Private Cloud Deployment Guide

FortiIsolator 3.0.0

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

April 3, 2025
FortiIsolator 3.0.0 Private Cloud Deployment Guide
51-300-1110656-20250403

TABLE OF CONTENTS

Change log

Date	Change Description
2025-03-31	Initial release.
2025-04-03	Updated Setting up the FortiIsolator environment on page 29.

Introduction

FortiIsolator 3.0.0 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 3.0.0 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	8 GB	1
HA controller	4	24 GB	At least 3 for redundancy
Worker controller	4	24 GB	At least 1
Worker isolator	4	24 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-build0117.kvm.zip`
FortiIsolator VM for VMware	`FIS_VM_VmWare-v3-build0117.vmware.zip`

vSphere	
FortiIsolator VM for VMware ESXi	`FIS_VM_ESXi-v3-build0117.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 on page 7
- Installing FortiIsolator VM for VMware vSphere on page 14
- Installing FortiIsolator VM for VMware ESXi on page 24

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)
3. Worker isolator
4. Worker controller

See the FortiIsolator 3.0.0 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

You can install FortiIsolator VM for Linux KVM manually or using a script.

To install FortiIsolator VM for Linux KVM using a script:

1. Download the `FIS_3.0_install_tool.zip` from here.
2. Unzip it and put all files in a same directory.
3. Edit `config.sh` to provide the IPs for all four VMs.
4. Move the FortiIsolator firmware for Linux KVM (`fis.qcow2`) into the same directory.
5. Run the following script to install all four VMs, which takes around 40 minutes.

   ```
   > ./FIS_30_Install.sh
   ```

FortiIsolator automatically installs all the necessary components and configures the environment settings.

To install FortiIsolator VM for Linux KVM manually:

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

About Virtual Machine Manager

Virtual Machine Manager

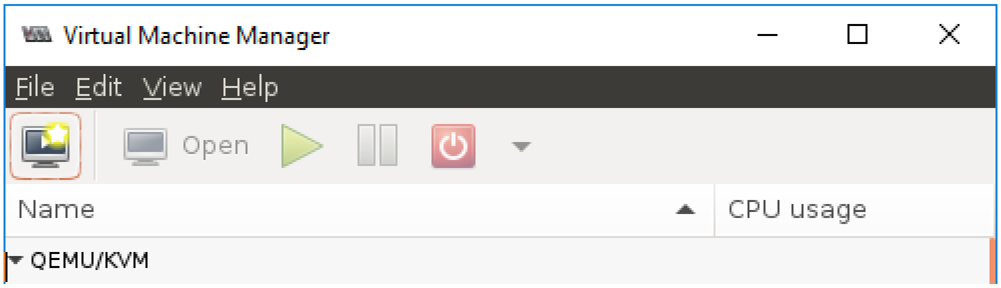
1.3.2

Powered by libvirt

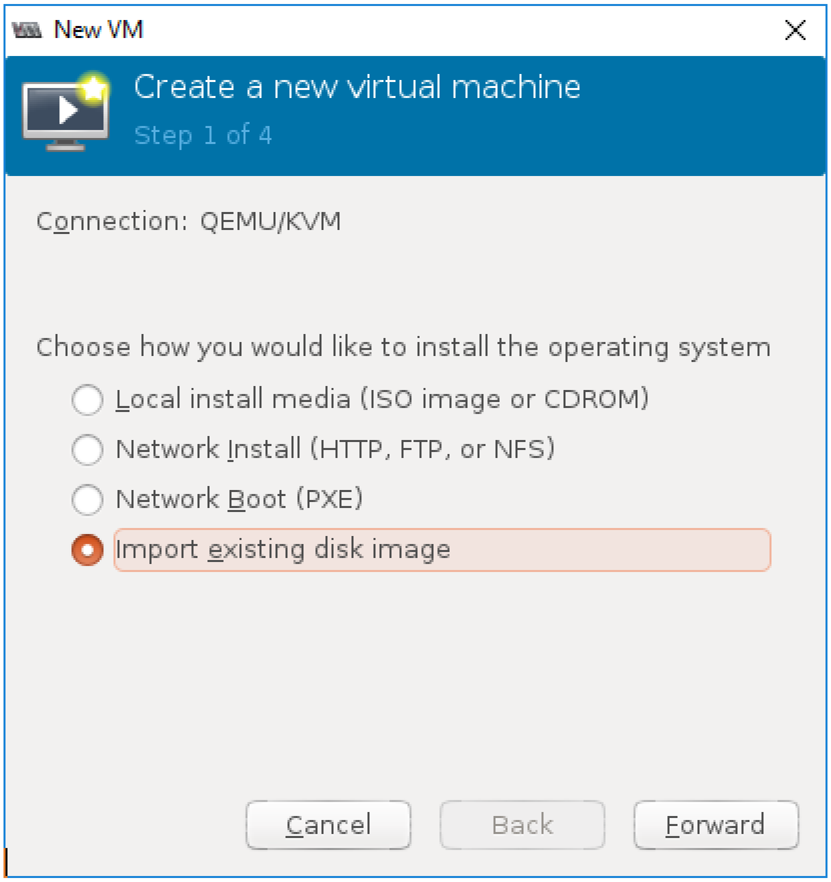
http://virt-manager.org/

Copyright (C) 2006-2014 Red Hat Inc.

2. Create a new virtual machine.



3. Select *Import existing disk image*.

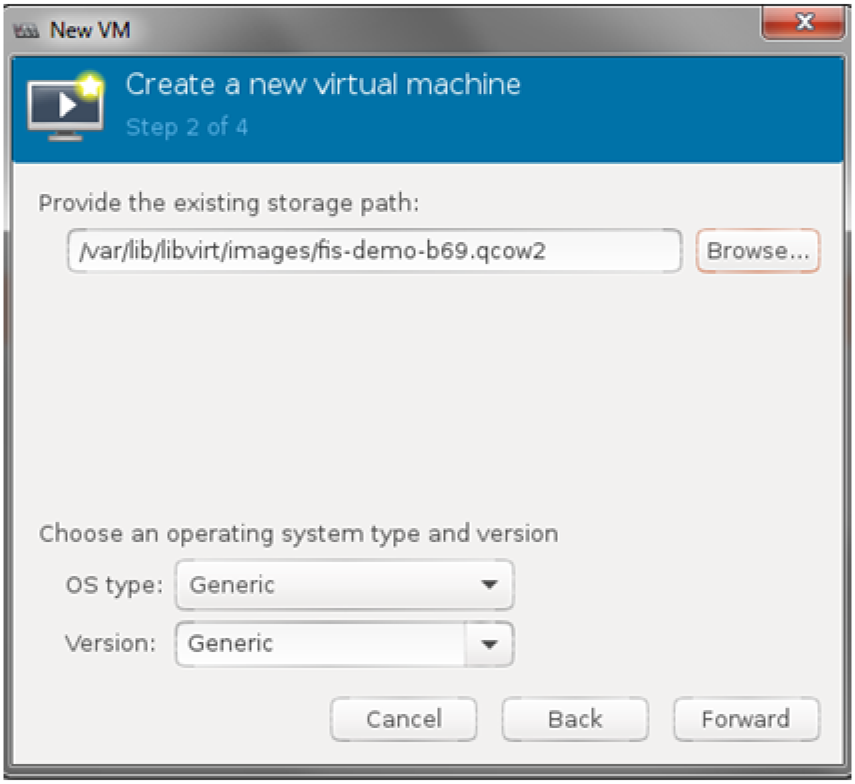


Connection: QEMU/KVM

Choose how you would like to install the operating system

○ Local install media (ISO image or CDROM)
○ Network Install (HTTP, FTP, or NFS)
○ Network Boot (PXE)
● Import existing disk image

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



Create a new virtual machine

Step 2 of 4

Provide the existing storage path:

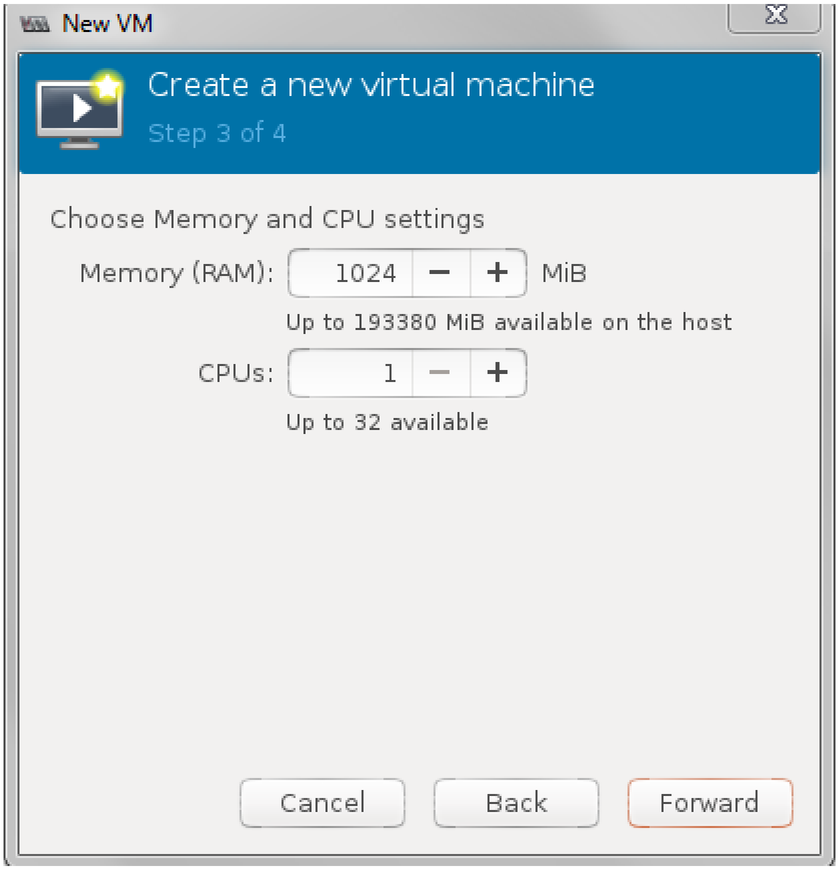
/var/lib/libvirt/images/fis-demo-b69.qcow2

