VMware ESXi への FireSIGHT Management Center の導入

内容

概要

このドキュメントでは、VMware ESXi で稼働する FireSIGHT Management Center（Defense Center とも呼ばれる）の初期設定について説明します。FireSIGHT Management Center により、1 つ以上の FirePOWER アプライアンス、次世代侵入防御システム（NGIPS）仮想アプライアンス、および FirePOWER サービスを備えた適応型セキュリティ アプライアンス（ASA）の管理が可能になります。

> **注：**このドキュメントは、FireSIGHT システムのインストール ガイドおよびユーザ ガイドの補足です。ESXi 特有の設定およびトラブルシューティングの問題については、VMware のナレッジ ベースとドキュメントを参照してください。

前提条件

使用するコンポーネント

このドキュメントの情報は、次のプラットフォームに基づいています。

- Cisco FireSIGHT Management Center
- Cisco FireSIGHT Management Center 仮想アプライアンス
- VMware ESXI 5.0

このドキュメントでは、「デバイス」は次のプラットフォームを指しています。

- Sourcefire FirePOWER 7000 シリーズ アプライアンス、および 8000 シリーズ アプライアンス
- VMware ESXi 用の Sourcefire NGIPS 仮想アプライアンス
- Cisco ASA 5500-X シリーズおよび FirePOWER サービス

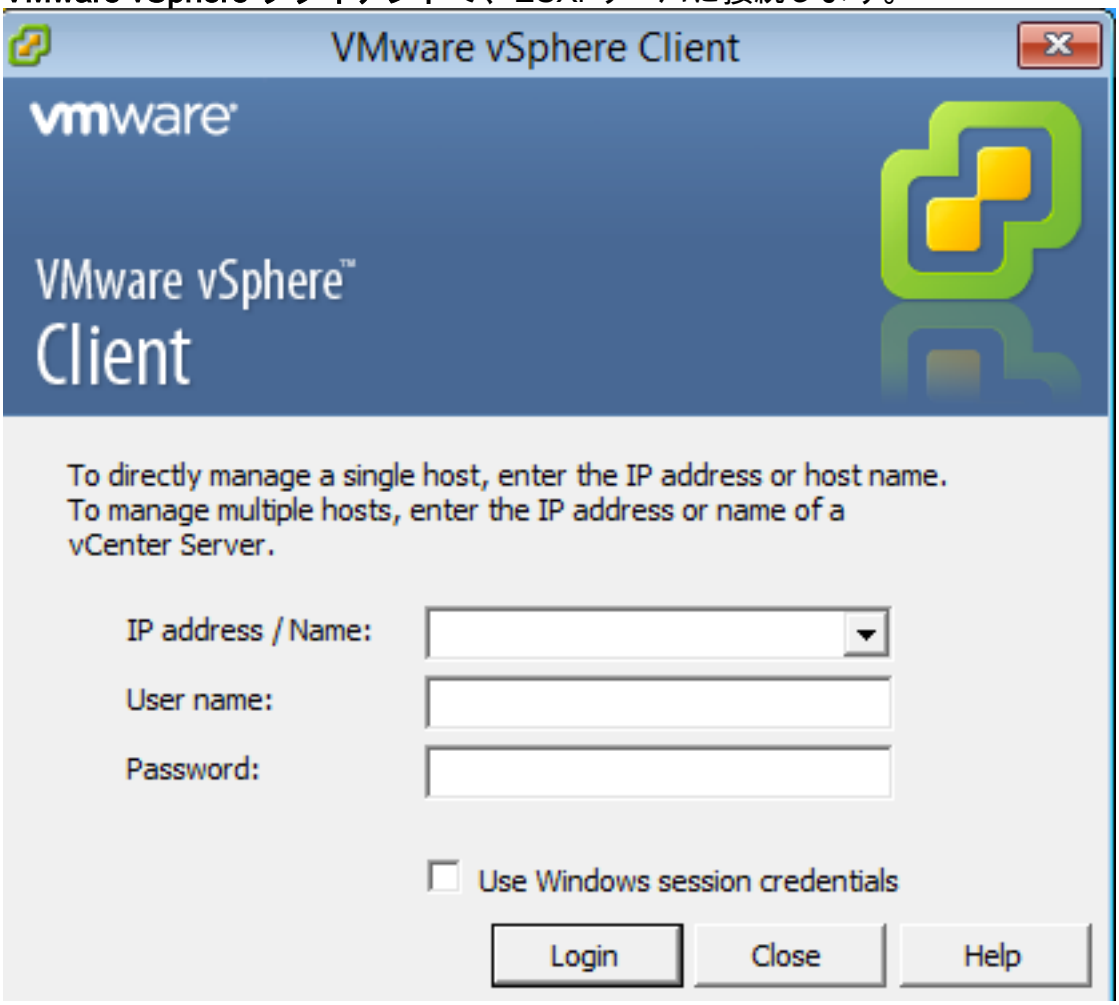
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています

。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

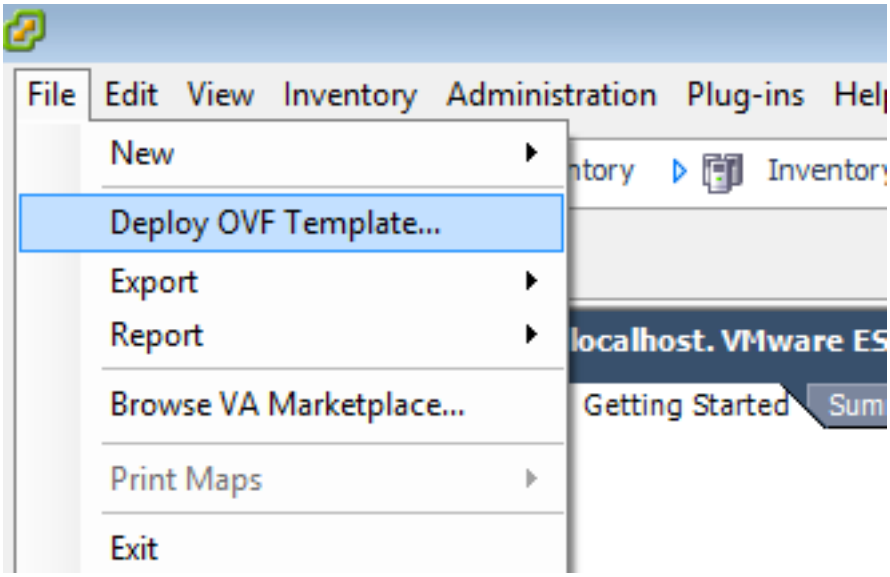
コンフィギュレーション

OVF テンプレートの展開

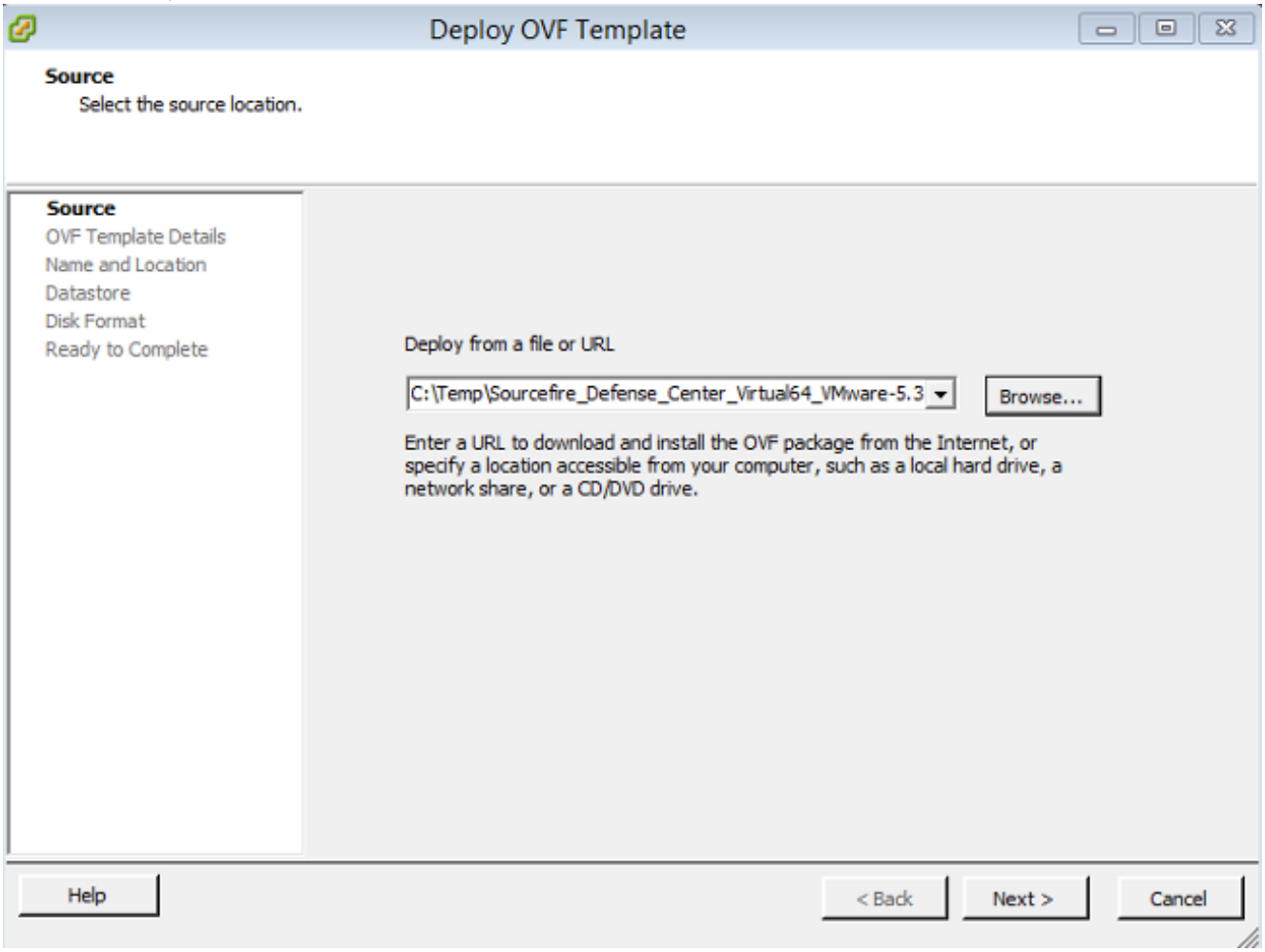
1. Cisco Support & Downloads サイトから **Cisco FireSIGHT Management Center 仮想アプライアンスをダウンロードします。**
2. ローカル ディレクトリに、tar.gz ファイルの内容を解凍します。
3. **VMware vSphere クライアント**で、ESXi サーバに接続します。



