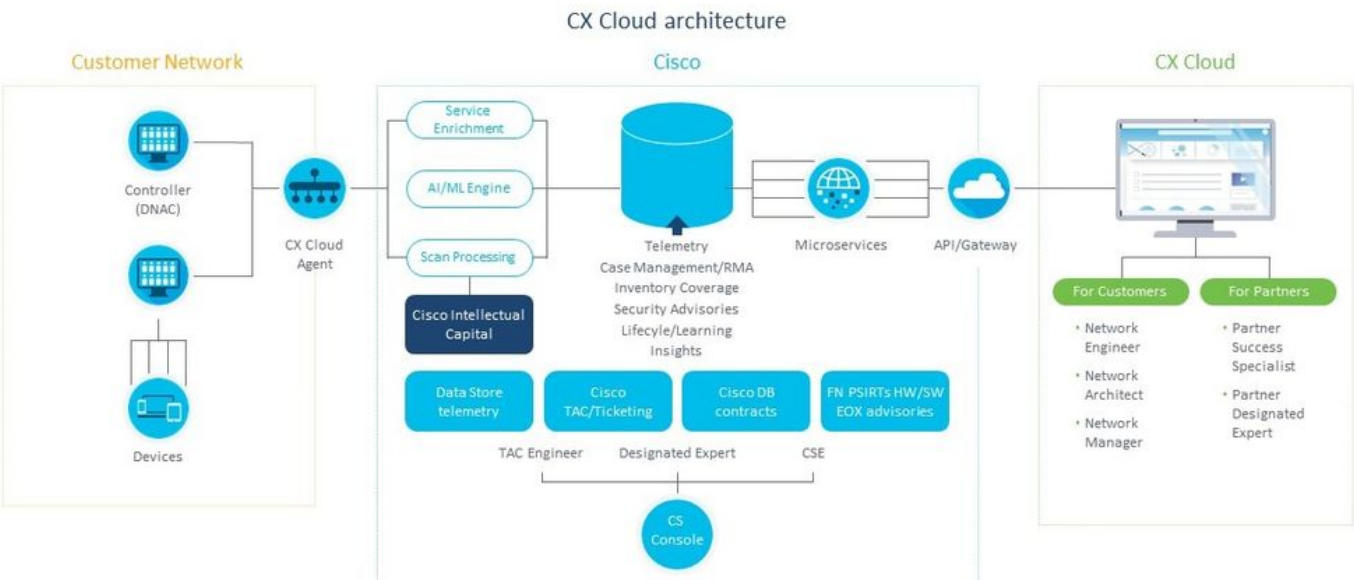
CX Cloud Agent Overview v2.0

Contents

Introduction

This document describes Cisco's Customer Experience (CX) Cloud Agent. Cisco's (CX) Cloud Agent is a modernized modular on-premise software platform that hosts lightweight containerized microservice capabilities. These capabilities can be installed, configured, and managed on customer premise from the cloud. CX Cloud Agent expedites the monetization of new offers, scales capabilities, and helps to develop next-generation services driven by big data, analytics, automation, Machine Learning/Artificial Intelligence (ML/AI), and streaming.

> **Note**: This guide is intended for CX Cloud Agent v2.0 users. Please refer to the Cisco CX Cloud Agent for other related information.



CX Cloud Agent Architecture

> **Note**: Images (and the content within) in this guide are for reference purpose only. Actual content can vary.

Prerequisites

CX Cloud Agent runs as a Virtual Machine (VM) and is available for download as an Open Virtual Appliance (OVA) or a Virtual Hard Disk (VHD).

Requirements to deploy:

- Any of these hypervisors: VMWare ESXi version 5.5 or laterOracle Virtual Box 5.2.30Windows Hypervisor version 2012 to 2016
- The hypervisor can host a VM which requires: 8 Core CPU16 GB Memory/RAM200GB Disk

Space
- For customers that use designated Cisco US data centers as the primary data region to store CX Cloud data:
  The CX Cloud Agent must be able to connect to the servers shown here, using the FQDN, and using HTTPS on TCP port 443:
  FQDN: agent.us.csco.cloud
  FQDN: ng.acs.agent.us.csco.cloud
  FQDN: cloudsso.cisco.com
  FQDN: api-cx.cisco.com
- For customers that use designated Cisco Europe data centers as the primary data region to store CX Cloud data:
  The CX Cloud Agent must be able to connect to both of the servers shown here, using the FQDN, and using HTTPS on TCP port 443:
  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
- For customers that use designated Cisco Asia Pacific data centers as the primary data region to store CX Cloud data:
  The CX Cloud Agent must be able to connect to both of the servers shown here, using the FQDN, and using HTTPS on TCP port 443:
  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

- For customers who use the designated Cisco Europe and Cisco Asia Pacific data centers as their primary data region, connectivity to FQDN: agent.us.csco.cloud is required only for registering the CX Cloud Agent with CX Cloud during initial setup. After the CX Cloud Agent is successfully registered with CX Cloud, this connection is no longer required.
- For local management of the CX Cloud Agent, port 22 must be accessible.

Other notes on CX Cloud Agent:

- An IP will automatically be detected if Dynamic Host Configuration Protocol (DHCP) is enabled in the VM environment. Otherwise, a free IPv4 address, Subnet mask, Default Gateway IP address, and DNS server IP address must be available.
- Only IPv4 is supported, not IPv6.
- The certified single node and High Availability (HA) Cluster Cisco Digital Network Architecture (DNA) Center versions from 1.2.8 to 1.3.3.9 and 2.1.2.0 to 2.2.3.5 are required.
- If the network has SSL interception, permit-list CX Cloud Agent’s IP address.

Critical Domains Access

To start the CX Cloud journey, users require access to these domains.

Major Domains	Other Domains

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

Domains specific to region:

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	agent.us.csco.cloud	agent.us.csco.cloud
ng.acs.agent.us.csco.cloud	agent.emea.csco.cloud ng.acs.agent.emea.csco.cloud	agent.apjc.csco.cloud ng.acs.agent.apjc.csco.cloud

Prerequistes to Upgrade to CX Cloud Agent v2.0

The prerequisites outlined in this section must be met prior to the upgrade to CX Cloud Agent v2.0.

1. Ensure that CX Cloud Agent v1.12.x and later must be installed prior to the initiation of the upgrade.
2. Perform these steps to configure the Domain Name Server if it is not already configured: Log in to the Command Line Interface (CLI) console of the CX Cloud Agent Virtual Machine.Execute the *cxcli agent configureDNS* command.Enter the DNS IP address.Click Exit.
3. Ensure that the customer's network allows the domain names in Critical Domain Access to complete the Cloud Agent re-registration during migration. CX Cloud Agent must be able to reach these domains and also the domains must be resolvable from DNS server. Contact the Network Team if any domain is unreachable.
4. Take a Cloud Agent VM snapshot before initiating v2.0 upgrade (proper access required).

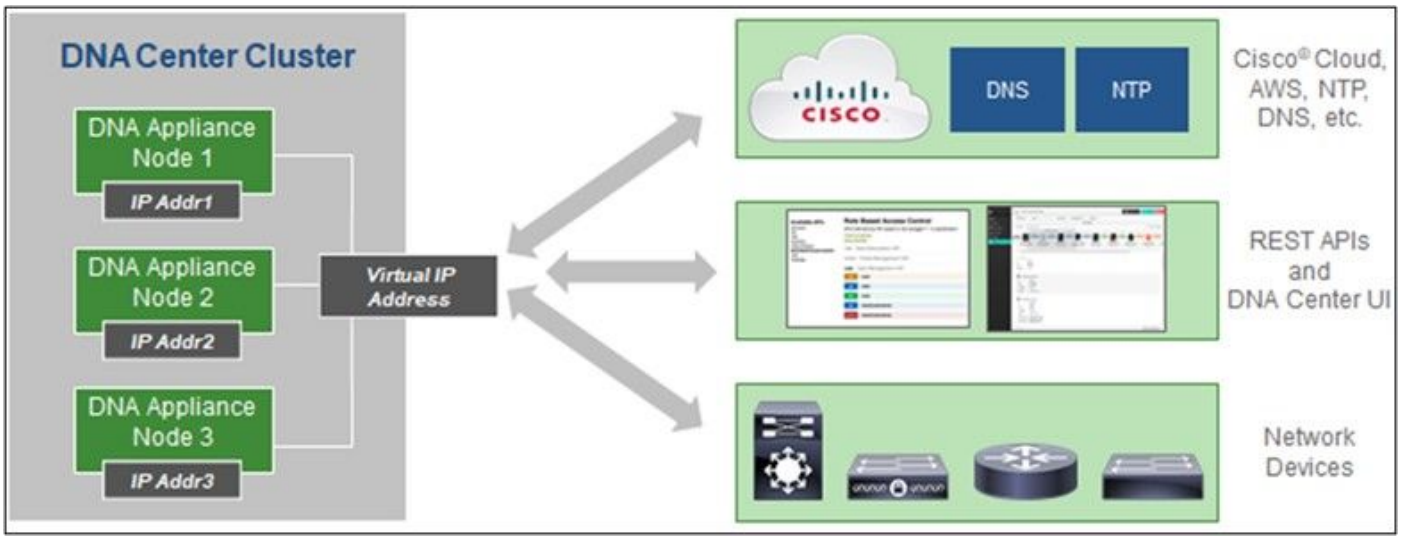
   Note: Versions prior to 1.10 must upgrade to v1.10 first, followed by incremental upgrades to v1.12.x, and then to v2.0. Users can upgrade from Admin Settings > Data Sources in CX Cloud portal. Click View Update to complete the upgrade.

Following conditions to be met for successful setup:

1. List of DNACs and their credentials
2. DNAC user with **Admin** or **Observer** role access
3. Virtual IP address or Standalone/Physical IP address for DNAC cluster
4. Successful reachability between Cloud Agent and DNAC
5. DNAC must have minimum 1 (one) managed device

Cisco DNA Center Certified Versions

Certified single node and HA Cluster Cisco DNA Center versions are from 1.2.8 to 1.3.3.9 and 2.1.2.0 to 2.2.3.5.



Multi-Node HA Cluster Cisco DNA Center

Supported Browsers

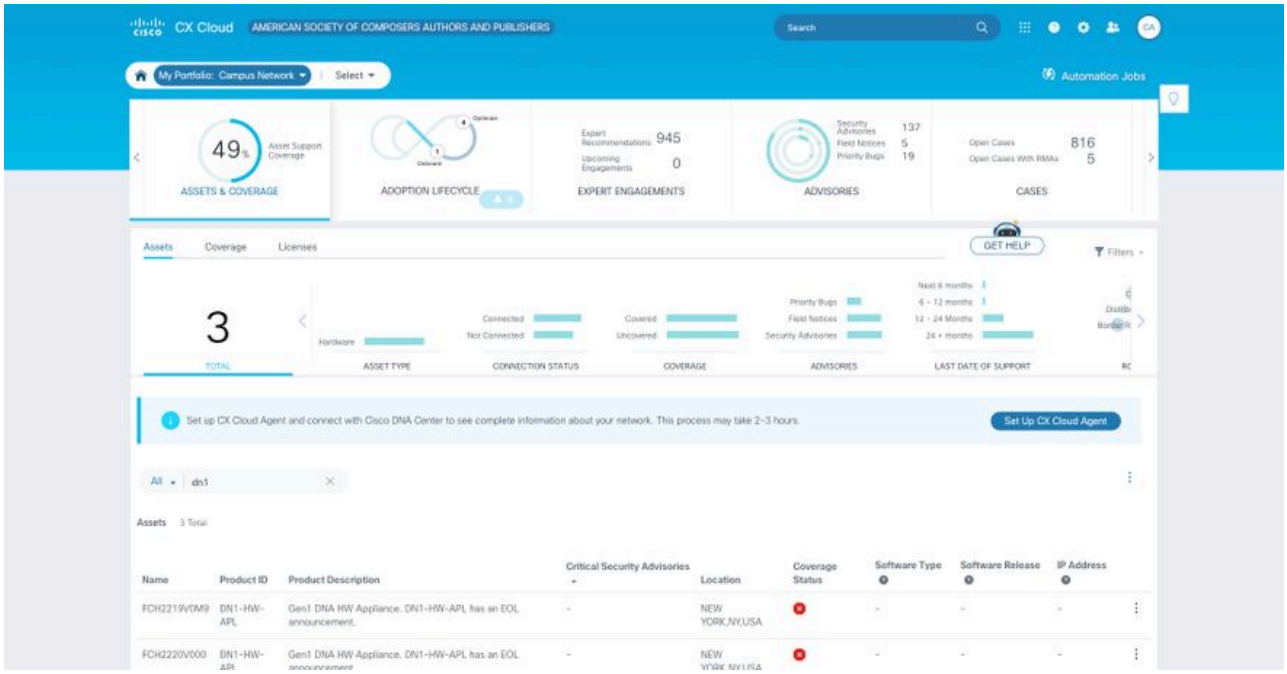
For the best experience on Cisco.com, we recommend the latest official release of the these browsers:

- Google Chrome
- Microsoft Edge
- Mozilla Firefox

Deploy CX Cloud Agent

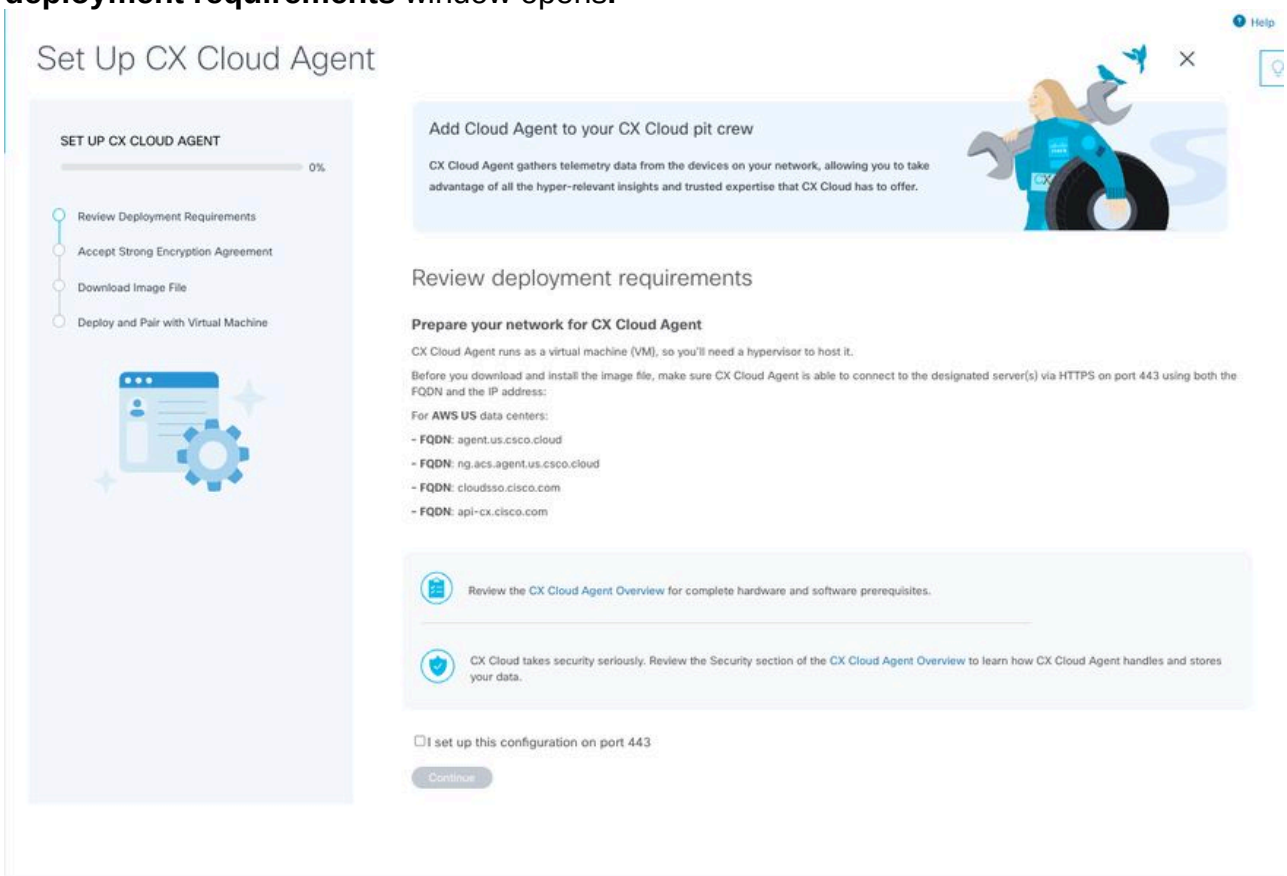
To deploy CX Cloud Agent:

1. Click cx.cisco.com to log in to CX Cloud.
2. Select Campus Network and navigate to ASSETS & COVERAGE tile.



Home page

3. Click **Set Up CX Cloud Agent** in the banner. The **Set Up CX Cloud Agent** - **Review deployment requirements** window opens**.**

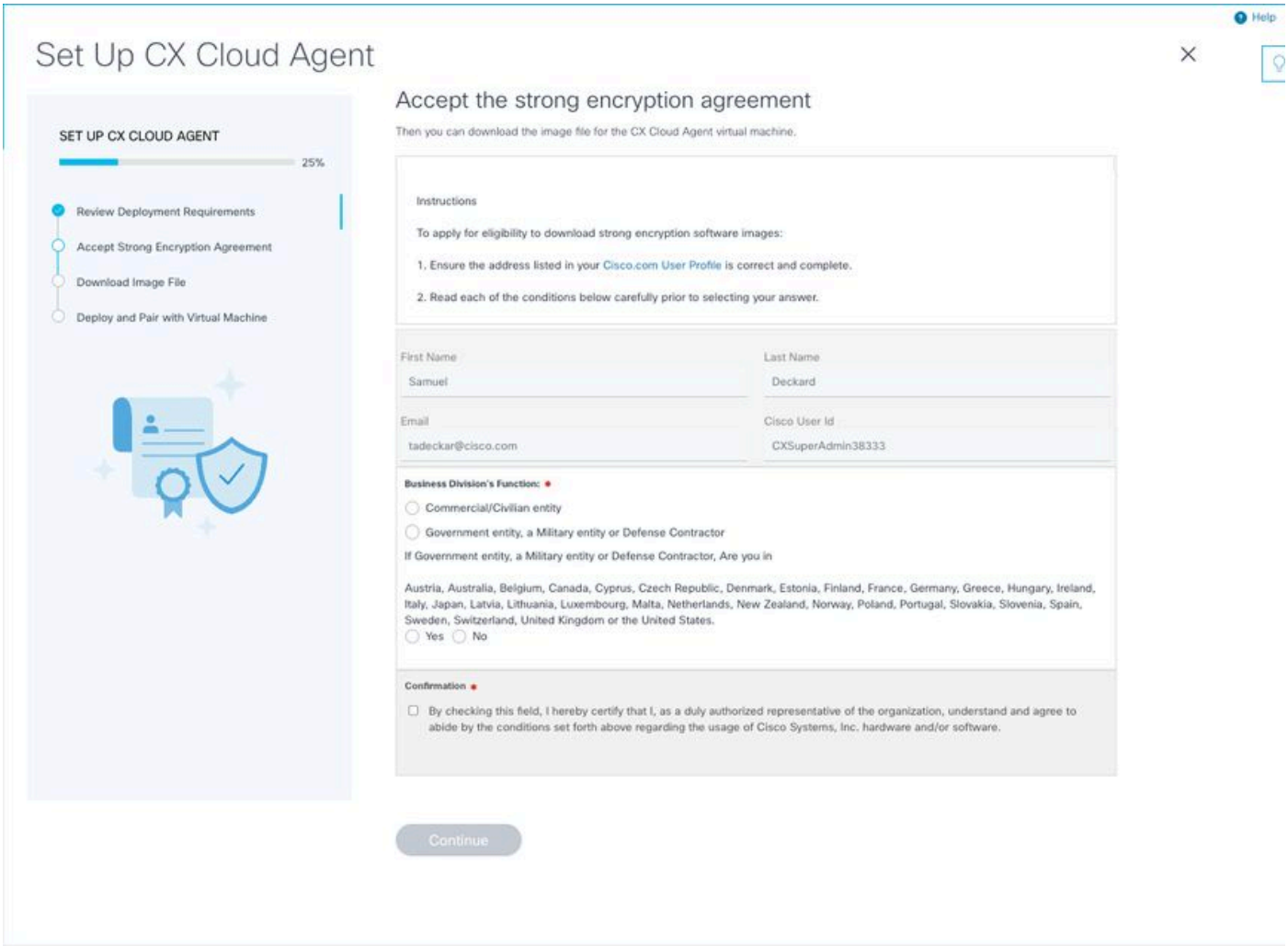


Review deployment requirements

4. Read the prerequisites in **Review deployment requirements** and select the check box for **I set up this configuration on port 443**.

Note: Images (and the content within) in this guide are for reference purpose only. Actual content can vary.

5. Click **Continue**. The **Set Up CX Cloud Agent - Accept the strong encryption agreement** window opens.



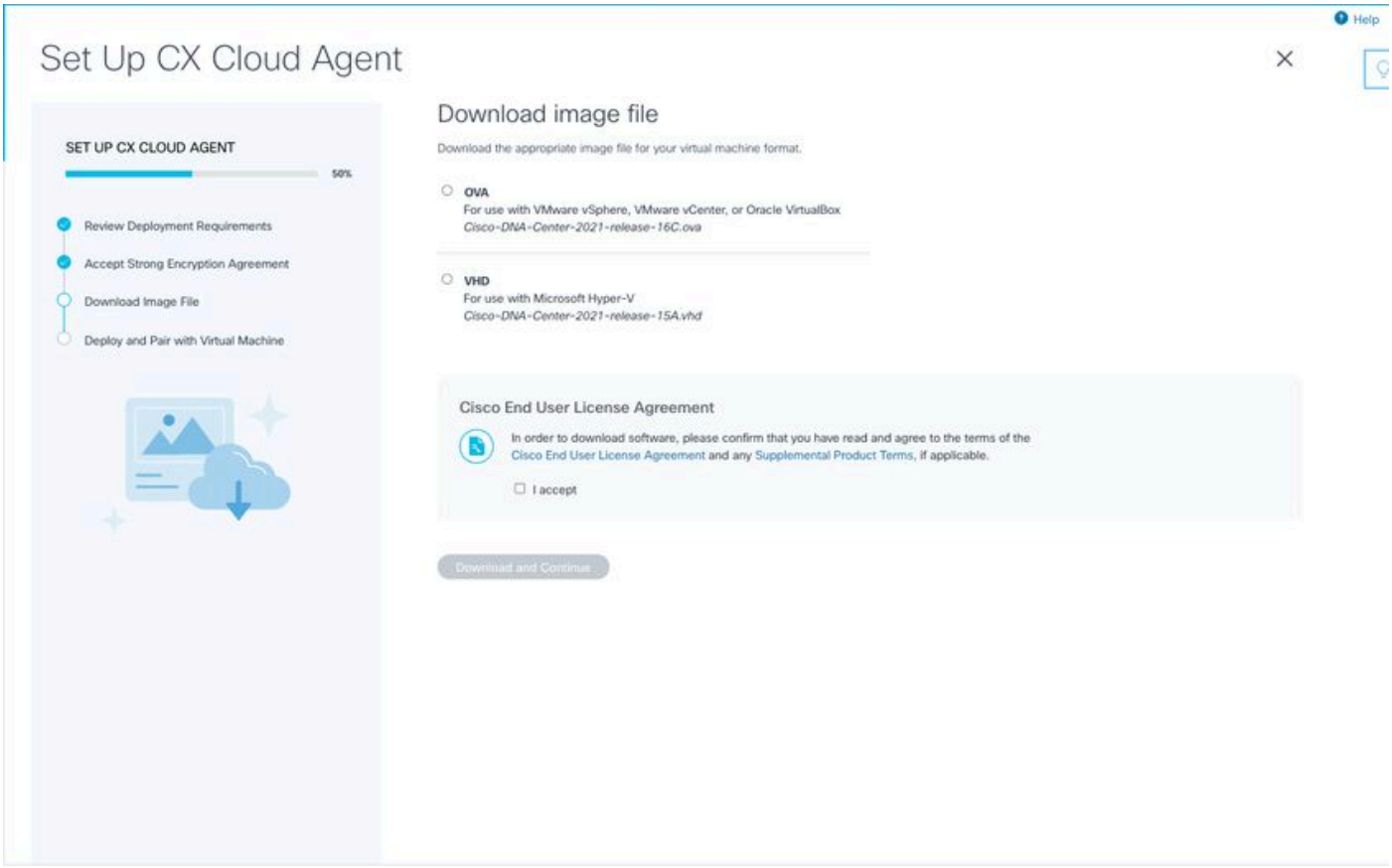
Encryption Agreement

6. Verify the pre-populated information in the **First Name,Last Name,E-mail**, and **CCO User Id** fields.

7. Select the appropriate Business division's function.

8. Select the Confirmation check box to agree to the usage conditions.

9. Click **Continue**. The **Set Up CX Cloud Agent - Download image file** window opens.



Download Image

10. Select the appropriate file format to download the image file required for installation.

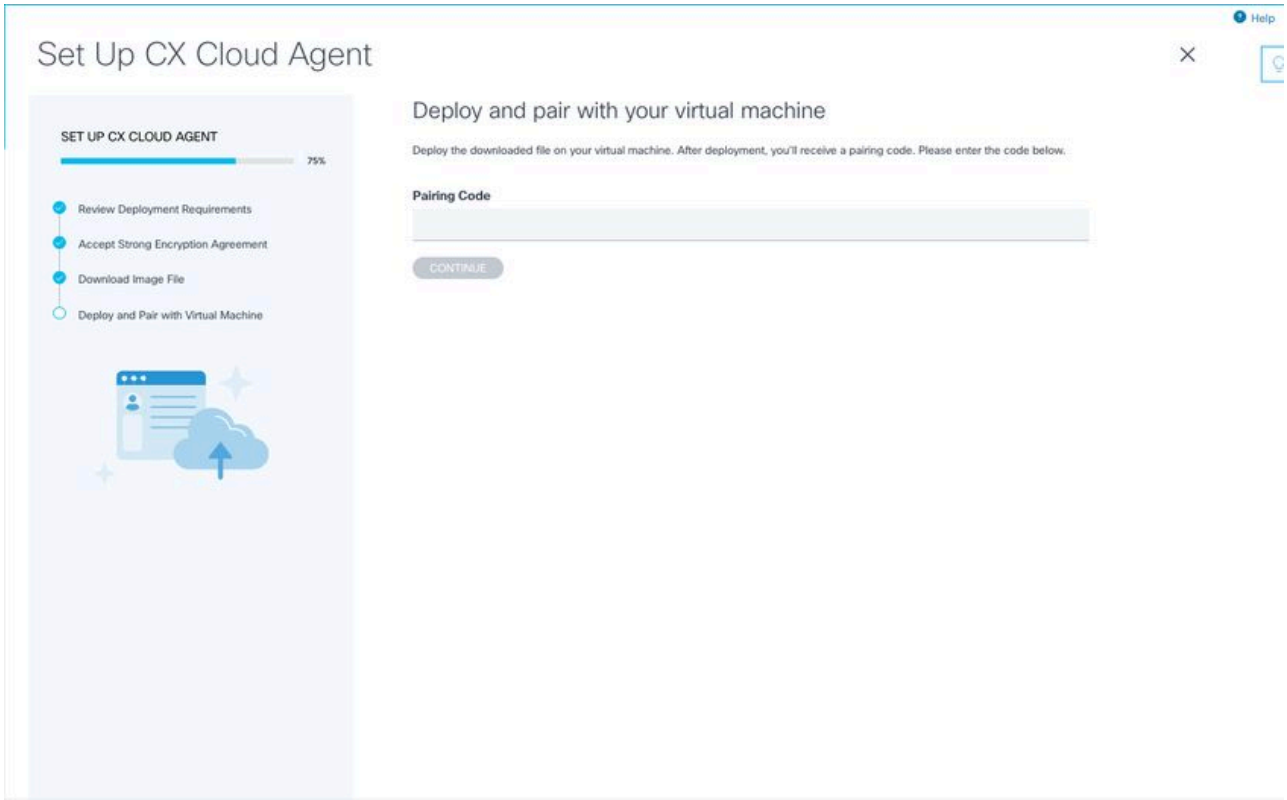
11. Select the **I accept** check box to agree to the Cisco End User License Agreement.

12. Click **Download and Continue**. The **Set Up CX Cloud Agent - Deploy and pair with your virtual machine** window opens.