Choose an operating system type and version

OS type: Generic

Version: Generic

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



Choose Memory and CPU settings

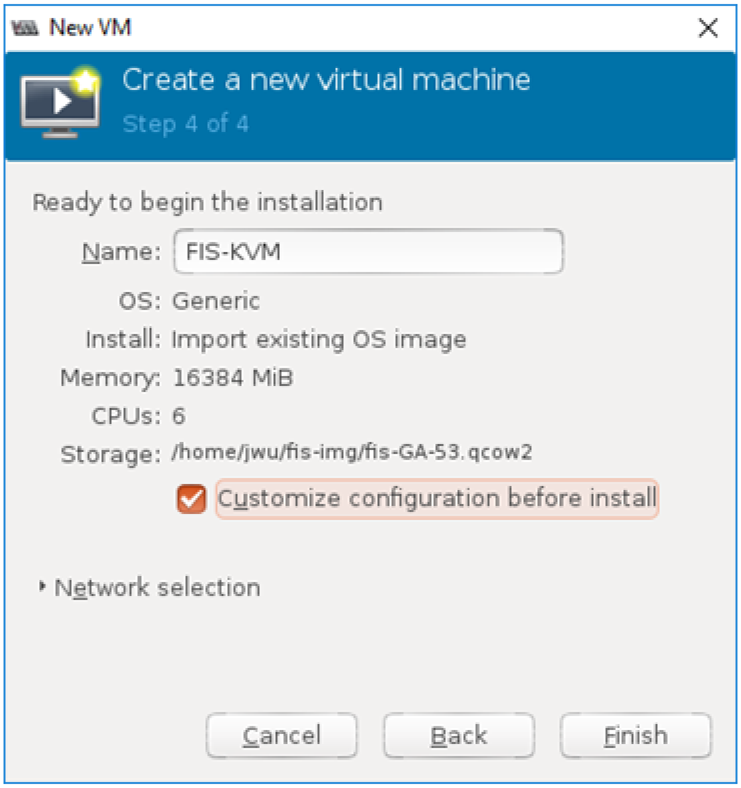
Memory (RAM): 1024 MiB

Up to 193380 MiB available on the host

CPUs: 1

Up to 32 available

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



Ready to begin the installation

Name: FIS-KVM

OS: Generic

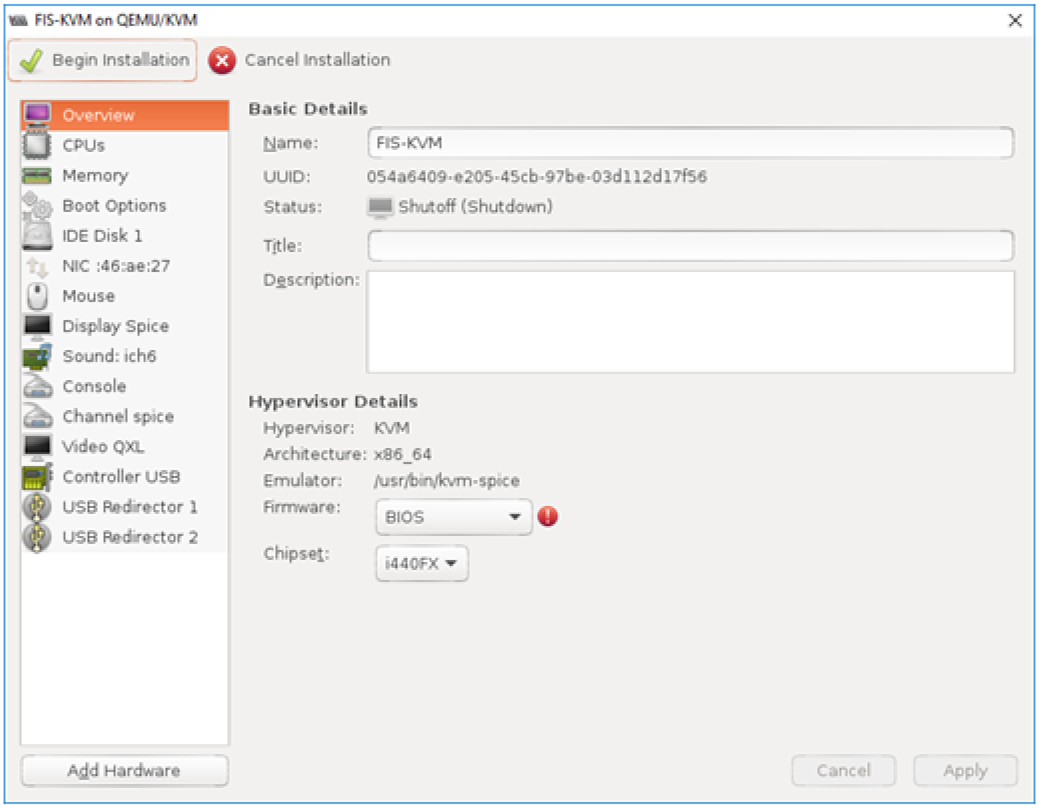
Install: Import existing OS image

Memory: 16384 MiB

CPUs: 6

Storage: /home/jwu/fis-img/fis-GA-53.qcow2

☑ Customize configuration before install



Basic Details

Name: FIS-KVM

UUID: 054a6409-e205-45cb-97be-03d112d17f56

Status: Shutoff (Shutdown)

Title:

Description:

Hypervisor Details

Hypervisor: KVM

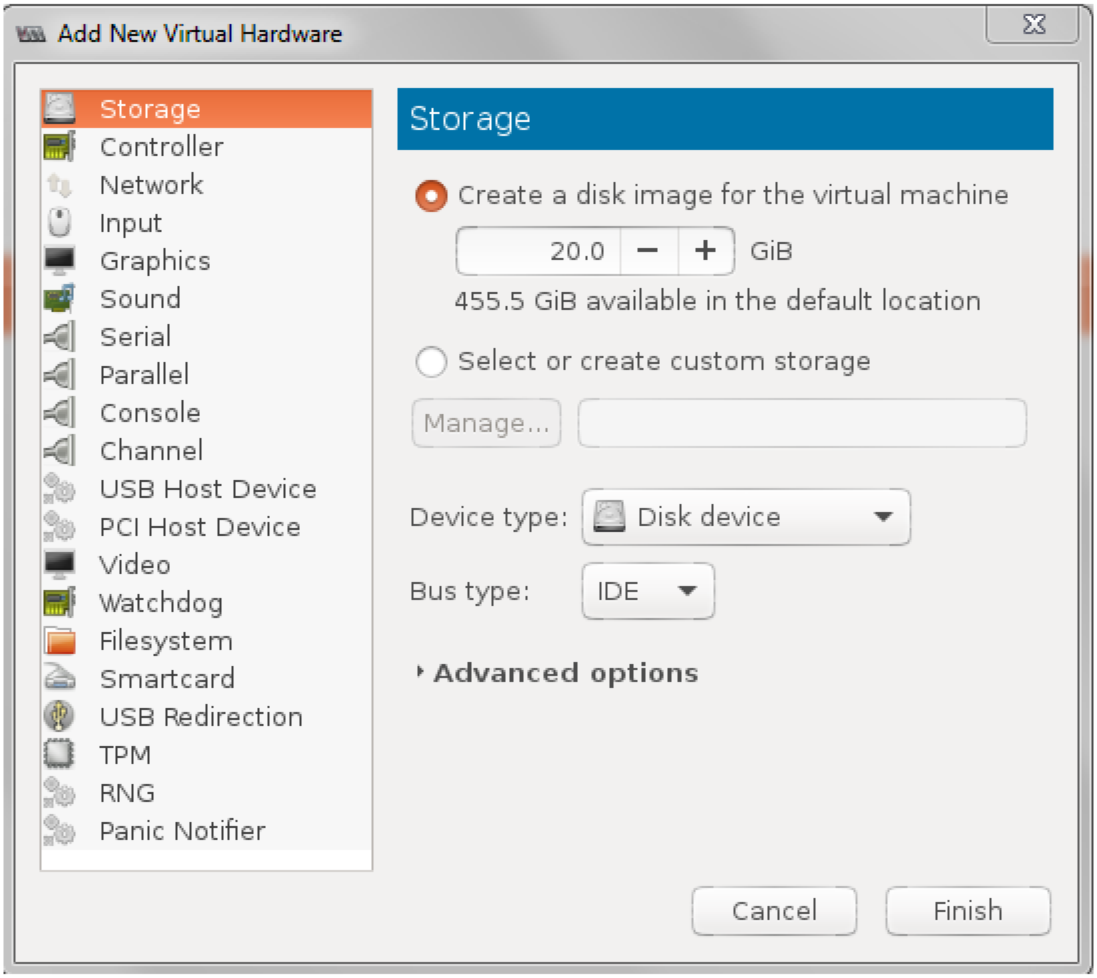
Architecture: x86_64

Emulator: /usr/bin/kvm-spice

Firmware: BIOS

Chipset: i440FX

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



Storage

● Create a disk image for the virtual machine

20.0 GiB

455.5 GiB available in the default location

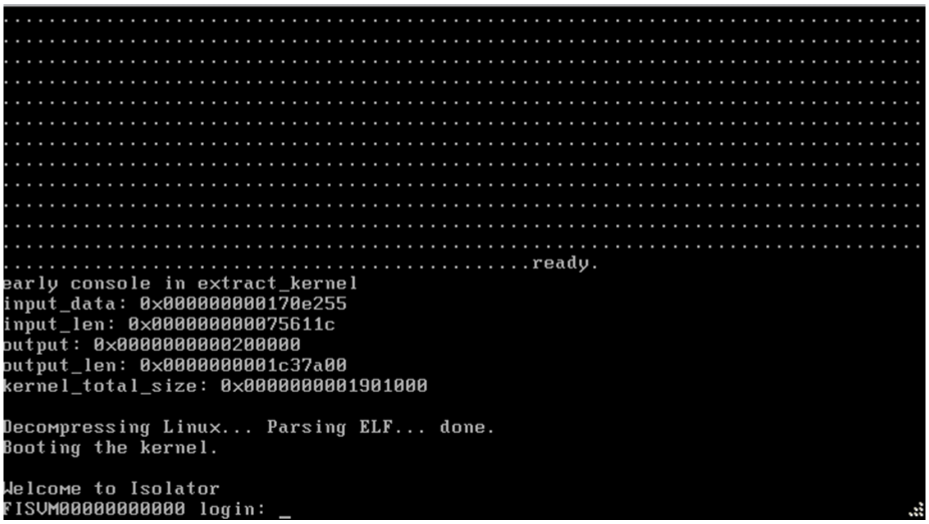
○ Select or create custom storage

Device type: Disk device

Bus type: IDE

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.



```
...............................................................................
...............................................................................
...............................................................................
...............................................................................
...............................................................................
...............................................................................
...............................................................................
...............................................................................
...............................................................................
...............................................................................
...............................................................................
...............................................................................
..............................................ready.
early console in extract_kernel
input_data: 0x000000000170e255
input_len: 0x000000000075611c
output: 0x0000000000200000
output_len: 0x0000000001c37a00
kernel_total_size: 0x0000000001901000

Decompressing Linux... Parsing ELF... done.
Booting the kernel.

Welcome to Isolator
FISVM000000000000 login: _
```

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)
3. Worker isolator
4. Worker controller

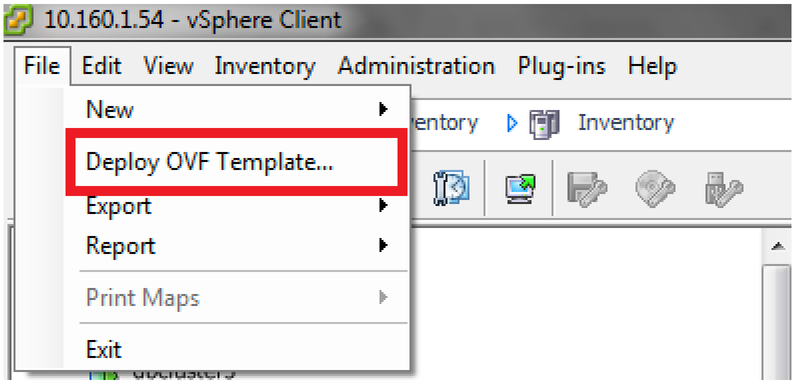
See the FortiIsolator 3.0.0 Administration Guide for more details about each component and how they communicate with each other.

