Deploy the ExtraHop Discover Appliance with VMware

Published: 2021-10-07

Published: 2021-10-07

The ExtraHop virtual appliance can help you to monitor the performance of your applications across internal networks, the public internet, or a virtual desktop interface (VDI), including database and storage tiers. ExtraHop can monitor application performance across geographically distributed environments such as branch offices or virtualized environments through intra-VM traffic.

Before you begin

- You must have familiarity with administering VMware. The images in this guide are from VMware version 6.7, and some of the menu selections might have changed.
- We recommend that you upgrade to the latest patch for the vSphere environment to avoid any known issues.

This guide explains how to deploy the following ExtraHop Discover virtual appliances on the VMware ESXi/ESX platform:

- EDA 1000v (Monitors up to 250 devices)
- Reveal(x) EDA 1100v (Monitors up to 250 devices)
- EDA 2000v (Monitors up to 1000 devices)
- EDA 6100v (Monitors up to 3000 devices)

Virtual machine requirements

Your hypervisor must be able to support the following specifications for the virtual Discover appliance.

- VMware ESX/ESXi server version 5.5 or later
- vSphere client to deploy the OVF file and to manage the virtual machine
- (Optional) If you want to enable packet captures, configure an additional storage disk during deployment
- The following table provides the server hardware requirements for each Discover appliance model:

Appliance	CPU	RAM	Disk
EDA 1000v	2 processing cores with hyper-threading support, VT-x or AMD-V technology, and 64-bit architecture. Supplemental Streaming SIMD Extensions 3 (SSSE3) support. If you want to enable SSL decryption, 3 CPUs are required. For more information, see Add a CPU Core to the EDA 1000v with VMware.	4 GB	46 GB or larger disk for data storage (thick-provisioned) 250 GB or smaller disk for packet captures (thick-provisioned)

Appliance	CPU	RAM	Disk
Reveal(x) EDA 1100v	4 processing cores with hyper-threading support, VT-x or AMD-V technology, and 64-bit architecture. Supplemental Streaming SIMD Extensions 3 (SSSE3) support.	8 GB	46 GB or larger disk for data storage (thick-provisioned) 250 GB or smaller disk for packet captures (thick-provisioned)
EDA 2000v	6 processing cores with hyper-threading support, VT-x or AMD-V technology, and 64-bit architecture. Supplemental Streaming SIMD Extensions 3 (SSSE3) support.	6 GB	255 GB or larger disk for data storage (thick-provisioned) 250 GB or smaller disk for packet captures (thick-provisioned)
EDA 6100v	16 processing cores with hyper-threading support, VT-x or AMD-V technology, and 64-bit architecture. Supplemental Streaming SIMD Extensions 3 (SSSE3) support.	64 GB	1 TB or larger disk for data storage (thick-provisioned) 500 GB or smaller disk for packet captures (thick-provisioned)

To ensure proper functionality of the virtual appliance:

- Make sure that the VMware ESX/ESXi server is configured with the correct date and time.
- Always choose thick provisioning. The ExtraHop datastore requires low-level access to the complete drive and is not able to grow dynamically with thin provisioning. Thin provisioning can cause metric loss, VM lockups, and capture issues.
- Do not change the default disk size on initial installation. The default disk size ensures correct lookback for ExtraHop metrics and proper system functionality. If your configuration requires a different disk size, contact your ExtraHop representative before you make any changes.
- Do not migrate the VM. Although it is possible to migrate when the datastore is on a remote SAN, ExtraHop does not recommend this configuration. If you must migrate the VM to a different host, shut down the virtual appliance first and then migrate with a tool such as VMware VMotion. Live migration is not supported.

Important: If you want to deploy more than one ExtraHop virtual appliance, create the new instance with the original deployment package or clone an existing instance that has never been started.

Network requirements

The following table provides guidance about configuring network ports for your virtual Discover appliance.