13. Refer to Network Configuration for OVA installation and continue to the next section to install the CX Cloud Agent.

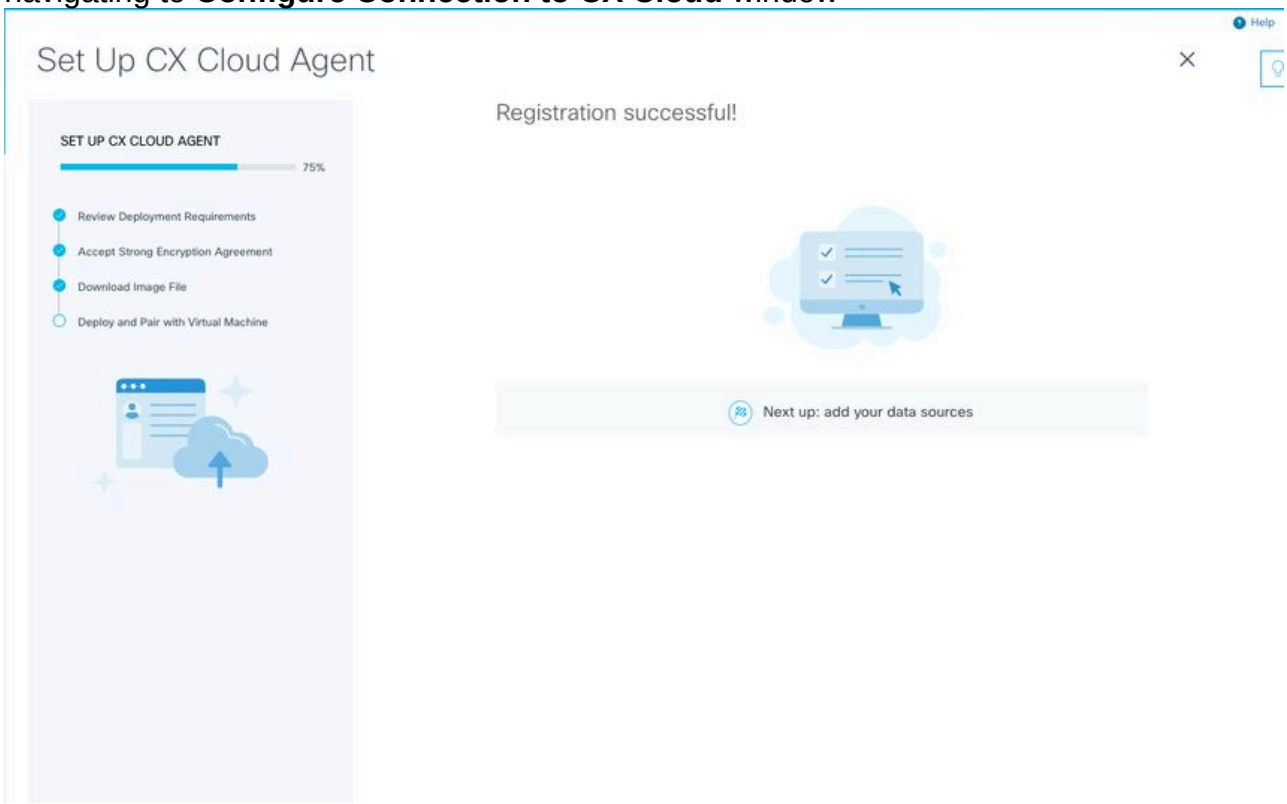
Connect CX Cloud Agent to CX Cloud

1. Enter the **Pairing Code** provided in the console dialog or Command Line Interface (CLI).

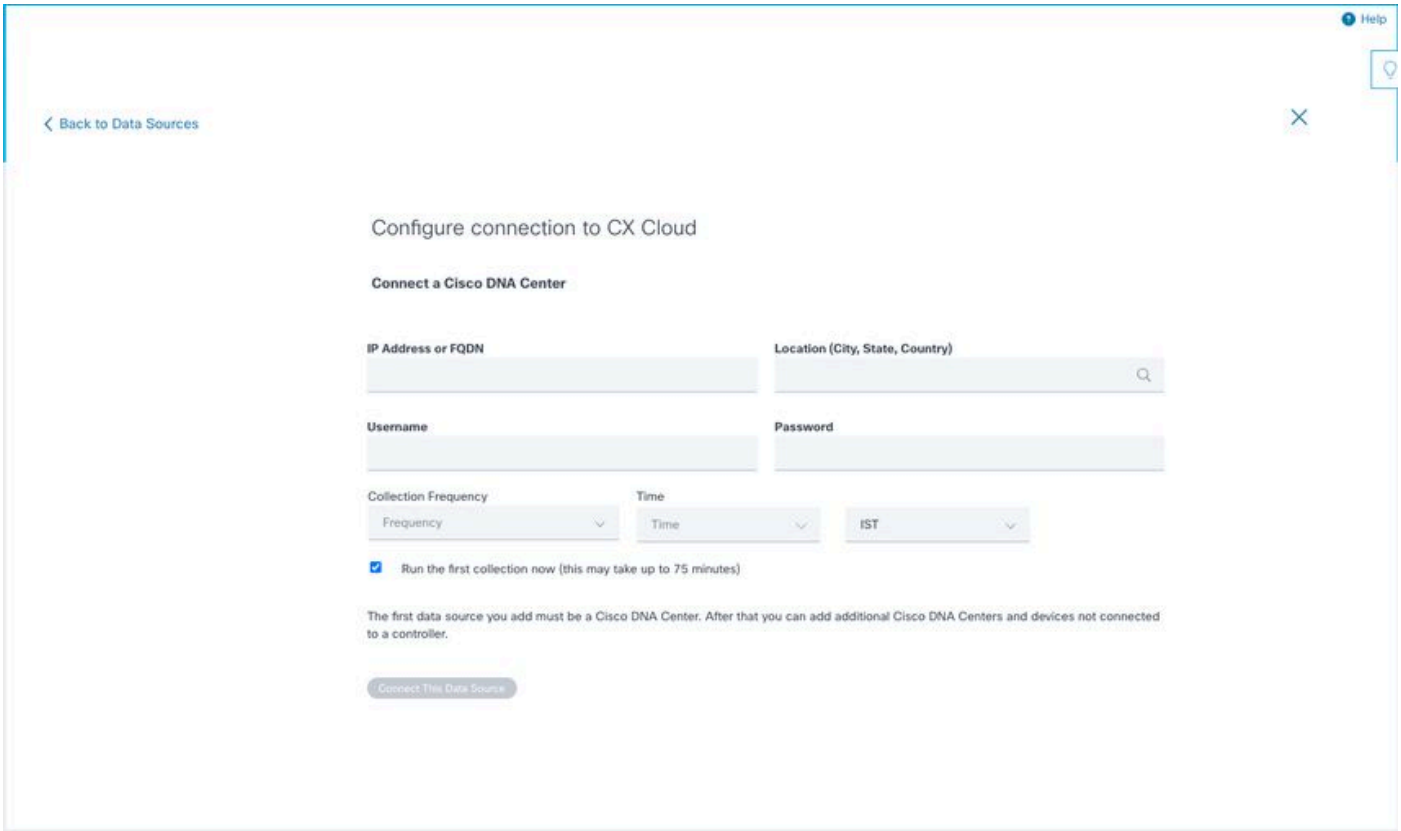


Pairing Code

2. Click **Continue** to register the CX Cloud Agent. The **Set Up CX Cloud Agent - Registration successful** window displays for few seconds before automatically navigating to **Configure Connection to CX Cloud** window

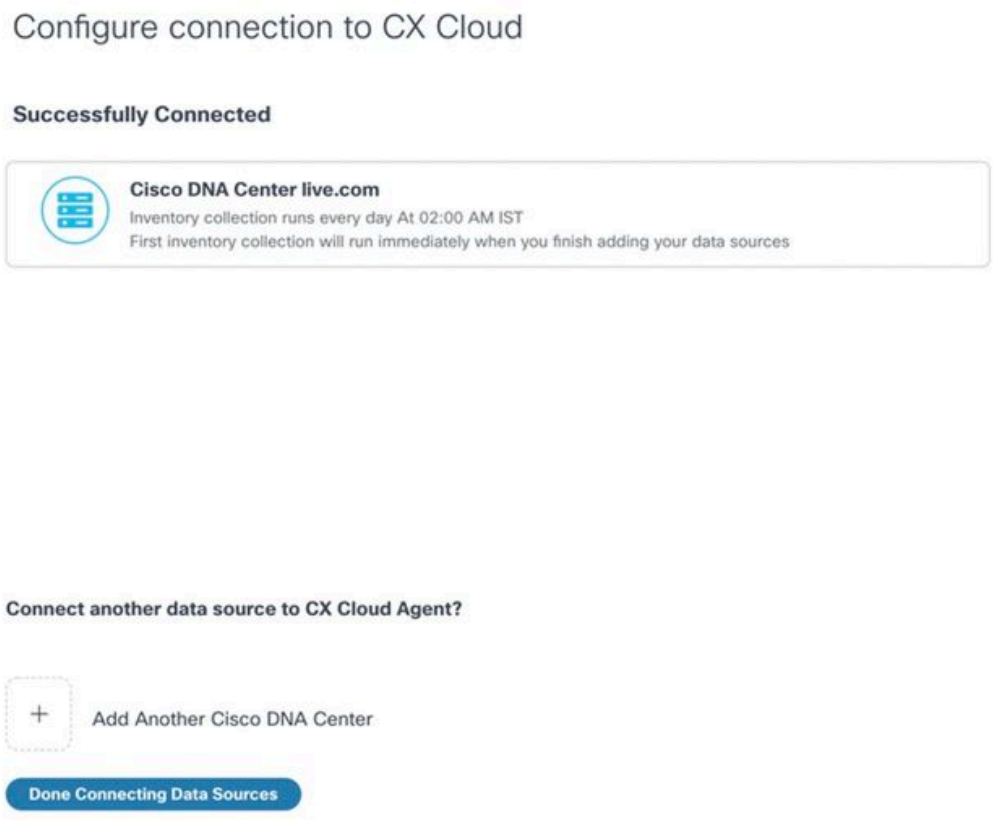


Registration Sucessful



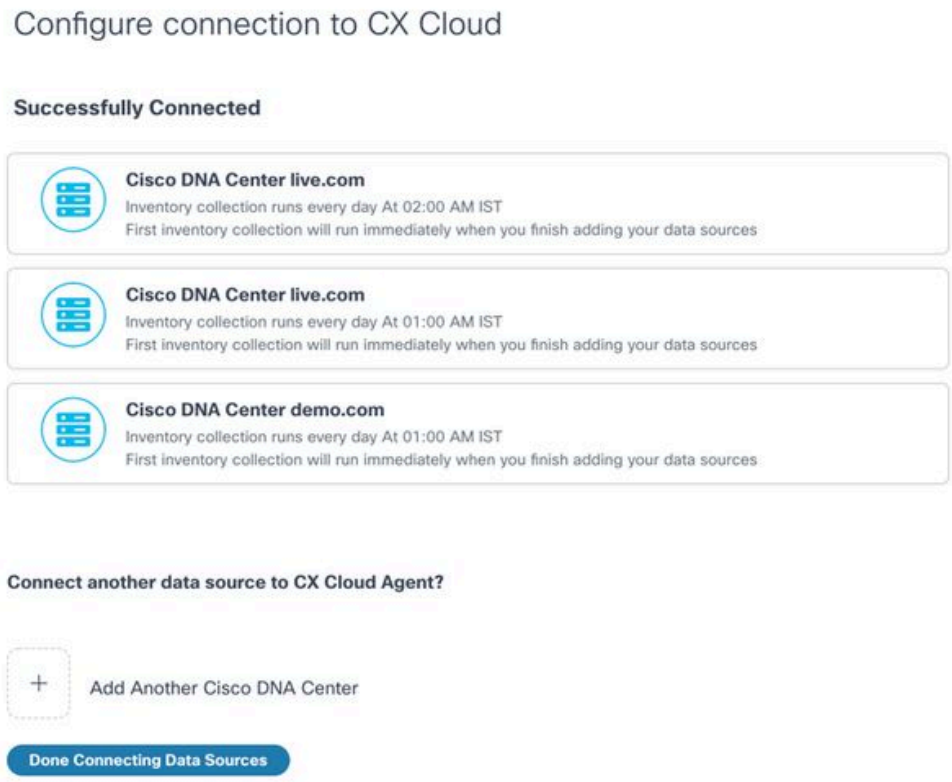
Configure Connection

3. Enter data and click **Connect This Data Source**. The confirmation message “Successfully Connected“ displays.



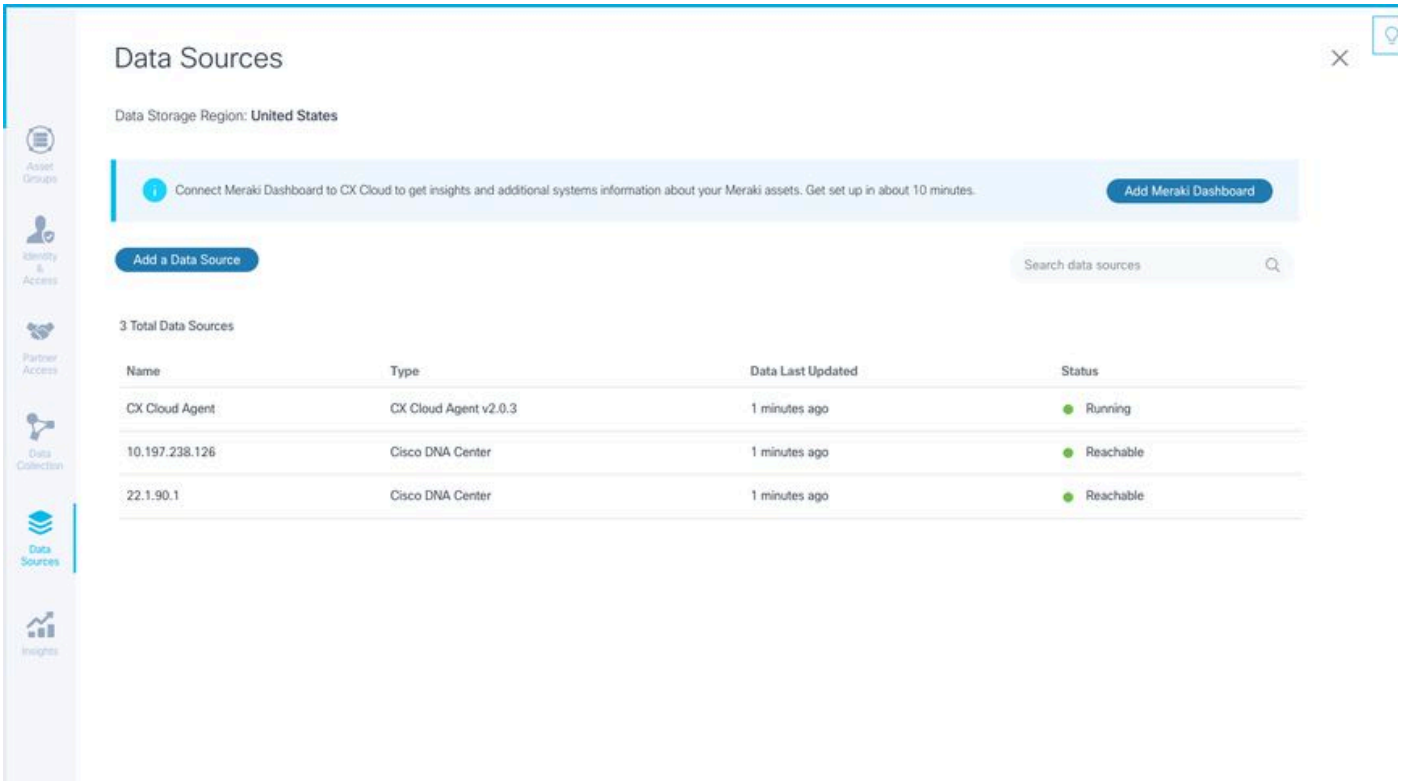
DNAC Added Successfully

Note: Click Add Another Cisco DNA Centerto add multiple DNACs.



Multiple DNACs Added

4. Click **Done Connecting Data Sources**. The **Data Sources** window opens.



Data Sources

Deployment and Network Configuration

Any of the these options can be selected to deploy the CX Cloud Agent:

- If you select VMware vSphere/vCenter Thick Client ESXi 5.5/6.0 go to Thick Client
- If you select VMware vSphere/vCenter Web Client ESXi 6.0 go to Web Client vSphere or Center
- If you select Oracle Virtual Box 5.2.30 go to Oracle VM
- If you select Microsoft Hyper-V go to Hyper-V

OVA Deployment

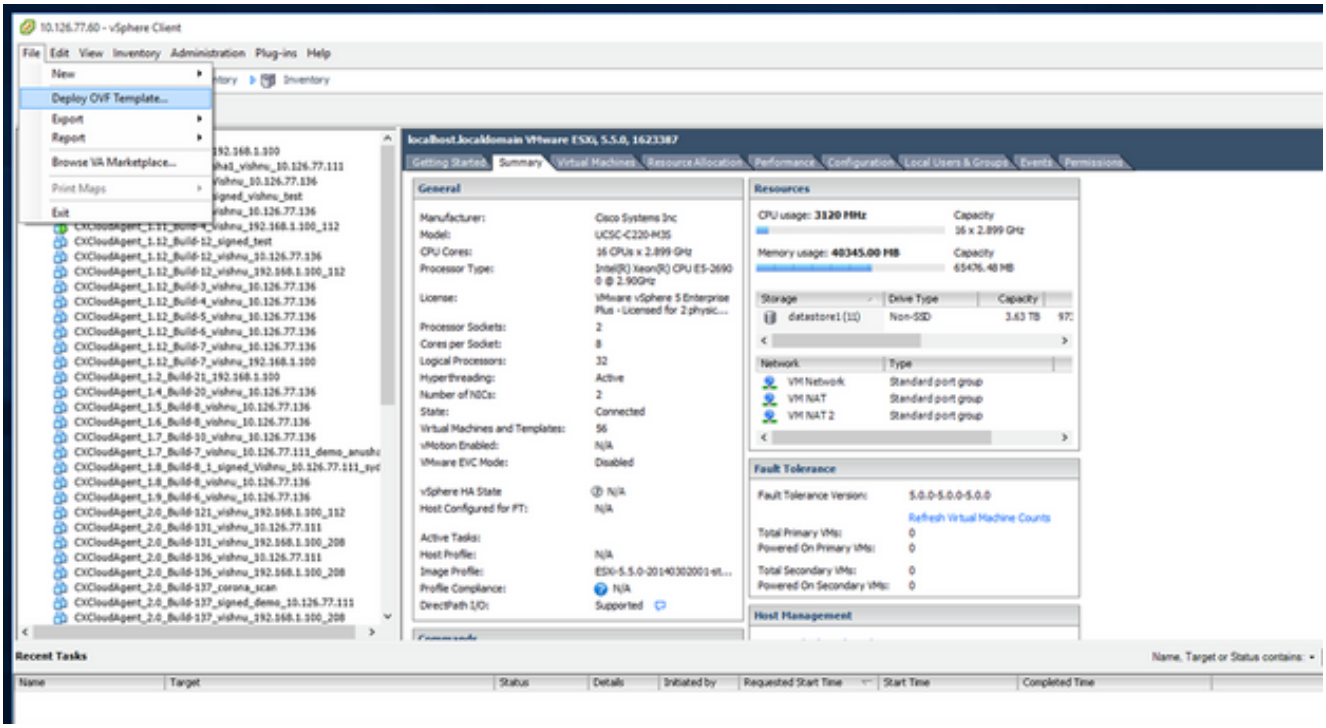
Thick Client ESXi 5.5/6.0 Installation

This client allows the deployment of CX Cloud Agent OVA by use of the vSphere thick client.