Prerequisites

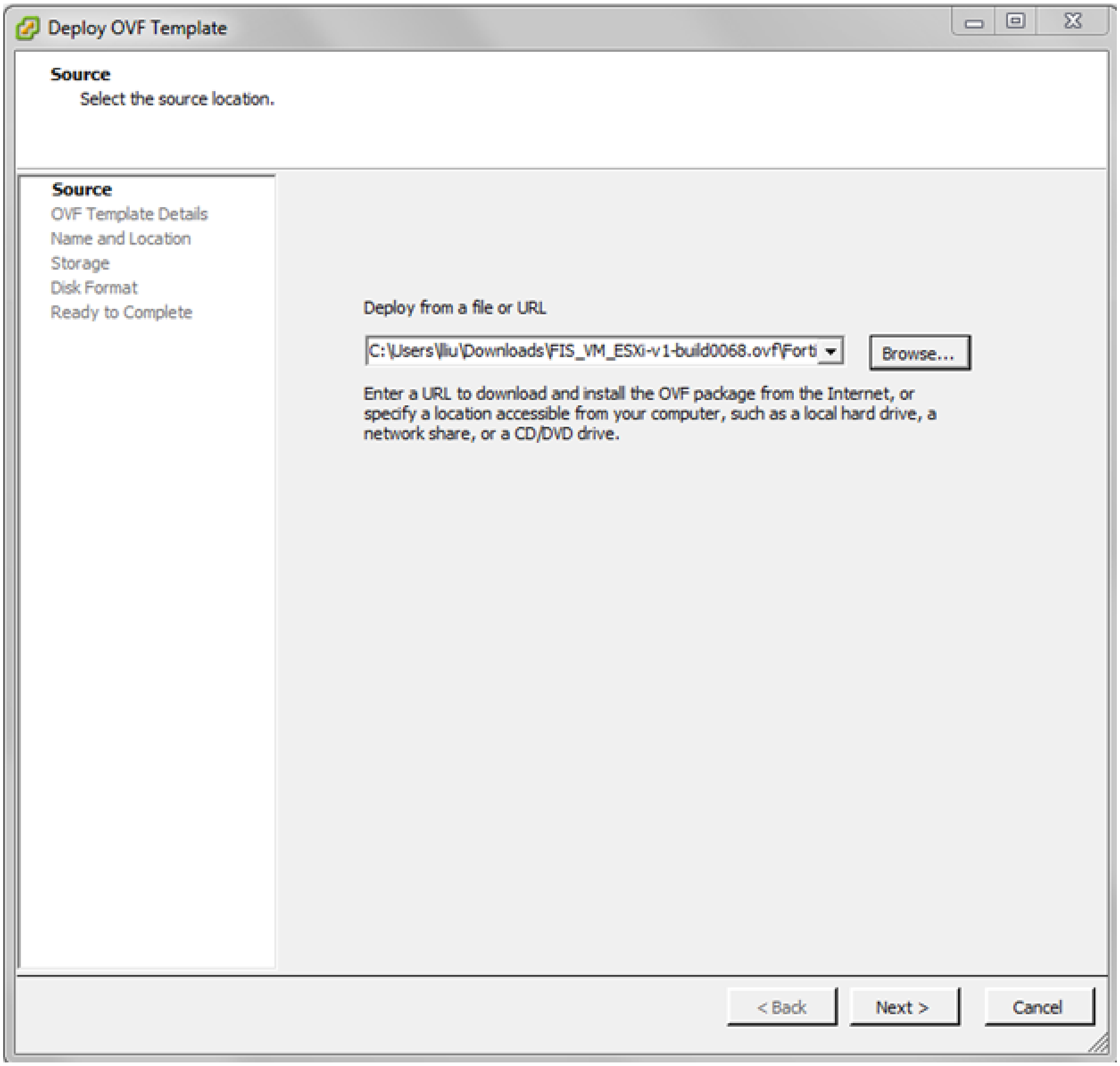
- You have downloaded the FortiIsolator firmware for VMware. See Downloading the FortiIsolator firmware and package files on page 6.
- Install VMware vSphere Client.
- Ensure that your system has one of the following combinations of hard disks and network adapters to support ESXI 6.0:
  - Two SCSI hard 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`.

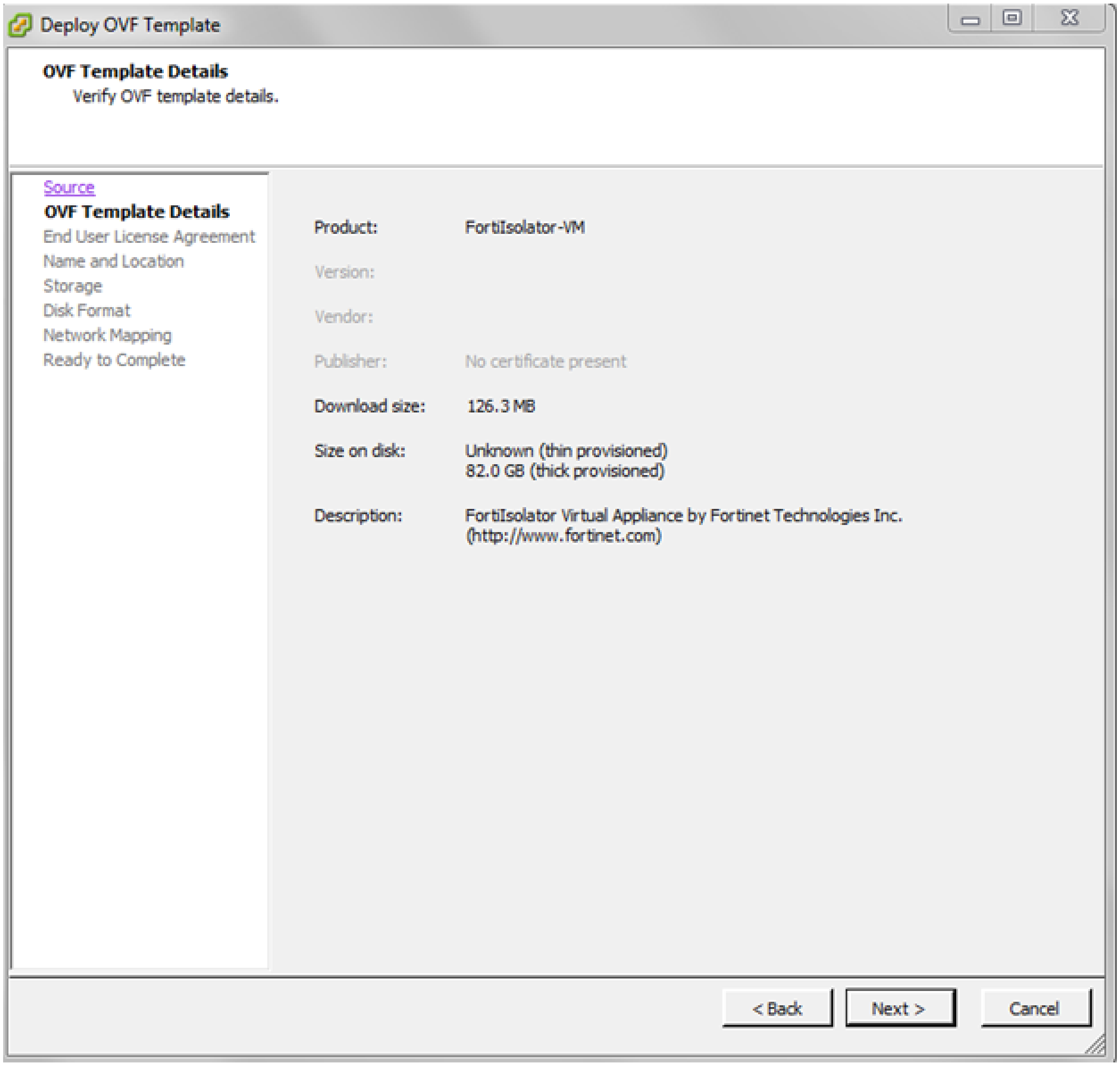


Deploy from a file or URL

C:\Users\lliu\Downloads\FIS_VM_ESXi-v1-build0068.ovf\Forti

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

3. Verify the OVF template details.



OVF Template Details

Verify OVF template details.

Product: FortiIsolator-VM

Version:

Vendor:

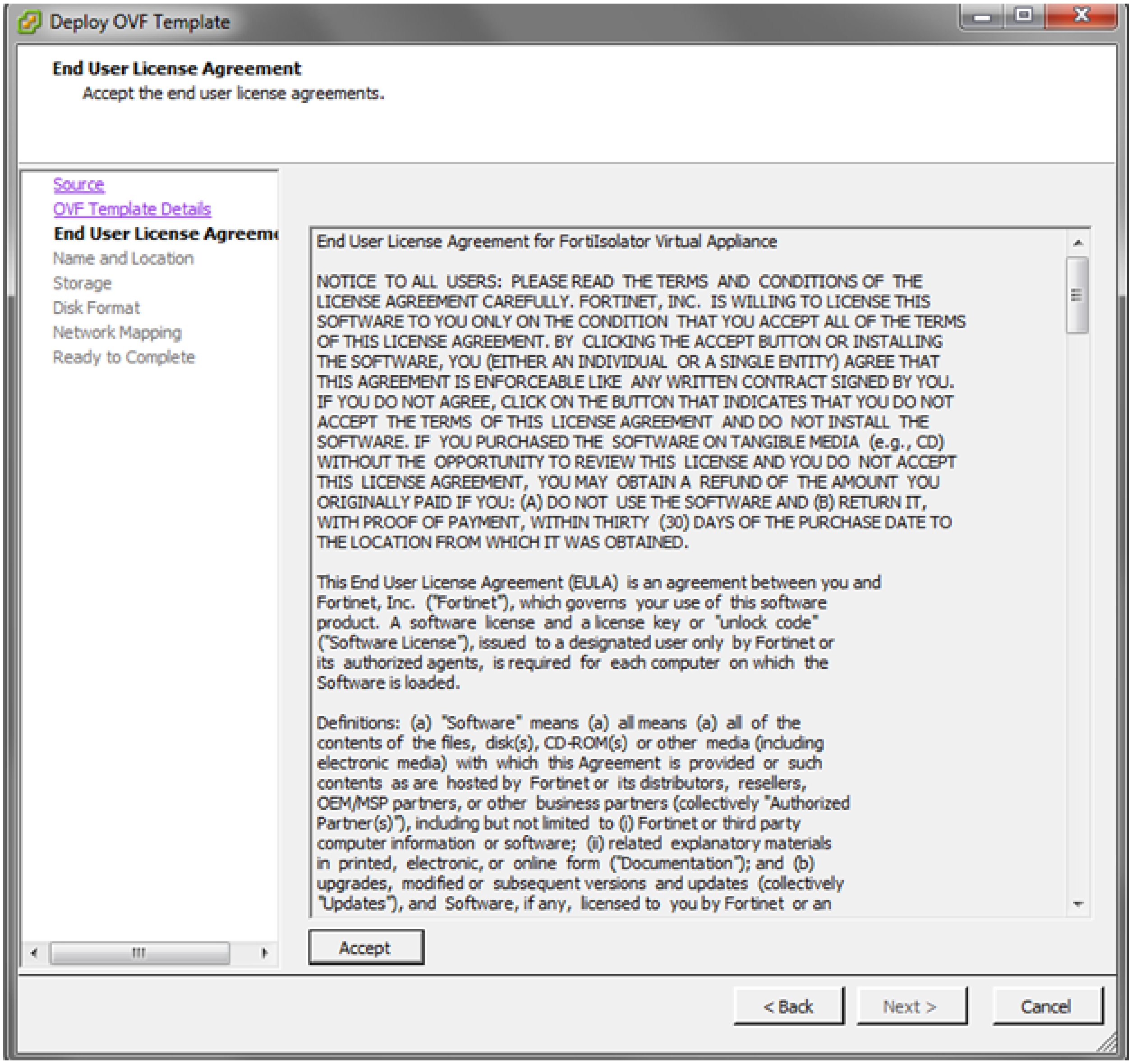
Publisher: No certificate present

Download size: 126.3 MB

Size on disk: Unknown (thin provisioned)
82.0 GB (thick provisioned)

Description: FortiIsolator Virtual Appliance by Fortinet Technologies Inc.
(http://www.fortinet.com)

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



End User License Agreement

Accept the end user license agreements.

