Installazione di FireSIGHT Management Center su VMware ESXi

Sommario

Introduzione

Questo documento descrive la configurazione iniziale di un centro di gestione FireSIGHT (noto anche come centro di difesa) che viene eseguito su VMware ESXi. Un centro di gestione FireSIGHT consente di gestire una o più appliance FirePOWER, Next-Generation Intrusion Prevention System (NGIPS) Virtual Appliance e Adaptive Security Appliance (ASA) con servizi FirePOWER.

> **Nota:** Questo documento è un supplemento alla Guida all'installazione e manuale dell'utente del sistema FireSIGHT. Per una domanda specifica relativa alla configurazione e alla risoluzione dei problemi di ESXi, consultare la knowledge base e la documentazione di VMware.

Prerequisiti

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti piattaforme:

- Cisco FireSIGHT Management Center
- Appliance virtuale Cisco FireSIGHT Management Center
- VMware ESXI 5.0

In questo documento, il termine "dispositivo" si riferisce alle seguenti piattaforme:

- Appliance Sourcefire FirePOWER serie 7000 e appliance serie 8000
- Sourcefire NGIPS Virtual Appliance per VMware ESXi
- Cisco ASA serie 5500-X con servizio FirePOWER

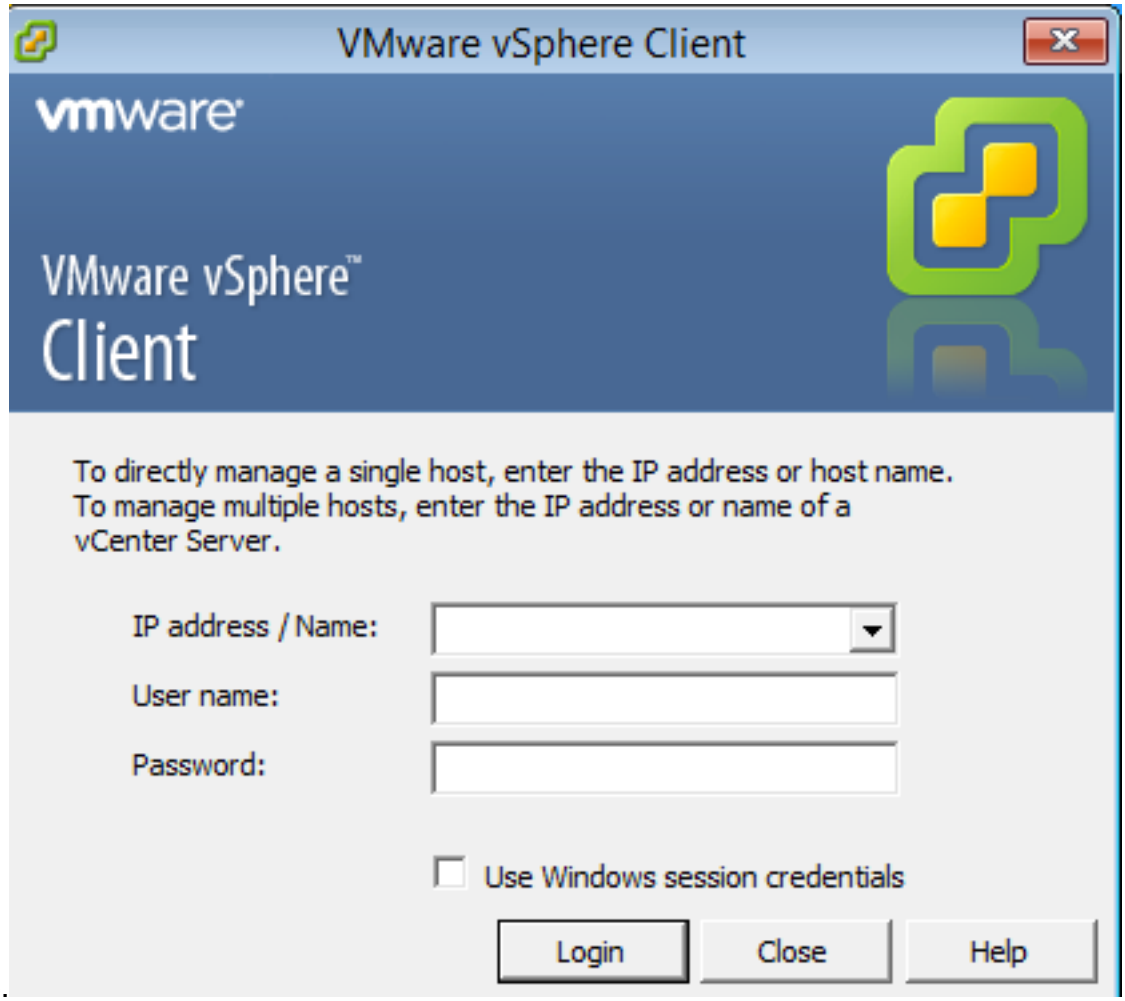
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata

ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

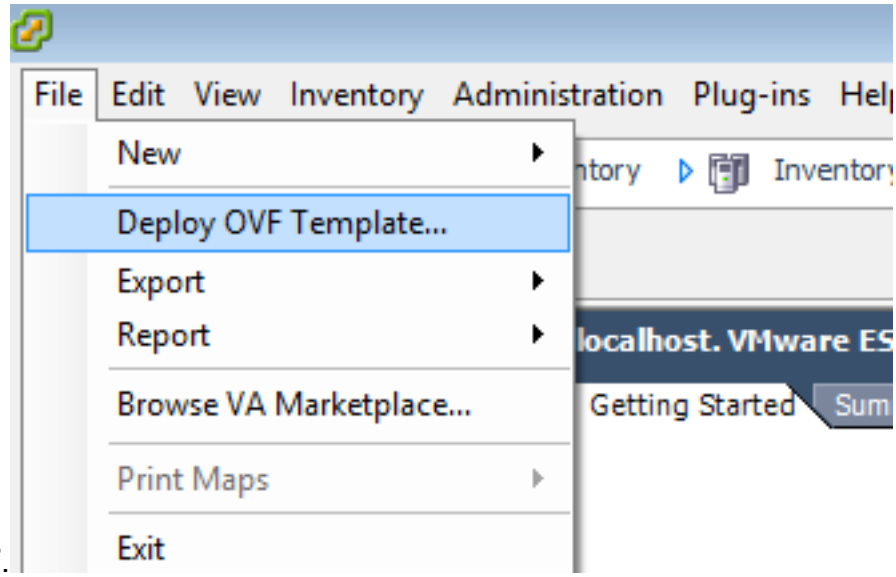
Configurazione

Distribuire un modello OVF

1. Scaricare **Cisco FireSIGHT Management Center Virtual Appliance** dal sito Cisco Support & Downloads.
2. Estrarre il contenuto del file tar.gz in una directory locale.
3. Connessione al server ESXi con un **client VMware vSphere**.

