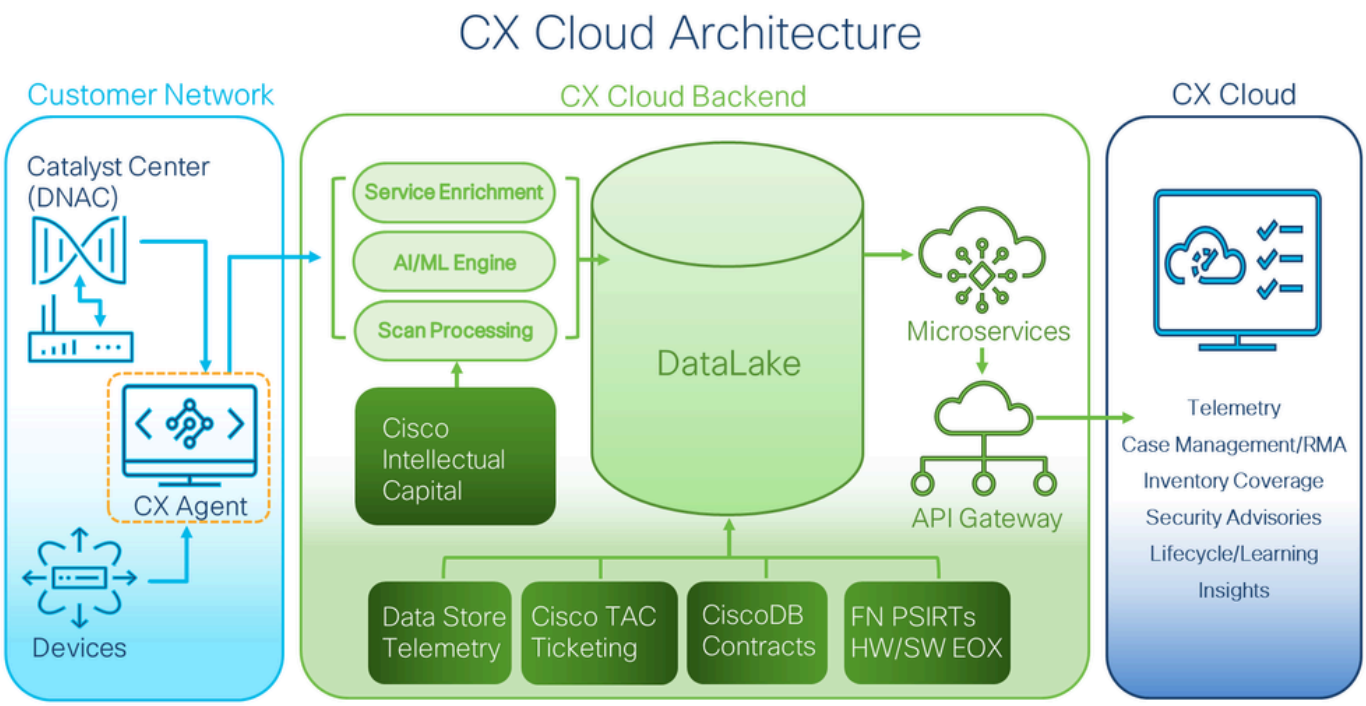
CX雲代理概述v2.2

目錄

簡介

本檔案介紹思科的客戶體驗(CX)雲代理。思科(CX)雲代理是一個高度可擴展的平台，可從客戶網路裝置收集遙測資料，為客戶提供切實可行的見解。CX雲代理支援將活動運行配置資料轉換為在CX雲中顯示的主動和預測性見解的人工智慧(AI)/機器學習(ML)。

本指南特定於CX雲代理v2.2及更高版本。請參閱Cisco CX雲代理頁面以訪問以前的版本。



CX雲架構

註：本指南中的影象（及其內容）僅供參考。實際內容可能有所不同。

必要條件

CX Cloud Agent 以虛擬機器 (VM) 的形式執行，並且可做為開放式虛擬裝置 (OVA) 或虛擬硬碟 (VHD) 下載。

部署要求：

- 以下任何虛擬機器監控程式：
  - VMware ESXi版本5.5或更高版本
  - Oracle Virtual Box 5.2.30或更高版本
  - Windows虛擬機器監控程式版本2012到2022
- 虛擬機器監控程式可以託管具有以下要求的虛擬機器：
  - 8 核心 CPU
  - 16 GB 記憶體/RAM
  - 200 GB 磁碟空間
- 對於使用指定美國資料中心作為儲存CX雲資料的主要資料區域的客戶，CX雲代理必須能夠連線到此處顯示的伺服器，使用完全限定域名(FQDN)，並在TCP埠443上使用HTTPS:
  - FQDN: agent.us.csco.cloud
  - FQDN: ng.acs.agent.us.csco.cloud
  - FQDN:cloudsso.cisco.com
  - FQDN:api-cx.cisco.com
- 對於使用指定歐洲資料中心作為主要資料區域來儲存CX雲資料的客戶：CX雲代理必須能夠連線到此處所示的兩個伺服器，使用FQDN，並在TCP埠443上使用HTTPS:
  - 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
- 對於將指定的亞太地區資料中心用作儲存CX雲資料的主要資料區域的客戶：CX雲代理必須能夠連線到此處所示的兩個伺服器，使用FQDN，並在TCP埠443上使用HTTPS:
  - 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
- 對於使用指定的歐洲和亞太地區資料中心作為其主要資料區域的客戶，僅在初始設定期間向CX雲註冊CX雲代理時需要連線到FQDN:agent.us.csco.cloud。成功向CX雲註冊CX雲代理後，不再需要此連線。
- 對於CX雲代理的本地管理，埠22必須可訪問。
- 下表彙總了必須開啟和啟用CX雲代理才能正常運行的埠和協定：

					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

其他附註：

- 如果在VM環境中啟用了動態主機配置協定(DHCP)，則自動檢測到IP；否則，必須提供可用IPv4地址、子網掩碼、預設網關IP地址和域名服務(DNS)伺服器IP地址
- 僅支援IPv4
- 經認證的單節點和高可用性(HA)集群Cisco DNA中心版本為2.1.2.x到2.2.3.x、2.3.3.x、2.3.5.x和Cisco Catalyst中心虛擬裝置和Cisco DNA中心虛擬裝置
- 如果網路具有SSL攔截，則允許清單CX雲代理的IP地址
- 對於所有直連資產，需要15級的SSH許可權
- 僅使用提供的主機名；不應使用靜態IP地址

關鍵網域存取

若要啟動 CX Cloud 歷程，使用者需要存取下列網域。僅使用提供的主機名；不使用靜態IP地址。

特定於CX雲代理門戶的域

主要網域	其他域
cisco.com	mixpanel.com
csco.cloud	cloudfront.net
split.io	eum-appdynamics.com
	appdynamics.com
	tiqcdn.com
	jquery.com

CX雲代理OVA特定的域

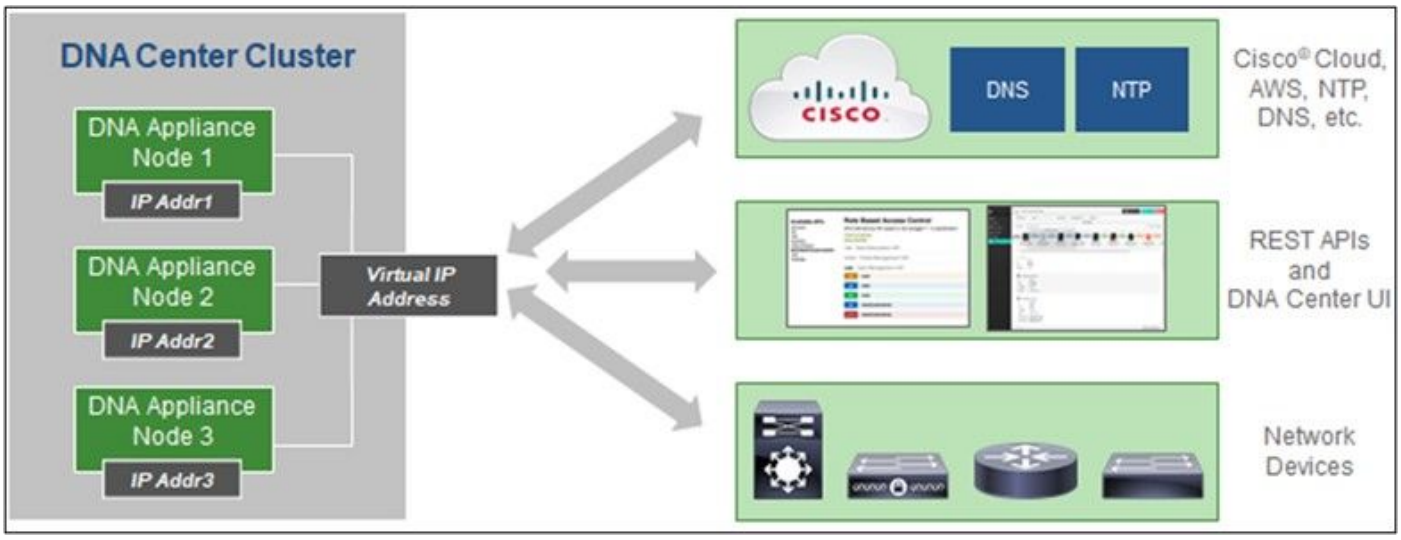
美洲	歐洲、中東和非洲	亞太地區、日本及中國
cloudsso.cisco.com	cloudsso.cisco.com	cloudsso.cisco.com
api-cx.cisco.com	api-cx.cisco.com	api-cx.cisco.com

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

注意：必須在埠443上為指定FQDN啟用重定向的情況下允許出站訪問。

Cisco DNA Center支援的版本

支援的單節點和HA集群Cisco DNA中心版本為2.1.2.x到2.2.3.x、2.3.3.x、2.3.5.x和Cisco Catalyst中心虛擬裝置和Cisco DNA中心虛擬裝置。



多節點 HA 叢集 Cisco DNA 中心

支援的瀏覽器

要獲得Cisco.com上的最佳體驗，建議使用以下瀏覽器的最新正式版本：

- Google Chrome
- Microsoft Edge
- Mozilla Firefox

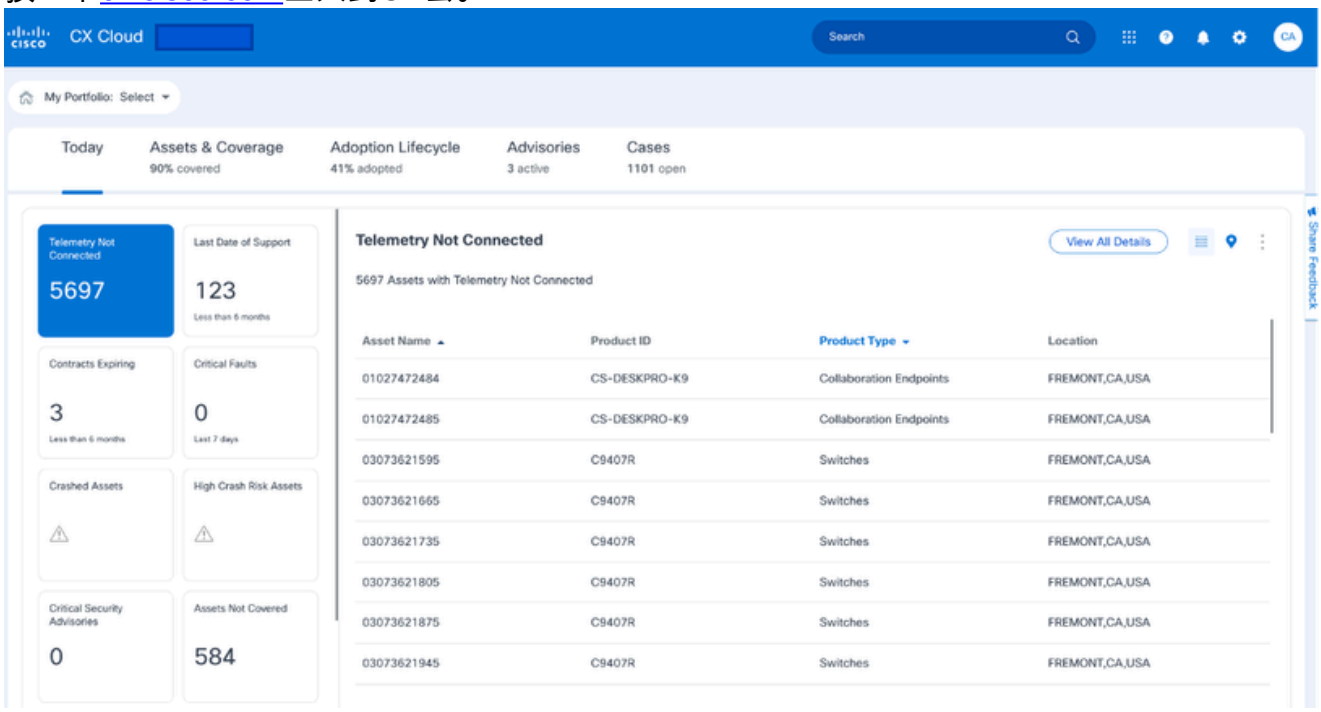
支援的產品清單

要檢視CX雲代理支援的產品清單，請參閱支援的產品清單。

連線資料來源

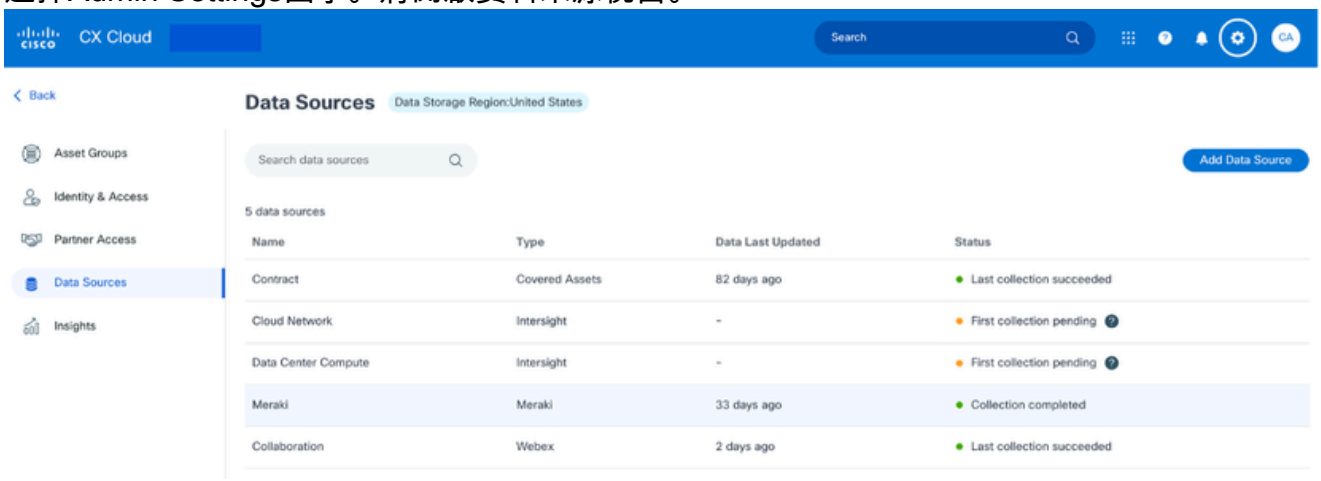
要連線資料來源：

1. 按一下cx.cisco.com登入到CX雲。



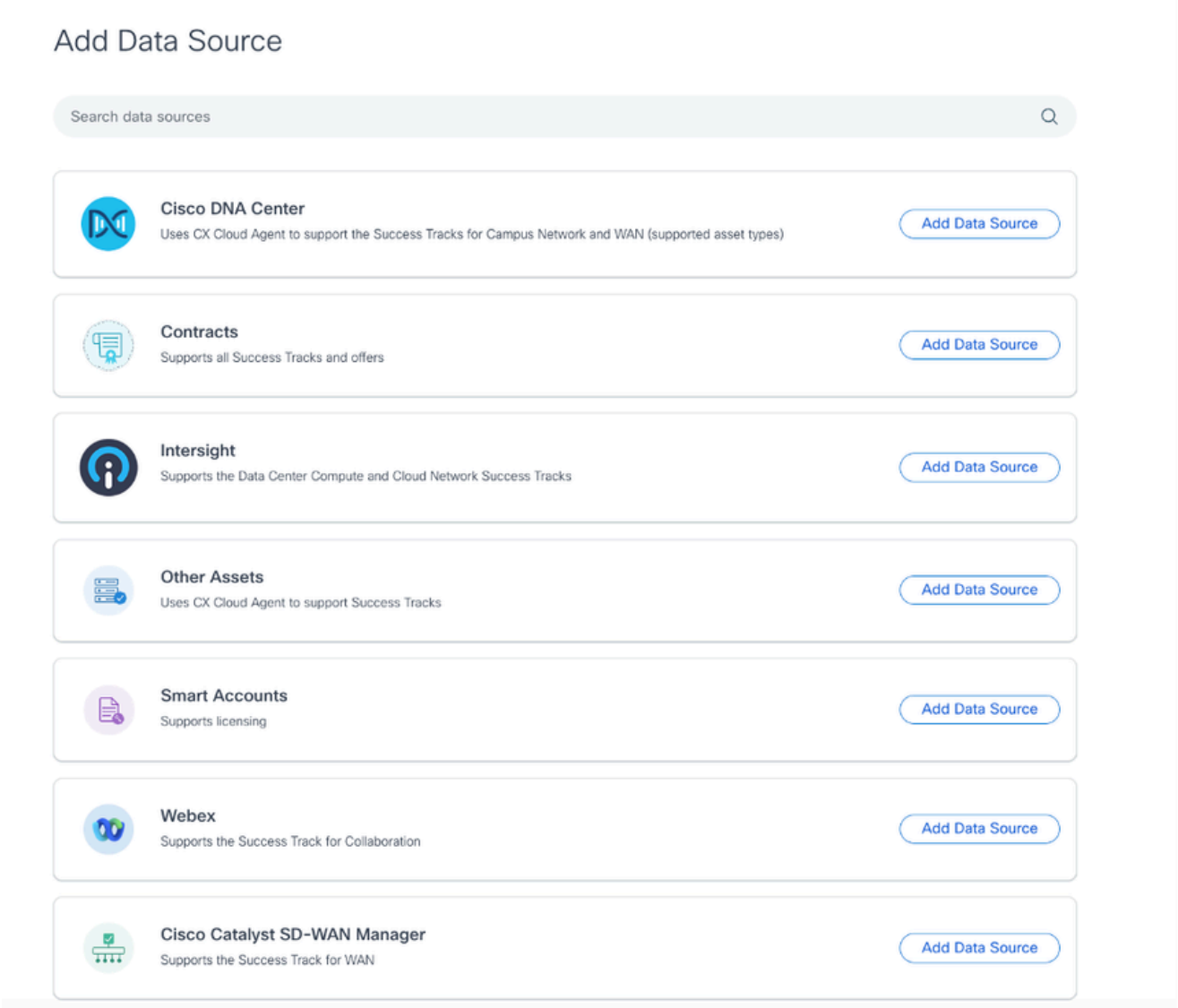
CX雲首頁

2. 選擇Admin Settings圖示。將開啟資料來源視窗。



資料來源

3. 按一下Add Data Source。Add Data Source視窗開啟。 顯示的選項可能因客戶預訂而異。



新增資料來源

4. 按一下Add Data Source以選擇適用的資料來源。如果之前未設定CX雲代理，則會開啟設定CX雲代理視窗，必須在此完成設定。如果設定完成，連線將繼續。請參閱以下章節之一以繼續：

設定CX雲代理

新增Cisco DNA Center作為資料來源

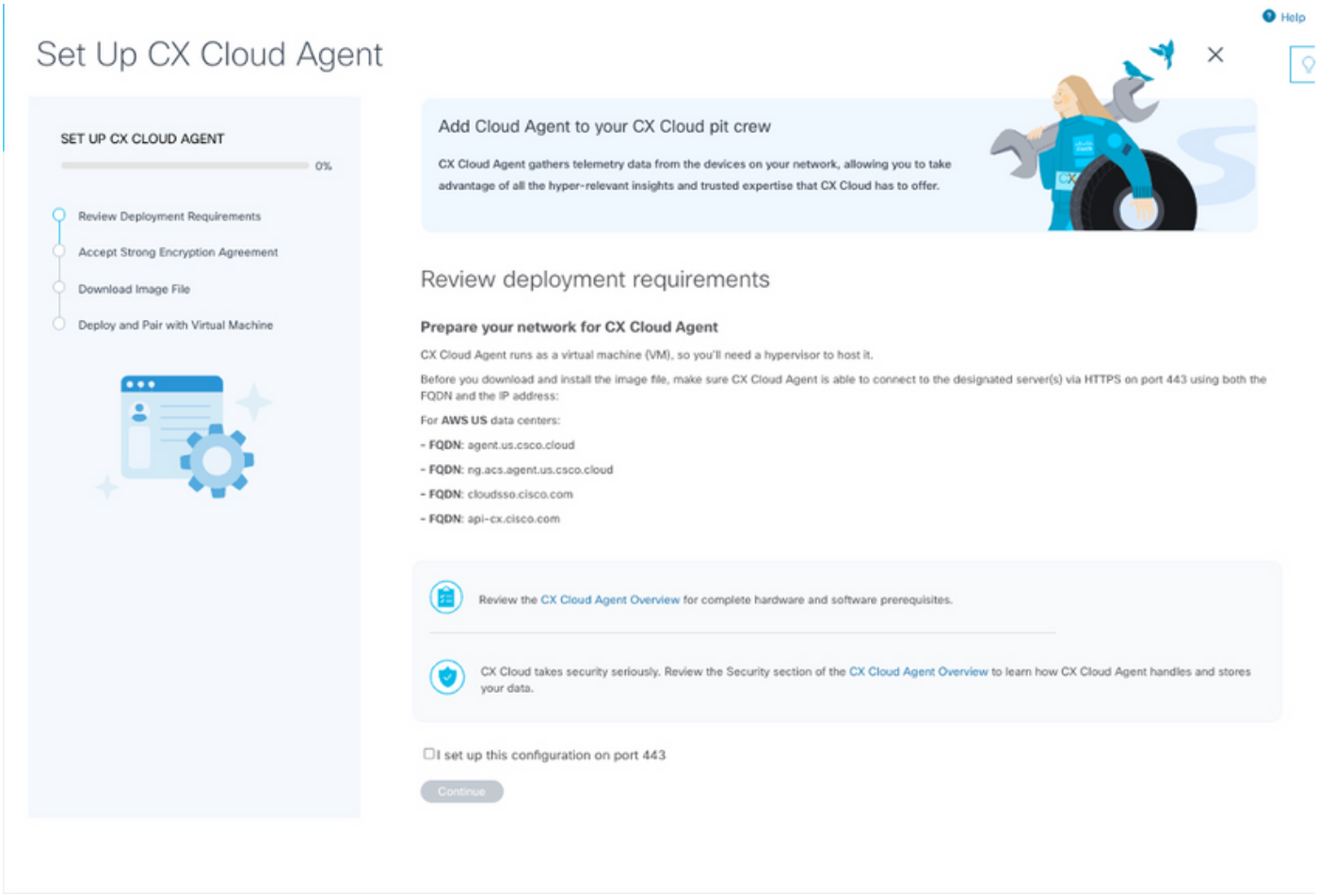
新增其他資產作為資料來源

注意：只有在以前未配置直接裝置連線的情況下，Other Assets選項才可用。

設定CX雲代理

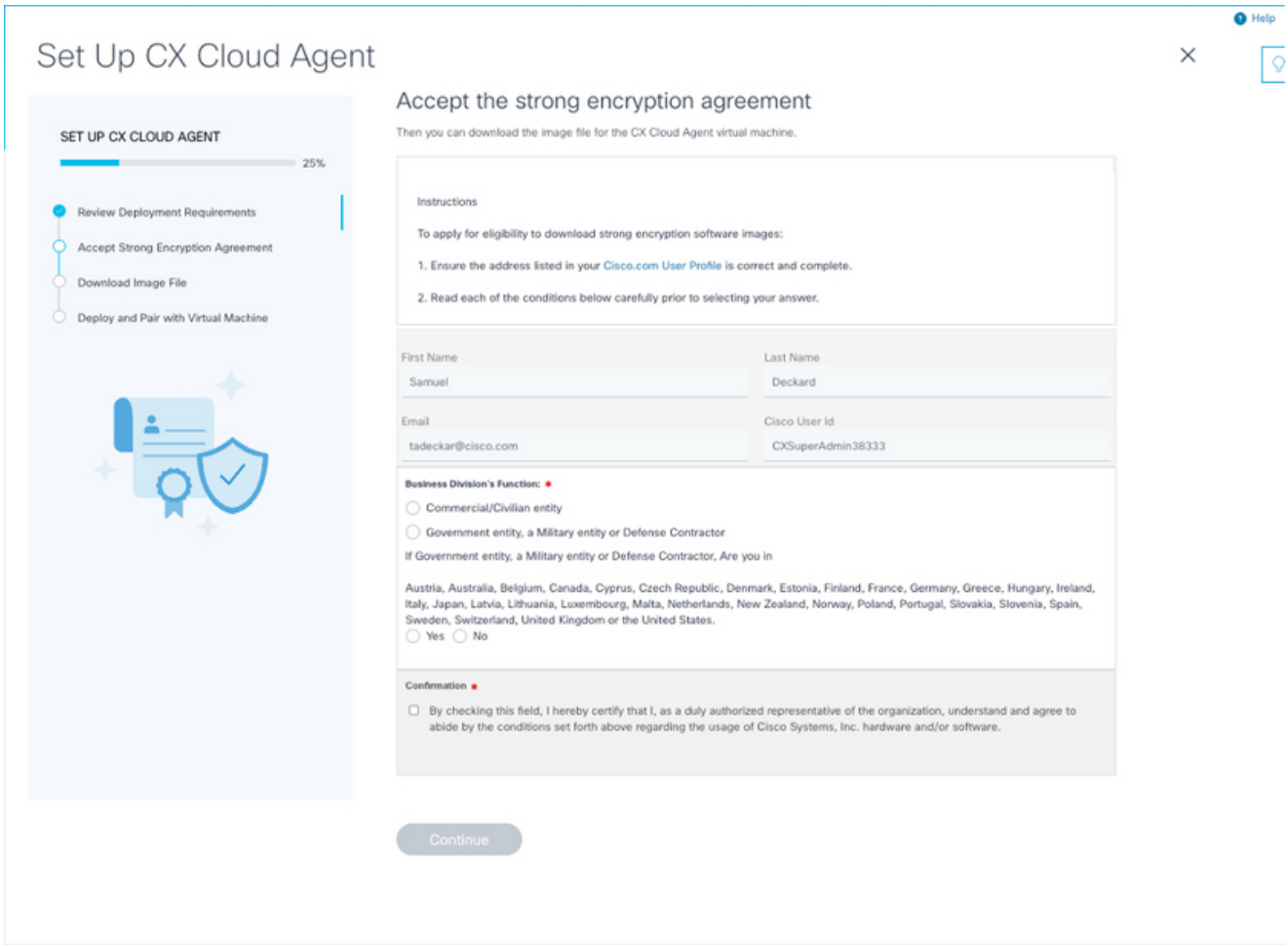
如果之前未完成連線資料來源，則在連線資料來源時提示設定CX雲代理。

要設定CX雲代理：



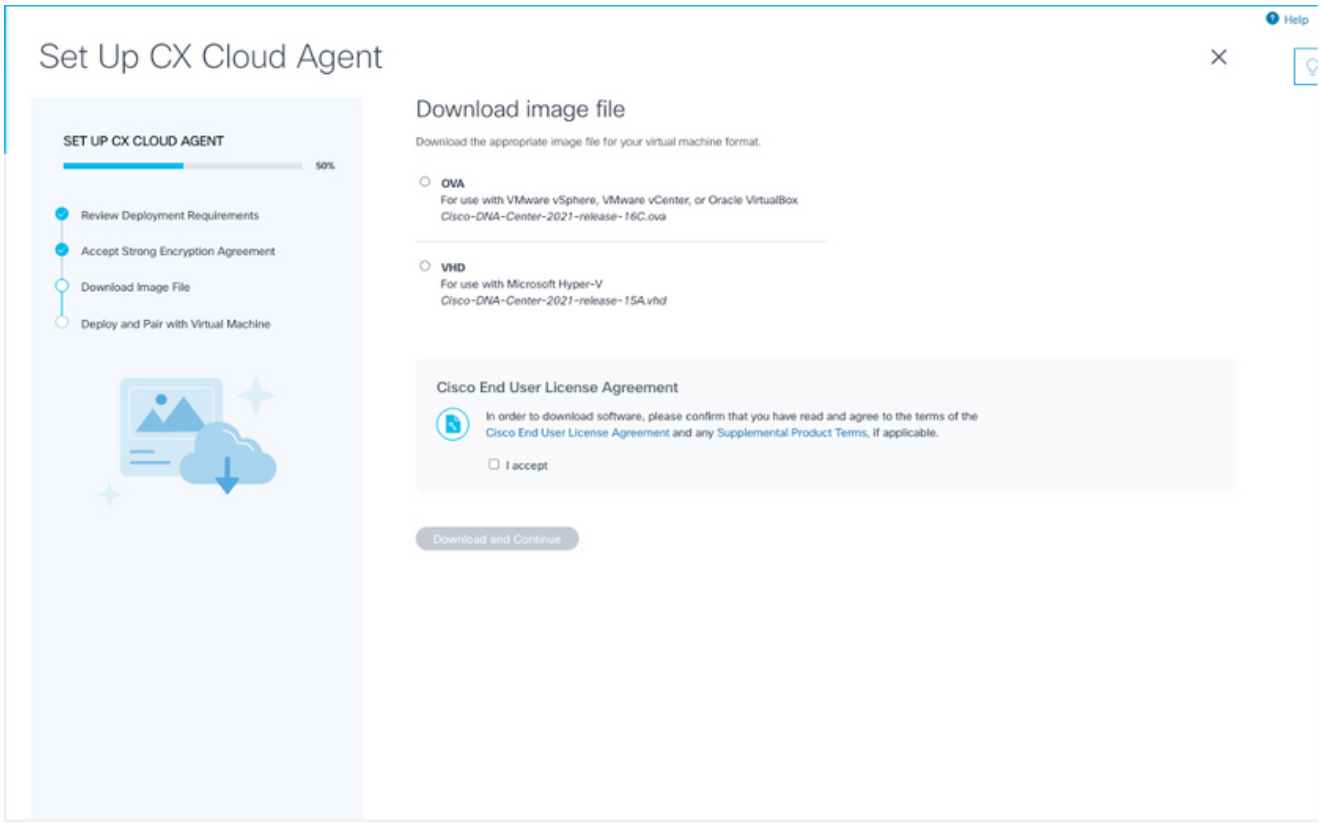
檢視部署要求

1. 檢視檢視部署要求，並選中I set up this configuration on port 443覈取方塊。
2. 按一下「Continue」（繼續）。此時將開啟「設定CX雲代理 — 接受強加密協定」視窗。



加密合約

3. 驗證First Name、Last Name、E-mail和Cisco User Id欄位中預先填充的資訊。
4. 選擇相應的業務部門的功能。
5. 選取「Confirmation」（確認）選取方塊，以同意使用條件。
6. 按一下「Continue」（繼續）。「設定CX雲代理 — 下載映像檔案」視窗開啟。



下載影像

7. 選擇適當的檔案格式下載安裝所需的映像檔案。
8. 選中I accept覈取方塊以同意思科終端使用者許可協定。
9. 按一下「Download and Continue」。「設定CX雲代理 — 部署並與虛擬機器配對」窗口開啟。
10. 請參閱網路配置以獲取下一節中所需的配對代碼。

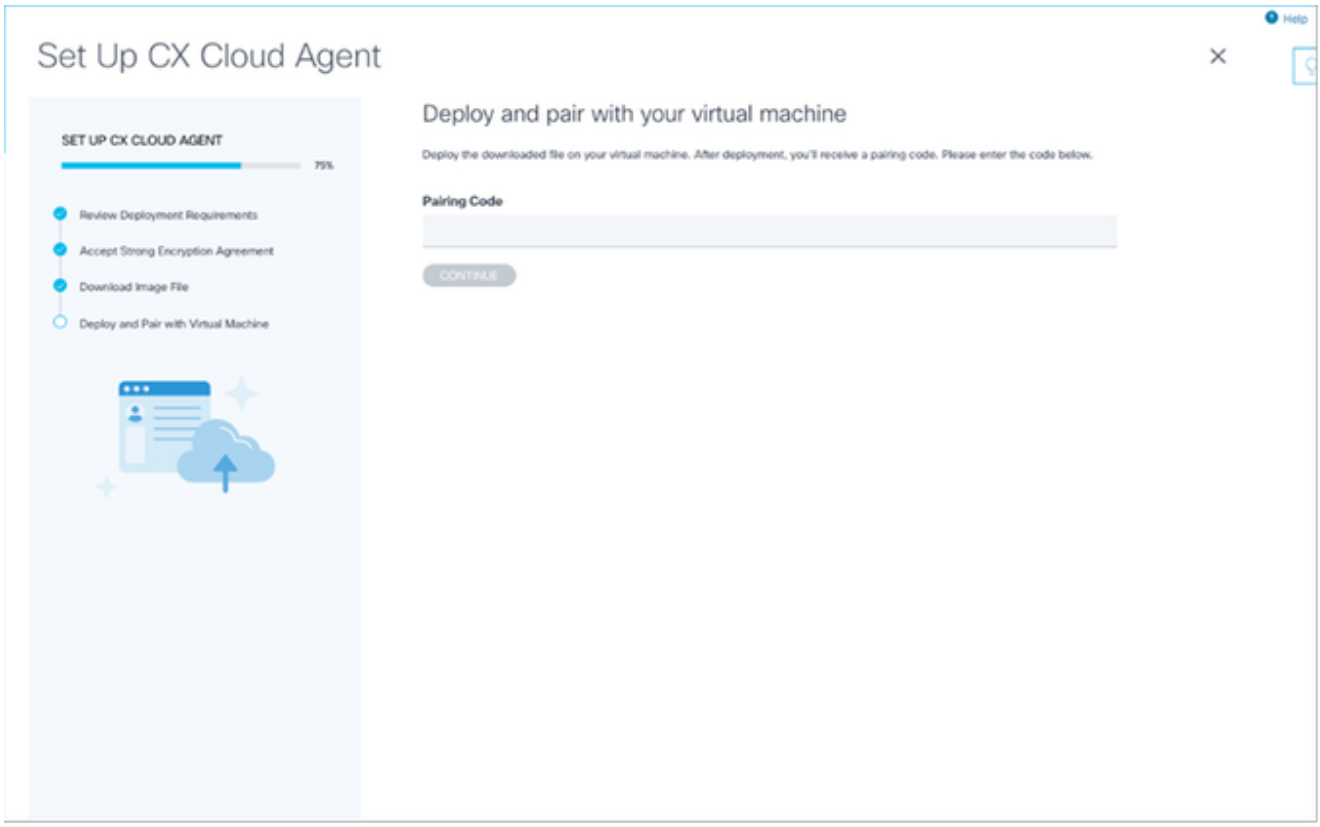
將 CX Cloud Agent 連線至 CX Cloud

要開始遙測收集，需要將CX雲代理連線到CX雲，以便可以更新UI中的資訊以顯示當前資產和見解。本節詳細介紹如何完成連線和故障排除指南。

要將CX雲代理連線到CX雲，請執行以下操作：

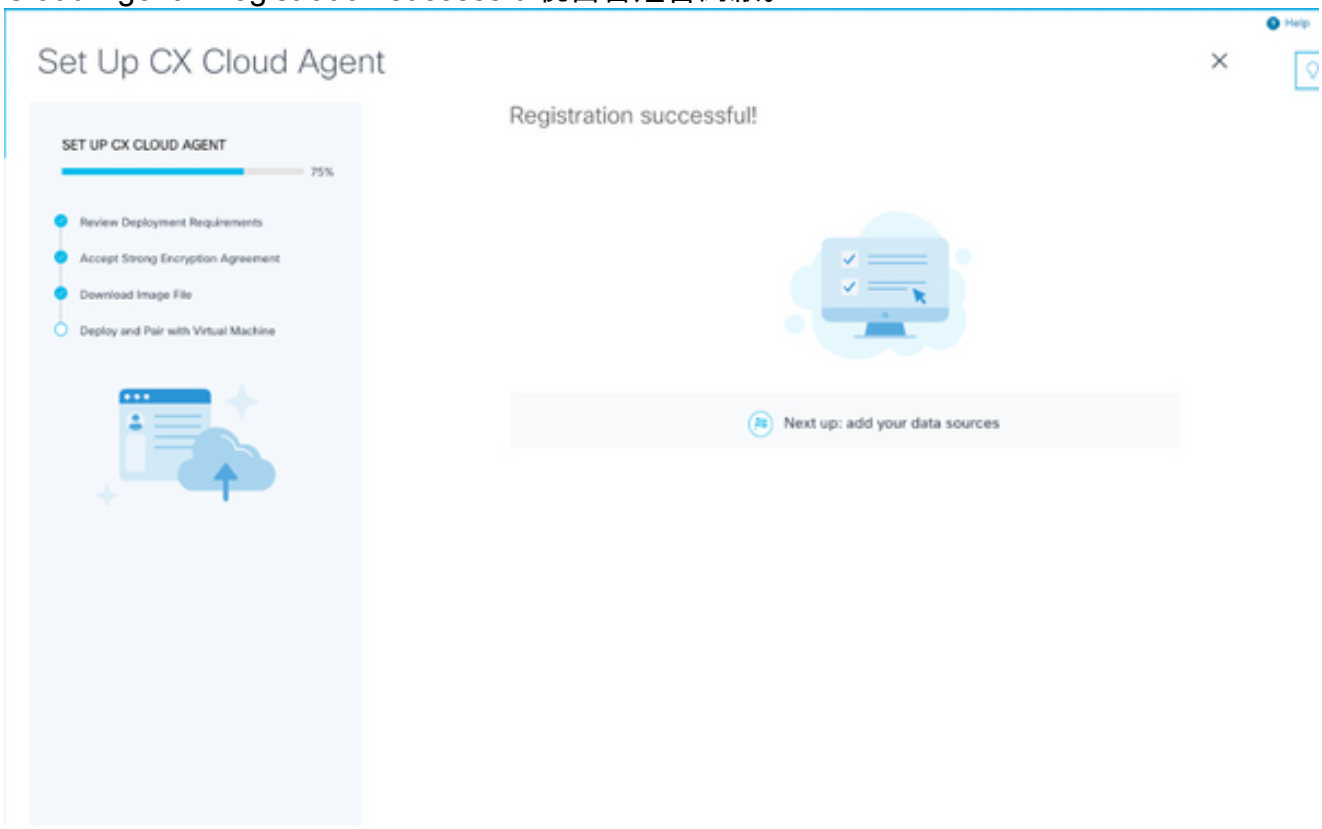
1. 輸入在控制檯對話方塊或通過Agent連線的虛擬機器的Command Line Interface(CLI)中提供的配對代碼。

> 注意：在部署下載的OVA檔案後收到配對代碼。



配對程式碼

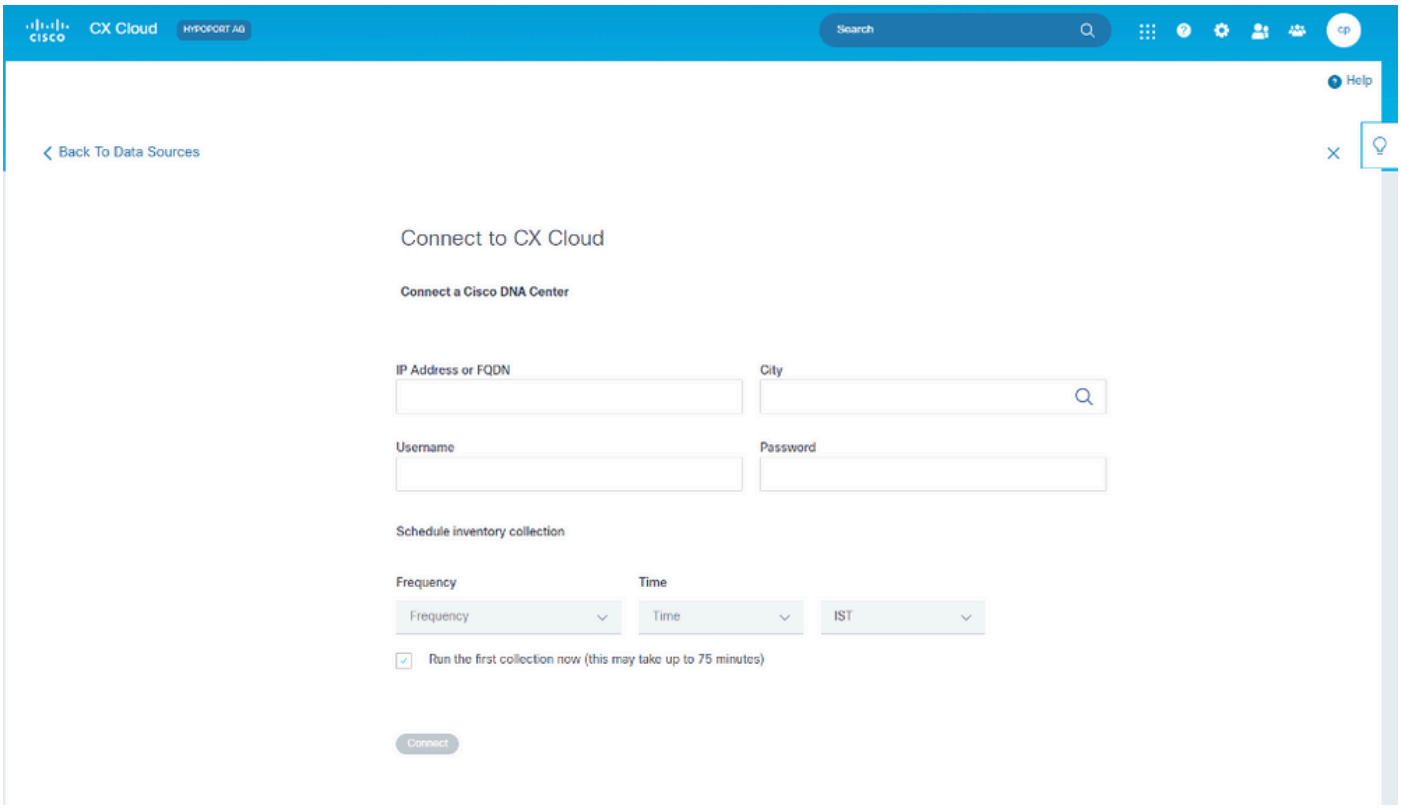
2. 按一下Continue註冊CX雲代理。在自動導航到Add Data Sources頁面之前，Set Up CX Cloud Agent - Registration successful視窗會短暫開啟。