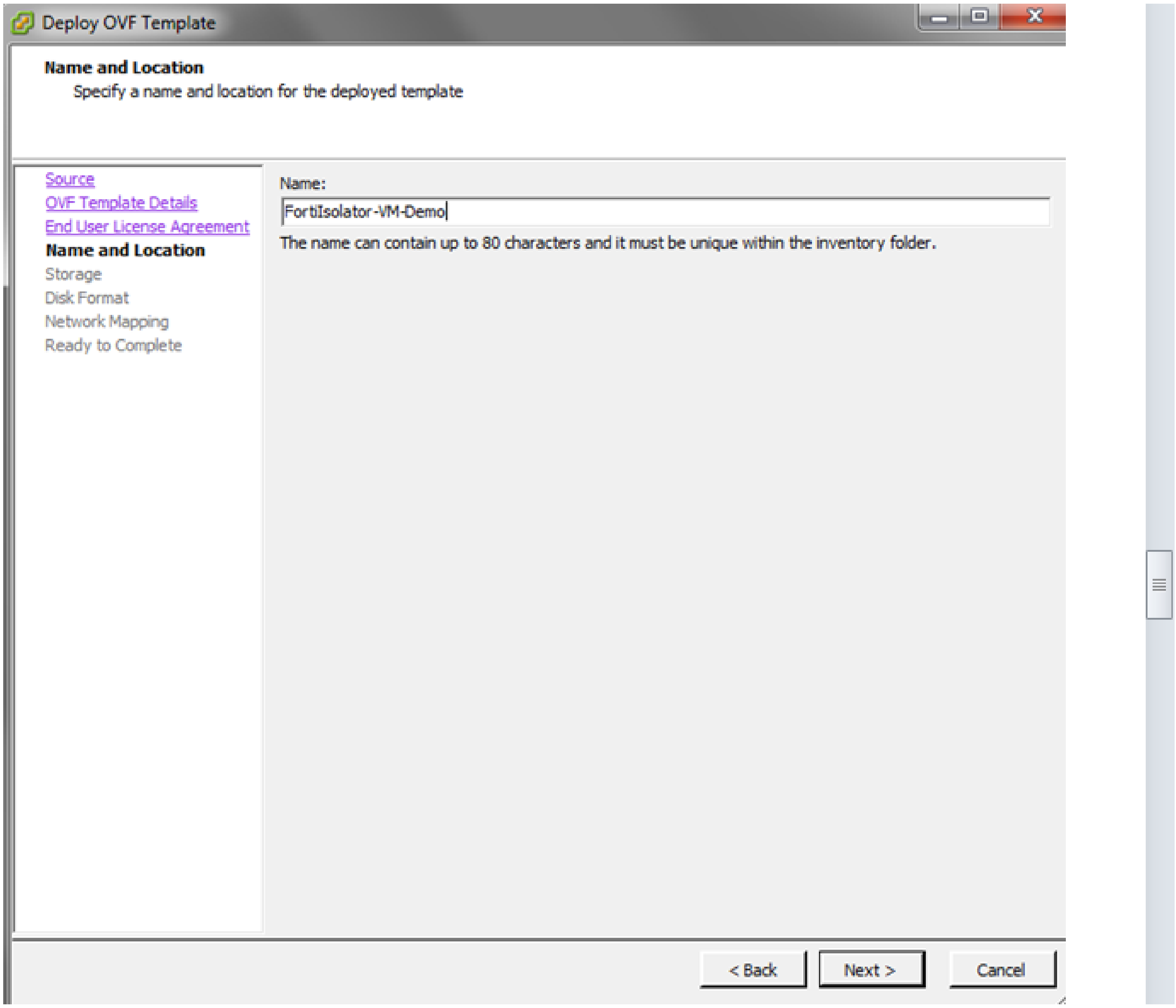
End User License Agreement for FortiIsolator Virtual Appliance

NOTICE TO ALL USERS: PLEASE READ THE TERMS AND CONDITIONS OF THE LICENSE AGREEMENT CAREFULLY. FORTINET, INC. IS WILLING TO LICENSE THIS SOFTWARE TO YOU ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. BY CLICKING THE ACCEPT BUTTON OR INSTALLING THE SOFTWARE, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN CONTRACT SIGNED BY YOU. IF YOU DO NOT AGREE, CLICK ON THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS LICENSE AGREEMENT AND DO NOT INSTALL THE SOFTWARE. IF YOU PURCHASED THE SOFTWARE ON TANGIBLE MEDIA (e.g., CD) WITHOUT THE OPPORTUNITY TO REVIEW THIS LICENSE AND YOU DO NOT ACCEPT THIS LICENSE AGREEMENT, YOU MAY OBTAIN A REFUND OF THE AMOUNT YOU ORIGINALLY PAID IF YOU: (A) DO NOT USE THE SOFTWARE AND (B) RETURN IT, WITH PROOF OF PAYMENT, WITHIN THIRTY (30) DAYS OF THE PURCHASE DATE TO THE LOCATION FROM WHICH IT WAS OBTAINED.

This End User License Agreement (EULA) is an agreement between you and Fortinet, Inc. ("Fortinet"), which governs your use of this software product. A software license and a license key or "unlock code" ("Software License"), issued to a designated user only by Fortinet or its authorized agents, is required for each computer on which the Software is loaded.

Definitions: (a) "Software" means (a) all means (a) all of the contents of the files, disk(s), CD-ROM(s) or other media (including electronic media) with which this Agreement is provided or such contents as are hosted by Fortinet or its distributors, resellers, OEM/MSP partners, or other business partners (collectively "Authorized Partner(s)"), including but not limited to (i) Fortinet or third party computer information or software; (ii) related explanatory materials in printed, electronic, or online form ("Documentation"); and (b) upgrades, modified or subsequent versions and updates (collectively "Updates"), and Software, if any, licensed to you by Fortinet or an

5. Name the new FortiIsolator virtual machine.



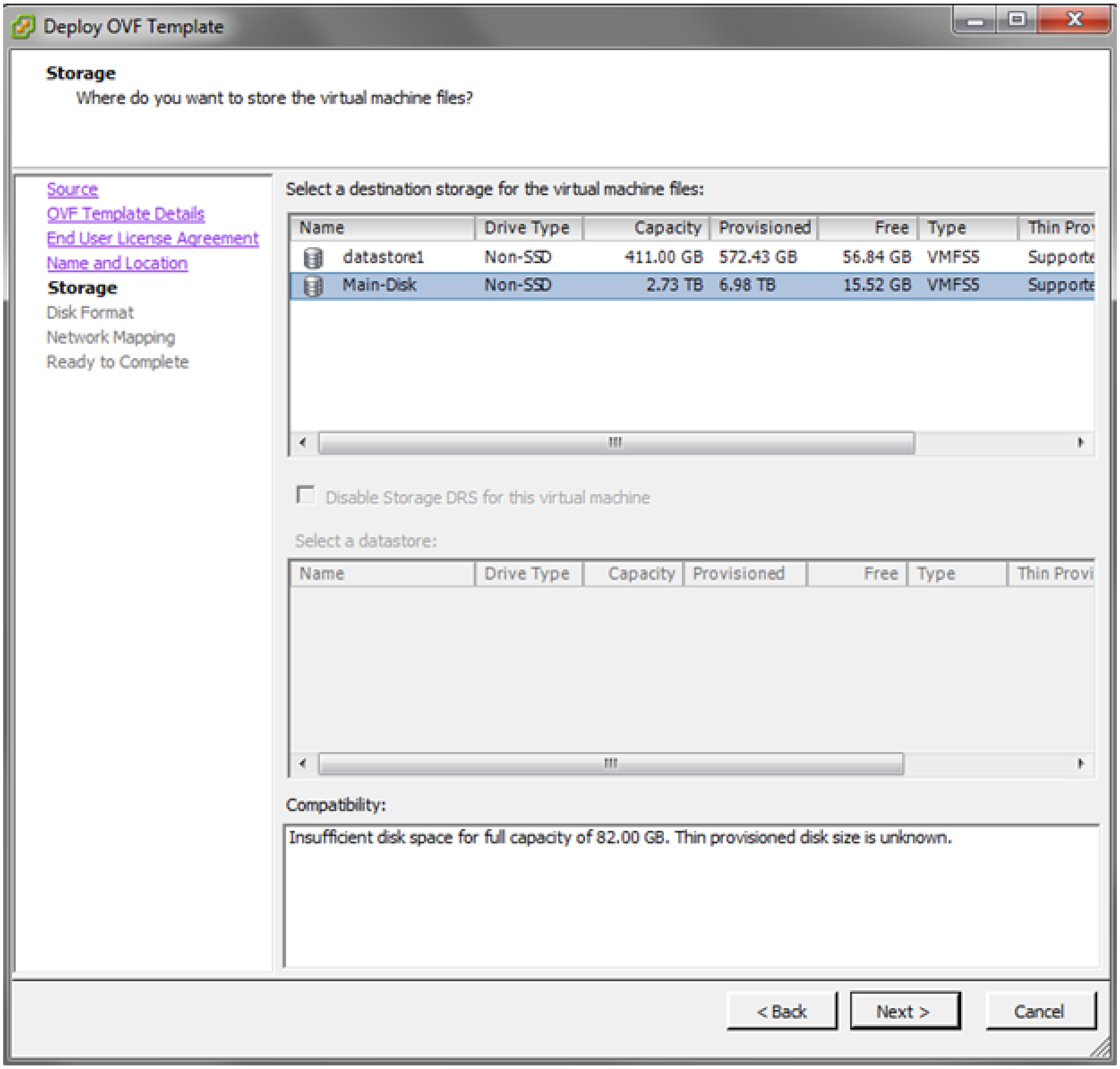
Name and Location

Specify a name and location for the deployed template

Name: FortiIsolator-VM-Demo

The name can contain up to 80 characters and it must be unique within the inventory folder.

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



Storage

Where do you want to store the virtual machine files?

