Desenvolvimento do centro de gerenciamento de FireSIGHT em VMware ESXi

Índice

Introdução

Este documento descreve a instalação inicial de um centro de gerenciamento de FireSIGHT (igualmente conhecido como o centro da defesa) que corridas em VMware ESXi. Um centro de gerenciamento de FireSIGHT permite que você controle uns ou vários dispositivos de FirePOWER, dispositivos de Viirtual do sistema da prevenção de intrusão da próxima geração (NGIPS), e ferramenta de segurança adaptável (ASA) com serviços de FirePOWER.

> **Note**: Este documento é um suplemento do guia e do Guia do Usuário de instalação de sistema de FireSIGHT. Para uma pergunta específica da configuração e do Troubleshooting de ESXi, refira a base de conhecimento e a documentação de VMware.

Pré-requisitos

Componentes Utilizados

A informação neste documento é baseada nestas Plataformas:

- Centro de gerenciamento de Cisco FireSIGHT
- Dispositivo virtual do centro de gerenciamento de Cisco FireSIGHT
- VMware ESXI 5.0

Neste documento, um “dispositivo” refere estas Plataformas:

- Dispositivos do 7000 Series de Sourcefire FirePOWER e dispositivos do 8000 Series
- Dispositivos virtuais de Sourcefire NGIPS para VMware ESXi
- 5500-X Series de Cisco ASA com serviço de FirePOWER

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto

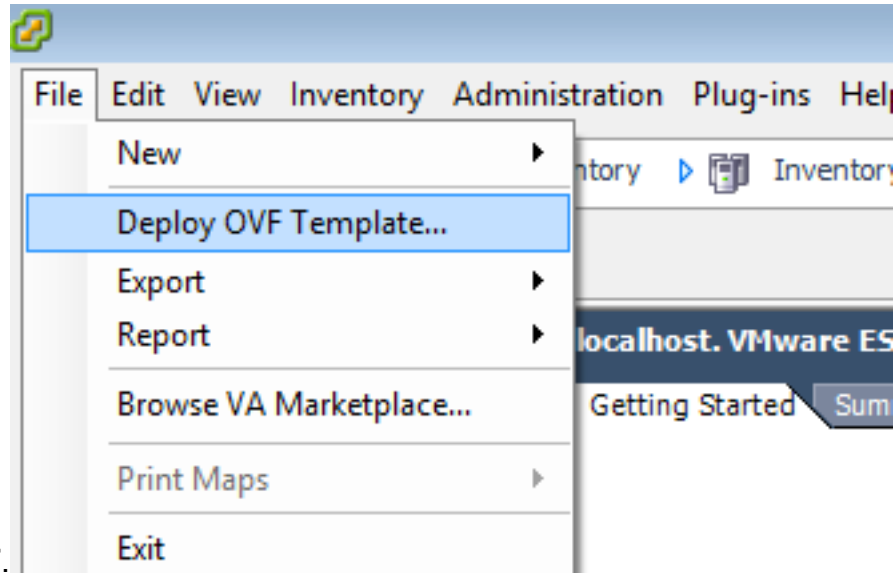
potencial de qualquer comando.

Configuração

Distribua um molde OVF

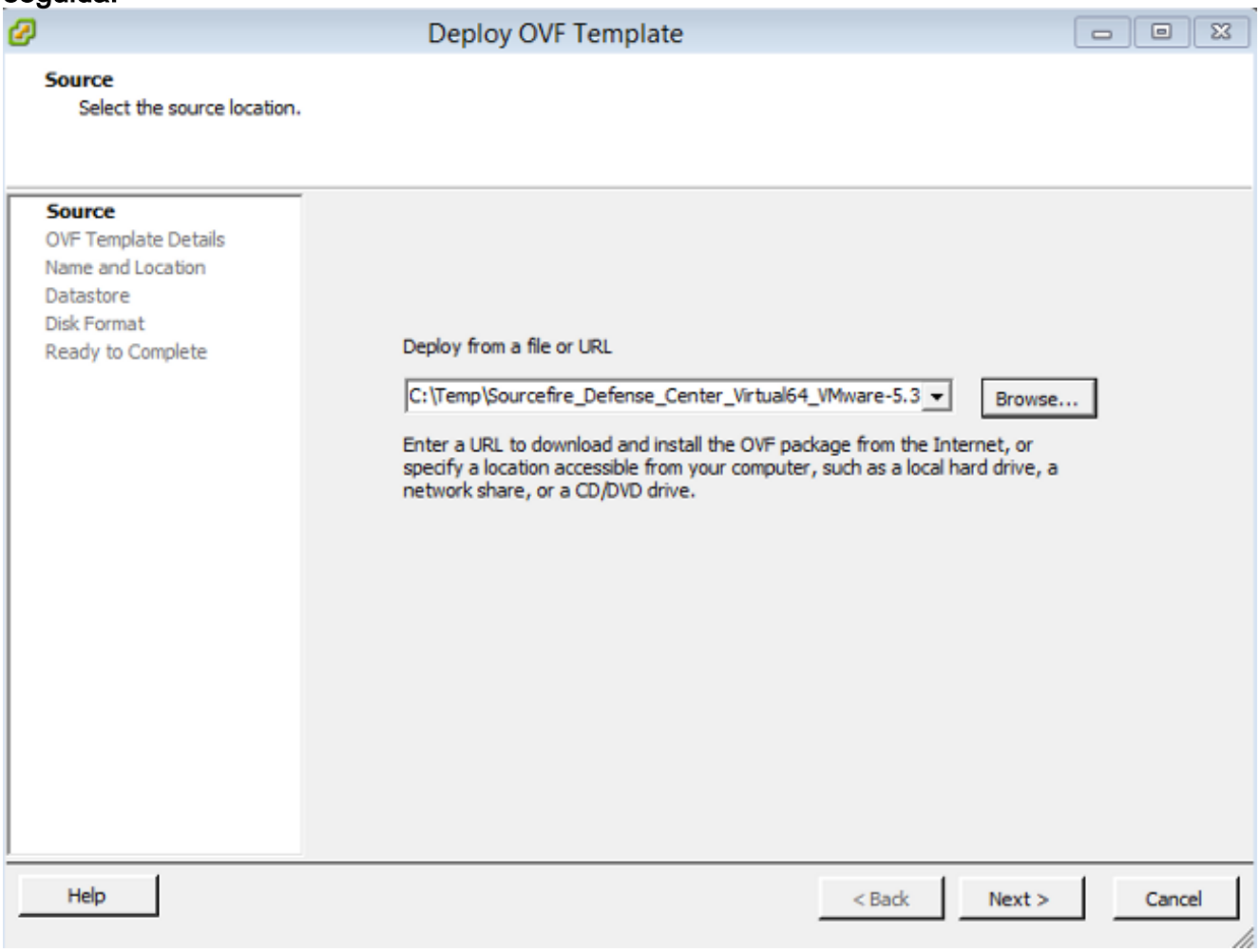
1. Transfira o **dispositivo virtual do centro de gerenciamento de Cisco FireSIGHT do** local do apoio & das transferências de Cisco.
2. Extraia os índices do arquivo de `tar.gz a um` diretório local.
3. Conecte a seu server de ESXi com um **cliente do vSphere de VMware**.