1. After you download the image, launch the VMware vSphere Client and log in.

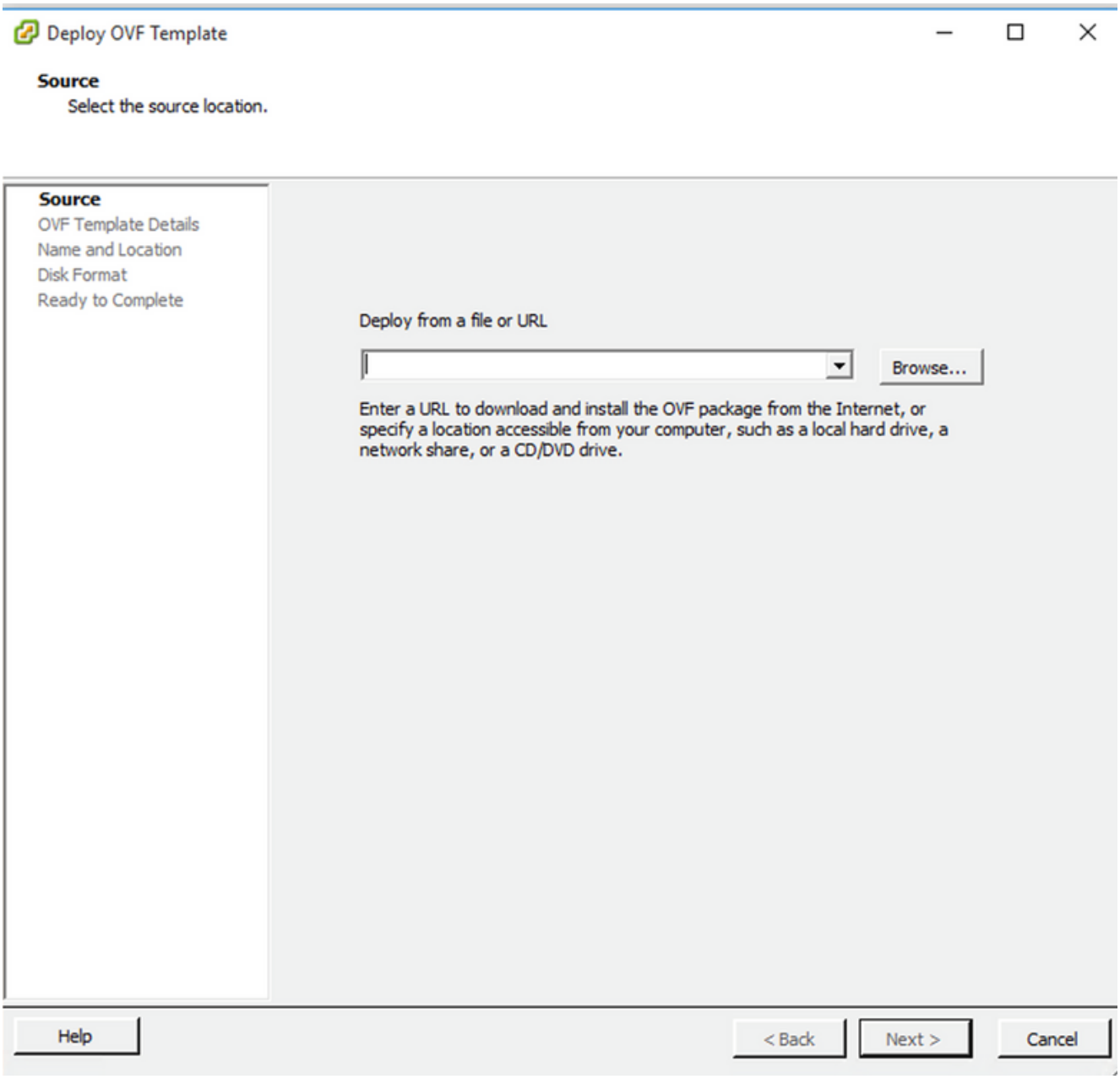
Login

2. Navigate to File > Deploy OVF Template.



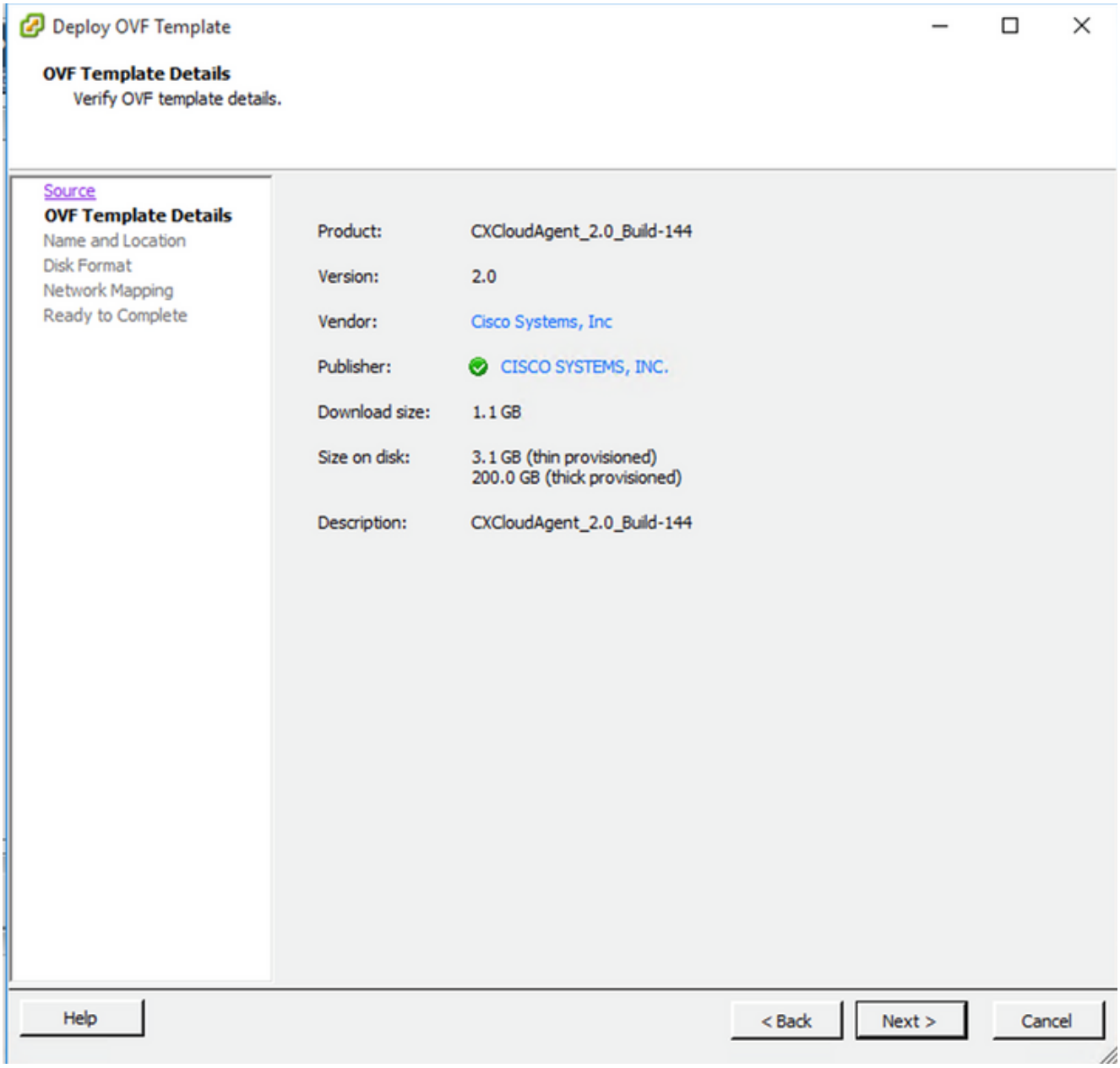
vSphere Client

3. Browse to select the OVA file and click Next.



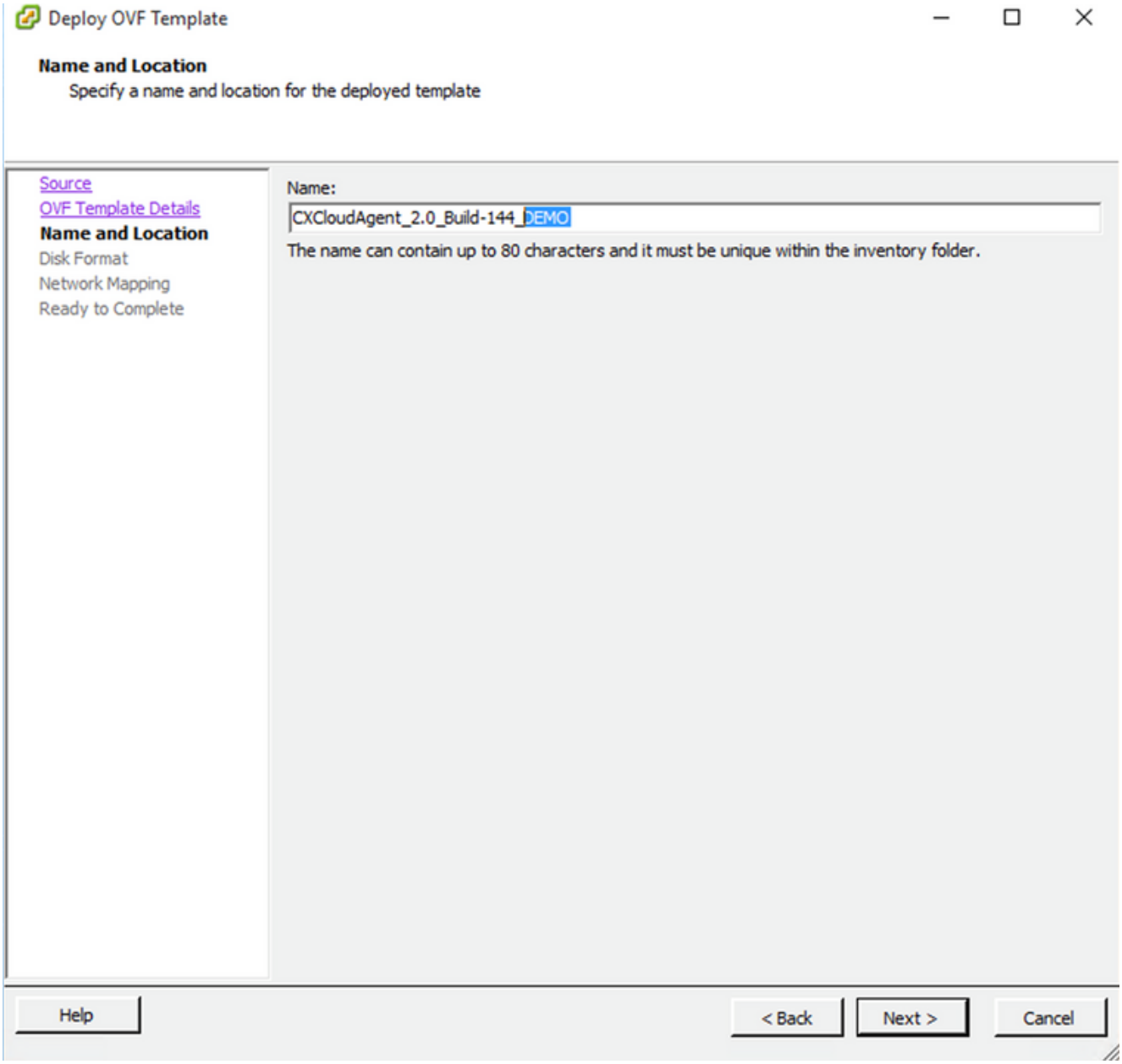
OVA Path

4. Verify the OVF Details and click Next.



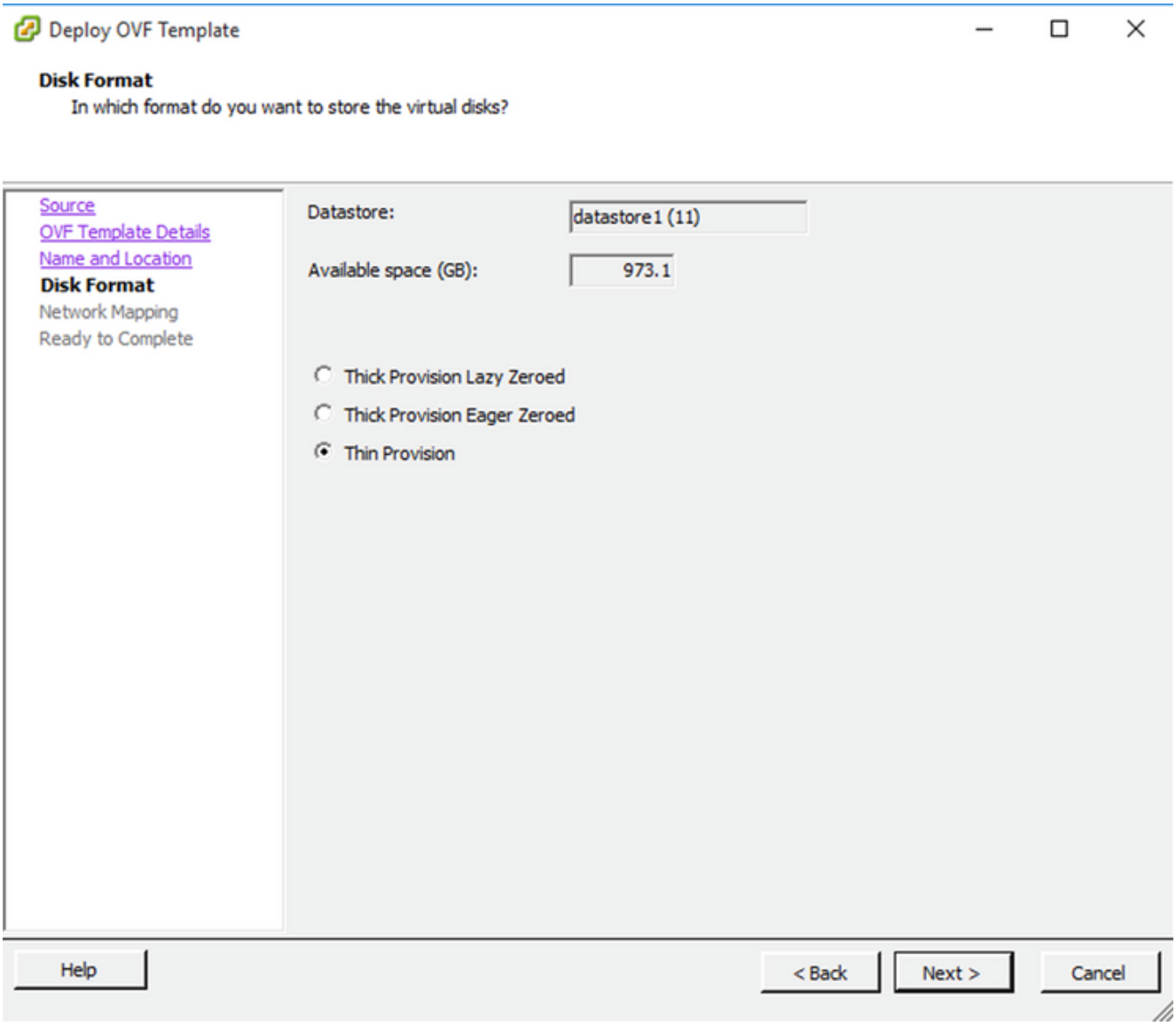
Template Details

5. Enter a Unique Name and click Next.



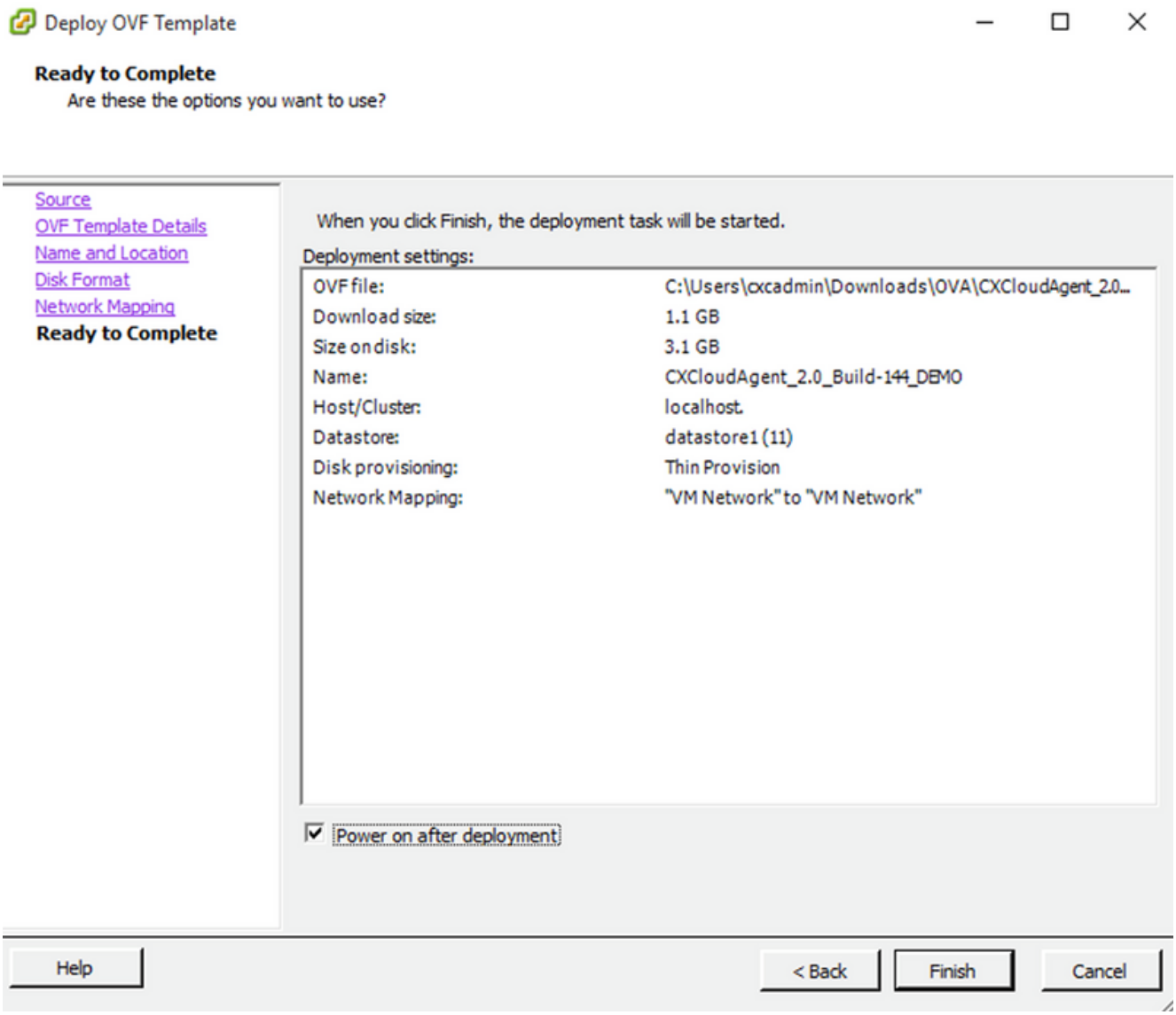
Name and Location

6. Select a Disk Format and click Next (Thin Provision is recommended).



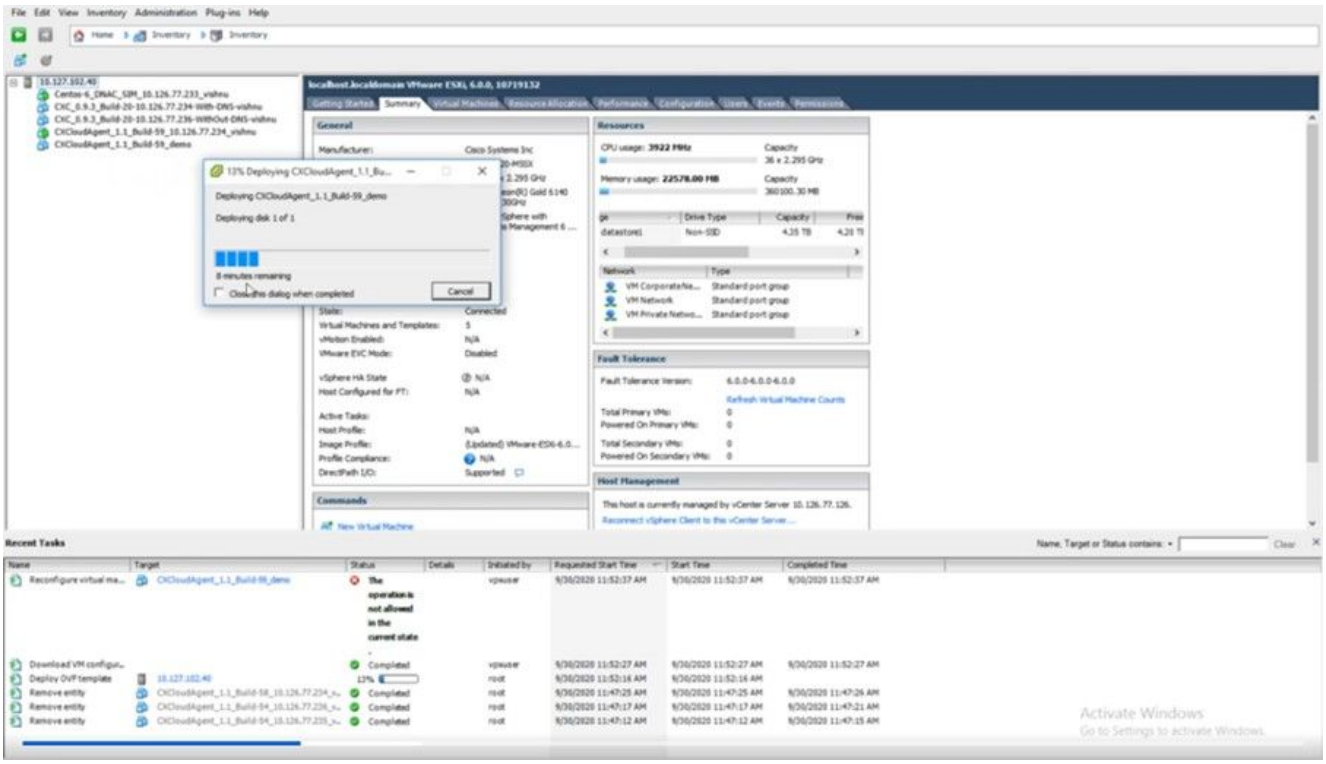
Disk Format

7. Select the Power on after deployment checkbox and click Finish.

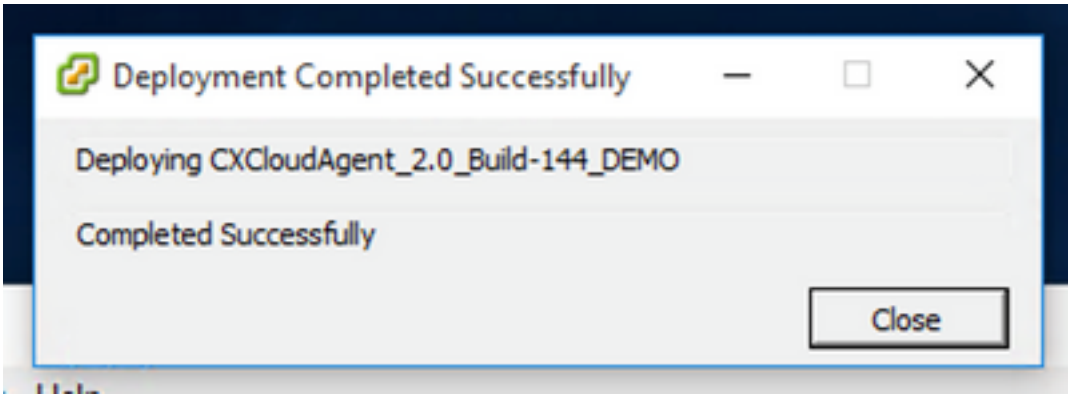


Ready to Complete

Deployment can take several minutes. Wait until you get a success message.



Deployment in Progress



Deployment Completed

8. Select the VM just deployed, open the console and go to **Network Configuration**.

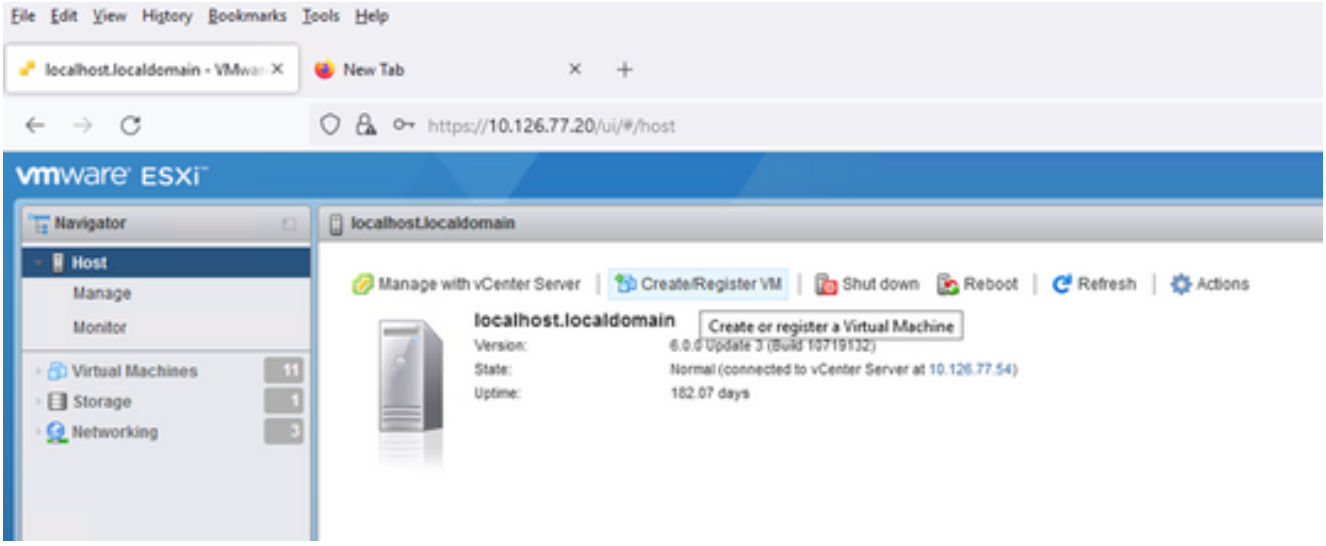
Web Client ESXi 6.0 Installation

This client deploys CX Cloud Agent OVA by use of the vSphere web.

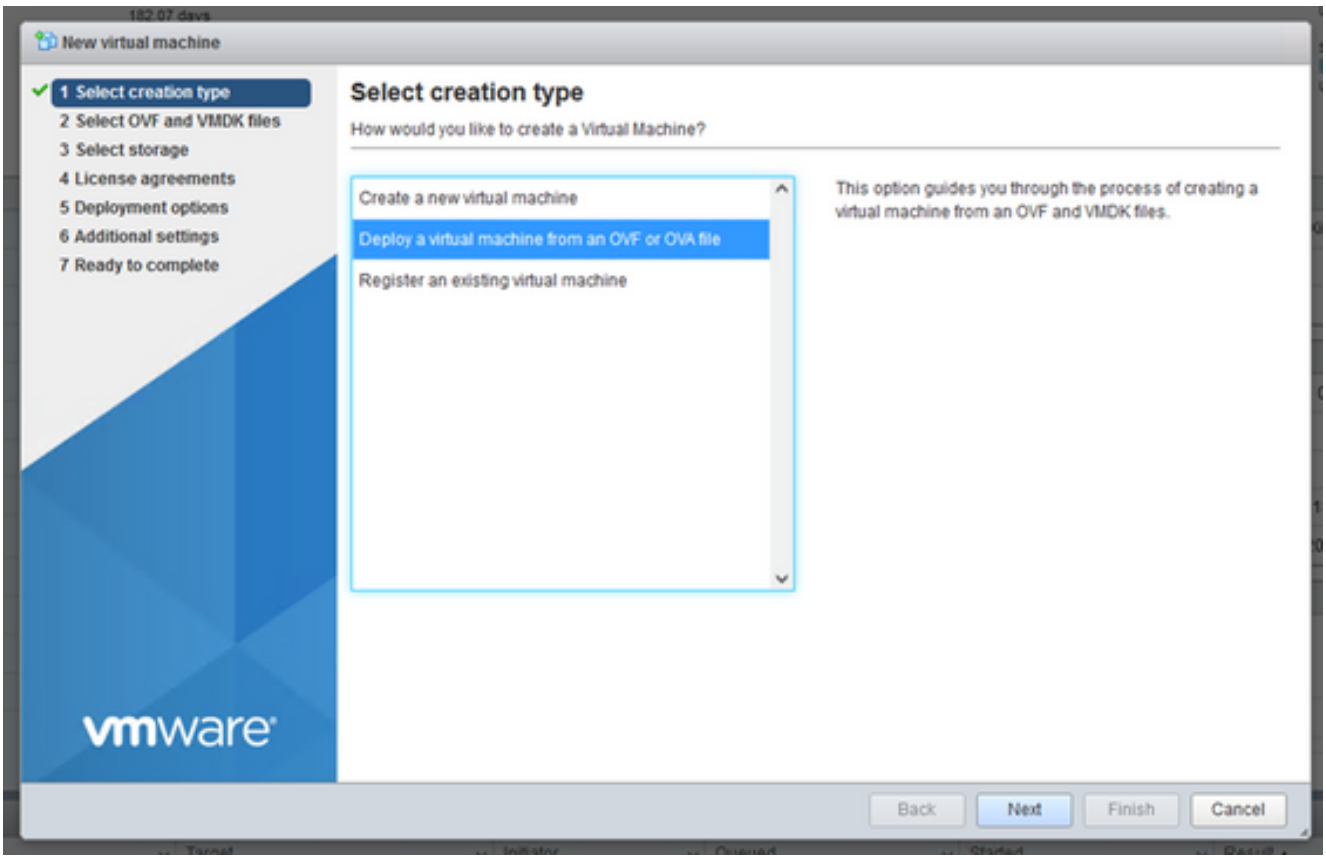
1. Log in to VMWare UI with the ESXi/hypervisor credentials used for deploying VM.

VMware ESXi Login

2. Select Virtual Machine > Create / Register VM.

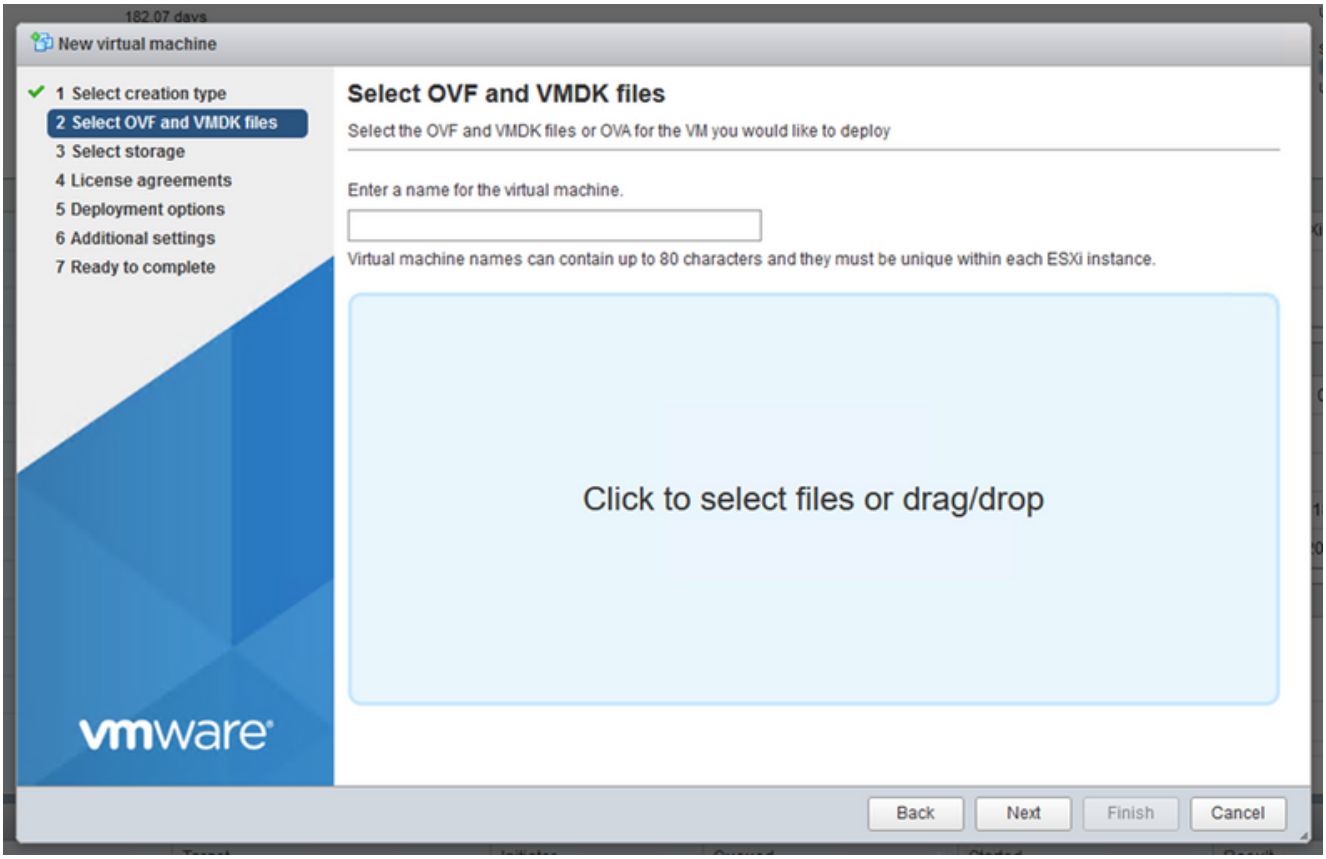


Create VM



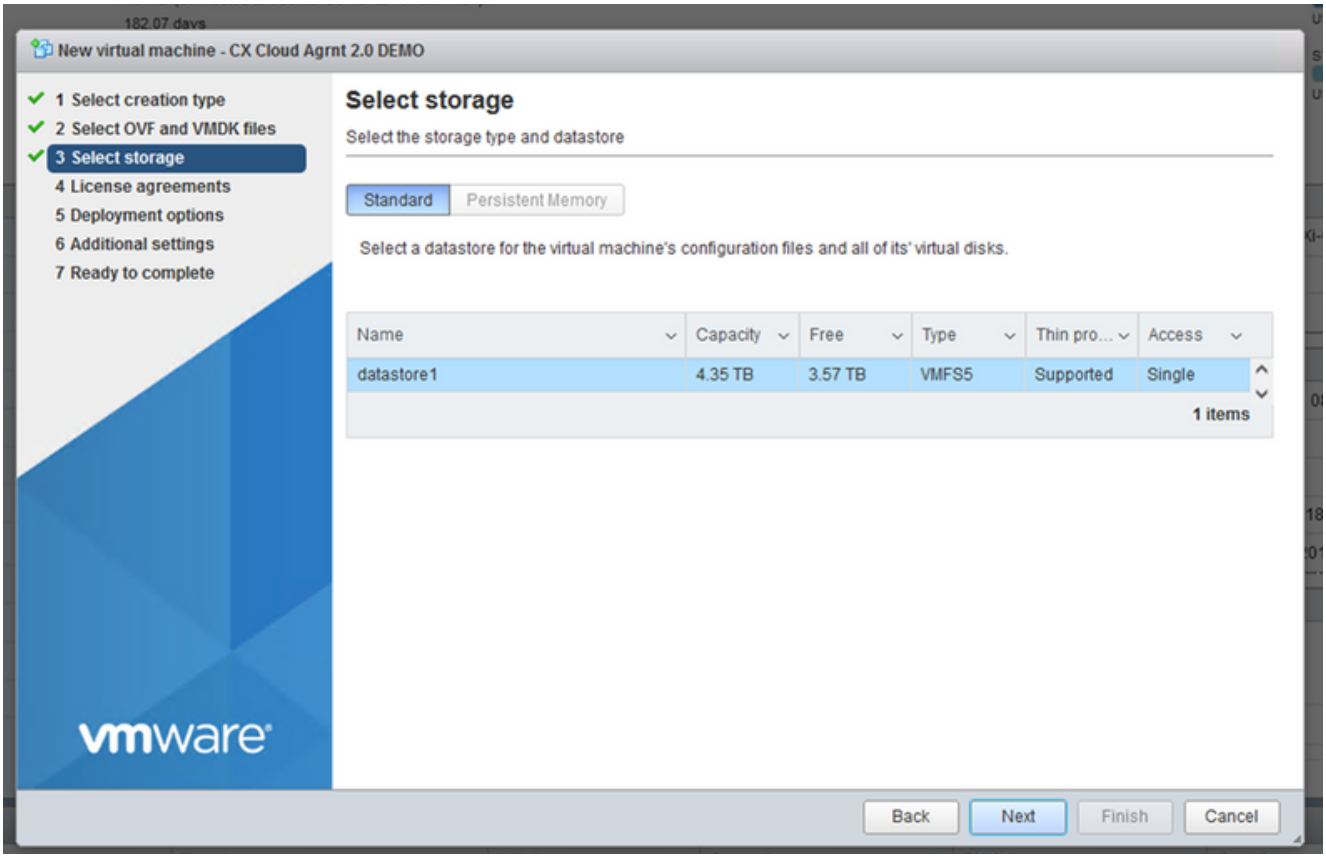
OVA Deployment

3. Select Deploy a virtual machine from an OVF or OVA file and click Next.
4. Enter the name of the VM, browse to select the file, or drag-and-drop the downloaded OVA file.
5. Click Next.

