Despliegue del centro de administración de FireSIGHT en VMware ESXi

Contenido

Introducción

Este documento describe la configuración inicial de un centro de administración de FireSIGHT (también conocido como centro de la defensa) que los funcionamientos en VMware ESXi. Un centro de administración de FireSIGHT permite que usted maneje uno o más dispositivos de la potencia de fuego, dispositivos de Viirtual del sistema de prevención de intrusiones de la última generación (NGIPS), y dispositivo de seguridad adaptante (ASA) con los servicios de la potencia de fuego.

> Nota: Este documento es un suplemento de la guía y del guía del usuario de instalación del sistema de FireSIGHT. Para una configuración de ESXi y una pregunta específicas del troubleshooting, refiera al Knowledge Base y a la documentación de VMware.

Prerrequisitos

Componentes Utilizados

La información sobre este documento se basa en estas Plataformas:

- Centro de administración de Cisco FireSIGHT
- Dispositivo virtual del centro de administración de Cisco FireSIGHT
- VMware ESXI 5.0

En este documento, un “dispositivo” refiere a estas Plataformas:

- Dispositivos de las 7000 Series de la potencia de fuego de Sourcefire y dispositivos de las 8000 Series
- Dispositivos virtuales de Sourcefire NGIPS para VMware ESXi
- 5500-X Series de Cisco ASA con el servicio de la potencia de fuego

La información que contiene este documento se creó a partir de los dispositivos en un ambiente

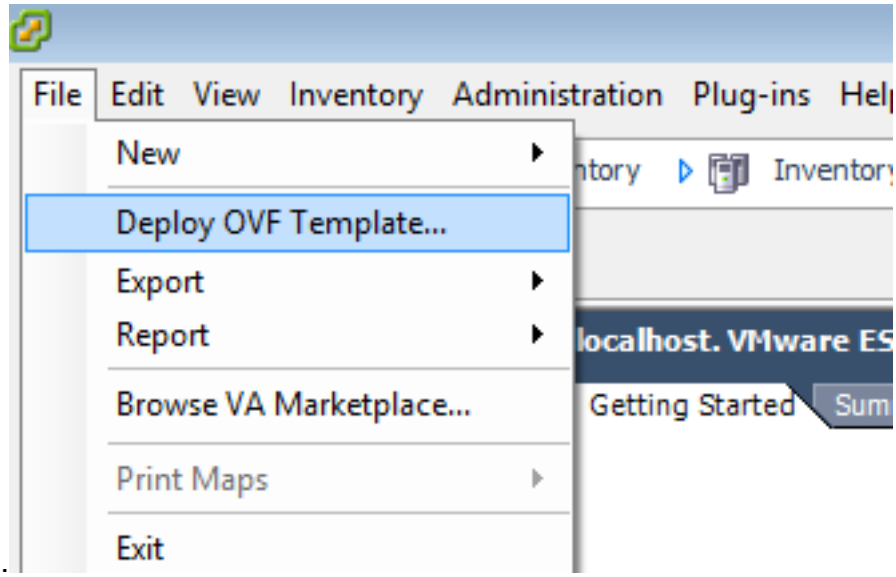
de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configuración

Despliegue una plantilla OVF

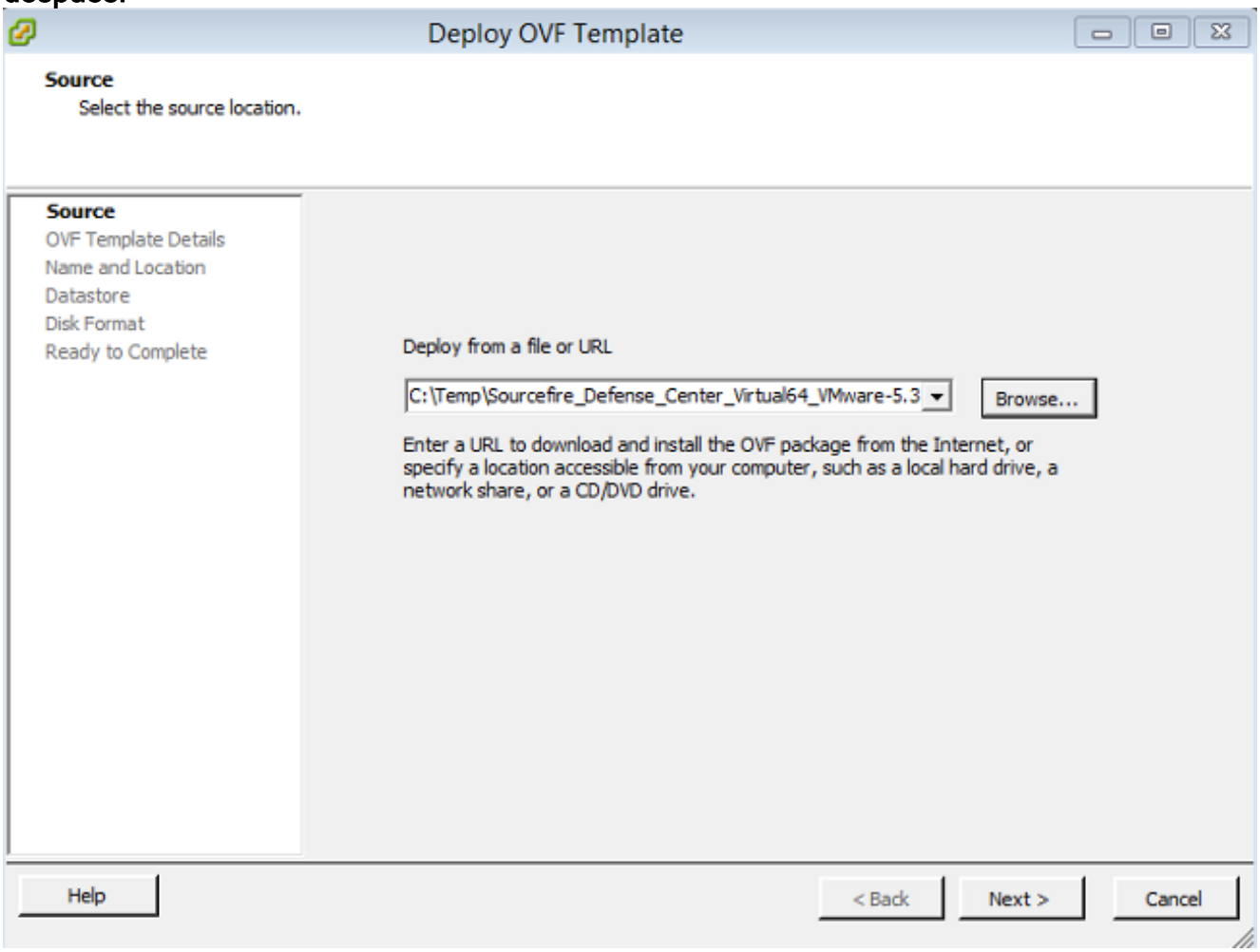
1. Descargue el **dispositivo virtual del centro de administración de Cisco FireSIGHT del** sitio del soporte y de las descargas de Cisco.
2. Extraiga el contenido del archivo de `tar.gz a un` directorio local.
3. Conecte con su servidor de ESXi con un **cliente del vSphere de VMware**.

