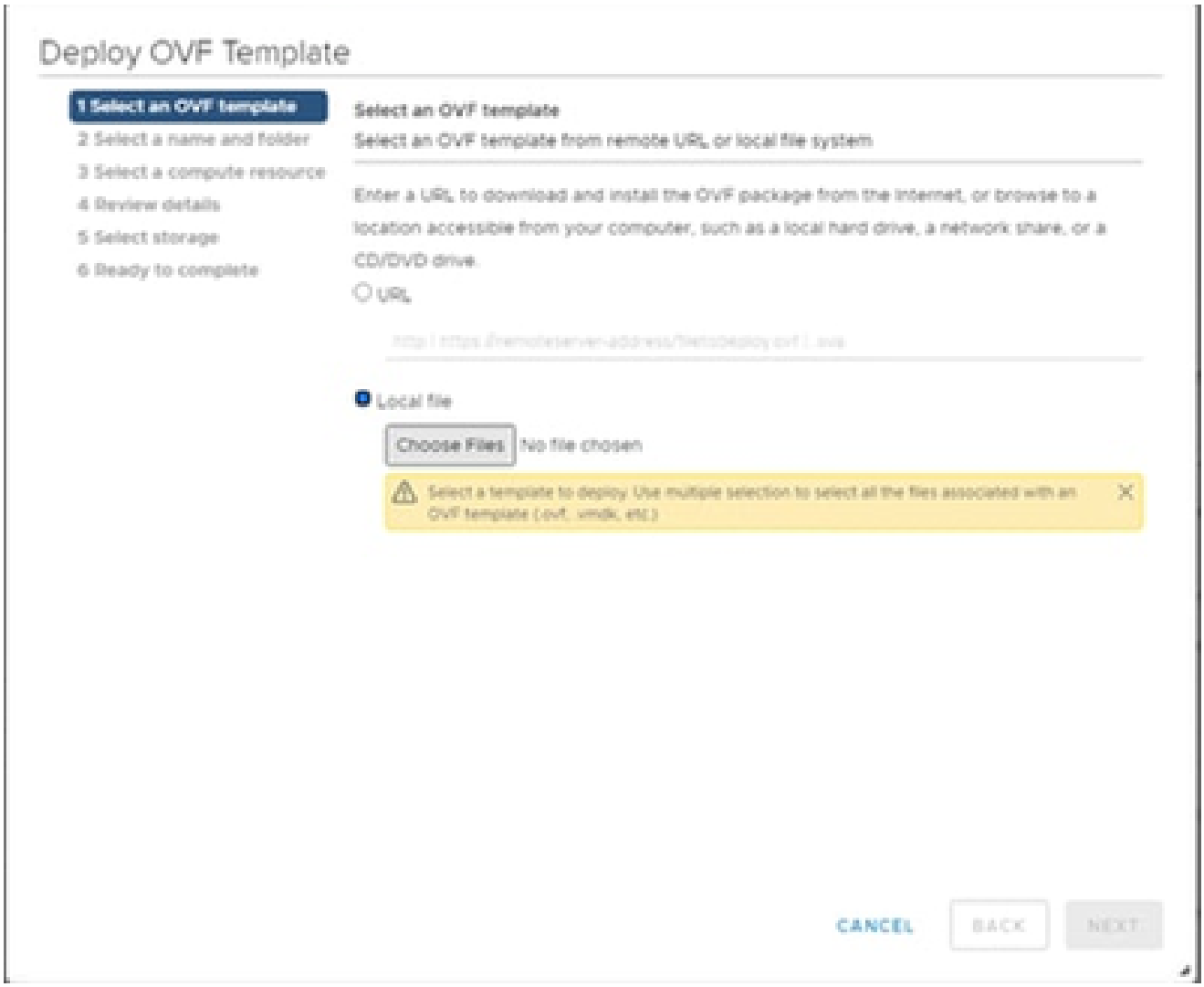


ホームページ

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。

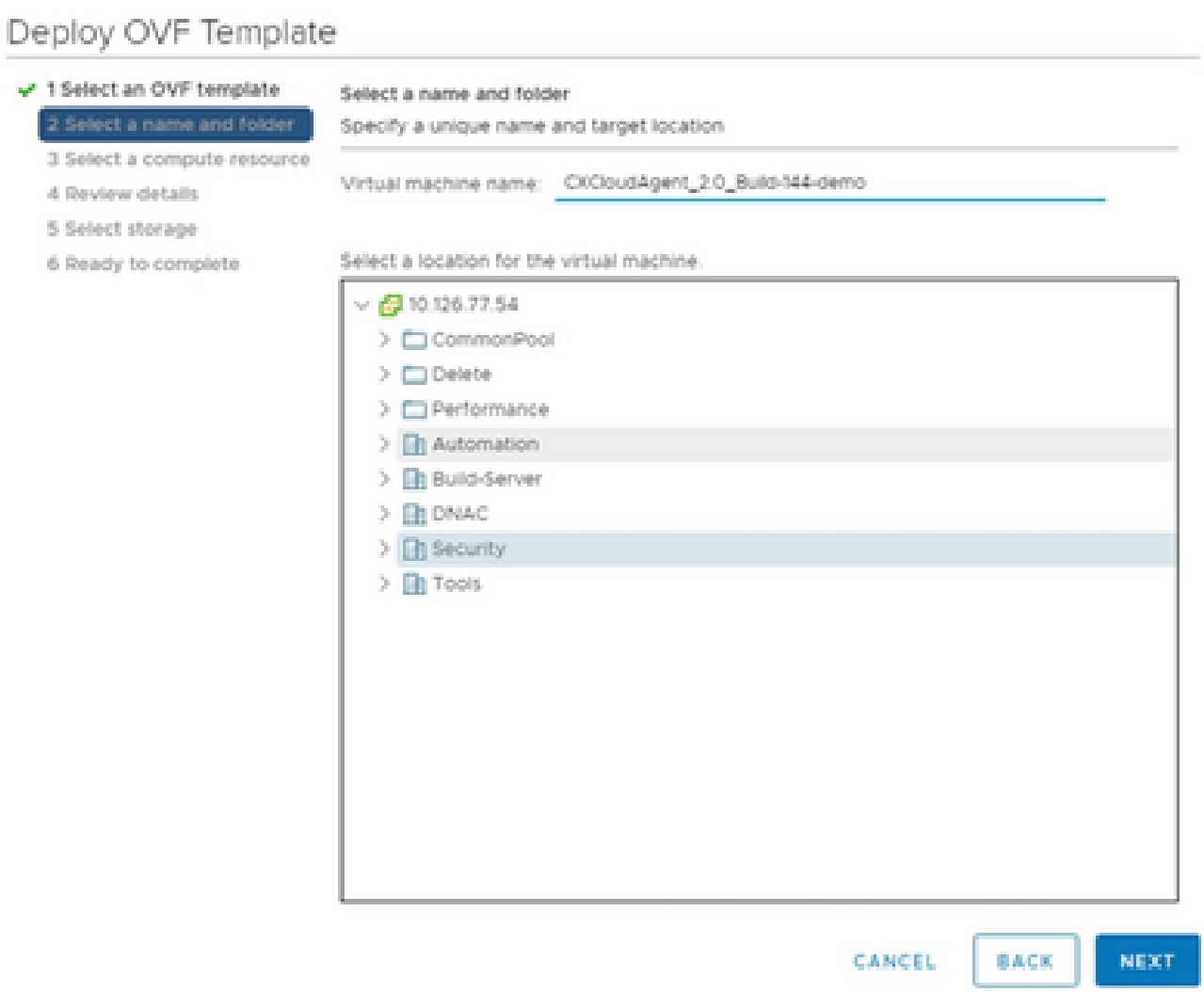


[アクション（ Actions ）]



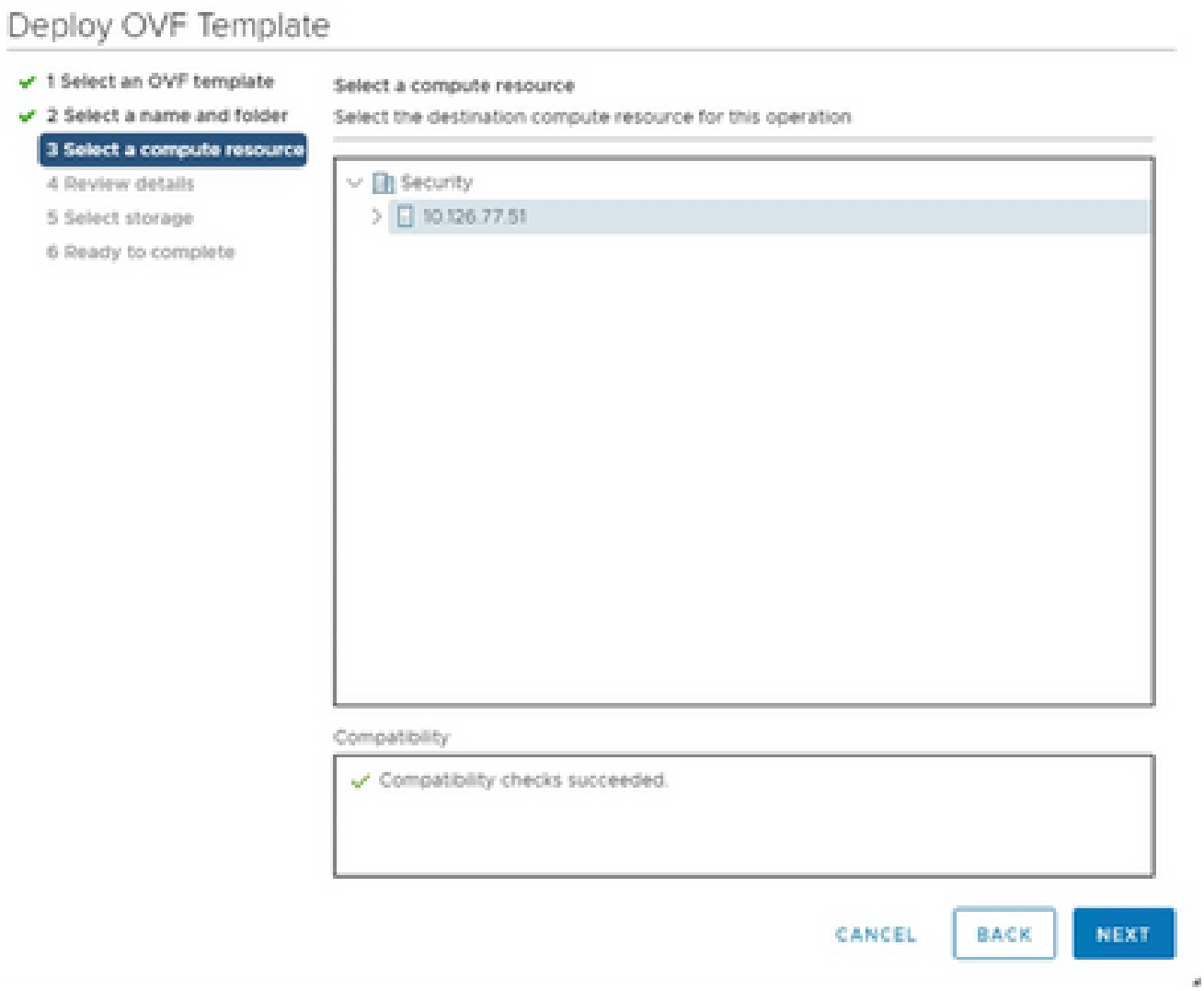
テンプレートの選択(Select Template)

