

在VMware ESXi上部署FireSIGHT管理中心

目錄

[簡介](#)

[必要條件](#)

[採用元件](#)

[組態](#)

[部署OVF模板](#)

[開啟電源並完成初始化](#)

[配置網路設定](#)

[執行初始設定](#)

[相關資訊](#)

簡介

本文檔介紹在VMware ESXi上運行的FireSIGHT管理中心（也稱為防禦中心）的初始設定。FireSIGHT管理中心允許您管理一個或多個FirePOWER裝置、下一代入侵防禦系統(Next Generation Intrusion Prevention System, NGIPS)虛擬裝置以及具備FirePOWER服務的自適應安全裝置(ASA)。

附註：本文檔是《FireSIGHT系統安裝指南》和《使用手冊》的補充。有關ESXi特定的配置和故障排除問題，請參閱VMware知識庫和文檔。

必要條件

採用元件

本檔案中的資訊是根據以下平台：

- Cisco FireSIGHT管理中心
- Cisco FireSIGHT管理中心虛擬裝置
- VMware ESXi 5.0

在本檔案中，「裝置」是指以下平台：

- Sourcefire FirePOWER 7000系列裝置和8000系列裝置
- 適用於VMware ESXi的Sourcefire NGIPS虛擬裝置
- 具備FirePOWER服務的Cisco ASA 5500-X系列

