Flowmon Virtual Appliances

A virtual appliance is a pre-configured virtual machine image, ready to run on a hypervisor or in the cloud. Virtual appliances are intended to eliminate the installation, configuration and maintenance costs associated with running complex stacks of software in heterogeneous environments.

Flowmon Networks provide a number of virtual appliances intended to simplify the deployment of Flowmon in on-premise virtualization platforms and public cloud environments. The following guide provides

- a description of types of appliances available to partners and customers,
- a list of supported platforms and environments,
- a set of step by step manuals for deploying Flowmon appliances in aforementioned platforms and environments.

For additional assistance, please contact Flowmon Support.

Virtual Appliance Types

Flowmon Probe

The Flowmon Probe appliance provides the functionality of a Flowmon Probe without the built-in Flowmon Collector. It is optimized for deployment in supported platforms listed below.

This specialized appliance enables cost-effective network traffic monitoring and flow data export in deployments with multiple Flowmon Probe instances and at least one Flowmon Collector instance. An additional Flowmon Collector instance, virtual or hardware-based, is required for flow data collection and analysis.

For the list of available models, refer to the Flowmon Probe Models List document.

Flowmon Collector

The Flowmon Collector appliance provides the functionality of a Flowmon Collector with a built-in Flowmon Probe. It is optimized for deployment in supported platforms listed below.

This combination enables flow data collection and network traffic monitoring without the necessity for deploying additional appliances.

For the list of available models, refer to the Flowmon Collector Models List document.

Flowmon for VMware

Overview

Flowmon for VMware gives network administrators and security engineers insight into what is happening in their infrastructure. Its powerful features can be used to gain control of bandwidth utilization, optimize network and application performance, reduce time to resolution during troubleshooting and keep the infrastructure protected against modern cyber-security threats.

Flowmon for VMware is

- a virtual appliance intended for the VMware environment,
- capable of collecting as well as generating flow data,
- fully under customer's control - including updates, backups, and configuration.

Flowmon for VMware supports

- IPFIX, NetFlow v5/v9 or sFlow data collection from Flowmon Probes or other compatible devices (e.g., customer routers),
- ingestion of Amazon VPC Flow Logs from AWS,
- traffic monitoring on local vSwitches,
- traffic monitoring on local dedicated physical interfaces,
- 3rd-party packet brokers such as Garland Prisms, Ixia CloudLens, or Gigamon,
- ERSPAN/GRE traffic mirroring.

This guide describes the deployment procedure of Flowmon for VMware using an OVF template with a default storage capacity of 40 GB. The storage capacity can be later changed to match the purchased license.

Features

Flowmon for VMware supports three modes of operation

- Probe,
- Collector,
- Collector and Probe.

Flowmon Probe

In this mode, the virtual appliance acts as a Flowmon Probe. It accepts mirrored traffic on monitoring ports and exports flow data to at least one remote Flowmon Collector instance.

Supported traffic mirroring solutions:

- VMware vSwitch Monitoring
- VMware Distributed vSwitch Monitoring
- VMware Dedicated Port Monitoring

Supported 3rd-party packet brokers:

- Ixia CloudLens
- Gigamon
- Garland Prisms

Flowmon Collector

In this mode, the virtual appliance acts as a Flowmon Collector and accepts supported flow formats from external probes, network devices, or Amazon VPC Flow Logs on management ports. For details on supported flow sources and formats, refer to the official Flowmon User Guide.

Flowmon Collector and Flowmon Probe

In this mode, the virtual appliance acts both as a Flowmon Probe and Flowmon Collector. Probe sends data to the locally available Collector. For details on configuration, refer to the official Flowmon User Guide.

Licensing

Flowmon for VMware is a virtual appliance using the Bring-Your-Own-License (BYOL) licensing model.

With BYOL, you can apply for a Free Trial License at flowmon.com.

For support or inquiries, see our contact information.

Prerequisites

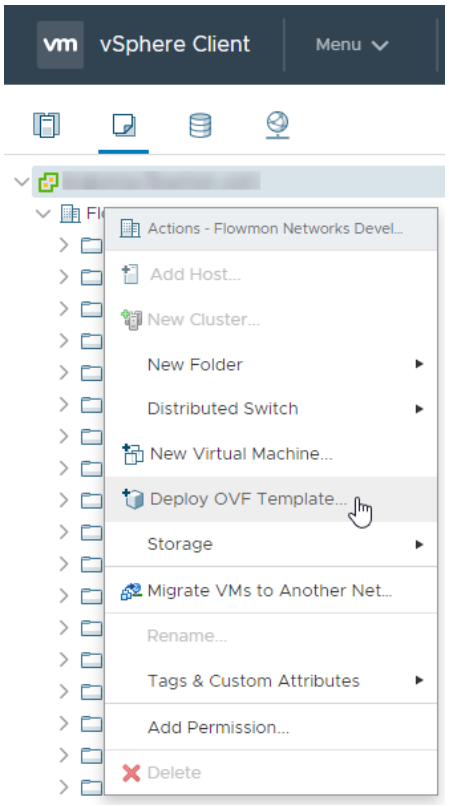
In order to follow this guide, you need the following:

1. VMware ESXi 5.5 or newer and VMware vSphere (demonstrated on vSphere v6.7).
2. Flowmon for VMware downloaded from the Partner Portal, archives for download are located in **Downloads / Products / Flowmon Virtual Appliances & Cloud / Flowmon for VMware**. Unless directed otherwise, pick the latest stable version with the desired set of modules.
3. A valid Flowmon license or a trial license from flowmon.com.

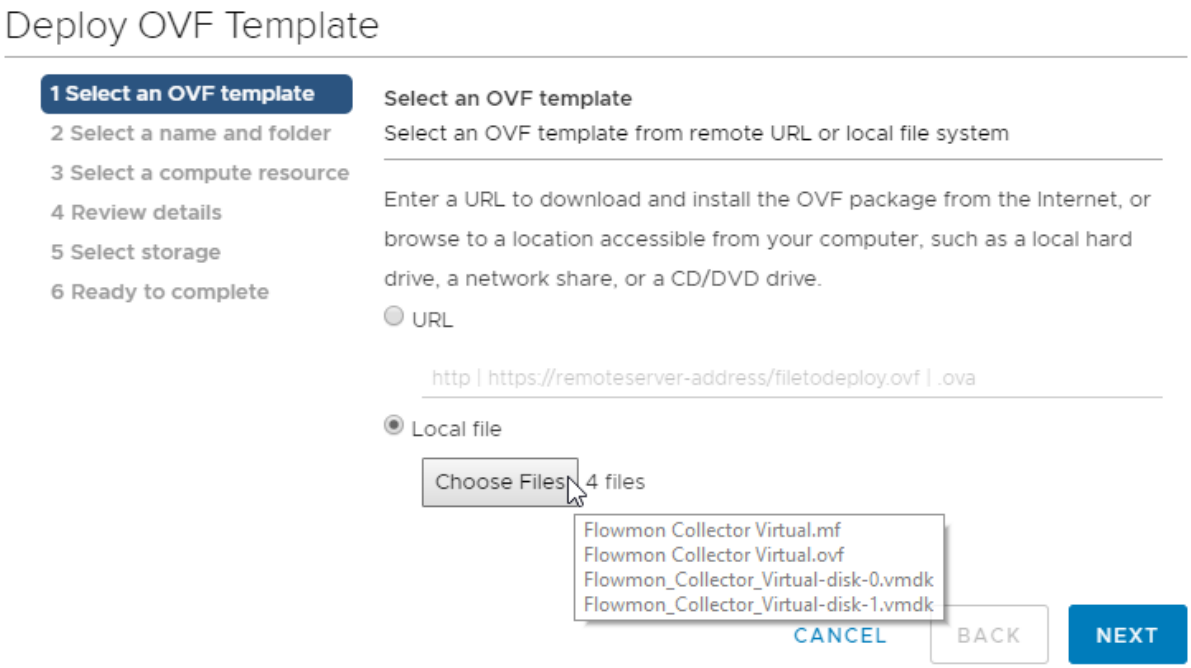
Deployment

The deployment of Flowmon for VMware consists of the following steps:

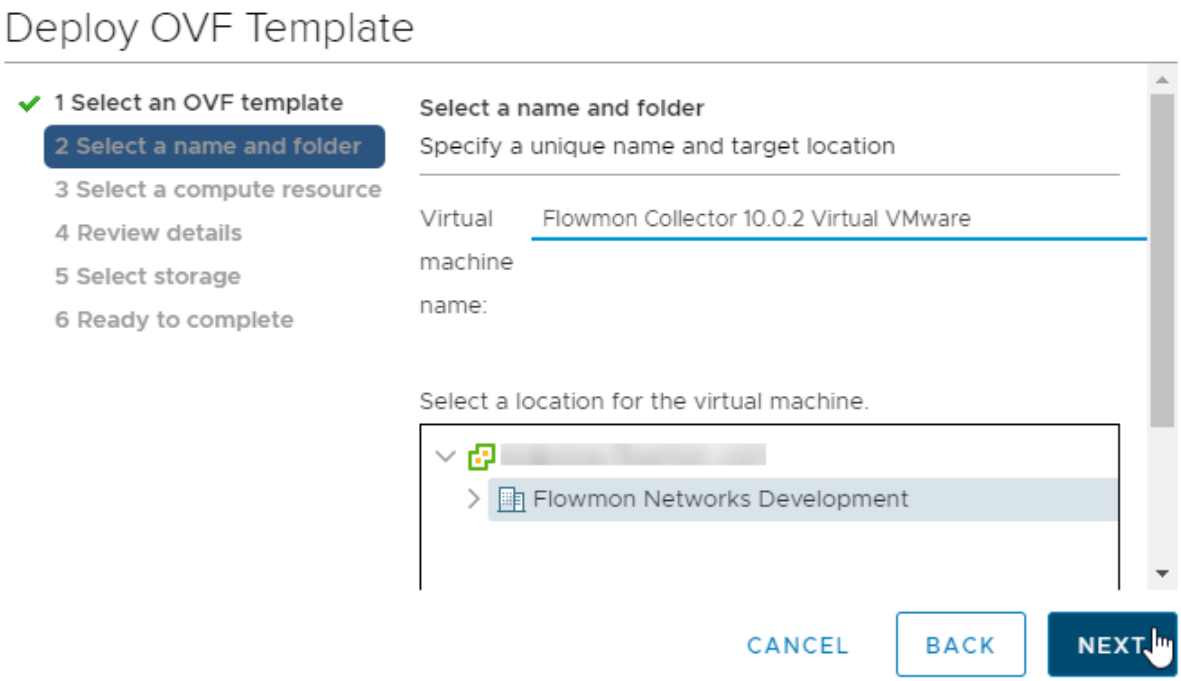
1. Decompress the downloaded zip file containing all the files necessary for installation.
2. In your vSphere Client in the **VMs and Templates** tab, right click on your **Datacenter** and click on **Deploy OVF Template**.



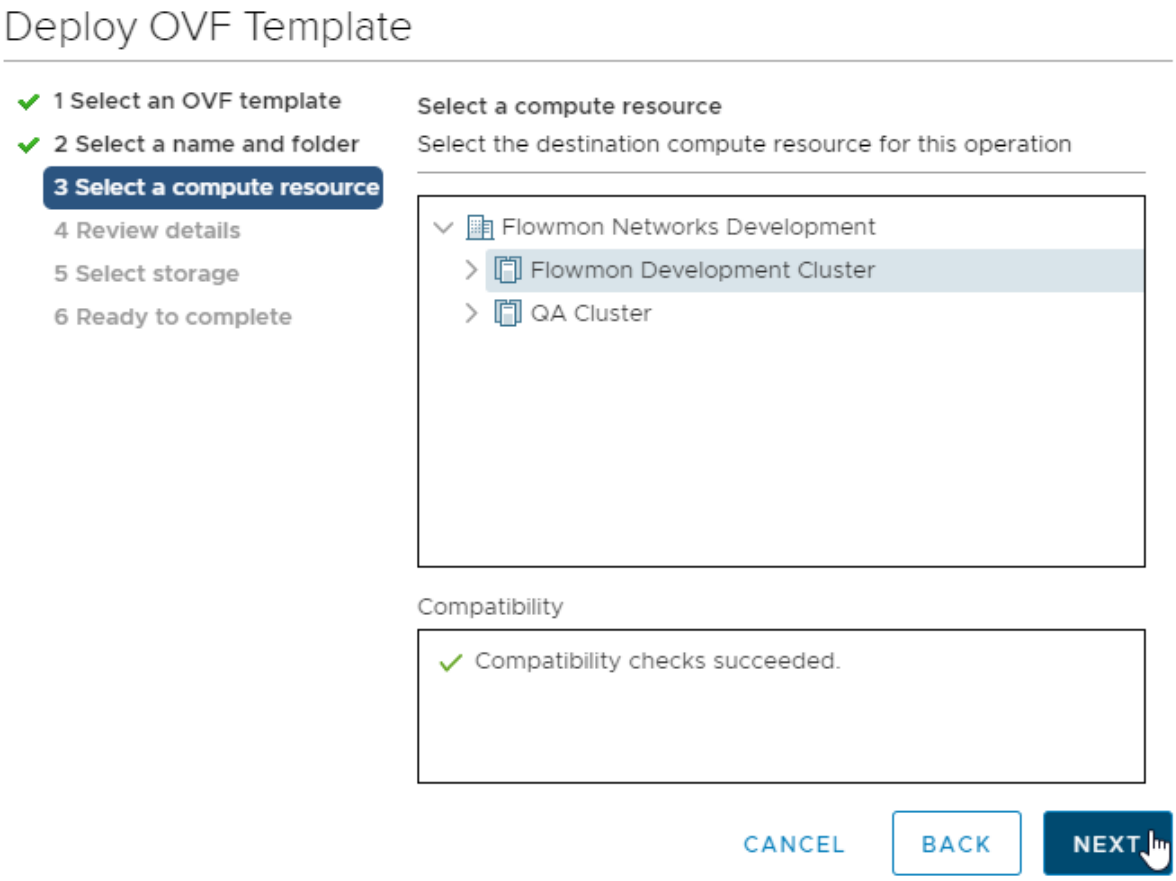
3. Select all the files from the downloaded and decompressed zip archive, **.mk**, **.ovf** and **.vmdk**, and click on the **Next** button.



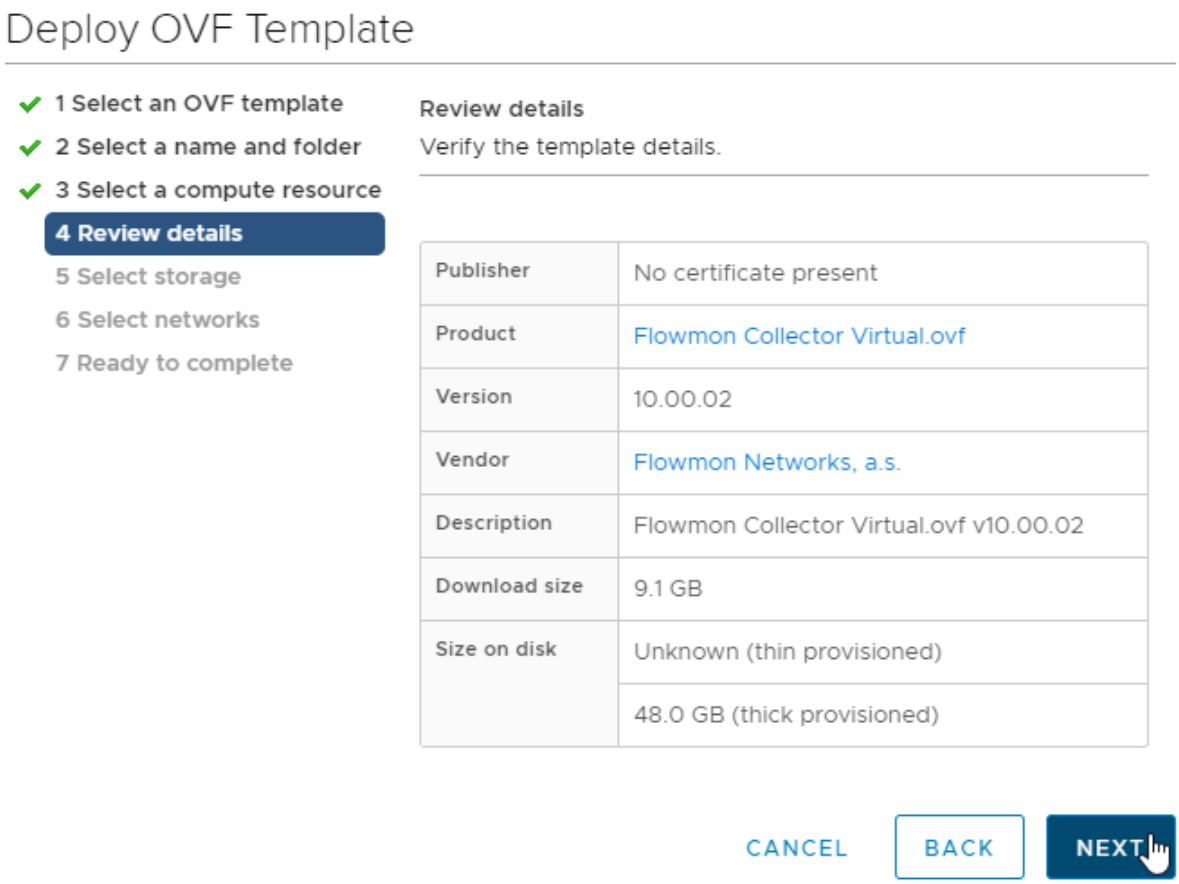
4. Enter a **Virtual machine name** and select a **Location** for your new virtual appliance and click on the **Next** button.



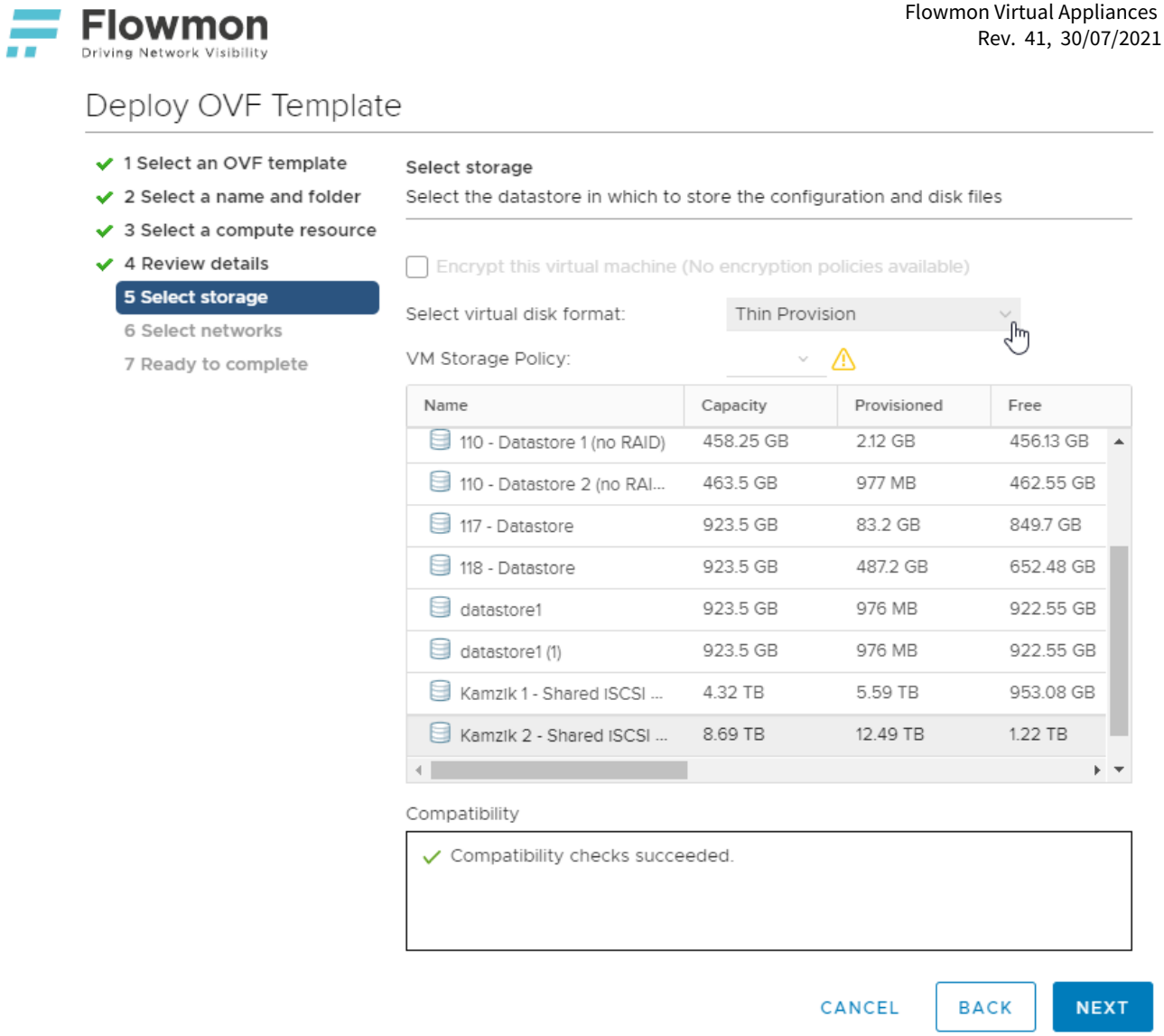
5. **Select a compute resource** and click on the **Next** button.



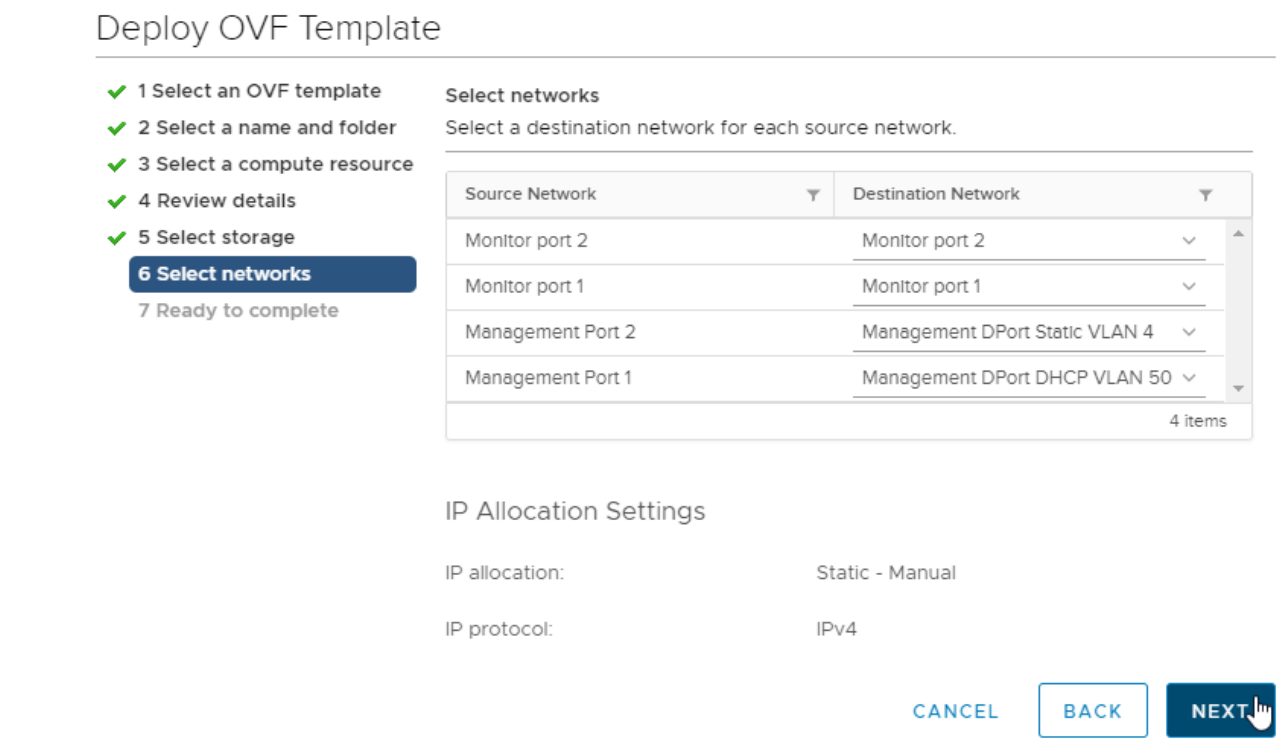
6. **Review details** and click on the **Next** button.



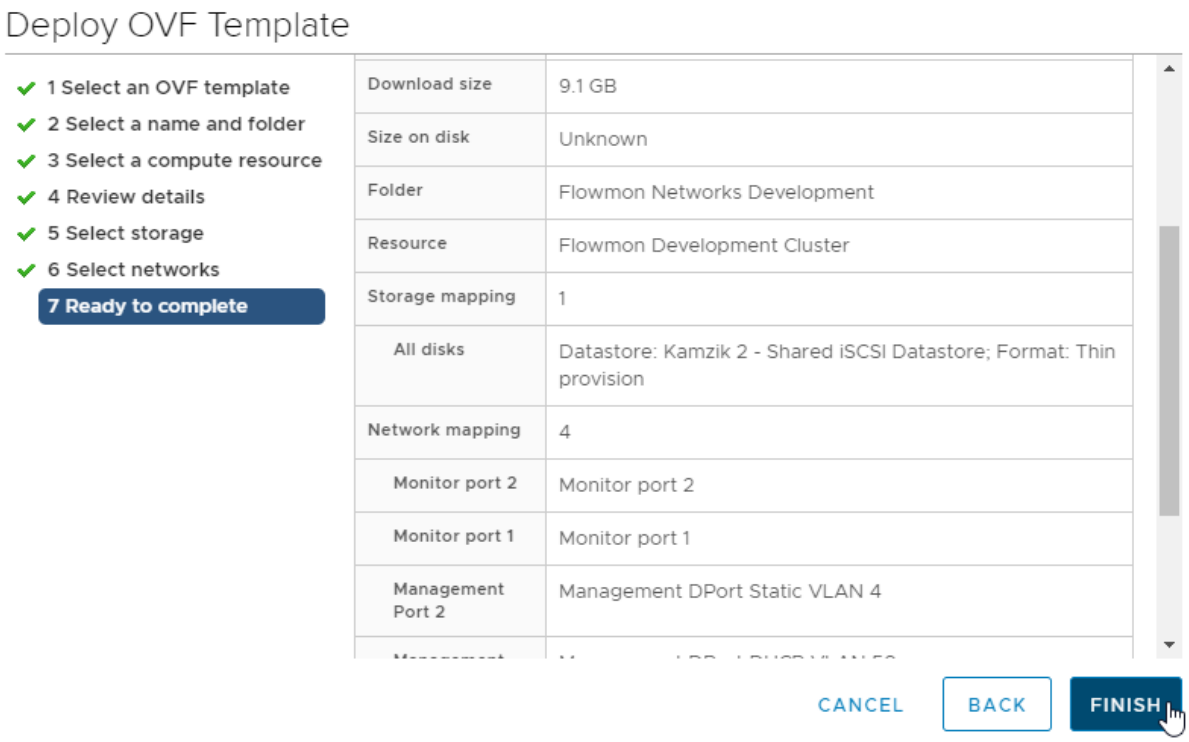
7. **Select storage** in which you want to store the configuration and disk files. After that, select **Thin provisioning** or **Thick provisioning** according to your preferences and click on the **Next** button.



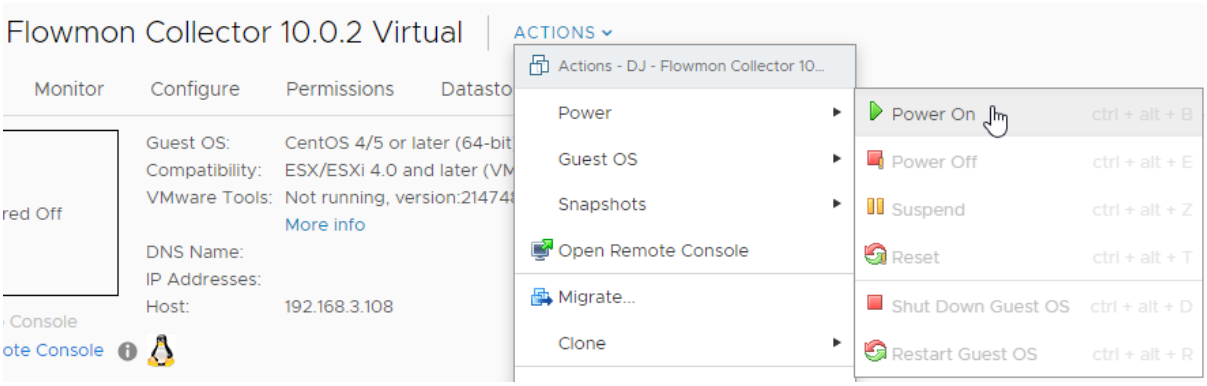
8. **Select networks** to be used by the virtual appliance. **Management ports** are used for access to the web interface. Connect them to your LAN. Then click on the **Next** button.



9. Review all the information and click on the **Finish** button to start the deployment process. It may take several minutes.



10. Find the newly created Flowmon virtual appliance and click on **Power On** in the **Actions / Power** menu. Wait for the appliance to start.

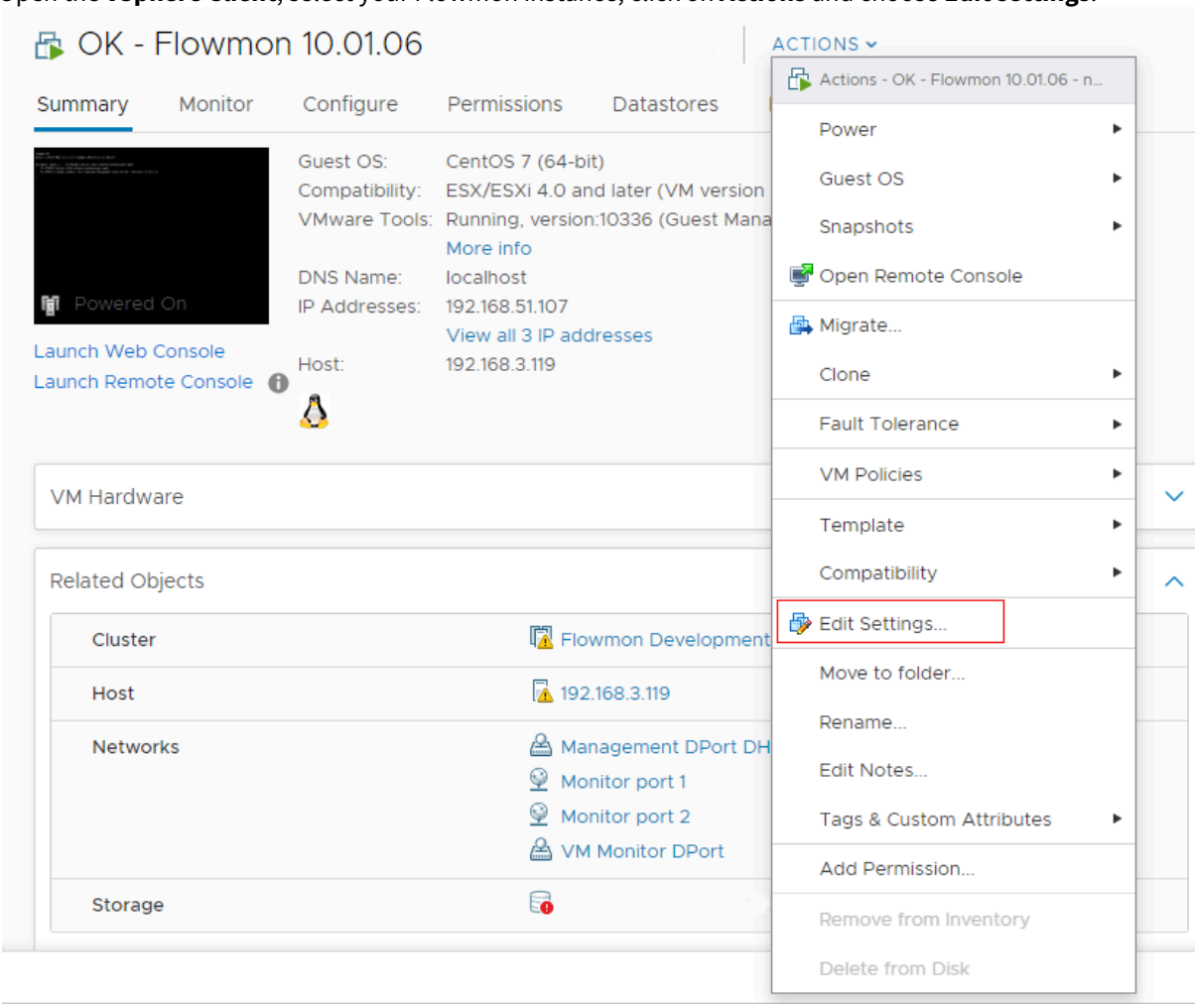


Virtual Disks

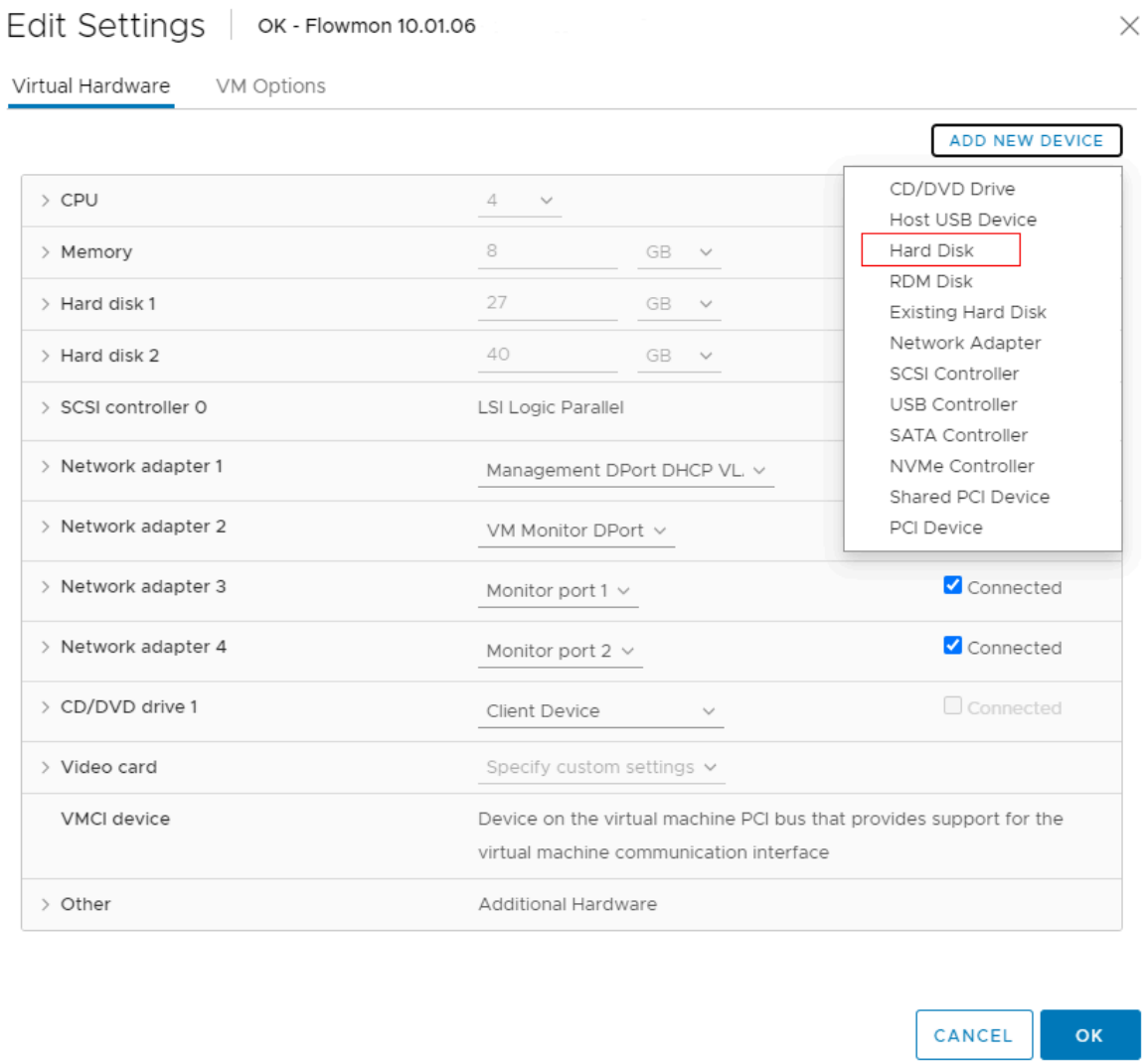
Once the new instance is running, you may provision additional data storage. After attaching an additional disk following this guide, refer to Post-installation Steps / Data Storage to activate it.

To attach an additional/replacement disk for data, you have to:

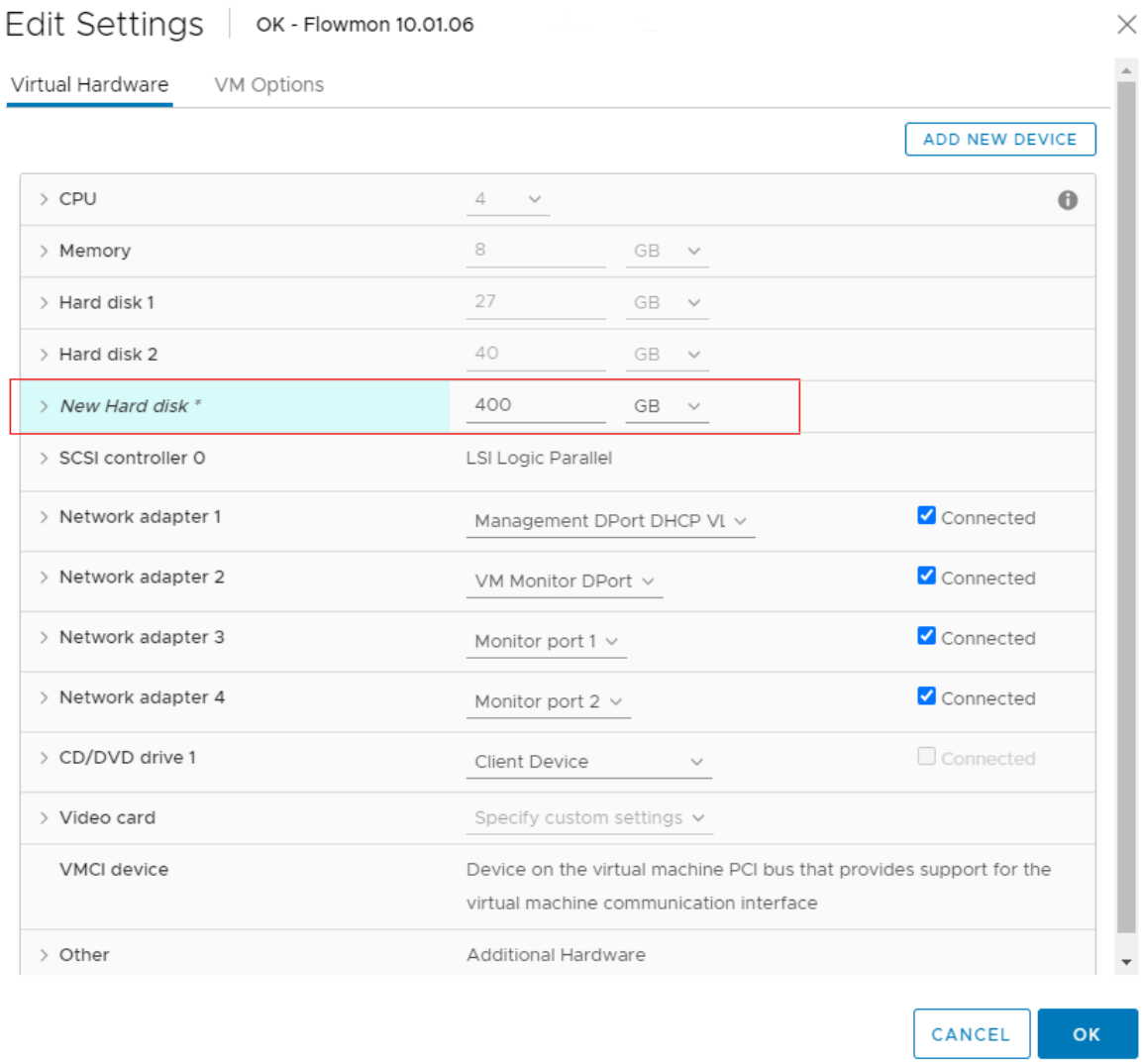
1. Open the **vSphere Client**, select your Flowmon instance, click on **Actions** and choose **Edit settings**.



2. Click on the **Add New Device** button to add a new **Hard Disk**.



3. Set disk size.



4. Check settings, click on the **OK** button.

Flowmon Configuration

Please refer to Post-installation Steps.

VMware Dedicated Port Monitoring

Overview

Flowmon for VMware has the ability to monitor traffic and generate NetFlow / IPFIX flow data. To enable this functionality for the monitoring of an external source connected to a physical port of the VMware host, please follow the steps outlined below.

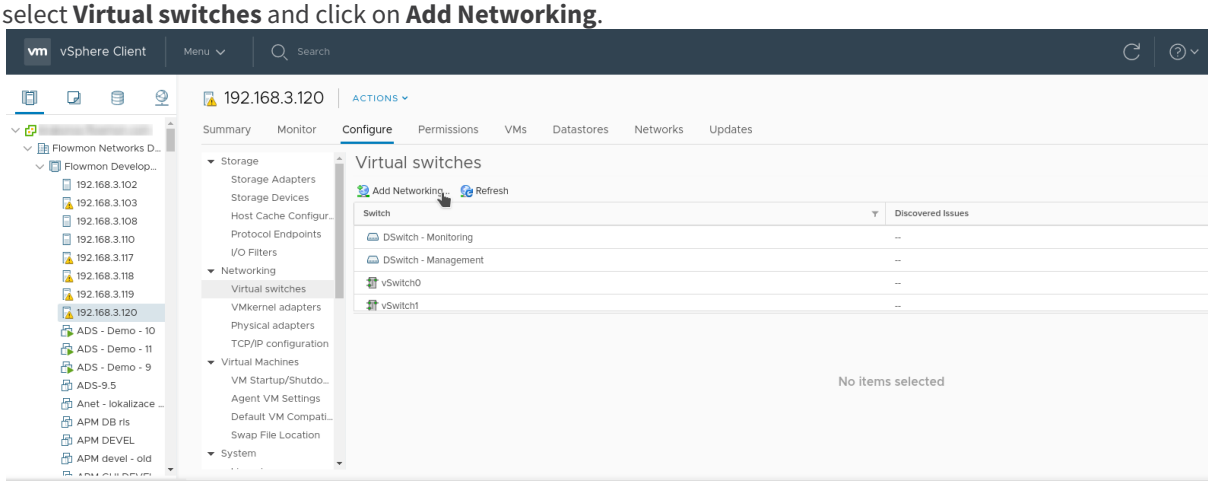
Prerequisites

- A running instance of Flowmon for VMware - Flowmon Collector (with a built-in Probe) or Flowmon Probe.
- An external source of network traffic connected to a physical network interface of the VMware host.

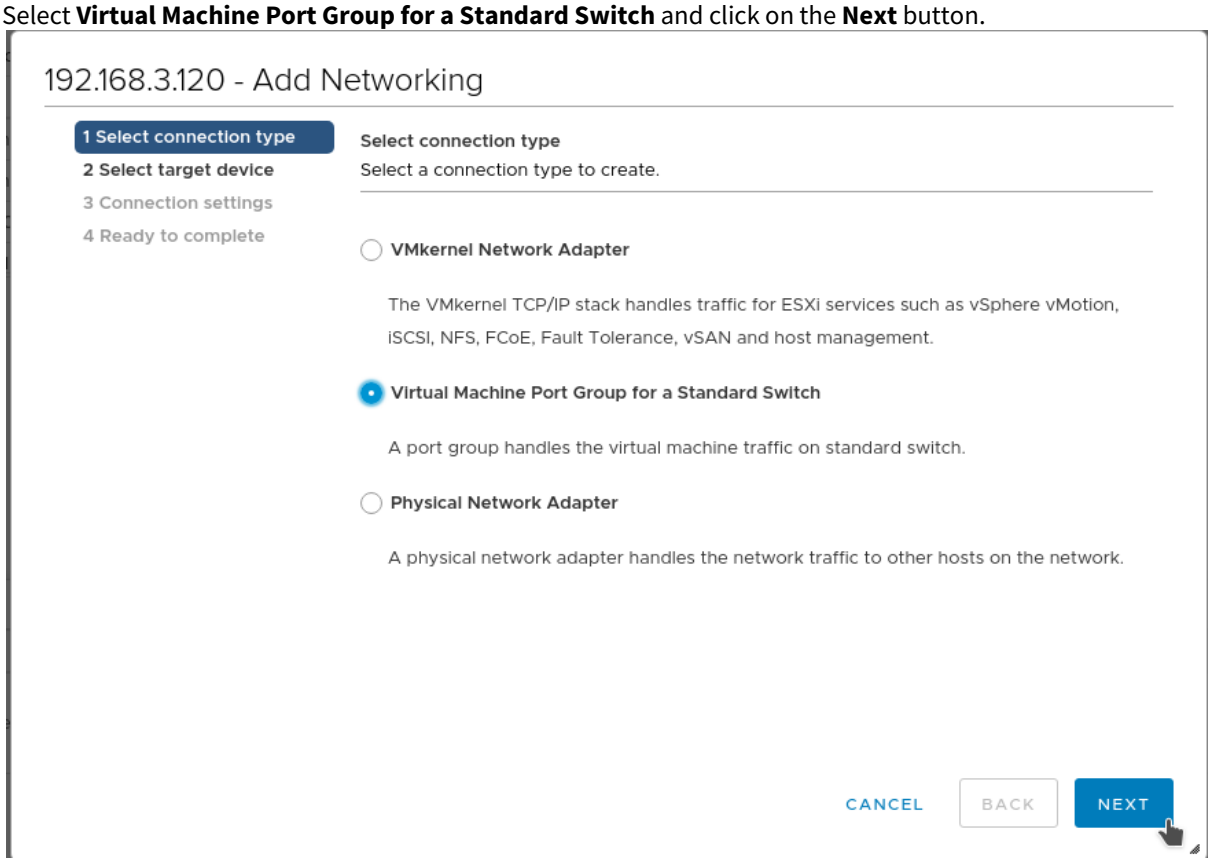
Deployment

Setting up dedicated port monitoring is done by assigning a specific physical interface to a virtual switch and connecting Flowmon's monitoring interface to the same virtual switch.

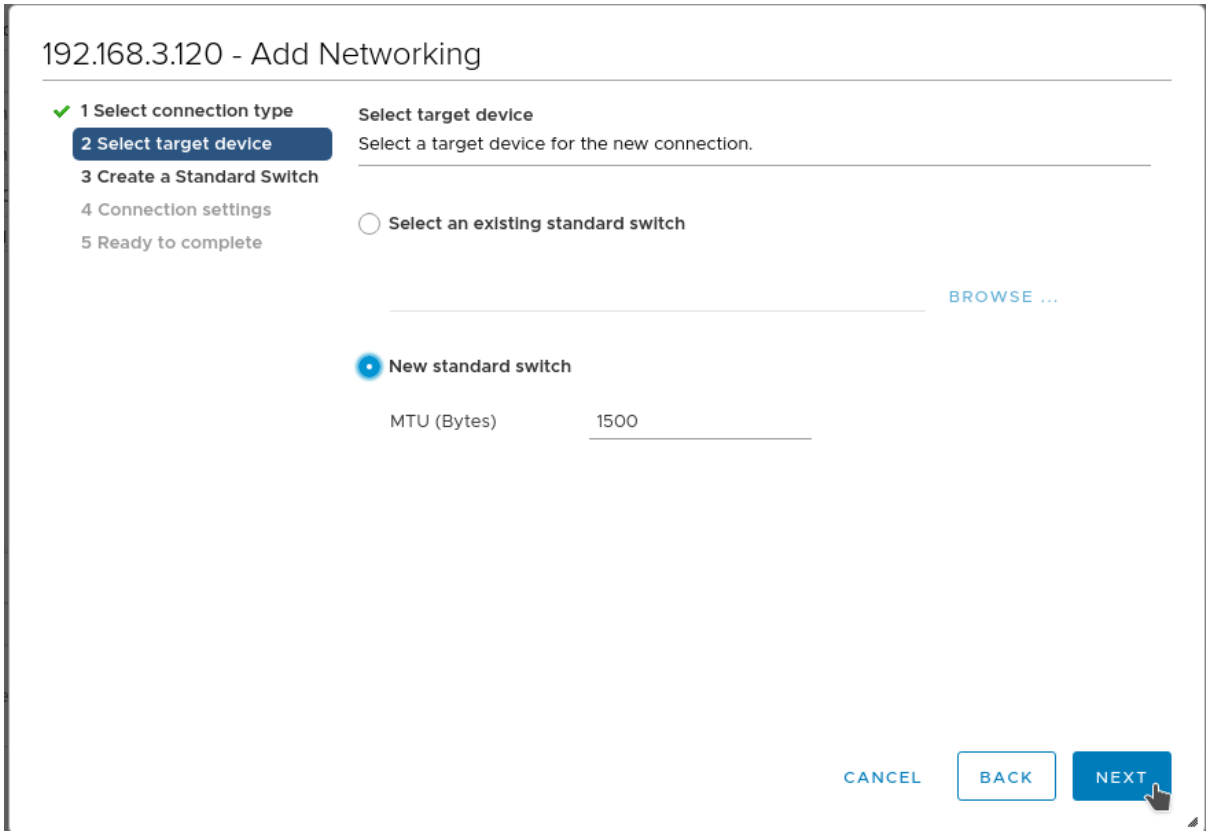
1. In the vSphere client, click on the IP address of a VMware host. Then click on the **Configure** tab, select **Virtual switches** and click on **Add Networking**.