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。



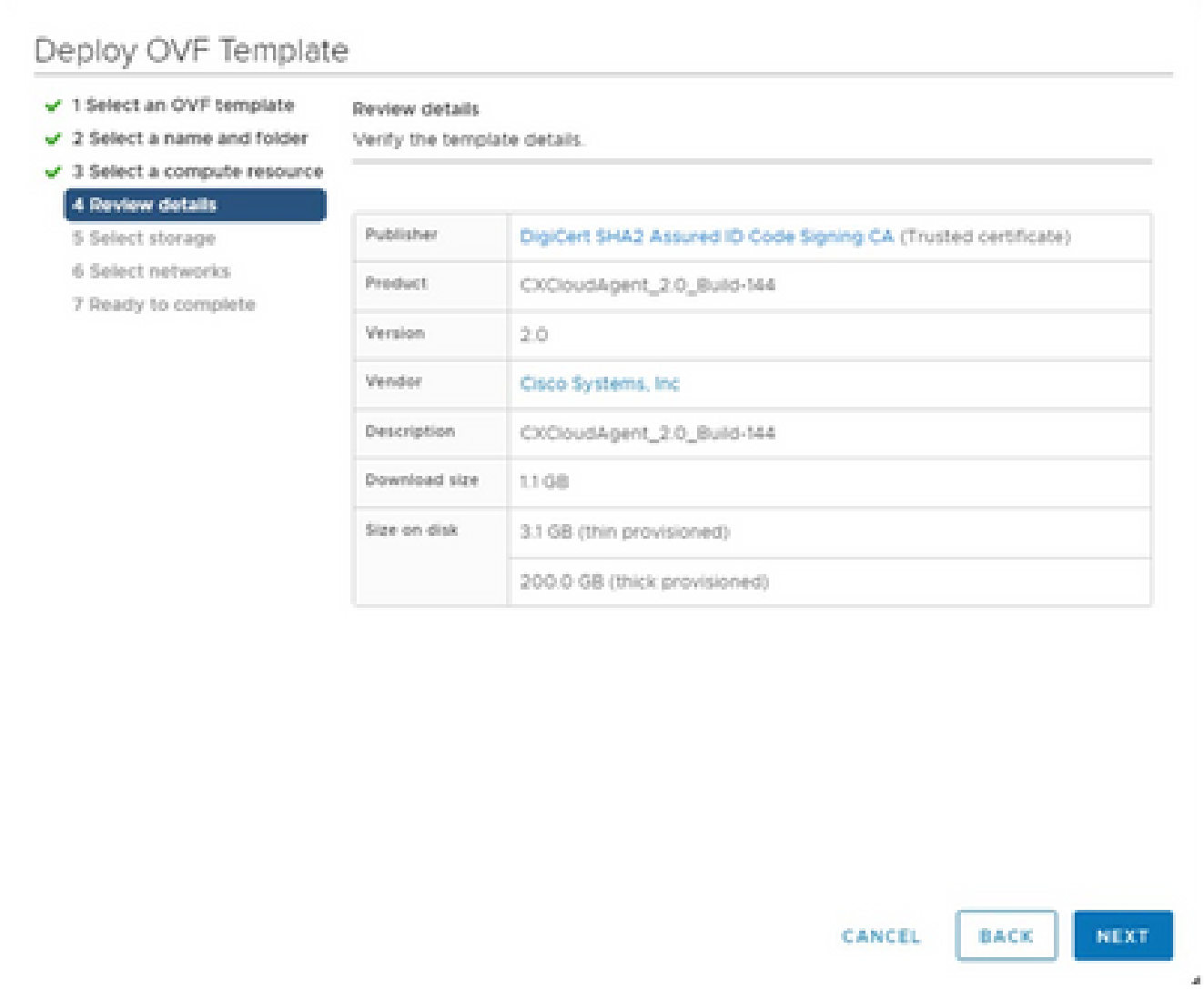
名前とフォルダ

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。



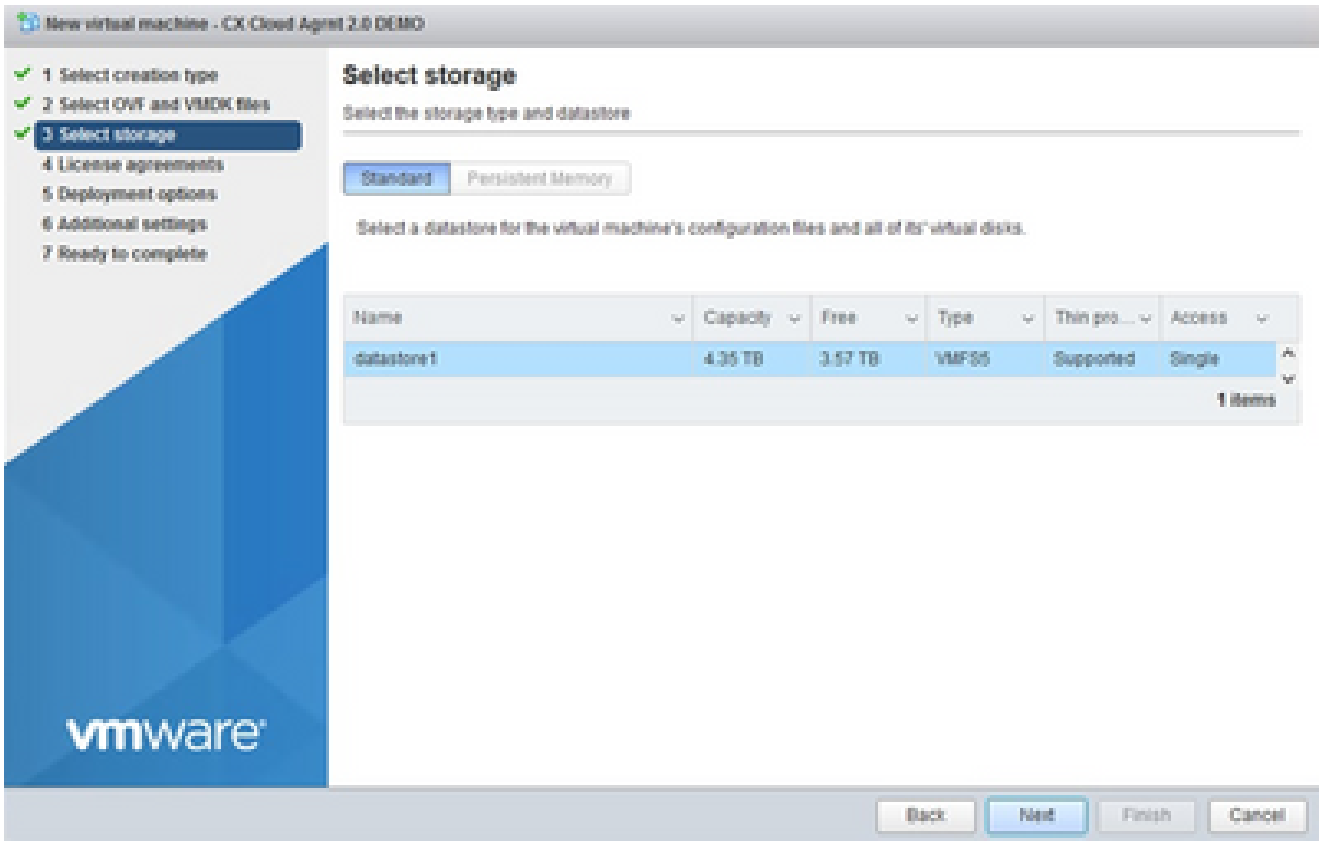
コンピュータリソースの選択

8. 詳細を確認し、[次へ（Next）] をクリックします。



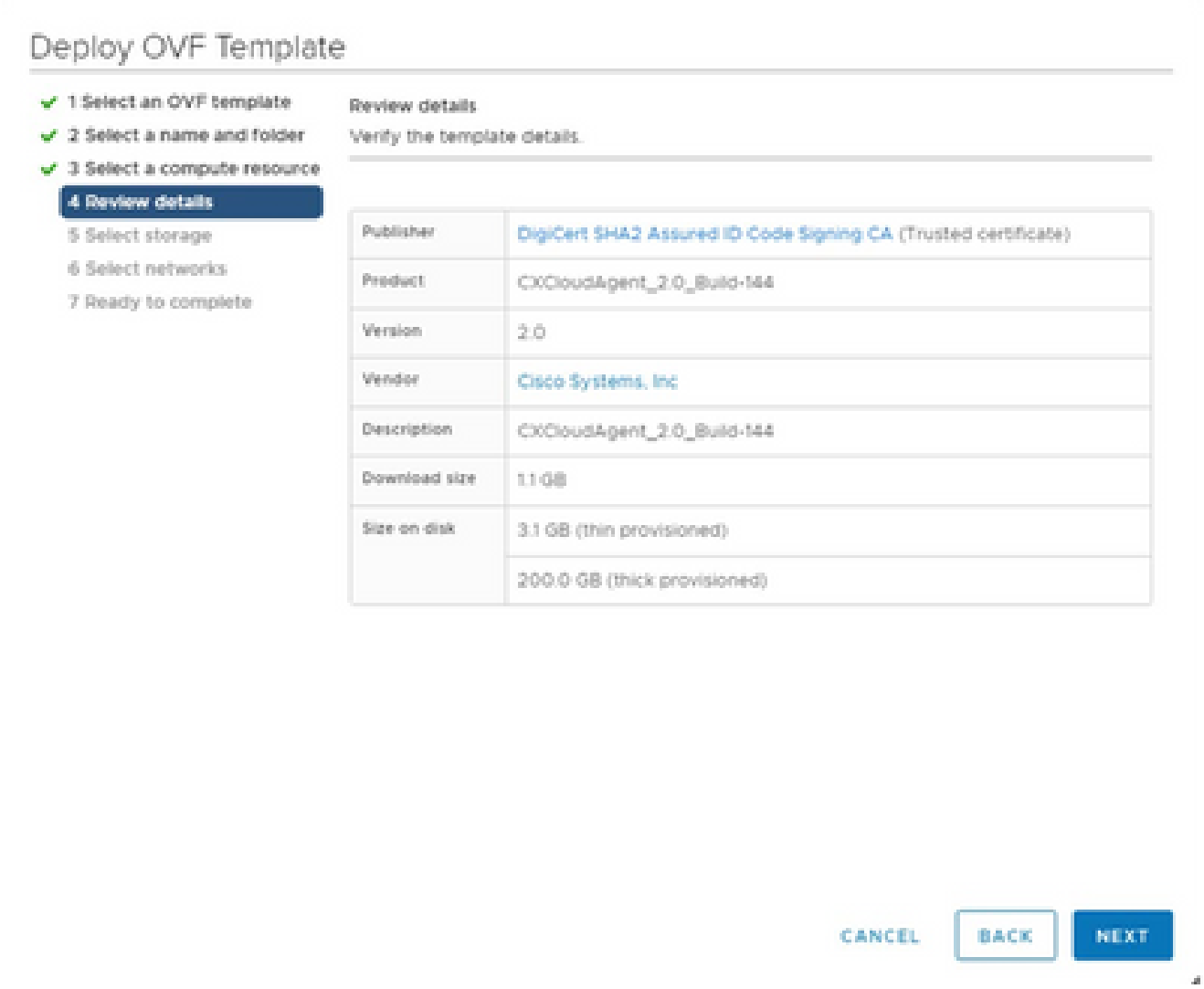
詳細の確認

9. 仮想ディスク形式を選択し、[次へ（Next）] をクリックします。



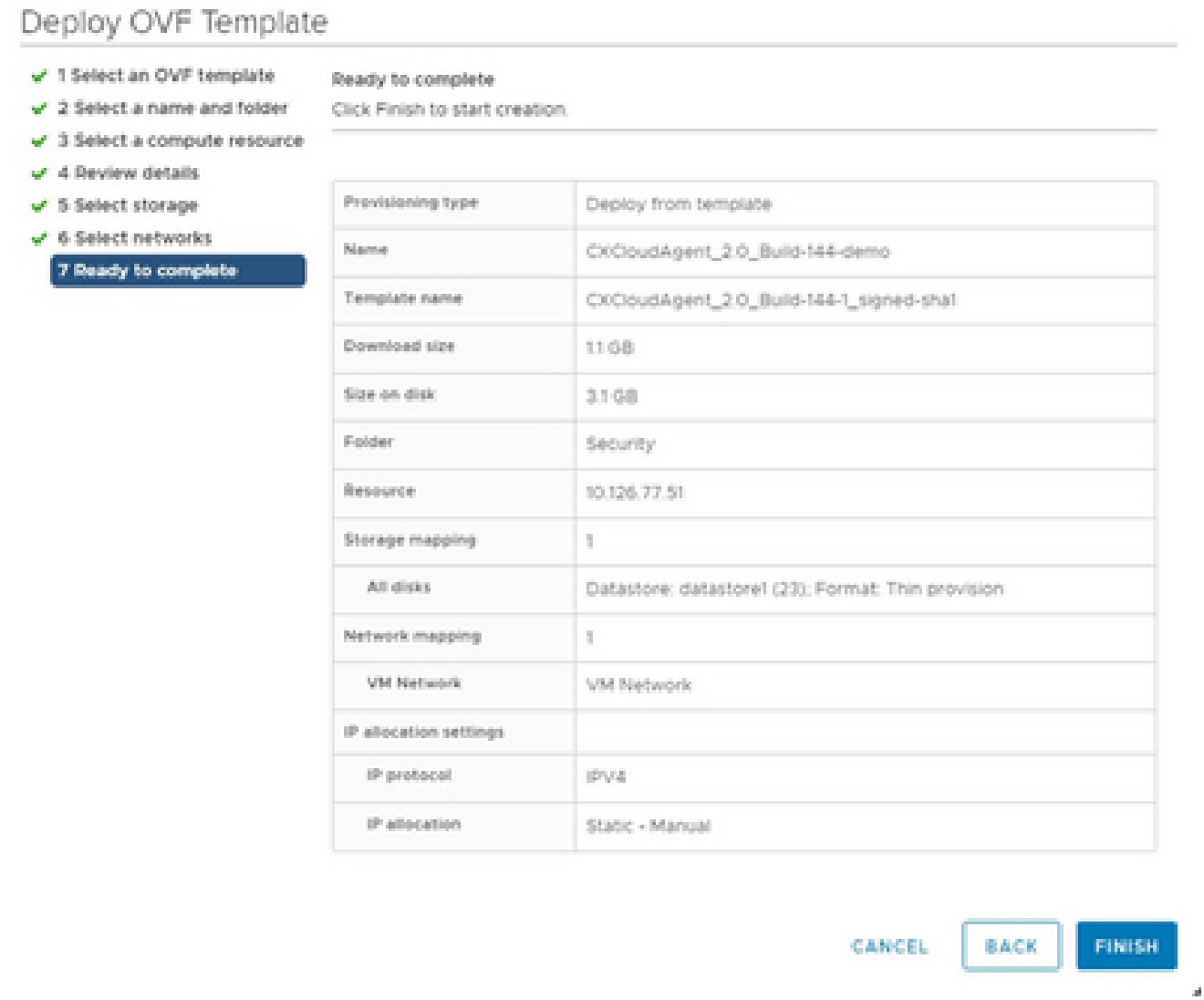
ストレージの選択

10. [Next] をクリックします。



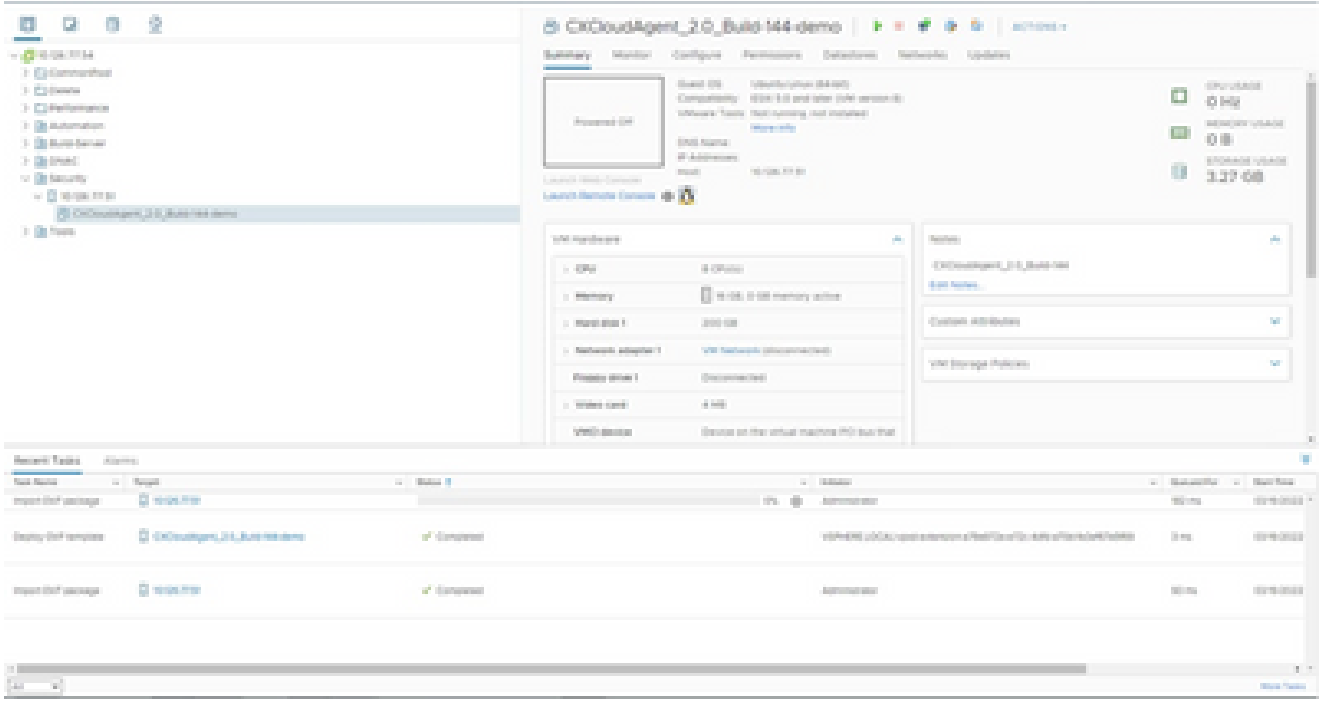
ネットワークの選択

11. [Finish] をクリックします。



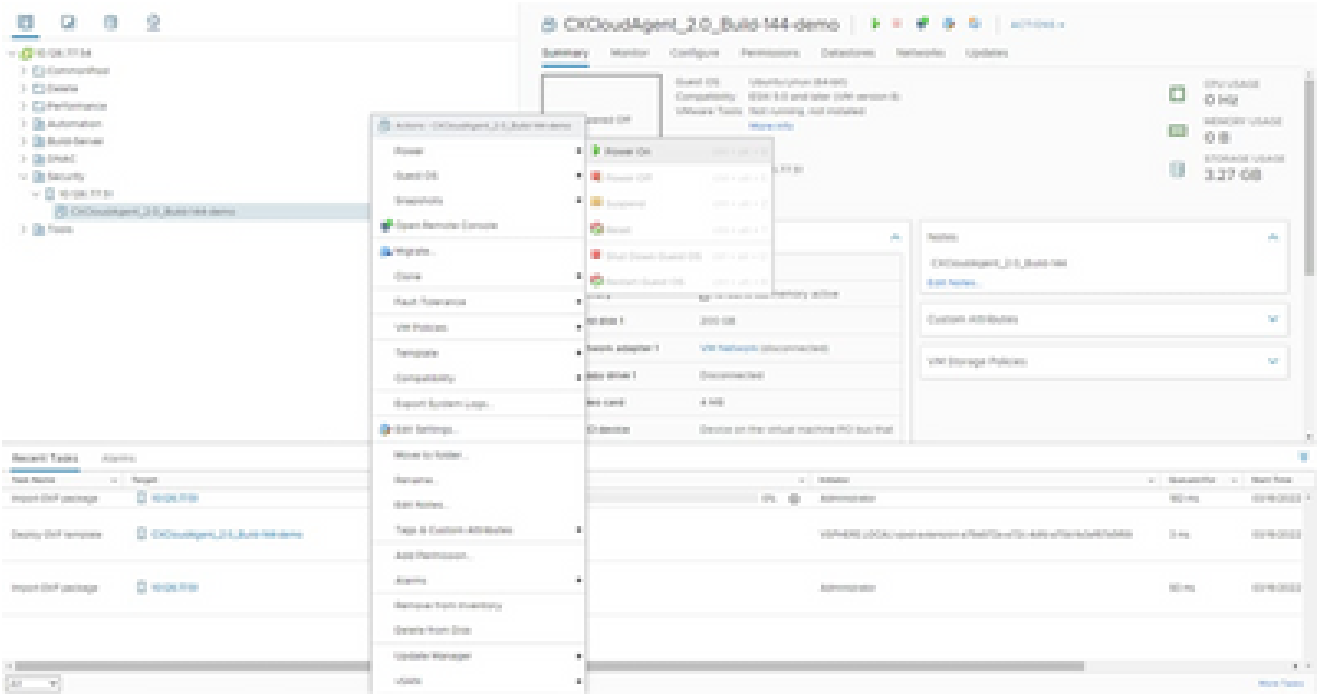
終了準備の完了（Ready to Complete）

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。