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

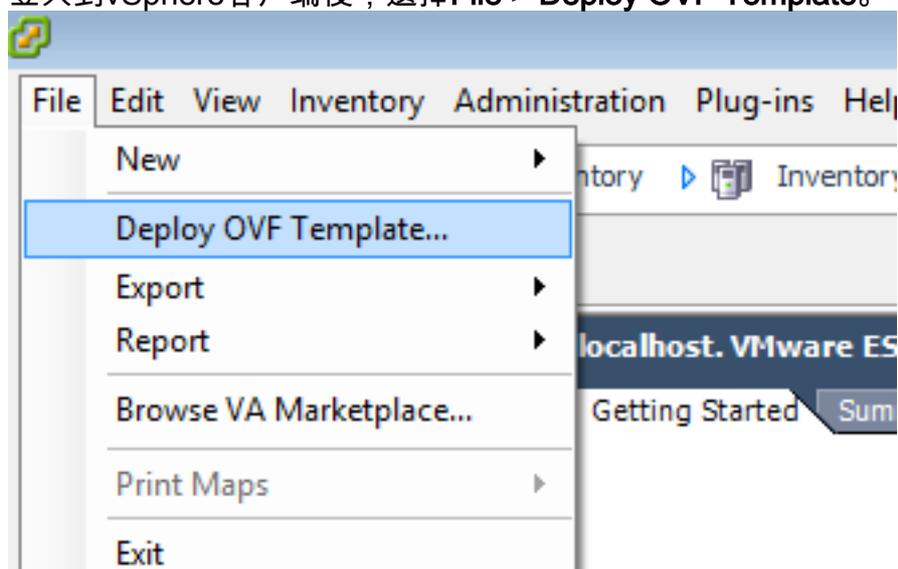
組態

部署OVF模板

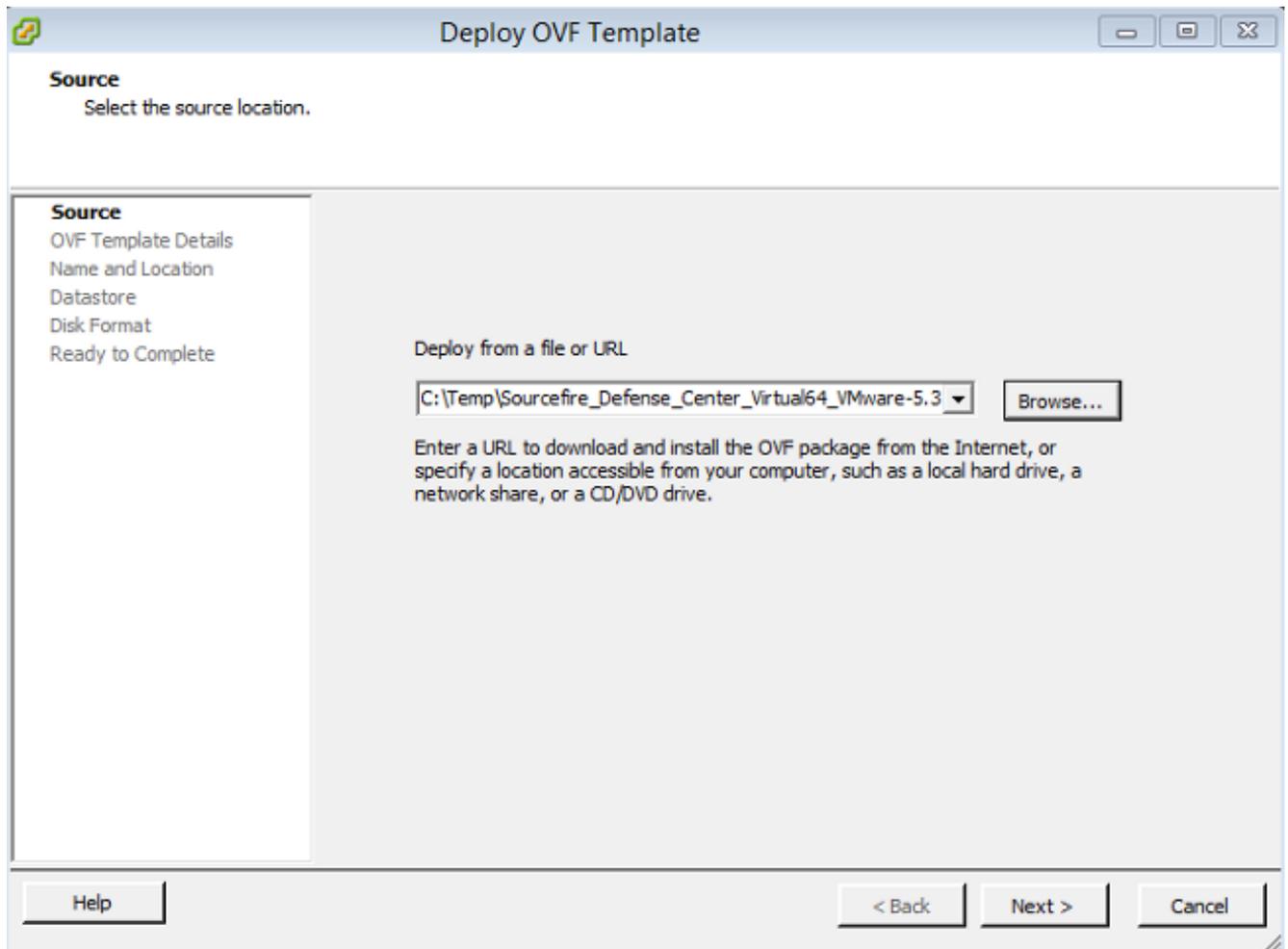
1. 從[思科支援和下載](#)站點下載Cisco FireSIGHT管理中心虛擬裝置。
