Déploiement de centre de Gestion de FireSIGHT sur le VMware ESXi

Contenu

[Introduction](#)
[Conditions préalables](#)
[Composants utilisés](#)
[Configuration](#)
[Déployez un modèle OVF](#)
[Mettez sous tension et remplissez l'initialisation](#)
[Configurez les paramètres réseau](#)
[Exécutez la première installation](#)
[Informations connexes](#)

Introduction

Ce document décrit la première installation d'un centre de Gestion de FireSIGHT (également connu sous le nom de centre de la défense) que des passages sur le VMware ESXi. Un centre de Gestion de FireSIGHT te permet pour gérer un ou plusieurs appliances de puissance de feu, appliances de Viirtual du système de prévention des intrusions de nouvelle génération (NGIPS), et appliance de sécurité adaptable (ASA) avec des services de puissance de feu.

> Remarque: Ce document est une annexe du guide d'installation et du guide utilisateur de système de FireSIGHT. Pour une configuration d'ESXi et une question spécifiques de dépannage, référez-vous à la base de connaissances et à la documentation de VMware.

Conditions préalables

Composants utilisés

Les informations sur ce document sont basées sur ces Plateformes :

- Centre de Gestion de Cisco FireSIGHT
- Appliance virtuelle de centre de Gestion de Cisco FireSIGHT
- VMware ESXI 5.0

Dans ce document, un « périphérique » se rapporte à ces Plateformes :

- Appliances de gamme 7000 de puissance de feu de Sourcefire et appliances de gamme 8000
- Appliances virtuelles de Sourcefire NGIPS pour le VMware ESXi
- Gamme 5500-X de Cisco ASA avec le service de puissance de feu

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-

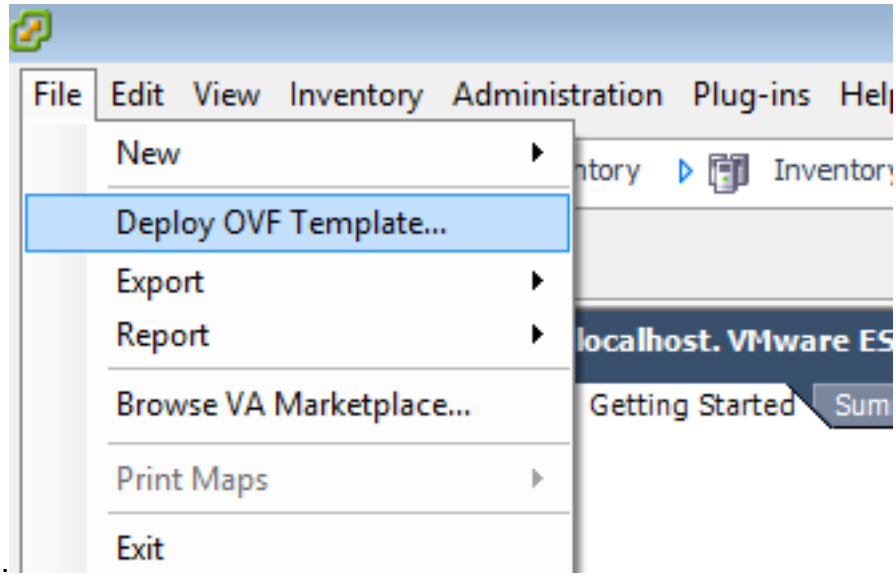
vous que vous comprenez l'effet potentiel de toute commande.

Configuration

Déployez un modèle OVF

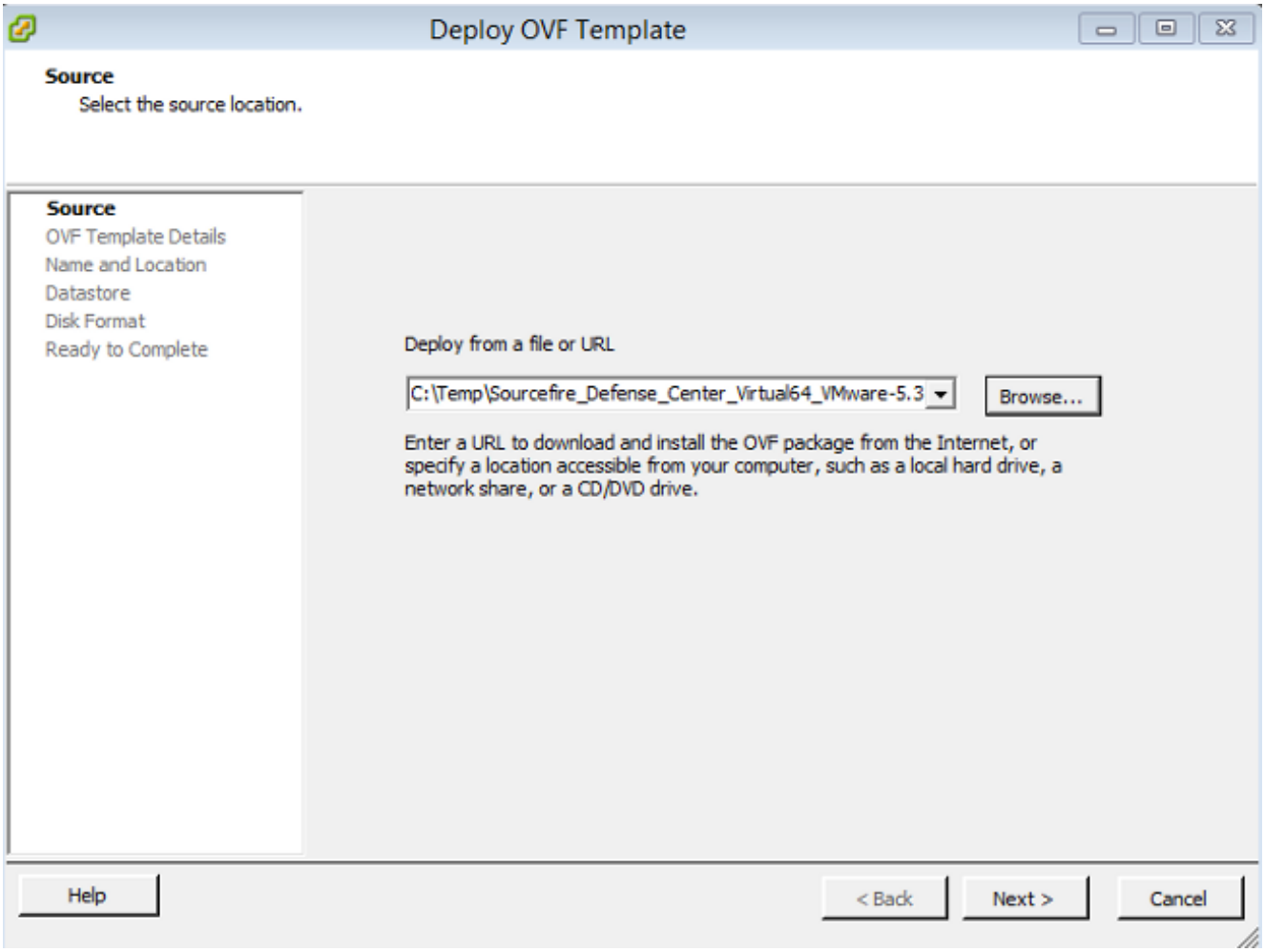
1. Téléchargez l'**appliance virtuelle de centre de Gestion de Cisco FireSIGHT du** site de support et de téléchargements de Cisco.
2. Extrayez le contenu du fichier de `tar.gz à un` répertoire local.
3. Connectez à votre serveur d'ESXi à un **client de vSphere de VMware**.