Select a destination storage for the virtual machine files:

Name	Drive Type	Capacity	Provisioned	Free	Type	Thin Pro
datastore1	Non-SSD	411.00 GB	572.43 GB	56.84 GB	VMFS5	Supporte
Main-Disk	Non-SSD	2.73 TB	6.98 TB	15.52 GB	VMFS5	Supporte

□ Disable Storage DRS for this virtual machine

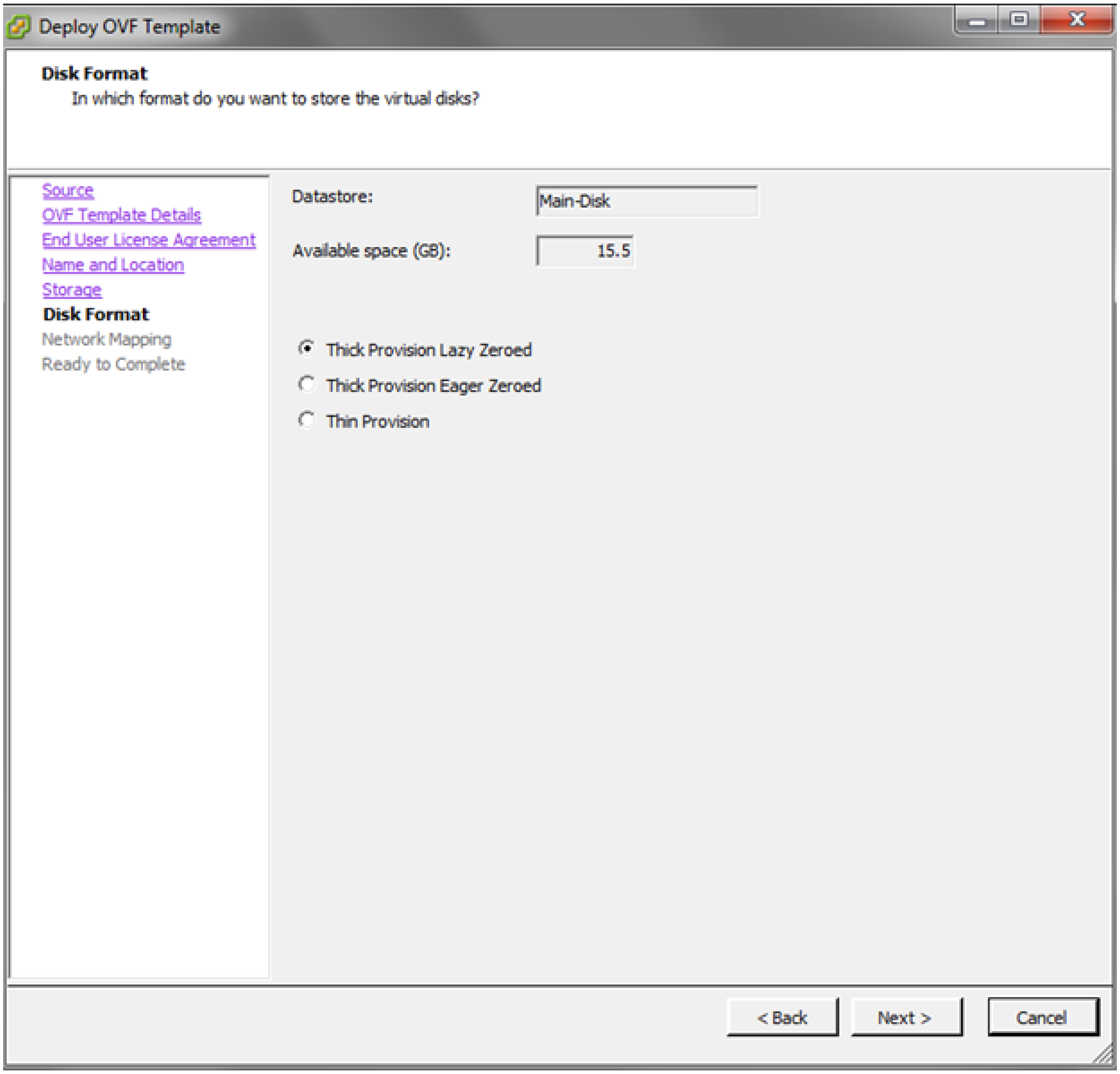
Select a datastore:

Name	Drive Type	Capacity	Provisioned	Free	Type	Thin Provi

Compatibility:

Insufficient disk space for full capacity of 82.00 GB. Thin provisioned disk size is unknown.

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.



Disk Format

In which format do you want to store the virtual disks?

Datastore: Main-Disk

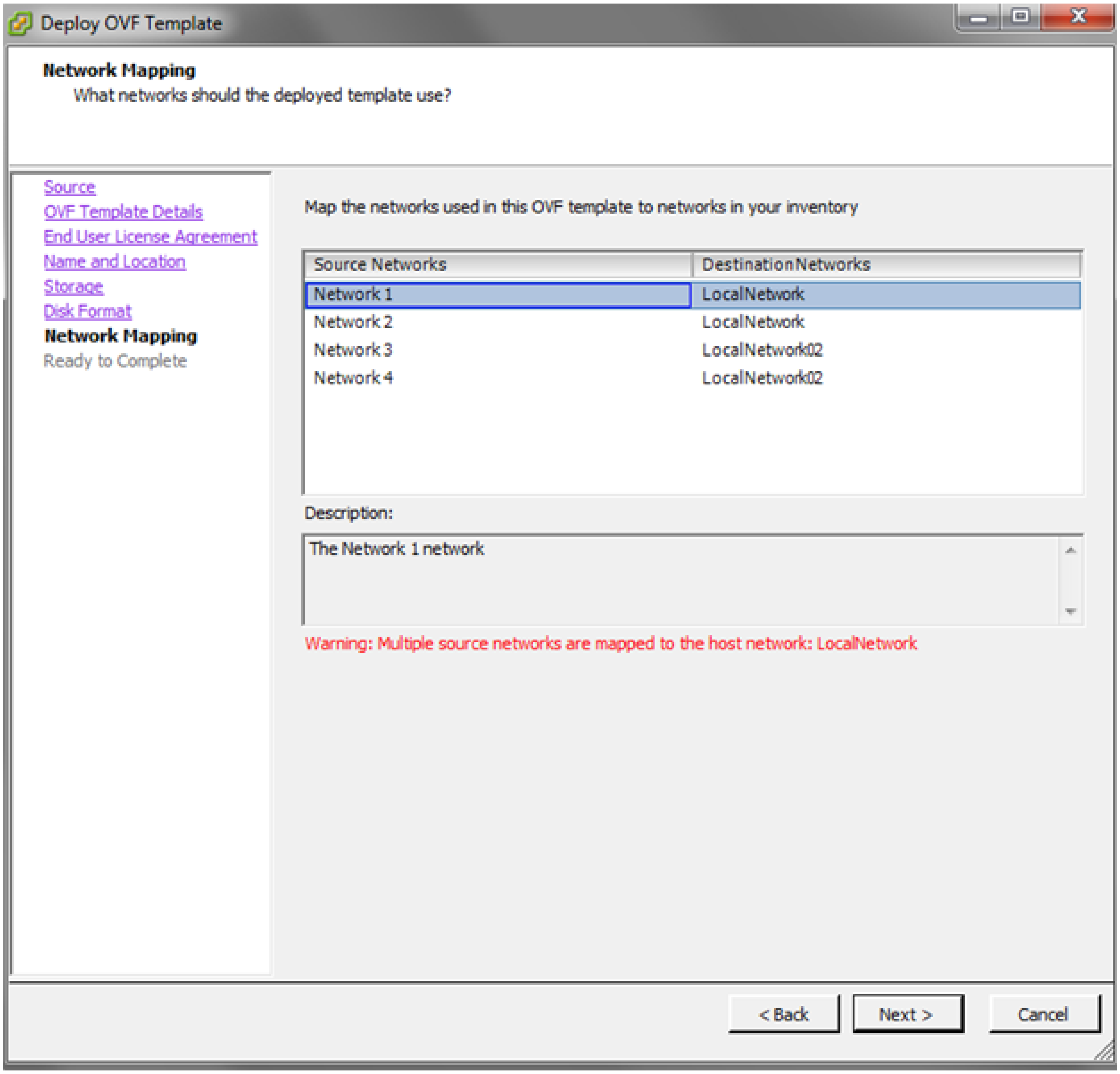
Available space (GB): 15.5

● Thick Provision Lazy Zeroed

○ Thick Provision Eager Zeroed

○ Thin Provision

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



Network Mapping

What networks should the deployed template use?

Map the networks used in this OVF template to networks in your inventory

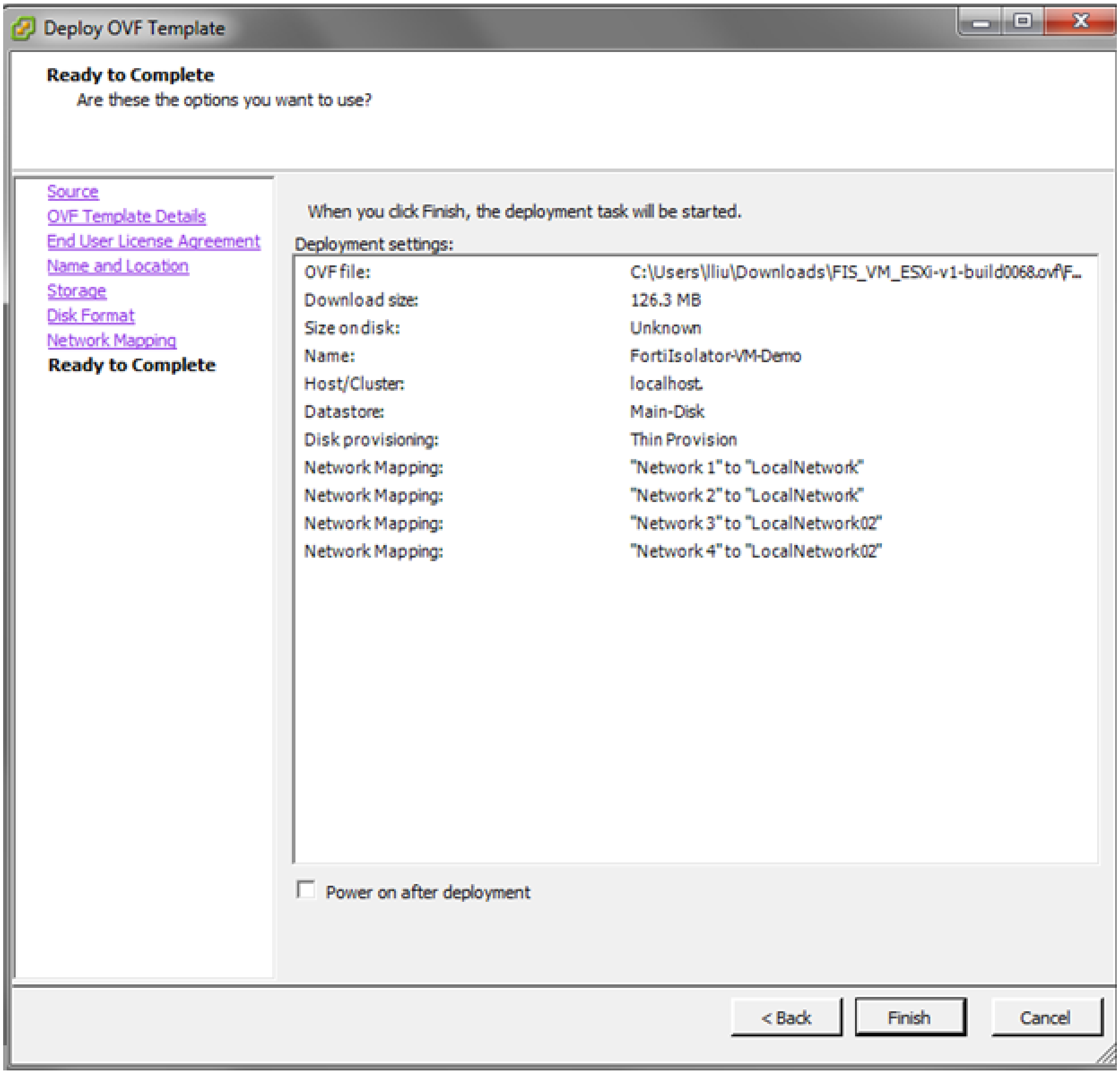
Source Networks	DestinationNetworks
Network 1	LocalNetwork
Network 2	LocalNetwork
Network 3	LocalNetwork02
Network 4	LocalNetwork02

Description:

The Network 1 network

Warning: Multiple source networks are mapped to the host network: LocalNetwork

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



Ready to Complete

Are these the options you want to use?