註冊成功

新增Cisco DNA Center作為資料來源

從資料來源連線視窗中選擇Cisco DNA Center(請參閱「連線資料來源」部分的連線資料來源影象)時，將開啟以下視窗：



連線到CX雲

要新增Cisco DNA Center作為資料來源：

1. 輸入Cisco DNA Center IP地址或虛擬IP地址或FQDN、City（Cisco DNA Center的位置）、Username和Password。

   註：請勿使用單個群集節點IP。

2. 通過輸入頻率和時間來指明CX雲代理在相連裝置上執行網路掃描和更新資訊的頻率，從而安排資產收集。

   註：第一次資產收集可能需要75分鐘。

3. 按一下「Connect」。系統將顯示包含Cisco DNA Center IP地址的確認資訊。

已成功連線

4. 按一下「Add Another Cisco DNA Center」、「Done」或「Back to Data Sources」，以導覽回「Data Sources」視窗。

新增其他資產作為資料來源

概觀

遙測收集已擴展至非由Cisco DNA中心管理的裝置，使客戶能夠檢視遙測衍生的見解和分析範圍更廣的裝置，並與之互動。初始設定CX Cloud Agent後，使用者可以選擇配置CX Cloud Agent以連線到CX Cloud監控的基礎設施中的20個其他Cisco DNA中心。使用者還可以將CX雲代理直接連線到其環境中的其他硬體資產，最多可以連線10,000台直連裝置。

使用者可以通過使用種子檔案唯一地識別要合併到CX雲中的裝置，或通過指定IP範圍（CX雲代理應對其進行掃描）來識別要合併到CX雲中的裝置。兩種方法都依賴簡單網路管理協定(SNMP)進行發現(SNMP)，並依賴安全外殼(SSH)進行連線。必須正確配置這些引數，才能成功收集遙測資料。

附註：
可以使用種子檔案或IP範圍。初始設定後無法更改此選擇。

附註：
初始種子檔案可以替換為另一個種子檔案，而初始IP範圍可以編輯為新的IP範圍。

從資料來源連線視窗中選擇其他資產時，將開啟以下視窗：

配置與CX雲的連線

要新增其他資產作為資料來源，請執行以下操作：

- 使用種子檔案模板上載種子檔案
- 提供IP地址範圍

探索通訊協定

基於種子檔案的直接裝置發現和基於IP範圍的發現都依靠SNMP作為發現協定。存在不同版本的SNMP，但CX Cloud Agent支援SNMPV2c和SNMP V3，且可以配置任一版本或同時配置兩個版本。使用者必須提供下面完整詳述的相同資訊才能完成配置並啟用SNMP管理的裝置與SNMP服務管理器之間的連線。

SNMPV2c和SNMPV3在安全性和遠端配置模型方面有所不同。SNMPV3使用支援SHA加密的增強型加密安全系統來驗證消息並確保其隱私。建議在所有的公共網路和面向Internet的網路上使用SNMPv3，以防範安全風險和威脅。在CX雲上，最好配置SNMPv3而不是SNMPv2c，但缺少內建對SNMPv3支援的舊版裝置除外。如果兩個版本的SNMP都是由使用者配置的，預設情況下，CX雲代理將嘗試使用SNMPv3與各個裝置通訊，如果通訊無法成功協商，則恢復為SNMPv2c。

連線通訊協定

作為直接裝置連線設定的一部分，使用者必須指定裝置連線協定的詳細資訊：SSH（或者telnet）。應使用SSHv2，但缺少相應內建支援的單個舊資產除外。請注意，SSHv1協定包含基本漏洞。在依賴SSHv1時，如果沒有額外的安全性，遙測資料和底層資產可能會因這些漏洞而受到損害。Telnet也不安全。通過telnet提交的憑證資訊（使用者名稱和密碼）不會加密，因此很容易受到危害，並且沒有額外的安全性。

使用種子檔案新增裝置

關於種子檔案

種子檔案是逗號分隔值(csv)檔案，其中每一行代表一個系統資料記錄。在種子檔案中，每個種子檔案記錄都對應一個唯一的裝置，CX雲代理應該從該裝置收集遙測。將從要匯入的種子檔案中捕獲每個裝置條目的所有錯誤或資訊消息，作為作業日誌詳細資訊的一部分。種子檔案中的所有裝置都被視為受管裝置，即使裝置在初始配置時無法訪問。如果要上載新的種子檔案來替換以前的種子檔案，則上次上載的日期將顯示在CX雲中。

CX Cloud Agent將嘗試連線到裝置，但可能無法處理每個裝置，以便在無法確定PID或序列號的情況下在「資源」頁中顯示。種子檔案中以分號開頭的任何行都會被忽略。種子檔案中的標題行以分號開頭，可在建立客戶種子檔案時保持原樣（建議選項）或將其刪除。

示例種子檔案（包括列標題）的格式不應以任何方式更改，這一點非常重要。按一下提供的連結以檢視PDF格式的種子檔案。此PDF僅供參考，可用於建立需要以.csv格式儲存的種子檔案。

按一下此連結可檢視可用於建立.csv格式種子檔案的種子檔案。

註：此PDF僅供參考，可用於建立需要以.csv格式儲存的種子檔案。

下表列出了所有必需的種子檔案列以及必須包含在每個列中的資料。

種子檔案列	列標題/識別符號	列的用途
A	IP地址或主機名	提供裝置的有效、唯一的IP地址或主機名。
B	SNMP通訊協定版本	SNMP協定是CX Cloud Agent所必需的，用於客戶網路中的裝置發現。值可以是snmpv2c或snmpv3，但由於安全方面的考慮，建議使用snmpv3。
思	snmpRo：如果col#=3被選為「snmpv2c」，則為必填	如果為特定裝置選擇了SNMPv2的舊變體，則必須指定裝置SNMP集合的snmpRO（只讀）憑據。否則，條目可以為空。
D	snmpv3UserName：如果將col#=3選為「snmpv3」，則為必填	如果選擇了SNMPv3與特定裝置進行通訊，則必須提供相應的登入使用者名稱。
E	snmpv3AuthAlgorithm：值可以是MD5或SHA	SNMPv3協定允許通過MD5或SHA演算法進行身份驗證。如果裝置設定了安全驗證，則必須提供各自的驗證演演算法。注意：MD5被視為不安全的，應在支援它的所有裝置上使用

種子檔案列	列標題/識別符號	列的用途
		SHA。
思	snmpv3AuthPassword ：密碼	如果在裝置上配置了MD5或SHA加密演算法，則需要為裝置訪問提供相關的身份驗證密碼。
G	snmpv3PrivAlgorithm：值可以是DES， 3DES	如果裝置配置了SNMPv3隱私演算法（此演算法用於加密響應），則需要提供相應的演算法。 注意：DES使用的56位金鑰太短，無法提供加密安全性，且支援它的所有裝置都應使用3DES。
H	snmpv3PrivPassword ：密碼	如果在裝置上配置了SNMPv3隱私演算法，則需要為裝置連線提供其各自的隱私密碼。
I	snmpv3EngineId :engineID，表示裝置的唯一ID，如果手動在裝置上配置，請指定引擎ID	SNMPv3 EngineID是表示每個裝置的唯一ID。在收集CX雲代理的SNMP資料集時，將傳送此引擎ID作為參考。如果客戶手動配置EngineID，則需要提供各自的EngineID。
J	cliProtocol：值可以是'telnet'、'sshv1'、'sshv2'。如果為空，則預設設定為「sshv2」	CLI用於直接與裝置互動。CX雲代理將此協定用於特定裝置的CLI收集。此CLI收集資料用於CX雲中的資產和其他見解報告。建議使用SSHv2；如果沒有其他網路安全措施，SSHv1和Telnet協定本身無法提供足夠的傳輸安全性。
K	cliPort:CLI協定埠號	如果選擇任何CLI協定，則需要提供其各自的埠號。例如，22表示SSH，23表示telnet。
L	cliUser:CLI使用者名稱(可以提供CLI使用者名稱/密碼或同時提供BOTH，但兩列（col#=12和col#=13）不能為空。)	需要提供裝置的相應CLI使用者名稱。CX雲代理在CLI收集期間連線到裝置時使用該功能。

種子檔案列	列標題/識別符號	列的用途
M	cliPassword :CLI使用者密碼(可以提供CLI使用者名稱/密碼或BOTH，但兩列（col#=12和col#=13）不能為空。)	需要提供裝置各自的CLI密碼。CX雲代理在CLI收集期間連線到裝置時使用該功能。
否	cliEnableUser	如果在裝置上配置了「enable」，則需要提供裝置的enableUsername值。
O	cliEnablePassword	如果在裝置上配置了「enable」，則需要提供裝置的enablePassword值。
P	未來支援（無需輸入）	保留供將來使用
Q	未來支援（無需輸入）	保留供將來使用
R	未來支援（無需輸入）	保留供將來使用
S	未來支援（無需輸入）	保留供將來使用

裝置的遙測處理限制

以下是處理裝置的遙測資料時的限制：

- 某些裝置可能在收集摘要中顯示為可訪問，但在CX雲資產頁中不可見。裝置檢測限制會阻止處理此類裝置遙測。
- 對於不屬於園區成功跟蹤範圍的裝置，CX雲資產頁中的遙測屬性可能不準確或丟失。
- 如果種子檔案或IP範圍集合中的裝置也是Cisco DNA Center清單的一部分，則對於Cisco DNA Center條目，僅報告一次該裝置。不會收集或處理種子檔案/IP範圍條目，以避免重複。

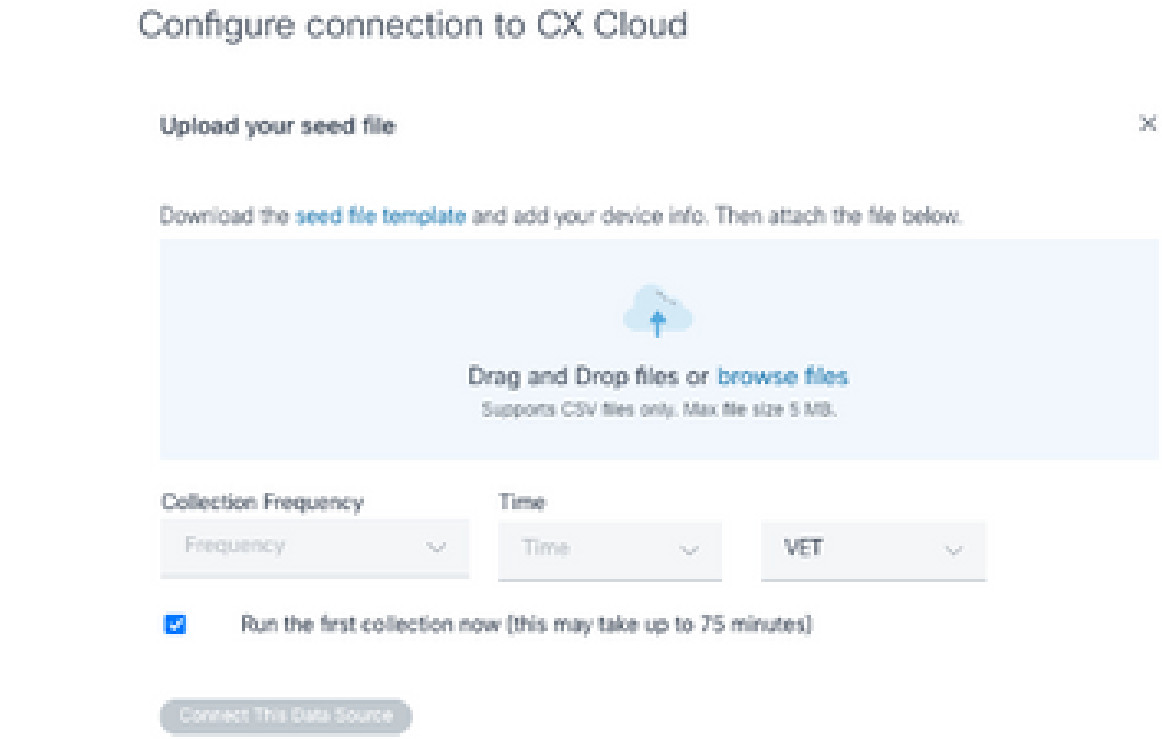
使用新的種子檔案新增裝置

使用新的種子檔案新增裝置：

1. 使用本文檔中的嵌入式連結(請參閱關於種子檔案)或通過配置到CX雲的連線視窗中的連結下載種子檔案模板(PDF)。

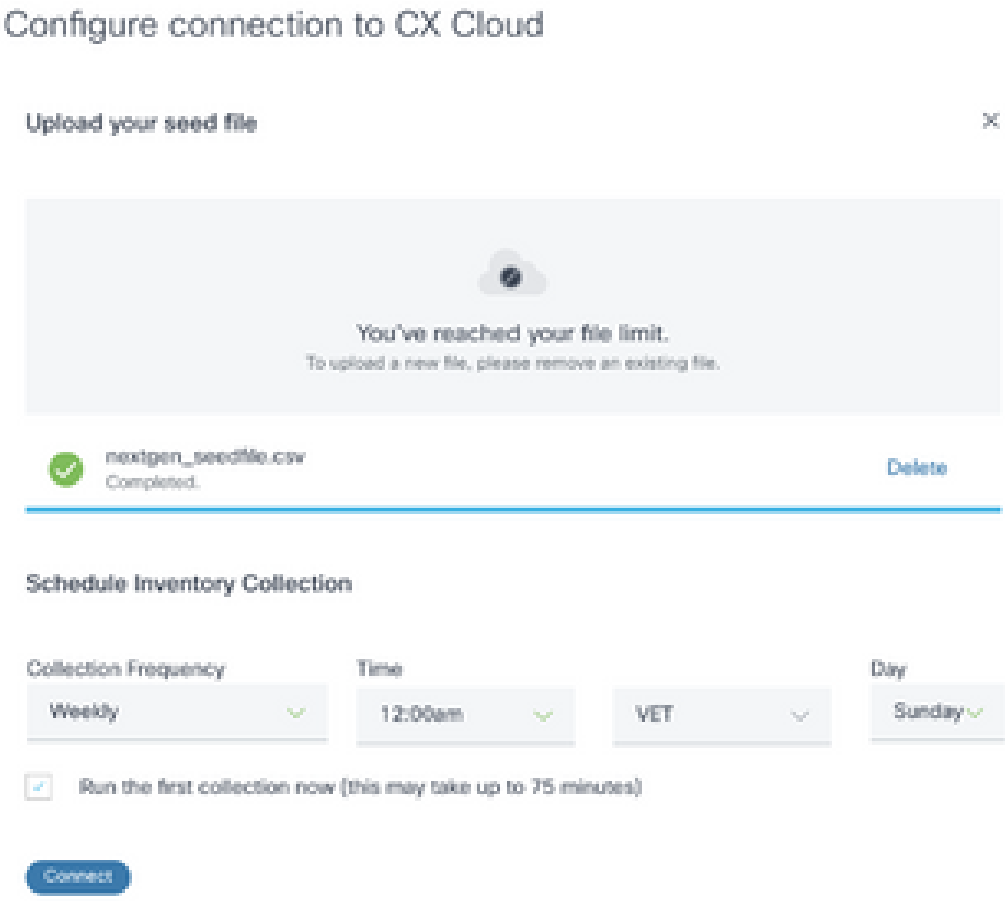
> 注意：下載初始種子檔案後，Configure Connection to CX Cloud視窗中的連結將不再可

用。



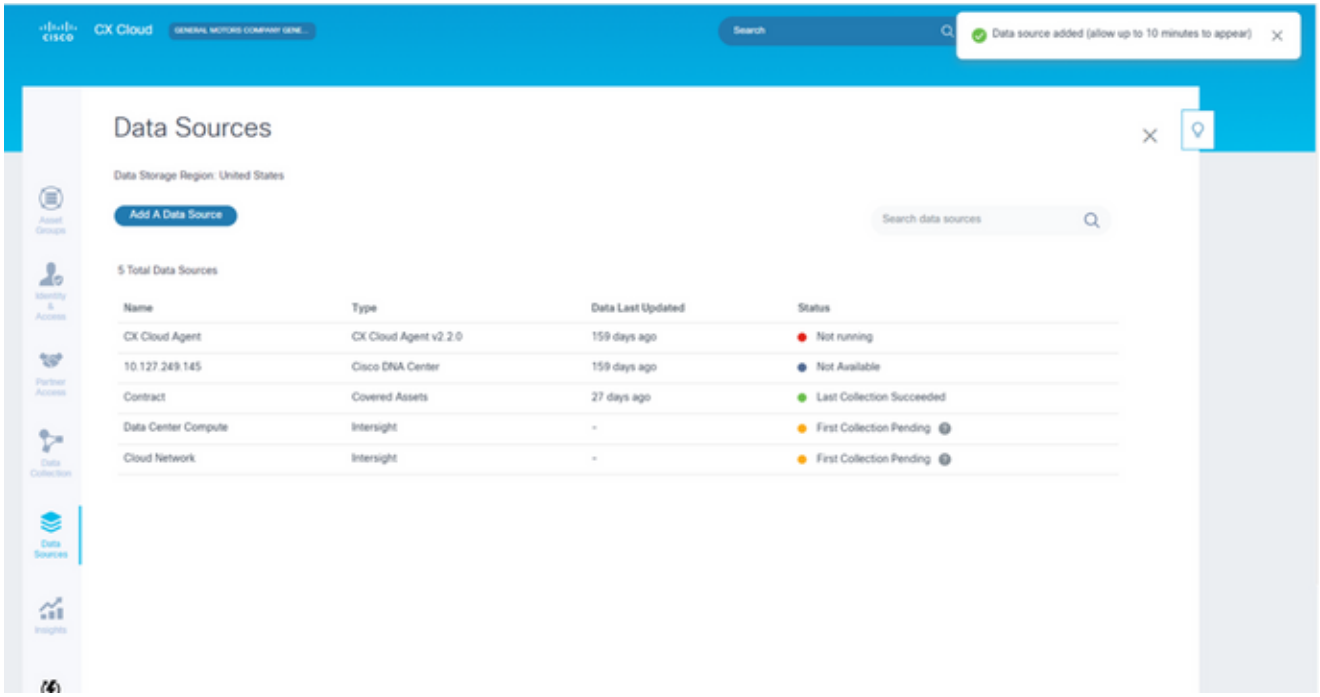
配置連線到CX雲視窗

2. 開啟Excel電子表格（或任何首選電子表格）並輸入標題，如模板所示。
3. 手動輸入資料或將資料匯入到檔案中。
4. 完成後，將模板另存為.csv檔案，以將該檔案匯入CX雲代理。



上載種子檔案視窗

5. 在「Upload your seed file」視窗中，拖放新建立的.csv檔案，或按一下「browse」檔案並導航至.csv檔案。
6. 完成Schedule Inventory Collection部分，然後按一下Connect。將開啟「資料來源」視窗，顯示一條確認消息。
7. 在完成CX雲的初始配置之前，CX雲代理必須通過處理種子檔案並與所有已識別裝置建立連線來執行第一次遙測收集。收集可以按需啟動，也可以根據此處定義的計畫運行。使用者可以通過選中Run the first collection now覈取方塊來執行第一個遙測連線。根據種子檔案中指定的條目數量和其他因素，此過程可能需要相當長的時間。



確認消息

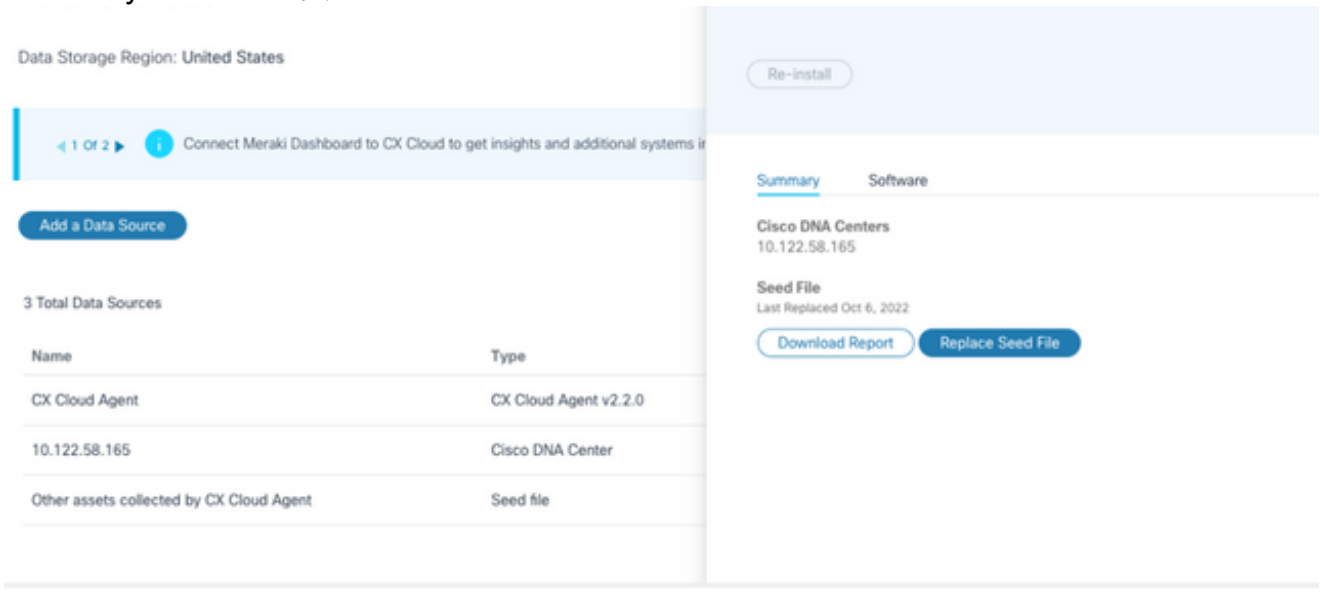
使用已修改的種子檔案新增裝置

要使用當前種子檔案新增、修改或刪除裝置，請執行以下操作：

1. 開啟先前建立的種子檔案，進行所需的更改，然後儲存檔案。

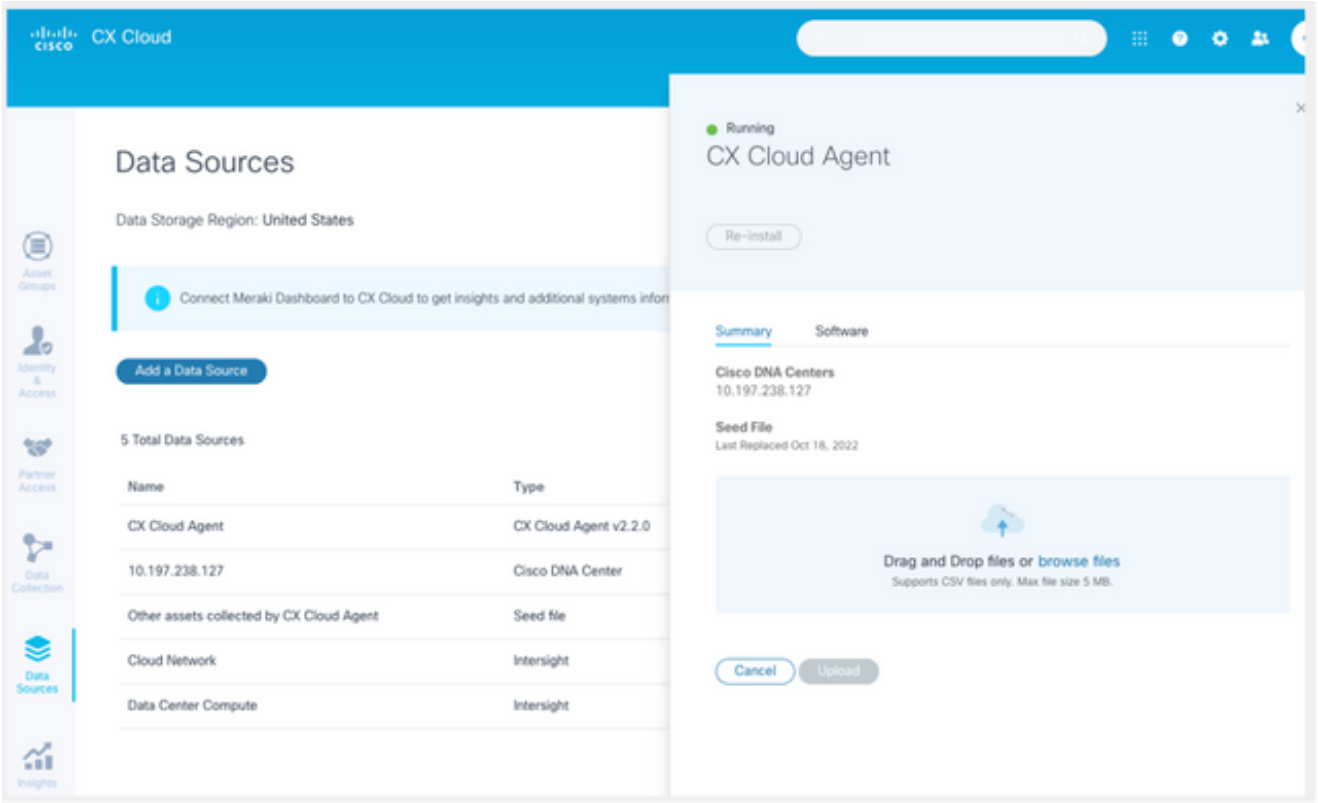
> 注意：要將資源新增到種子檔案，請將這些資源追加到以前建立的種子檔案，然後重新載入該檔案。這是必要的，因為上傳新的種子檔案將替換當前的種子檔案。僅最新上傳的種子檔案用於發現和收集。

2. 從資料來源頁中，選擇具有CX雲代理型別的資料來源。將開啟一個詳細資訊視窗，其中包含Summary和Software頁籤。



詳細資訊視窗

3. 按一下Download Report，為所選資料來源生成所有資產的報告。報告提供有關裝置IP地址、序列號、可達性、命令型別、命令狀態和命令錯誤的資訊（如果適用）。
4. 按一下替換種子檔案。CX Cloud Agent視窗將開啟。



CX雲代理視窗

5. 將已修改的種子檔案拖放到視窗中，或瀏覽到該檔案並將其新增到視窗中。
6. 按一下「Upload」。

使用IP範圍新增裝置

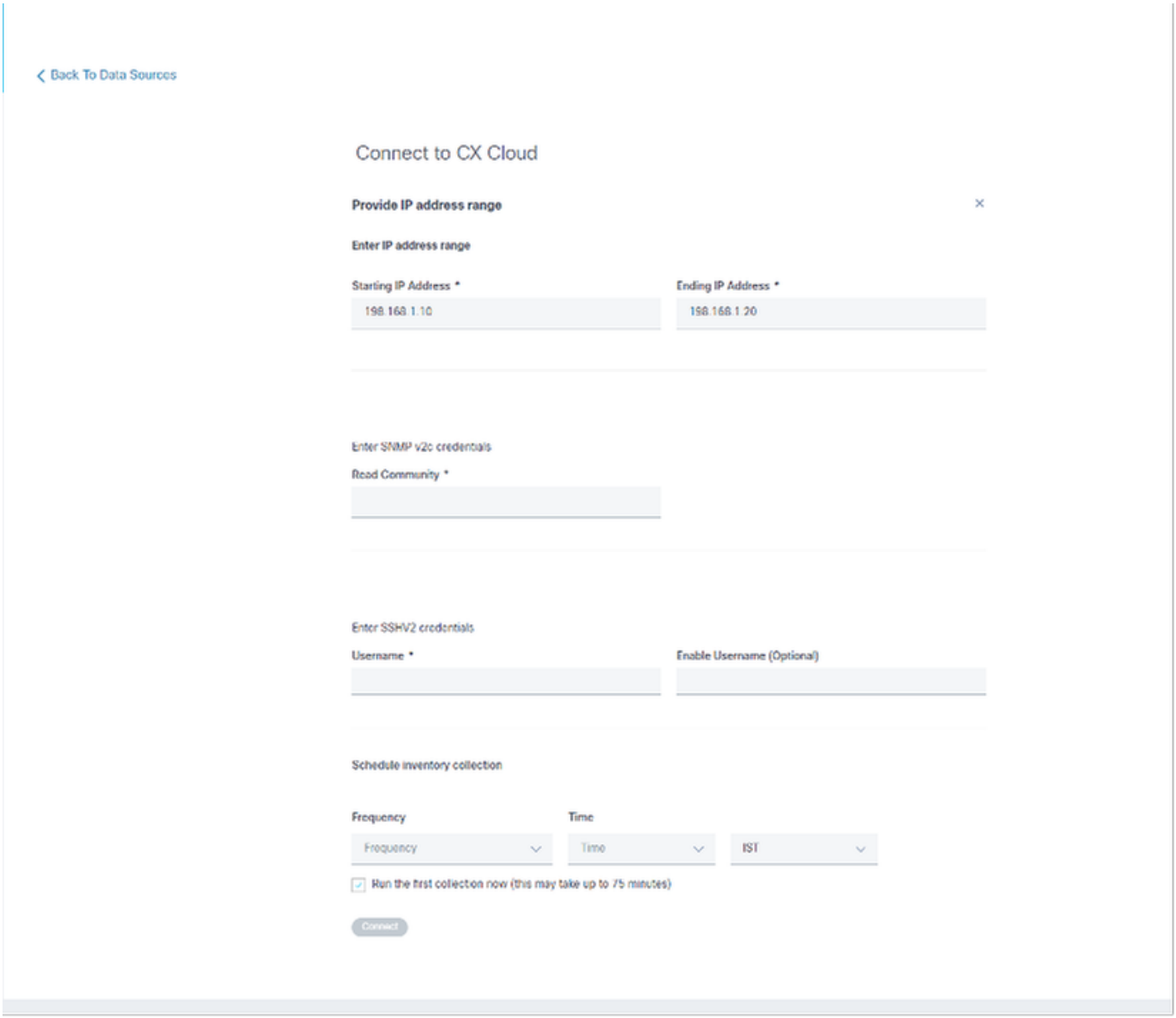
IP範圍允許使用者識別硬體資產，然後根據IP地址從這些裝置收集遙測資料。通過指定單個網路級別IP範圍，可以唯一標識用於遙測收集的裝置，CX雲代理應使用SNMP協定對其進行掃描。如果選擇IP範圍來標識直連裝置，則所引用的IP地址應儘可能限制性，同時允許覆蓋所有必需的資產。

- 可以提供特定IP，也可以使用萬用字元替換IP的八位組以建立範圍
- 如果在設定期間識別的IP範圍中未包括特定IP地址，則CX雲代理不會嘗試與具有此類IP地址的裝置通訊，也不會從此類裝置收集遙測資料
- 輸入*.*.*.*可讓CX雲代理將使用者提供的憑據用於任何IP。例如：172.16.*.*允許將憑證用於172.16.0.0/16子網中的所有裝置
- 如果網路或客戶群(IB)有任何變更，則可以修改IP範圍。請參閱編輯IP範圍部分

CX Cloud Agent將嘗試連線到設備，但在無法確定PID或序列號的情況下，可能無法處理每個裝置以在Assets(資產)檢視中顯示。

附註：

按一下Edit IP Address Range啟動按需裝置發現。向指定的IP範圍新增或刪除任何新裝置（內部或外部）時，客戶必須始終按一下編輯IP地址範圍(請參閱編輯IP範圍部分)並完成啟動按需裝置發現所需的步驟，以將任何新新增的裝置包含到CX Cloud Agent收集清單中。



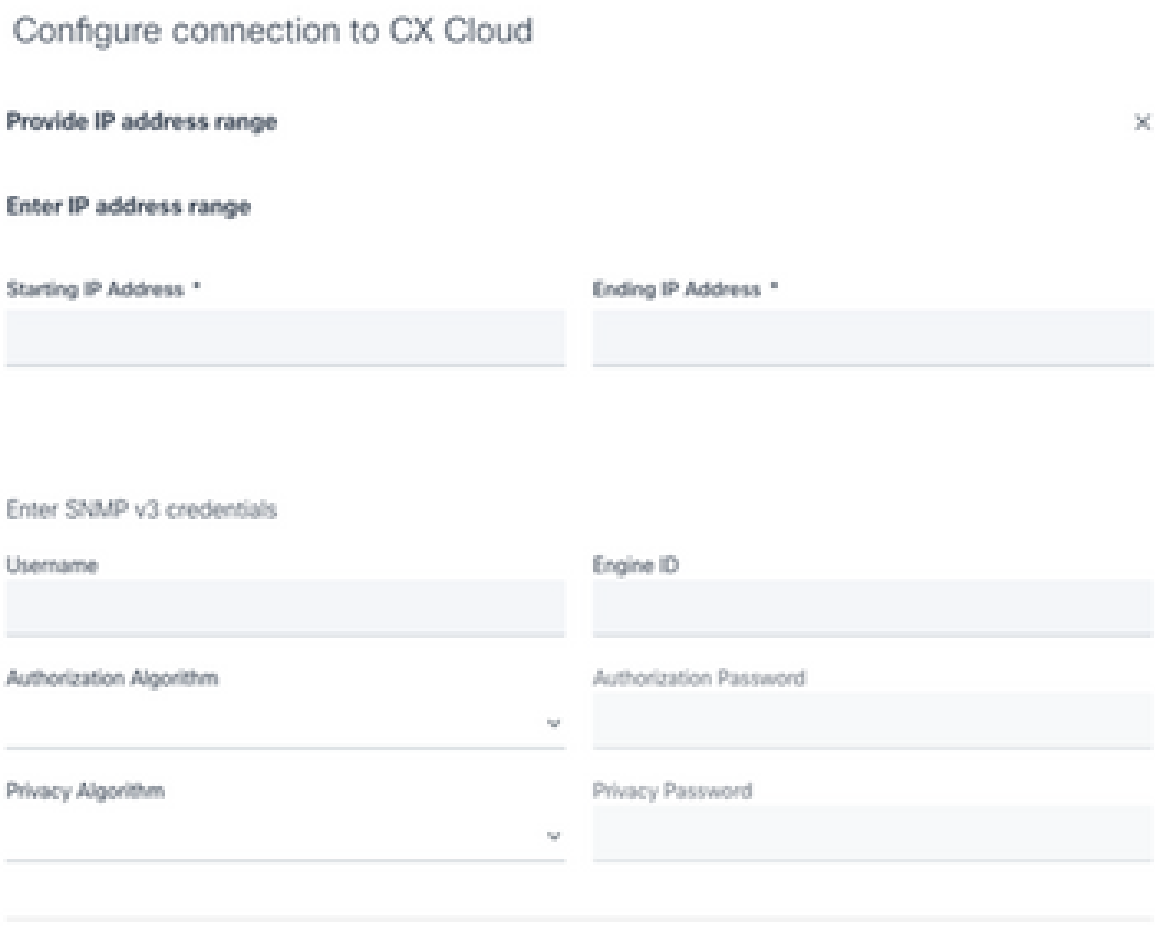
初始IP地址範圍視窗

使用IP範圍新增裝置需要使用者通過配置UI指定所有適用的憑據。顯示的欄位因在前幾個視窗中選擇的協定而異。如果對同一協定進行了多項選擇（例如，同時選擇SNMPv2c和SNMPv3或同時選擇SSHv2和SSHv1），則CX雲代理將根據各個裝置功能自動協商協定選擇。

當使用IP地址連線裝置時，客戶應確保IP範圍內所有相關協定以及SSH版本和Telnet憑證有效，否則連線將失敗。

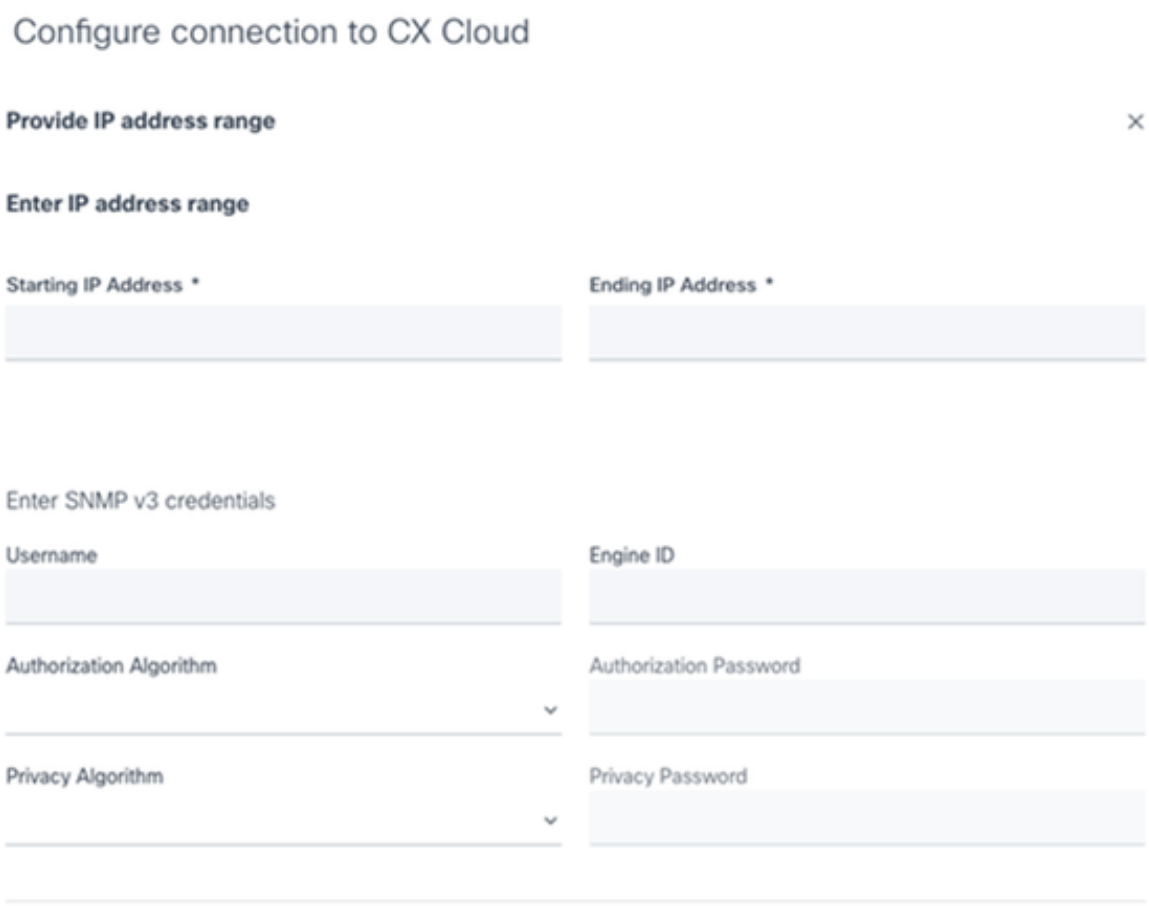
使用IP範圍新增裝置：

1. 在Configure connection to CX Cloud視窗中，選擇Provide an IP Address range選項。

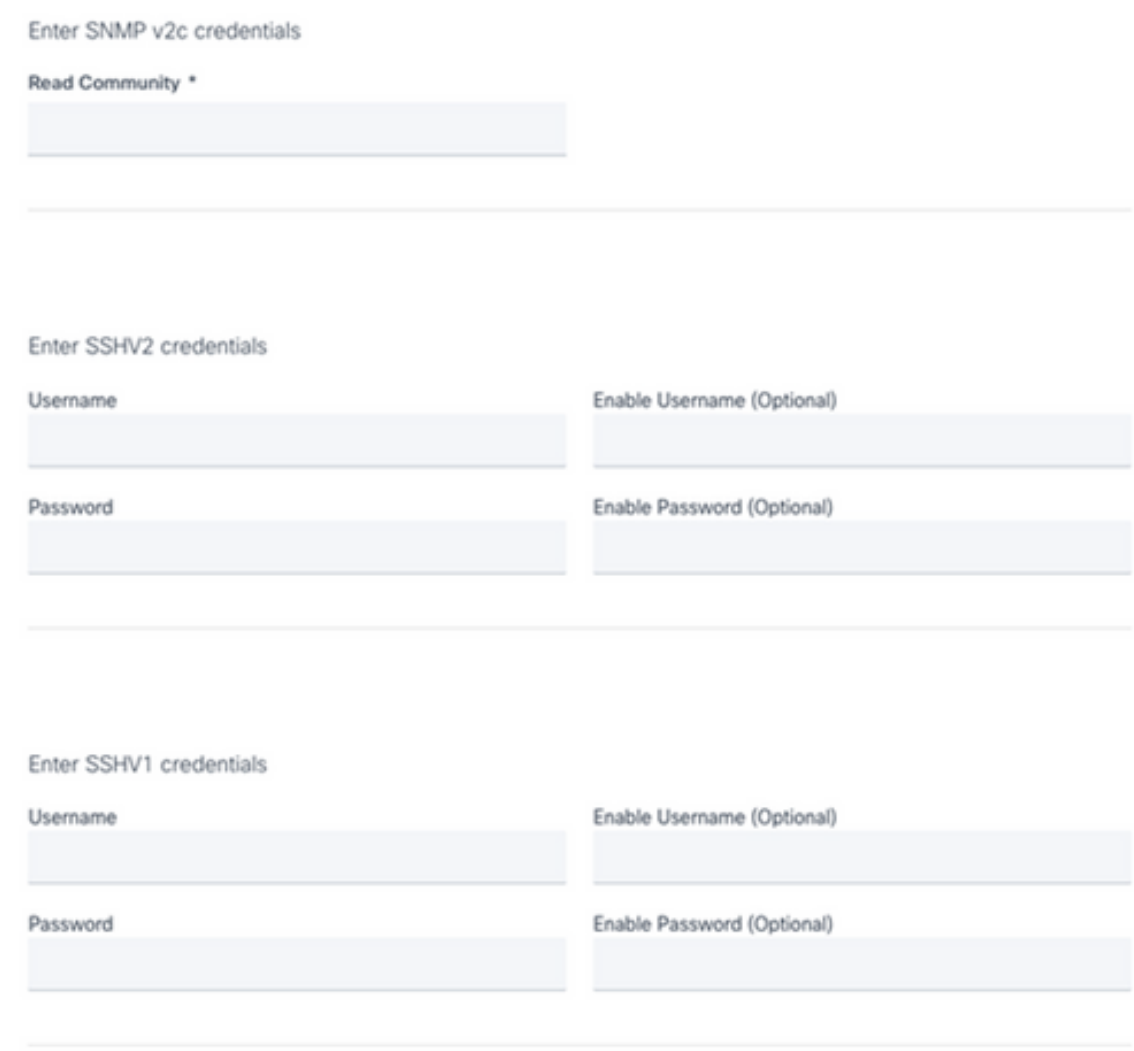


使用IP地址表單新增裝置

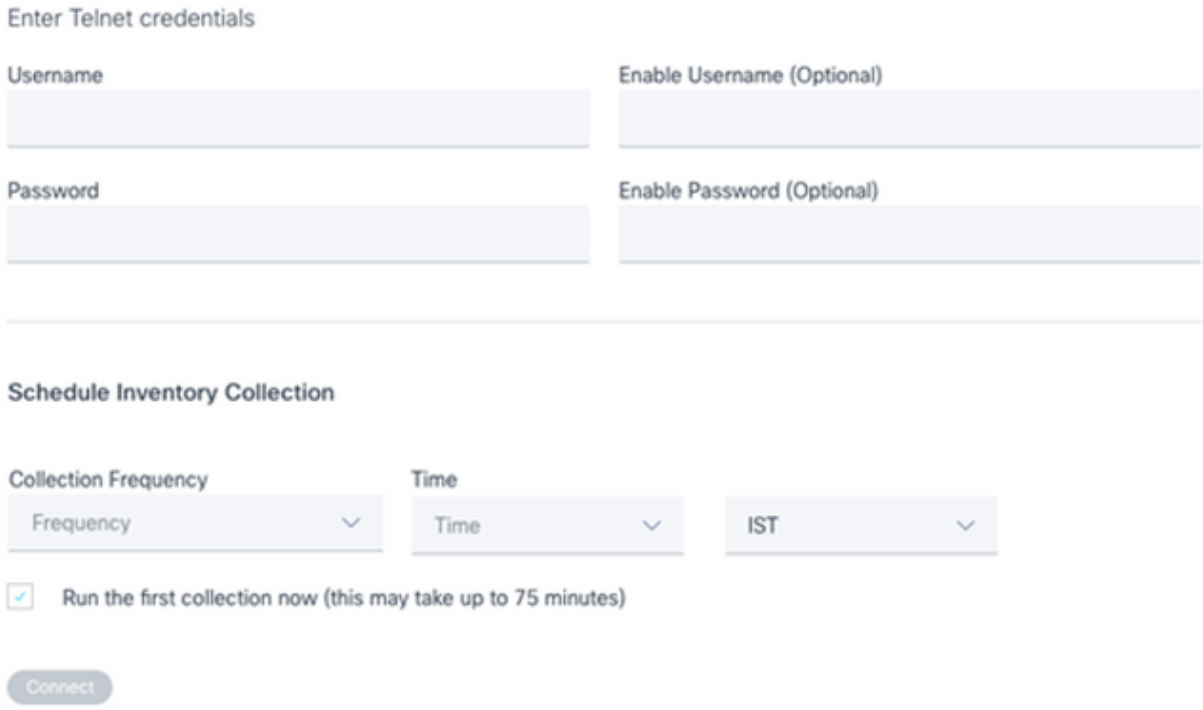
2. 填寫表格並提供相關資訊。
3. 可以選擇多個連線選項。以下螢幕顯示選項的配置憑據。有關每個連線選項的憑據欄位的說明，請參閱關於種子檔案。