4. Une fois que vous ouvrez une session au client de vSphere, choisissez le **fichier > déploient**

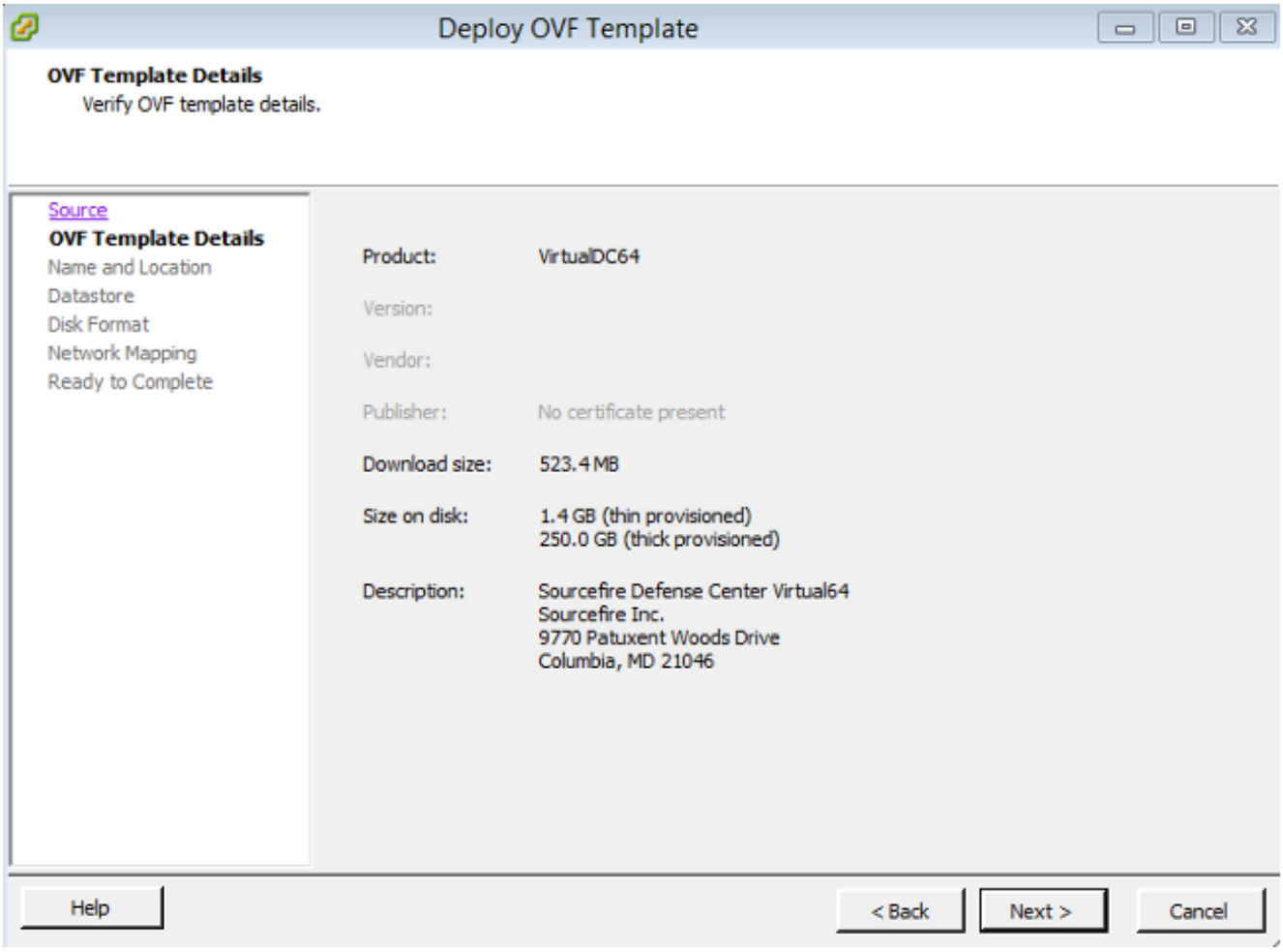


le modèle OVF.