4. Una vez que usted inicia sesión al cliente del vSphere, elija el **archivo > despliegan la**

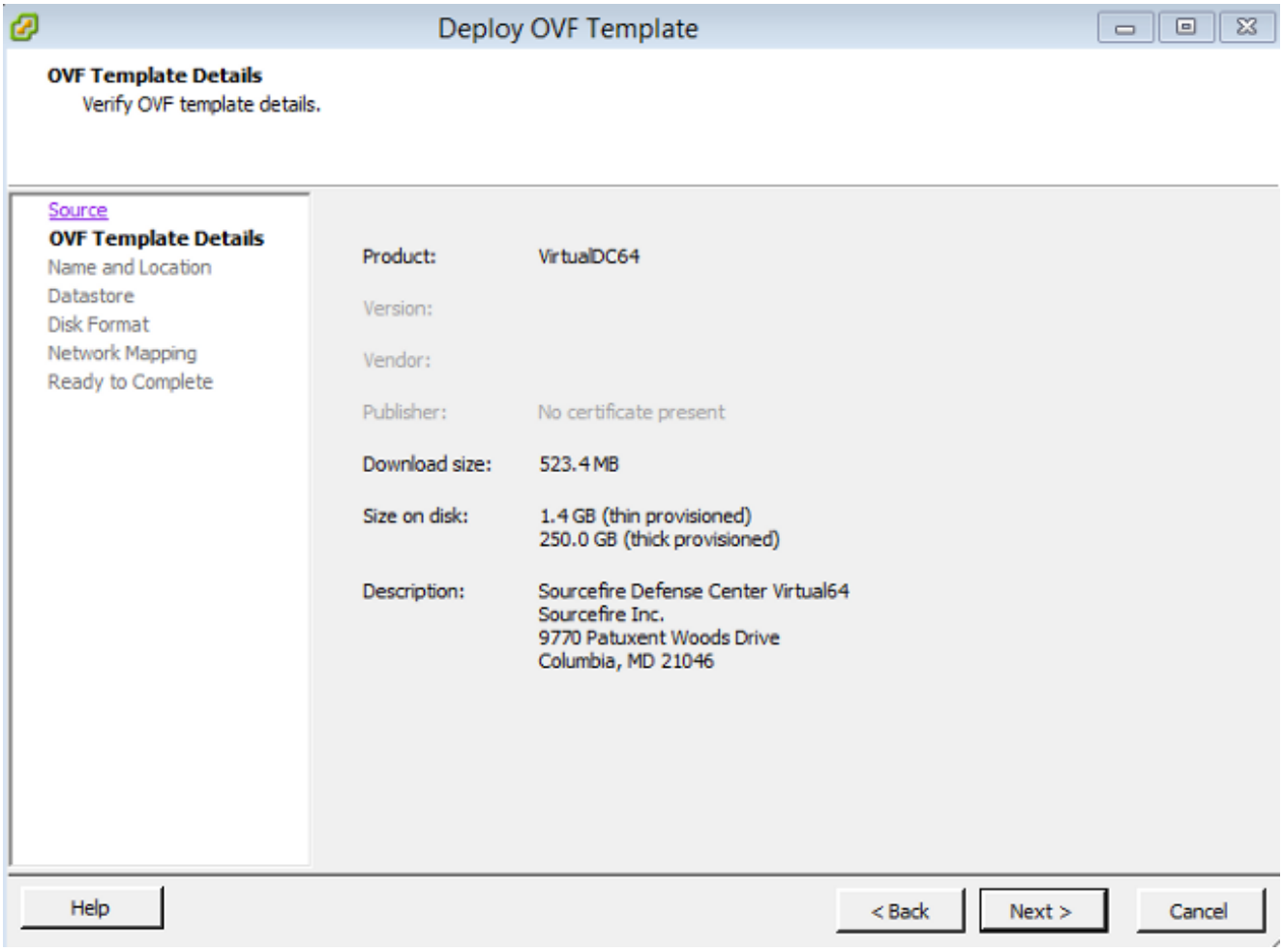


plantilla OVF.