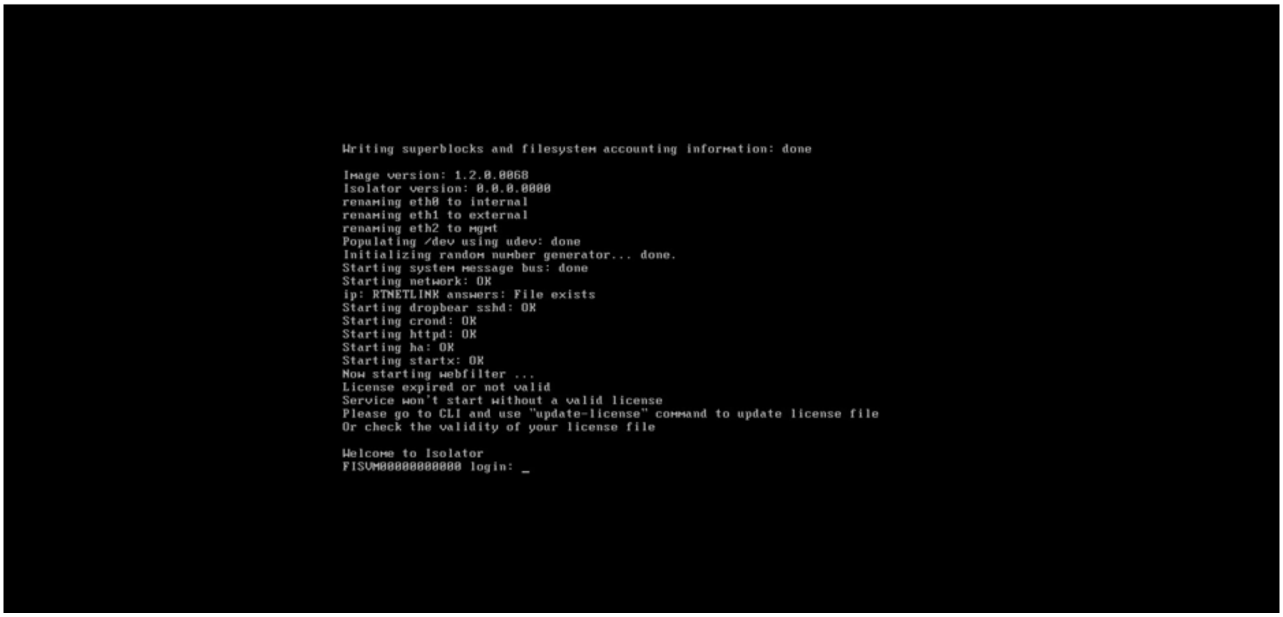
When you click Finish, the deployment task will be started.

Deployment settings:

OVF file:	C:\Users\lliu\Downloads\FIS_VM_ESXi-v1-build0068.ovf\F...
Download size:	126.3 MB
Size on disk:	Unknown
Name:	FortiIsolator-VM-Demo
Host/Cluster:	localhost.
Datastore:	Main-Disk
Disk provisioning:	Thin Provision
Network Mapping:	"Network 1" to "LocalNetwork"
Network Mapping:	"Network 2" to "LocalNetwork"
Network Mapping:	"Network 3" to "LocalNetwork02"
Network Mapping:	"Network 4" to "LocalNetwork02"

□ Power on after deployment

10. Start the FortiIsolator VM.



```
Writing superblocks and filesystem accounting information: done

Image version: 1.2.0.0068
Isolator version: 0.0.0.0000
renaming eth0 to internal
renaming eth1 to external
renaming eth2 to mgmt
Populating /dev using udev: done
Initializing random number generator... done.
Starting system message bus: done
Starting network: OK
ip: RTNETLINK answers: File exists
Starting dropbear sshd: OK
Starting crond: OK
Starting httpd: OK
Starting ha: OK
Starting startx: OK
Now starting webfilter ...
License expired or not valid
Service won't start without a valid license
Please go to CLI and use "update-license" command to update license file
Or check the validity of your license file

Welcome to Isolator
FISVM000000000000 login: _
```

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)
3. Worker isolator
4. Worker controller

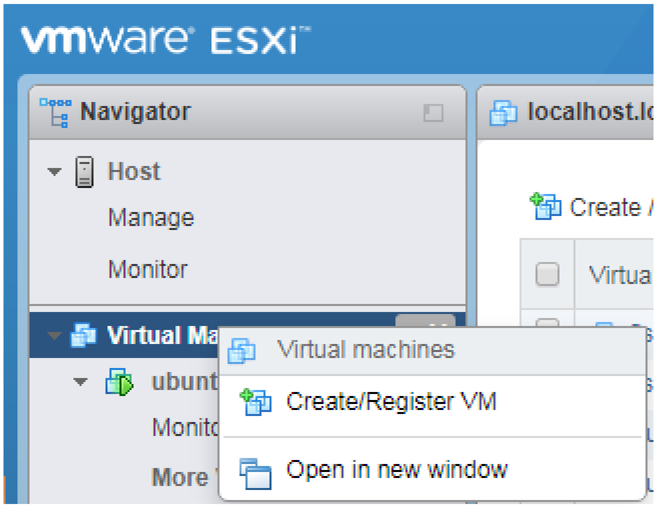
See the FortiIsolator 3.0.0 Administration Guide for more details about each component and how they communicate with each other.

Prerequisites

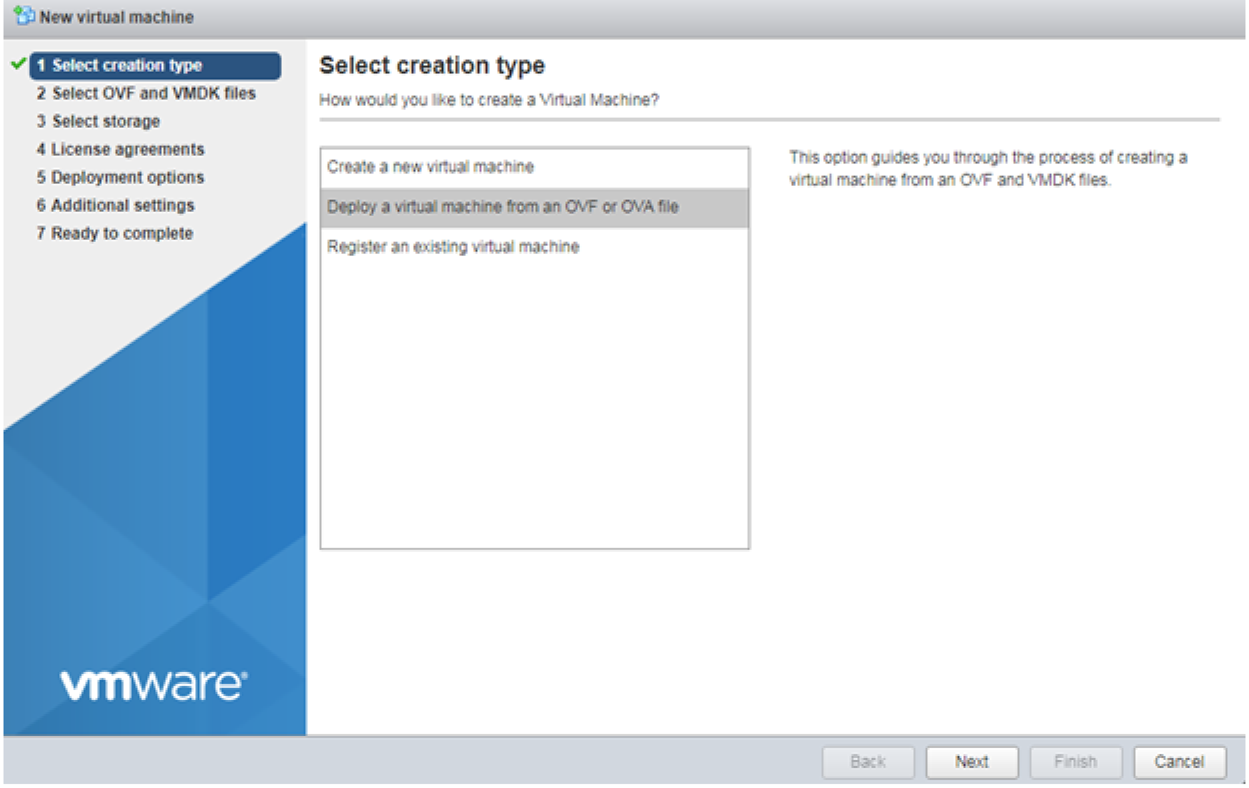
- You have download the FortiIsolator firmware for ESXi. See Downloading the FortiIsolator firmware and package files on page 6.
- Install VMware ESXi.
- Ensure that your system has one of the following combinations of hard disks and network adapters to support ESXI 6.5:
  - Two SCSI hard disks and three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


New virtual machine

1 Select creation type
2 Select OVF and VMDK files
3 Select storage
4 License agreements
5 Deployment options
6 Additional settings
7 Ready to complete