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。

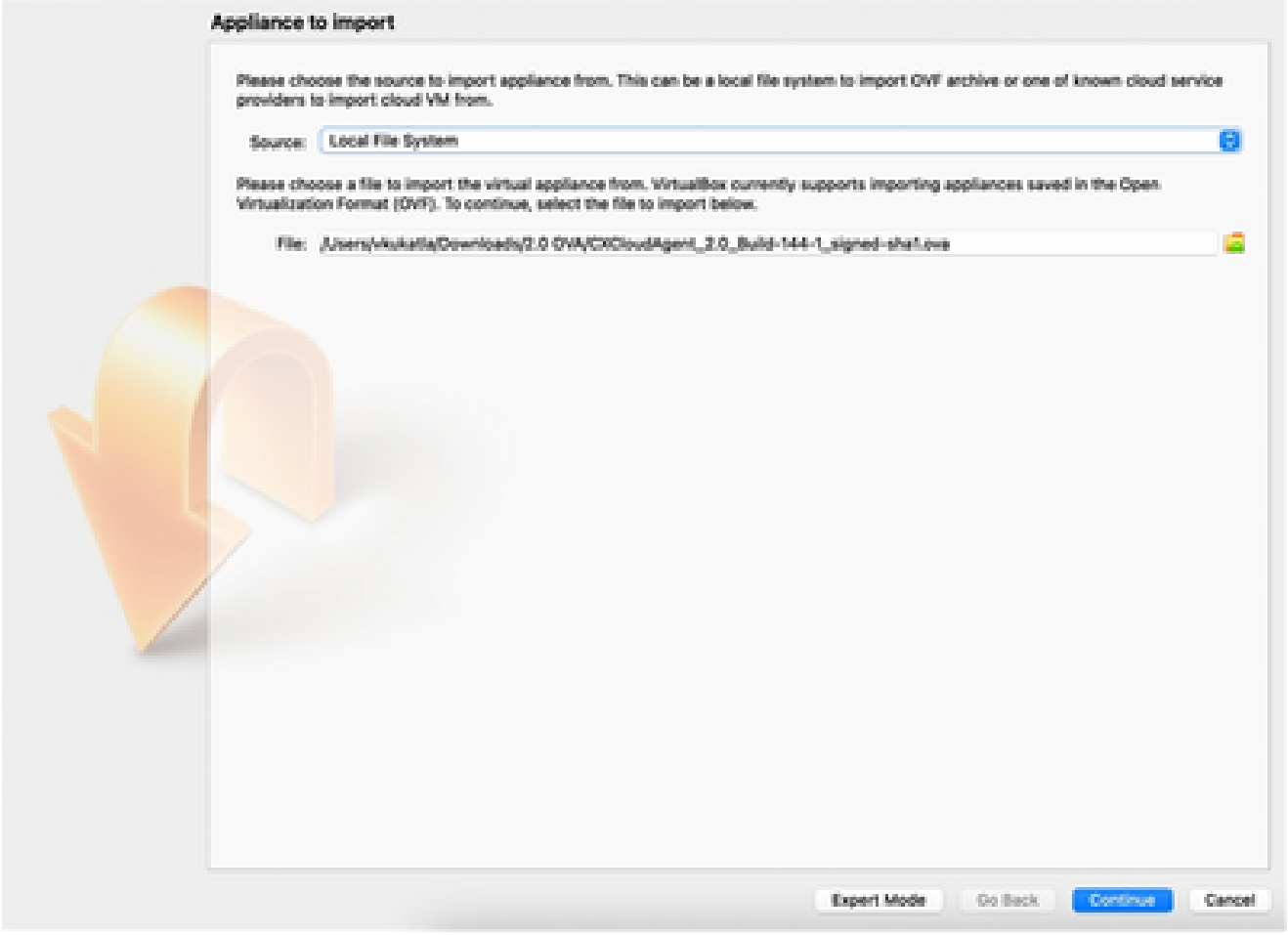
Oracle Virtual Box 5.2.30 のインストール

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。

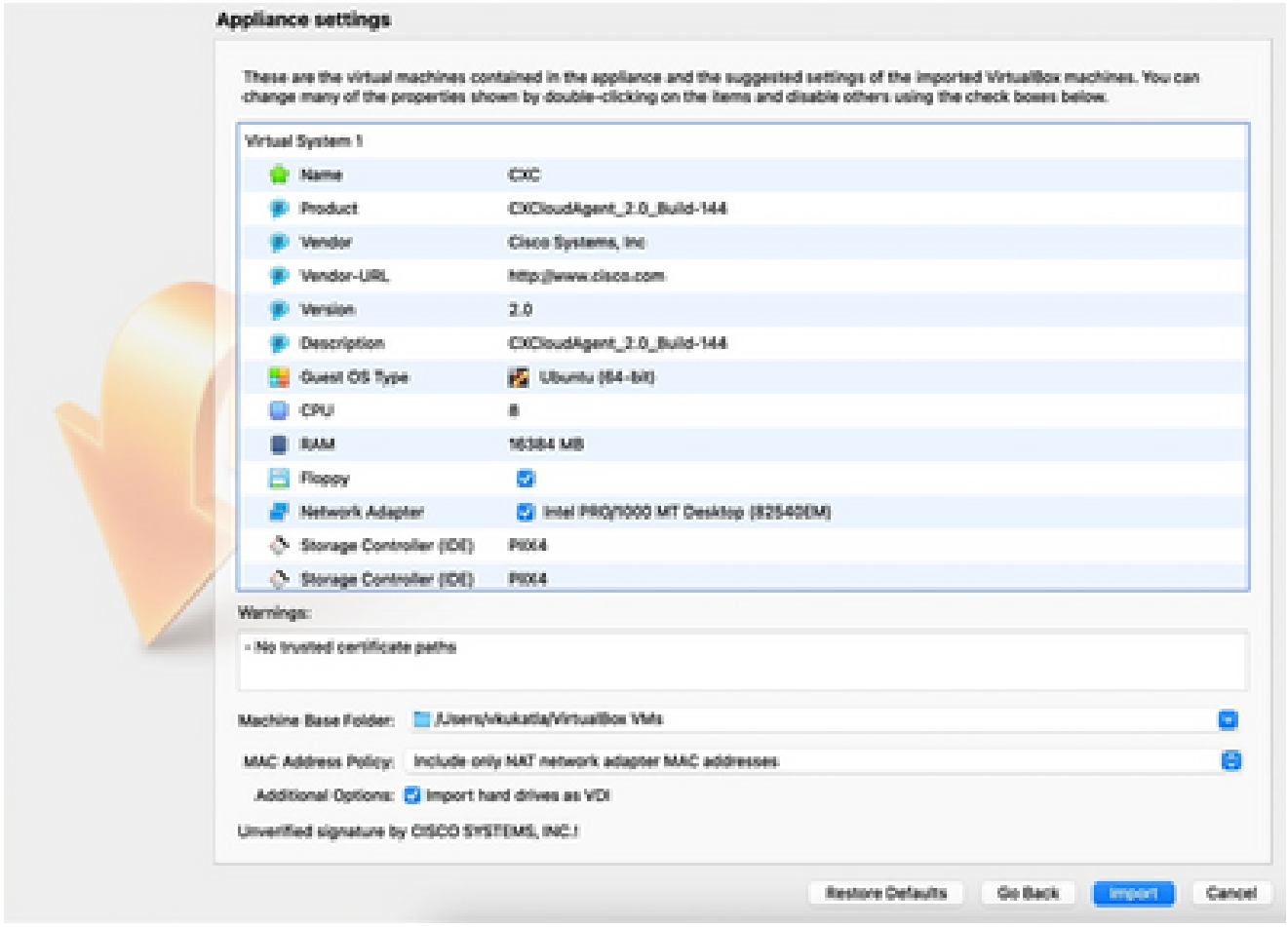
Oracle VM

2. インポートする OVA ファイルを参照します。



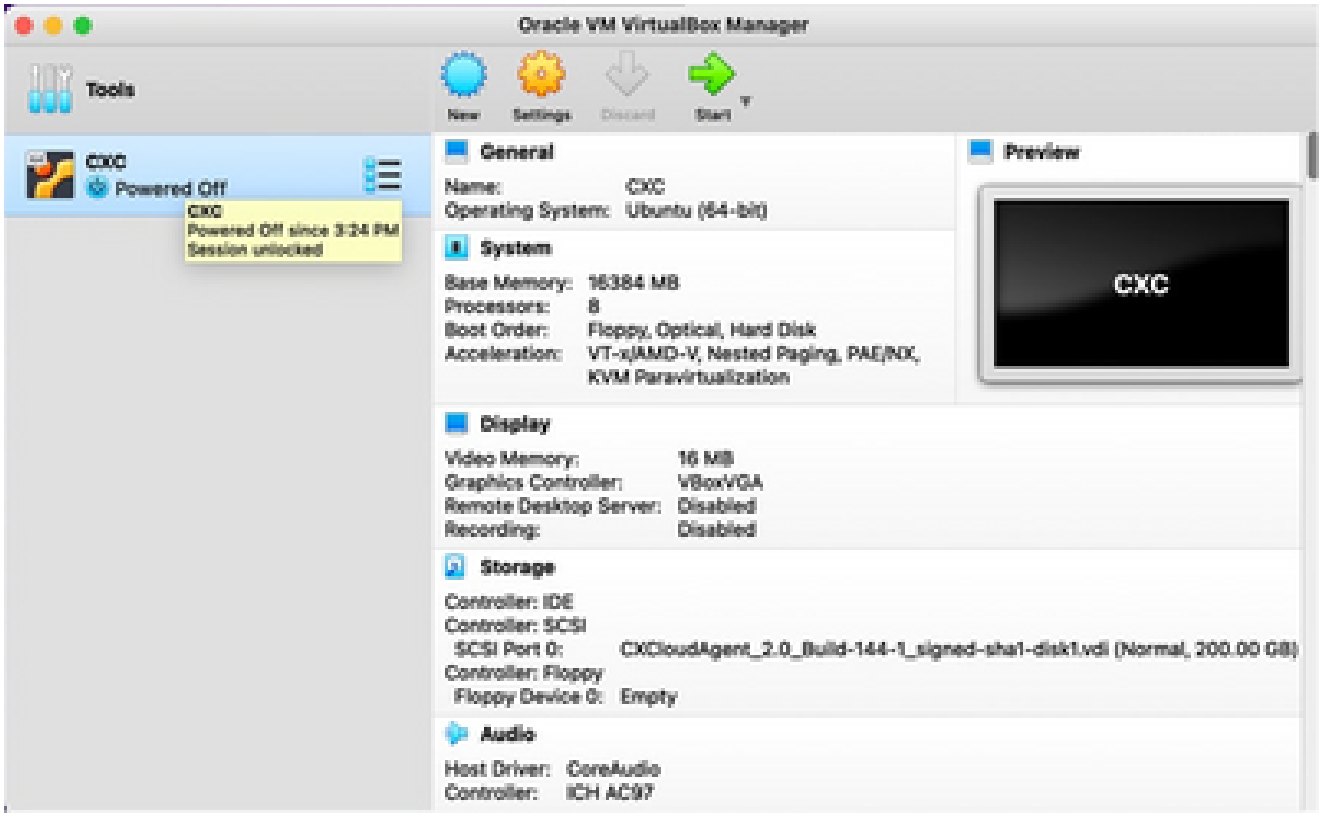
ファイルの選択

3. [Import] をクリックします。

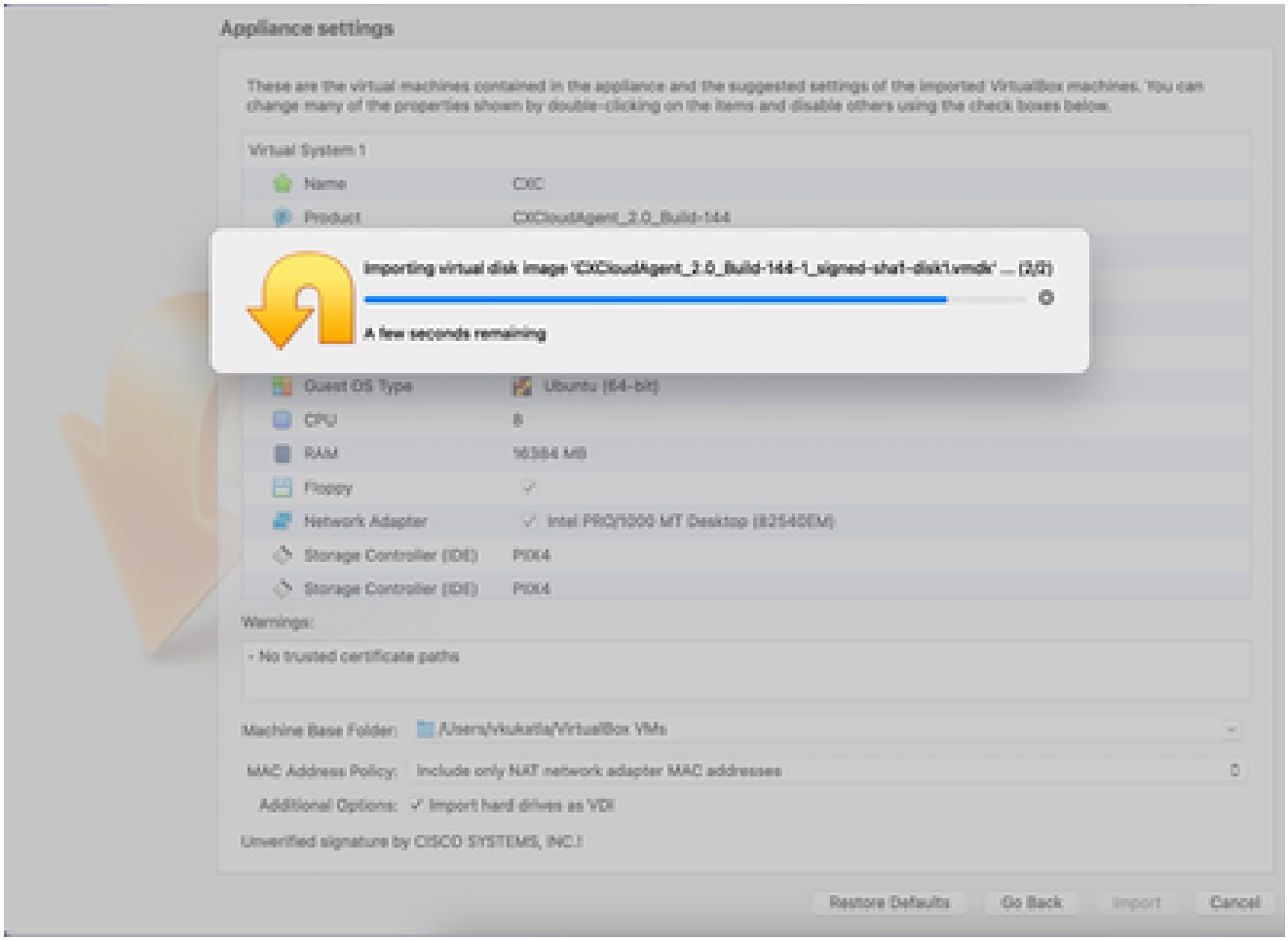


ファイルのインポート

4. 導入したばかりのVMを選択し、Startをクリックします。

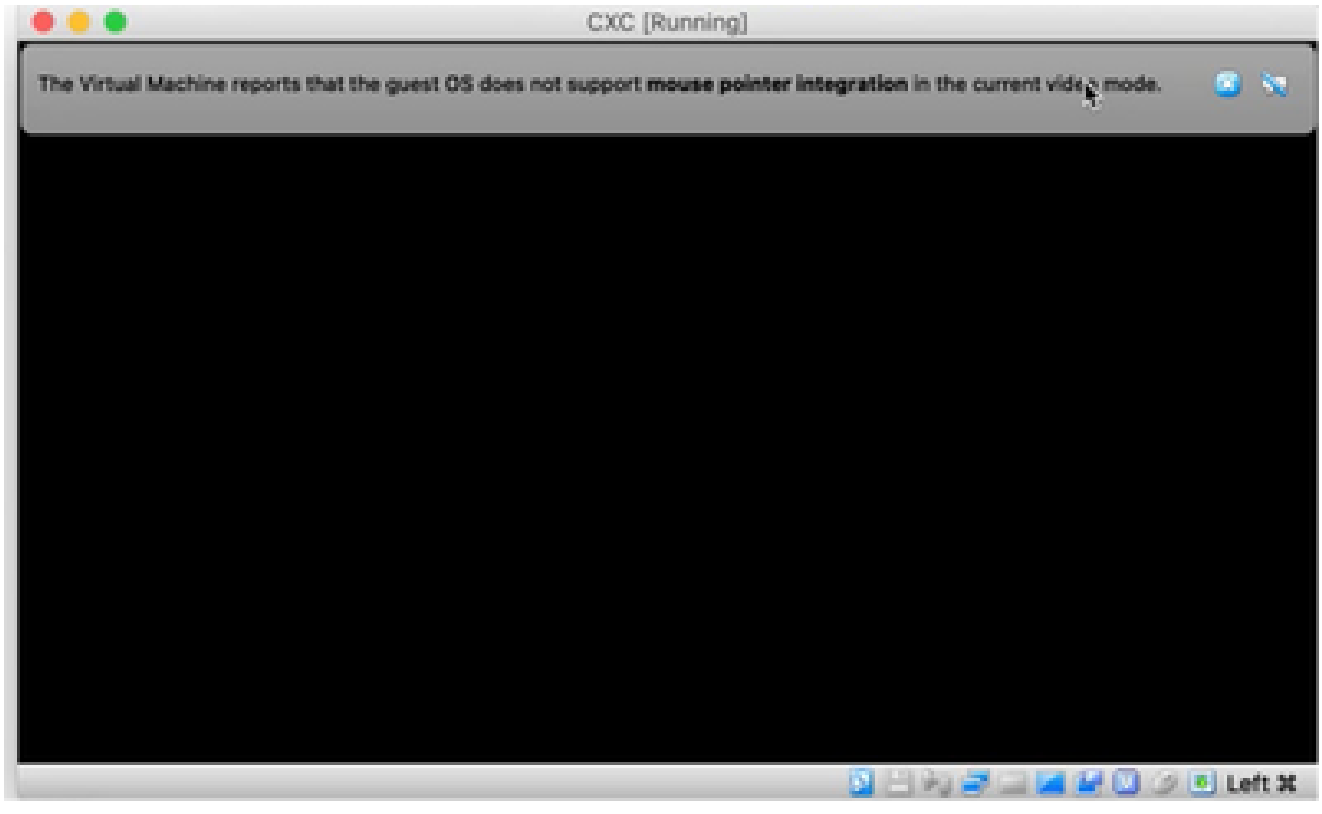


VM コンソールの起動



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。



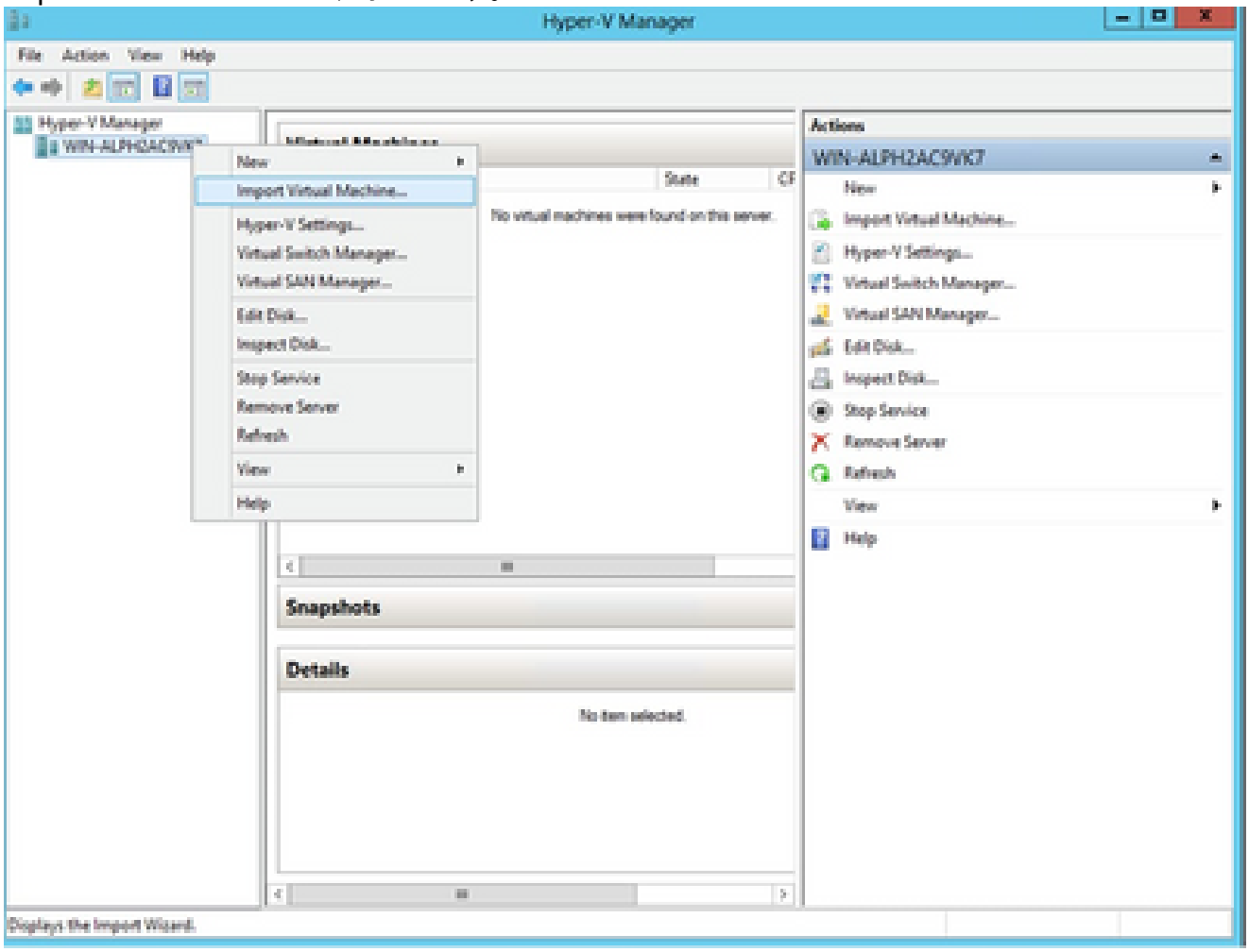
[コンソールを開く（ Open Console ）]