Configure connection to CX Cloud
Provide IP address range
Enter IP address range
Starting IP Address *
Ending IP Address *
Enter SNMP v3 credentials
Username
Engine ID
Authorization Algorithm
Authorization Password
Privacy Algorithm
Privacy Password

SNMP v3憑證

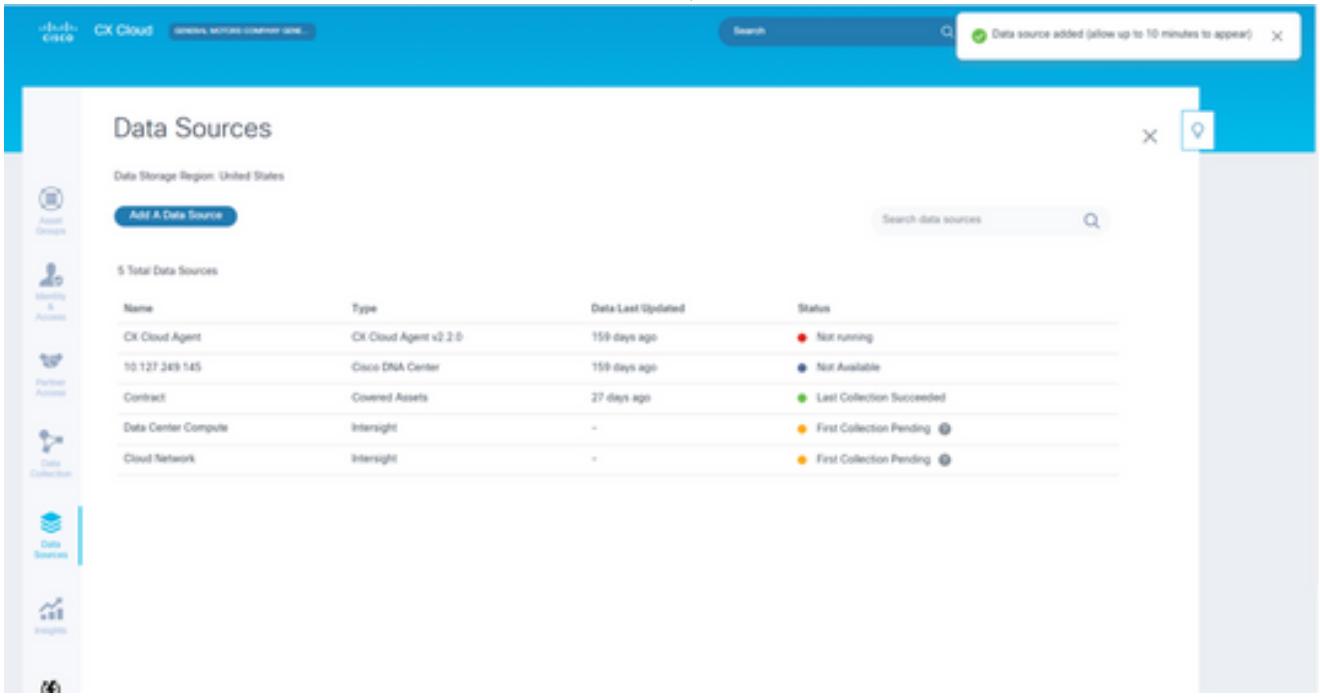


SNMP v2、SSHV2和SSHV1憑證



Telnet憑證和網路掃描計畫

4. 按一下「Connect」。 將開啟「資料來源」視窗，顯示一條確認消息。

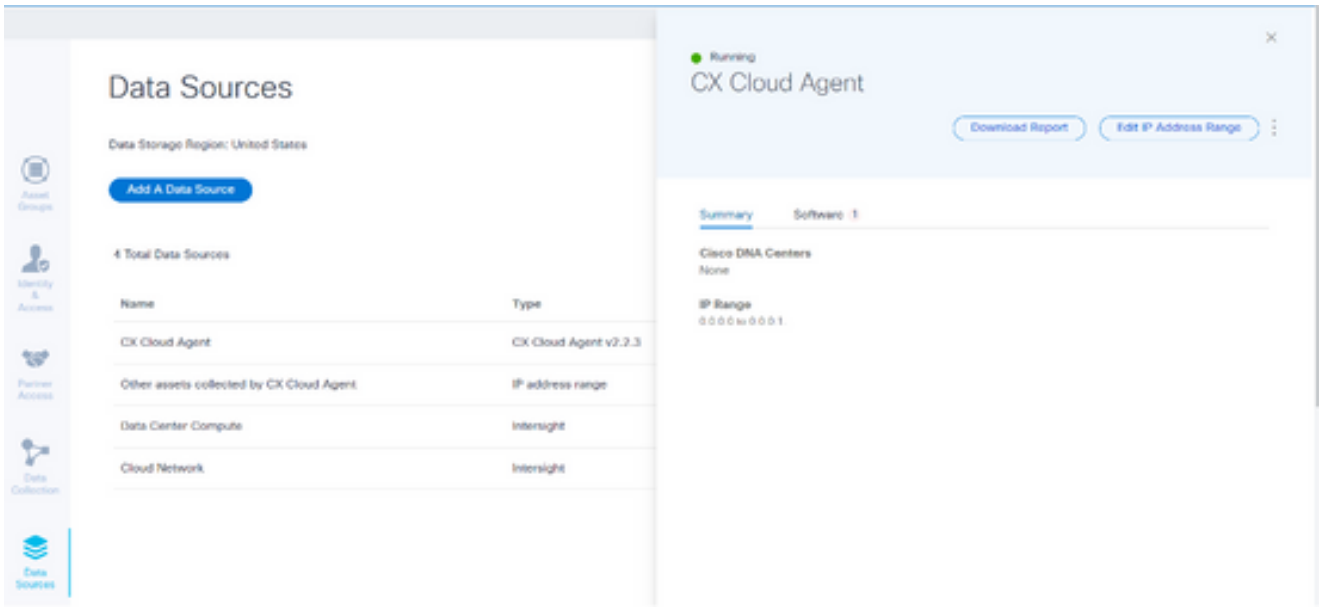


確認

編輯IP範圍

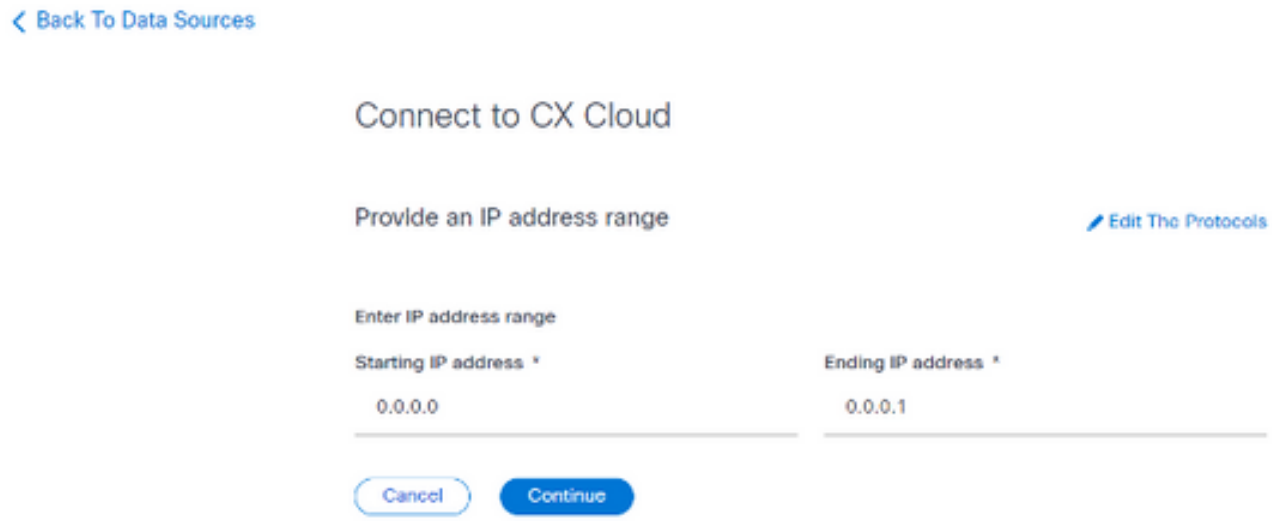
編輯IP範圍；

1. 定位至「數據源」視窗。



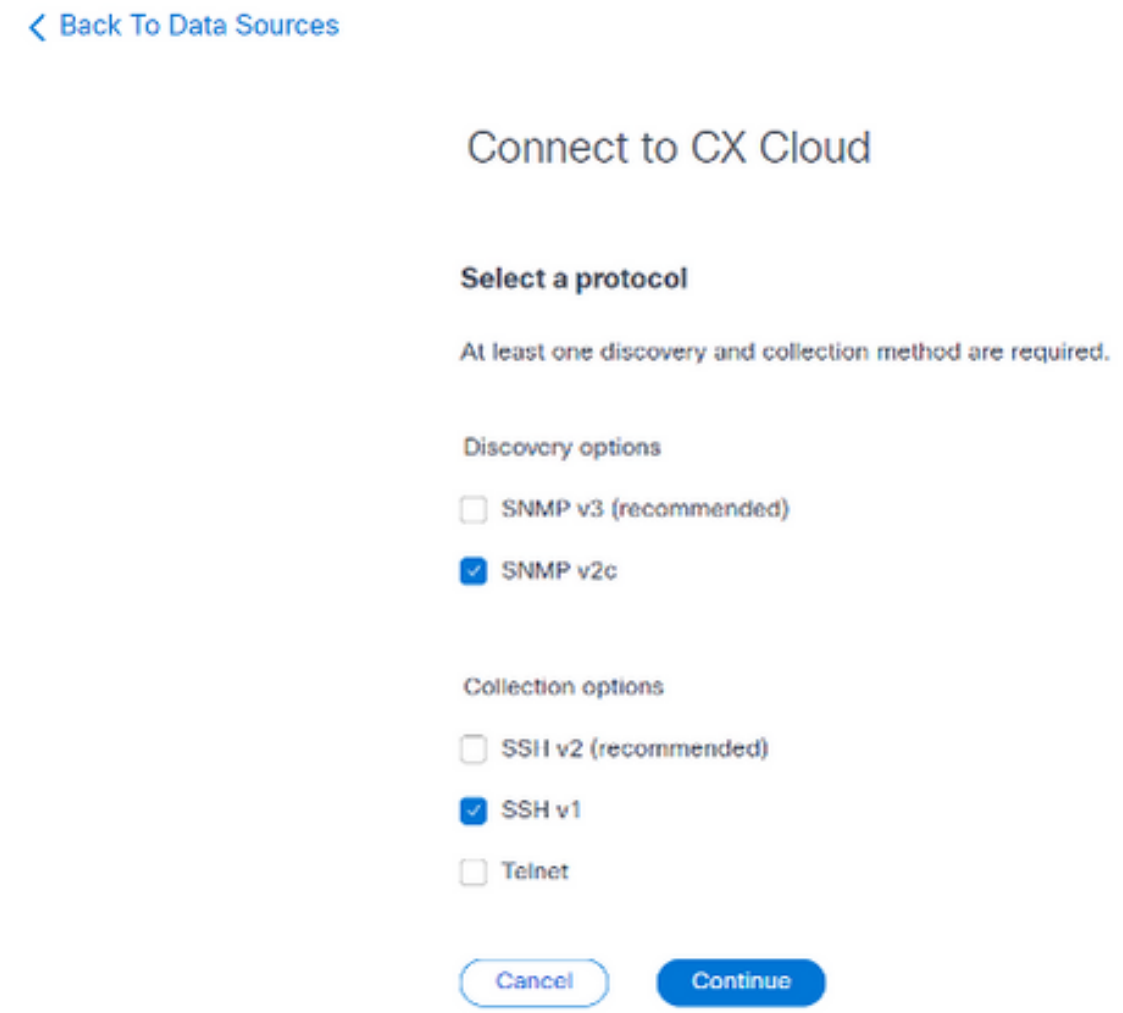
資料來源

2. 按一下需要在「資料來源」中編輯IP範圍的CX Cloud Agent。將開啟詳細資訊視窗。
3. 按一下Edit IP Address Range。Connect to CX Cloud視窗開啟。



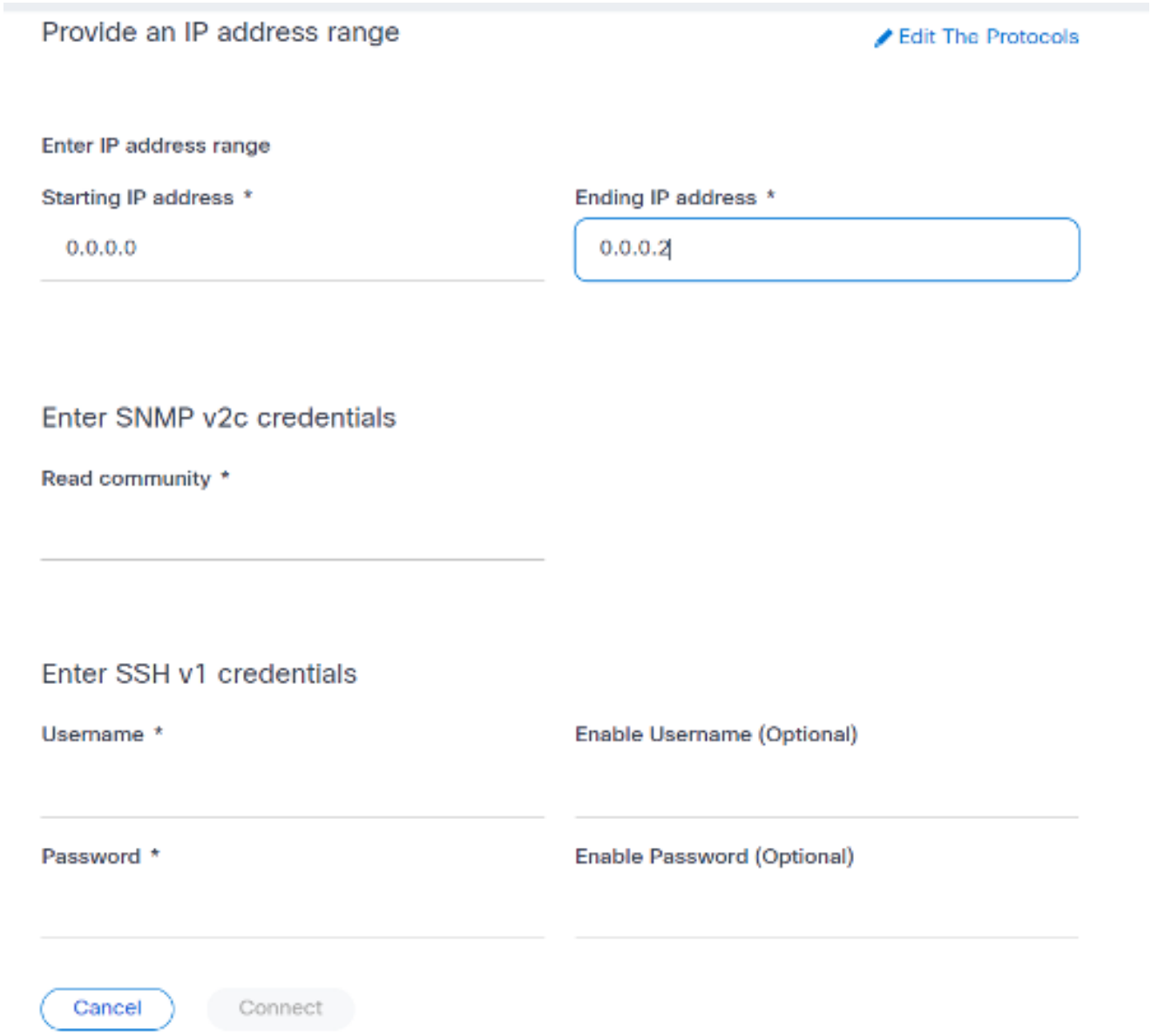
提供IP範圍

4. 在起始IP地址和結束IP地址欄位中更新新的IP。
5. 按一下Edit the Protocols連結。Connect to CX Cloud - Select a protocol視窗開啟。



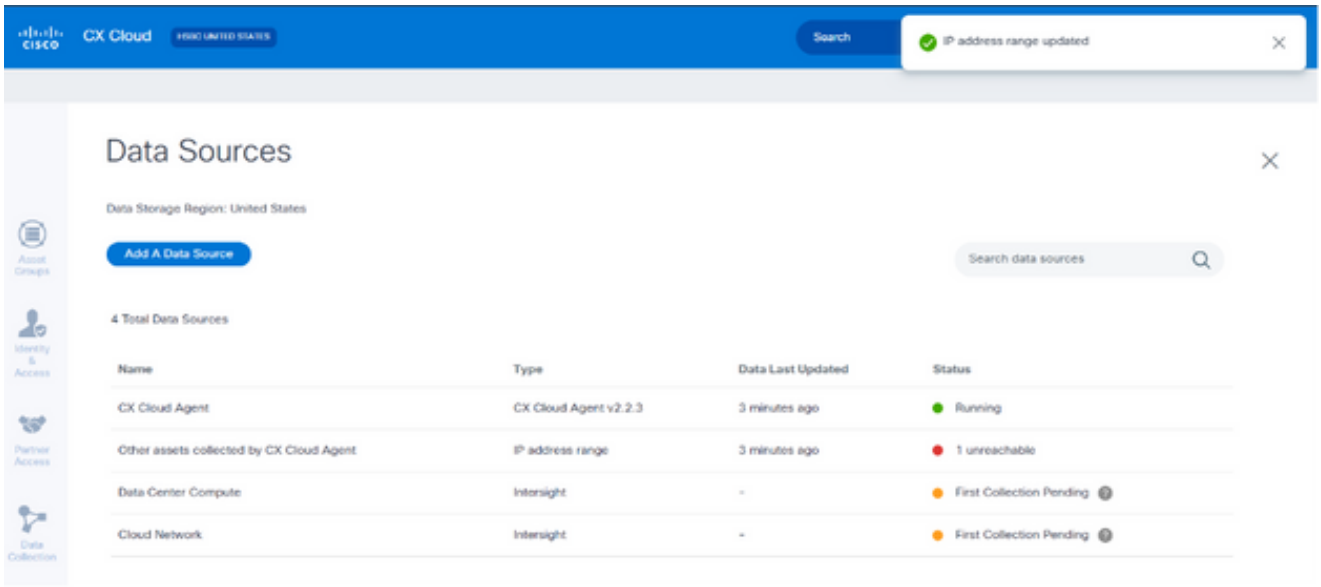
選擇協定

6. 通過按一下相應的覈取方塊選擇適用的協定。
7. 按一下「Continue」（繼續）。Provide an IP address range視窗開啟。



輸入憑據

8. 輸入配置憑據。
9. 按一下「Connect」。將開啟「資料來源」視窗，顯示一條確認消息。



確認

註：確認消息不能確保可訪問已編輯範圍內的裝置，並且已接受憑證。

關於從多個控制器中發現的裝置

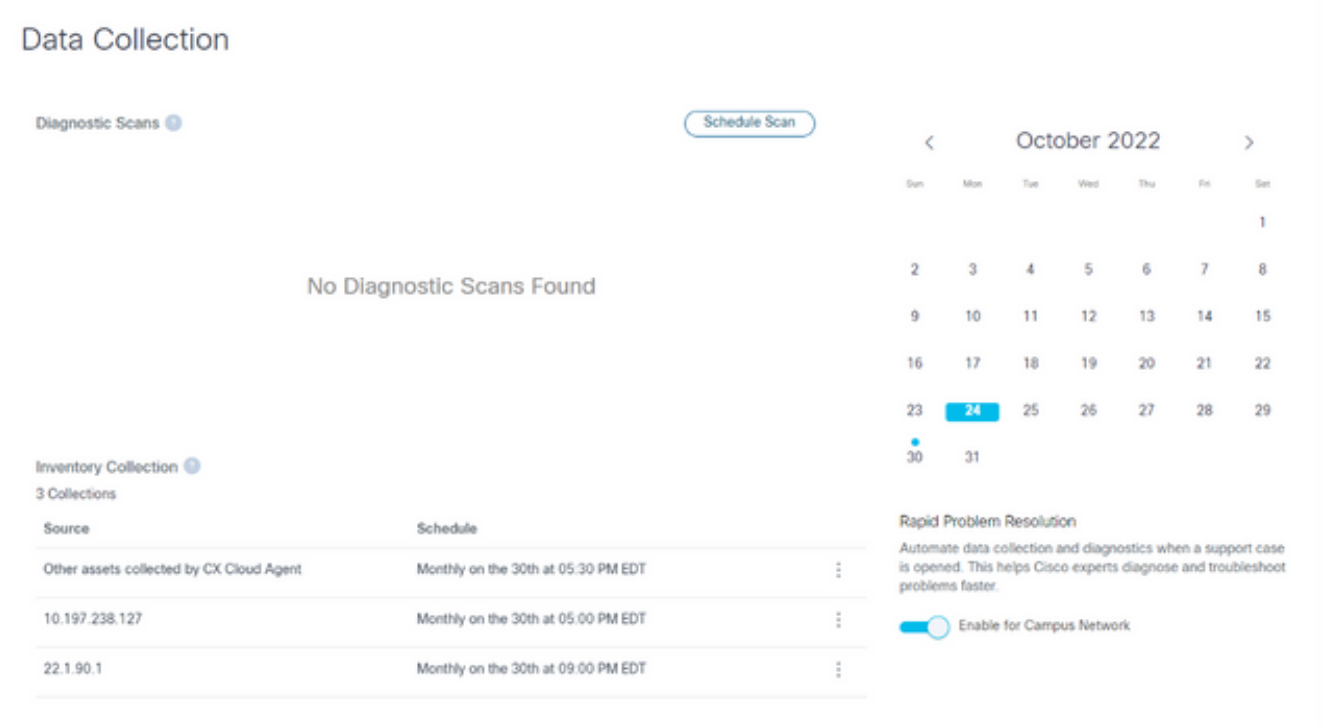
Cisco DNA Center和直接裝置連線至CX雲代理可能會發現某些裝置，從而導致從這些裝置收集重複資料。為避免收集重複資料，且只有一個控制器來管理裝置，需要確定CX雲代理管理裝置的優先順序。

- 如果裝置首先由Cisco DNA Center發現，然後通過直接裝置連線（使用種子檔案或IP範圍）重新發現，則Cisco DNA Center優先控制裝置。
- 如果裝置首先通過直接裝置連線到CX雲代理被發現，然後由Cisco DNA Center重新發現，則Cisco DNA Center將優先控制裝置。

安排診斷掃描

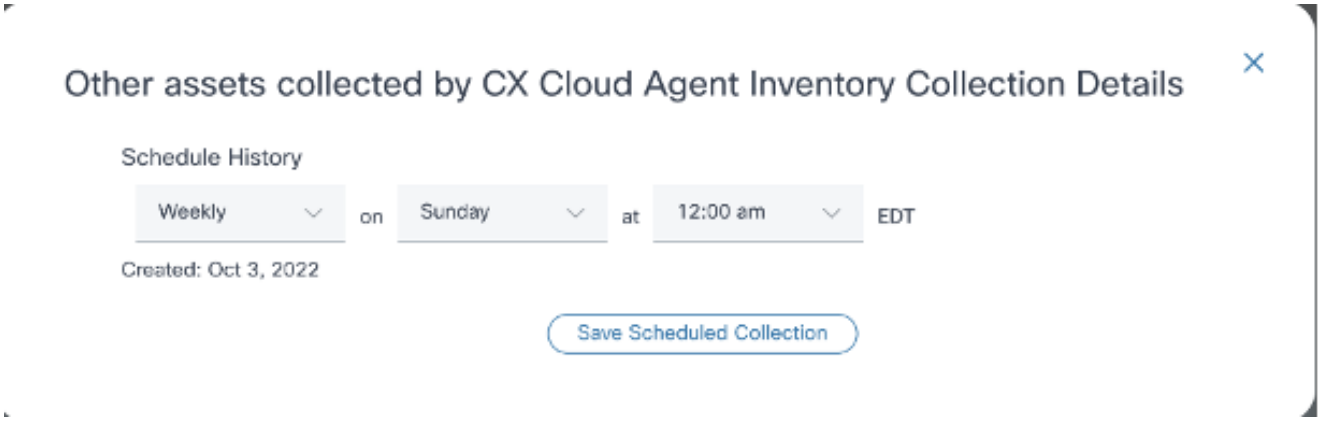
計畫診斷掃描：

1. 在Home頁面上，按一下Settings（齒輪）圖示。
2. 在「數據源」頁上，在左窗格中選擇Data Collection。
3. 按一下Schedule Scan。



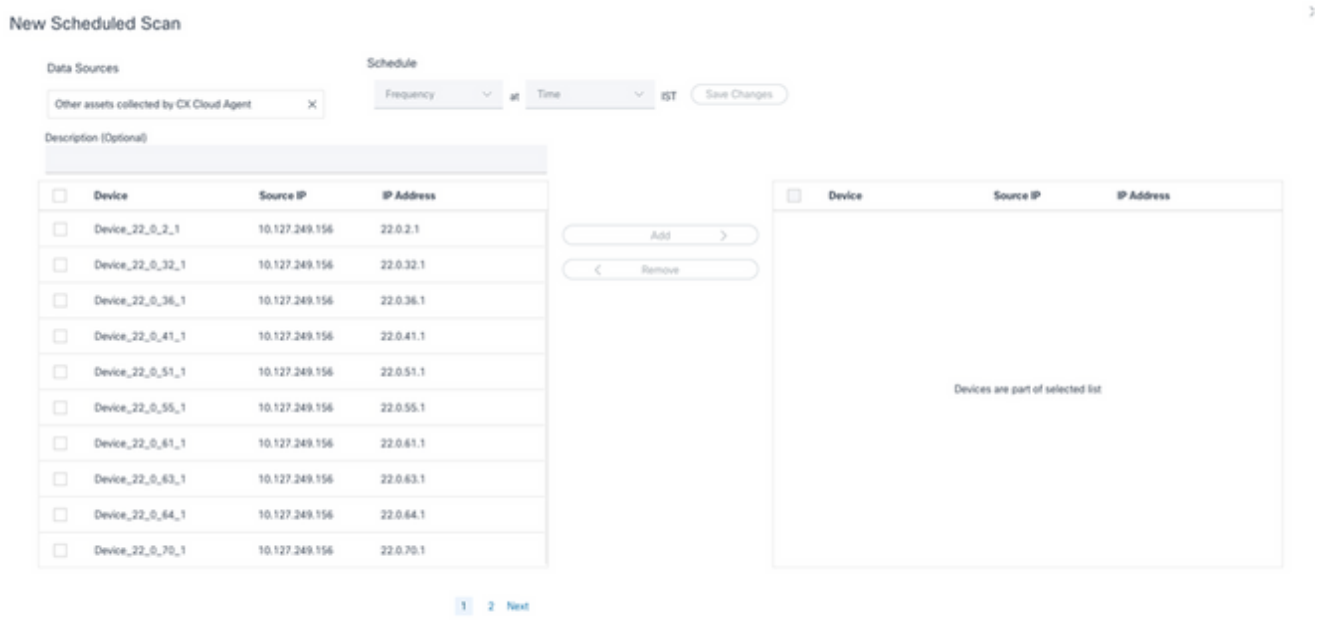
資料收集

4. 為此掃描配置計畫。



配置掃描計畫

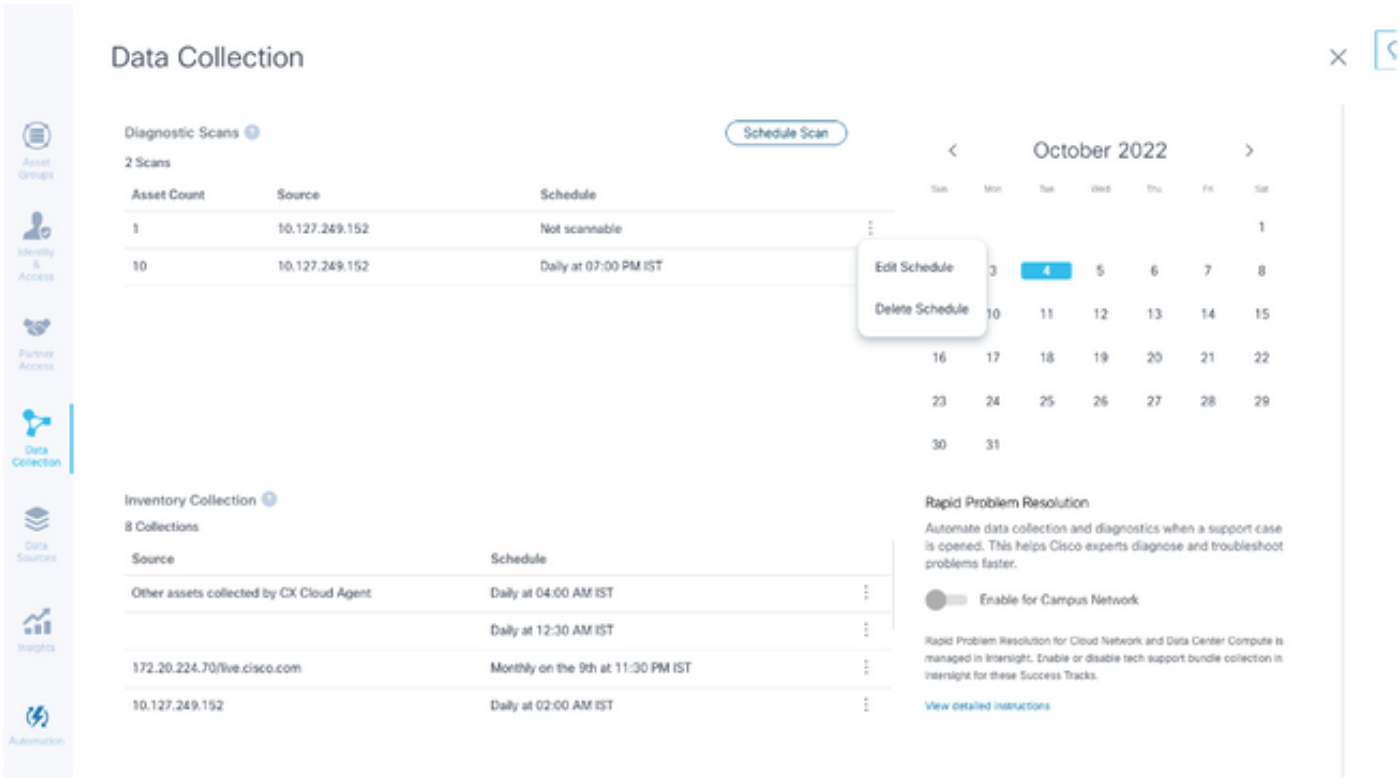
5. 在裝置清單中，選擇要掃描的所有裝置，然後按一下Add。



安排掃描

6. 計畫完成後，按一下Save Changes。

可以從Data Collection頁面編輯和刪除診斷掃描和資產收集計畫。



具有編輯和刪除計畫選項的資料收集

部署和網路組態

選擇以下任一選項以部署CX雲代理：

- 要選擇VMware vSphere/vCenter Thick Client ESXi 5.5/6.0，請轉至Thick Client
- 要選擇VMware vSphere/vCenter Web客戶端ESXi 6.0，請轉到Web客戶端或vSphere Center
- 要選擇Oracle Virtual Box 5.2.30，請轉至Oracle VM
- 若要選擇Microsoft Hyper-V，請轉到Hyper-V