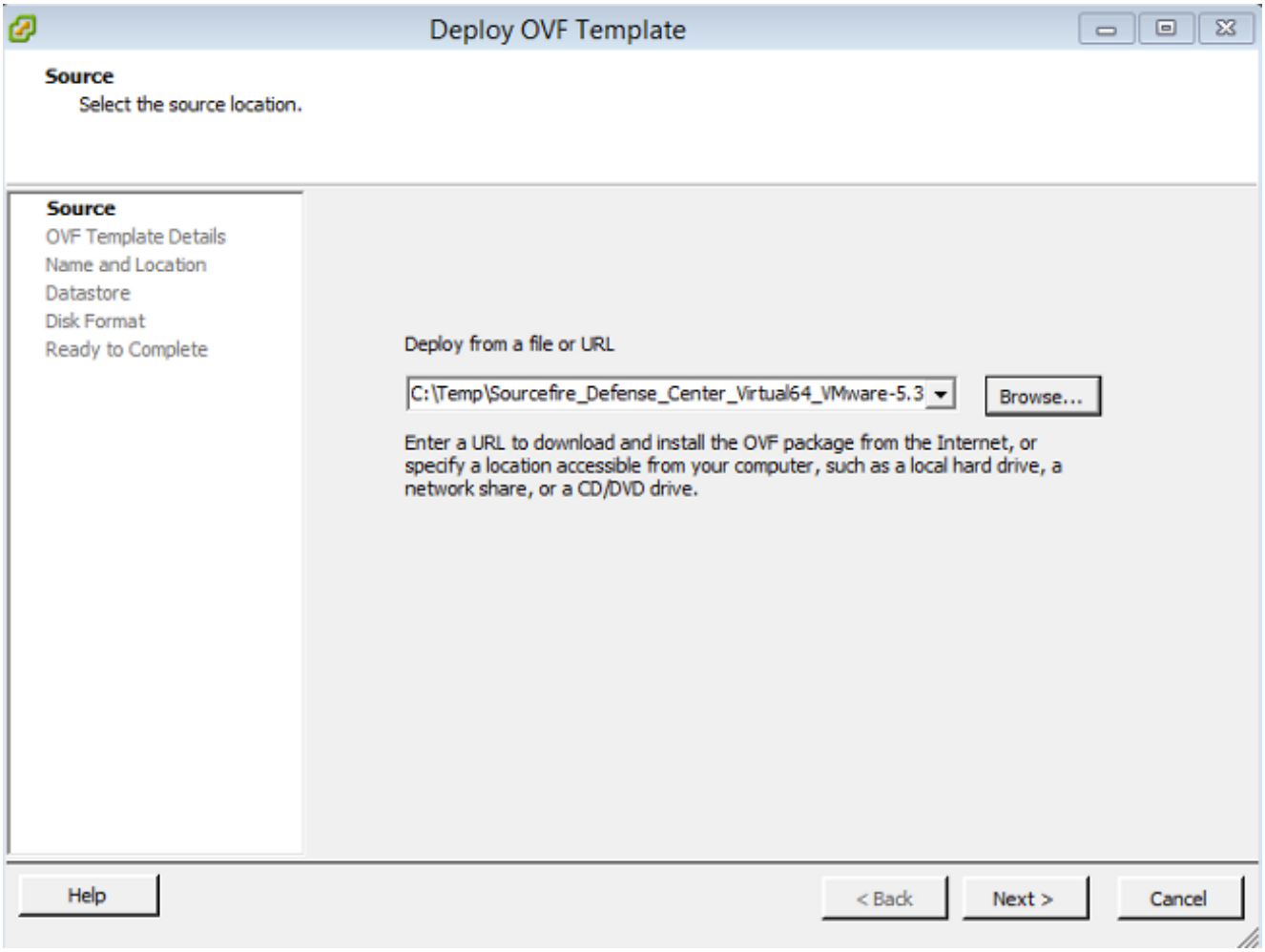


4. Una volta eseguito il login al client vSphere, scegliere **File > Distribuisci modello**

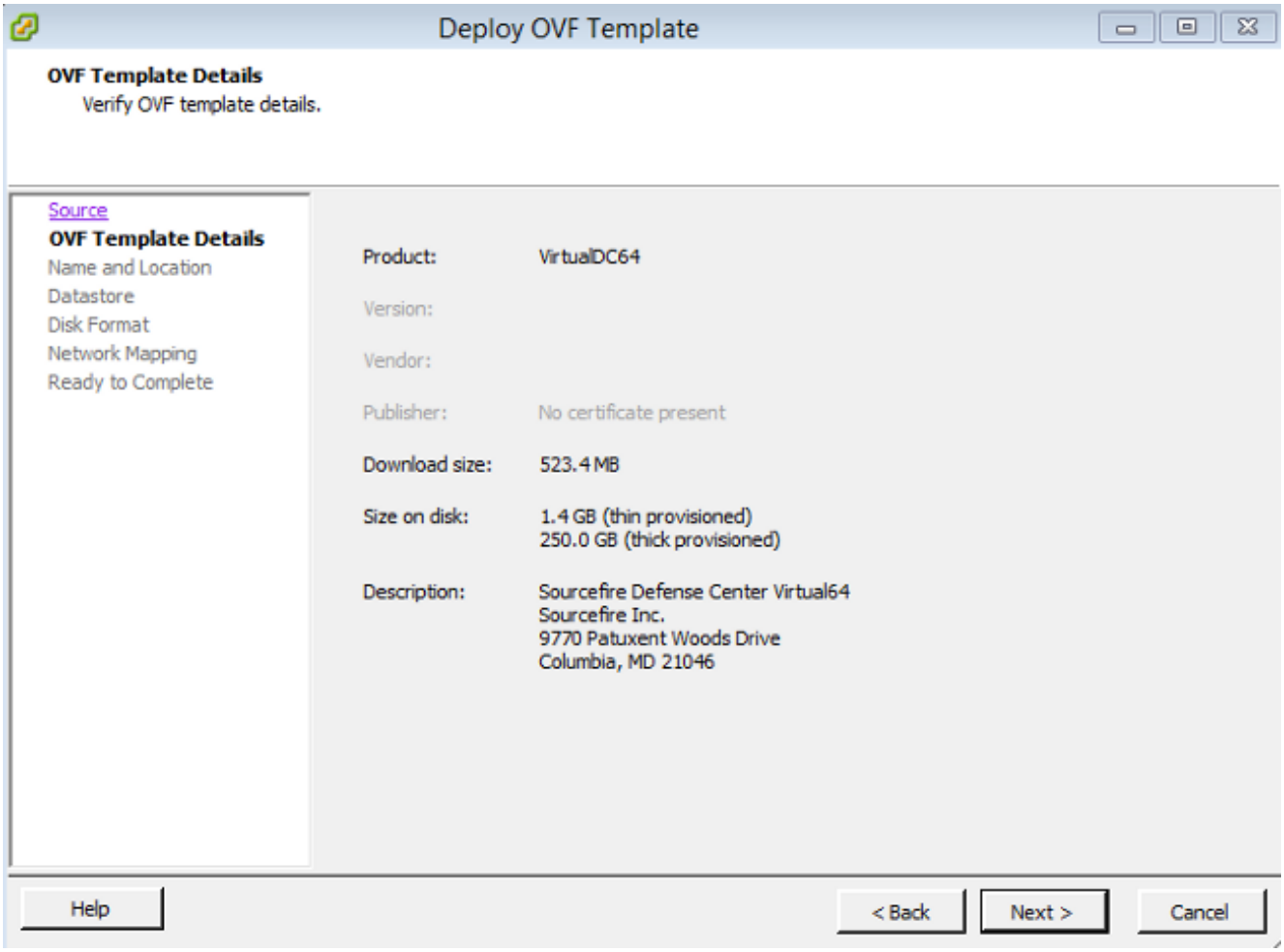


OVF.

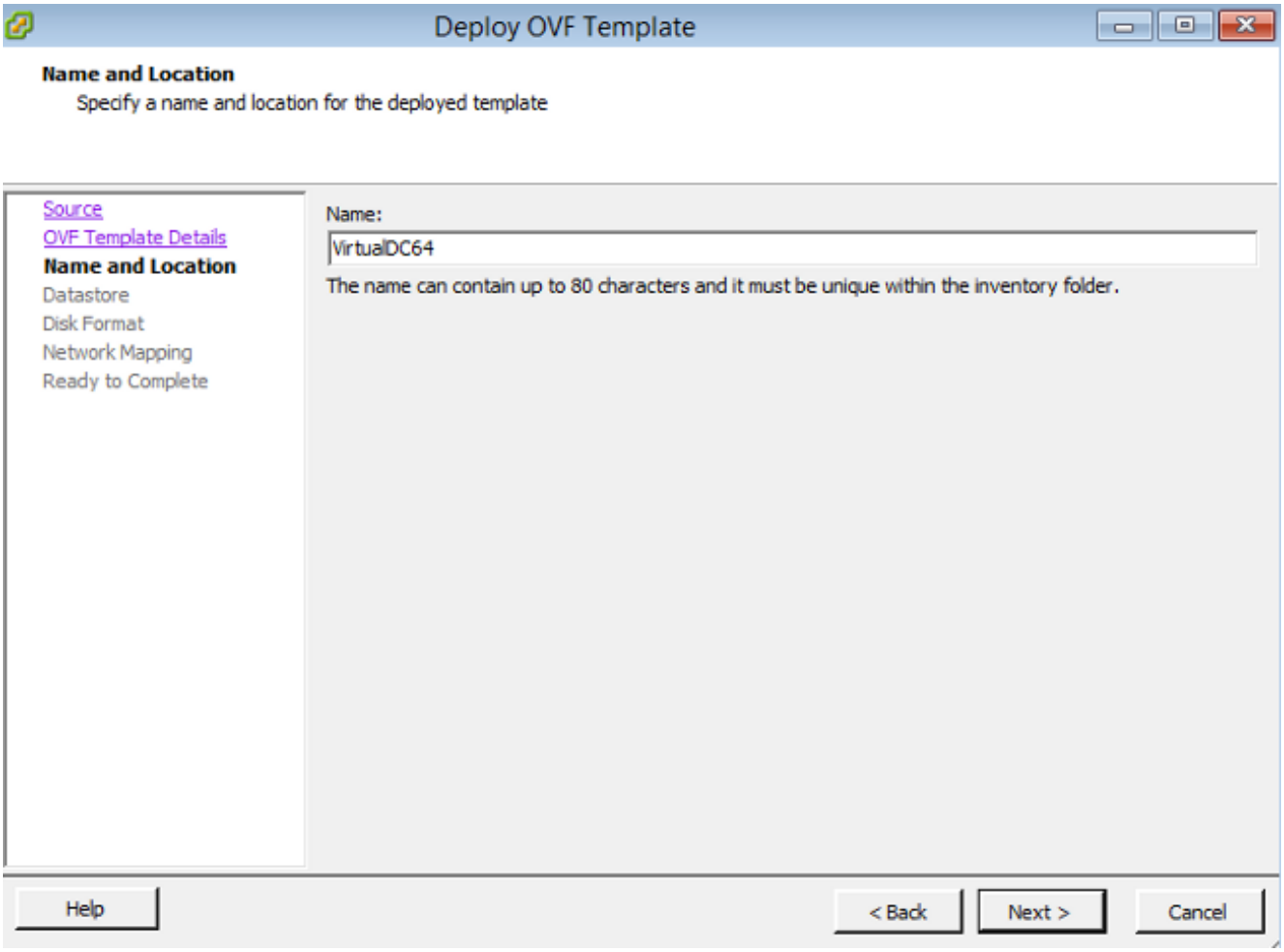
5. Fare clic su **Sfoglia** e individuare i file estratti nel passaggio 2. Scegliere il file OVF Sourcefire_Defense_Center_Virtual64_VMware-ESXi-X.X-xxx.ovf e fare clic su **Avanti.**