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

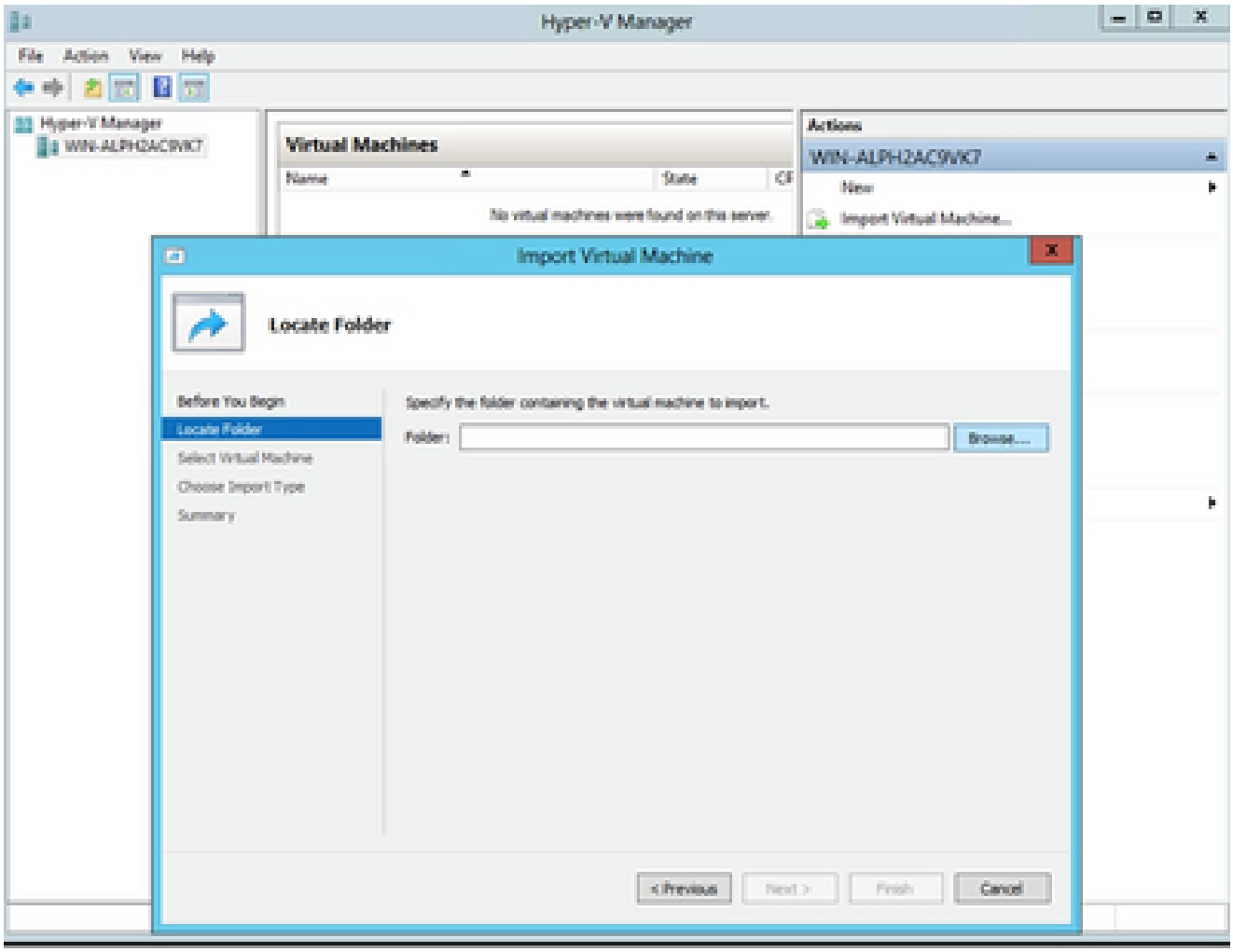
次の手順を実行します。

1. Import Virtual Machineを選択します。



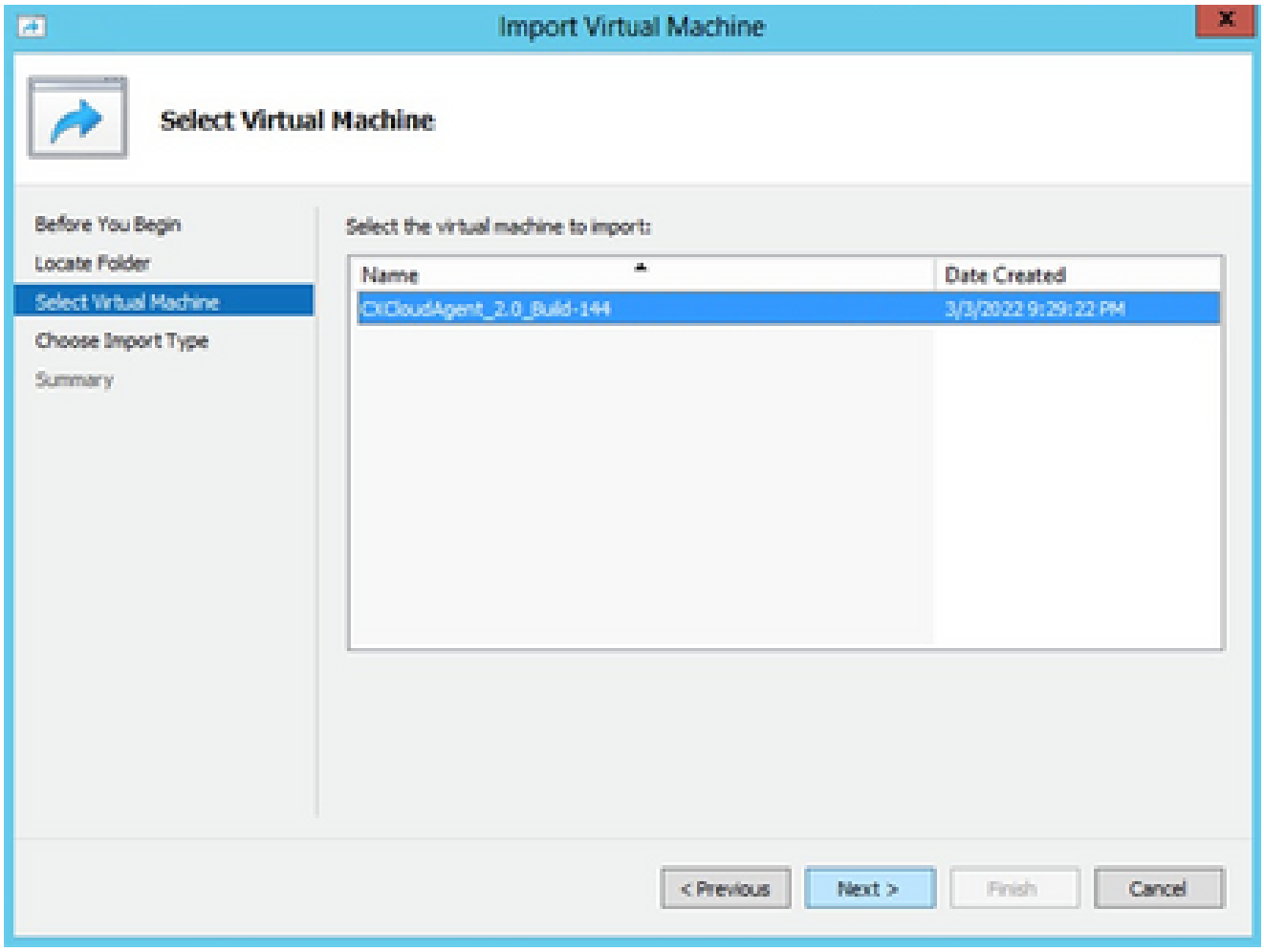
Hyper Vマネージャー

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。



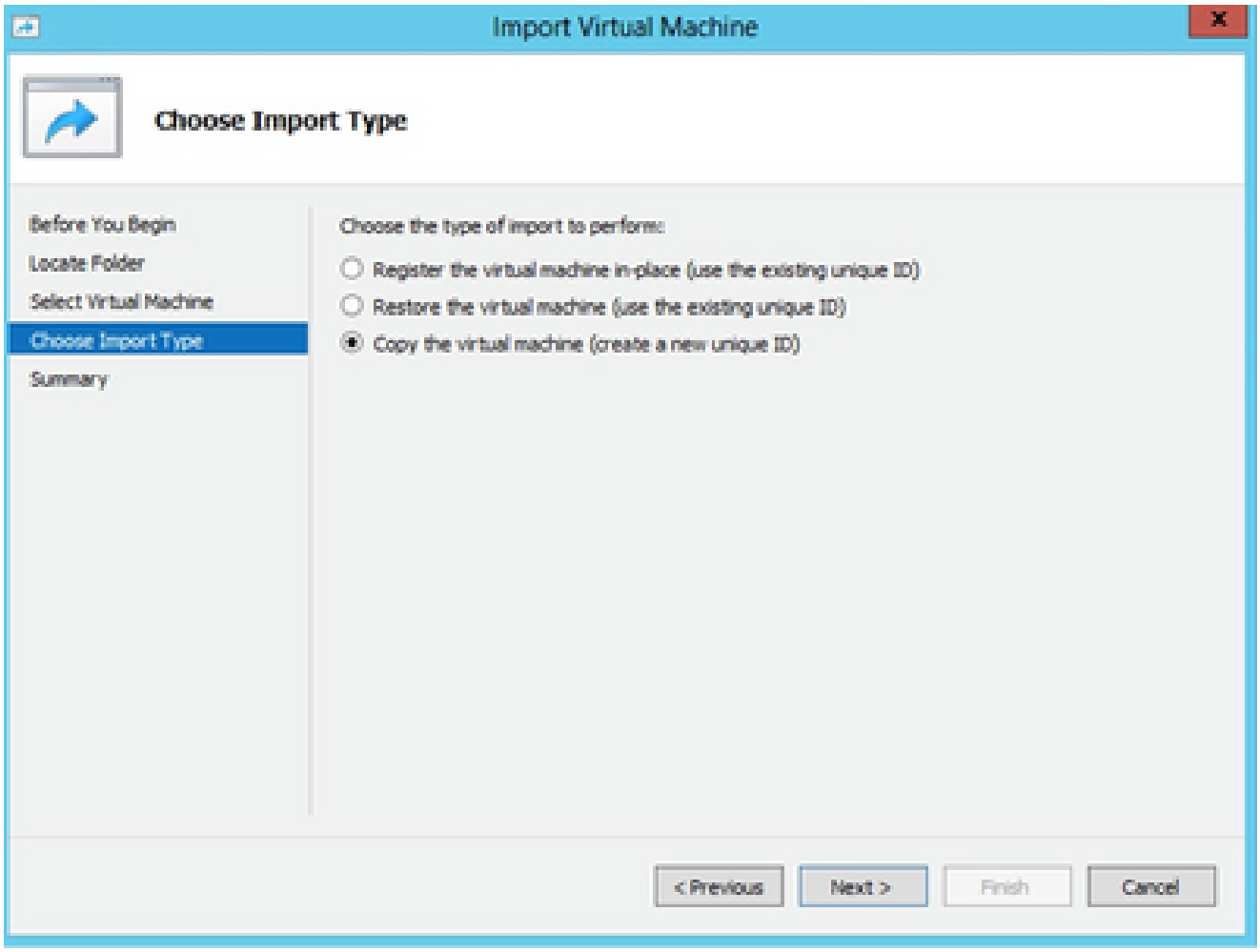
インポートするフォルダ

4. VMを選択し、Nextをクリックします。



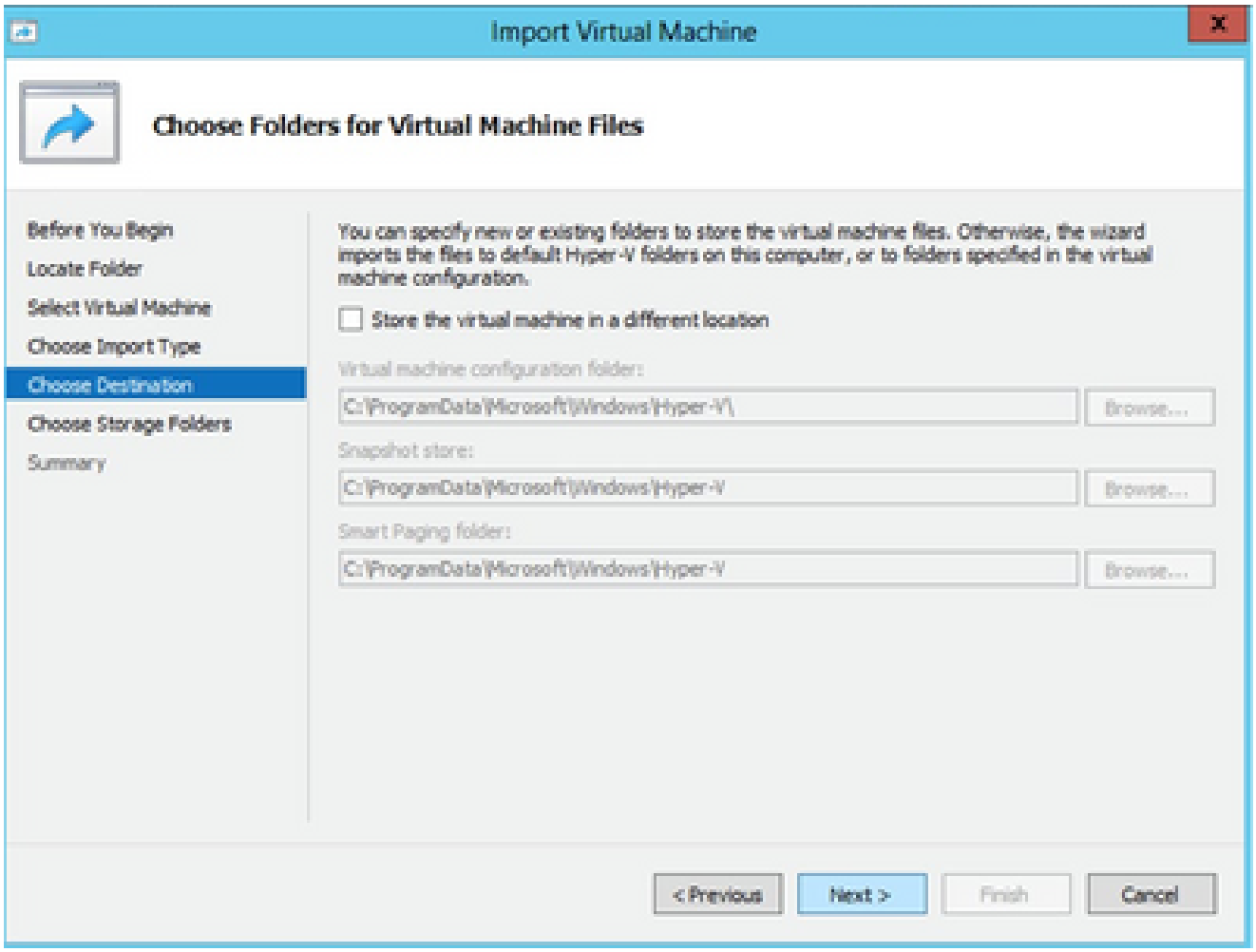
[VMの選択（Select VM）]