Appliance	Management	Monitor
EDA 1000v	One 1-Gbps Ethernet network port is required (for management). The management port must be accessible on port 443.	Two 1-Gbps Ethernet network ports are required. One for the physical port mirror and one for management. The physical

Appliance	Management	Monitor
		port mirror interface must be connected to the port mirror of the switch. While it is possible to configure a 10-Gbps Ethernet network port for the port mirror interface, it is not recommended as the virtual appliance cannot process more than 1 Gbps of traffic.
EDA 2000v	One 1-Gbps Ethernet network port is required (for management). The management interface must be accessible on port 443.	Two to four 1-Gbps Ethernet network ports are required for the physical port mirror and management. The physical port mirror interface must be connected to the port mirror of the switch. The VMware ESX server must support network interface drivers. While it is possible to configure a 10-Gbps Ethernet network port for the port mirror interface, it is not recommended as the virtual appliance cannot process more than 3 Gbps of traffic.
EDA 6100v	One 1-Gbps Ethernet network port is required (for management). The management interface must be accessible on port 443. The management interface can be configured as an additional ERSPAN/RPCAP target.	A 10-Gbps Ethernet network port is recommended for the physical port mirror. The physical port mirror interface must be connected to the port mirror destination on the switch. The VMware ESX server must support network interface drivers. Optionally, you can configure 1-3 1-Gbps Ethernet network ports to receive packet monitor traffic.

Important: If your deployment includes a Command appliance or Reveal(x) 360, the following workflow ensures the best performance for initial device synchronization. First, connect all sensors to the Command appliance or Reveal(x) 360, then configure network traffic forwarding to the sensors.

Note: For registration purposes, the virtual Discover appliance requires outbound DNS connectivity on UDP port 53 unless managed by the ExtraHop Command appliance.

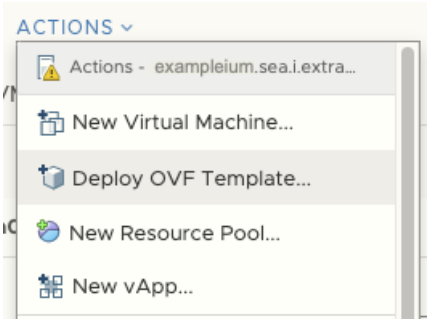
Deploy the OVA file through the VMware vSphere web client

ExtraHop distributes the Discover virtual appliance package in the open virtual appliance (OVA) format.

Before you begin

If you have not already done so, download the ExtraHop Discover virtual appliance OVA file for VMware from the ExtraHop Customer Portal.

1. Start the VMware vSphere web client and connect to your ESX server.
2. Select the data center where you want to deploy the Discover virtual appliance.
3. Select **Deploy OVF Template...** from the Actions menu.



4. Follow the wizard prompts to deploy the virtual machine. For most deployments, the default settings are sufficient.
   a) Select Local file and then click **Choose Files**.
   b) Select the OVA file on your local machine and then click **Open**.
   c) Click **Next**.
   d) Specify a name and location for the appliance and then click **Next**.
   e) Select the destination compute resource location, verify that the compatibility checks are successful and then click **Next**.
   f) Review the template details and then click **Next**.
   g) For Disk Format, select **Thick Provision Lazy Zeroed** and then click **Next**.
   h) Map the OVF-configured network interface labels with the correct ESX-configured interface labels and then click **Next**.
   i) Verify the configuration and then click **Finish** to begin the deployment. When the deployment is complete, you can see the unique name you assigned to the ExtraHop VM instance in the inventory tree for the ESX server to which it was deployed.
5. The Discover appliance contains a preconfigured bridged virtual interface with the network label, VM Network. If your ESX has a different interface label, you must reconfigure the network adapter on the Discover virtual appliance before starting the appliance.
   a) Select the Summary tab.
   b) Click **Edit Settings**, select **Network adapter 1**, select the correct network label from the Network label drop-down list, and then click **OK**.
6. Select the Discover virtual appliance in the ESX Inventory and then select **Open Console** from the Actions menu.
7. Click the console window and then press ENTER to display the IP address.