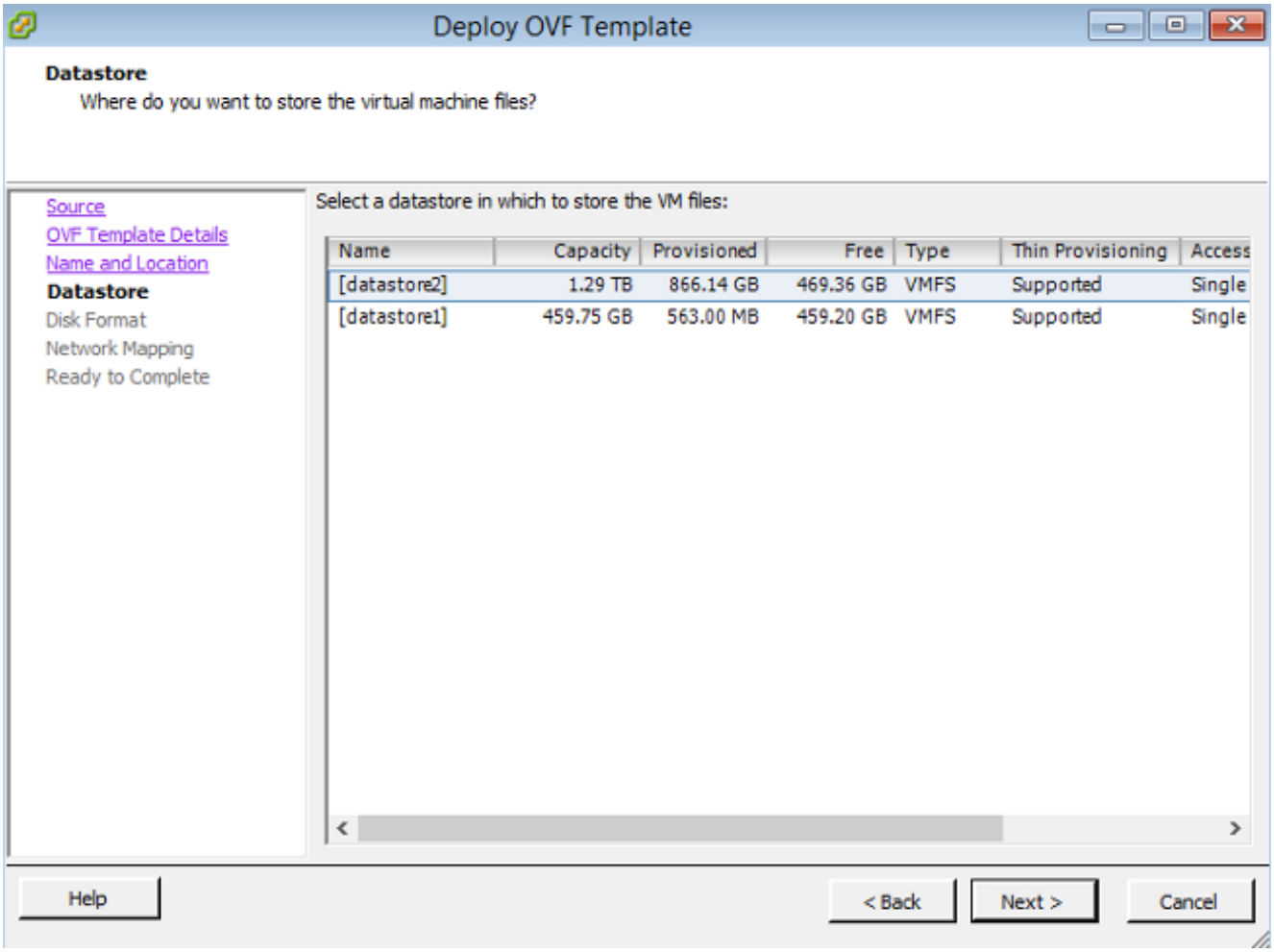
6. Nella schermata **Dettagli modello OVF**, fare clic su **Avanti** per accettare le impostazioni predefinite.



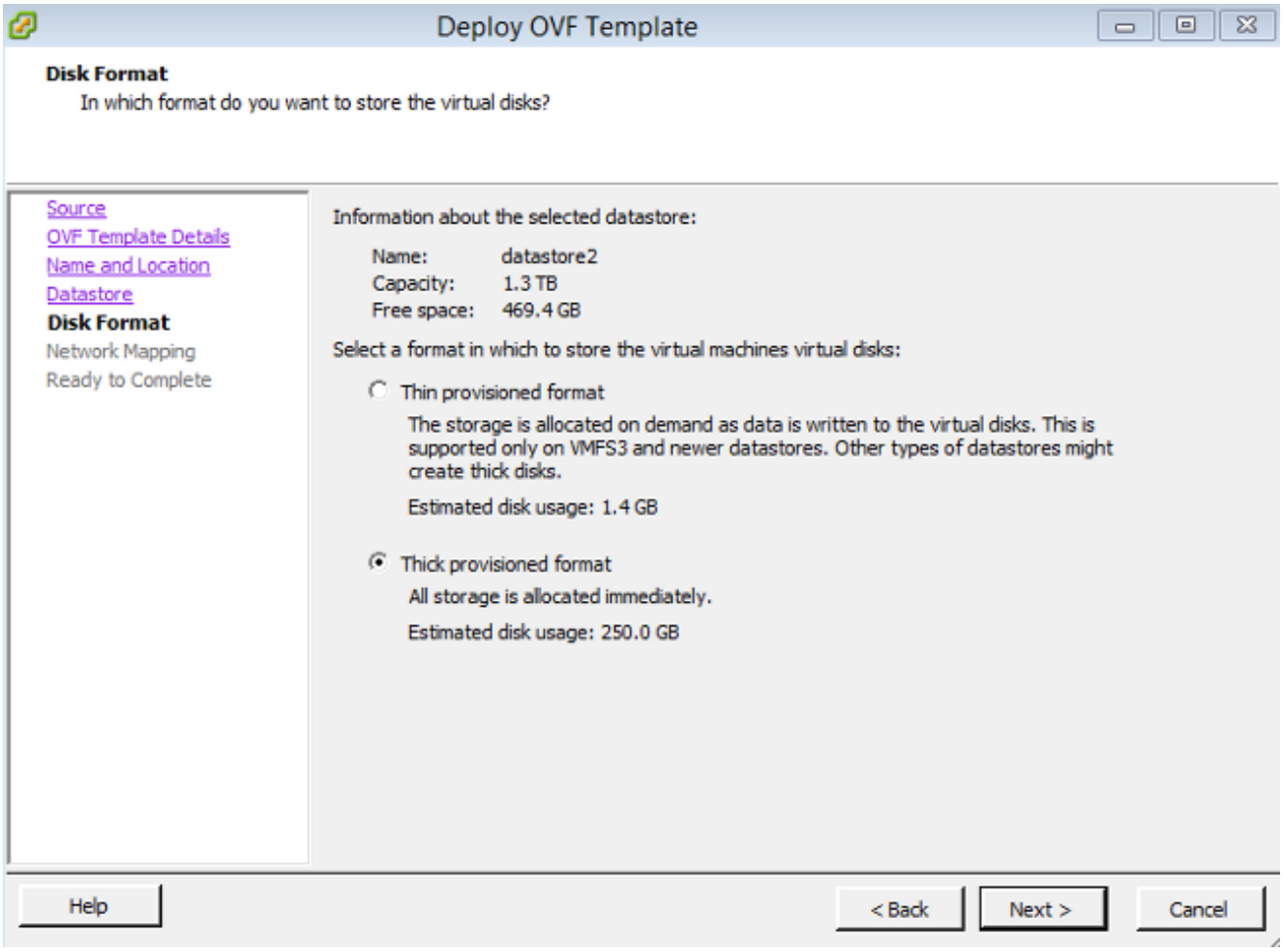
7. Specificare un nome per il centro di gestione e fare clic su **Avanti**.



