

دليل FireSIGHT Management Center VMware ESXi

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المكونات المستخدمة](#)
- [التكوين](#)
- [نشر قالب OVF](#)
- [تشغيل التشغيل والتهيئة الكاملة](#)
- [تكوين إعدادات الشبكة](#)
- [تنفيذ الإعداد الأولي](#)
- [معلومات ذات صلة](#)

المقدمة

يوضح هذا المستند الإعداد الأولي لمركز إدارة FireSIGHT (المعروف أيضا باسم Defense Center) الذي يعمل على برنامج VMware ESXi. يتيح لك مركز إدارة FireSIGHT إدارة جهاز واحد أو أكثر من أجهزة FirePOWER والجيل التالي من الأجهزة الافتراضية لنظام منع التطفل (NGIPS) وأجهزة الأمان المعدلة (ASA) مع خدمات FirePOWER.

ملاحظة: هذا المستند هو ملحق لدليل تثبيت نظام FireSIGHT ودليل المستخدم. للحصول على سؤال حول تكوين ESXi المحدد واستكشاف الأخطاء وإصلاحها، ارجع إلى قاعدة معارف VMware والمستندات.

المتطلبات الأساسية

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى الأنظمة الأساسية التالية:

- Cisco FireSIGHT Management Center
- الجهاز الظاهري Cisco FireSIGHT Management Center
- VMware ESXi 5.0

في هذا المستند، يشير "الجهاز" إلى الأنظمة الأساسية التالية:

- أجهزة Sourcefire FirePOWER 7000 Series وأجهزة Series 8000
- الأجهزة الظاهرية Sourcefire NGIPS لـ VMware ESXi
- سلسلة Cisco ASA 5500-X مع خدمة FirePOWER

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

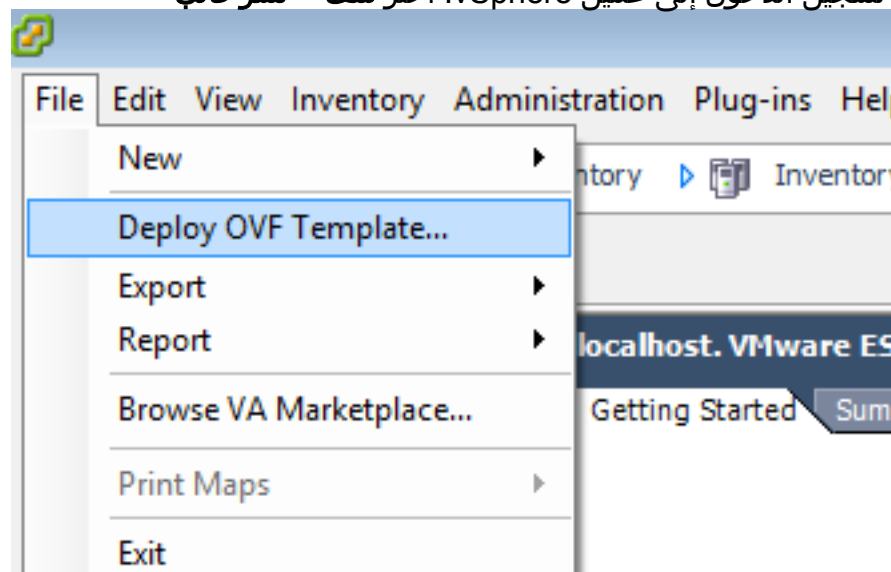
نشر قالب OVF

1. قم بتنزيل الجهاز الظاهري Cisco FireSIGHT Management Center من موقع [دعم وتنزيلات Cisco](#).
2. قم باستخراج محتويات ملف tar.gz إلى دليل محلي.
3. تمتع بالاتصال بخادم ESXi لديك باستخدام عميل vSphere من