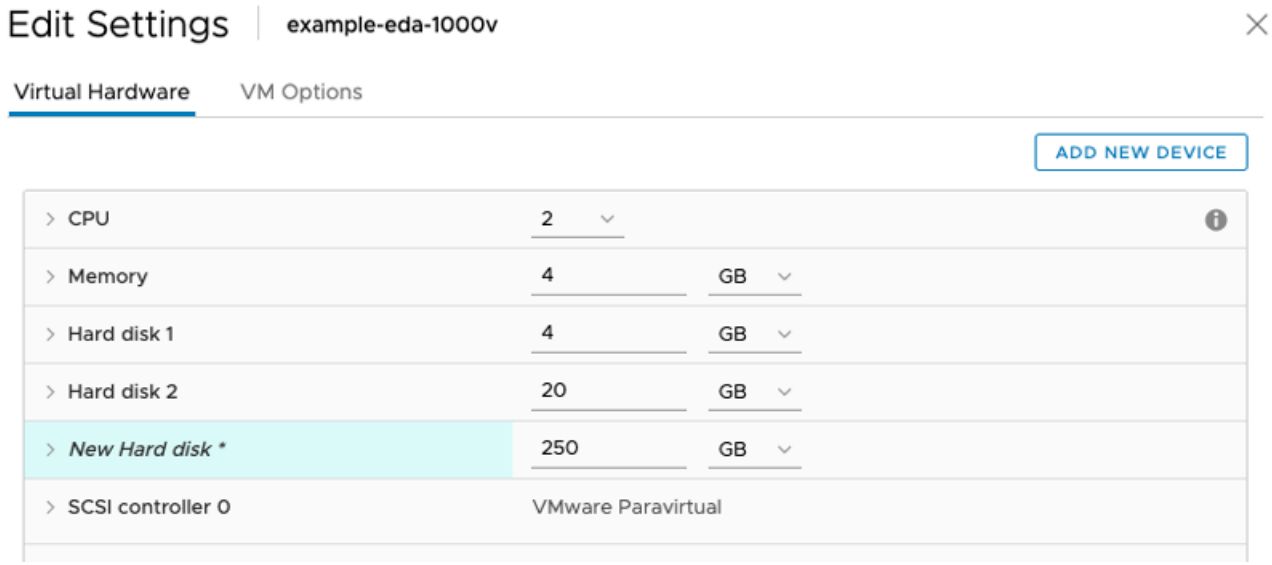
   Note: DHCP is enabled by default on the ExtraHop virtual appliance. To configure a static IP address, see the Configure a Static IP Address section.
8. In VMware ESXi, configure the virtual switch to receive traffic and restart to see the changes.

Add a packet capture disk in VMware

If your Discover appliance is licensed for packet capture you must configure an additional disk to store the packet capture files.

1. Select your Discover appliance virtual machine in the Virtual Machines inventory list.
2. From the Actions drop-down list , select **Edit Settings**.
3. Click **Add New Device** and then click **Hard Disk**.

4. In the New Hard disk field, type the following disk size, based on the Discover appliance you are deploying:
   - 250 GB for the EDA 1000v, EDA 1100v, and EDA 2000v
   - 500 GB for the EDA 6100v



5. Expand the New Hard disk settings and confirm that **Thick Provision Lazy Zeroed** is selected for Disk Provisioning. The remaining disk settings do not need to be changed.
6. Click **OK**.

Configure a static IP address through the CLI

The ExtraHop system is delivered with DHCP enabled. If your network does not support DHCP, no IP address is acquired, and you must configure a static address manually.

Important: For deployments that include a Discover appliance that is connected to a Command appliance, we strongly recommend configuring a unique hostname. If the IP address on the sensor is changed, the Command appliance can re-establish connection easily to the sensor by hostname.