OVA 部署

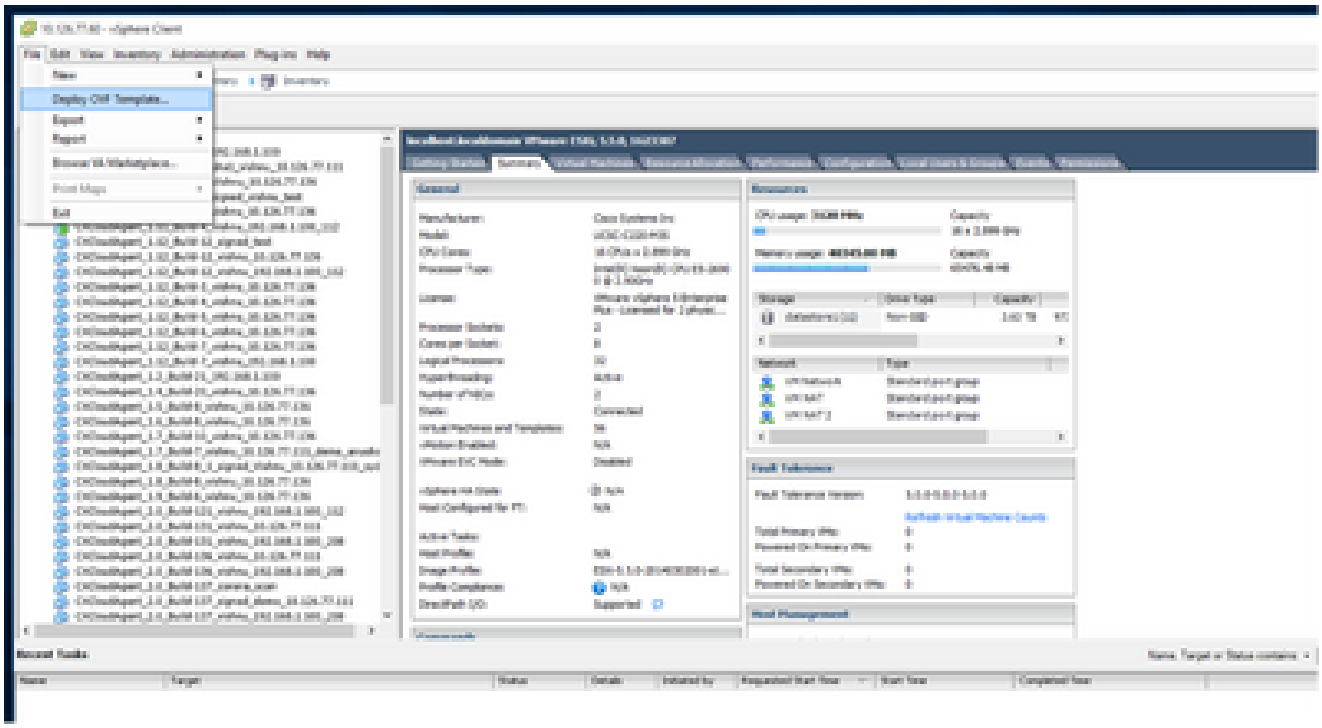
複雜型用戶端 ESXi 5.5/6.0 安裝

此客戶端允許使用vSphere胖客戶端部署CX雲代理OVA。

1. 下載映像後，啟動VMware vSphere客戶端並登入。

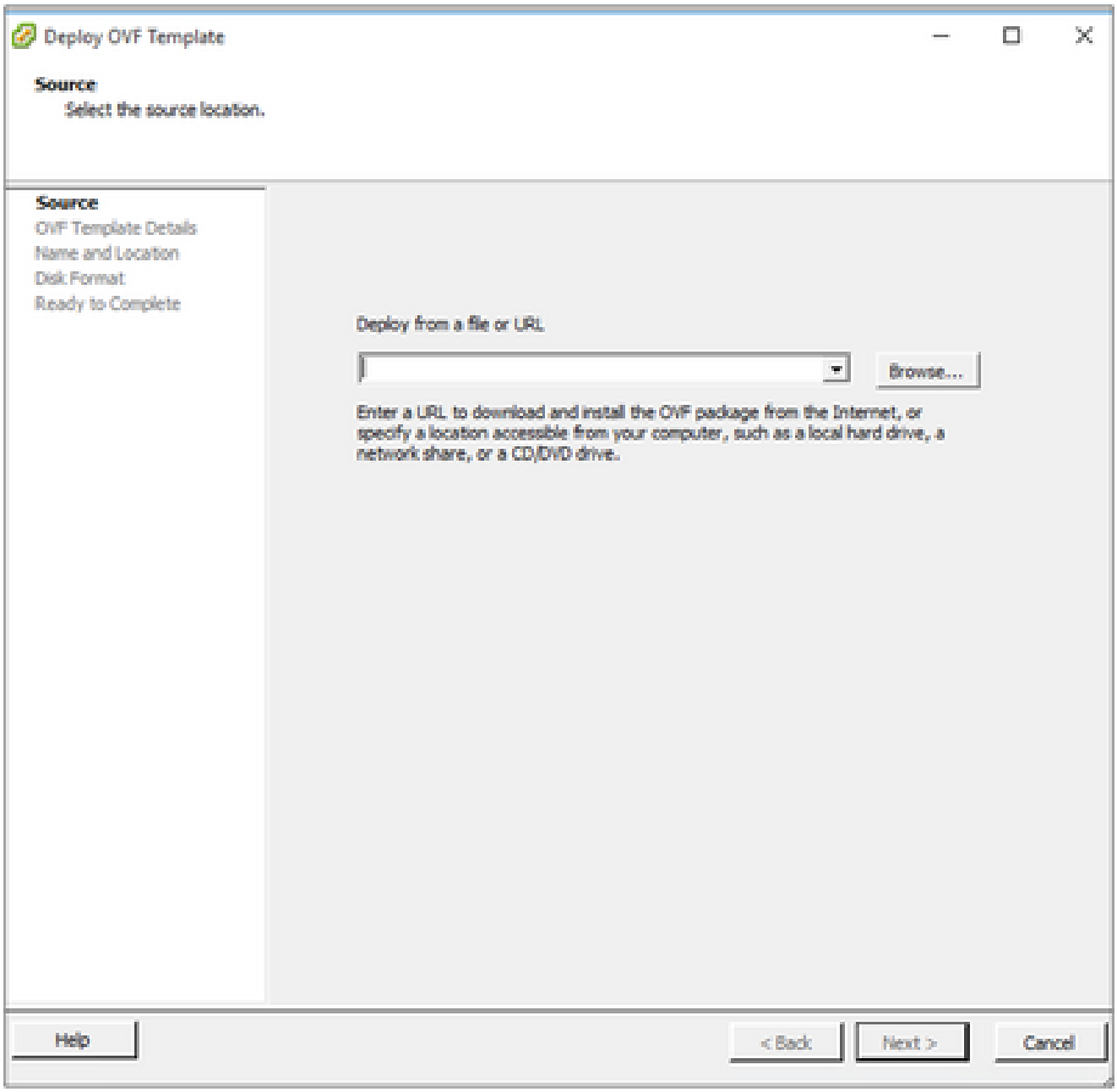
登入

2. 從選單中選擇檔案>部署OVF模板。



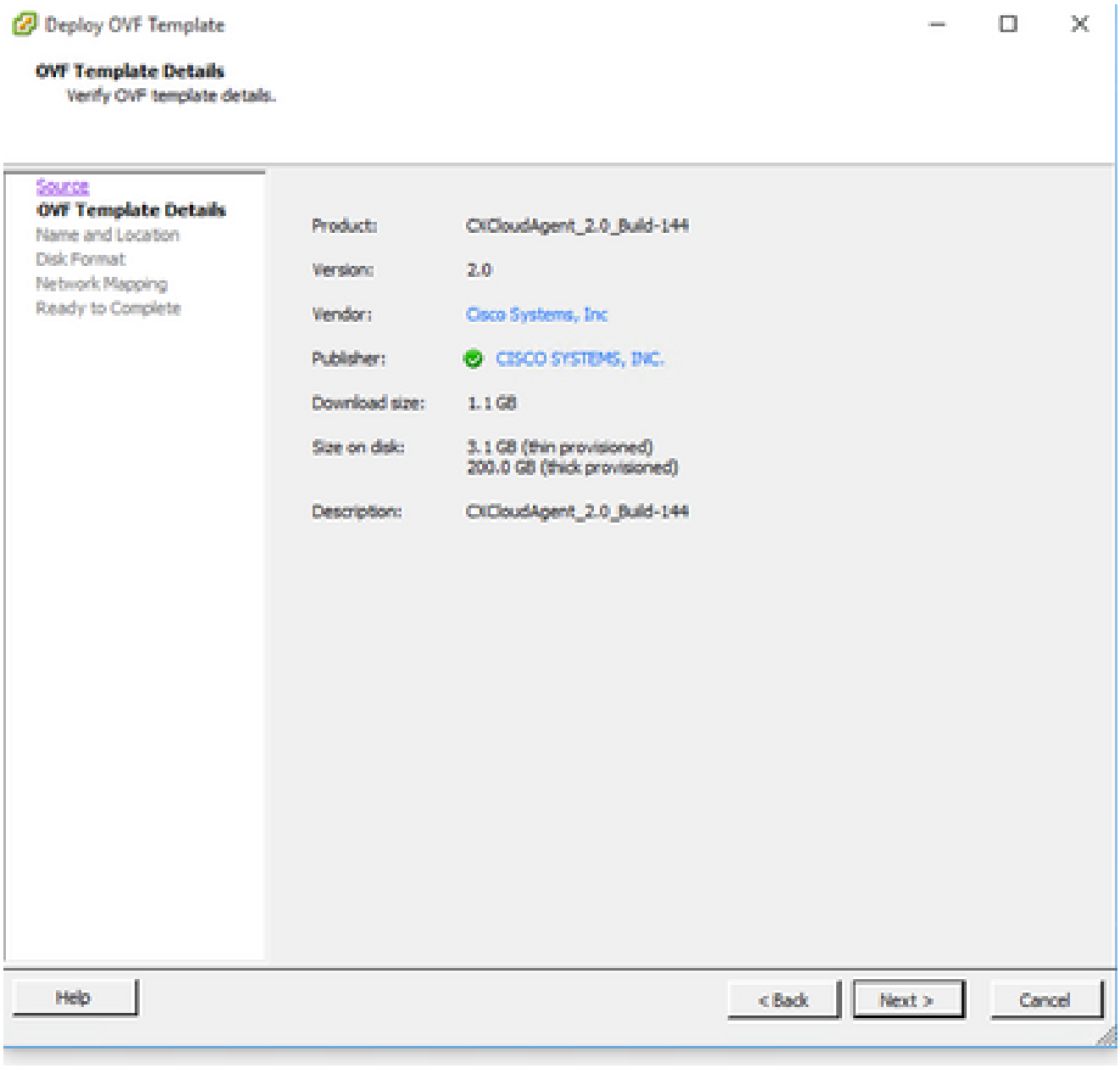
vSphere 用戶端

3. 瀏覽以選擇OVA檔案，然後按一下Next。



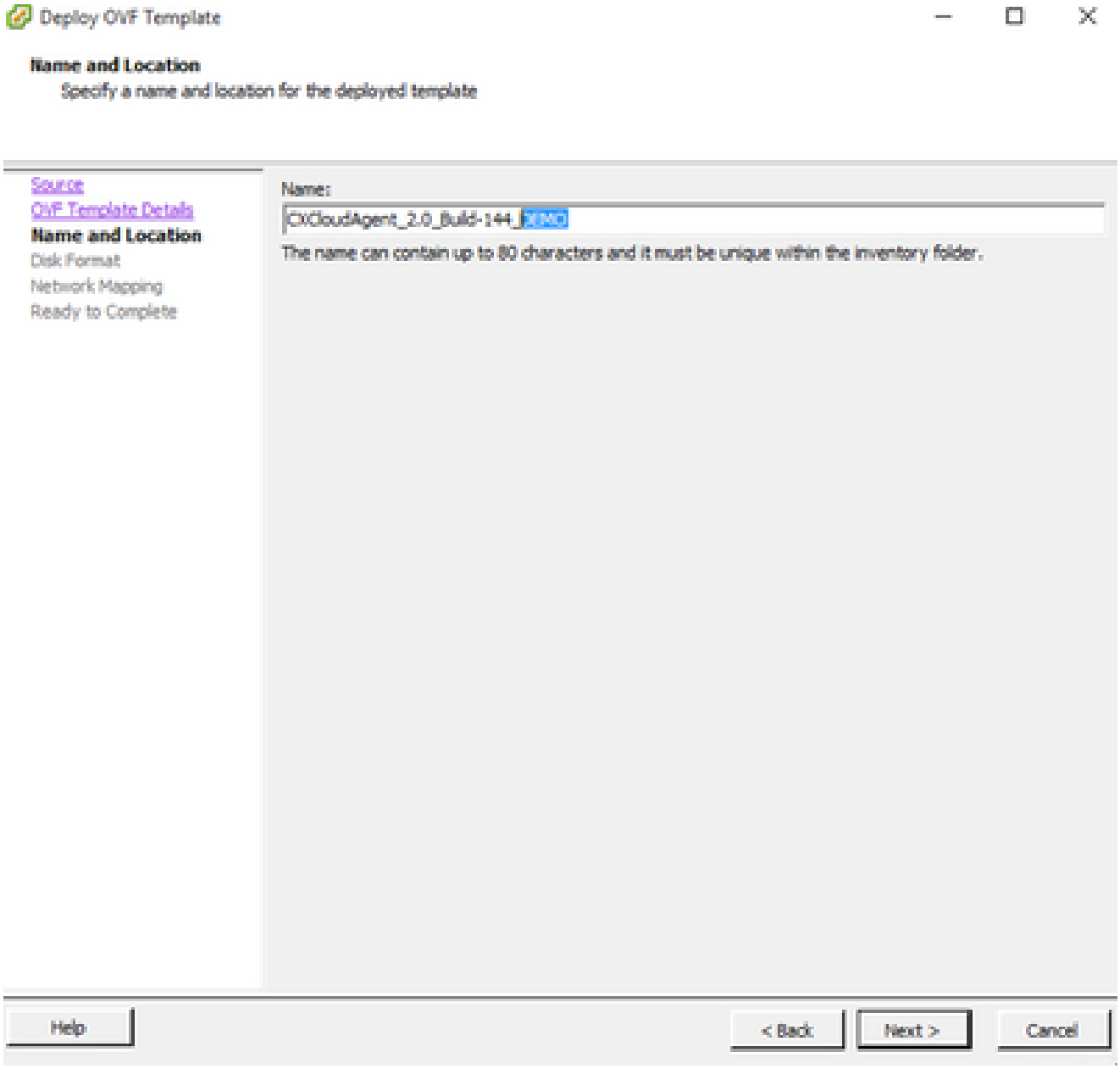
OVA 路徑

4. 驗證OVF Details，然後按一下Next。



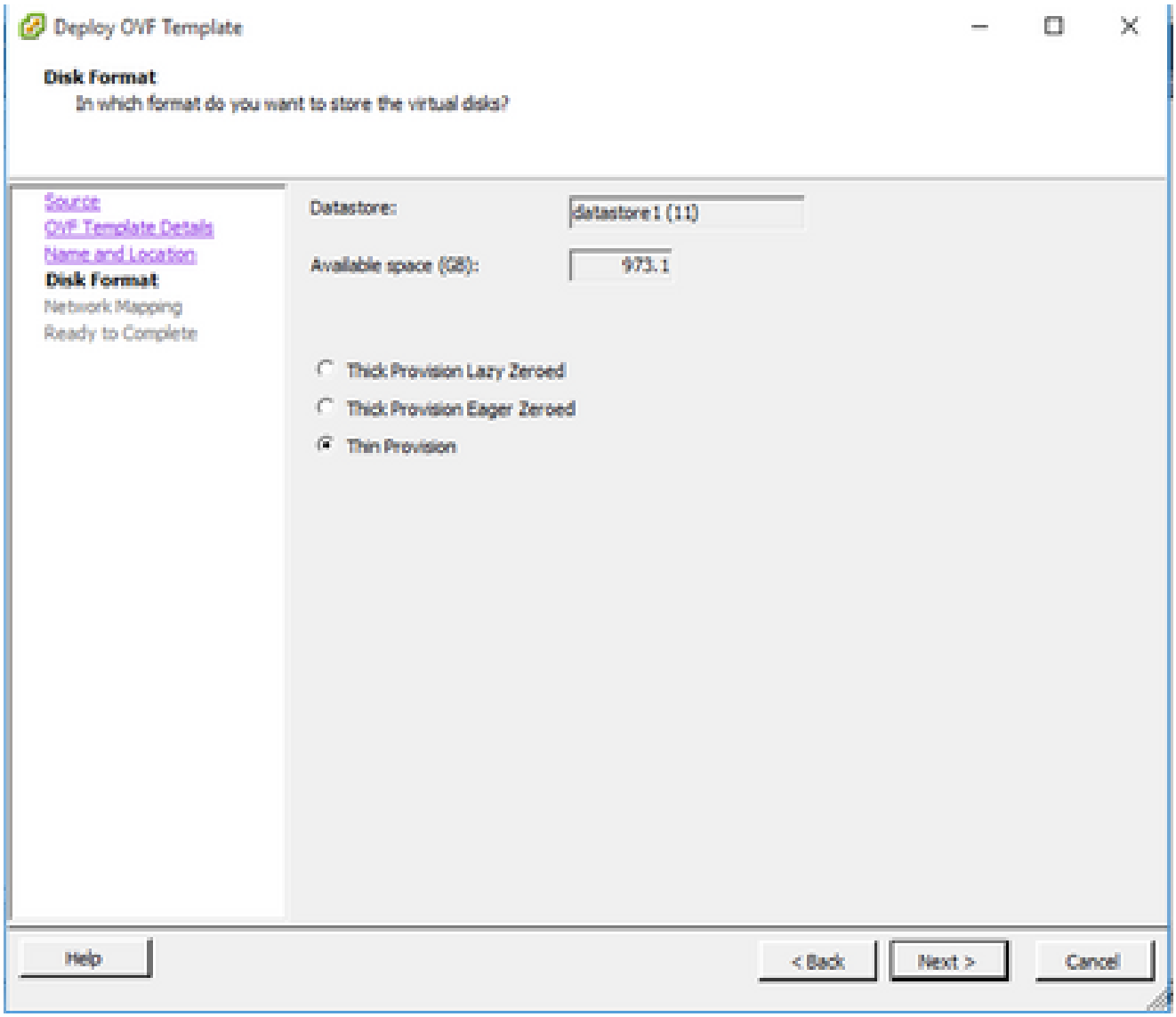
範本詳細資料

5. 輸入Unique Name，然後按一下Next。



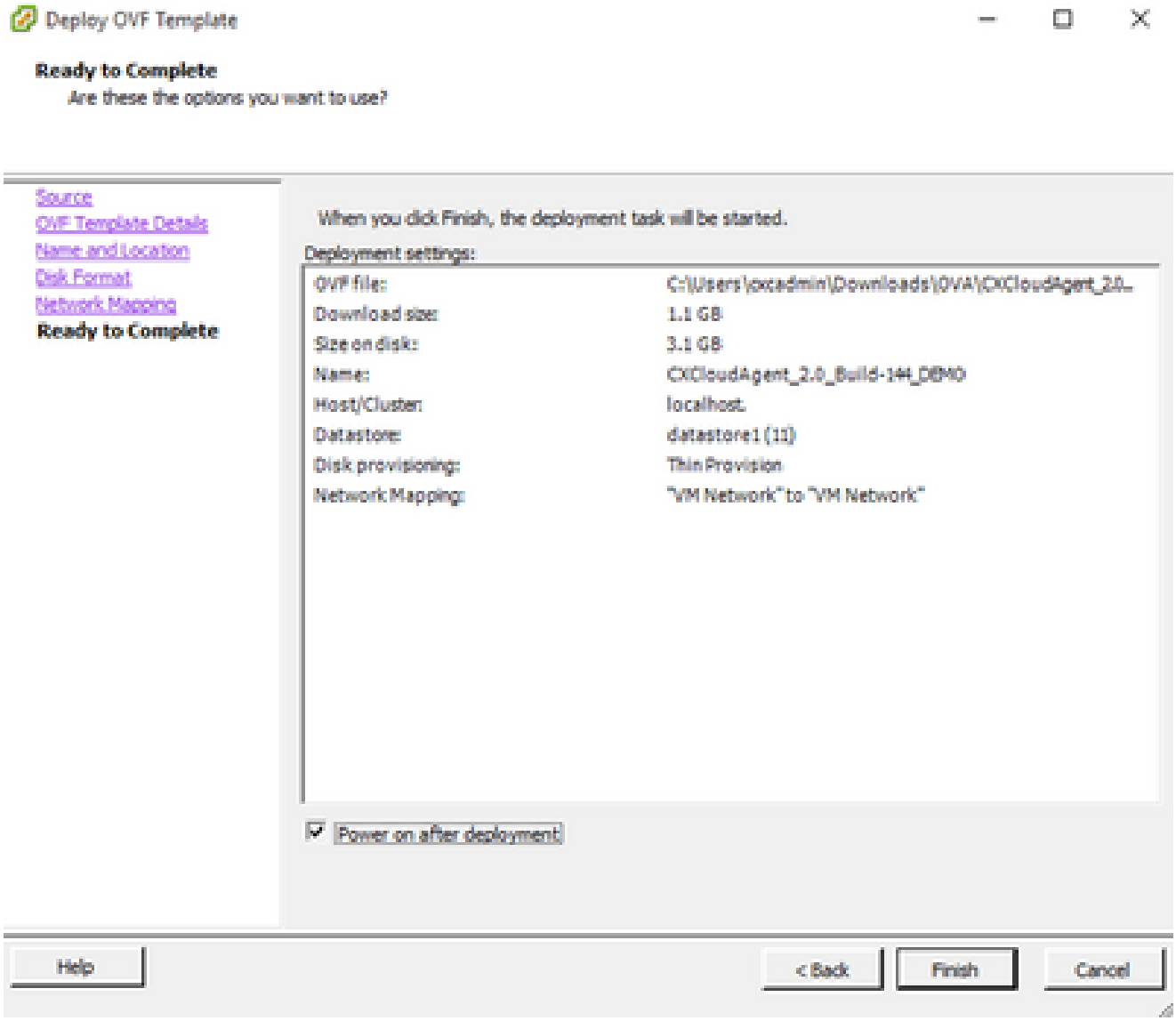
名稱與位置

6. 選擇Disk Format，然後按一下Next（建議使用Thin Provision）。



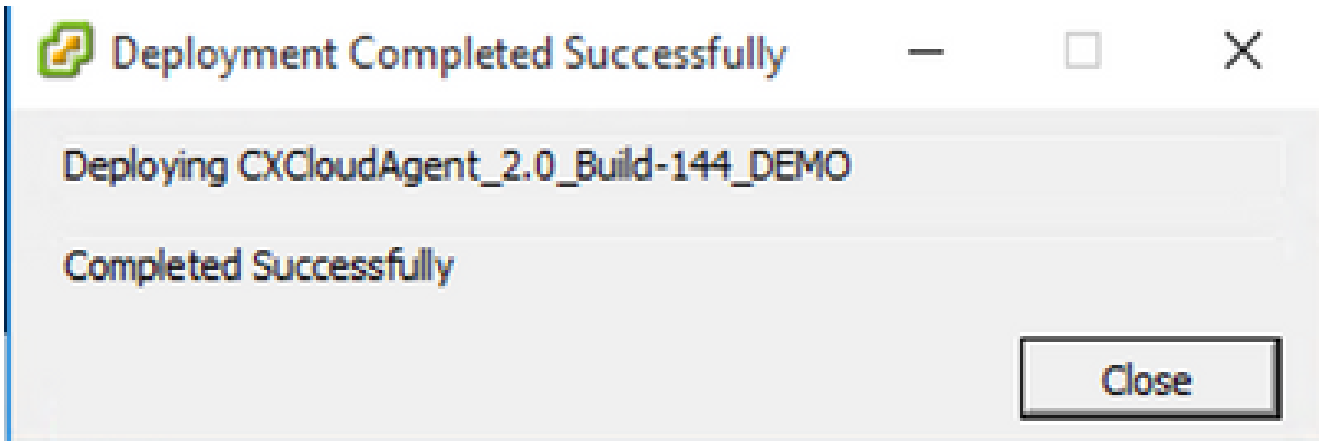
磁碟格式

7. 選中Power on after deployment覈取方塊並按一下 關閉。



準備完成

部署過程可能需要幾分鐘時間。成功部署後將顯示WConfirmation。



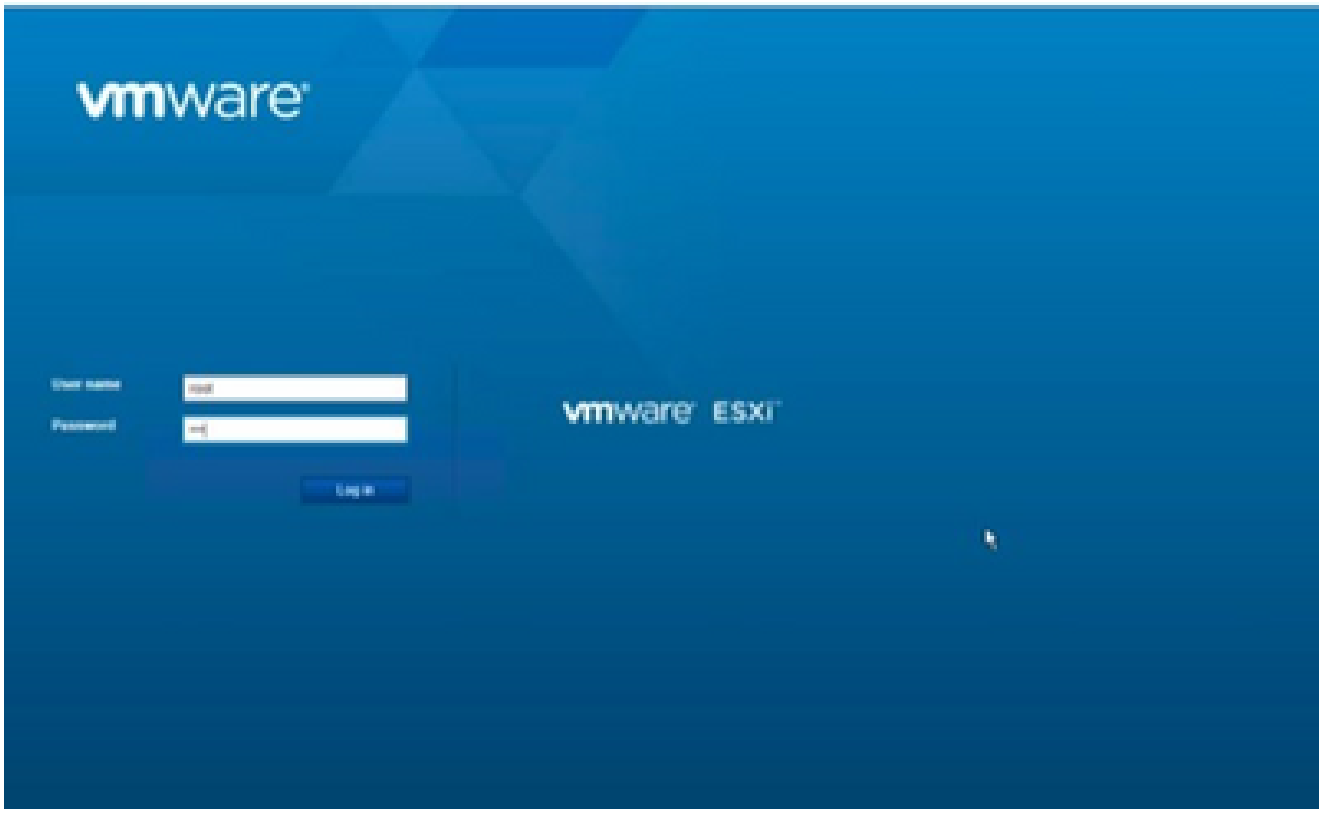
部署完成

8. 選擇已部署的VM，開啟控制檯，然後轉到網路配置以繼續執行後續步驟。

Web 用戶端 ESXi 6.0 安裝

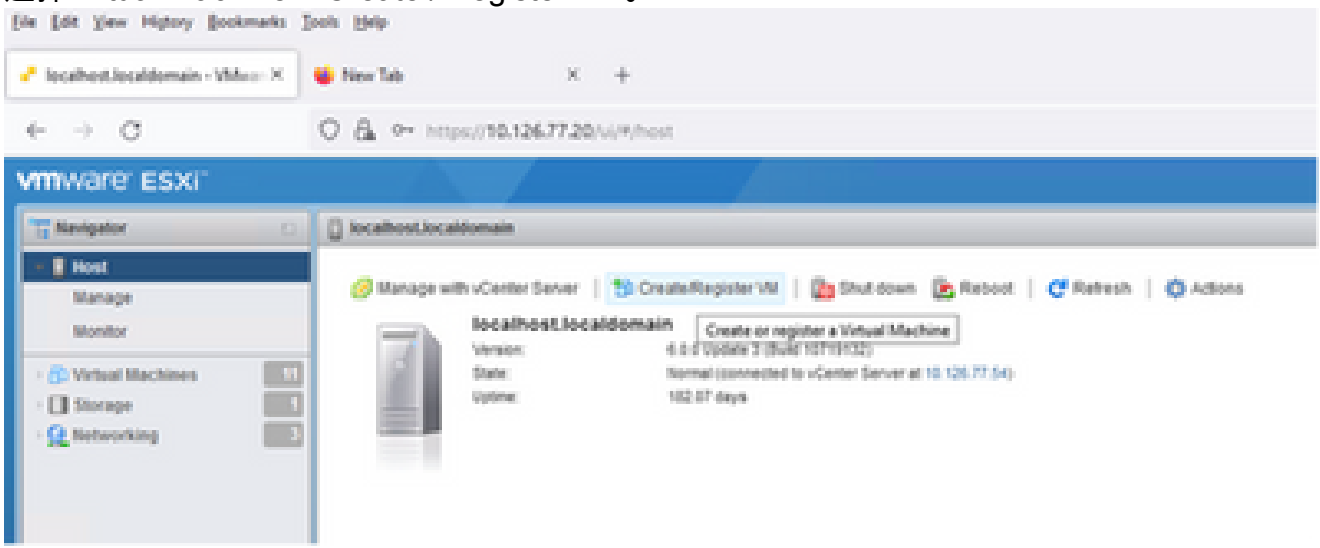
此客戶端使用vSphere Web部署CX雲代理OVA。

1. 使用用於部署VM的ESXi/虛擬機器監控程式憑證登入到VMWare UI。



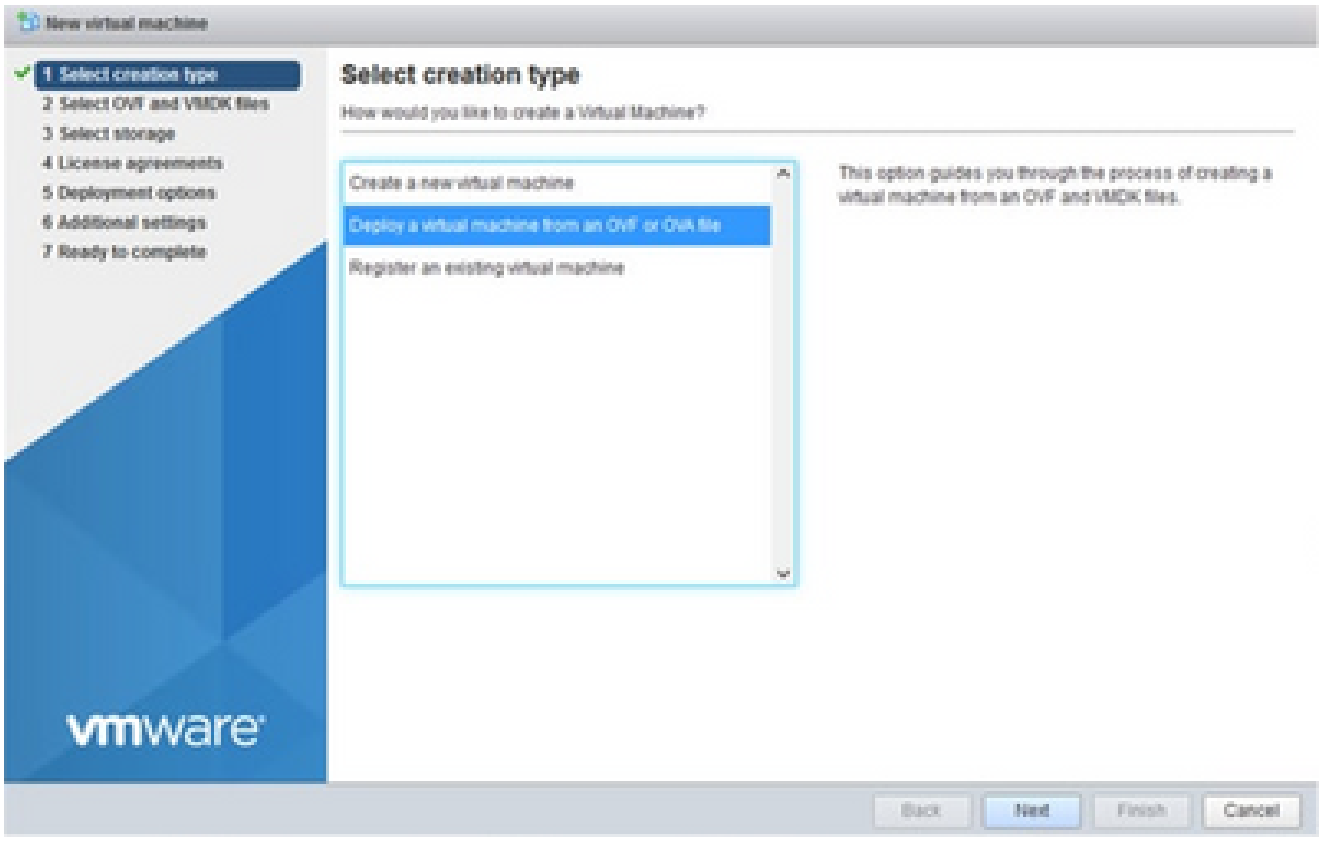
VMware ESXi 登入

2. 選擇Virtual Machine > Create / Register VM。



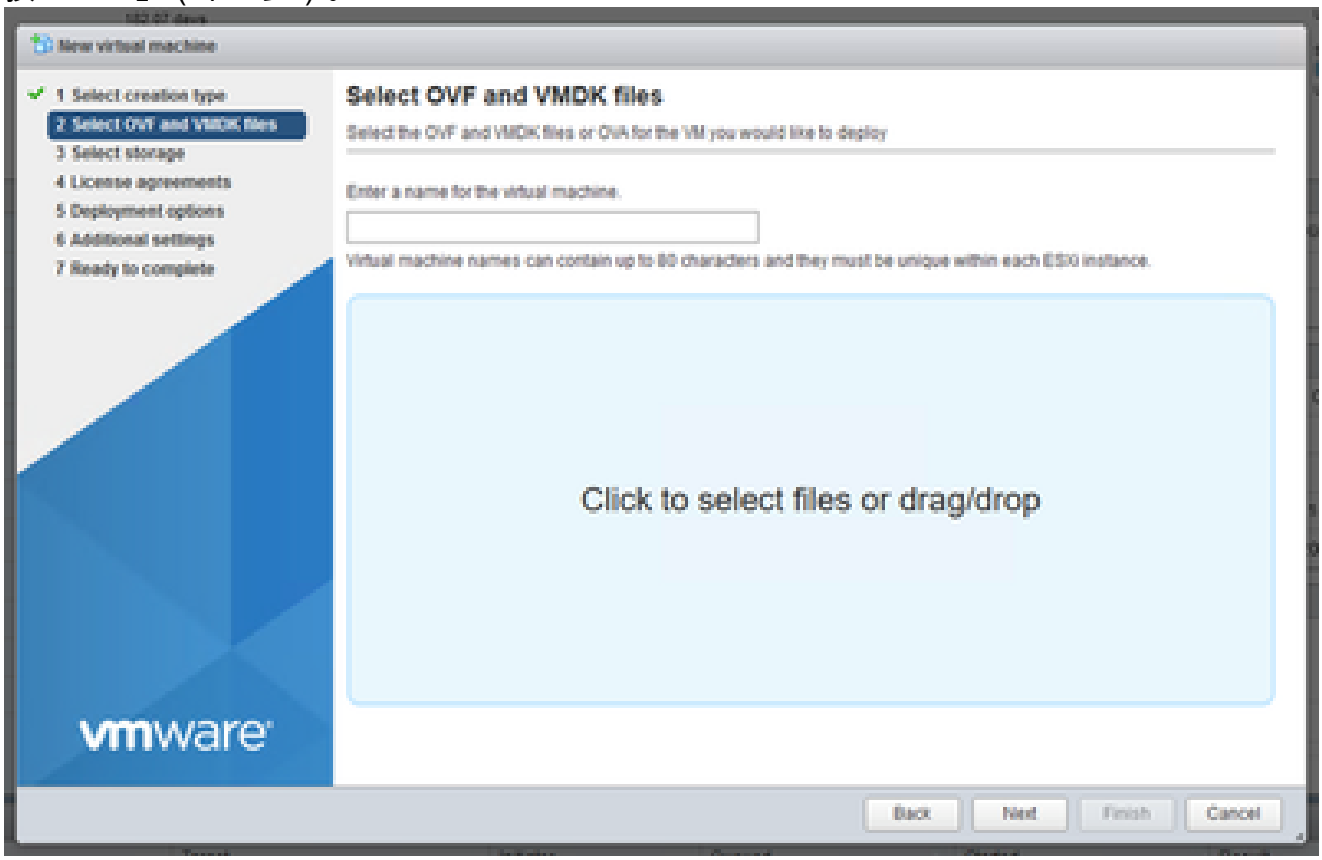
建立 VM

3. 選取「Deploy a virtual machine from an OVF or OVA file」（從 OVF 或 OVA 檔案部署虛擬機器），並按一下「Next」（下一步）。



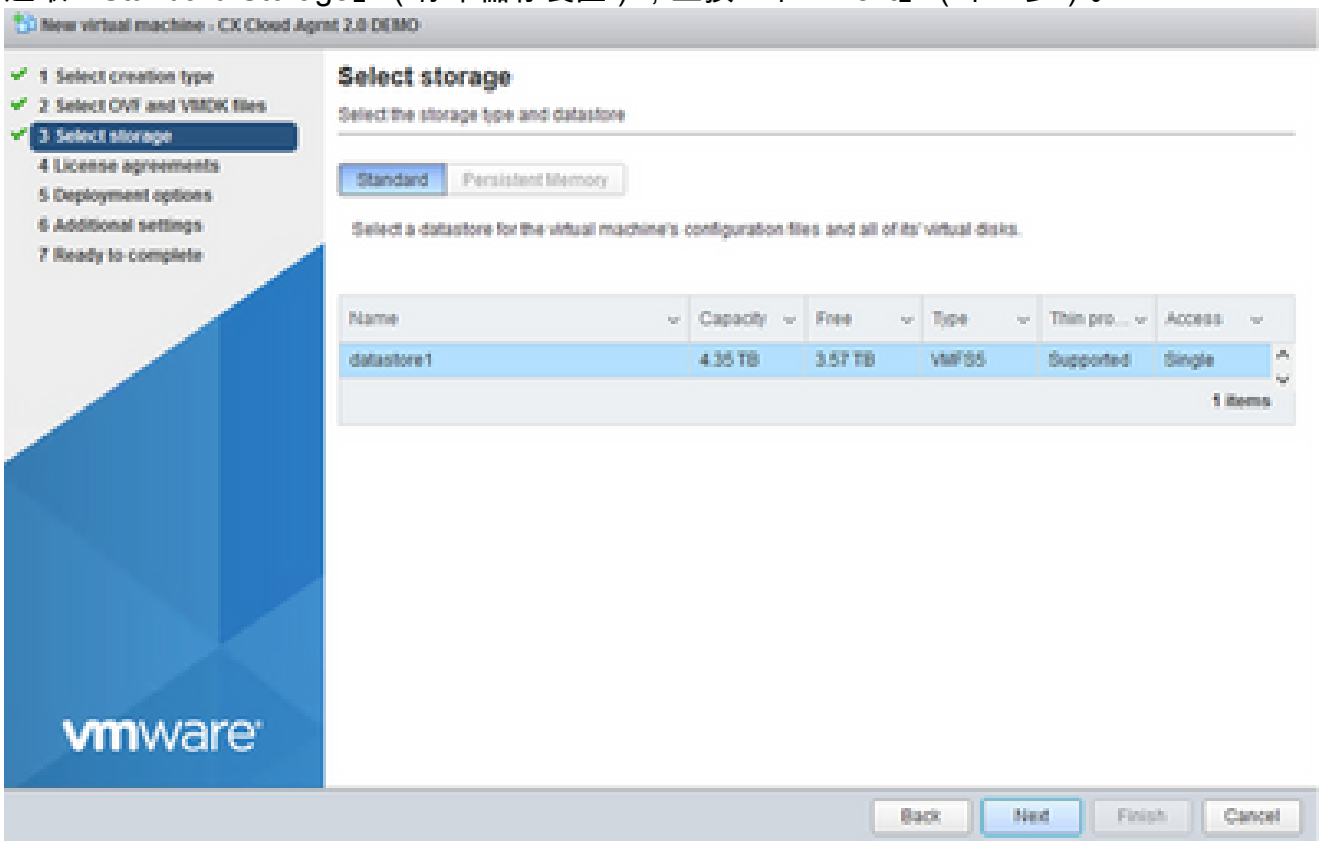
選擇建立型別

4. 輸入VM的名稱，瀏覽以選擇檔案，或拖放下載的OVA檔案。
5. 按「Next」（下一步）。



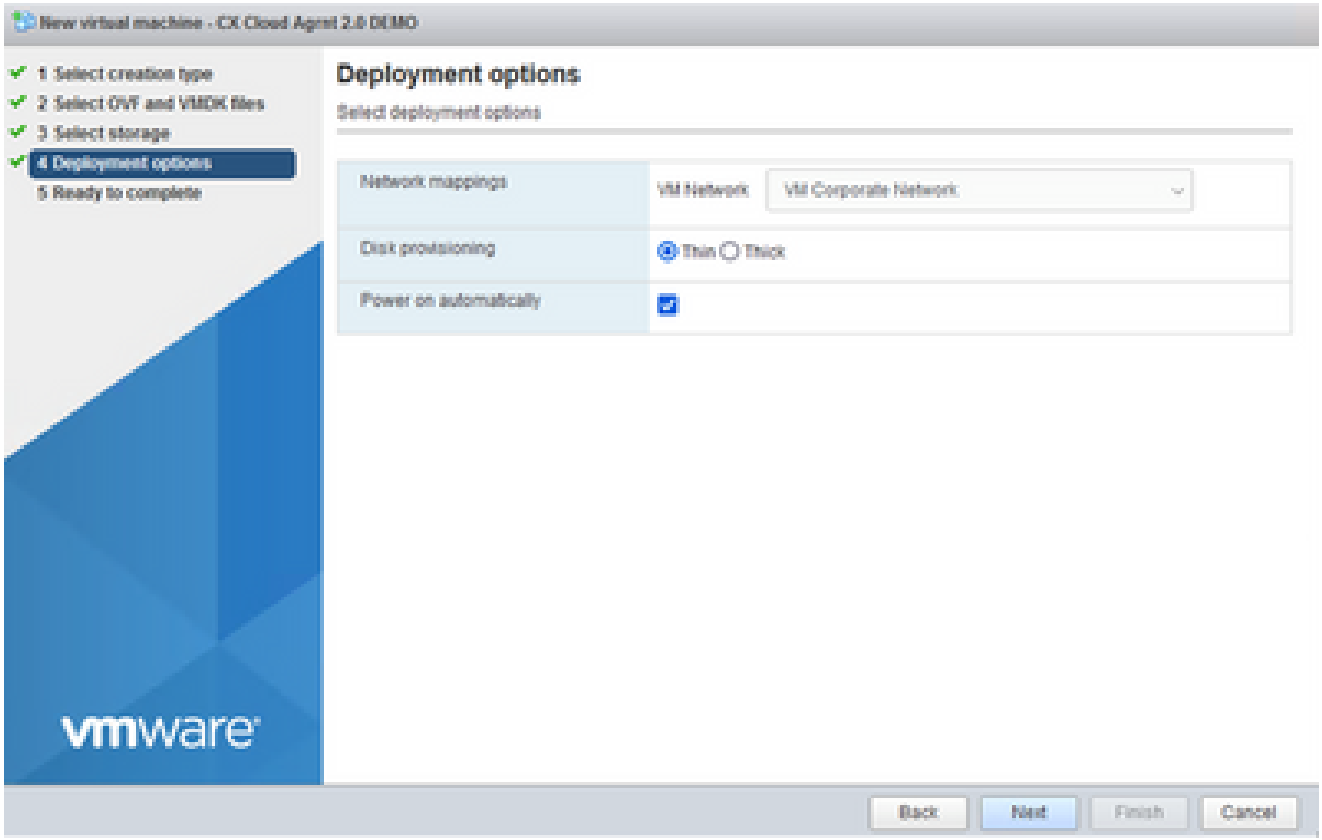
OVA 選擇

6. 選取「Standard Storage」（標準儲存裝置），並按一下「Next」（下一步）。



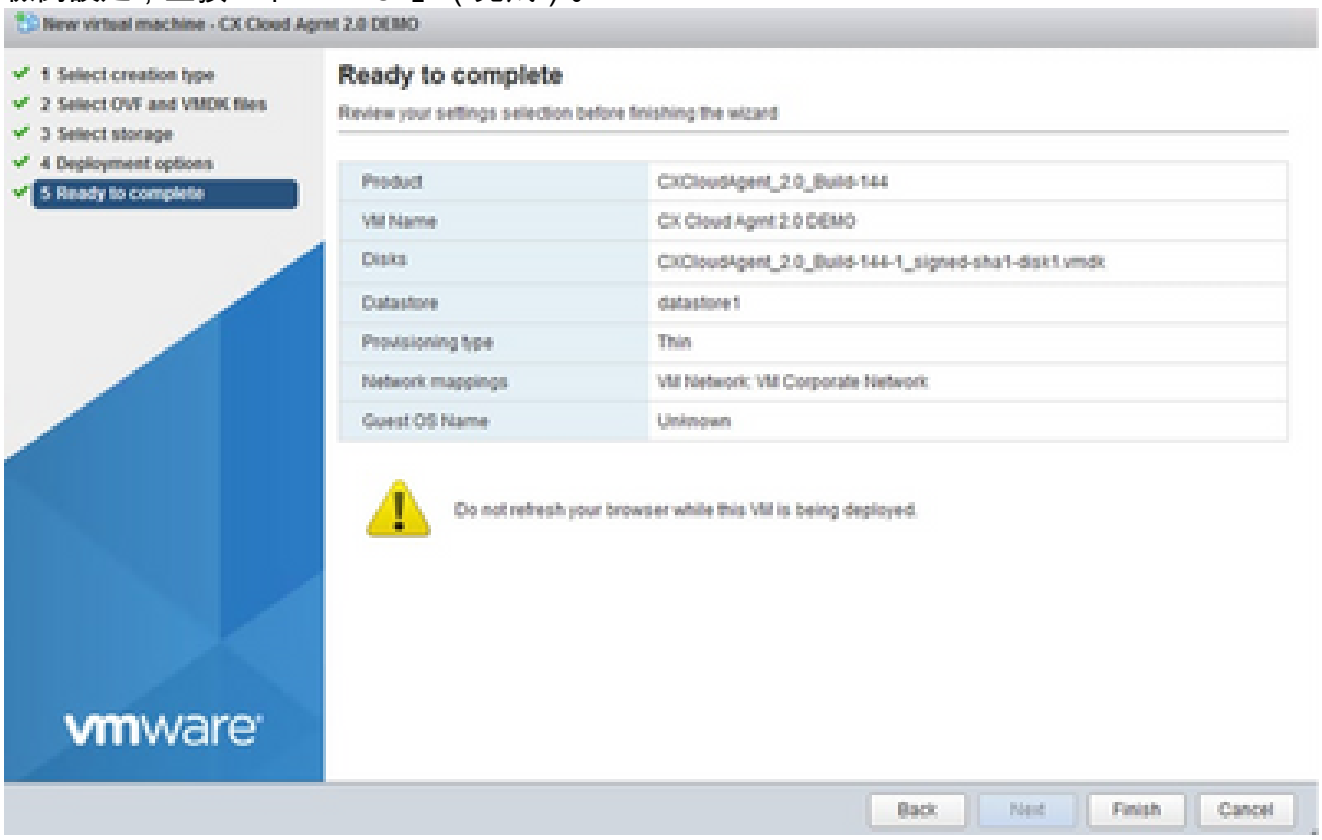
選取儲存裝置

7. 選擇適當的部署選項，然後按一下 下一頁.

