VMware ESXi에 FireSIGHT Management Center 구축

목차

소개

이 문서에서는 VMware ESXi에서 실행되는 FireSIGHT Management Center(Defense Center라고도 함)의 초기 설정에 대해 설명합니다.FireSIGHT Management Center를 사용하면 하나 이상의 FirePOWER 어플라이언스, NGIPS(Next Generation Intrusion Prevention System) 가상 어플라이언스, ASA(Adaptive Security Appliance) with FirePOWER Services를 관리할 수 있습니다.

> **참고:**이 문서는 FireSIGHT System Installation Guide 및 User Guide의 보충 자료입니다.ESXi 관련 구성 및 문제 해결 질문은 VMware 기술 자료 및 설명서를 참조하십시오.

사전 요구 사항

사용되는 구성 요소

이 문서의 정보는 다음 플랫폼을 기반으로 합니다.

- Cisco FireSIGHT Management Center
- Cisco FireSIGHT Management Center 가상 어플라이언스
- VMware ESXI 5.0

이 문서에서 "디바이스"는 다음 플랫폼을 가리킵니다.

- Sourcefire FirePOWER 7000 Series 어플라이언스 및 8000 Series 어플라이언스
- VMware ESXi용 Sourcefire NGIPS 가상 어플라이언스
- Cisco ASA 5500-X Series with FirePOWER Service

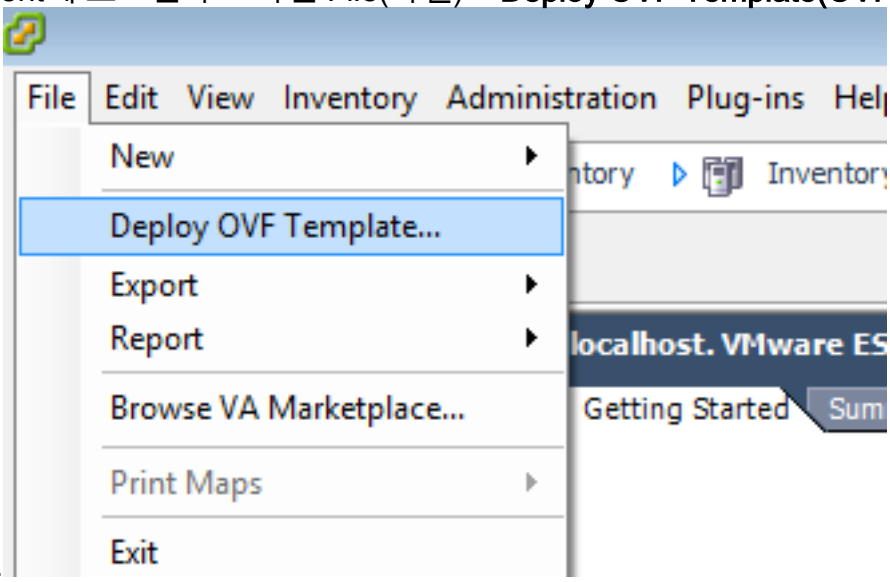
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

OVF 템플릿 구축

1. Cisco 지원 및 다운로드 사이트에서 **Cisco FireSIGHT Management Center Virtual Appliance**를 다운로드합니다.
2. tar.gz 파일의 내용을 로컬 디렉토리로 추출합니다.
3. VMware vSphere 클라이언트를 사용하여 ESXi **서버에 연결합니다**

4. vSphere Client에 로그인하고 나면 File(파일) **> Deploy OVF Template(OVF 템플릿 구축)을**

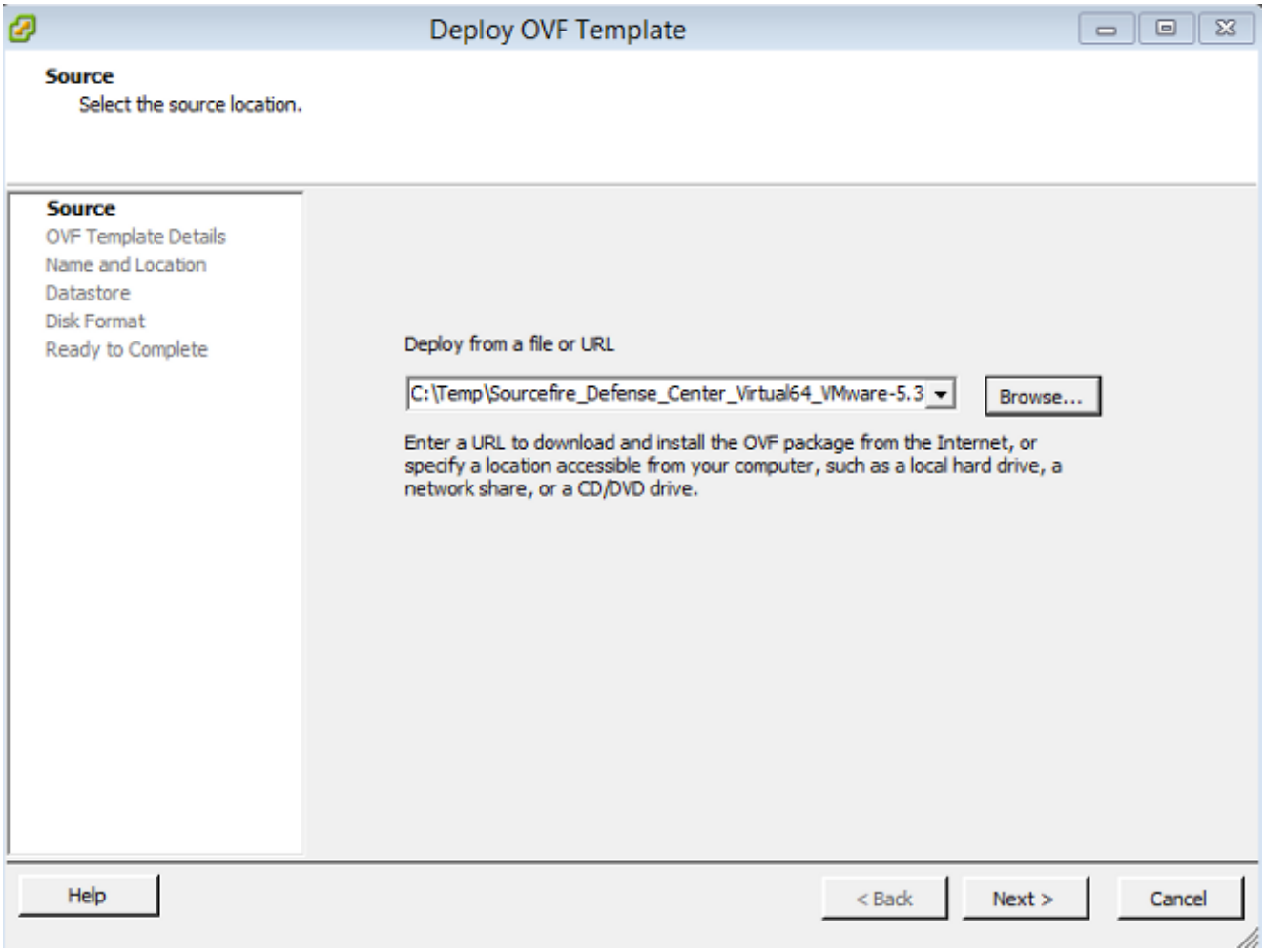


선택합니다.