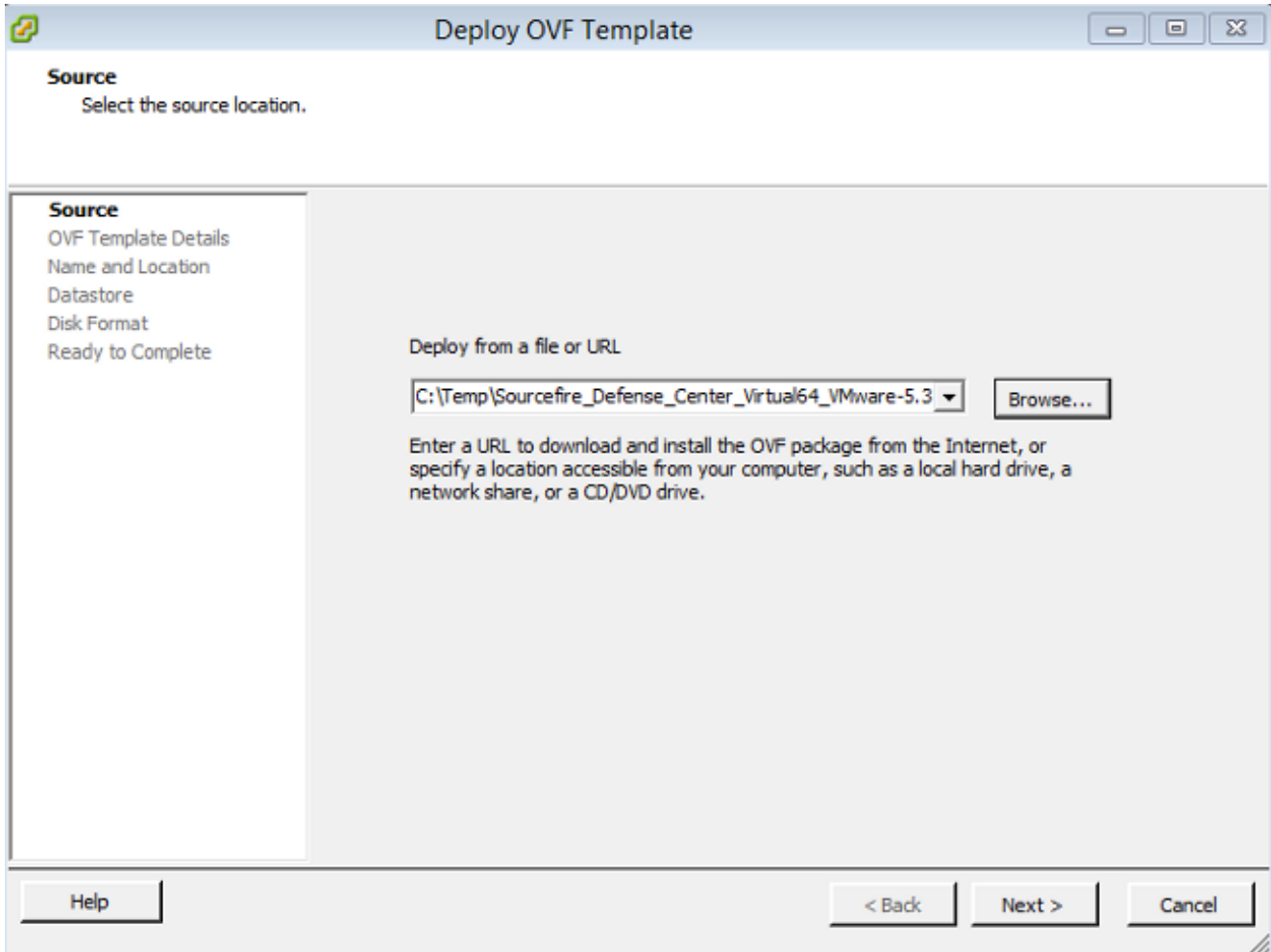
.VMware

4. بمجرد تسجيل الدخول إلى عميل vSphere، أختار ملف < نشر قالب

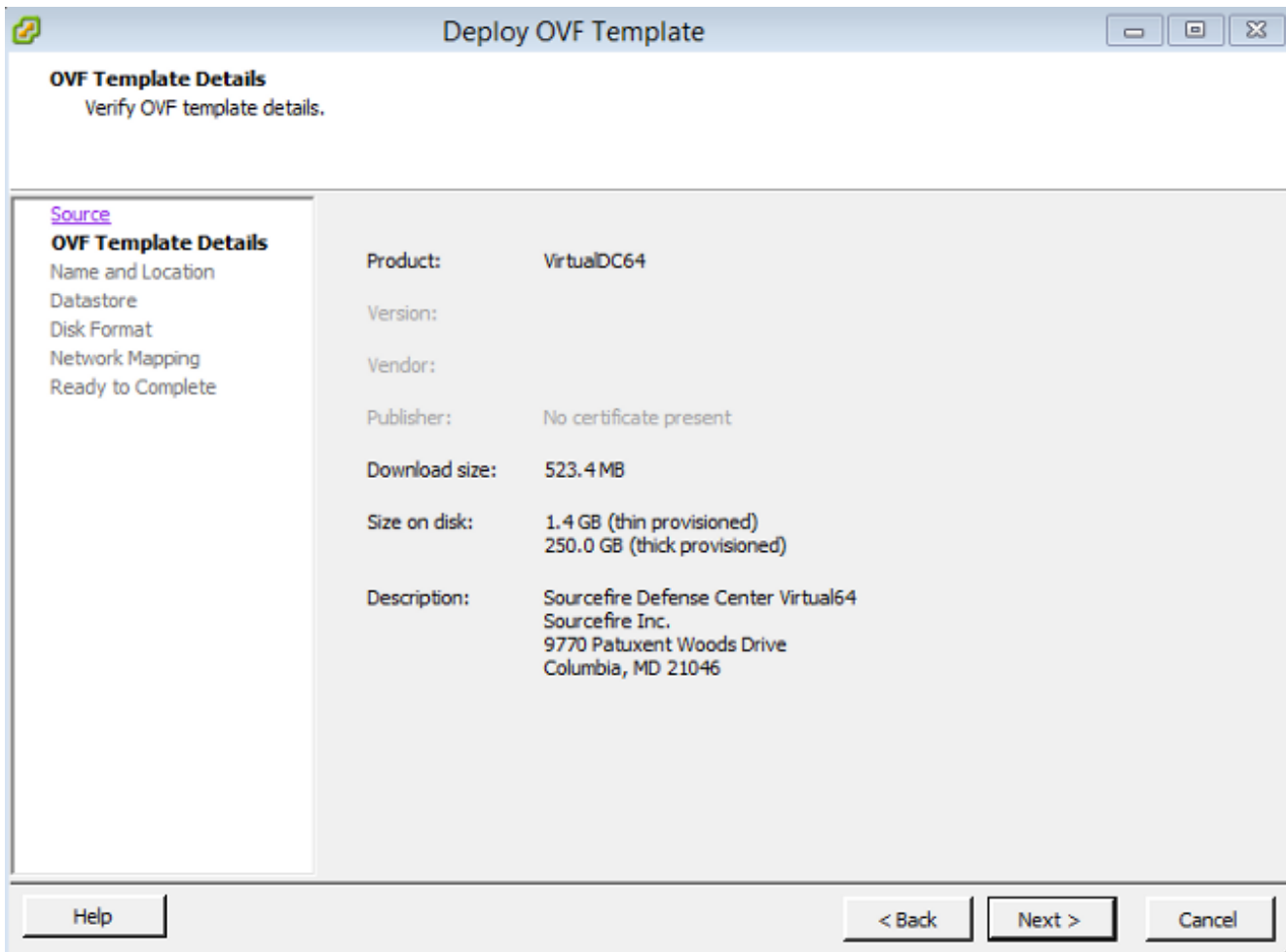


.OVF

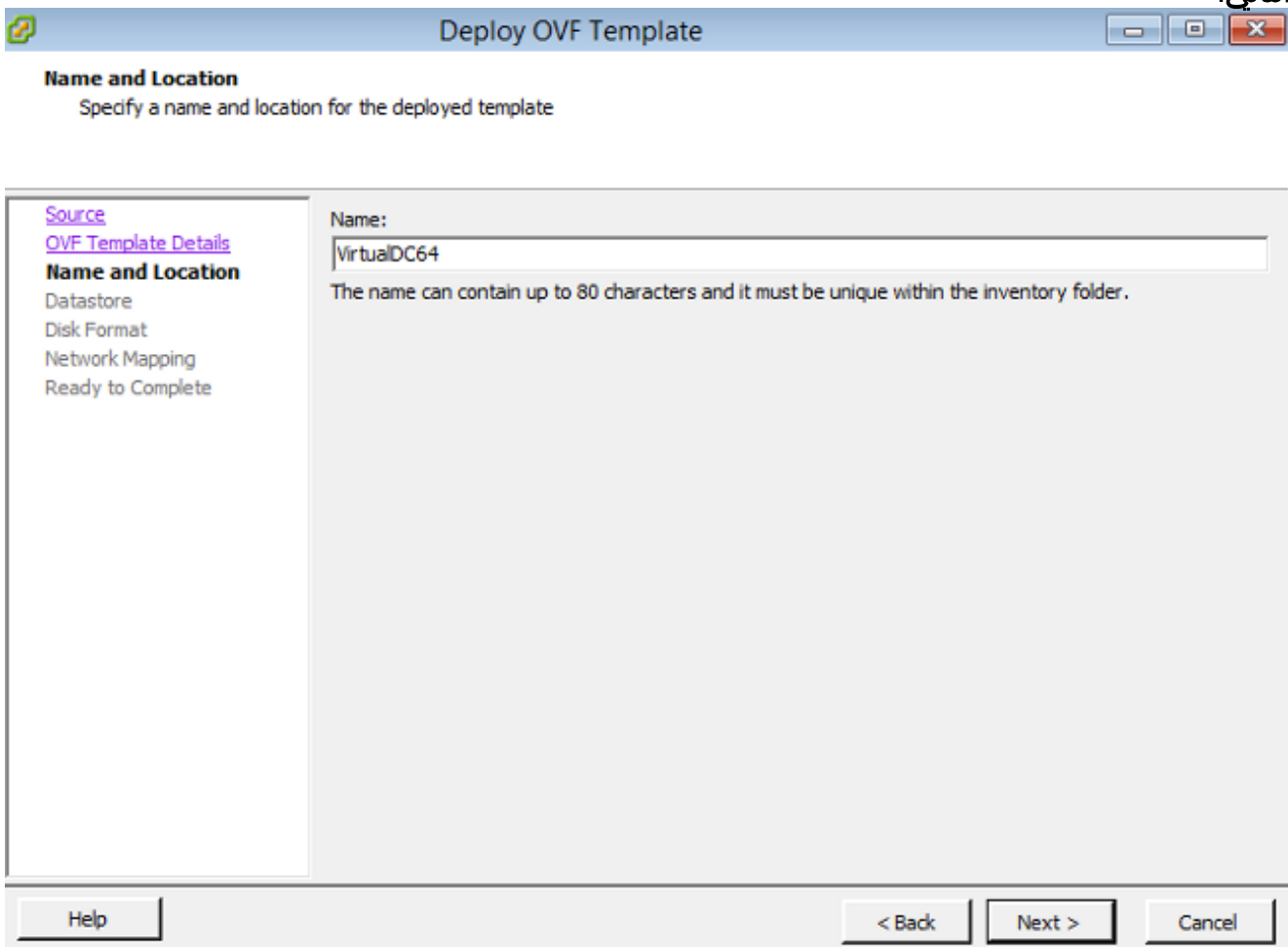
5. انقر فوق **إستعراض** وحدد موقع الملفات التي قمت باستخراجها في الخطوة 2. أختار ال OVF مبرد Sourcefire_defense_center_virtual64_VMware-ESXi-X.X.xxx.ovf وطققة بعد