2. 將tar.gz檔案的內容解壓到本地目錄。
3. 使用VMware vSphere Client連線到ESXi伺服器。



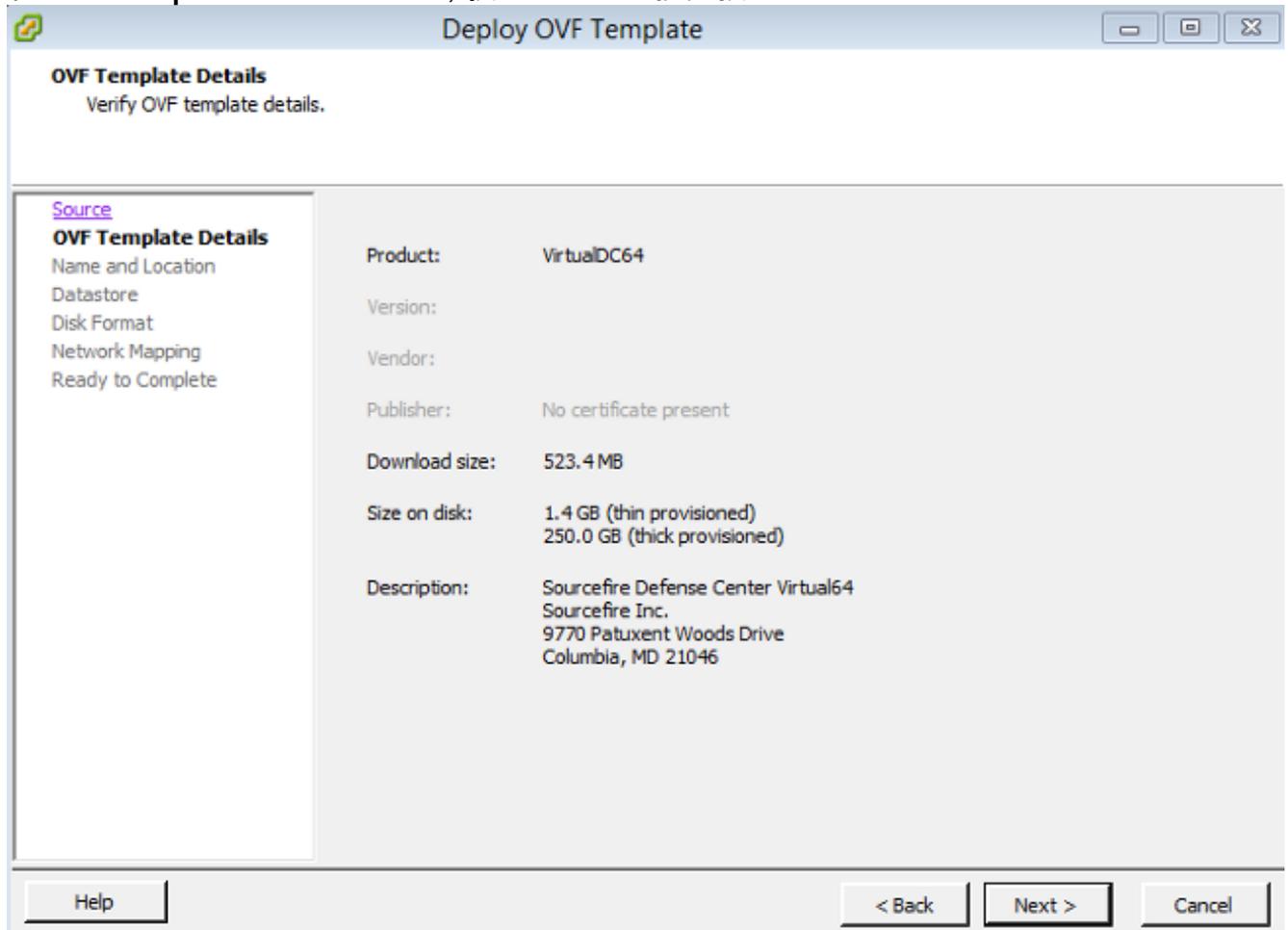
4. 登入到vSphere客戶端後，選擇File > Deploy OVF Template。