5. Browse(**찾아보기**)를 클릭하고 2단계에서 추출한 파일을 찾습니다. OVF 파일

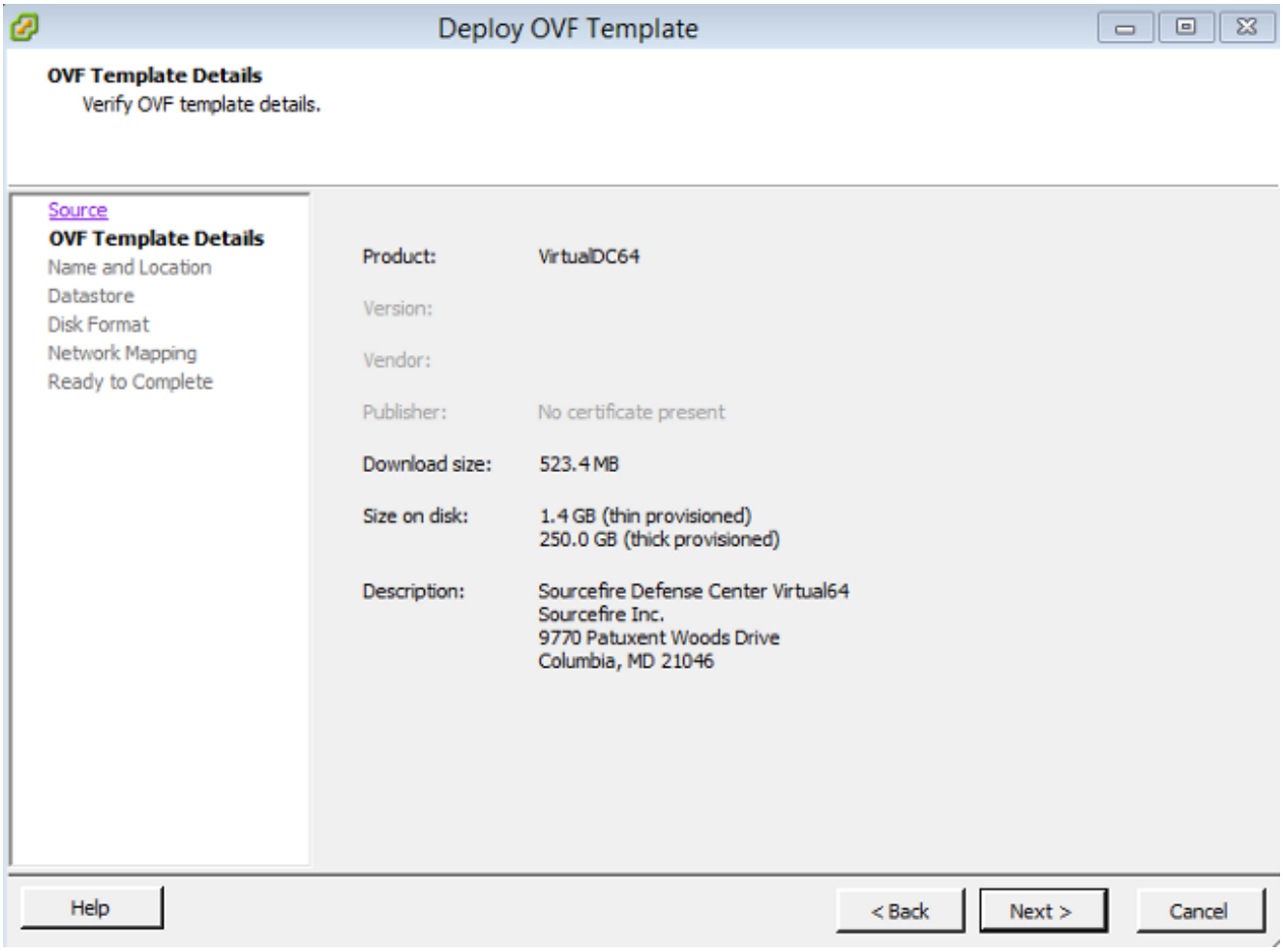
Sourcefire_Defense_Center_Virtual64_VMware-ESXi-X.X.xxx.ovf를 선택하고 **Next**를 클릭합니다

.