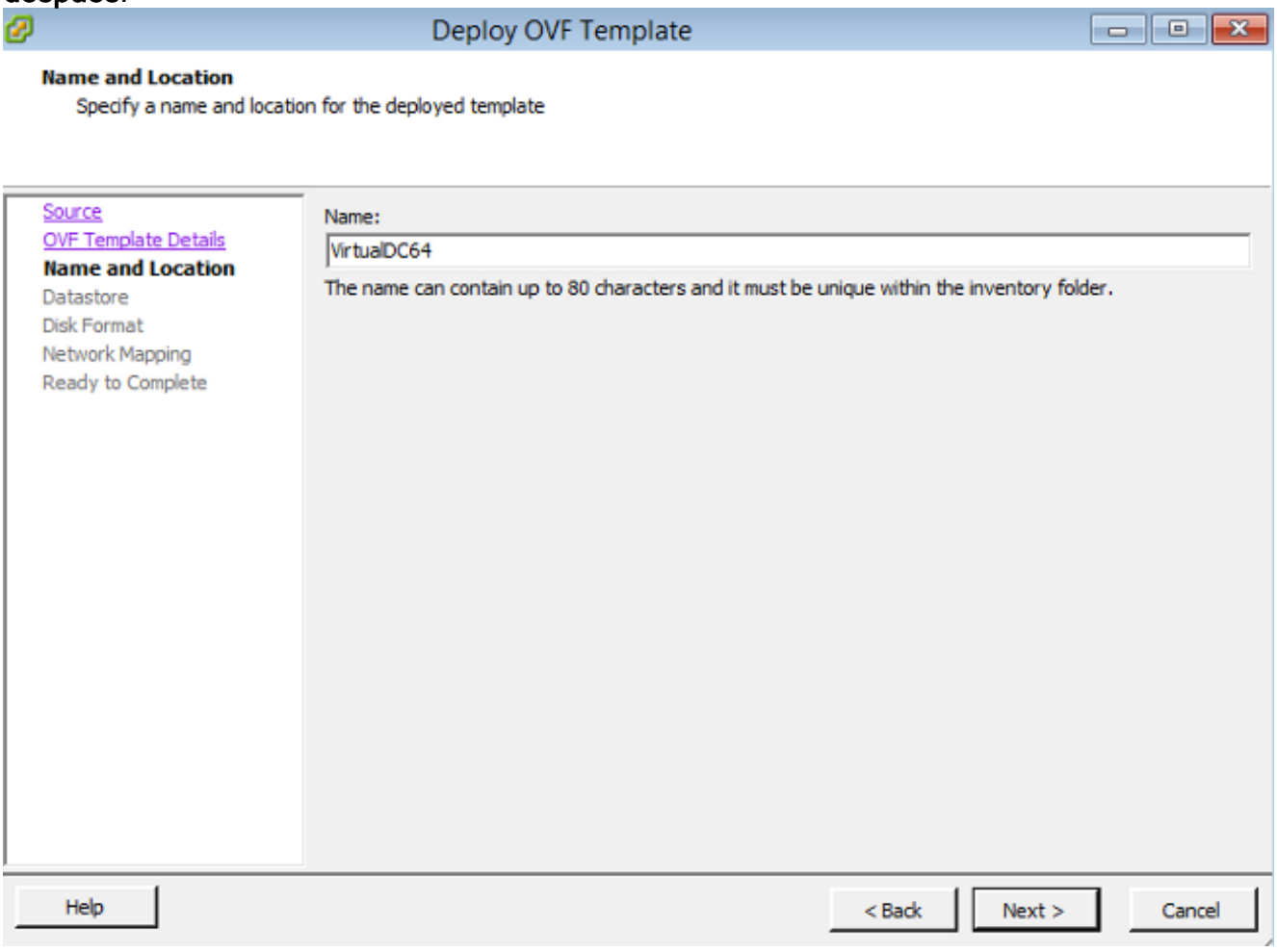
5. El tecleo **hojea** y localiza los archivos que usted extrajo en el paso 2. elige el archivo `Sourcefire_Defense_Center_Virtual64_VMware-ESXi-X.X.X-xxx.ovf` OVF y hace clic
después.



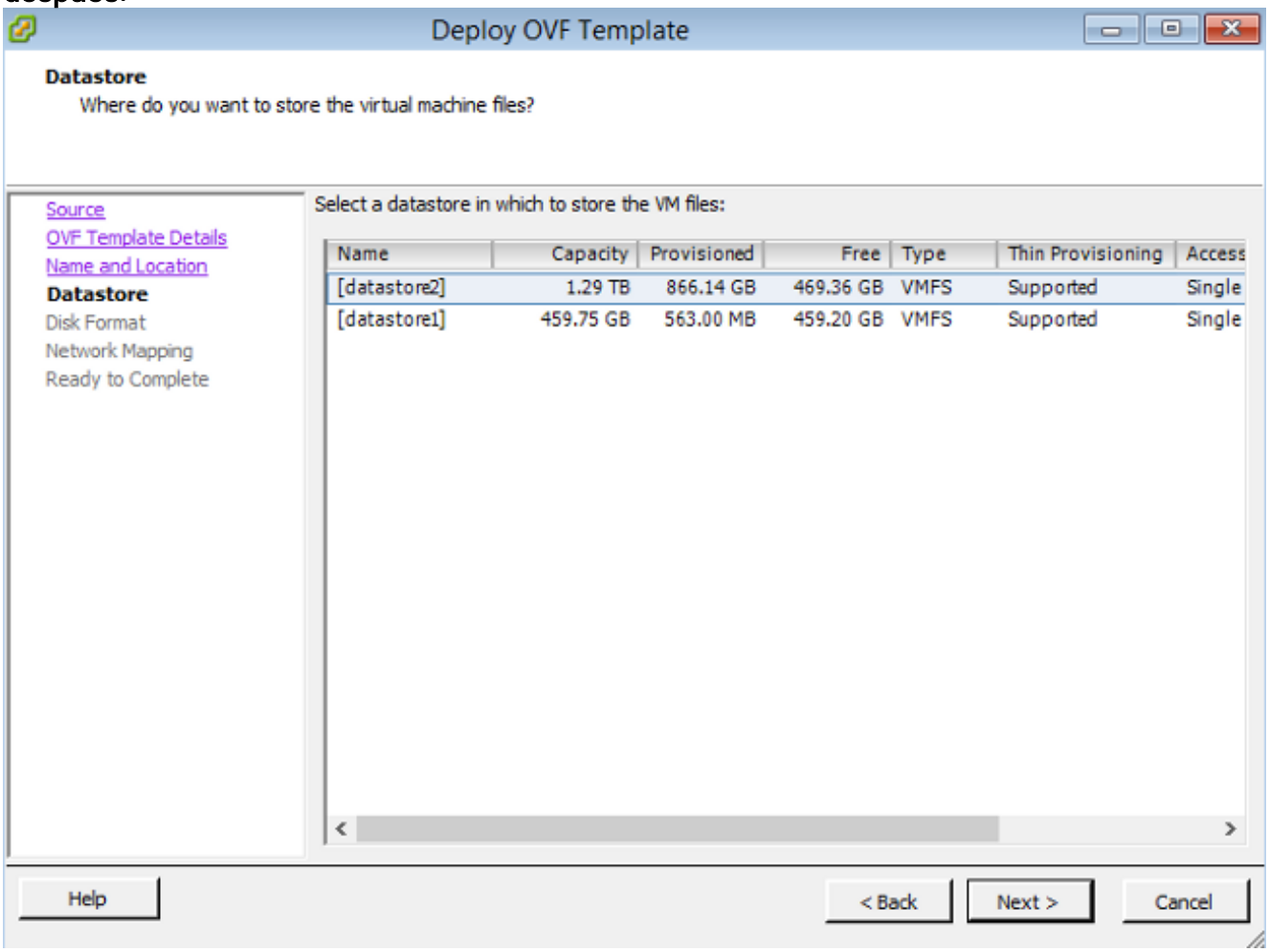
6. Sobre los **detalles de la plantilla OVF** defienda, haga clic **después** para validar las configuraciones
predeterminadas.