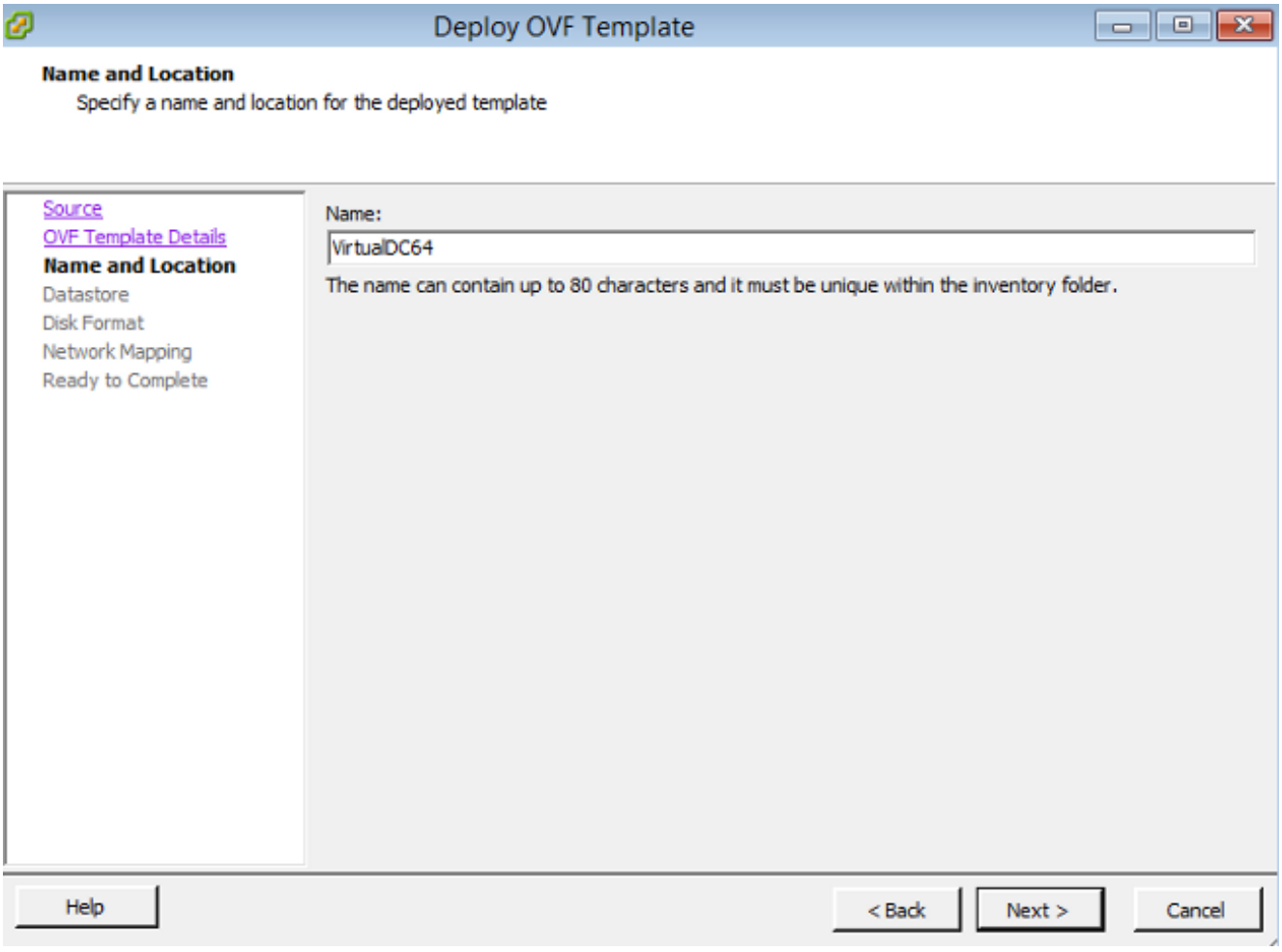
5. Cliquez sur **parcourent** et localisent les fichiers que vous avez extraits dans l'étape 2. choisissez le fichier `Sourcefire_Defense_Center_Virtual64_VMware-ESXi-X.X.X-xxx.ovf` OVF et cliquez sur Next.



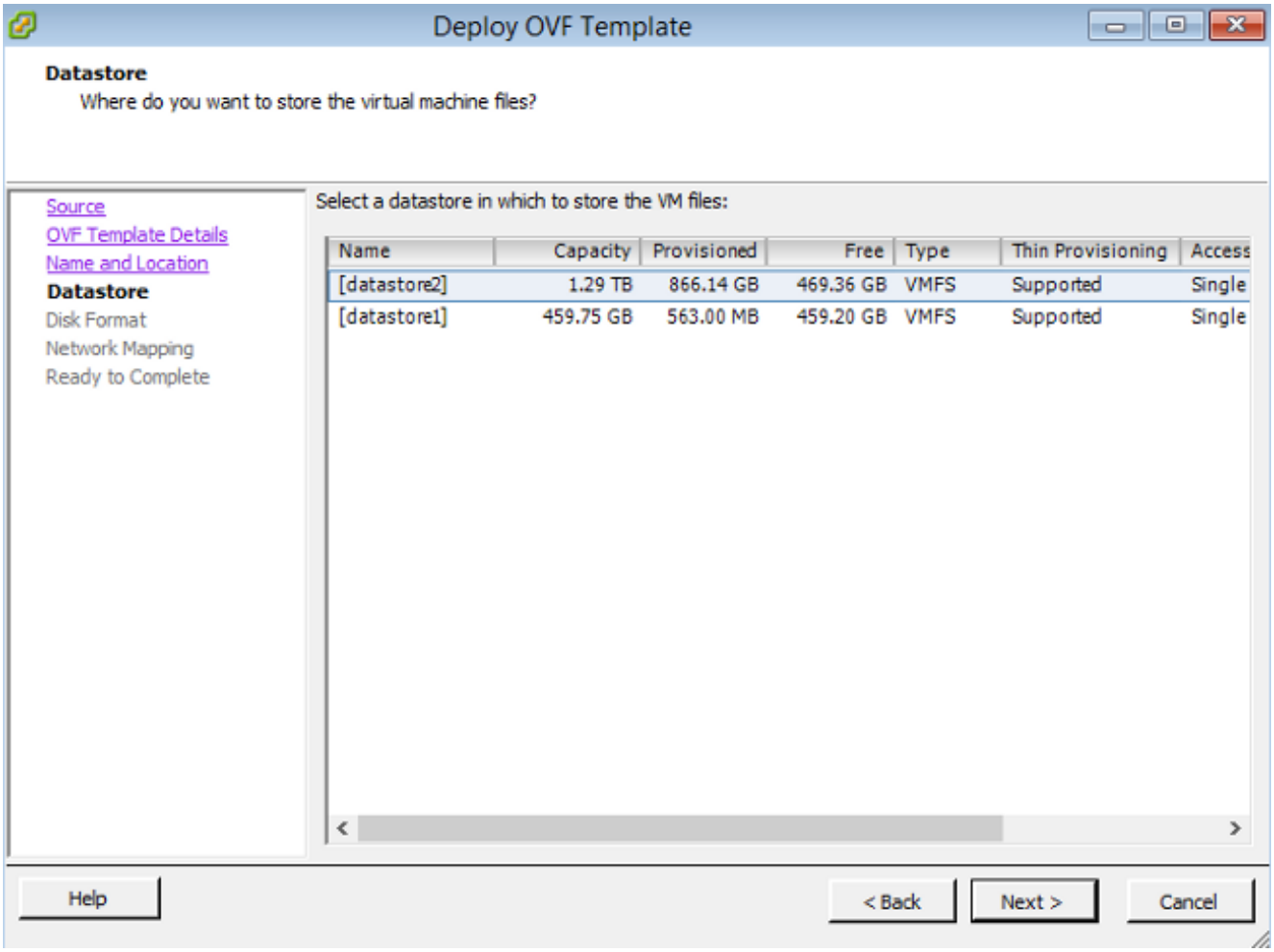
6. Sur le **modèle OVF les détails** examinent, cliquent sur Next afin de recevoir les valeurs par défaut.