1. Access the CLI through an SSH connection, by connecting a USB keyboard and SVGA monitor to the appliance, or through an RS-232 serial cable and a terminal emulator program. The terminal emulator must be set to 115200 bps with 8 data bits, no parity, 1 stop bit (8N1), and hardware flow control should be disabled.
2. At the login prompt, type `shell` and then press ENTER.
3. At the password prompt, type `default`, and then press ENTER.
4. To configure the static IP address, run the following commands:
   a) Enable privileged commands:

   ```
   enable
   ```

   b) At the password prompt, type `default`, and then press ENTER.
   c) Enter configuration mode:

   ```
   configure
   ```

d) Enter the interface configuration mode:

```
interface
```

e) Run the `ip` command and specify the IP address and DNS settings in the following format: `ip ipaddr <ip_address> <netmask> <gateway> <dns_server>`

For example:

```
ip ipaddr 10.10.2.14 255.255.0.0 10.10.1.253 10.10.1.254
```

f) Leave the interface configuration section:

```
exit
```

g) Save the running config file:

```
running_config save
```

h) Type y and then press ENTER.

Configure the Discover appliance

After you configure an IP address for the Discover appliance, open a web browser and navigate to the ExtraHop system through the configured IP address. Accept the license agreement and then log in. The default login name is `setup` and the password is `default`. Enter the product key to license the system.

After the system is licensed, and you have verified that traffic is detected, complete the recommended procedures in the post-deployment checklist.

Mirror Wire Data

This section includes procedures for mirroring data to your ExtraHop virtual appliance.

Mirroring internal and external traffic

The ExtraHop Discover virtual appliance can be configured to monitor network traffic in the following network configuration examples.

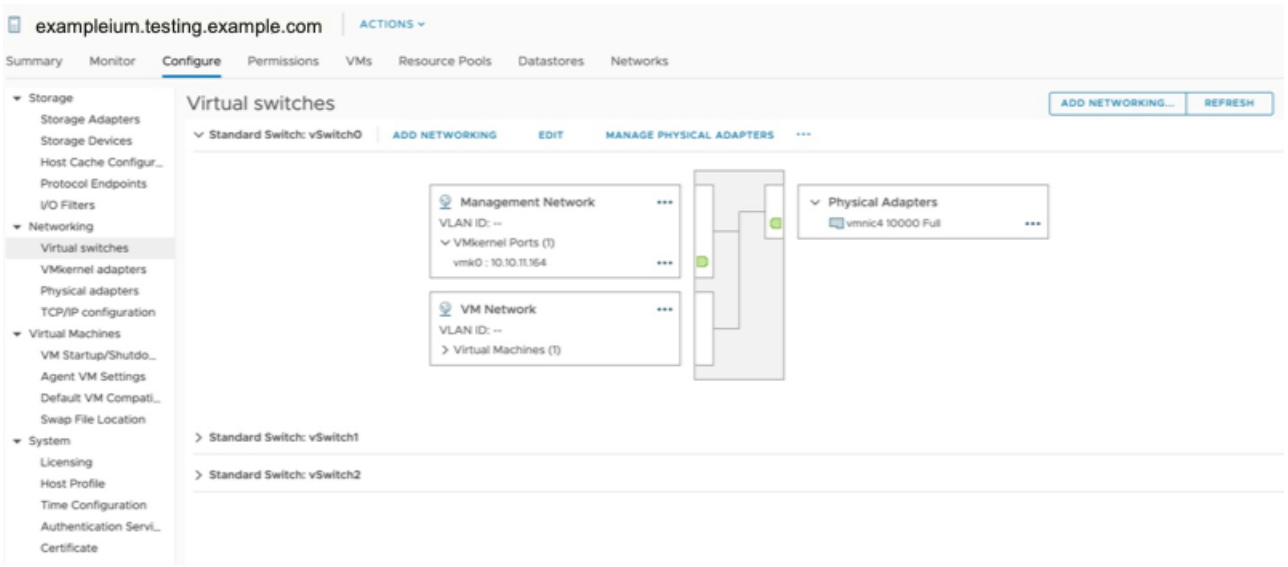
- Monitoring Intra-VM Traffic
  - One virtual interface on the EDA 1000v
  - Up to three virtual interfaces on the EDA 2000v or EDA 6100v
- Monitoring external mirrored traffic to the VM
- Monitoring external mirrored traffic to the VM (EDA 2000v or EDA 6100v)
- Monitoring both intra-VM and external mirrored traffic to the VM (EDA 2000v or EDA 6100v)

Note: Monitoring external network-mirrored traffic requires an external NIC and an associated virtual switch.

