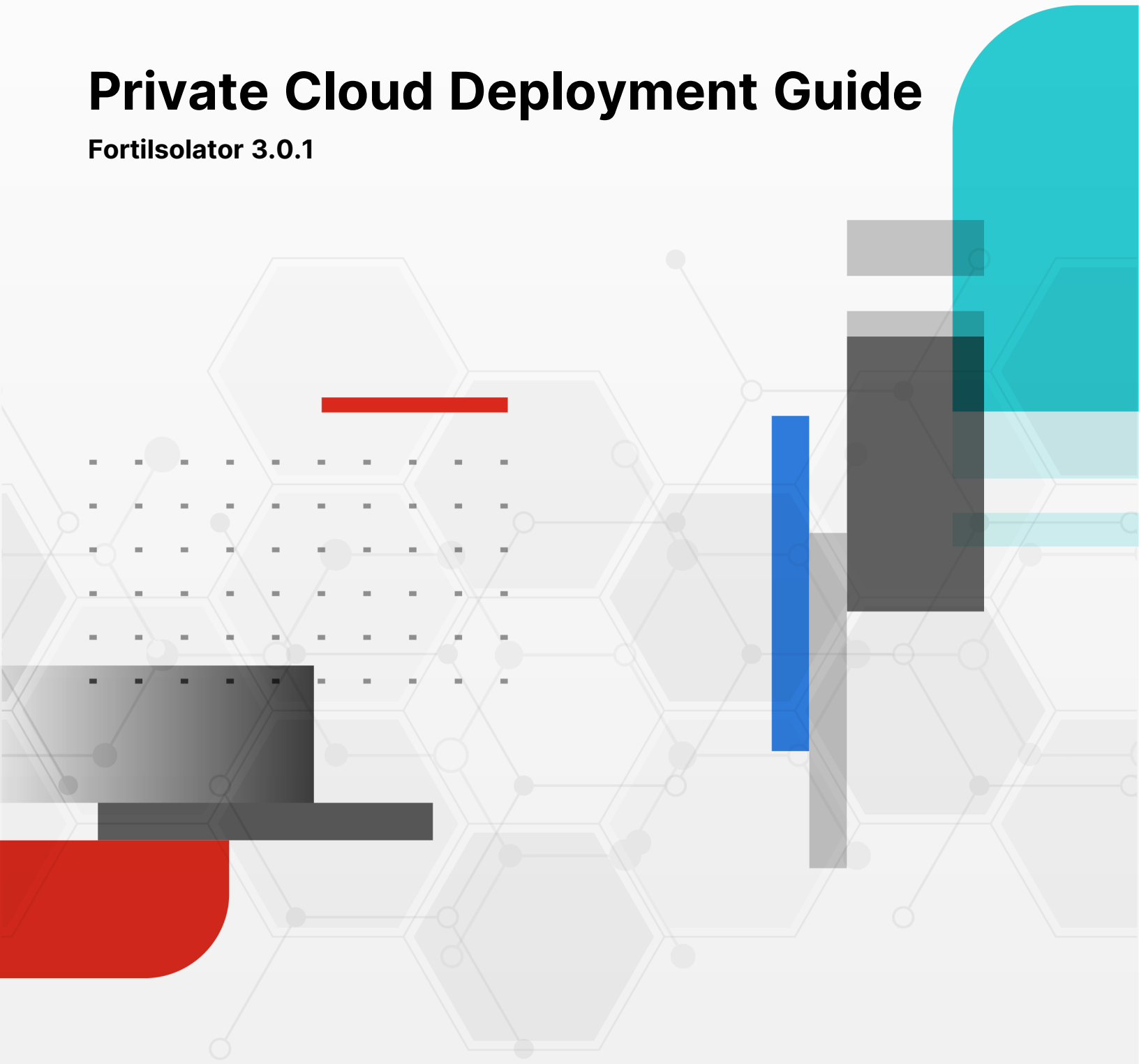
Private Cloud Deployment Guide

FortiIsolator 3.0.1



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

January 20, 2026
FortiIsolator 3.0.1 Private Cloud Deployment Guide
51-301-1110656-20260120

TABLE OF CONTENTS

Change log

Date	Change Description
2025-09-29	Initial release.
2025-11-03	Updated Setting up the FortiIsolator environment on page 29.
2025-11-20	Updated Setting up the FortiIsolator environment on page 29.
2026-01-20	Updated Installing FortiIsolator VM for Linux KVM on page 7.

Introduction

FortiIsolator 3.0.1 supports deployment on the following VM platforms:

- Linux KVM
- VMware vSphere
- VMware ESXi

For information about using FortiIsolator in general, see the FortiIsolator Administration Guide.

Deploying the FortiIsolator

The deployment of FortiIsolator includes the following steps:

1. System requirements on page 6
2. Downloading the FortiIsolator firmware and package files on page 6
3. Deploying the FortiIsolator on your VM platform on page 7
4. Setting up the FortiIsolator environment on page 29

System requirements

To deploy the FortiIsolator, you must set up VMs for each component. See the FortiIsolator 3.0.1 Administration Guide for more details about each component and how they communicate with each other.

The following tables lists the system requirements of each component VM. Make sure that all VMs on which a FortiIsolator component will be installed comply with those requirements.

Component	Number of CPUs	Memory	Number of VMs needed
Registry	2	16 GB	1 for standalone or 2 for HA
Controller HA	4	48 GB	1 for standalone and 3+ for HA  Kubernetes relies on an odd number of control plane nodes (e.g., 3, 5, or more) to maintain quorum and ensure continuous operation if one node fails.
Worker controller	4	48 GB	At least 1
Worker isolator	4	48 GB	1 per 50 sessions

Downloading the FortiIsolator firmware and package files

Before you install the FortiIsolator on your VM, ensure you have downloaded the FortiIsolator firmware for your VM by following the steps below:

1. Go to https://support.fortinet.com.
2. Click *Login* and log in to the Fortinet Support website.
3. From the *Support* > *Downloads* menu, select *Firmware Download*.
4. In the *Select Product* dropdown menu, select *FortiIsolator*.
5. On the *Download* tab, navigate to the FortiIsolator firmware file for your VM or appliance type in the *Image Folders/Files* section.

FortiIsolator VM for Linux KVM	`FIS_VM_KVM-v3-build0151.kvm.zip`
FortiIsolator VM for VMware vSphere	`FIS_VM_VmWare-v3-build0151.vmware.zip`
FortiIsolator VM for VMware ESXi	`FIS_VM_ESXi-v3-build0151.ovf.zip`

6. Click *HTTPS* to download the firmware.
7. Unzip the firmware package.
8. Download the following package files, which you will need to upload to the FortiIsolator GUI when Setting up the FortiIsolator environment on page 29:
   - `FIS_auth_DOCKER-v3-build0117.xz`
   - `FIS_fisfs_DOCKER-v3-build0117.xz`
   - `FIS_log_DOCKER-v3-build0117.xz`
   - `office-1.6.tar.gz`
   - `FIS_postgres_DOCKER-v3-build0117.xz`
   - `FIS_update_DOCKER-v3-build0117.xz`
   - `FIS_wf_DOCKER-v3-build0117.xz`

Continue to install the firmware on your VM by referring to Deploying the FortiIsolator on your VM platform on page 7.

Deploying the FortiIsolator on your VM platform

To deploy the FortiIsolator, you must set up VMs for each component in the correct order.

Refer to the following topics for detailed instructions about deploying the FortiIsolator on your VM platform:

Installing FortiIsolator VM for Linux KVM

To install FortiIsolator, set up VM(s) for the following components in the exact order:

1. Registry
2. Controller HA
3. Worker isolator
4. Worker controller

See the FortiIsolator 3.0.1 Administration Guide for more details about each component and how they communicate with each other.

FortiIsolator VM for Linux KVM supports both Video Graphics Array (VGA) and virtual serial console connections.

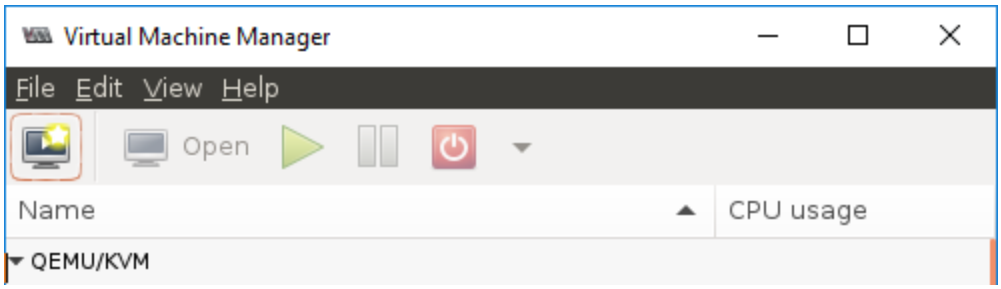
Prerequisites

- You have downloaded the FortiIsolator firmware for Linux KVM. See Downloading the FortiIsolator firmware and package files on page 6.
- Ensure that your system has at least two hard disks of the following types:
  - IDE
  - SATA
  - SCSI
  - Virtio
- Ensure that your system has at least three network interfaces of the following types:
  - Hypervisor default (Rt18139)
  - E1000

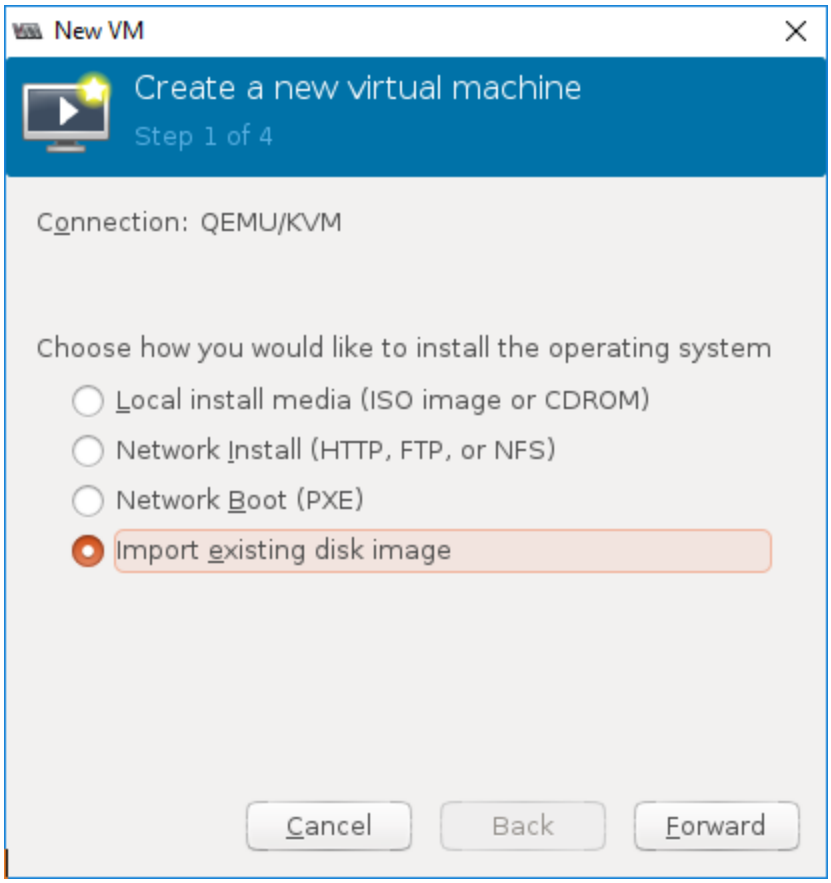
To install FortiIsolator VM for Linux KVM:

1. Launch KVM with Virtual Machine Manager (https://virt-manager.org/).

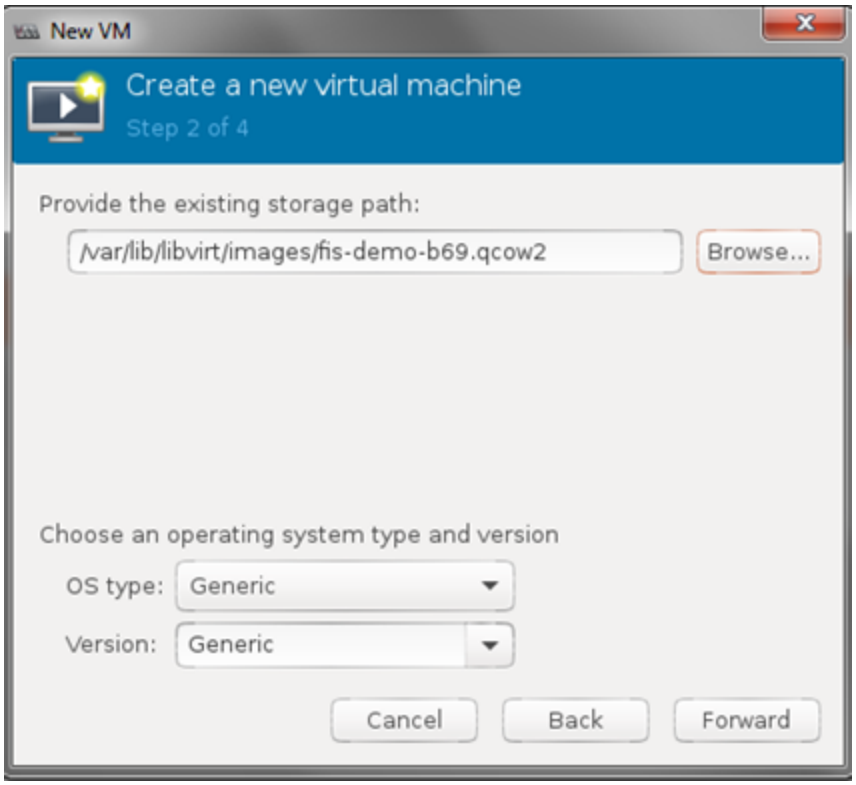
2. Create a new virtual machine.



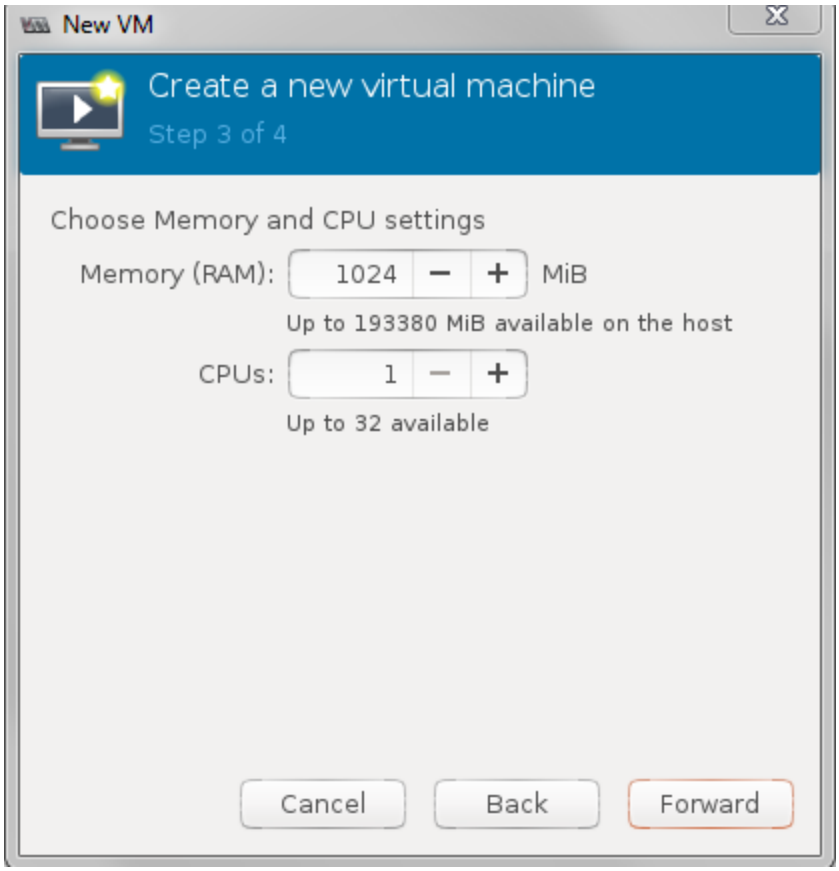
3. Select *Import existing disk image*.



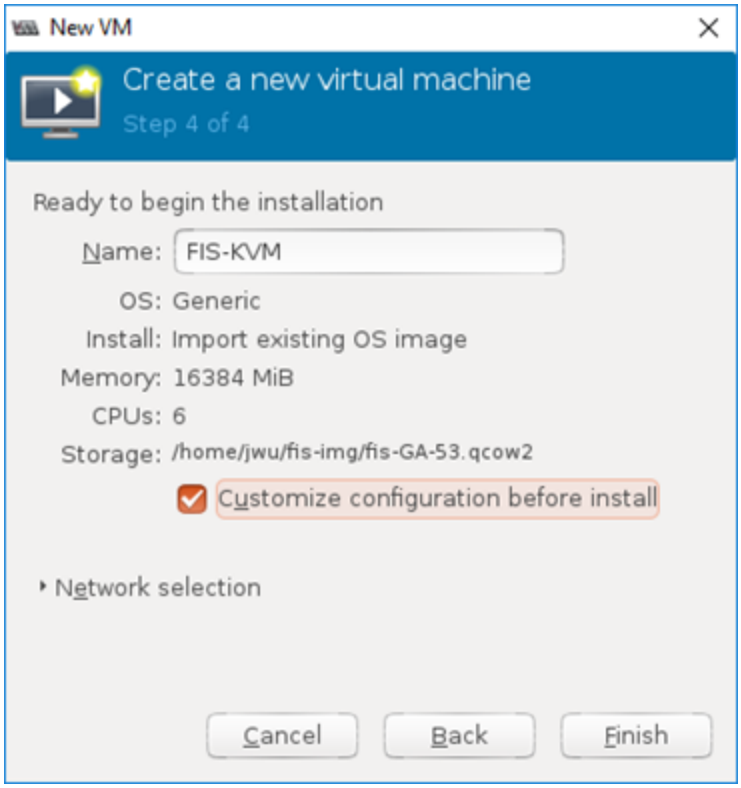
4. Browse and select the FortiIsolator image (for example, `fis.qcow2`).