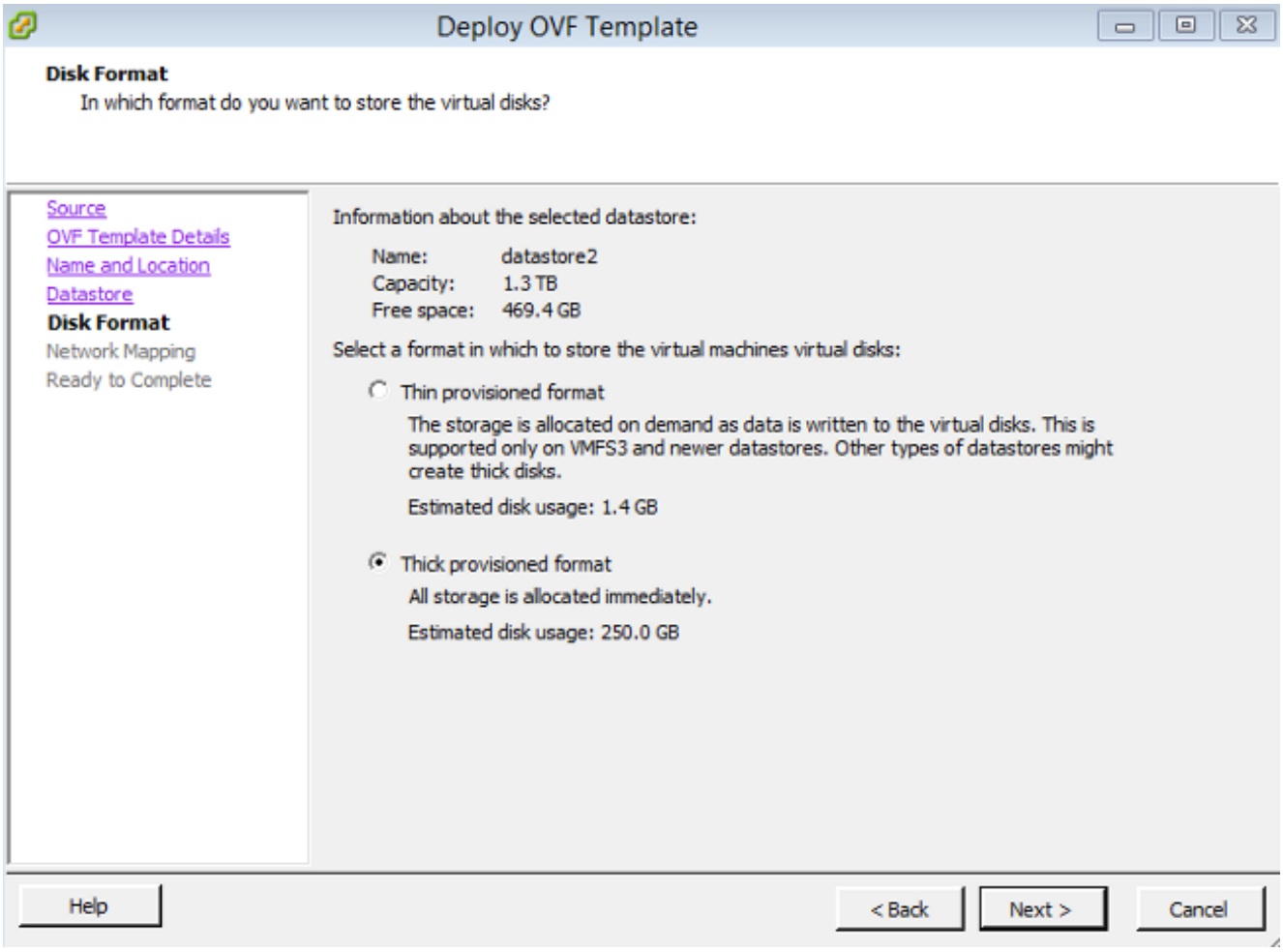
7. Fournissez un nom pour le centre de Gestion et cliquez sur Next.