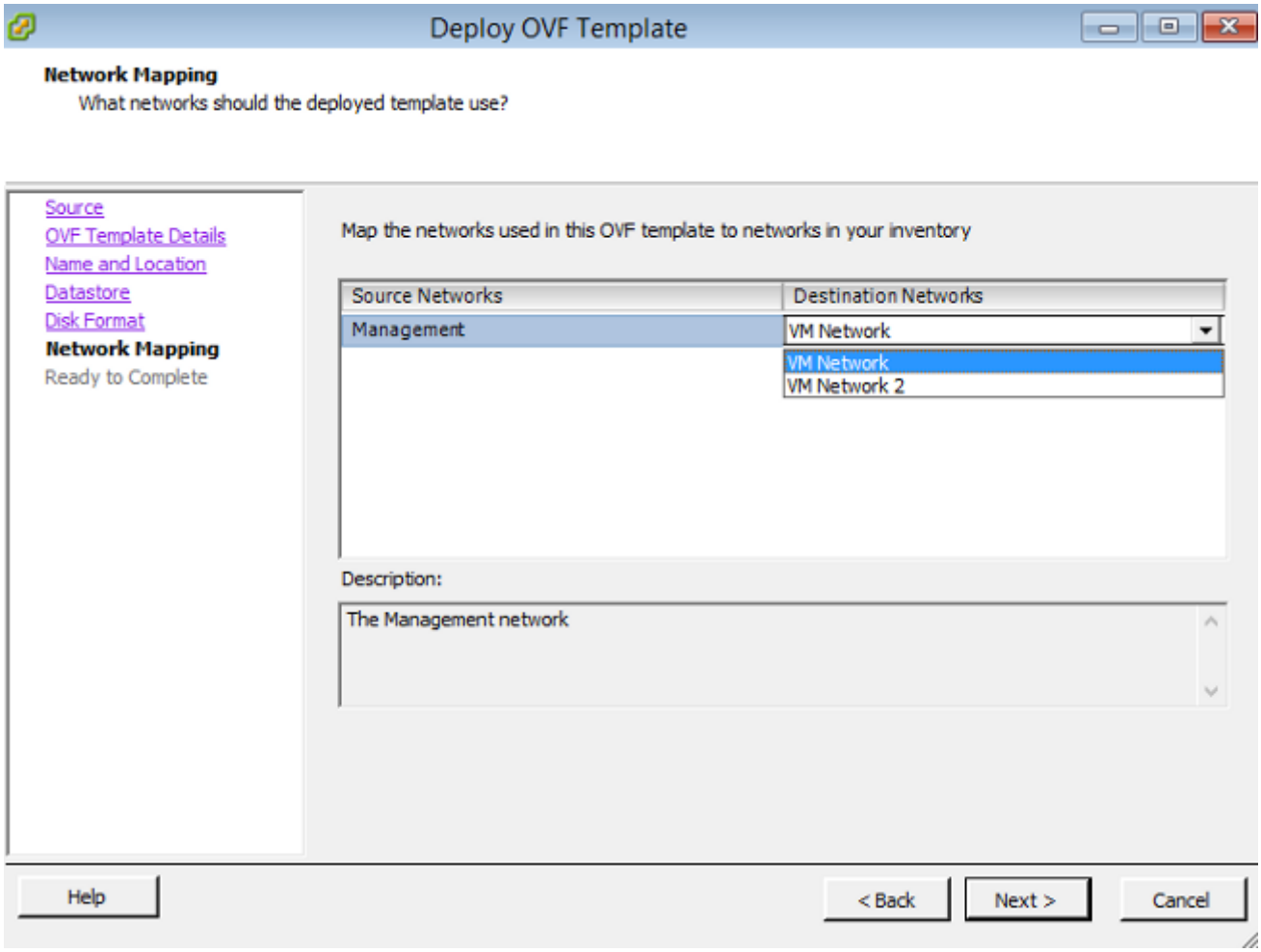
8. Scegliere un **archivio dati** in cui creare la macchina virtuale e fare clic su **Avanti**.



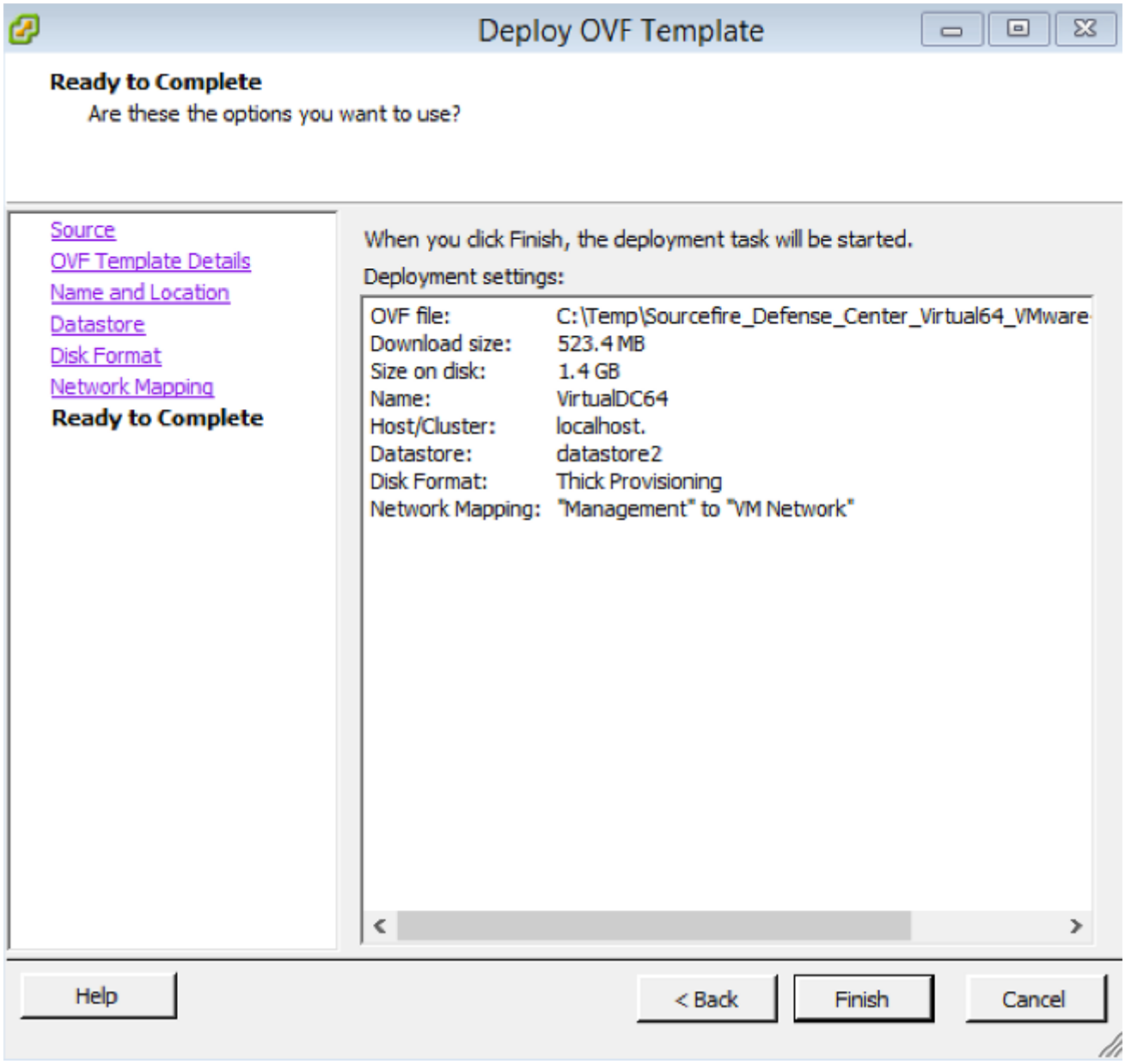
9. Fare clic sul pulsante di opzione **Thick provisioning format** per **Disk Format** e fare clic su **Next** (Avanti). Il formato Thick Provisioning alloca lo spazio su disco necessario al momento della creazione di un disco virtuale, mentre il formato Thin Provisioning utilizza lo spazio su richiesta.