5. 按一下**瀏覽**並找到在步驟2中解壓的檔案。選擇OVF檔案 Sourcefire_Defense_Center_Virtual64_VMware-ESXi-X.X.X-xxx.ovf，然後按一下下一步。



6. 在OVF Template Details螢幕上，按一下Next以接受預設設定。



7. 提供管理中心的名稱，然後按一下下一步。

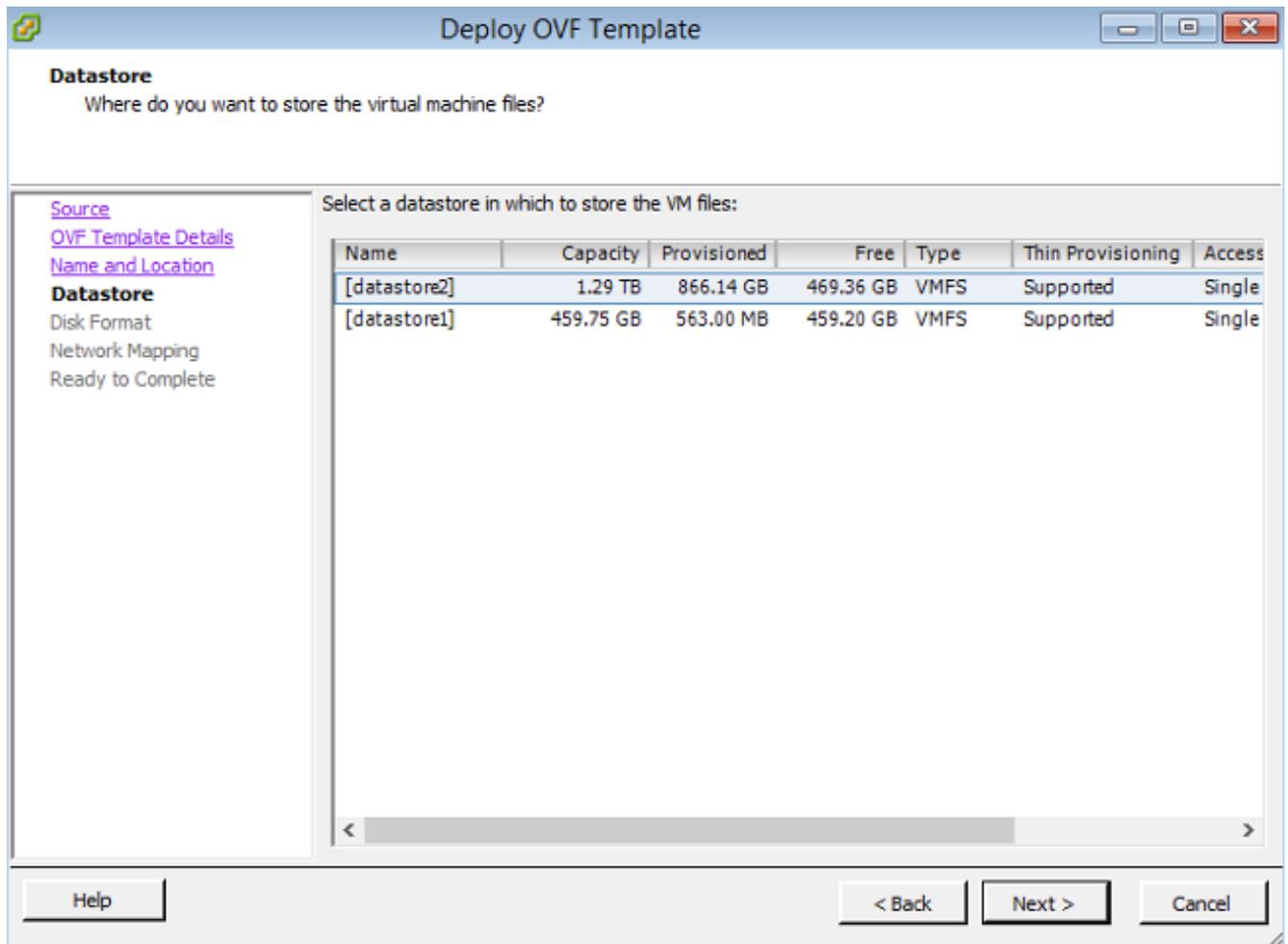
The screenshot shows a window titled "Deploy OVF Template" with standard window controls (minimize, maximize, close) in the top right corner. Below the title bar, the text "Name and Location" is displayed, followed by the instruction "Specify a name and location for the deployed template".