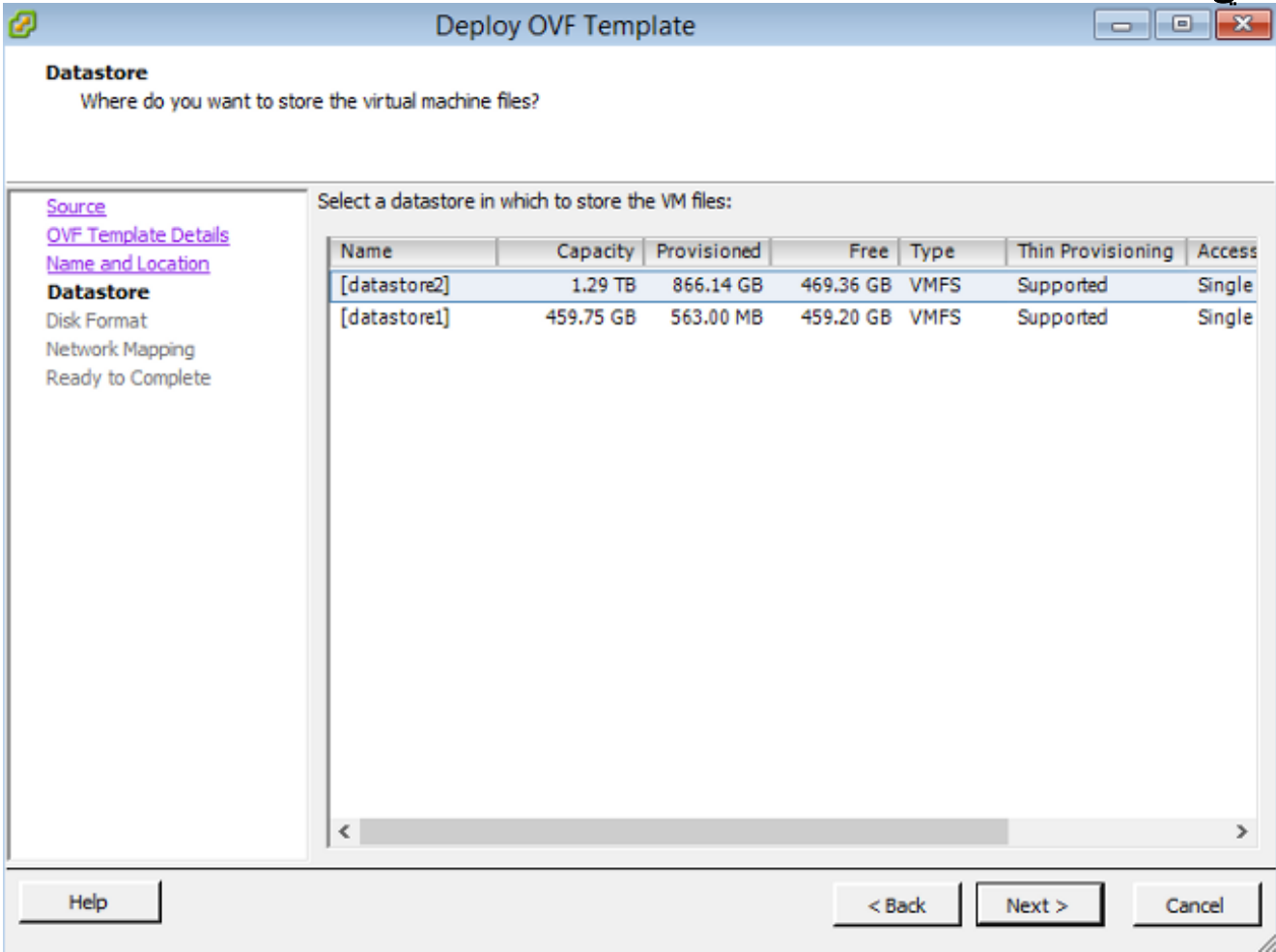
6. في شاشة تفاصيل قالب OVF، انقر التالي لقبول الإعدادات الافتراضية.