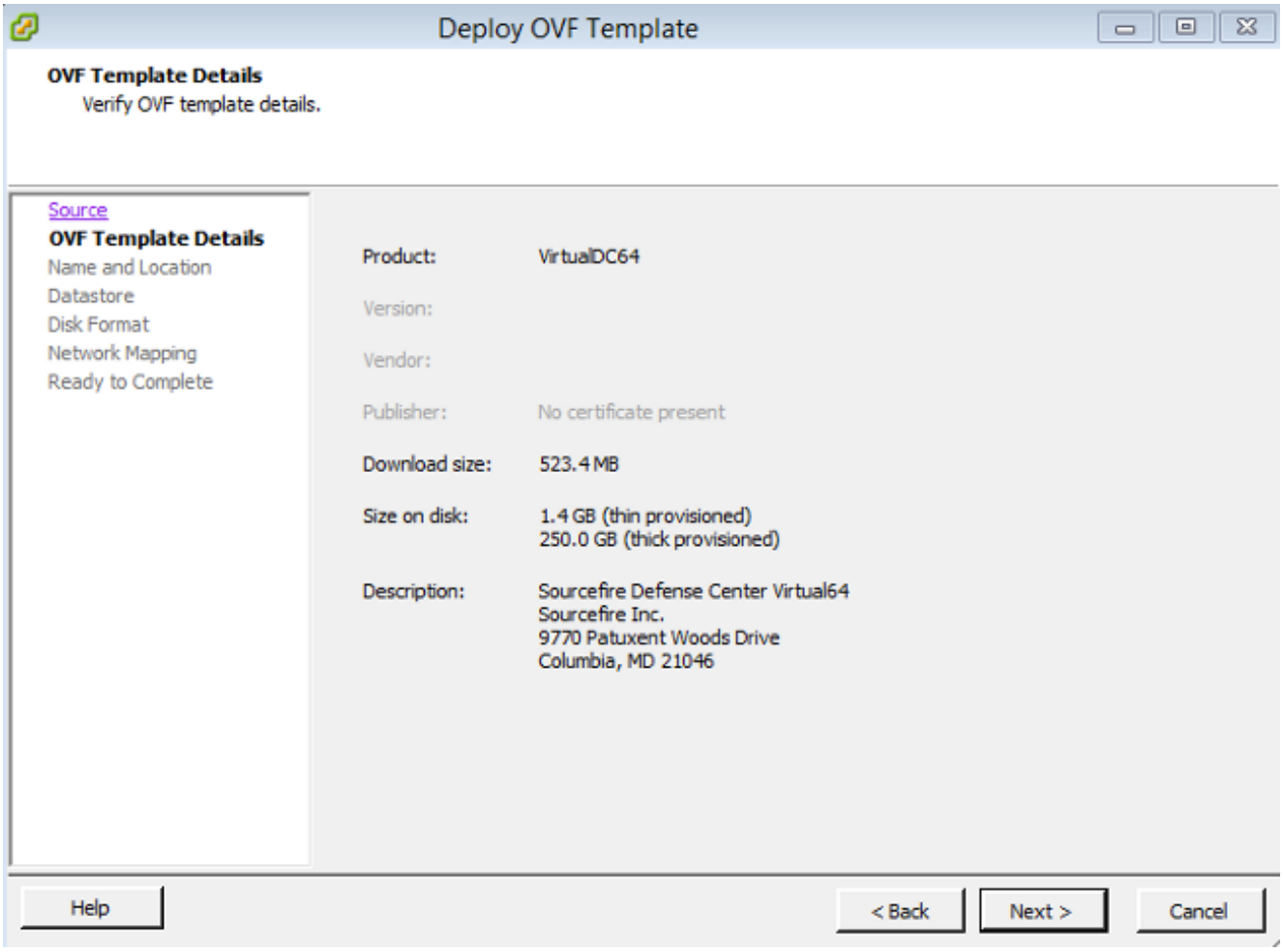
4. vSphere クライアントにログインしたら、[File] > [Deploy OVF Template] を選択します。



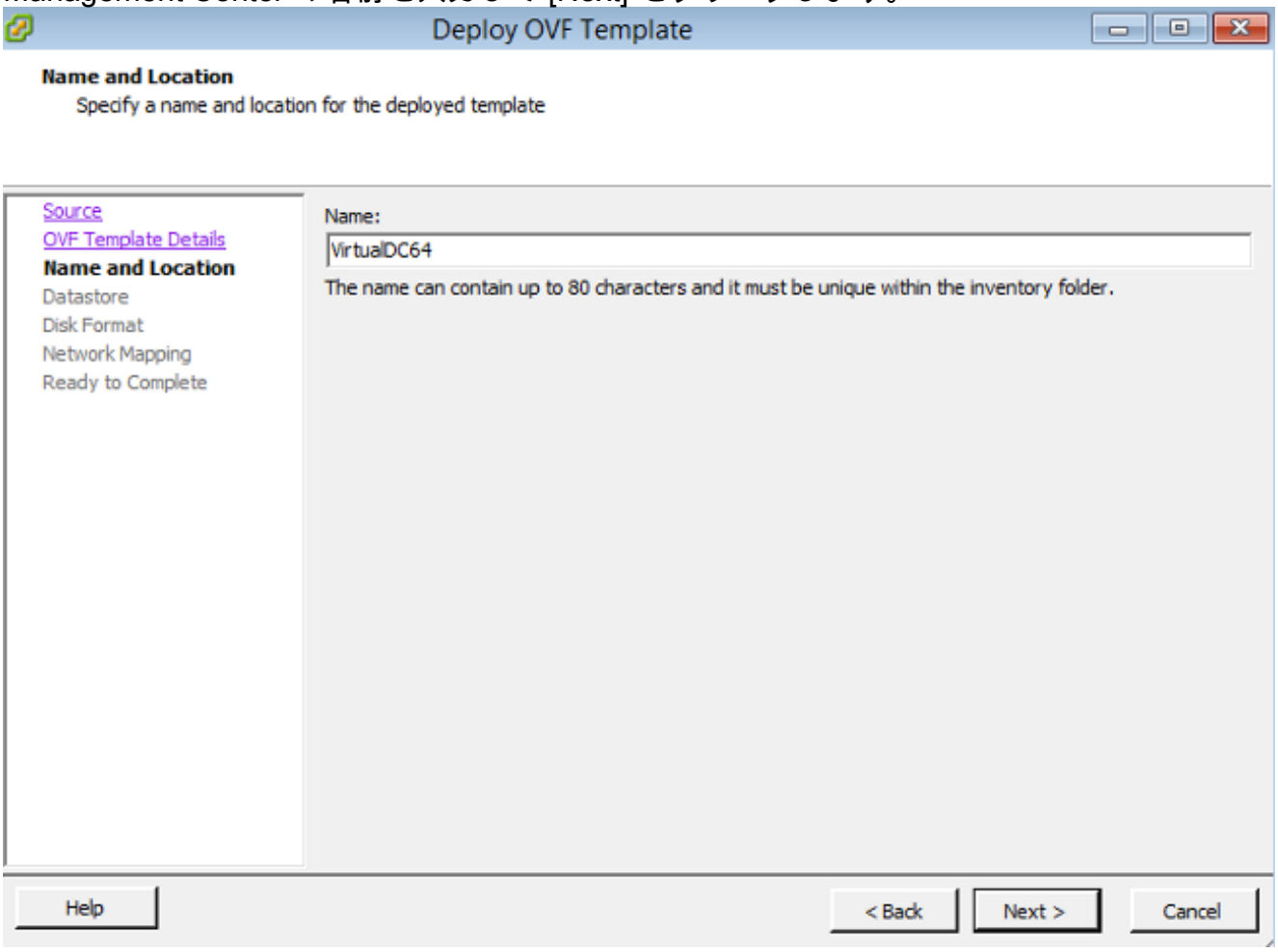
5. [Browse] をクリックして、ステップ 2 で取得したファイルを検索します。OVF ファイル Sourcefire_Defense_Center_Virtual64_VMware-ESXi-X.X.X-xxx.ovf を選択して、[Next] をクリックします。