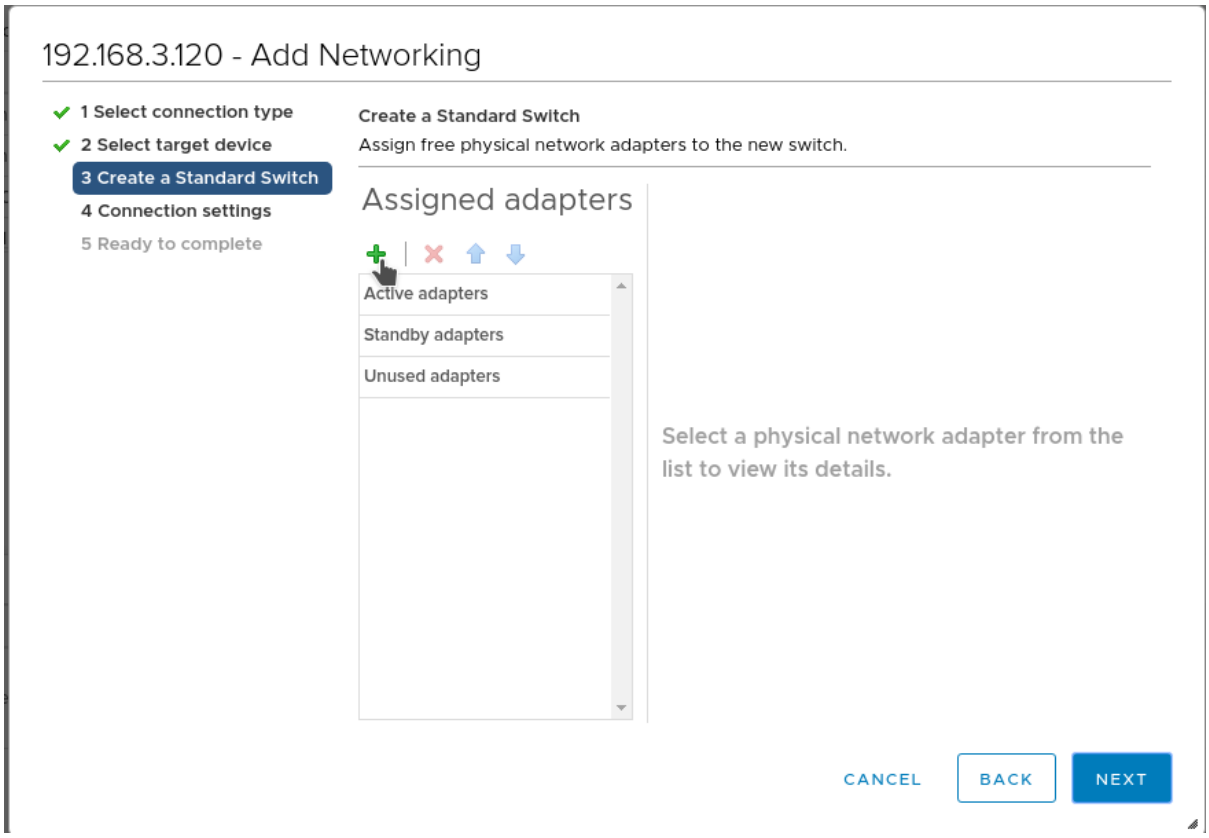
2. Select **Virtual Machine Port Group for a Standard Switch** and click on the **Next** button.



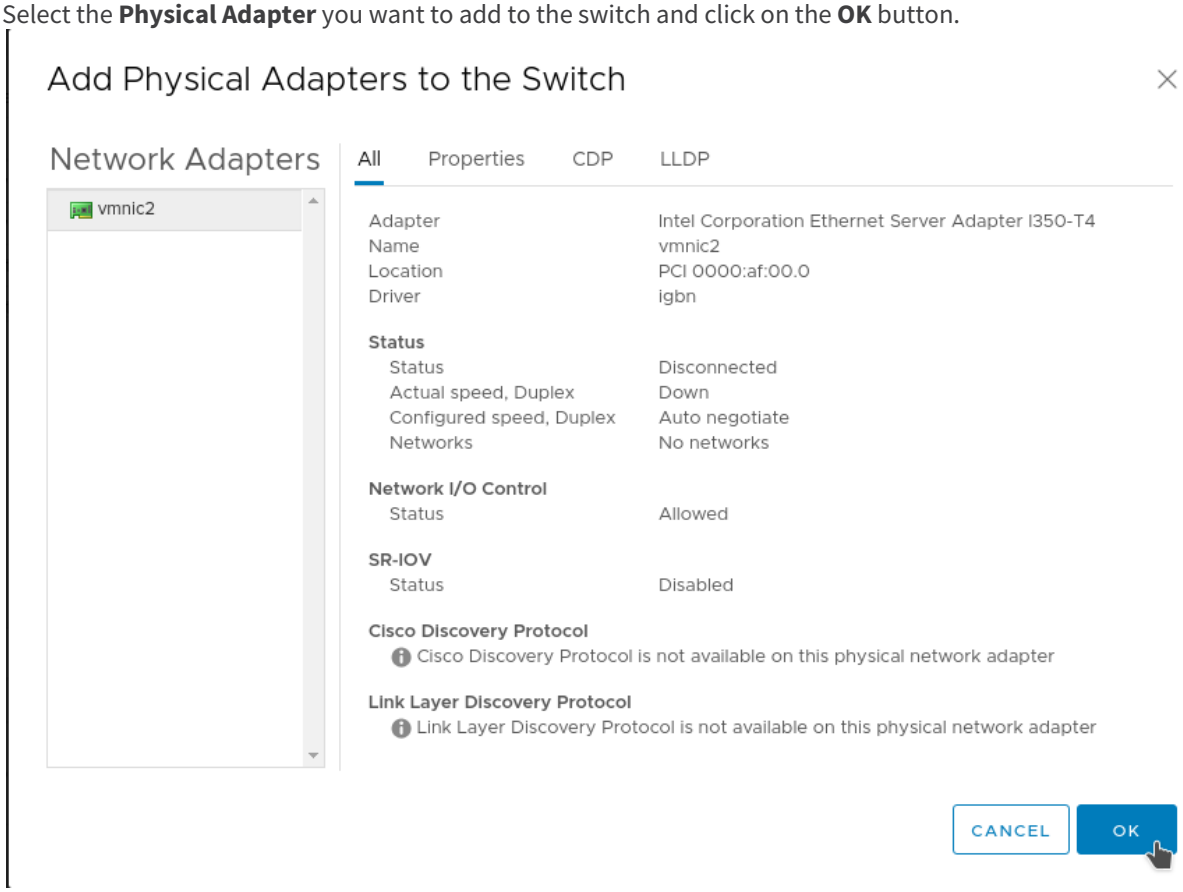
3. Select **New standard switch** and click on the **Next** button.



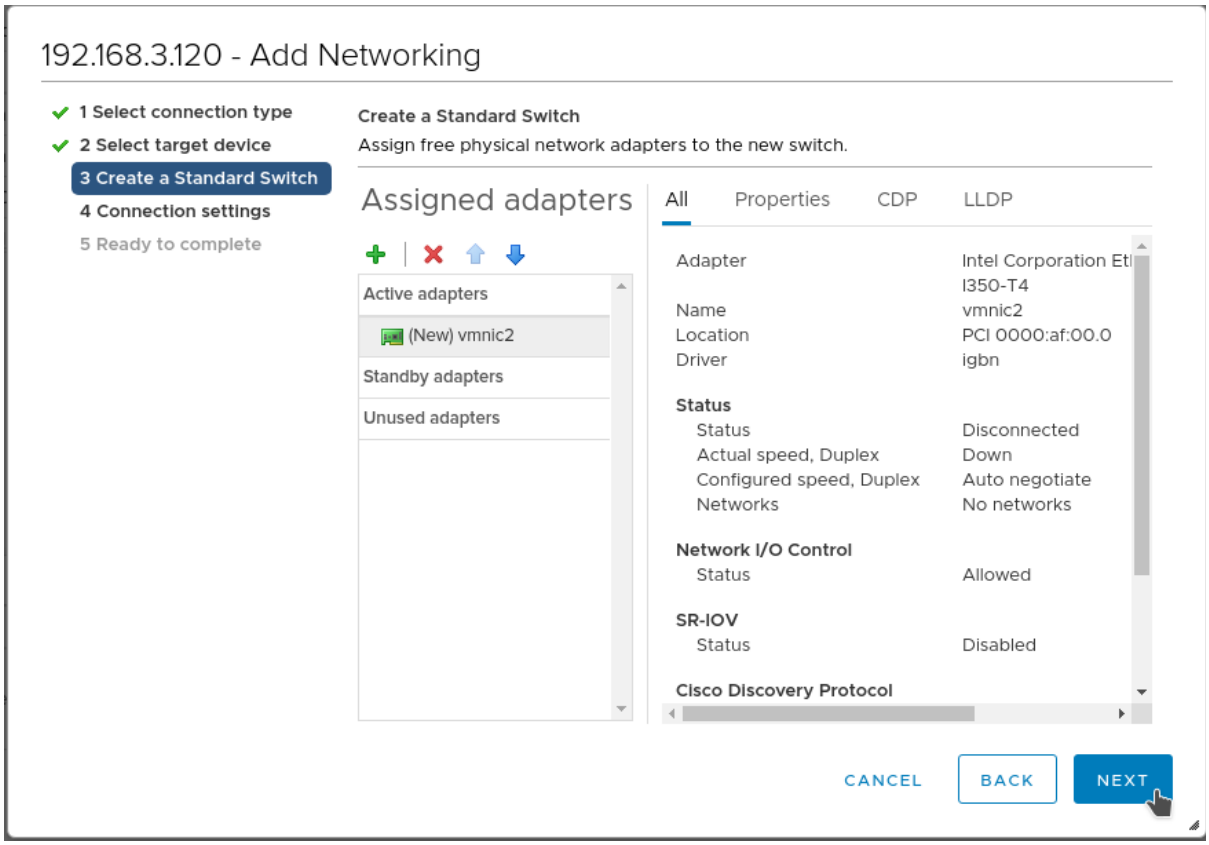
4. Click on the **Plus** button.



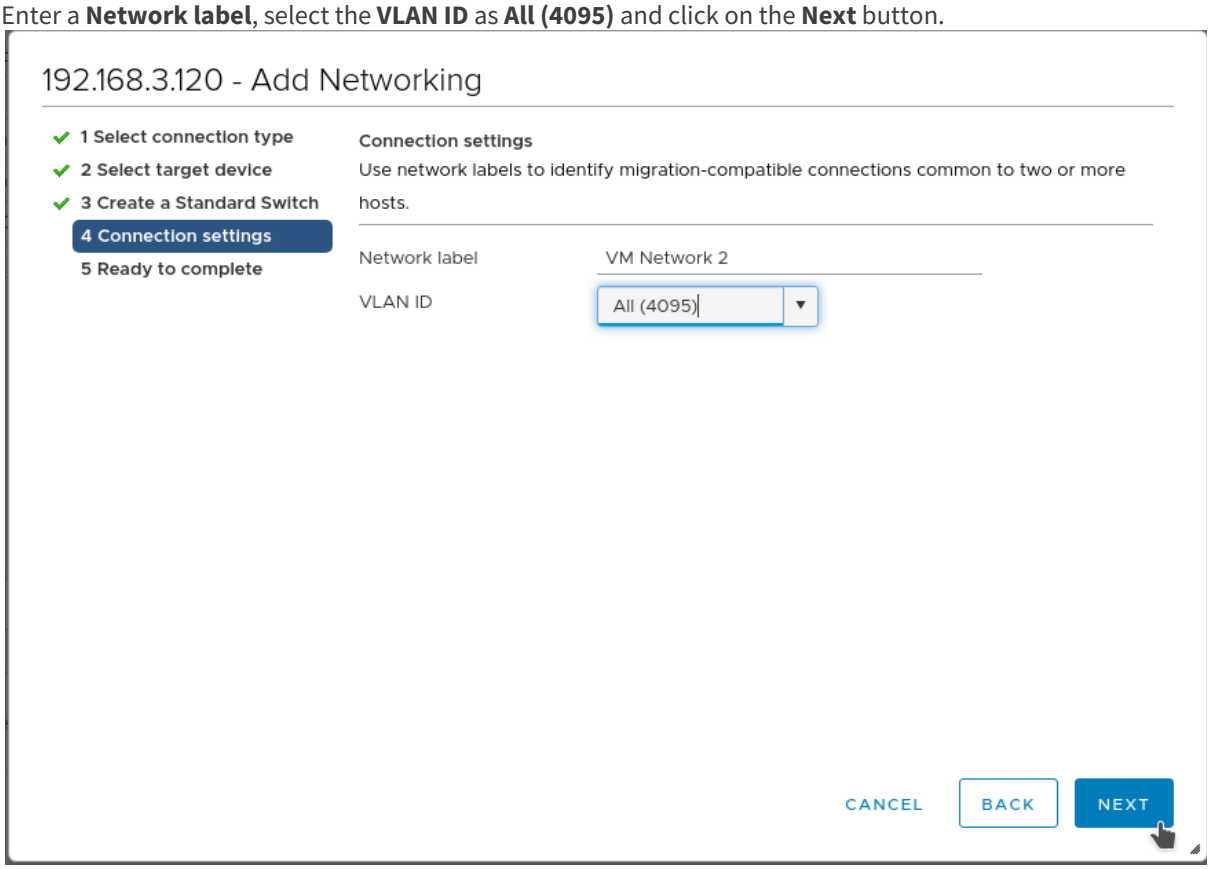
5. Select the **Physical Adapter** you want to add to the switch and click on the **OK** button.



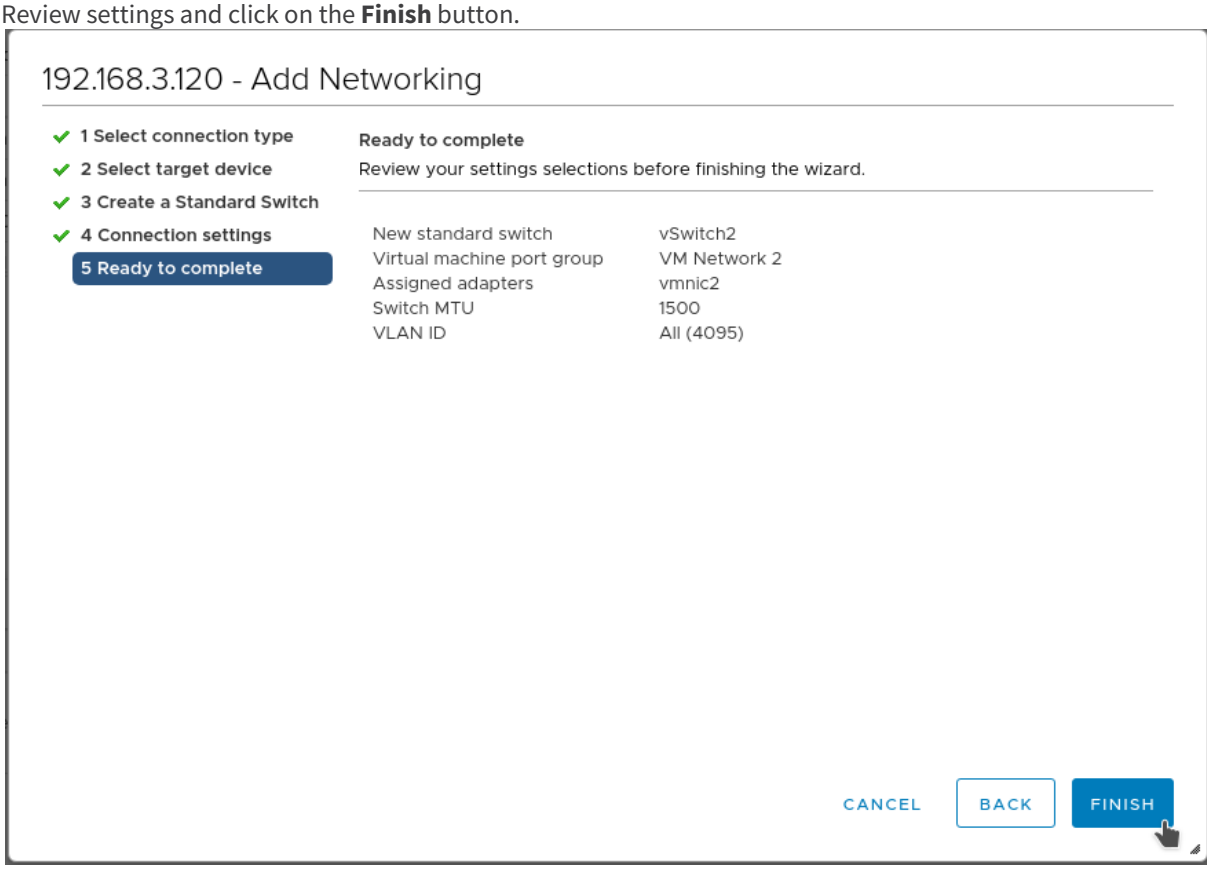
6. Click on the **Next** button.



7. Enter a **Network label**, select the **VLAN ID** as **All (4095)** and click on the **Next** button.



8. Review settings and click on the **Finish** button.



9. Now continue with VMware vSwitch Monitoring and connect Flowmon's monitoring interface to the same virtual switch to complete the configuration.

Flowmon Configuration

No configuration specific for VMware dedicated port monitoring is necessary. See instructions on how to enable a monitoring port in the Flowmon User Guide.

VMware vSwitch Monitoring

Overview

Flowmon for VMware has the ability to monitor traffic and generate NetFlow / IPFIX flow data. To enable this functionality for the monitoring of a VMware vSwitch local to the VMware host where Flowmon is running, please follow the steps outlined below.

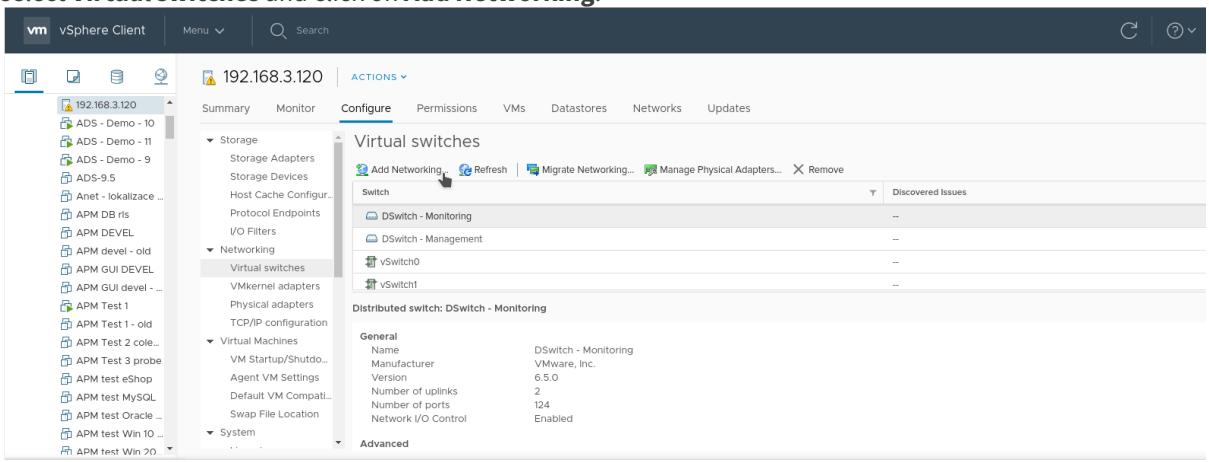
Prerequisites

- A running instance of Flowmon for VMware - Flowmon Collector (with a built-in Probe) or Flowmon Probe.

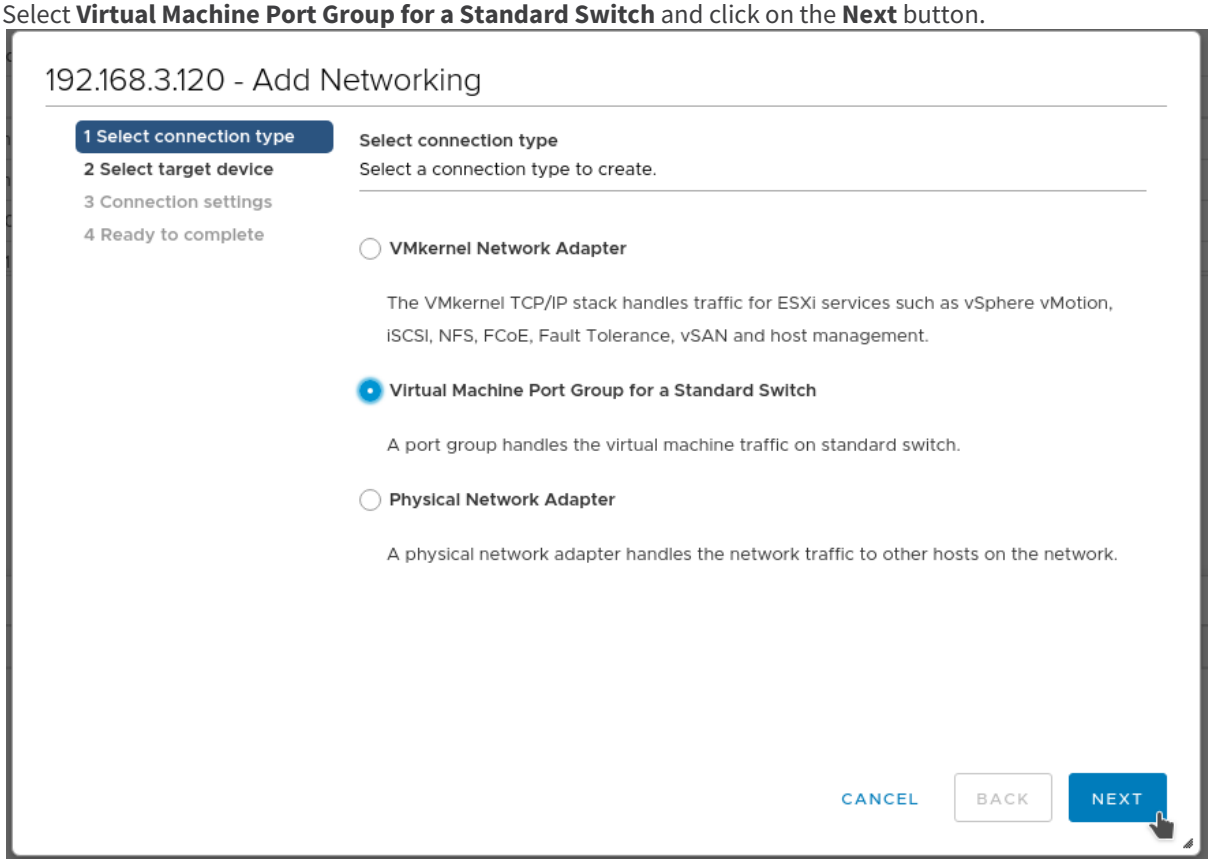
Deployment

Setting up vSwitch monitoring is done by creating a new port group and configuring it to use the promiscuous mode.

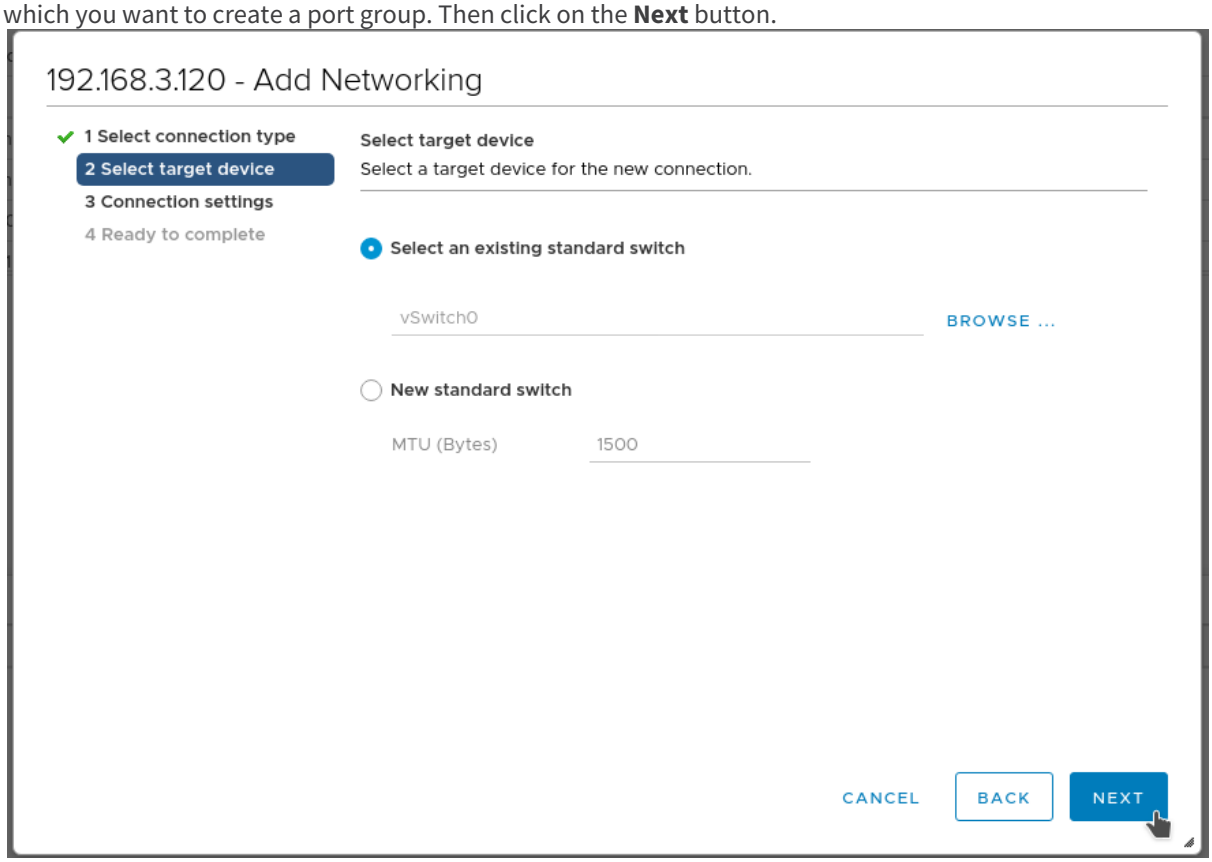
1. In the vSphere client, click on the IP address of a VMware host. Then click on the **Configure** tab, select **Virtual switches** and click on **Add Networking**.



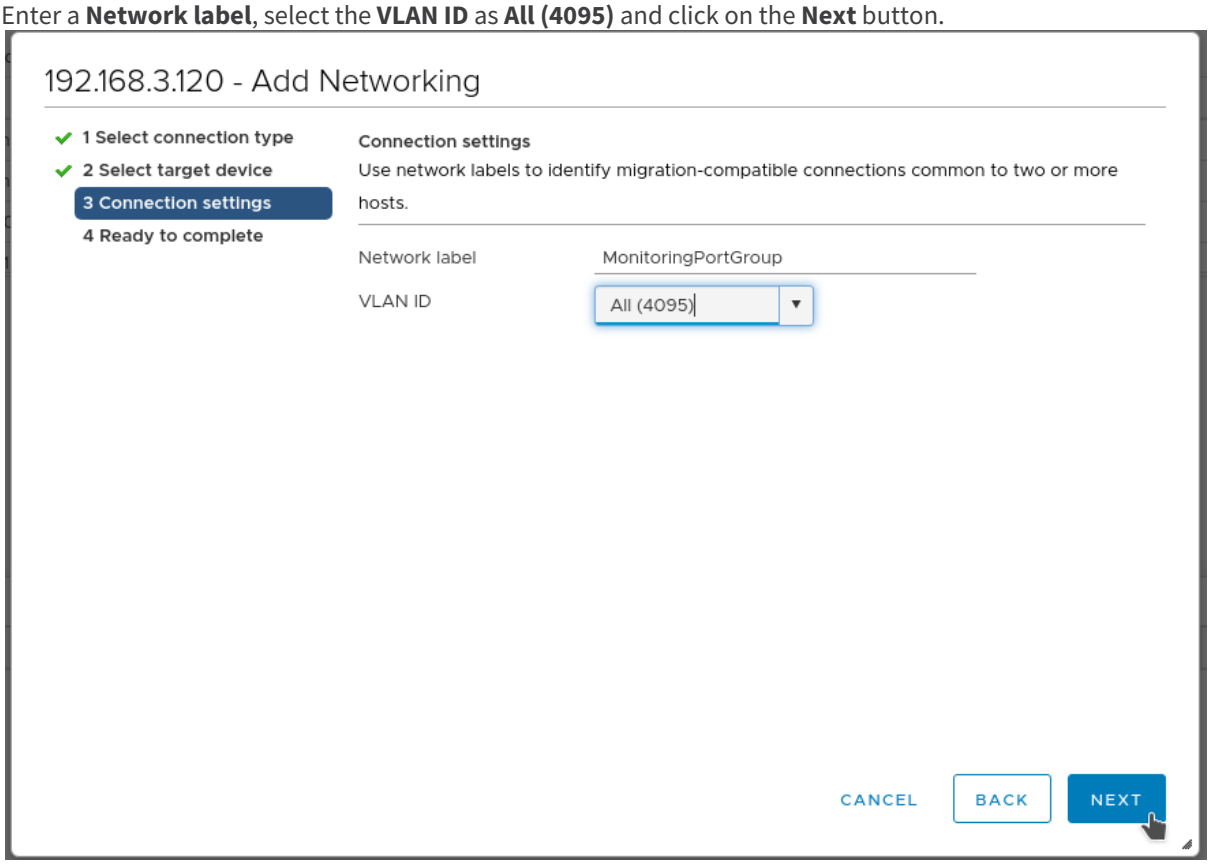
2. Select **Virtual Machine Port Group for a Standard Switch** and click on the **Next** button.



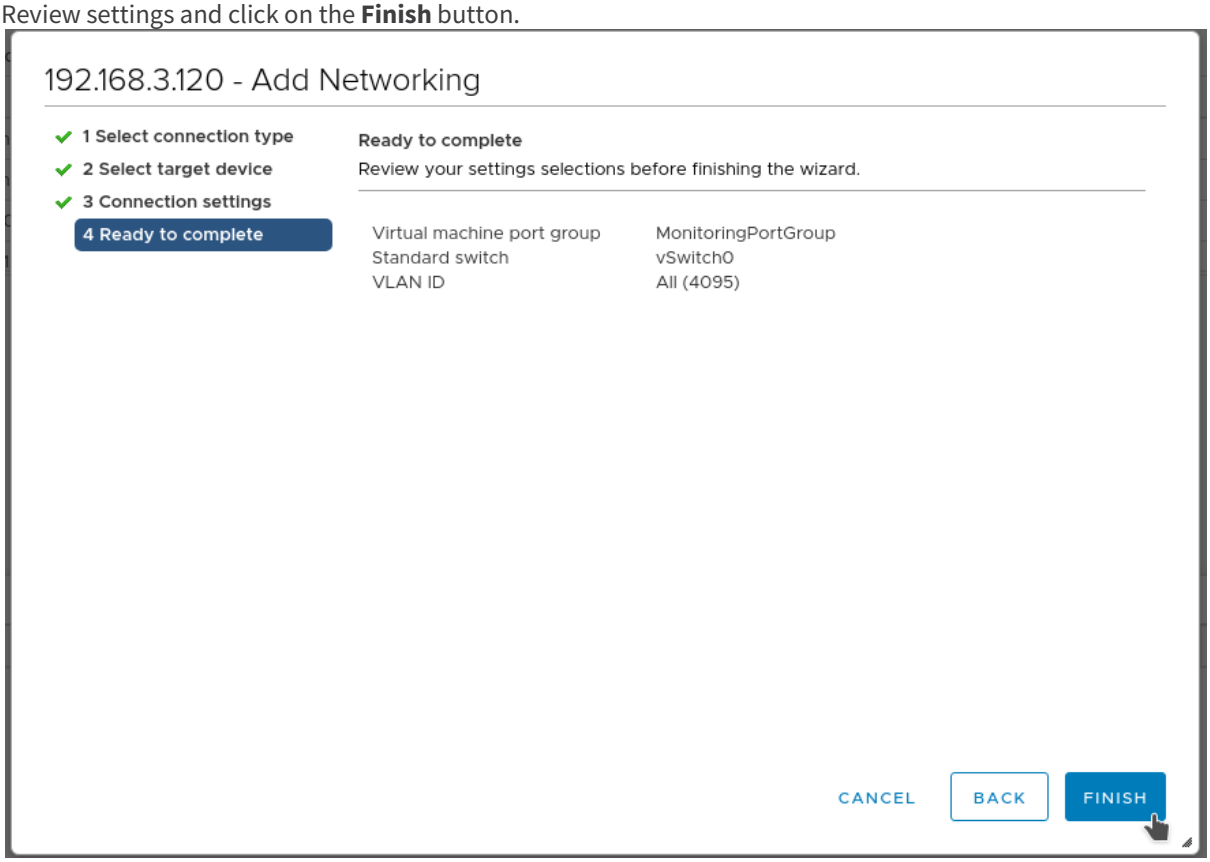
3. Click on the **Select an existing standard switch** option and browse the existing switches. Select the one for which you want to create a port group. Then click on the **Next** button.



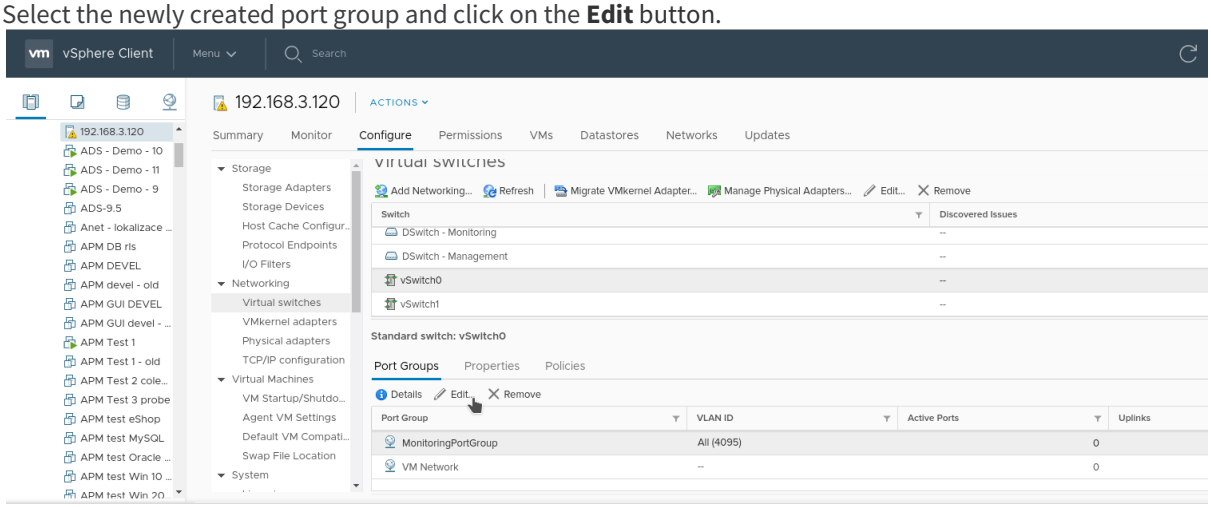
4. Enter a **Network label**, select the **VLAN ID** as **All (4095)** and click on the **Next** button.



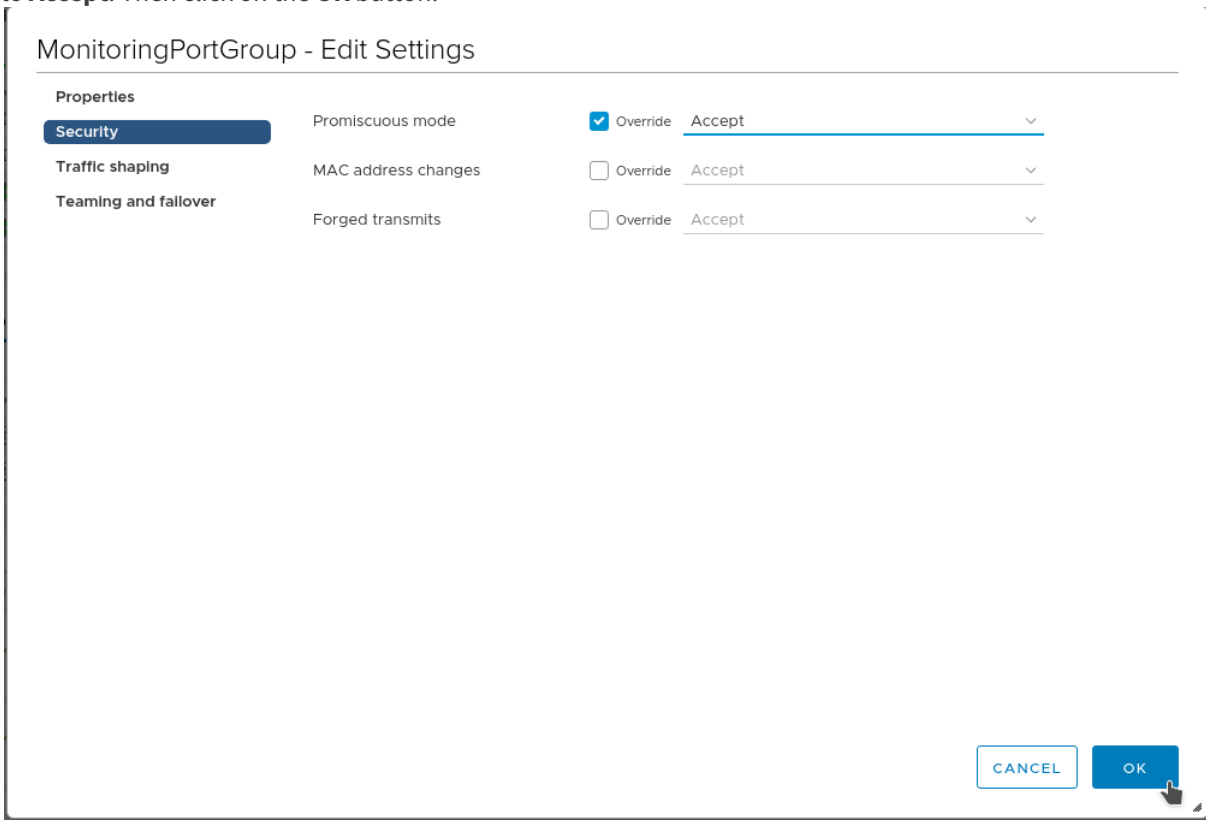
5. Review settings and click on the **Finish** button.



6. Select the newly created port group and click on the **Edit** button.



7. Go to the **Security** tab and check the **Override** checkbox next to **Promiscuous mode** and set the value to **Accept**. Then click on the **OK** button.



Flowmon Configuration

No configuration specific for VMware vSwitch monitoring is necessary. See instructions on how to enable a monitoring port in the Flowmon User Guide.

VMware Distributed vSwitch Monitoring

Overview

Flowmon for VMware has the ability to monitor traffic and generate NetFlow / IPFIX flow data. To enable this functionality for the monitoring of a VMware Distributed vSwitch (DSwitch), please follow the steps outlined below.

Network traffic from a virtual machine is monitored by a Flowmon instance running on the same host. This concept requires a Flowmon instance deployed on each physical host where monitored virtual machines could potentially run.

Prerequisites

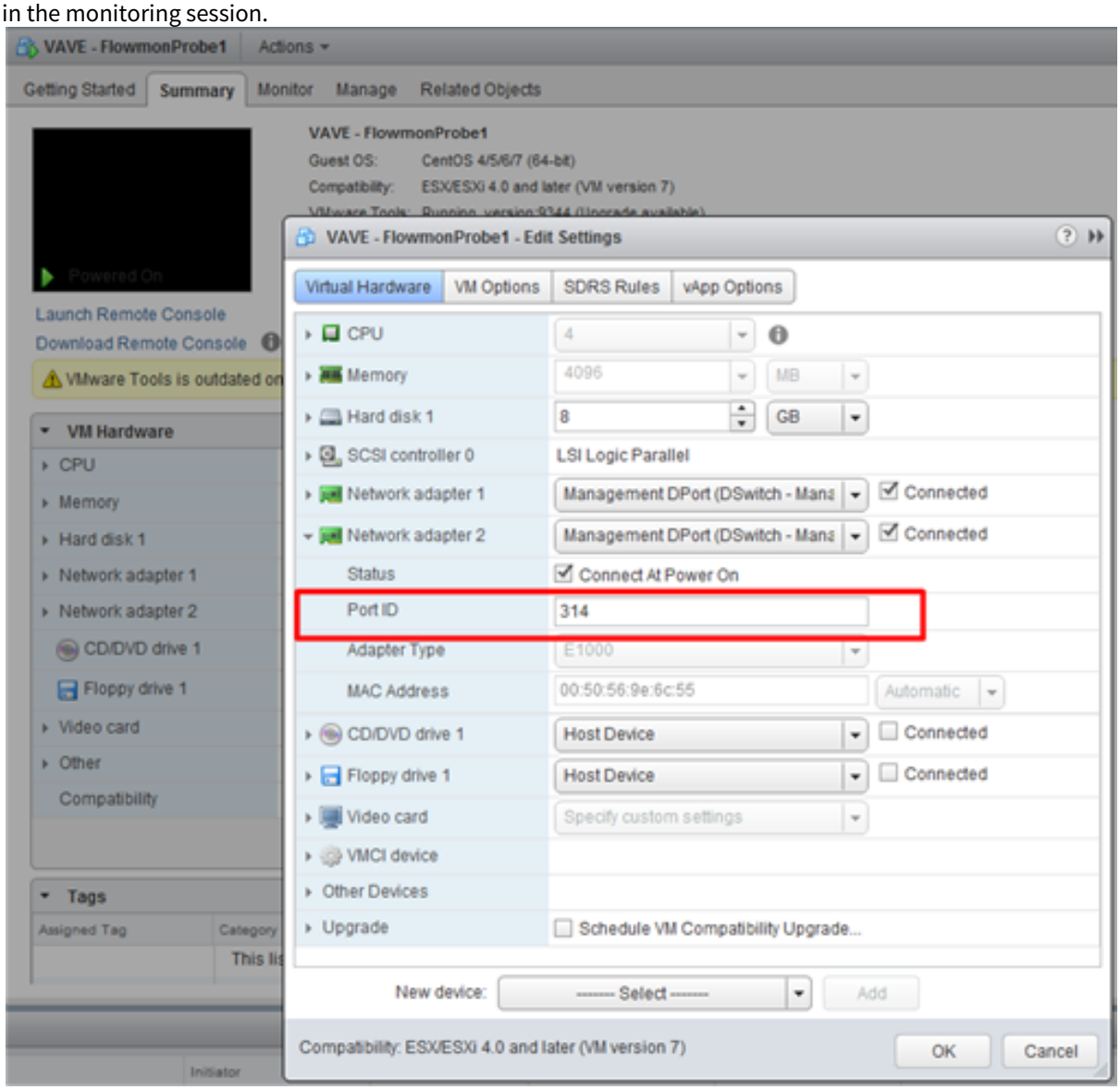
- A running instance of Flowmon for VMware - Flowmon Collector (with a built-in Probe) or Flowmon Probe.

Deployment

In order to monitor a DSwitch, distributed port mirroring needs to be configured. Flowmon for VMware has to be deployed on each VMware host (ESXi server) and connected to the DSwitch you wish to monitor.

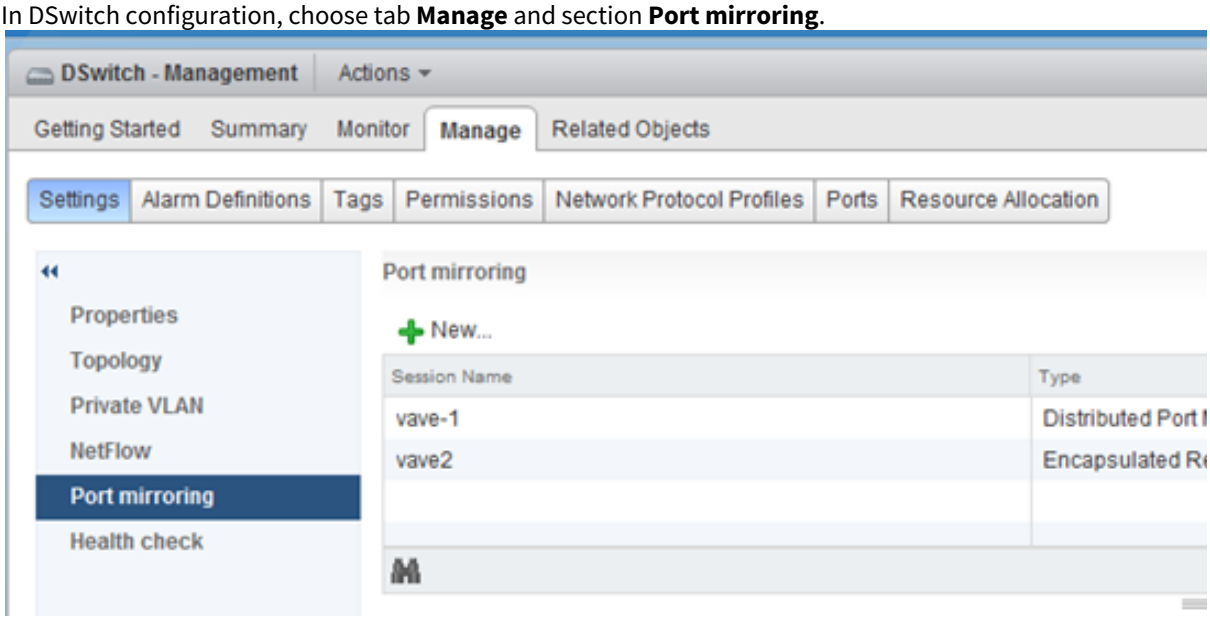
1. **Port ID**s of all Flowmon monitoring ports need to be collected. Port IDs can be found in **Edit settings** – **Network adapter** settings. For an appliance with one monitoring port, check the port ID of **Network adapter 2**. For appliances with more monitoring ports, check port IDs of for **Network adapters from 3 to *x*** (*x* equals 4, 6, 8 depending on the number of monitoring ports – 2, 4, 6). Port IDs will be used as destinations

in the monitoring session.

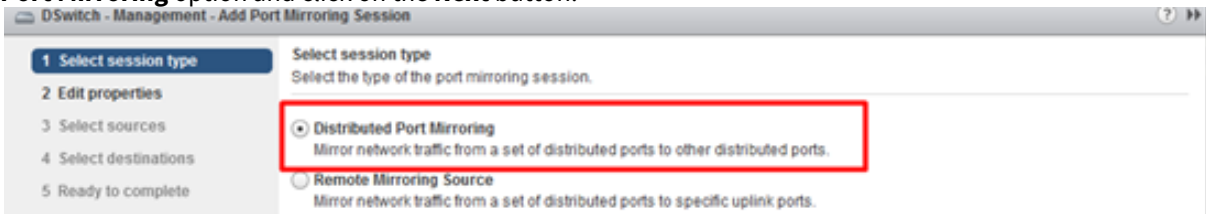


2. Using the same procedure, collect **Port ID**s of virtual machines that should be monitored. These Port IDs will be used as sources in the monitoring session.

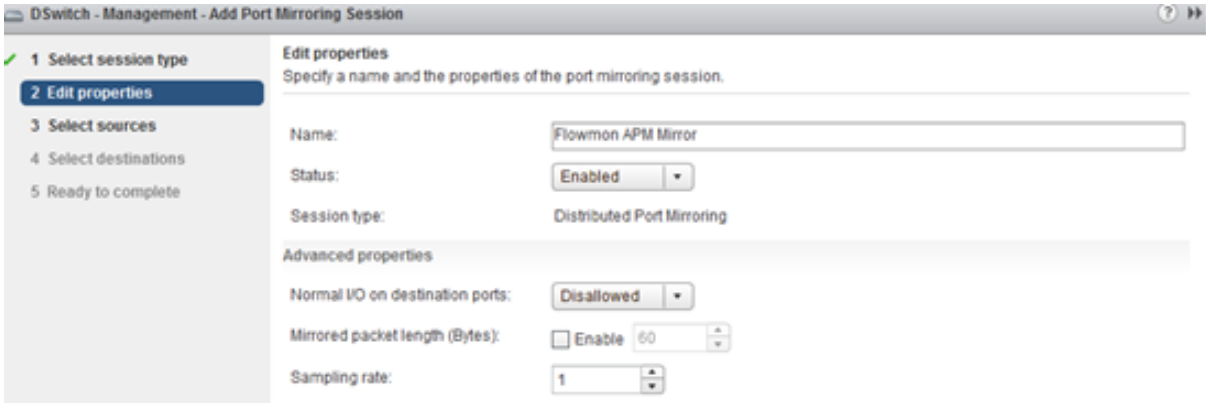
3. In DSwitch configuration, choose tab **Manage** and section **Port mirroring**.



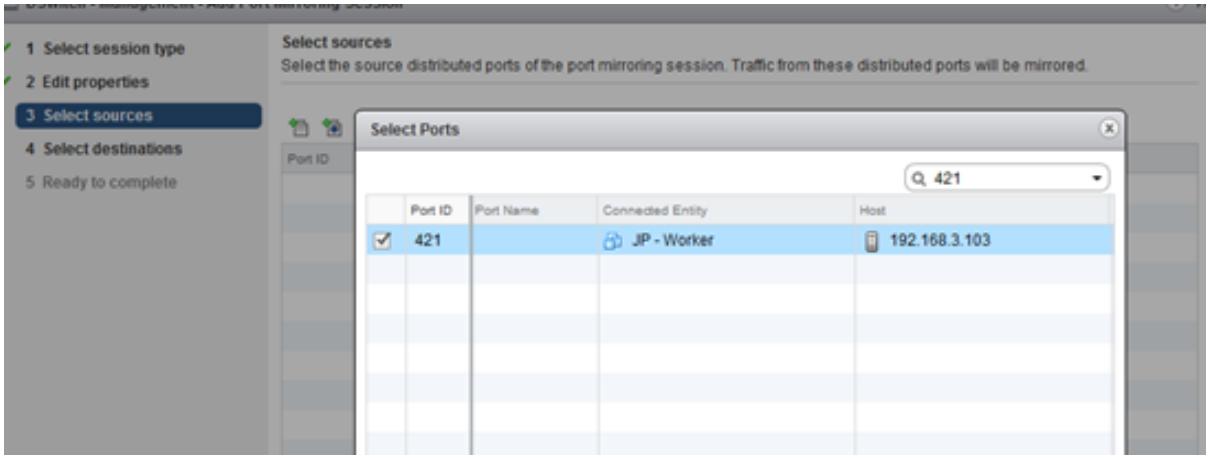
4. Create a new monitoring session by clicking on the **New** button. In the first step, choose the **Distributed Port Mirroring** option and click on the **Next** button.