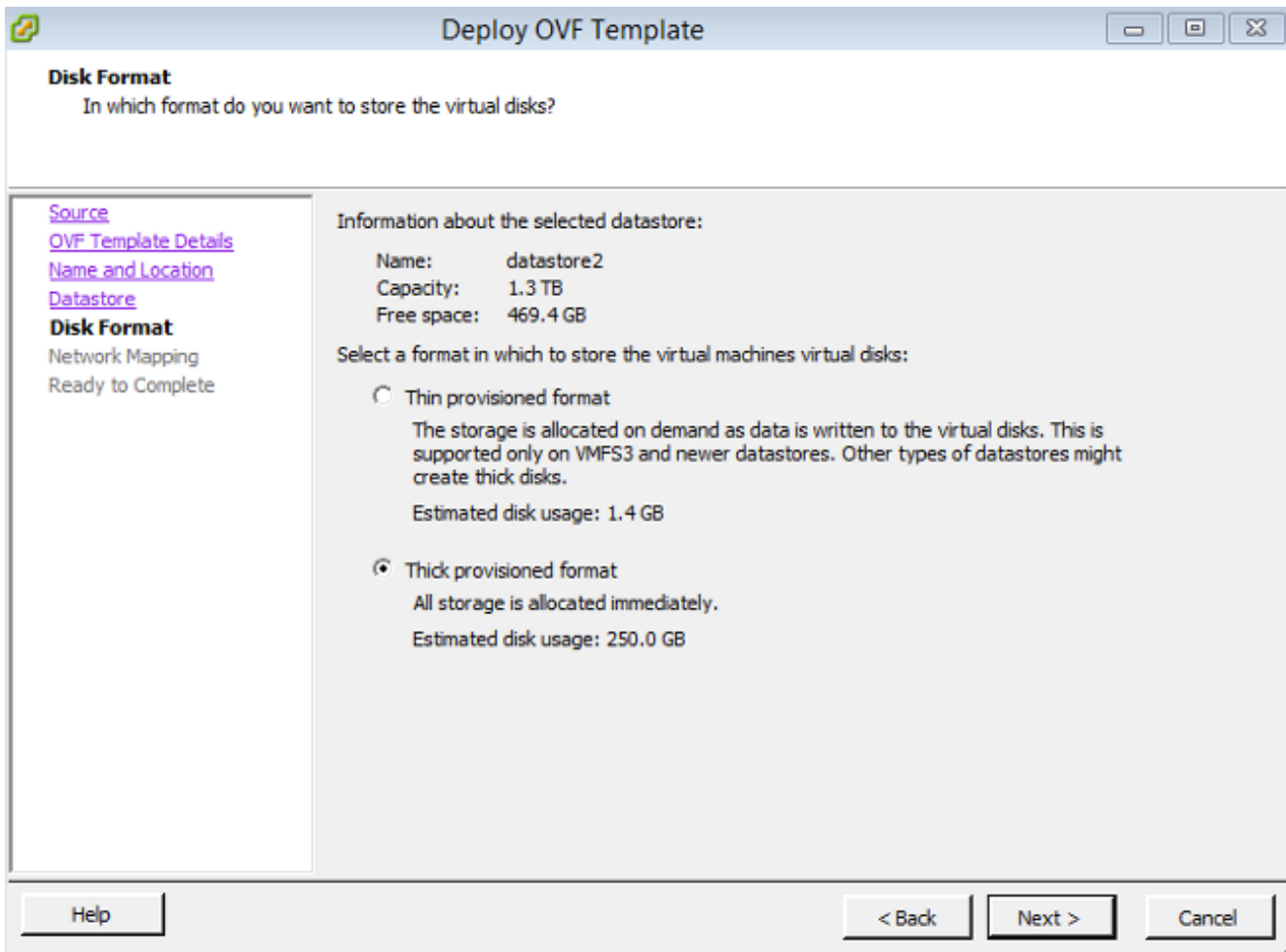
7. قم بتوفير اسم لمركز الإدارة وانقر فوق التالي.