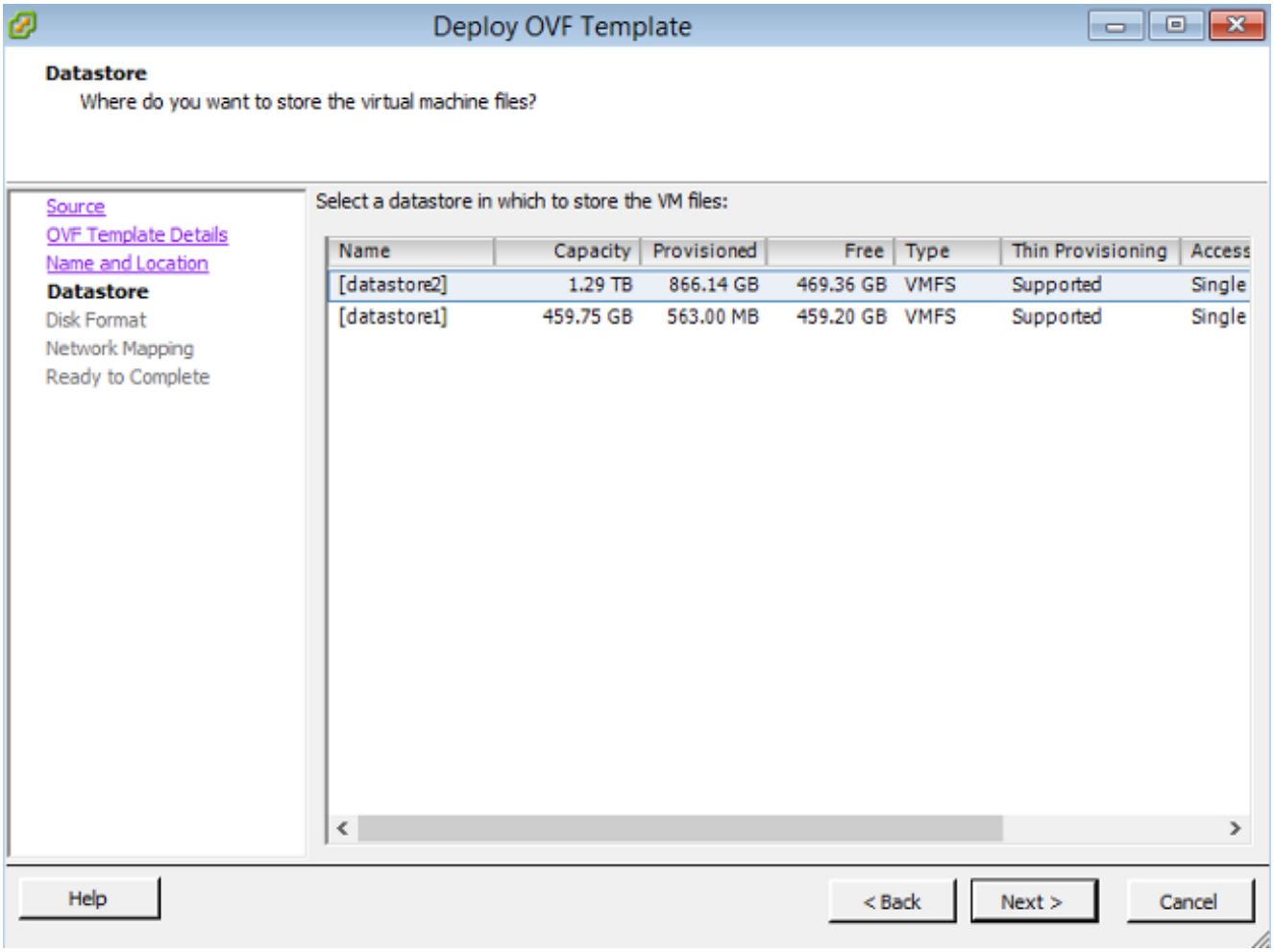
6. **[OVF Template Details] 画面で** [Next] をクリックして、デフォルトの設定を受け入れます。