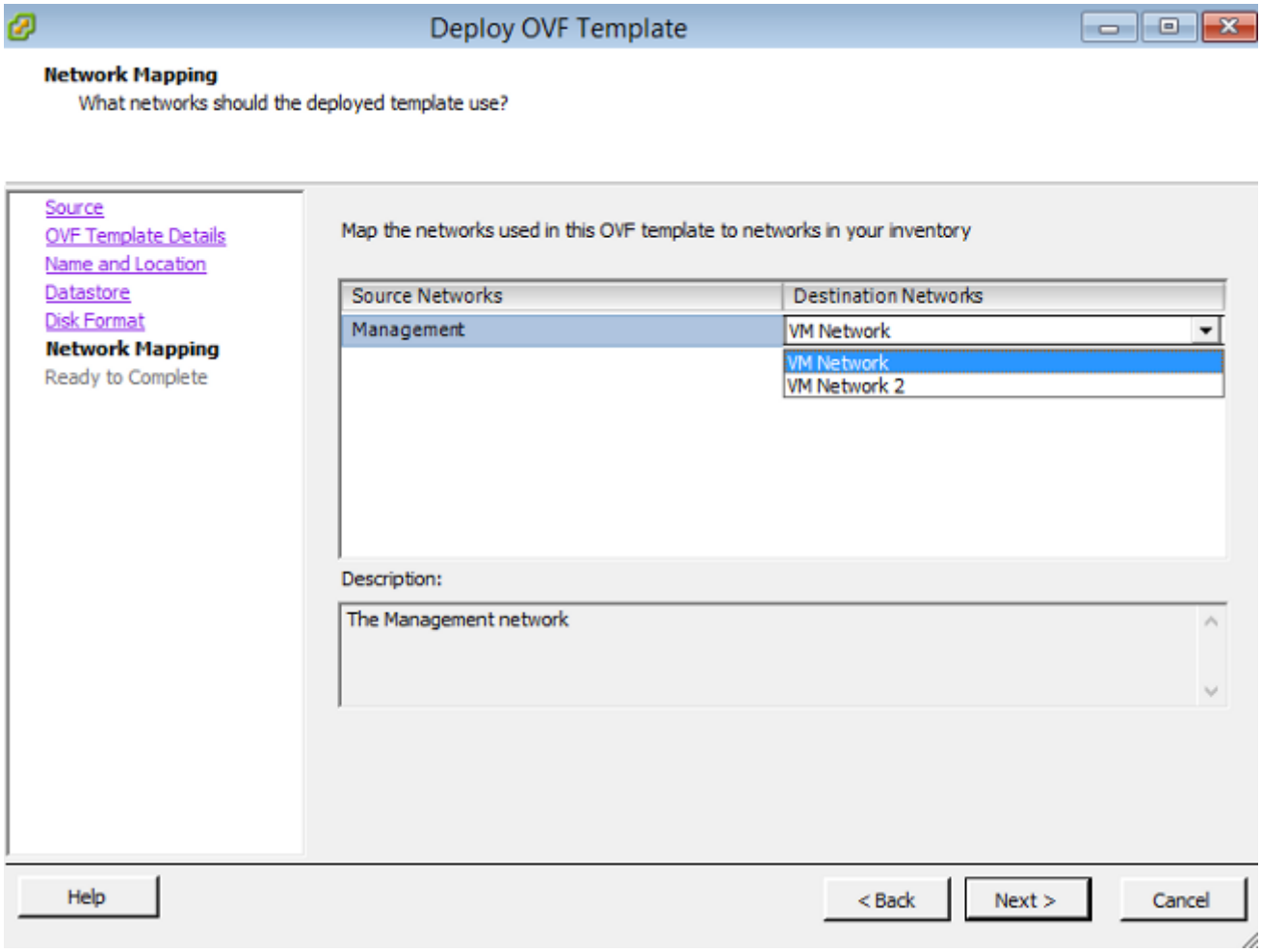
8. Choisissez un **Datastore** sur lequel vous voulez créer le virtual machine et cliquer sur Next.



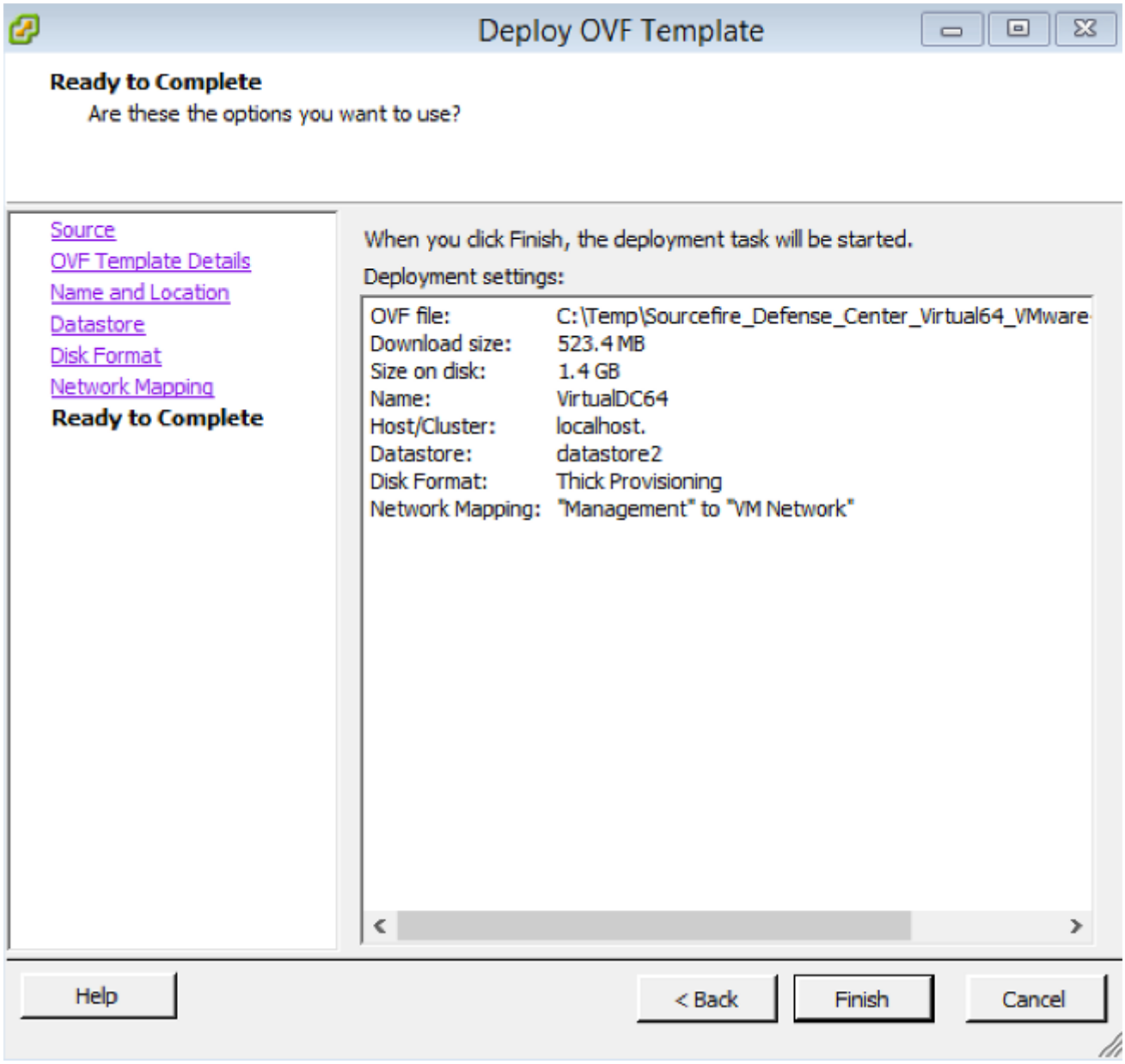
9. Cliquez sur la case d'option **provisioned épaisse de format** pour le **format de disque** et cliquez sur Next. Le format épais de ravitaillement alloue l'espace disque nécessaire au moment de créer un disque virtuel, tandis que les utilisations de format de provisionnement léger espacent le à la
demande.