On the left side, there is a vertical list of steps: "Source", "OVF Template Details", "Name and Location" (which is highlighted in bold), "Datastore", "Disk Format", "Network Mapping", and "Ready to Complete".

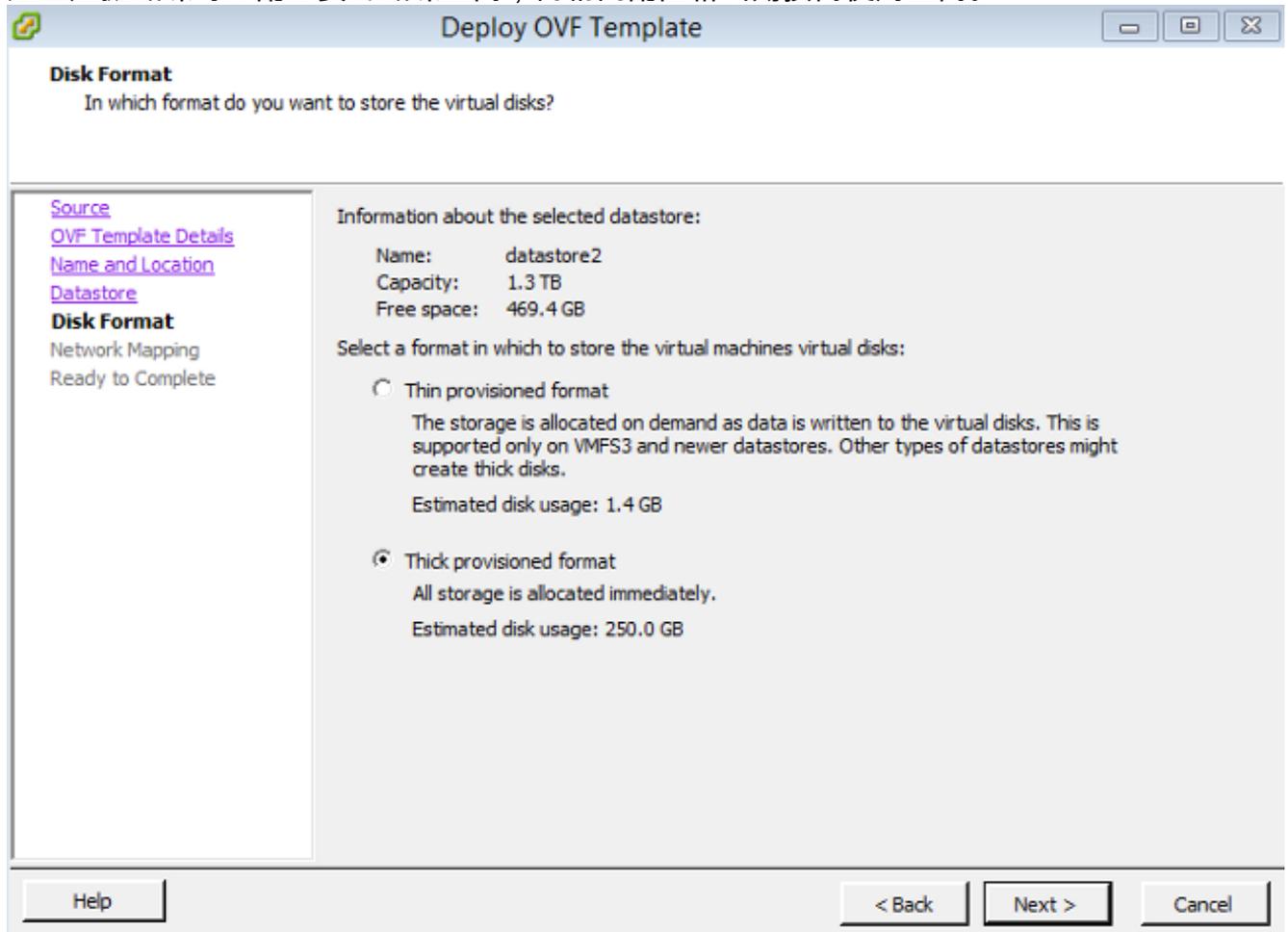
The main area of the window contains a "Name:" label above a text input field. The input field contains the text "VirtualDC64". Below the input field, a note states: "The name can contain up to 80 characters and it must be unique within the inventory folder."

At the bottom of the window, there are three buttons: "Help" on the left, "< Back" in the center, and "Next >" on the right, followed by a "Cancel" button on the far right.