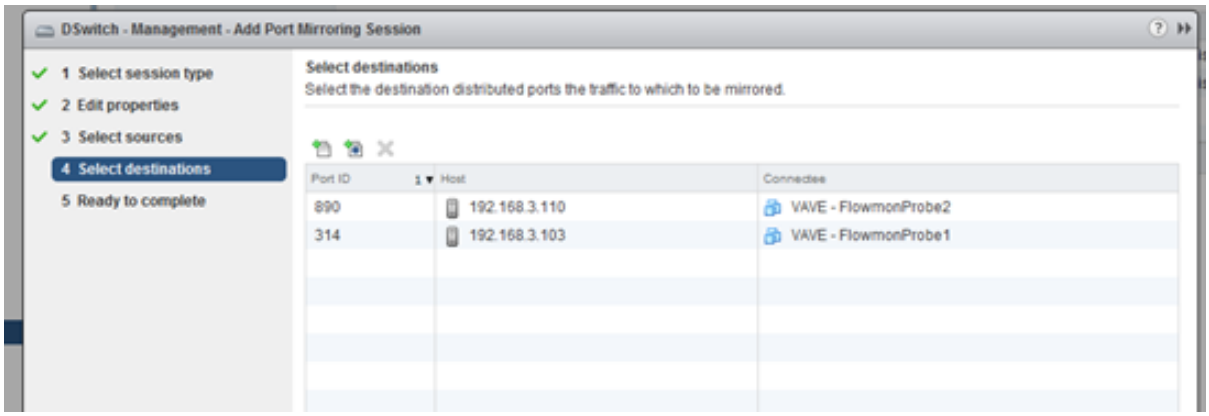
5. Enter a name for the session and click on the **Next** button.



6. In the **Select sources** window, choose Port IDs of virtual machines that should be monitored and clink on the **Next** button.



7. In the **Select destinations** window, choose Port IDs of Flowmon's monitoring interfaces and click on the **Next** button.



8. Check the settings before clicking on the **Finish** button.

> ⚠ When you add a new virtual machine that you would like to monitor, it is necessary to update the list of source ports.

Flowmon Configuration

> ⚠ To ensure continuous traffic visibility, disable migration for all Flowmon instances.

No configuration specific for VMware Distributed vSwitch monitoring is necessary. See instructions on how to enable a monitoring port in the Flowmon User Guide.

Flowmon for KVM

Overview

Flowmon for KVM gives network administrators and security engineers insight into what is happening in their infrastructure. Its powerful features can be used to gain control of bandwidth utilization, optimize network and application performance, reduce time to resolution during troubleshooting and keep the infrastructure protected against modern cyber-security threats.

Flowmon for KVM is

- a virtual appliance intended for the KVM environment,
- capable of collecting as well as generating flow data,
- fully under customer's control - including updates, backups, and configuration.

Flowmon for KVM supports

- IPFIX, NetFlow v5/v9 or sFlow data collection from Flowmon Probes or other compatible devices (e.g., customer routers),
- ingestion of Amazon VPC Flow Logs from AWS,
- traffic monitoring on local Open vSwitches,
- traffic monitoring on local dedicated physical interfaces,
- 3rd-party packet brokers such as Garland Prisms, Ixia CloudLens, or Gigamon,
- ERSPAN/GRE traffic mirroring.

This guide describes the deployment procedure of Flowmon for KVM using a set of qcow2 disk images. The storage capacity can be later changed to match the purchased license.

Features

Flowmon for KVM supports three modes of operation:

- Probe,
- Collector,
- Collector and Probe.

Flowmon Probe

In this mode, the virtual appliance acts as a Flowmon Probe. It accepts mirrored traffic on monitoring ports and exports flow data to at least one remote Flowmon Collector instance.

Supported traffic mirroring solutions:

- KVM Open vSwitch Port Mirroring

Supported 3rd-party packet brokers:

- Ixia CloudLens
- Gigamon
- Garland Prisms

Flowmon Collector

In this mode, the virtual appliance acts as a Flowmon Collector and accepts supported flow formats from external probes, network devices, or Amazon VPC Flow Logs on management ports. For details on supported flow sources and formats, refer to the official Flowmon User Guide.

Flowmon Collector and Flowmon Probe

In this mode, the virtual appliance acts both as a Flowmon Probe and Flowmon Collector. Probe sends data to the locally available Collector. For details on configuration, refer to the official Flowmon User Guide.

Licensing

Flowmon for KVM is a virtual appliance using the Bring-Your-Own-License (BYOL) licensing model.

With BYOL, you can apply for a Free Trial License at flowmon.com.

For support or inquiries, see our contact information.

Prerequisites

In order to follow this guide, you need the following:

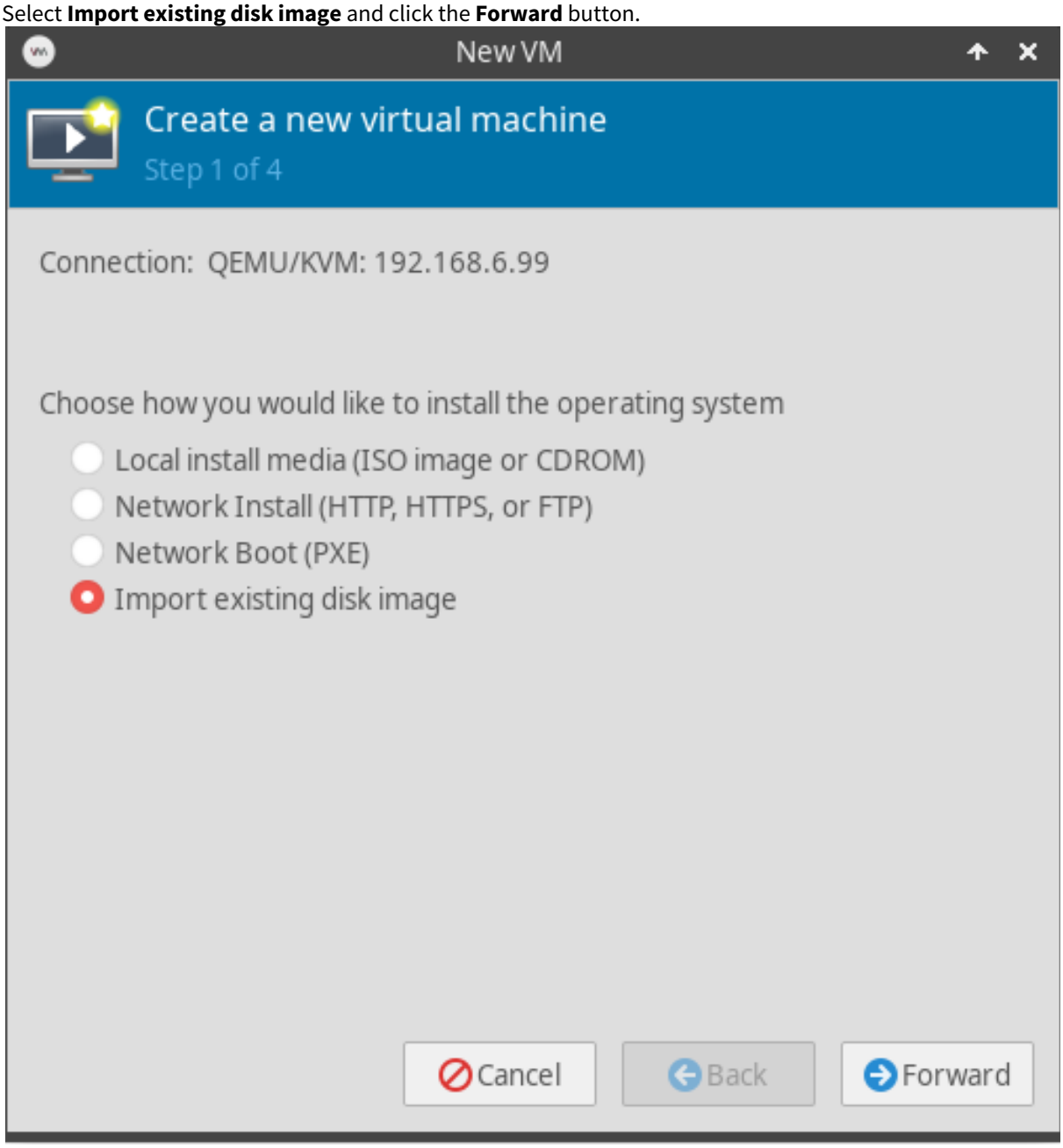
1. KVM-based host with a graphical user interface and **Virtual Machine Manager** installed.
2. Flowmon for KVM downloaded from the Partner Portal, archives for download are located in **Downloads / Products / Flowmon Virtual Appliances & Cloud / Flowmon for KVM**. Unless directed otherwise, pick the latest stable version with the desired set of modules.
3. A valid Flowmon license or a trial license from flowmon.com.

Deployment

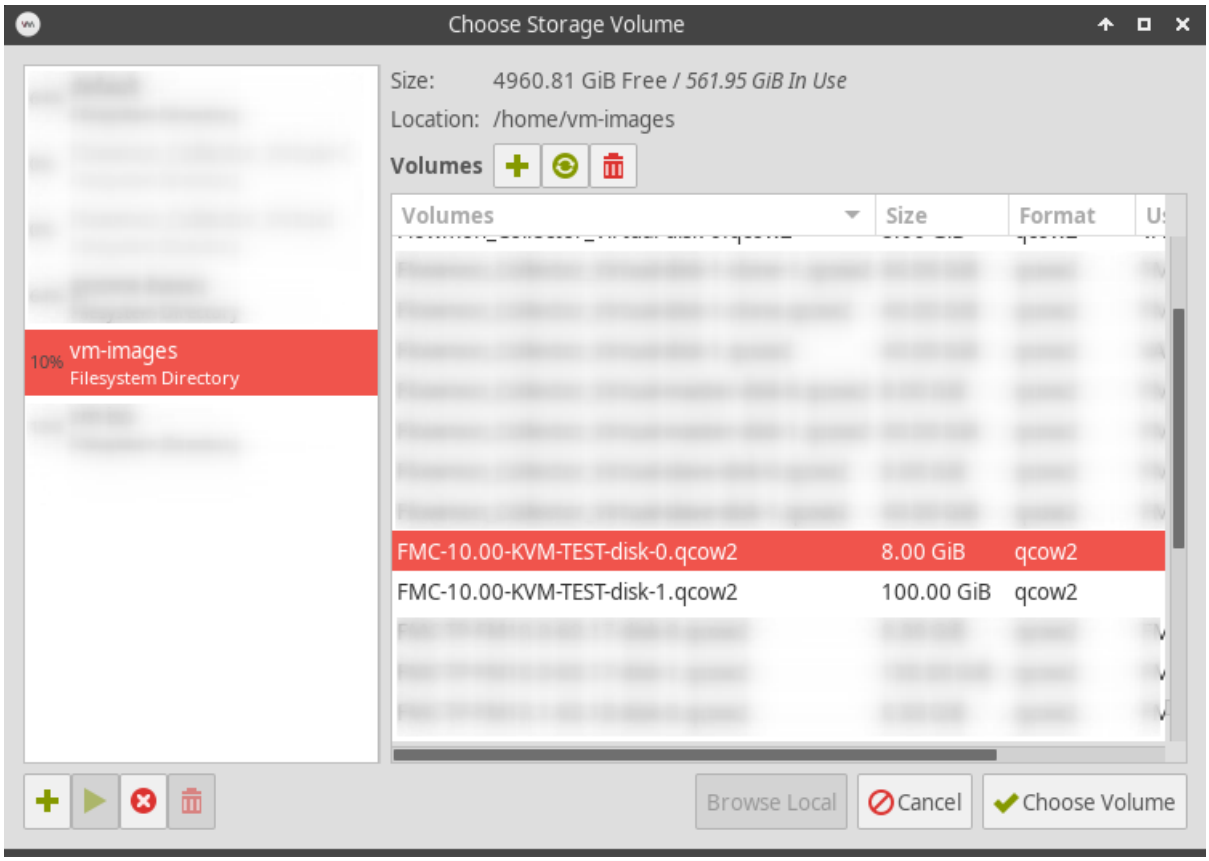
The deployment of Flowmon for KVM consists of the following steps:

1. Unzip the archive.
2. Start the **Virtual Machine Manager** application.
3. Select **File** – **New virtual machine**.

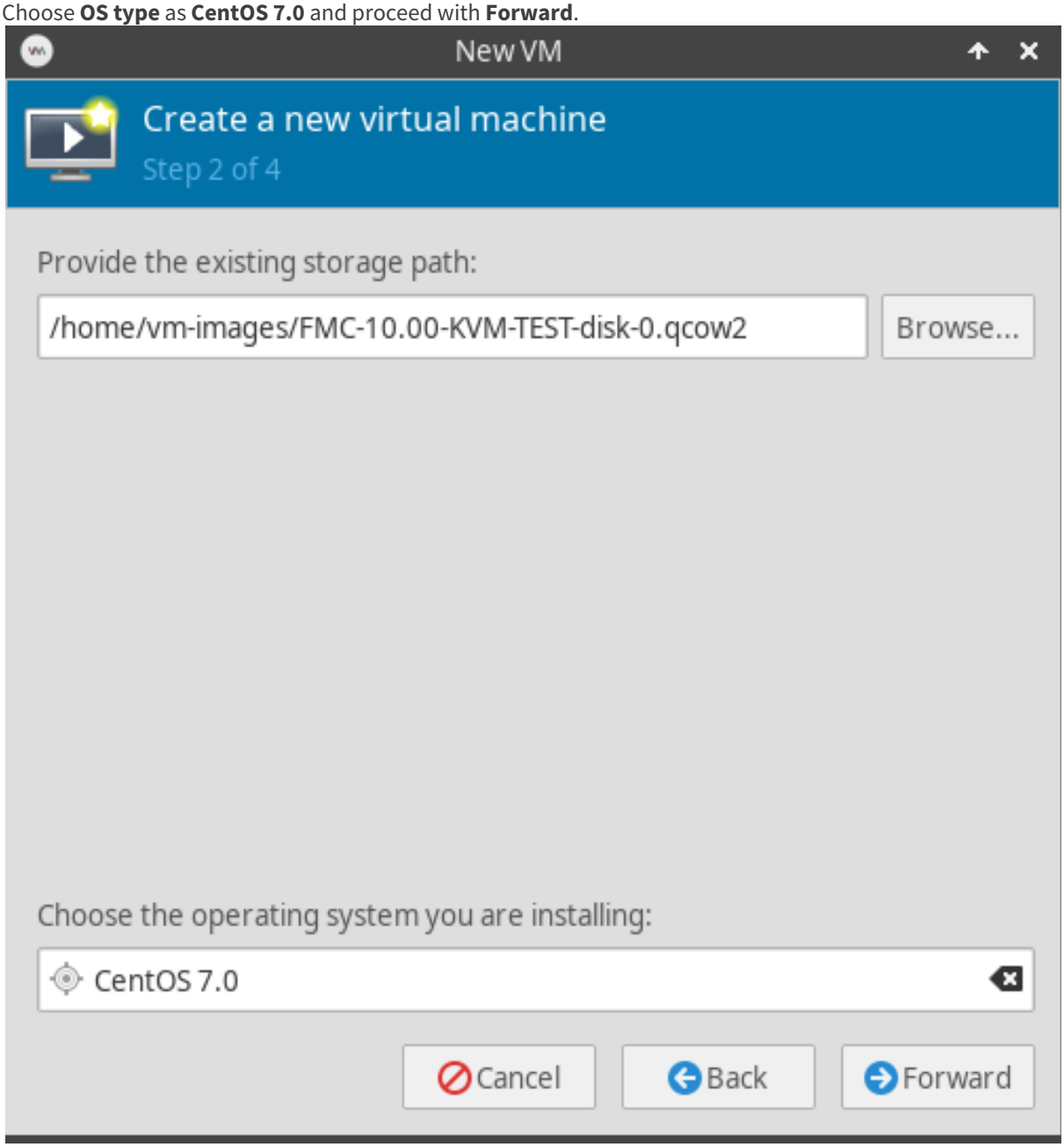
4. Select **Import existing disk image** and click the **Forward** button.



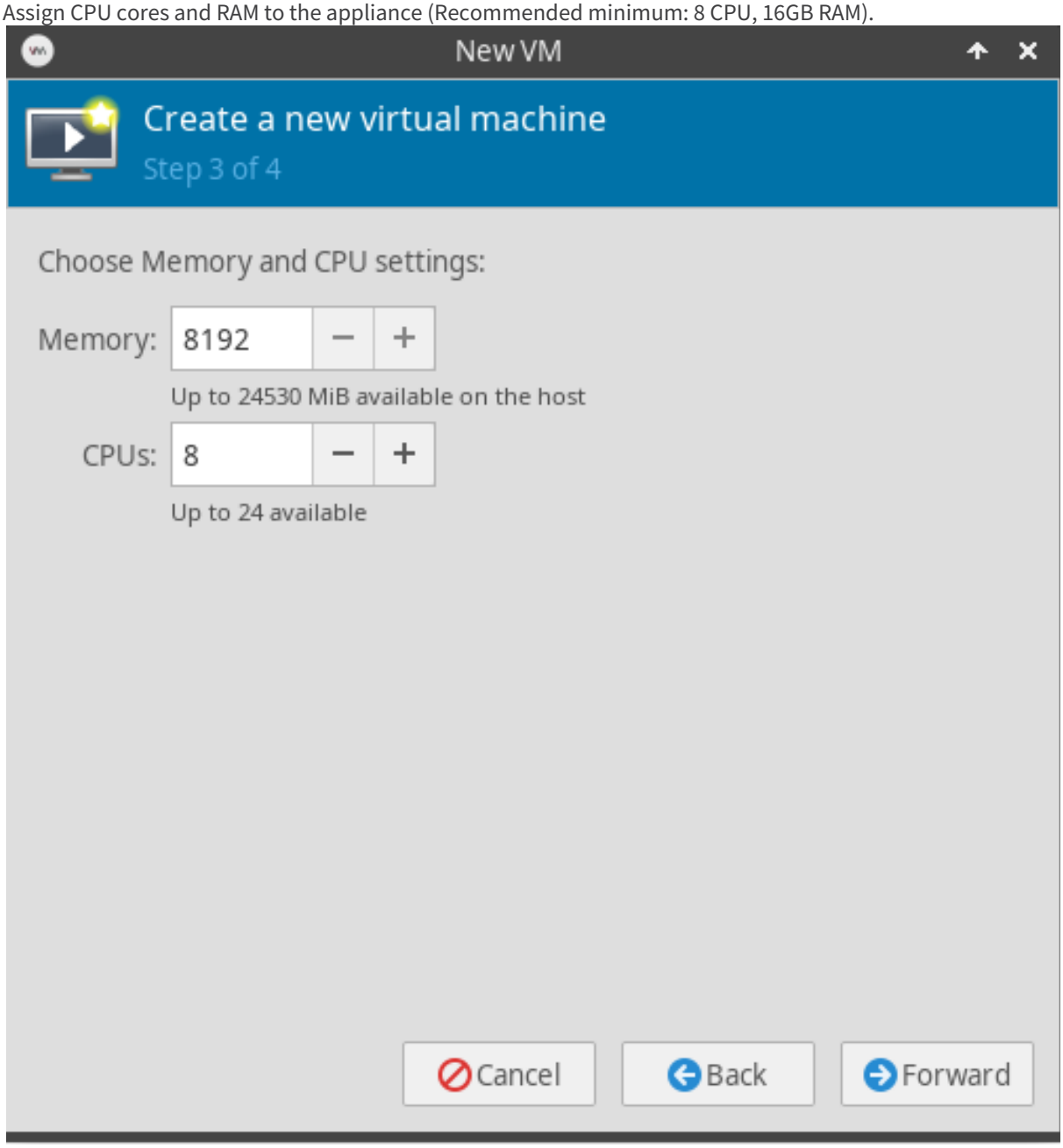
5. Select path to the unzipped file from step 2, choose disk 0 and confirm the settings with the **Choose volume** button.


Choose Storage Volume
Size: 4960.81 GiB Free / 561.95 GiB In Use
Location: /home/vm-images
Volumes
10%
vm-images
Filesystem Directory
Volumes
Size
Format
FMC-10.00-KVM-TEST-disk-0.qcow2
8.00 GiB
qcow2
FMC-10.00-KVM-TEST-disk-1.qcow2
100.00 GiB
qcow2
Browse Local
Cancel
Choose Volume

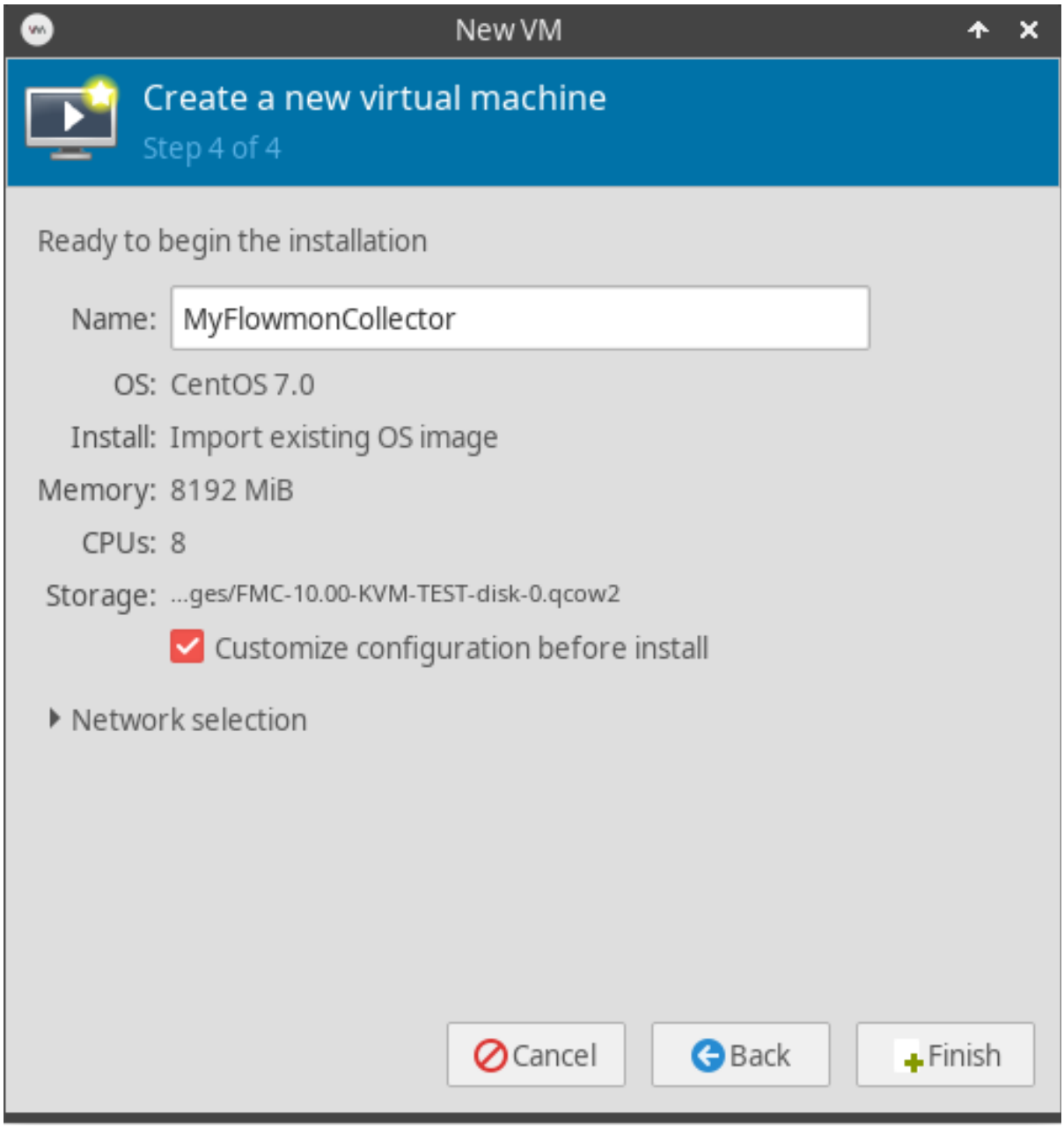
6. Choose **OS type** as **CentOS 7.0** and proceed with **Forward**.



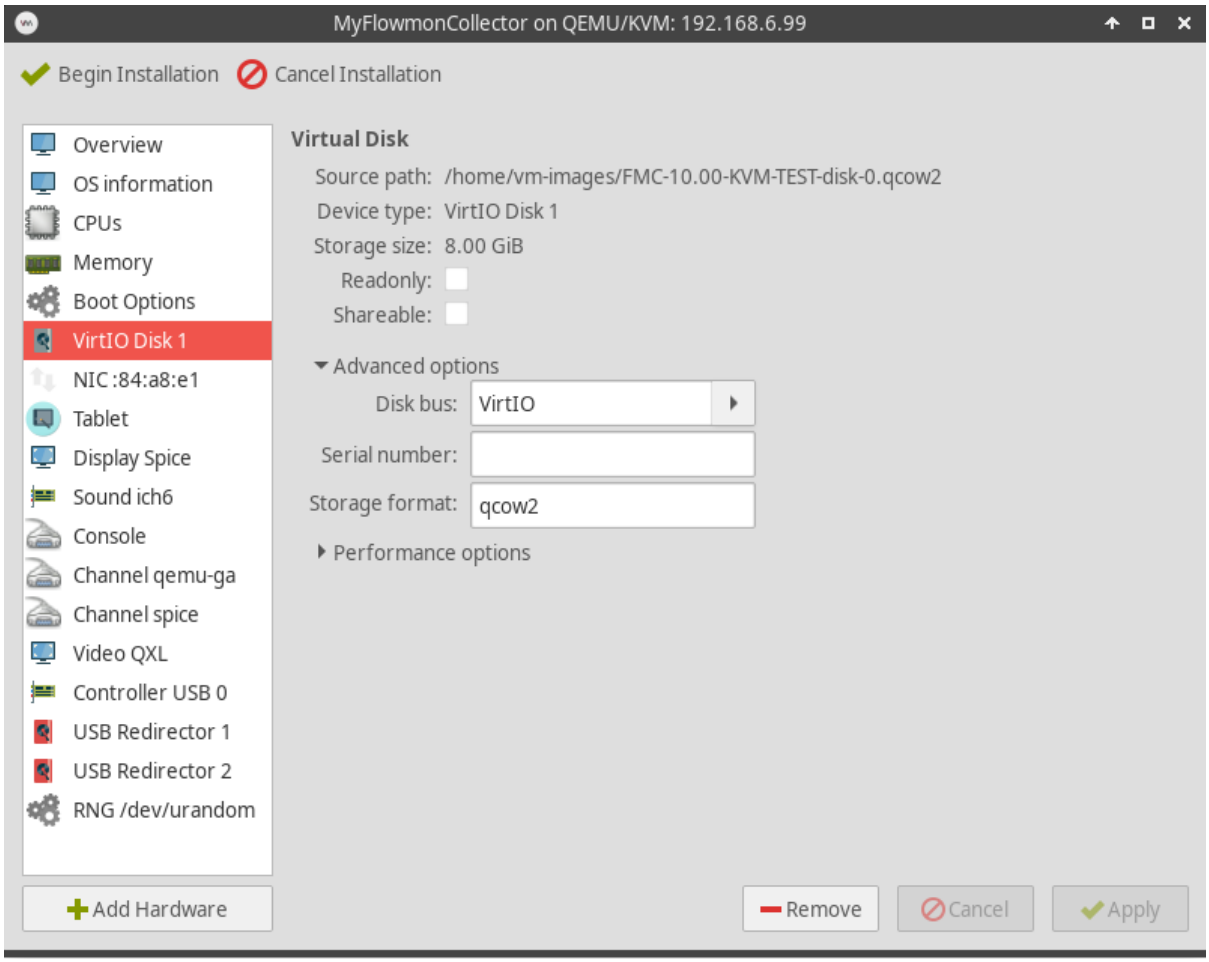
7. Assign CPU cores and RAM to the appliance (Recommended minimum: 8 CPU, 16GB RAM).



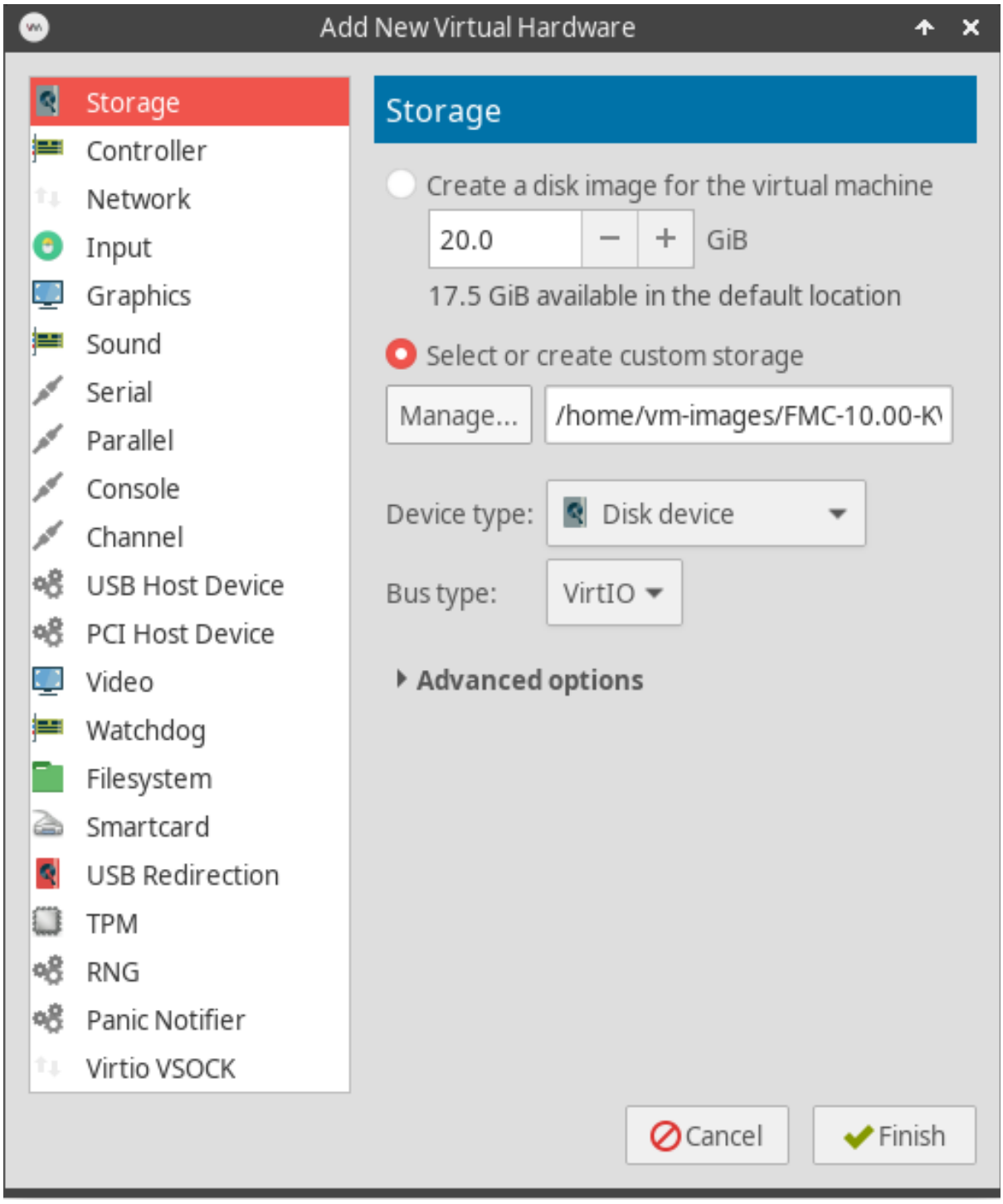
8. Set a name for the appliance, check option **Customize configuration before install** and **Finish** the configuration.



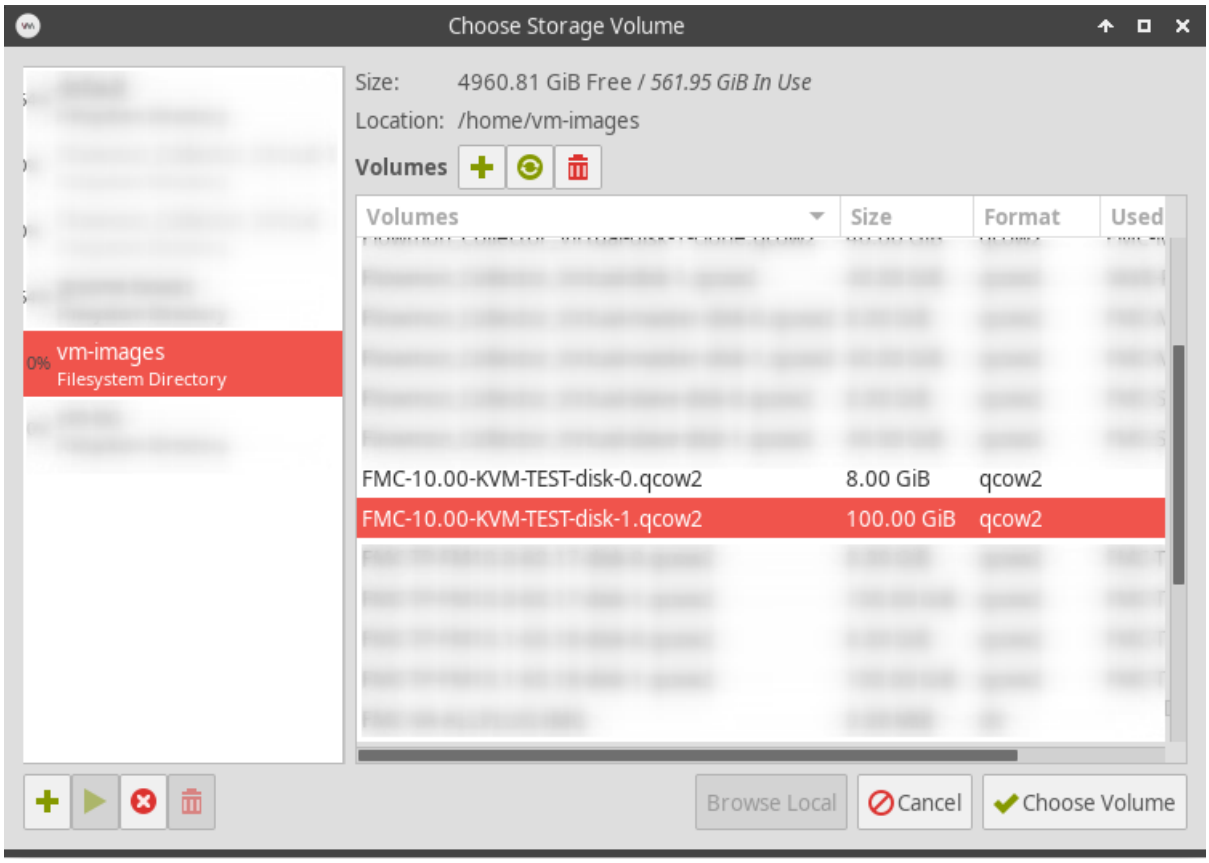
9. Select **VirtIO Disk 1**, set **Disk bus** to **VirtIO** and **Apply** the settings. Then click **Add Hardware** in order to add a data drive.



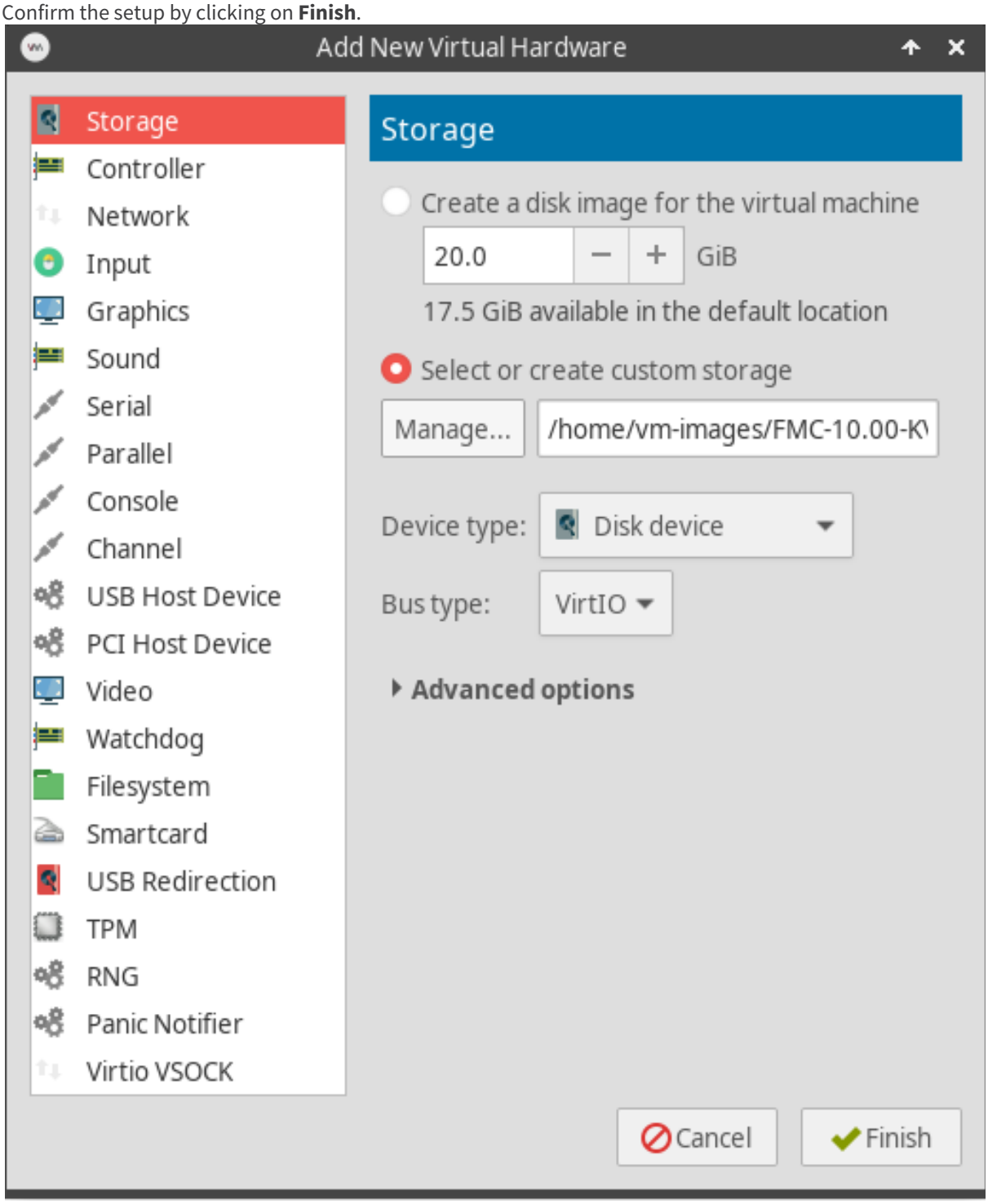
10. Select the **Storage** option and choose **Select or create custom storage**. The **Bus type** option has to be set to **VirtIO**. Then browse images by clicking on **Manage...**.


Add New Virtual Hardware
Storage
Controller
Network
Input
Graphics
Sound
Serial
Parallel
Console
Channel
USB Host Device
PCI Host Device
Video
Watchdog
Filesystem
Smartcard
USB Redirection
TPM
RNG
Panic Notifier
Virtio VSOCK
Storage
Create a disk image for the virtual machine
20.0
GiB
17.5 GiB available in the default location
Select or create custom storage
Manage...
/home/vm-images/FMC-10.00-K
Device type:
Disk device
Bus type:
VirtIO
Advanced options
Cancel
Finish

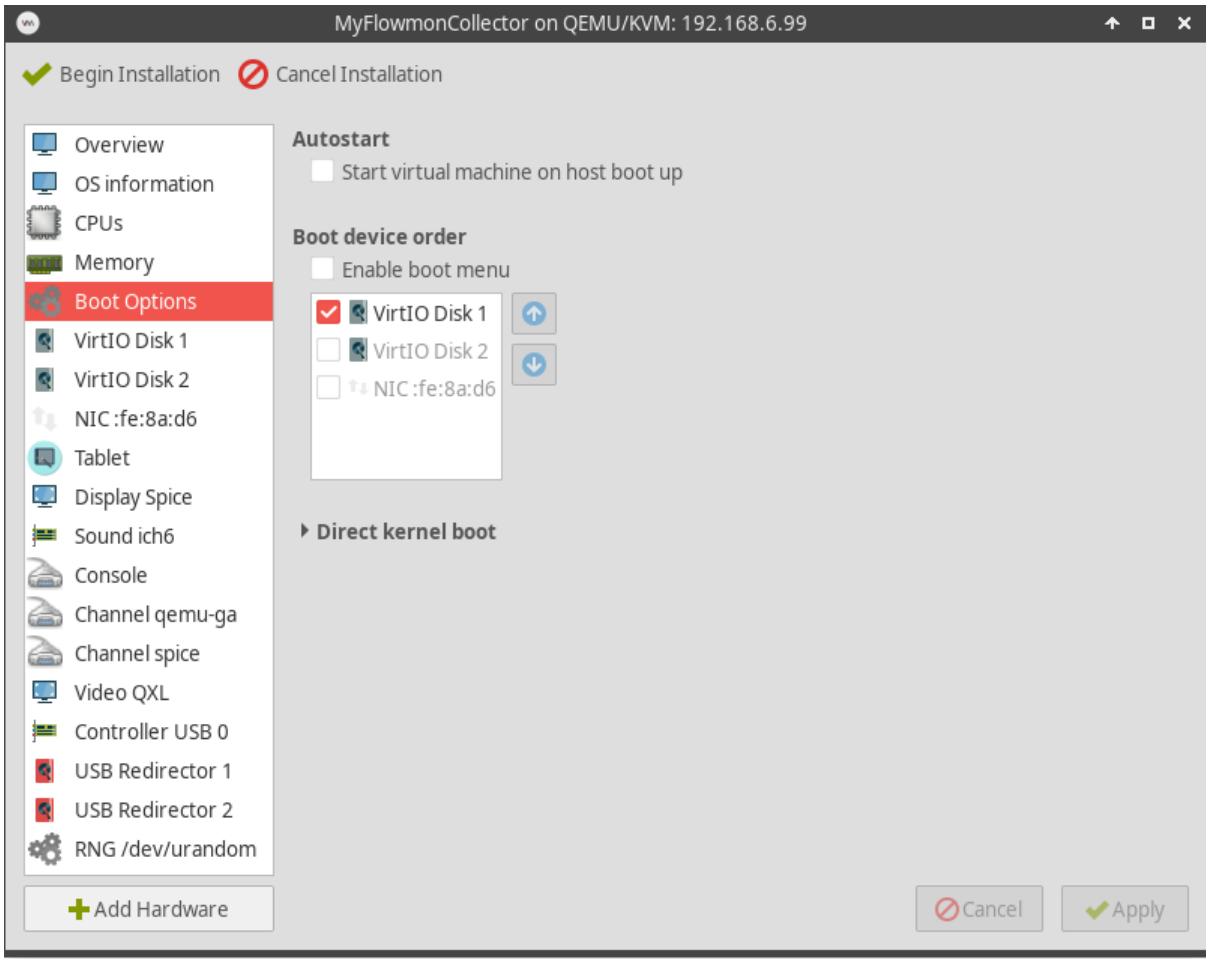
11. Select disk 1 and click on the **Choose Volume** button.



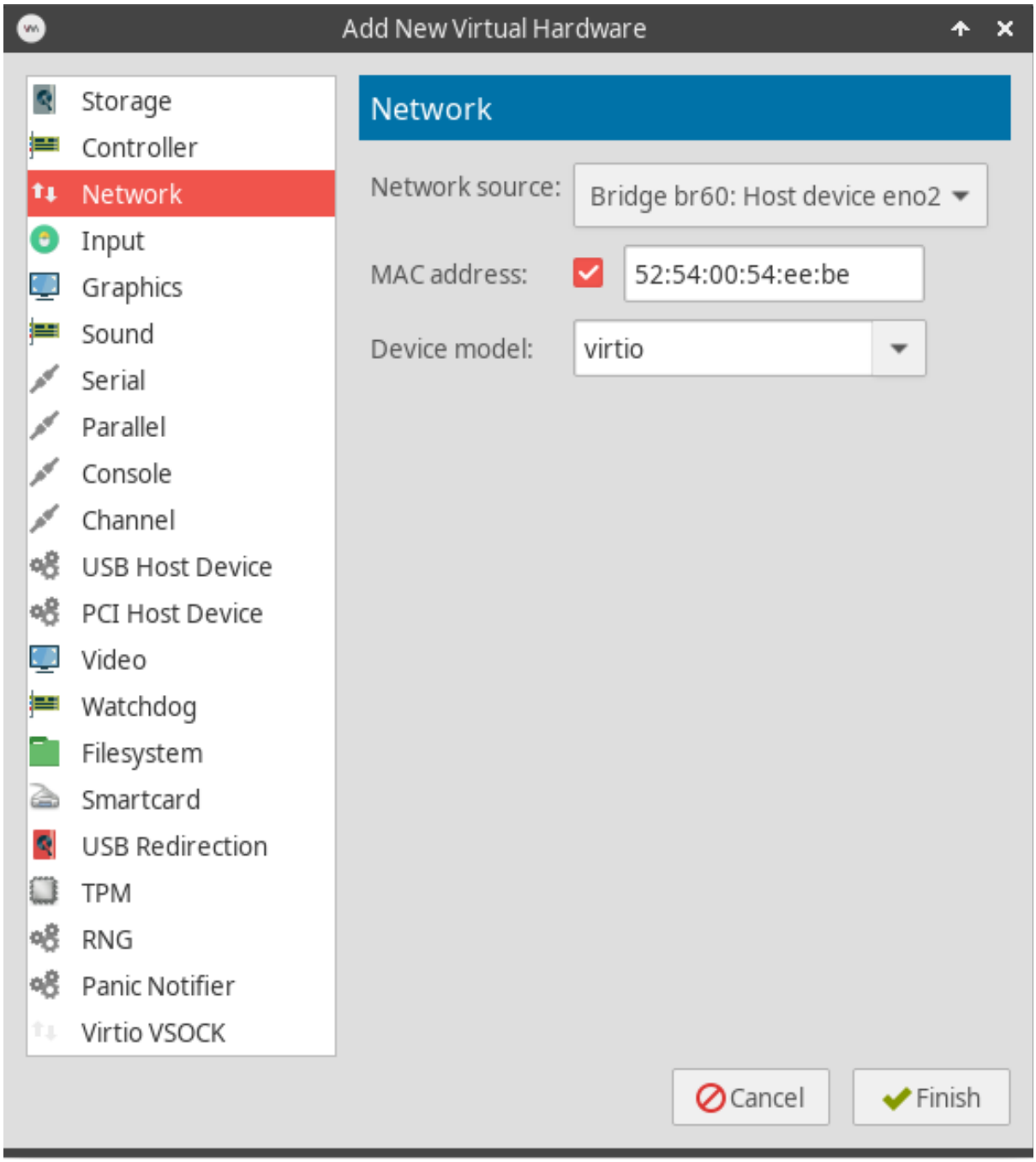
12. Confirm the setup by clicking on **Finish**.



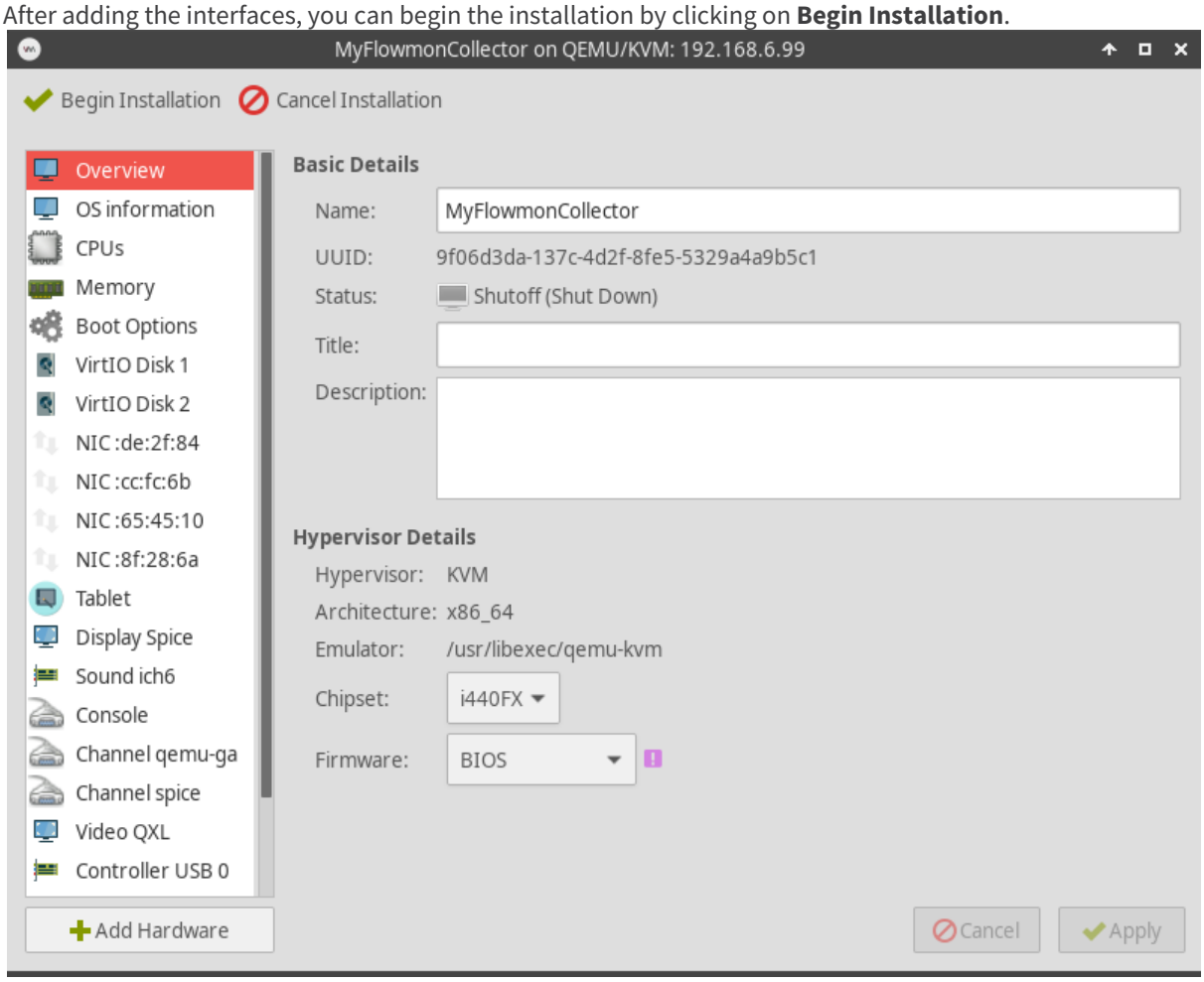
13. Select the **Boot Options** category and select **VirtIO Disk 1** as a primary disk from which to boot the appliance.



14. Add as many interfaces as necessary to create all interfaces of a Flowmon appliance (three more for Flowmon Collector, 1+N for Flowmon Probe with N monitoring ports). Click on **Add Hardware**, select **Network**, choose **Network source** and **Device model** (**virtio**) and click on **Finish**.