4. Uma vez que você entra ao cliente do vSphere, escolha o **arquivo > distribuem o molde**

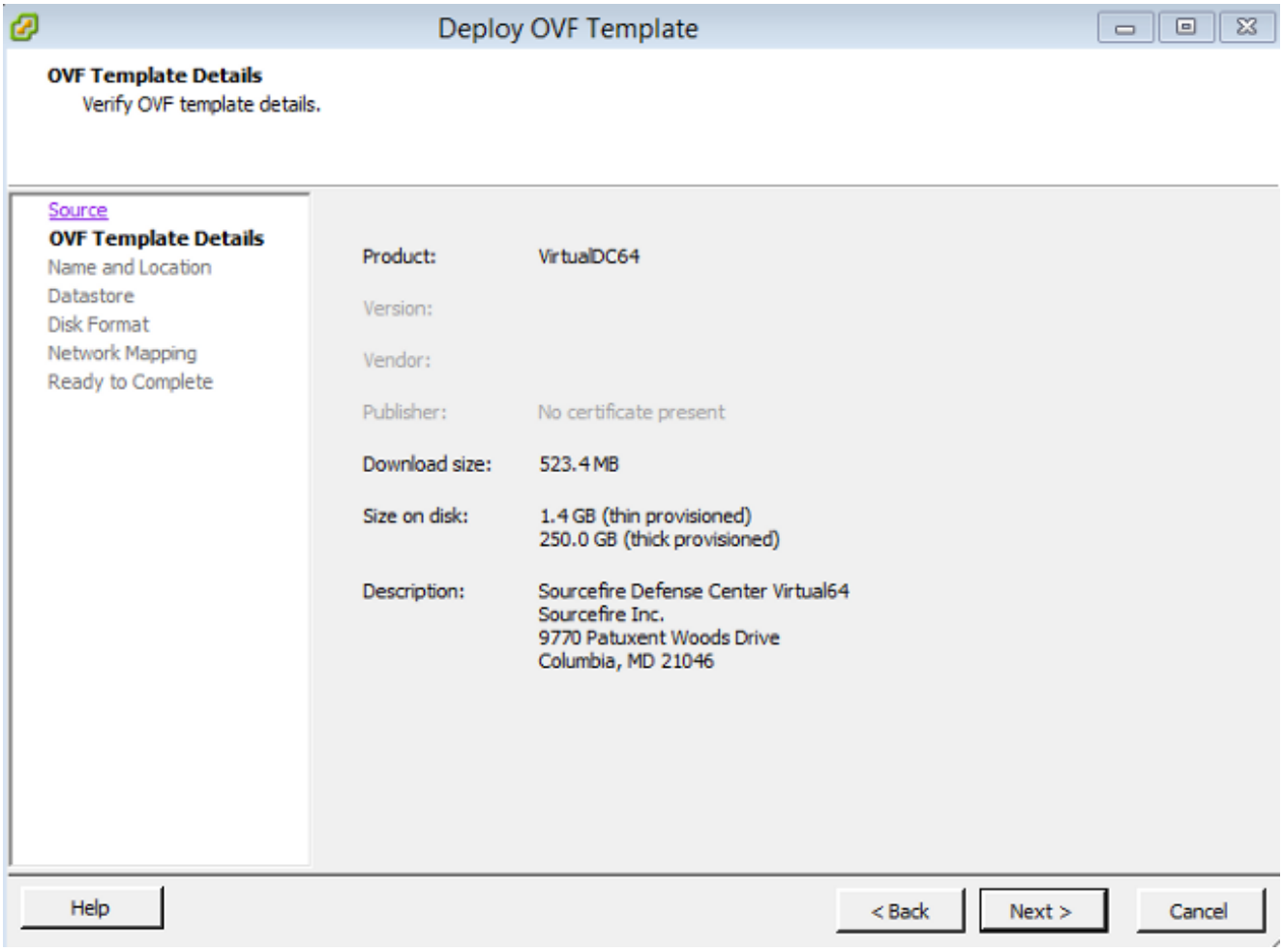


OVF.