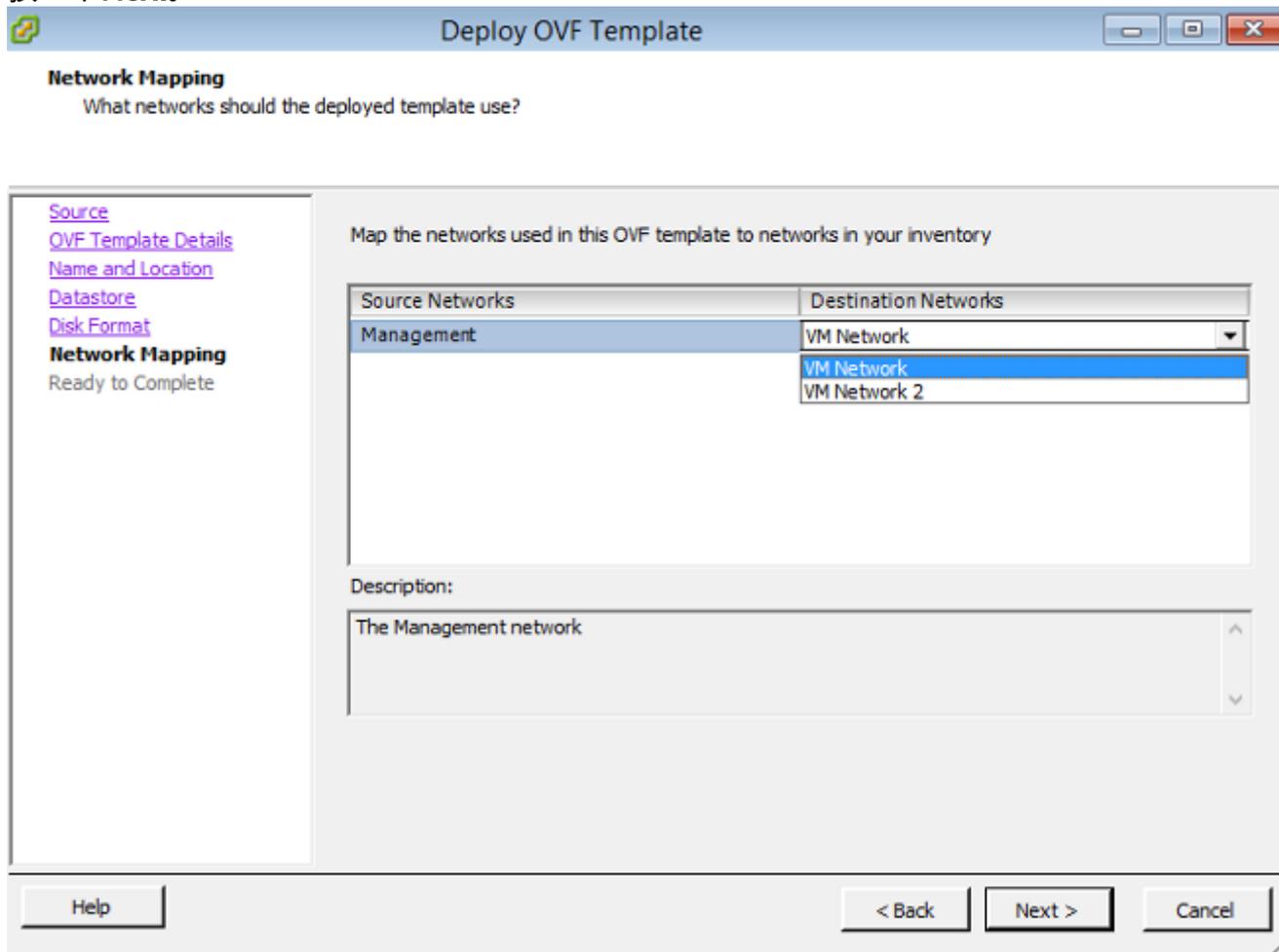
8. 選擇要在其上建立虛擬機器的資料儲存區，然後按一下下一步。



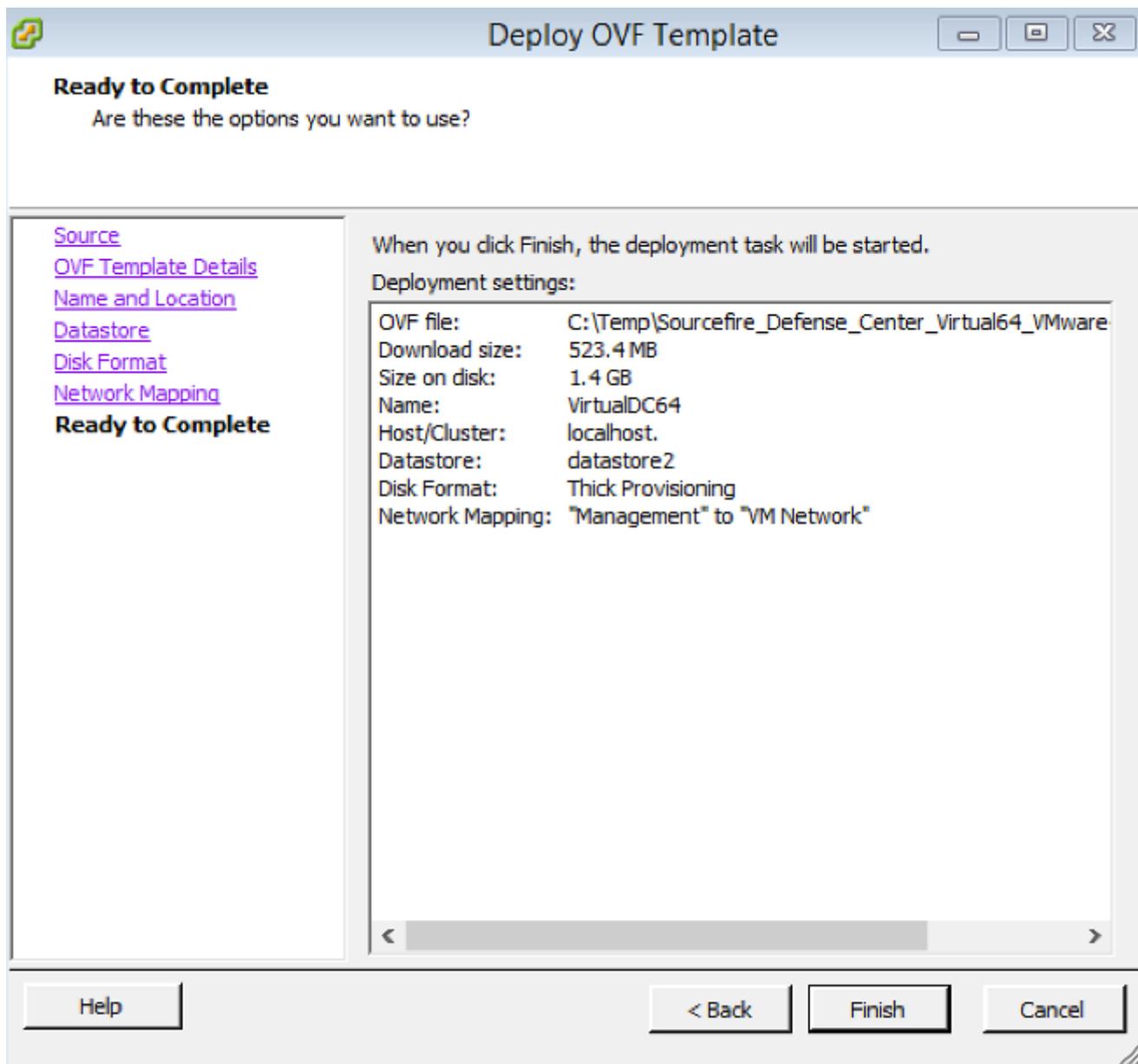
9. 按一下**Disk Format**的**Thick provisioned format**單選按鈕，然後按一下**Next**。密集配置格式在建立虛擬磁碟時分配必要的磁碟空間，而精簡配置格式則按需使用空間。