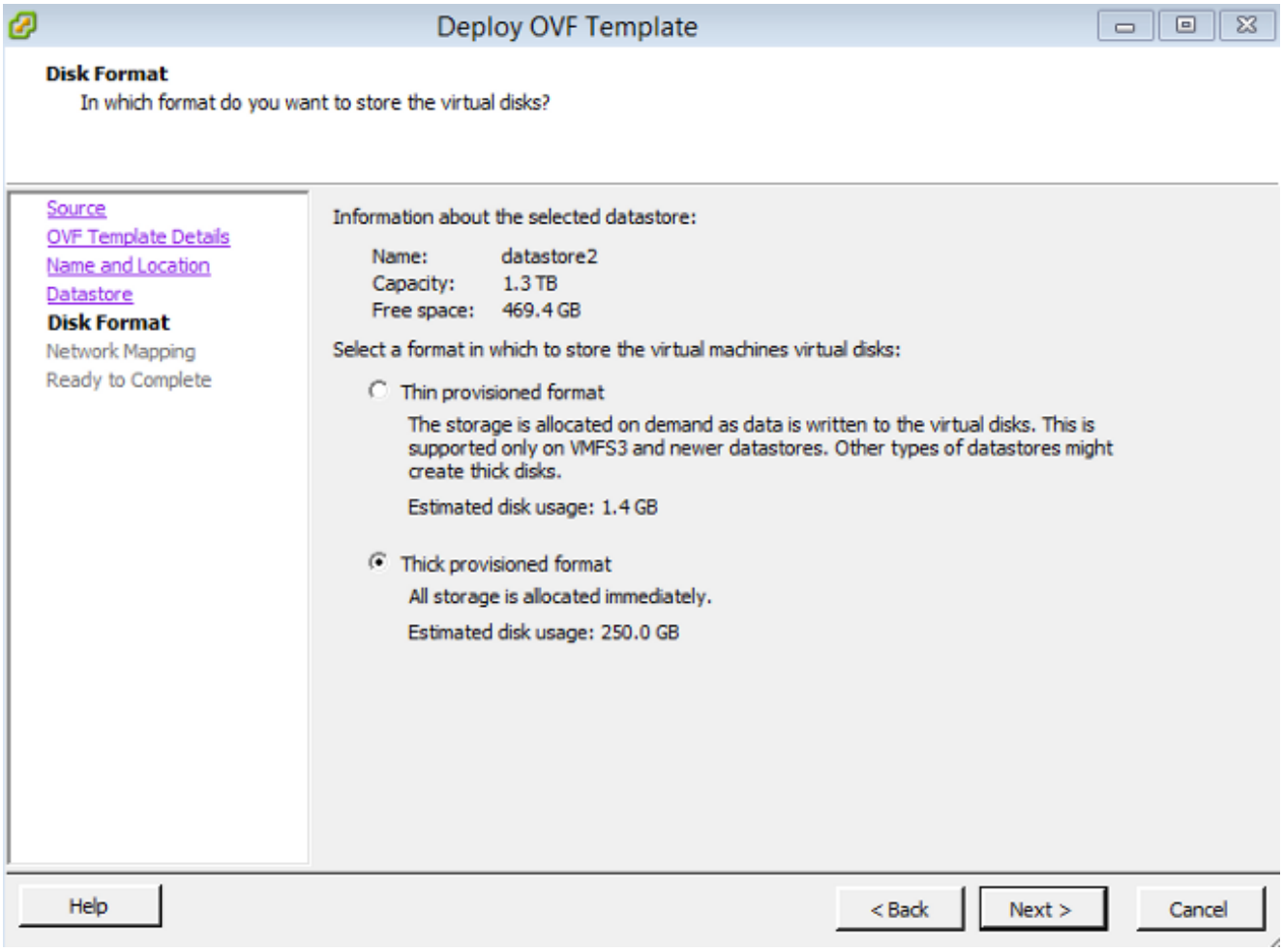
7. Management Center の名前を入力して [Next] をクリックします。



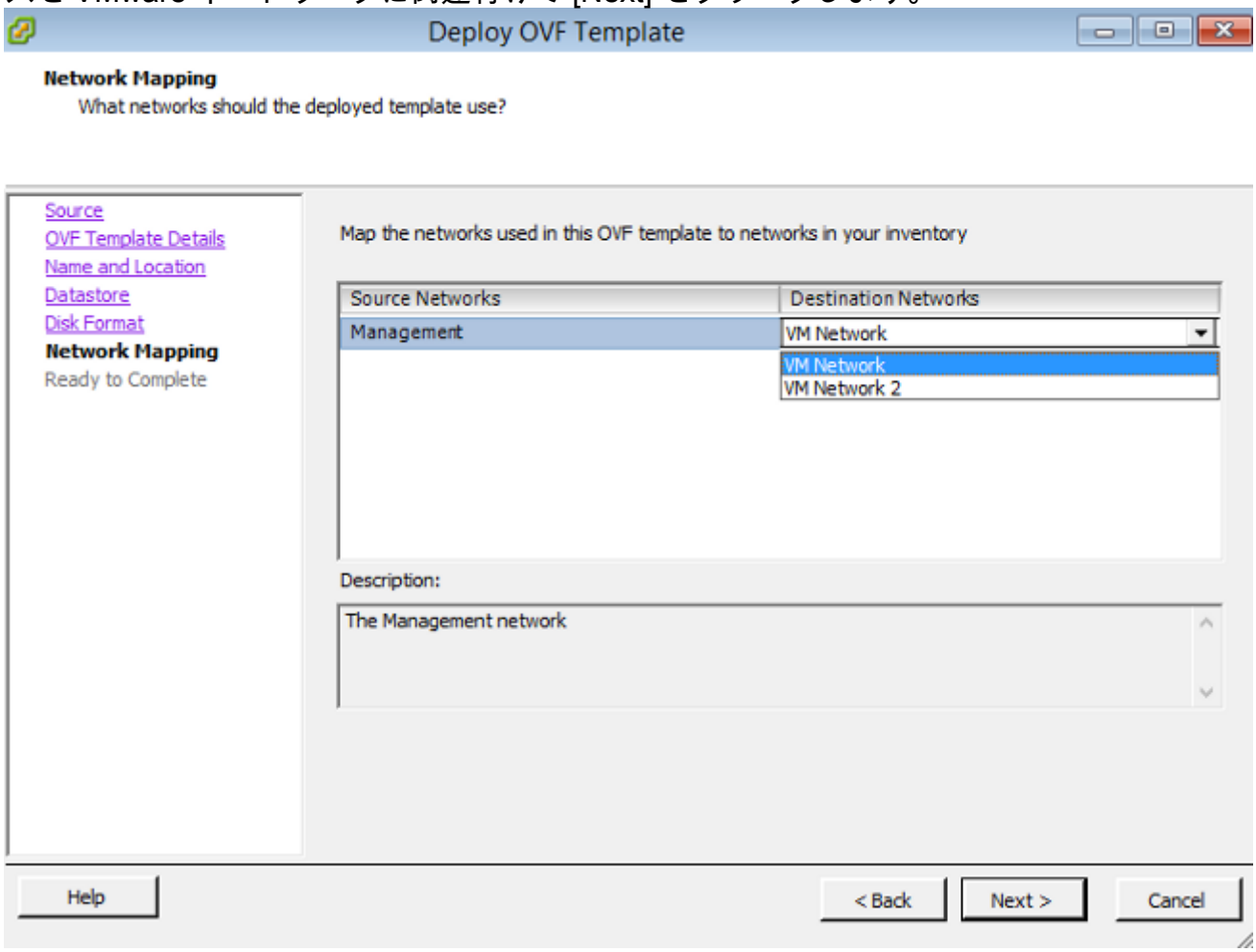
8. 仮想マシンを作成する [Datastore] を選択し、[Next] をクリックします。