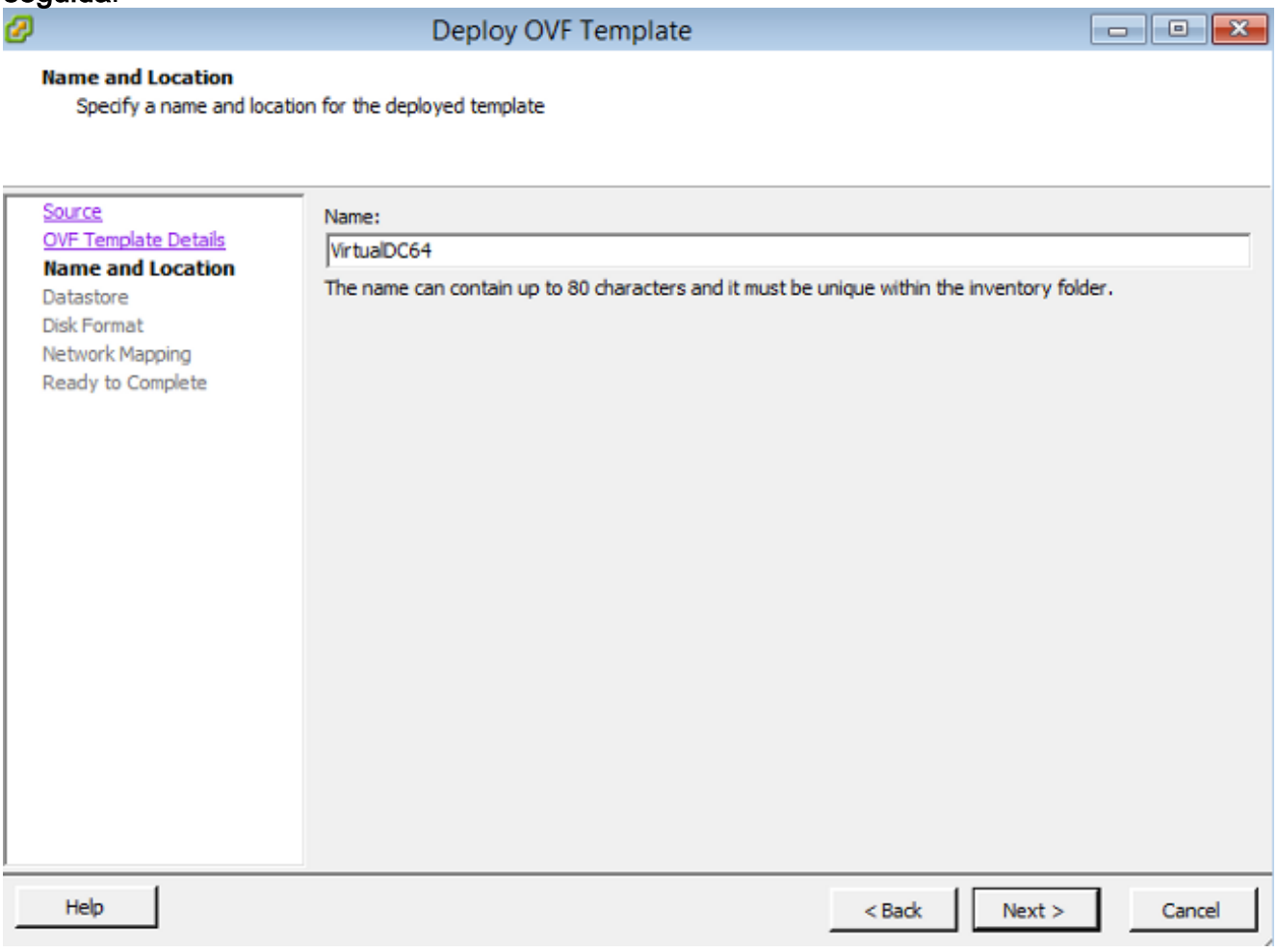
5. O clique **consulta** e encontra os arquivos que você extraiu em etapa 2. escolhe o arquivo `Sourcefire_Defense_Center_Virtual64_VMware-ESXi-X.X.X-xxx.ovf` OVF e o clica **em seguida.**



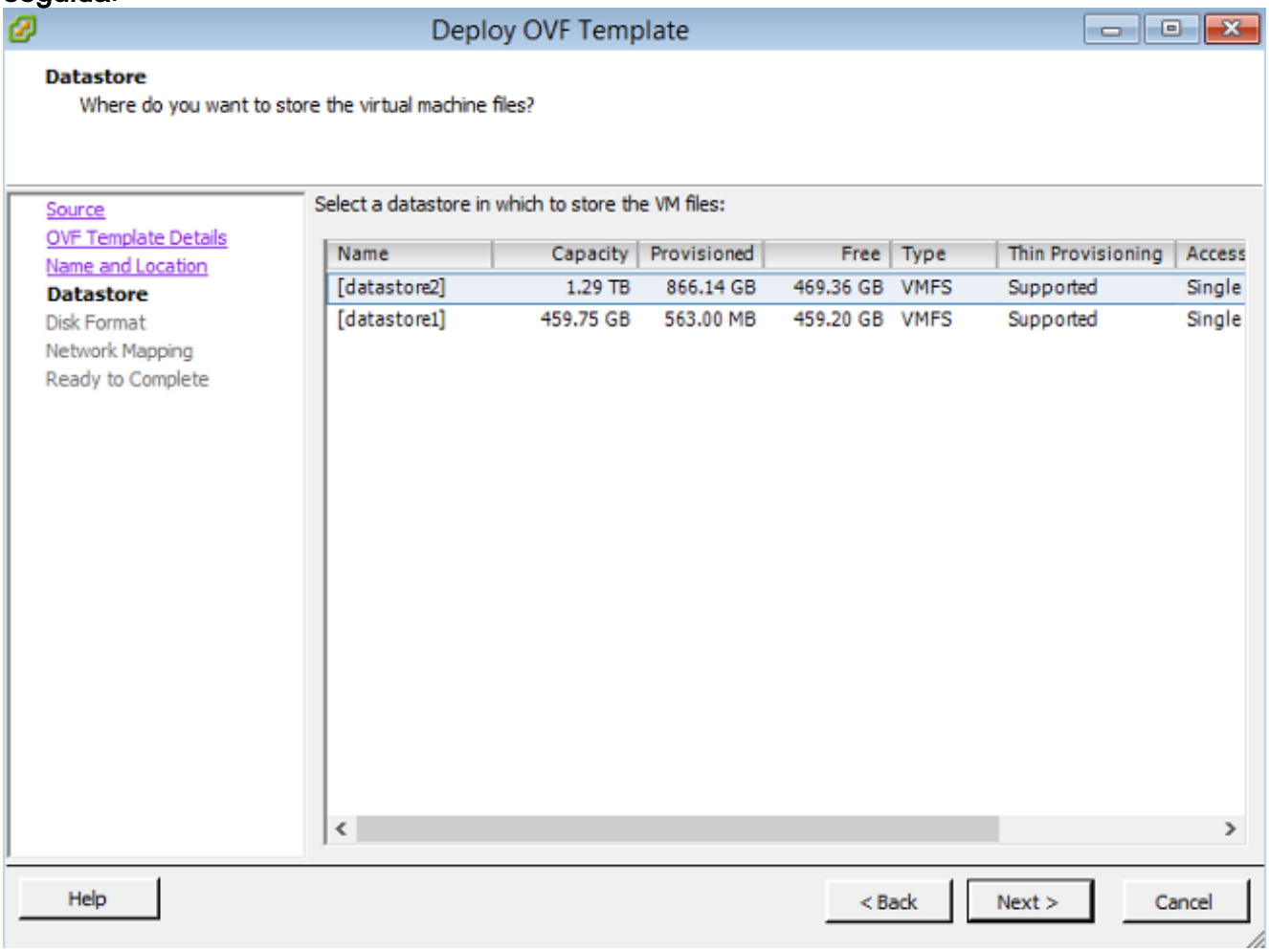
6. **Nos detalhes do molde OVF** selecione, clique **em seguida** a fim aceitar as configurações padrão.