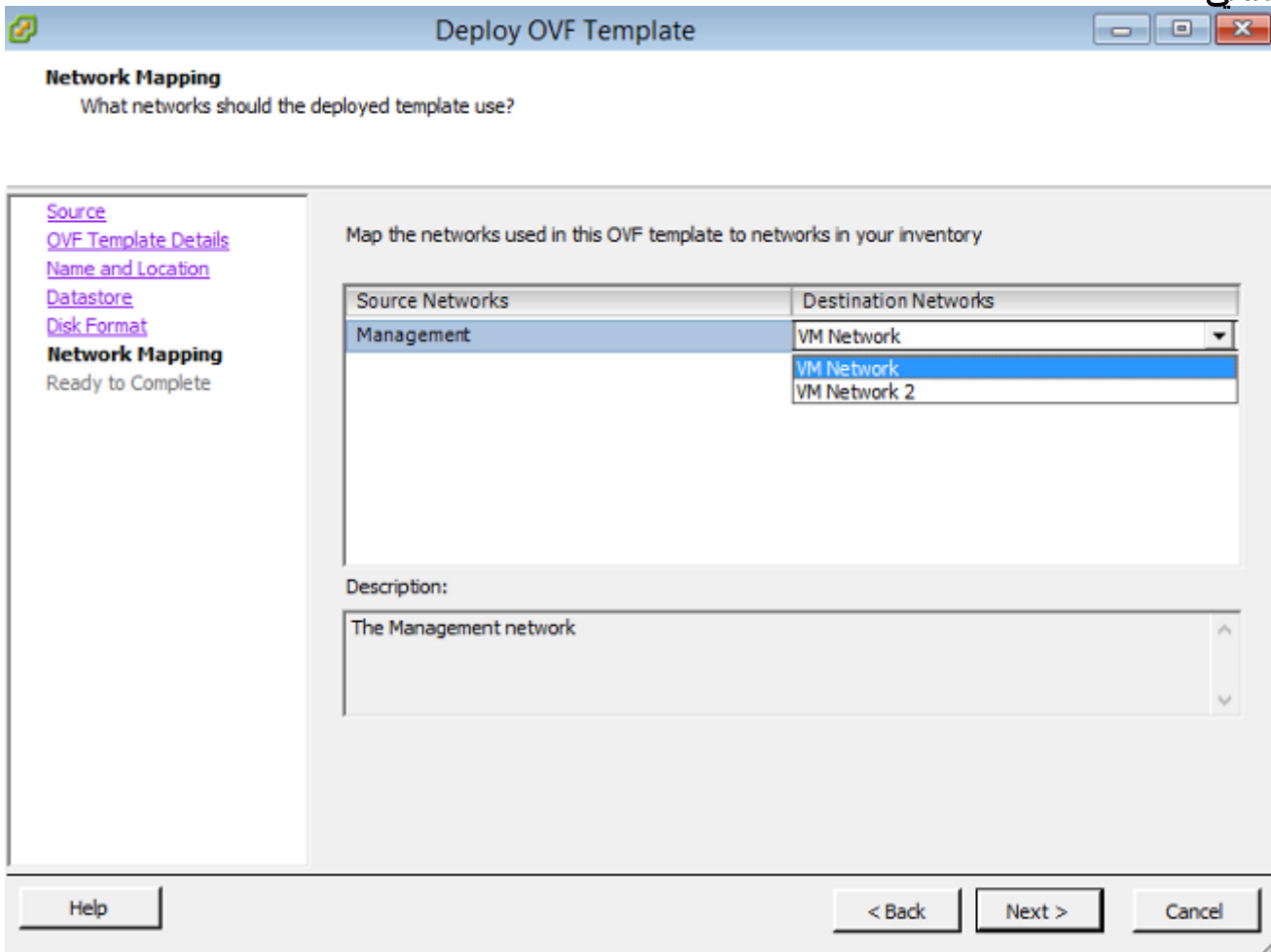
8. أختَر Datastore الذي تريد إنشاء الجهاز الظاهري عليه وانقر فوق التالي.