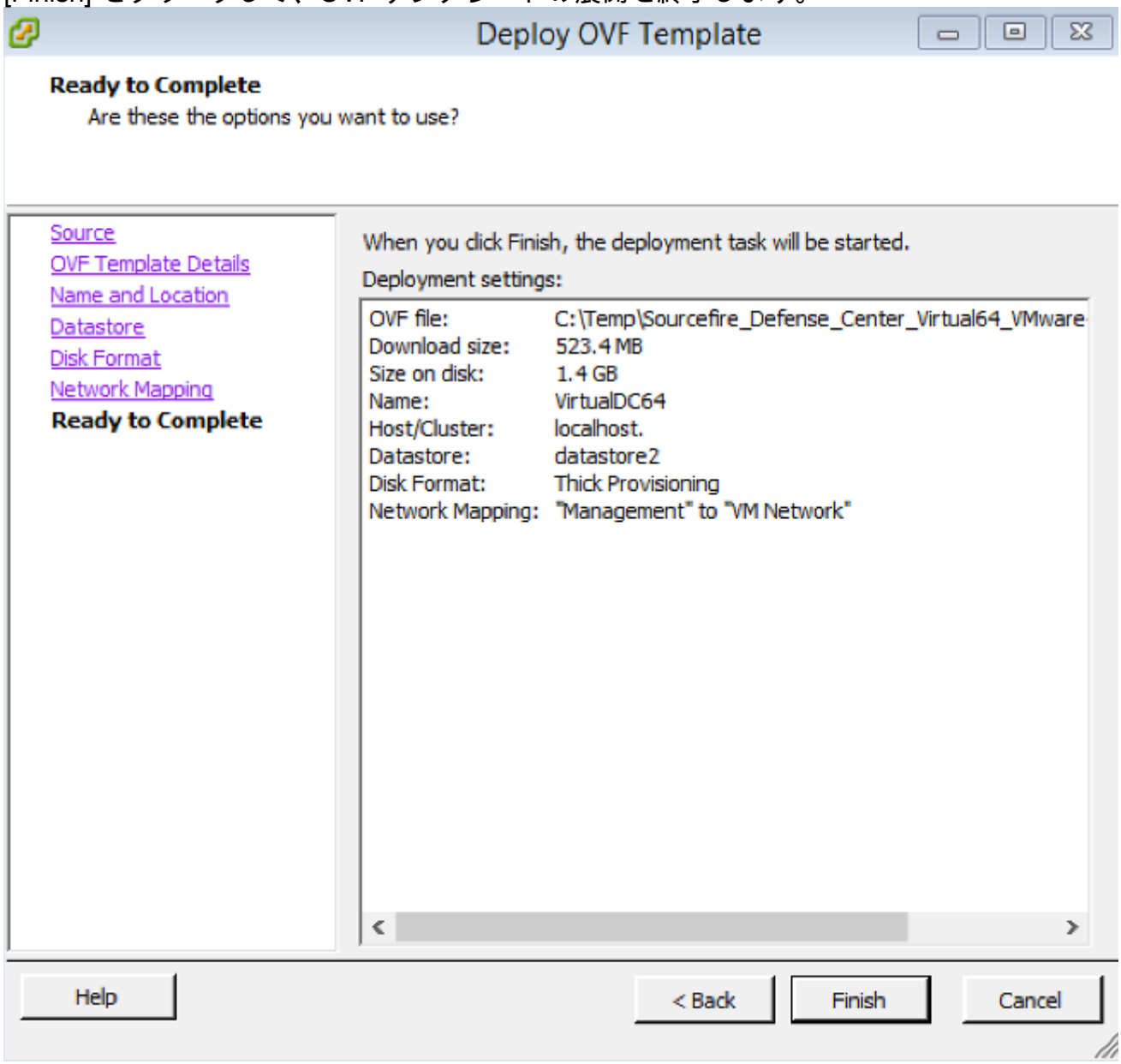
9. [Disk Format] に対して [Thick provisioned format] のオプション ボタンをクリックして、[Next] をクリックします。シックプロビジョニング形式では、仮想ディスクの作成時に必要なディスク領域が割り当てられます。シンプロビジョニング形式では、必要に応じて領域が使用されます。



10. [Network Mapping] セクションで、FireSIGHT Management Center の管理インターフェイスを VMware ネットワークに関連付けて [Next] をクリックします。