Add New Virtual Hardware
Storage
Controller
Network
Input
Graphics
Sound
Serial
Parallel
Console
Channel
USB Host Device
PCI Host Device
Video
Watchdog
Filesystem
Smartcard
USB Redirection
TPM
RNG
Panic Notifier
Virtio VSOCK
Network
Network source:
Bridge br60: Host device eno2
MAC address:
52:54:00:54:ee:be
Device model:
virtio
Cancel
Finish

15. After adding the interfaces, you can begin the installation by clicking on **Begin Installation**.



Flowmon Configuration

Please refer to Post-installation Steps.

KVM Open vSwitch Port Mirroring

Overview

Flowmon for KVM has the ability to monitor traffic and generate NetFlow / IPFIX flow data. To enable this functionality for the monitoring of an Open vSwitch local to the KVM host where Flowmon is running, please follow the steps outlined below.

Prerequisites

- A running instance of Flowmon for KVM - Flowmon Collector (with a built-in Probe) or Flowmon Probe.

Deployment

Since Virtual Machine Manager does not support Open vSwitch (OVS), you have to manually modify the configuration of your Flowmon instance.

1. Open Flowmon's XML descriptor for editing.

```
virsh edit <name-of-your-Flowmon-in-Virtual-Machine-Manager>
```

2. Add each monitoring port of your Flowmon to an **OVSbridge** previously created in your OVS. Each monitoring port type has to be set to **openvswitch**. Substitute **[name_of_your_OVSbridge]** for the name of your OVS bridge.

```
<interface type='bridge'>
  <mac address='52:54:00:9f:46:cc'/>
  <source bridge='[name_of_your_OVSbridge]'/>
  <virtualport type='openvswitch'>
        <parameter interfaceid='c9a700ed-9576-45aa-81f3-
b7d94b73cc91'/>
  </virtualport>
  <!-- ... -->
</interface>
```

3. **Create a mirror** in your OVS bridge.

```
ovs-vsctl -- --id=@m create mirror \
          name=<custom-name-of-the-mirror> \
          -- add bridge \
          <name-of-the-OVS-bridge-where-to-add-the-mirror> \
          mirrors @m
```

4. If you would like to mirror specific ports, **configure per-port mirroring**.
Display UUIDs of all **vnet** interfaces associated with OVS.

```
ovs-vsctl show
```

This example shows UUIDs for vnet[0-5].

```
for p in vnet{0..5}; do
  echo "$p: $(ovs-vsctl get port "$p" _uuid)"
done
```

For each interface created in OVS that you want to monitor set up its mirroring to the mirror created in step 3. The following command mirrors both ingress and egress traffic of the source port.

```
ovs-vsctl set mirror <name-of-the-mirror-from-step-3> \
          select_src_port=<UUID-of-the-vnet-interface-you-want-to-monitor> \
          select_dst_port=<UUID-of-the-vnet-interface-you-want-to-monitor>
```

5. If your traffic is isolated in VLANs, you can **select specific VLAN IDs to mirror**.

```
ovs-vsctl set mirror <name-of-the-mirror-from-step-3> select-vlan=<csv-list-of-vlan-ids-to-mirror>
```

6. **Select and set VLAN ID** for mirroring output. Flowmon's monitoring interface(s) must belong to this VLAN to receive mirrored traffic.

```
ovs-vsctl set mirror <name-of-the-mirror-from-step-3> output-vlan=<selected-vlan-id>
```

7. **Tag Flowmon's monitoring interface(s)** with VLAN ID.

```
ovs-vsctl set port <port-name> tag=<selected-vlan-id-from-step-7>
# or for multiple VLANs
ovs-vsctl set port <port-name> trunks=<csv-list-of-vlan-ids>
```

Flowmon Configuration

No configuration specific for KVM Open vSwitch monitoring is necessary. See instructions on how to enable a monitoring port in the Flowmon User Guide.

Flowmon for Hyper-V

Overview

Flowmon for Hyper-V gives network administrators and security engineers insight into what is happening in their infrastructure. Its powerful features can be used to gain control of bandwidth utilization, optimize network and application performance, reduce time to resolution during troubleshooting and keep the infrastructure protected against modern cyber-security threats.

Flowmon for Hyper-V is

- a virtual appliance intended for the Hyper-V environment,
- capable of collecting as well as generating flow data,
- fully under customer's control - including updates, backups, and configuration,

Flowmon for Hyper-V supports

- IPFIX, NetFlow v5/v9 or sFlow data collection from Flowmon Probes or other compatible devices (e.g., customer routers),
- ingestion of Amazon VPC Flow Logs from AWS,
- traffic monitoring on local vSwitches,
- traffic monitoring on local dedicated physical interfaces,
- 3rd-party packet brokers such as Garland Prisms, Ixia CloudLens, or Gigamon,
- ERSPAN/GRE traffic mirroring.

This guide describes the deployment procedure of Flowmon for Hyper-V using a set of vhdx disk images. The storage capacity can be later changed to match the purchased license.

Features

Flowmon for Hyper-V supports three modes of operation:

- Probe,
- Collector,
- Collector and Probe.

Flowmon Probe

In this mode, the virtual appliance acts as a Flowmon Probe. It accepts mirrored traffic on monitoring ports and exports flow data to at least one remote Flowmon Collector instance.

Supported traffic mirroring solutions:

- Hyper-V Virtual Switch Port Monitoring
- Hyper-V Network Interface Mirroring

Supported 3rd-party packet brokers:

- Ixia CloudLens
- Gigamon
- Garland Prisms

Flowmon Collector

In this mode, the virtual appliance acts as a Flowmon Collector and accepts supported flow formats from external probes, network devices, or Amazon VPC Flow Logs on management ports. For details on supported flow sources and formats, refer to the official Flowmon User Guide.

Flowmon Collector and Flowmon Probe

In this mode, the virtual appliance acts both as a Flowmon Probe and Flowmon Collector. Probe sends data to the locally available Collector. For details on configuration, refer to the official Flowmon User Guide.

Licensing

Flowmon for Hyper-V is a virtual appliance using the Bring-Your-Own-License (BYOL) licensing model.

With BYOL, you can apply for a Free Trial License at flowmon.com.

For support or inquiries, see our contact information.

Prerequisites

In order to follow this guide, you need the following:

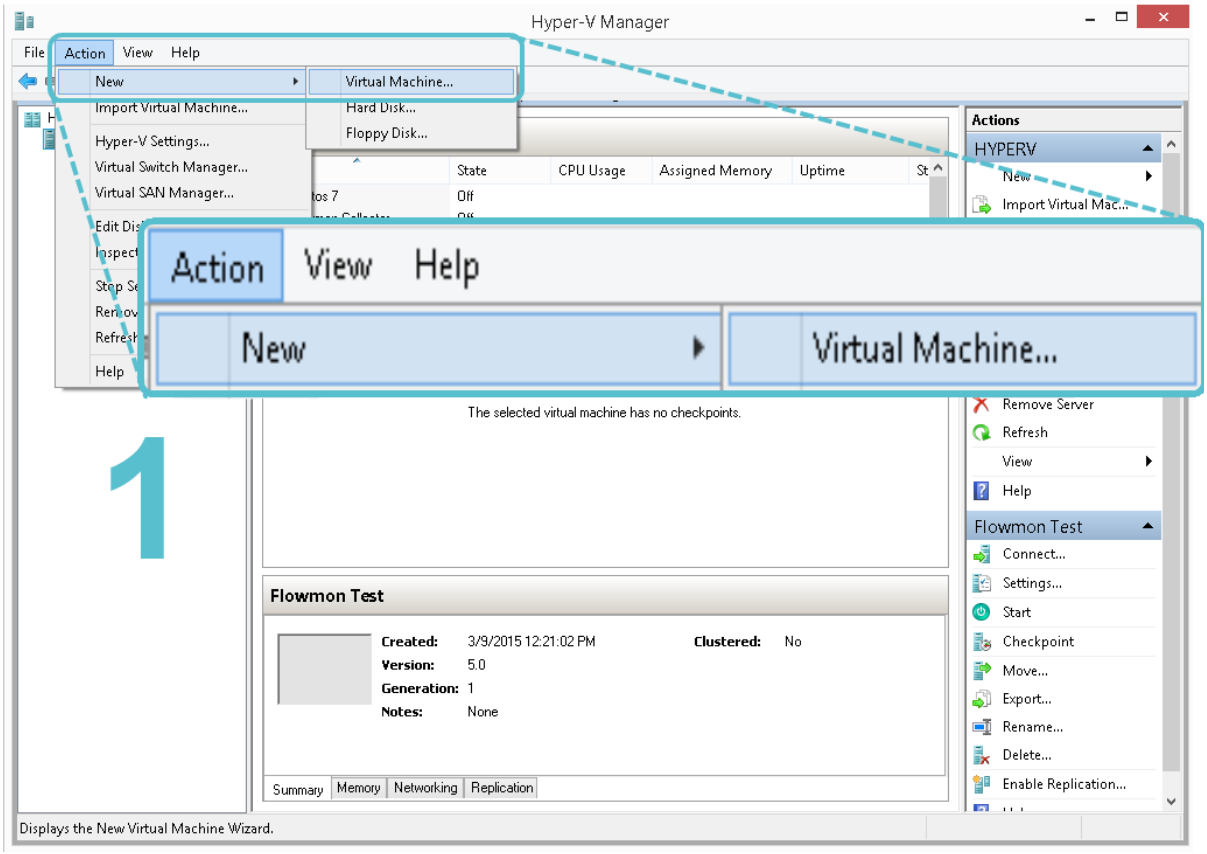
1. A Hyper-V host with a graphical user interface and **Hyper-V Manager** installed.
2. Flowmon for Hyper-V downloaded from the Partner Portal, archives for download are located in **Downloads / Products / Flowmon Virtual Appliances & Cloud / Flowmon for Hyper-V**. Unless directed otherwise, pick the latest stable version with the desired set of modules.
3. A valid Flowmon license or a trial license from flowmon.com.

Deployment

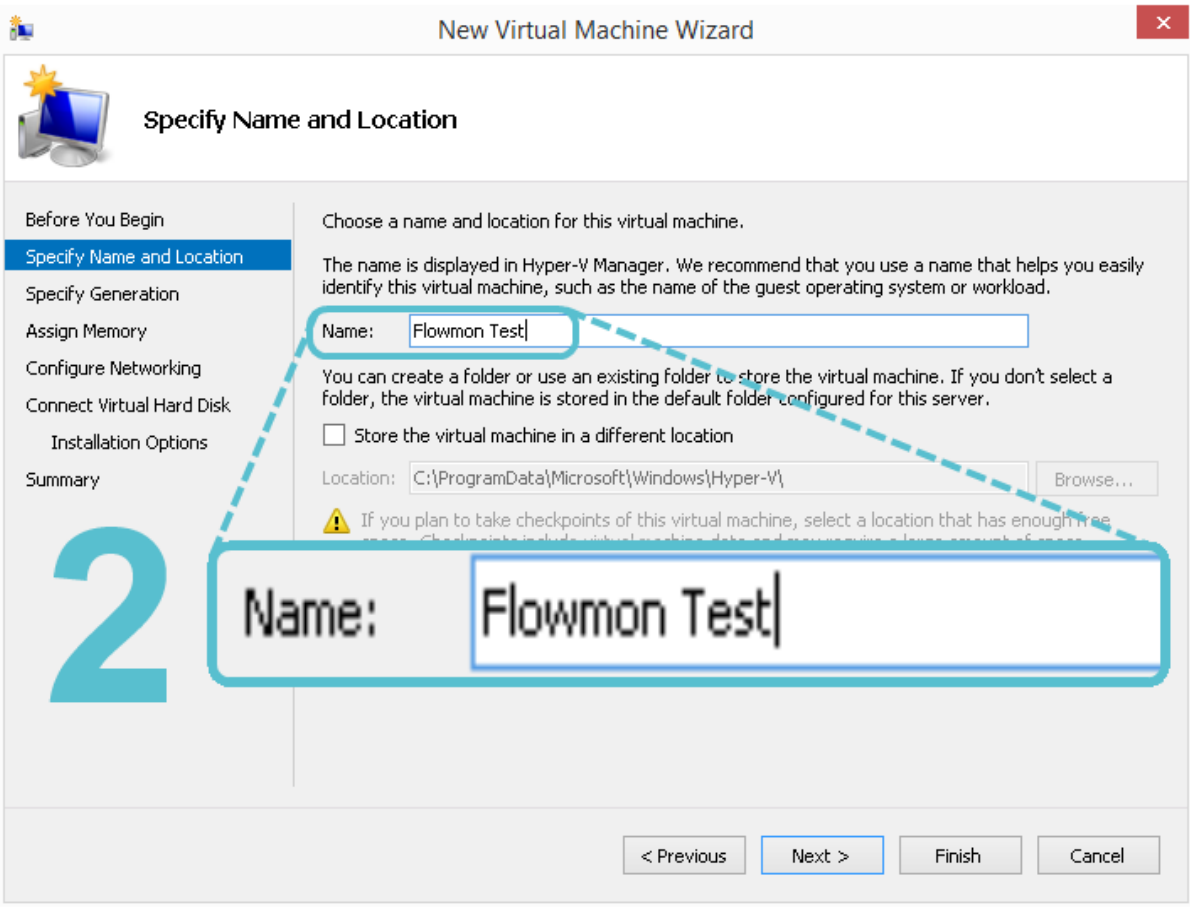
For each Flowmon deployment, individual copies of the provided VHDX files are needed. You can reuse VHDX file to deploy multiple instances.

The deployment of Flowmon for Hyper-V consists of the following steps:

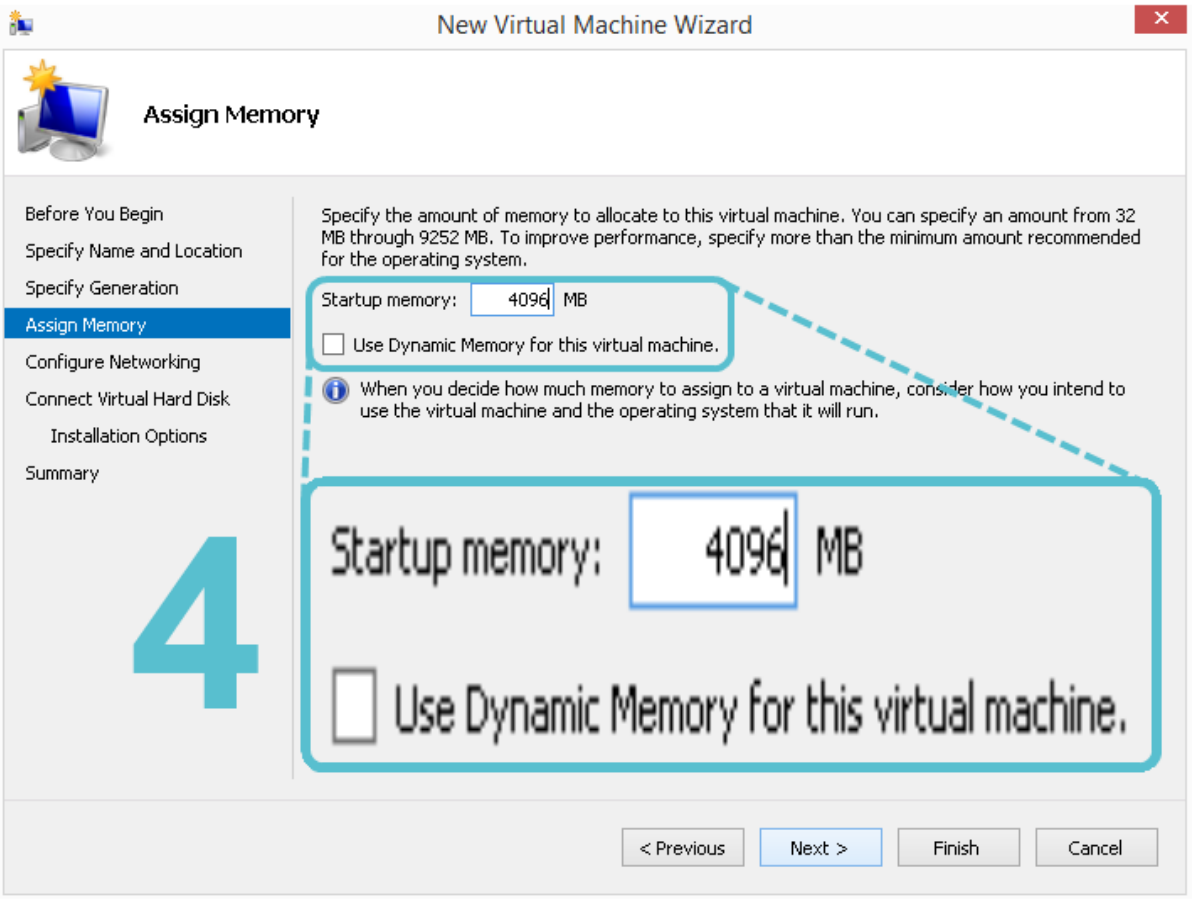
- Unzip the archive. In **Hyper-V Manager**, click in the main menu on **Action**, select **New** and **Virtual Machine**.



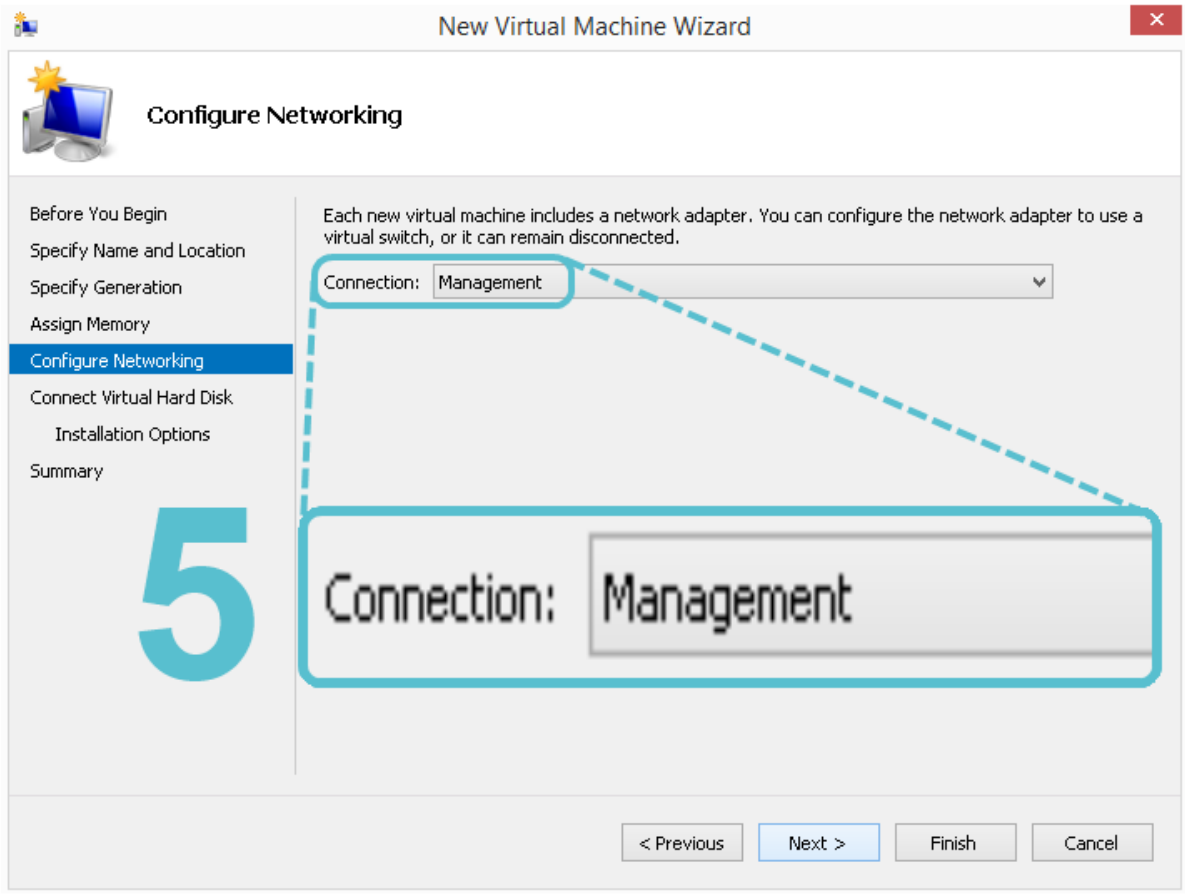
- Provide a **name** for the virtual machine.



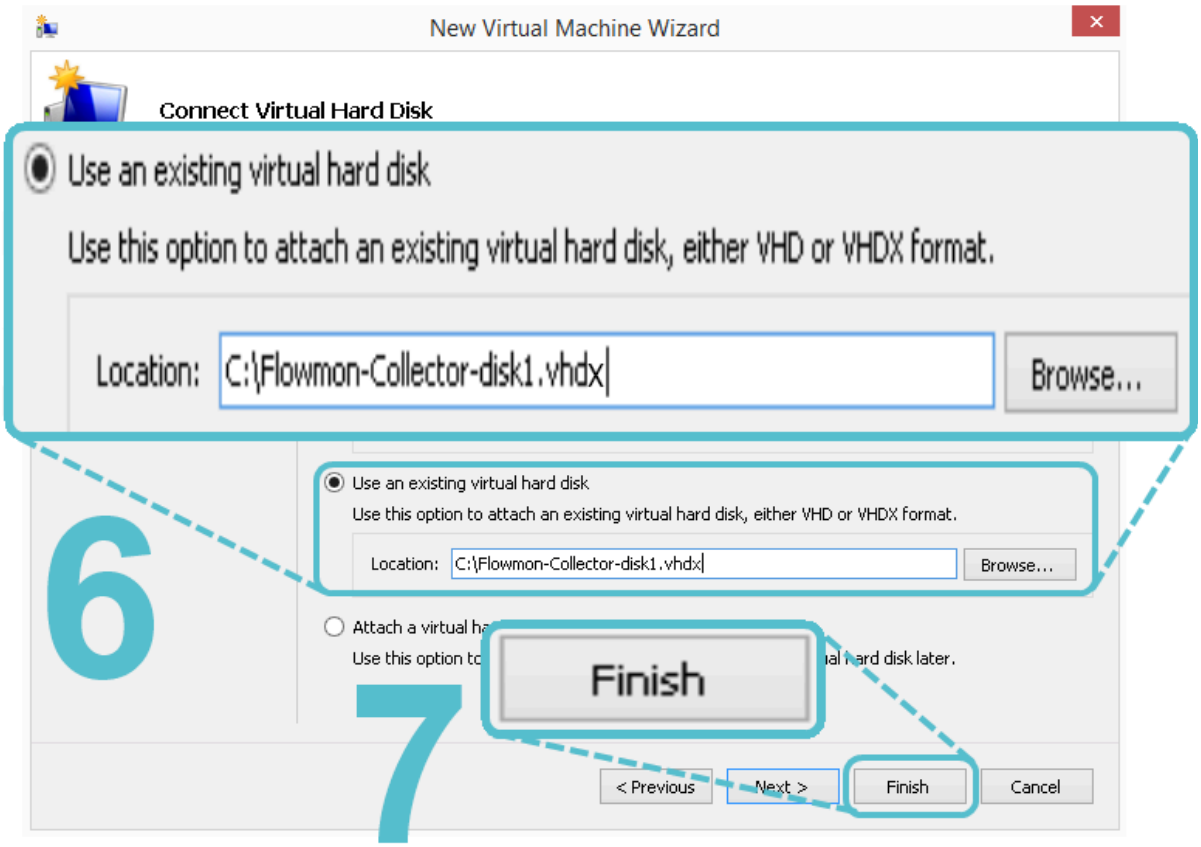
- As the generation of the new virtual machine, select **Generation 2**.
- Assign **memory**.



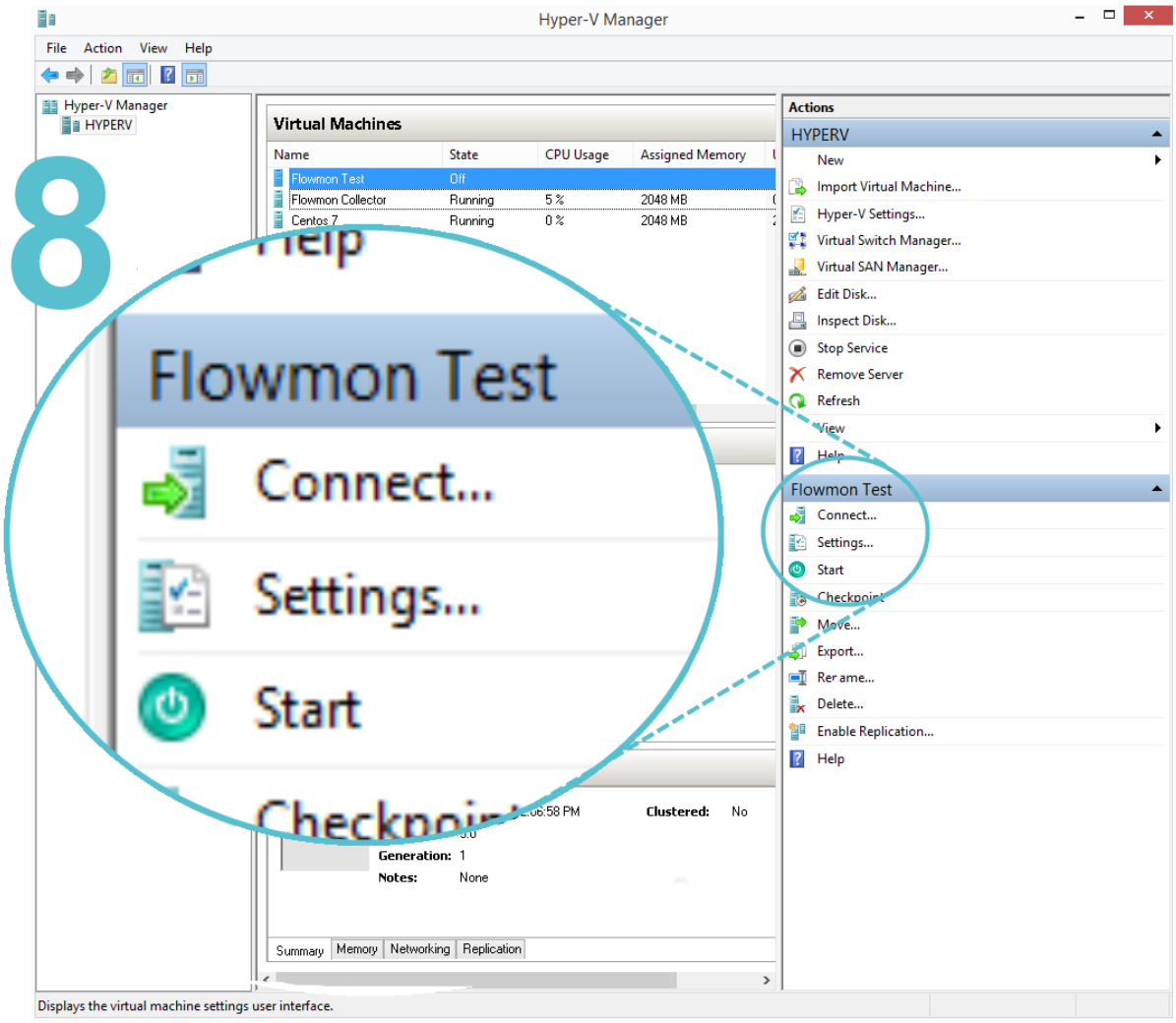
- In **Configure Networking**, select connection for Flowmon's **Management Interface 1**.



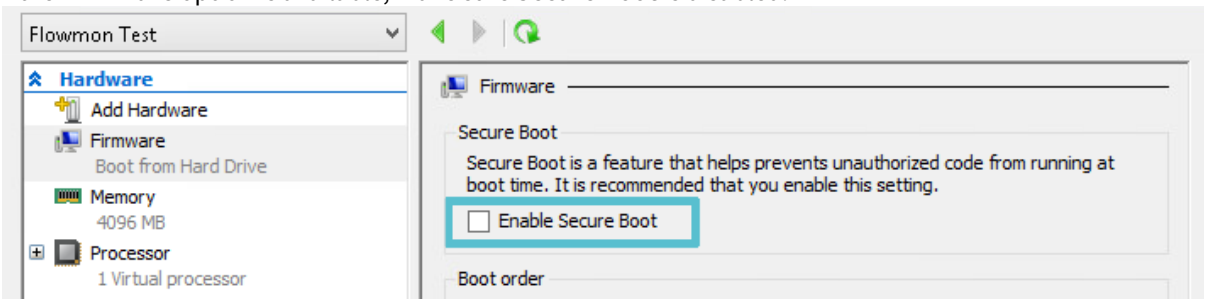
- In **Connect Virtual Hard Disk**, select **Use an existing virtual hard disk**. Pick the first VHDX file. Click on **Finish**.



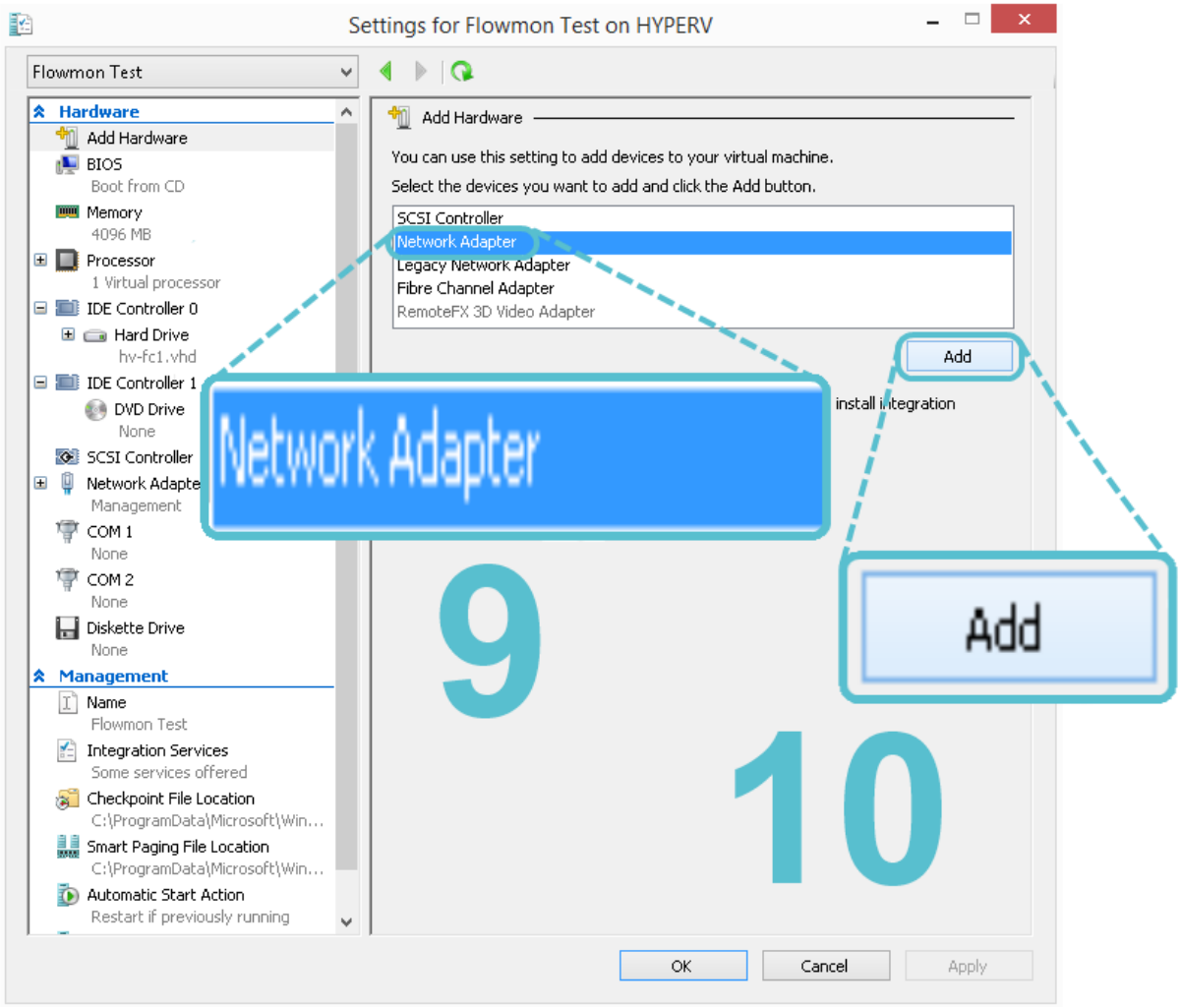
- Open **Settings** on the newly created virtual machine.



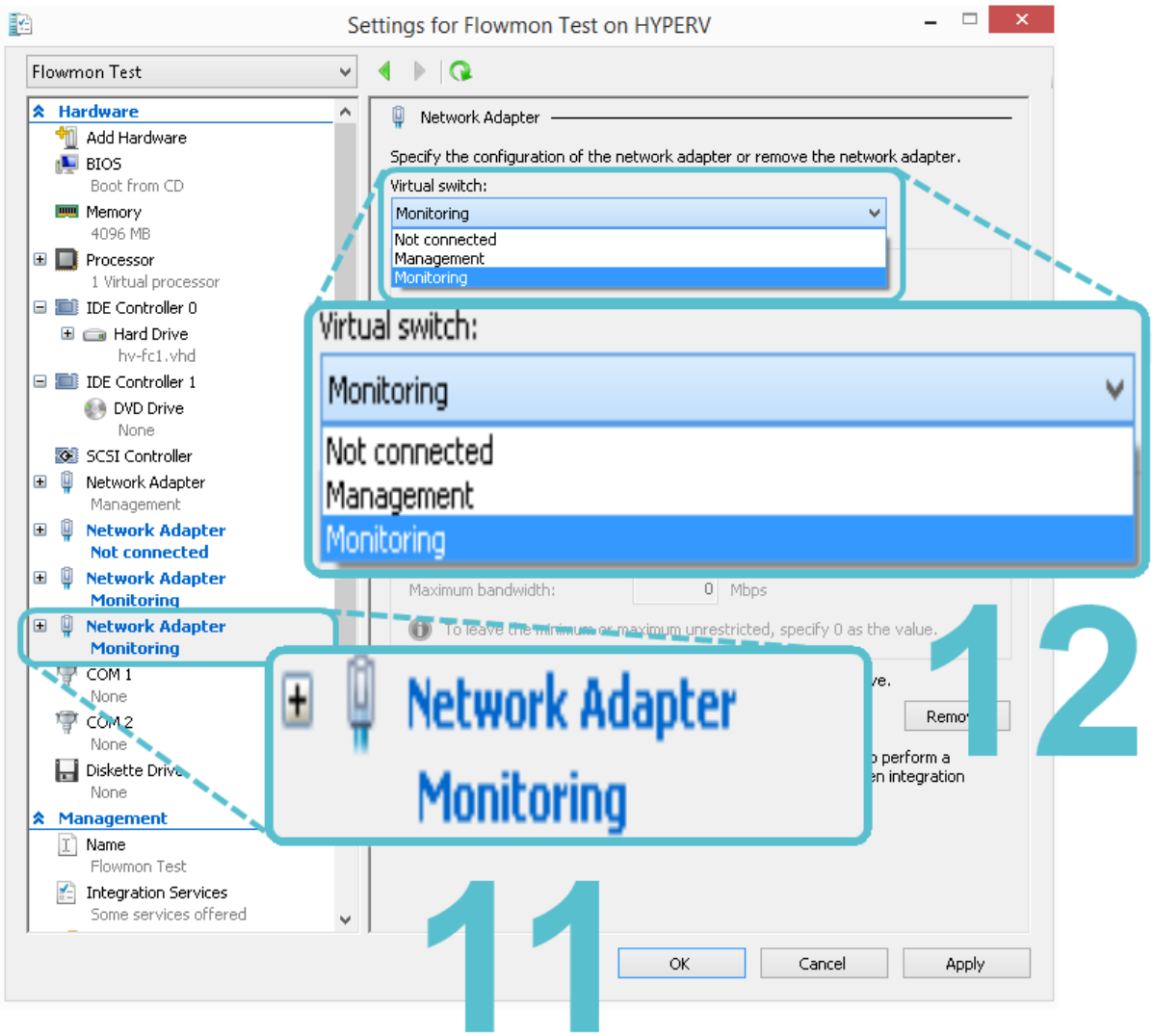
- If the **Firmware** option is available, make sure **Secure Boot** is disabled.



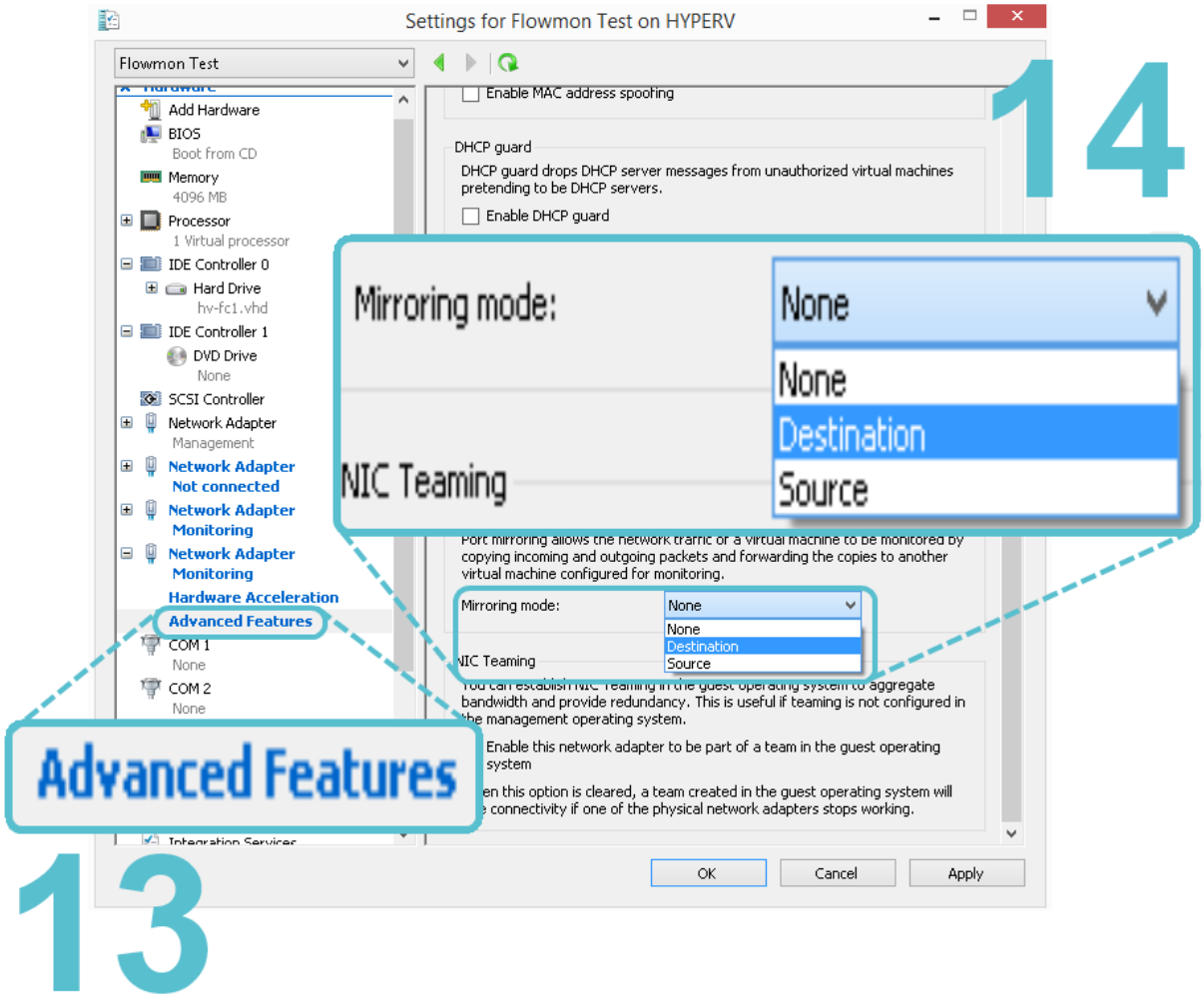
- Add multiple network adapters. Click on **Add Hardware** and add a **Network Adapter**. For additional management interface add one adapter. For two monitoring ports add two networks adapters.



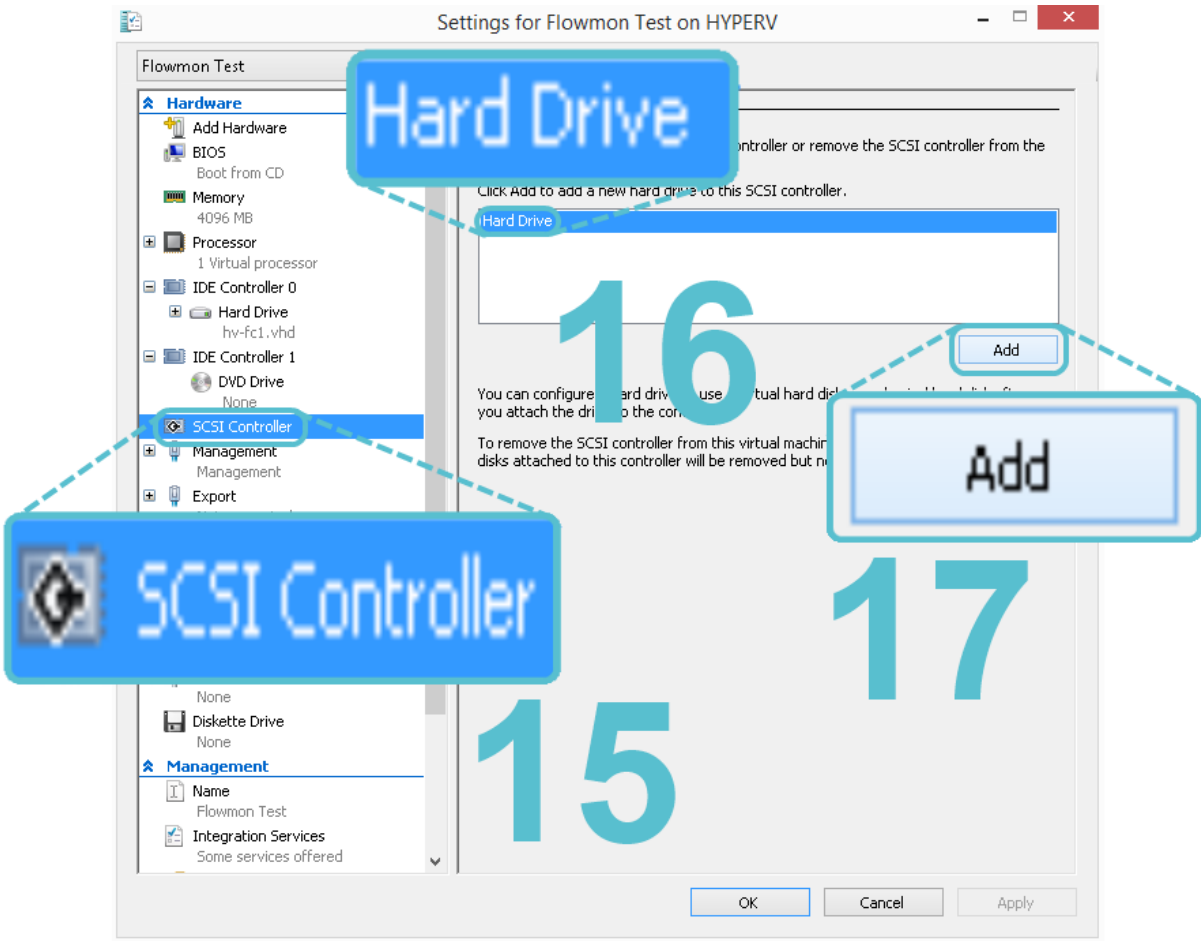
- For each new network adapter, select a **virtual switch**.



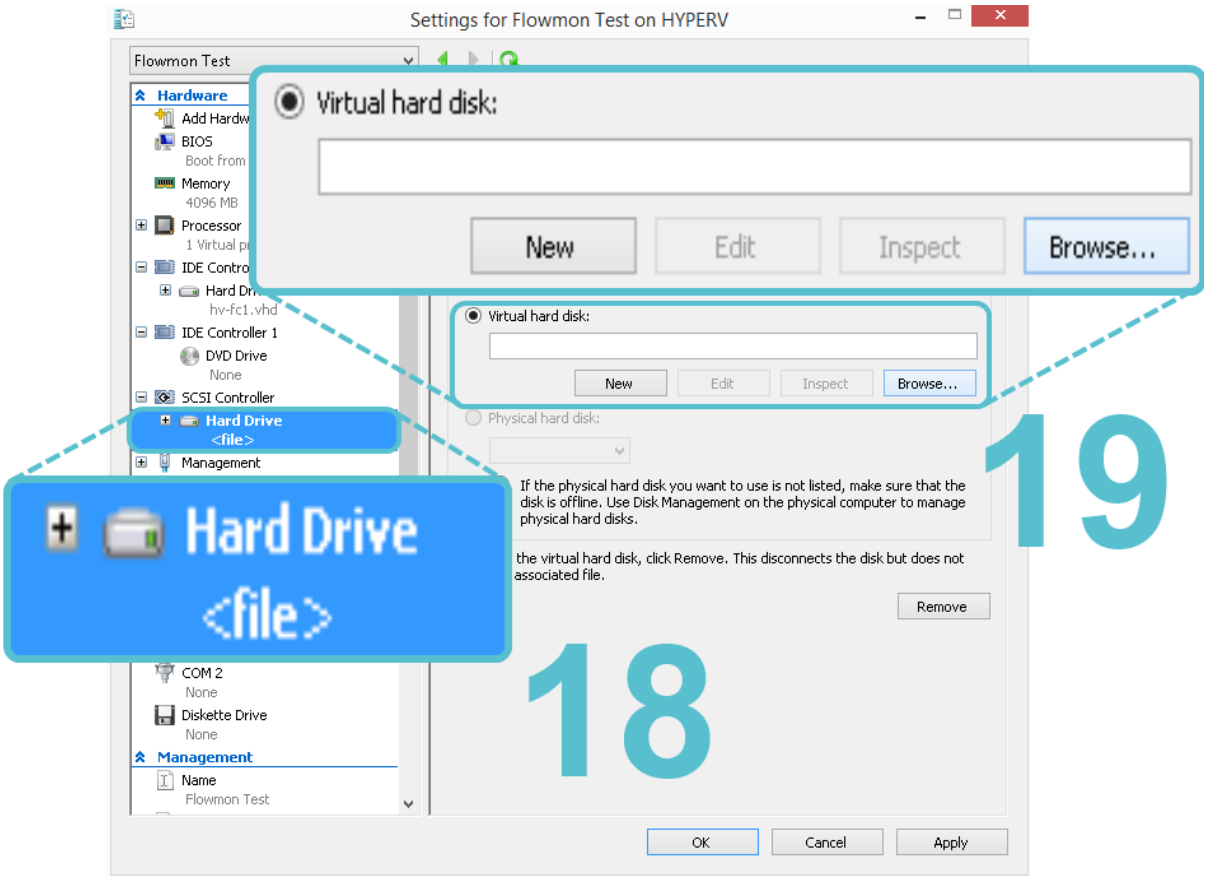
- For each new network adapter intended for monitoring, click on **Advanced Features** and select **Mirroring mode** as **Destination**.



- Add the second VHDX file as a hard drive to your SCSI controller. Select **SCSI Controller**, select **Hard Drive** and click on the **Add** button.



- Click on the newly created **Hard Drive** and select path to the second VHDX file.



Flowmon Configuration

Please refer to Post-installation Steps.

Hyper-V Network Interface Mirroring

Overview

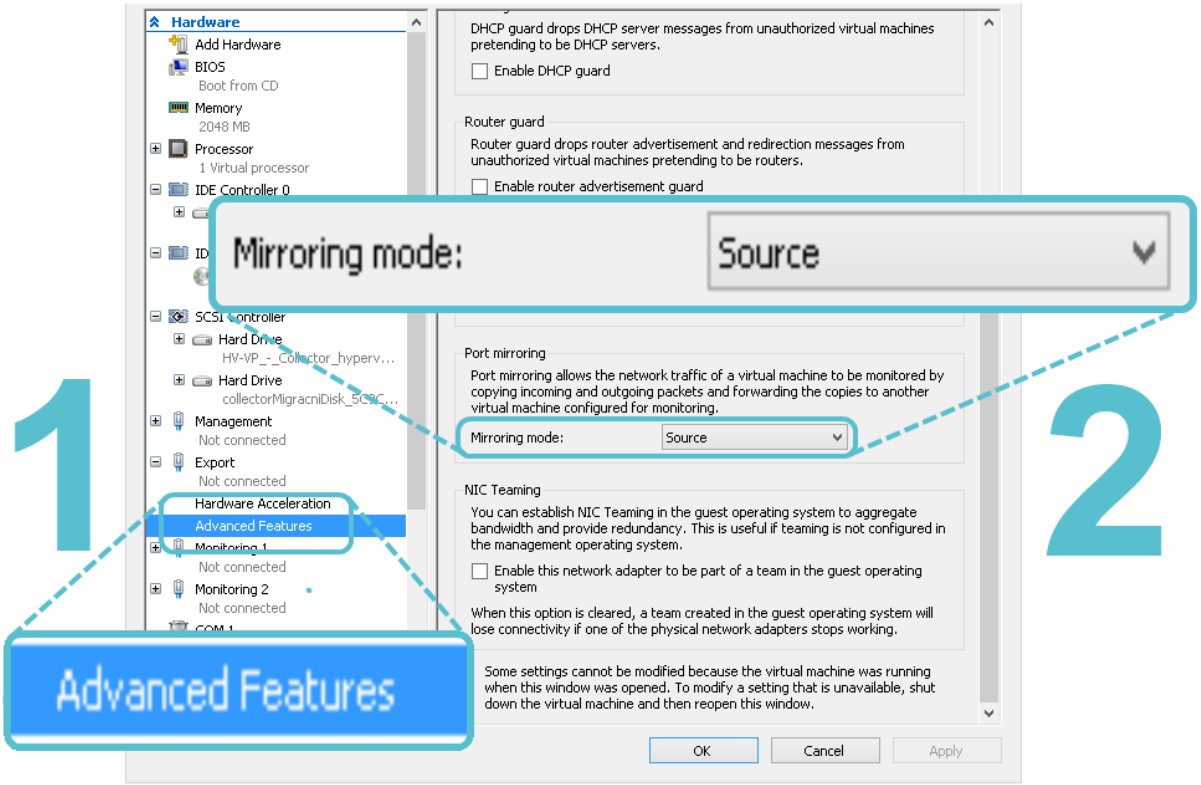
Flowmon for Hyper-V has the ability to monitor traffic and generate NetFlow / IPFIX flow data. To enable this functionality for the monitoring of network interfaces of virtual machines local to the Hyper-V host where Flowmon is running, please follow the steps outlined below.