10. 在**Network Mapping**部分中，將FireSIGHT管理中心的管理介面與VMware網路相關聯，然後按一下**Next**。

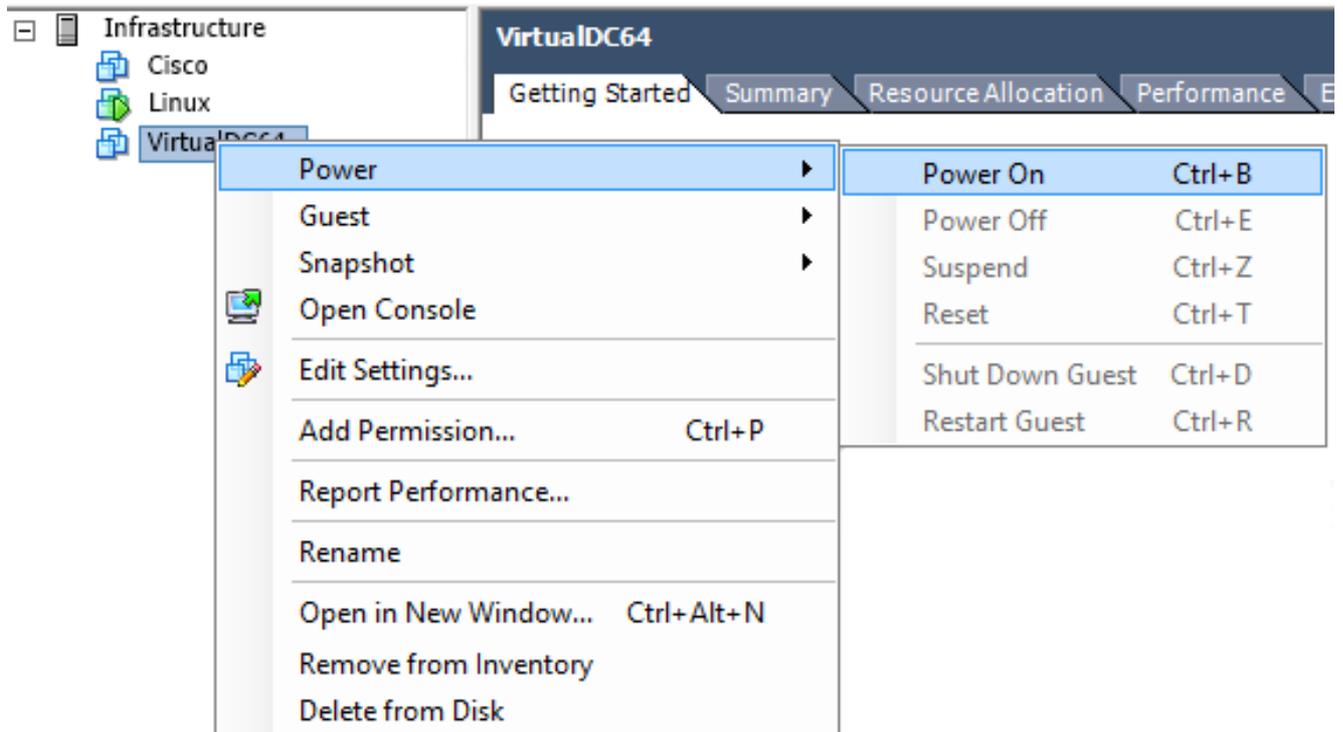


11. 按一下**完成**以完成OVF模板部署。

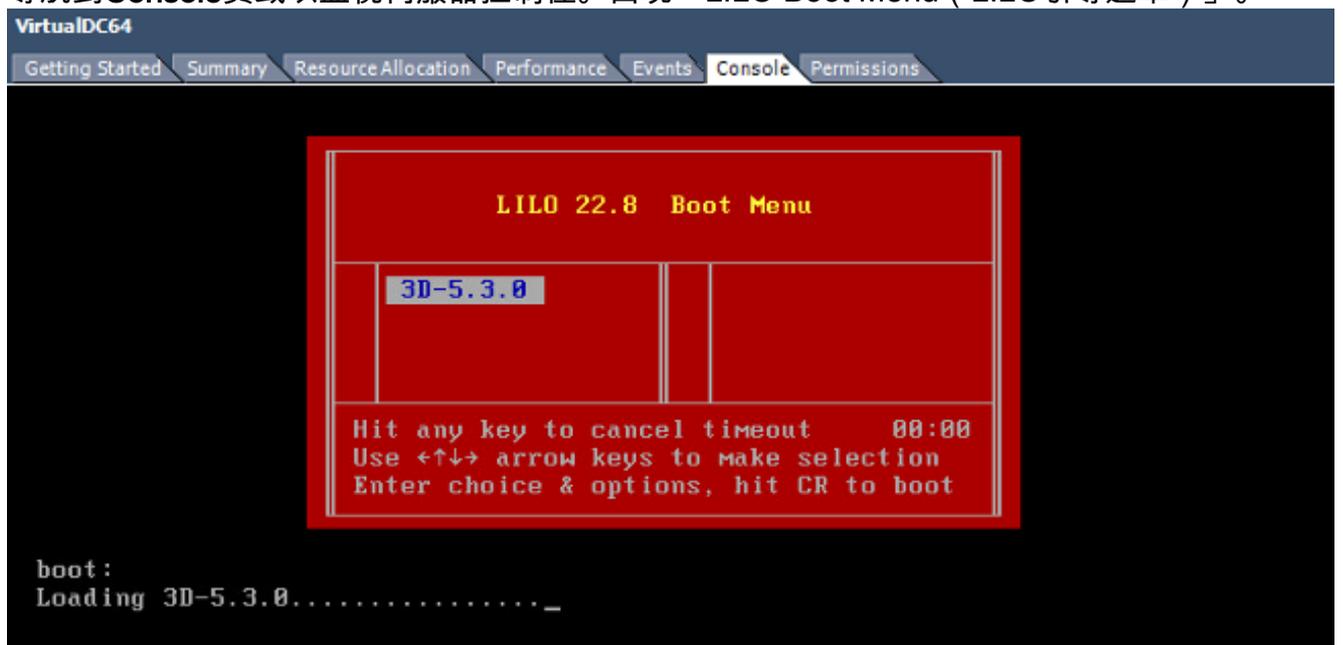


開啟電源並完成初始化

1. 導航到新建立的虛擬機器。 按一下右鍵伺服器名稱，然後選擇**Power > Power On**以首次啟動伺服器。



2. 導航到Console頁籤以監視伺服器控制檯。出現「LILO Boot Menu (LILO引導選單)」。



BIOS資料檢查成功後，初始化過程開始。首次啟動可能需要額外的時間才能完成，因為配置資料庫是首次初始化的。

```
Firstboot detected, executing scripts
Executing S03install-math-pari.sh [ OK ]
Executing S04async_syslog_dc.sh [ OK ]
Executing S04fix-httpd.sh [ OK ]
Executing S05set-mgmt-port [ OK ]
Executing S06addusers [ OK ]
Executing S07uuid-init [ OK ]
Executing S09configure_mysql [ OK ]
```

```
***** Attention *****
```

```
Initializing the configuration database. Depending on available
system resources (CPU, memory, and disk), this may take 30 minutes
or more to complete.
```

```
***** Attention *****
```

```
Executing S10database
_
```