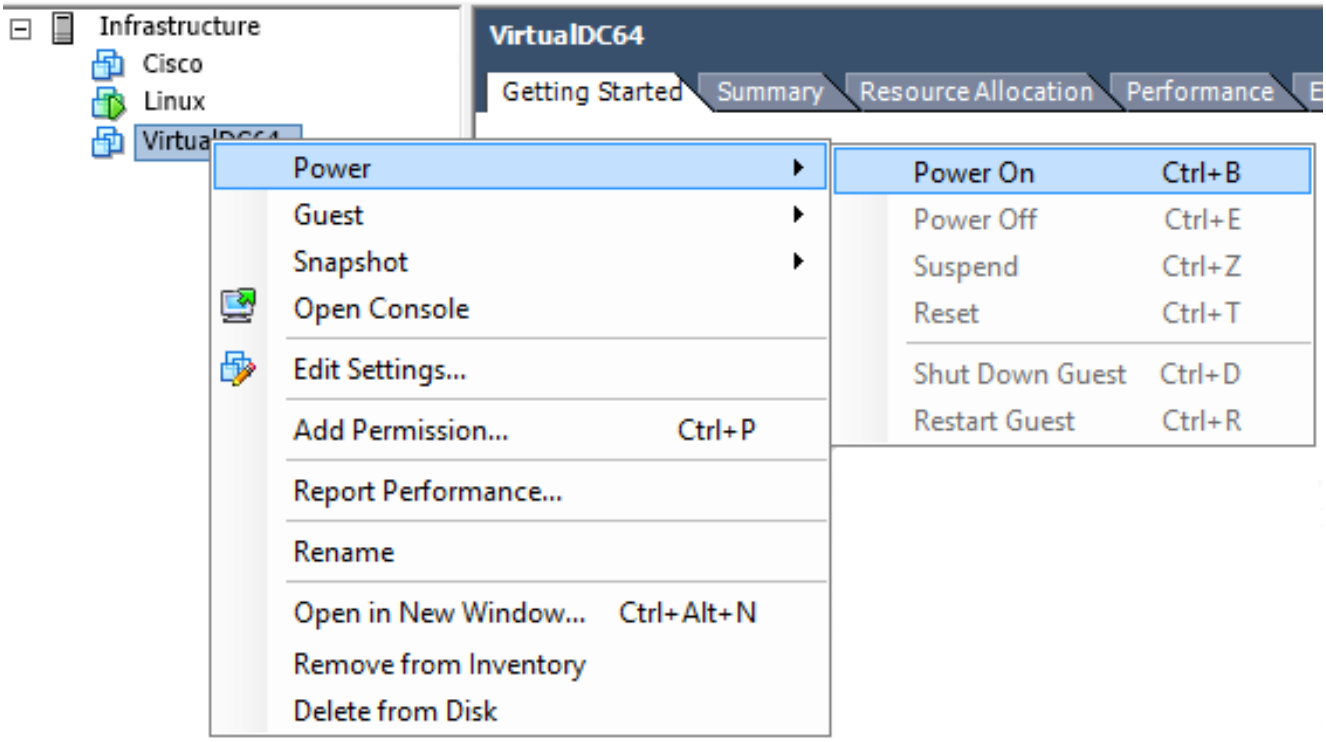


11. [Finish] をクリックして、OVF テンプレートの展開を終了します。

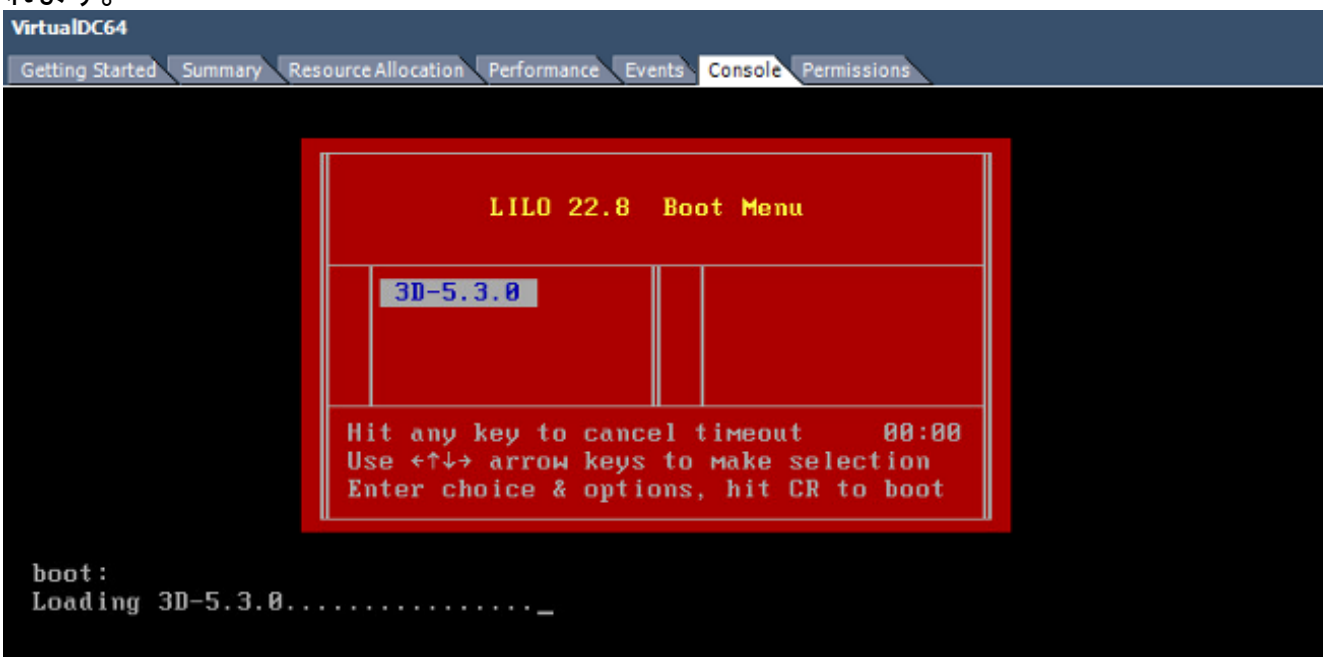


電源投入と初期設定の実行

1. 新しく作成された仮想マシンにアクセスします。 サーバ名を右クリックし、[Power] > [Power On] を選択して、サーバの最初の起動を実行します。



2. [Console] タブを選択し、サーバのコンソールを監視します。[LILO Boot] メニューが表示されます。



BIOS のデータのチェックが正常に終了すると、初期設定プロセスが開始されます。最初の起動には少し時間がかかることがありますが、これは最初に設定データベースを初期設定するためです。

```
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
_
```

初期設定プロセスが完了すると、「No such device」というメッセージが表示されることがあります。

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

3. [Enter] キーを押すとログイン プロンプトが表示されます。

```
 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: _
```

注：メッセージ「WRITE SAME failed.手動でゼロにする」 システムを初めて起動した後に表示される場合があります。これは不具合を示すものではなく、VMwareストレージドライバがWRITE SAMEコマンドをサポートしていないことを正しく示します。 システムはこのメッセージを表示し、フォールバックコマンドを実行して同じ操作を実行します。

ネットワークの設定

1. Sourcefire3D のログイン プロンプトで、ログインするには次のクレデンシャルを使用します。 バージョン 5.x の場合ユーザ名:**admin**パスワード：**Sourcefire**バージョン 6.x 以降の場合ユーザ名:**admin**パスワード：**Admin123ヒント**：GUI の初期設定のプロセスにおいて、デフォルトのパスワードを変更することができます。
2. ネットワークの初期設定は、スクリプトで行います。スクリプトは root ユーザとして実行する必要があります。rootユーザーに切り替えるには、**sudo su – コマンド**とパスワード**SourcefireまたはAdmin123**（6.x用）を入力します。 root ユーザとして Management Center のコマンド ラインにログインした場合は注意してください。