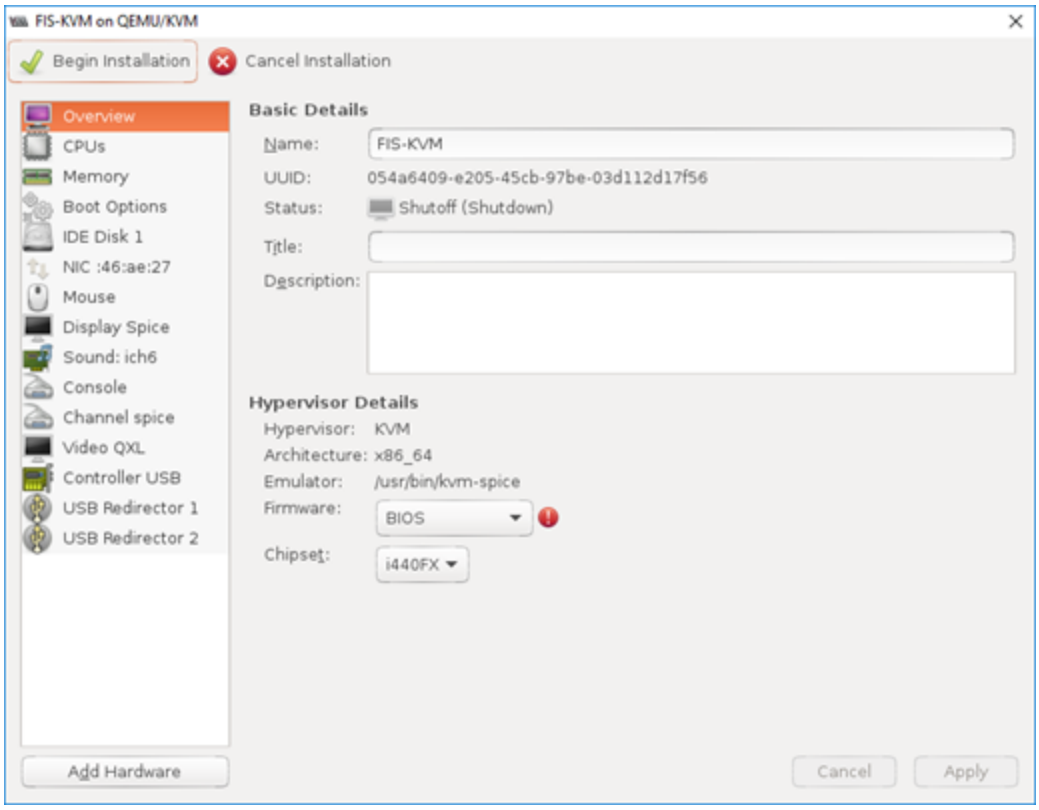


5. Configure the CPU and memory as required by each VM. See System requirements on page 6.

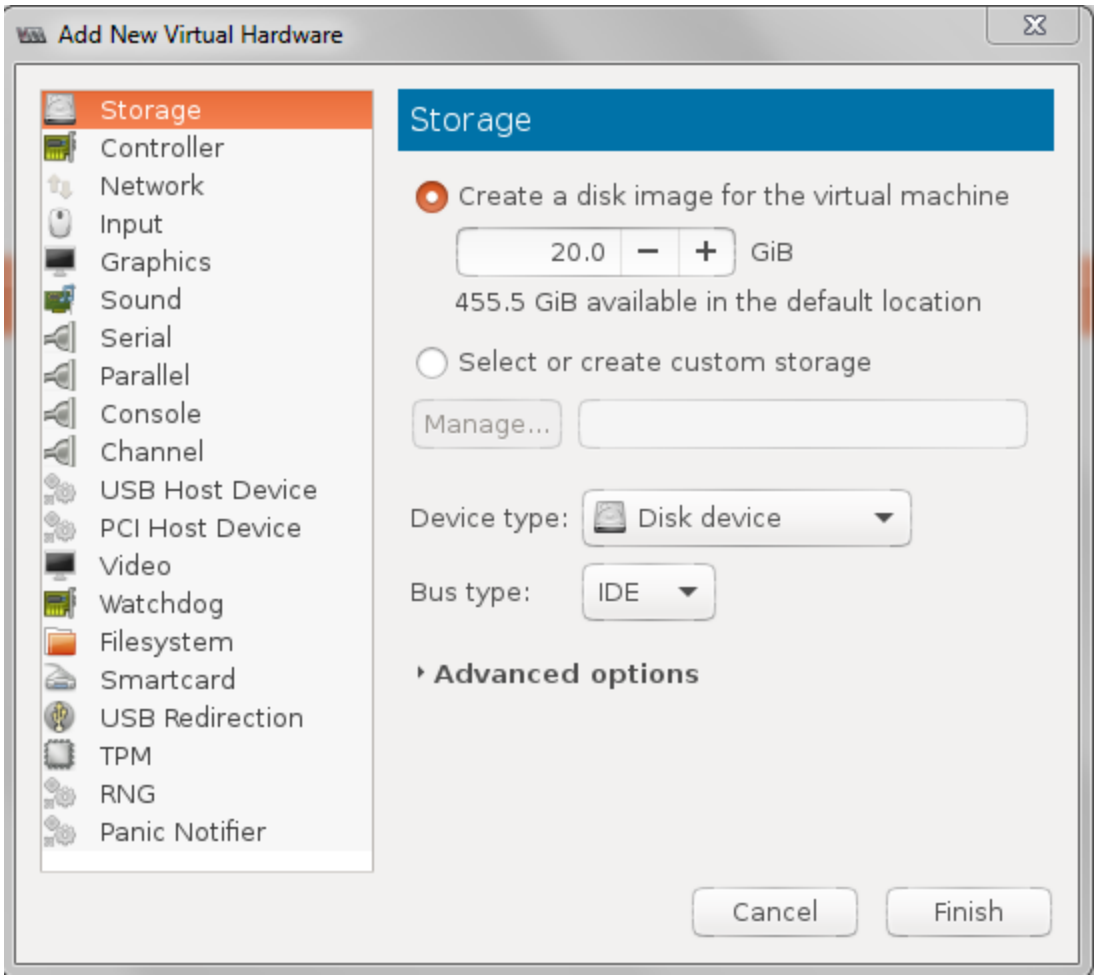


6. Name the new virtual machine, and select *Customize configuration before install*.




FIS-KVM on QEMU/KVM
Begin Installation
Cancel Installation
Overview
CPUs
Memory
Boot Options
IDE Disk 1
NIC :46:ae:27
Mouse
Display Spice
Sound: ich6
Console
Channel spice
Video QXL
Controller USB
USB Redirector 1
USB Redirector 2
Basic Details
Name: FIS-KVM
UUID: 054a6409-e205-45cb-97be-03d112d17f56
Status: Shutoff (Shutdown)
Title:
Description:
Hypervisor Details
Hypervisor: KVM
Architecture: x86_64
Emulator: /usr/bin/kvm-spice
Firmware: BIOS
Chipset: i440FX
Add Hardware
Cancel
Apply

7. Add an IDE disk. Accept the default values.



8. Add three network interfaces and configure them accordingly.
   - Network 1: Internal Interface
   - Network 2: External Interface
   - Network 3: Management Interface
   - Network 4: HA Interface

9. Click *Begin Installation* to load the KVM image.

10. Wait for the installation to complete.
11. Repeat the steps above to create the remaining VMs. Note that you need to set up at least 3 controller HA VMs,

Continue to set up the FortiIsolator environment by referring to Setting up the FortiIsolator environment on page 29.

Installing FortiIsolator VM for VMware vSphere

To install FortiIsolator, set up VM(s) for the following components in the exact order:

1. Registry
2. Controller HA
3. Worker isolator
4. Worker controller

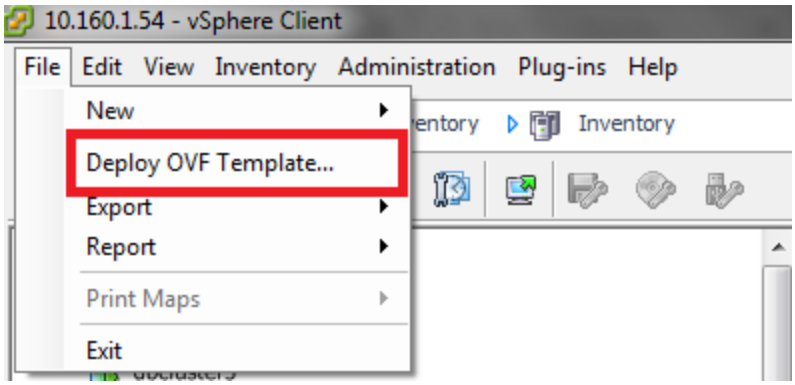
See the FortiIsolator 3.0.1 Administration Guide for more details about each component and how they communicate with each other.

Prerequisites

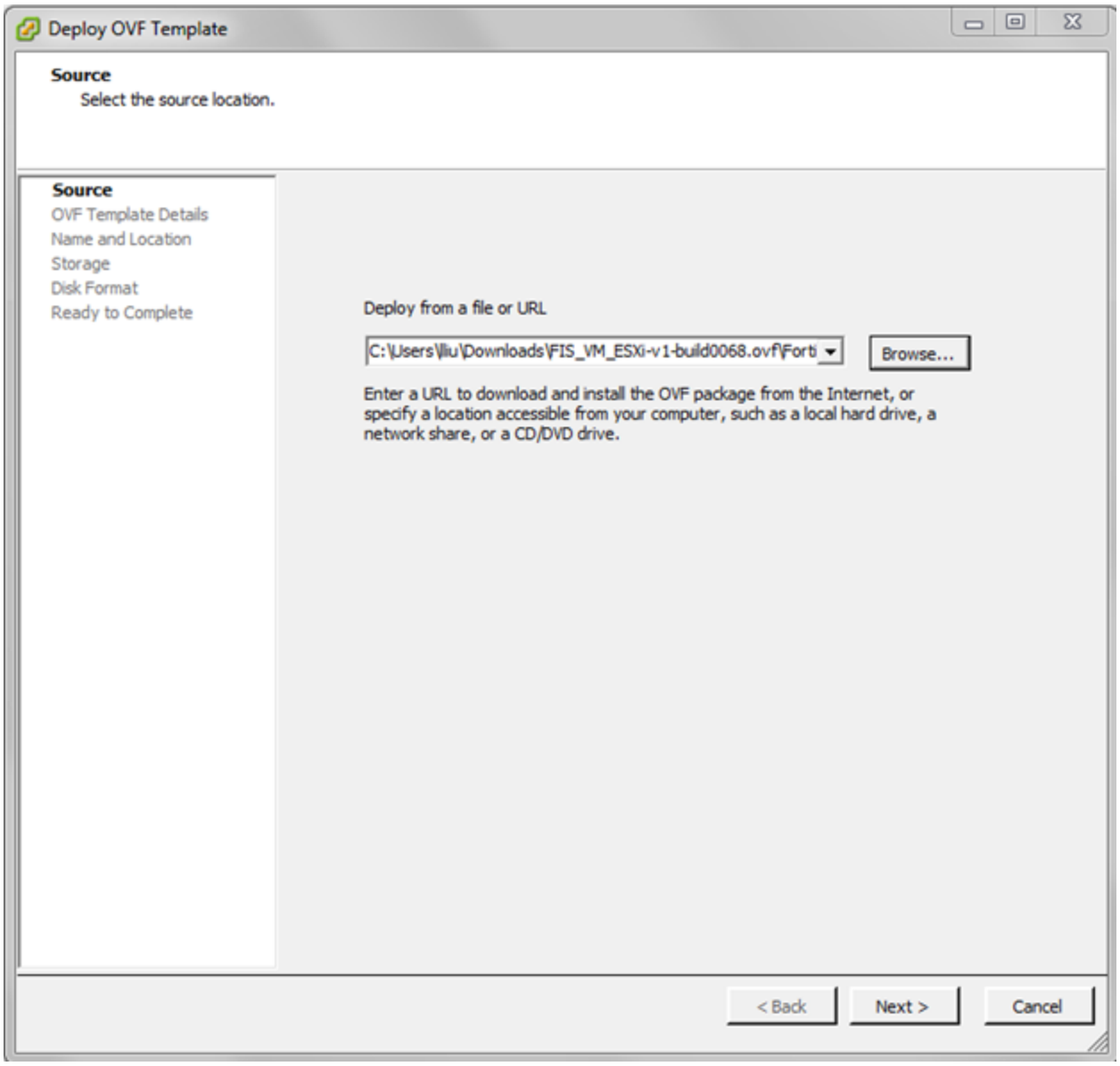
- You have downloaded the FortiIsolator firmware for VMware. See Downloading the FortiIsolator firmware and package files on page 6.
- Install VMware vSphere Client.
- Ensure that your system has one of the following combinations of hard disks and network adapters to support ESXI 6.0:
  - Two SCSI hard disks and three VMXNET 3 network adapters (this is the default)
  - One IDE hard disk and one SCSI hard disk and three E1000 network adapters

To install FortiIsolator VM for Microsoft VMware vSphere:

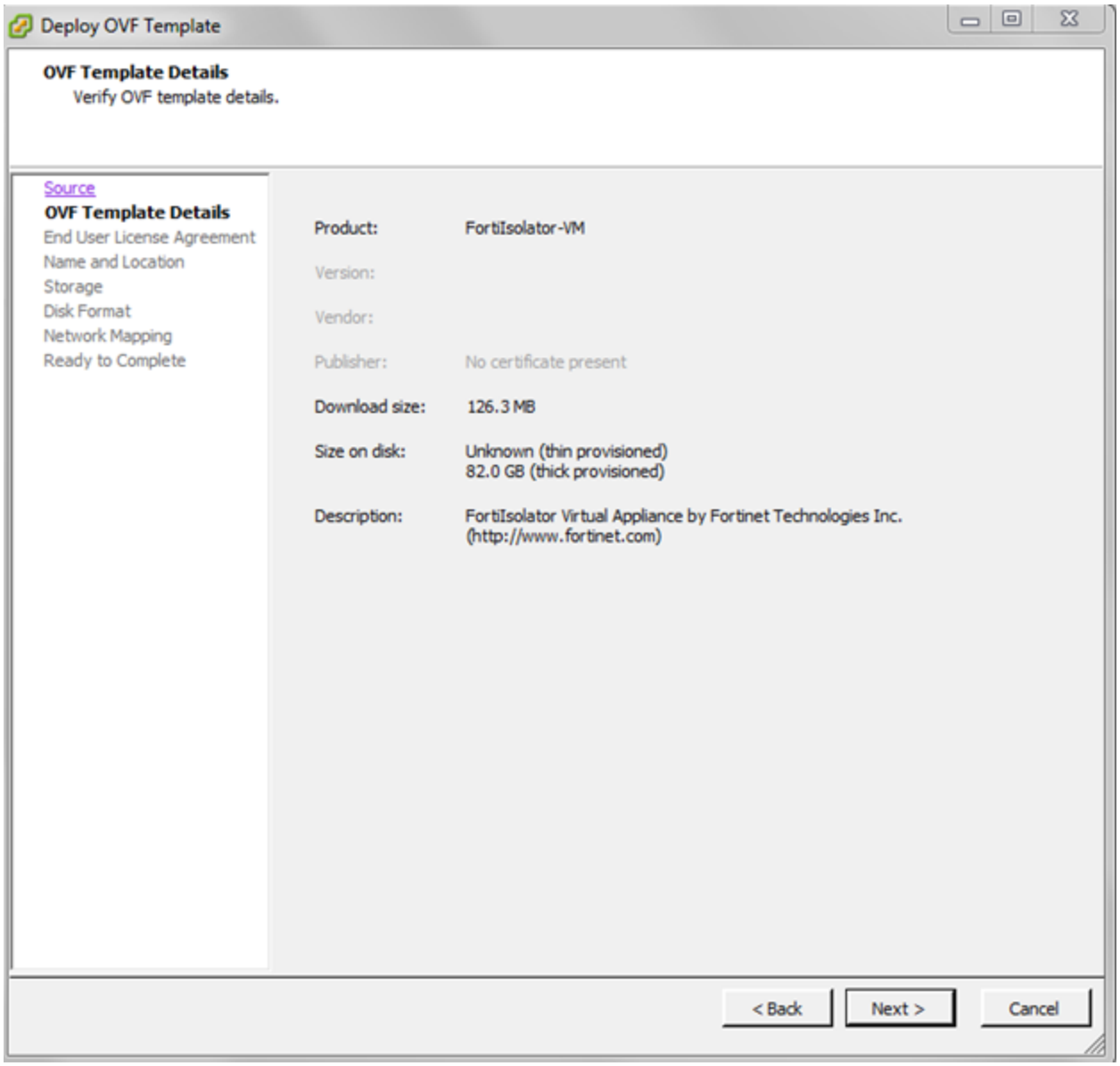
1. Create a new virtual machine in vSphere Client by selecting *File* > *Deploy OVF Template*.