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。



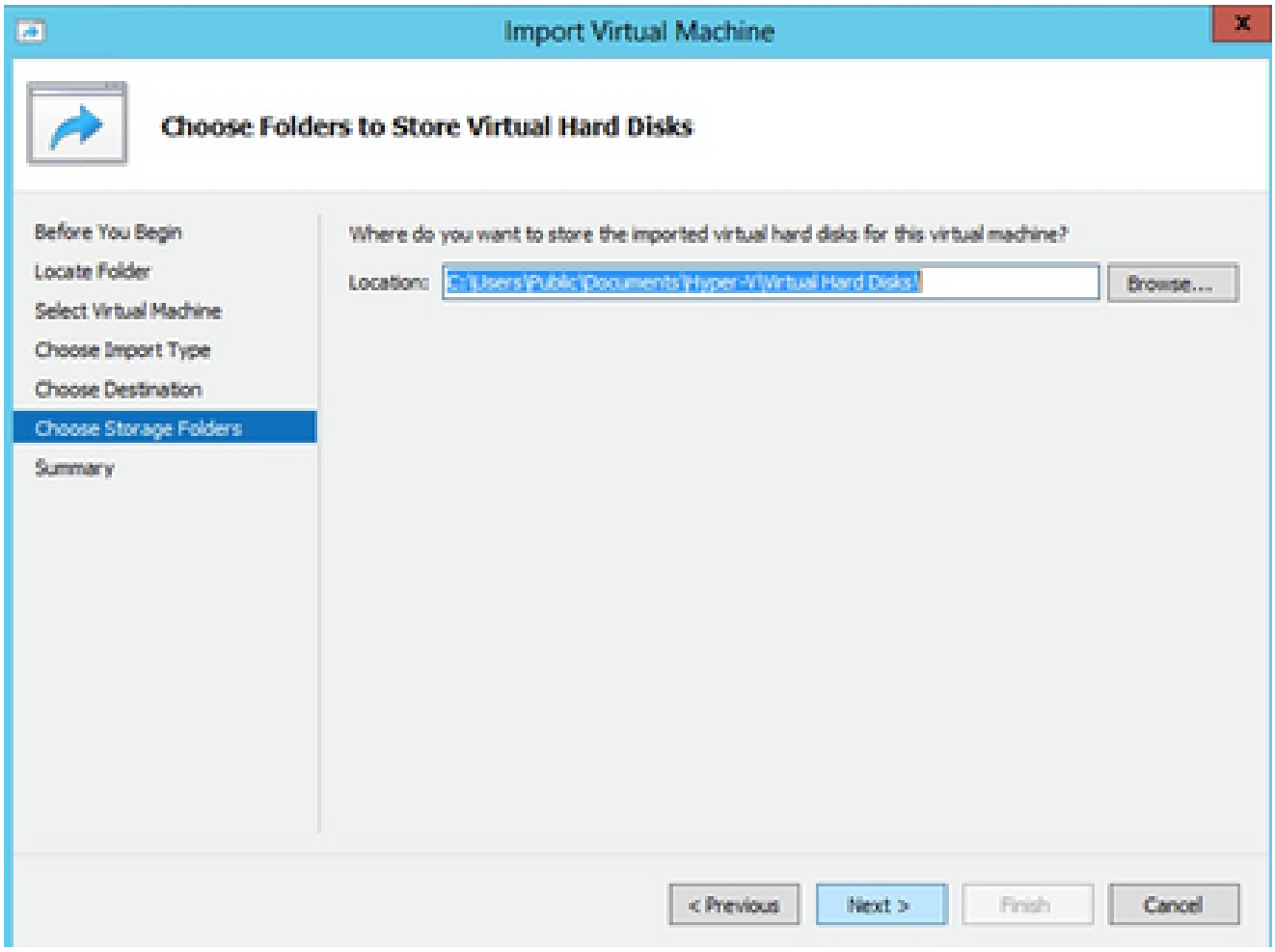
インポート タイプ

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。



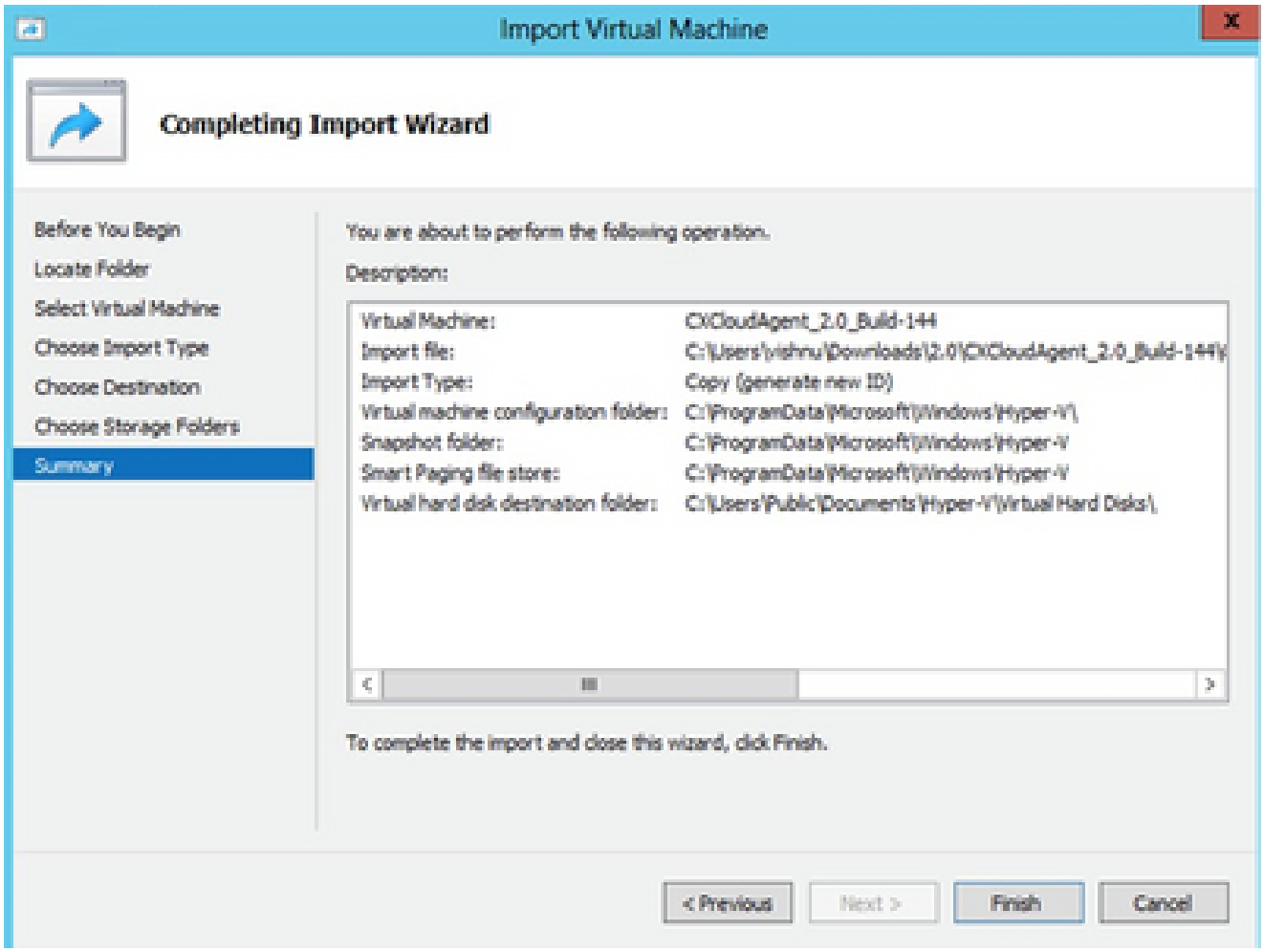
仮想マシンファイルのフォルダの選択

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。



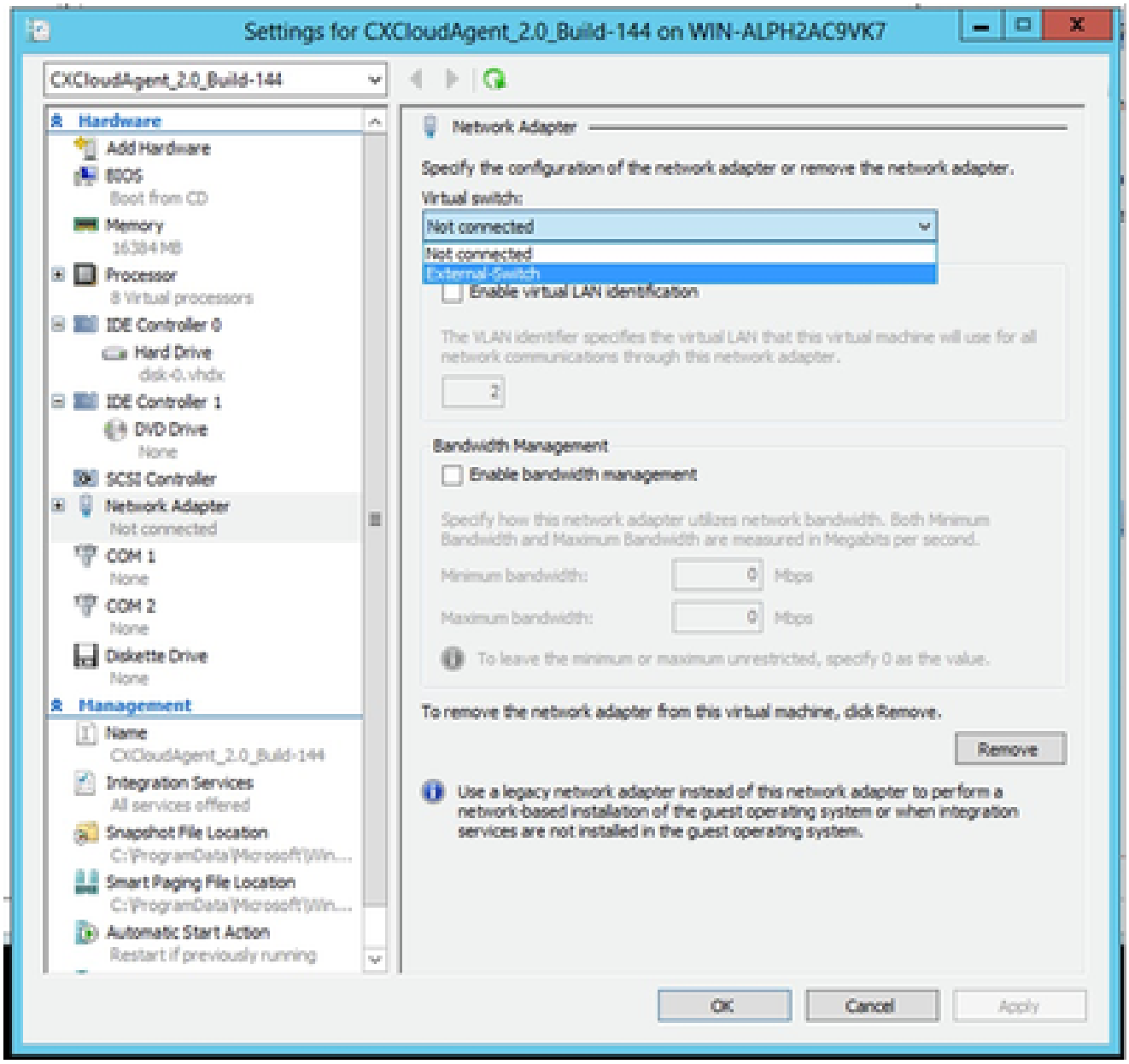
仮想ハードディスクを格納するフォルダ

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。



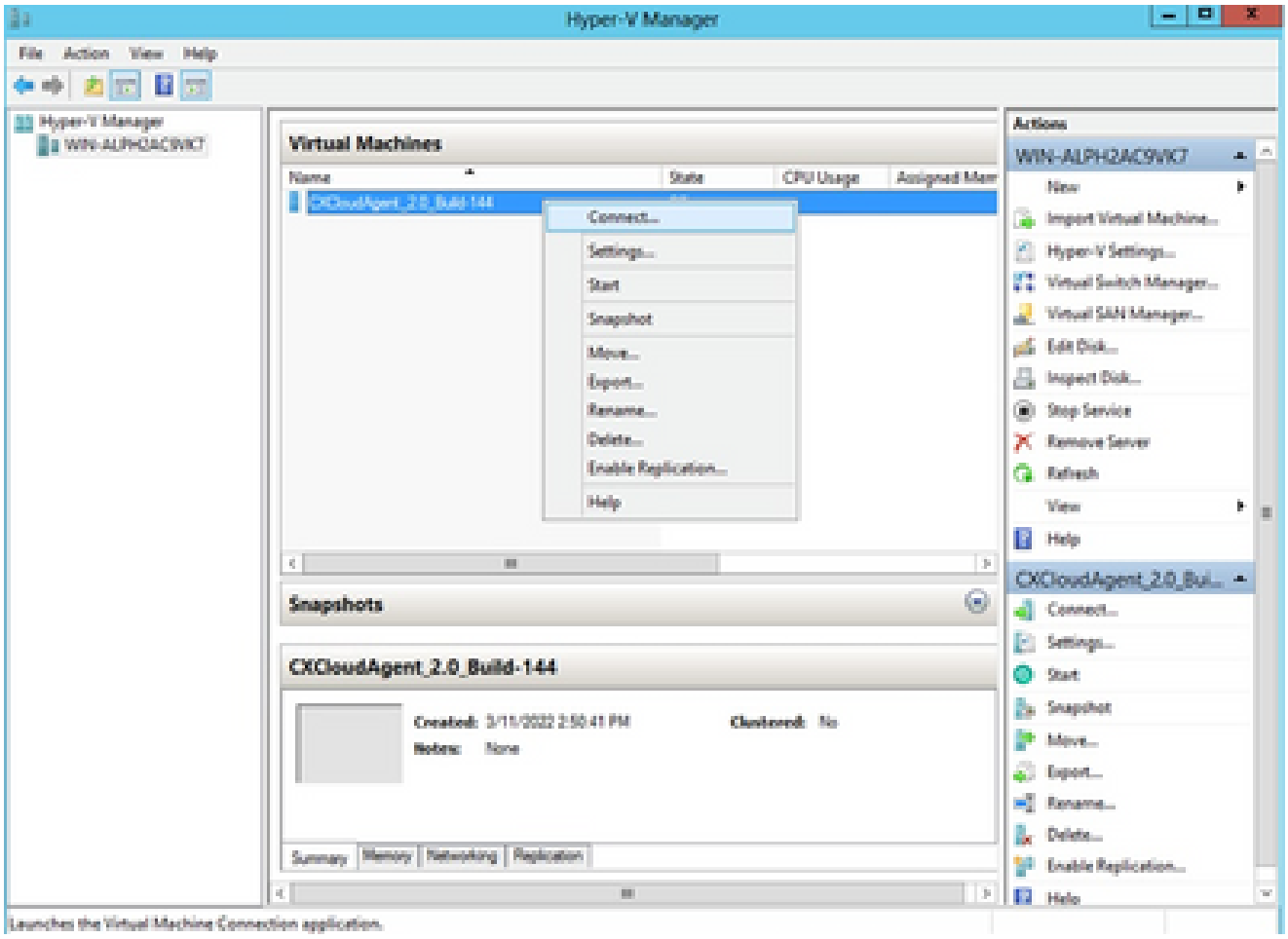
要約

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。

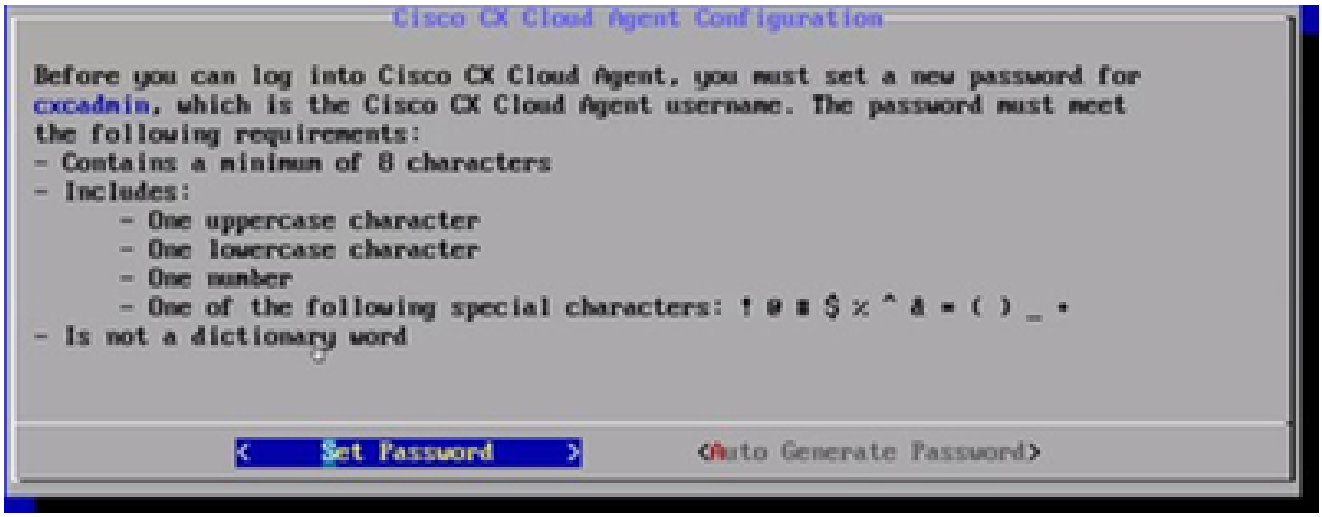


VM の起動

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

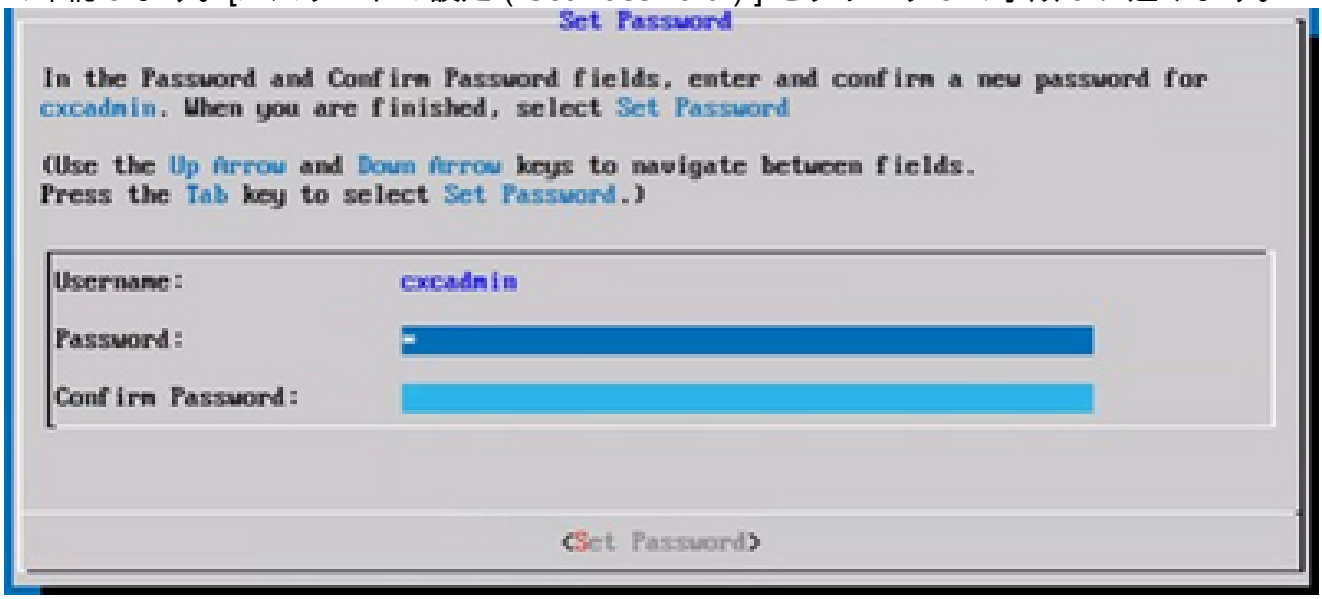
1. Set Passwordをクリックしてcxcadminの新しいパスワードを追加するか、Auto Generate Passwordをクリックして新しいパスワードを取得します。