10. Sur la section de **mappage de réseau**, associez l'interface de gestion du centre de Gestion de FireSIGHT à un réseau de VMware et cliquez sur Next.

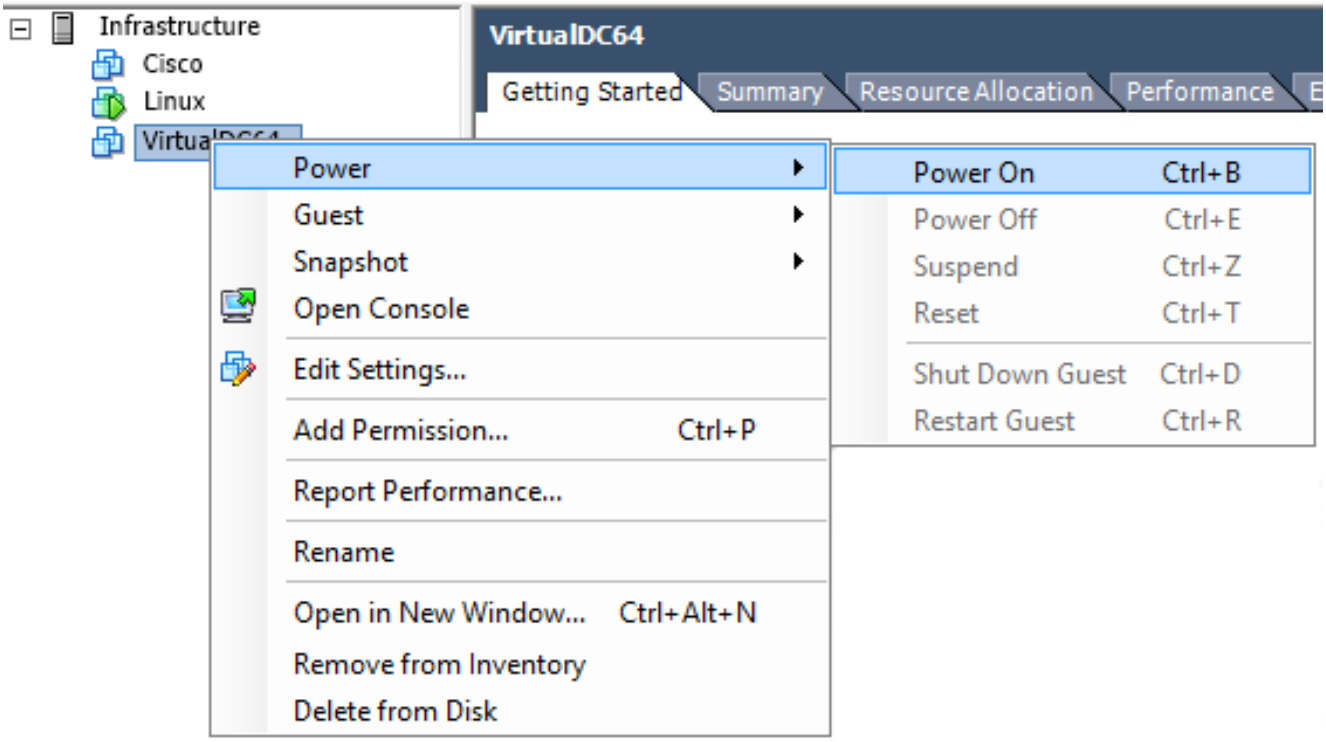


11. Cliquez sur Finish afin de se terminer le déploiement de modèle OVF.

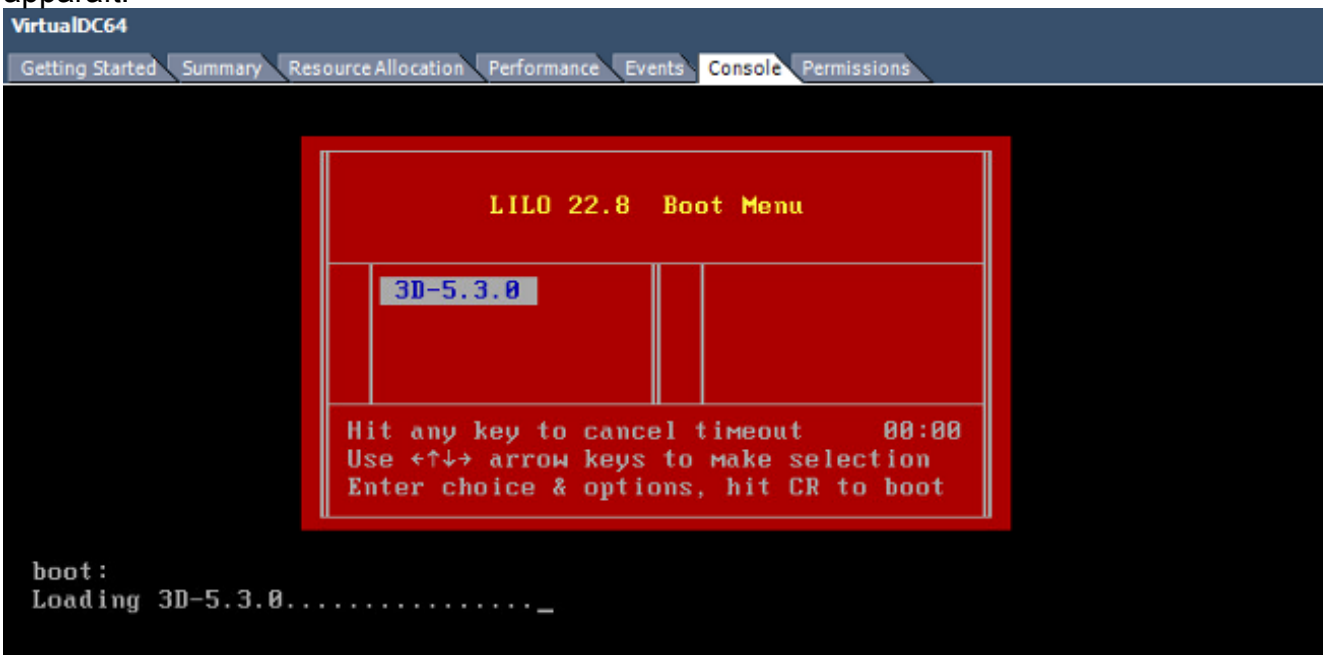


Mettez sous tension et remplissez l'initialisation

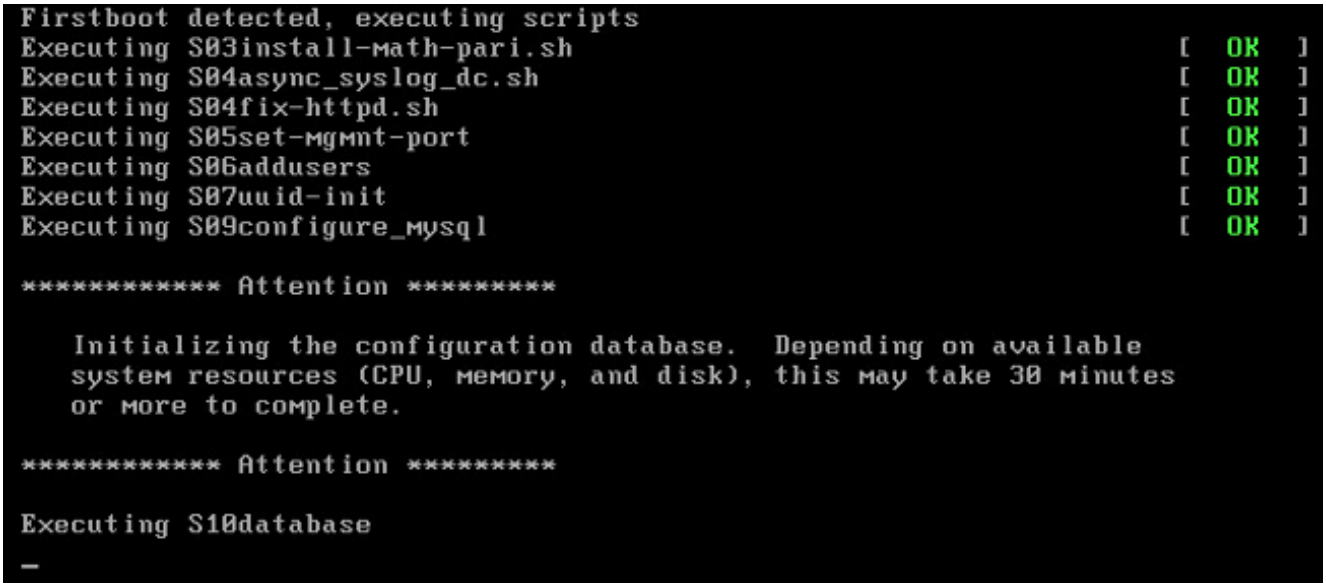
1. Naviguez vers le virtual machine de création récente. Cliquez avec le bouton droit le nom du serveur et choisissez l'**alimentation > mettent sous tension** afin d'initialiser le serveur pour la première
   fois.



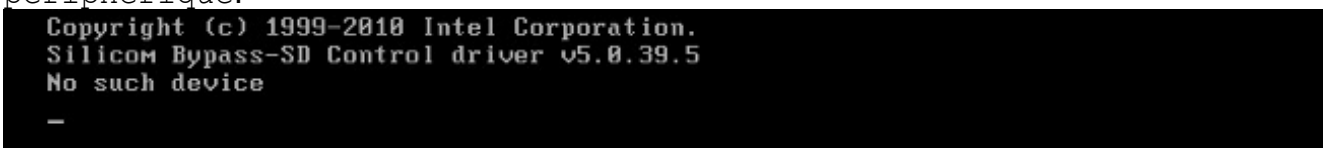
2. Naviguez vers l'onglet de **console** afin de surveiller la console de serveur. Le menu de démarrage LILO apparaît.



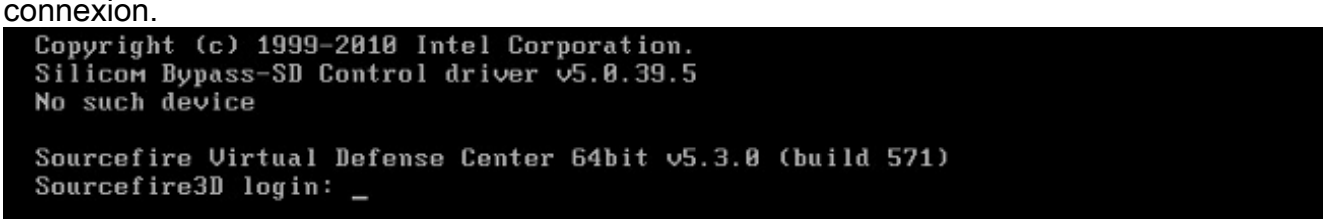
Une fois que le contrôle de données BIOS est réussi, les débuts de processus d'initialisation. Le premier démarrage pourrait prendre du temps supplémentaire de se terminer pendant que la base de données de configuration est initialisée pour la première fois.



Une fois complet, vous pourriez voir un message pour `aucun un tel périphérique`.



3. La presse **entrent** afin d'obtenir une invite d'ouverture de connexion.