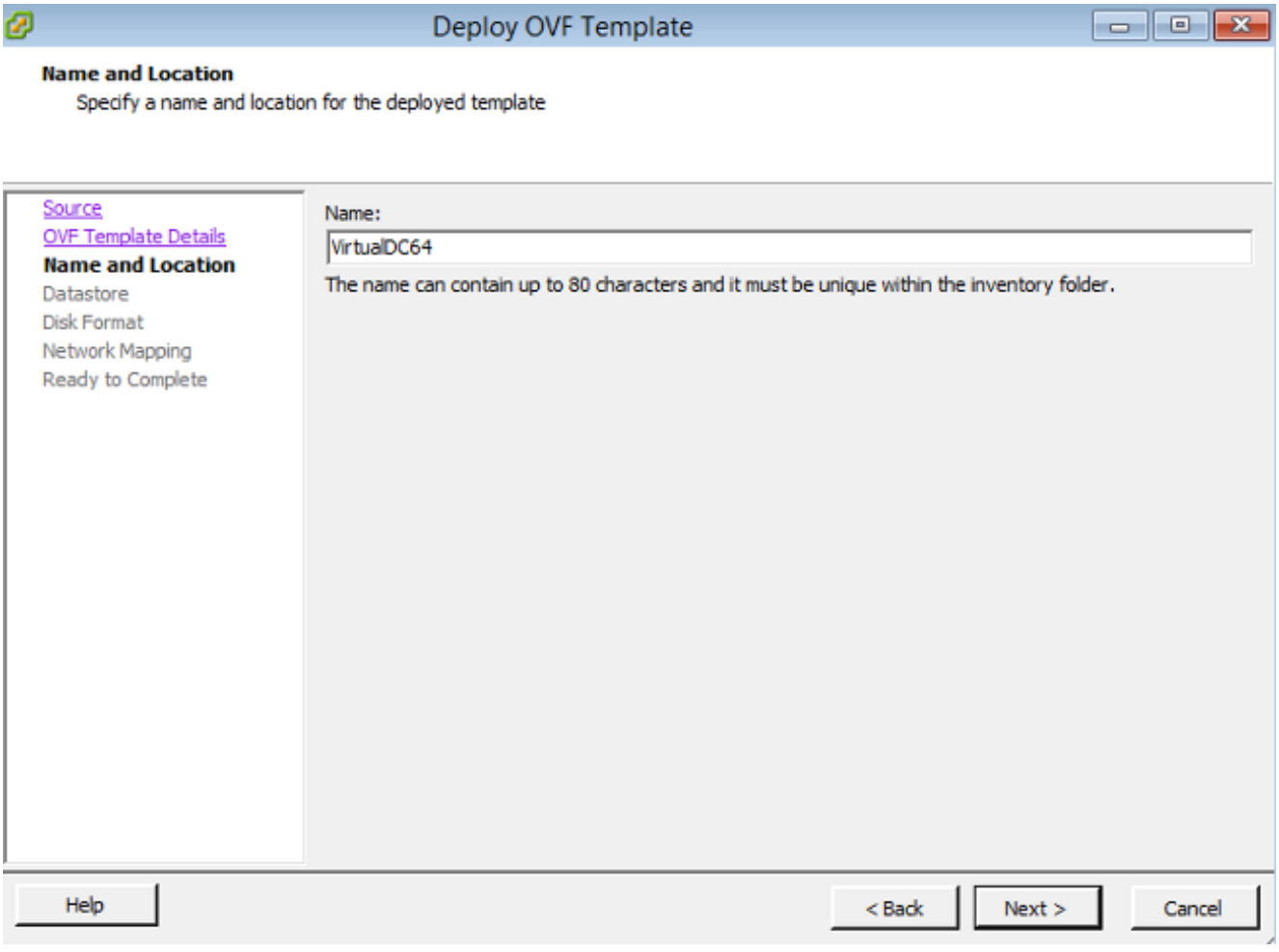
6. OVF **Template Details(OVF 템플릿 세부사항)** 화면에서 **Next(다음)**를 클릭하여 기본 설정을 적용합니다

.



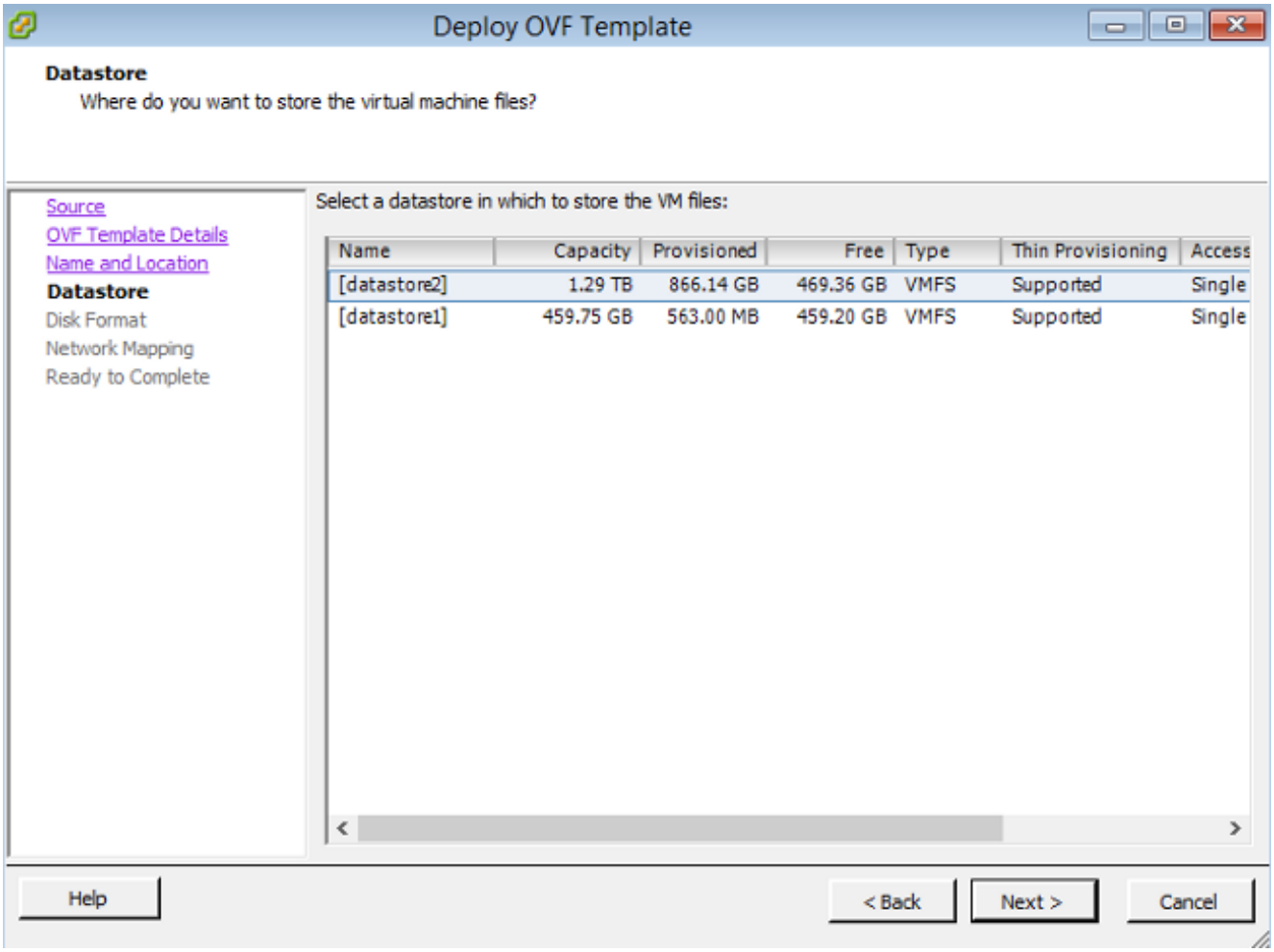
7. Management Center의 이름을 입력하고 Next(**다음**)를 클릭합니다

.