完成後，您可能會看到No these device的消息。

```
Copyright (c) 1999-2010 Intel Corporation.
Silicom Bypass-SD Control driver v5.0.39.5
No such device
_
```

3. 按Enter鍵以取得登入提示。

```
Copyright (c) 1999-2010 Intel Corporation.
Silicom Bypass-SD Control driver v5.0.39.5
No such device
```

```
Sourcefire Virtual Defense Center 64bit v5.3.0 (build 571)
Sourcefire3D login: _
```

附註：消息「WRITE SAME failed.手動清零。」首次引導系統後可能會出現。這並非表示存在缺陷，而是正確地表明VMware儲存驅動程式不支援WRITE SAME命令。系統會顯示此消息，並繼續執行回退命令以執行相同操作。

配置網路設定

1. 在Sourcefire3D登入提示中，使用以下憑證登入：5.x版使用者名稱:admin密碼：**Sourcefire6.x**及更新版本使用者名稱:admin密碼：**Admin123**提示：您可以在GUI中更改初始設定過程中的預設密碼。
2. 網路的初始配置使用指令碼完成。您需要以root使用者身份運行指令碼。若要切換到root使用者，請輸入**sudo su -**命令以及密碼**Sourcefire**或**Admin123**（6.x版）。以root使用者身份登入管理中心命令列時要小心。
admin@Sourcefire3D:~\$ sudo su -
Password:
3. 若要開始網路配置，請輸入**configure-network**指令碼作為root。

```
root@Sourcefire3D:~# configure-network
Do you wish to configure IPv4? (y or n) y
```

系統將要求您提供管理IP地址、網路掩碼和預設網關。確認設定後，網路服務將重新啟動。因此，管理介面關閉並返回。

```
Do you wish to configure IPv4? (y or n) y
Management IP address? [192.168.45.45] 192.0.2.2
Management netmask? [255.255.255.0]
Management default gateway? 192.0.2.1

Management IP address?          192.0.2.2
Management netmask?             255.255.255.0
Management default gateway?     192.0.2.1

Are these settings correct? (y or n) y

Do you wish to configure IPv6? (y or n) n
e1000: eth0: e1000_watchdog_task: NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None
ADDRCONF(NETDEV_UP): eth0: link is not ready
ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready

Updated network configuration.

Updated comms. channel configuration.

Please go to https://192.0.2.2/ or https://[]/ to finish installation.
root@Sourcefire3D:~# _
```

執行初始設定

1. 設定網路設定後，開啟Web瀏覽器並透過HTTPS(在本範例中為<https://192.0.2.2>)瀏覽至設定的IP。出現提示時，驗證預設SSL證書。使用以下憑據登入：5.x版 使用者名稱:admin密碼：**Sourcefire6.x**及更新版本使用者名稱:admin密碼：**Admin123**
2. 在接下來的螢幕中，除了密碼更改和服務條款接受外，所有GUI配置部分都是可選的。如果已知資訊，建議使用設定嚮導來簡化管理中心的初始配置。配置後，按一下**Apply**將配置應用到管理中心和註冊裝置。配置選項的簡要概述如下：**更改密碼**：允許您更改預設管理員帳戶的密碼。需要更改密碼。**網路設定**：允許您為裝置或虛擬機器的管理介面修改先前配置的IPv4和IPv6網路設定。**時間設定**：建議您使用可靠的NTP源同步管理中心。可以通過系統策略配置IPS感測器，使其時間與管理中心同步。可以選擇手動設定時間和顯示時區。**定期規則更新匯入**：在初始設定期間啟用定期的Snort規則更新，也可以立即安裝。**定期地理位置更新**：在初始設定期間啟用定期地理定位規則更新，也可以立即安裝。**自動備份**：計畫自動配置備份。**許可證設定**：新增功能許可證。**裝置註冊**：允許您新增、許可初始訪問控制策略並將其應用於預註冊裝置。主機名/IP地址和註冊金鑰應與FirePOWER IPS模組上配置的IP地址和註冊金鑰匹配。**一般使用者授權合約**：需要接受EULA。

Change Password

Use these fields to change the password for the admin account. Sourcefire recommends that you use a password that has at least eight alphanumeric characters of mixed case and includes at least one numeric character. Avoid using words that appear in a dictionary.

| | |
|--------------|----------------------|
| New Password | <input type="text"/> |
| Confirm | <input type="text"/> |

Network Settings

Use these fields to specify network-related information for the management interface on the appliance.

| | |
|------------------------------|---|
| Protocol | <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6 <input type="radio"/> Both |
| IPv4 Management IP | <input type="text"/> |
| Netmask | <input type="text"/> |
| IPv4 Default Network Gateway | <input type="text"/> |
| Hostname | <input type="text"/> |
| Domain | <input type="text"/> |
| Primary DNS Server | <input type="text"/> |
| Secondary DNS Server | <input type="text"/> |
| Tertiary DNS Server | <input type="text"/> |

相關資訊

- [適用於VMware的Firepower管理中心虛擬快速入門手冊6.0版](#)
- [技術支援與文件 - Cisco Systems](#)