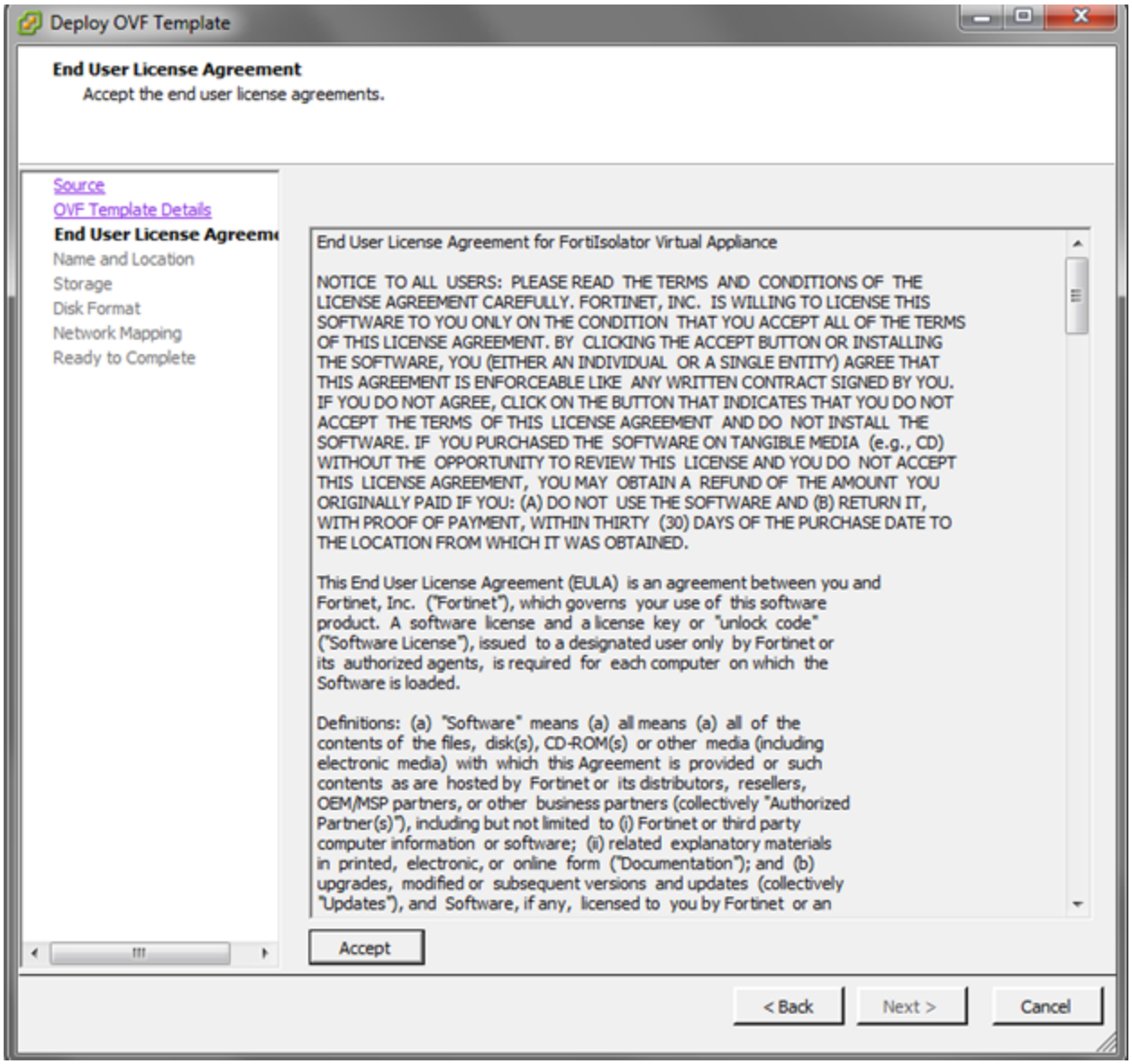
2. Browse to the folder that contains the FortiIsolator files and select `FortiIsolator.ovf`.



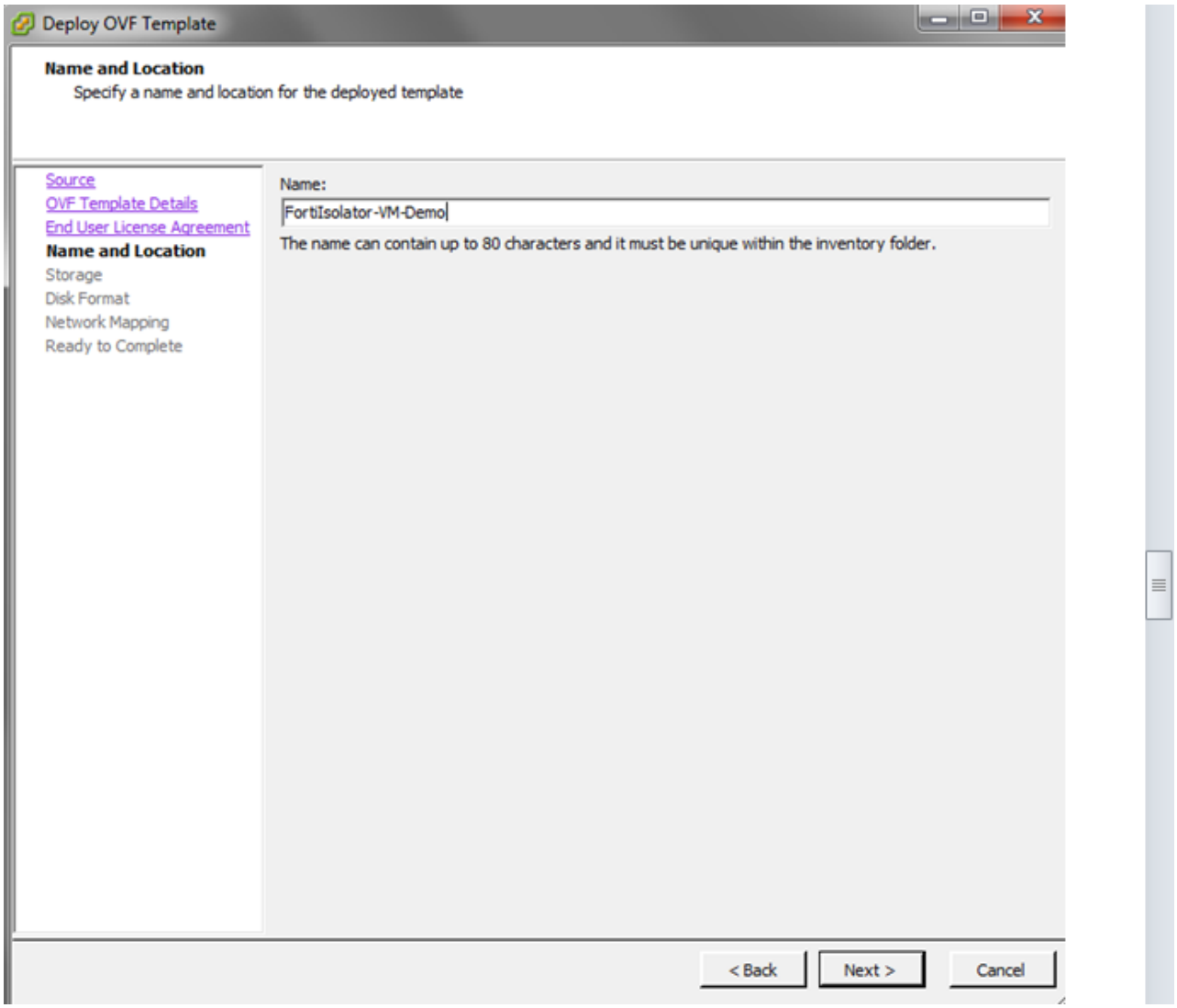
3. Verify the OVF template details.



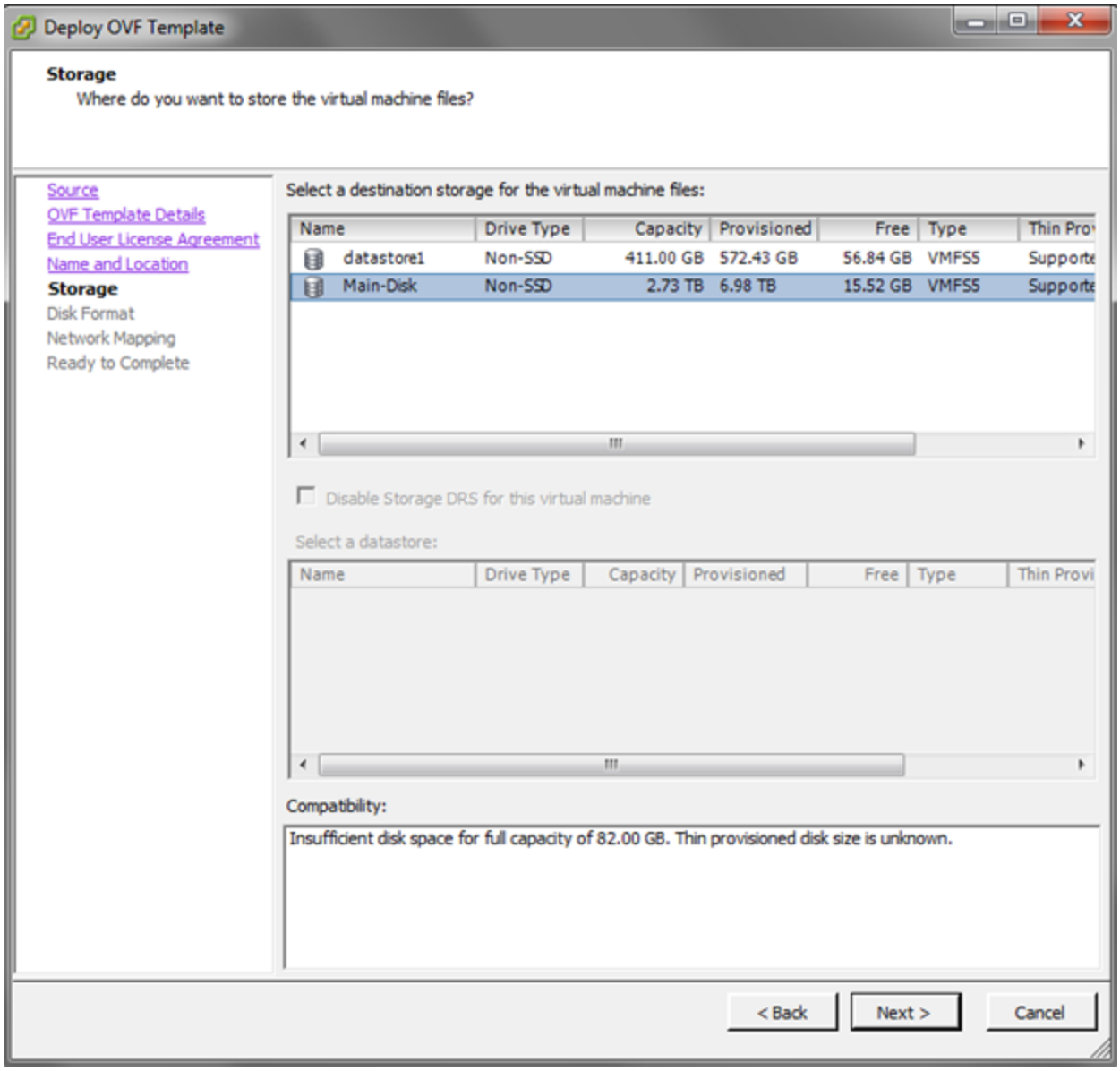
4. Review and accept the FortiIsolator End User License Agreement.