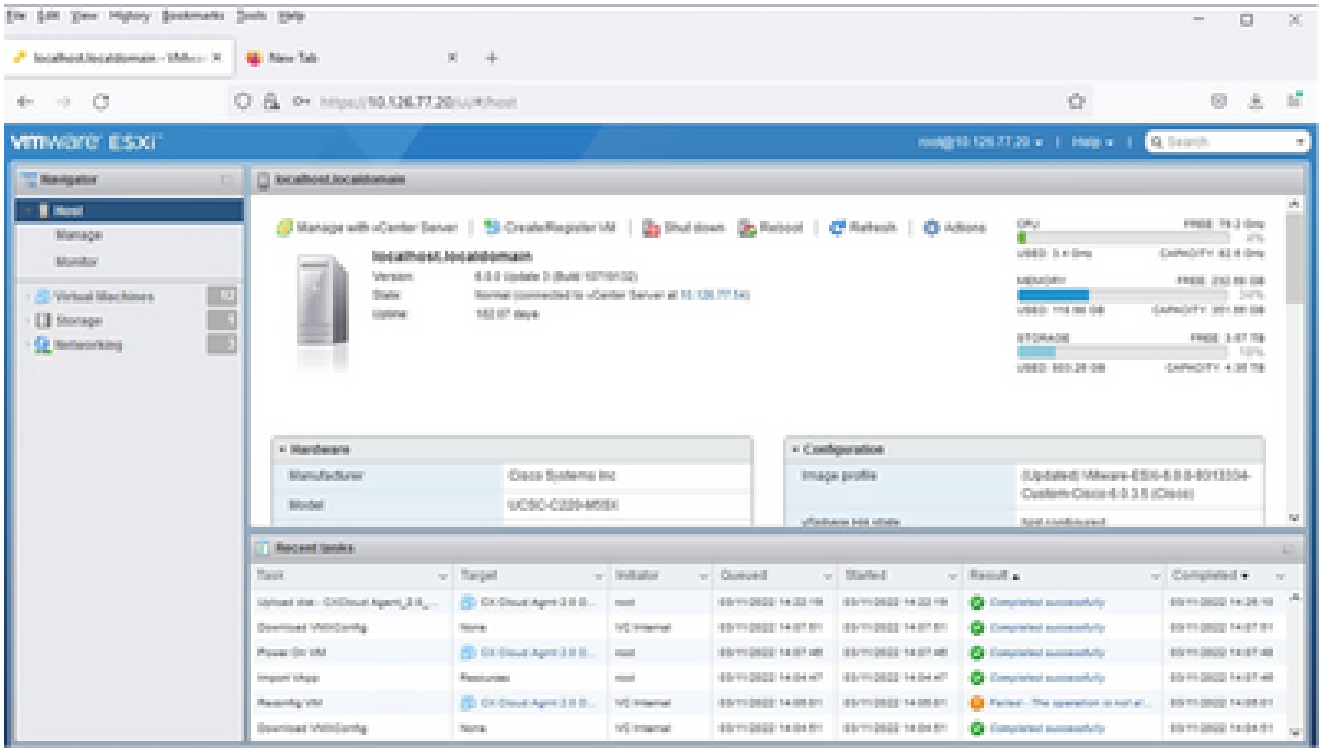


部署選項

8. 檢閱設定，並按一下「Finish」（完成）。

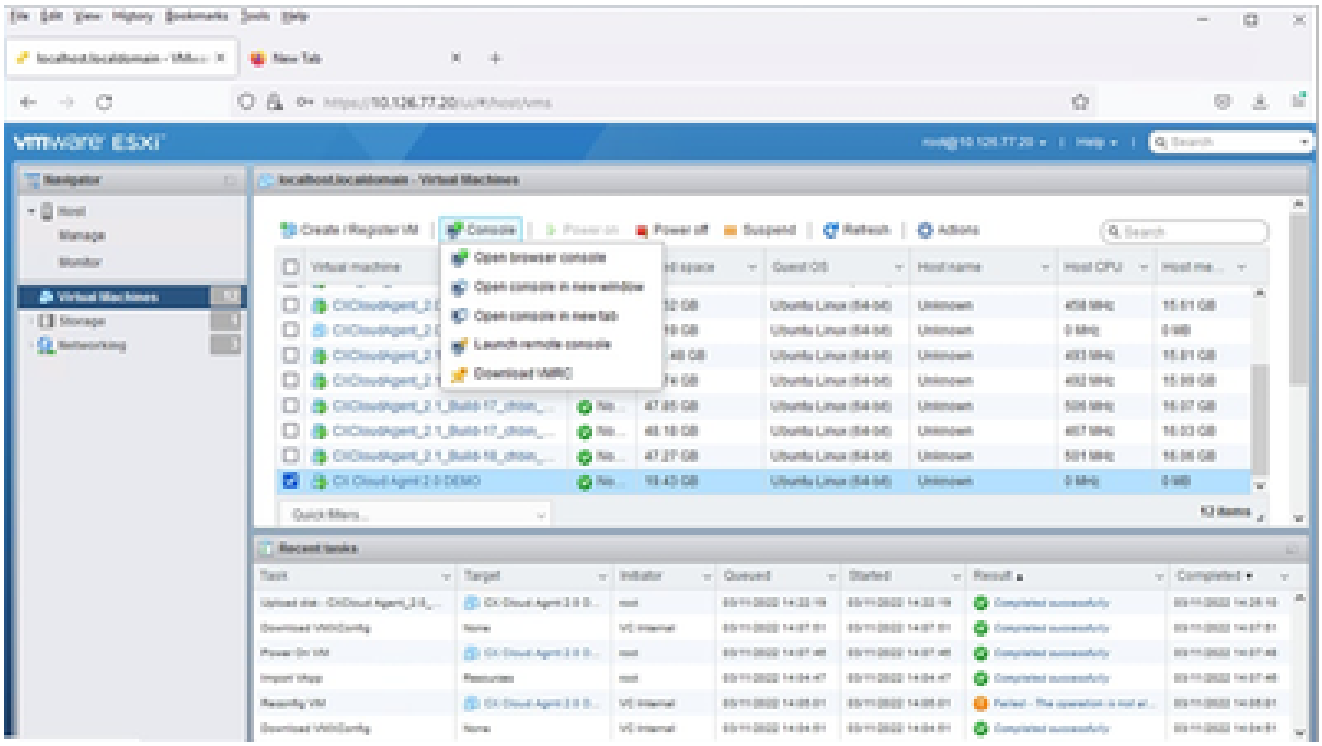


準備完成



成功完成

9. 選擇剛部署的VM，然後選擇Console > Open browser console。



主控台

10. 導覽至Network Configuration，繼續執行以下步驟。

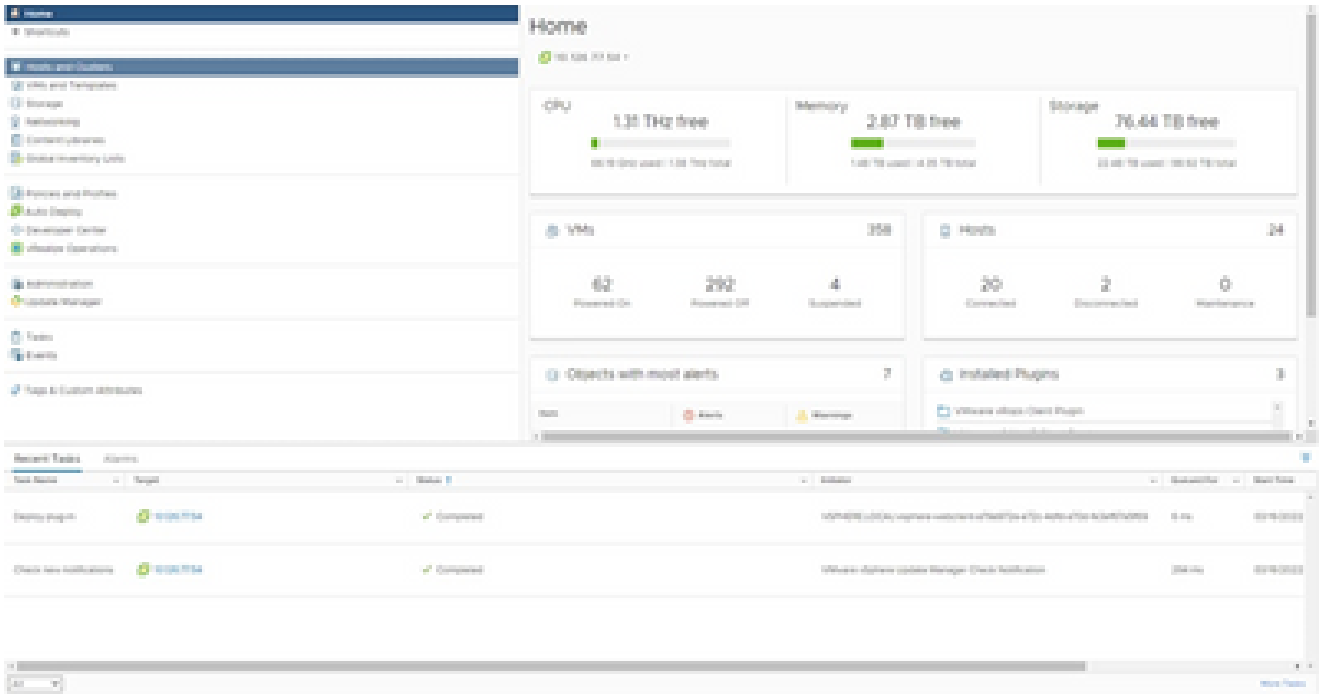
Web 用戶端 vCenter 安裝

執行下列操作：

1. 使用ESXi/虛擬機器監控程式憑證登入到vCenter客戶端。

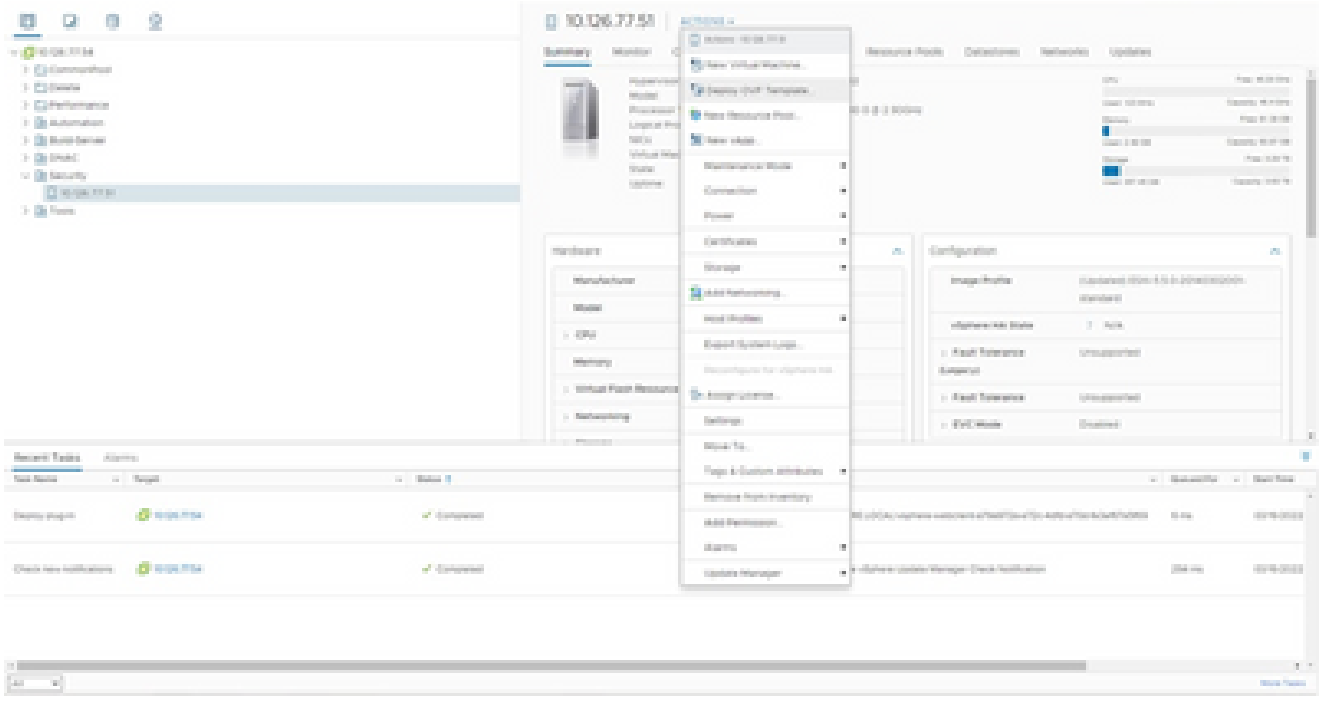
登入

2. 在Home頁中，按一下Hosts and Clusters。

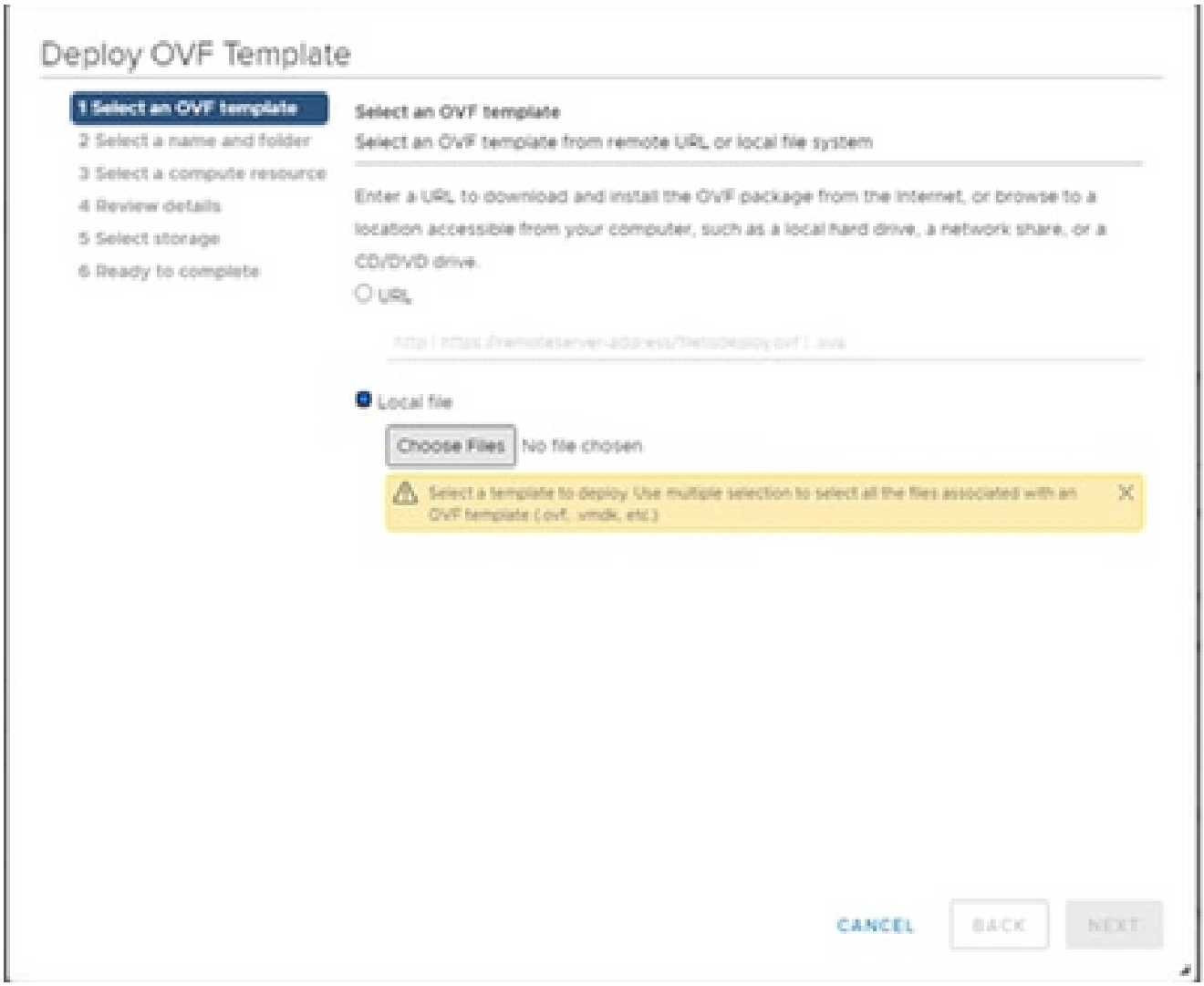


首頁

3. 選取 VM，並按一下「Action > Deploy OVF Template」（動作 > 部署 OVF 範本）。

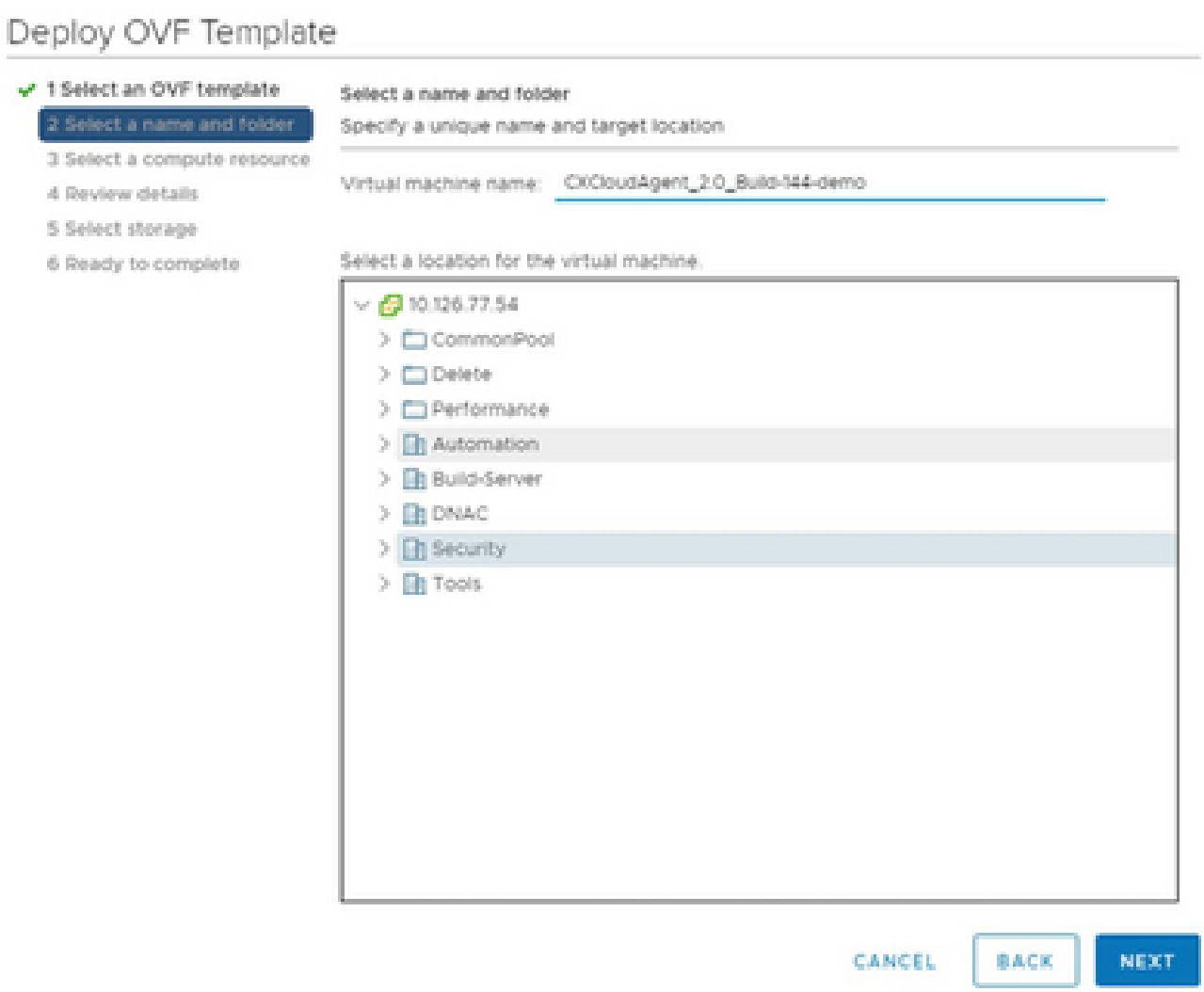


動作



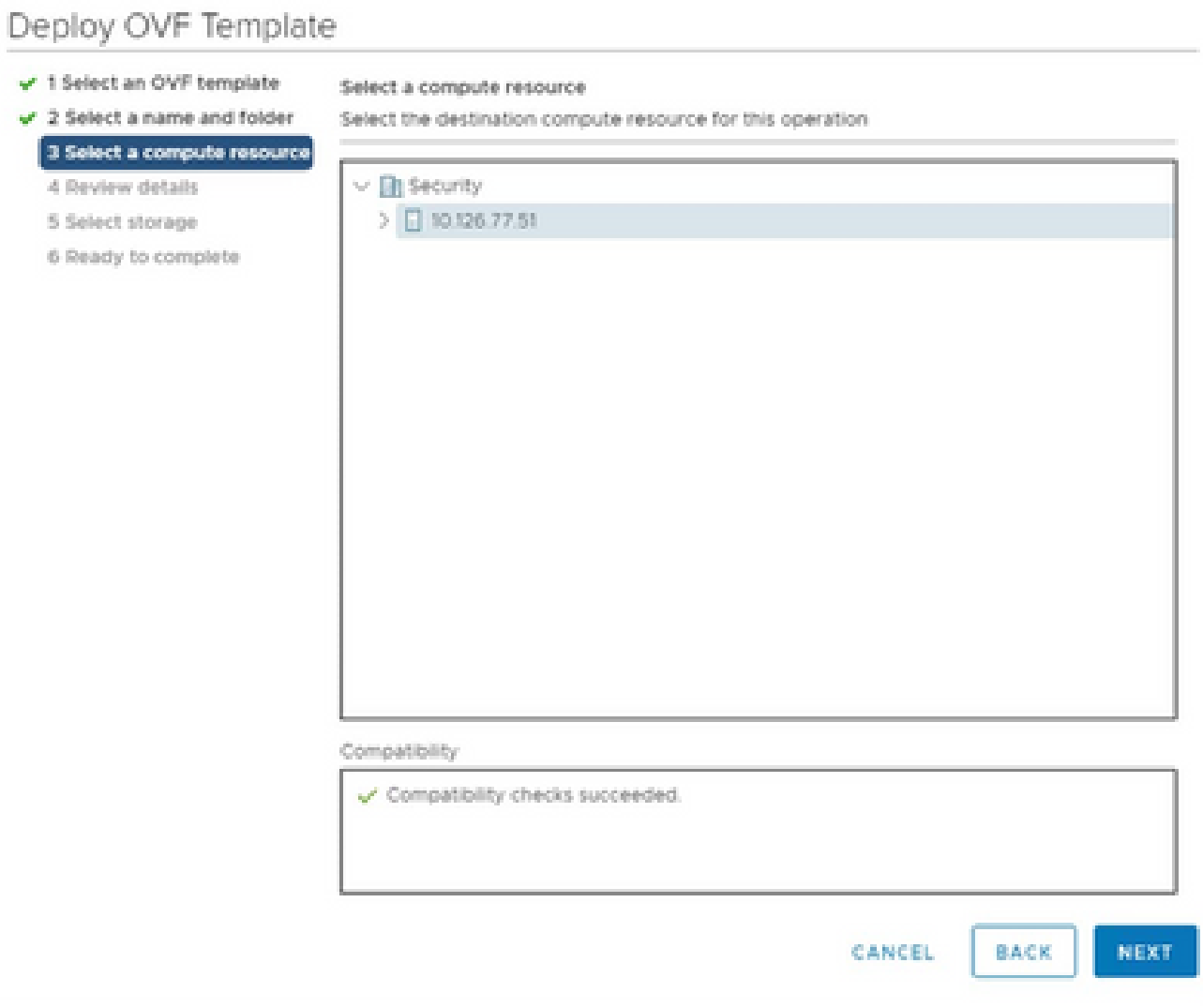
選取範本

4. 直接新增URL或瀏覽以選擇OVA檔案，然後按一下下一步。
5. 輸入唯一的名稱，並在需要時瀏覽到該位置。
6. 按「Next」（下一步）。



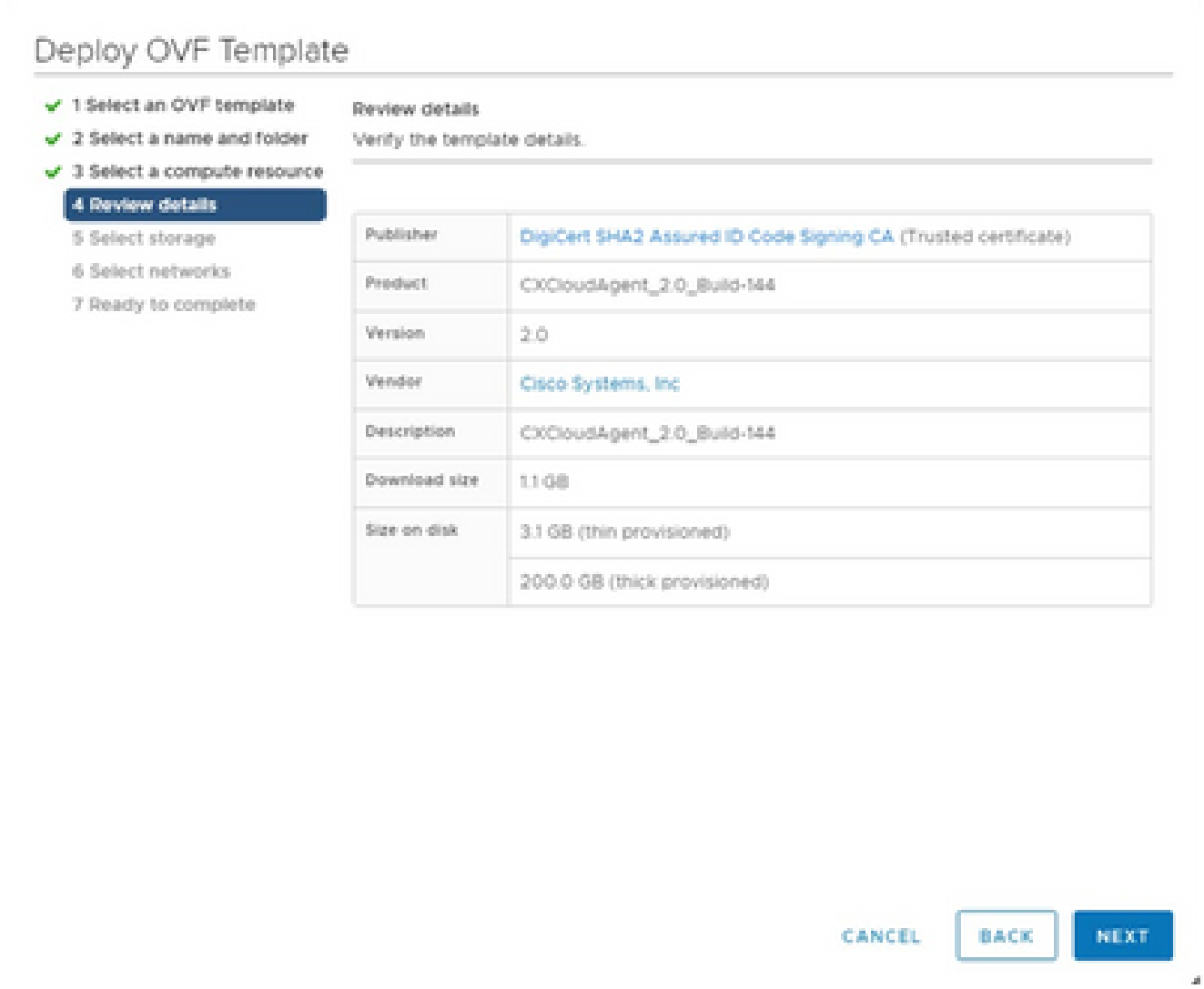
名稱和資料夾

7. 選擇計算資源，然後按一下下一步。



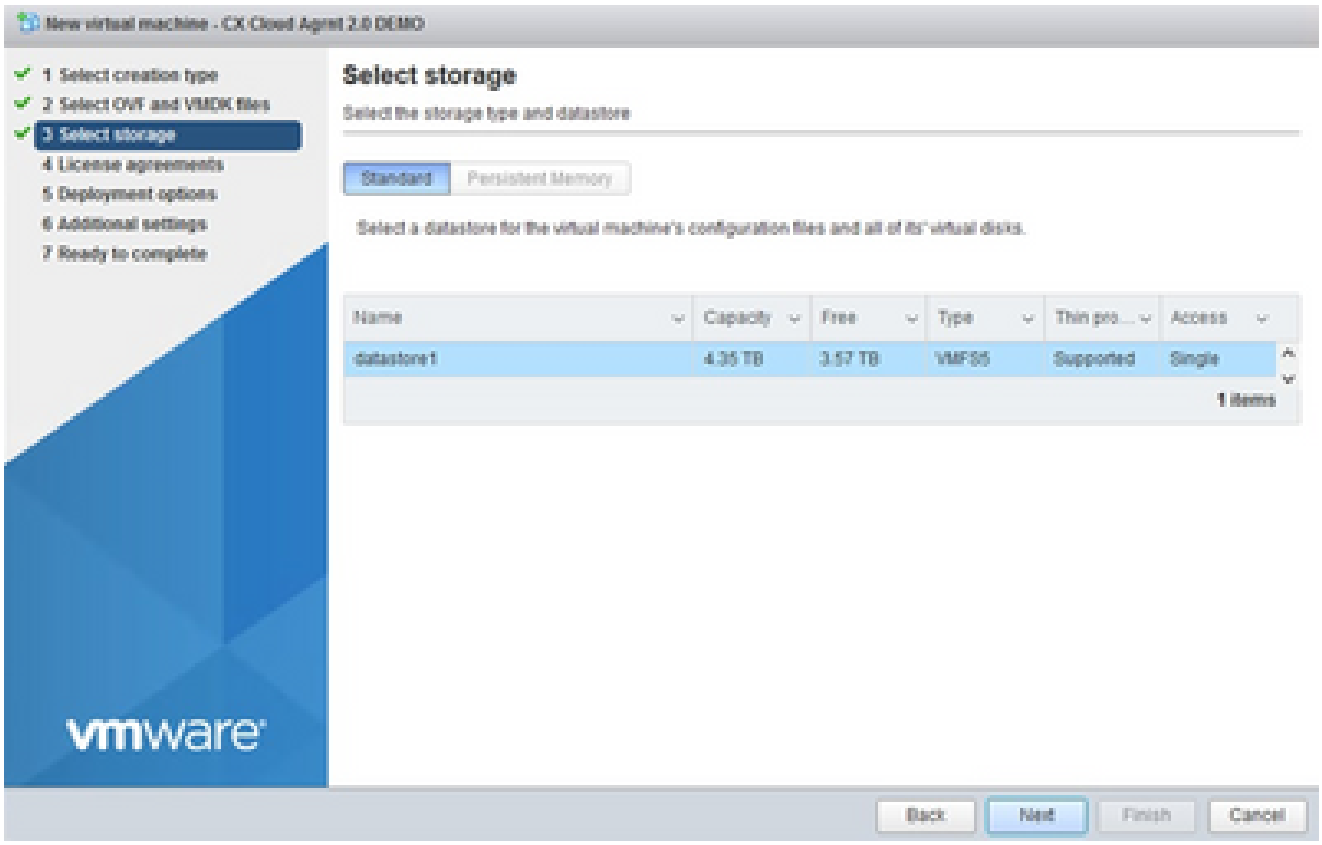
選擇電腦資源

8. 檢閱詳細資料，並按一下「Next」（下一步）。



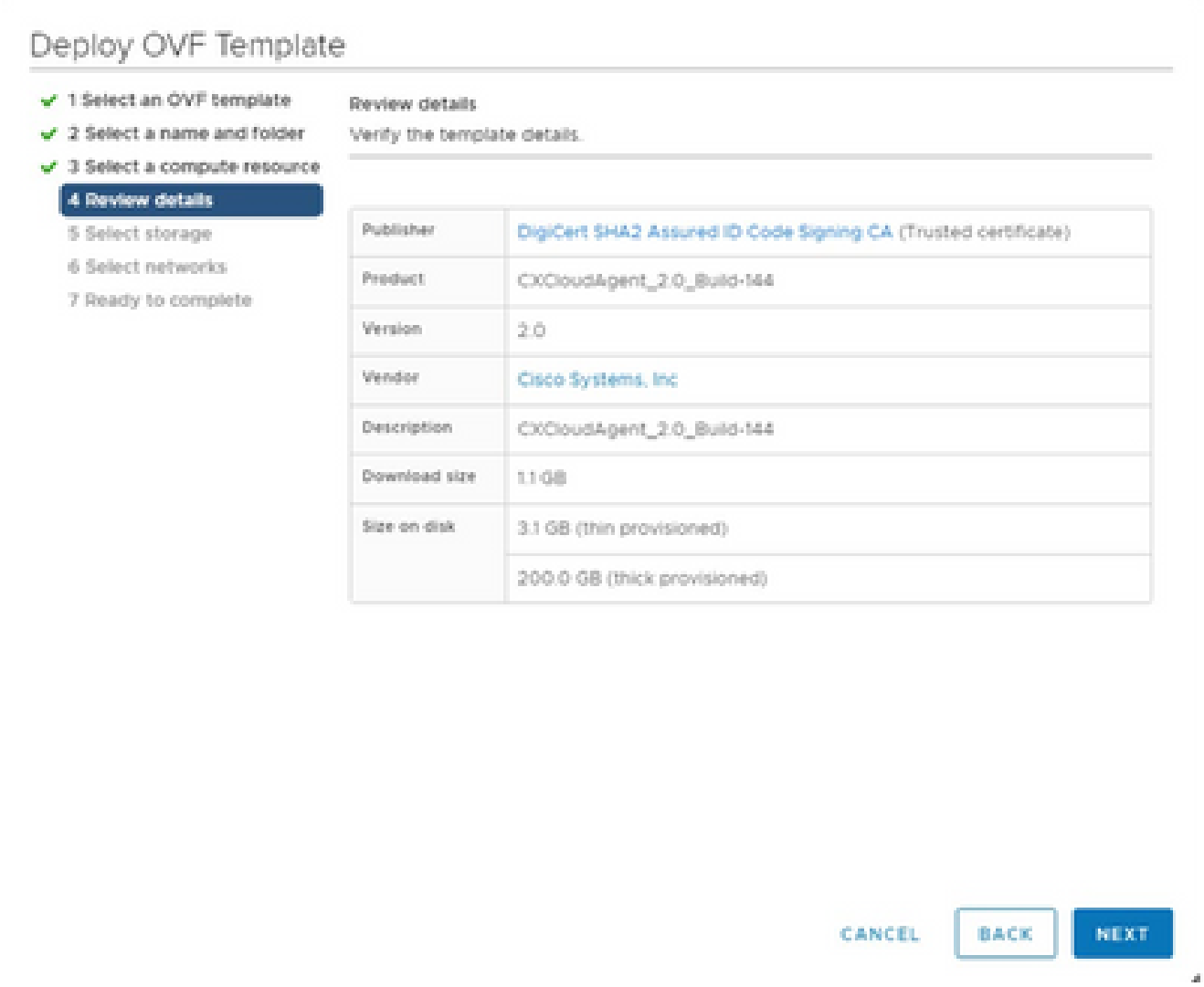
檢閱詳細資料

9. 選取虛擬磁碟格式，並按一下「Next」（下一步）。



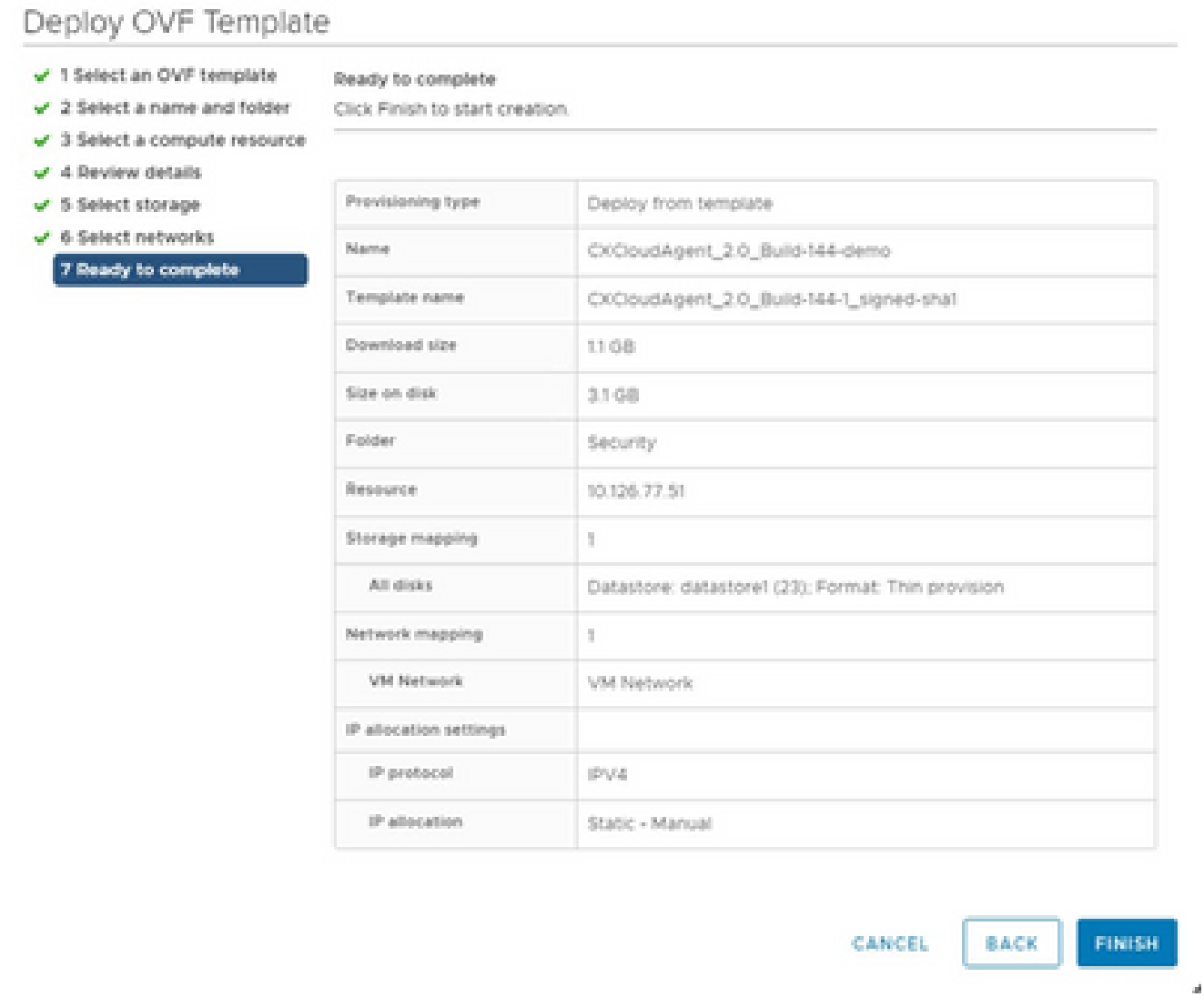
選取儲存裝置

10. 按「Next」（下一步）。



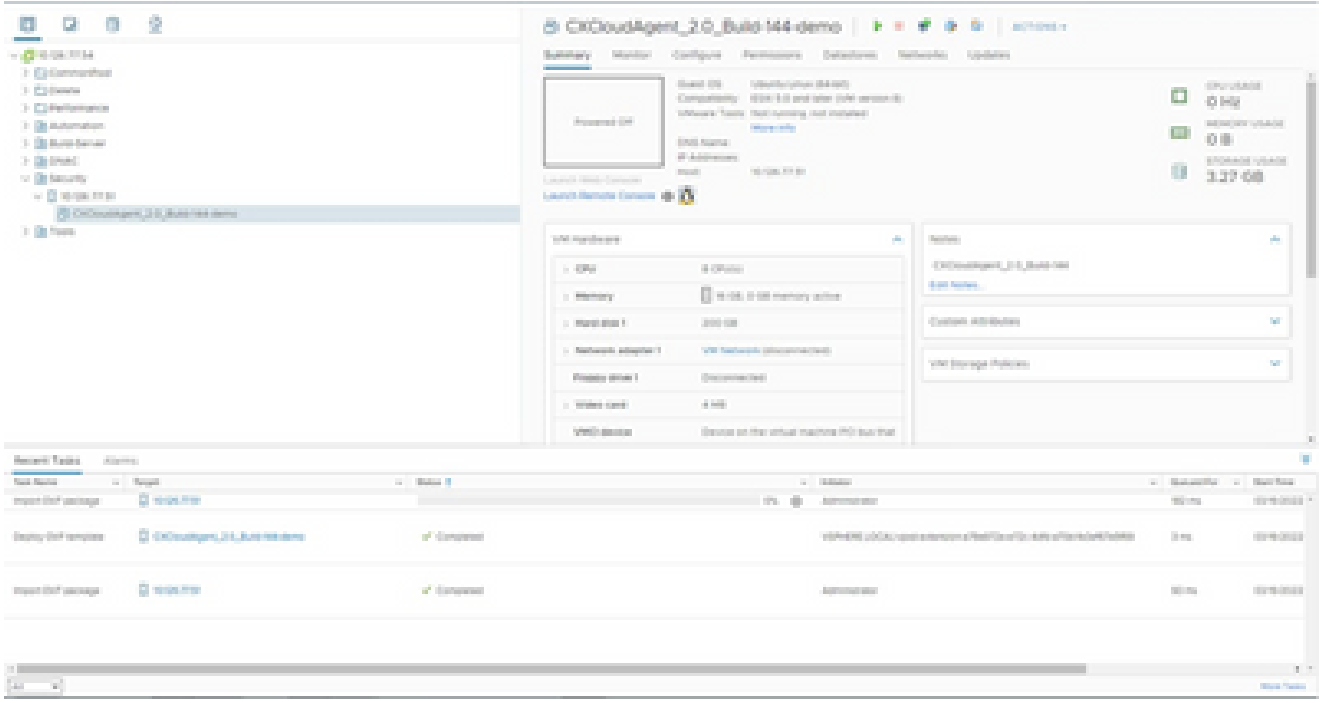
選擇網路

11. 按一下「Finish」（結束）。



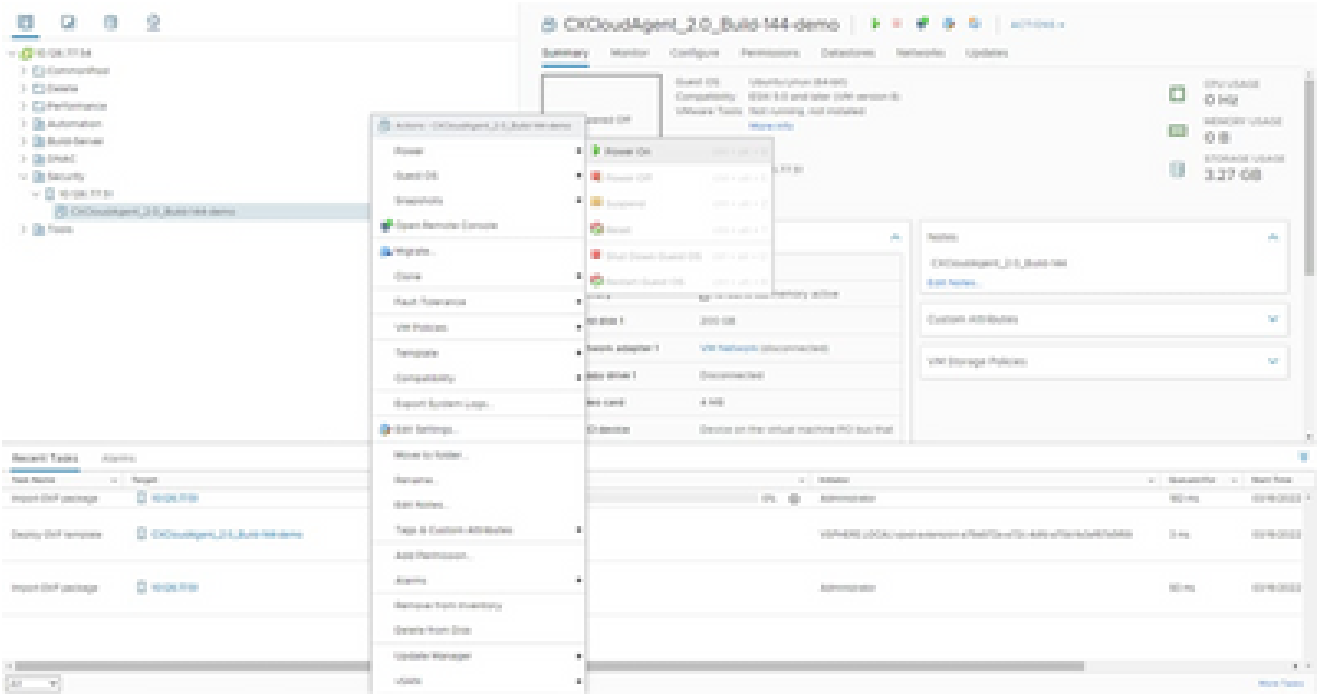
準備完成

12. 按一下新新增的虛擬機器的名稱以檢視狀態。



已新增VM

13. 安裝後，開啟VM的電源並開啟控制檯。



開啟主控台

14. 導覽至Network Configuration，繼續執行以下步驟。

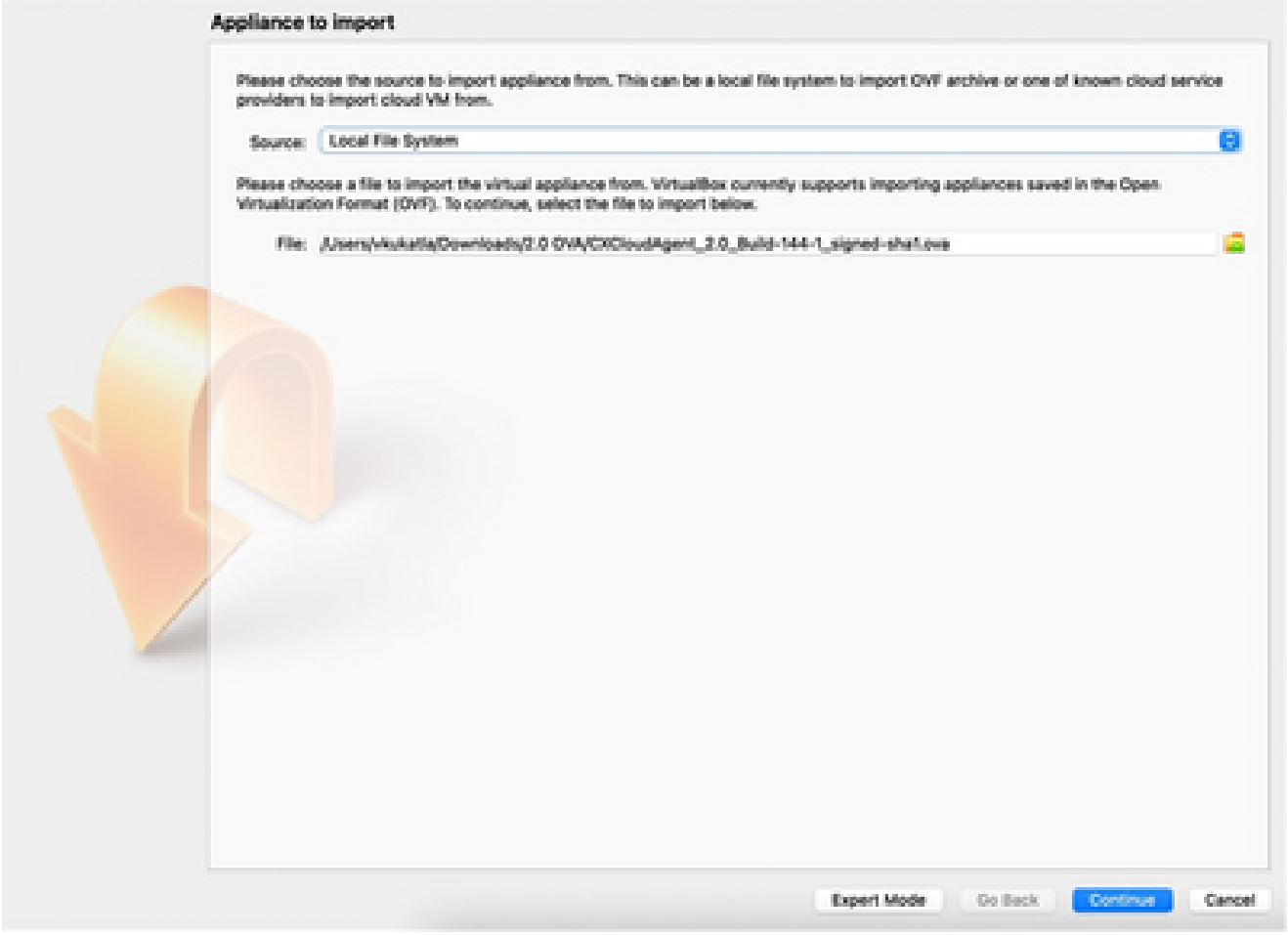
Oracle Virtual Box 5.2.30 安裝

此客戶端通過Oracle虛擬盒部署CX雲代理OVA。

1. 開啟Oracle VM UI並選擇檔案 > 匯入裝置。

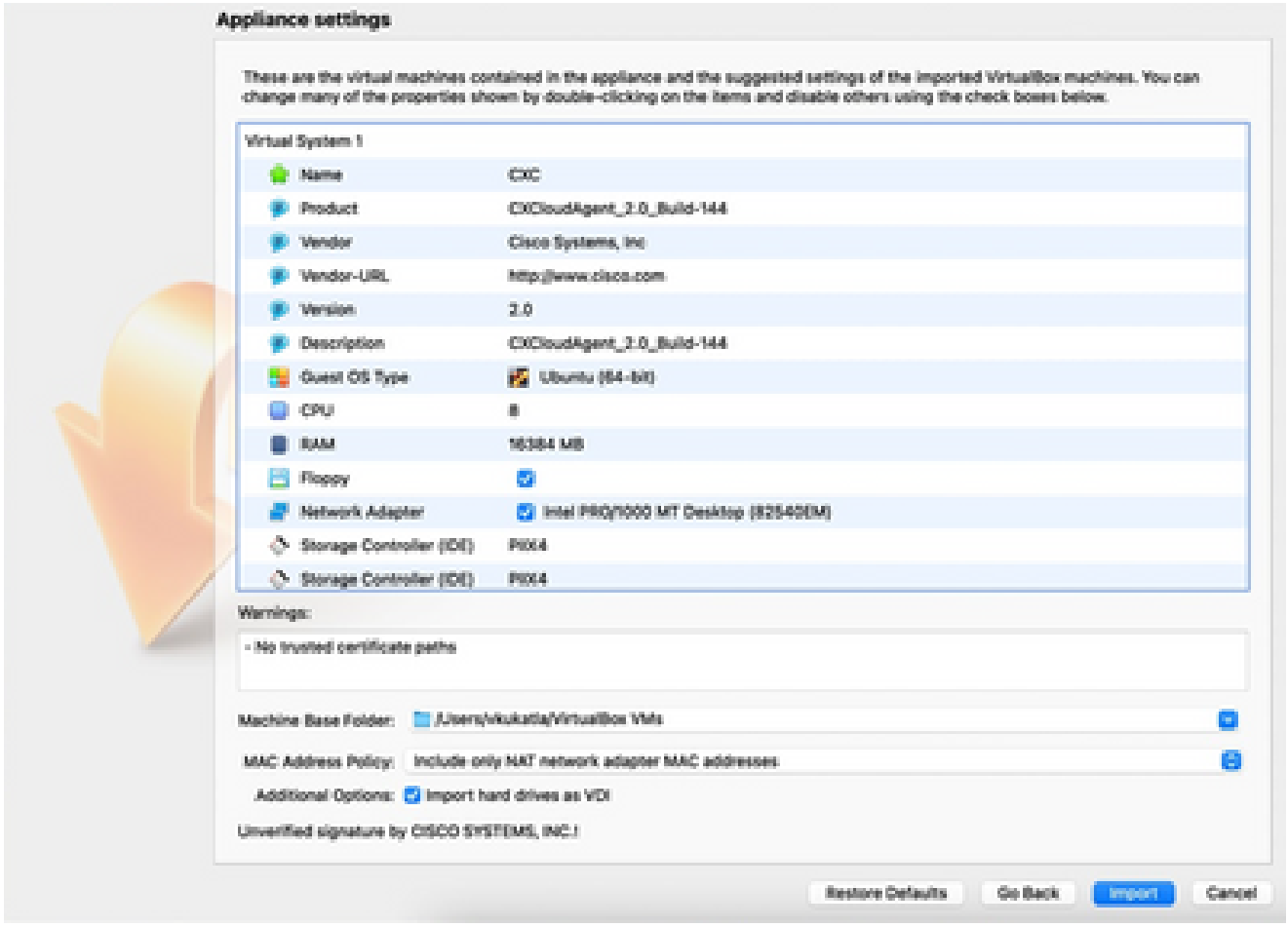
Oracle VM

2. 瀏覽以匯入 OVA 檔案。