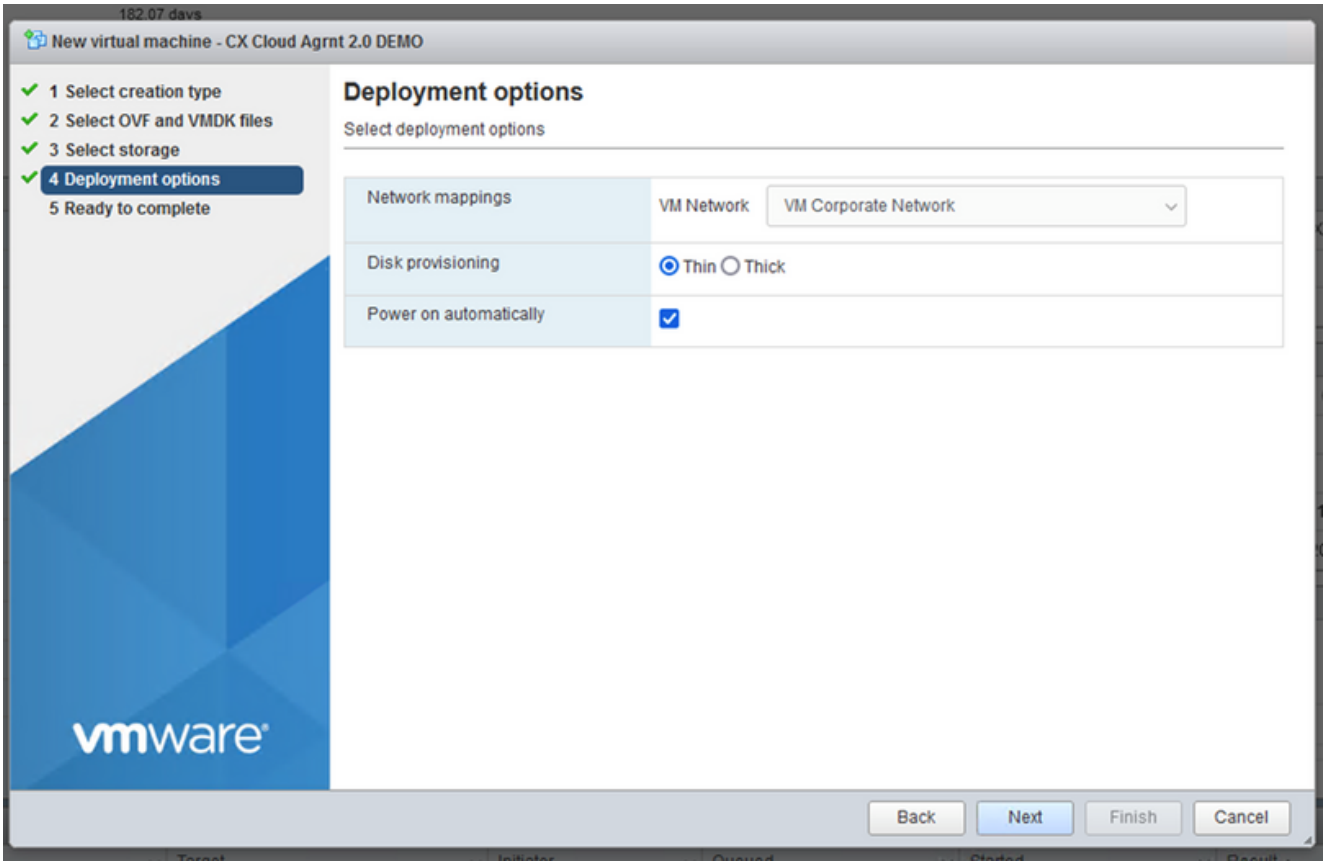


OVA Selection

6. Select Standard Storage and click Next.

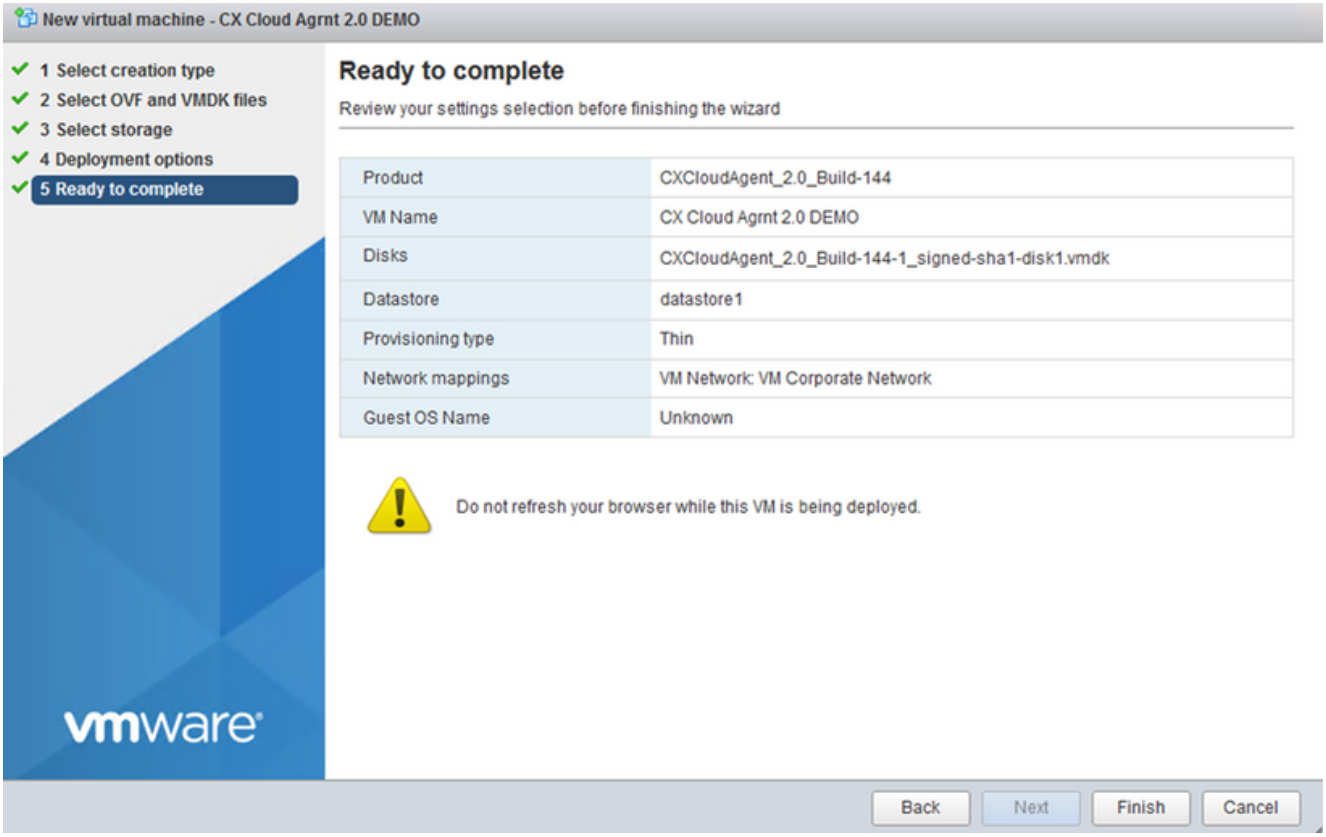


Select Storage

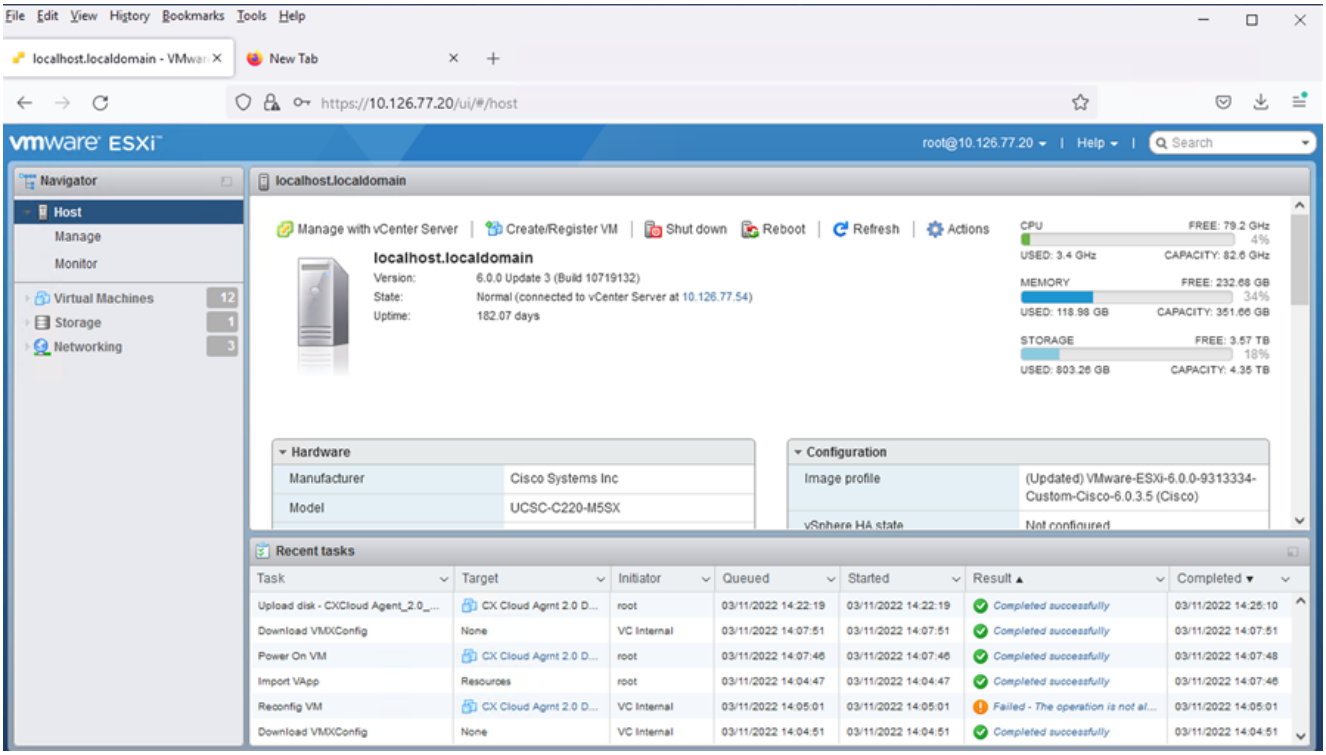


Deployment Options

7. Select the appropriate Deployment options and click Next.

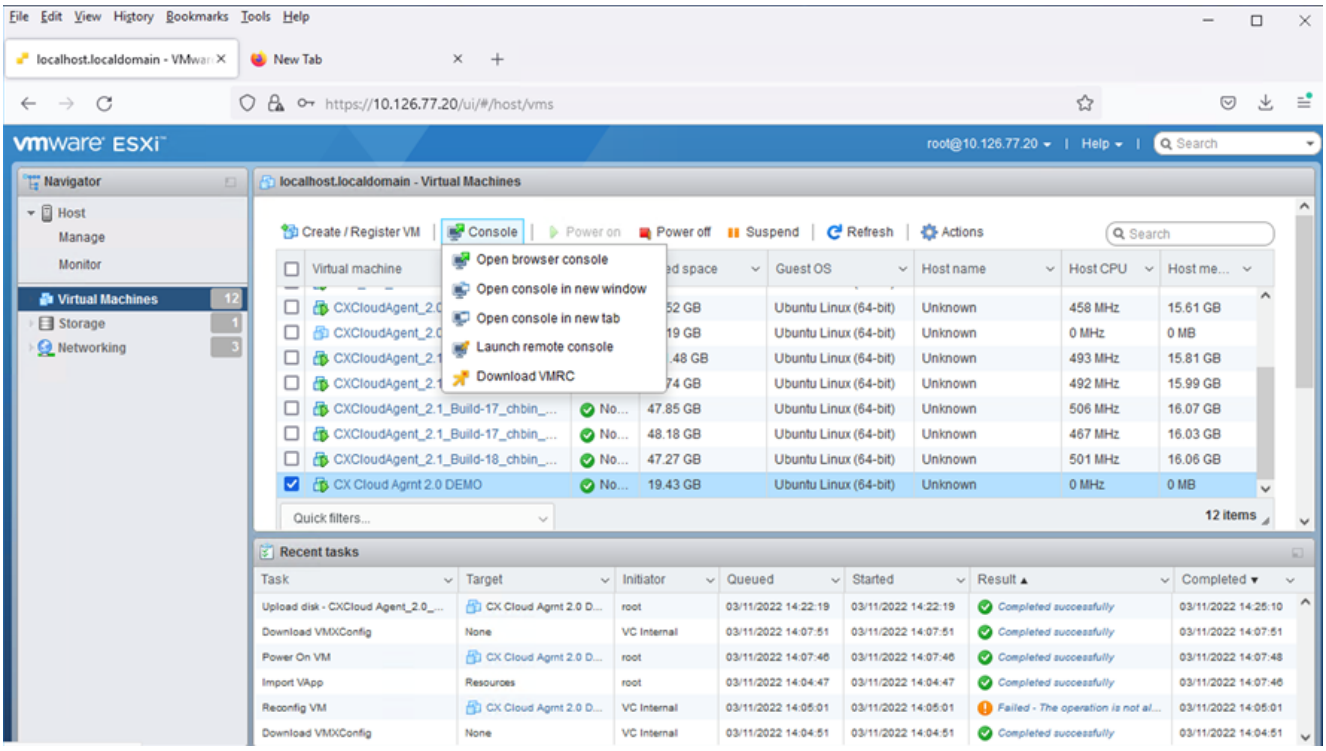


Ready to Complete



Successful Completion

8. Review the settings and click Finish.
9. Select the VM just deployed and select Console > Open browser console.



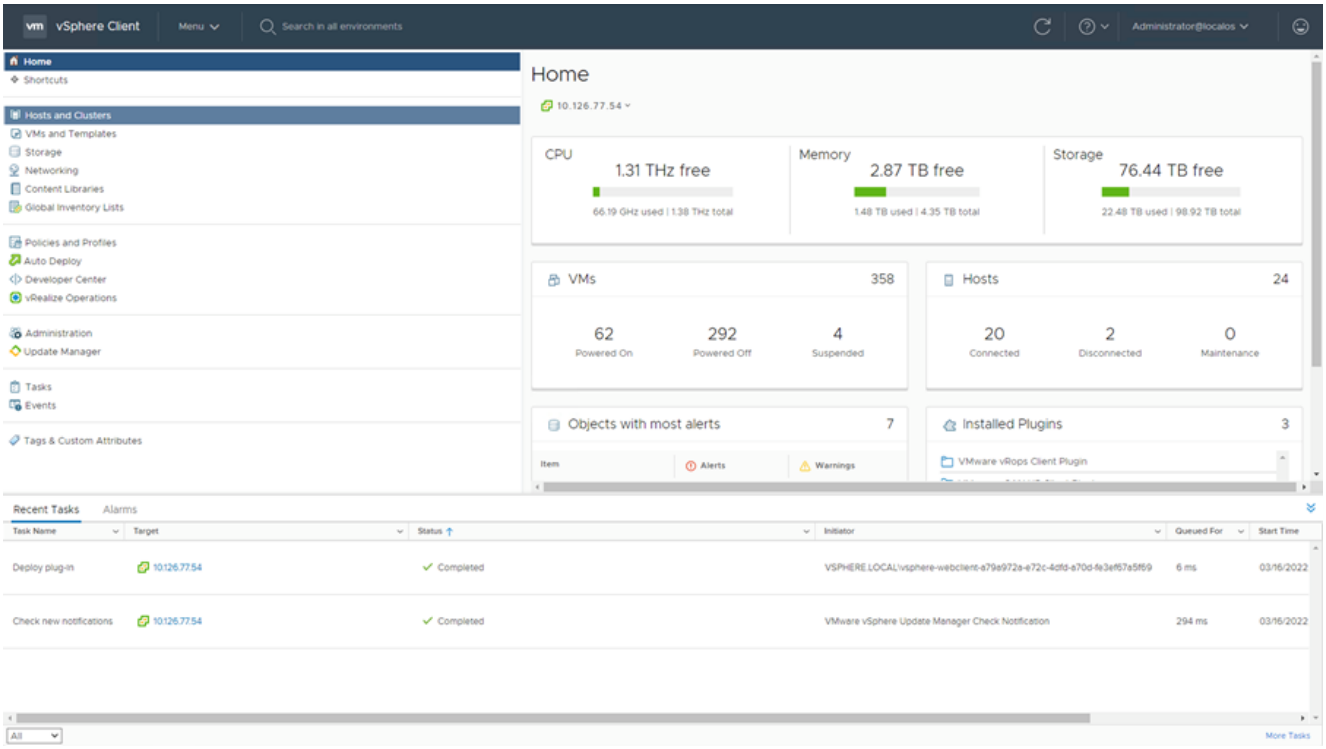
Open Console

10. Navigate to **Network Configuration**.

Web Client vCenter Installation

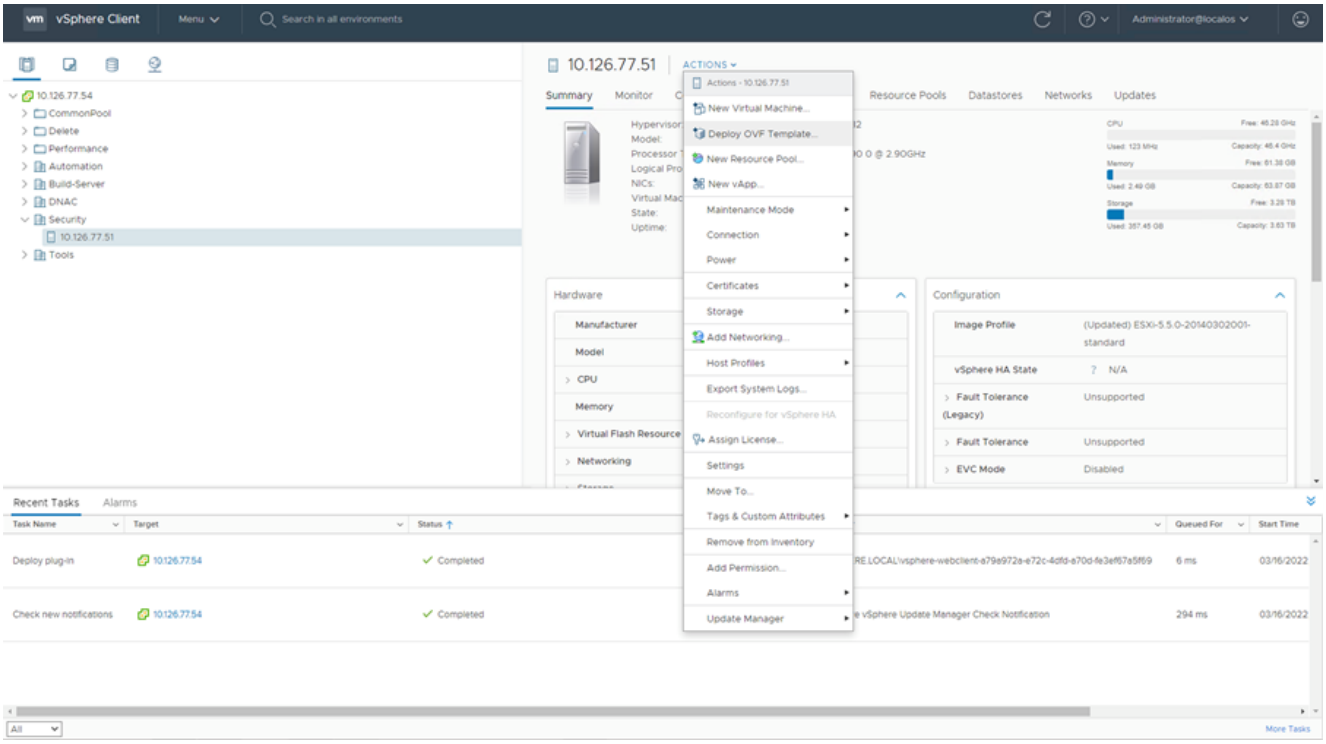
1. Log into vCenter Client using the ESXi/hypervisor credentials.

Login

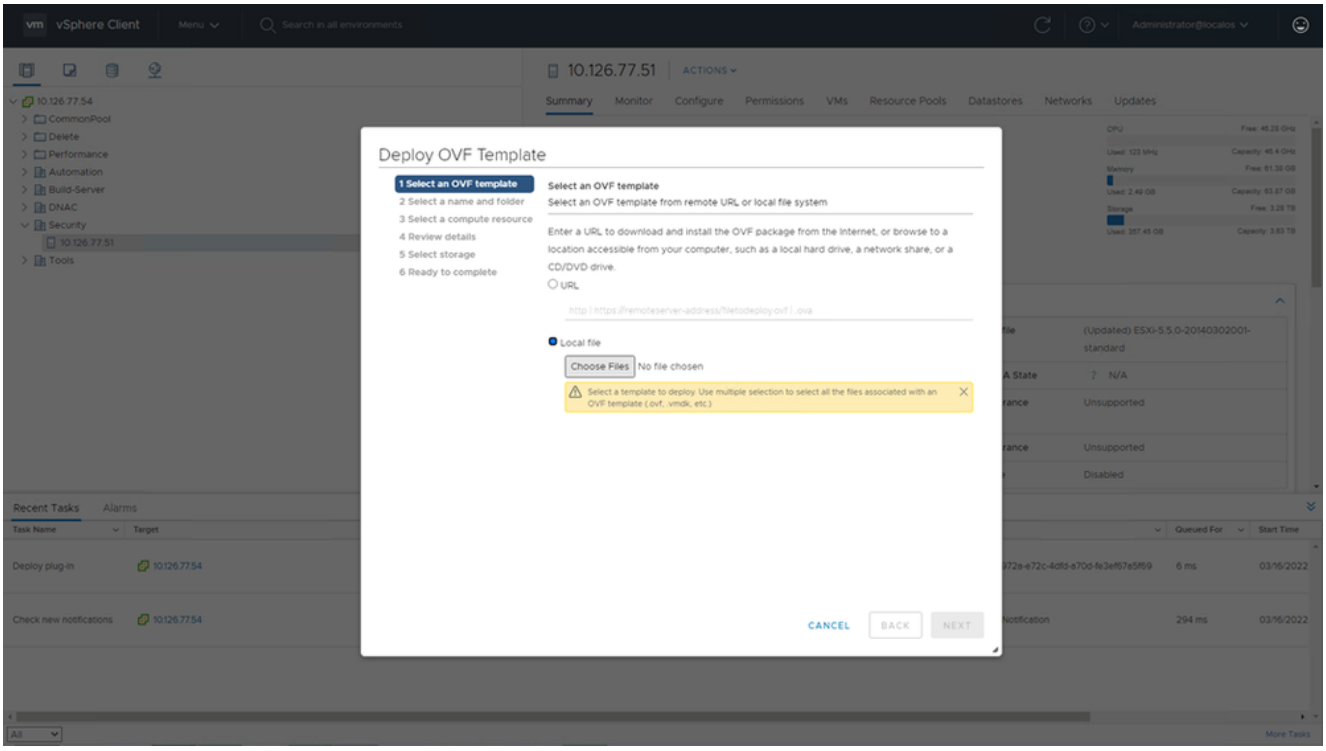


Home Screen

2. On the Home page click Hosts and Clusters.
3. Select the VM and click Action > Deploy OVF Template.

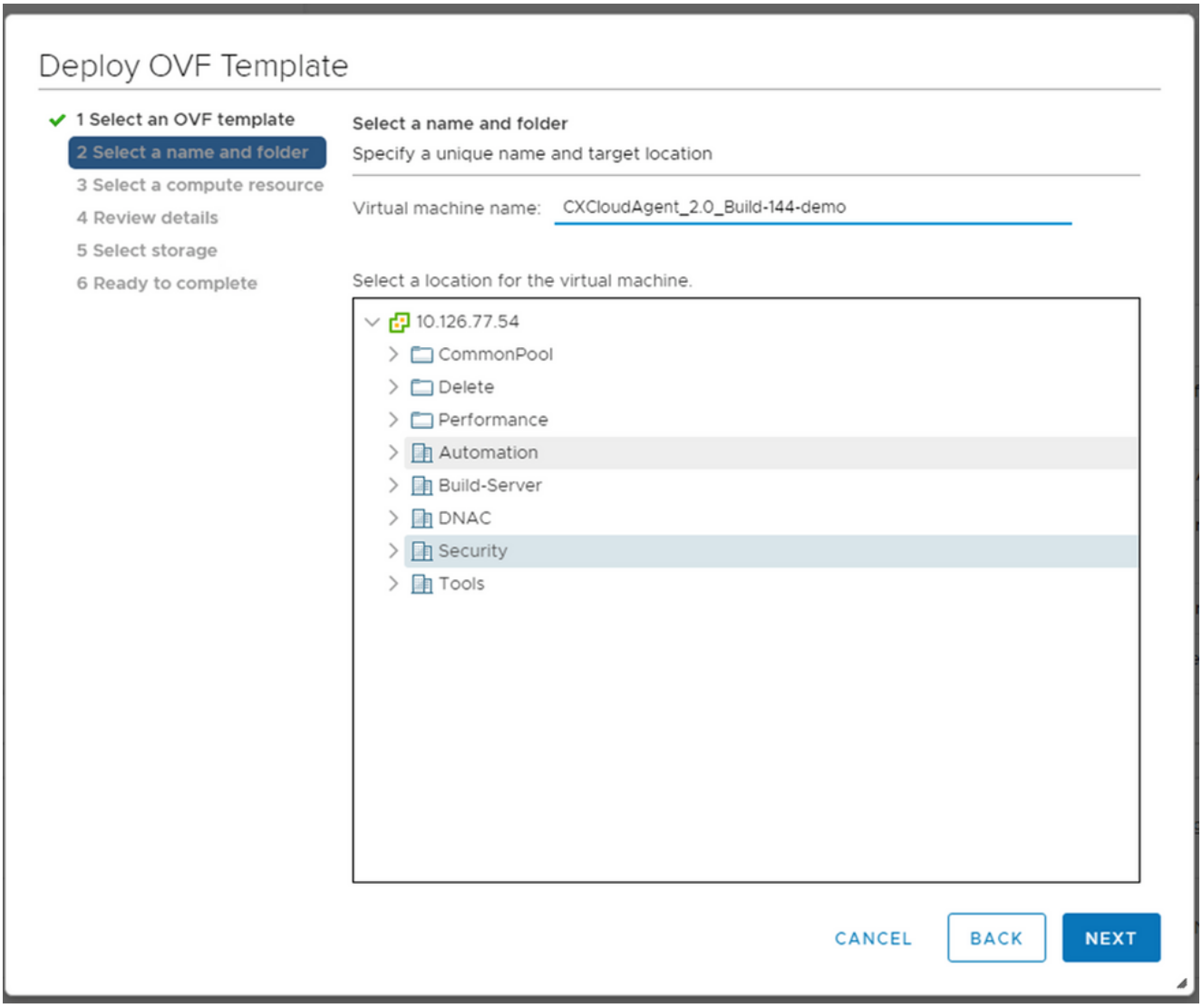


Actions



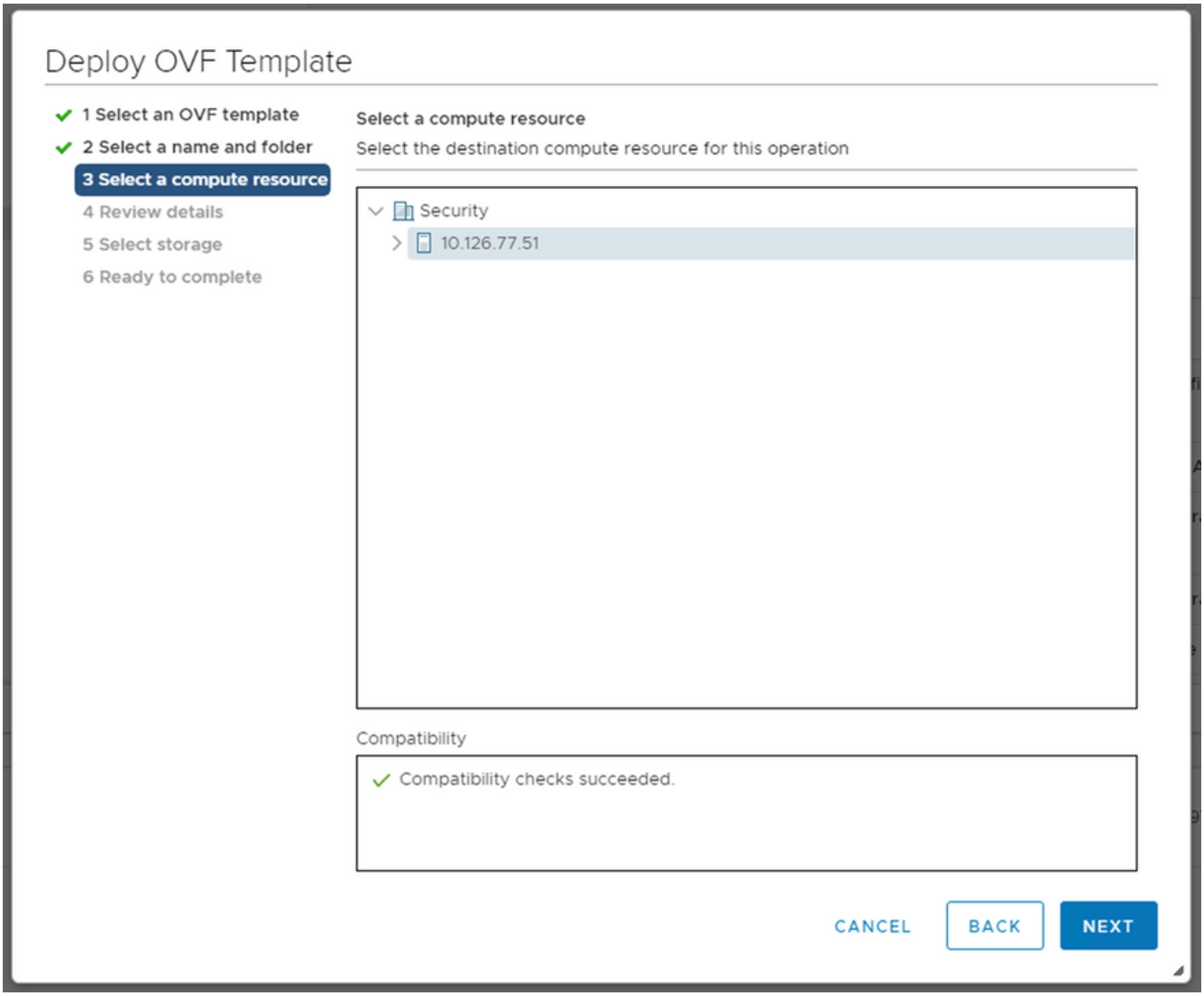
Select Template

4. Add the URL directly or browse to select the OVA file and click Next.
5. Enter a unique name and browse to the location if required .
6. Click Next.