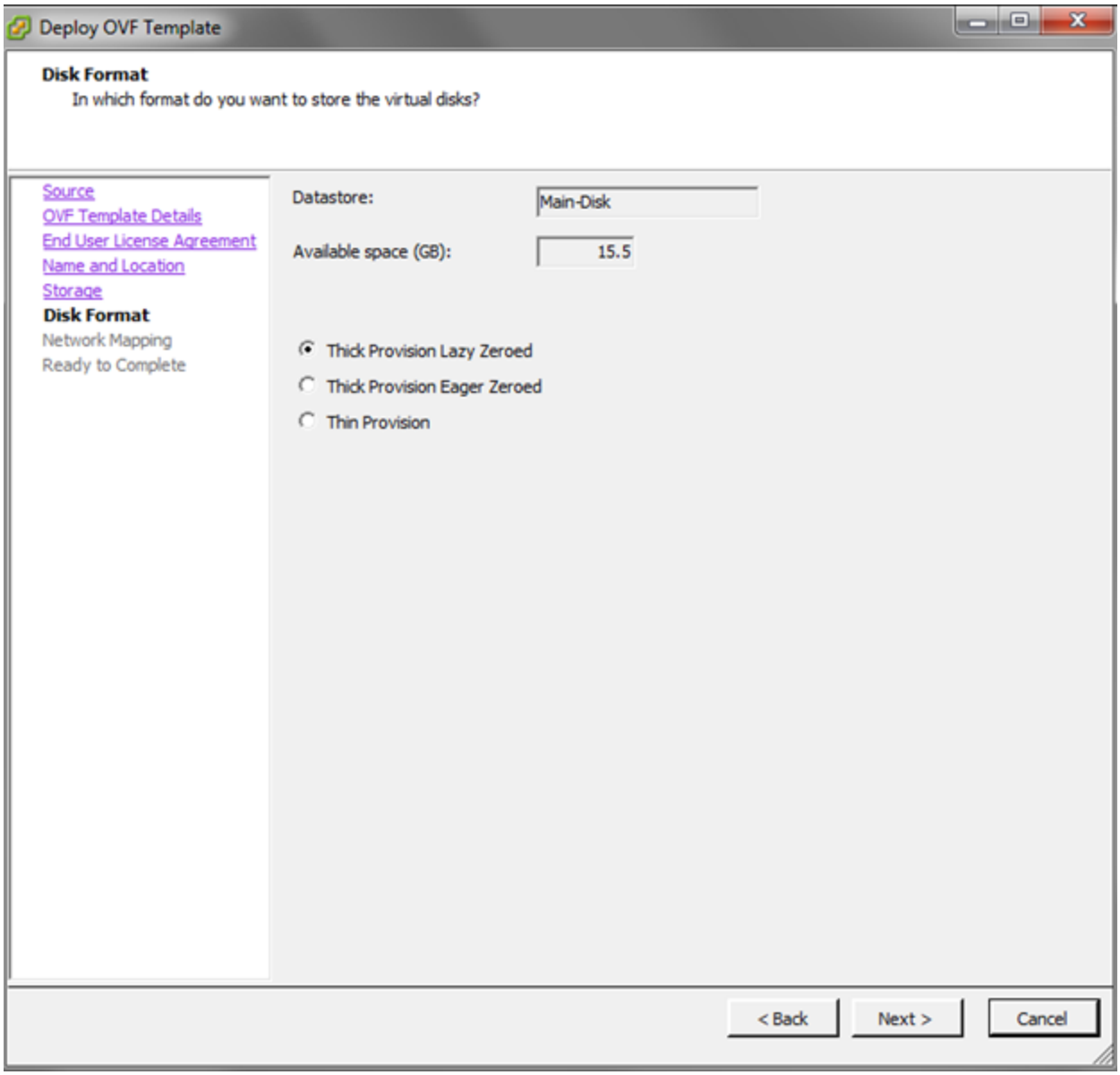
5. Name the new FortiIsolator virtual machine.



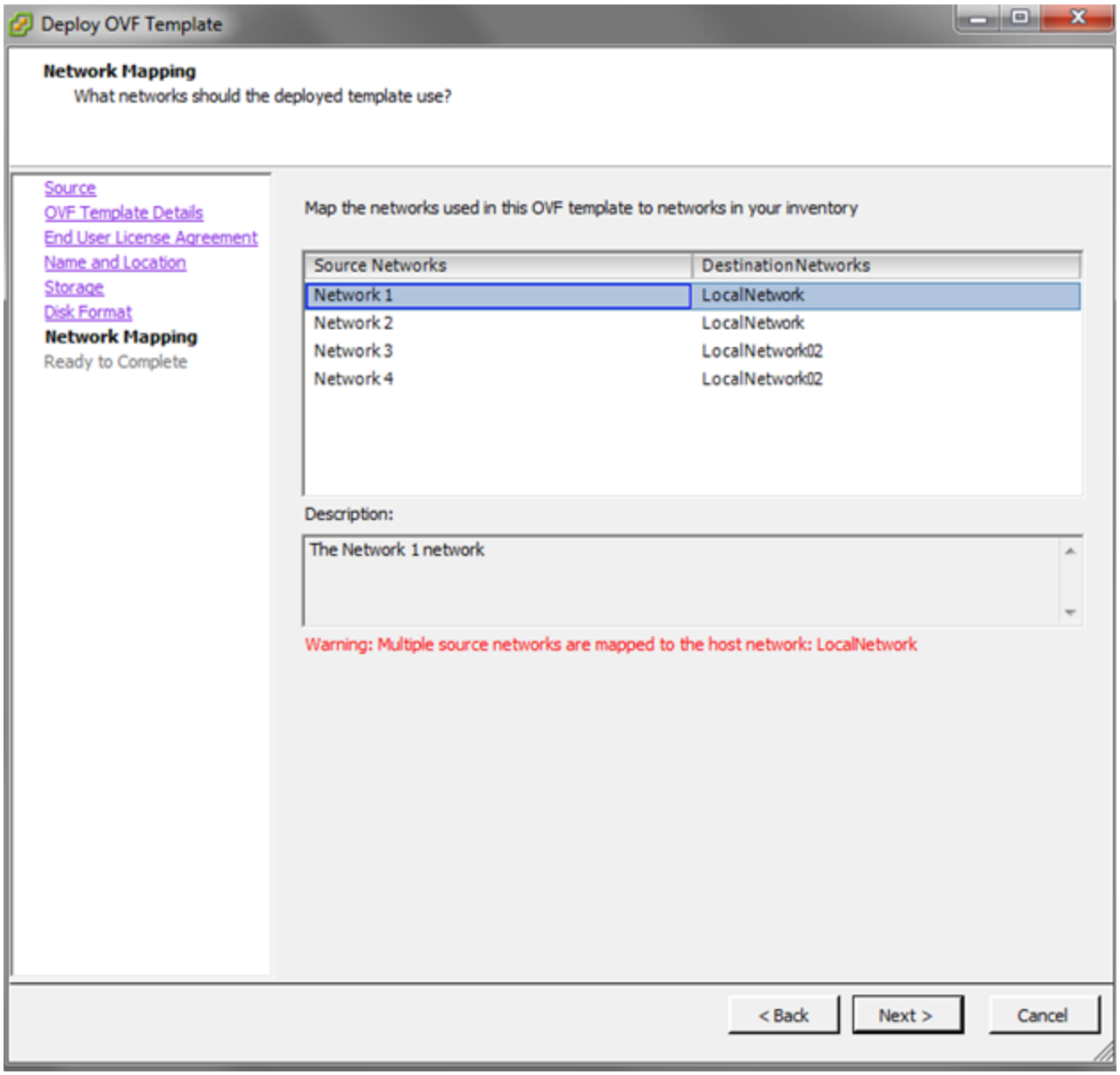
6. Select the datastore where you want to install the FortiIsolator VM.



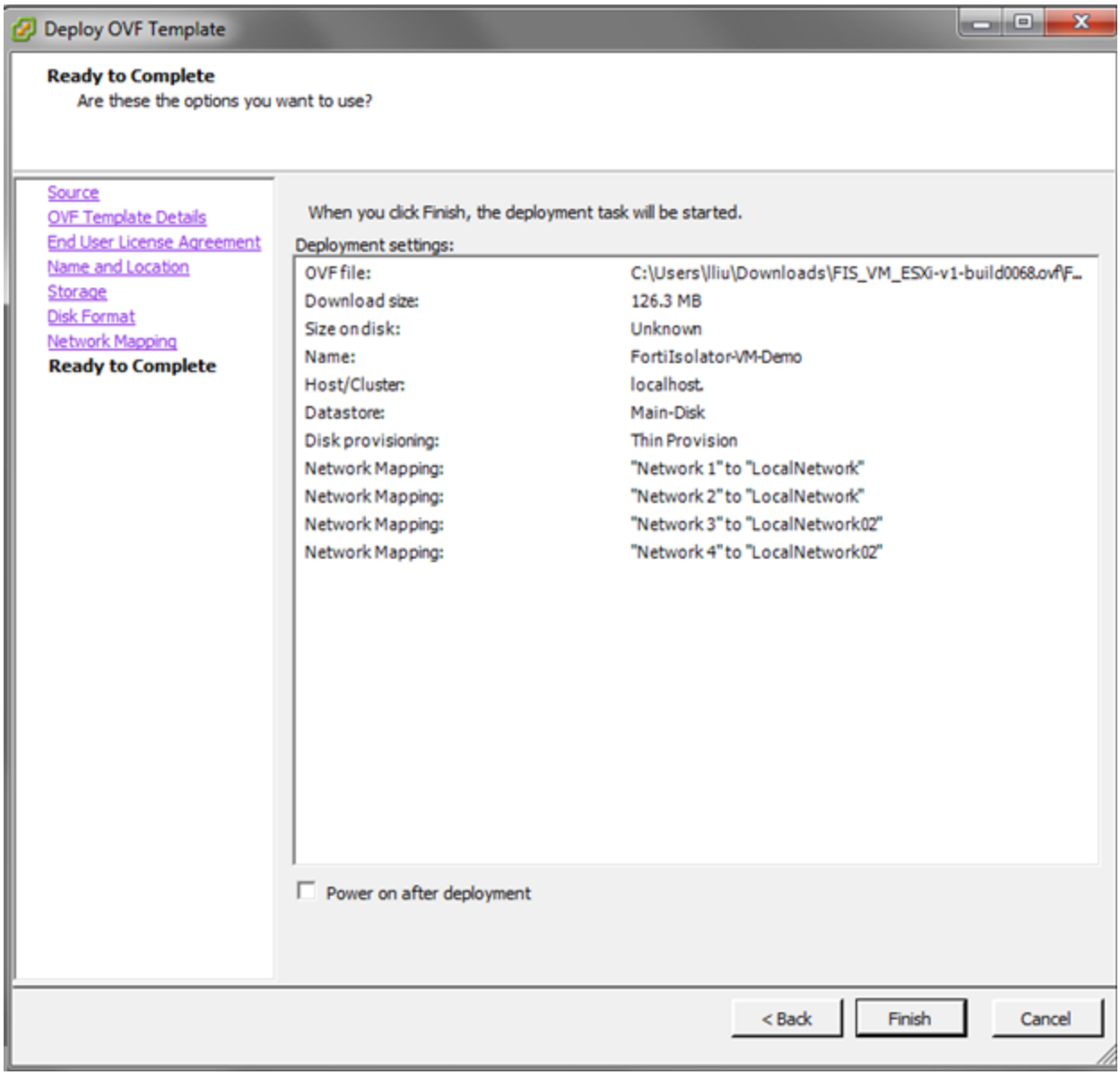
7. Select the disk provisioning format. For optimal performance, select a *Thick Provision* option. Configure the CPU and memory as required by each VM. See System requirements on page 6.