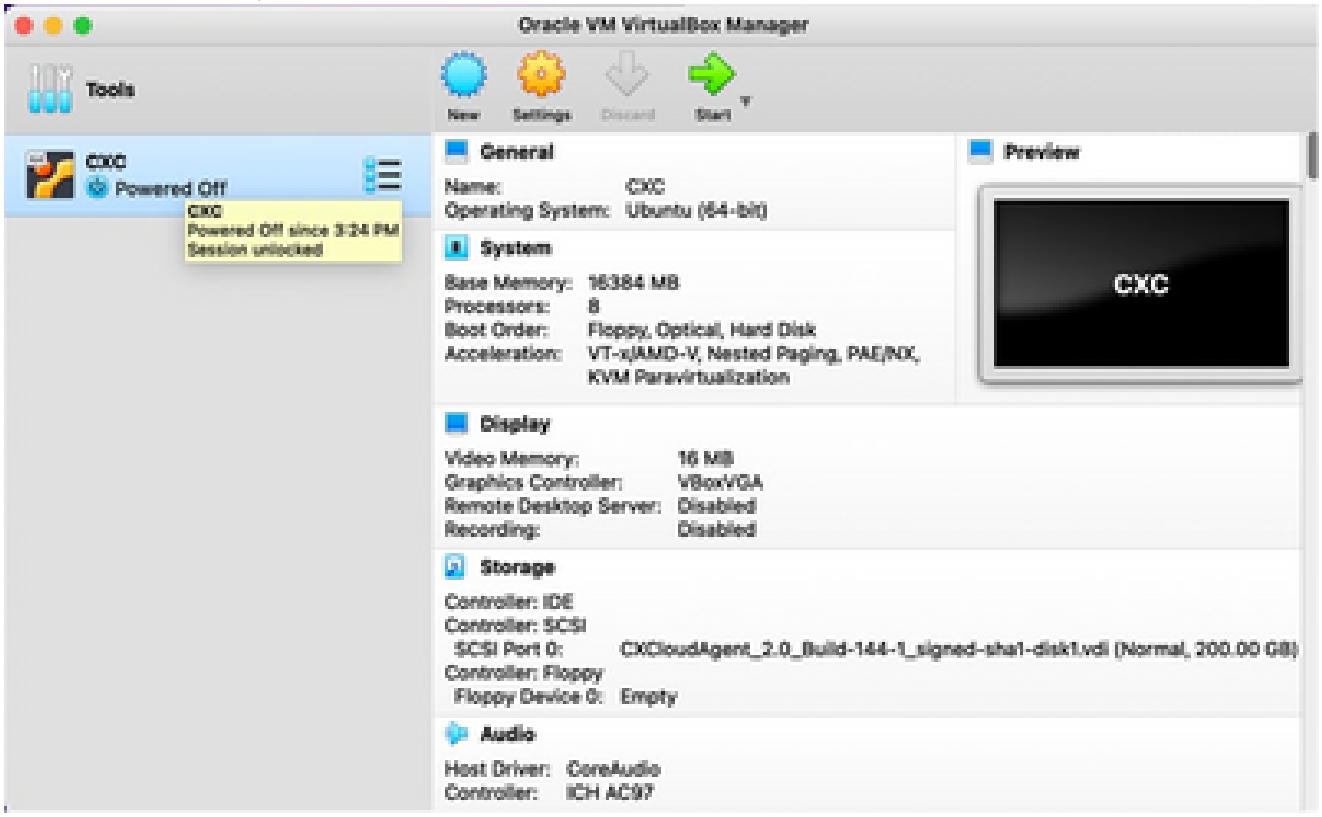
選取檔案

3. 按一下「Import」（匯入）。

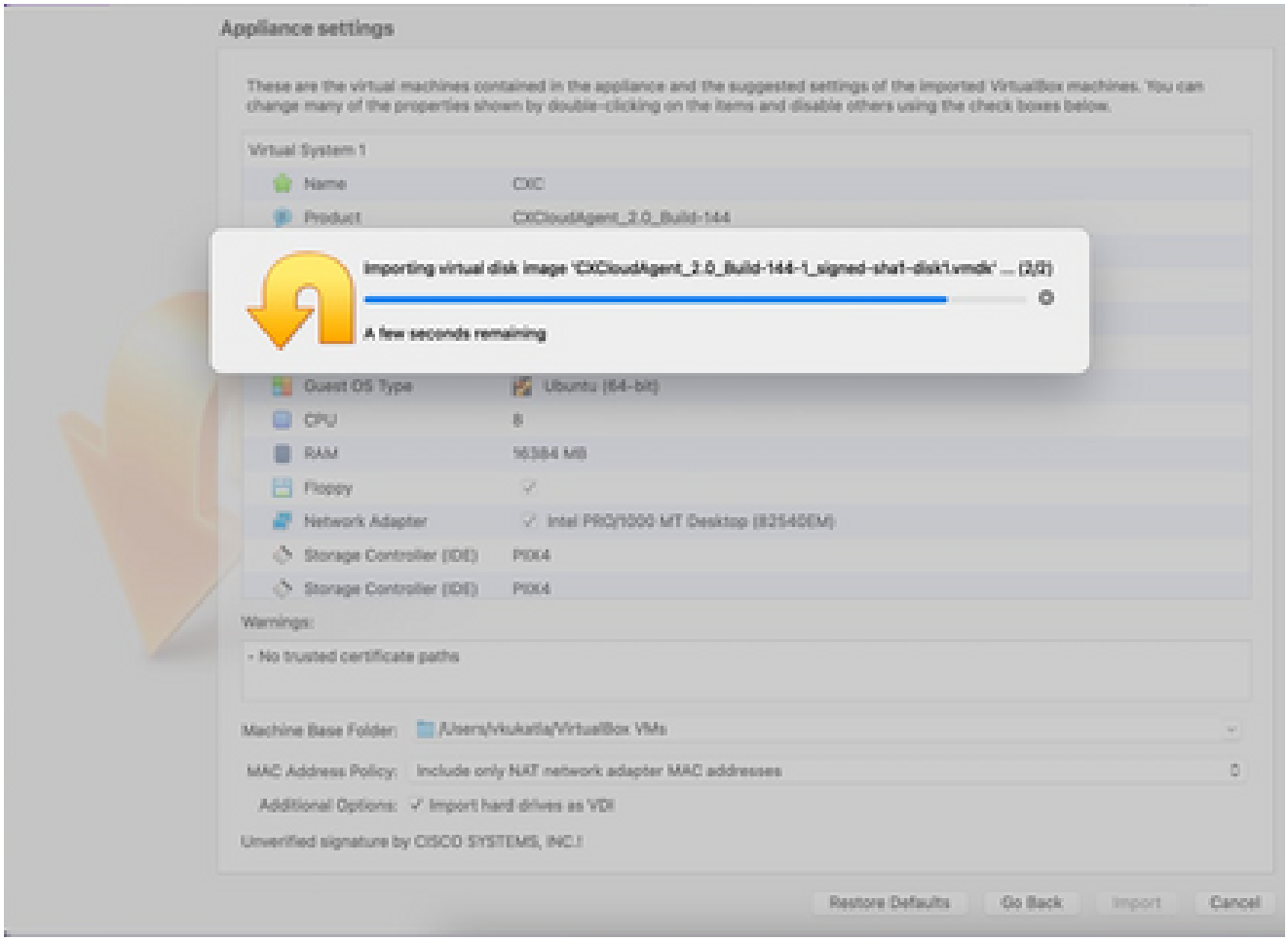


匯入檔案

4. 選擇剛部署的VM，然後按一下Start。

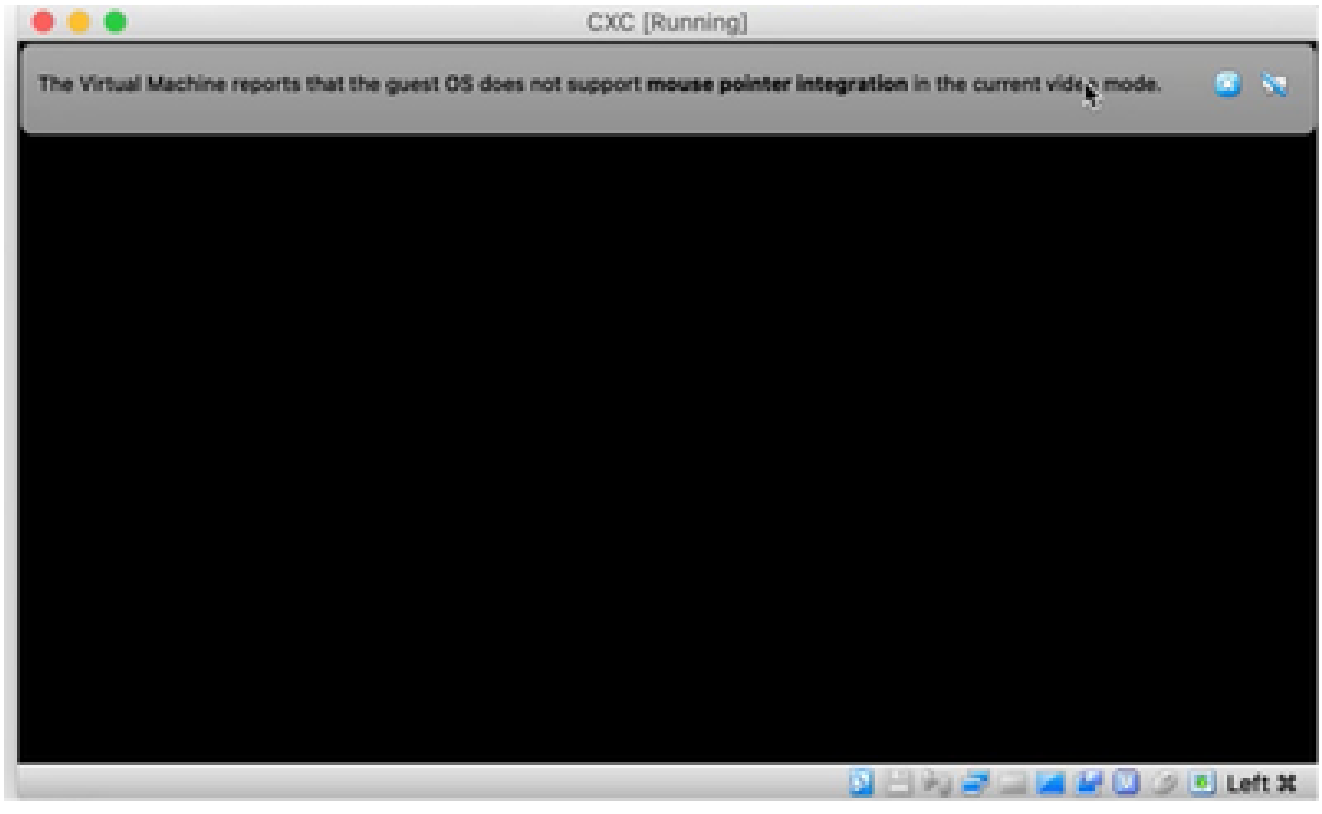


VM 主控台啟動



匯入進行中

5. 開啟VM電源。系統隨即會顯示控制檯。



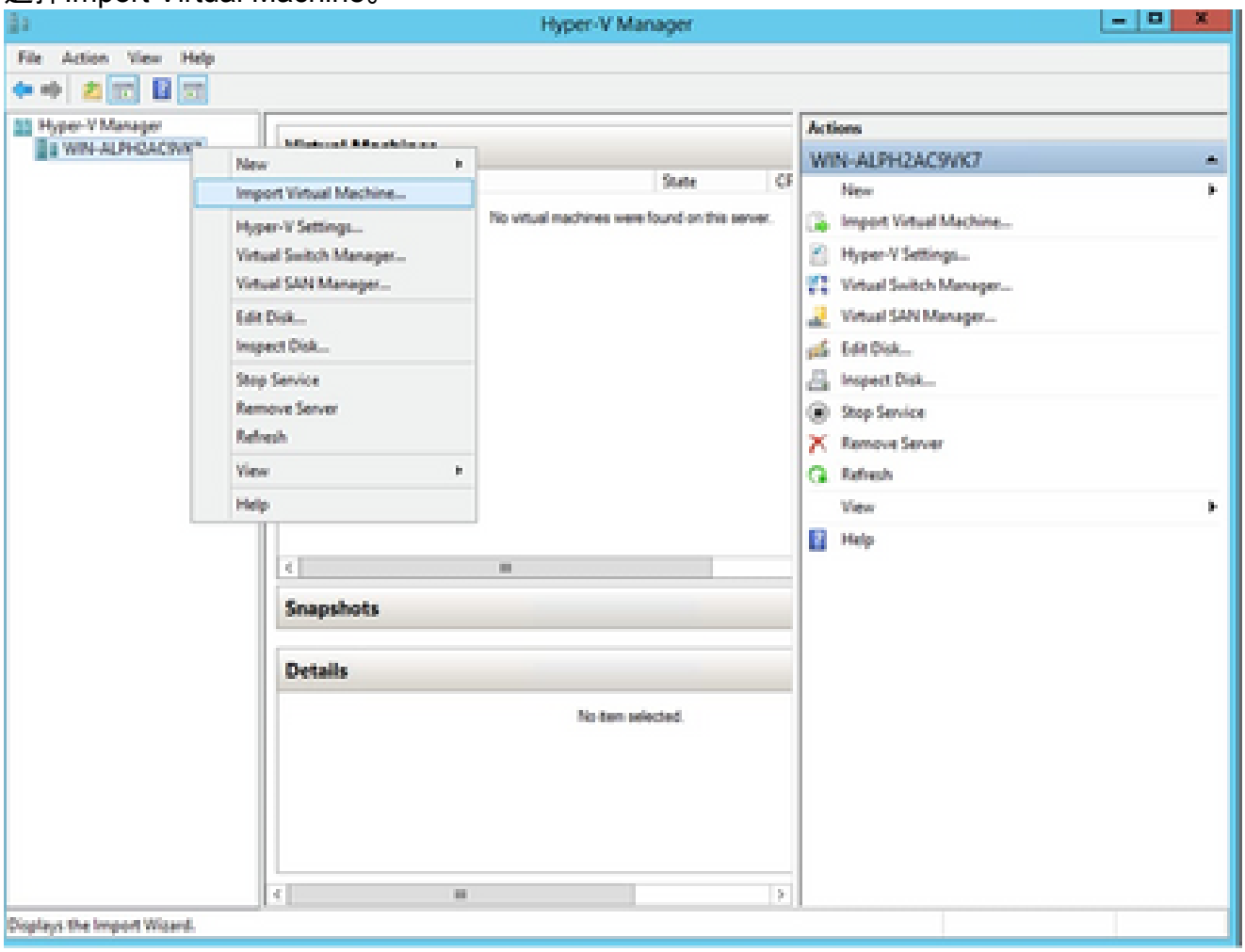
開啟主控台

6. 導覽至Network Configuration，繼續執行以下步驟。

Microsoft Hyper-V 安裝

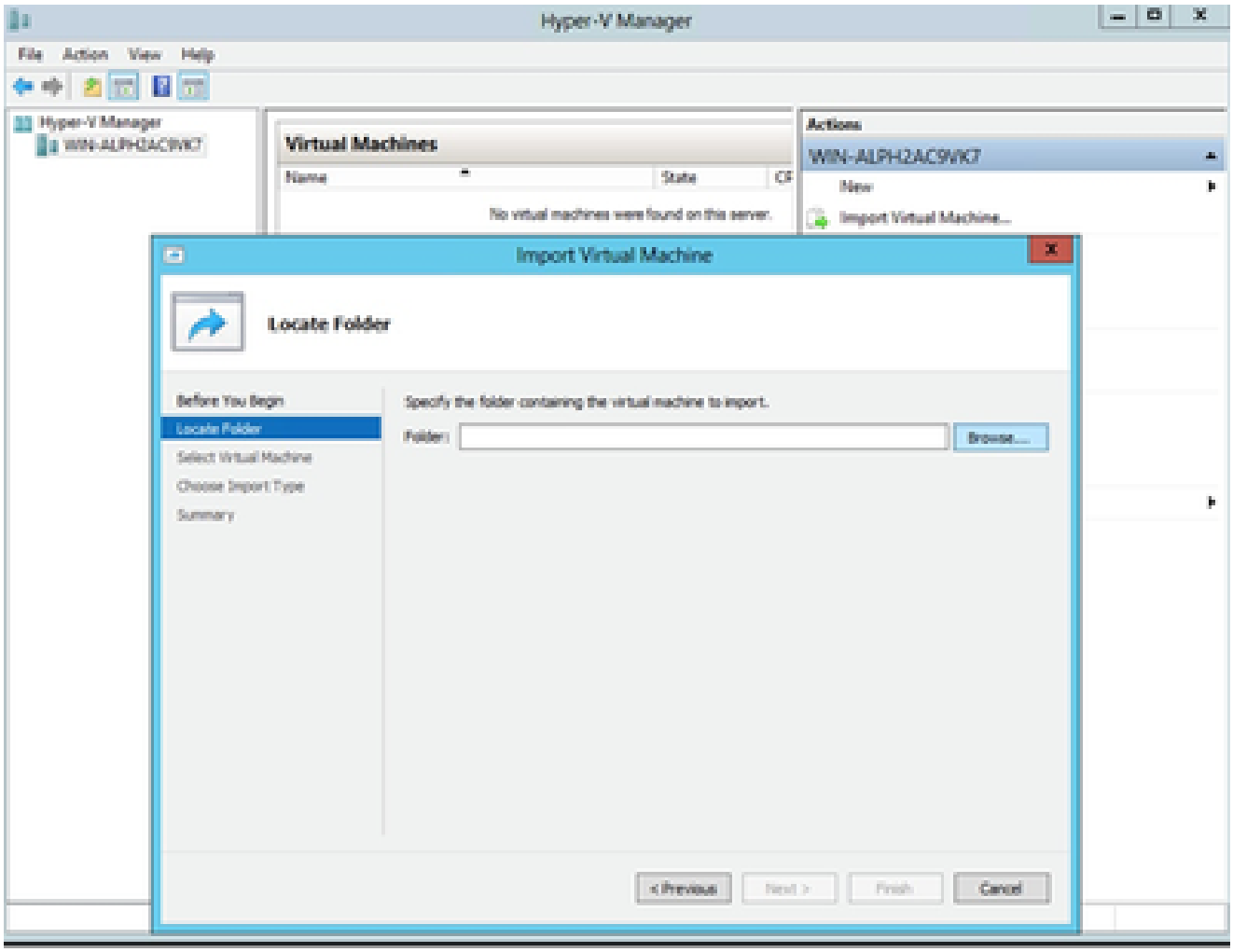
執行下列操作：

1. 選擇Import Virtual Machine。



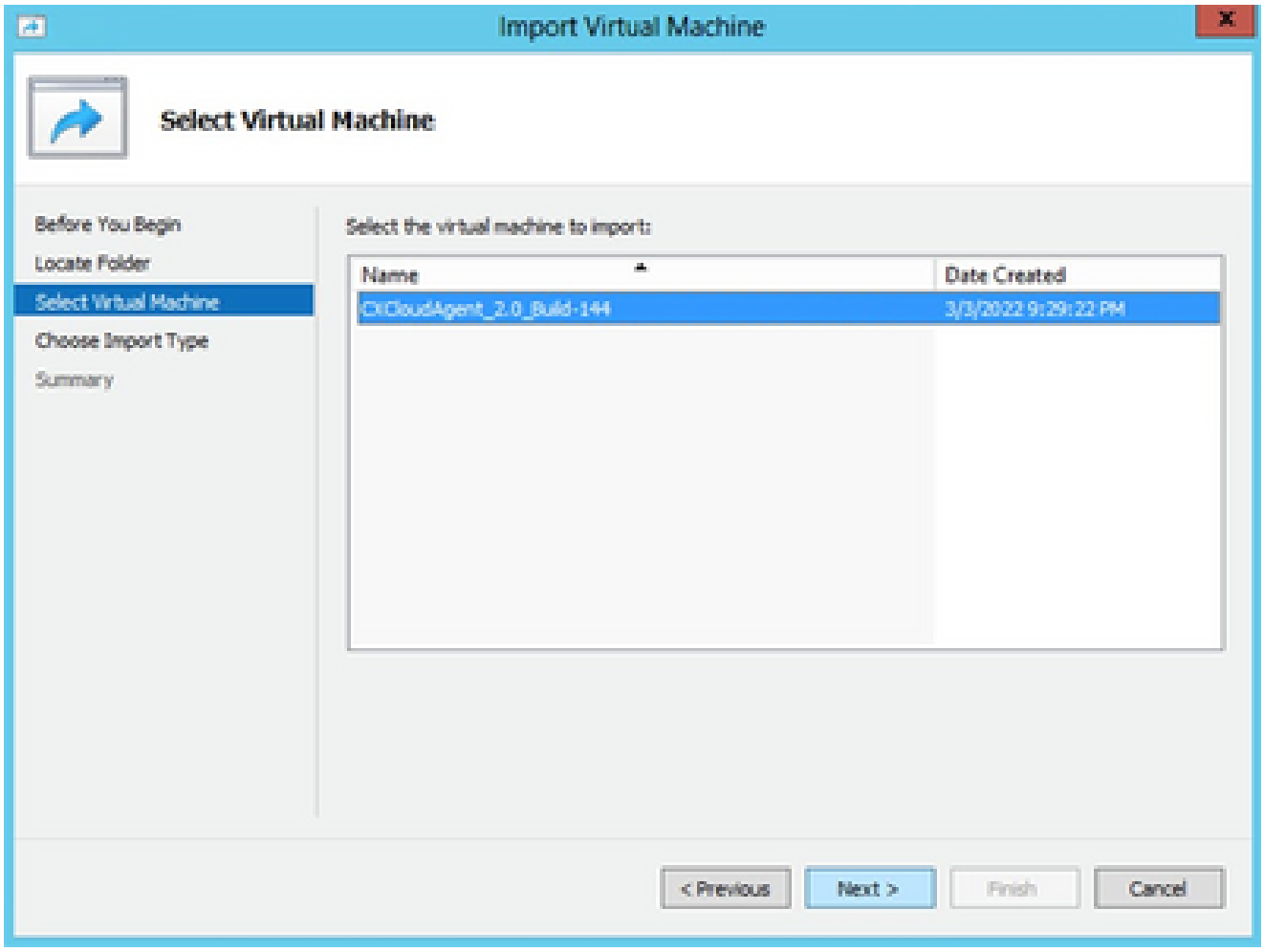
Hyper V管理員

2. 瀏覽並選取下載資料夾。
3. 按「Next」（下一步）。



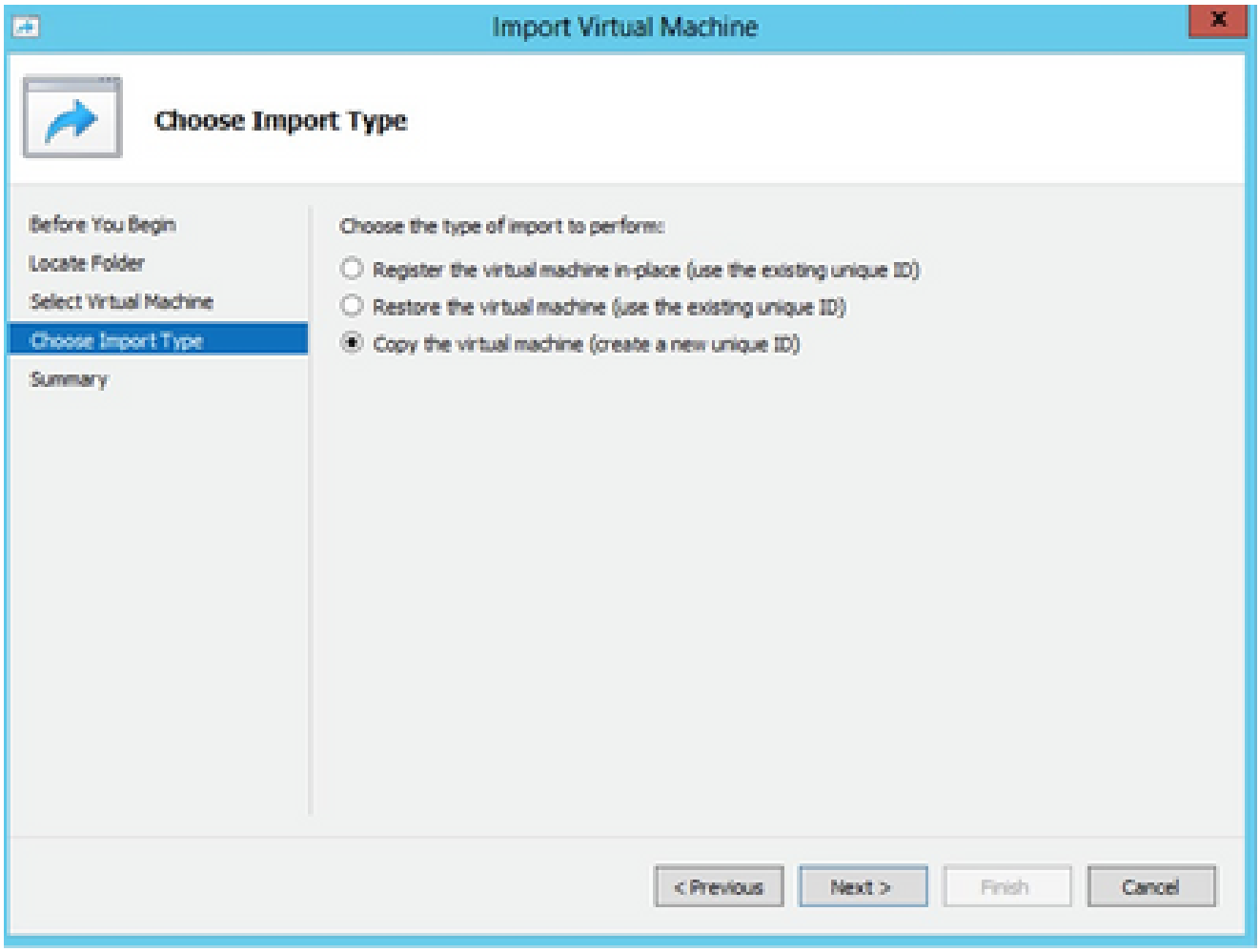
要匯入的資料

4. 選擇VM並按一下下一步。



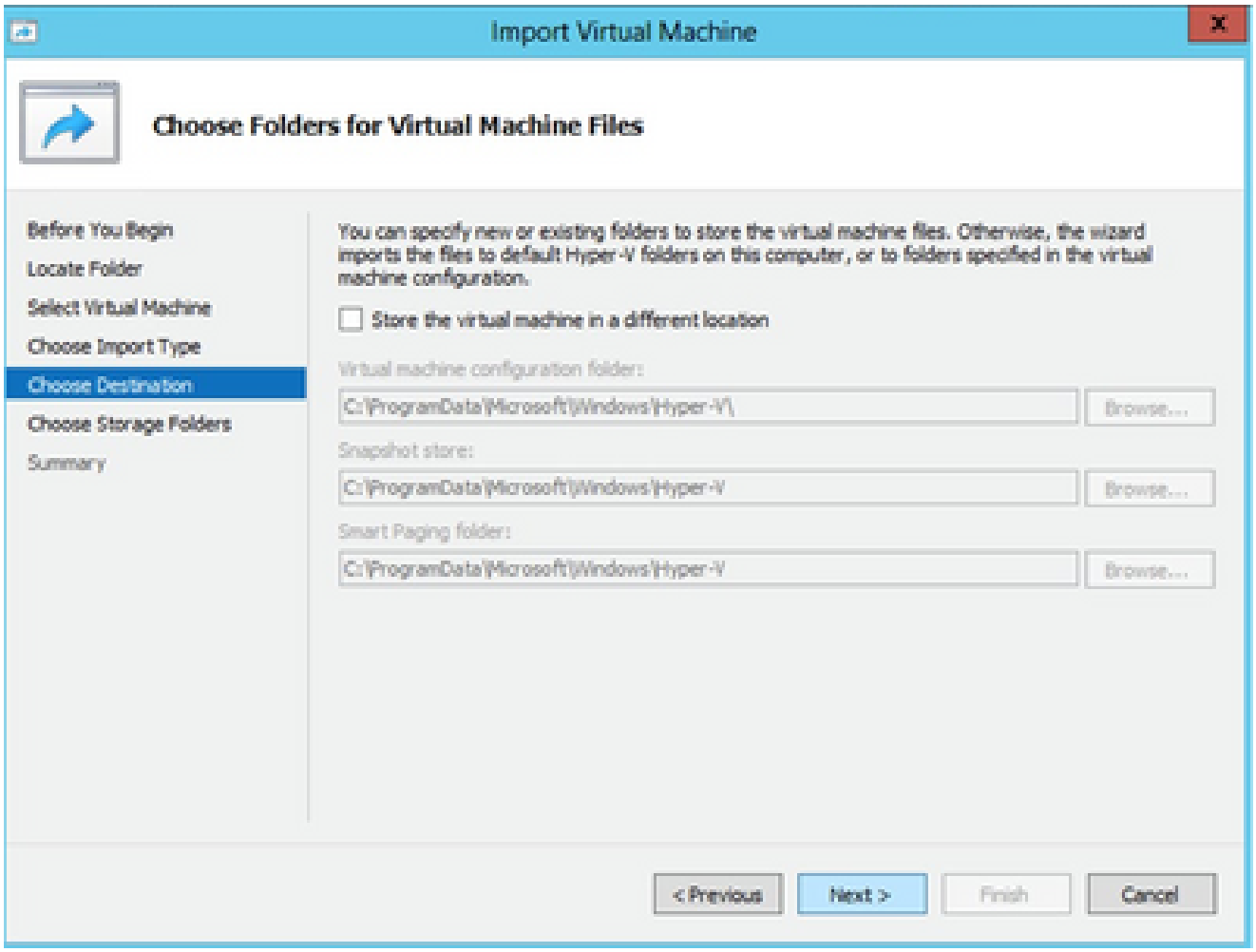
選取 VM

5. 選擇複製虛擬機器（建立新的唯一ID）單選按鈕，然後按一下下一步。



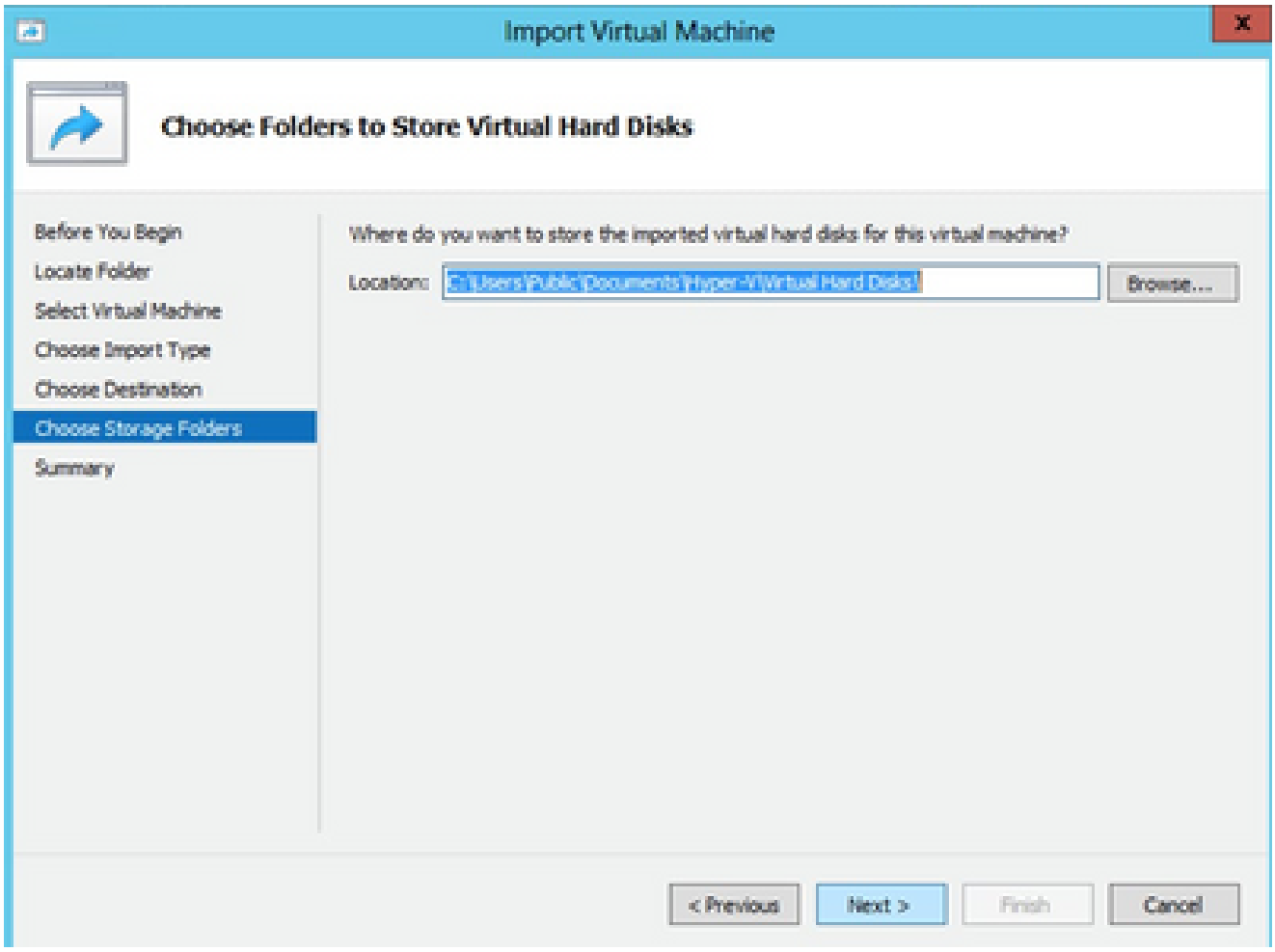
匯入類型

6. 瀏覽以選取 VM 檔案的資料夾。建議使用預設路徑。
7. 按「Next」（下一步）。



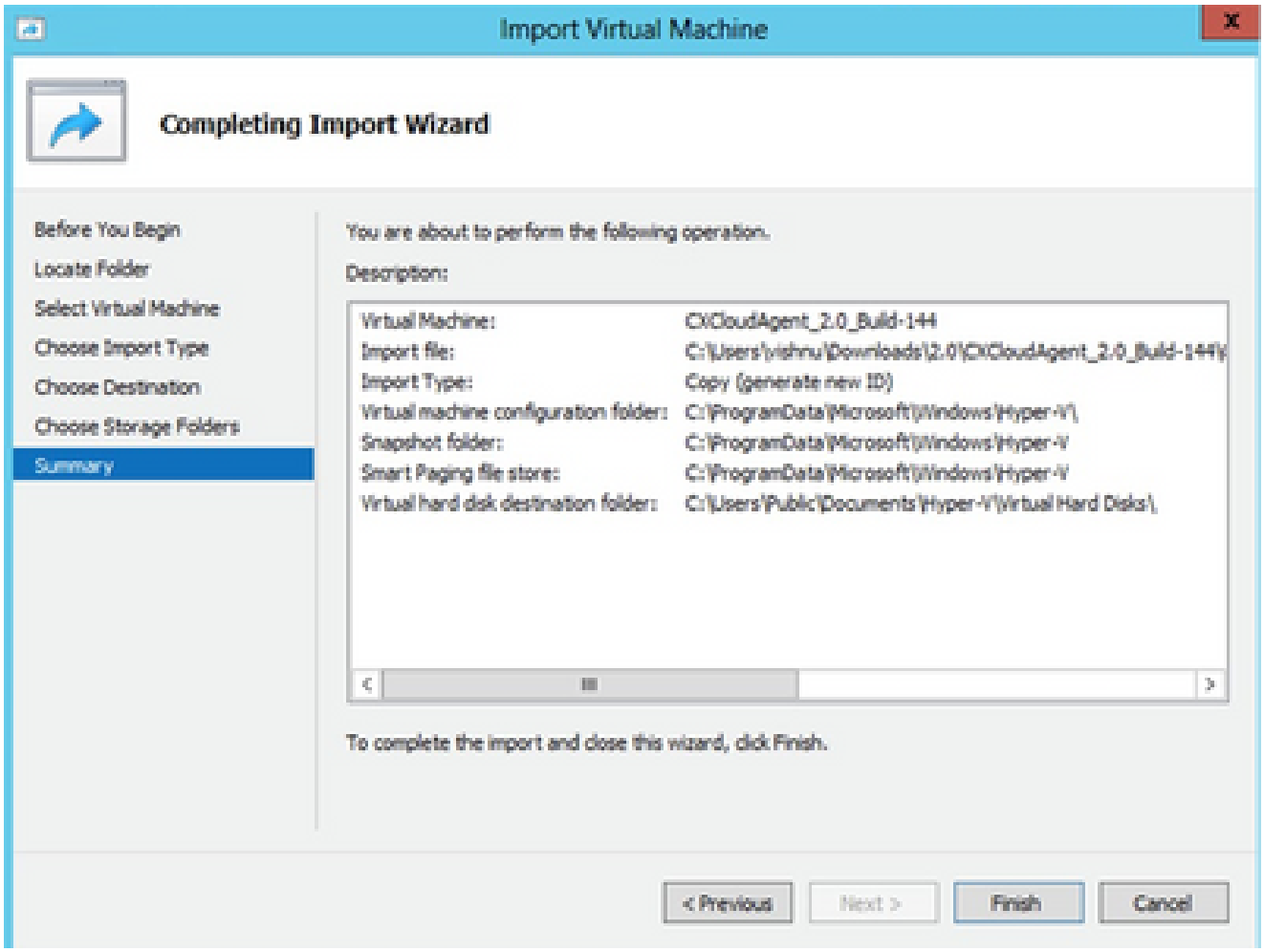
為虛擬機器檔案選擇資料夾

8. 瀏覽並選取要存放 VM 硬碟的資料夾。建議使用預設路徑。
9. 按「Next」（下一步）。



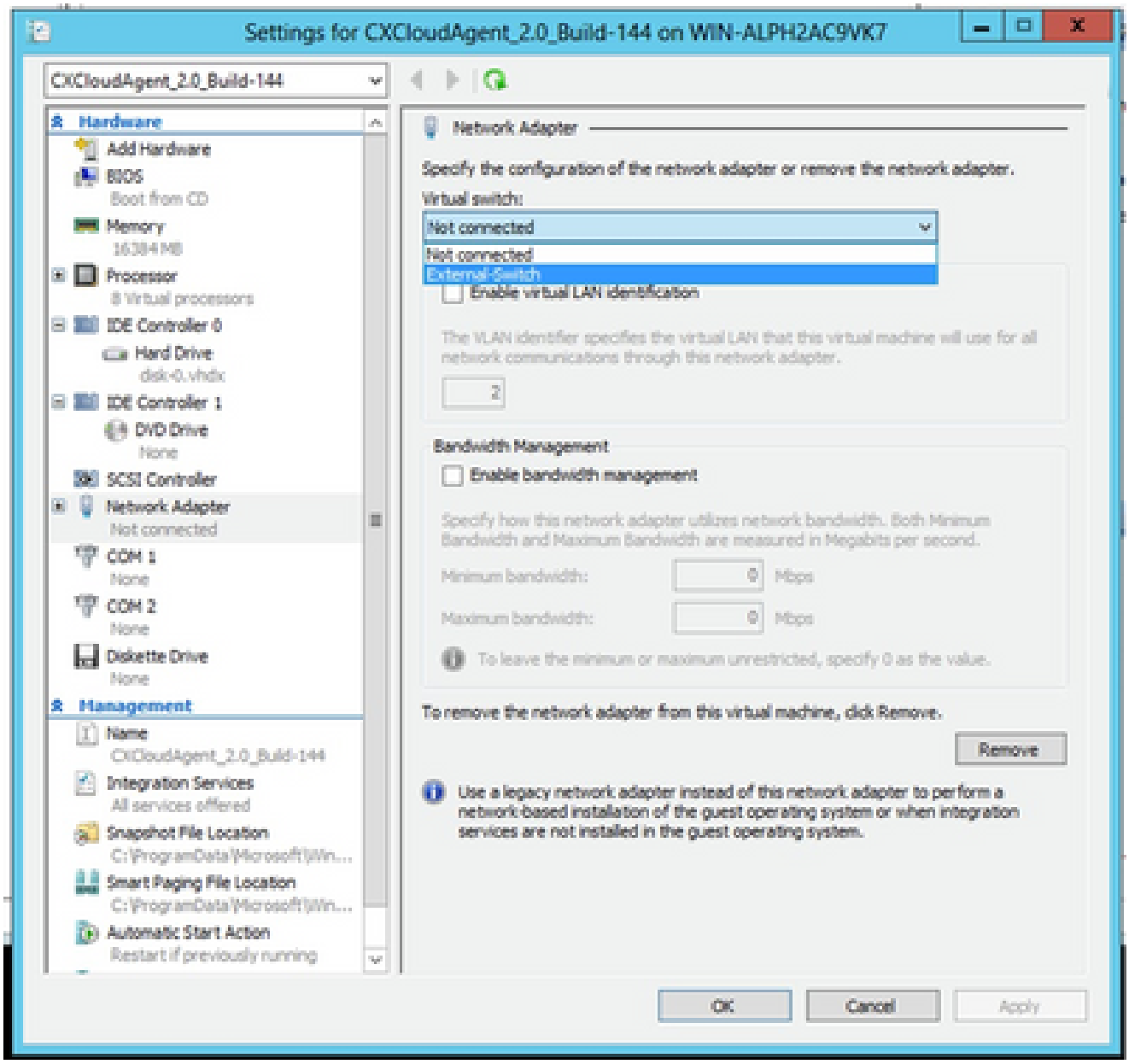
用於儲存虛擬硬碟的資料夾

10. 將顯示VM摘要。驗證所有輸入並按一下Finish。



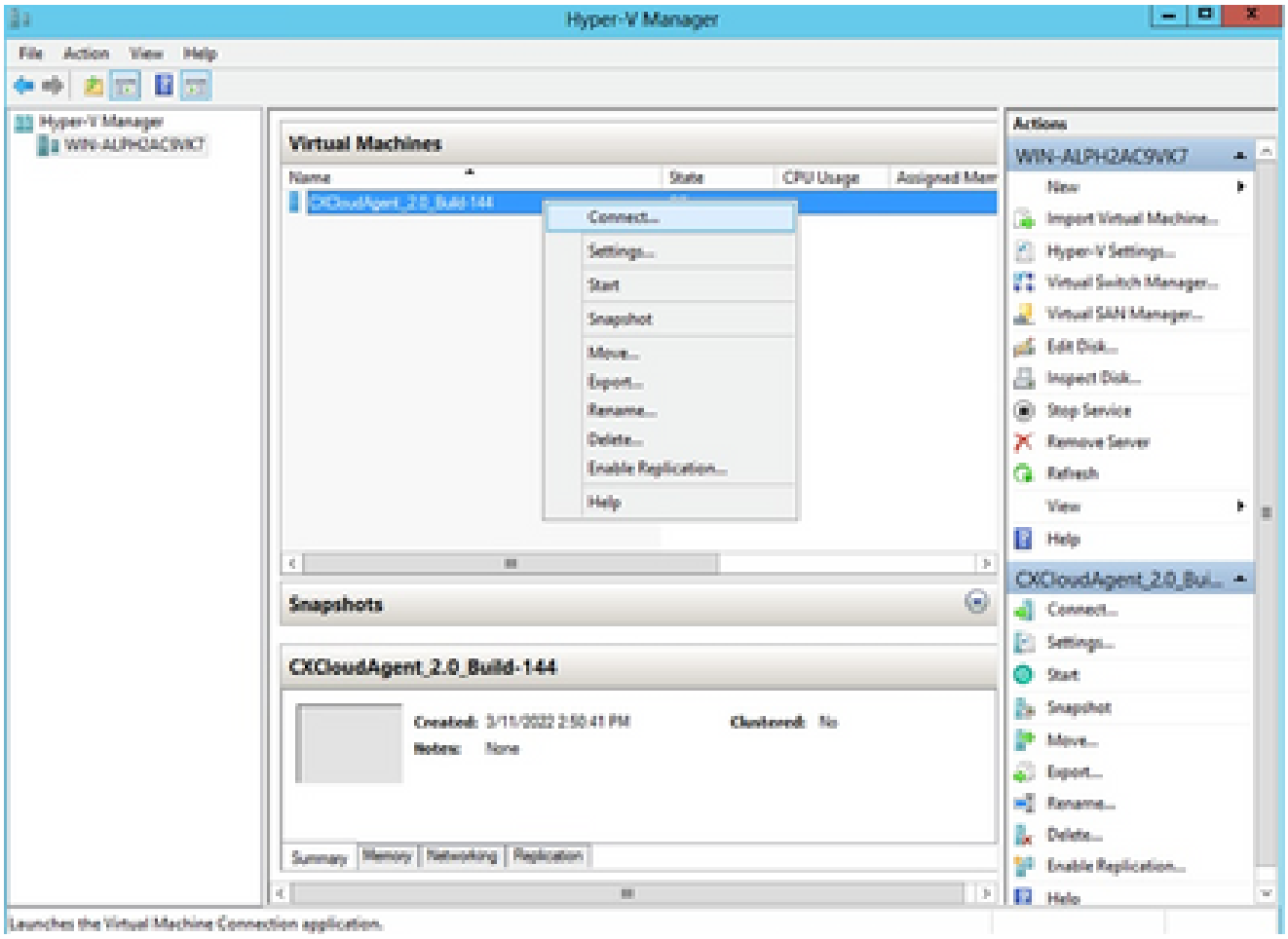
摘要

11. 成功完成匯入後，將在Hyper-V上建立新的VM。開啟VM設定。
12. 在左側窗格中選取網路介面卡，並從下拉式清單選擇可用的虛擬交換器。



虛擬交換器

13. 選擇Connect以啟動VM。

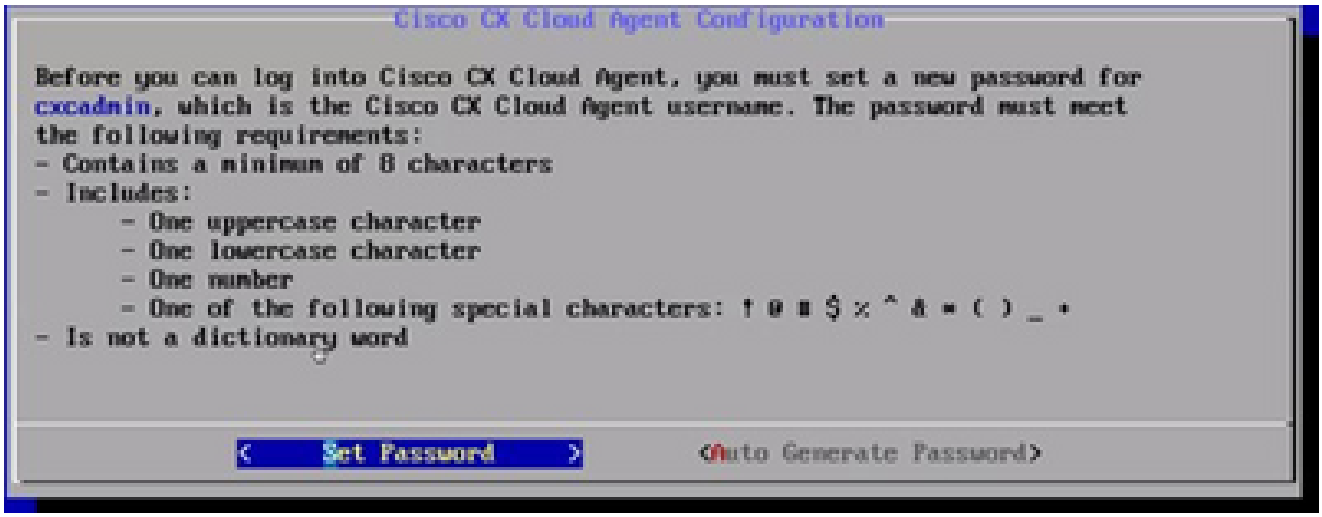


正在啟動 VM

14. 導覽至Network Configuration，繼續執行以下步驟。

網路設定

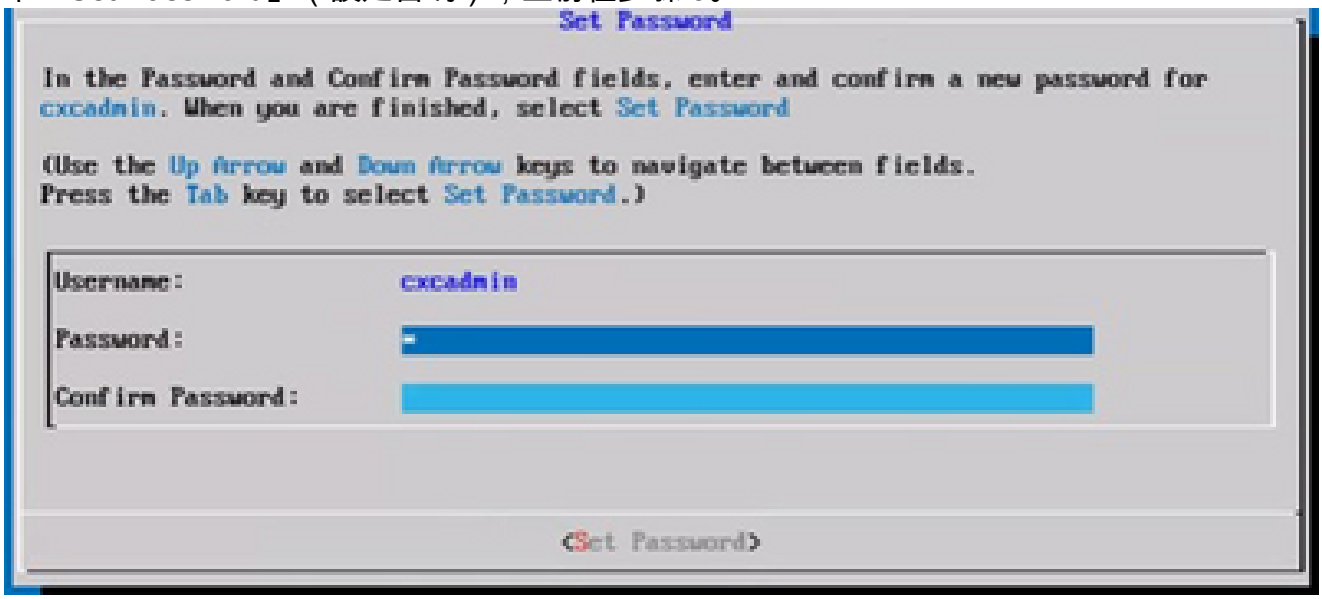
1. 按一下Set Password為cxcadmin新增新密碼，或按一下Auto Generate Password以獲取新密碼。



設定密碼

2. 如果已選取「Set Password」（設定密碼），請輸入 cxcadmin 的密碼，並確認該密碼。按一

下「Set Password」（設定密碼），並前往步驟 3。