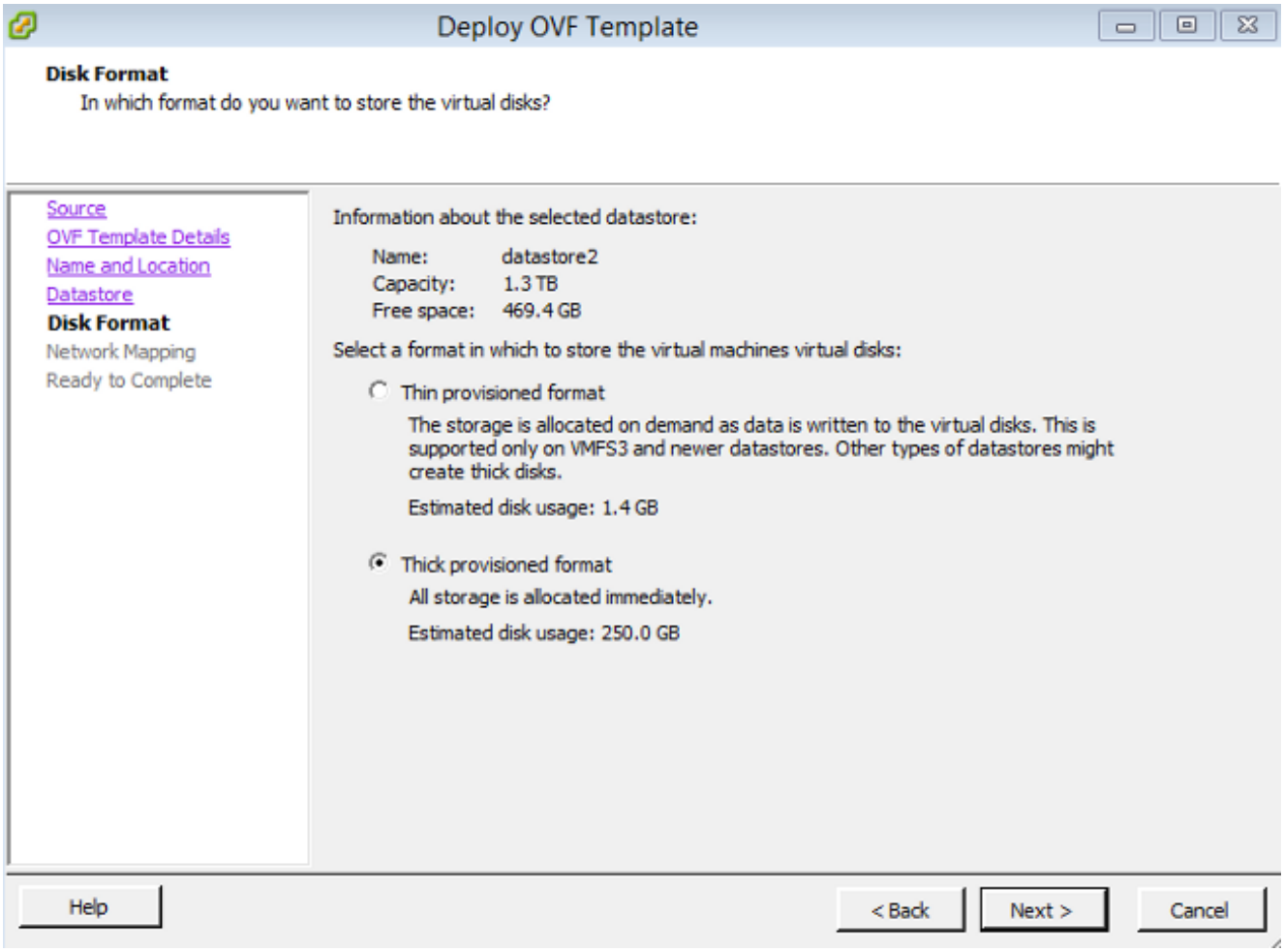
8. 가상 머신을 **생성할** 데이터 저장소를 선택하고 **Next**(다음)를 클릭합니다

.



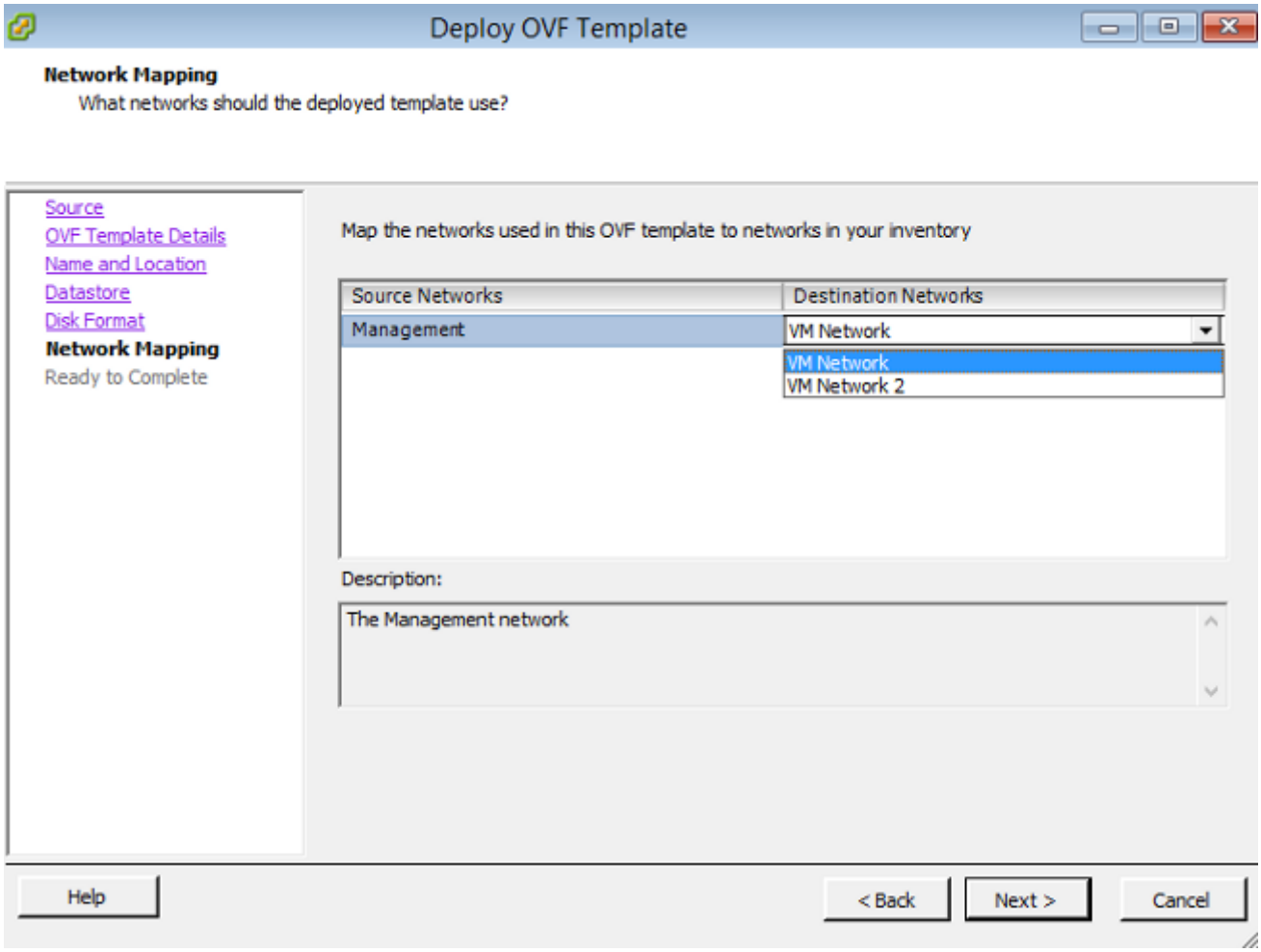
9. Disk Format(**디스크 형식**)에 대해 **Thick provisioned format(씩 프로비저닝 형식)** 라디오 버튼을 클릭하고 **Next(다음)**를 클릭합니다.thick provisioning 형식은 가상 디스크를 생성할 때 필요한 디스크 공간을 할당하는 반면, 씬 프로비저닝 형식은 온디맨드 공간을 사용합니다