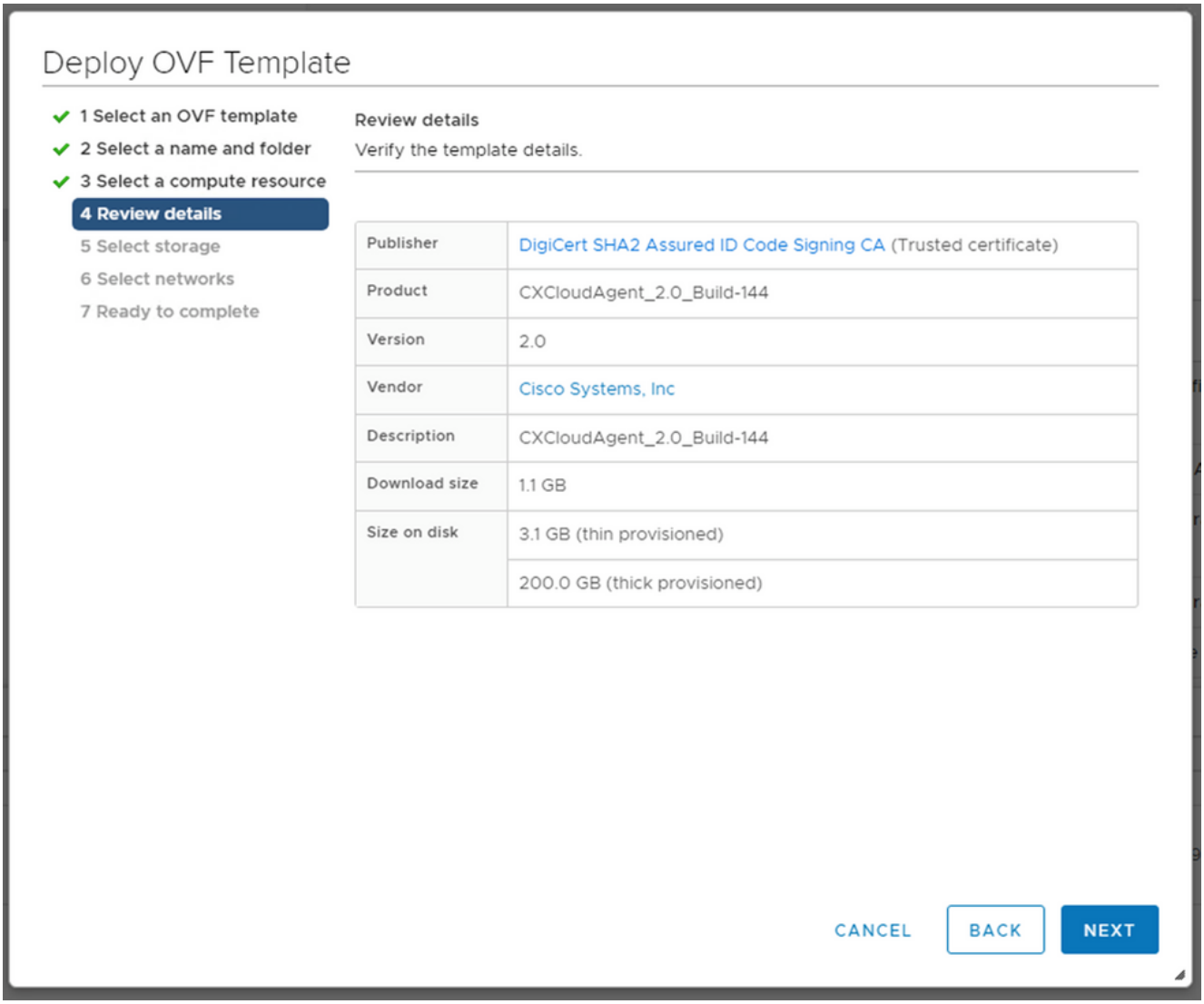
Name and Folder

7. Select compute resource and click Next.



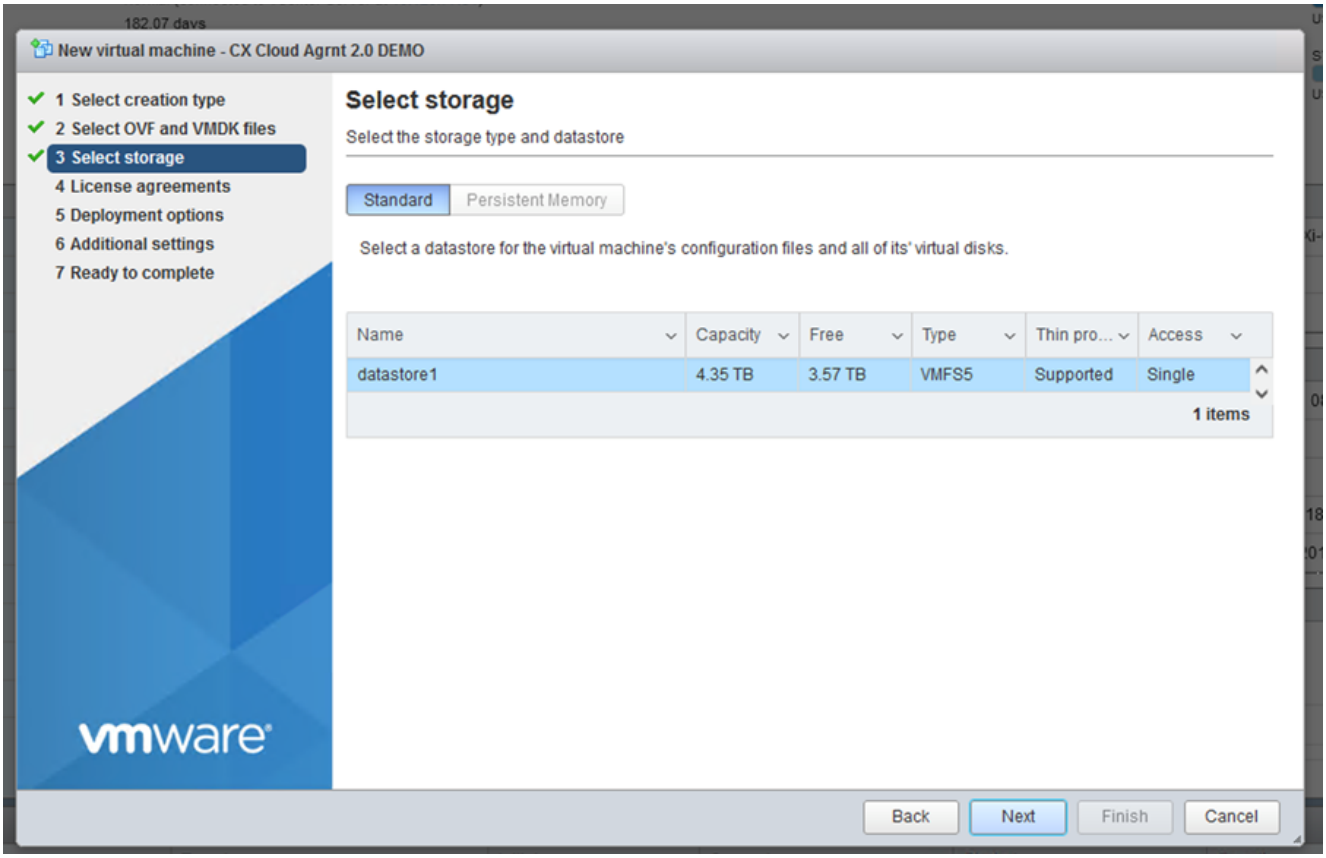
Select Compute Resource

8. Review the details and click Next.



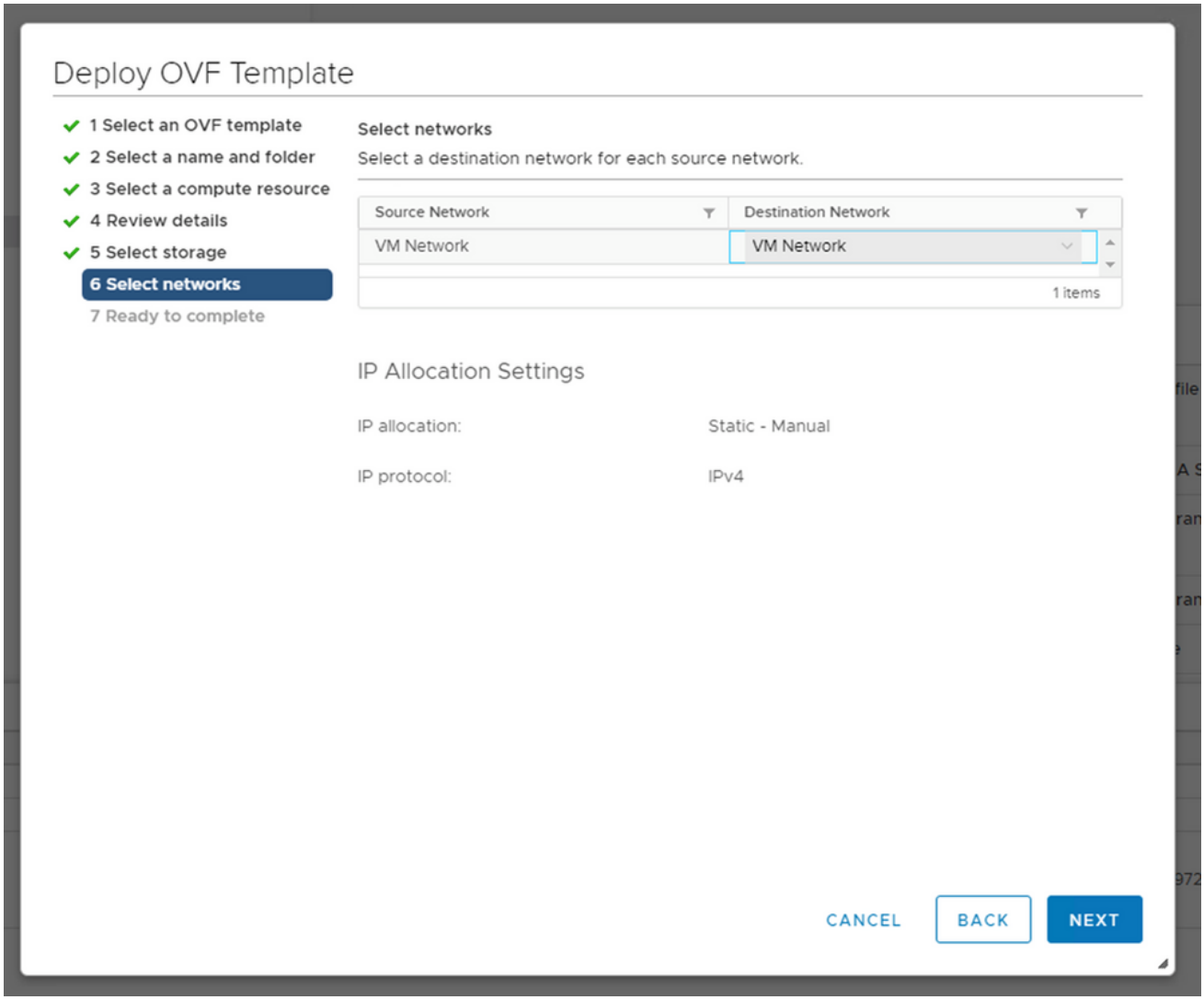
Review Details

9. Select the virtual disk format and click Next.



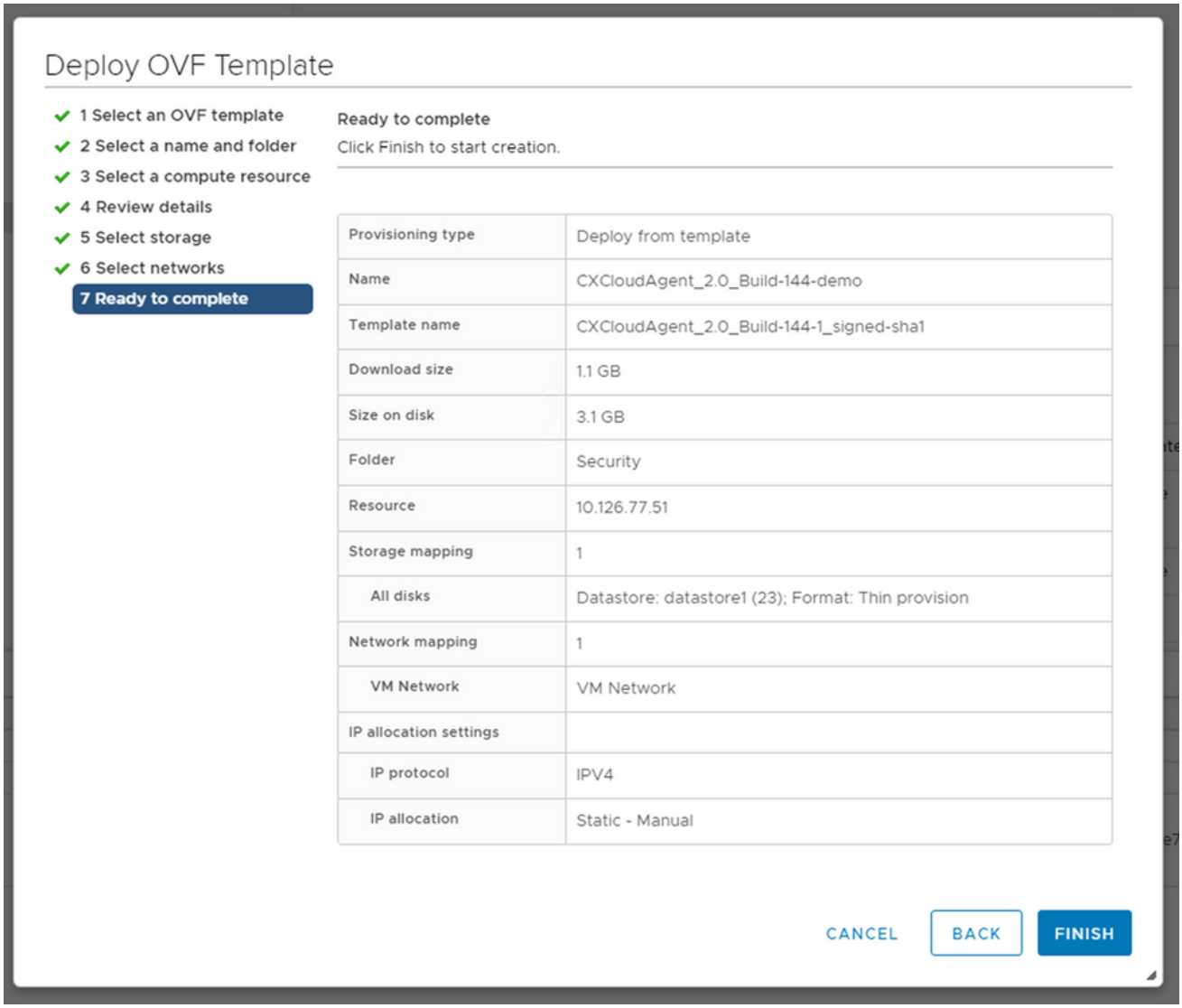
Select Storage

10. Click Next.



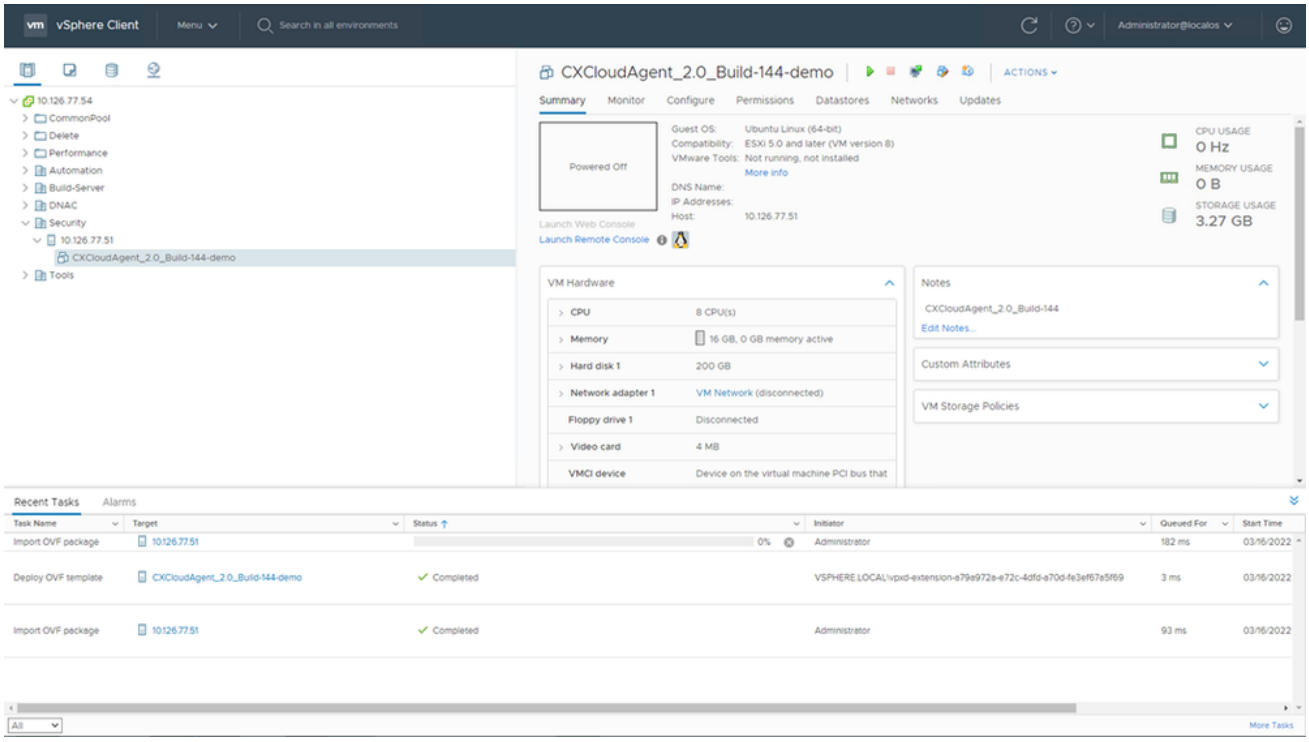
Select Networks

11. Click Finish.



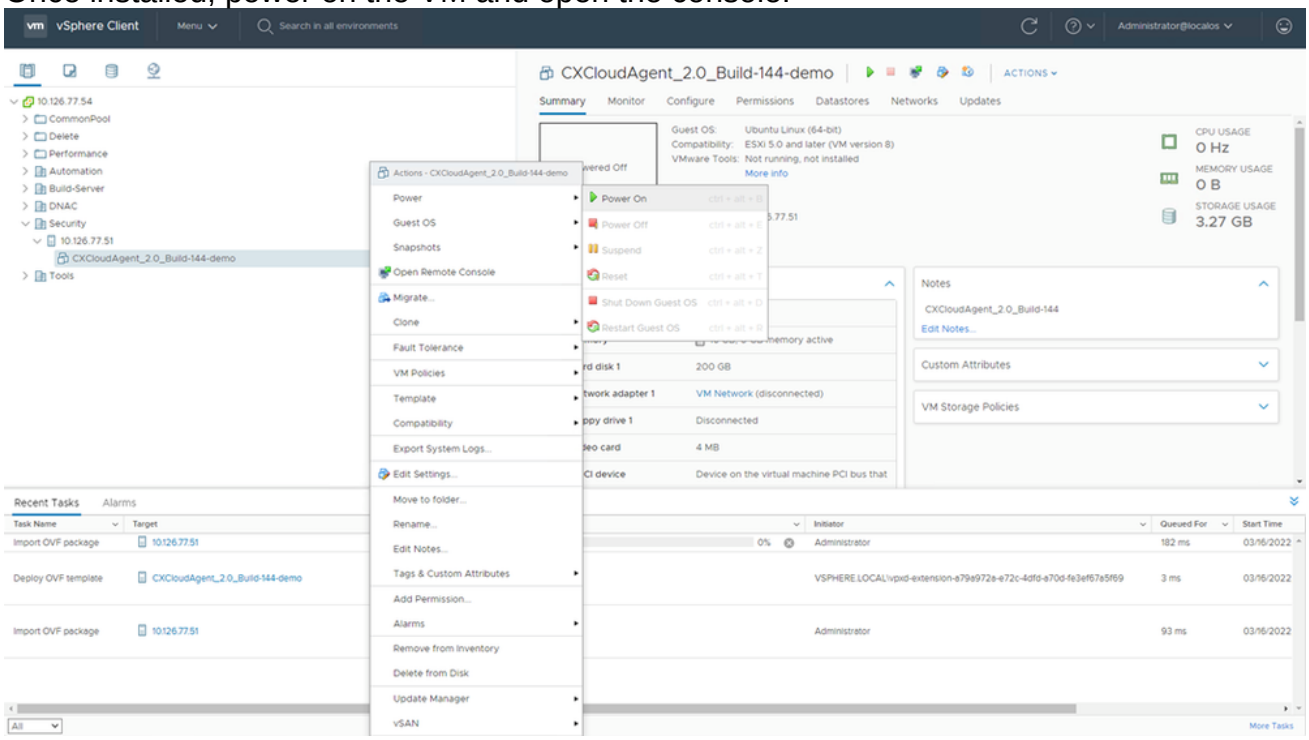
Ready to Complete

12. A new VM is added. Click on its name to view the status.



Added VM

13. Once installed, power on the VM and open the console.



Open Console

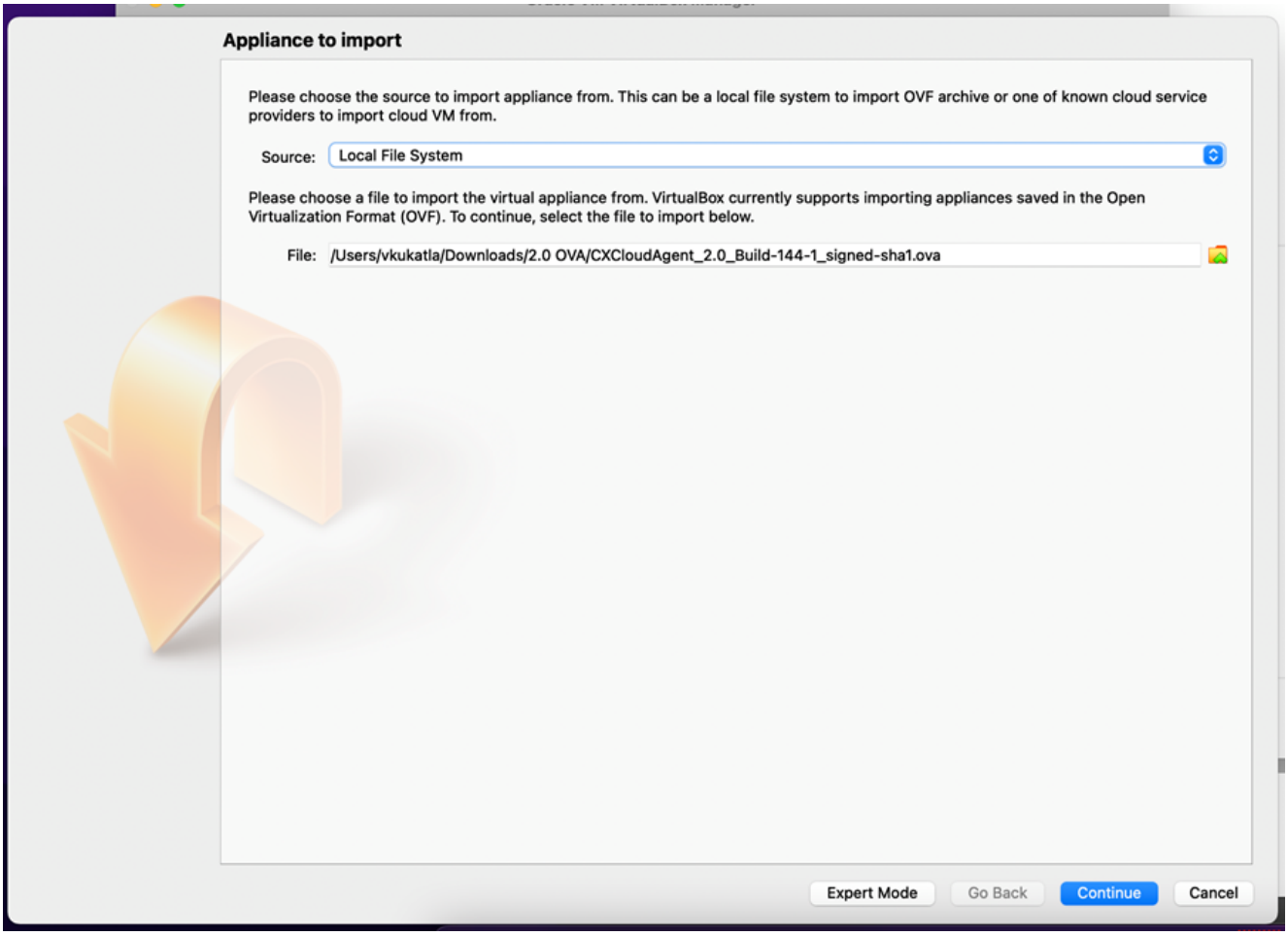
14. Navigate to [Network Configuration](#).

Oracle Virtual Box 5.2.30 Installation

This client deploys CX Cloud Agent OVA though the Oracle Virtual Box.