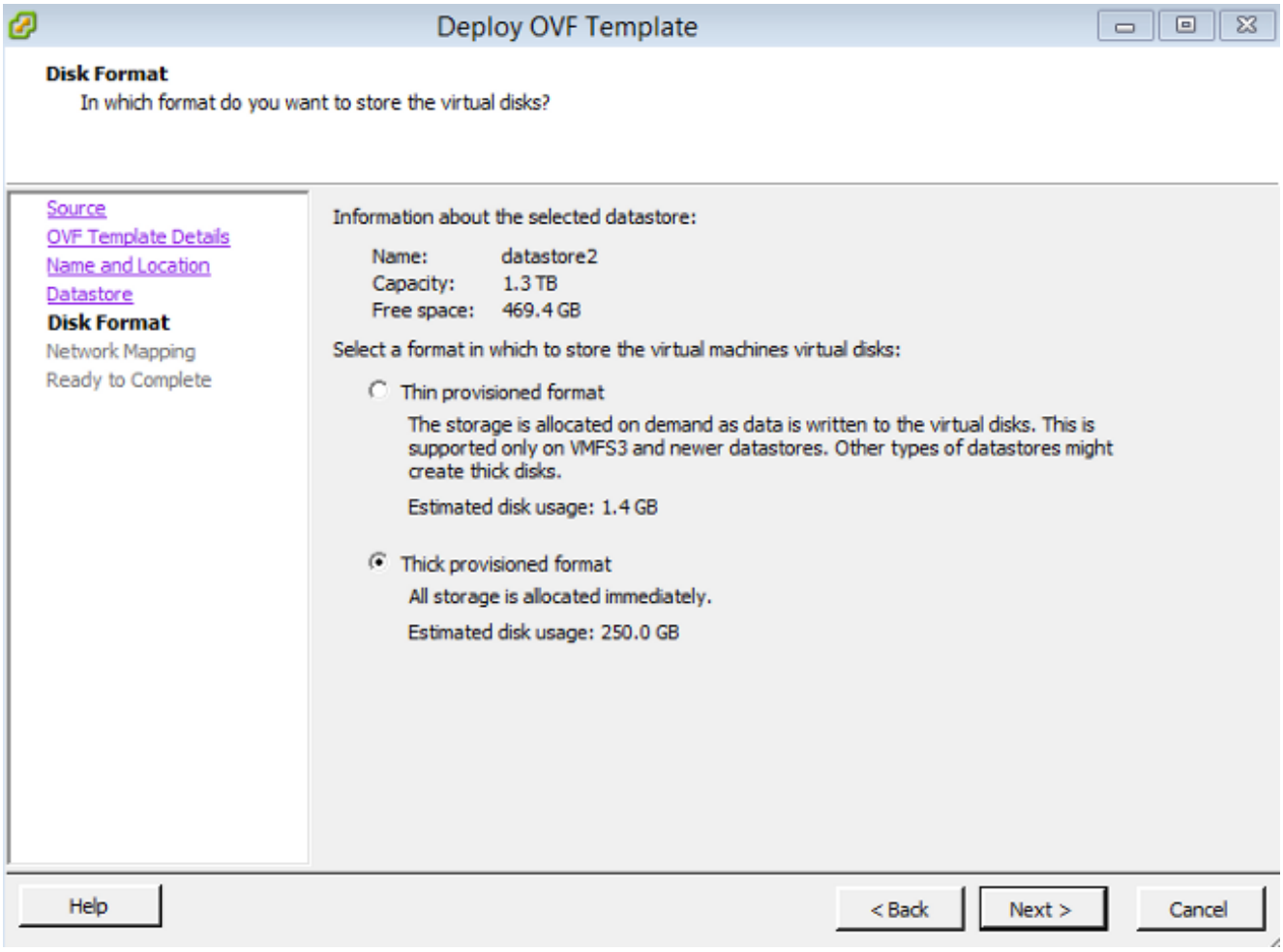
7. Forneça um nome para o centro de gerenciamento e clique-o em seguida.