10. Nella sezione **Mappatura di rete**, associare l'interfaccia di gestione di FireSIGHT Management Center a una rete VMware e fare clic su **Avanti**.

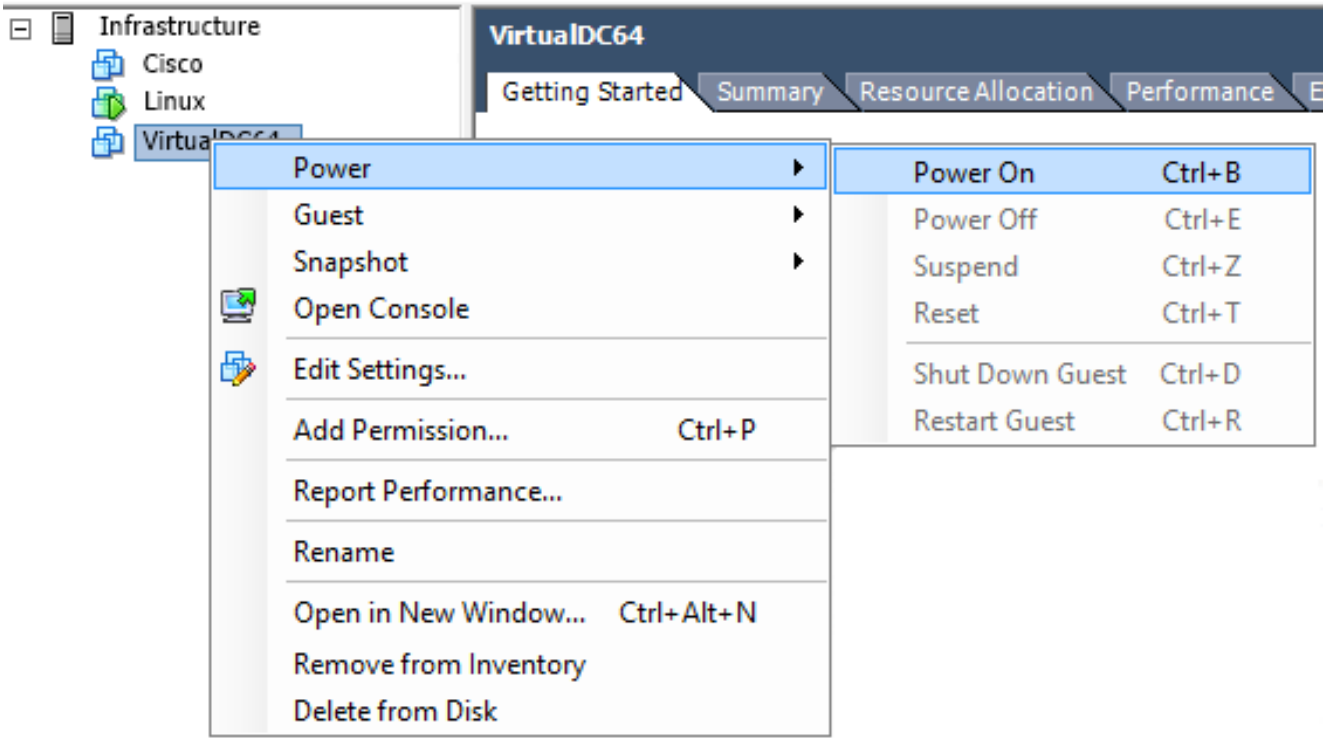


11. Per completare la distribuzione del modello OVF, fare clic su **Fine**.

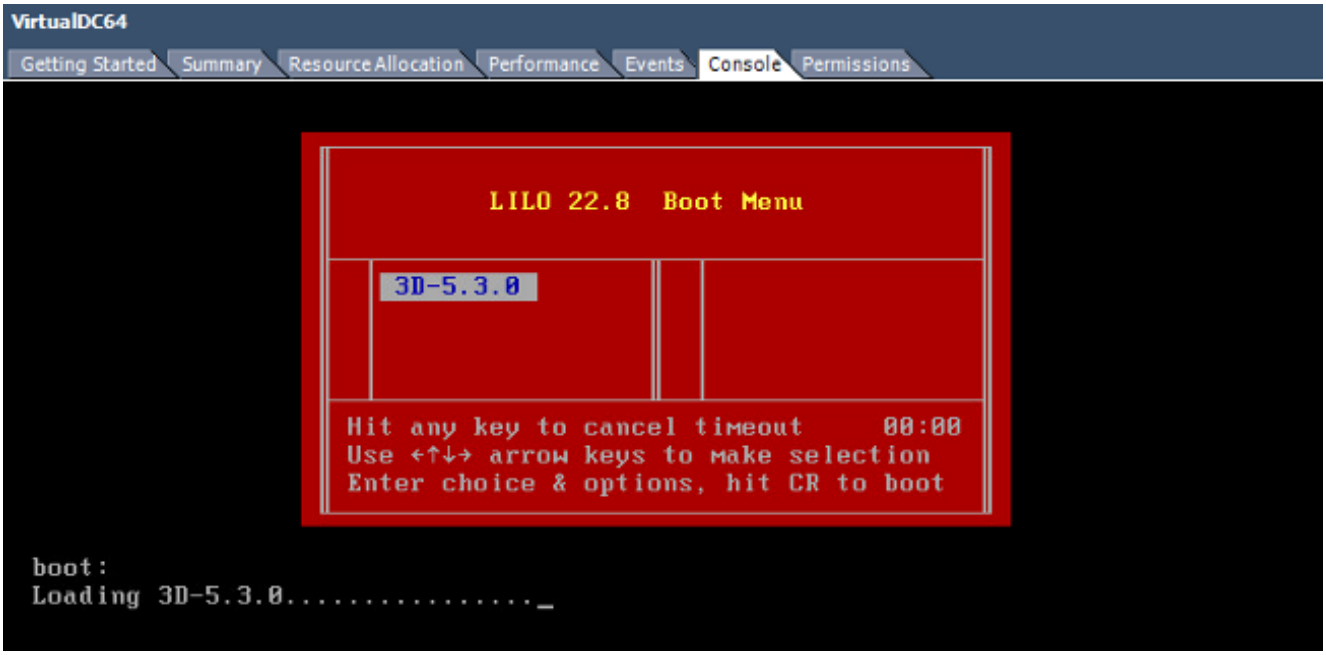


Accensione e completamento dell'inizializzazione

1. Passare alla macchina virtuale appena creata. Fare clic con il pulsante destro del mouse sul nome del server e scegliere **Accensione** per avviare il server per la prima volta.



2. Per monitorare la console del server, passare alla scheda **Console**. Viene visualizzato il menu di avvio
LILO.



Una volta completato il controllo dei dati del BIOS, viene avviato il processo di inizializzazione. Poiché il database di configurazione viene inizializzato per la prima volta, il completamento del primo avvio potrebbe richiedere più
tempo.

```
Firstboot detected, executing scripts
Executing S03install-math-pari.sh                                  [  OK  ]
Executing S04async_syslog_dc.sh                                    [  OK  ]
Executing S04fix-httpd.sh                                          [  OK  ]
Executing S05set-mgmnt-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
_
```

Al termine, potrebbe essere visualizzato un messaggio per Nessun dispositivo di questo tipo.