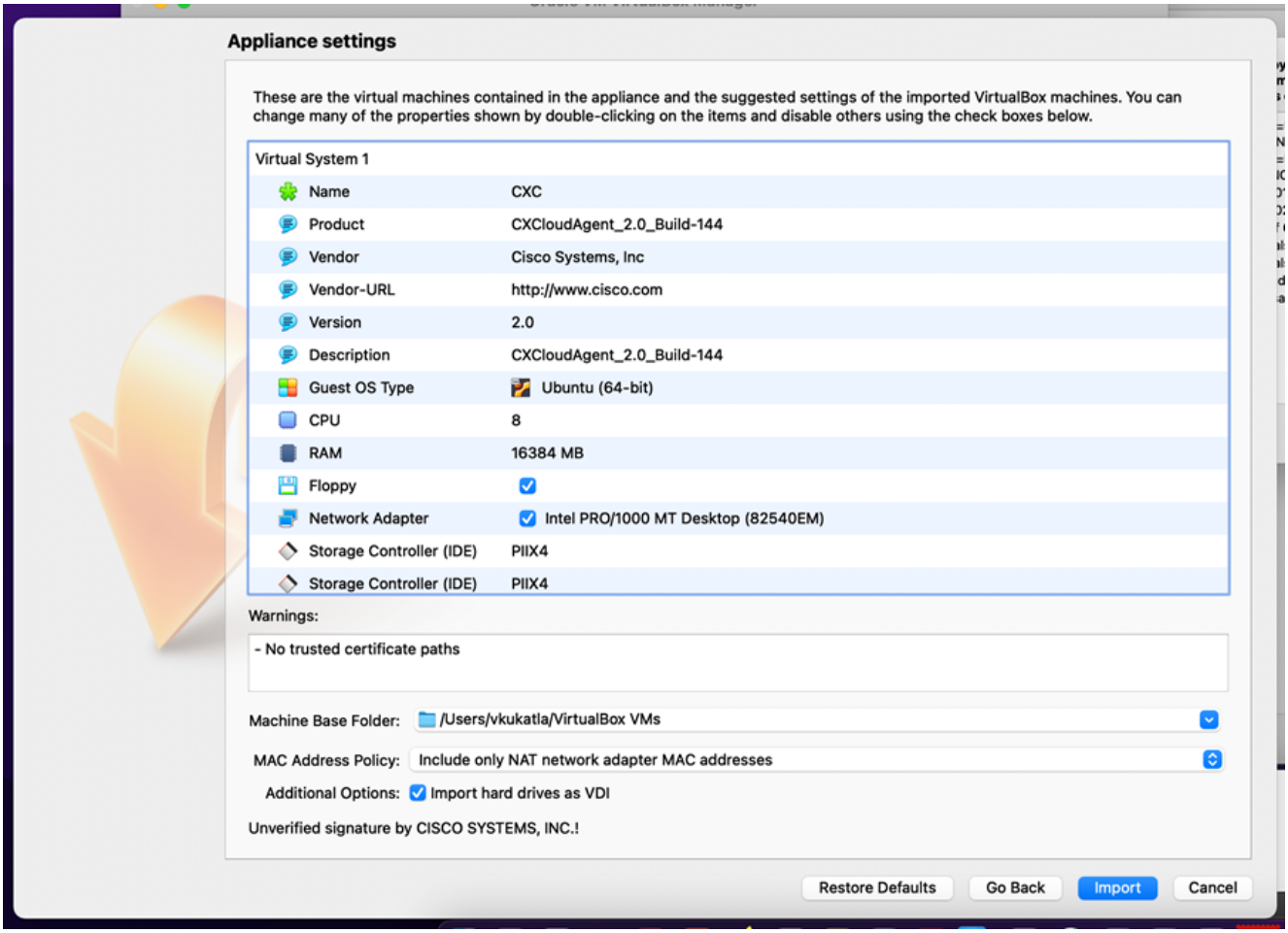
Oracle VM

1. Open the Oracle VM UI and select File > Import Appliance.
2. Browse to import the OVA file.



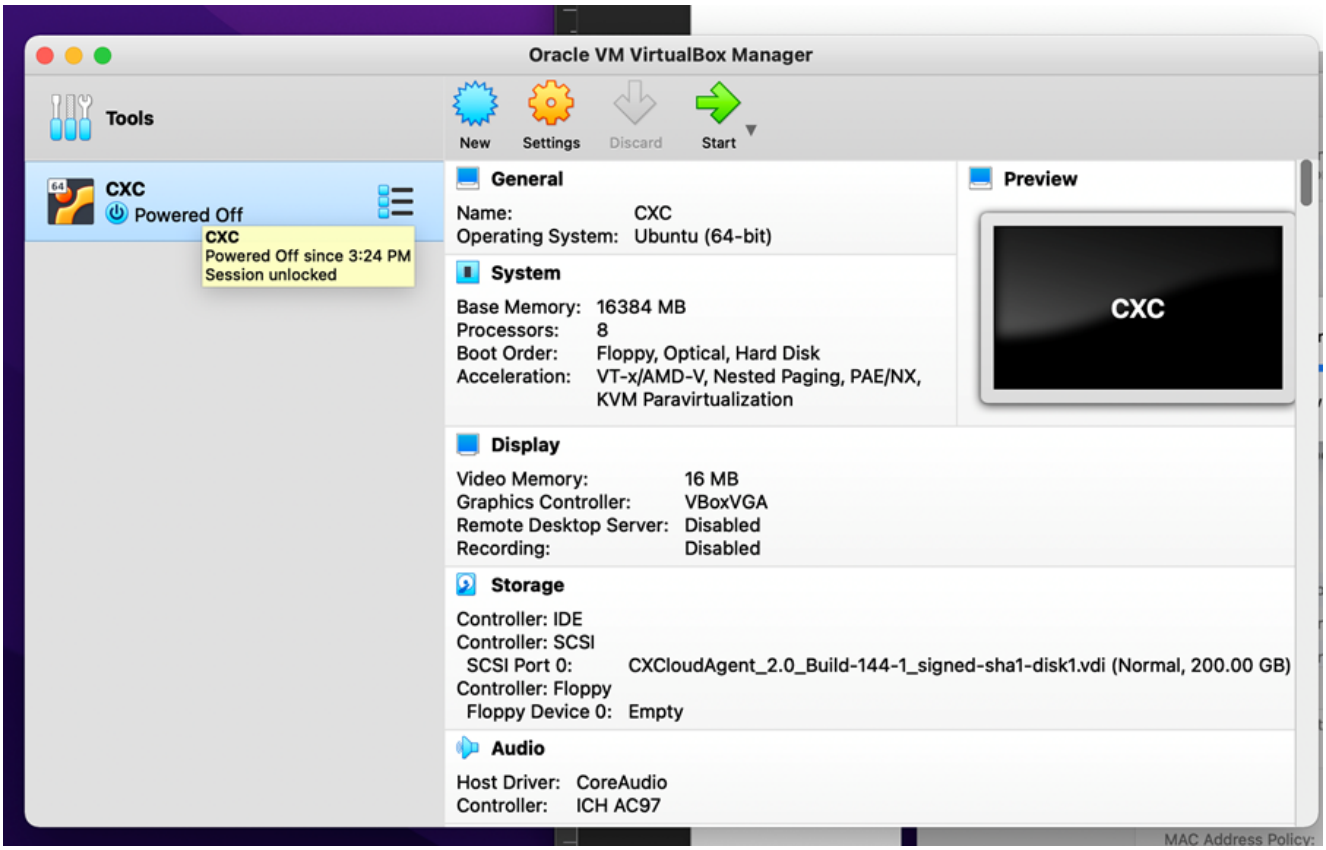
Select File

3. Click Import.

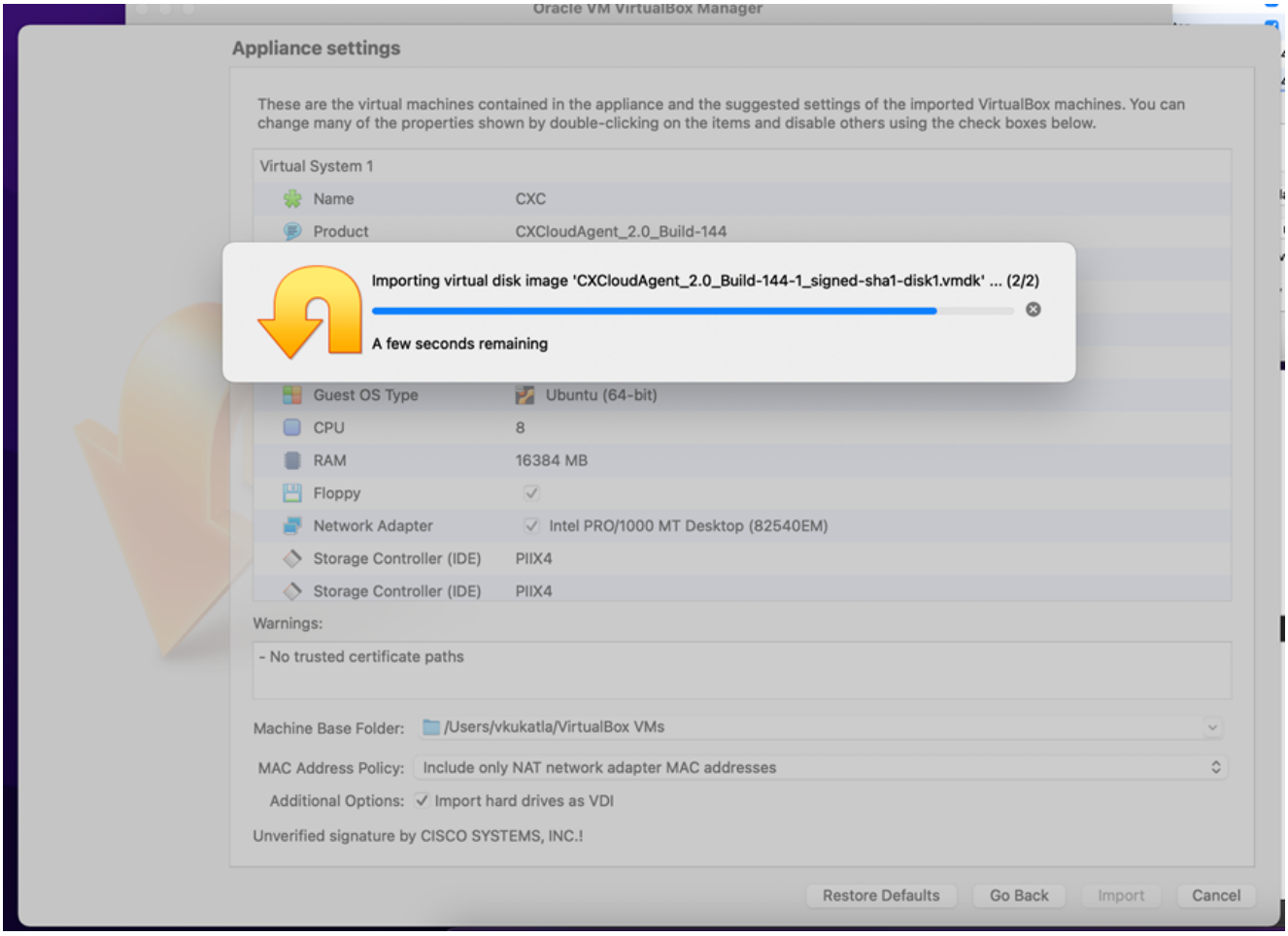


Import File

4. Select the VM just deployed and click Start.

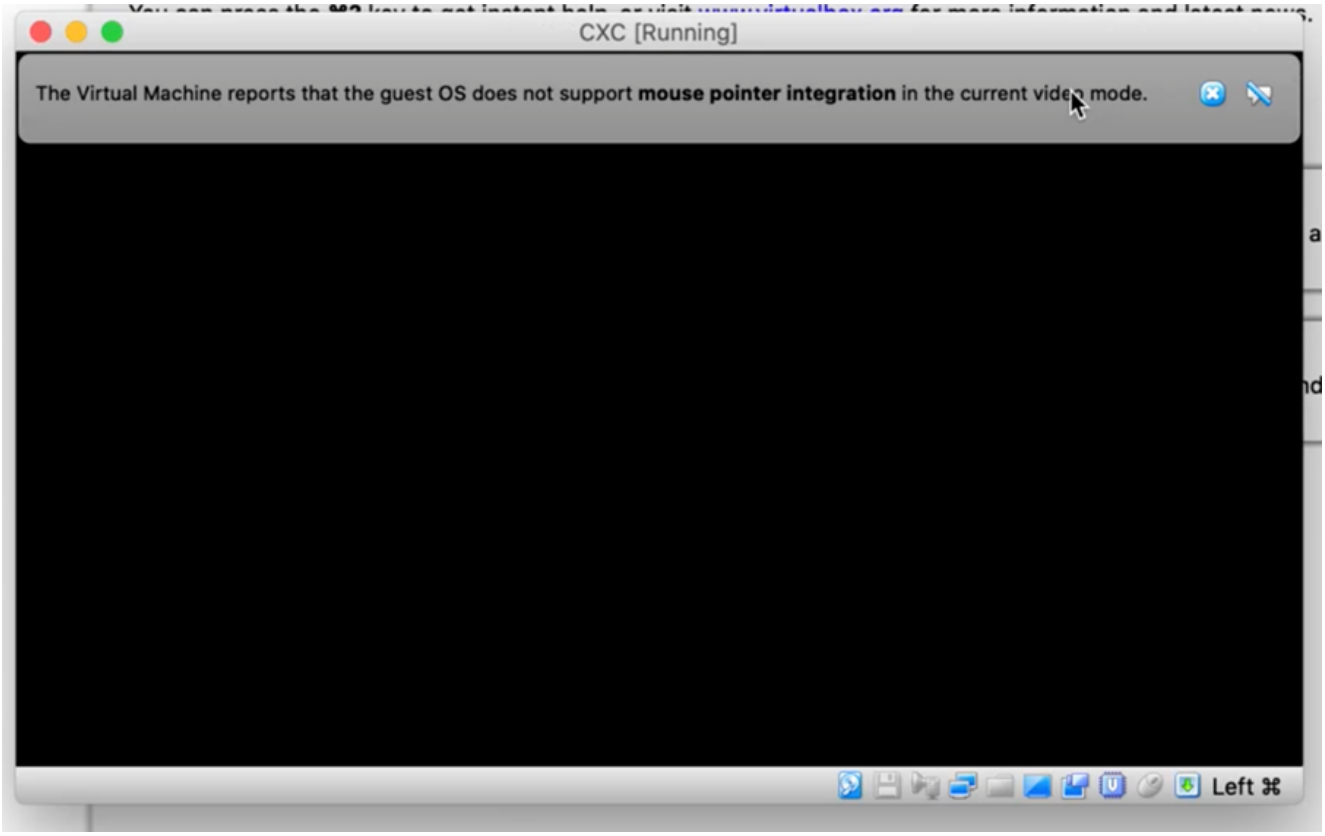


VM Console Startup



Import in Progress

5. Power on the VM. The console displays.

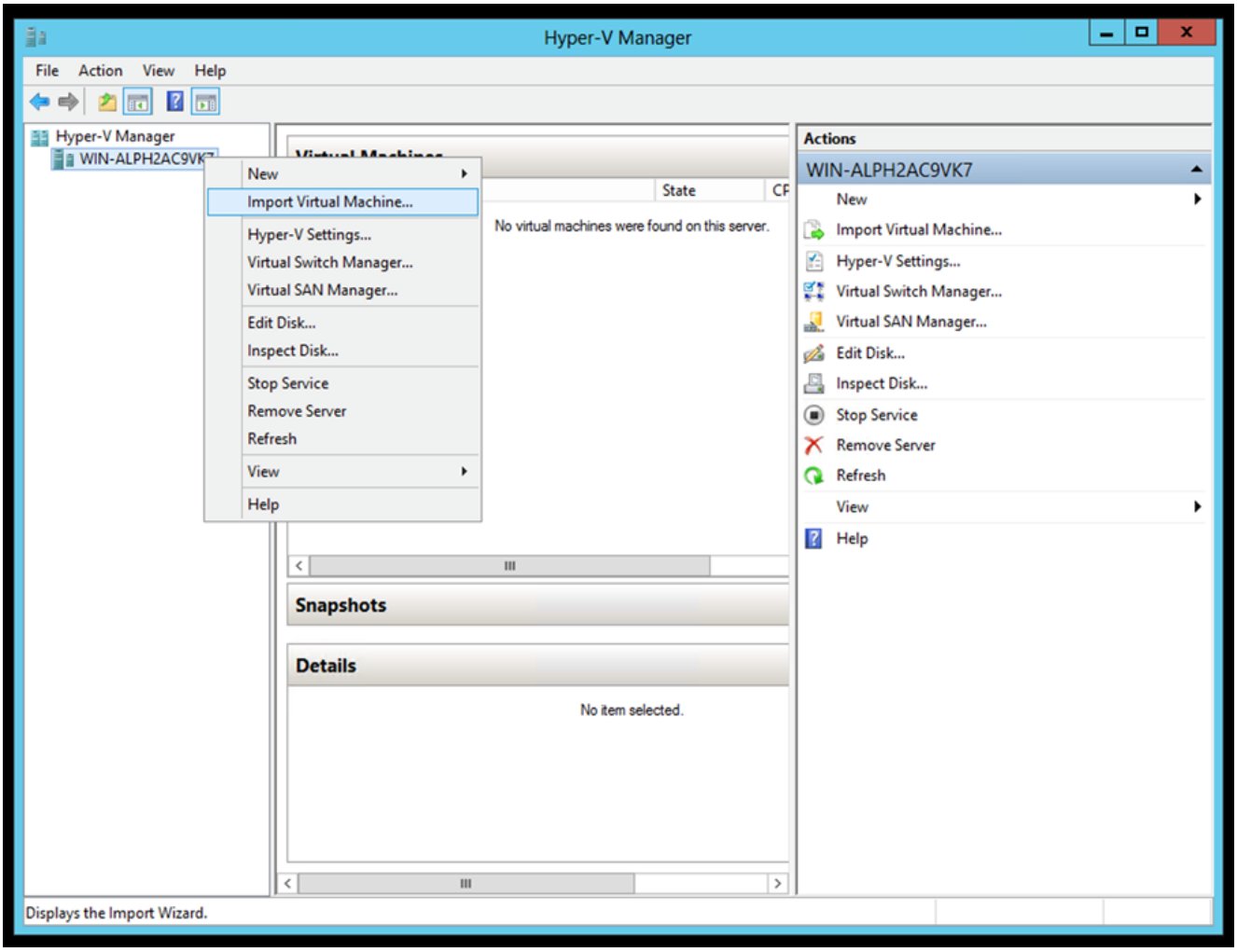


Open the Console

6. Navigate to **Network Configuration**.

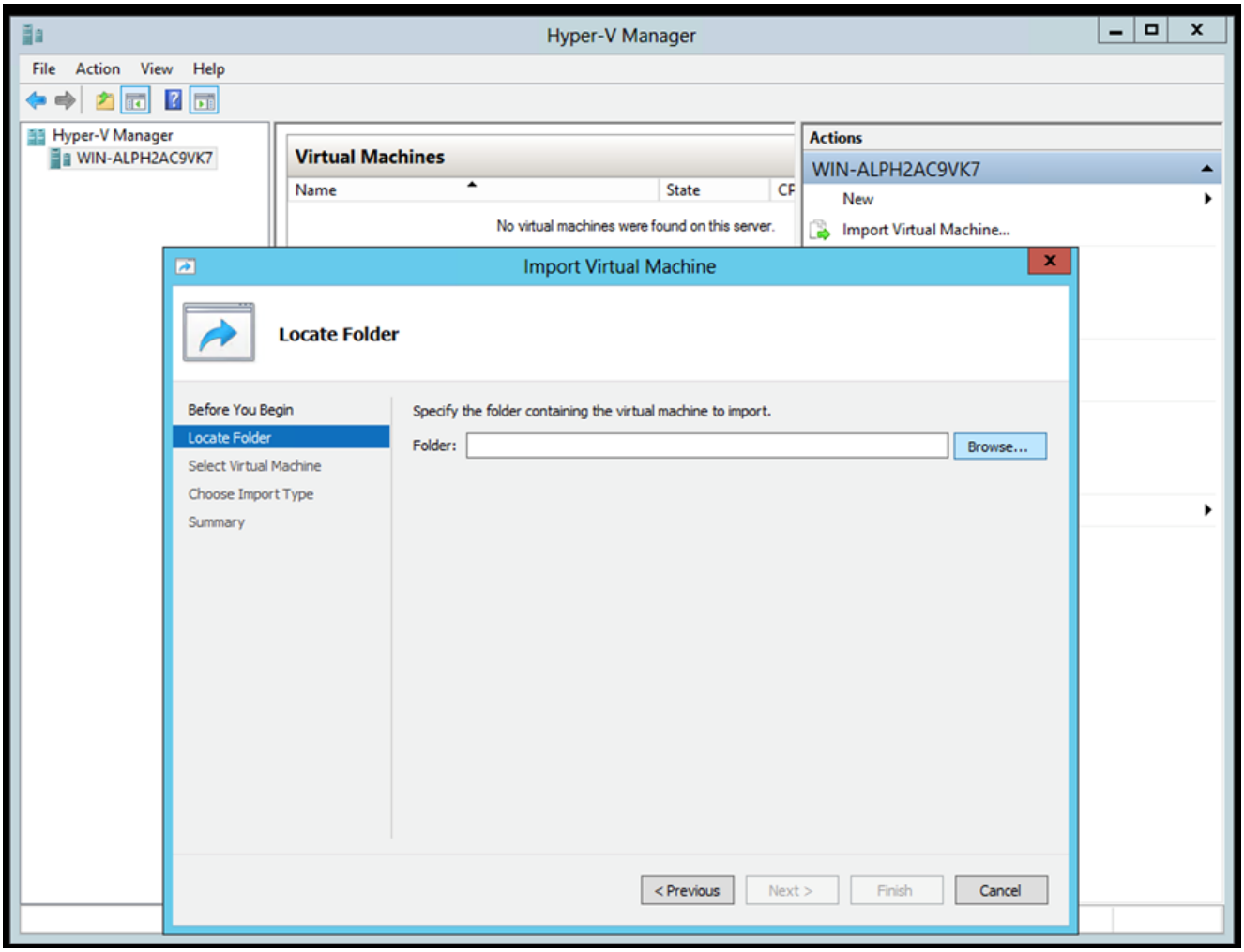
Microsoft Hyper-V Installation

1. Select Import Virtual Machine.



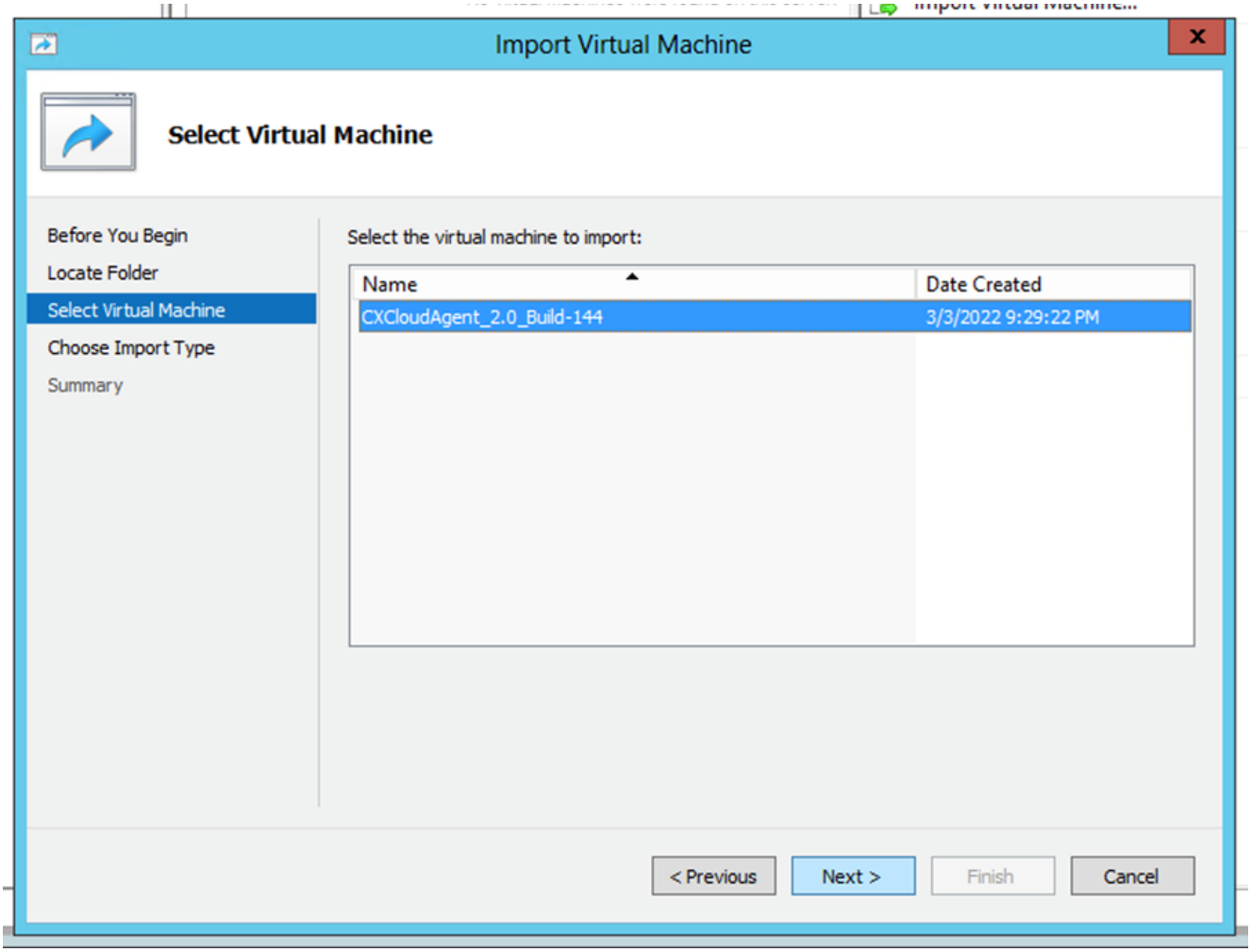
Hyper-V Manager

2. Browse and select the download folder.
3. Click Next.



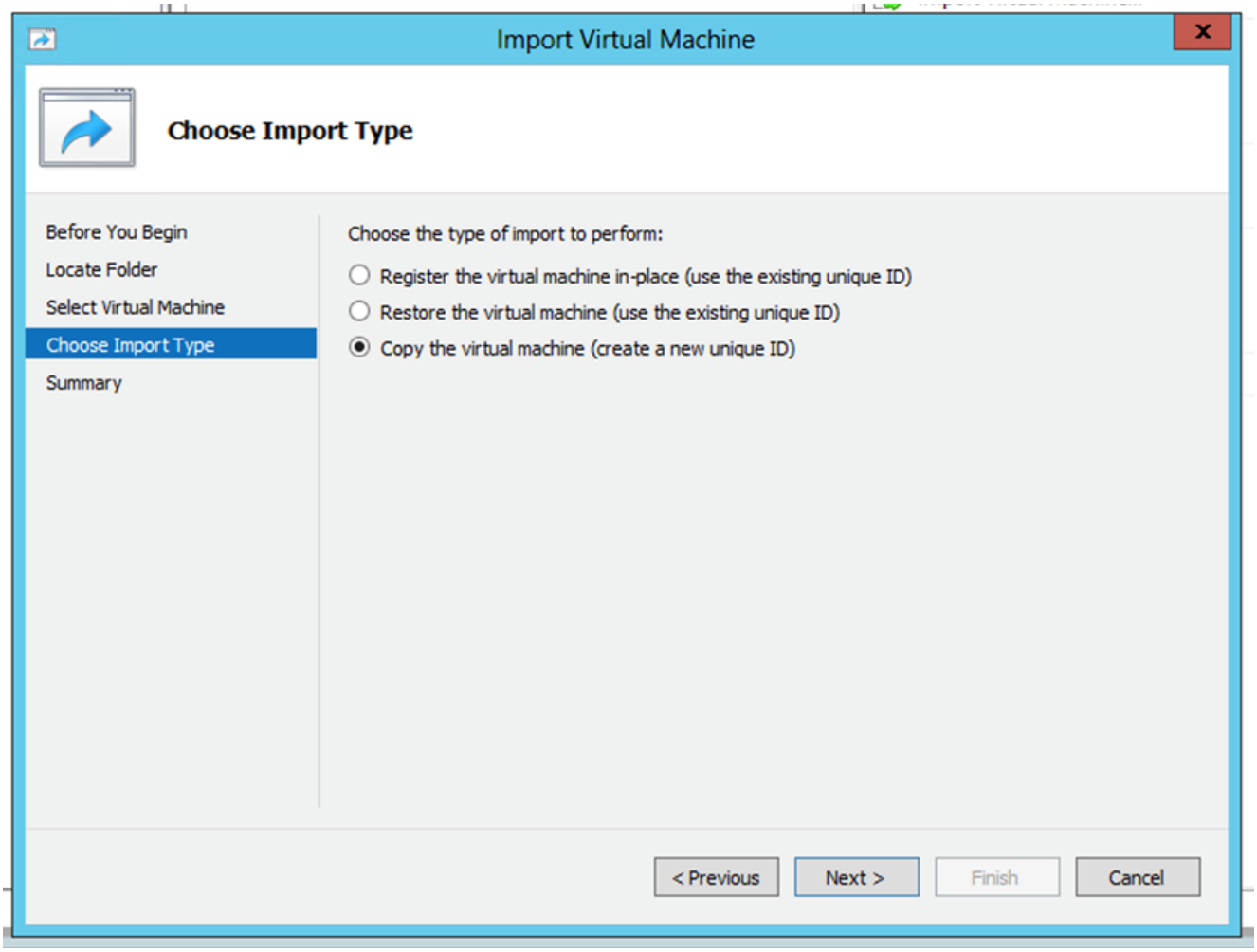
Folder to Import

4. Select the VM and click Next.



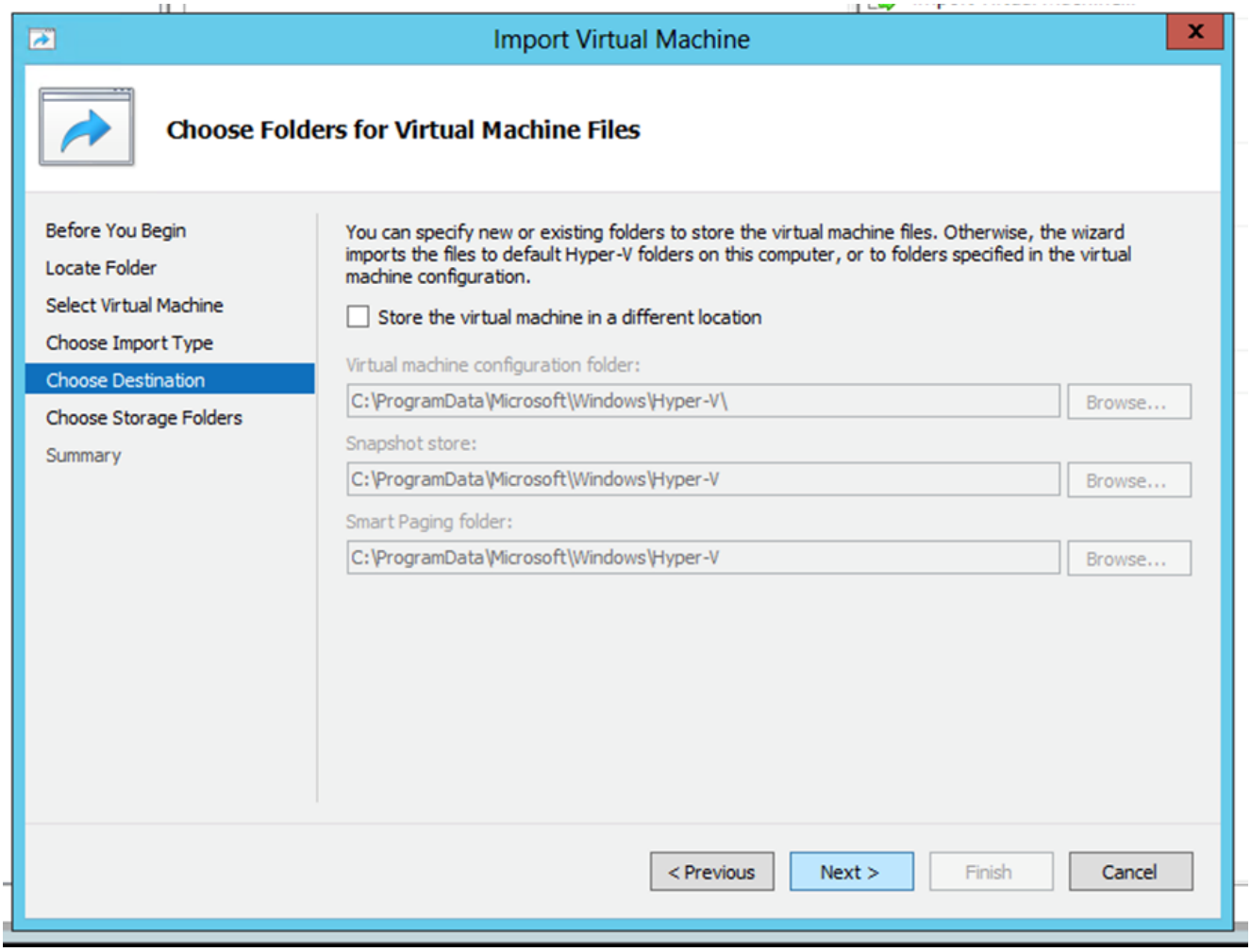
Select VM

5. Select the Copy the virtual machine (create a new unique ID) radio button and click Next.



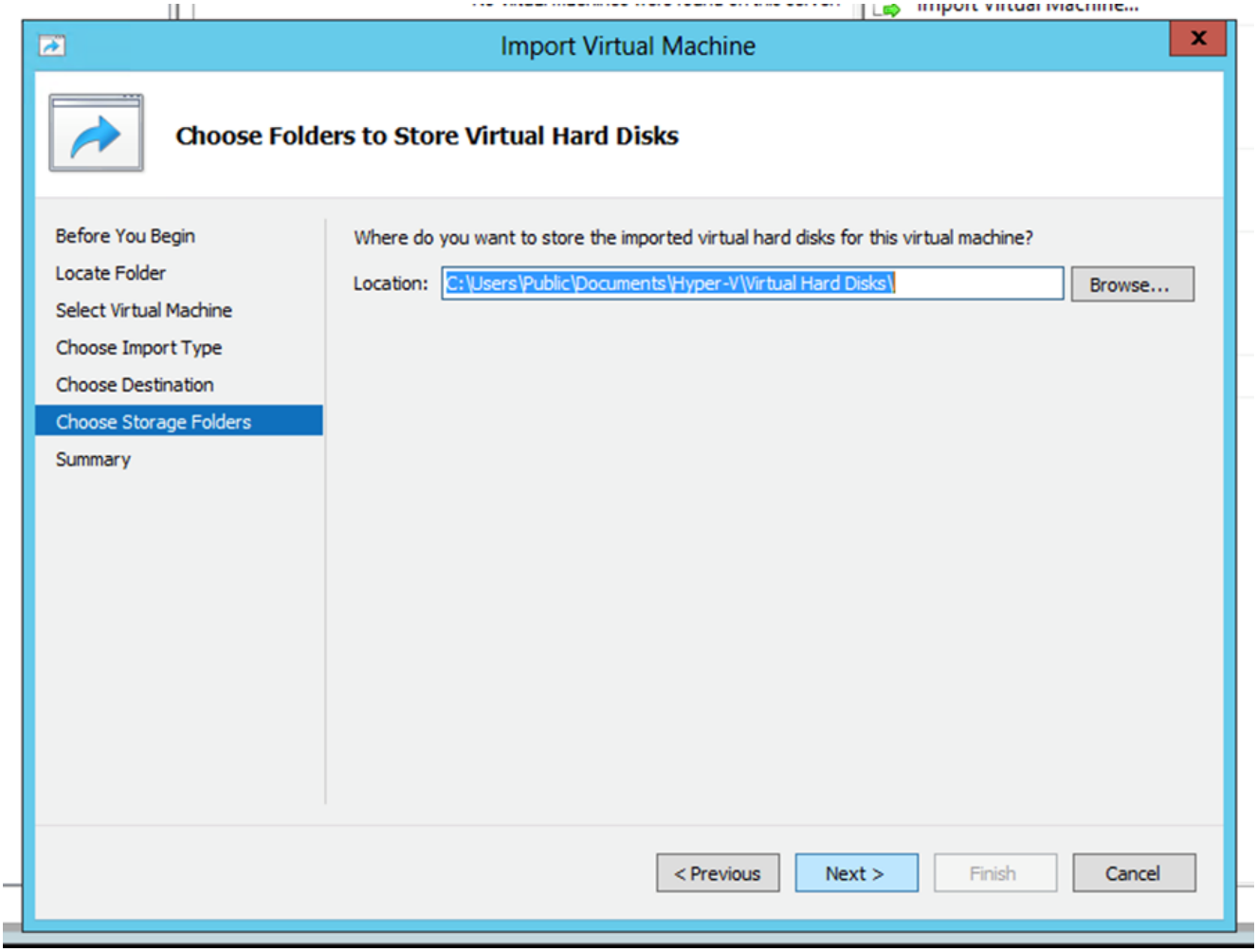
Import Type

6. Browse to select the folder for VM files. It is recommended to use default paths.
7. Click Next.



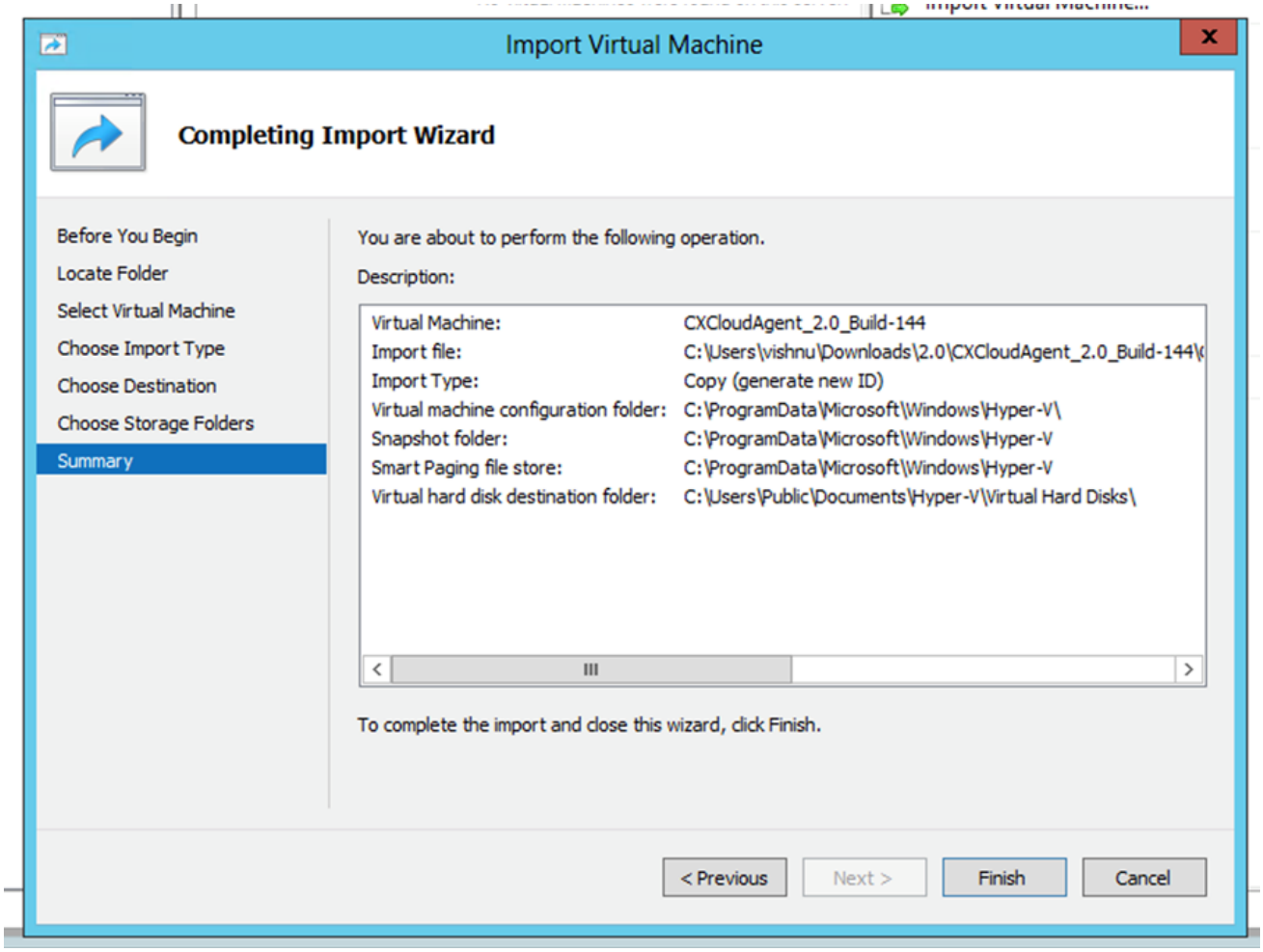
Choose Folder

8. Browse and select the folder to store the VM hard disk. It is recommended to use default paths.
9. Click Next.



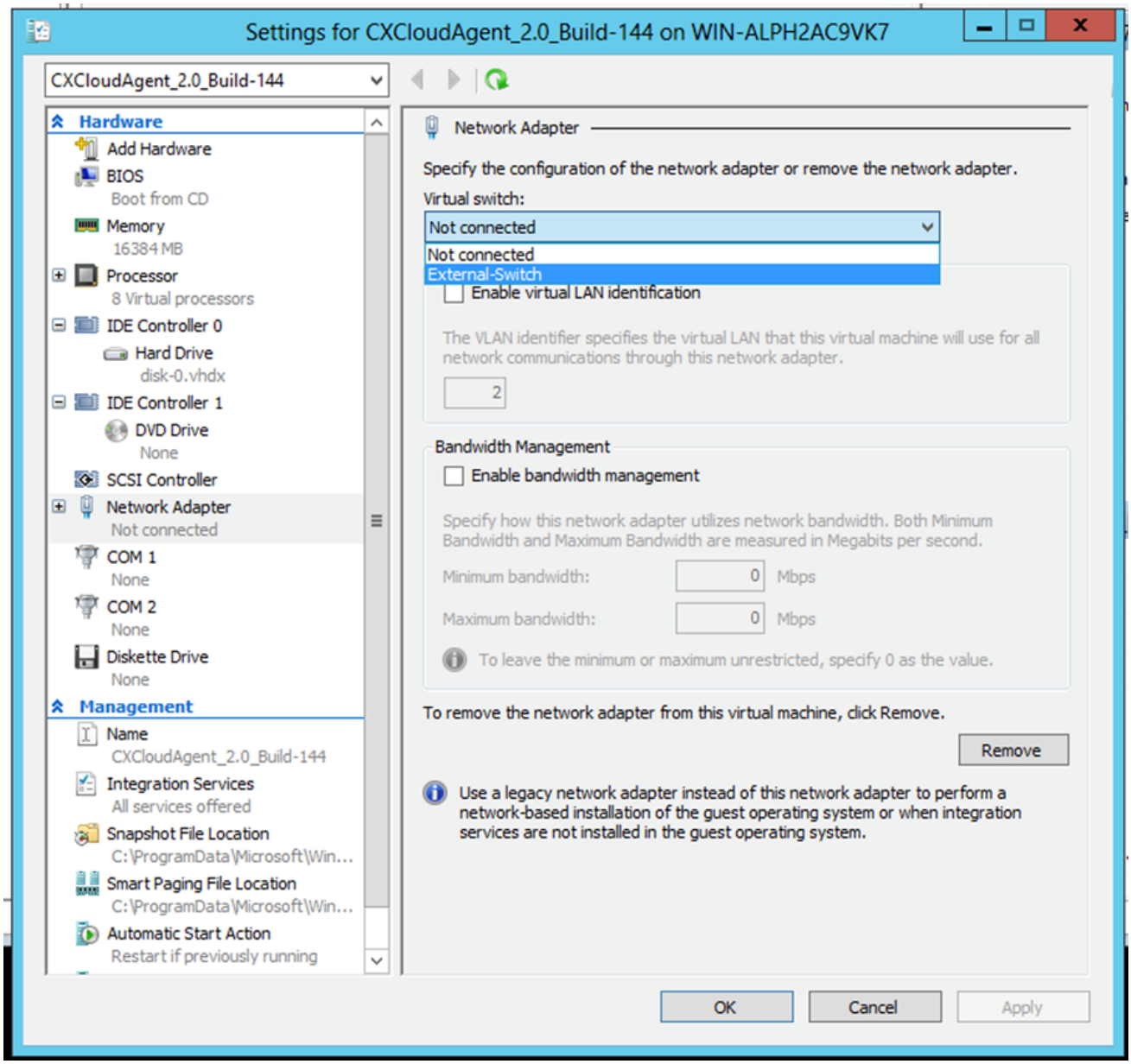
Folder to Store Virtual hard Disks

10. The VM summary displays. Verify all inputs and click Finish.