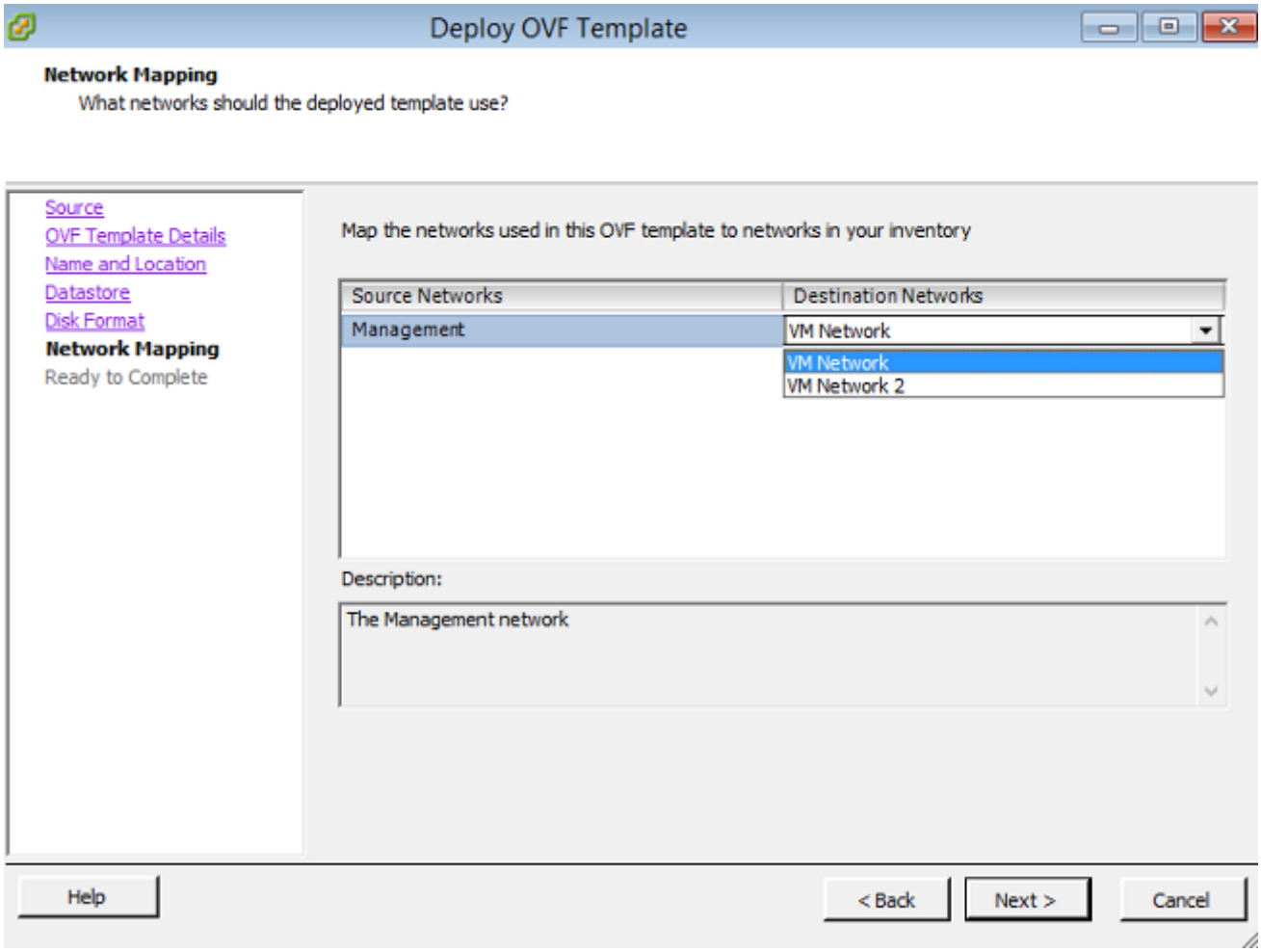
8. Escolha um **Datastore em** que você quer criar a máquina virtual e a clicar **em seguida**.



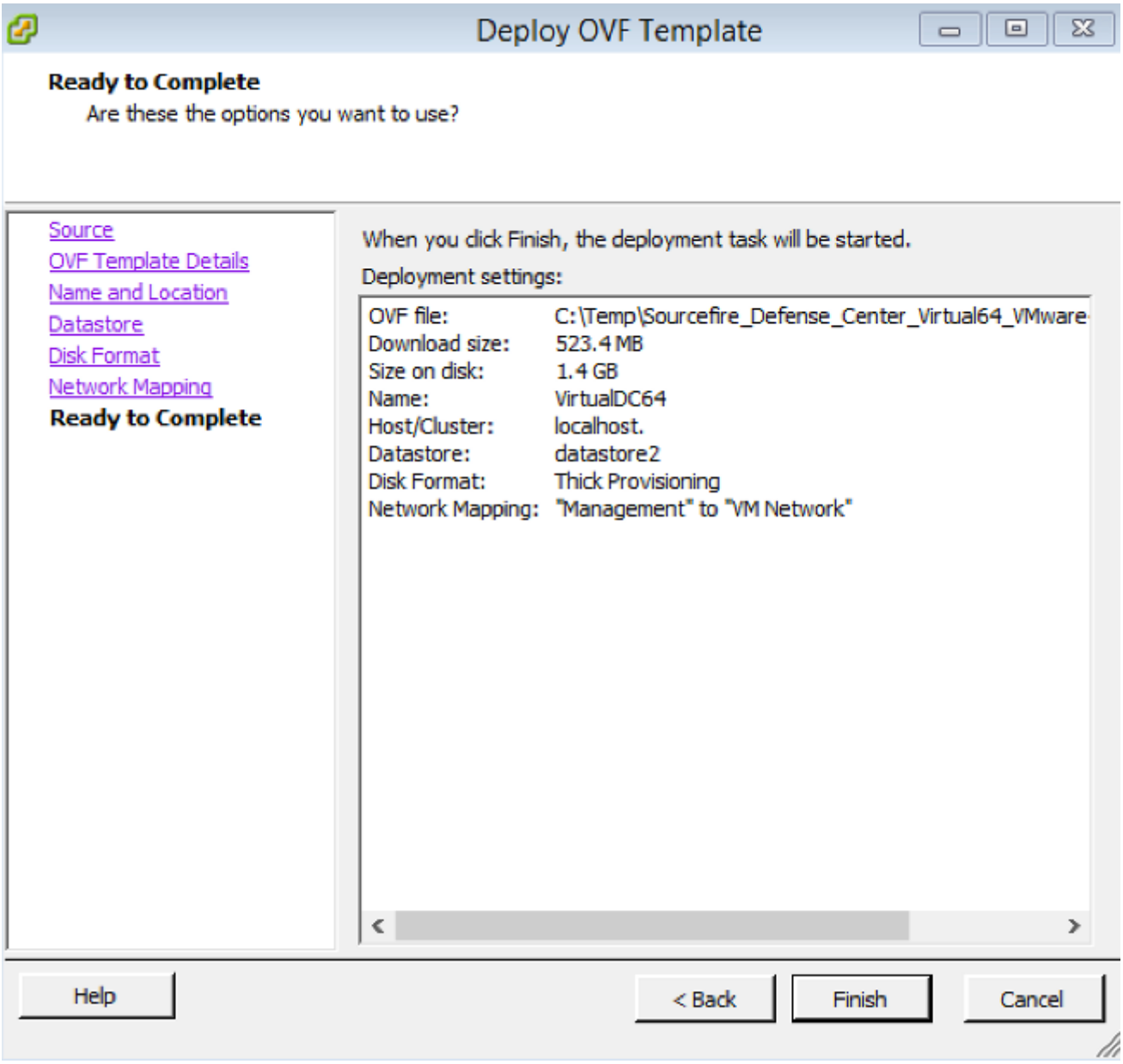
9. Clique o botão de rádio **fornecida grosso do formato** para o **formato do disco** e clique-o **em seguida**. O formato grosso do abastecimento atribui o espaço de disco necessário na altura de criar um disco virtual, visto que o formato fino do abastecimento usa o espaço por encomenda.