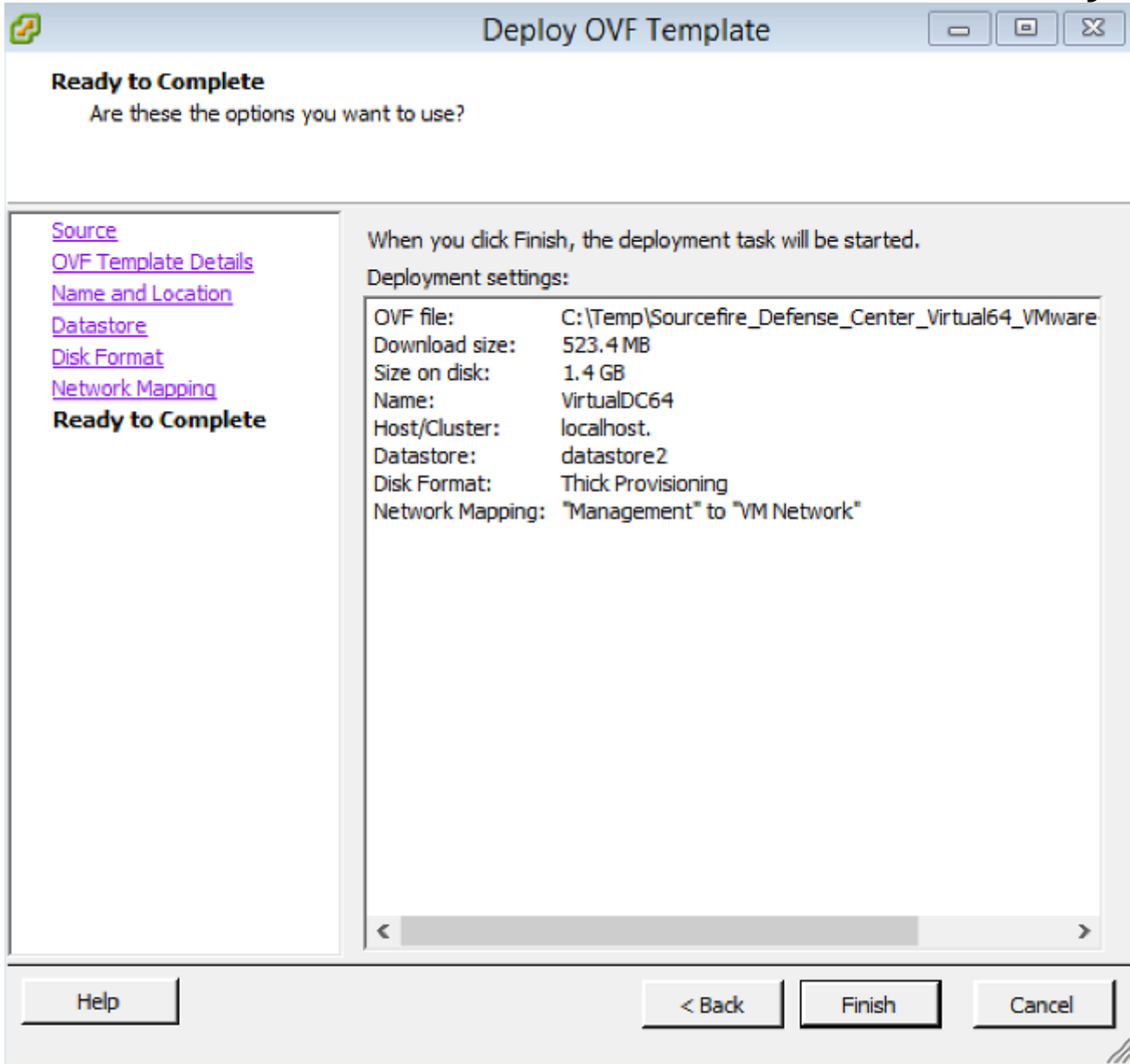


9. انقر فوق زر الخيار **تنسيق المزود السميكة لتنسيق القرص**، ثم انقر فوق **التالي**. يقوم تنسيق الإمداد السميكة بتخصيص مساحة القرص اللازمة في وقت إنشاء قرص ظاهري، بينما يستخدم تنسيق الإمداد الدقيق المساحة حسب الطلب.



10. في قسم تخطيط الشبكة، قم بإقران واجهة إدارة مركز إدارة FireSIGHT بشبكة VMware وانقر على التالي.





تشغيل التشغيل والتهيئة الكاملة

1. انتقل إلى الجهاز الظاهري الذي تم إنشاؤه حديثًا. انقر بزر الماوس الأيمن فوق اسم الخادم واختر الطاقة < تشغيل الطاقة لتمهيد الخادم لأول مرة.


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

—

وبمجرد اكتمالها، قد ترى رسالة لعدم وجود مثل هذا الجهاز.

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

—

3. اضغط على Enter للحصول على مطالبة تسجيل الدخول.

```
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: _
```

ملاحظة: فشلت رسالة الكتابة نفسها. قد يظهر الأمر يدويا zeroing بعد تمهيد النظام لأول مرة. لا يشير ذلك إلى وجود عيب، ولكنه يشير بشكل صحيح إلى أن برنامج تشغيل وحدة التخزين من VMware لا يدعم الأمر write نفسه. يعرض النظام هذه الرسالة، ويمضي باستخدام أمر احتياطي لتنفيذ العملية نفسها.

تكوين إعدادات الشبكة

1. في مطالبة تسجيل الدخول إلى Sourcefire3D، أستخدم بيانات الاعتماد هذه لتسجيل الدخول: للإصدار x.5 اسم المستخدم: admin وكلمة المرور: Sourcefire للإصدار x.6 والإصدارات الأحدث اسم المستخدم: admin وكلمة المرور: Admin123. ستتمكن من تغيير كلمة المرور الافتراضية في عملية الإعداد الأولي في واجهة المستخدم الرسومية (GUI).
2. يتم إجراء التكوين الأولي للشبكة باستخدام برنامج نصي. أنت تحتاج أن تقوم بتشغيل النص التنفيذي كمستخدم جذري. دخلت in order to مفتاح إلى الجذر مستعمل، ال sudo su - أمر مع الكلمة Sourcefire أو Admin123 (ل x.6).
- admin@Sourcefire3D:~\$ sudo su
:Password
3. دخلت in order to بدأت الشبكة تشكيل، ال configure-network برمجية كجذر.

```
root@Sourcefire3D:~# configure-network
Do you wish to configure IPv4? (y or n) y
```