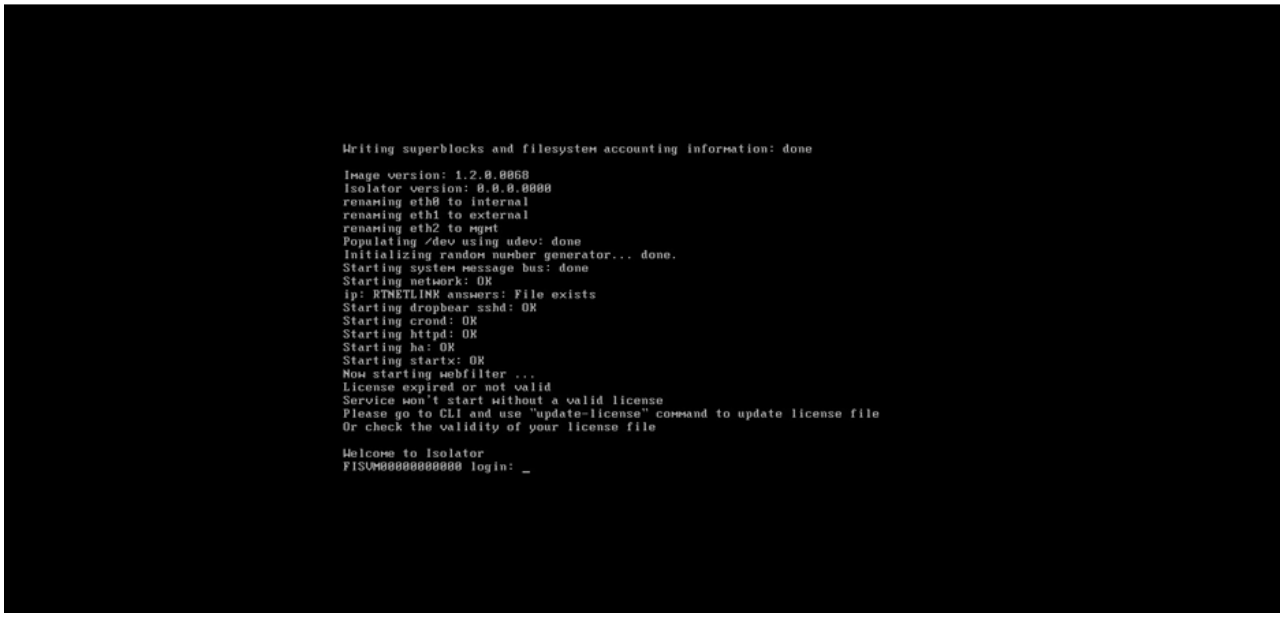
8. Configure the required network interfaces. Add four network interfaces for Network Mapping and configure them accordingly:
   - Network 1: Internal Interface
   - Network 2: External Interface
   - Network 3: Management Interface
   - Network 4: HA Interface


Deploy OVF Template
Network Mapping
What networks should the deployed template use?
Source
OVF Template Details
End User License Agreement
Name and Location
Storage
Disk Format
Network Mapping
Ready to Complete
Map the networks used in this OVF template to networks in your inventory
Source Networks
Destination Networks
Network 1
LocalNetwork
Network 2
LocalNetwork
Network 3
LocalNetwork02
Network 4
LocalNetwork02
Description:
The Network 1 network
Warning: Multiple source networks are mapped to the host network: LocalNetwork
< Back
Next >
Cancel

9. Verify the template deployment options, and click *Finish*.



10. Start the FortiIsolator VM.



11. Repeat the steps above to create the remaining VMs. Note that you need to set up at least 3 controller HA VMs,
12. Log in to FortiIsolator. The default username is `admin` and the default password is `fortinet`.

Continue to set up the FortiIsolator environment by referring to Setting up the FortiIsolator environment on page 29.

Installing FortiIsolator VM for VMware ESXi

To install FortiIsolator, set up VM(s) for the following components in the exact order:

1. Registry
2. Controller HA
3. Worker isolator
4. Worker controller

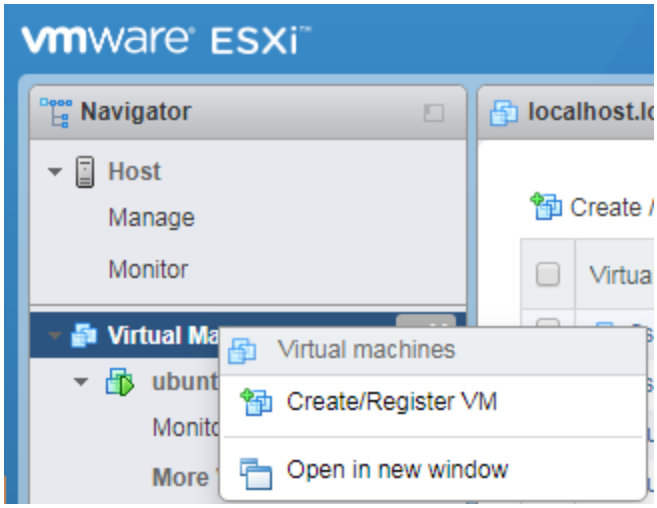
See the Fortiisolator 3.0.1 Administration Guide for more details about each component and how they communicate with each other.

Prerequisites

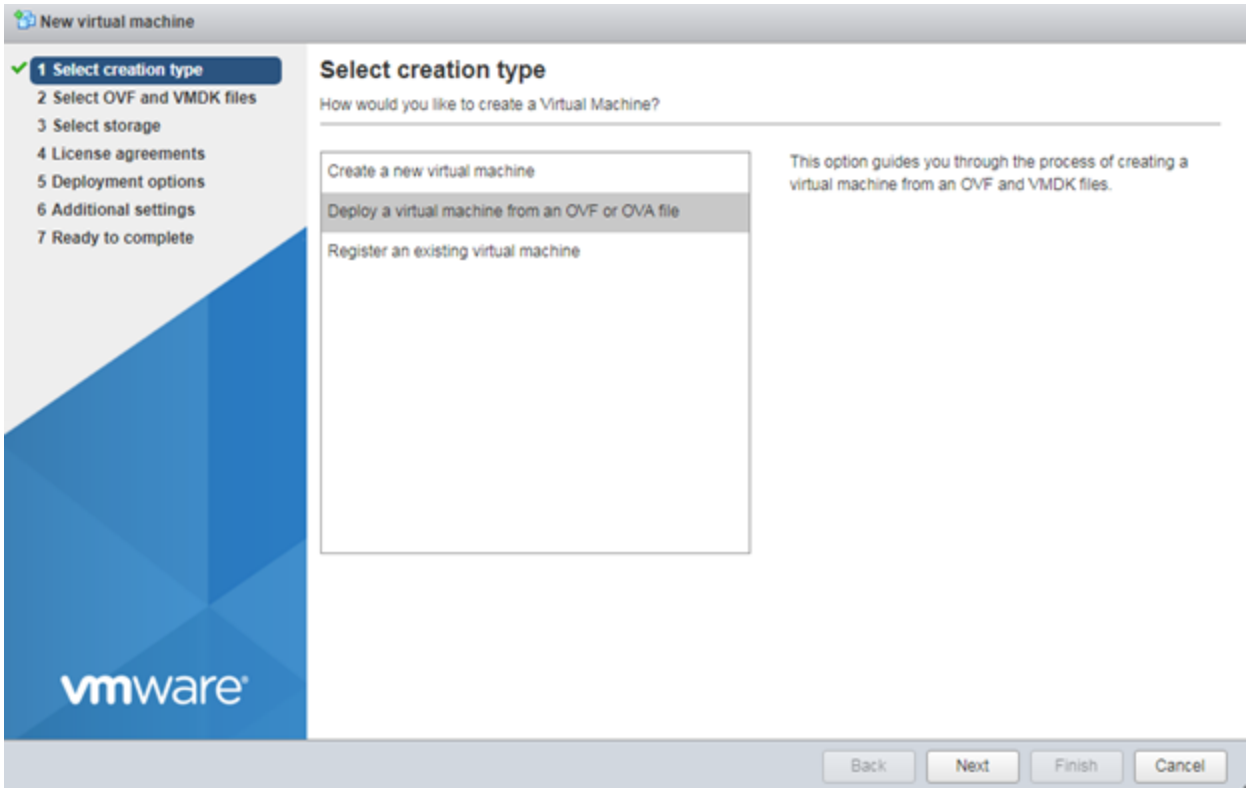
- You have download the FortiIsolator firmware for ESXi. See Downloading the FortiIsolator firmware and package files on page 6.
- Install VMware ESXi.
- Ensure that your system has one of the following combinations of hard disks and network adapters to support ESXI 6.5:
  - Two SCSI hard disks and three VMXNET 3 network adapters (this is the default)
  - Two SCSI hard disks and three E1000 network adapters

To install FortiIsolator VM for Microsoft VMware ESXi:

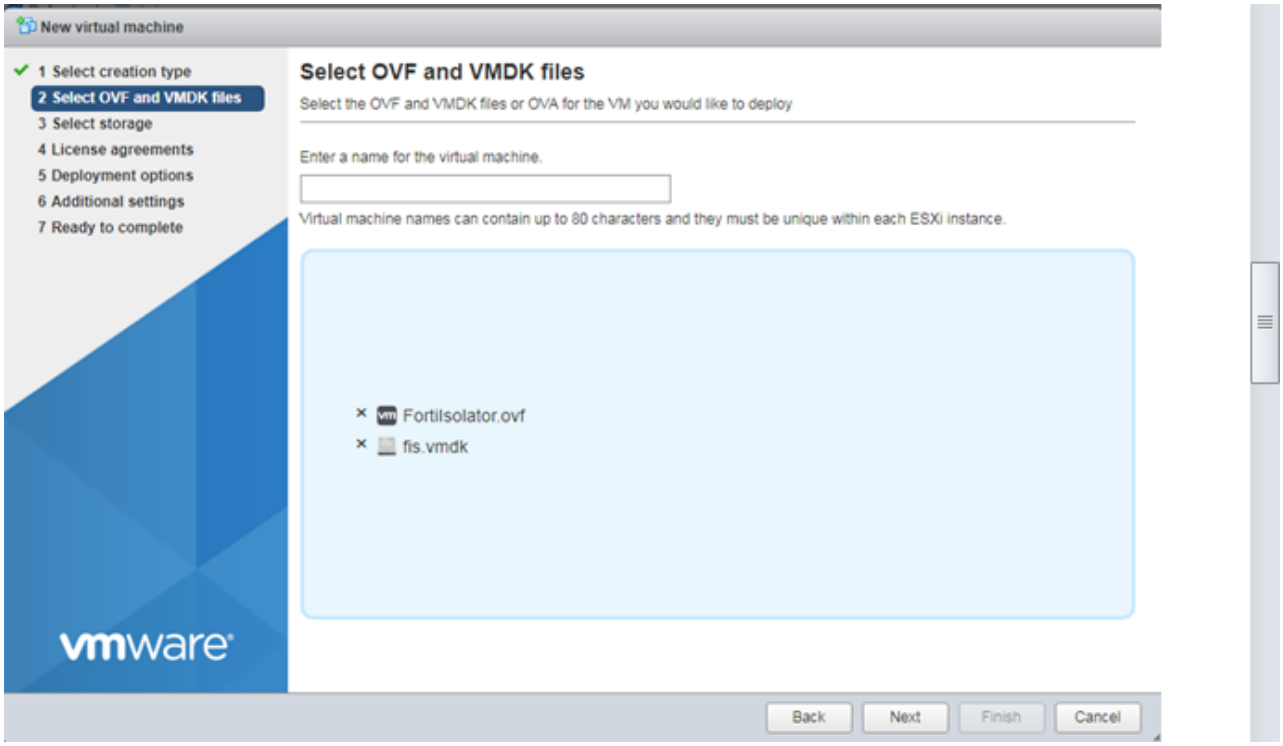
1. In the ESXi home page, click *Virtual Machine*, and then right-click and select *Create/Register VM*.



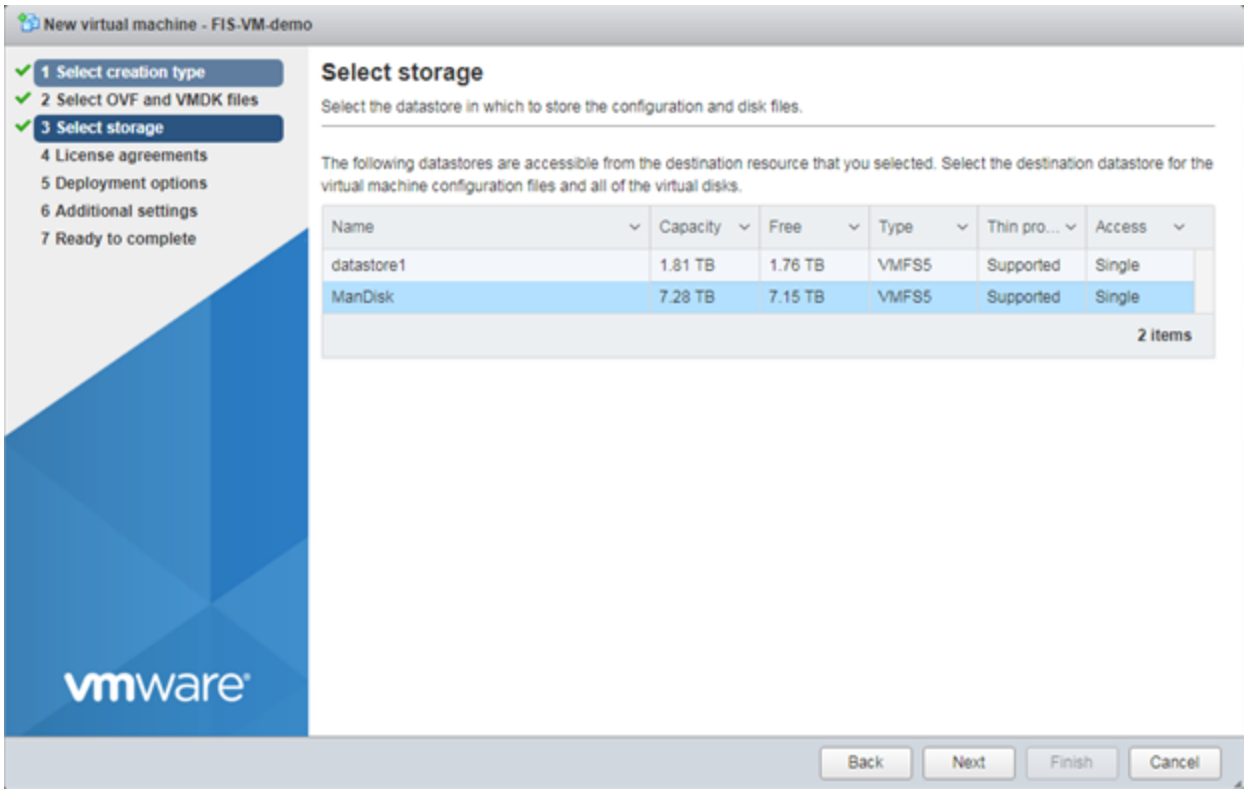
2. In the *Select creation type* step, click *Deploy a virtual machine from an OVF or OVA file*.



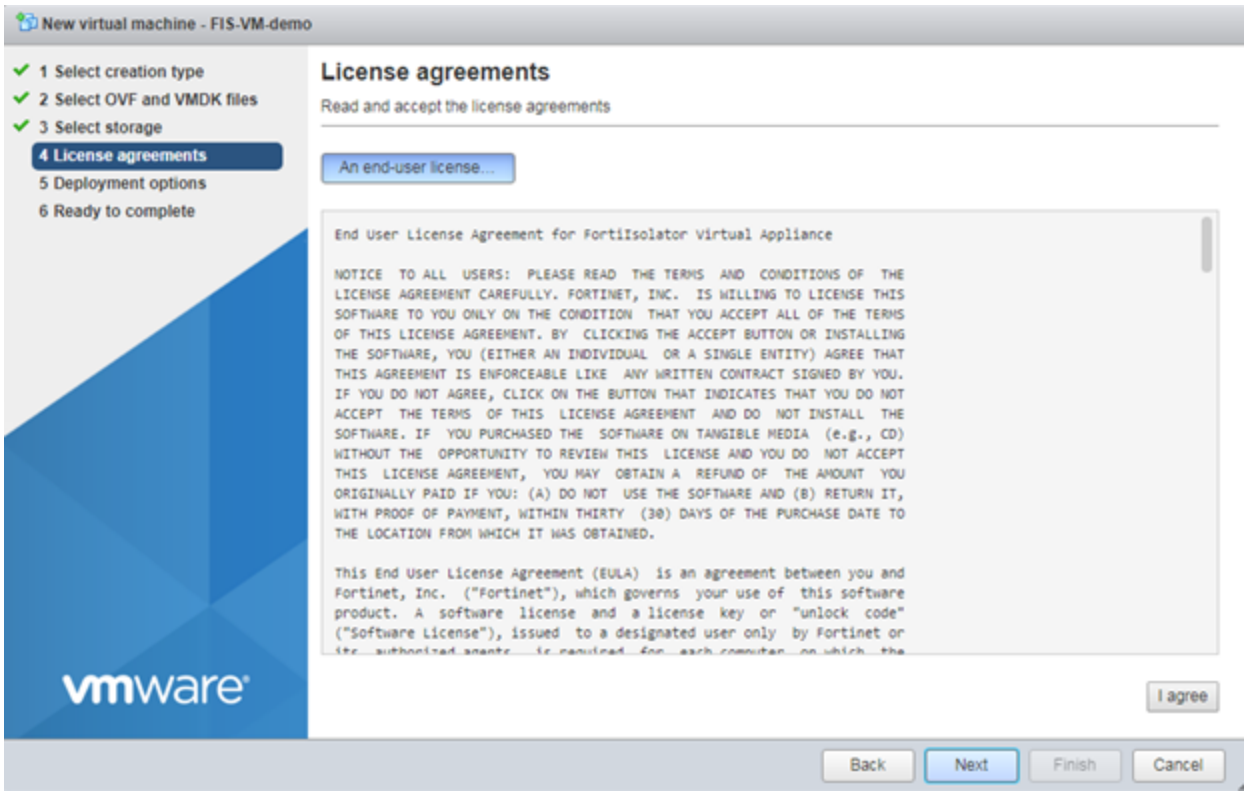
3. In the *Select OVF and VMDK files* step, select both the `FortiIsolator.ovf` and `fis.vmdk` files.



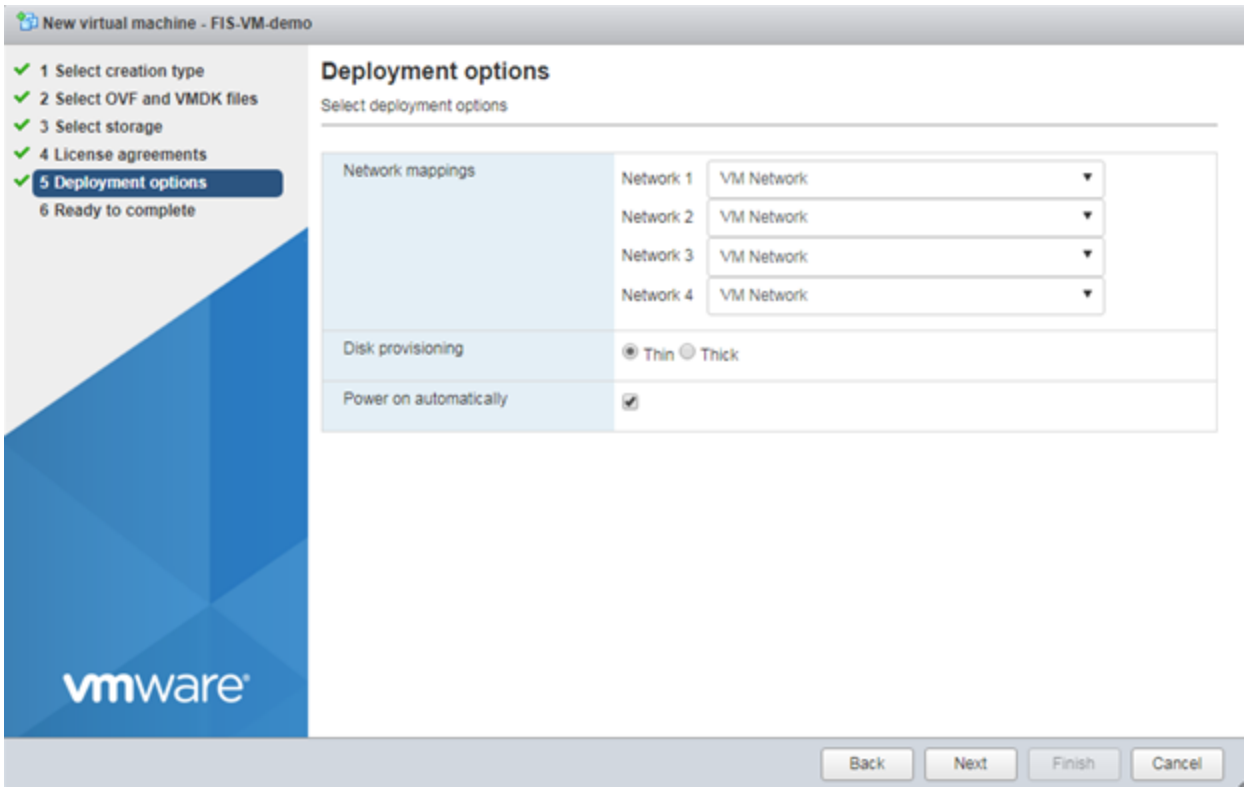
4. In the *Select storage* step, select the datastore where you want to install the FortiIsolator VM. Configure the CPU and memory as required by each VM. See System requirements on page 6.