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。



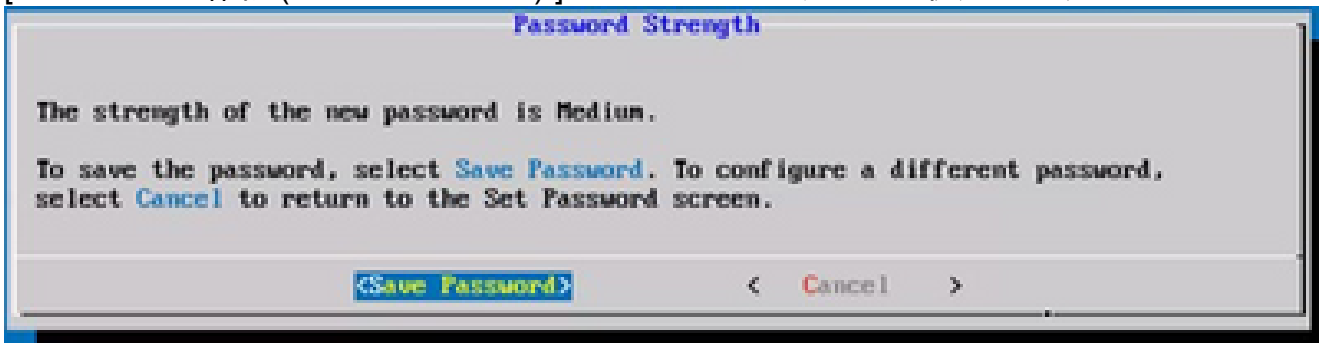
新しいパスワード

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。

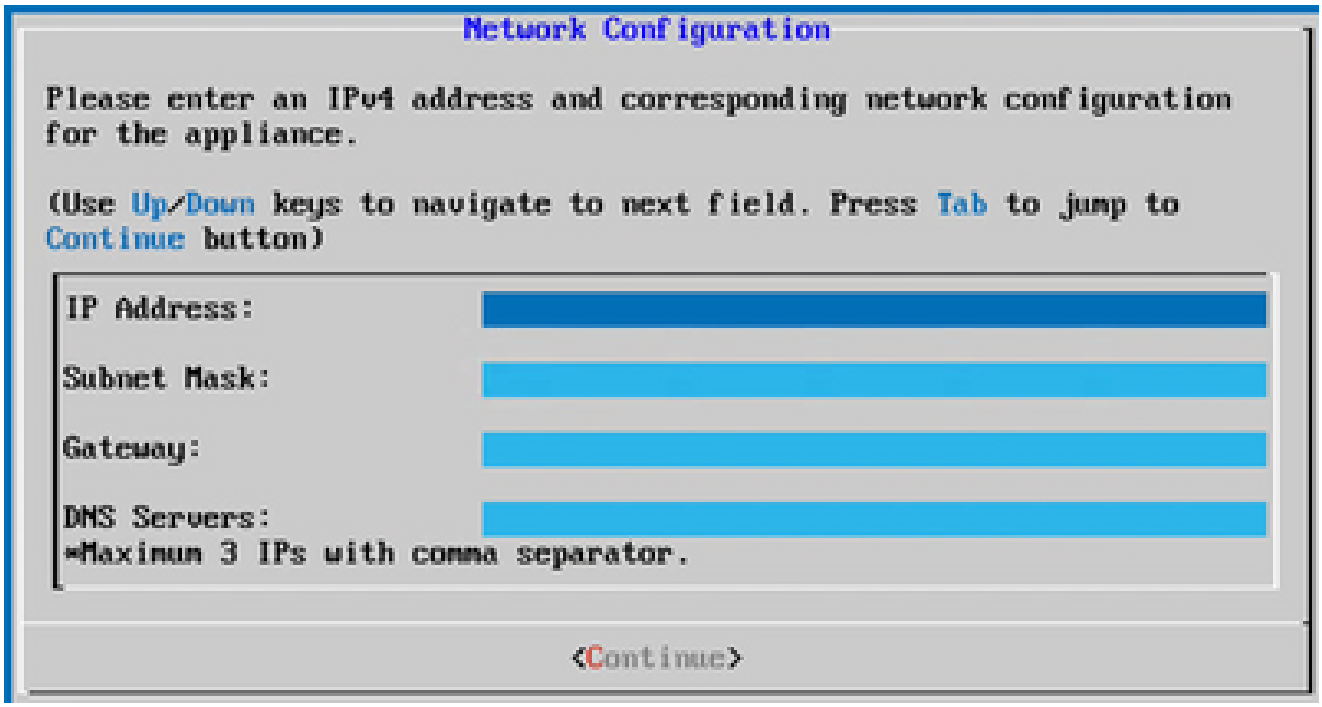
自動生成パスワード

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。

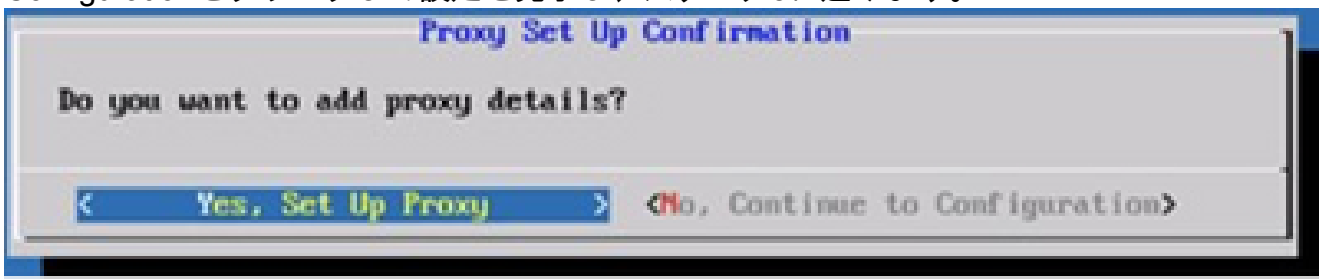


ネットワーク設定

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。

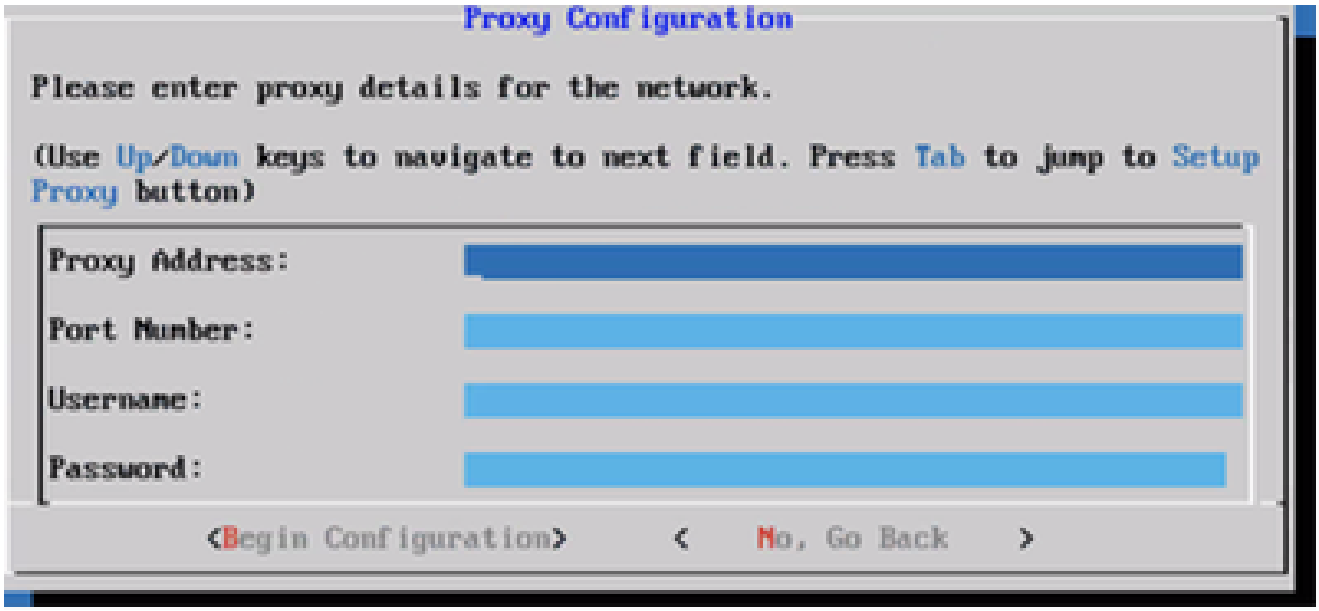
コンフィギュレーション

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。



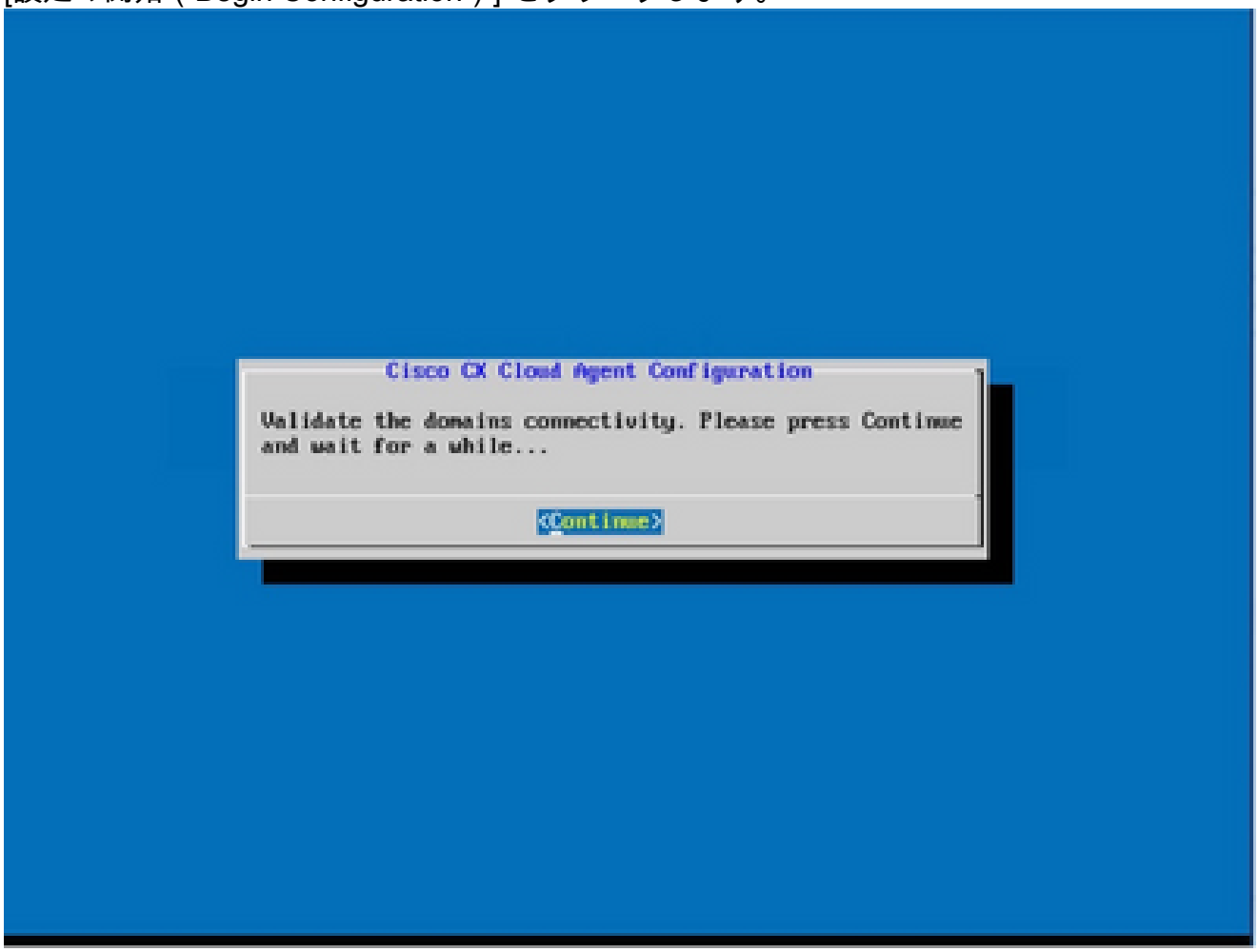
プロキシ設定

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。



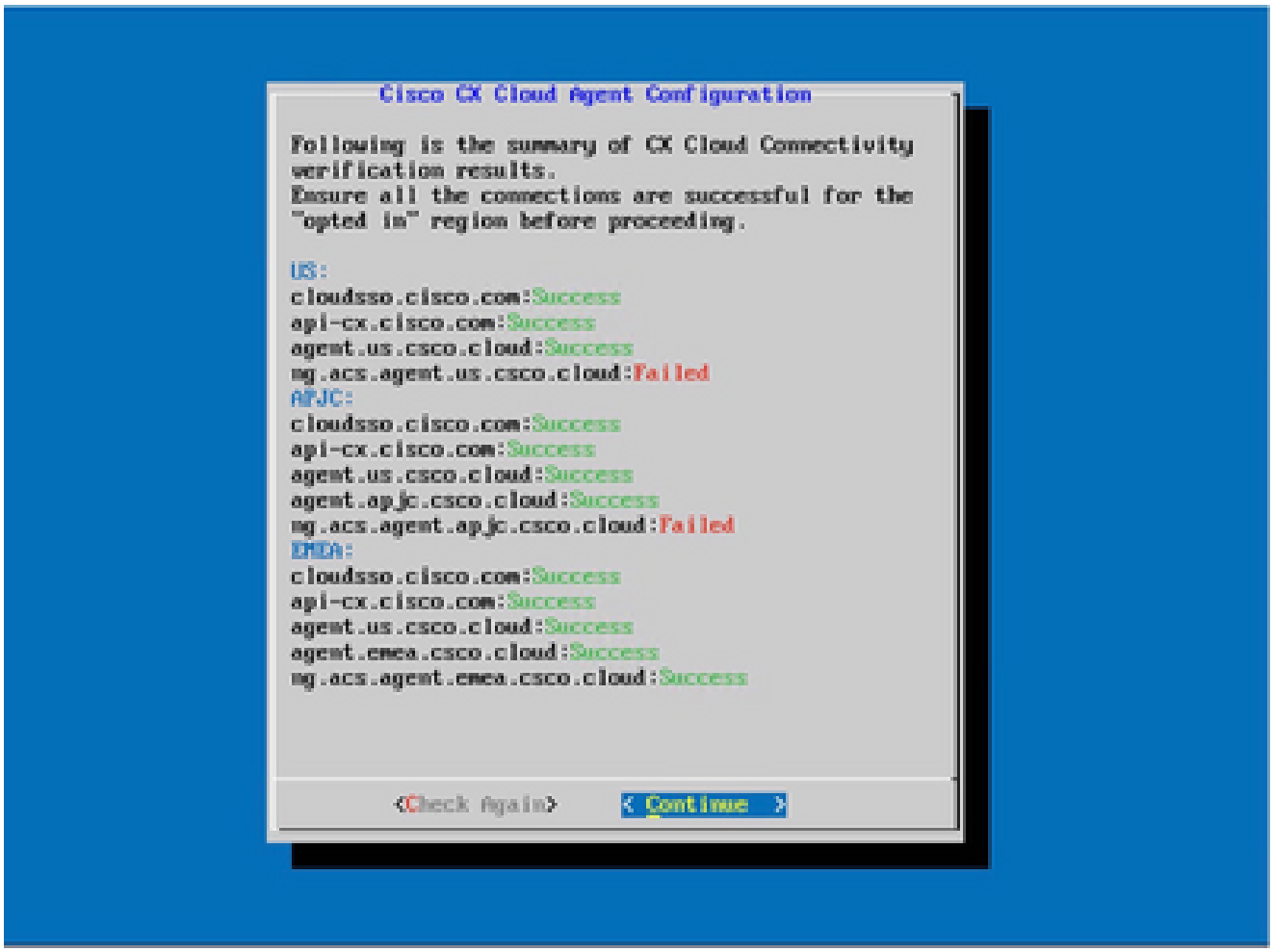
プロキシ設定

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



Begin configuration

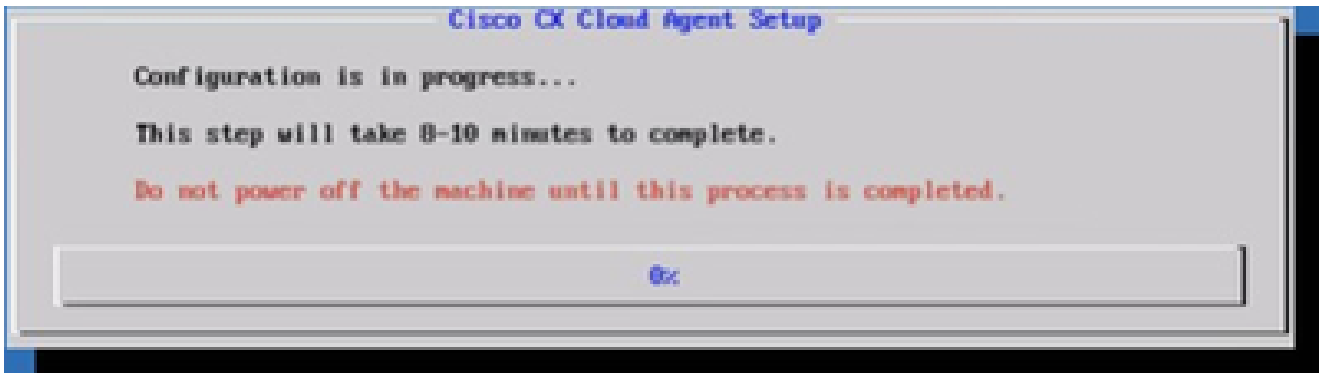
9. [Continue] をクリックします。



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。