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

3. Premere **Invio** per ottenere una richiesta di accesso.

```
 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: _
```

Nota: Viene visualizzato il messaggio "WRITE SAME failed. Azzeramento manuale." potrebbe apparire dopo il primo avvio del sistema. Questo non indica un difetto, ma indica correttamente che il driver di storage VMware non supporta il comando WRITE SAME. Il sistema visualizza questo messaggio e procede con un comando di fallback per eseguire la stessa operazione.

Configurazione delle impostazioni di rete

1. Al prompt di accesso di Sourcefire3D, utilizzare le seguenti credenziali per eseguire l'accesso: Per la versione 5.xUsername: **admin**Password: **Sourcefire**Per la versione 6.x e successiveUsername: **admin**Password: **Admin123Suggerimento**: È possibile modificare la password predefinita durante il processo di configurazione iniziale nella GUI.
2. La configurazione iniziale della rete viene eseguita con uno script. È necessario eseguire lo script come utente root. Per passare all'utente root, immettere il comando **sudo su -** insieme alla password **Sourcefire o Admin123** (per 6.x). Prestare attenzione quando si accede alla riga di comando di Management Center come utente root.

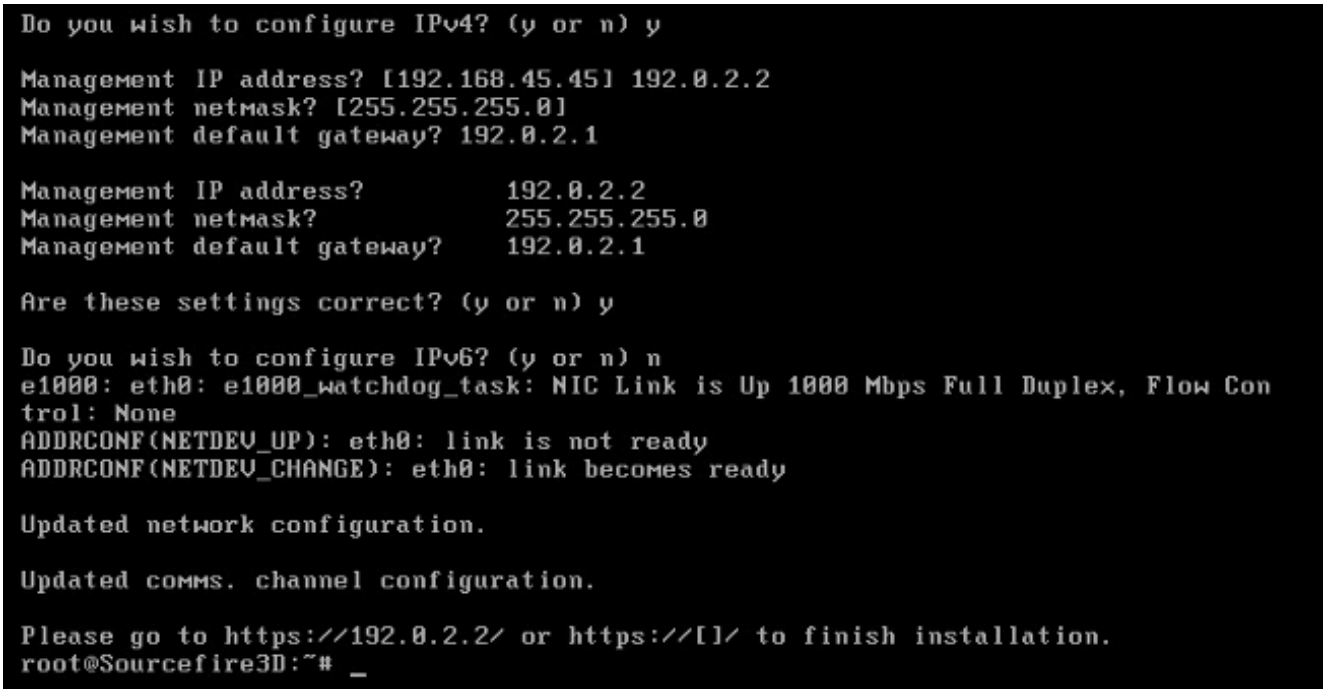
```
admin@Sourcefire3D:~$ sudo su -
Password:
```