Prerequisites

- A running instance of Flowmon for Hyper-V - Flowmon Collector (with a built-in Probe) or Flowmon Probe.

Deployment

- Right click on each virtual machine you would like to monitor and select **Settings**. For each selected network adapter click on **Advanced Features** and set **Mirroring mode** to **Source**. Keep in mind that your Flowmon's monitoring port must be attached to the same virtual switch as these network adapters.



- Make sure your Flowmon instance has **Mirroring mode** set to **Destination** and resides on the same virtual switch.

Optionally, if you intend to monitor VLAN traffic:

- **Connect** to the Hyper-V host hosting your Flowmon instance.

- Open **powershell** and rename all network adapters associated with your Flowmon instance. Adjust the number of interfaces, if necessary. Replace **NameOfCreatedVirtualMachine** with the name of your Flowmon instance in Hyper-V.

```
$VMNetAdap = Get-VMNetworkAdapter -VMName "NameOfCreatedVirtualMachine"
rename-VMNetworkAdapter -VMNetworkAdapter $VMNetAdap[0] -newname "Management 1"
rename-VMNetworkAdapter -VMNetworkAdapter $VMNetAdap[1] -newname "Management 2"
rename-VMNetworkAdapter -VMNetworkAdapter $VMNetAdap[2] -newname "Monitoring 1"
rename-VMNetworkAdapter -VMNetworkAdapter $VMNetAdap[3] -newname "Monitoring 2"
```

- For each monitoring interface that is intended for VLAN traffic monitoring, configure a **trunk**. Replace **NameOfCreatedVirtualMachine** with the name of your Flowmon instance in Hyper-V.

```
Set-VMNetworkAdapterVlan -Trunk -AllowedVlanIdList "1-4094" -VMName "NameOfCreatedVirtualMachine" -VMNetworkAdapterName "Monitoring 1" -NativeVlanId 0
Set-VMNetworkAdapterVlan -Trunk -AllowedVlanIdList "1-4094" -VMName "NameOfCreatedVirtualMachine" -VMNetworkAdapterName "Monitoring 2" -NativeVlanId 0
```

Flowmon Configuration

No configuration specific for Hyper-V network interface mirroring is necessary. See instructions on how to enable a monitoring port in the Flowmon User Guide.

Hyper-V Virtual Switch Port Monitoring

Overview

Flowmon for Hyper-V has the ability to monitor traffic and generate NetFlow / IPFIX flow data. To enable this functionality for the monitoring of a Virtual Switch local to the Hyper-V host where Flowmon is running, please follow the steps outlined below.

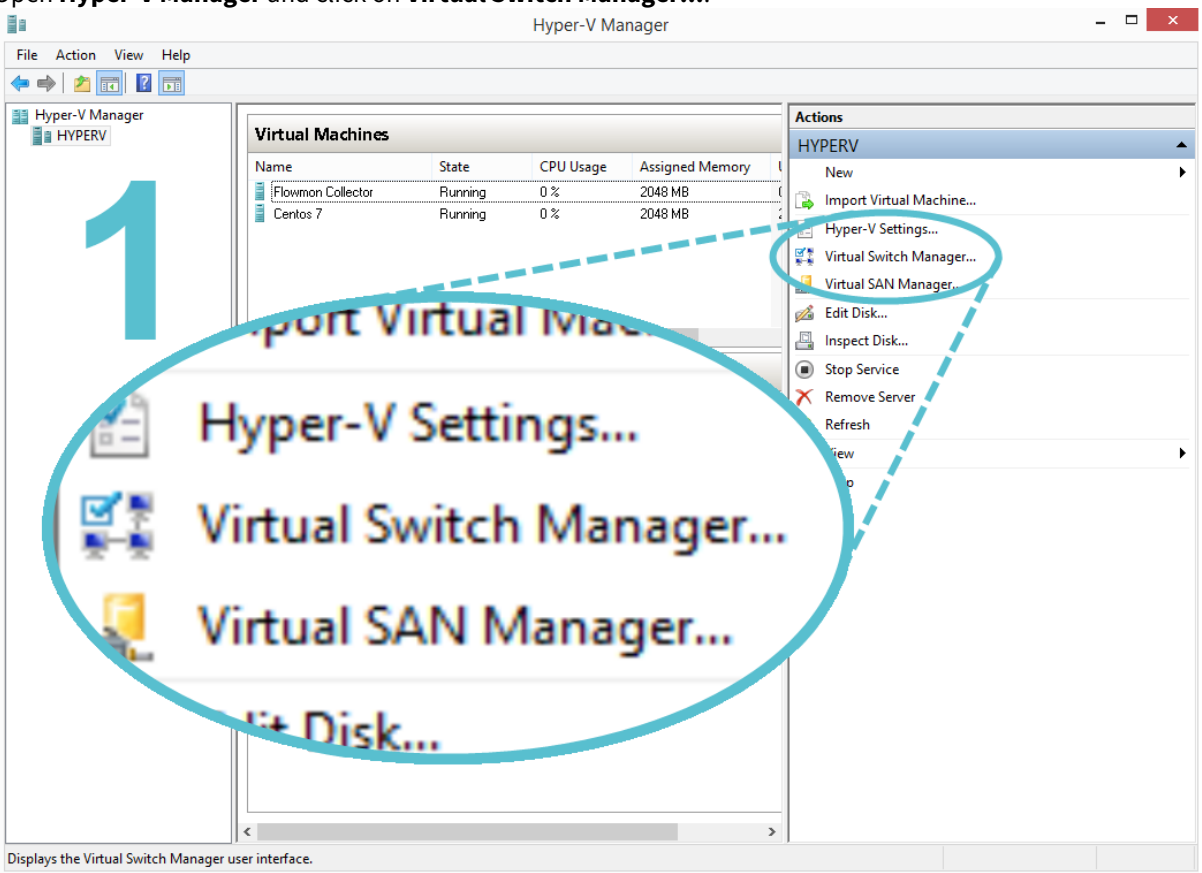
Prerequisites

- A running instance of Flowmon for Hyper-V - Flowmon Collector (with a built-in Probe) or Flowmon Probe.

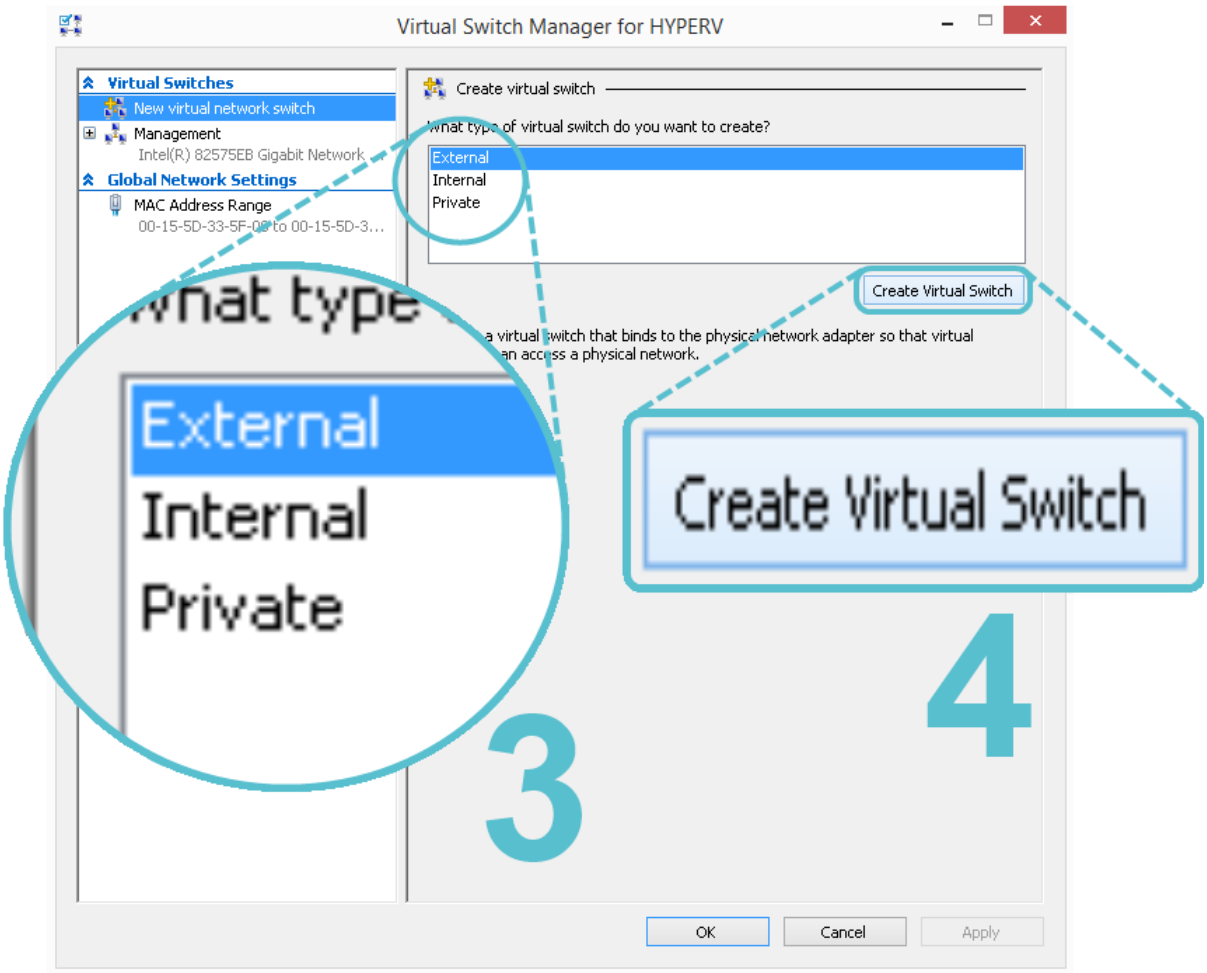
Deployment

In order to create a new Hyper-V Virtual Switch, you have to:

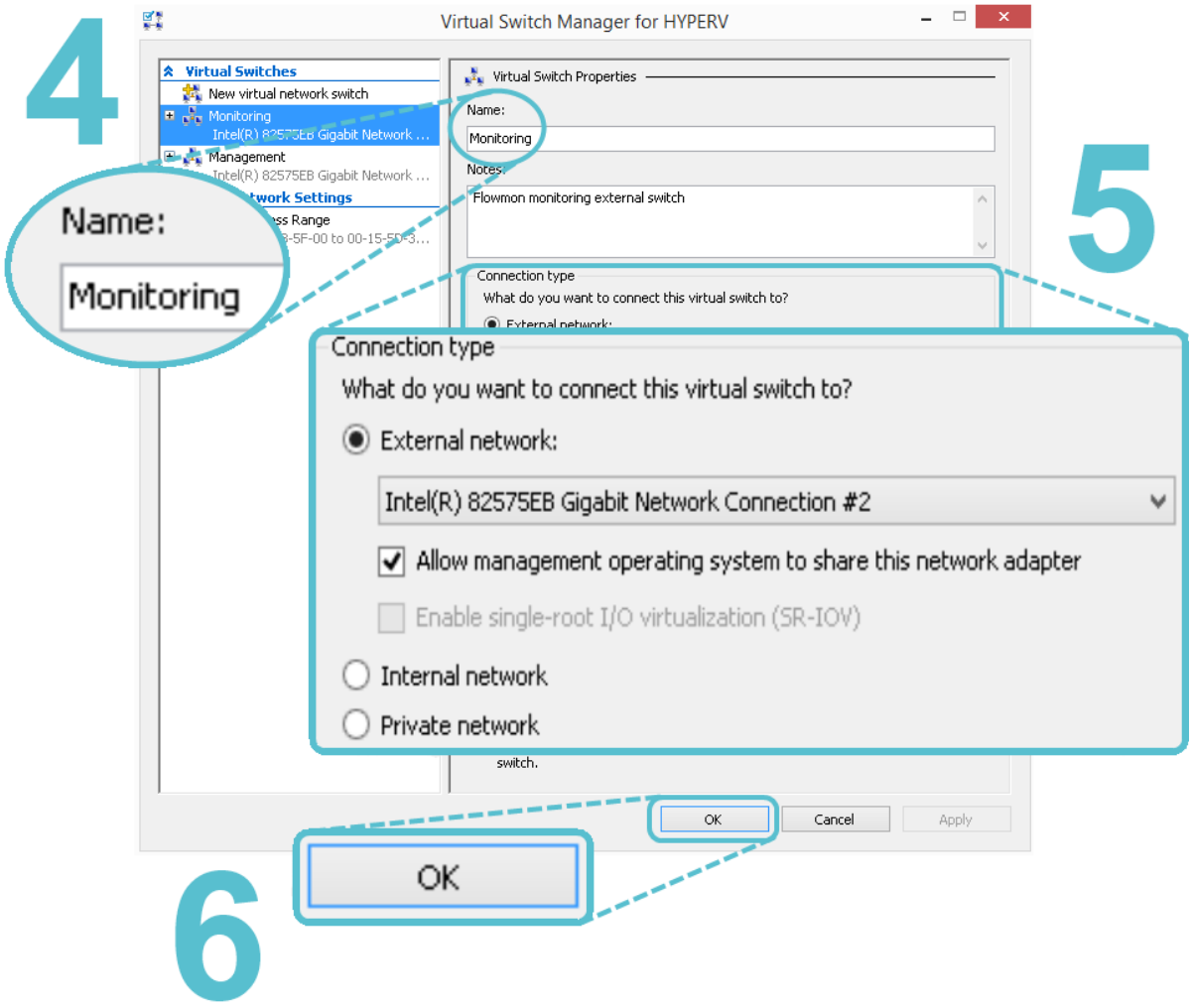
- Open **Hyper-V Manager** and click on **Virtual Switch Manager...**.



- Click on **Create Virtual Switch** and select switch type. External switch is bound to a physical interface, Internal or Private is not.



- Choose a name for the virtual switch and, if it is an external switch, select the appropriate **External** network and click on **OK**.



In order to monitor an existing Hyper-V Virtual Switch, you have to:

- **Connect** to the Hyper-V host.
- Open **powershell** and set up traffic mirroring to the virtual switch of your choice.
  Replace **NameOfCreatedSwitch** with the name of your virtual switch.
  This configuration will mirror all external traffic to any virtual interface marked with **Mirroring mode** - **Destination** connected to the same virtual switch.

```
$portFeature=Get-VMSystemSwitchExtensionPortFeature -FeatureName
"Ethernet Switch Port Security Settings"
$portFeature.SettingData.MonitorMode = 2

Add-VMSwitchExtensionPortFeature -ExternalPort -SwitchName
"NameOfCreatedSwitch" -VMSwitchExtensionFeature $portFeature
```

For internal or shared management switches, use the following.

```
$portFeature=Get-VMSystemSwitchExtensionPortFeature -FeatureName
"Ethernet Switch Port Security Settings"
$portFeature.SettingData.MonitorMode = 2


Add-VMSwitchExtensionPortFeature -ManagementOS
-VMSwitchExtensionFeature $portFeature
```

- Make sure your Flowmon instance is connected to this virtual switch and its monitoring interface is configured as a **Destination** for mirroring.

Optionally, if you intend to monitor VLAN traffic:

- **Connect** to the Hyper-V host.
- Open **powershell** and rename all network adapters associated with your Flowmon instance. Adjust the number of interfaces, if necessary. Replace **NameOfCreatedVirtualMachine** with the name of your Flowmon instance in Hyper-V.

```
$VMNetAdap = Get-VMNetworkAdapter -VMName
"NameOfCreatedVirtualMachine"
rename-VMNetworkAdapter -VMNetworkAdapter $VMNetAdap[0] -newname
"Management 1"
rename-VMNetworkAdapter -VMNetworkAdapter $VMNetAdap[1] -newname
"Management 2"
rename-VMNetworkAdapter -VMNetworkAdapter $VMNetAdap[2] -newname
"Monitoring 1"
rename-VMNetworkAdapter -VMNetworkAdapter $VMNetAdap[3] -newname
"Monitoring 2"
```

- For each monitoring interface that is intended for VLAN traffic monitoring, configure a **trunk**. Replace **NameOfCreatedVirtualMachine** with the name of your Flowmon instance in Hyper-V.

```
Set-VMNetworkAdapterVlan -Trunk -AllowedVlanIdList "1-4094" -VMName
"NameOfCreatedVirtualMachine" -VMNetworkAdapterName "Monitoring 1"
-NativeVlanId 0
Set-VMNetworkAdapterVlan -Trunk -AllowedVlanIdList "1-4094" -VMName
"NameOfCreatedVirtualMachine" -VMNetworkAdapterName "Monitoring 2"
-NativeVlanId 0
```

Flowmon Configuration

No configuration specific for Hyper-V Virtual Switch monitoring is necessary. See instructions on how to enable a monitoring port in the Flowmon User Guide.

Flowmon for AWS

Overview

Flowmon for AWS gives network administrators and security engineers insight into what is happening in their cloud infrastructure. Its powerful features can be used to gain control of bandwidth utilization, optimize network and application performance, reduce time to resolution during troubleshooting and keep the infrastructure protected against modern cyber-security threats.

Flowmon for AWS is

- published in the official AWS Marketplace,
- deployed in the form of an AWS Virtual Machine Instance,
- capable of collecting as well as generating flow data,
- suitable for cost optimization with dynamic instance resizing based on current/planned utilization.,
- fully under customer's control - including updates, backups, and configuration.

Flowmon for AWS supports

- native traffic mirroring with Amazon VPC Traffic Mirroring,
- ingestion of Amazon VPC Flow Logs,
- 3rd party vTAP solutions such as Garland Prisms, Ixia CloudLens, or Gigamon,
- ERSPAN/GRE traffic mirroring.

Features

Flowmon for AWS supports three modes of operation:

- Probe,
- Collector,
- Collector and Probe.

Flowmon Probe

In this mode, the virtual appliance acts as a Flowmon Probe. It accepts mirrored traffic on monitoring ports and exports flow data to at least one remote Flowmon Collector instance.

Supported traffic mirroring solutions:

- Amazon VPC Traffic Mirroring

Supported 3rd-party packet brokers:

- Ixia CloudLens
- Gigamon
- Garland Prisms

Flowmon Collector

In this mode, the virtual appliance acts as a Flowmon Collector and accepts supported flow formats from external probes, network devices, or Amazon VPC Flow Logs on management ports. For details on supported flow sources and formats, refer to the official Flowmon User Guide.

Flow sources specific to AWS:

- Amazon VPC Flow Logs

Flowmon Collector and Flowmon Probe

In this mode, the virtual appliance acts both as a Flowmon Probe and Flowmon Collector. Probe sends data to the locally running Collector. For details on configuration, refer to the official Flowmon User Guide.

Licensing

Flowmon for AWS is a virtual appliance with Bring-Your-Own-License (BYOL) and AWS Free Trial support.

With BYOL, you can apply for a Free Trial License at flowmon.com. We recommend this approach.

With AWS Free Trial, customers can try one instance of this appliance for 30 days. There will be no hourly software charges for that instance but AWS infrastructure charges will still apply. An AWS Free Trial will automatically convert to a paid hourly subscription upon expiration.

Select the licensing scheme appropriate for your use case and requirements. When in doubt, select the BYOL appliance and request a Free Trial License from flowmon.com.

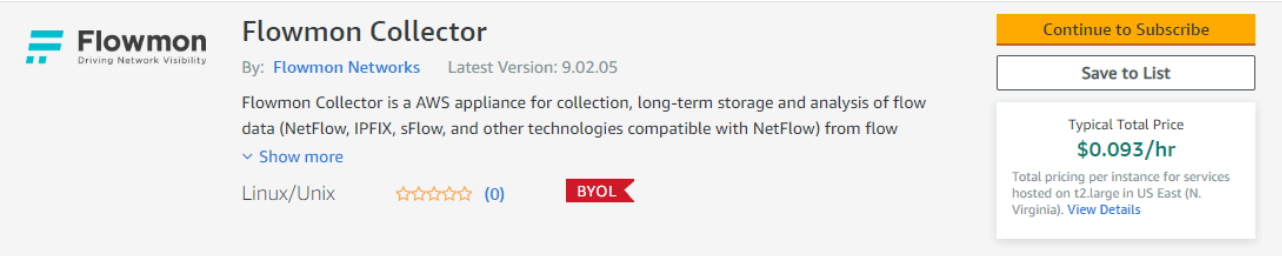
For support or inquiries, see our contact information.

AWS Marketplace

Flowmon for AWS is available as a Virtual Appliance (VA) in AWS Marketplace.

In order to deploy virtual machines instances based on this appliance, you have to **Subscribe** to it. Activating a subscription involves the following steps:

1. Sign in or create a new account at AWS Marketplace.
2. Select the appropriate version of Flowmon for AWS based on your requirements and licensing limitations. When in doubt, select the most recent version available with the BYOL licensing scheme.
3. Subscribe to the appliance to make it available for deployment.



Prerequisites

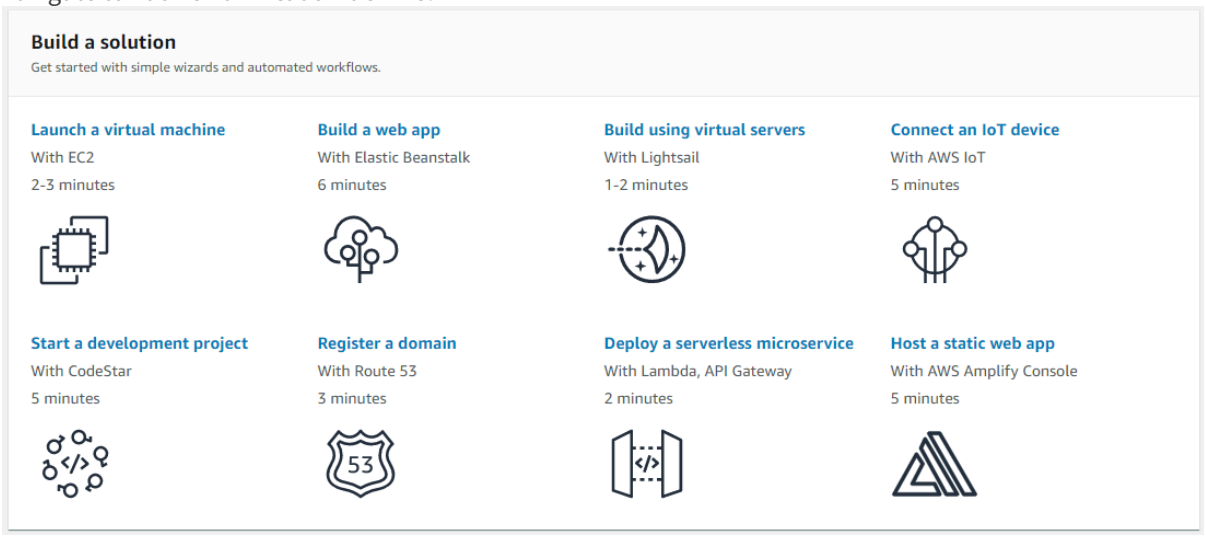
In order to follow this guide, you need the following:

1. A web browser compatible with the AWS Console.
2. A trial license from flowmon.com.
3. An active AWS user account with a subscription (free or paid). To properly evaluate all features of Flowmon for AWS, a paid subscription is required!

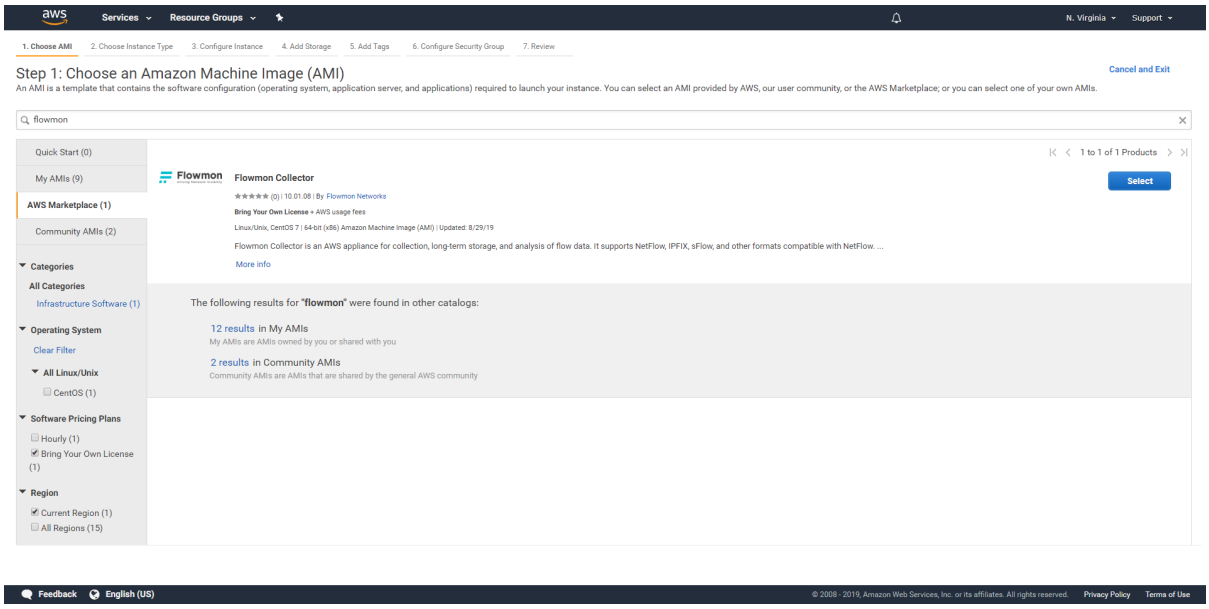
Deployment

The deployment of Flowmon for AWS consists of the following steps:

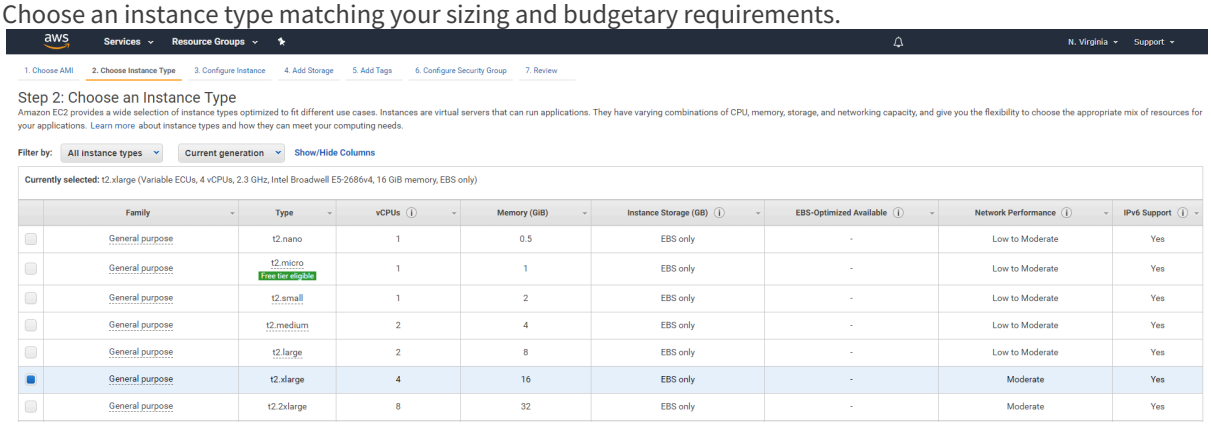
1. Log in to the AWS Console. Select a region appropriate for your deployment.
2. Navigate to **Launch a virtual machine**.



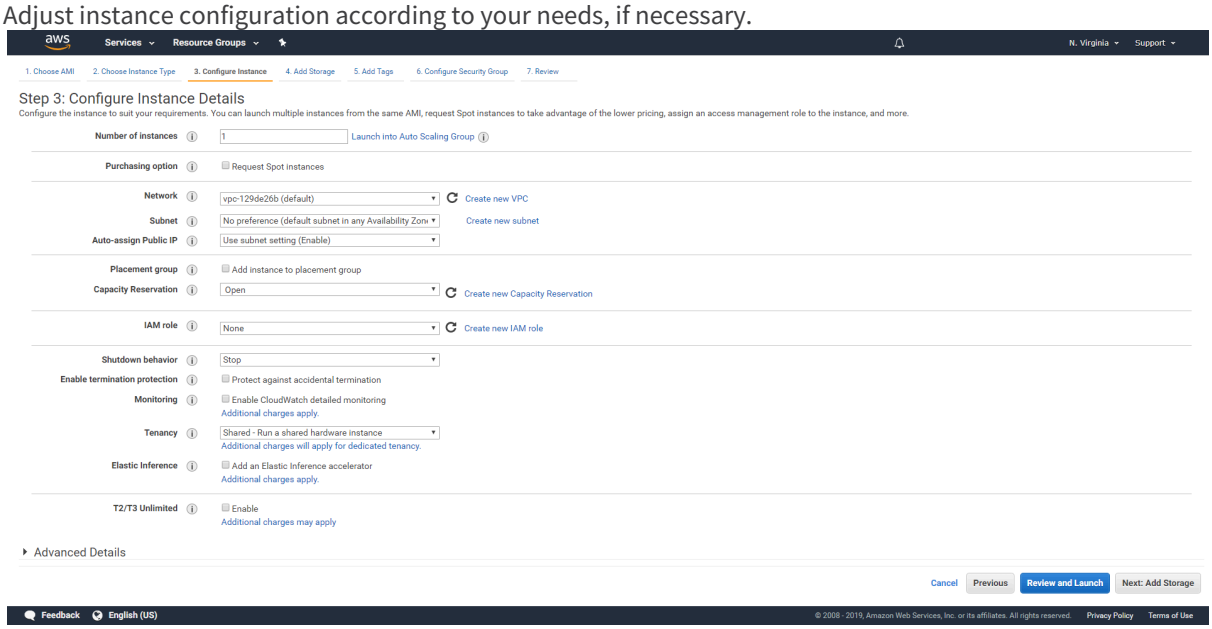
3. Switch to **AWS Marketplace** tab on the left. Search for "Flowmon", with **BYOL Software Pricing Plan**. **Select** an appliance. **Continue**.



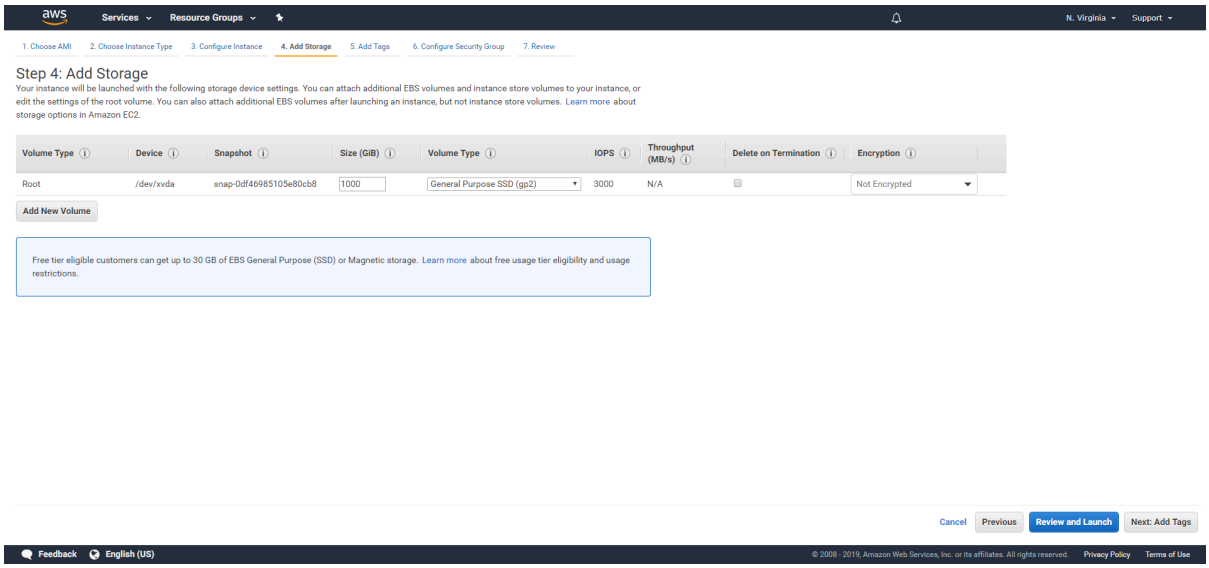
4. Choose an instance type matching your sizing and budgetary requirements.



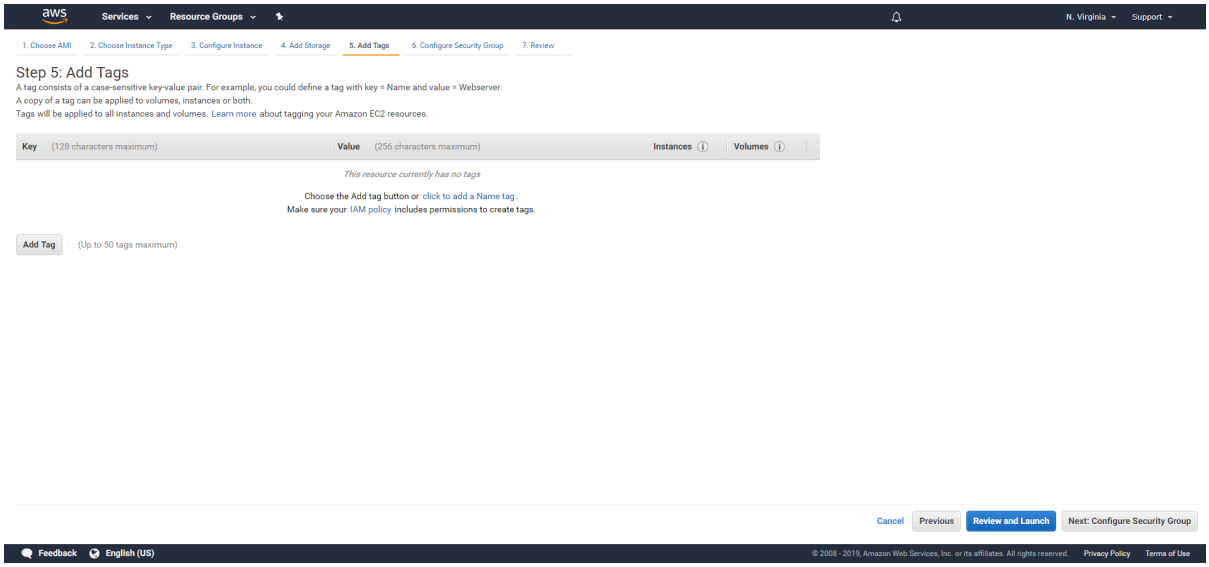
5. Adjust instance configuration according to your needs, if necessary.



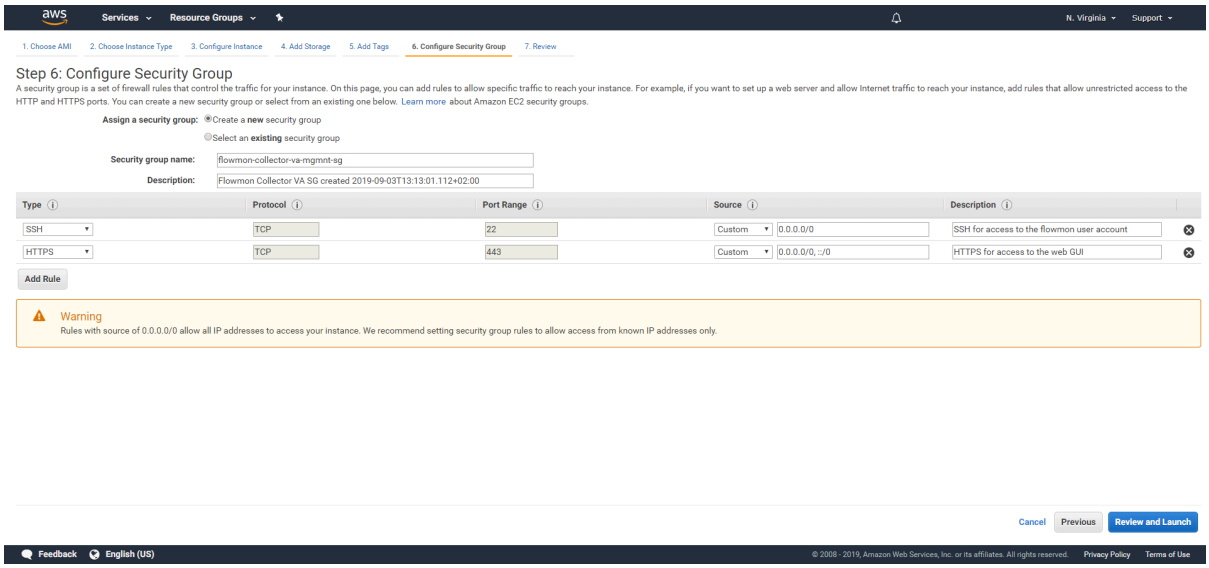
6. Add storage configuration. Make sure to uncheck disk deletion upon instance termination for a production-grade system!
   It is recommended to **add a separate data volume** matching the capacity allowed in your license. In any case, the volume **should not be smaller than 500 GB** for performance reasons.



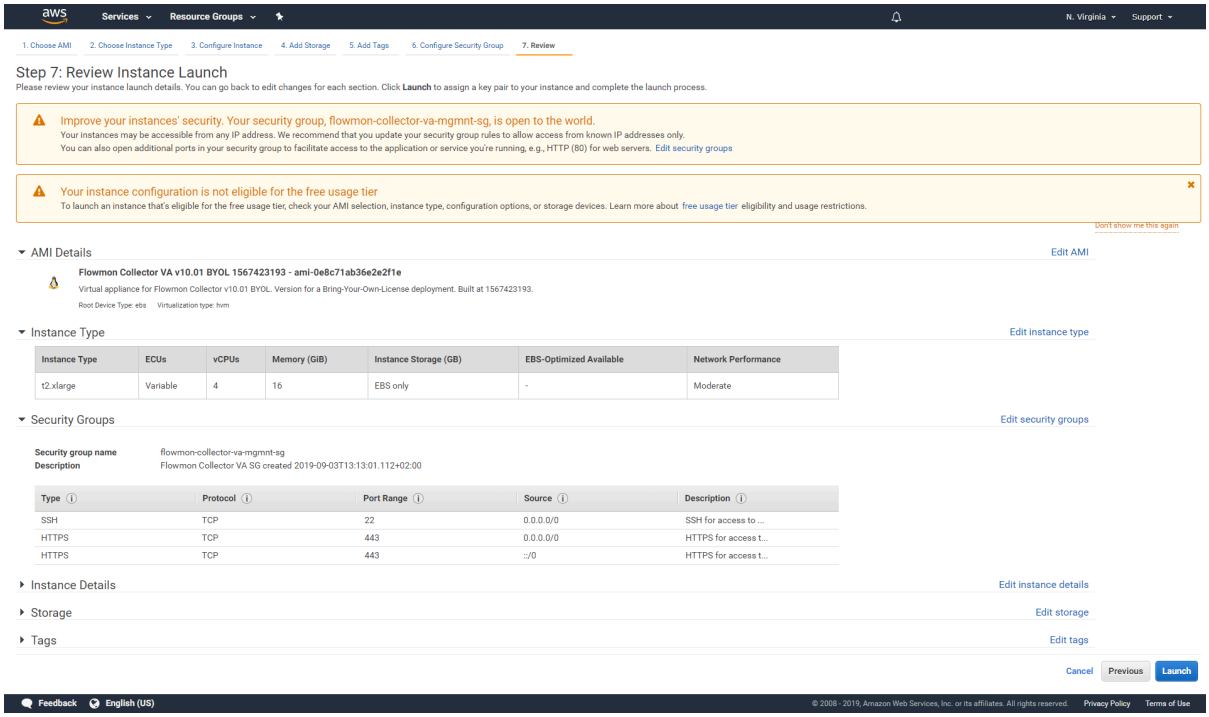
7. **Add tags**, if necessary. Tags may help you manage a larger number of instances or distinguish between similar instances.



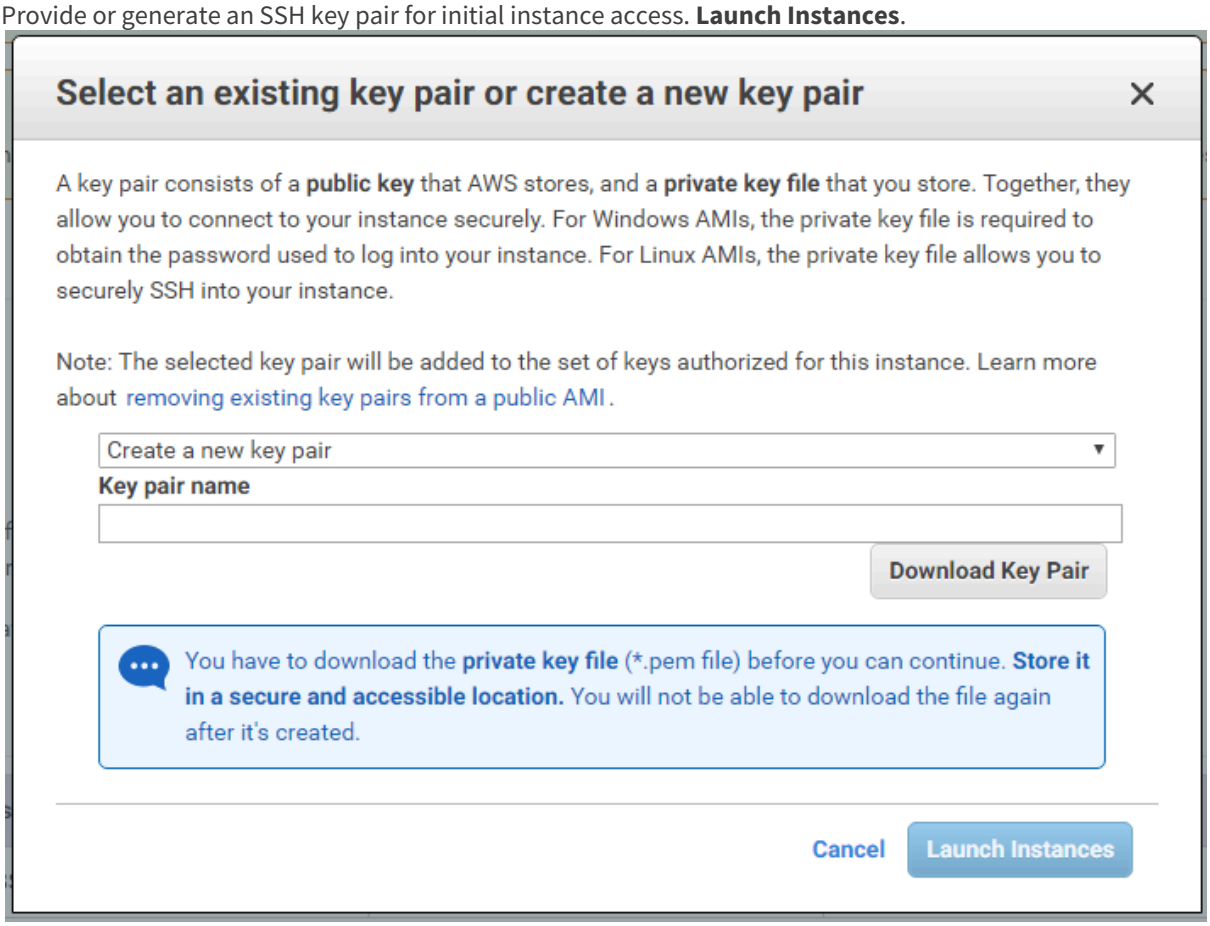
8. **Configure security group** rules. SSH and HTTP/HTTPS should be allowed from selected network segments. Here, consider adding ICMP rules to allow ping or TCP/UDP rules to allow connection to the Flowmon Collector listeners on specific ports.



9. **Review and Launch** the instance.



10. Provide or generate an SSH key pair for initial instance access. **Launch Instances**.

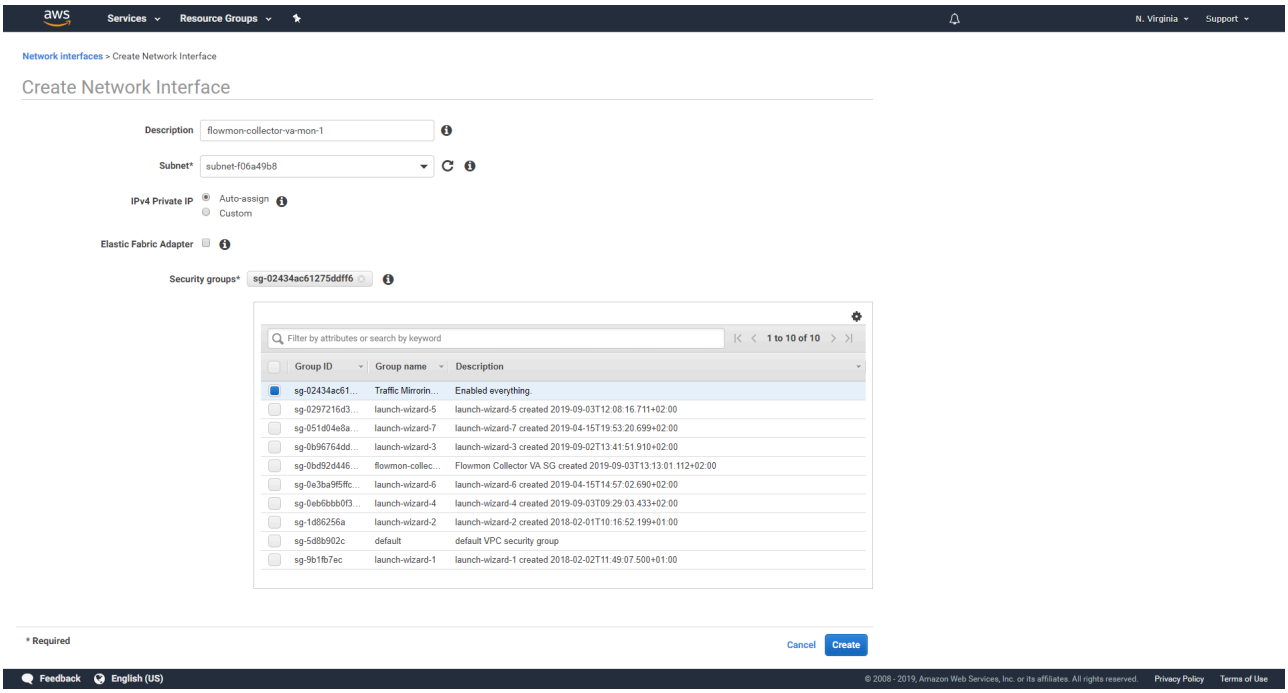


11. Wait for the launched instance to be **Running**.

Virtual Network Interfaces

By default, virtual machine instances in AWS EC2 are created with a single virtual network interface. In order to fully utilize the deployed appliance, to use it as a probe as well as a collector, you need to add at least one additional virtual network interface. In total, the appliance supports four virtual network interfaces, two for management and two for monitoring. The following steps outline the basic configuration, please, keep in mind that they may need to be adjusted for your deployment and use case.

Create a virtual network interface in the VPC and subnet used for traffic mirroring. This interface will be your **Mirror Target** when you configure Amazon VPC Traffic Mirroring. The security group should allow incoming **UDP** traffic on port **4789** from the mirrored subnet.



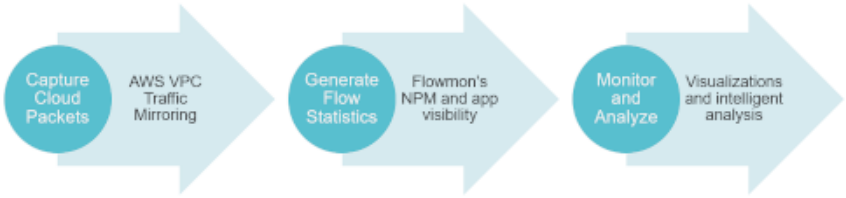
Flowmon Configuration

Please refer to Post-installation Steps.

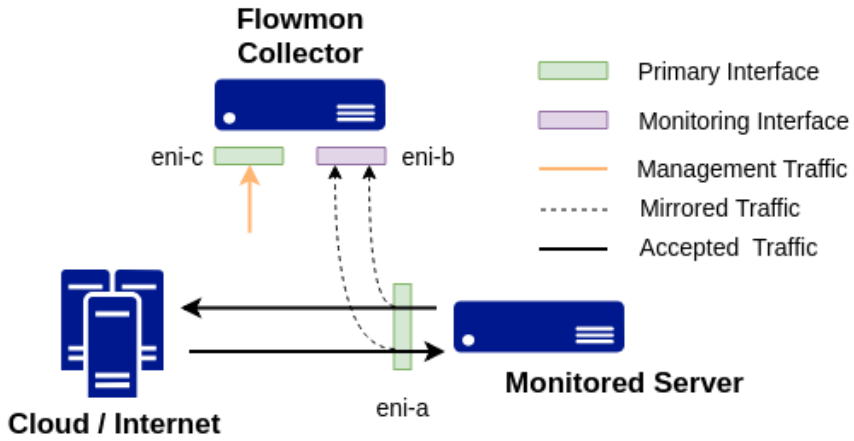
Amazon VPC Traffic Mirroring

Overview

Flowmon takes advantage of Amazon Virtual Public Cloud (Amazon VPC) traffic mirroring in AWS to help customers get an instant insight, to resolve network performance issues, identify optimization opportunities and secure infrastructure across different environments to support business-critical services.



The aim is to mirror the network traffic passing through a desired network interface (**eni-a** in the figure below) and send it to an interface where the mirrored traffic can be processed, visualized and analyzed with Flowmon Collector (**eni-b** in the figure below).



Utilization of AWS traffic mirroring in achieving network visibility with Flowmon Collector.

Prerequisites

1. A running instance of Flowmon for AWS.
2. A number of running client instances where traffic mirroring can be configured.
3. A deployment compliant with Traffic Mirroring Limits and Considerations.