10. Na seção do **mapeamento de rede**, associe a interface de gerenciamento do centro de gerenciamento de FireSIGHT a uma rede de VMware e clique-a **em seguida**.

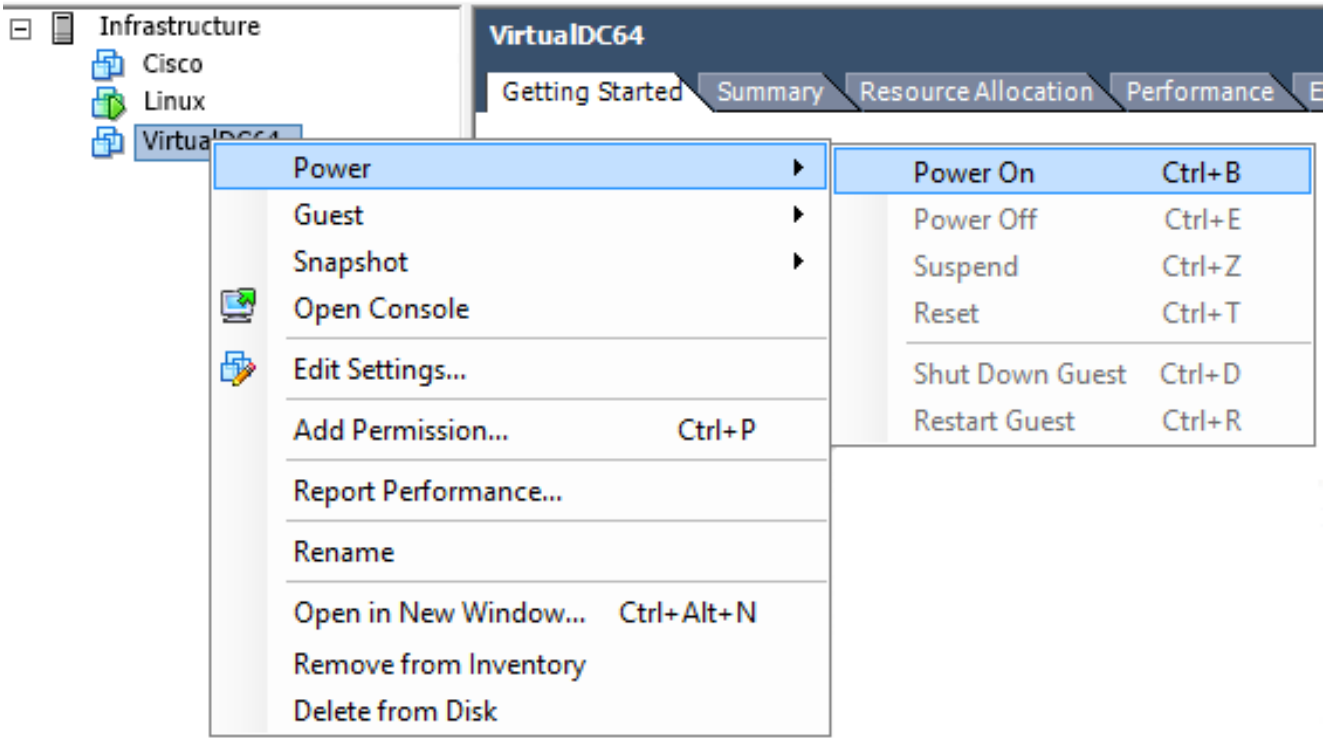


11. Clique o **revestimento** a fim terminar o desenvolvimento do molde OVF.

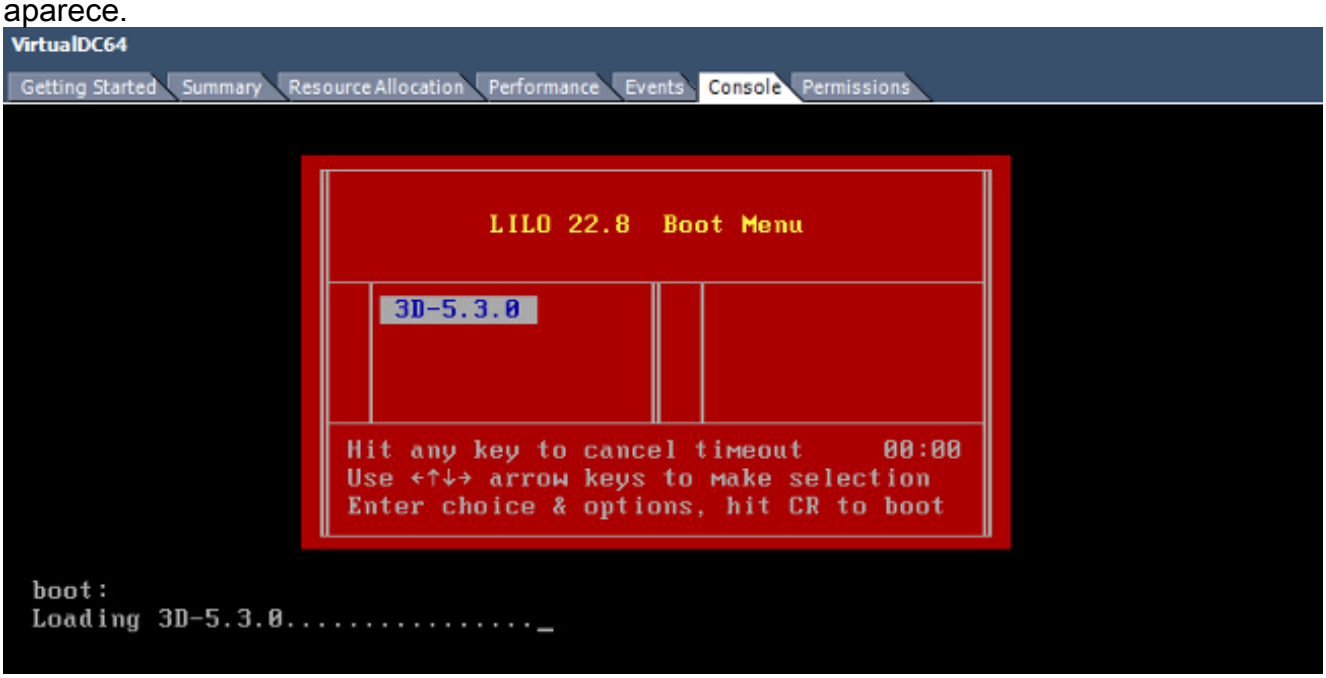


Potência sobre e iniciação completa

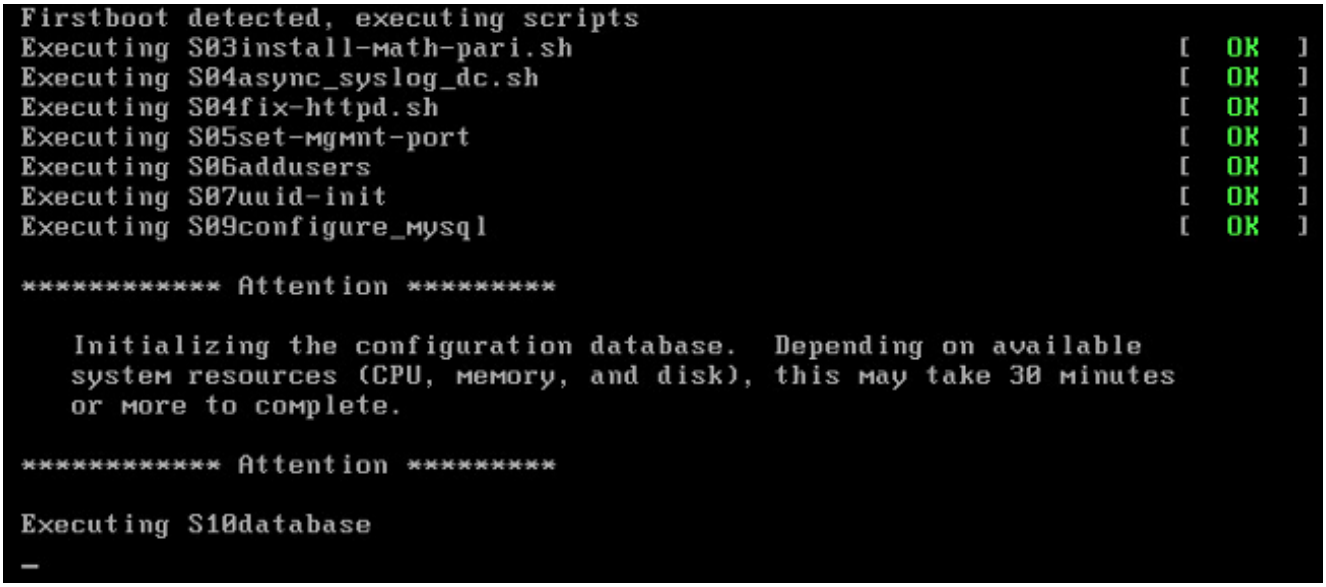
1. Navegue à máquina virtual recém-criado. Clicar com o botão direito o nome do servidor e escolha a **potência > a potência** a fim carreg **sobre** pela primeira vez acima do server.



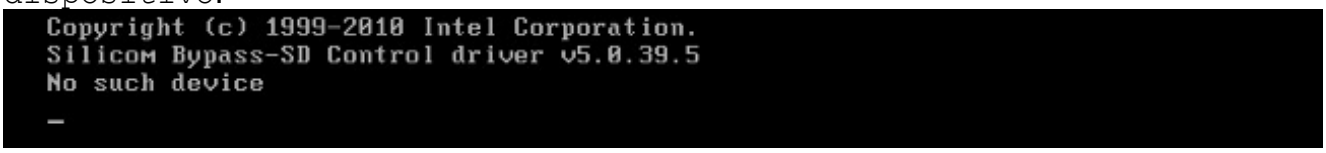
2. Navegue à aba do **console** a fim monitorar o console de servidor. O menu da bota LILO aparece.



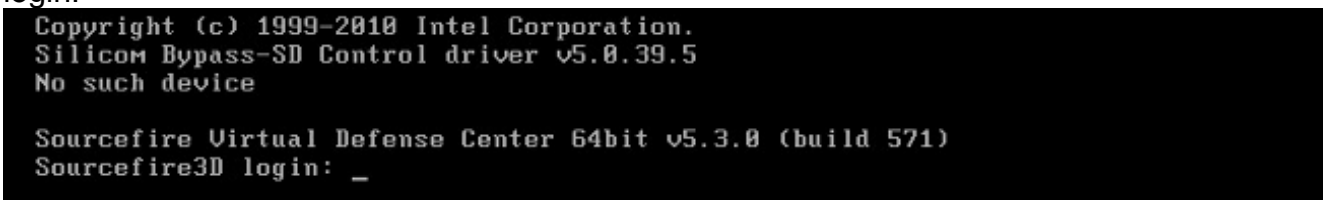
Uma vez que a verificação de dados BIOS é bem sucedida, o processo de inicialização começa. A primeira bota pôde tomar o tempo adicional terminar enquanto a base de dados de configuração é inicializada pela primeira
vez.



Uma vez que completo, você pôde ver uma mensagem para `nenhum tal dispositivo`.



3. A imprensa **entra** a fim obter uma alerta de login.



Note: Uma mensagem "`ESCREVE MESMOS falhados. Manualmente zerando.`" pode aparecer depois que o sistema é carreg acima de pela primeira vez. Isto não indica um defeito, ele indica corretamente que o direcionador do armazenamento de VMware não apoia a `ESCRITA o MESMO` comando. O sistema indica esta mensagem, e continua com um comando da reserva executar a mesma operação.

Configurar as configurações de rede

1. Na alerta de login `Sourcefire3D`, use estas credenciais para entrar: Para a versão 5.xNome de usuário: **admin**Senha: **Sourcefire**Para a versão 6.x e mais recenteNome de usuário: **admin**Senha: **Admin123****Tip**: Você poderá mudar a senha padrão no processo da instalação inicial no GUI.
2. A configuração inicial da rede é feita com um script. Você precisa de executar o script como um `usuário de raiz`. A fim comutar ao `usuário de raiz`, inscreva o **comando su - do sudo** junto com a senha **`Sourcefire ou Admin123`** `(para 6.x)`. Exercite o cuidado quando registrado na linha de comando do centro de gerenciamento como um usuário de raiz.