.



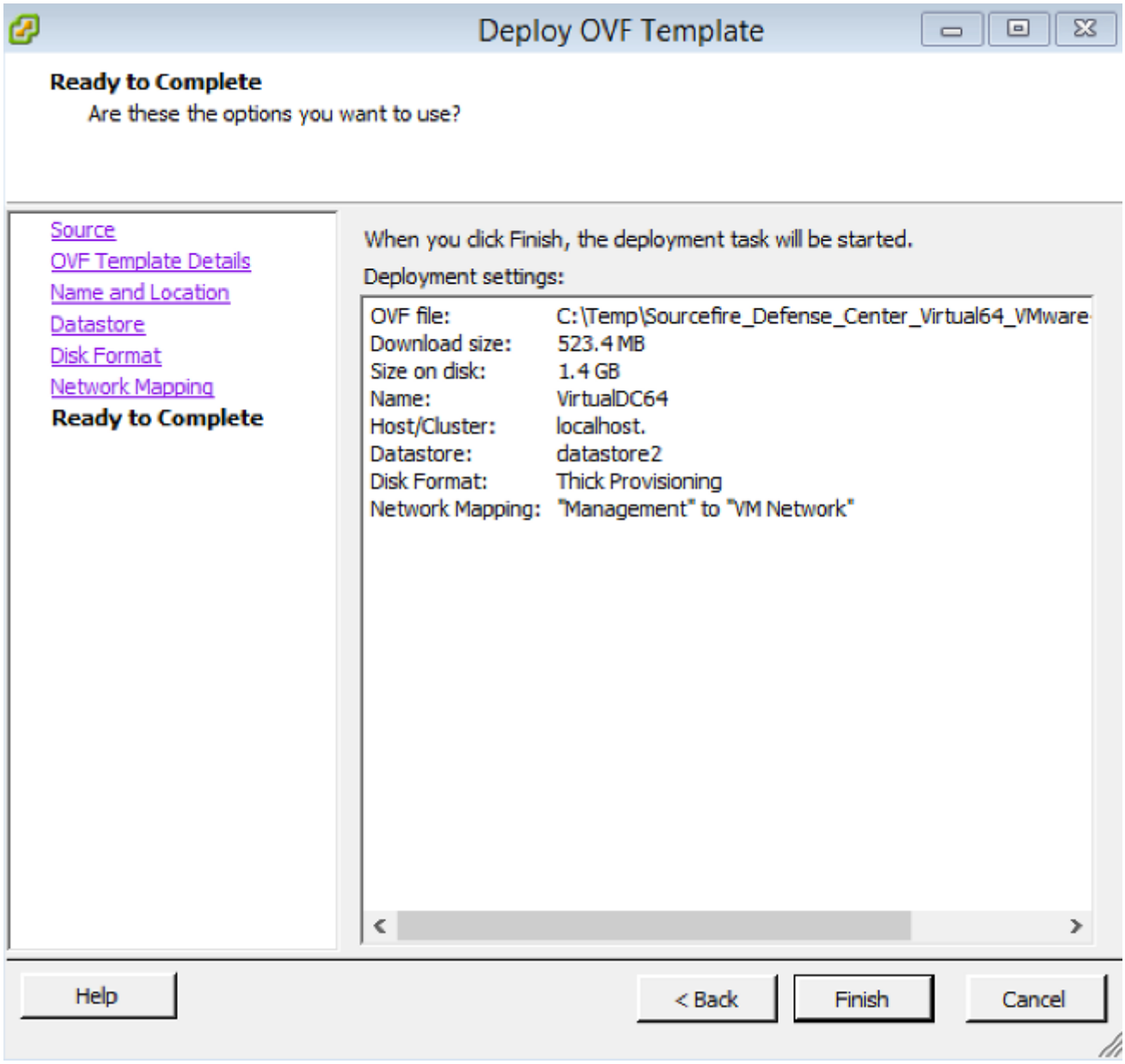
10. Network **Mapping**(네트워크 매핑) 섹션에서 FireSIGHT Management Center의 관리 인터페이스를 VMware 네트워크에 연결하고 Next(다음)를 **클릭합니다**

.