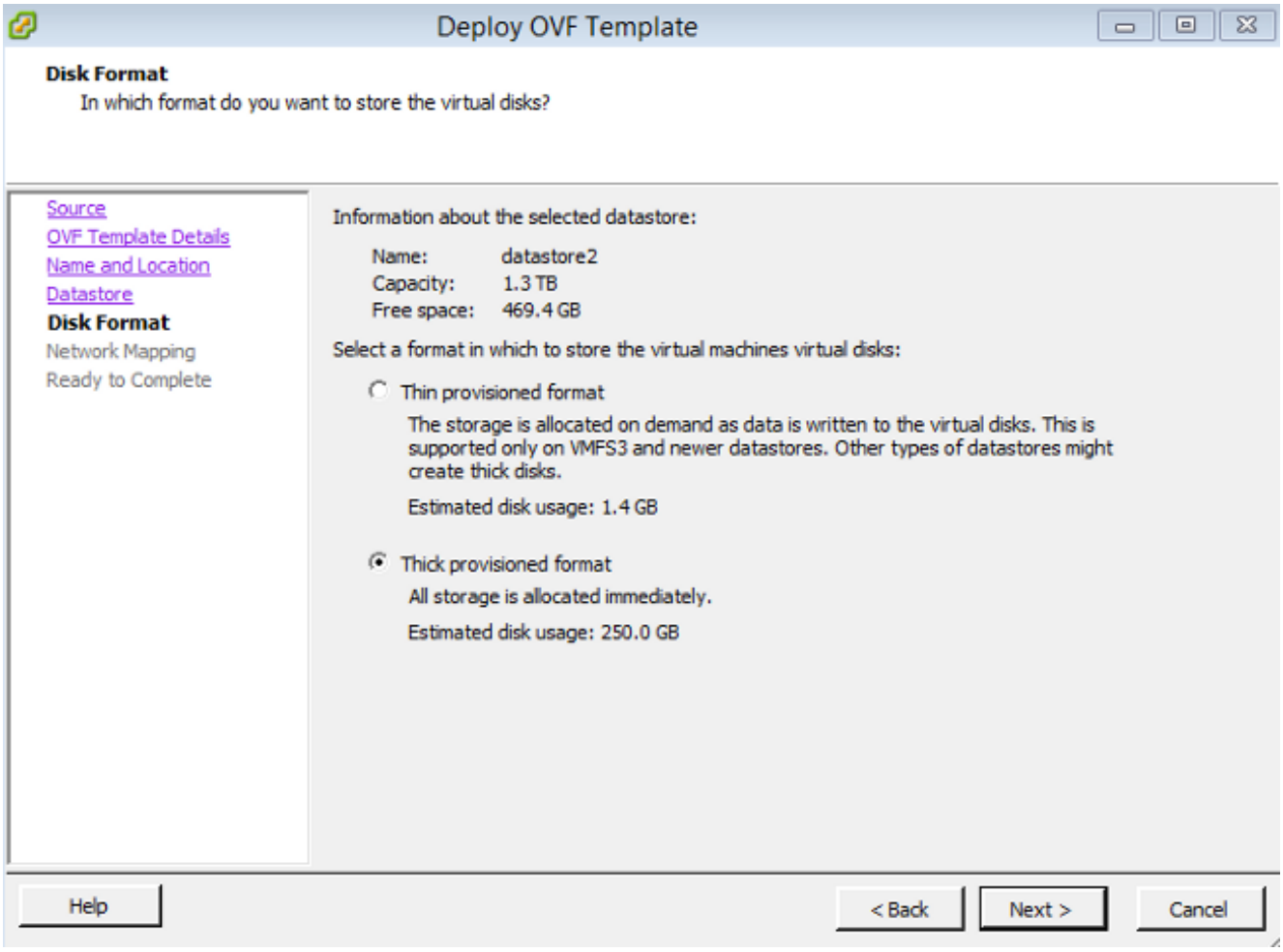
7. Proporcione un nombre para el centro de administración y haga clic **después**.