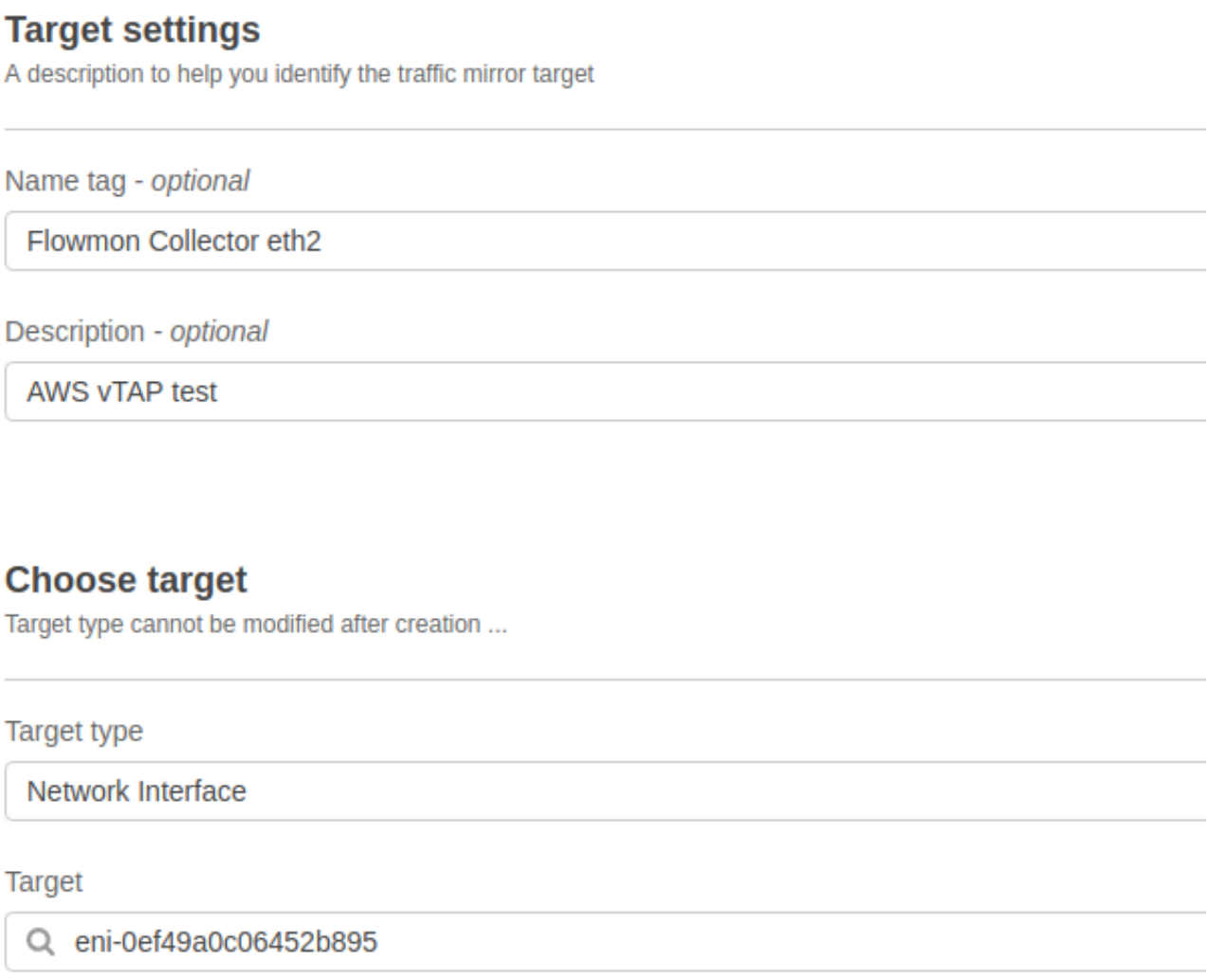
Deployment

In order to configure VPC traffic mirroring in AWS, you have to perform the following steps:

1. Create a **Traffic Mirror Target**
2. Create a **Traffic Mirror Filter**
3. Create a **Traffic Mirror Session**
4. Allow **VxLAN** traffic to collector

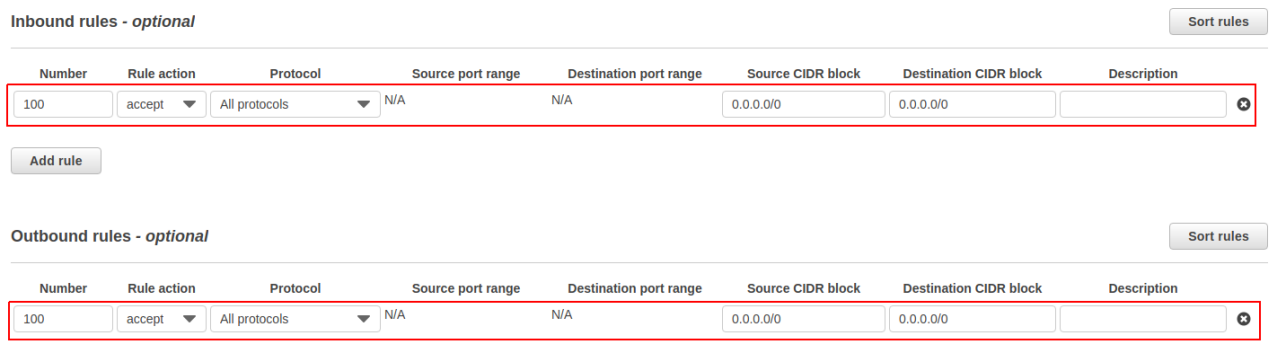
Create Traffic Mirror Target

1. In AWS Web Console, choose the **VPC** service.
2. Choose **Mirror Targets** in the **Traffic Mirroring** section.
3. Click on the **Create traffic mirror target** button.
4. Choose any name and description you want, but it is important that the **Target type** is **Network Interface** and the **Target** is Flowmon's monitoring interface.
5. Create the mirror target.



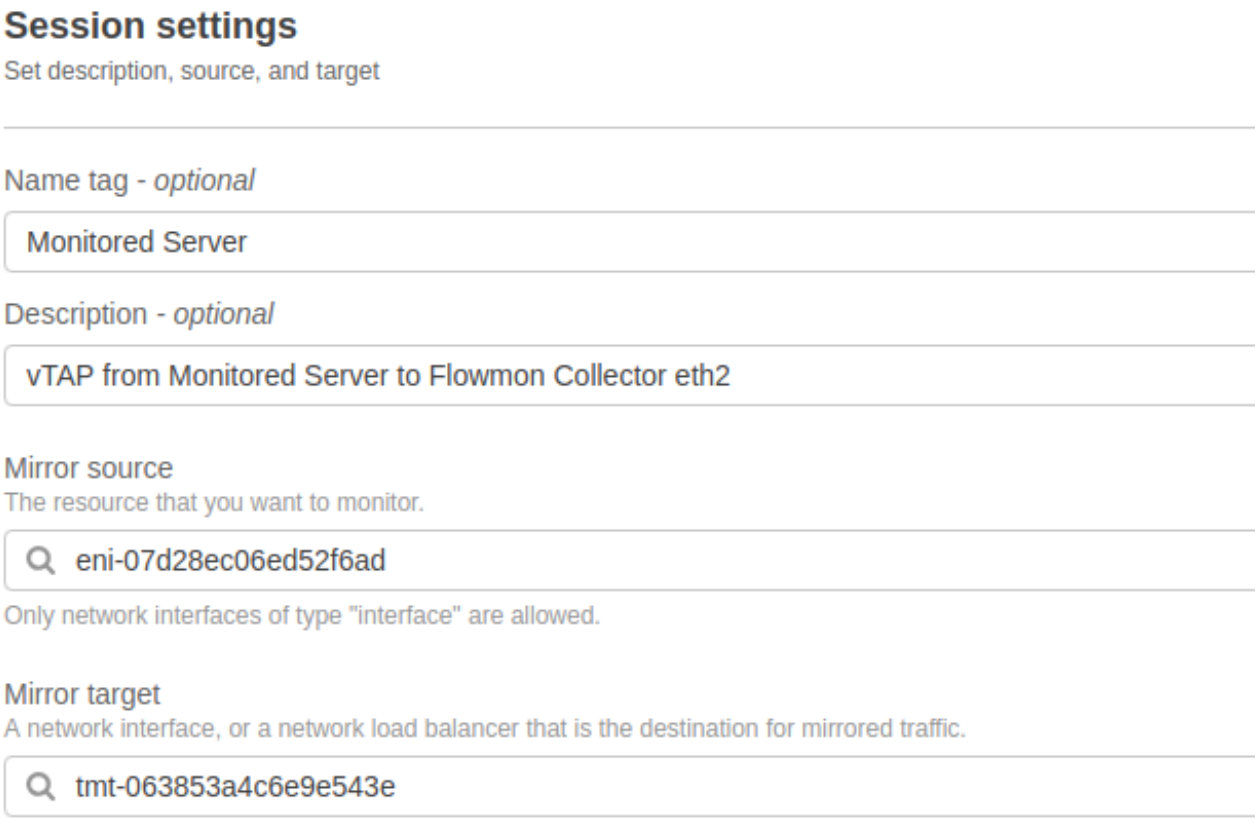
Create Traffic Mirror Filter

1. Choose **Mirror Filters** in the **Traffic Mirroring** section.
2. Click on the **Create traffic mirror filter** button.
3. Choose any name and description you want.
4. Describe the type of inbound and outbound traffic you want to be mirrored (all traffic, in our example in the picture below).
5. Create the mirror filter.



Create Traffic Mirror Session

1. Choose **Mirror Sessions** in the **Traffic Mirroring** section.
2. Click on the **Create traffic mirror session** button.
3. Choose any name and description you want.
4. Set virtual instance's port as the **Mirror source**.
5. Provide **Mirror target** and **Mirror filter** created in Steps 1 and 2.
6. Create the mirror session.

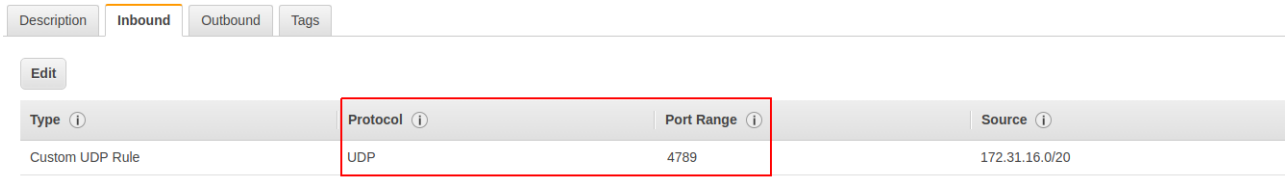


Allow VxLAN Traffic To Collector

All mirrored traffic is encapsulated with **VxLAN** protocol which works over **UDP** on port **4789**.

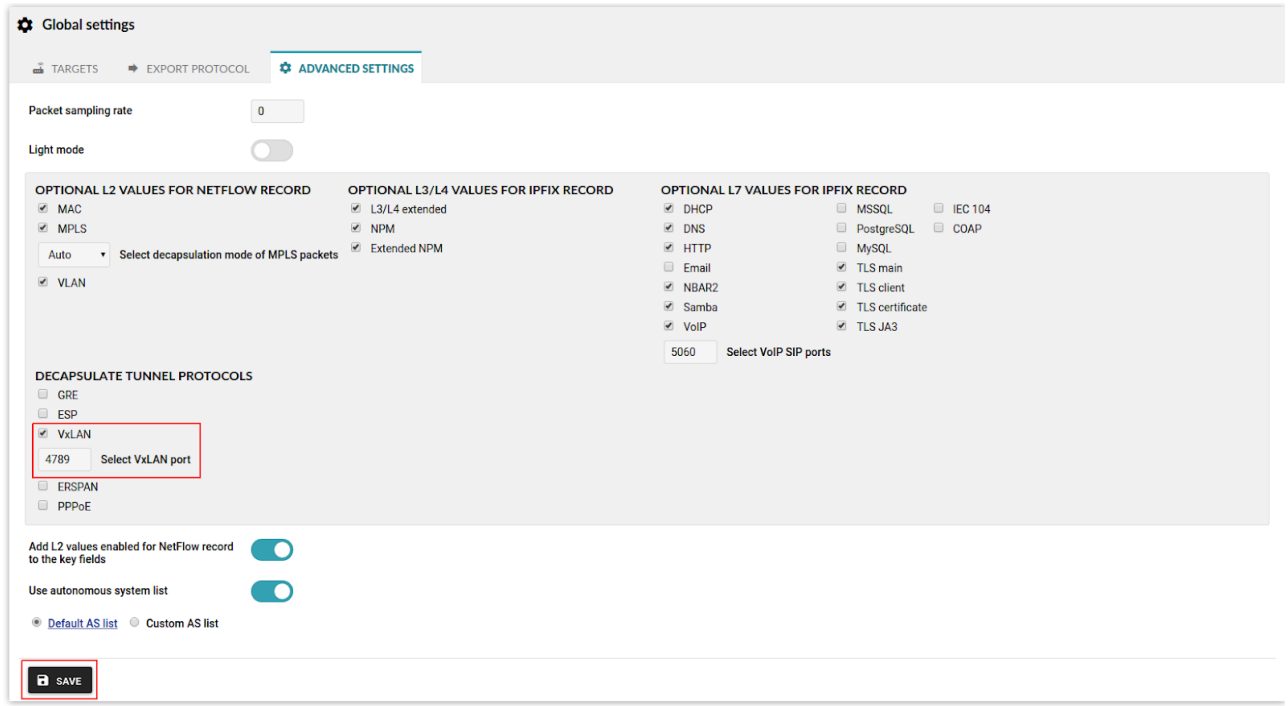
1. In AWS Web Console, choose the **EC2** service.
2. Find the **Security Group** applied to Flowmon's monitoring interface in the **Security groups** panel.
3. Add inbound rule to enable receiving VxLAN traffic from IP address of virtual instance's interface.

4. Save the inbound rule.



Flowmon Configuration

1. Go to **Flowmon Configuration Center** of your Flowmon Collector.
2. Choose the **Monitoring Ports** panel.
3. Under **Global settings -> Advanced settings** enable **VxLAN** decapsulation on port **4789**.
4. Click on the **Save** button.



Amazon VPC Flow Logs

Overview

The AWS FlowLog Converter is a configurable module of Flowmon Monitoring Center (FMC). It enables the user to collect, process and visualize AWS VPC Flow Logs (further referred to as flow logs) which contain information about the traffic captured in Amazon Virtual Private Cloud.

The flow logs are periodically acquired from Amazon CloudWatch, processed, converted to IPFIX format and subsequently sent to Flowmon Collector to a defined UDP port. Flowmon Collector treats data from this port as regular flows recovered from any other port.

Prerequisites

To set up the flow logs in your cloud and forward them to AWS CloudWatch, please follow the instructions specified in the official AWS Flow Logs documentation. It is important that every flow log stream contains flow logs from one interface only.

Deployment

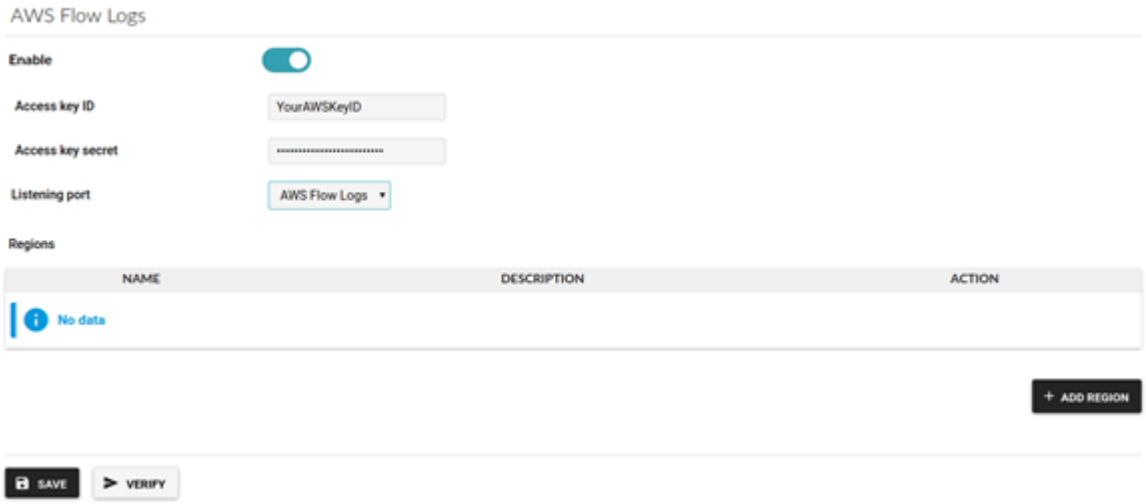
To start receiving flow logs in Flowmon Monitoring Center, follow these instructions.

First, configure the access information, regions and log groups from which the flow logs will be retrieved.

Configuration Center -> FMC Configuration -> AWS Flow Logs

The *access key ID* and the *secret access key* are mandatory credentials provided by Amazon.

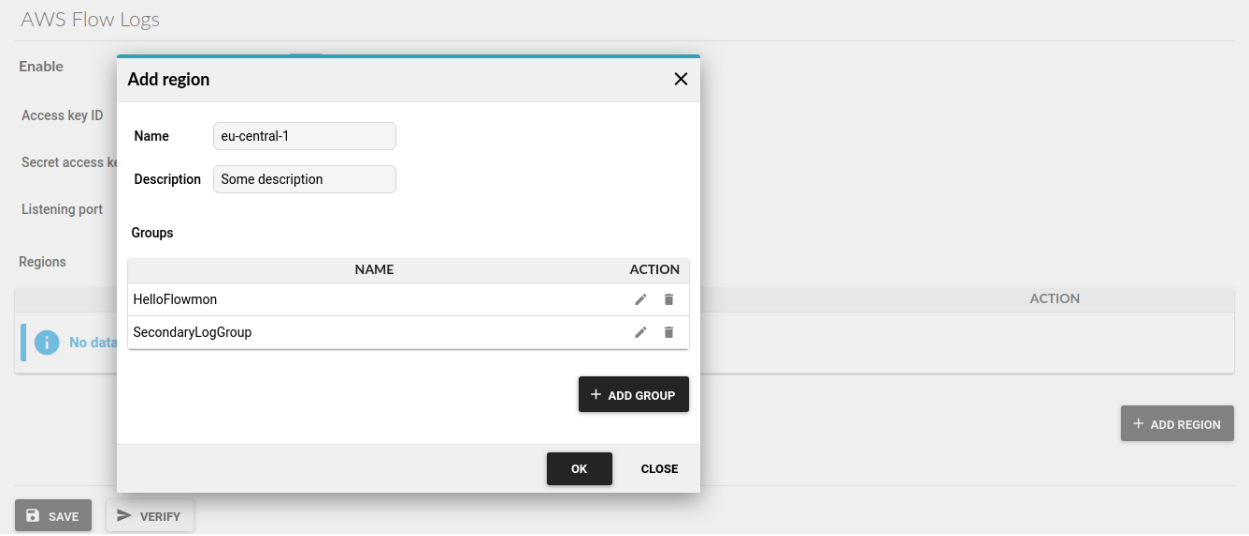
Select any suitable listening port, the port must accept **UDP** with flows in **IPFIX**.



Click the **Add Region** button to configure the endpoints where the flow logs should be retrieved.

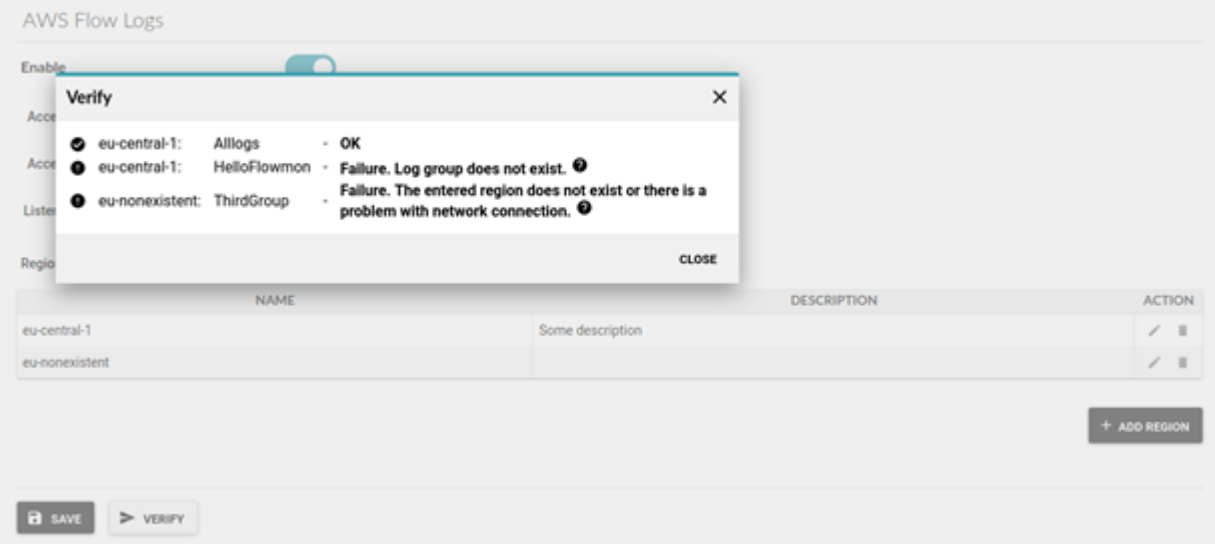
Insert the name of the region (without availability zone) in which your flow logs are physically stored. List of all possible regions can be found here. Note that the region **Name** field is expected to contain values like *eu-central-1* rather than *EU (Frankfurt).* It is also possible to define short description of the region.

Lastly, it is necessary to provide at least one log group (by clicking the **Add group** button and filling in the name). All flow log streams in the provided group will be processed and every stream will be shown as a unique interface of the log group in the **Monitoring Center**.



The provided configuration can be optionally verified by clicking the **Verify** button. This will check whether the FMC is able to connect to the specified log groups using the provided AWS credentials.

Note that the provided configuration undergoes the verification process every time the **Save** button is clicked.



Newly created configuration must be saved (by clicking the **Save** button). This will start the process of retrieving the Flow logs. To stop the process of retrieving, disable it and click the **Save** button.

Flowmon Configuration

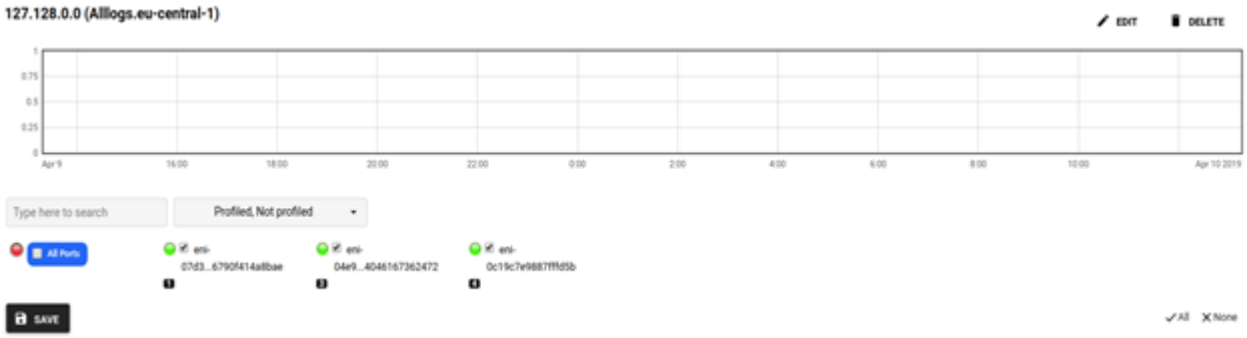
It can take up to 20 minutes (see Limitations) before first flow logs can be visualized.

Every log group has internally assigned a unique IP address (from subnet 127.128.0.0/16) and is treated as a unique flow source.

All sources can be found in **Flowmon Monitoring Center -> Sources.**

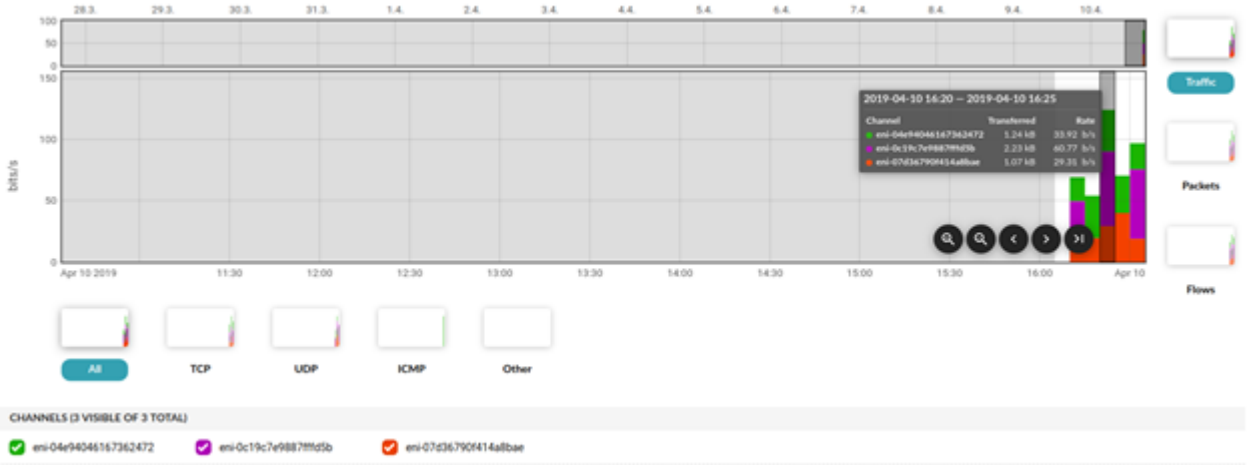
Click the **Profile** button to see traffic of the individual streams.

Select all available streams and click the **Save** button.



Switch to: **Flowmon Monitoring Center -> Profiles -> Sources -> *Your Log Group***

It is possible to view and analyze flows from flow logs as if they were flows from regular data sources.



Limitations

There are some limitations which stem from the flow logs themselves that need to be taken into account.

- If your network interface has multiple IPv4 addresses and traffic is sent to a secondary private IPv4 address, the flow log displays the primary private IPv4 address in the destination IP address field.
- If traffic is sent to an ENI and the destination is not any of the ENI IP addresses, the flow log displays the primary private IPv4 address in the destination IP address field.
- If traffic is sent from an ENI and the source is not any of the ENI IP addresses, the flow log displays the primary private IPv4 address in the source IP address field.
- If traffic is sent to or sent by a network interface, the flow log always displays the primary private IPv4 address, regardless of the packet source or destination, in the interface IP address field.

Flow logs do not capture all IP traffic. The following types of traffic are not logged:

- Traffic generated by instances when they contact the Amazon DNS server. If you use your own DNS server, then all traffic heading to that DNS server is logged.
- Traffic generated by a Windows instance for activation of the Amazon Windows license.
- Traffic to and from 169.254.169.254 for the instance metadata.
- Traffic to and from 169.254.169.123 for the Amazon Time Sync service.
- DHCP traffic.

- Traffic to the reserved IP address for the default VPC router. For more information, see VPC and Subnet Sizing.
- Traffic between an endpoint network interface and a Network Load Balancer network interface. For more information, see VPC Endpoint Services (AWS PrivateLink).
- Some flow log records might get skipped during the capture window. This may be because of an internal capacity constraint, or an internal error.

The delay between the time when the traffic actually occurred and the time it can be seen in Monitoring Center can reach up to 20 minutes in the worst case scenario, however; the delay will get smaller with a higher amount of traffic volume present in the monitored cloud. This is caused by the 10-15 minutes capture window in which the packets are aggregated to the flow logs before being published, and by the subsequent 5 minutes delay before Flowmon Collector closes the current profile and shows the traffic in the GUI.

Flowmon Collector stores incoming flows to a currently opened profile, and therefore it is advised to select multiple adjacent profiles when searching for flows in a particular time.

Flowmon for Azure

Overview

Flowmon for Azure gives network administrators and security engineers insight into what is happening in their cloud infrastructure. Its powerful features can be used to gain control of bandwidth utilization, optimize network and application performance, reduce time to resolution during troubleshooting and keep the infrastructure protected against modern cyber-security threats.

Flowmon for Azure is

- published in the official Azure Marketplace,
- deployed in the form of an Azure Virtual Machine Instance,
- capable of collecting as well as generating flow data,
- suitable for cost optimization with dynamic instance resizing based on current/planned utilization,
- fully under customer's control - including updates, backups, and configuration.

Flowmon for Azure supports

- native traffic mirroring with Azure Virtual Network TAP (in selected regions, as a preview),
- 3rd party vTAP solutions such as Garland Prisms, Ixia CloudLens, or Gigamon.

Features

Flowmon for Azure supports three modes of operation:

- Probe,
- Collector,
- Collector and Probe.

Flowmon Probe

In this mode, the virtual appliance acts as a Flowmon Probe. It accepts mirrored traffic on monitoring ports and exports flow data to at least one remote Flowmon Collector instance.

Supported traffic mirroring solutions:

- Azure Virtual Network TAP

Supported 3rd-party packet brokers:

- Ixia CloudLens
- Gigamon
- Garland Prisms

Flowmon Collector

In this mode, the virtual appliance acts as a Flowmon Collector and accepts supported flow formats from external probes, network devices on management ports. For details on supported flow sources and formats, refer to the official Flowmon User Guide.

Flowmon Collector and Flowmon Probe

In this mode, the virtual appliance acts both as a Flowmon Probe and Flowmon Collector. Probe sends data to the locally available Collector. For details on configuration, refer to the official Flowmon User Guide.

Licensing

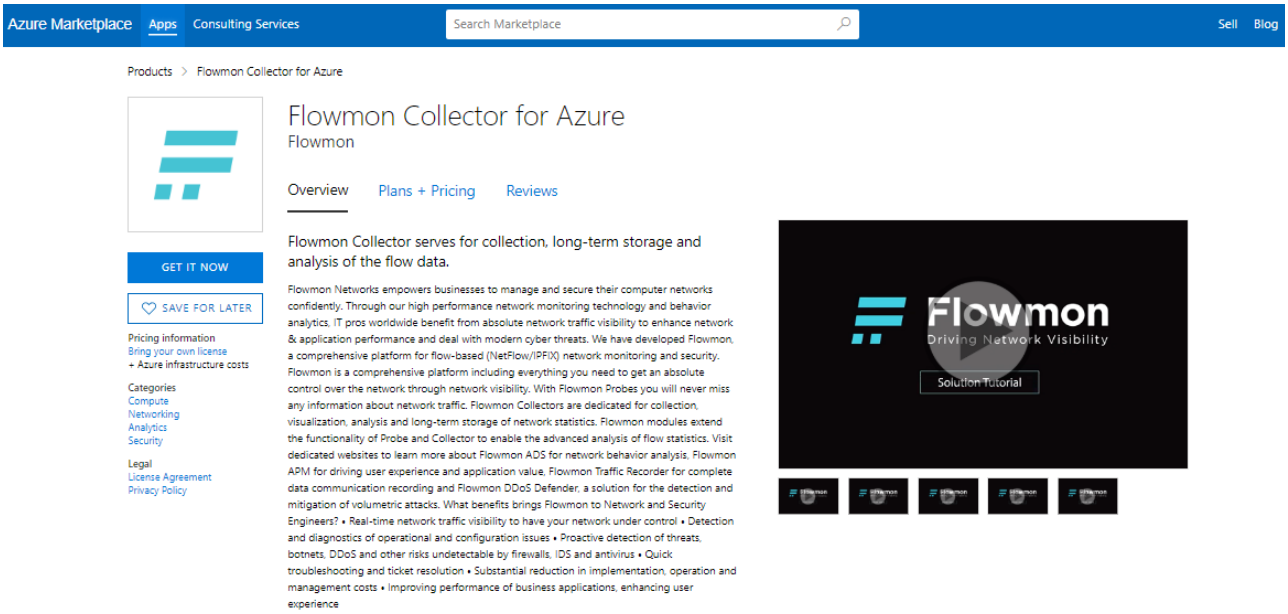
Flowmon for Azure is a virtual appliance with a Bring-Your-Own-License (BYOL) support.

With BYOL, you can apply for a Free Trial License at flowmon.com.

For support or inquiries, see our contact information.

Azure Marketplace

Flowmon for Azure is available as a Virtual Appliance (VA) in Azure Marketplace.



Prerequisites

In order to follow this guide, you need the following:

1. A web browser compatible with the Azure Portal.
2. A trial license from flowmon.com.
3. An active Azure user account with a subscription (free or paid).

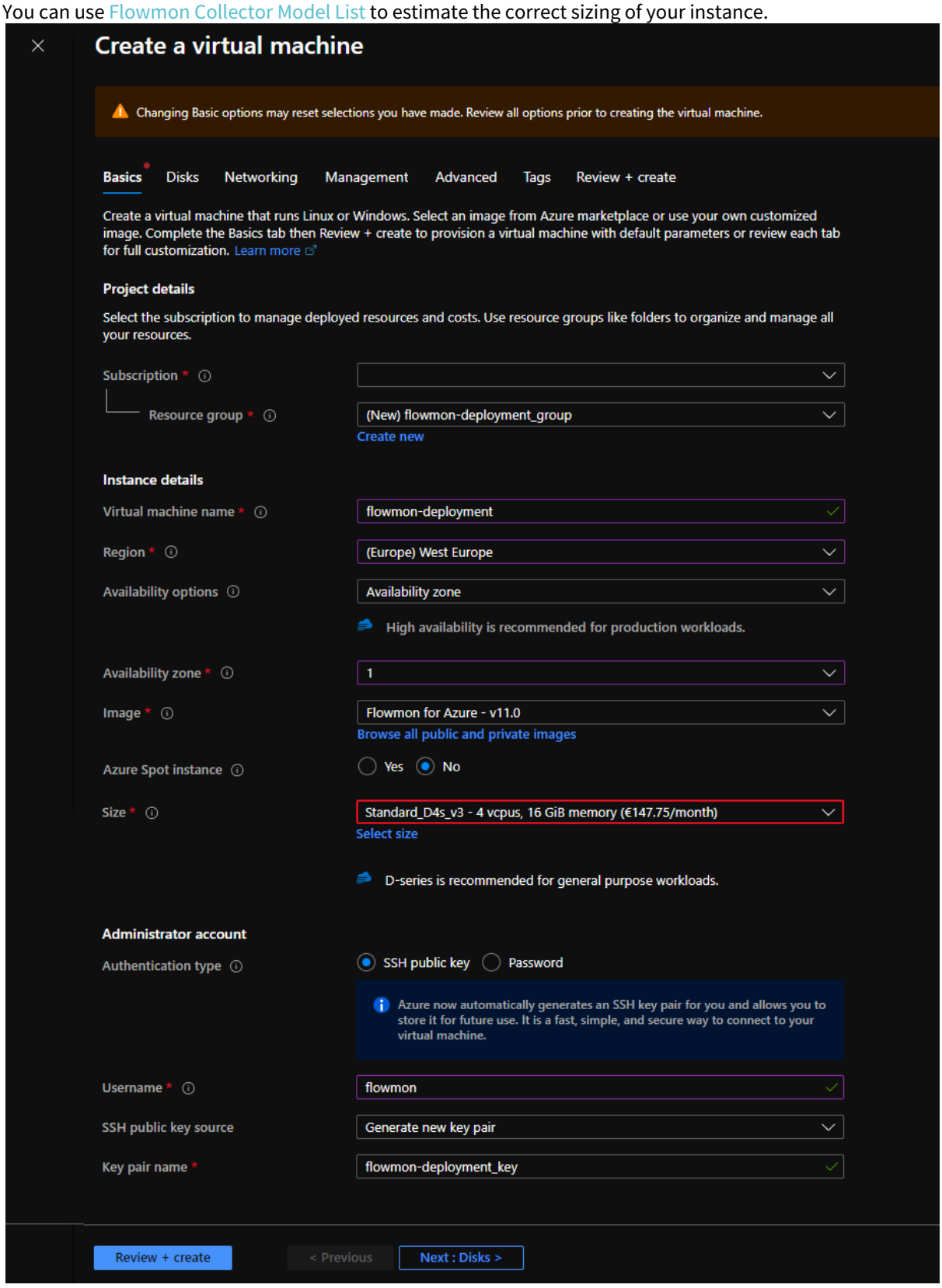
Deployment

The deployment of Flowmon for Azure consists of the following steps:

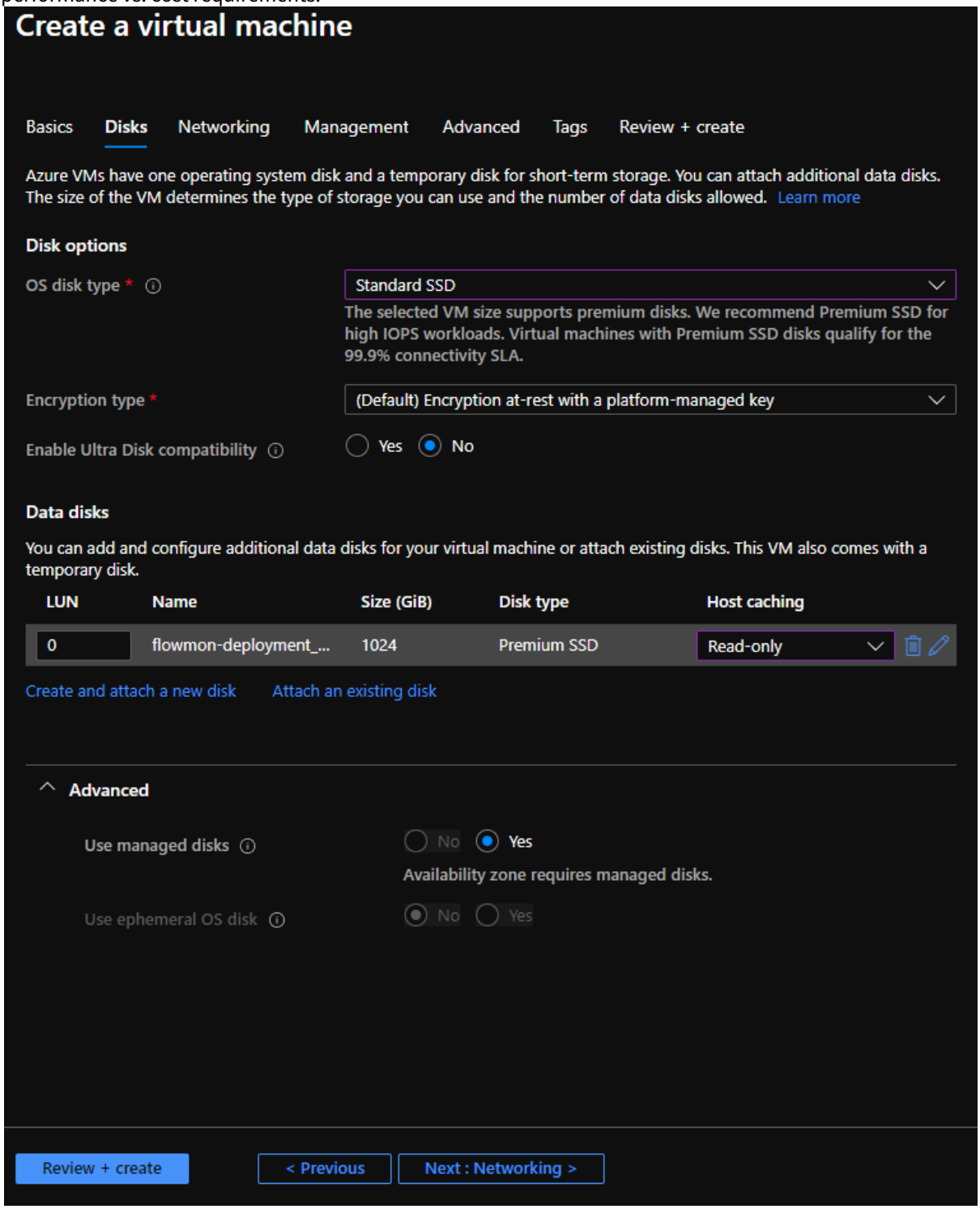
1. Log in to the Azure Portal.

2. Navigate to the Azure Marketplace page for Flowmon.
3. **Get It Now!**
4. **Continue** with the deployment in the Azure Portal.
5. **Create** a virtual machine instance.
6. Provide mandatory information such as **Virtual machine name**, **Resource group**, **SSH key** for the **flowmon** user account, etc.

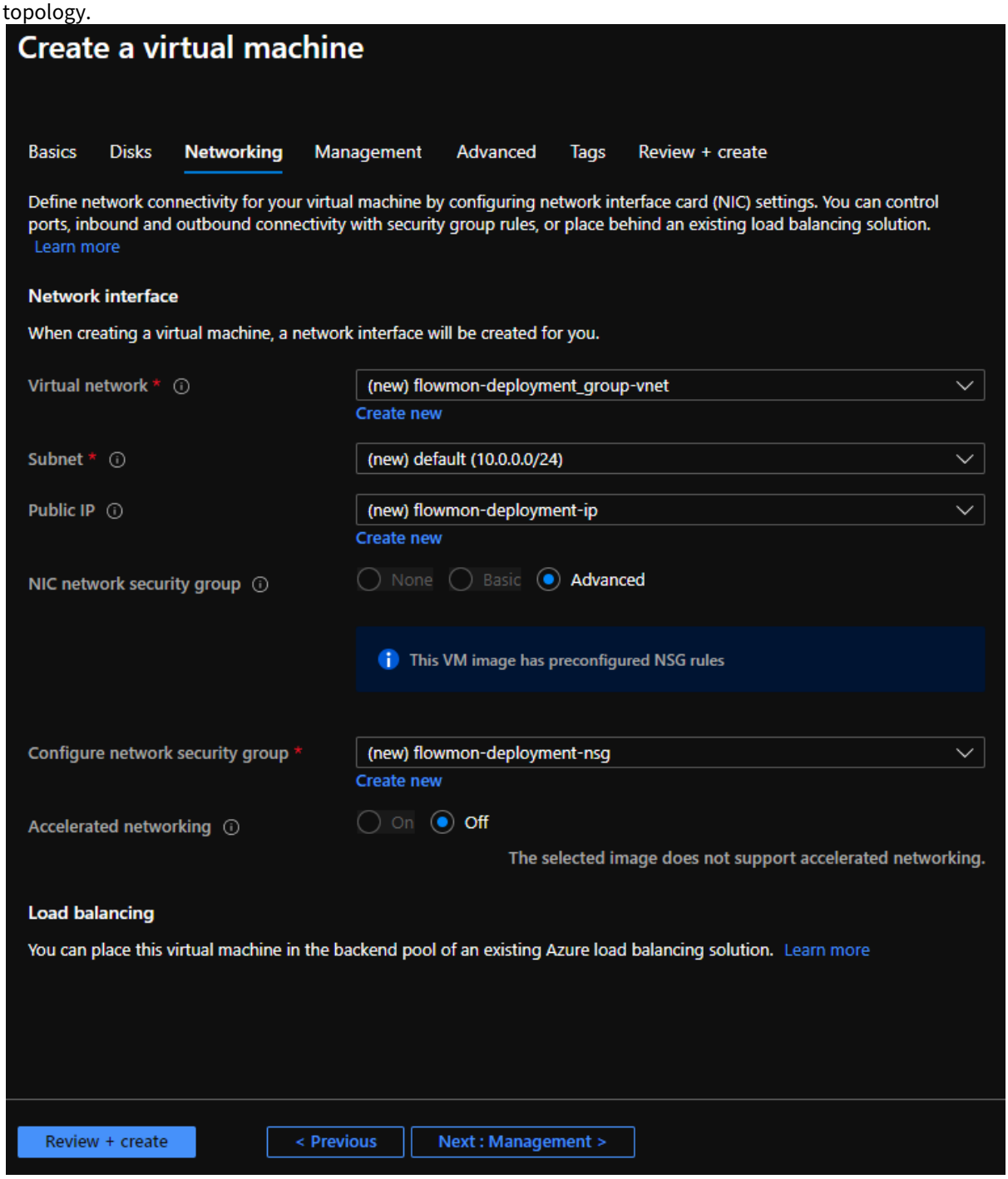
You can use Flowmon Collector Model List to estimate the correct sizing of your instance.



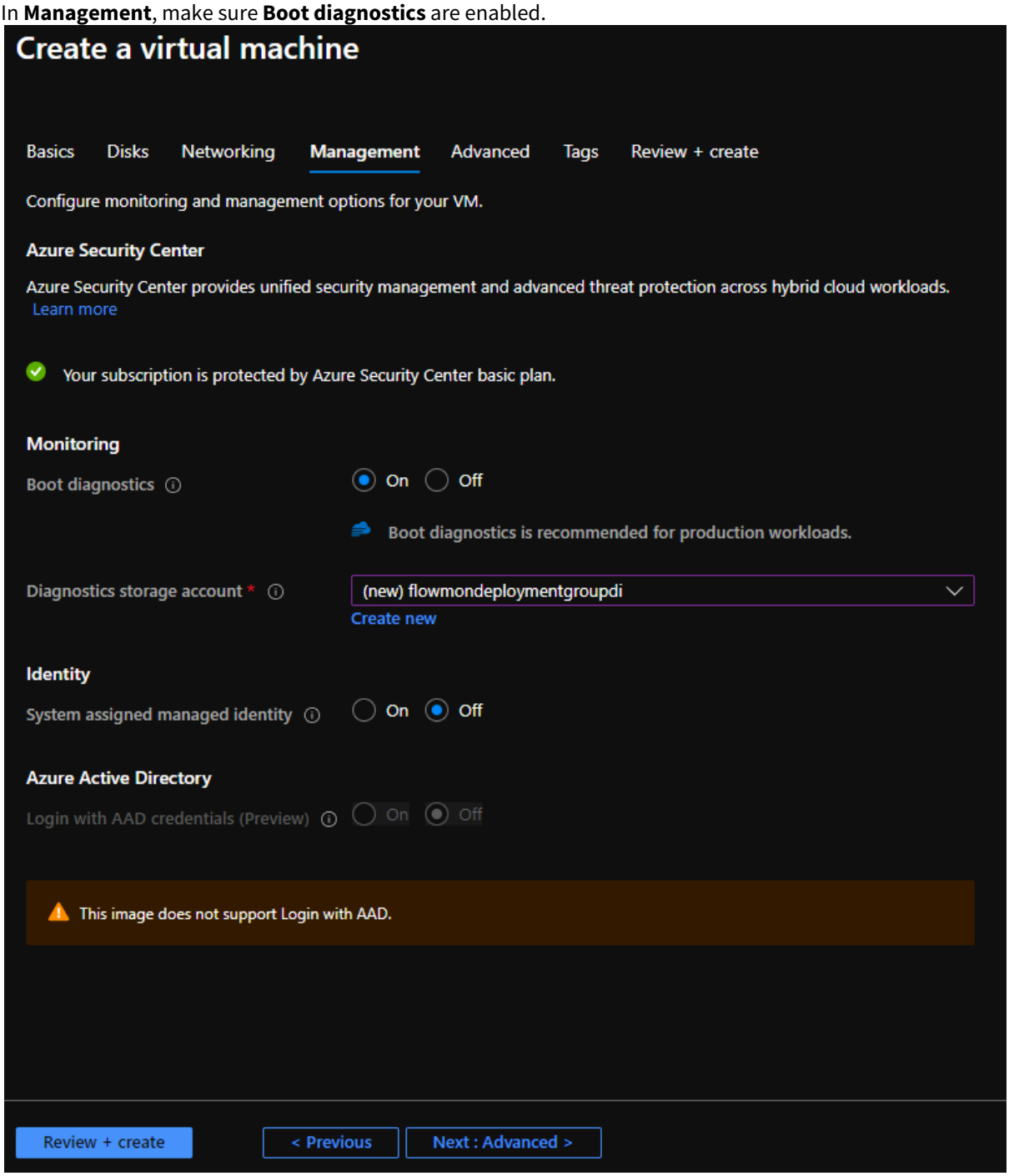
7. In **Disks**, add an additional block device to serve as data storage. Select disk types suitable for your performance vs. cost requirements.



8. In **Networking**, review network interface settings and adjust them based on the specifics of your network topology.

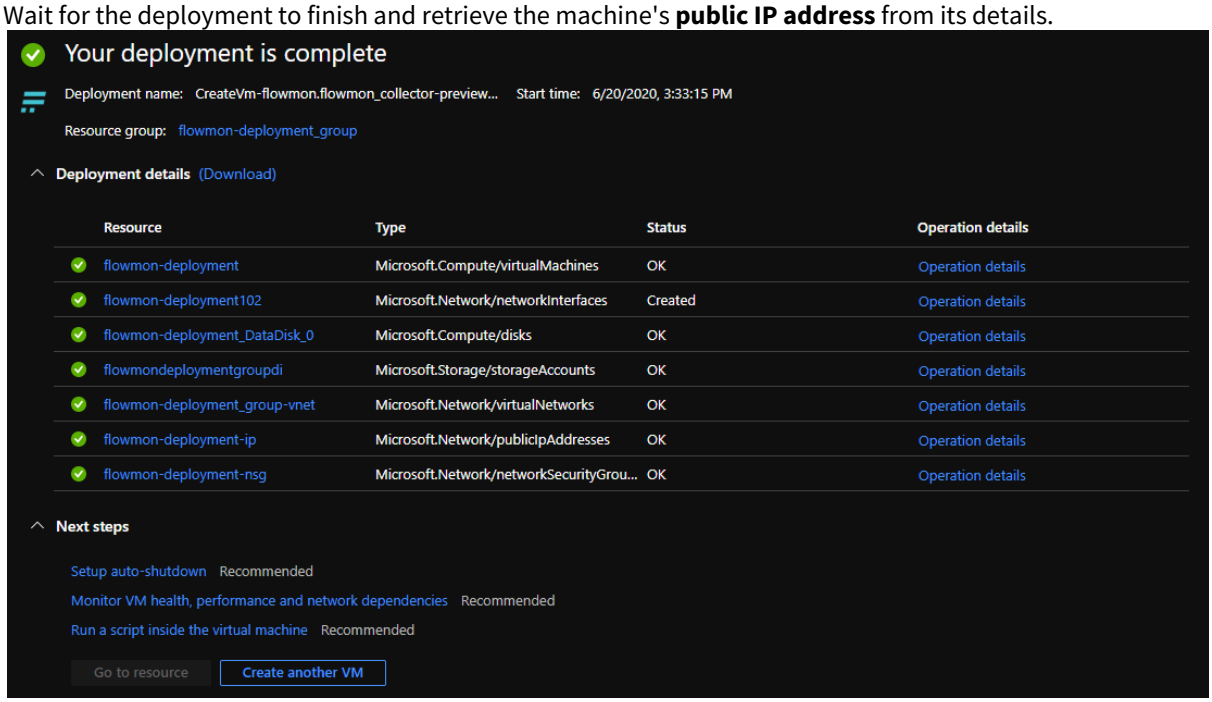


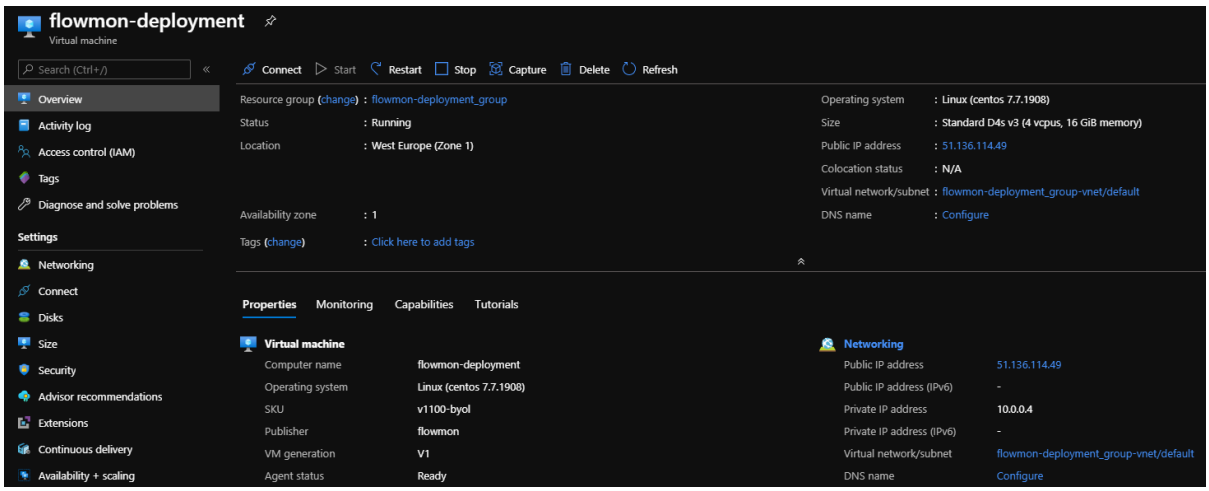
9. In **Management**, make sure **Boot diagnostics** are enabled.