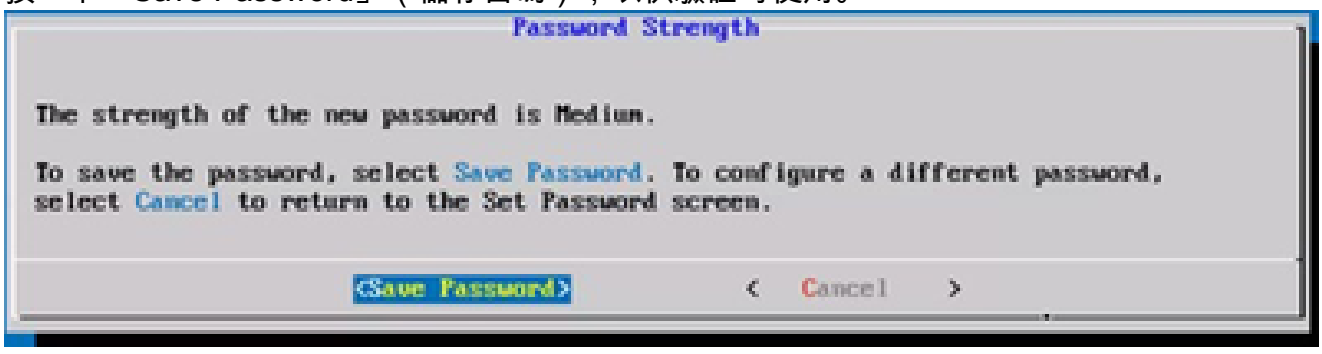
新密碼

或

如果選擇Auto Generate Password，請複製生成的密碼並將其儲存起來供將來使用。按一下「Save Password」（儲存密碼），並前往步驟 4。

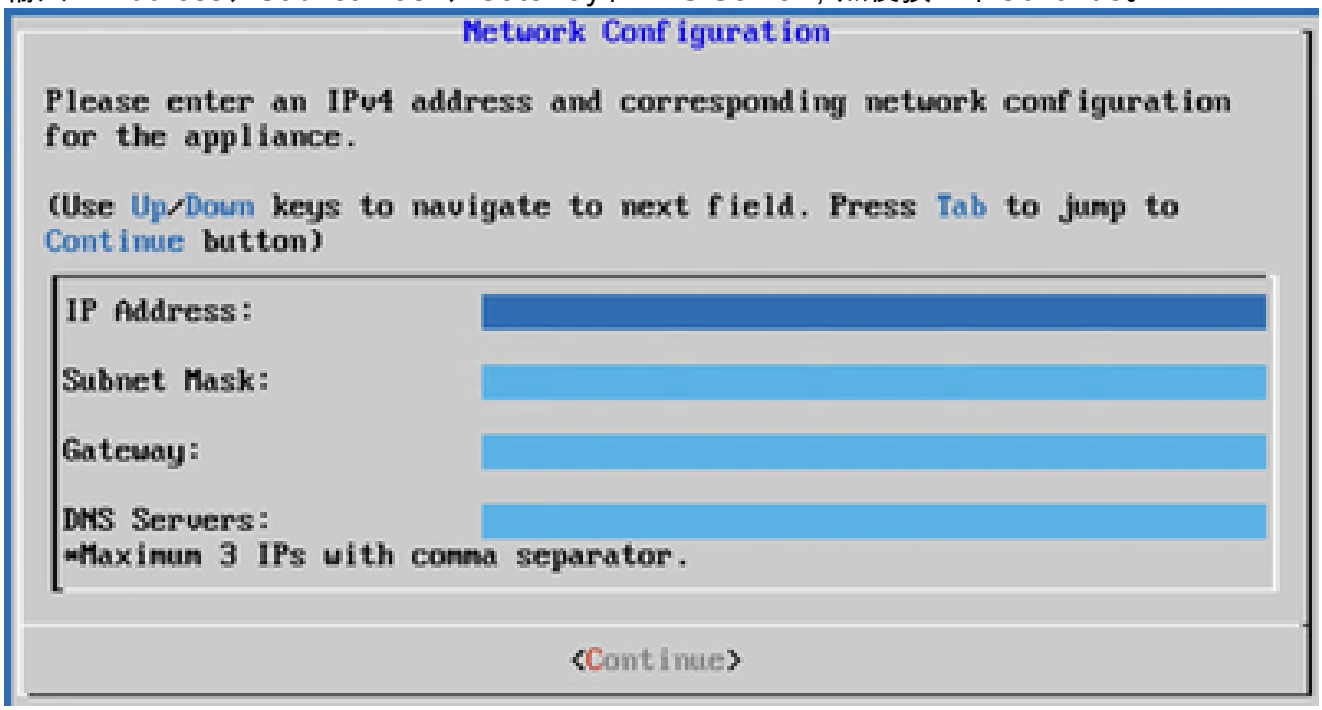
自動產生密碼

3. 按一下「Save Password」（儲存密碼），以供驗證時使用。



儲存密碼

4. 輸入IP Address、Subnet Mask、Gateway和DNS Server，然後按一下Continue。

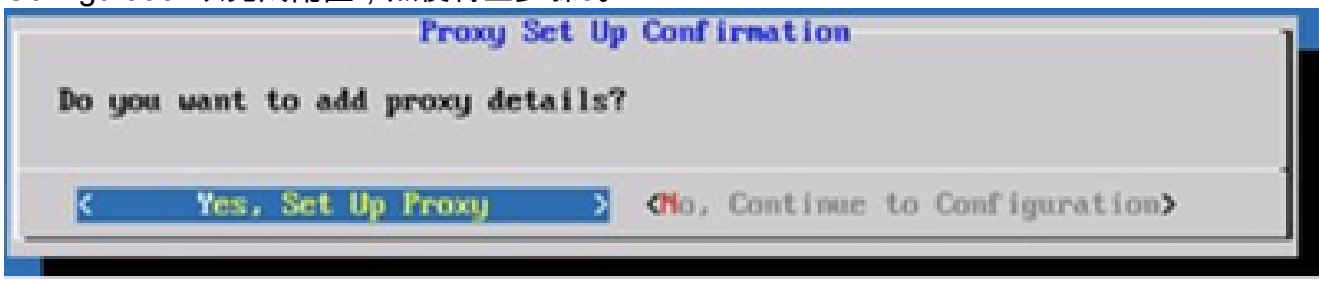


網路設定

5. 確認項目，並按一下「Yes, Continue」（是，繼續）。

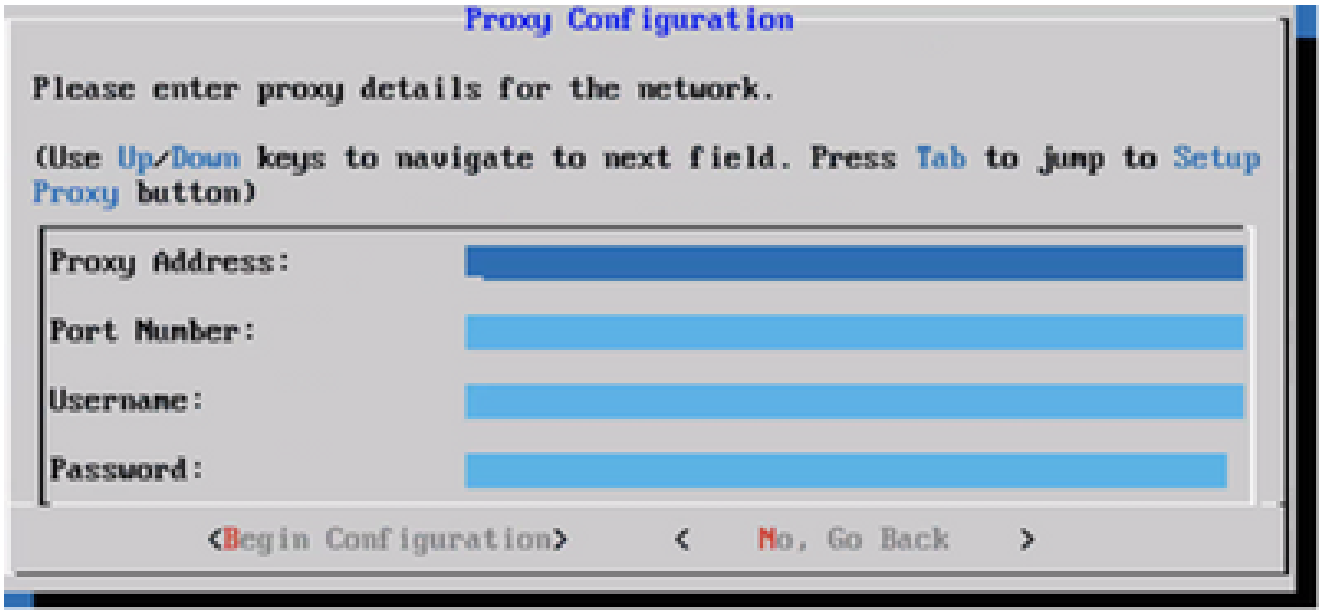
組態

6. 要設定代理詳細資訊，請按一下Yes， Set Up Proxy，或按一下No， Continue to Configuration以完成配置，然後轉至步驟8。



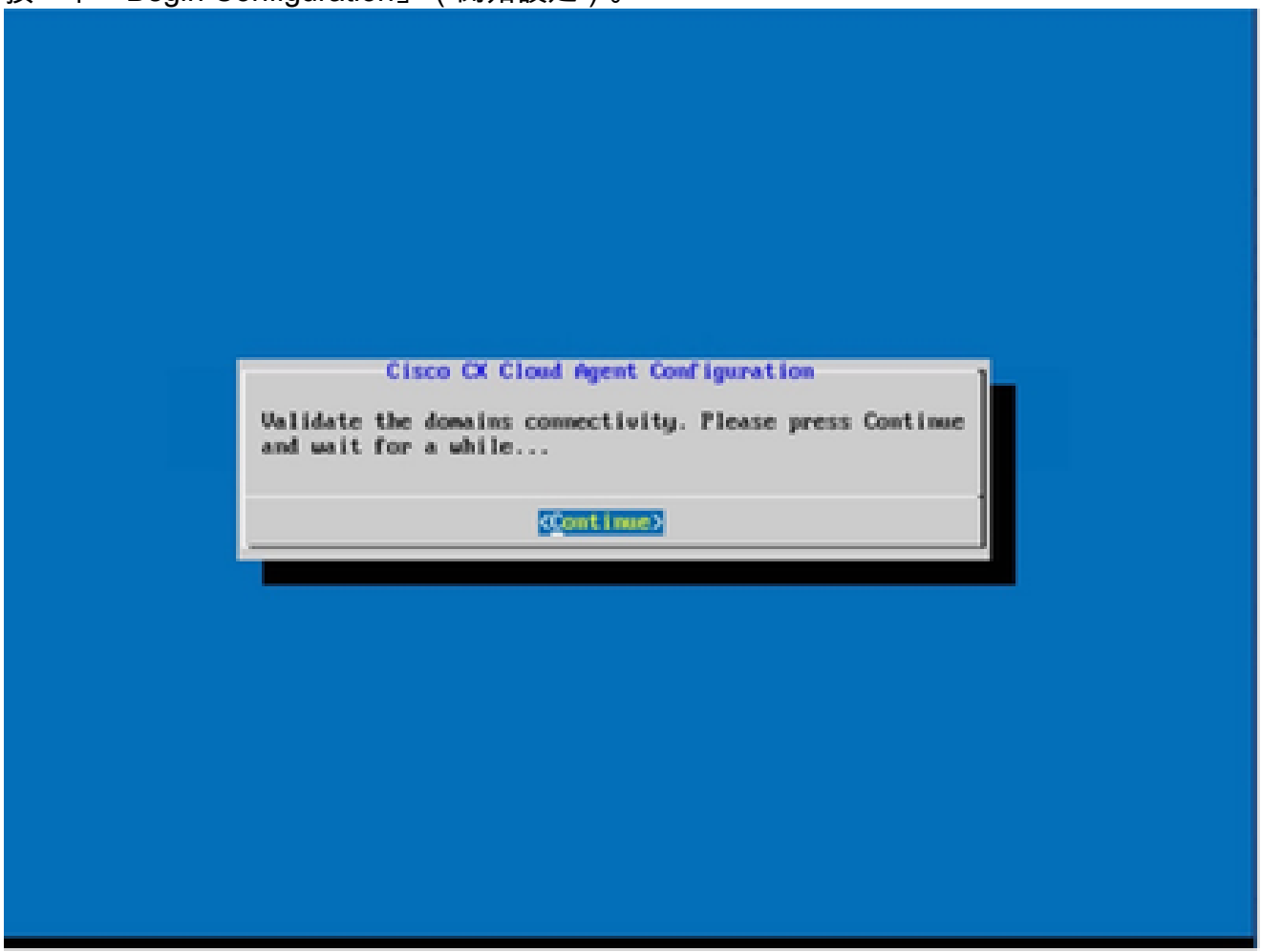
Proxy

7. 輸入 Proxy 位址、連接埠號碼、使用者名稱和密碼。



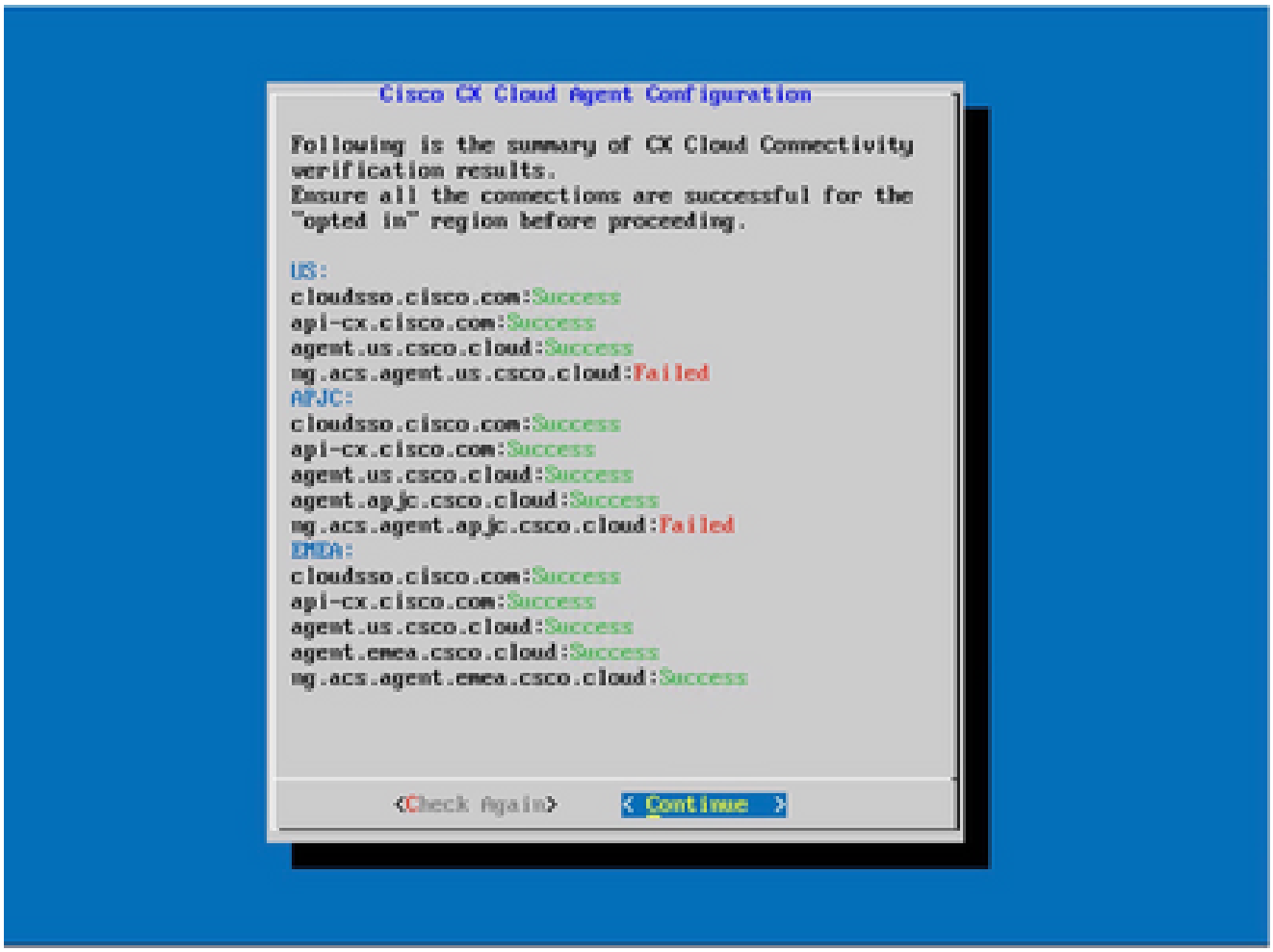
Proxy 組態

8. 按一下「Begin Configuration」（開始設定）。



開始配置

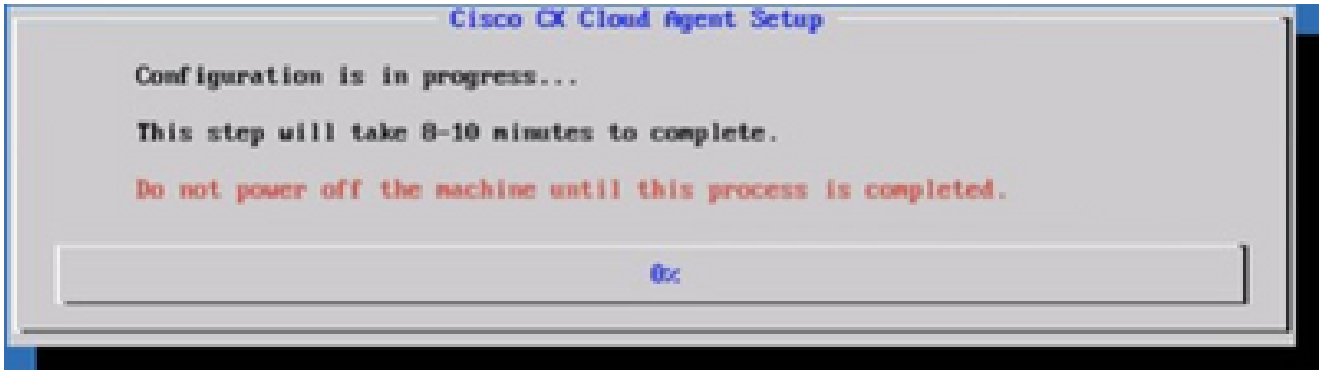
9. 按一下「Continue」（繼續）。



繼續配置

10. 按一下Continue繼續配置以成功到達域。完成配置可能需要幾分鐘。

> 注意：如果無法成功訪問域，則客戶必須通過更改其防火牆來修復域可訪問性，以確保域可訪問。解決域可訪問性問題後，按一下Check Again。

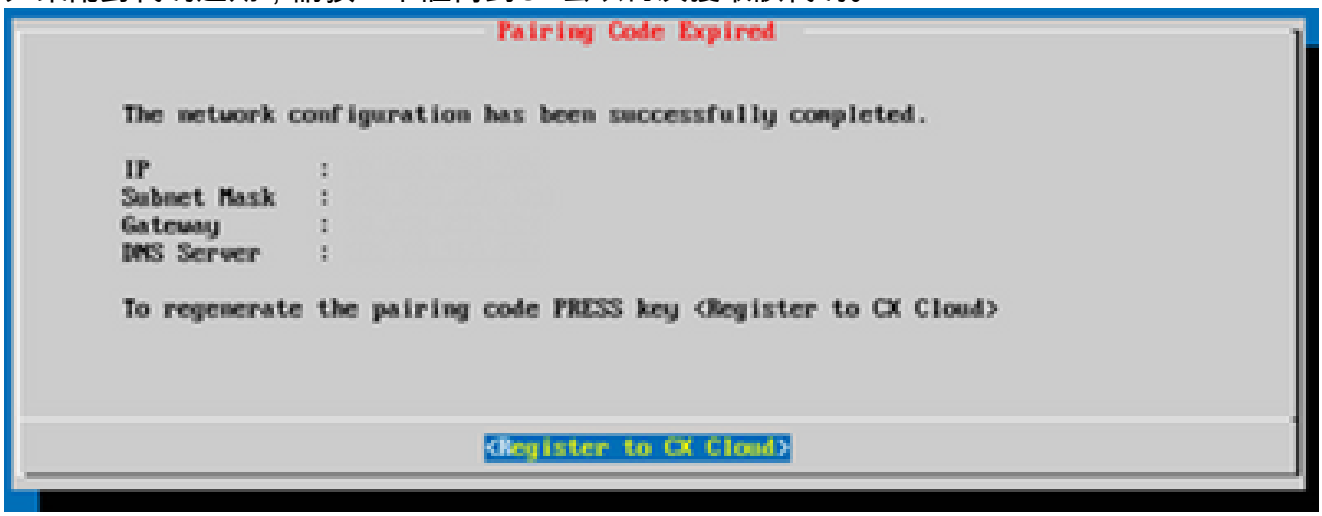


設定進行中

11. 複製配對程式碼，並返回 CX Cloud 繼續設定。

配對程式碼

12. 如果配對代碼過期，請按一下註冊到CX雲以再次獲取該代碼。



程式碼已到期

13. 按一下「OK」（確定）。

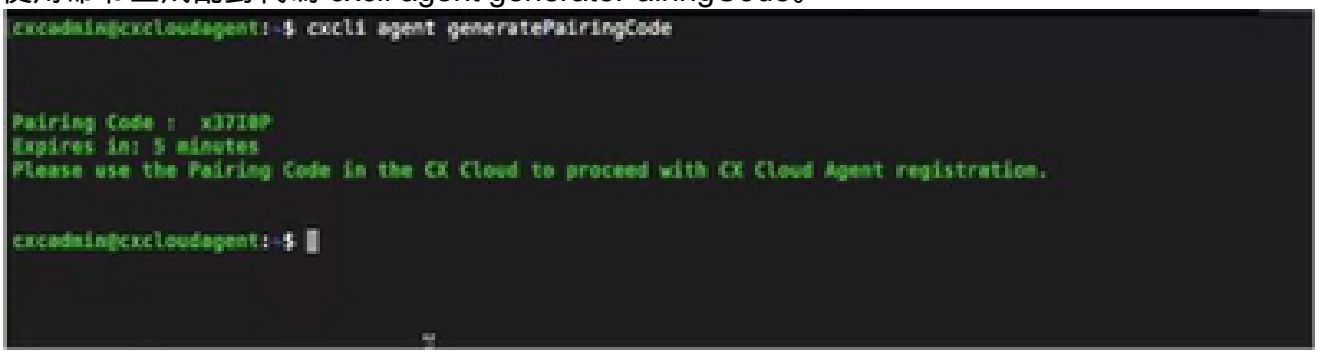
註冊成功

使用CLI生成配對代碼的備用方法

使用者還可以使用CLI選項生成配對代碼。

使用CLI生成配對代碼：

1. 使用cxcadmin使用者憑據通過SSH登入雲代理。
2. 使用命令生成配對代碼 cxcli agent generatePairingCode。



產生配對程式碼 CLI

3. 複製配對程式碼，並返回 CX Cloud 繼續設定。

配置Cisco DNA Center以將系統日誌轉發到CX雲代理

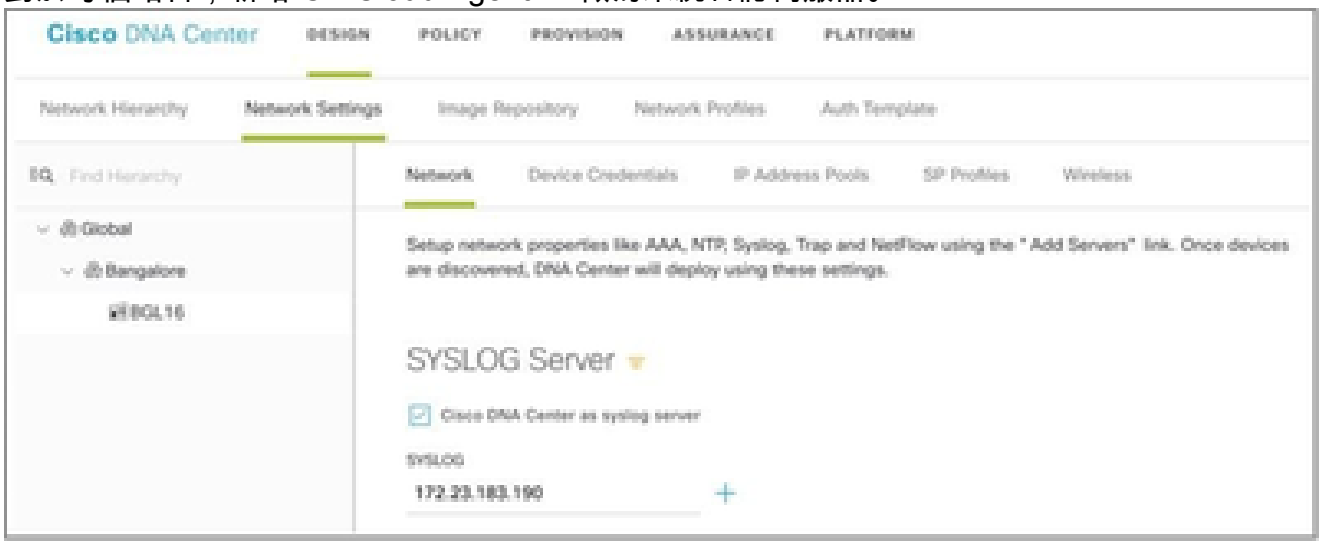
必要條件

支援的Cisco DNA Center版本為2.1.2.0到2.2.3.5、2.3.3.4到2.3.3.6、2.3.5.0和Cisco DNA Center Virtual Appliance