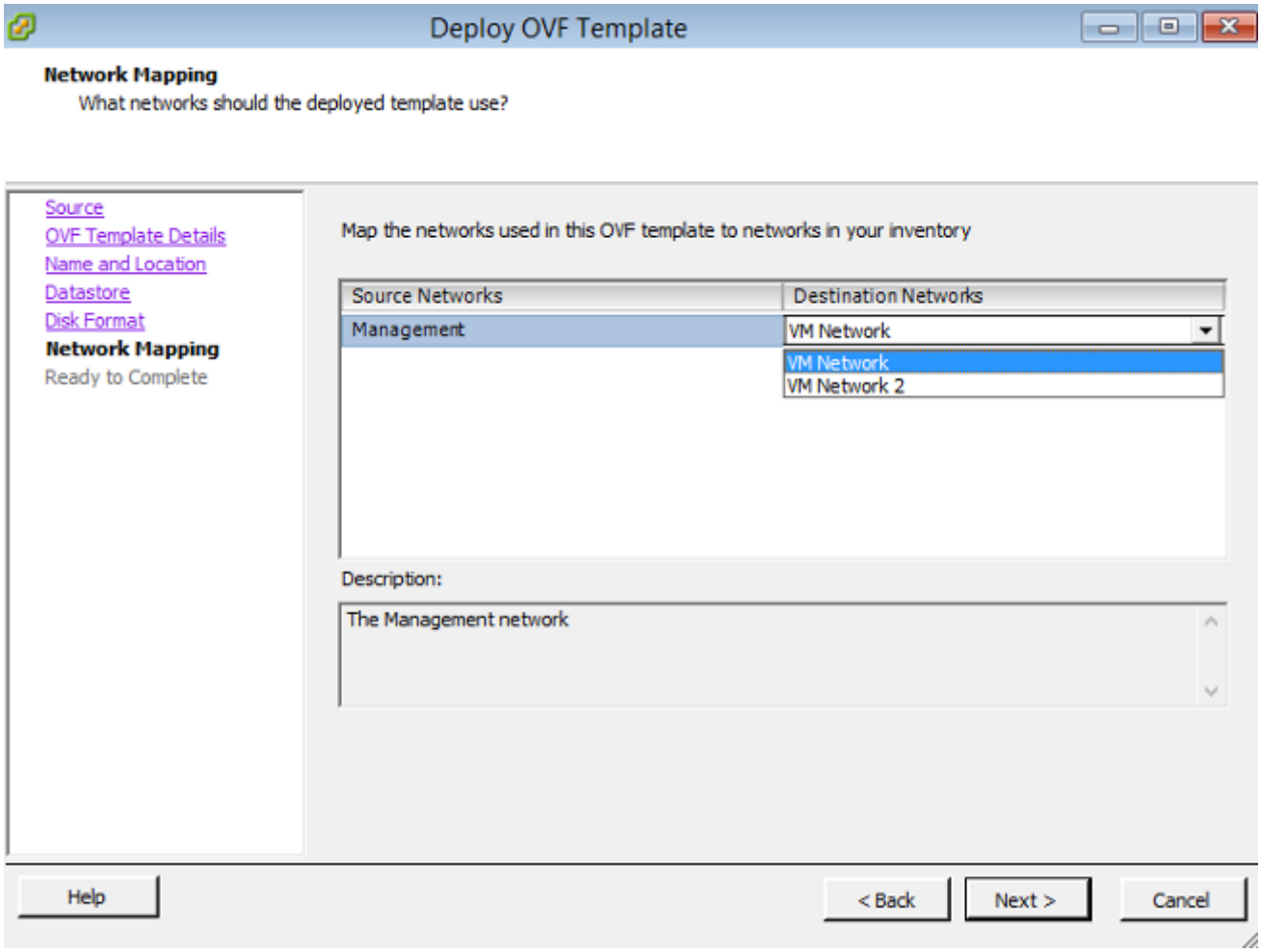
8. Elija un **Datastore** en el cual usted quiera crear la máquina virtual y hacer clic **después**.



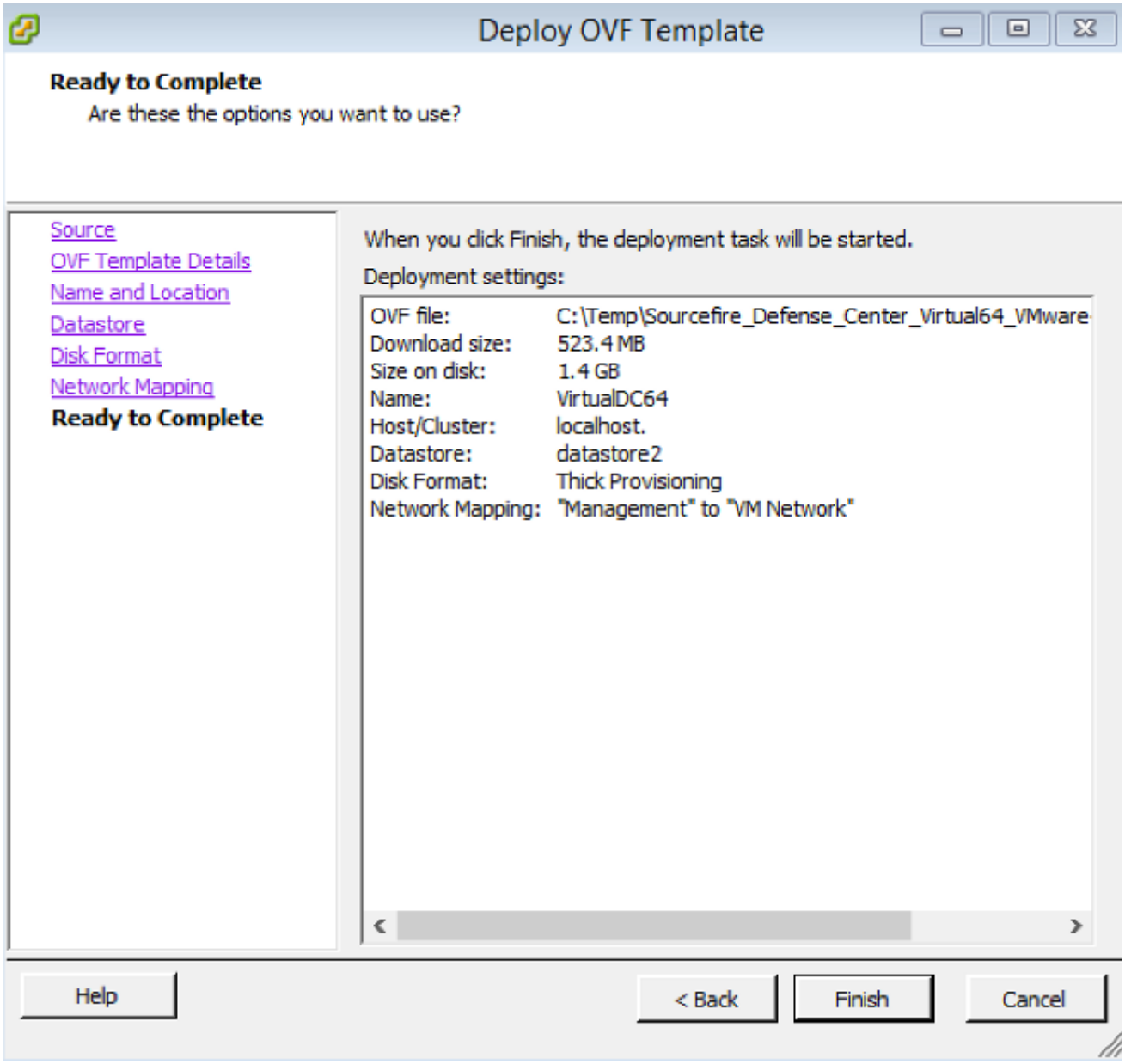
9. Haga clic el botón de radio **grueso del formato del aprovisionado** para el **formato del disco** y haga clic **después**. El formato grueso del aprovisionamiento afecta un aparato el espacio en disco necesario a la hora de crear un disco virtual, mientras que el formato fino del aprovisionamiento utiliza el espacio a
pedido.