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

3. A fim começar a configuração de rede, entre no script da configurar-**`rede`** como a `raiz`.

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

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

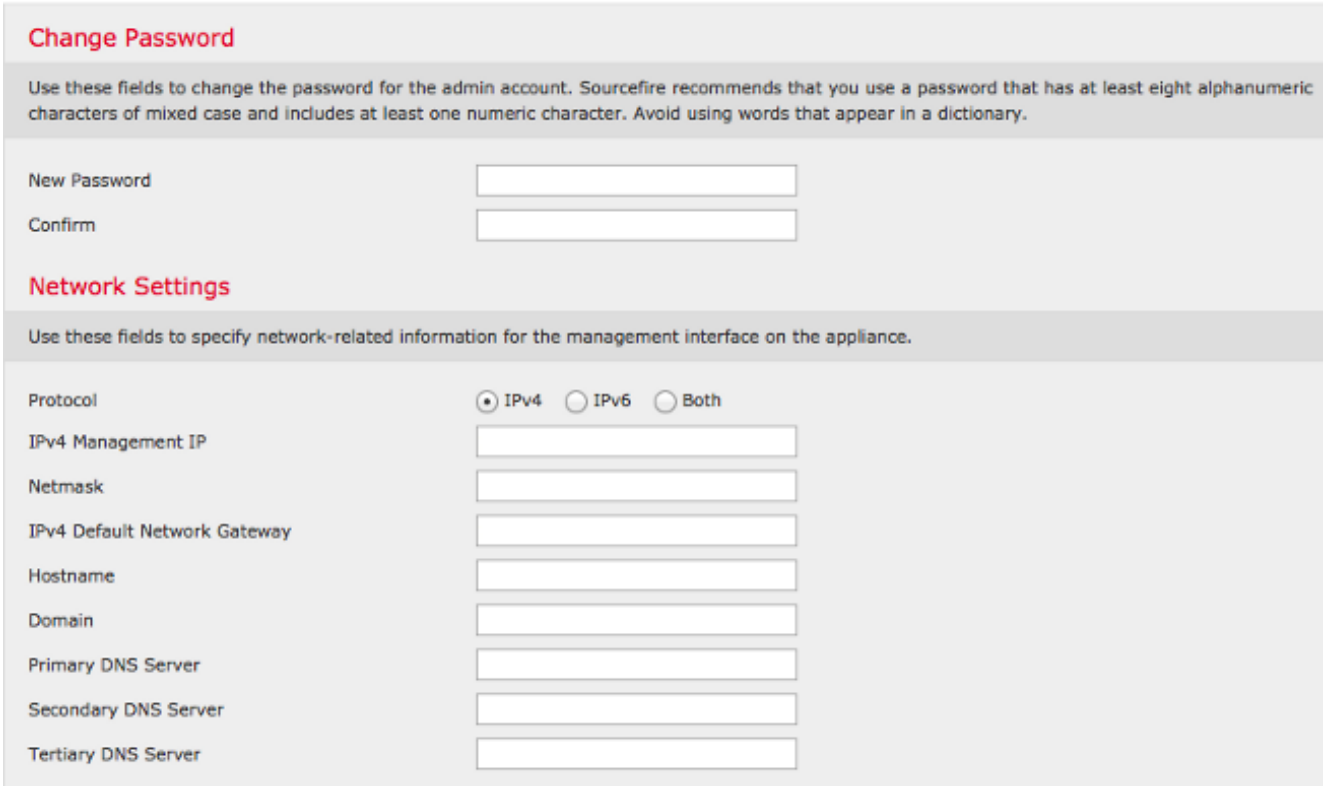
Você será pedido para fornecer um endereço IP de gerenciamento, um netmask, e um gateway padrão. Uma vez que você confirma os ajustes, o serviço de rede reinicia. Em consequência, a interface de gerenciamento vai para baixo e volta então.

```
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:~# _
```

Execute a instalação inicial

1. Depois que as configurações de rede são configuradas, abra um navegador da Web e consulte ao IP configurado através de HTTPS (https://192.0.2.2 neste exemplo). Autentique o certificado do padrão SSL se alertado. Use estas credenciais a fim entrar:Para a versão 5.x Nome de usuário: **admin**Senha: **Sourcefire**Para a versão 6.x e mais recenteNome de usuário: **admin**Senha: **Admin123**
2. Na tela que segue, todas as seções de configuração GUI são opcionais à exceção da mudança da senha e da aceitação dos termos de serviço. Se a informação é sabida, recomenda-se usar o assistente de configuração a fim simplificar a configuração inicial do centro de gerenciamento. Uma vez que configurado, o clique **aplica-se** a fim aplicar a configuração ao centro de gerenciamento e aos dispositivos registrados. Uma breve visão geral das opções de configuração é como segue:**Senha da mudança:** Permite que você mude a senha para a conta admin do padrão. Exige-se para mudar a senha. **Configurações de rede:** Permite que você altere as configurações de rede previamente configuradas do IPv4 e do IPv6 para a interface de gerenciamento do dispositivo ou da máquina virtual.**Configurações de tempo:** Recomenda-se que você sincronização o centro de gerenciamento com uma fonte segura NTP. Os sensores IPS podem ser configurados com a política de sistema para sincronizar seu tempo com o centro de gerenciamento. Opcionalmente, a hora e a zona de hora (fuso horário) do indicador podem ser ajustadas manualmente.**Importações de retorno da atualização da regra:** As atualizações de retorno da regra do Snort Enable e instalam opcionalmente agora durante a instalação inicial.**Atualizações de retorno de Geolocation:** As atualizações de retorno da regra do geolocation Enable e instalam opcionalmente agora durante a instalação inicial.**Backup**

automáticos: Backup da configuração automática da programação.**Ajustes da licença:** Adicionar a licença de recurso.**Registro do dispositivo:** Permite que você adicione, licencie, e aplique políticas iniciais do controle de acesso aos dispositivos preregistered. O hostname/endereço IP de Um ou Mais Servidores Cisco ICM NT e a chave do registro devem combinar o endereço IP de Um ou Mais Servidores Cisco ICM NT e a chave do registro configurados no módulo ips de FirePOWER.**Contrato de licença do utilizador final:** A aceitação do EULA é
exigida.



Informações Relacionadas

- [Guia de início rápido virtual do centro de gerenciamento de FirePOWER para VMware, versão 6.0]
- [Suporte Técnico e Documentação - Cisco Systems]