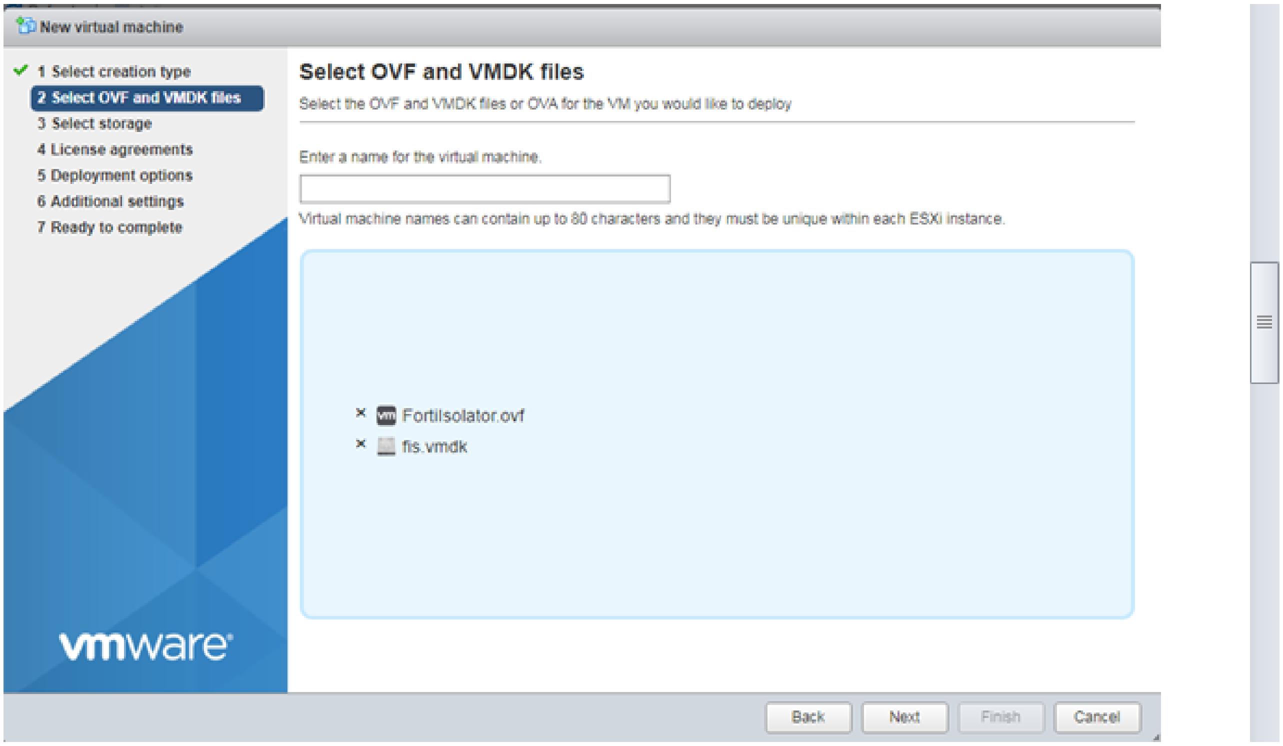
Select creation type

How would you like to create a Virtual Machine?

Create a new virtual machine
Deploy a virtual machine from an OVF or OVA file
Register an existing virtual machine

This option guides you through the process of creating a virtual machine from an OVF and VMDK files.

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



New virtual machine

- ✓ 1 Select creation type
- 2 Select OVF and VMDK files
- 3 Select storage
- 4 License agreements
- 5 Deployment options
- 6 Additional settings
- 7 Ready to complete

Select OVF and VMDK files

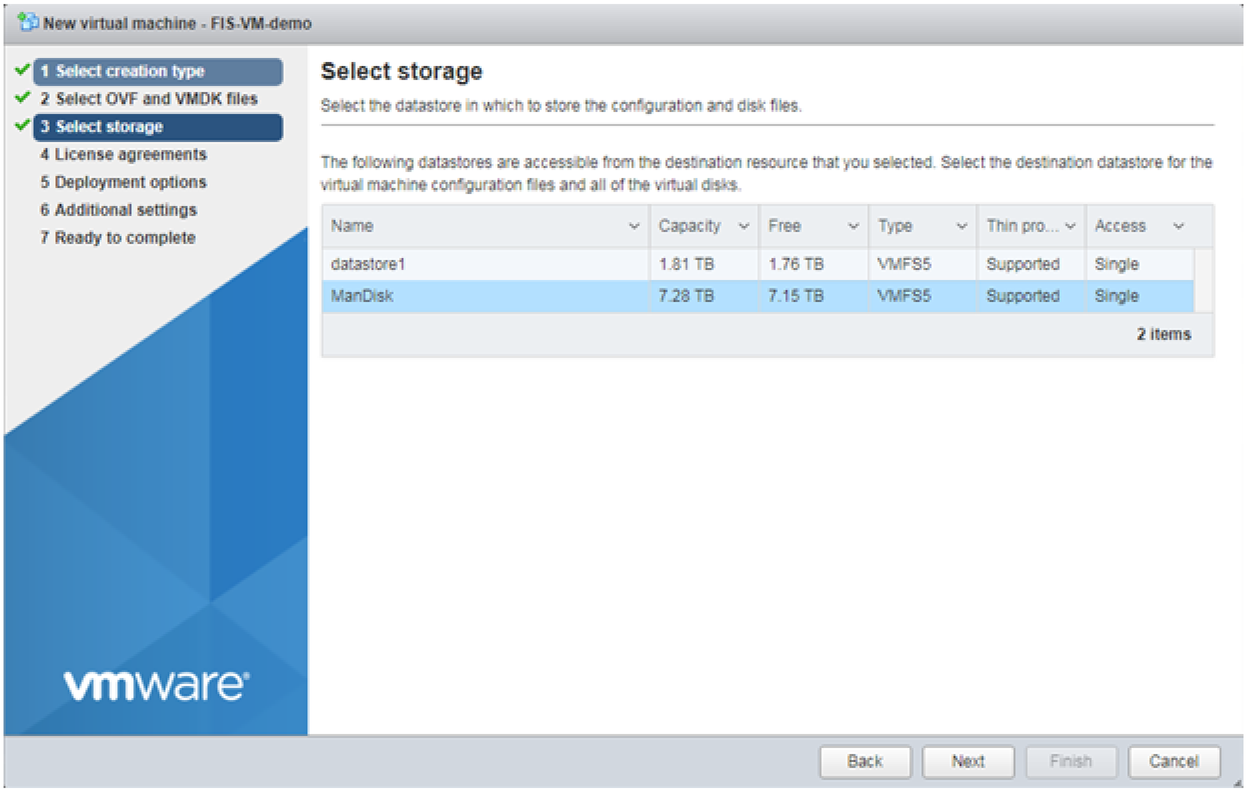
Select the OVF and VMDK files or OVA for the VM you would like to deploy

Enter a name for the virtual machine.

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.

- × FortiIsolator.ovf
- × fis.vmdk

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.



New virtual machine - FIS-VM-demo

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- 4 License agreements
- 5 Deployment options
- 6 Additional settings
- 7 Ready to complete

Select storage

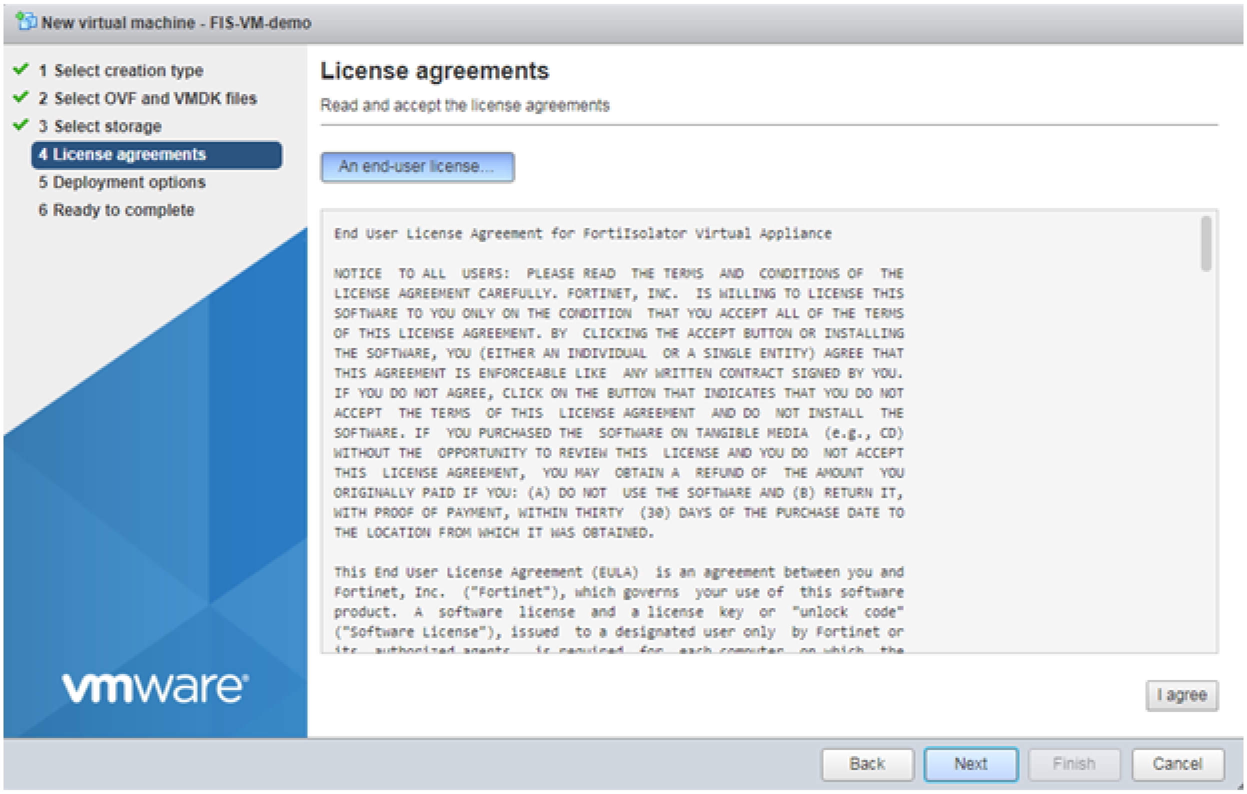
Select the datastore in which to store the configuration and disk files.

The following datastores are accessible from the destination resource that you selected. Select the destination datastore for the virtual machine configuration files and all of the virtual disks.

Name	Capacity	Free	Type	Thin pro...	Access
datastore1	1.81 TB	1.76 TB	VMFS5	Supported	Single
ManDisk	7.28 TB	7.15 TB	VMFS5	Supported	Single

2 items

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



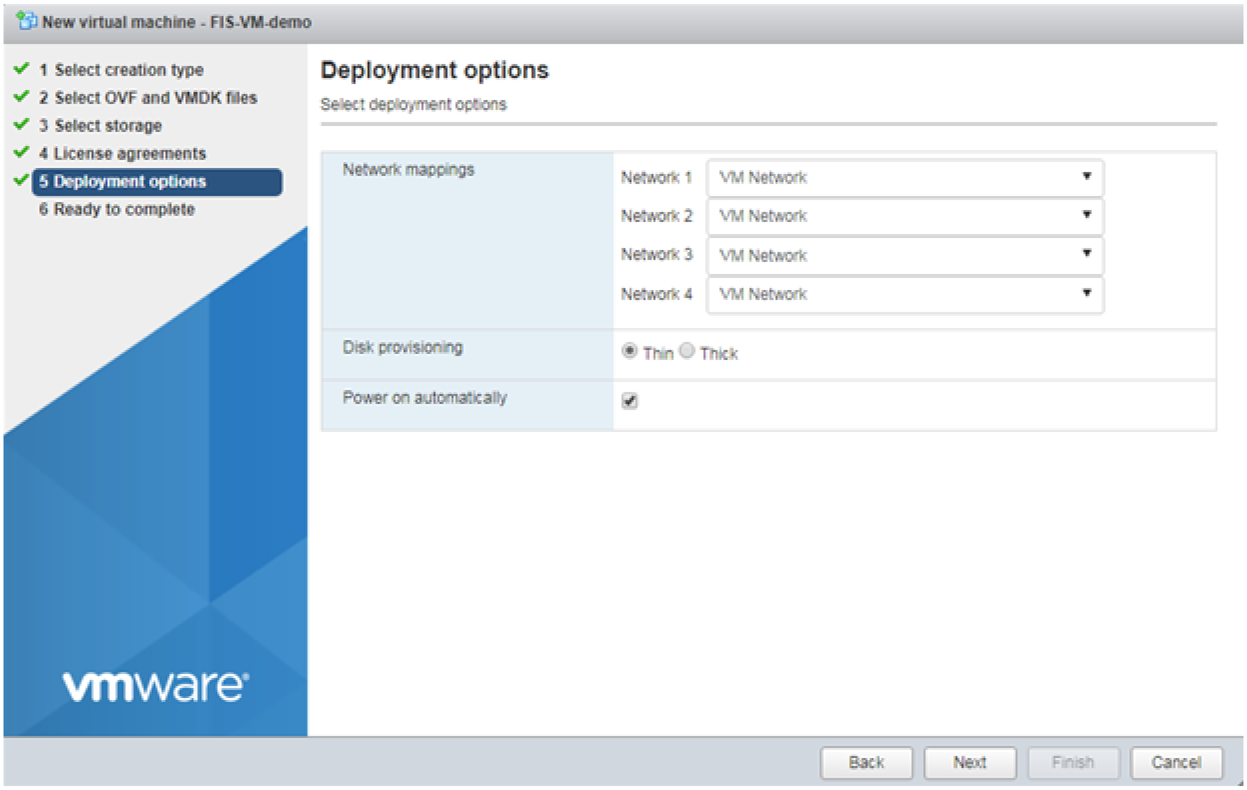
End User License Agreement for FortiIsolator Virtual Appliance