10. En la sección de la **asignación de red**, asocie la interfaz de administración del centro de administración de FireSIGHT a una red de VMware y haga clic **después**.

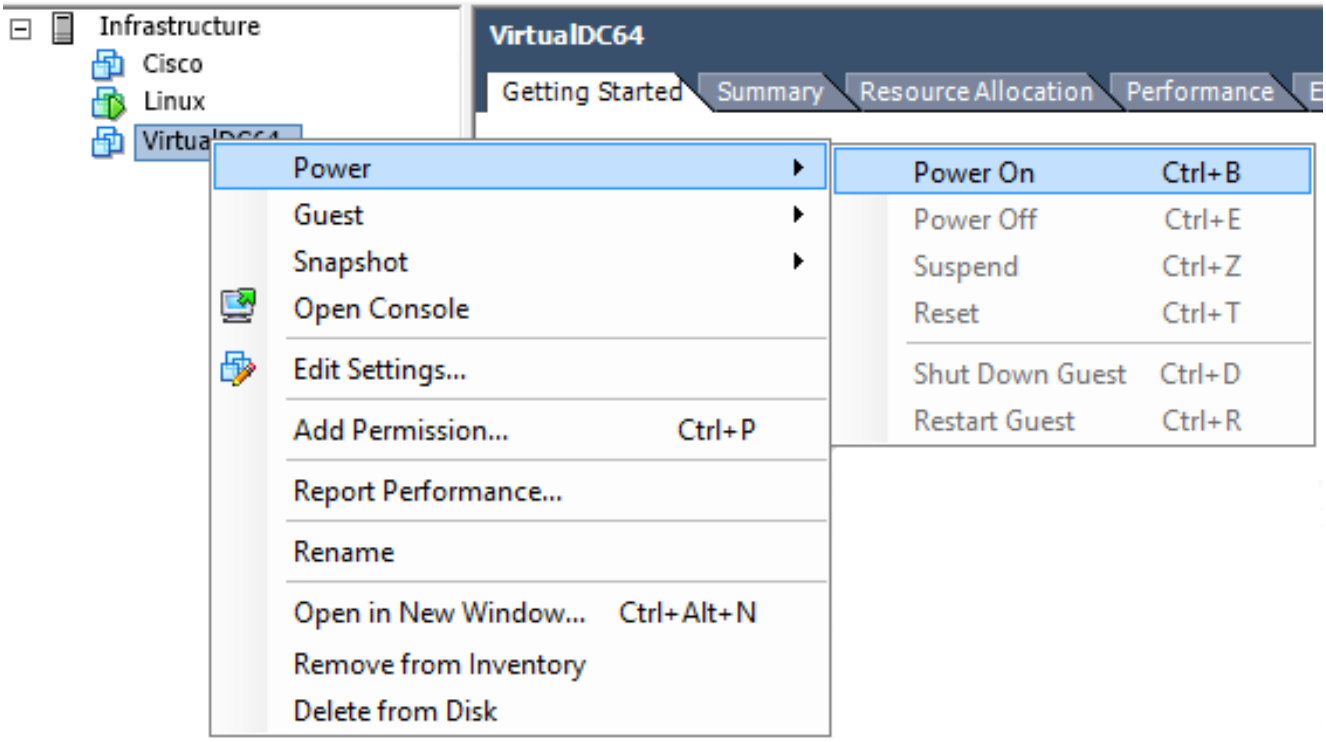


11. Clic en Finalizar para completar el despliegue de la plantilla OVF.

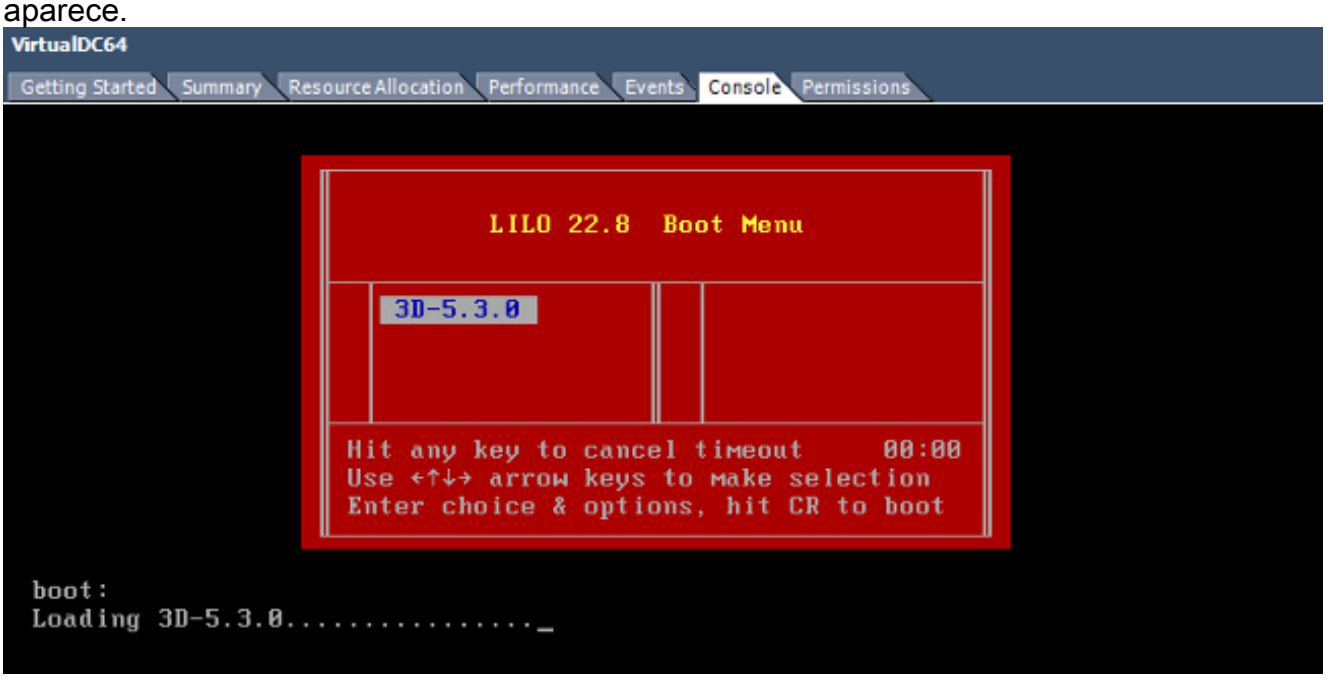


Poder encendido e inicialización completa

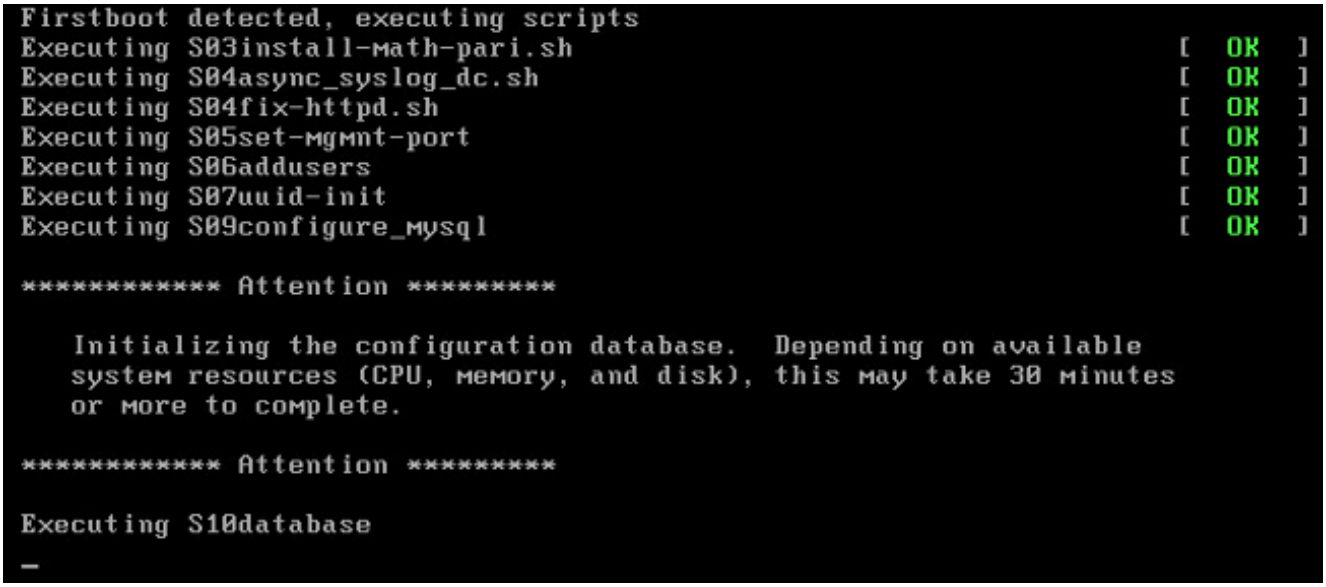
1. Navegue a la máquina virtual creada recientemente. Haga clic con el botón derecho del ratón Nombre del servidor y elija el **poder > el poder encendido** para iniciar encima del servidor por primera
   vez.



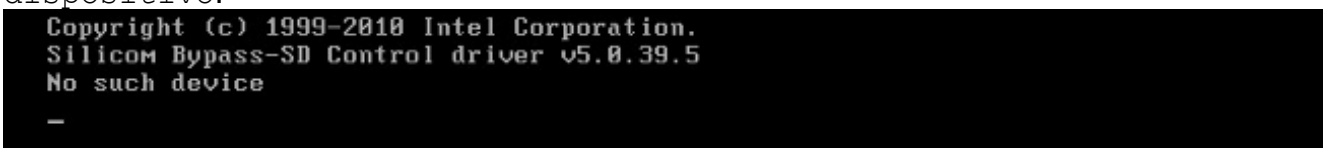
2. Navegue a la lengueta de la **consola** para monitorear la consola del servidor. El menú del inicio LILO
aparece.



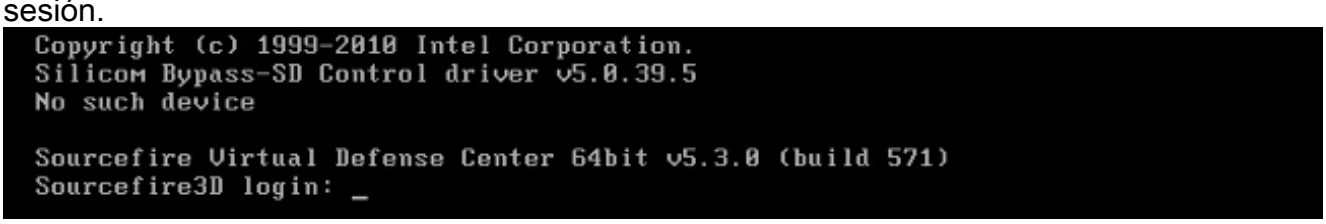
Una vez que la Verificación de datos BIOS es acertada, el proceso de inicialización comienza. El primer inicio pudo tardar el tiempo adicional para completar mientras que la base de datos de la configuración se inicializa por primera
vez.



Una vez completo, usted puede ser que vea un mensaje para `ningún tal dispositivo`.



3. Presione ENTER para conseguir un prompt de inicio de sesión.