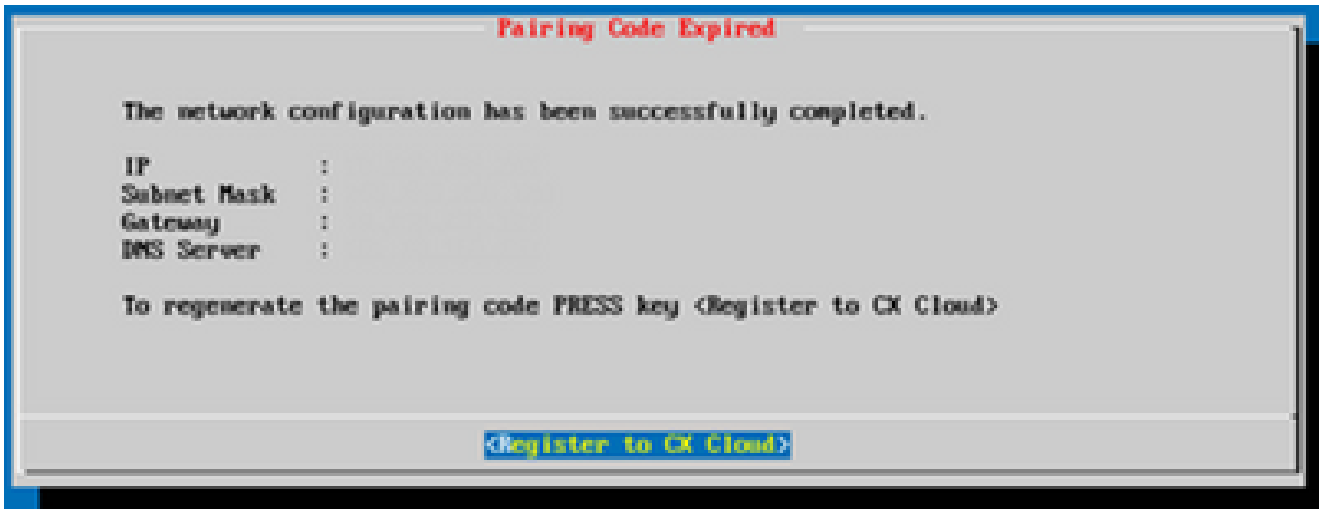


設定が進行中です

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。

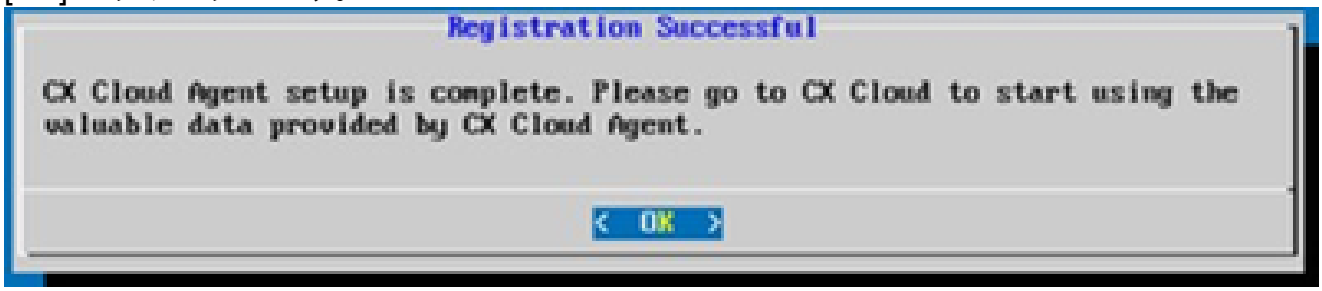
ペアリングコード

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。



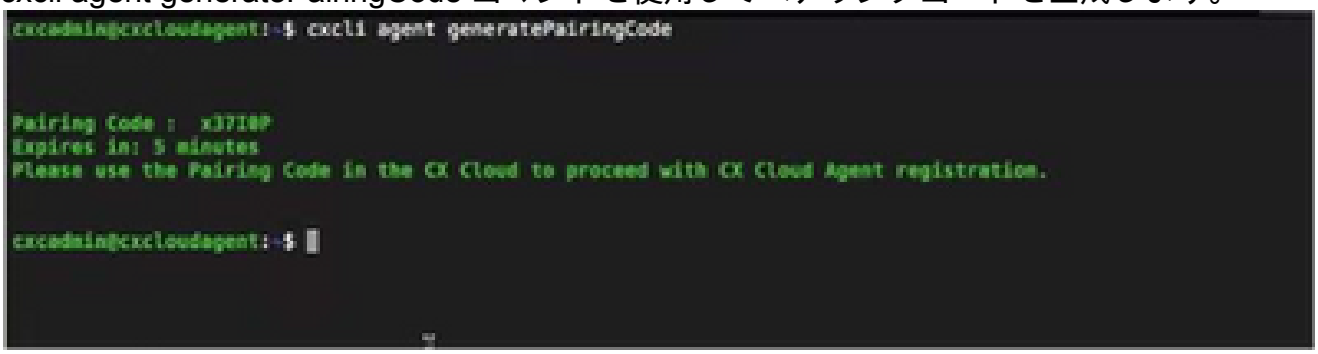
登録に成功しました

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。



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

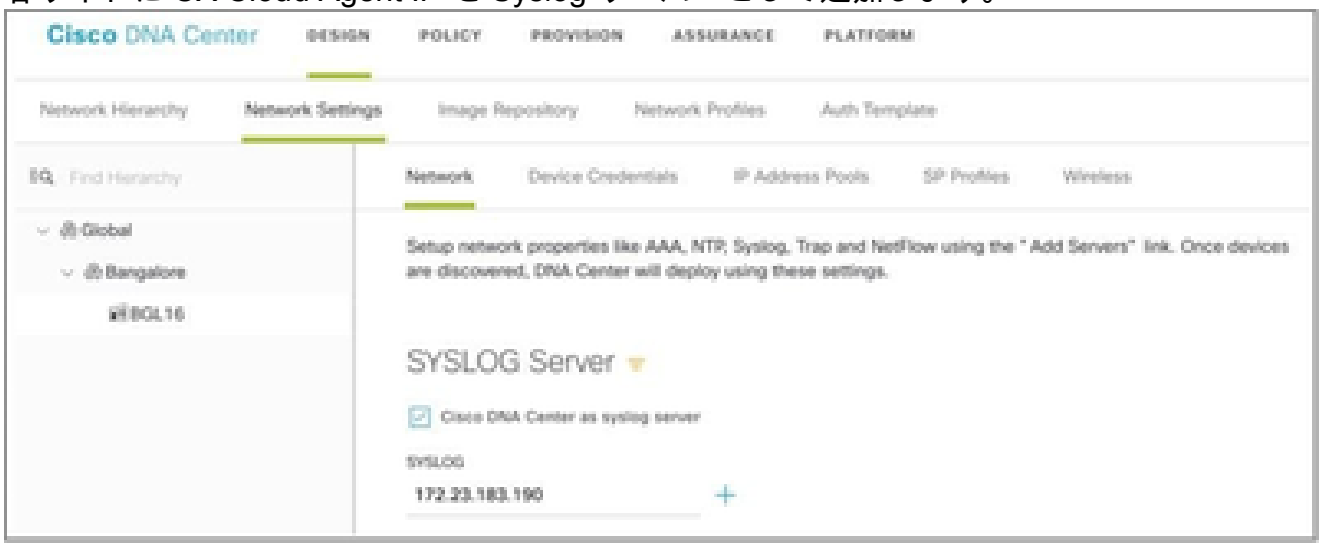
前提条件

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。

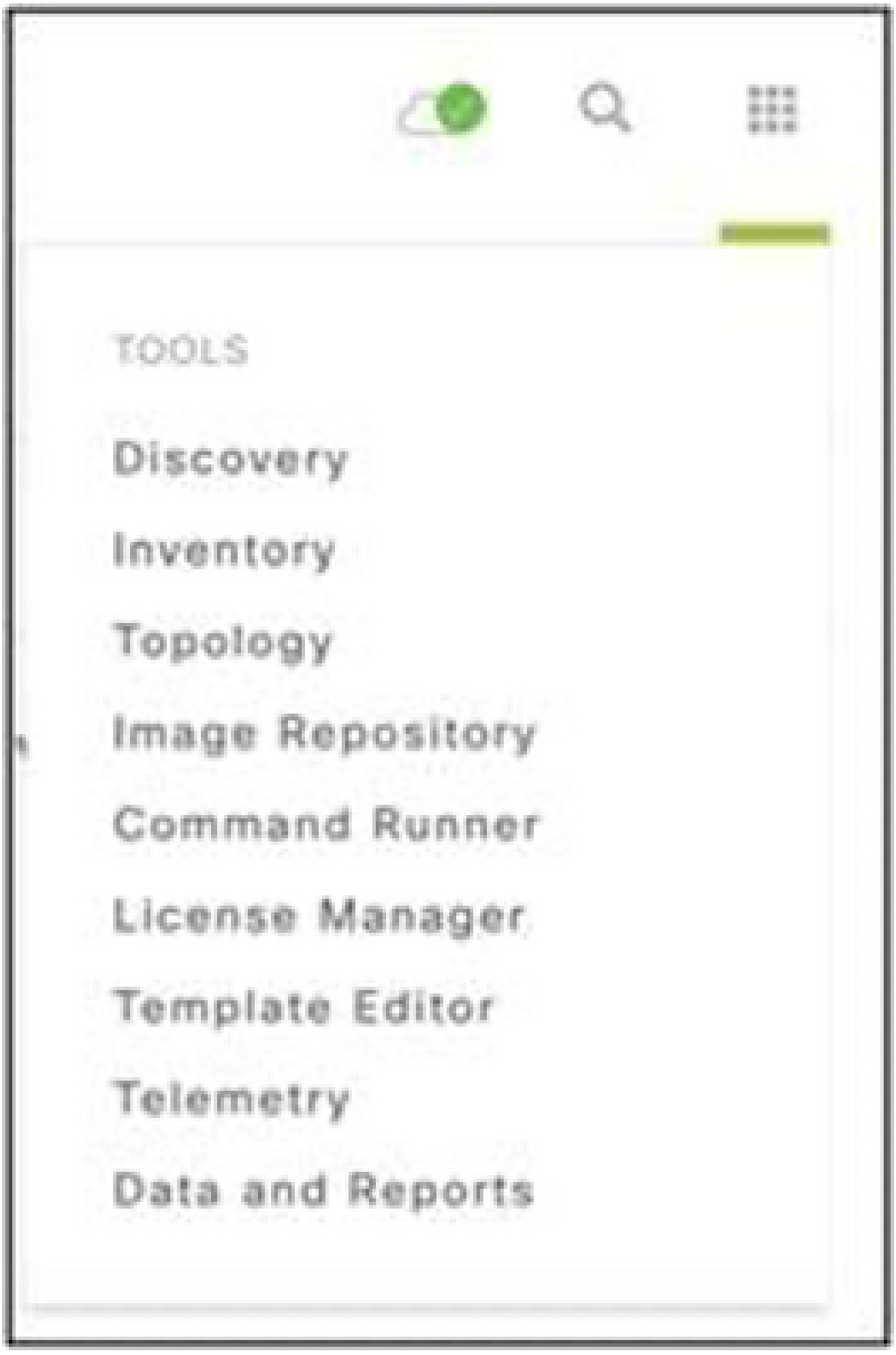
Cisco IOS® XEコンフィギュレーションガイド

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）]

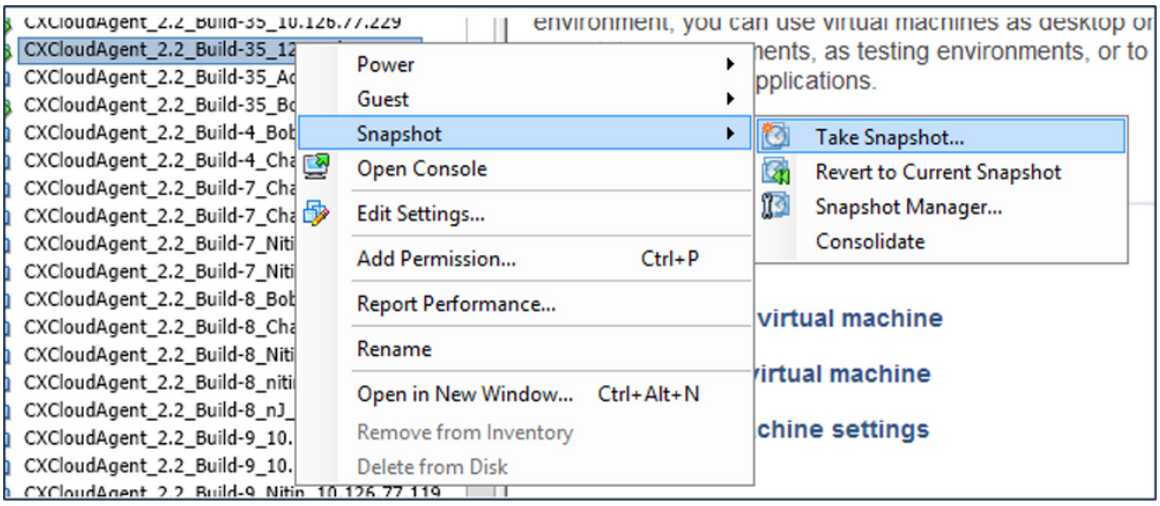
CX Cloud VMのバックアップと復元

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。

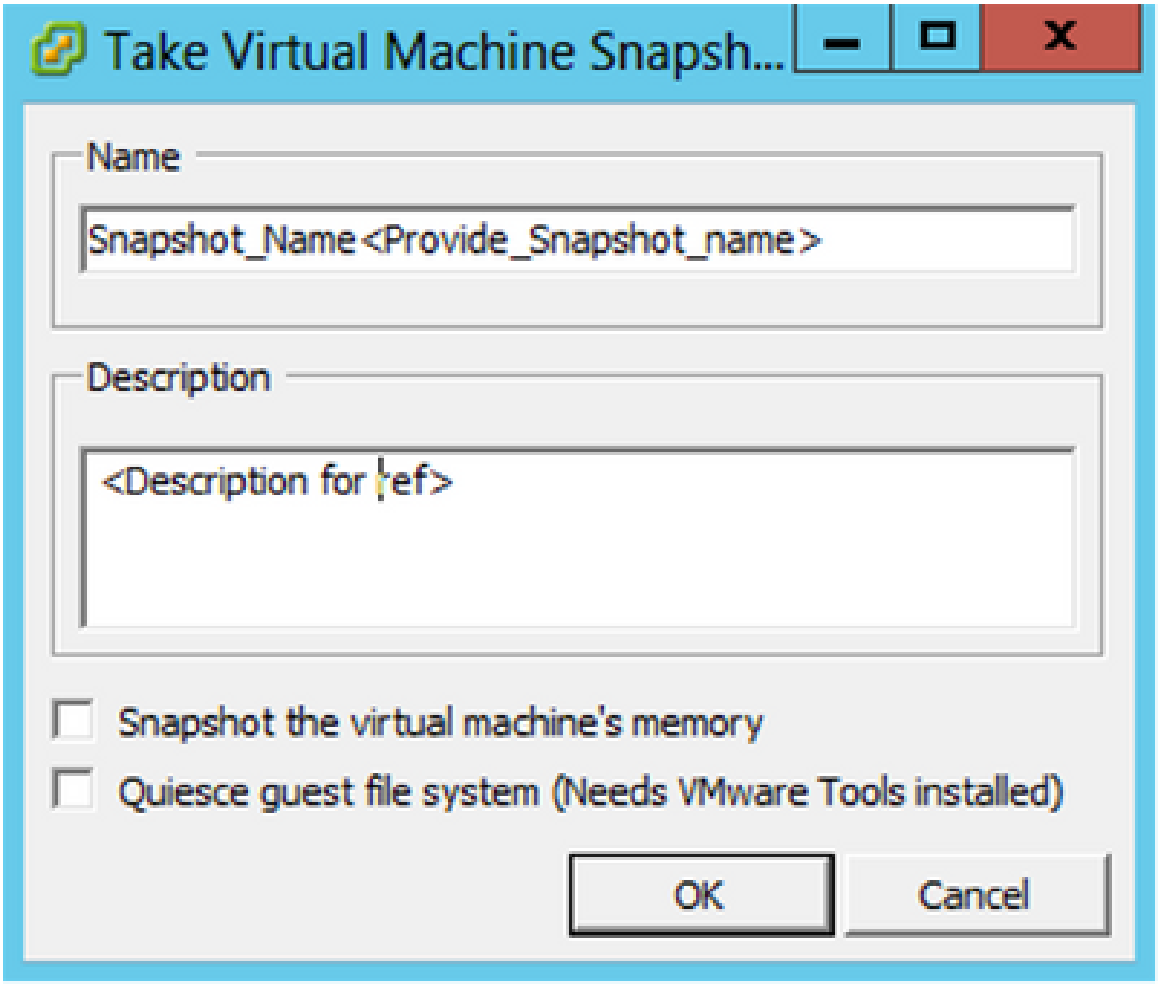
バックアップ

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）]