配置系統日誌轉發設定

要在Cisco DNA Center中配置Syslog Forwarding to CX Cloud Agent，請執行以下步驟：

1. 啟動 Cisco DNA 中心。
2. 前往「Design」（設計）>「Network Settings」（網路設定）>「Network」（網路）。
3. 對於每個站台，新增 CX Cloud Agent IP 做為系統日誌伺服器。



系統日誌伺服器

附註：
配置完成後，與該站點關聯的所有裝置都將配置為向CX雲代理傳送級別為「關鍵」的系統日

誌。裝置必須關聯到站點，才能啟用從裝置到CX雲代理的系統日誌轉發。
更新系統日誌伺服器設定時，與該站點關聯的所有裝置都會自動設定為預設關鍵級別。

配置其他資產以將系統日誌轉發到CX雲代理

必須將裝置配置為向CX雲代理傳送系統日誌消息，才能使用CX雲的故障管理功能。

注意：只有園區成功跟蹤第2級裝置才有資格配置其他資產以轉發系統日誌。

具有轉發功能的現有系統日誌伺服器

執行syslog伺服器軟體的配置說明，並將CX雲代理IP地址新增為新目標。

注意：轉發系統日誌時，請確保保留原始系統日誌消息的源IP地址。

沒有轉發功能的現有系統日誌伺服器或沒有系統日誌伺服器

將每台裝置配置為將系統日誌直接傳送到CX雲代理IP地址。有關特定配置步驟，請參閱以下文檔。

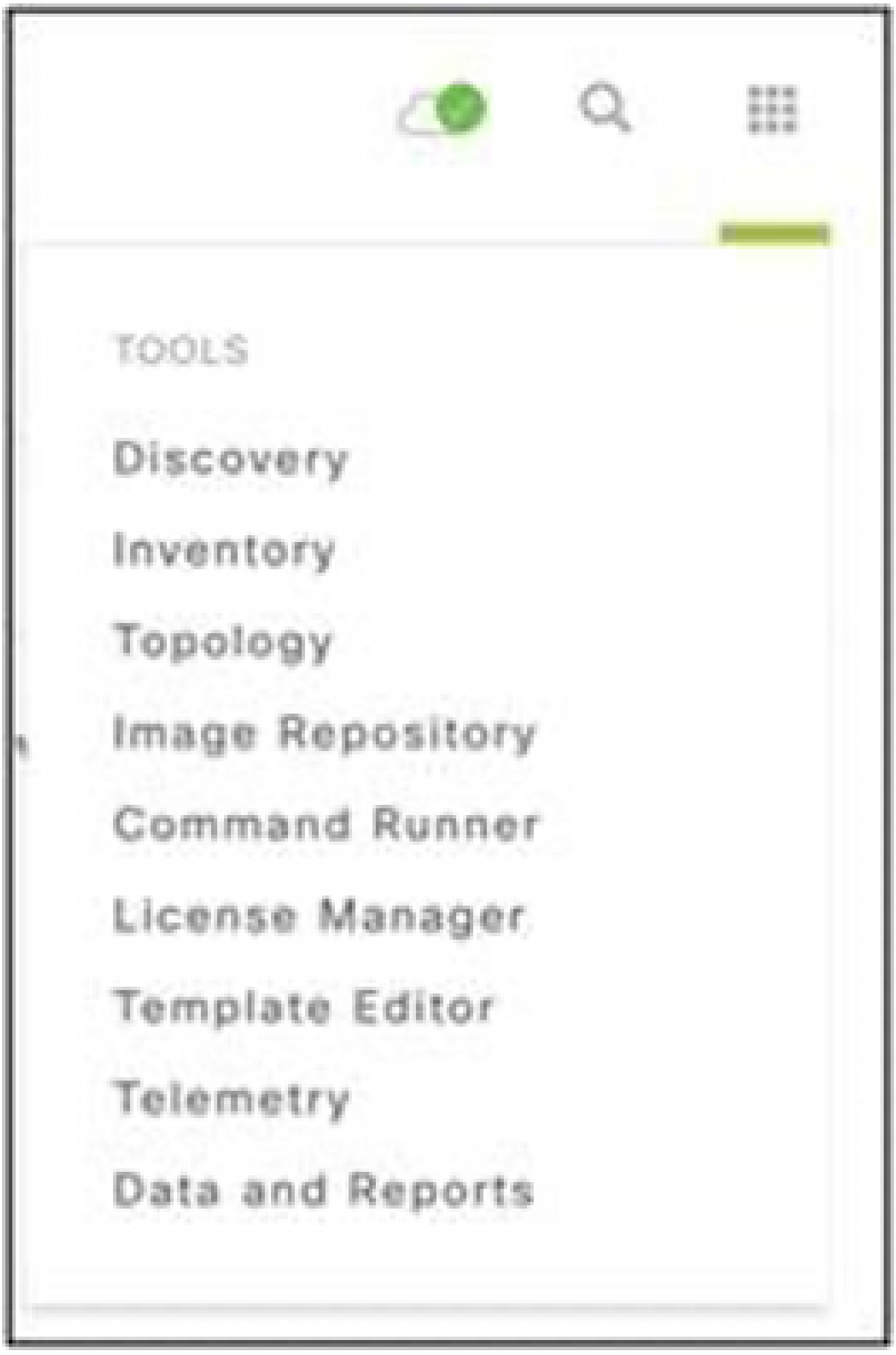
IOS-XE配置指南

AireOS無線控制器配置指南

啟用資訊級別系統日誌設定

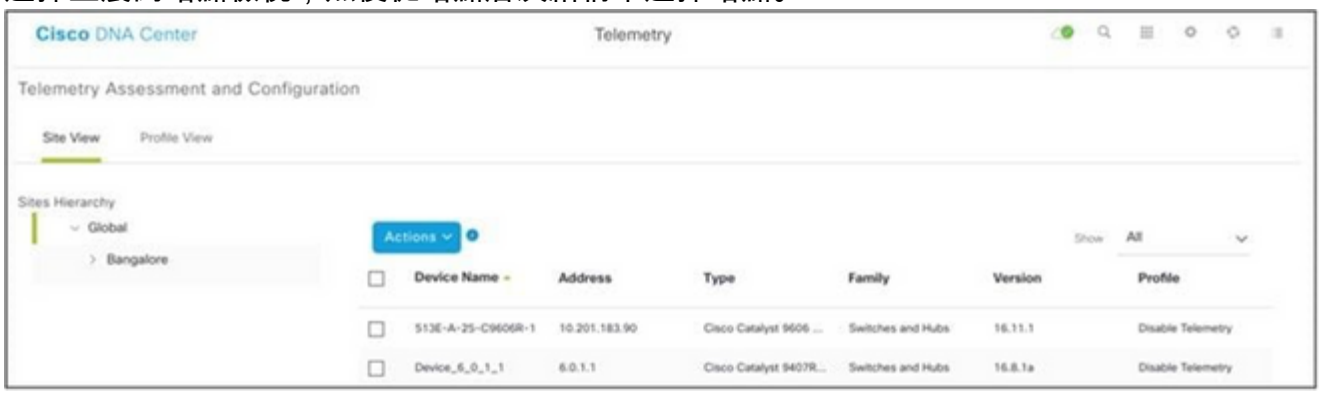
要使系統日誌資訊級別可見，請執行以下步驟：

1. 導覽至Tools>Telemetry。


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

工具選單

2. 選擇並展開站點檢視，然後從站點層次結構中選擇站點。



站台檢視

3. 選擇所需站點，並選中Device name(裝置名稱)覈取方塊的所有裝置。

4. 從Actions下拉選單中選擇Optimal Visibility。

動作

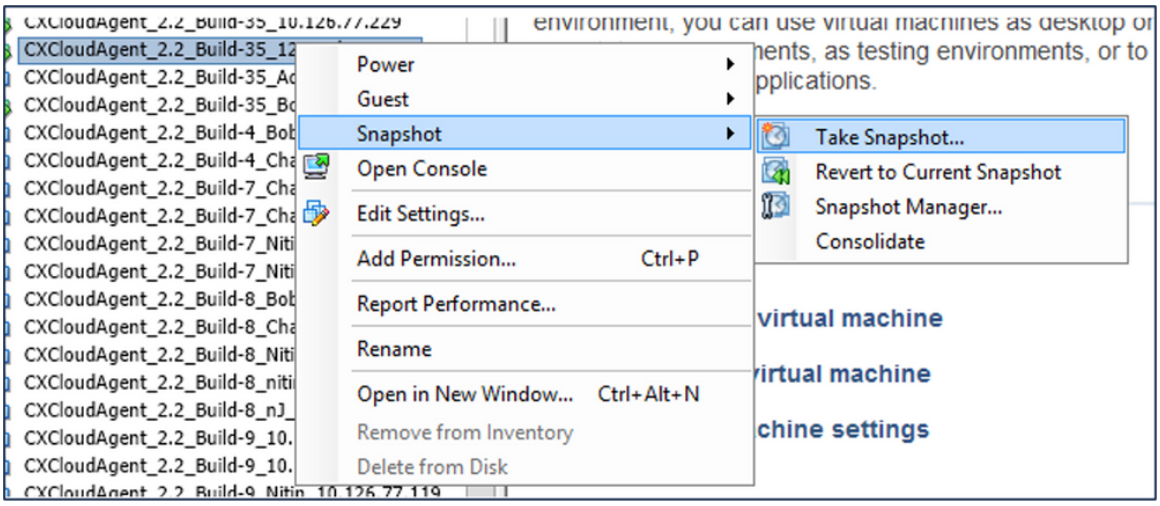
備份和恢復CX雲虛擬機器

建議使用快照功能在特定時間點保留CX雲代理虛擬機器的狀態和資料。此功能可推動CX雲虛擬機器恢復到拍攝快照的特定時間。

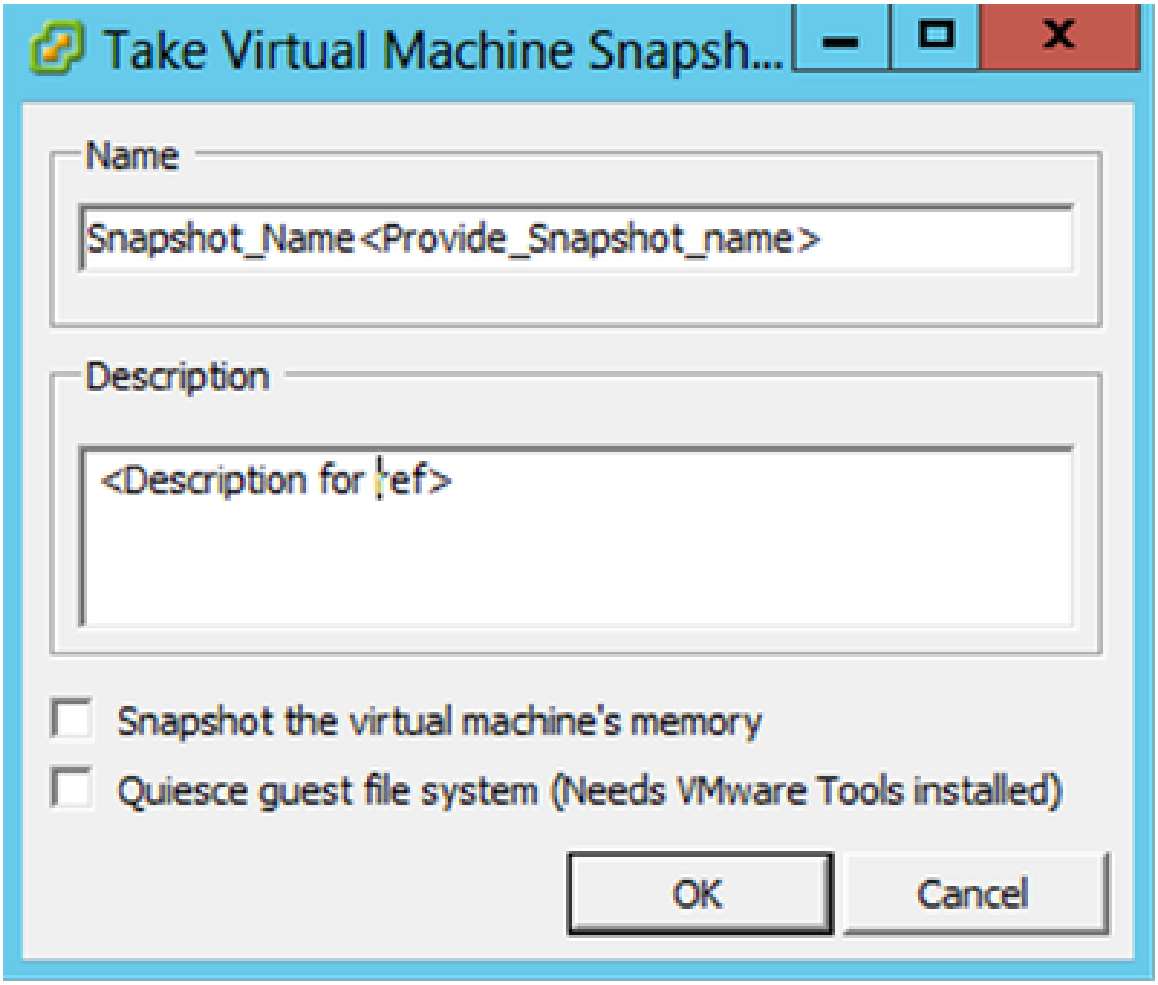
備份

要備份CX雲虛擬機器：

1. 按一下右鍵VM，然後選擇Snapshot > Take Snapshot。將開啟Take Virtual Machine Snapshot視窗。



選取 VM

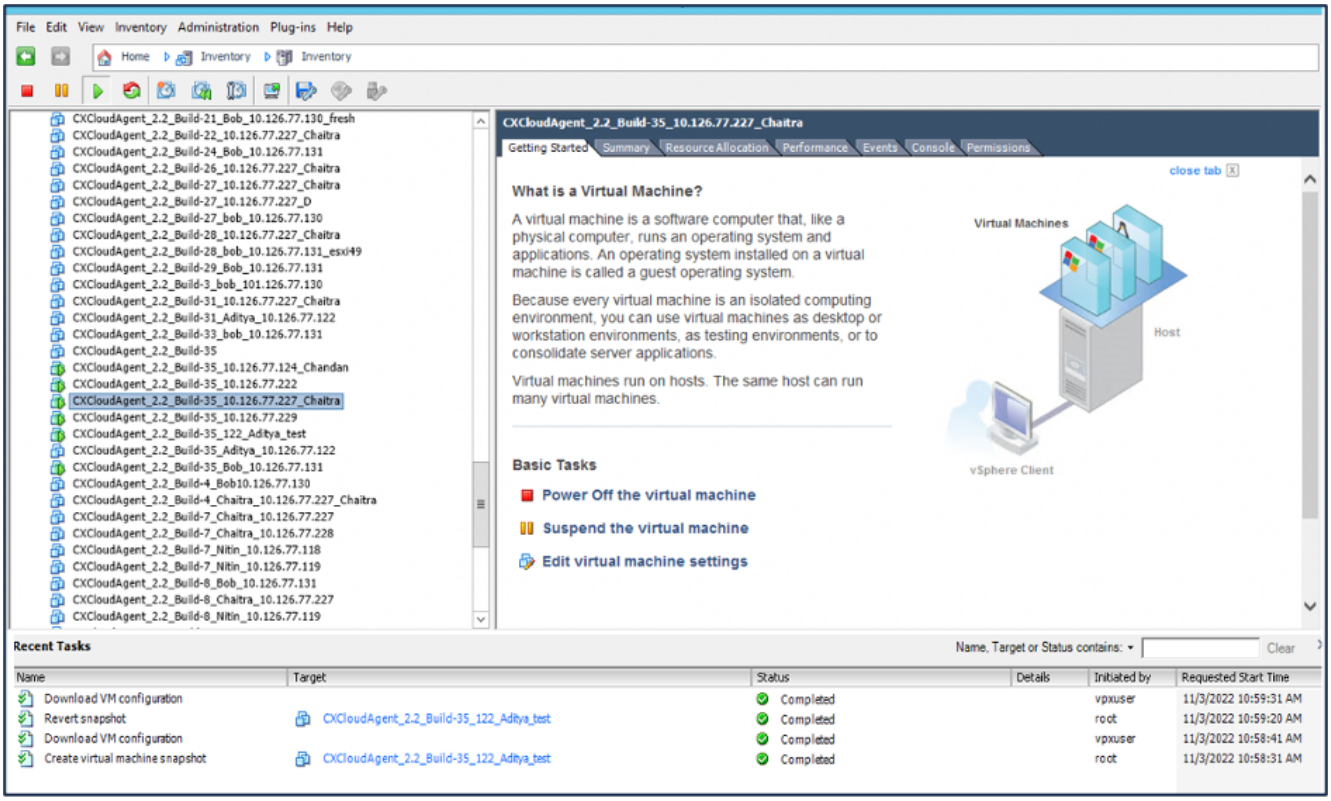


生成虛擬機器快照

2. 輸入名稱和說明。

註：驗證是否已清除「Snapshot the virtual machine's memory（虛擬機器記憶體的快照）」覈取方塊。

3.按一下確定。建立虛擬機器快照狀態在「最近的任務」清單中顯示為已完成。

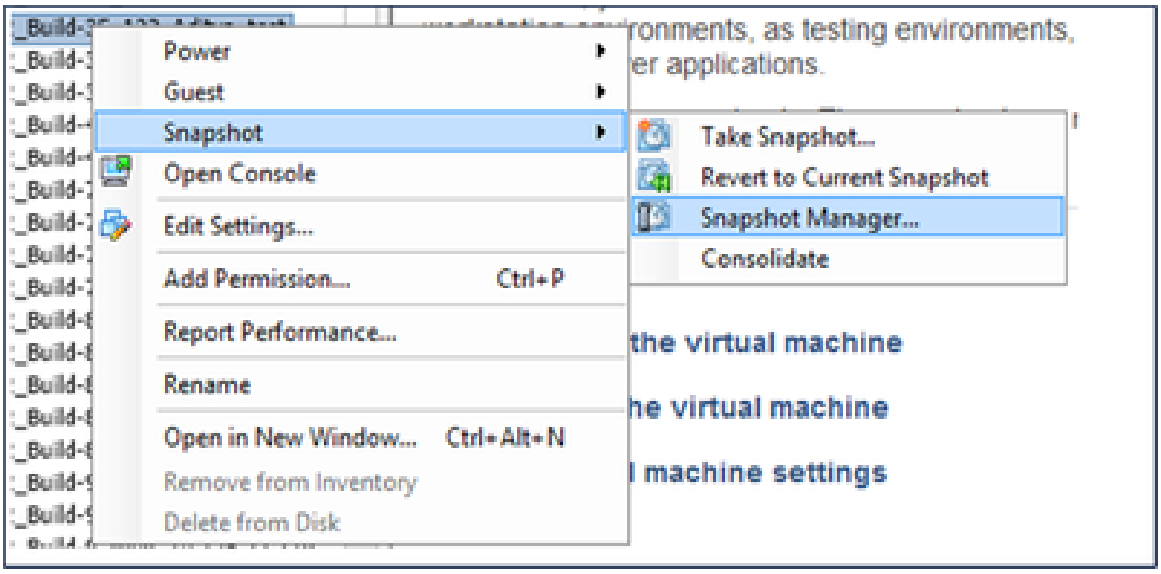


最近的任務

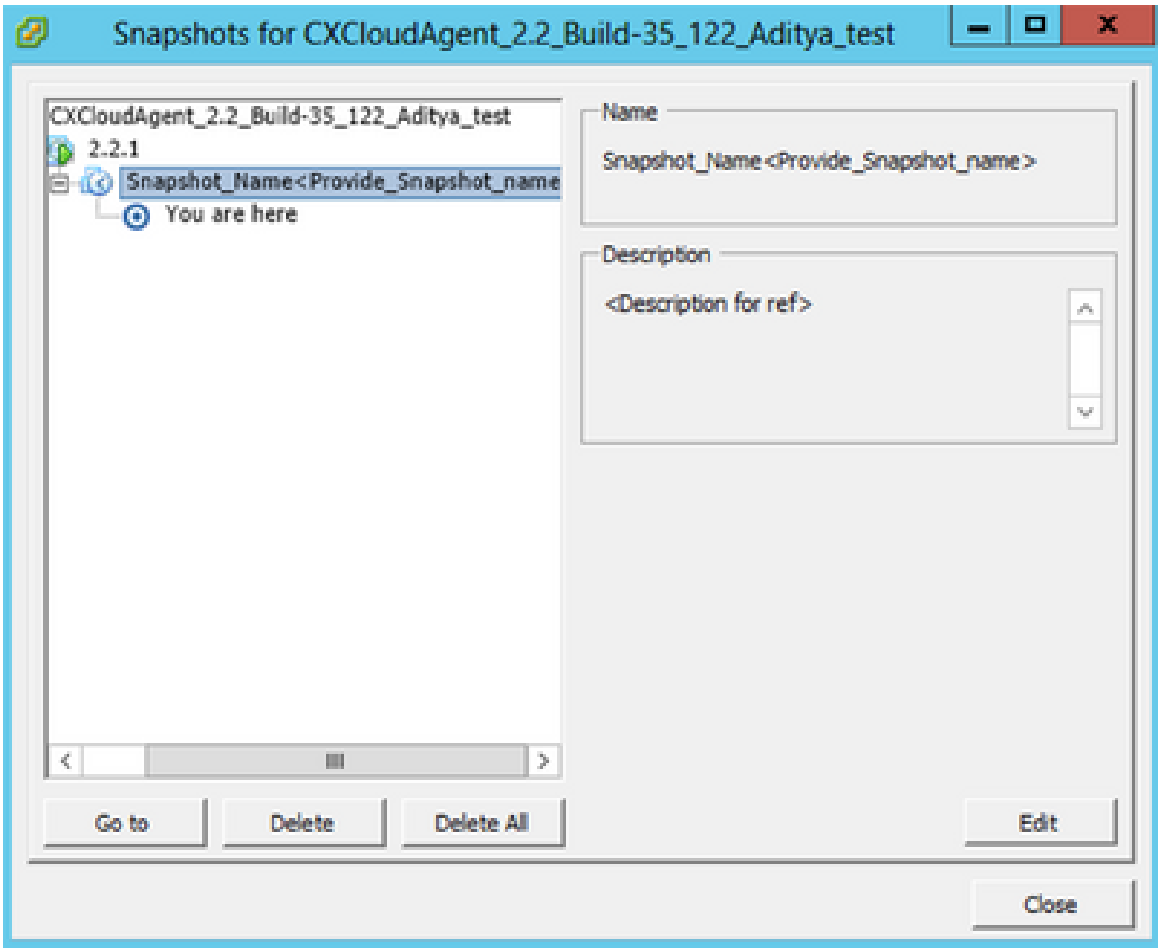
還原

要恢復CX雲虛擬機器：

1. 按一下右鍵VM，然後選擇Snapshot > Snapshot Manager。將打開VM的快照視窗。

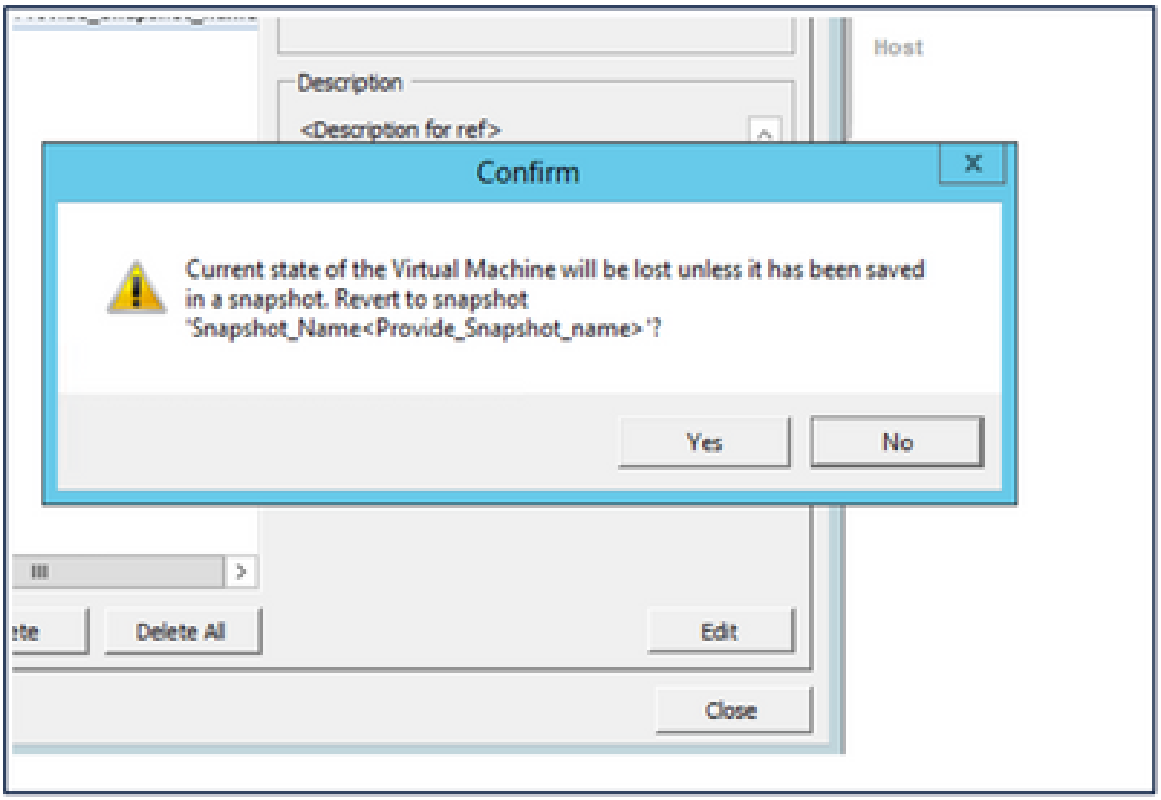


選擇VM視窗



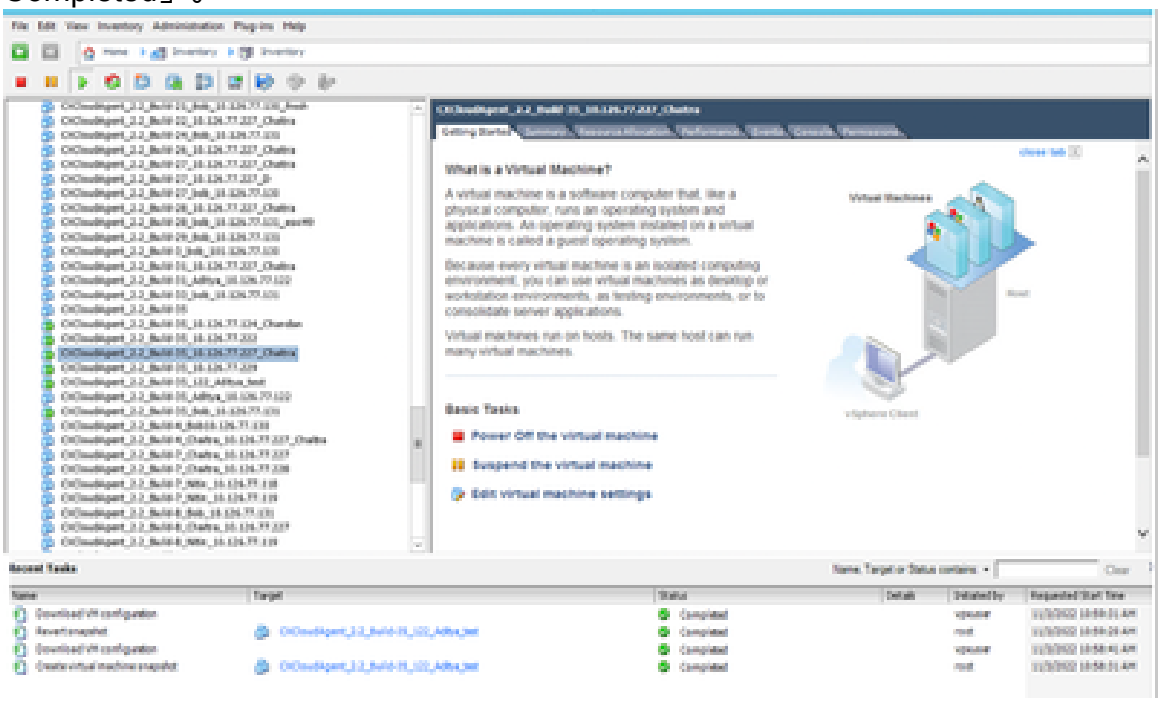
Snapshots視窗

2. 按一下Go to。Confirm視窗開啟。



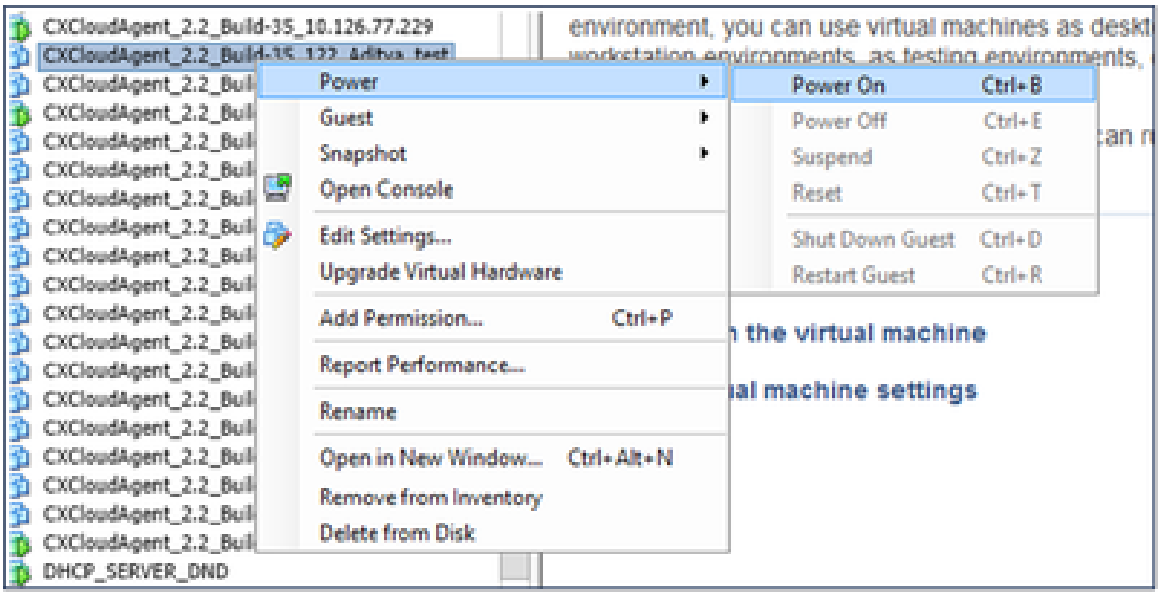
確認視窗

3. 按一下「Yes」。Revert snapshot狀態在「Recent Tasks」清單中顯示為「Completed」。



最近的任務

4. 按一下右鍵VM並選擇Power > Power On以開啟VM。



安全性

CX雲代理可確保客戶的端到端安全性。CX雲和CX雲代理之間的連線是TLS安全的。雲代理的預設SSH使用者只能執行基本操作。

實體安全

在安全的VMware伺服器公司中部署CX雲代理OVA映像。OVA 是透過思科軟體下載中心所安全分享

。開機載入器（單一使用者模式）密碼是使用隨機的唯一密碼設定的。使用者必須參考此常見問題才能設定此引導載入程式（單使用者模式）密碼。

帳戶安全性

部署期間，將建立cxcadmin使用者帳戶。使用者在初始配置期間被迫設定密碼。cxcadmin使用者/憑據用於訪問CX雲代理API和通過SSH連線到裝置。

cxcadmin使用者具有許可權最少的受限訪問許可權。cxcadmin密碼遵循安全策略，是單向雜湊密碼，有效期為90天。cxcadmin使用者可以使用名為remoteaccount的實用程式建立cxcroot使用者。cxcroot使用者可以獲得root許可權。

網路安全

可以使用SSH和cxcadmin使用者憑據訪問CX雲代理VM。傳入連接埠限制為 22 (ssh)，514(Syslog)。

驗證

基於密碼的身份驗證：裝置維護單個使用者(cxcadmin)，使使用者能夠對CX雲代理進行身份驗證和通訊。

- 使用 ssh 在設備上進行根權限動作

cxcadmin使用者可以使用名為remoteaccount的實用程式建立cxcroot使用者。此實用程式顯示RSA/ECB/PKCS1v1_5加密密碼，該密碼只能從SWIM門戶(https://swims.cisco.com/abraxas/decrypt)解密。只有授權人員才能訪問此門戶。cxcroot使用者可以使用此解密的密碼獲得root許可權。密碼的有效期僅兩天。cxcadmin使用者必須在密碼到期後重新建立帳戶並從SWIM門戶獲取密碼。

強化

CX雲代理裝置遵循Center of Internet Security強化標準。

資料安全

CX Cloud Agent 設備不會儲存任何客戶個人資訊。

裝置憑證應用程式（作為其中一個pod運行）將加密的伺服器憑證儲存在安全資料庫中。所收集的資料不會以任何形式儲存在裝置內，除非在處理時暫時儲存。收集完成後，遙測資料會儘快上傳到CX雲，並在確認上傳成功後立即從本地儲存中刪除。

資料傳輸

註冊軟體包包含所需唯一的X.509設備證書和金鑰，用於建立與Iot Core的安全連線。使用該代理可通過傳輸層安全(TLS)v1.2使用消息隊列遙測傳輸(MQTT)建立安全連線

記錄與監視

日誌不包含任何形式的個人身份資訊(PII)資料。稽核日誌會捕獲在CX雲代理裝置上執行的所有對安全性敏感的操作。

思科遙測命令

CX雲使用Cisco遙測命令中列出的API和命令檢索資產遙測。本文檔根據命令對Cisco DNA Center庫存、診斷橋接器、Intersight、合規性見解、故障以及CX雲代理收集的所有其他遙測源的適用性對命令進行分類。

資產遙測中的敏感資訊在傳輸到雲之前會被掩蔽。CX雲代理遮蔽所有直接向CX雲代理傳送遙測資料的收集資產的敏感資料。這包括密碼、金鑰、社群字串、使用者名稱等。在將資訊傳輸到CX雲代理之前，控制器為所有控制器管理的資產提供資料掩蔽。在一些情況下，控制器管理的資產遙測可以進一步匿名化。請參閱對應的產品支援檔案以瞭解更多有關遙測匿名化的資訊(例如，《Cisco DNA Center管理員指南》的匿名化資料一節)。

雖然無法自定義遙測命令清單且無法修改資料掩碼規則，但客戶可以通過指定資料來源來控制哪些資產的遙測CX雲訪問，如本文件(針對CX雲代理收集的其他資產)的控制器管理裝置的產品支援文檔或連線資料來源部分中所述。

安全摘要

安全性功能	說明
開機載入器密碼	開機載入器（單一使用者模式）密碼是使用隨機的唯一密碼設定的。使用者必須參考常見問題才能設定其引導載入程式（單使用者模式）密碼。
使用者存取	SSH： ·使用cxcadmin使用者訪問裝置需要安裝期間建立的憑據 ·使用cxcroot使用者訪問裝置需要授權人員使用SWIM門戶解密憑證
使用者帳戶	· cxcadmin：已建立預設使用者帳戶；使用者可以使用cxcli執行CX Cloud Agent應用程式命令，並對裝置具有最低許可權；cxcroot使用者及其加密密碼是使用cxcadmin使用者生成的 · cxcroot:cxcadmin可以使用實用程式「remoteaccount」建立此使用者；使用者可使用此帳戶獲得root許可權
cxcadmin 密碼原則	·使用SHA-256對密碼進行單向雜湊並安全儲存 ·最少八(8)個字元，包含以下三個類別：大寫、小寫、數字和特殊字元

cxcroot 密碼原則	· cxcroot密碼已加密RSA/ECB/PKCS1v1_5 ·生成的密碼需要在SWIM門戶中解密 · cxcroot使用者和密碼有效期為兩天，可以使用cxcadmin使用者重新生成
ssh 登入密碼原則	·最少八個字元，包含以下三個類別：大寫、小寫、數字和特殊字元 ·五次失敗的登入嘗試將密碼鎖住30分鐘；密碼將在90天後過期
連接埠	開啟傳入連接埠 – 514(Syslog) 和 22 (ssh)
資料安全	·未儲存客戶資訊 ·未儲存任何裝置資料 ·加密並儲存在資料庫中的Cisco DNA Center伺服器憑證

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。