Remarque: Un message « `ÉCRIVENT MÊMES a manqué. Manuellement mettant à zéro.` » peut apparaître après que le système soit initialisé pour la première fois. Ceci n'indique pas un défaut, il indique correctement que le gestionnaire de mémoire de VMware ne prend en charge pas l'`INSCRIPTION la MÊME` commande. Le système affiche ce message, et se poursuit par une commande de retour d'exécuter la même exécution.

Configurez les paramètres réseau

1. Sur l'invite d'ouverture de connexion `Sourcefire3D`, employez ces qualifications pour ouvrir une session : Pour la version 5.xNom d'utilisateur : **admin**Mot de passe : **Sourcefire**Pour la version 6.x et ultérieuresNom d'utilisateur : **admin**Mot de passe : **Admin123**Conseil : Vous pourrez changer le mot de passe par défaut dans le processus de première installation dans le GUI.
2. La configuration initiale du réseau est faite avec un script. Vous devez exécuter le script en tant qu'`utilisateur de base`. Afin de commuter à l'`utilisateur de base`, entrez dans le **sudo su -** commandez avec le mot de passe **Sourcefire ou Admin123** `(pour 6.x)`. Exercez l'attention une fois connecté dans la ligne de commande de centre de Gestion en tant qu'utilisateur de base. `admin@Sourcefire3D:~$ sudo su -`
`Password:`
3. Afin de commencer la configuration réseau, écrivez le script de **configure network** comme `racine`.