3. Per iniziare la configurazione di rete, immettere lo script **configure-network** come root.

```
root@Sourcefire3D:~# configure-network

Do you wish to configure IPv4? (y or n) y
```

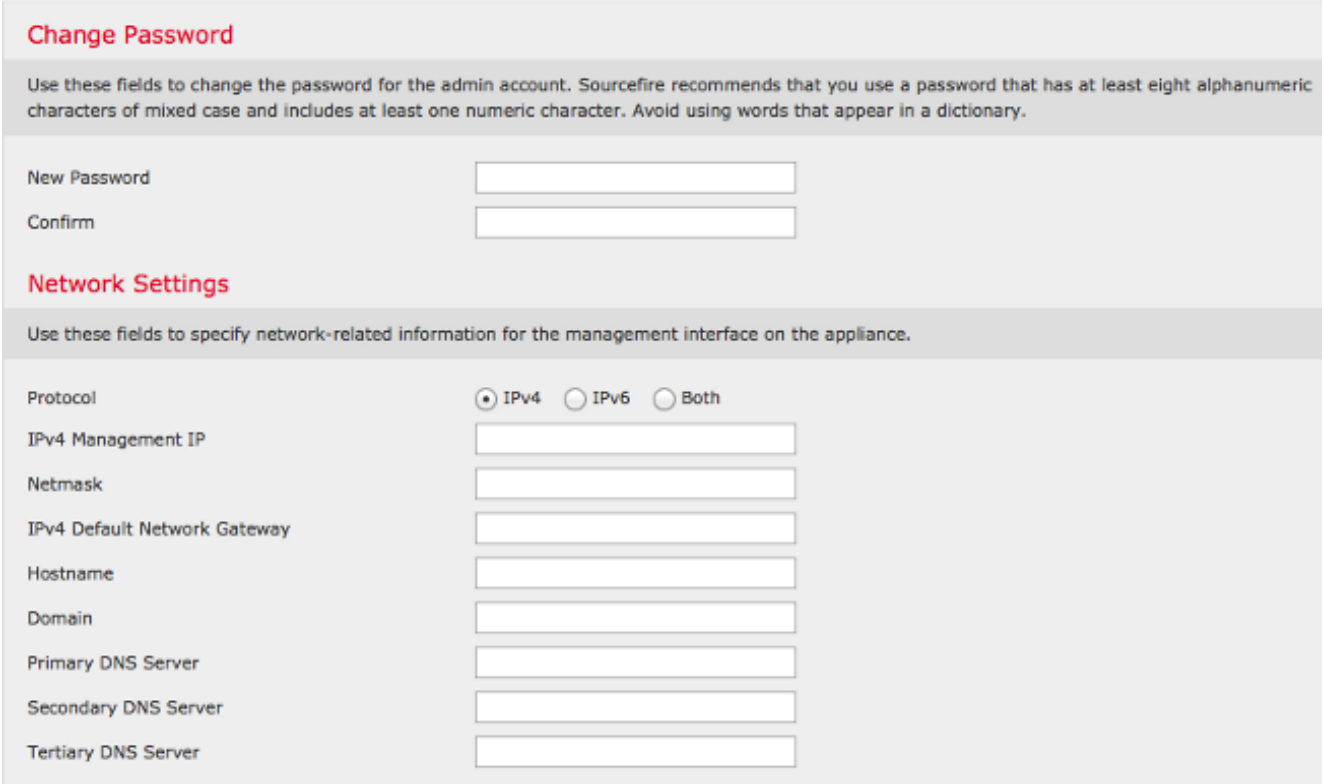
Verrà richiesto di specificare un indirizzo IP di gestione, una netmask e un gateway predefinito. Una volta confermate le impostazioni, il servizio di rete viene riavviato. Di conseguenza, l'interfaccia di gestione si interrompe e poi ritorna.



Esegui installazione iniziale

1. Dopo aver configurato le impostazioni di rete, aprire un browser Web e individuare l'indirizzo IP configurato tramite HTTPS (in questo esempio, all'indirizzo https://192.0.2.2). Se richiesto, autenticare il certificato SSL predefinito. Per accedere, usare queste credenziali:Per la versione 5.x Username: **admin**Password: **Sourcefire**Per la versione 6.x e successiveUsername: **admin**Password: **Admin123**
2. Sullo schermo seguente, tutte le sezioni di configurazione GUI sono facoltative ad eccezione della modifica della password e dell'accettazione dei termini del servizio. Se le informazioni sono note, si consiglia di utilizzare l'installazione guidata per semplificare la configurazione iniziale di Management Center. Una volta configurata, fare clic su **Apply** (Applica) per applicare la configurazione al Management Center e ai dispositivi registrati. Di seguito è riportata una breve panoramica delle opzioni di configurazione.**Cambia password:** Consente di modificare la password per l'account amministratore predefinito. È necessario modificare la password. **Impostazioni di rete:** Consente di modificare le impostazioni di rete IPv4 e IPv6 configurate in precedenza per l'interfaccia di gestione dell'accessorio o della macchina virtuale.**Impostazioni ora:** È consigliabile sincronizzare il centro di gestione con una fonte NTP affidabile. I sensori IPS possono essere configurati tramite criteri di sistema per sincronizzare l'ora con il centro di gestione. L'ora e il fuso orario possono essere impostati manualmente.**Importazioni aggiornamento regole ricorrenti:** Abilitare gli aggiornamenti ricorrenti delle regole Snort e installarli ora durante l'installazione iniziale.**Aggiornamenti geolocalizzazione ricorrenti:** Abilita gli aggiornamenti ricorrenti delle regole di geolocalizzazione e facoltativamente installa ora durante la configurazione iniziale.**Backup automatici:** Pianificare backup di configurazione automatici.**Impostazioni licenza:** Aggiungere la licenza per le funzionalità.**Registrazione dispositivo:** Consente di aggiungere, concedere in licenza e applicare policy di controllo dell'accesso iniziali ai dispositivi

preregistrati. Il nome host/indirizzo IP e la chiave di registrazione devono corrispondere all'indirizzo IP e alla chiave di registrazione configurati nel modulo FirePOWER IPS.**Contratto di licenza con l'utente finale:** È necessaria l'accettazione del Contratto.



Informazioni correlate

- [Guida rapida virtuale di Firepower Management Center per VMware, versione 6.0]
- [Documentazione e supporto tecnico – Cisco Systems]