NOTICE TO ALL USERS: PLEASE READ THE TERMS AND CONDITIONS OF THE LICENSE AGREEMENT CAREFULLY. FORTINET, INC. IS WILLING TO LICENSE THIS SOFTWARE TO YOU ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. BY CLICKING THE ACCEPT BUTTON OR INSTALLING THE SOFTWARE, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN CONTRACT SIGNED BY YOU. IF YOU DO NOT AGREE, CLICK ON THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS LICENSE AGREEMENT AND DO NOT INSTALL THE SOFTWARE. IF YOU PURCHASED THE SOFTWARE ON TANGIBLE MEDIA (e.g., CD) WITHOUT THE OPPORTUNITY TO REVIEW THIS LICENSE AND YOU DO NOT ACCEPT THIS LICENSE AGREEMENT, YOU MAY OBTAIN A REFUND OF THE AMOUNT YOU ORIGINALLY PAID IF YOU: (A) DO NOT USE THE SOFTWARE AND (B) RETURN IT, WITH PROOF OF PAYMENT, WITHIN THIRTY (30) DAYS OF THE PURCHASE DATE TO THE LOCATION FROM WHICH IT WAS OBTAINED.

This End User License Agreement (EULA) is an agreement between you and Fortinet, Inc. ("Fortinet"), which governs your use of this software product. A software license and a license key or "unlock code" ("Software License"), issued to a designated user only by Fortinet or its authorized agents is required for each computer on which the

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



New virtual machine - FIS-VM-demo

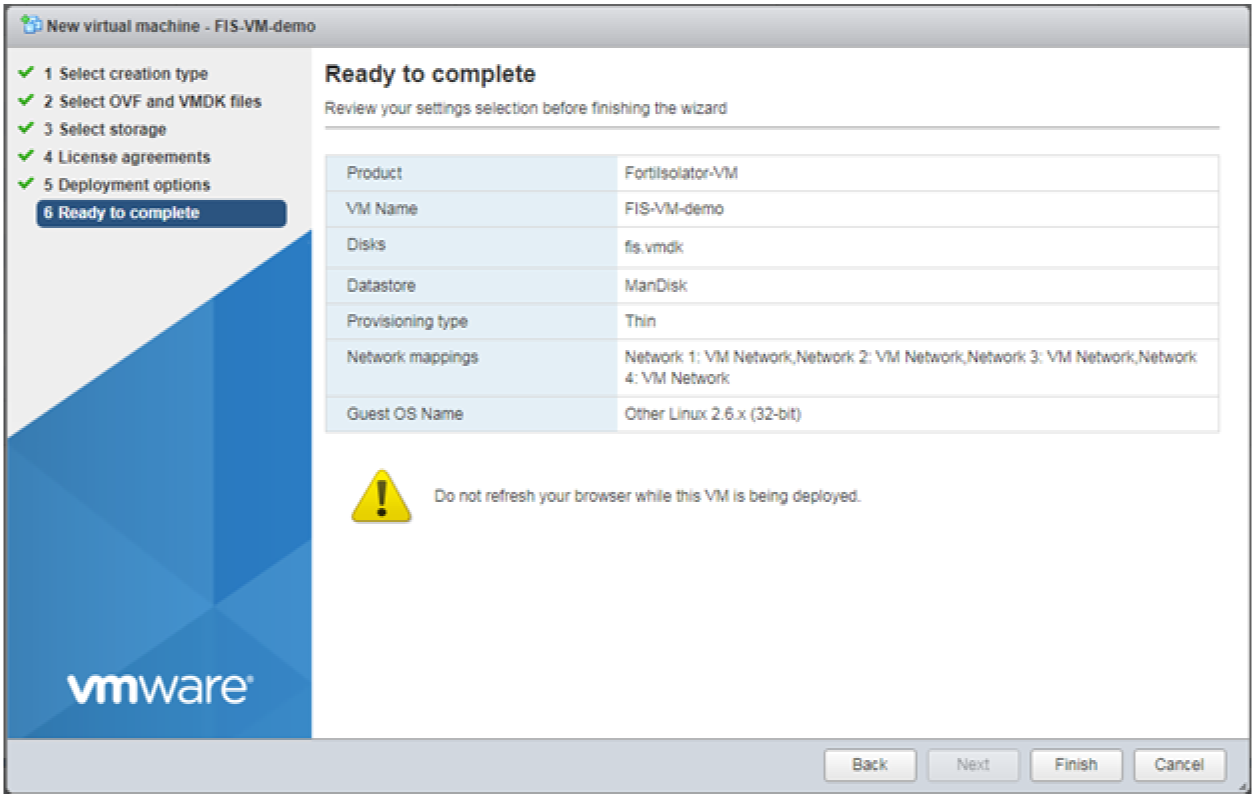
- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- ✓ 4 License agreements
- ✓ 5 Deployment options
- 6 Ready to complete

Deployment options

Select deployment options

Network mappings	Network 1: VM Network Network 2: VM Network Network 3: VM Network Network 4: VM Network
Disk provisioning	● Thin ○ Thick
Power on automatically	☑

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



New virtual machine - FIS-VM-demo

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- ✓ 4 License agreements
- ✓ 5 Deployment options
- 6 Ready to complete

Ready to complete

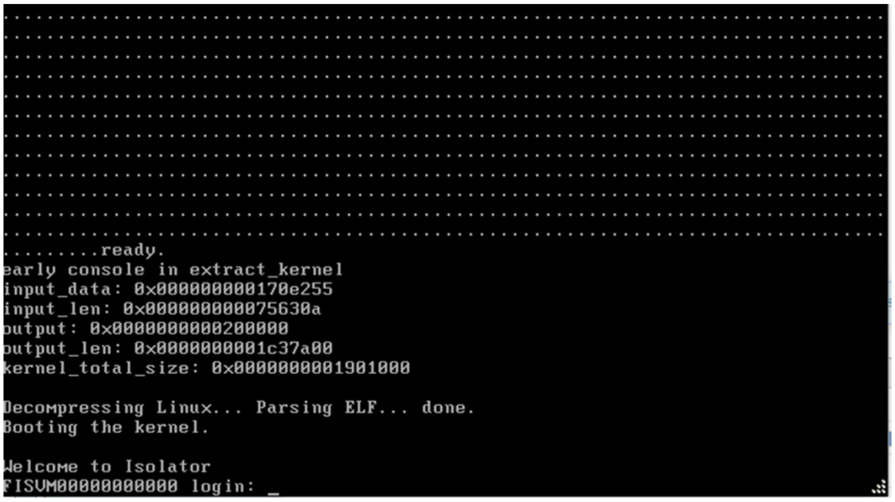
Review your settings selection before finishing the wizard

Product	FortiIsolator-VM
VM Name	FIS-VM-demo
Disks	fis.vmdk
Datastore	ManDisk
Provisioning type	Thin
Network mappings	Network 1: VM Network,Network 2: VM Network,Network 3: VM Network,Network 4: VM Network
Guest OS Name	Other Linux 2.6.x (32-bit)

Do not refresh your browser while this VM is being deployed.

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*.



```
...........................................................................................
...........................................................................................
...........................................................................................
...........................................................................................
...........................................................................................
...........................................................................................
...........................................................................................
...........................................................................................
...........................................................................................
...........................................................................................
...........................................................................................
...........................................................................................
.........ready.
early console in extract_kernel
input_data: 0x000000000170e255
input_len: 0x000000000075630a
output: 0x0000000000200000
output_len: 0x0000000001c37a00
kernel_total_size: 0x0000000001901000

Decompressing Linux... Parsing ELF... done.
Booting the kernel.

Welcome to Isolator
FISVM0000000000 login: _
```

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:

If you installed the FortiIsolator VM for Linux KVM using the script (see To install FortiIsolator VM for Linux KVM using a script: on page 8), skip steps 1-4 and proceed to step 5 as the configuration steps have already been completed by the script.

Configuring the host VM for registry

1. Run the following commands to 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>
   ```
2. Configure the host type to be registry by running `set host-type 2`.
3. Configure the database server by running `set database-server <registry ha-ip>`.
4. Configure the registry IP by running set `registry-vip <registry ha-ip> <port> <username> <password>`.
5. Configure portal IP by running `set portal-ip <central-mgmt-ip>`, where, `<central-mgmt-ip>` is the worker isolator management IP.

6. Configure the run mode by running `set run-mode 1`.
7. Reboot the machine.

Configuring the host VM for controller HA

1. Run the following commands to 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>
   set dns <primary dns> <secondary dns>
   ```
2. Configure the host type to be controller HA by running `set host-type 3`.
3. Configure the host role to be controller by running `set host-role controller`.
4. Configure the database server by running `set database-server <registry ha-ip>`.
5. Configure the run mode by running `set run-mode 1`.
6. Configure the system model to be VM by running `set system-model VM`.
7. Reboot the machine.
8. Repeat the steps above for each additional host VM for controller HA. You need at least three host VMs for controller HA.

Configuring the host VM for worker isolator

1. Run the following commands to 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>
   set dns <primary dns> <secondary dns>
   ```
2. Configure the host type to be worker by running `set host-type 0`.
3. Configure the host role to be worker isolator by running `set host-role worker_isolator`.
4. Configure the database server by running `set database-server <registry ha-ip>`.
5. Configure the run mode by running `set run-mode 1`.
6. Reboot the machine.

Configuring the host VM for worker controller

1. Run the following commands to 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>
   set dns <primary dns> <secondary dns>
   ```
2. Configure the host type to be worker by running `set host-type 0`.
3. Configure the host role to be worker controller by running `set host-role worker_controller`.
4. Configure the database server by running `set database-server <registry ha-ip>`.

5. Configure the run mode by running `set run-mode 1`.
6. Reboot the machine.

5. 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.

6. 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.

FORTINET®

www.fortinet.com