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

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

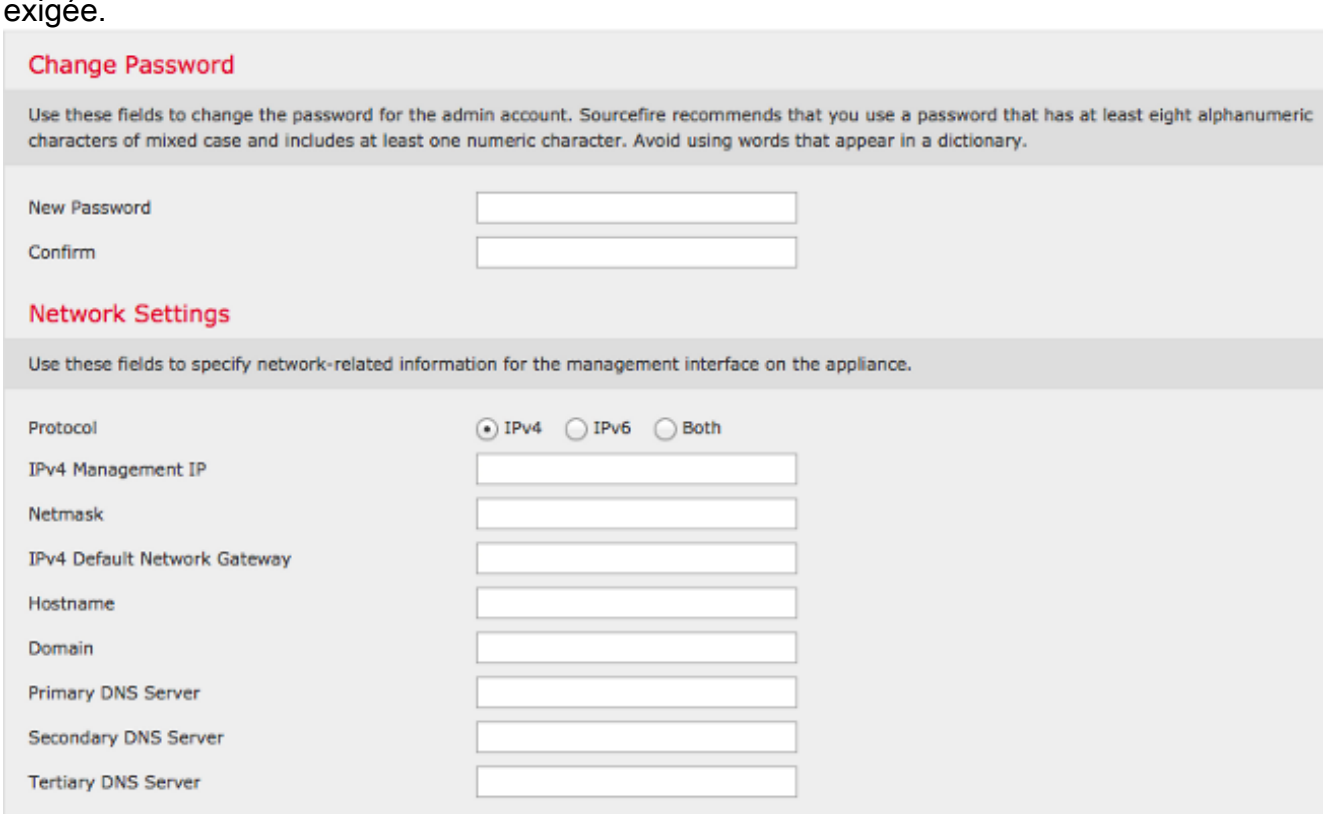
Vous serez invité à fournir une adresse IP, un netmask, et une passerelle par défaut de Gestion. Une fois que vous confirmez les configurations, les reprises de service réseau. En conséquence, l'interface de gestion descend et revient
alors.

```
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:~# _
```

Exécutez la première installation

1. Après que les paramètres réseau soient configurés, ouvrez un navigateur Web et parcourez à l'IP configuré par l'intermédiaire de HTTPS (https://192.0.2.2 dans cet exemple). Authentifiez le certificat ssl par défaut s'incité. Employez ces qualifications afin d'ouvrir une session :Pour la version 5.x Nom d'utilisateur : **admin**Mot de passe : **Sourcefire**Pour la version 6.x et ultérieuresNom d'utilisateur : **admin**Mot de passe : **`Admin123`**
2. Sur l'écran qui suit, toutes les sections de configuration GUI sont facultatives excepté la modification de mot de passe et l'acceptation des termes de services. Si les informations sont connues, elles sont recommandées d'utiliser l'assistant de configuration afin de simplifier la configuration initiale du centre de Gestion. Une fois que configuré, cliquez sur Apply **afin d'appliquer la configuration au centre de Gestion et aux périphériques enregistrés.** Une brève présentation des options de configuration est comme suit :**Change Password :** Te permet pour changer le mot de passe pour le compte par défaut d'admin. On l'exige pour changer le mot de passe. **Paramètres réseau :** Te permet pour modifier les paramètres réseau précédemment configurés d'ipv4 et d'IPv6 pour l'interface de gestion de l'appliance ou du virtual machine.**Paramètres horaires :** Il est recommandé que vous sync le centre de Gestion avec un ntp source fiable. Les capteurs IPS peuvent être configurés par la stratégie de système pour synchroniser leur temps avec le centre de Gestion. Sur option, le fuseau horaire de temps et d'affichage peut être placé manuellement.**Importations récurrentes de mise à jour de règle :** L'enable se reproduisant reniflent des mises à jour de règle et les installent sur option maintenant pendant la première installation.**Mises à jour périodiques de Geolocation :** Activez les mises à jour récurrentes de règle de geolocation et les installez sur option maintenant pendant la première installation.**Sauvegardes automatiques :**

Sauvegardes de configuration automatique de programme.**Configurations de permis :** Ajoutez le permis de caractéristique.**Enregistrement de périphérique :** Te permet pour ajouter, autoriser, et appliquer des stratégies initiales de contrôle d'accès aux périphériques preregistered. L'adresse Internet/adresse IP et la clé d'enregistrement devraient apparier l'adresse IP et l'enregistrement clé configurés sur le module IPS de puissance de feu.**Contrat de licence utilisateur final :** L'acceptation du CLUF est exigée.



Informations connexes

- Guide de démarrage rapide virtuel de centre de Gestion de puissance de feu pour VMware, version 6.0
- Support et documentation techniques - Cisco Systems