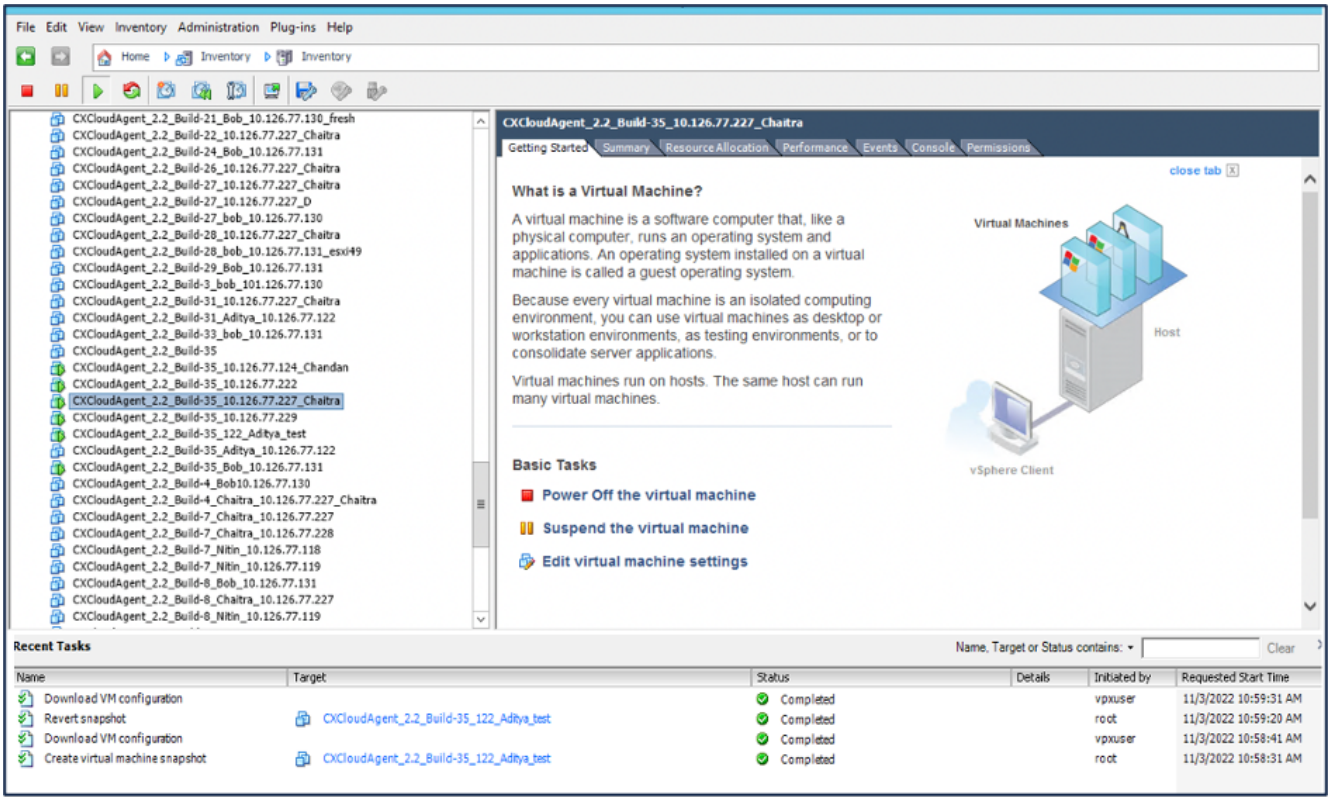


仮想マシンのスナップショットの作成

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。

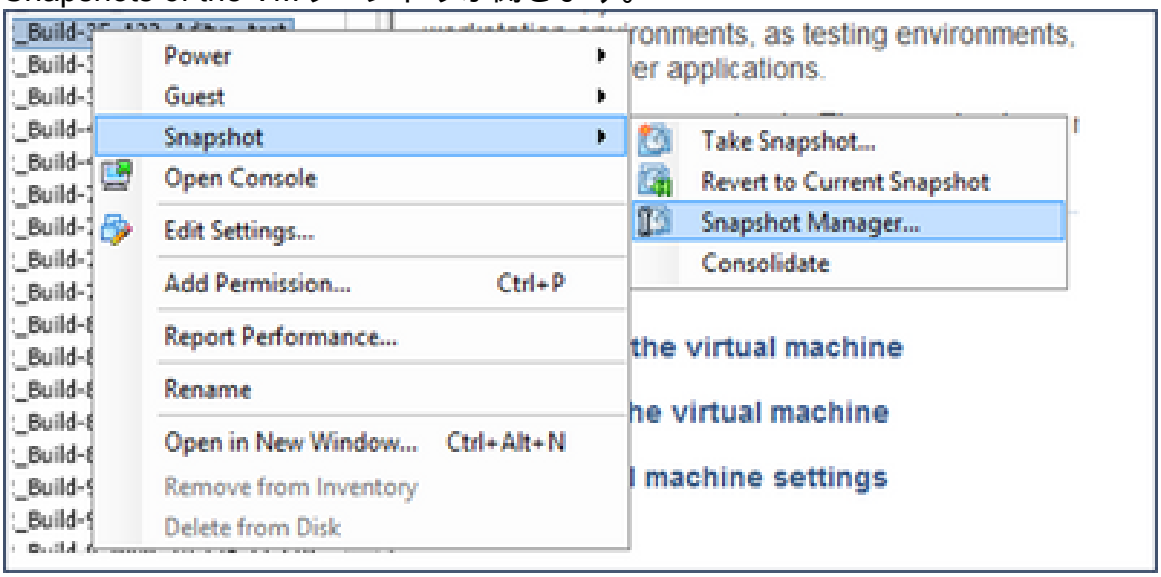


最近のタスク

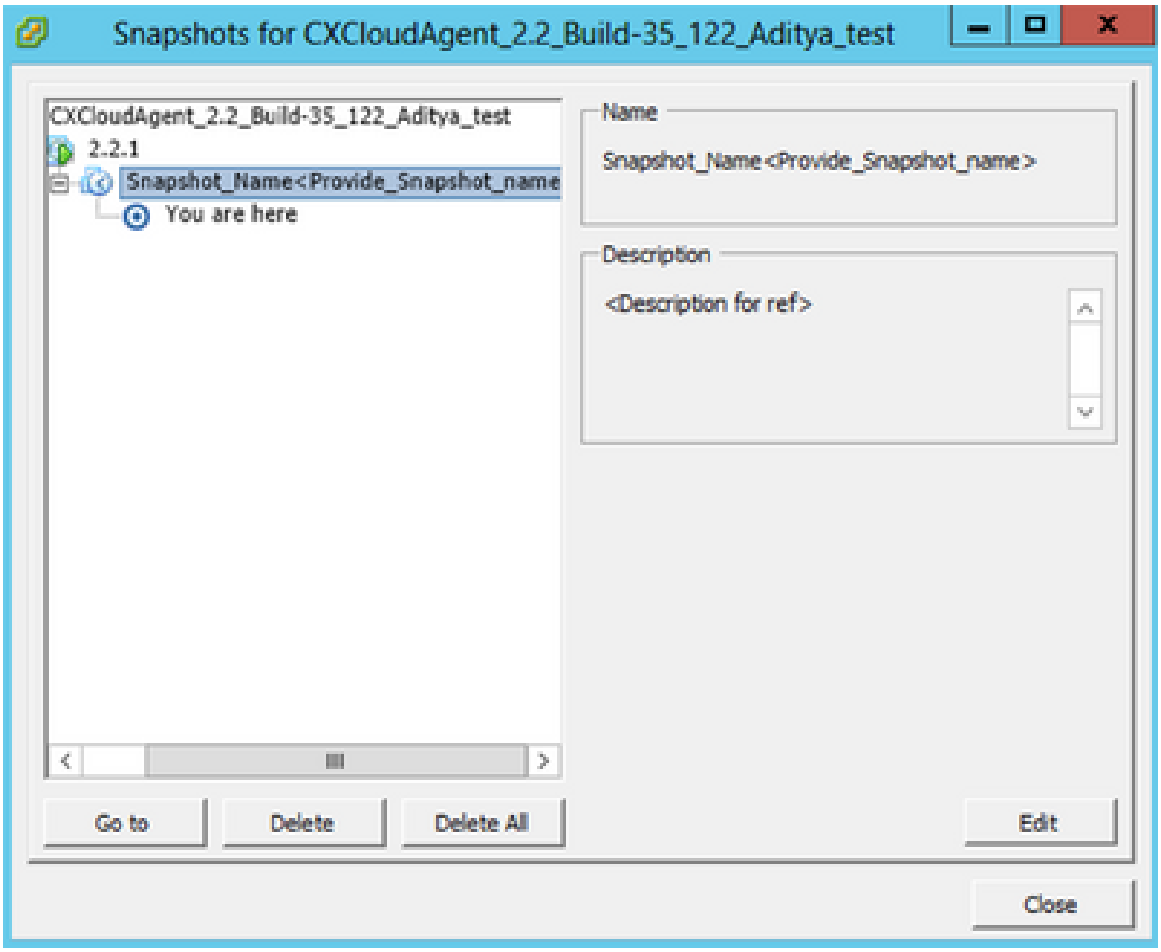
復元

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。

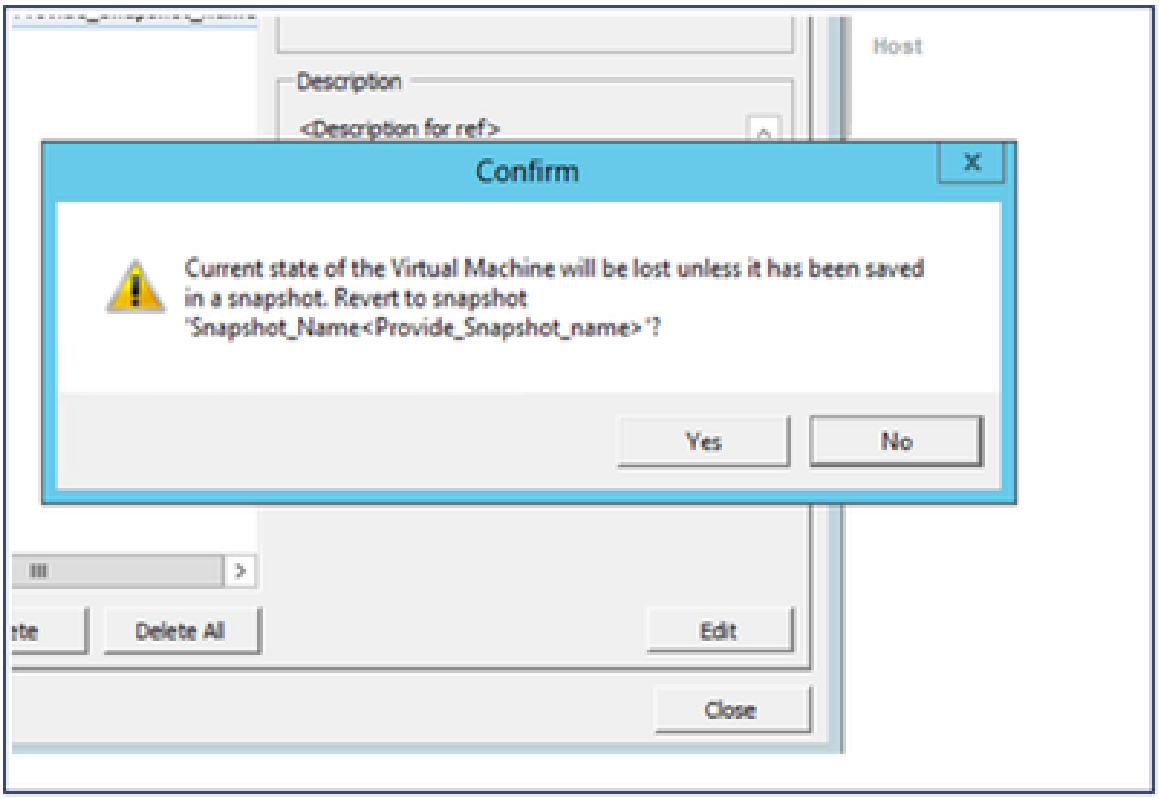


Select VMウィンドウ



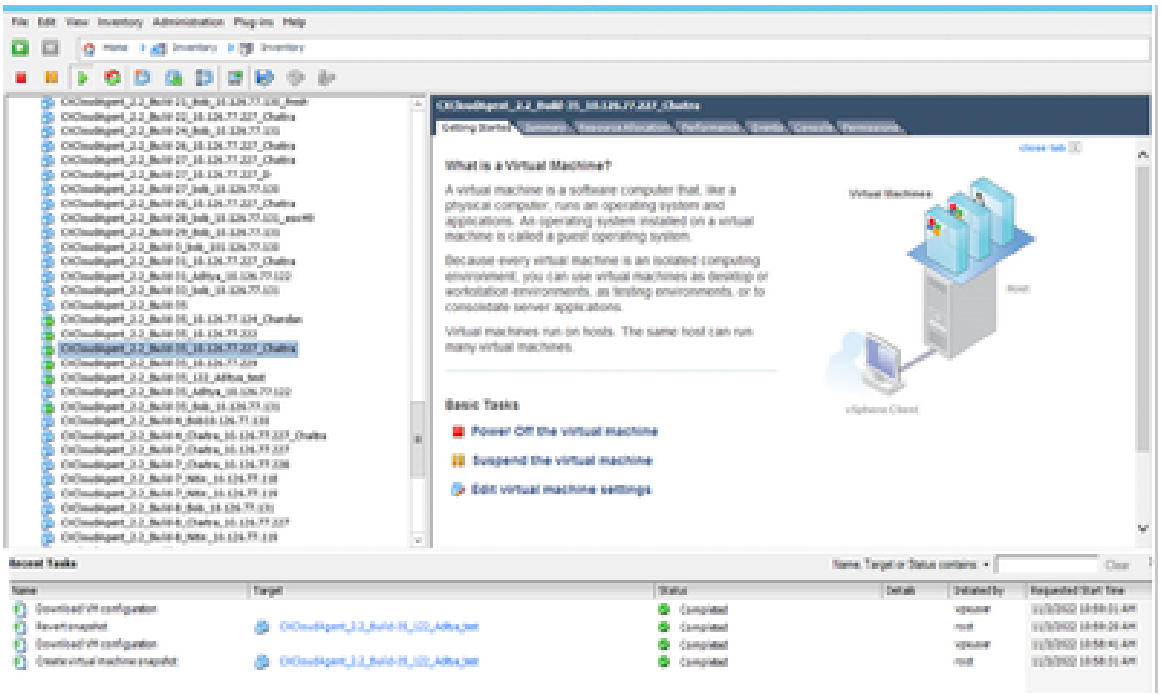
「スナップショット」ウィンドウ

2. Go toをクリックします。Confirmウィンドウが開きます。



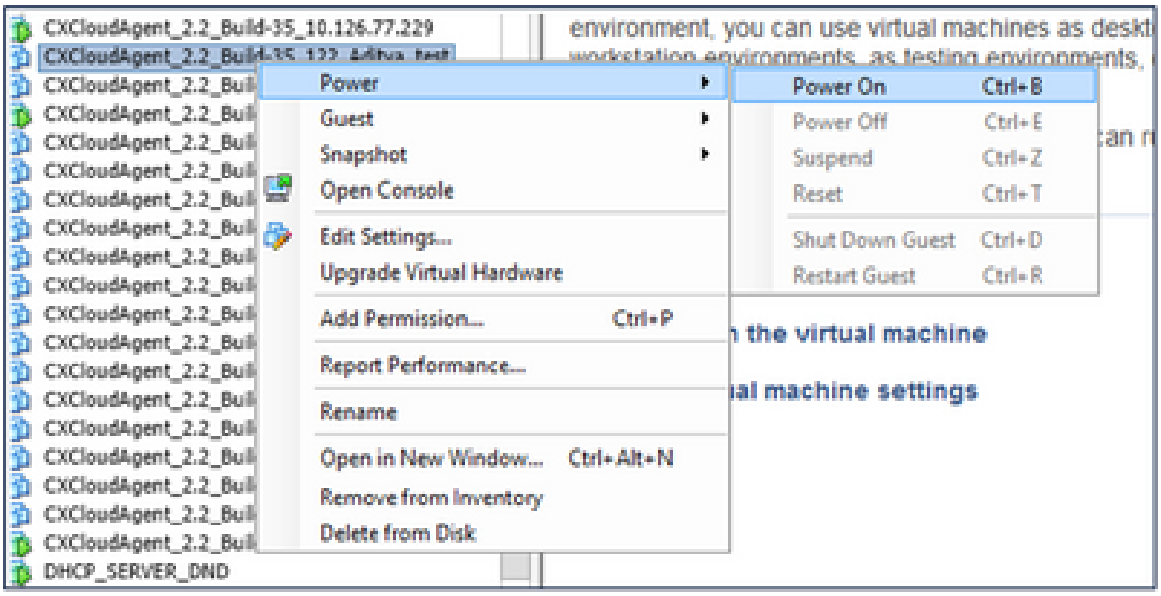
確認ウィンドウ

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 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cxcroot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。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、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、Iot 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 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。 · 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種類を含む、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つのカテゴリを含む。 ・ 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。
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 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。

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。