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

3. ネットワークの設定を開始するには、**root として、configure-network** スクリプトを入力します。

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

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

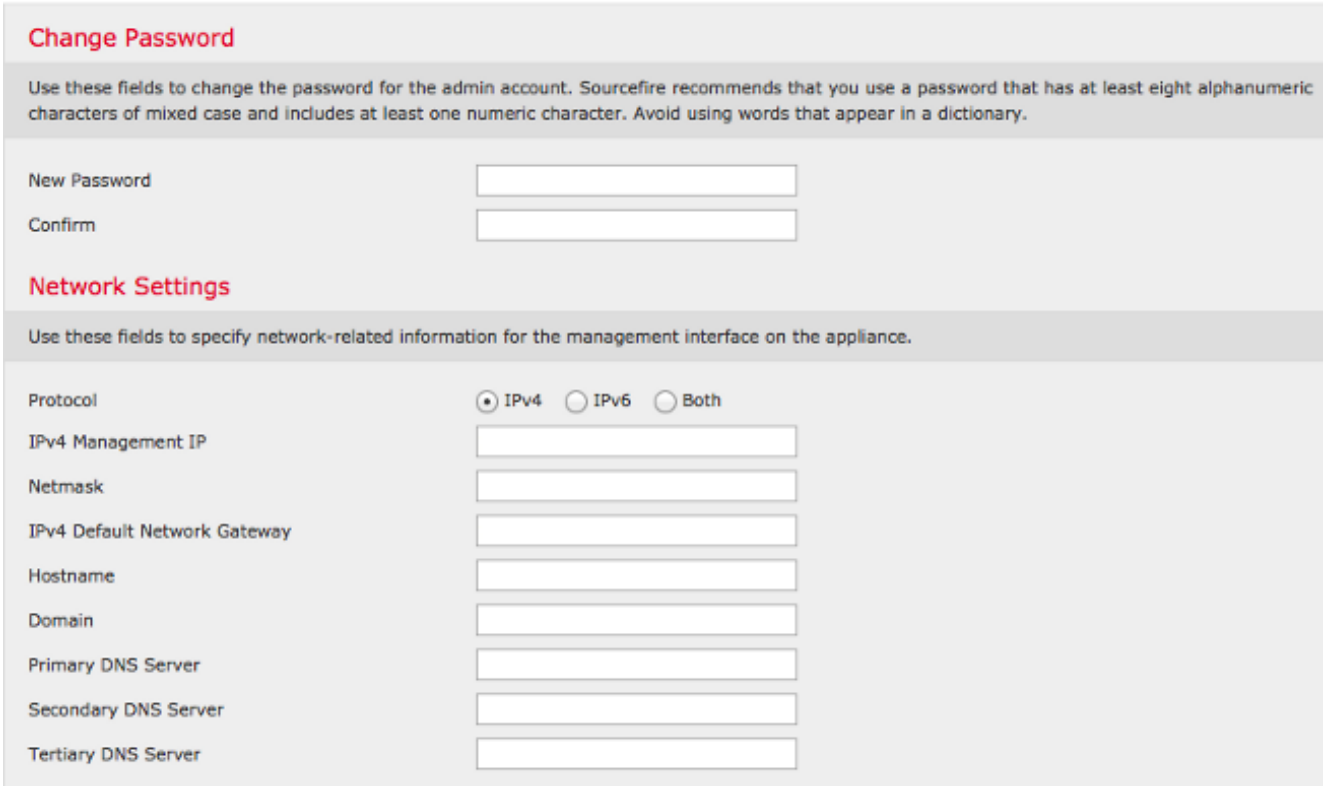
管理 IP アドレス、ネットマスク、およびデフォルト ゲートウェイを指定するよう要求され

ます。設定を確定すると、ネットワーク サービスが再起動されます。結果として、管理インターフェイスが停止して、その後、元に戻ります。

```
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:~# _
```

初期設定の実行

1. ネットワーク設定が完了したら、Web ブラウザを開いて、設定した IP を HTTPS（この例では https://192.0.2.2）を通じて検索します。 要求された場合は、デフォルトの SSL 証明書を認証します。ログインには次のクレデンシャルを使用します。バージョン 5.x の場合 ユーザ名:**admin**パスワード：**Sourcefire**バージョン 6.x 以降の場合ユーザ名:**admin**パスワード：**Admin123**
2. 次の画面では、パスワードの変更およびサービス利用規約の承認を除いて、GUI のすべての設定セクションはオプションです。 情報がわかっている場合は、Management Center の初期設定を簡単に行うために、セットアップ ウィザードを使用することをお勧めします。設定が完了したら [Apply] をクリックして、Management Center および登録したデバイスに対して設定を適用します。 設定オプションの概要は次のとおりです。**Change Password：** デフォルトの admin アカウントのパスワードを変更することができます。 パスワードを変更する必要があります。 **Network Settings：** アプライアンスまたは仮想マシンの管理インターフェイスに対して事前設定されている IPv4 およびIPv6 ネットワークの設定を変更することができます。**Time Settings：** Management Center を信頼できる NTP ソースと同期させることを推奨します。IPS センサーは、システム ポリシーを通じて Management Center の時刻と同期するように設定することができます。 オプションで、時刻、および表示のタイム ゾーンを手動で設定することができます。**Recurring Rule Update Imports：** Snort ルールの定期更新を有効にして、オプションで初期設定中にインストールできます。**Recurring Geolocation Updates：** 地理情報ルールの定期更新を有効にして、オプションで初期設定中にインストールできます。**Automatic Backups：** 設定の自動的なバックアップをスケジュールします。**License Settings：** 機能ライセンスを追加します。**Device Registration：** ライセンスを追加し、最初のアクセス制御ポリシーを、あらかじめ登録されているデバイスに適用することができます。 ホスト名/IP アドレスと登録キーは、FirePOWER IPS モジュールで設定した IP アドレスと登録キーと一致しなければなりません。**End User License Agreement：** EULA の承認は必須です。



関連情報

- VMware 向け FirePOWER Management Center 仮想クイック スタート ガイド バージョン 6.0
- テクニカル サポートとドキュメント – Cisco Systems