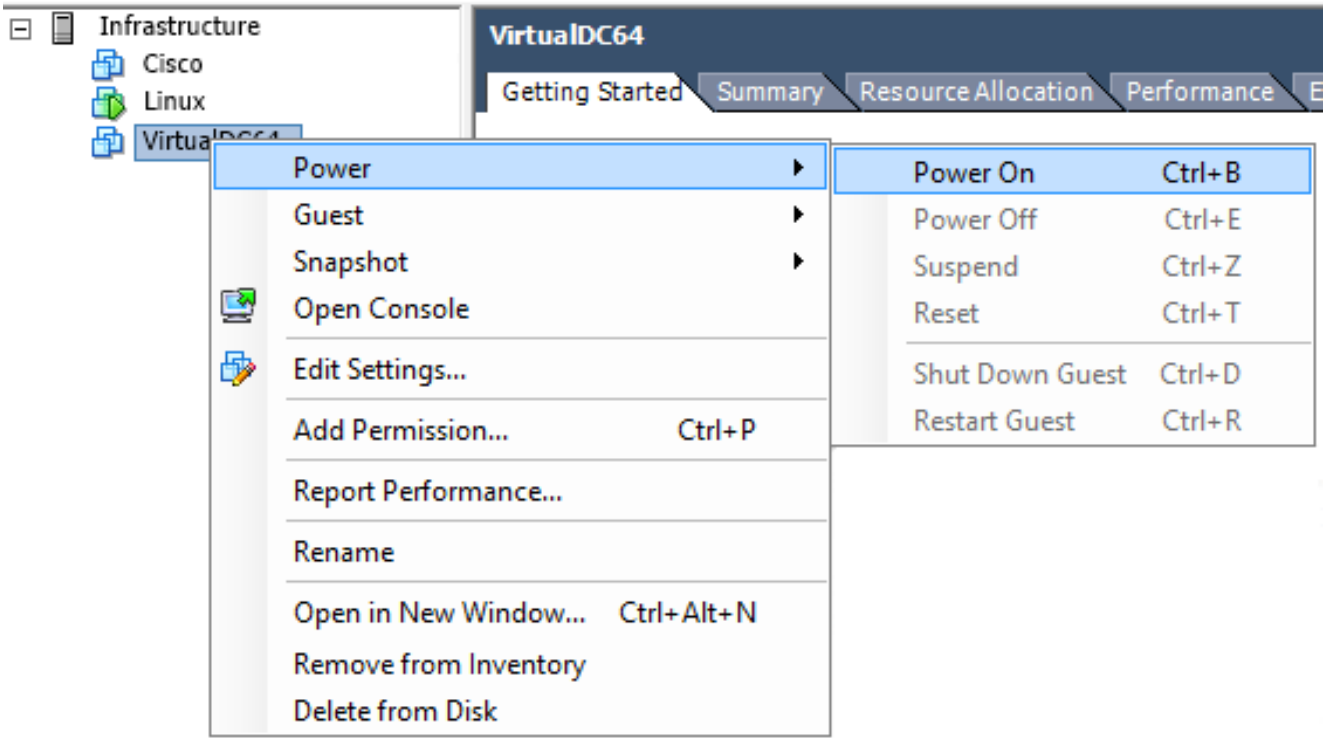
11. OVF 템플릿 구축을 완료하려면 Finish를 클릭합니다

.



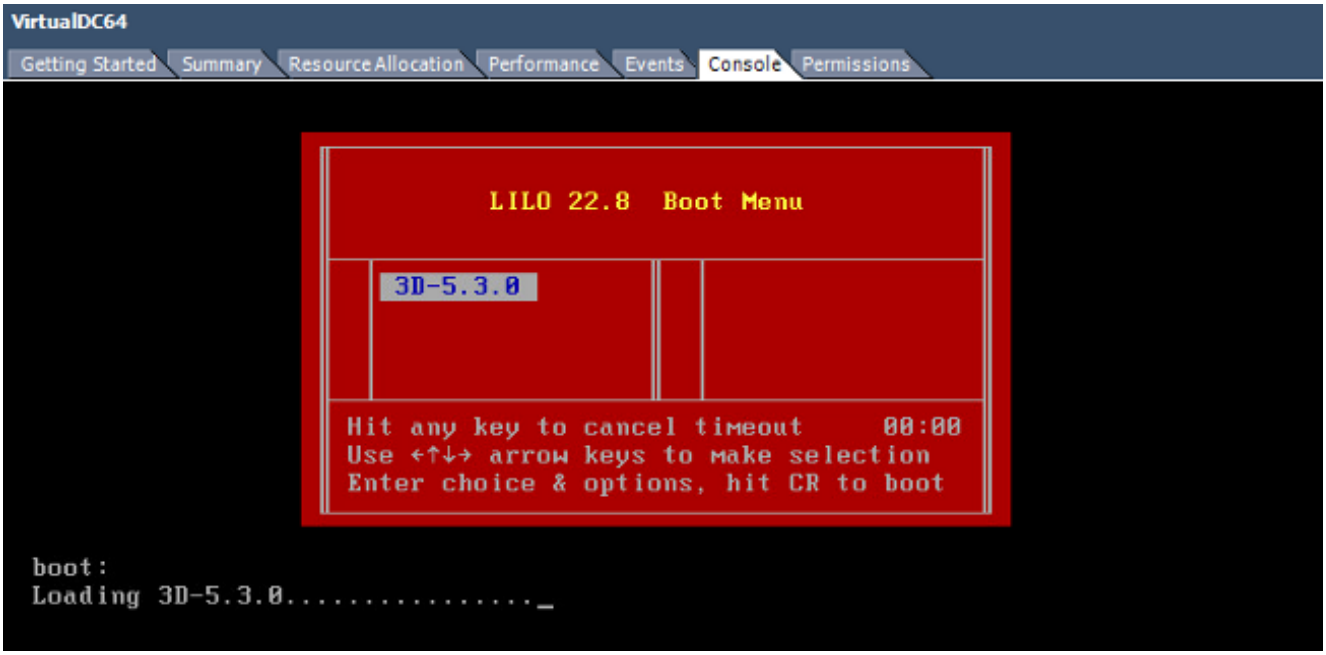
전원 켜기 및 초기화 완료

1. 새로 생성된 가상 머신으로 이동합니다. 서버 이름을 마우스 오른쪽 버튼으로 클릭하고 **Power(전원) > Power On(전원 켜기)을** 선택하여 서버를 처음으로 부팅합니다
.