10. **Review + create** the new instance.

11. Wait for the deployment to finish and retrieve the machine's **public IP address** from its details.



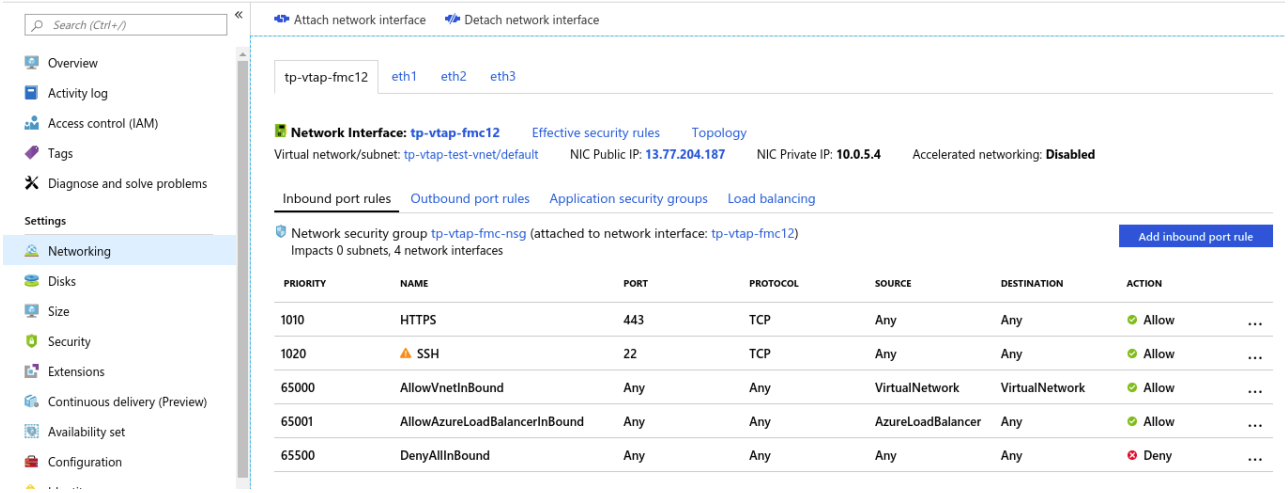


12. If you need to use this instance as Flowmon Probe, please refer to the Virtual Network Interfaces section below.

Virtual Network Interfaces

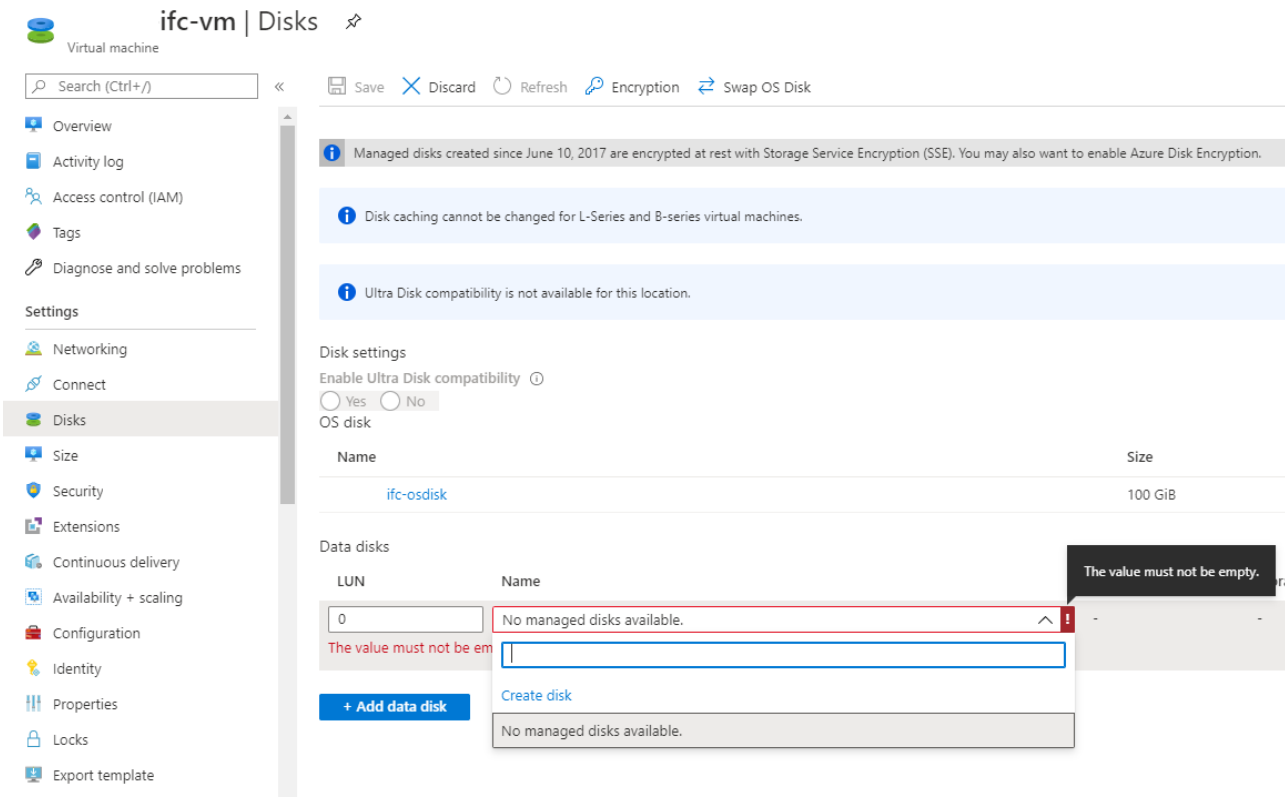
Once the new instance is running, you may provision additional monitoring interfaces (depending on your license). The most common configuration is **eth0** for management and **eth1/eth2** for monitoring.

Make sure to identify interfaces by MAC address inside the running instance, order and numbering may be different!



Virtual Disks

Once the new instance is running, you may provision additional data storage if you haven't already done that during the initial deployment process. It is recommended to store flow data on a disk other than the OS disk automatically provided with the instance. Adjust disk capacity based on your license.



Flowmon Configuration

Please refer to Post-installation Steps.

Azure Virtual Network TAP

The Azure Virtual Network TAP service preview is currently suspended by Microsoft and therefore unavailable for customer deployments.

Azure NSG Flow Logs v2

Azure NSG Flow Logs (v2) are currently not supported by Flowmon Collector.

Flowmon for Google Cloud

Overview

Flowmon for Google Cloud gives network administrators and security engineers insight into what is happening in their cloud infrastructure. Its powerful features can be used to gain control of bandwidth utilization, optimize network and application performance, reduce time to resolution during troubleshooting and keep the infrastructure protected against modern cyber-security threats.

Flowmon for Google Cloud is

- published in the official Google Cloud Marketplace,
- deployed in the form of a Google Cloud Compute Instance,
- capable of collecting as well as generating flow data,
- suitable for cost optimization with dynamic instance resizing based on current/planned utilization,
- fully under customer's control - including updates, backups, and configuration.

Flowmon for Google Cloud supports

- native traffic mirroring with VPC Packet Mirroring,
- 3rd party vTAP solutions such as Garland Prisms, Ixia CloudLens, or Gigamon.

Features

Flowmon for Google Cloud supports three modes of operation:

- Probe,
- Collector,
- Collector and Probe.

Flowmon Probe

In this mode, the virtual appliance acts as a Flowmon Probe. It accepts mirrored traffic on monitoring ports and exports flow data to at least one remote Flowmon Collector instance.

Supported traffic mirroring solutions:

- Google Cloud VPC Packet Mirroring

Support 3rd-party packet brokers:

- Ixia CloudLens
- Gigamon
- Garland Prisms

Flowmon Collector

In this mode, the virtual appliance acts as a Flowmon Collector and accepts supported flow formats from external probes, network devices on management ports. For details on supported flow sources and formats, refer to the official Flowmon User Guide.

Flowmon Collector and Flowmon Probe

In this mode, the virtual appliance acts both as a Flowmon Probe and Flowmon Collector. Probe sends data to the locally available Collector. For details on configuration, refer to the official Flowmon User Guide.

Licensing

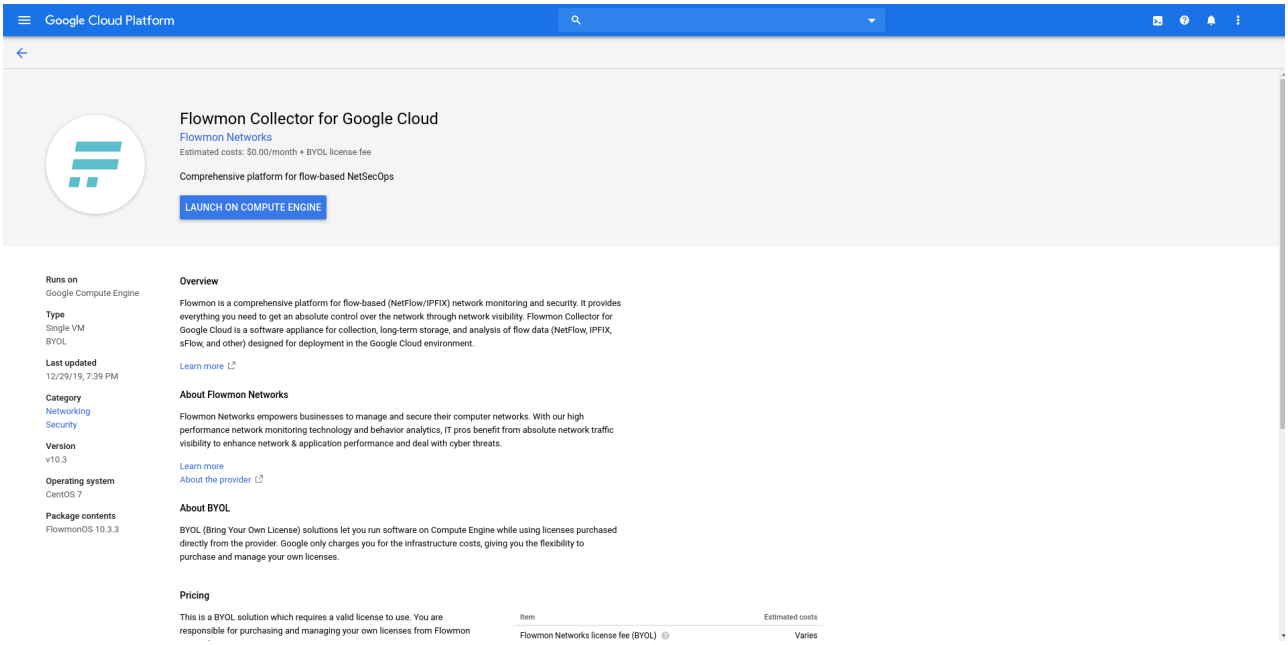
Flowmon for Google Cloud is a virtual appliance with a Bring-Your-Own-License (BYOL) support.

With BYOL, you can apply for a Free Trial License at flowmon.com.

For support or inquiries, see our contact information.

Google Cloud Marketplace

Flowmon for Google Cloud is available as a Virtual Appliance (VA) in Google Cloud Marketplace.



Prerequisites

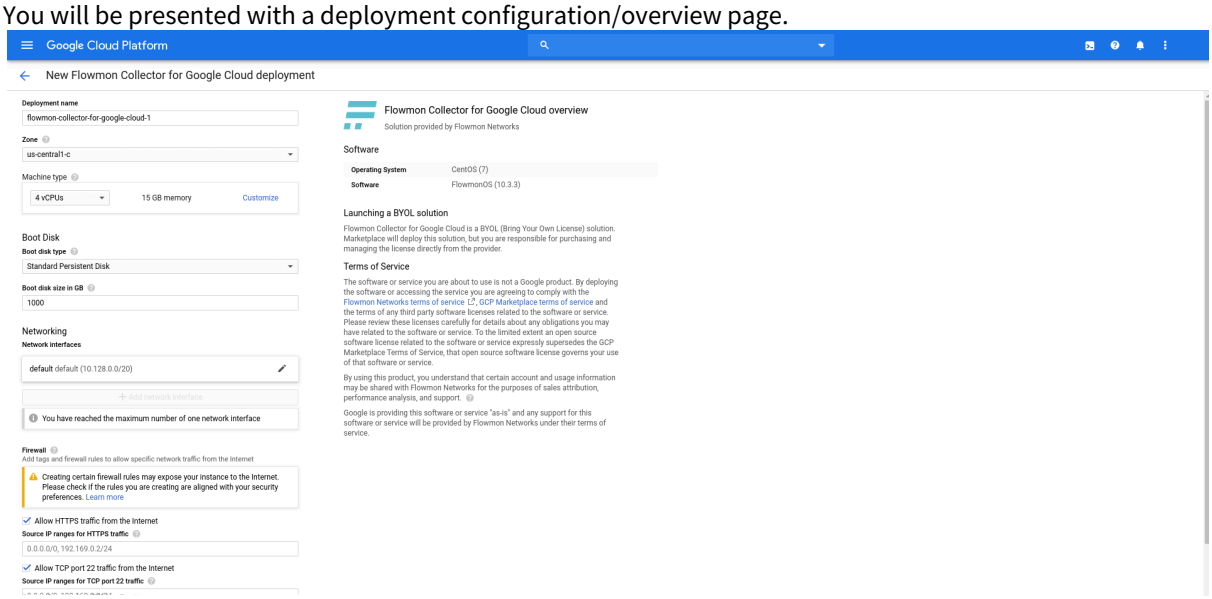
In order to follow this guide, you need the following:

1. A web browser compatible with the Google Cloud Marketplace page.
2. A trial license from flowmon.com.
3. An active Google Cloud project with a billing account associated with it. Google Cloud's Free Trial credit is supported.

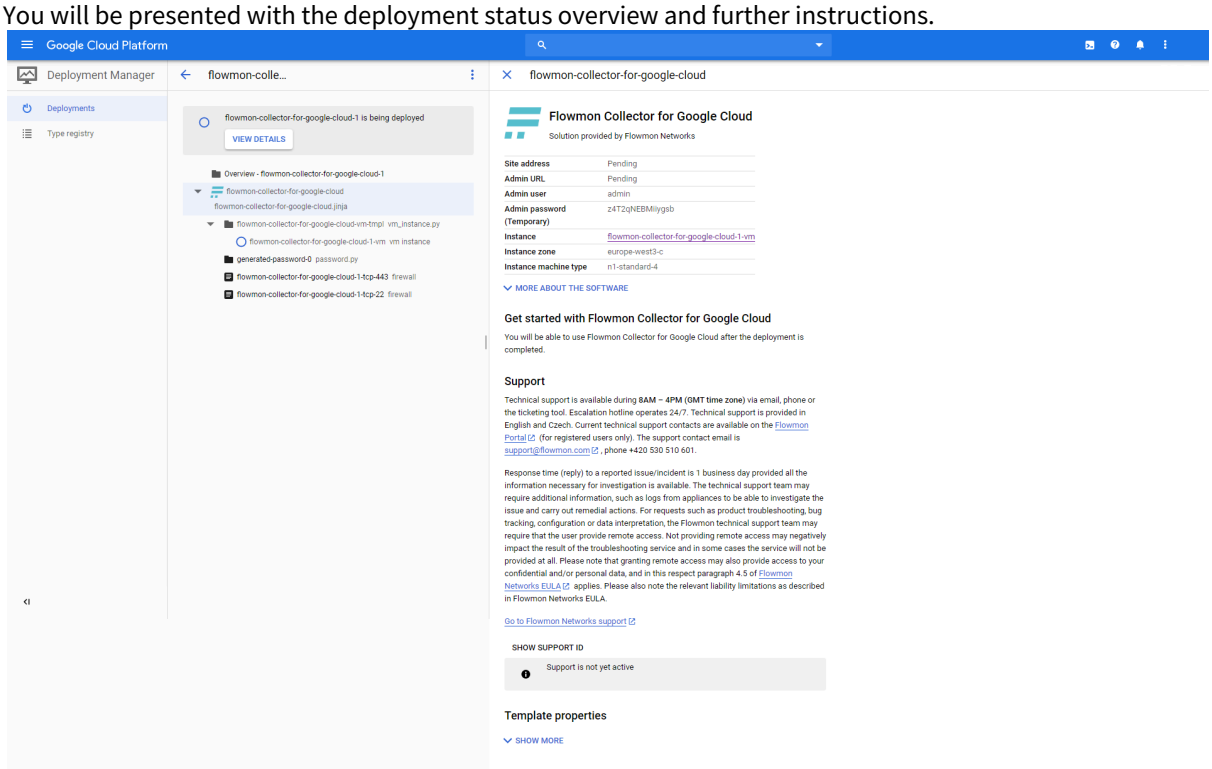
Deployment

The deployment of Flowmon for Google Cloud consists of the following steps:

1. Log in to the Google Cloud Console.
2. Navigate to the Google Cloud Marketplace page for Flowmon.
3. Select **Launch on Compute Engine**.
4. You will be presented with a deployment configuration/overview page.



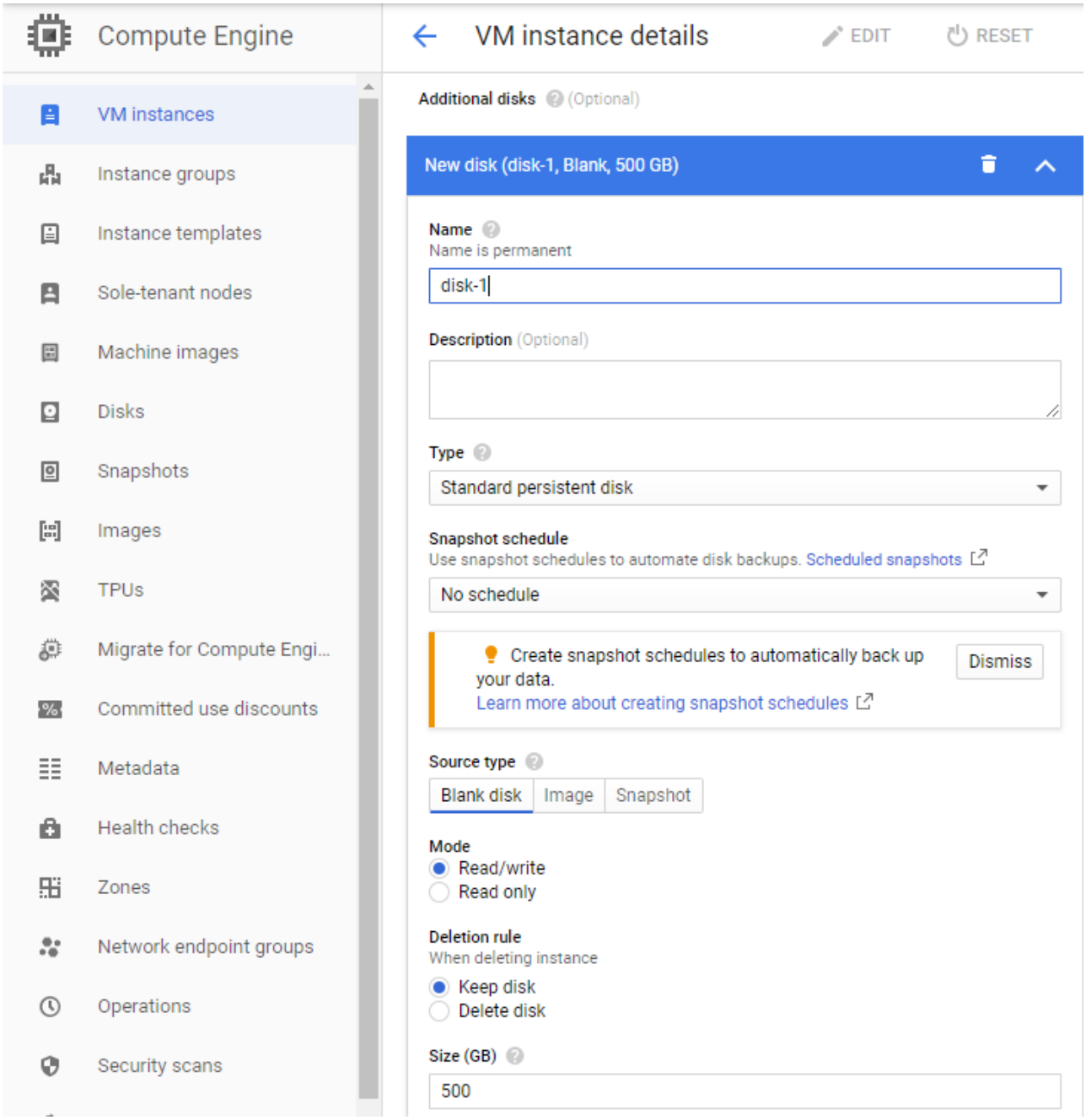
5. Adjust properties of the deployment. Pay special attention to **Boot Disk** size and **Networking**.
   Minimal **Boot Disk** size is 40 (in GB). You will be able to add a second disk suitable for your storage requirements later (see Virtual Disks below).
   Minimal number of **Network Interfaces** is 1 (for a management port), maximal number is 4 (for an additional management interface or monitoring ports used for the built-in Flowmon Probe). Every interface must be assigned to a different VPC with a non-overlapping subnet addressing scheme. The first interface will have an **Ephemeral Public IP** address automatically assigned during deployment.
6. Select **Deploy**.
7. You will be presented with the deployment status overview and further instructions.



8. Google Cloud's Deployment Manager will notify you once the deployment has finished. Follow on-screen instructions and log in to your running instance. Pay attention to **Admin URL**, **Admin user** and **Admin password**.

Virtual Disks

Once the new instance is running, you may provision additional data storage. It is recommended to store flow data on a disk other than the OS disk automatically provided with the instance. Adjust disk capacity based on your license.



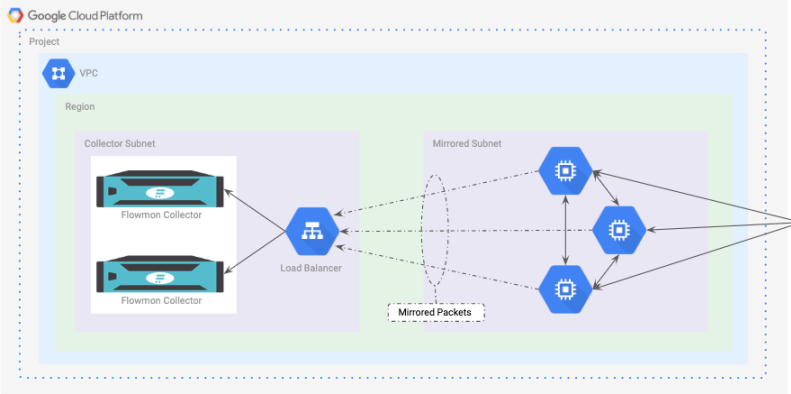
Flowmon Configuration

Please refer to Post-installation Steps.

Google Cloud VPC Packet Mirroring

Overview

Google Cloud's VPC Packet Mirroring provides continuous mirroring of virtual machine network traffic to a packet collector without using agents.



This guide follows a simple deployment scenario in which a single Flowmon Collector resides within the same VPC as mirrored instances. For advanced deployment scenarios, please refer to the official VPC Packet Mirroring documentation.

Prerequisites

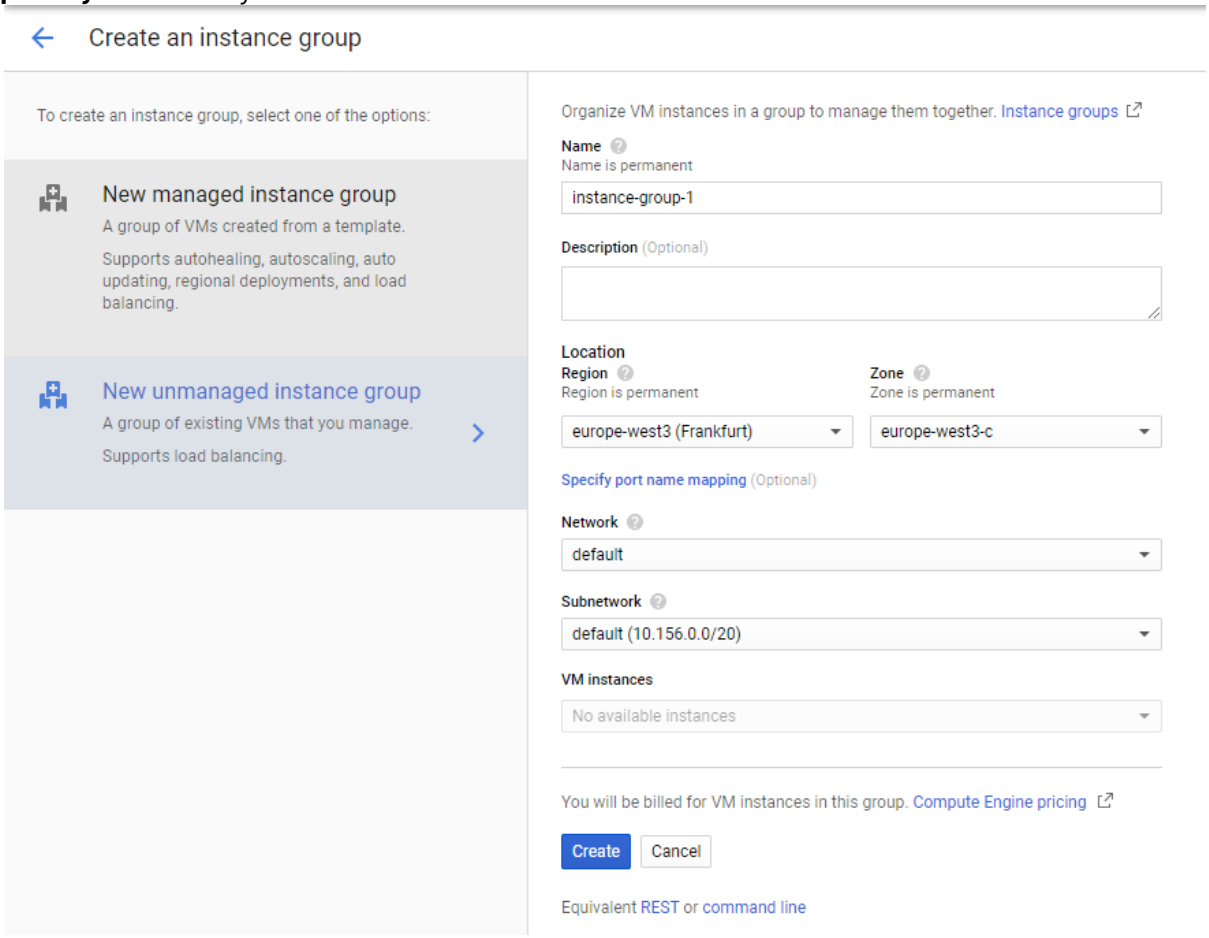
Before your start enabling VPC Packet Mirroring in your infrastructure, please make sure you

- have considered budgetary implications of running packet mirroring,
- have a Flowmon Collector instance running with two or more network interfaces and an appropriate license (with at least one monitoring port),
- have instances you wish to monitor in the same VPC as one of the monitoring interfaces of your Flowmon instance.

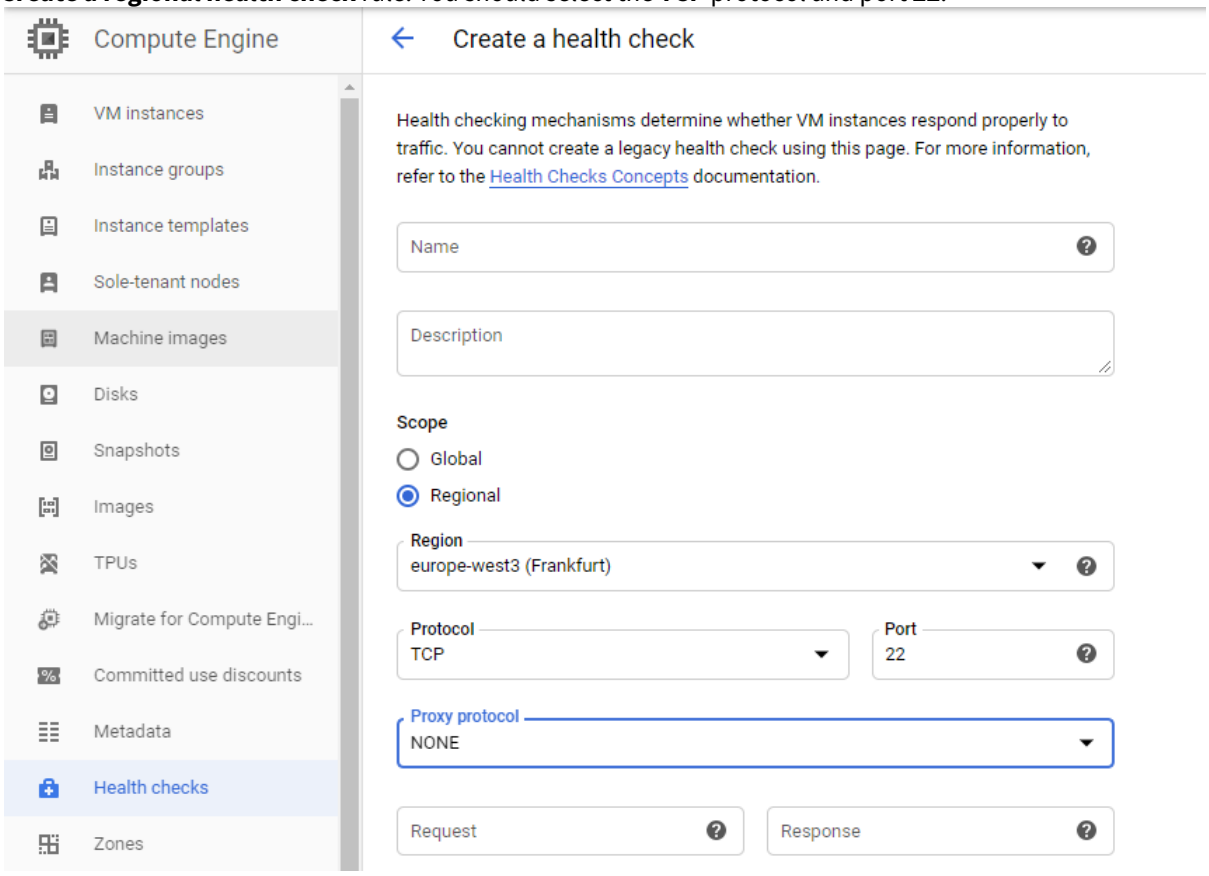
Deployment

- **Log in** to the Google Cloud Console. In all following steps, always select the **Region** and/or **Zone** that hosts your instances.

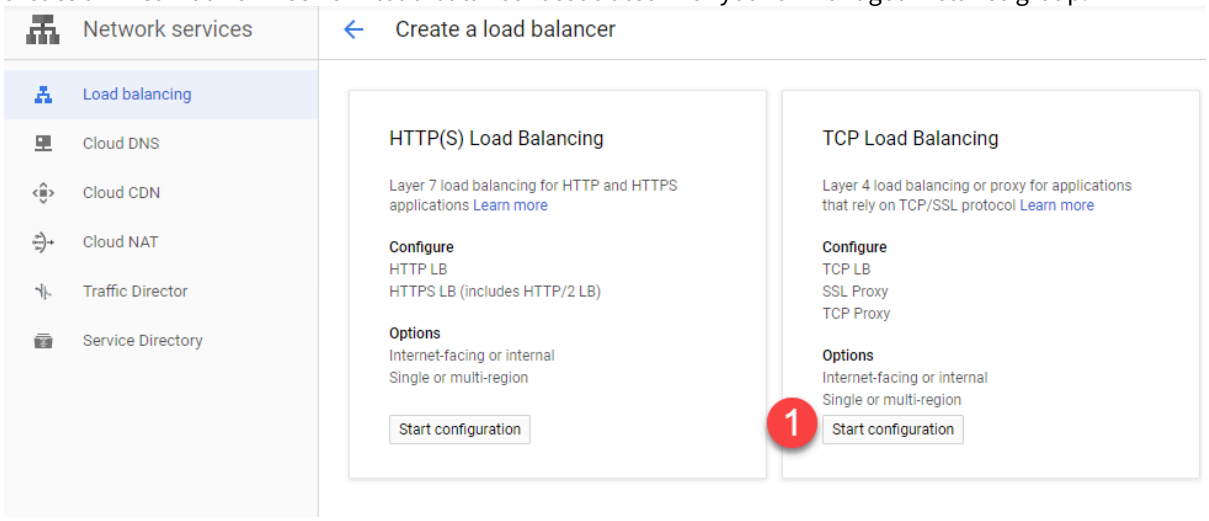
- **Create an unmanaged instance group** for your Flowmon instance(s). Select the **Network** that contains **the primary interface** of your instances.

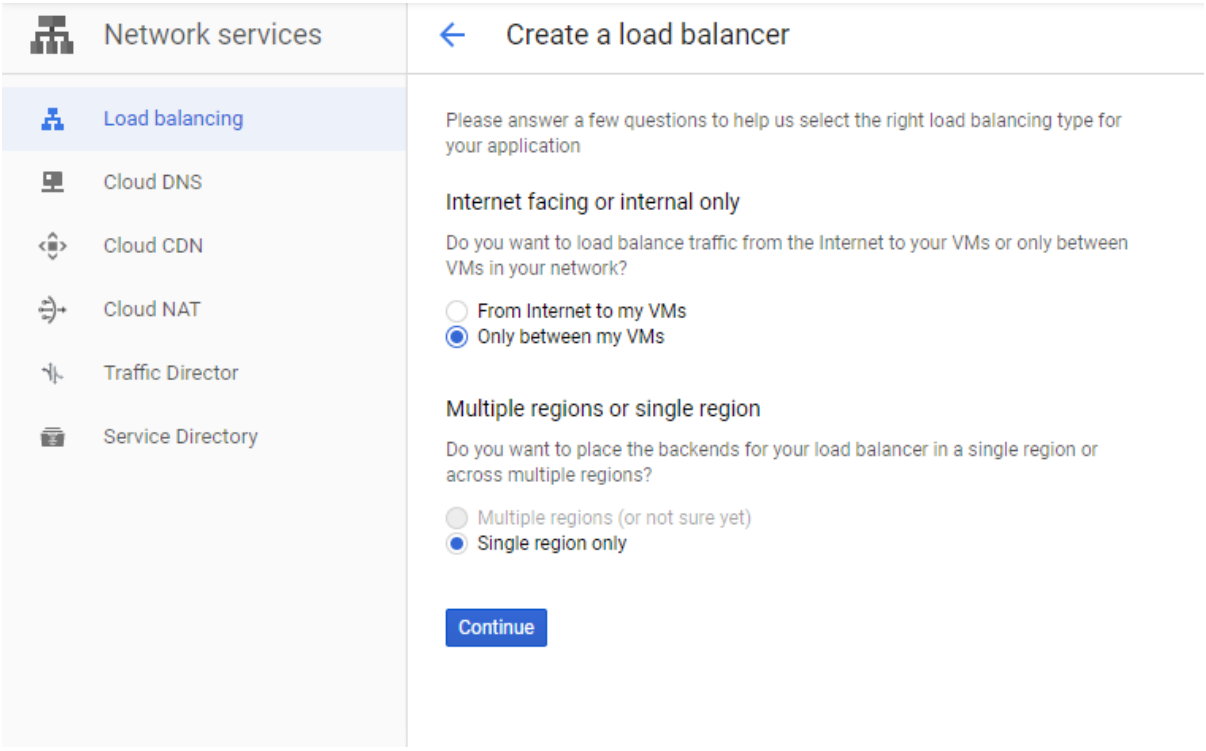


- **Create a regional health check** rule. You should select the **TCP** protocol and port **22**.

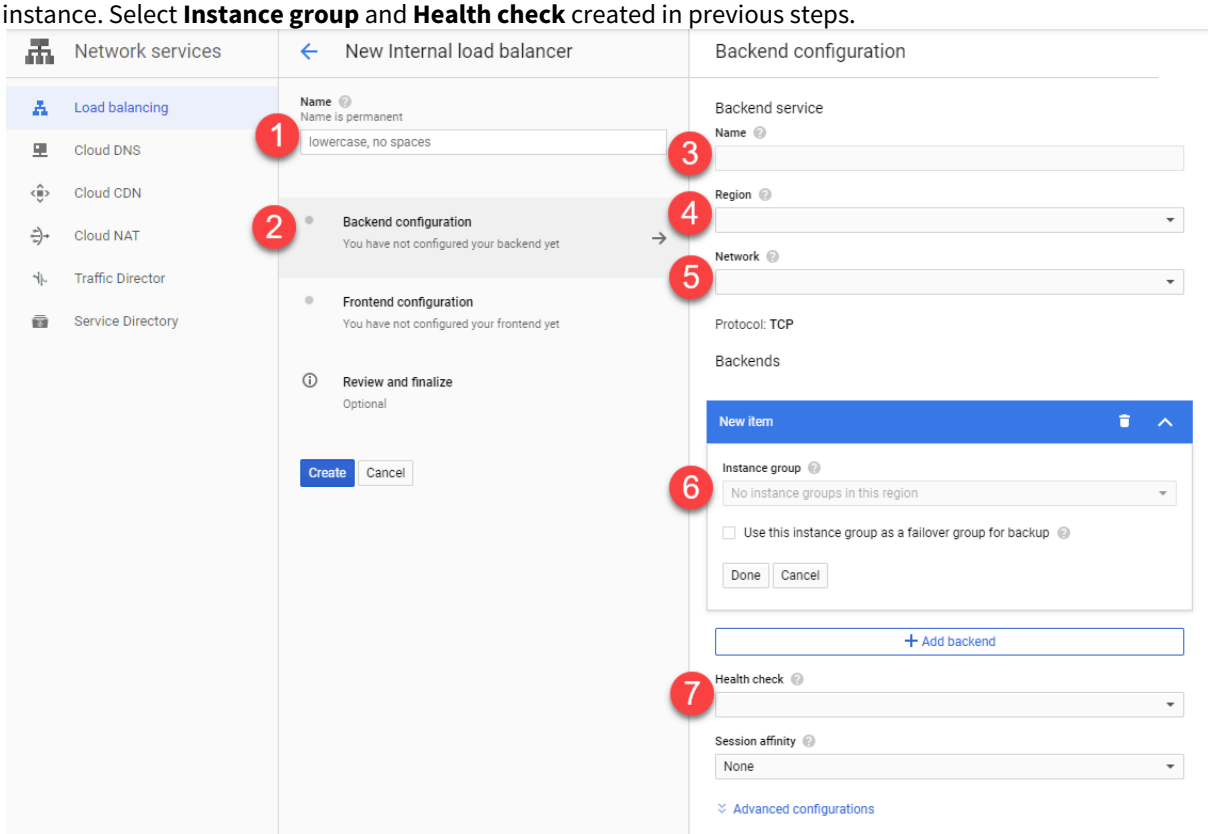


- **Create an internal TCP network load balancer** associated with your unmanaged instance group.

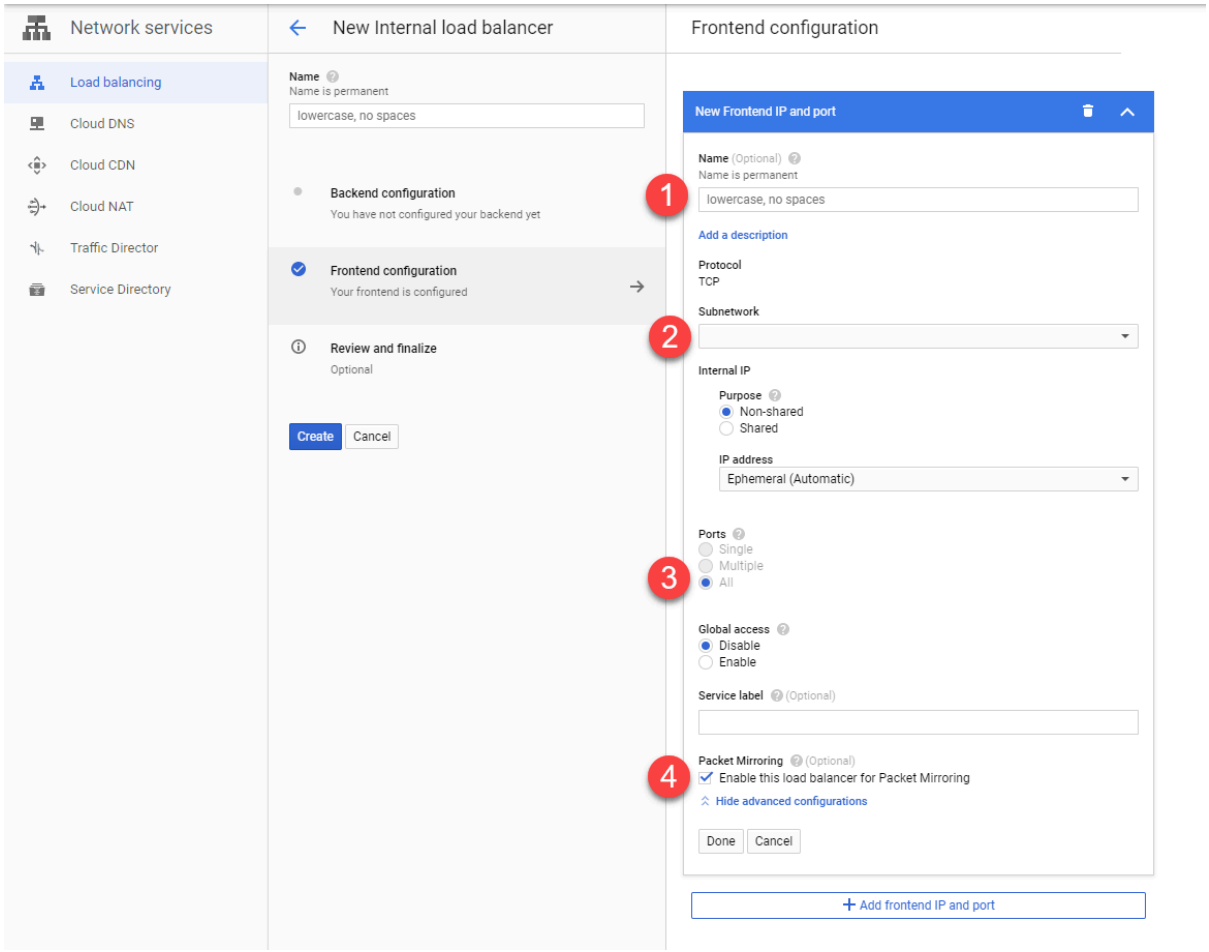




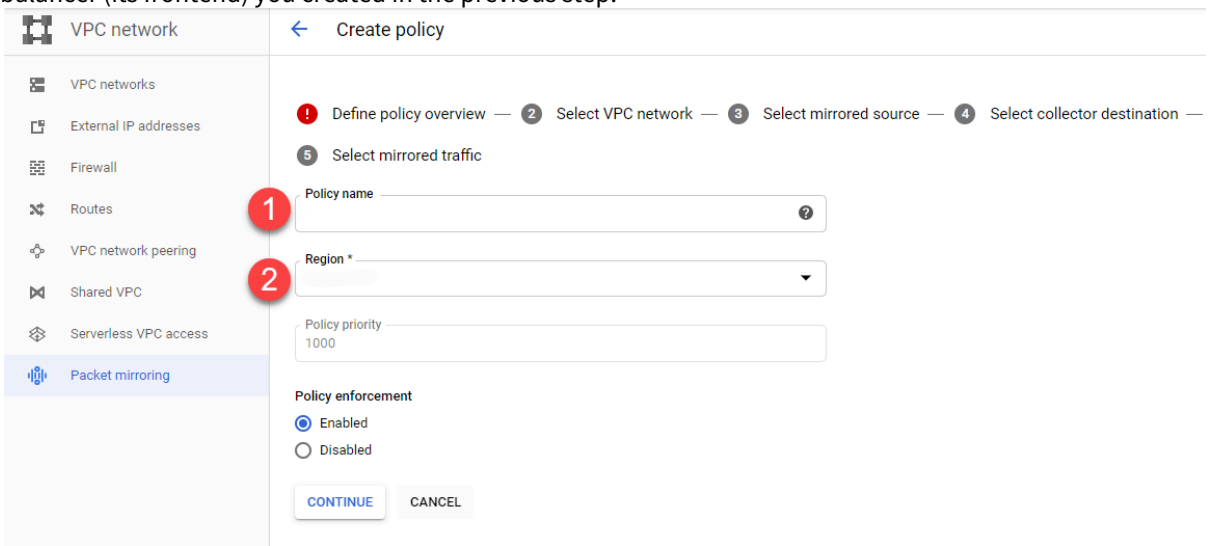
In the backend configuration, select the **Network** that contains the **monitoring interface** of your Flowmon instance. Select **Instance group** and **Health check** created in previous steps.

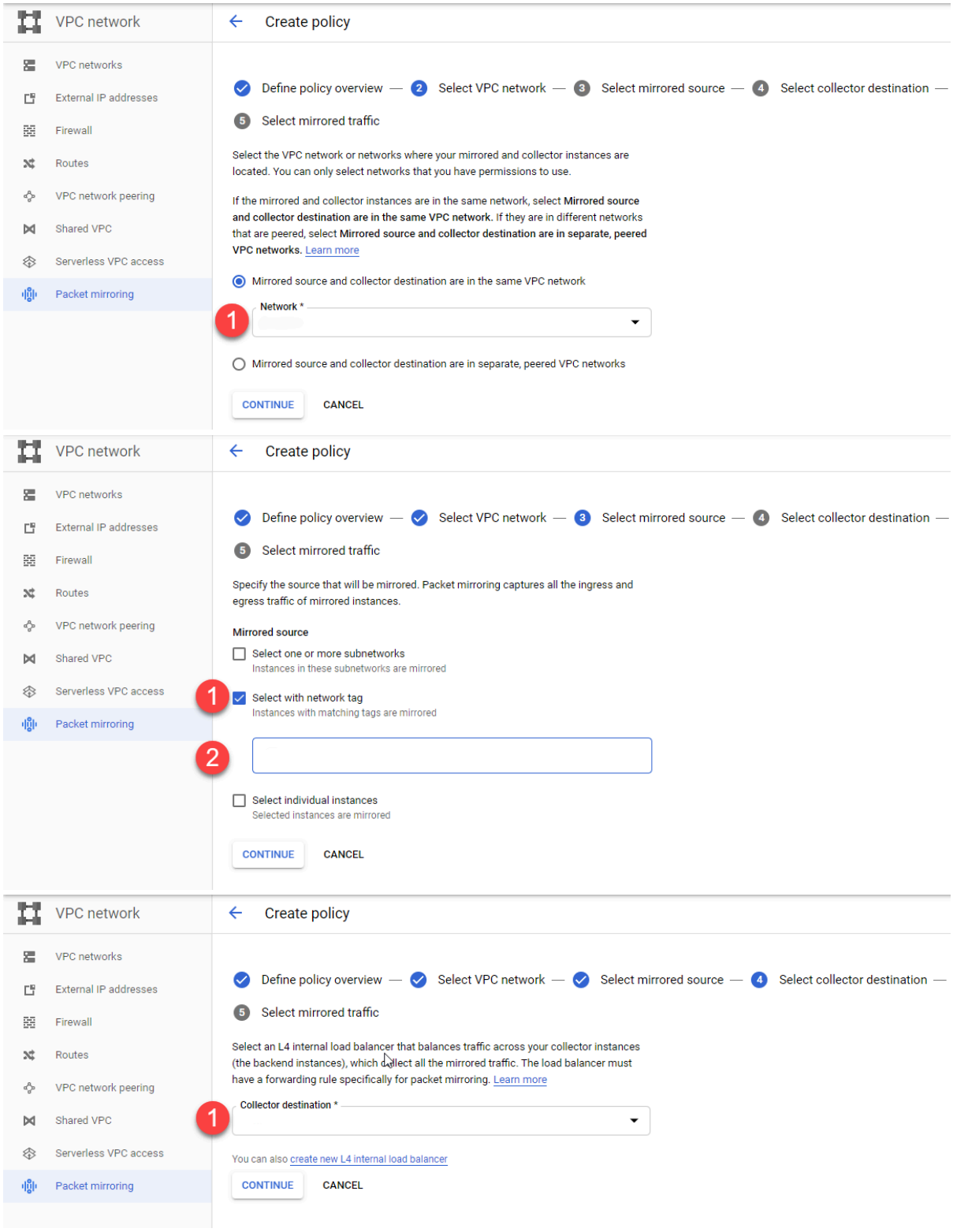


In the frontend configuration, select the **Subnetwork** that contains the **monitoring interface** of your Flowmon instance. **Enable the load balancer for packet mirroring.**



- **Create a packet mirroring policy**. Select the **Network** containing your Flowmon and mirrored instances, provide a **Tag** marking the virtual machine instances you wish to mirror. **Collector destination** is the load balancer (its frontend) you created in the previous step.





For Google Cloud Console or API guides, please refer to the official VPC Packet Mirroring documentation.

Flowmon Configuration

> ⚠ In order to accept and correctly respond to TCP health-checks, you must enable and configure an IP address on Flowmon's monitoring port. This also includes adjustments in local routing for the monitoring port in question, please refer to the official documentation for details.

No other configuration specific for VPC Packet Mirroring is necessary. See instructions on how to enable a monitoring port in the Flowmon User Guide.

Google Cloud VPC Flow Logs

Google Cloud VPC Flow Logs are currently not supported by Flowmon Collector.

Post-installation Steps

Follows a basic set of important configuration steps that should be performed on each Flowmon instance after its deployment has been completed. It is by no means an exhaustive list, it is meant to serve as a jumping-off point for new users. Please refer to the Flowmon User Guide for detailed instructions and documentation of all available configuration options.