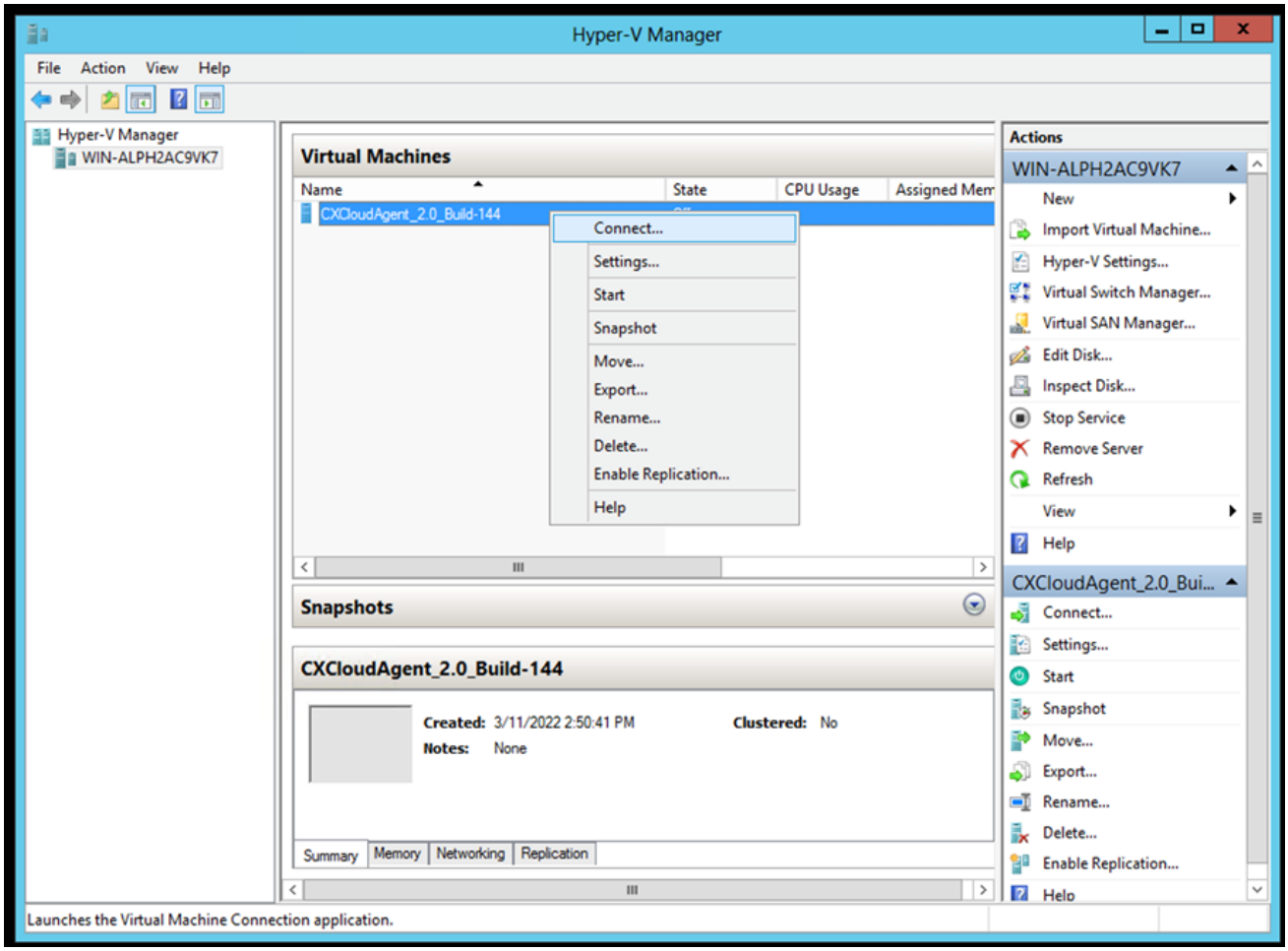
Summary

11. Once the import is completed successfully, a new VM is created on Hyper-V. Open the VM setting.
12. Select the network adaptor on the left pane and choose the available Virtual Switch from the drop-down.



Virtual Switch

13. Select Connect to start the VM.



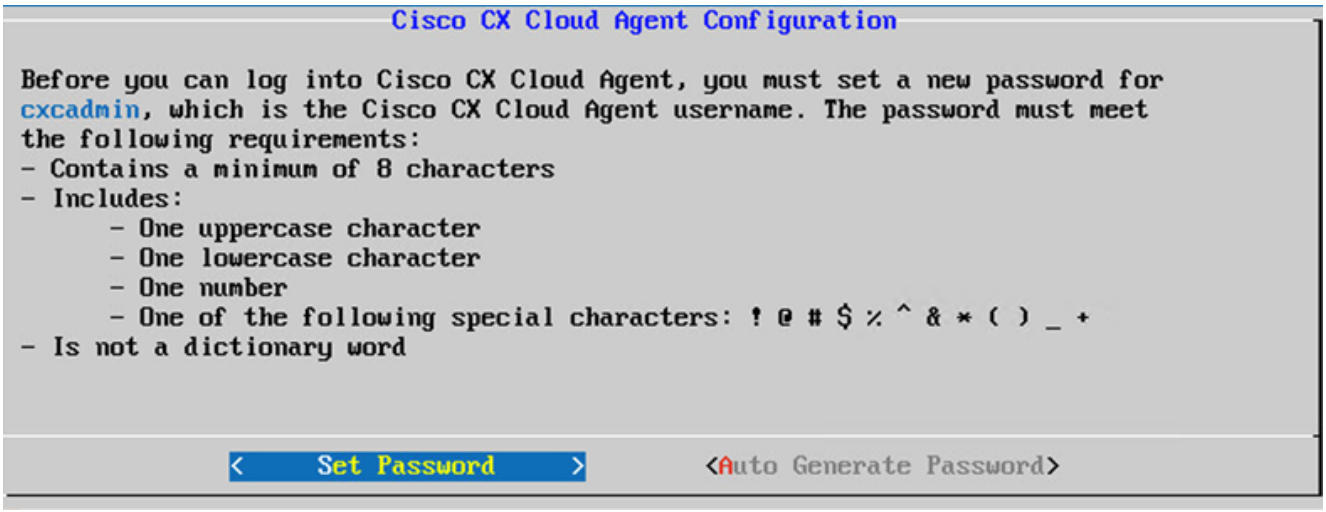
Starting VM

14. Navigate to **Network Configuration**.

Network Configuration

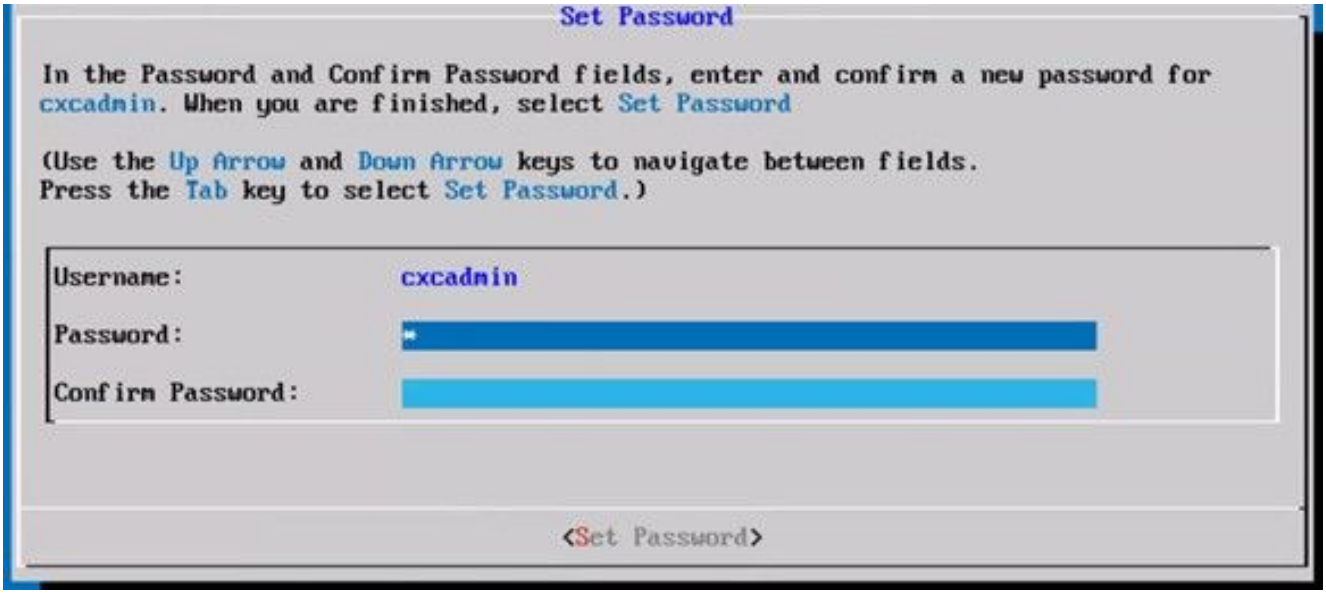
VM Console

1. Click Set Password to add a new password for cxcadmin OR click Auto Generate Password to get a new password.



Set Password

2. If Set Password is selected, enter the password for cxcadmin and confirm it. Click Set Password and go to Step 3.



New Password

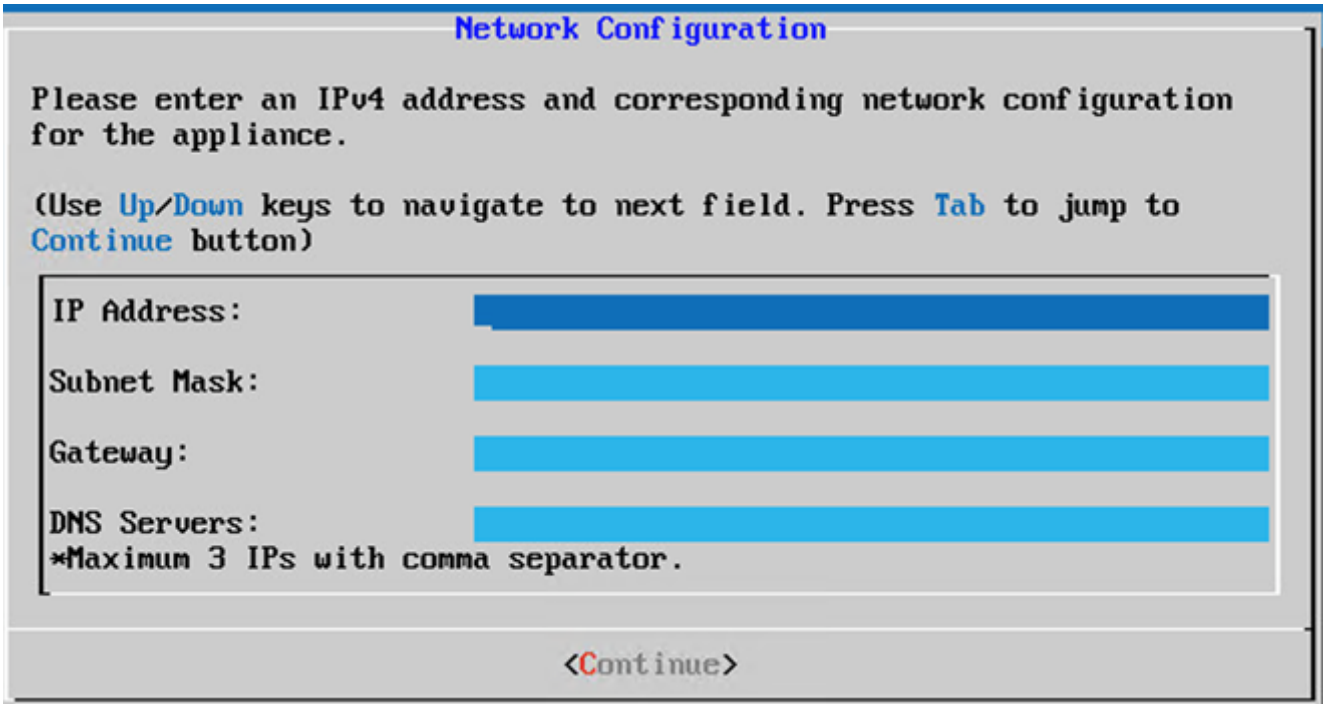
OR If Auto Generate Password is selected, copy the password generated and store it for future use. Click Save Password and go to Step 4.

Auto Generated Password

3. Click Save Password to use it for authentication.

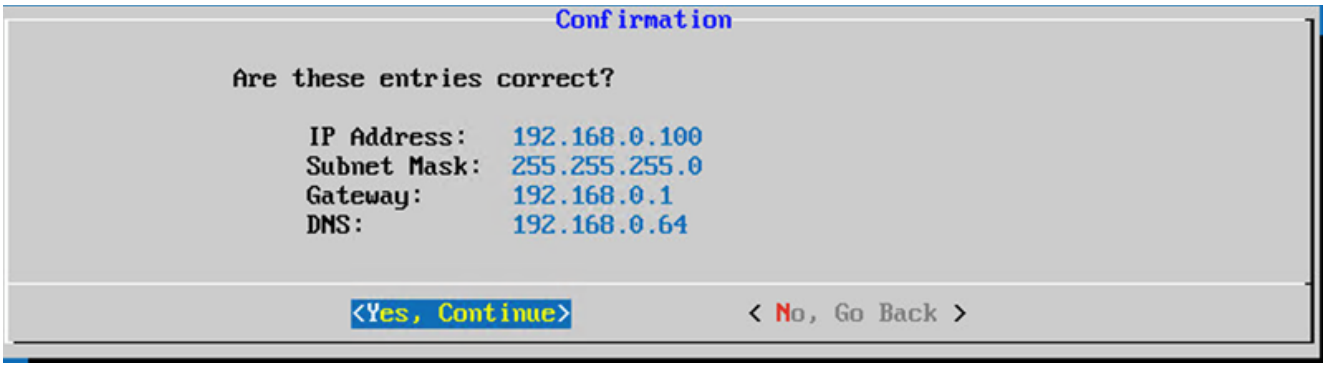
Save Password

4. Enter the IP Address, Subnet Mask, Gateway, and DNS Server and click Continue.



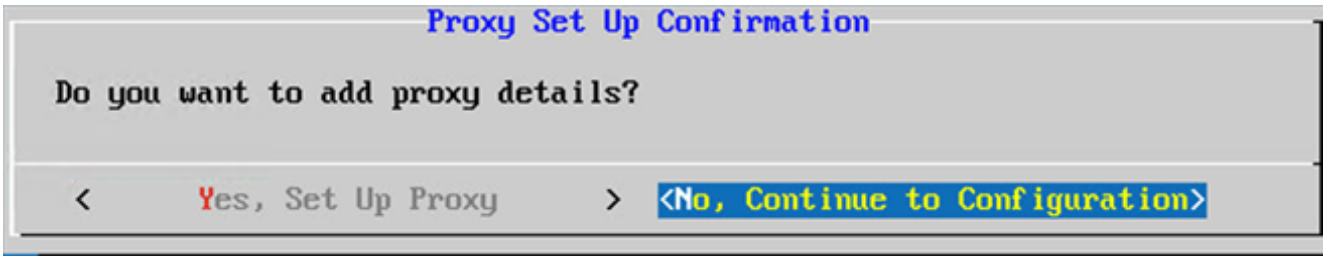
Network Configuration

5. Confirm the entries and click Yes, Continue.



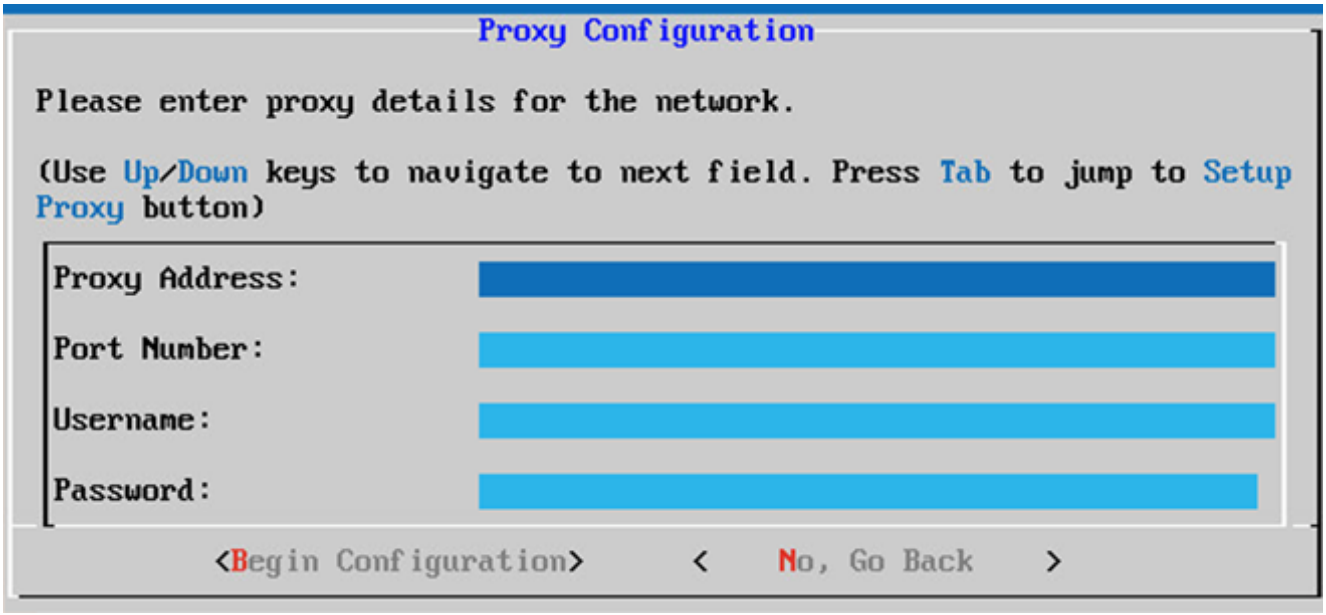
Confirmation

6. To set the proxy details, click Yes, Set Up Proxy or click No, Continue to Configuration to complete the configuration and go to Step 8.