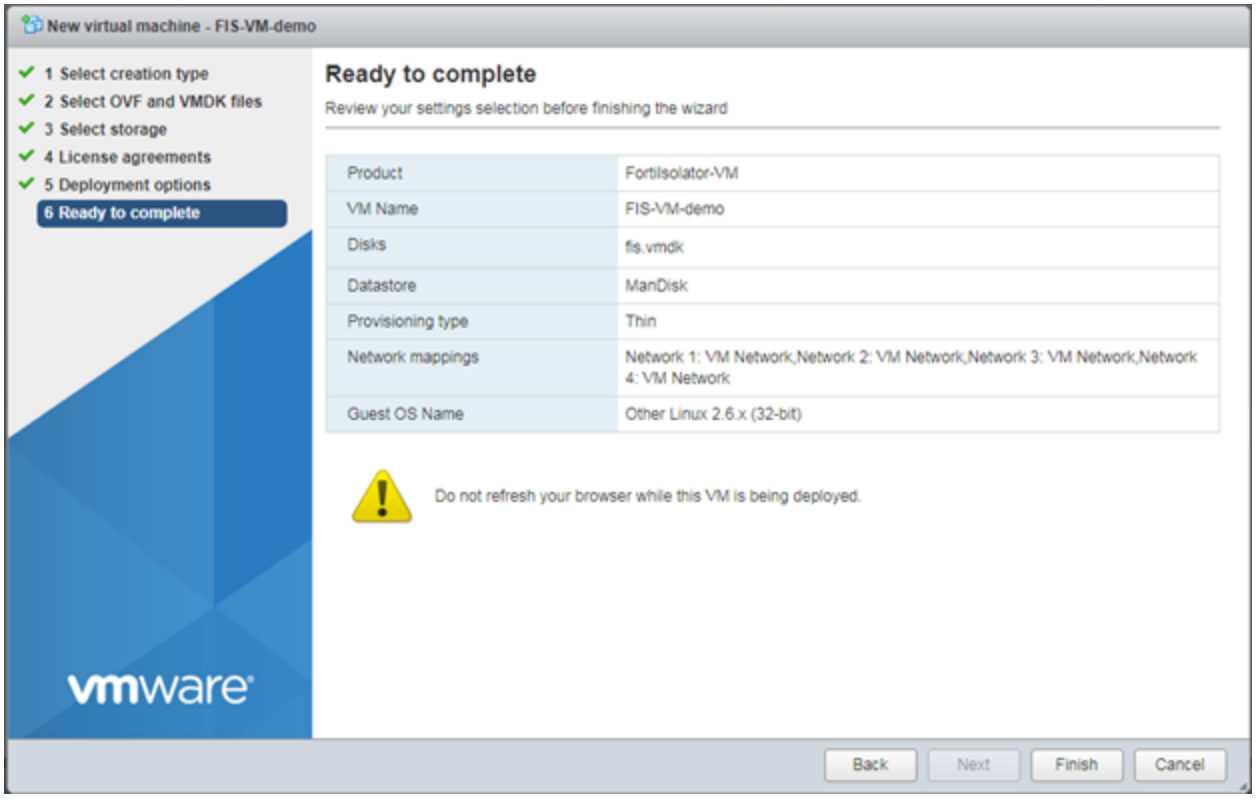
5. Review and accept the FortiIsolator End User License Agreement.



6. In the *Deployment options* step, configure *Network mappings* with four network interfaces accordingly:
   - Network 1: Internal Interface
   - Network 2: External Interface
   - Network 3: Management Interface
   - Network 4: HA Interface



7. Configure *Disk provisioning*, and select the *Power on automatically* checkbox.
8. Verify the deployment options, and click *Finish*.



9. To start the VM, right-click the FortiIsolator VM name, and select *Power* > *Power on*.

10. To open the FortiIsolator VM console, click *Console* > *Open browser console*.

11. Log in to FortiIsolator. The default username is `admin` and the default password is `fortinet`.
12. Repeat the steps above to create the remaining VMs. Note that you need to set up at least 3 controller HA VMs,

Continue to set up the FortiIsolator environment by referring to Setting up the FortiIsolator environment on page 29.

Setting up the FortiIsolator environment

After installing the FortiIsolator firmware on your VMs, set up the FortiIsolator environment by configuring each VM as follows in the exact order:

Configuring the host VM for registry

1. Log into the CLI as root using the following credentials:
   - **username**: root
   - **password**: fortinet
2. Configure the network interfaces:

```
set internal-ip <ip>/<subnet>
set internal-gw 0.0.0.0/0 <gw>
set mgmt-ip <ip>/<subnet>
set set ha-ip <ip>/<subnet>
set dns <primary dns> <secondary dns>
```

3. Configure the host type to be registry:

```
set host-type 2
```

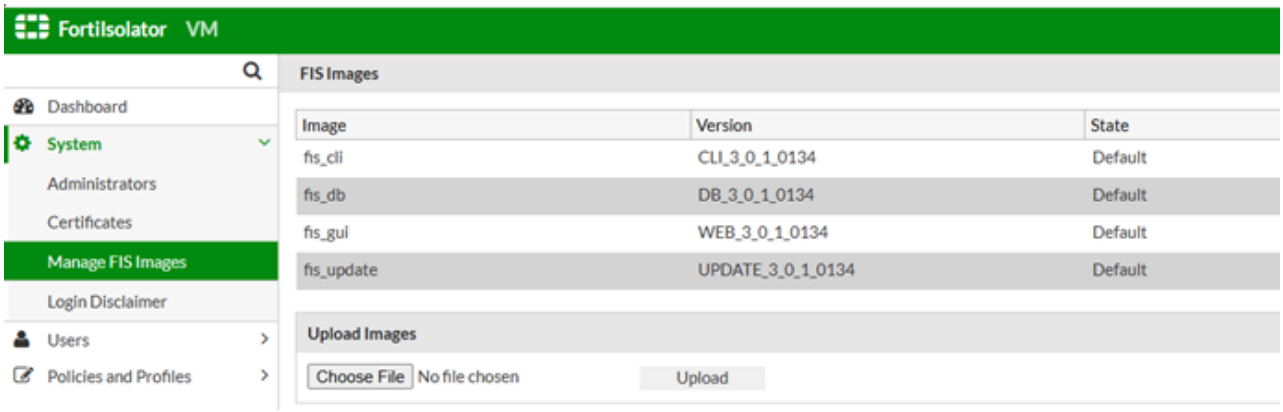
4. Configure the database server:

```
set database-server <ip> 6379 admin <password>
```

5. Configure the run mode:

```
set run-mode 1
```

6. Reboot the machine. The process will take a few minutes.
7. After the machine is up, enter the registry management IP from a web browser and verify that the *System* > *Manage FIS Images* page displays the following:



If the update container image is not included, upload it in the global GUI and apply it in the local GUI.

8. Set the region of the machine to be San Jose:

```
set region san-jose  <total_session_per_region> <region_ip>
```

For example, `set region san-jose 99 172.30.156.47`.

9. If you are configuring registry HA, continue with the following steps:
   a. Repeat the steps above on the second registry machine.
   b. Set registry on each registry node to include both primary and secondary:

```
set registry <primary-registry-ip> <secondary-registry-ip>
```

   For example, `set registry 192.168.3.23 192.168.3.24`.
   c. Set database server on each registry node to point to its own HA IP:

```
set database-server <HA IP> <port> <username> <password>
```

   For example, `set database-server 192.168.3.23 6379 admin password`.

Configuring the host VM for controller HA

1. Log into the CLI as root using the following credentials:
   - **username**: root
   - **password**: fortinet
2. Configure the network interfaces:

```
set internal-ip <ip>/<subnet>
set internal-gw 0.0.0.0/0 <gw>
set mgmt-ip <ip>/<subnet>
set ha-ip <ip>/<subnet>
```

3. Configure the host type to be controller HA:

```
set host-type 3
```

4. Configure the host role to be controller:

```
set host-role controller
```

5. Configure the database server:

```
set database-server admin <password>
```

6. Configure the registry server:

```
set registry <registry ha-ip>
```

If you have set up registry HA with two registry servers, specify the HA IP for both registry servers:

```
set registry <primary-registry-ip> <secondary-registry-ip>.
```

For example, `set registry 192.168.3.23 192.168.3.24`.

7. Configure the run mode:

```
set run-mode 1
```

8. Configure the system model to be VM

```
set system-model VM
```

9. Reboot the machine.
10. Set the region of the machine to be San Jose:

```
set region san-jose
```

11. Repeat the steps above for each additional host VM for controller HA. You need at least three host VMs for controller HA.
12. On each controller HA VM, run `cli status` and `kubectl get nodes` to verify that it has successfully joined the registry.

Do not configure the registry VIP or Portal IP on controller VMs. Controller VMs will automatically retrieve these from the Redis database. Any VIPs configured directly on a controller VM will not be utilized.

Configuring the host VM for worker isolator

1. Log into the CLI as root using the following credentials:
   - **username**: root
   - **password**: fortinet
2. Configure the network interfaces:

```
set internal-ip <ip>/<subnet>
set internal-gw 0.0.0.0/0 <gw>
set mgmt-ip <ip>/<subnet>
set ha-ip <ip>/<subnet>
```

3. Configure the host type to be worker

```
set host-type 0
```

4. Configure the host role to be worker isolator:

```
set host-role worker_isolator
```

5. Configure the database server:

```
set database-server admin <password>
```

6. Configure the registry server:

```
set registry <registry ha-ip>
```

7. Reboot the machine.

Configuring the host VM for worker controller

1. Log into the CLI as root using the following credentials:
   - **username**: root
   - **password**: fortinet
2. Configure the network interfaces:

```
set internal-ip <ip>/<subnet>
set internal-gw 0.0.0.0/0 <gw>
set mgmt-ip <ip>/<subnet>
set ha-ip <ip>/<subnet>
```

3. Configure the host type to be worker:

```
set host-type 0
```

4. Configure the host role to be worker controller:

```
set host-role worker_controller
```

5. Configure the database server:

```
set database-server admin <password>
```

6. Configure the registry server:

```
set registry <registry ha-ip>
```

7. Reboot the machine.

Do not configure the registry VIP or Portal IP on worker VMs. Worker VMs will automatically retrieve these from the Redis database. Any VIPs configured directly on a worker VM will not be utilized.

Verifying the configuration

After the reboot is complete, verify the connection is established by visiting `https://[internal-ip]/isolator/https://www.google.com/`. You may need to clear your browser cache before logging in to the FortiIsolator GUI to make sure that the FortiIsolator GUI displays correctly.

Alternatively, run the following commands in the CLI to verify the configuration:

1. Run `fnsysctl kubectl get pod` to get the full list of pods.
2. Wait for one minute and run `fnsysctl result` to verify that all pods are functioning correctly.

Next steps

1. Install the packages that you downloaded earlier when Downloading the FortiIsolator firmware and package files on page 6. See Manage FIS Images in the Administration Guide for detailed instructions.
2. Backup the system or configuration as needed. See System configuration in the Administration Guide.

www.fortinet.com