Nota: Un mensaje "`ESCRIBE LO MISMO fallada. Manualmente poniendo a cero.`" puede aparecer después de que el sistema se inicie encima de por primera vez. Esto no indica un defecto, él indica correctamente que el driver del almacenamiento de VMware no soporta la `ESCRITURA EL MISMO` comando. El sistema visualiza este mensaje, y procede con un comando del retraso de realizar la misma operación.

Configure las configuraciones de red

1. En el prompt de inicio de sesión `Sourcefire3D`, utilice estas credenciales para iniciar sesión: Para la versión 5.xNombre de usuario: **admin**Contraseña **Sourcefire**Para la versión 6.x y posteriorNombre de usuario: **admin**Contraseña **Admin123**Consejo: Usted podrá cambiar la contraseña predeterminada en el proceso de la configuración inicial en el GUI.
2. La configuración inicial de la red se hace con un script. Usted necesita ejecutar el script como `usuario raíz`. Para conmutar al `usuario raíz`, ingrese el **comando su - del sudo** junto con la contraseña **Sourcefire o Admin123** `(para 6.x)`. Ejercite la precaución cuando está registrado en la línea de comando del centro de administración como usuario raíz. `admin@Sourcefire3D:~$ sudo su -`
`Password:`
3. Para comenzar la configuración de red, ingrese el script de la configuración-**red** como `raíz`.