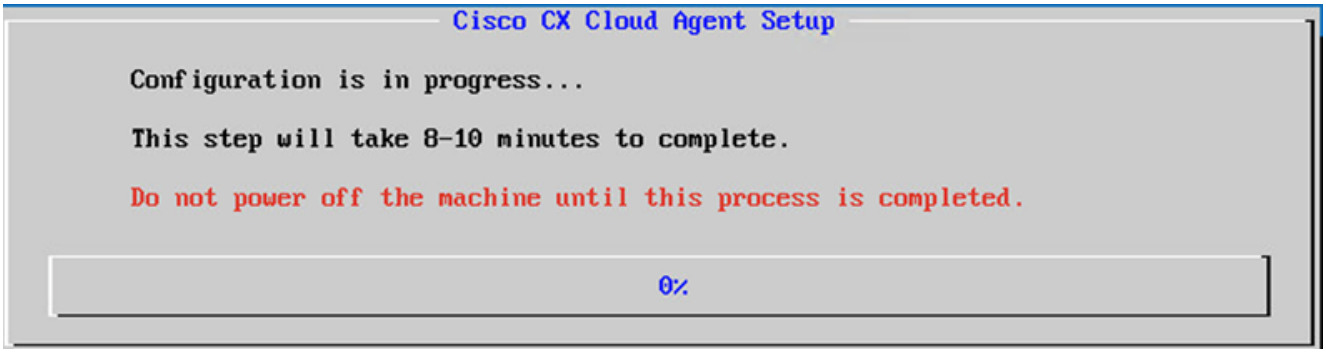
Proxy Setup

7. Enter the Proxy Address, Port Number, Username, and Password.



Proxy Configuration

8. Click Begin Configuration. The configuration can take several minutes to complete.

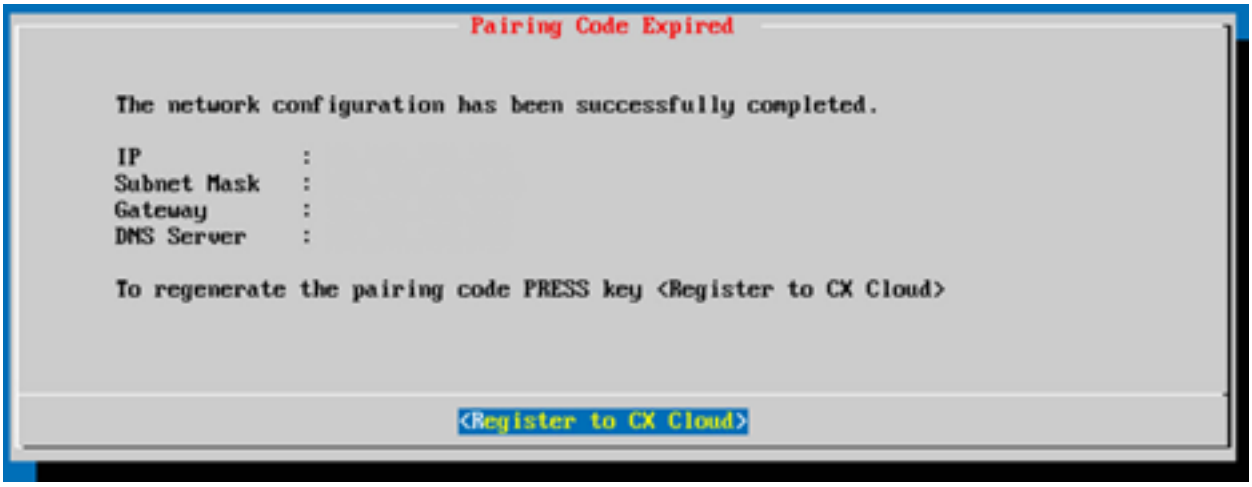


Configuration in Progress

9. Copy the Pairing Code and return to CX Cloud to continue the setup.

Pairing Code

10. If the Pairing Code expires, click Register to CX Cloud to obtain the code again.



Code Expired

11. Click OK.

Registration Successful

12. Return to the Connecting CX Cloud Agent to CX Cloud section and perform the listed steps.

Alternative Approach to Generate Pairing Code Using CLI

Users can also generate a pairing code by using CLI options.

To generate a pairing code through the use of CLI:

1. Log in to the Cloud Agent via SSH using the cxcadmin user credential.

2. Generate the pairing code using the command *cxcli agent generatePairingCode*.

Generate Pairing code CLI

3. Copy the Pairing Code and return to CX Cloud to continue the setup. For more information, refer to Connecting to Customer Portal.

Configure Cisco DNA Center to Forward Syslog to CX Cloud Agent

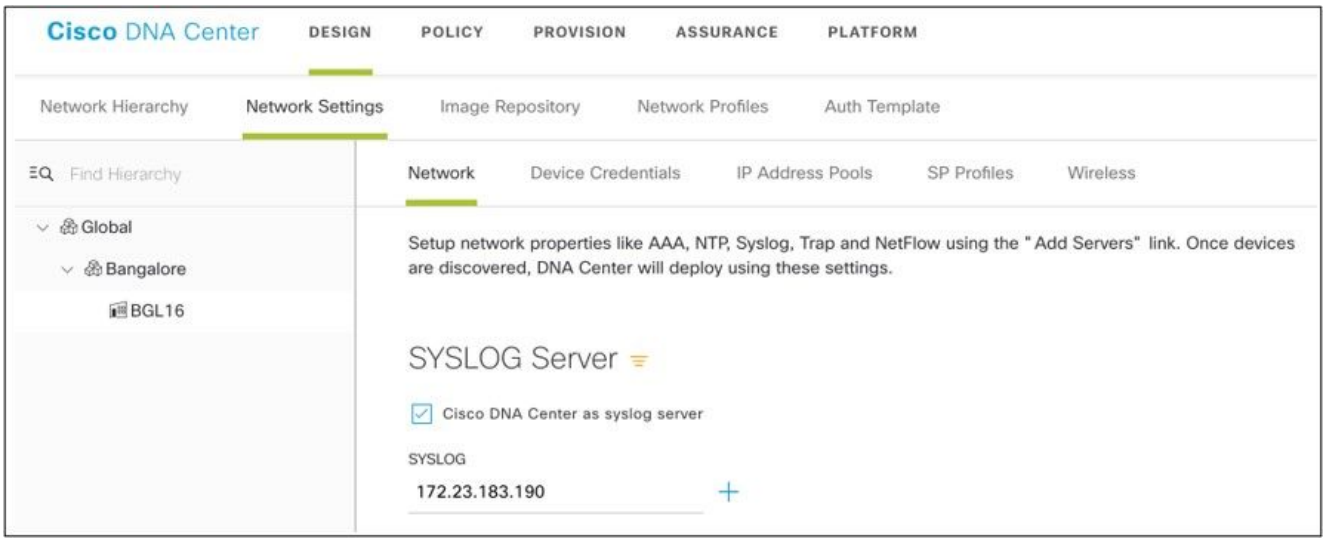
Prerequisite

Supported Cisco DNA Center versions are from 1.2.8 to 1.3.3.9 and from 2.1.2.0 to 2.2.3.5.

Configure Syslog Forwarding Setting

To configure Syslog Forwarding to CX Cloud Agent in Cisco DNA Center using UI, perform these steps:

1. Launch Cisco DNA Center.
2. Go to Design > Network Settings > Network.
3. For each site, add the CX Cloud Agent IP as the Syslog Server.



Syslog Server

Notes:
- Once configured, all devices associated with that site are configured to send syslog with level critical to CX Cloud Agent.
- Devices must be associated to a site for enabling the syslog forwarding from the device to CX Cloud Agent.
- When a syslog server setting is updated, all devices associated with that site are automatically set to default critical level.

Enable Information Level Syslog Settings

To make Syslog Information level visible, perform the these steps:

1. Navigate to Tools > Telemetry.

Tools Menu

2. Select and expand the Site View and select a site from site hierarchy.

Site View

3. Select the required site and select all devices using the Device name check box.

4. From the Actions drop-down, select Optimal Visibility.

Actions

Security

CX Cloud Agent assures the customer of end-to-end security. The connection between CX Cloud and CX Cloud Agent is encrypted. CX Cloud Agent's Secure Socket Shell (SSH) supports 11 different ciphers.

Physical Security

Deploy CX Cloud Agent OVA image in a secured VMware server firm. The OVA is shared securely through Cisco software download center. Bootloader (single user mode) password is set with a randomly unique password. Users must refer to FAQ to set this bootloader (single-user mode) password.

User Access

CX Cloud users can only get authentication and access the Cloud Agent APIs.

Account Security

On deployment, the cxcadmin user account is created. Users are forced to set a password during the initial configuration. cxcadmin user/credentials are used to access both the CX Cloud Agent APIs and to connect the appliance over SSH.

The cxcadmin user has restricted access with the least privileges. The cxcadmin password follows the security policy and is one-way hashed with an expiry period of 90 days. The cxcadmin user can create a cxcroot user using the utility called remoteaccount. The cxcroot user can gain root privileges. Passphrase expires in two days.

Network Security

The CX Cloud Agent VM can be accessed using ssh with cxcadmin user credentials. Incoming ports are restricted to 22 (SSH), 514(Syslog).

Authentication

Password based authentication: Appliance maintains a single user - ‘cxcadmin’ which enables the user to authenticate and communicate with the CX Cloud Agent.

- Root privileged actions on the appliance using ssh cxcadmin user can create cxcroot user, using a utility called remoteaccount. This utility displays an RSA/ECB/PKCS1v1_5 encrypted password which can be decrypted only from SWIM portal (https://swims.cisco.com/abraxas/decrypt). Only authorized personnel have access to this portal. cxcroot user can gain root privileges using this decrypted password. Passphrase is valid only for two days. cxcadmin user needs to recreate the account and get the password from SWIM portal post password expiry.

Hardening

CX Cloud Agent appliance follows CIS hardening standards.

Data Security

CX Cloud Agent appliance does not store any customer personal information.

Device credential application (running as one of the pods) stores encrypted Cisco DNA Center server credentials inside secured database. Cisco DNA Center collected data is not stored in any form inside the appliance. The data collected is uploaded to the backed soon after the collection is complete, and the data is purged from the agent.

Data Transmission

The registration package contains the required unique X.509 device certificate and keys to establish secure connection with Iot Core. Using that agent establishes a secure connection using MQTT over TLS v1.2

Logs and Monitoring

Logs do not contain any form of sensitive information. Audit logs capture all security-sensitive actions performed on the CX Cloud Agent appliance.

Security Summary

Security Features	Description
Bootloader Password	Bootloader (Single user mode) password is set with a randomly unique password. User must refer FAQ to set his bootloader (single user mode) password.
User Access	SSH: • Access to appliance using cxcadmin user requires credentials created during installation. • Access to appliance using cxcroot user requires credentials to be decrypted using SWIM portal by authorized personnel.
User Accounts	• cxcadmin: This is a default user account created. User can execute CX Cloud Agent application commands using cxcli and has least privileges on the appliance. cxcroot user and its encrypted password is generated using cxcadmin user • cxcroot: cxcadmin can create this user using the utility ‘remoteaccount’. User can gain root privileges with this account.
cxcadmin password policy	• Password is one-way hashed using SHA-256 and stored securely. • Minimum eight (8) characters, that contains three of these categories: upper cases, lower case, numbers, and special characters
cxcroot password policy	• cxcroot password is RSA/ECB/PKCS1v1_5 encrypted. • The passphrase generated needs to be decrypted in SWIM portal. • The cxcroot user and password is valid for max two days and can be regenerated using cxcadmin user.
ssh login password policy	• Minimum eight (8) characters, that contains three of these categories: upper cases, lower case, numbers, and special characters. • 5 failed log in attempts will lock the box for 30min. The password expires in 90 days.
Ports	Open Incoming Ports – 514(Syslog) and 22 (SSH)
Data Security	No Customer information stored. No Device data stored.

Cisco DNA Center server credentials encrypted and stored in the database.

Frequently Asked Questions

CX Cloud Agent

Deployment

Q - With "Re-install" option, can the user deploy the new Cloud Agent with new IP Address?

A - Yes

Q - What are the available file formats for installation?

A - OVA and VHD

Q - What is the environment on which the installable can be deployed?

A - OVA

VMWare ESXi version 5.5 or later

Oracle Virtual Box 5.2.30 or later

VHD

Windows Hypervisor 2012 to 2016

Q - Can CX Cloud Agent detect IP address in a DHCP environment?

A - Yes, in case of DHCP environment, the IP address assignment during IP configuration is taken care. However, the IP address change expected for the CX Cloud Agent at any point in future is not supported. Also, the customer is recommended to reserve the IP for the Cloud Agent in their DHCP environment.

Q - Does CX Cloud Agent support both IPv4 and IPv6 configuration?

A - No, only IPV4 is supported.

Q - During IP configuration, is IP address validated?

A - Yes, IP address syntax and duplicate IP address assignment will be validated.

Q - What is the approximate time taken for the OVA deployment and IP configuration?

A - The OVA deployment depends on the speed of the network to copy the data. The IP configuration takes approximately 8-10 minutes that includes Kubernetes and container creations.

Q - Is there any limitation with respect to any hardware type?

A - The host machine on which OVA is deployed must meet the requirements provided as part of

the CX portal setup. The CX Cloud Agent is tested with VMware/Virtual box running on a hardware with Intel Xeon E5 processors with vCPU to CPU ratio set at 2:1. If a less powerful processor CPU or larger ratio is used, the performance can degrade.

Q - Can we generate the pairing code anytime?

A - No, the pairing code can be generated only if the Cloud Agent is not registered.

Q - What are the bandwidth requirements between DNACs (for upto 10 clusters or 20 non-clusters) and Agent?

A -The bandwidth is not a constraint when the Agent and DNAC are in the same LAN/WAN network in the customer environment. The minimum required network bandwidth is 2.7 Mbits/sec for inventory collections of 5000 devices +13000 Access Points for an Agent to DNAC connection. If syslogs are collected for L2 insights, minimum required bandwidth is 3.5 Mbits/sec covers for 5000 devices +13000 Access Points for inventory, 5000 devices syslogs and 2000 devices for scans - all run in parallel from Agent.

Releases and Patches

Q - What are the different kinds of versions listed for the upgrade of CX Cloud Agent?

A - Shown here are the set of the released versions of CX Cloud Agent that are listed:

- A.x.0 (where x is the latest production major feature release, example:1.3.0)
- A.x.y (where A.x.0 is mandatory and incremental upgrade to be initiated, x is the latest production major feature release, and y is the latest upgrade patch that is live, example: 1.3.1).
- A.x.y-z (where A.x.0 is mandatory and incremental upgrade to be initiated, x is the latest production major feature release, and y is the latest upgrade patch that is live, and z is the spot-patch that is an instant fix for a very short span of time, example: 1.3.1-1)

where A is a long-term release spread across 3-5 years span.

Q - Where to find the latest released CX Cloud Agent version and how to upgrade the existing CX Cloud Agent?

A - Go to Admin Settings > Data Sources. Click the View Update and perform the instructions shared on screen.

Authentication and Proxy configuration

Q - What is the default user of the CX Cloud Agent Application?

A - cxcadmin

Q - How is the password set for the default user?

A - Password is set during network configuration.

Q - Is there any option available to reset the password after Day-0?

A - No specific option is provided by the agent to reset the password, but you can use the linux commands to reset the password for cxcadmin.

Q - What are the password policies to configure CX Cloud Agent?

A - Password policies are:

- Password maximum age (length) set to 90 days
- Password minimum age (length) set to 8
- Password maximum length 127 characters.
- At least one upper case and one lower case must be provided.
- Must contain at least one special character (for example, !$%^&*()_+|~-=\`{}[]:";'<>?,/).
- These characters are not be permitted Special 8-bit characters (for example, ¬£, Å ´, ¥, ë, ¬ø, ü)Spaces
- The password must not be the last recently used 10 passwords.
- Must not contain regular expression i.e.
- Must not contain these words or derivatives thereof: cisco, sanjose, and sanfran

Q - How to set Grub password?

A - To set the Grub Password, perform these steps:

1. Run ssh as cxcroot and provide the token [Contact the support team to get the cxcroot token]
2. Execute sudo su, provide the same token
3. Execute the command grub-mkpasswd-pbkdf2 and set the GRUB password. Hash of the provided password will be printed, copy the content.
4. vi to the file /etc/grub.d/00_header**.** Navigate to the end of file and replace the hash output followed by the content password_pbkdf2 root ***** with the obtained hash for the password you got in step 3
5. Save the file with the command :wq!
6. Execute the command update-grub

Q - What is the expiry period for password of cxcadmin?

A - The password expiry in 90 days.

Q - Does the system disable the account after consecutive unsuccessful login attempts?

A - Yes, the account gets disabled after 5 consecutive unsuccessful attempts. The lockout period is 30 minutes.

Q - How to generate passphrase?

A - Perform these steps,

1. Run ssh and login as cxcadmin user
2. Execute the command *remoteaccount cleanup -f*
3. Execute the command *remoteaccount create*

Q - Does proxy host support both hostname and IP?

A - Yes, but to use hostname, user must provide the DNS IP during network configuration.

Secure Shell SSH

Q - What are the ciphers supported by ssh shell?

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

Q - How to login to console?

A - Follow the steps to login:

1. Login as cxcadmin user.
2. Provide the cxcadmin password.

Q - Are SSH logins logged?

A - Yes, they are logged as part of the var/logs/audit/audit.log.

Q - What is the idle session out time?

A - SSH session timeout occurs if the Cloud Agent is idle for five (5) minutes.

Ports and Services

Q - What are the ports kept open by default on the CX Cloud Agent?

A - These ports are available:

- Outbound port: The deployed CX Cloud Agent can connect to Cisco backend as indicated in the table on HTTPS port 443 or via a proxy to send data to Cisco. The deployed CX Cloud Agent can connect to Cisco DNA Center on HTTPS port 443.

.

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	agent.emea.csco.cloud	agent.apjc.csco.cloud
ng.acs.agent.us.csco.cloud	ng.acs.agent.emea.csco.cloud	ng.acs.agent.apjc.csco.cloud

Note: In addition to the domains listed, when EMEA or APJC customers reinstall the Cloud Agent, the domain agent.us.csco.cloud must be allowed in the customer firewall.

The domain agent.us.csco.cloud is no longer needed after successful reinstallation.

Note: Ensure that return traffic must be allowed on port 443.

- Inbound port: For local management of the CX Cloud Agent, 514(Syslog) and 22 (ssh) must be accessible. The customer must allow port 443 in their firewall to receive data from CX Cloud.

CX Cloud Agent Connection with Cisco DNA Center

Q - What is the purpose and relationship of Cisco DNA Center with CX Cloud Agent r?

A - Cisco DNA Center is the Cloud Agent that manages the customer premise network devices. CX Cloud Agent collects the inventory information of the devices from the configured Cisco DNA Center and uploads the inventory information that is available as “Asset View” in CX Cloud.

Q - Where can the user provide Cisco DNA Center details on the CX Cloud agent?

A - During the Day 0 - CX Cloud Agent setup, the user can add the Cisco DNA Center details from CX Cloud portal. In addition, during Day N operations, users can add additional DNA Centers from Admin Settings > Data source.

Q - How many Cisco DNA Centers can be added?

A - Either 10 Cisco DNAC clusters.or 20 DNAC non-clusters.

Q - What role the Cisco DNA Center user can have?

A - The user role can be either admin or observer.

Q – How to reflect the modifications in CX Agent due to changes in connected DNA Center credentials?

A - Execute these command from the CX Cloud Agent console:

cxcli agent modifyController

Contact support for any issues during DNAC credentials update.

Q - How are the Cisco DNA Center details stored in CX Cloud Agent?

A - Cisco DNA Center credentials are encrypted using AES-256 and stored in CX Cloud Agent database. CX Cloud Agent database is protected with a secured user ID and password.

Q - What kind of encryption will be used while accessing Cisco DNA Center API from CX Cloud Agent?

A - HTTPS over TLS 1.2 is used for the communication between Cisco DNA Center and CX Cloud Agent.

Q - What are the operations performed by CX Cloud Agent on the integrated Cisco DNA Center Cloud Agent?

A - CX Cloud Agent collects data that Cisco DNA Center has about the network devices and uses the Cisco DNA Center command runner interface to talk to end devices and execute CLI commands (show command). No config change commands are executed

Q - What are default data collected from Cisco DNA Center and uploaded to backend?

A-

- Network Entity
- Modules

- Show version
- Config
- Device image information
- Tags

Q - What are the additional data collected from Cisco DNA Center and uploaded to Cisco backend?

A - You get all the information here.

Q - How is the inventory data uploaded to backend?

A - CX Cloud Agent uploads the data via TLS 1.2 protocol to Cisco backend server.

Q - What is the frequency of inventory upload?

A - Collection is triggered as per the user-defined schedule and is uploaded to the Cisco backend.

Q - Can the user re-schedule inventory?

A - Yes, an option is available to modify the schedule information from Admin Settings> Data Sources.

Q - When does the connection timeout occur between Cisco DNA Center and Cloud Agent?

A - Timeouts are categorizes as follows:

- For initial connection, timeout is max 300 seconds. If connection is not established between Cisco DNA Center and Cloud Agent within max 5 minutes, then the connection terminates.
- For recurring, typical, or updates: response timeout is 1800 seconds. If the response is not received or not able to read within 30 minutes, then the connection terminates.

CX Cloud Agent Used Diagnostic Scan

Q - What are the commands executed on the device for scan?

A - Commands that need to be executed on the device for the scan are dynamically determined during the scanning process. The set of commands can change over time, even for the same device (and not in control of Diagnostic Scan).

Q - Where are the scan results stored and profiled?

A - The scanned results are stored and profiled in Cisco backend.

Q - Are the duplicates (By hostname or IP) in Cisco DNA Center, added to Diagnostic Scan when Cisco DNA Center source is plugged in?

A - No, duplicates will be filtered and only the unique devices will be extracted.

Q - What happens when one of the command scans fails?

A - The device scan will be completely stopped and will be marked as unsuccessful.

CX Cloud Agent System Logs

Q - What health information is sent to the CX Cloud?

A - Application logs, Pod status, Cisco DNA Center details, audit logs, system details, and hardware details.

Q - What system details and hardware details are collected?

A - Sample output:


```
system_details":{
"os_details":{
"containerRuntimeVersion":"docker://19.3.12",
"kernelVersion":"5.4.0-47-generic",
"kubeProxyVersion":"v1.15.12",
"kubeletVersion":"v1.15.12",
"machineID":"81edd7df1c1145e7bcc1ab4fe778615f",
"operatingSystem":"linux",
"osImage":"Ubuntu 20.04.1 LTS",
"systemUUID":"42002151-4131-2ad8-4443-8682911bdadb"
},
"hardware_details":{
"total_cpu":"8",
"cpu_utilization":"12.5%",
"total_memory":"16007MB",
"free_memory":"9994MB",
"hdd_size":"214G",
"free_hdd_size":"202G"
}
}
}
```


Q - How is the health data sent to backend?

A - With CX Cloud Agent, the health service (servicability) streams the data to Cisco backend.

Q - What is the CX Cloud Agent’s health data log retention policy in the backend?

A - The CX Cloud Agent’s health data log retention policy in the backend is 120 days.

Q - What are the types of uploads available?

A - Three types of uploads available,

1. Inventory upload
2. Syslog upload
3. Agent Health upload: 3 things as part of health upload Services health – every 5 minutesPodlog – every 1 hourAudit log – every 1 hour

Troubleshooting

Issue: Not able to access the configured IP.

Solution: Execute ssh using configured IP. If connection times out, the possible reason is IP misconfiguration. In this case, reinstall by configuring a valid IP. This can be done via portal with the reinstall option provided in the Admin Setting page.

Issue: How to verify if the services are up and running after the registration?

Solution: Execute the command shown here and verify if the pods are up and running.

1. ssh to the configured IP as cxcadmin.
2. Provide the password.
3. Execute the command *kubectl get pods*.

The pods can be in any state such as running, Initializing, or Container creating but after 20 minutes, the pods must be in running state.

If state is *is not running* or *Pod Initialaizing*, check the pod description with the command shown here

kubectl describe pod <podname>

The output will have the information on the pod status.

Issue: How to verify whether SSL Interceptor is disabled at customer Proxy?
Solution: Execute the curl command shown here to verify the server certificate section. The response has the certificate details of concsoweb server.

curl -v --header 'Authorization: Basic xxxxxx' https://concsoweb-prd.cisco.com/

* Server certificate:

* subject: C=US; ST=California; L=San Jose; O=Cisco Systems, Inc.; CN=concsoweb-prd.cisco.com

* start date: Feb 16 11:55:11 2021 GMT

* expire date: Feb 16 12:05:00 2022 GMT

* subjectAltName: host "concsoweb-prd.cisco.com" matched cert's "concsoweb-prd.cisco.com"

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

* SSL certificate verify ok.

>GET / HTTP/1.1

Issue: kubectl commands failed and shows the error as “The connection to the server X.X.X.X:6443 was refused - did you specify the right host or port”
Solution:

- Verify for resource availability. [example: CPU, Memory]
- Wait for the Kubernetes service to start

Issue: How to get the details of collection failure for a command/device

Solution:

- Execute `kubectl get pods` and get the collection pod name.
- Execute `kubectl logs <collectionPodName>` to get the command/device specific details.

Issue: kubectl command not working with error "[authentication.go:64] Unable to authenticate the request due to an error: [x509: certificate has expired or is not yet valid, x509: certificate has expired or is not yet valid]"

Solution:Run the commands shown here as *cxcroot* user

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

Collection Failure Responses

Collection failure cause can be any constraints or issues seen with the added controller or devices present in the controller.

The table shown here has the error snippet for use cases seen under the Collection microservice during the collection process.

Use Case	Log Snippet in collection microservice

If the requested device is not found in Cisco DNA Center	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": " No device found with id 02eb08be-b13f-4d25-9d63-eaf4e882f7
	}

If the requested device is not reachable from Cisco DNA Center	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "Error occurred while executing command: show version\nError connecting to device [Host: 172.21.137.221:22]No route to host : No route to host
	}

If the requested device is not reachable	{

from Cisco DNA Center	"command": "show version", "status": "Failed", "commandResponse": "", "errorMessage": "Error occured while executing command : show version\nError connecting to device [Host: X.X.X.X]Connection timed out: /X.X.X.X:22 : Connectio timed out: /X.X.X.X:22" }

If the requested command is not available in device	{
	"command": "show run-config",
	"status": "Success",
	"commandResponse": " Error occured while executing command : show run-config\n\nshow run-config\n ^\n% Invalid input detected at \u0027^\u0027 marker.\n\nXXCT5760#",
	"errorMessage": ""
	}

If the requested device does not have SSHv2 and Cisco DNA Center tries to connect the device with SSHv2	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "Error occured while executing command : show version\nSSH2 closed : Remote party uses incompatible protocol, it is not SSH-2 compatible."
	}

If command is disabled in Collection microservice	{
	"command": "config paging disable",
	"status": "Command_Disabled",
	"commandResponse": "Command collection is disabled",
	"errorMessage": ""
	}

If the Command Runner Task failed and task URL is not returned by Cisco DNA Center	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "The command runner task failed for device %s. Task URL is em
	}

If the Command Runner Task failed to get created in Cisco DNA Center	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "The command runner task failed for device %s, RequestURL: % task details."
	}

If the Collection microservice not receiving response for a Command Runner request from Cisco DNA Center	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "The command runner task failed for device %s, RequestURL: %
	}

If Cisco DNA Center is not completing the task within the configured timeout (5 mins per command in Collection microservice)	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "Operation Timedout. The command runner task failed for device RequestURL: %s. No progress details."
	}

If the Command Runner Task failed and file ID is empty for the submitted task by Cisco DNA Center	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "The command runner task failed for device %s, RequestURL: % id is empty."
	}

If the Command Runner Task failed and file ID tag is not returned by Cisco DNA Center	{ "command": "show version", "status": "Failed",

If the device is not eligible for command runner execution	"commandResponse": "",
	"errorMessage": "The command runner task failed for device %s, RequestURL: %
	file id details."
	}
	{
	"command": "config paging disable",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "Requested devices are not in inventory,try with other devices a
	in inventory"
	}

If the command runner is disabled for the user	{
	"command": "show version",
	"status": "Failed",
	"commandResponse": "",
	"errorMessage": "{\"message\":\"Role does not have valid permissions to access th
	API\"}\n"
	}

Diagnostic Scan Failure Responses

Scan failure and the cause can be from any of the listed components

When the user initiates a scan from the portal, occasionally it results as “failed: Internal server error”

The cause for the issue can be any of the listed components

- Control Point
- Network Data Gateway
- Connector
- Diagnostic Scan
- CX Cloud Agent Microservice [devicemanager, collection]
- Cisco DNA center
- APIX
- Mashery
- Ping Access
- IRONBANK
- IRONBANK GW
- Big Data Broker (BDB)

To see the logs:

1. Log into the CX Cloud Agent console
2. ssh to cxcadmin and provide the password
3. Execute kubectl get pods
4. Obtain the pod name of collection, connector, and servicability.
5. To verify the collection, connector, and servicability microservice logs

- Execute kubectl logs <collectionpodname>
- Execute kubectl logs <connector>
- Execute kubectl logs <servicability>

The table shown here displays the error snippet seen under Collection microservice and servicability microservice logs that occurs due to the issues/constraints with the components.

Use case	Log snippet in collection microser
The device can be reachable and supported, but the commands to execute on that device is block-listed on the Collection microservice	{ "command": "config paging disable", "status": "Command_Disabled", "commandResponse": "Command collection is disabled", }
If the device which is attempted for scan is not available. Occurs in a scenario, when there is a sync issue between the components such as portal, diagnostic Scan, CX component, and Cisco DNA Center	No device found with id 02eb08be-b13f-4d25-9d6 eaf4e882f71a
If the device that is attempted for scan is busy, (in a scenario) where the same device is been part of other job and no parallel requests are handled from Cisco DNA Center for the device.	All requested devices are already being queried b command runner in another session. Please try o devices".
If the device is not supported for scan	Requested devices are not in inventory, try with o devices available in inventory
If the device attempted for scan is unreachable	"Error occurred while executing command: show udi\nError connecting to device [Host: x.x.x.x:22] route to host : No route to host
If Cisco DNA Center is not reachable from Cloud Agent or Collection microservice of the Cloud Agent is not receiving response for a Command Runner request from Cisco DNA Center	{ "command": "show version", "status": "Failed", "commandResponse": "", "errorMessage": "The command runner task faile device %s, RequestURL: %s." }

Use Case	Log snippet in Control Point Agent microservice
If the scan request has schedule details missing	Failed to execute request {"message":"23502: null value in column \"schedule\" violates not-null constraint"}
If the scan request has device details missing	Failed to create scan policy. No valid devices in the request
If the connection between the CPA and connectivity is down	Failed to execute request.
If the requested device for scan is not available in Diagnostic Scans	Failed to submit the request to scan. Reason = {\"message\":\"Device wit Hostname=x.x.x.x' was not found\"}