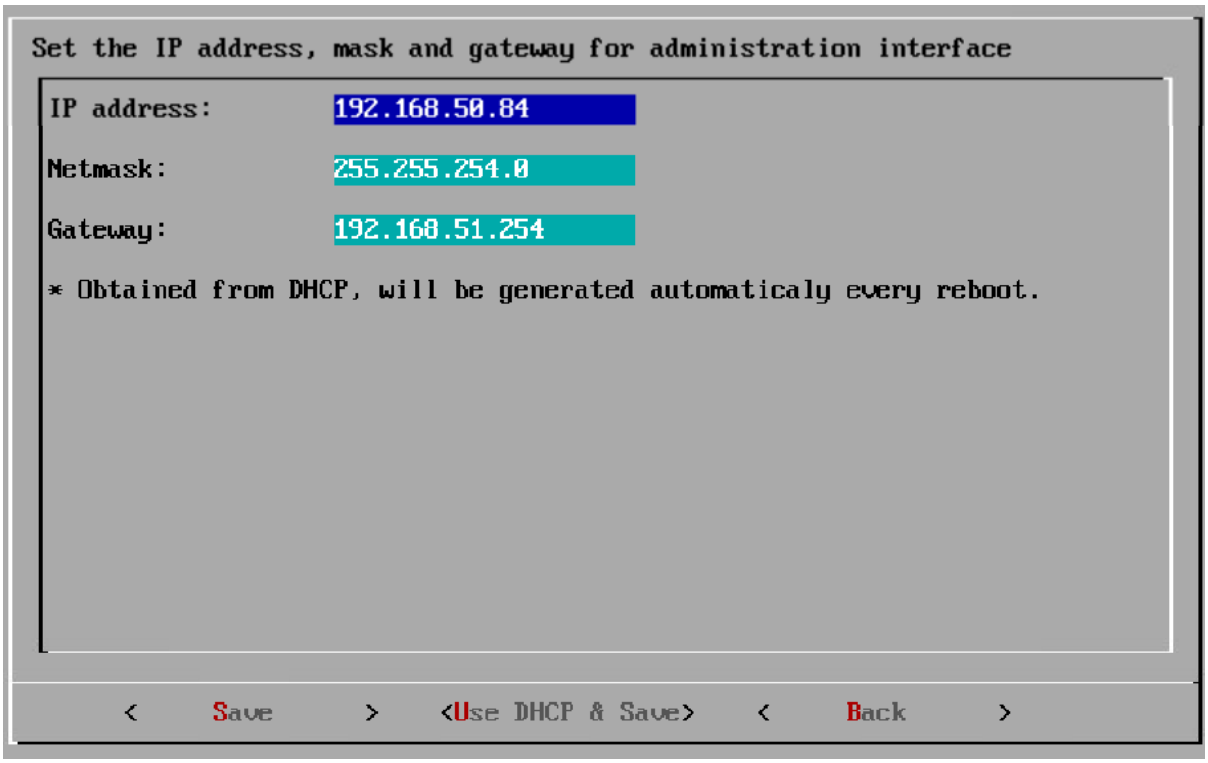
A full copy of the Flowmon User Guide is distributed with every Flowmon appliance and is accessible via the question mark (?) icon in the upper right corner of the web interface.

Management Interface

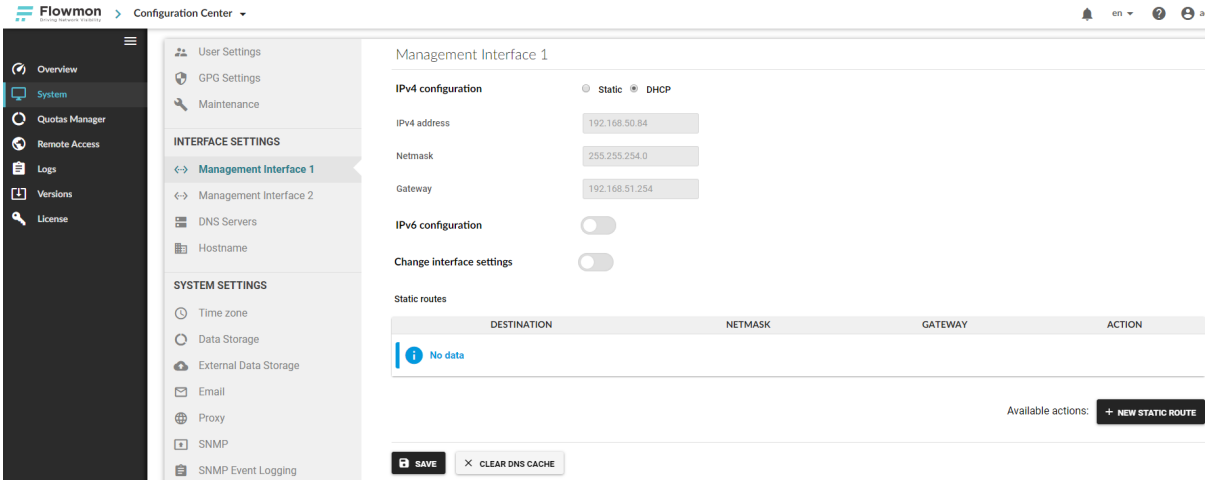
> **Note**
>
> This section applies only to Flowmon instances in virtualization platforms that require manual IP configuration of virtual network interfaces. Disregard this section if the platform of your choice:
>
> - supports DHCP and you connected Flowmon's management interface to a network where DHCP is enabled,
> - is a cloud platform, such as AWS EC2, Azure or Google Cloud.

To start using your Flowmon instance, it has to be accessible over the network. In order to do that, you have to configure an IP address on its first management interface.

1. Access the **(Virtual) Console** of the running instance and click on the black area shown on the screen. You will be asked to log in. Type **flowmon** as login and **inv3a-t3ch** as password. After that, type **sysconfig** and press **Enter**.
2. Select **Management port 1** in the menu using the up/down arrow keys and press **Enter**. On the next screen, you can set a new **IP address**, **Netmask** and **Gateway** for the web interface. Use the TAB key to move to the **Save** button and press **Enter**.



3. Log out and close the **(Virtual) Console**.
4. Later on, this configuration is available in the web interface. Enter **Configuration Center** and navigate to the **System** tab and open **Management Interface 1** settings to configure the IP address. Do not forget to **Save** the changes.



Web Interface

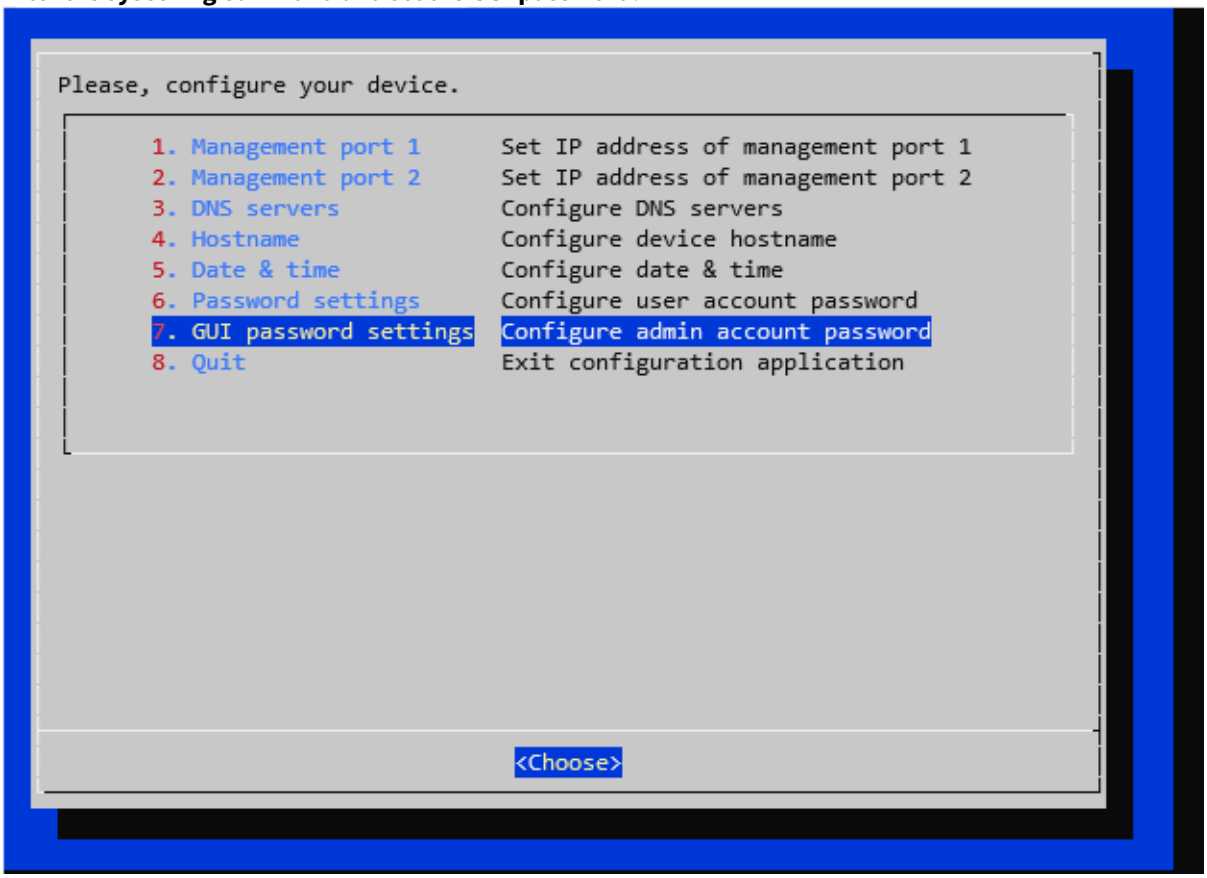
Access to the web interface is secured with a password-based authentication. In order to configure the **GUI password**, access the newly created instance via SSH.

Note

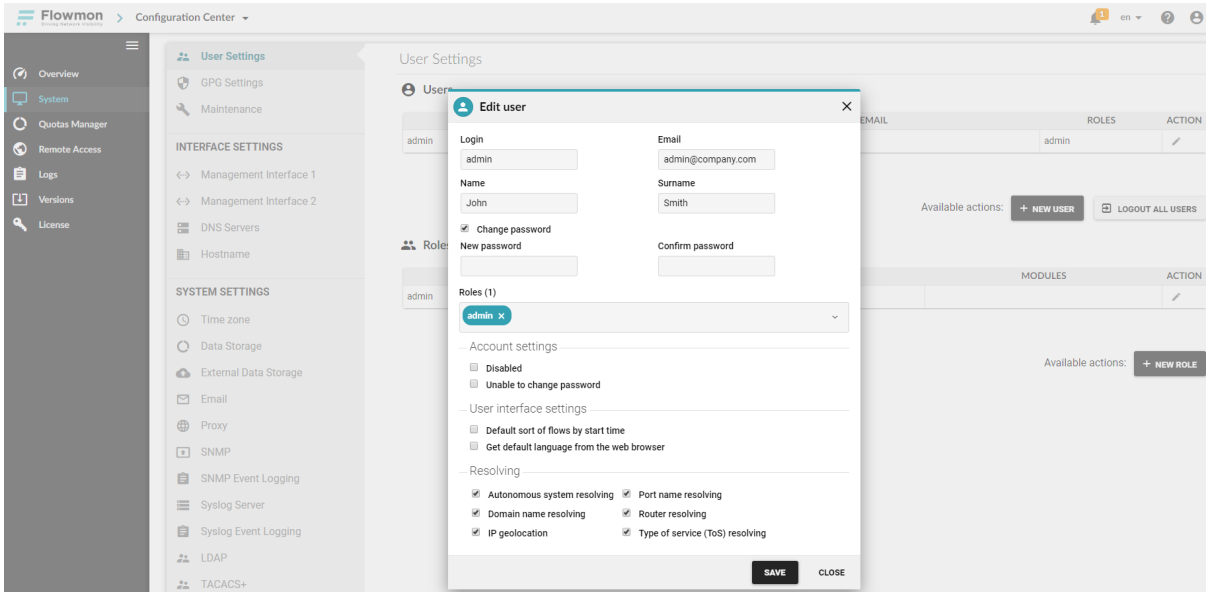
In the cloud, access to SSH is secured by a key pair and there is no default password. Please refer to the platform-specific official documentation for ways to provide SSH public keys to instances on boot.

In on-premise virtualization, access to SSH is secured by a default password **inv3a-t3ch**. This password should be changed immediately after the first successful SSH login, for security reasons.

1. Access the Flowmon instance via SSH. Using the user name **flowmon** and the IP address of its first management interface.
2. Enter the **sysconfig** command and set the **GUI password**.

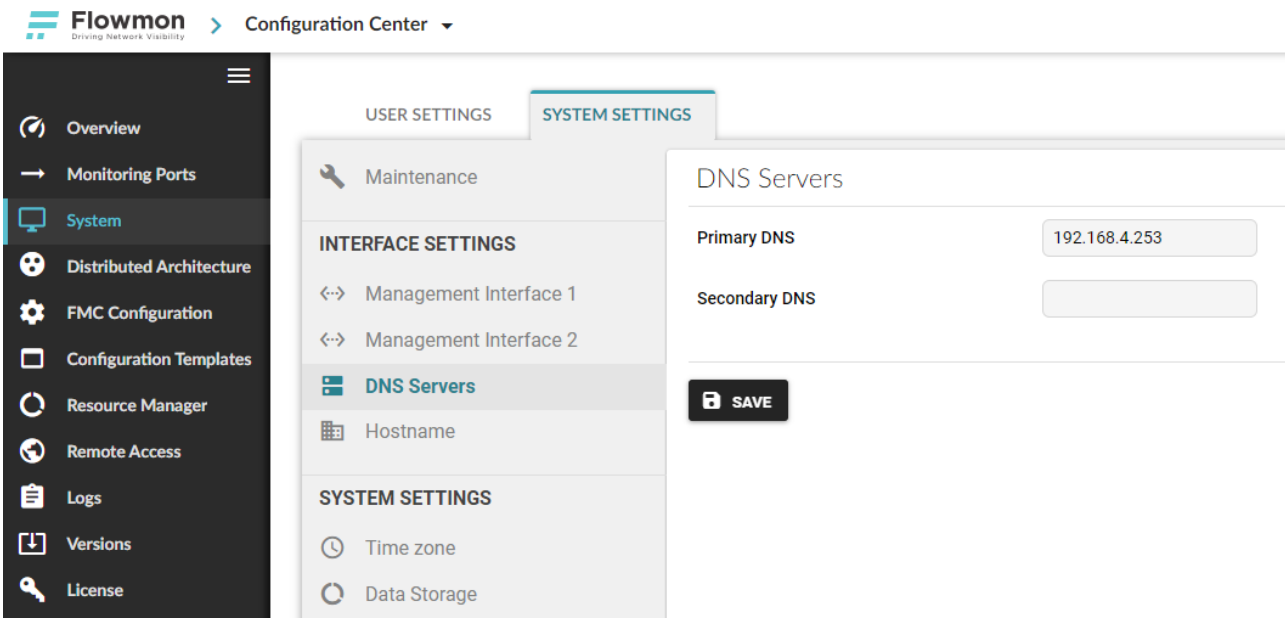


3. Once the password is configured, access the Flowmon instance in the browser via HTTPS and proceed with Flowmon configuration as described below or in the official Flowmon User Guide.
4. Later on, this functionality is available in the web interface. Enter **Configuration Center**, the **System** tab, **User Settings**. To change the **admin** password, click on the **Edit** button (pencil icon) when logged in as admin, check the **Change password** checkbox and then type in and confirm the new password.



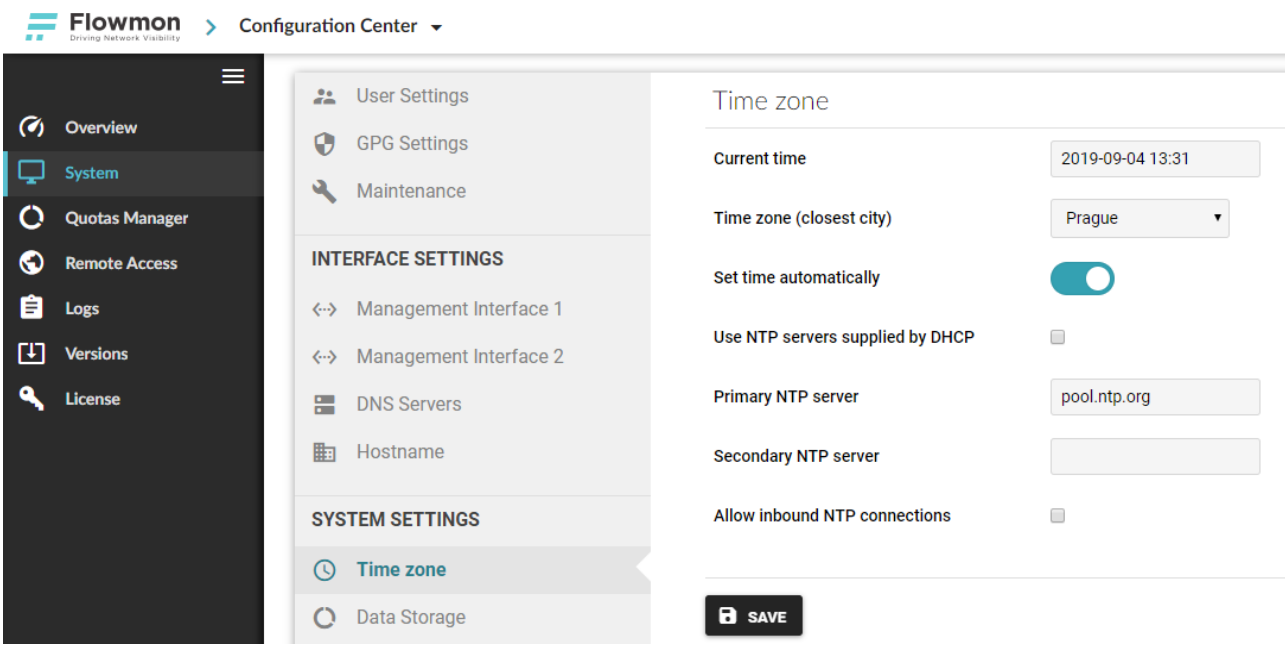
DNS Servers

In the web interface, enter **Configuration Center**, **System** tab and open **DNS Servers** settings. Configure IP addresses of the **Primary** and **Secondary DNS** servers.



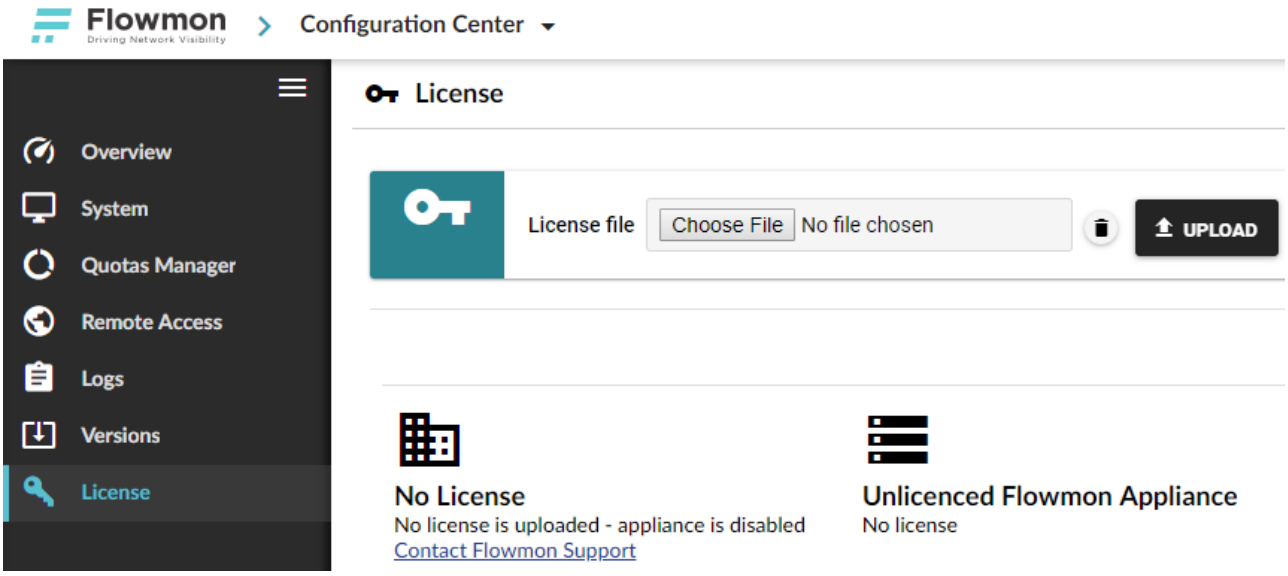
Time and Date

In the web interface, enter **Configuration Center**, **System** tab and open **Time zone** settings to set the current time and time zone. Precise time configuration is crucial for a correct flow data analysis. Do not forget to **Save** the changes.



Upload License

For a properly functioning appliance, it is necessary to apply a valid license. Enter **Configuration Center**, **License** tab, choose the license file and **Upload** it to your appliance.

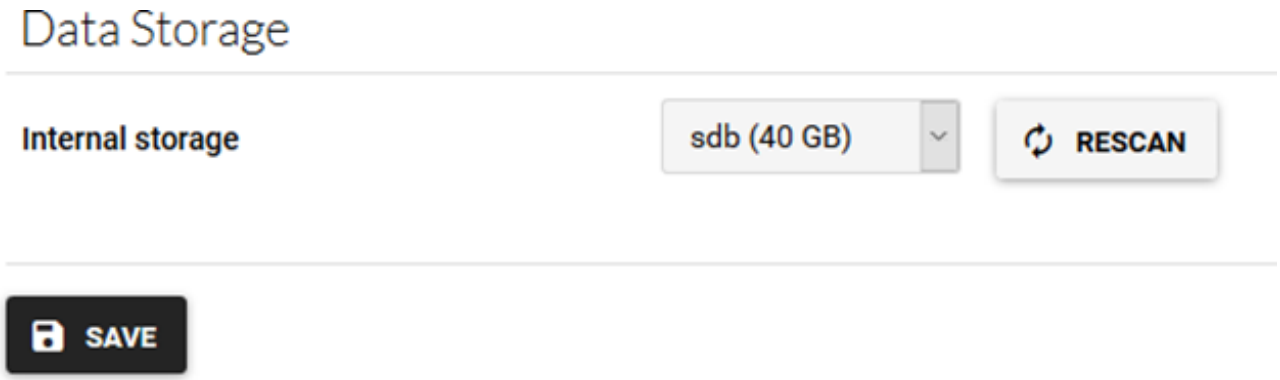


Data Storage

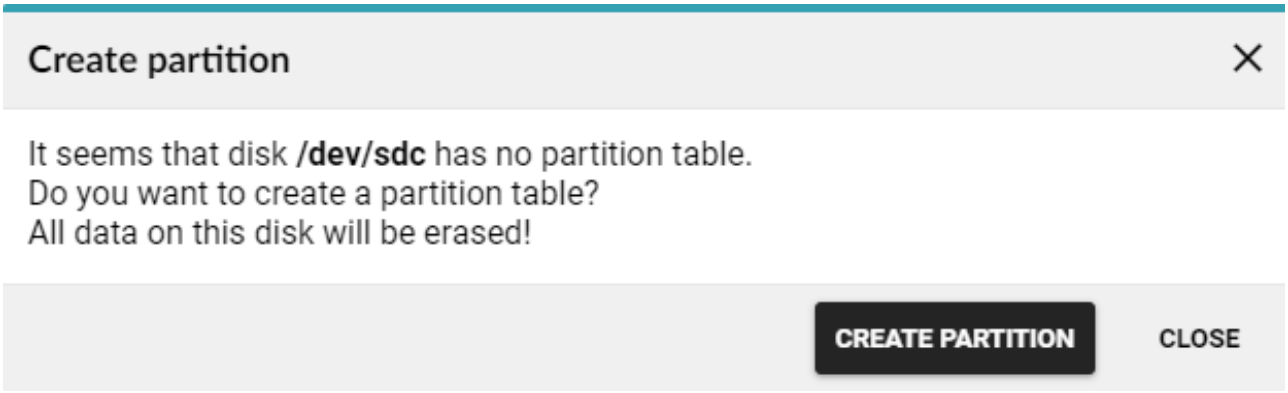
It is recommended to use a separate disk for storing Flowmon's data. In the web interface, enter **Configuration Center**, **System** tab and open **Data Storage**.

Select the desired disk from the drop down menu (list of available disks can be updated by clicking the **Rescan** button). Confirm the selection by pressing the **Save** button. System will check the selected disk and verify the partition table and filesystem (only EXT3, EXT4 and XFS filesystems are supported). If there are any files or

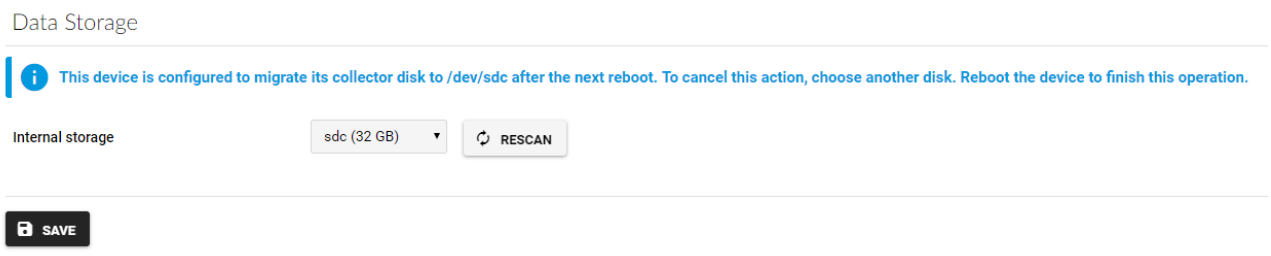
directories present on the new disk, the system compares their names to those present on the old disk. The files and directories with same colliding names will be replaced! The migration operation is finished by rebooting the device. Thus the reboot can take (much) more time than usually, because all the data are being copied and checked.



If the new disk has no partition table (for example new data storage created in virtual environment), the system will alert this and ask the user to create new partition table by clicking on the button **Create partition**. This will destroy all data on this disk!



When this operation is confirmed, the new partition table is created and system is configured to perform the data migration. Until the device is restarted, this action can be canceled anytime by choosing the original storage in the selection. If it is not canceled, then during the reboot the disk is formatted to EXT3/4 (<16TB) or XFS (>16TB) filesystem and data are copied from the original storage. If everything is done correctly, then the system will boot with the new storage. If any error occurs, system will boot with the original storage.



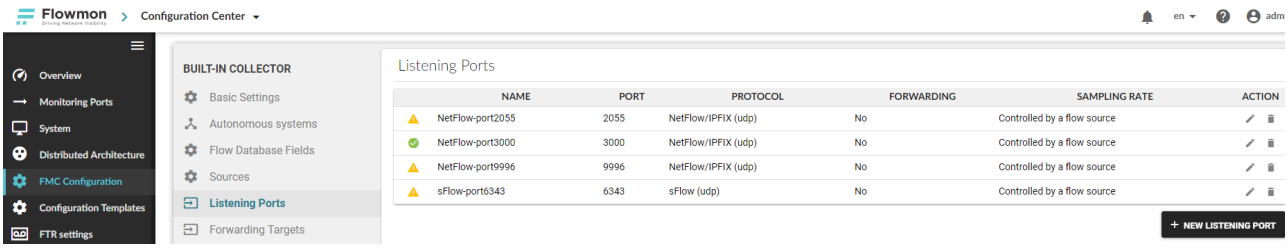
During the disk check, the following scenarios may occur:

- New disk has no partition table (described above) - user will be asked whether to create a new partition table. If so, the system will be configured to perform new disk formatting to EXT3/4 or XFS and data migration.
- New disk has a valid partition table and is not formatted - during the device reboot the disk is formatted to the EXT3/4 or XFS filesystem and data are copied.

- New disk is formatted to a filesystem different from EXT3/4 or XFS - migration will not be performed and an error will be alerted.
- New disk is formatted to the EXT3/4 filesystem and is smaller than 16 TB and contains files or directories with the same names as on the old disk (i.e. their names collide) - the user is warned that some files or directories on the new disk will be overwritten.
- New disk is formatted to the XFS filesystem and is bigger than 16 TB and contains files or directories with the same names as on the old disk (i.e. their names collide) - the user is warned that some files or directories on the new disk will be overwritten.
- New disk is formatted to the XFS filesystem and is smaller than 16 TB - during the device reboot the disk is formatted to the EXT3/4 filesystem and data are copied.
- New disk is formatted to the EXT3/4 or XFS filesystem and do not contain any files or directories with colliding names - during the device reboot the data will be copied from original disk to the new one.

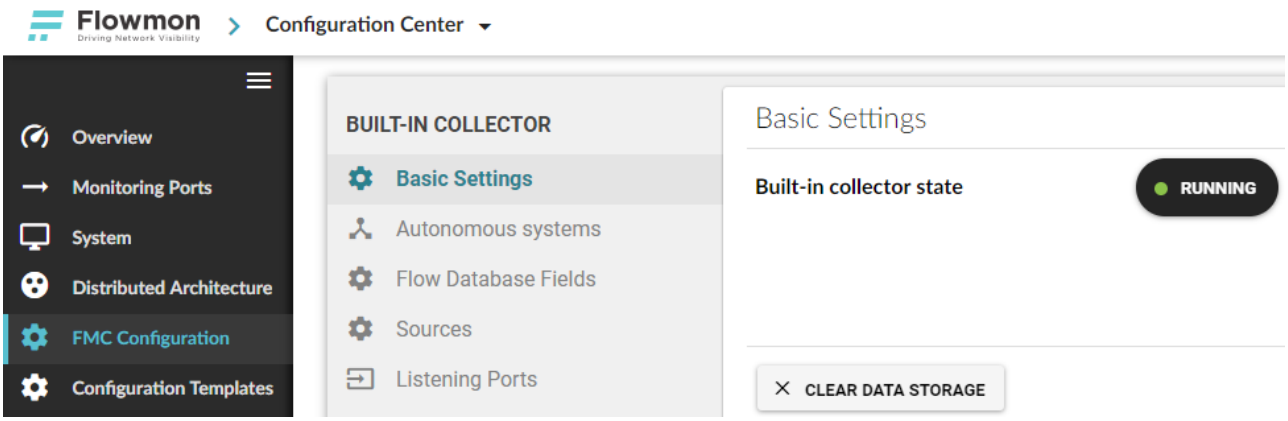
Collector Listening Ports

Enter **Configuration Center** and navigate to the **FMC Configuration** tab and open **Listening Ports** settings. Here you can add new sources or configure existing NetFlows/sFlow source parameters, like the source name, receiving port, protocol type and forwarding.



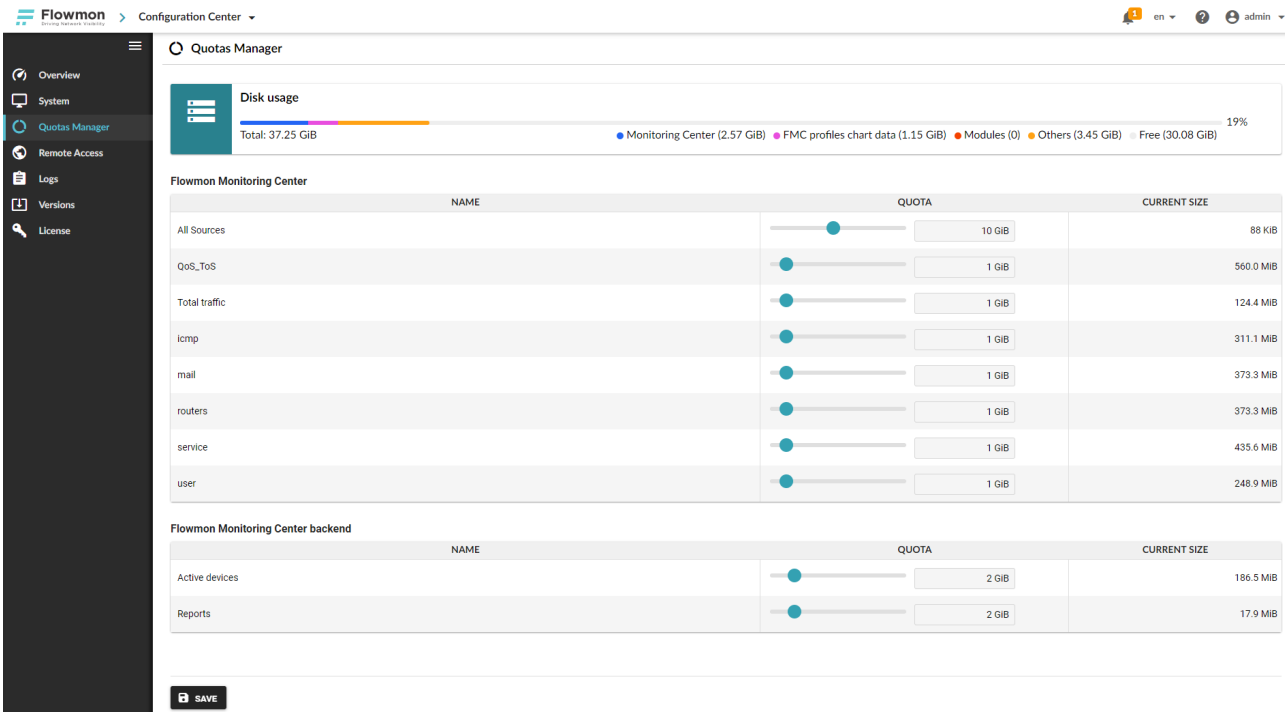
Collector Initialization

Initialize the built-in collector database in **Configuration Center**, the **FMC Configuration** tab, **Basic Settings** by clicking on the **Clear Data Storage** button. This step will clear the database! All collected NetFlow data will be lost!



Quotas

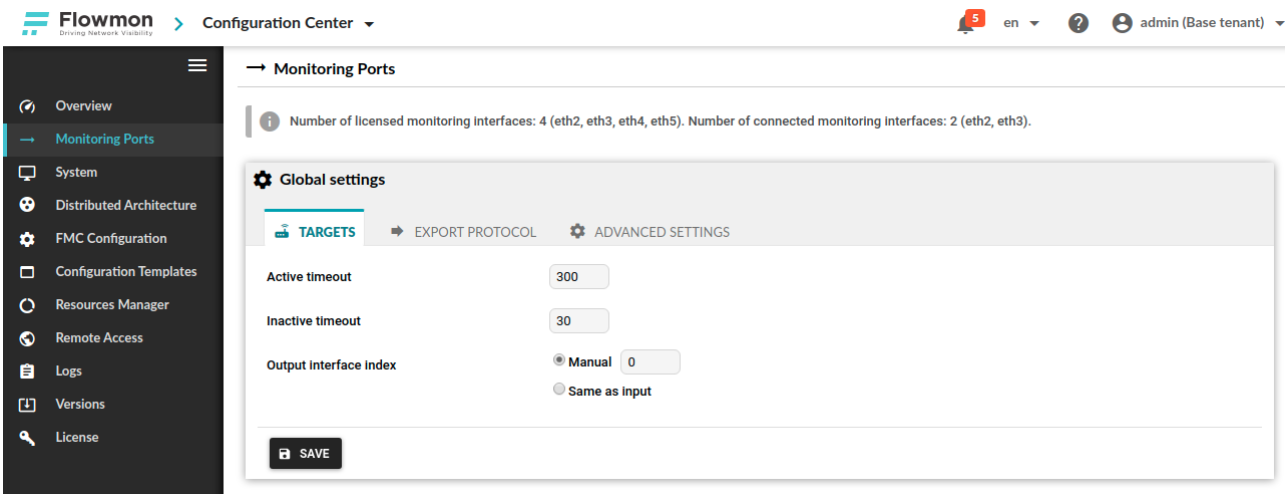
To check the space allocated to the live profile and other plugins, open **Configuration Center** and the **Quotas Manager** tab. It is recommended that at least 10GB is allocated for the live profile and 2GB for each additional module. Do not forget to **Save** the changes.



Monitoring Traffic

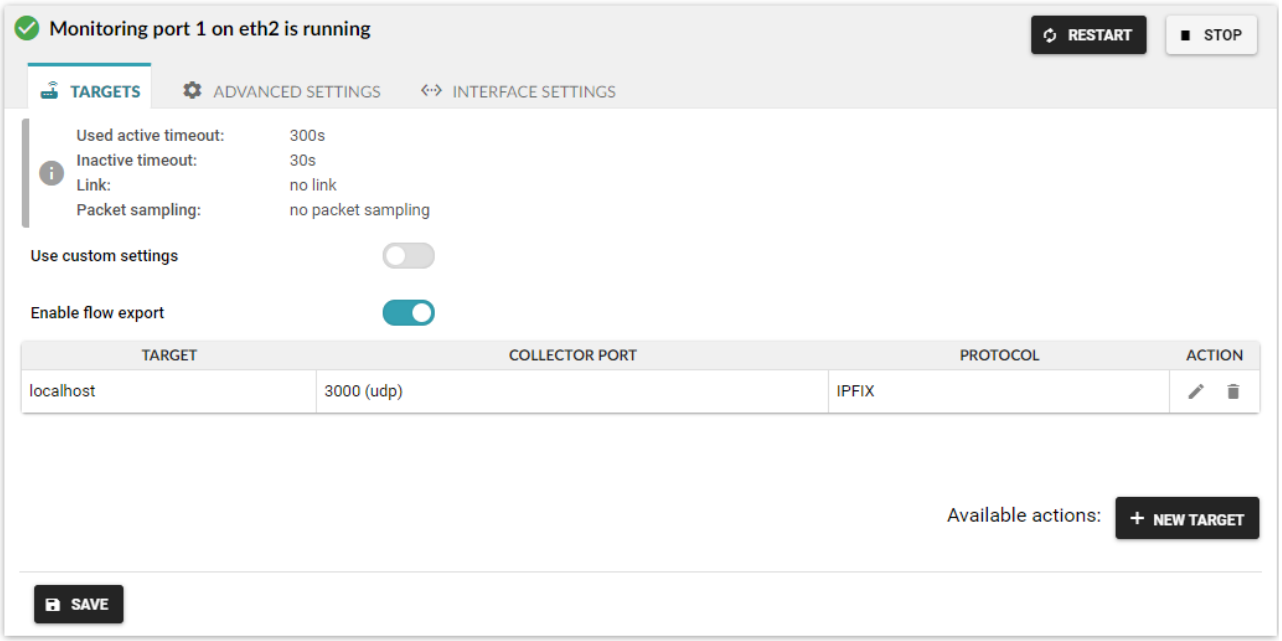
The monitoring port is a process running over each monitoring interface. It analyzes every single received packet and computes flow statistics. The statistics are exported to a collector (e.g. external Flowmon Collector or the local collector). The administrator can check the status of monitoring ports, start/stop monitoring ports or set new configuration. Each monitoring port is configured by dedicated management panel or it can be switched to the global mode in which some tabs will be configured according to the Global settings.

Go to **Monitoring Ports**.



Active timeout ensures that the very long flows will be exported in specified time. Timeout is checked for each incoming packet. If corresponding flow is lasting longer than specified time interval, it is deleted from the flow cache and exported to collector.

Inactive timeout avoids keeping old, inactive flow records in the flow cache forever. When no packets belonging to the flow are observed for the specified time interval, flow record is exported to collector.

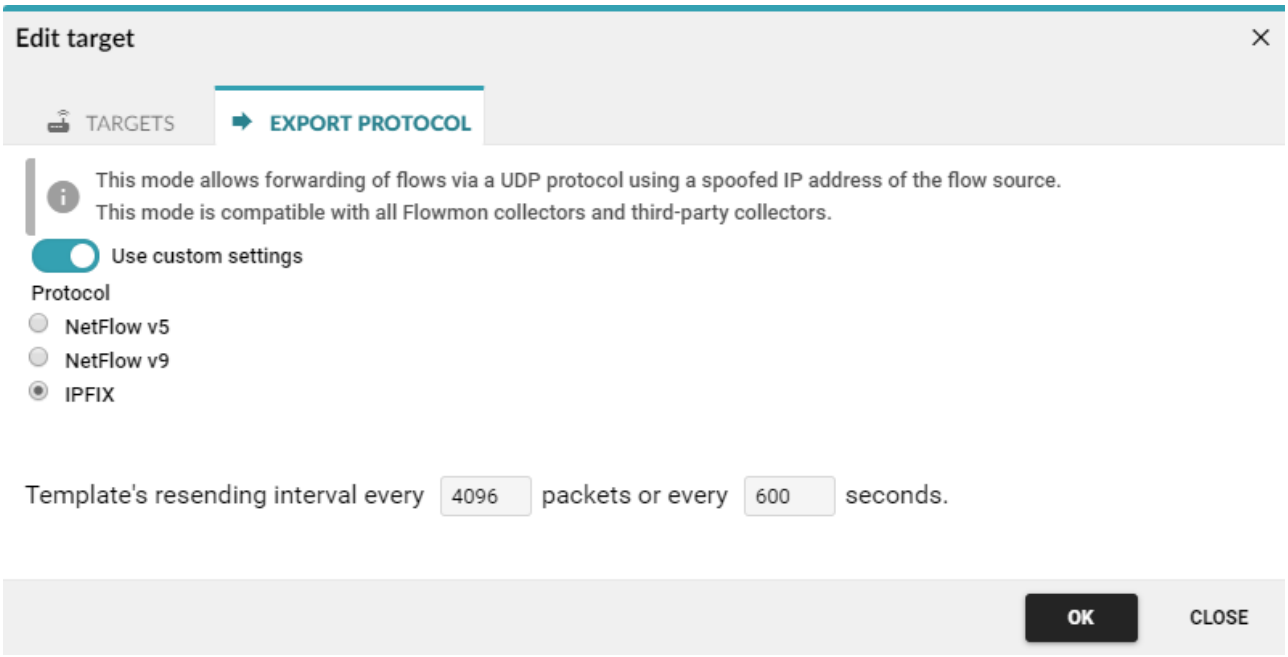


To start the flow monitoring port press the **Start** button. If the monitoring port starts correctly, button **Start** will change to **Stop** and button **Set Defaults** will change to **Restart** . To use default monitoring port configuration, stop it and then press **Set Defaults** button.

In the **Targets** tab you can configure various number of targets (i.e. collectors) where the flow exports are to be exported. The targets can be added or removed by pressing the **New target** or **Delete** button. Every target is specified by items **Target address** and **Collector port**. The address item is an address to a collector. If the probe built-in collector is to be used, use the address localhost. The port item specifies the listener port of the collector. For the built-in collector use the port 3000. The **Flow sampling rate** value defines a deterministic sampling (e.g sampling interval 1 in 3 flows) for monitoring port flows. If you enter a N value, every Nth flow will be exported. This is useful in situation when the collector is overloaded by incoming flows. The zero value disables this feature.
The **Network protocol** option can be selected in corresponding drop-down menu. UDP (default) or TCP protocol can be selected. TCP protocol is supported for IPFIX export protocol only. If TCP is selected as network protocol, the

encryption TCP/TLS can be enabled. For TCP/TLS, the set of keys and certificates have to be generated for flow exporting device (monitoring port) and for collector. All certificates must be signed by the same certification authority (CA). Its certificate (CA certificate) must be provided together with the monitoring port key and certificate to each monitoring port target using TCP/TLS protocol. The provided key(s) must not be encrypted.

In the **Export protocol** tab you can select the Export protocol NetFlow v5, NetFlow v9 and IPFIX. By unchecking the **Use custom settings** toggle switch and clicking on button **OK** will be this tab configured according to the global configuration. Additionally, the frequency of sending the template can be configured.



Collecting Data

Send NetFlow v5, NetFlow v9 or IPFIX flow data to **Management Interface 1** of your Flowmon Collector. For available listening ports, corresponding supported flow data formats, and flow collection status, refer to **FMC Configuration / Listening Ports**.

To start analyzing your data, go to **Monitoring Center**.

3rd-party Packet Brokers

The following 3rd-party packet brokers are currently supported:

- Garland Prisms
- Ixia CloudLens
- Gigamon

Garland Prisms

Overview

This solution is leveraging Garland Prisms - to provide network traffic - and Flowmon with extension modules for NPMD, network behavior analysis, performance monitoring, DDoS detection and on-demand packet capture - to provide insight into network traffic. With Garland Prisms agents installed on all monitored virtual instances, a copy of the network traffic is routed to monitoring interfaces of a Flowmon instance for processing and analysis.

This document outlines steps necessary to start analyzing network traffic in your cloud deployment with Garland Prisms and Flowmon.

Prerequisites

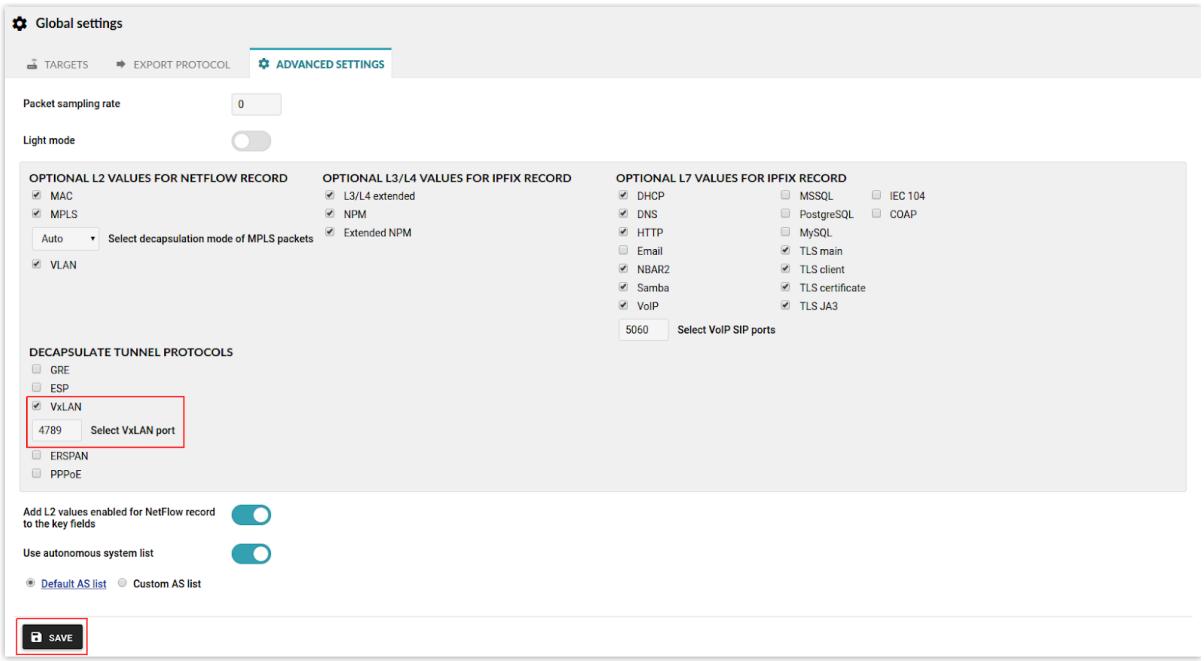
1. A running instance of Flowmon (AWS, Azure or Google Cloud).
2. A number of running client instances where Garland Prisms agents can be installed.

Deployment

For an up-to-date deployment guide, please refer to the official documentation for Garland Prisms.

Flowmon Configuration

1. Go to **Flowmon Configuration Center** of your Flowmon instance.
2. Choose the **Monitoring Ports** panel.
3. Under **Global settings -> Advanced settings** enable **VxLAN** decapsulation on port **4789**.
4. Click on the **Save** button.



Ixia CloudLens

Overview

Flowmon and Ixia have joined to provide true cloud visibility. The solution is leveraging Ixia CloudLens Agents - to provide network traffic - and Flowmon with extension modules for NPMD, network behavior analysis, performance monitoring, DDoS detection and on-demand packet capture - to provide insight into network traffic. With Ixia CloudLens Agents installed on all monitored virtual instances, a copy of the network traffic is routed to their counterpart running on the Flowmon Collector VA instance for processing and analysis.

This document outlines steps necessary to start analyzing network traffic in your cloud deployment with Ixia CloudLens and Flowmon.

Prequisites

1. A running instance of Flowmon (AWS, Azure or Google Cloud).
2. A number of running client instances where Ixia CloudLens Agents can be installed.

Deployment

For an up-to-date deployment guide, please refer to the official Ixia CloudLens documentation.

Flowmon Configuration

To install an Ixia CloudLens Agent on Flowmon, open an SSH connection to the Flowmon instance via its management IP address and run the following commands. Replace **PROJECT_KEY** with the value retrieved from the Ixia Portal during project creation.

1. Start **docker** and enable it as a service.

```
sudo systemctl start docker
sudo systemctl enable docker
```

2. Run container with Ixia CloudLens Agent.

```
sudo docker run --name ixia-cloudlens-agent-fmc \
                -v /:/host \
                -v /var/run/docker.sock:/var/run/docker.sock \
                -d --restart=always --net=host \
                --privileged --restart=on-failure \
                ixiacom/cloudlens-agent \
                --server agent.ixia.cloud \
                --accept_eula yes \
                --apikey $PROJECT_KEY
```

3. Verify that the container is running.

```
sudo docker ps | grep ixia-cloudlens-agent-fmc
```

See Post-installation Steps or follow instructions on how to enable a monitoring port in the Flowmon User Guide.

Gigamon

Overview

This solution is leveraging Gigamon Visibility Platform - to provide network traffic - and Flowmon with extension modules for NPMD, network behavior analysis, performance monitoring, DDoS detection and on-demand packet capture - to provide insight into network traffic. With Gigamon VTap agents installed on all monitored virtual instances, a copy of the network traffic is routed to monitoring interfaces of a Flowmon instance for processing and analysis.

This document outlines steps necessary to start analyzing network traffic in your cloud deployment with Gigamon and Flowmon.

Prerequisites

1. A running instance of Flowmon (AWS, Azure or Google Cloud).
2. A number of running client instances where Gigamon vTAP agents can be installed.

Deployment

In order to be able to use Gigamon, several components are needed. They can be either virtual or physical appliances. For a fully virtualized installation, you need to have instances of

- Gigamon Fabric Manager,
- VSeries Node,
- VSeries Controller,
- VTap Controller.

In order to send packets to Gigamon Visibility Fabric, you need to install Gigamon vTAP on every host you want to monitor.

For more information about the Gigamon Solution and up-to-date installation guides, see

- Gigamon Visibility Platform for AWS - Configuration Guide
- GigaSECURE® Cloud for Azure - Getting Started Guide

There is no need to install anything on your Flowmon.

Flowmon Configuration

1. Go to **Flowmon Configuration Center** of your Flowmon instance.
2. Choose the **Monitoring Ports** panel.
3. Under **Global settings -> Advanced** settings enable **VxLAN** decapsulation on port **4789**.

4. Click on the **Save** button.