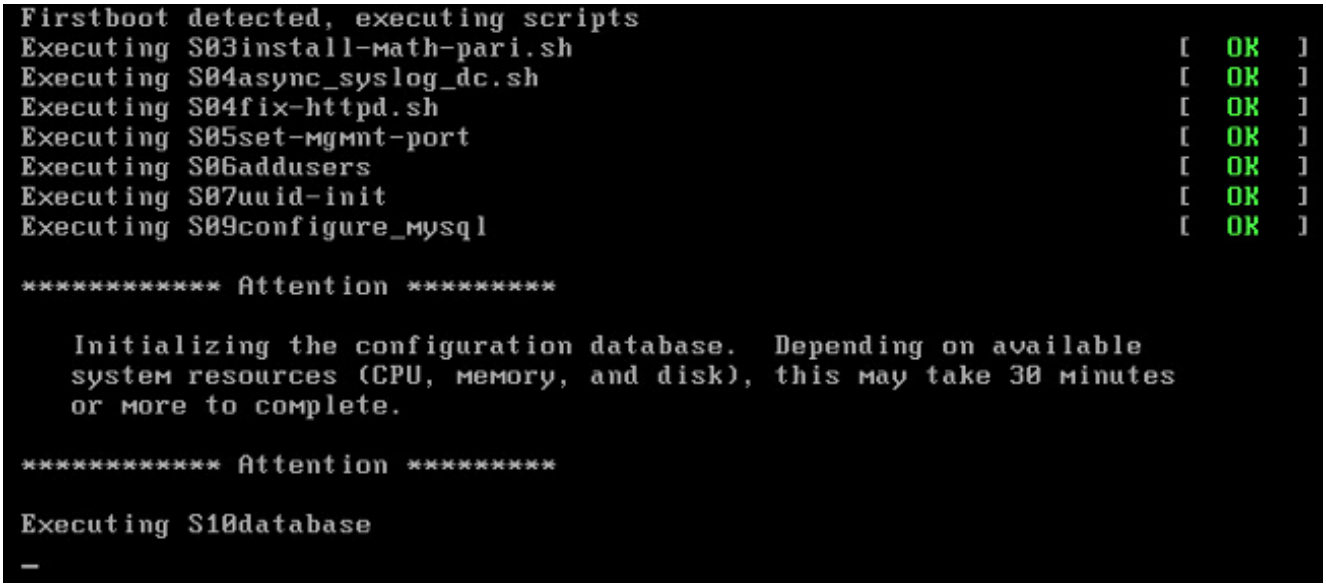
2. 서버 콘솔을 모니터링하려면 **Console** 탭으로 이동합니다.LILO Boot(LILO 부팅) 메뉴가 나타납니다

.



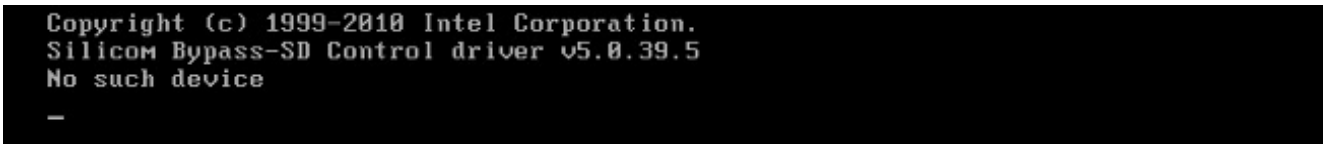
BIOS 데이터 확인이 성공하면 초기화 프로세스가 시작됩니다.구성 데이터베이스가 처음으로 초기화되므로 첫 번째 부팅을 완료하는 데 시간이 더 걸릴 수 있습니다

.



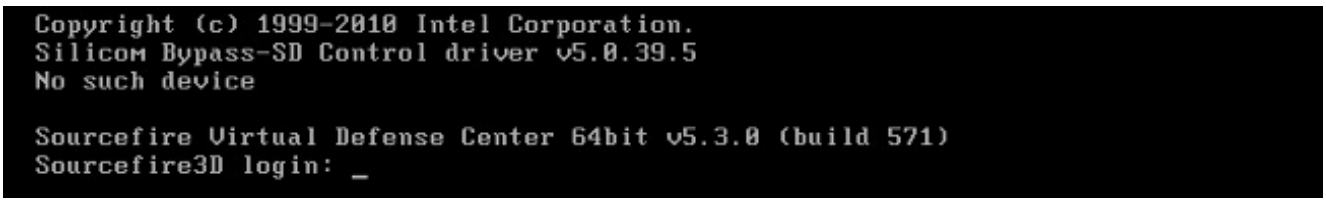
완료되면 해당 장치가 없다는 메시지가 표시될 수 있습니다

.



3. 로그인 프롬프트를 가져오려면 Enter를 누릅니다

.



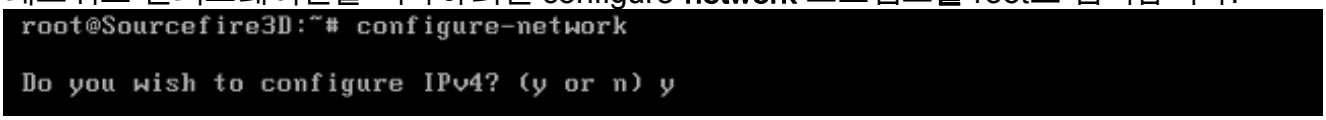
참고:"WRITE SAME(쓰기 동일) 메시지가 실패했습니다.수동 제로링." 시스템이 처음 부팅된 후에 나타날 수 있습니다.이는 결함을 나타내지 않으며, VMware 스토리지 드라이버가 WRITE SAME 명령을 지원하지 않음을 올바르게 나타냅니다. 시스템은 이 메시지를 표시하고 fallback 명령을 사용하여 동일한 작업을 수행합니다.

네트워크 설정 구성

1. Sourcefire3D 로그인 프롬프트에서 다음 자격 증명을 사용하여 로그인합니다. 버전 5.x사용자 이름:**관리자**암호:**Sourcefire**버전 6.x 이상사용자 이름:**관리자**암호:**관리자123팁**:GUI의 초기 설정 프로세스에서 기본 비밀번호를 변경할 수 있습니다.
2. 네트워크의 초기 컨피그레이션은 스크립트로 수행됩니다.루트 사용자로 스크립트를 실행해야 합니다.루트 사용자로 전환하려면 비밀번호 Sourcefire **또는 Admin123**(6.x용)와 함께 sudo su - 명령을 입력합니다. Management Center 명령줄에 루트 사용자로 로그인할 때 주의해야 합니다.

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

3. 네트워크 컨피그레이션을 시작하려면 configure-**network** 스크립트를 root로 입력합니다.