ستتم مطالبتك بتوفير عنوان IP للإدارة وقناع الشبكة والبوابة الافتراضية. بمجرد تأكيد الإعدادات، تتم إعادة تشغيل خدمة الشبكة. ونتيجة لذلك، تنخفض واجهة الإدارة ثم تعود مرة أخرى.

```
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:~# _
```

تنفيذ الإعداد الأولي

1. بعد تكوين إعدادات الشبكة، افتح مستعرض ويب واستعرض إلى IP الذي تم تكوينه عبر HTTPS (<https://192.0.2.2> في هذا المثال). مصادقة شهادة SSL الافتراضية إذا طلب منك ذلك. أستخدم بيانات الاعتماد هذه لتسجيل الدخول: للإصدار x.5 اسم المستخدم: **admin** كلمة المرور: **Sourcefire** للإصدار x.6 والإصدارات الأحدث اسم المستخدم: **admin** كلمة المرور: **Admin123**
2. على الشاشة التي تلي، تكون جميع أقسام تكوين واجهة المستخدم الرسومية إختيارية باستثناء تغيير كلمة المرور وقبول شروط الخدمة. وفي حالة معرفة المعلومات، يوصى باستخدام معالج الإعداد لتبسيط التكوين الأولي لمركز الإدارة. وبمجرد تكوينها، انقر فوق **تطبيق** لتطبيق التكوين على مركز الإدارة والأجهزة المسجلة. توجد نظرة عامة مختصرة على خيارات التكوين على النحو التالي: **تغيير كلمة المرور**: يسمح لك بتغيير كلمة المرور لحساب المسؤول الافتراضي. مطلوب تغيير كلمة المرور. **إعدادات الشبكة**: يسمح لك بتعديل إعدادات شبكة IPv4 و IPv6 التي تم تكوينها مسبقاً لواجهة إدارة الجهاز أو الجهاز الظاهري. **إعدادات الوقت**: يوصى بمزامنة مركز الإدارة مع مصدر NTP يمكن الاعتماد عليه. يمكن تهيئة أجهزة استشعار IPS من خلال سياسة النظام لمزامنة وقتها مع "مركز الإدارة". وبشكل إختياري، يمكن تعيين الوقت والمنطقة الزمنية للعرض يدوياً. **عمليات الاستيراد المتكررة لتحديث القاعدة**: قم بتمكين تحديثات قاعدة الشخص المتكررة ويتم تثبيتها الآن إختيارياً أثناء الإعداد الأولي. **تحديثات الموقع الجغرافي المتكررة**: تمكين تحديثات قاعدة الموقع الجغرافي المتكررة والتثبيت إختيارياً الآن أثناء الإعداد الأولي. **النسخ الاحتياطية التلقائية**: جدولة عمليات النسخ الاحتياطي التلقائية للتكوين. **إعدادات الترخيص**: إضافة ترخيص الميزة. **تسجيل الأجهزة**: يسمح لك بإضافة سياسات التحكم في الوصول الأولية وترخيصها وتطبيقها على الأجهزة المسجلة مسبقاً. يجب أن يتطابق اسم المضيف/عنوان IP ومفتاح التسجيل مع عنوان IP ومفتاح التسجيل اللذين تم تكوينهما على الوحدة النمطية FirePOWER IPS. **إتفاق ترخيص المستخدم النهائي**: يلزم قبول قانون تكافؤ الفرص.

Change Password

Use these fields to change the password for the admin account. Sourcefire recommends that you use a password that has at least eight alphanumeric characters of mixed case and includes at least one numeric character. Avoid using words that appear in a dictionary.

New Password	<input type="text"/>
Confirm	<input type="text"/>

Network Settings

Use these fields to specify network-related information for the management interface on the appliance.

Protocol	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6 <input type="radio"/> Both
IPv4 Management IP	<input type="text"/>
Netmask	<input type="text"/>
IPv4 Default Network Gateway	<input type="text"/>
Hostname	<input type="text"/>
Domain	<input type="text"/>
Primary DNS Server	<input type="text"/>
Secondary DNS Server	<input type="text"/>
Tertiary DNS Server	<input type="text"/>

معلومات ذات صلة

- [دليل البدء السريع الظاهري لـ VMware J Firepower Management Center، الإصدار 6.0](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت
ملاعلاء انءمچي فني مدختسمل معدى وتحم مي دقتل ةيرشبلاو
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاغل مهتغب
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىلإ أمئاد عوچرلاب ي صؤتو تامچرتل هذه ةقدنع اهتيلوئسم Cisco
Systems (رفوتم طبارلا) ي لصلأل يزي لچنل دن تسمل