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

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

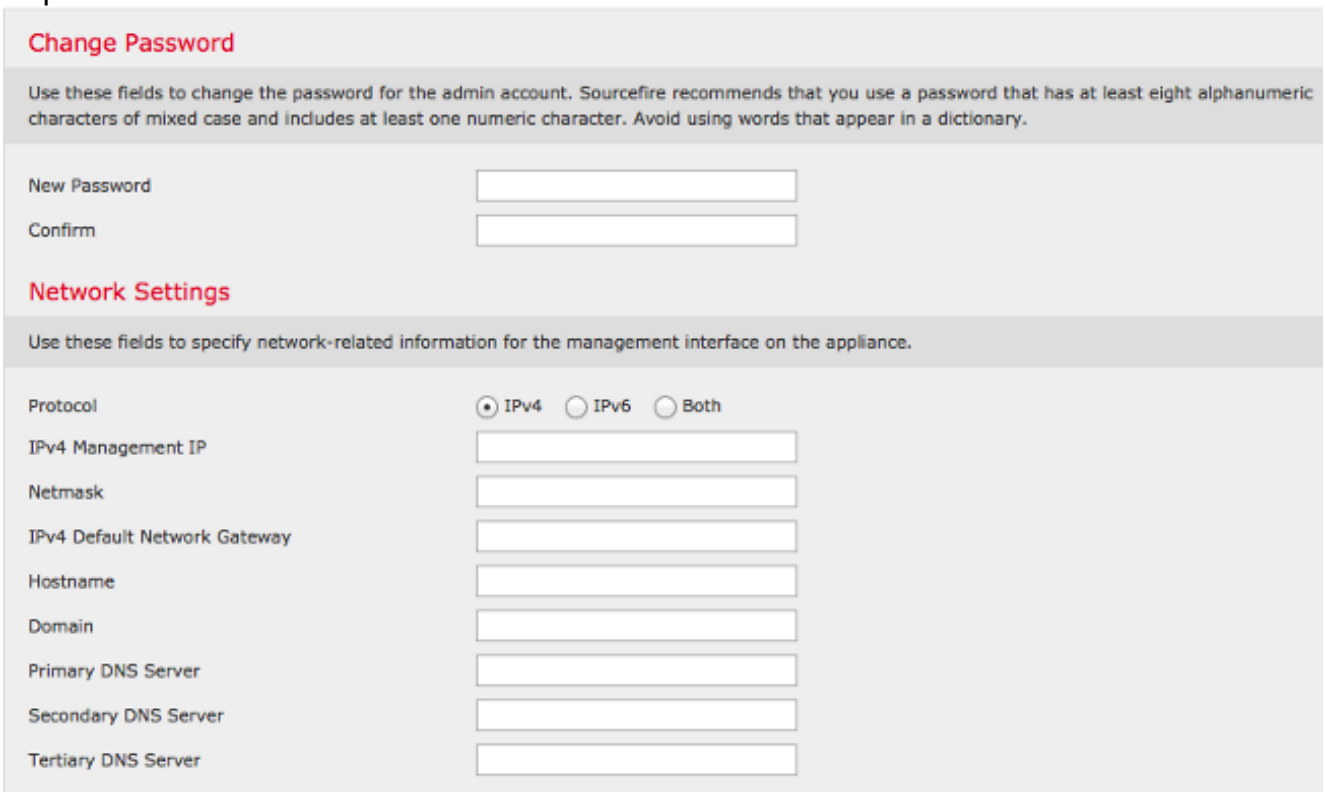
Le pedirán proporcionar un IP Address de administración, el netmask, y el default gateway. Una vez que usted confirma las configuraciones, el servicio de red recomienza. Como consecuencia, la interfaz de administración va abajo y después se vuelve.

```
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 Con
trol: 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:~# _
```

Realice la configuración inicial

1. Después de que se configuren las configuraciones de red, abra a un buscador Web y hojee al IP configurado vía HTTPS (https://192.0.2.2 en este ejemplo). Autentique el certificado del valor por defecto SSL si está indicado. Utilice estas credenciales para iniciar sesión:Para la versión 5.x Nombre de usuario: **admin**Contraseña **Sourcefire**Para la versión 6.x y posteriorNombre de usuario: **admin**Contraseña **Admin123**
2. En la pantalla que sigue, todas las secciones de Configuración del GUI son opcionales a excepción del cambio de la contraseña y de la aceptación de los términos del servicio. Si se sabe la información, se recomienda para utilizar al asistente para la configuración para simplificar la configuración inicial del centro de administración. Una vez que está configurado, el tecleo **se aplica** para aplicar la configuración al centro de administración y a los dispositivos registrados. Una breve descripción de las opciones de configuración es como sigue:**Contraseña del cambio:** Permite que usted cambie la contraseña para la cuenta de administración predeterminada. Se requiere para cambiar la contraseña. **Configuraciones de red:** Permite que usted modifique las configuraciones de red previamente configuradas del IPv4 y del IPv6 para la interfaz de administración del dispositivo o de la máquina virtual.**Configuraciones horarias:** Se recomienda que usted sincroniza el centro de administración con una fuente confiable NTP. Los sensores IPS se pueden configurar con la política del sistema para sincronizar su tiempo con el centro de administración. Opcionalmente, la hora y el huso horario de la visualización se pueden fijar manualmente.**Importaciones de la actualización de la regla que se repiten:** Habilite las actualizaciones de la regla del Snort que se repiten y instalelas opcionalmente ahora durante la configuración inicial.**Actualizaciones de Geolocation que se repiten:** Habilite las

actualizaciones de la regla del geolocation que se repiten y instalelas opcionalmente ahora durante la configuración inicial.**Respaldos automáticos:** Respaldos de la configuración automática del horario.**Configuraciones de la licencia:** Agregue la licencia de función.**Registro del dispositivo:** Permite que usted agregue, que autorice, y que aplique las directivas iniciales del control de acceso a los dispositivos preregistered. El nombre de host/la dirección IP y la clave del registro deben hacer juego la dirección IP y la clave del registro configuradas en el módulo ips de la potencia de fuego.**Acuerdo de licencia de usuario final:** La aceptación del EULA se
requiere.



Información Relacionada

- Guía de inicio rápido virtual del centro de administración de la potencia de fuego para VMware, versión 6.0
- Soporte Técnico y Documentación - Cisco Systems