관리 IP 주소, 넷마스크 및 기본 게이트웨이를 제공하라는 메시지가 표시됩니다.설정을 확인하면 네트워크 서비스가 다시 시작됩니다.그 결과 관리 인터페이스가 다운된 다음 다시 돌아

옵니다

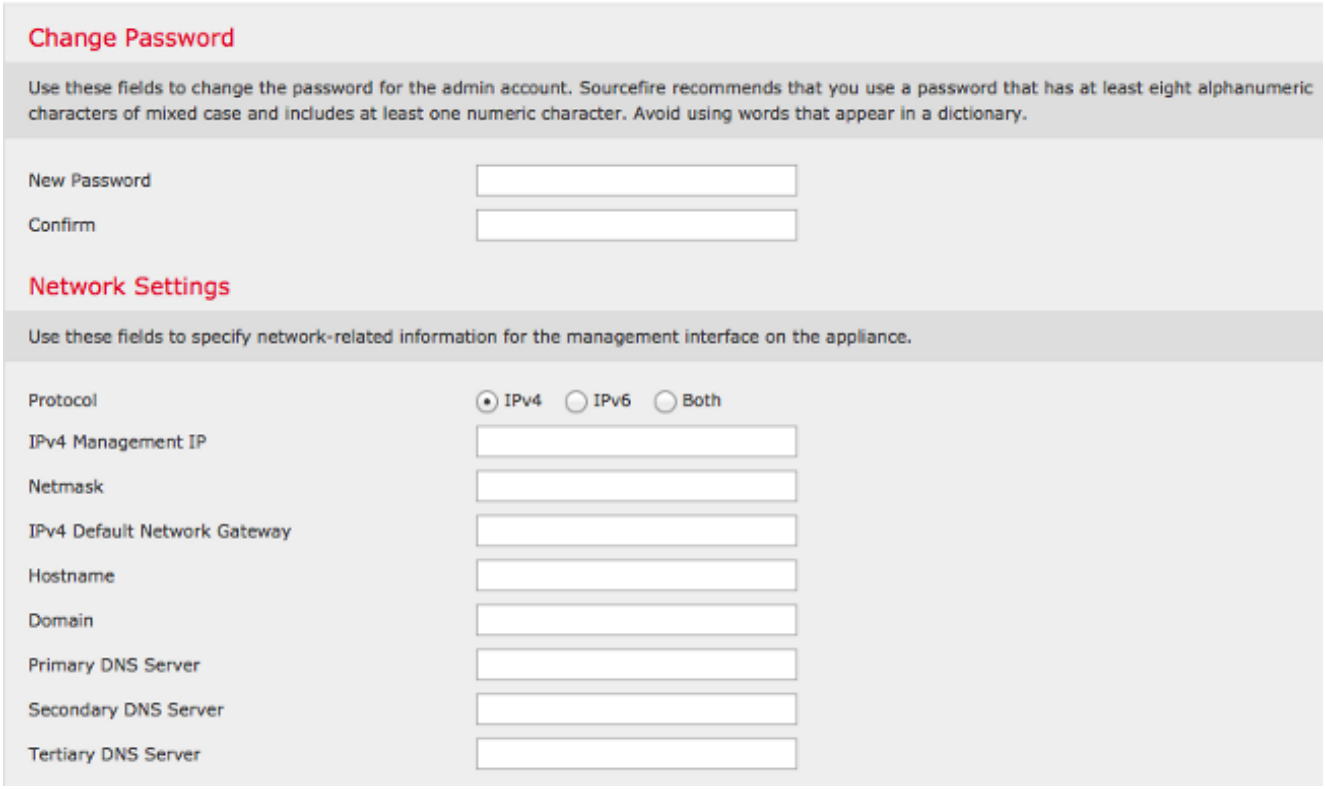
.

```
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:~# _
```

초기 설정 수행

1. 네트워크 설정을 구성한 후 웹 브라우저를 열고 HTTPS를 통해 구성된 IP를 찾습니다(이 예에서는 https://192.0.2.2). 프롬프트가 표시되면 기본 SSL 인증서를 인증합니다.다음 자격 증명을 사용하여 로그인합니다.버전 5.x 사용자 이름:**관리자**암호:**Sourcefire**버전 6.x 이상사용자 이름:**관리자**암호:**관리자123**
2. 다음 화면에서는 비밀번호 변경 및 서비스 약관에 동의하는 경우를 제외하고 모든 GUI 컨피그레이션 섹션은 선택 사항입니다. 정보가 알려진 경우 Management Center의 초기 컨피그레이션을 간소화하기 위해 설정 마법사를 사용하는 것이 좋습니다.구성이 완료되면 **Apply를** 클릭하여 Management Center 및 등록된 디바이스에 컨피그레이션을 적용합니다. 구성 옵션에 대한 간단한 개요는 다음과 같습니다.**암호 변경:** 기본 관리자 계정의 비밀번호를 변경할 수 있습니다. 비밀번호를 변경해야 합니다. **네트워크 설정:** 어플라이언스 또는 가상 머신의 관리 인터페이스에 대해 이전에 구성된 IPv4 및 IPv6 네트워크 설정을 수정할 수 있습니다.**시간 설정:** Management Center를 신뢰할 수 있는 NTP 소스와 동기화하는 것이 좋습니다.IPS 센서는 시스템 정책을 통해 Management Center와 시간을 동기화하도록 구성할 수 있습니다. 선택적으로 시간 및 표시 표준 시간대를 수동으로 설정할 수 있습니다.**반복 규칙 업데이트 가져오기:** 반복 Snort 규칙 업데이트를 활성화하고 초기 설정 중에 지금 설치할 수도 있습니다.**반복 지오로케이션 업데이트:** 반복 지오로케이션 규칙 업데이트를 활성화하고 초기 설정 중에 지금 설치할 수도 있습니다.**자동 백업:** 자동 구성 백업을 예약합니다.**라이센스 설정:** 기능 라이센스를 추가합니다.**장치 등록:** 사전 등록된 디바이스에 초기 액세스 제어 정책을 추가, 라이센스 및 적용할 수 있습니다. 호스트 이름/IP 주소 및 등록 키는 FirePOWER IPS 모듈에 구성된 IP 주소 및 등록 키와 일치해야 합니다.**최종 사용자 사용권 계약:** EULA에 동의해야 합니다

.



관련 정보

- [Firepower Management Center Virtual Quick Start Guide for VMware, 버전 6.0]
- [기술 지원 및 문서 – Cisco Systems]