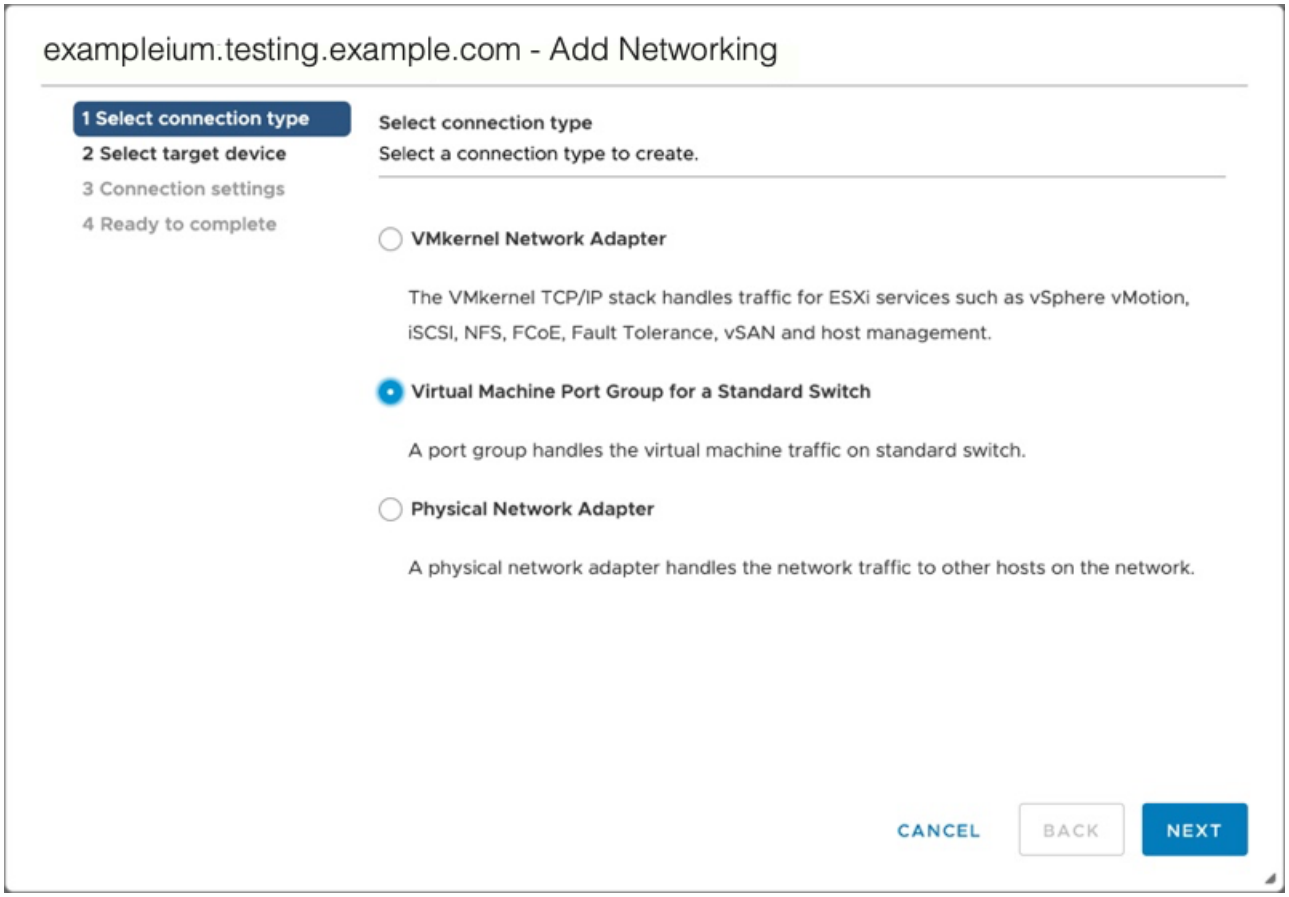
Monitoring intra-VM traffic

This scenario requires a second VM port group on the default virtual switch of the ESX host for monitoring traffic within the virtual switch as well as external traffic in and out of the switch.

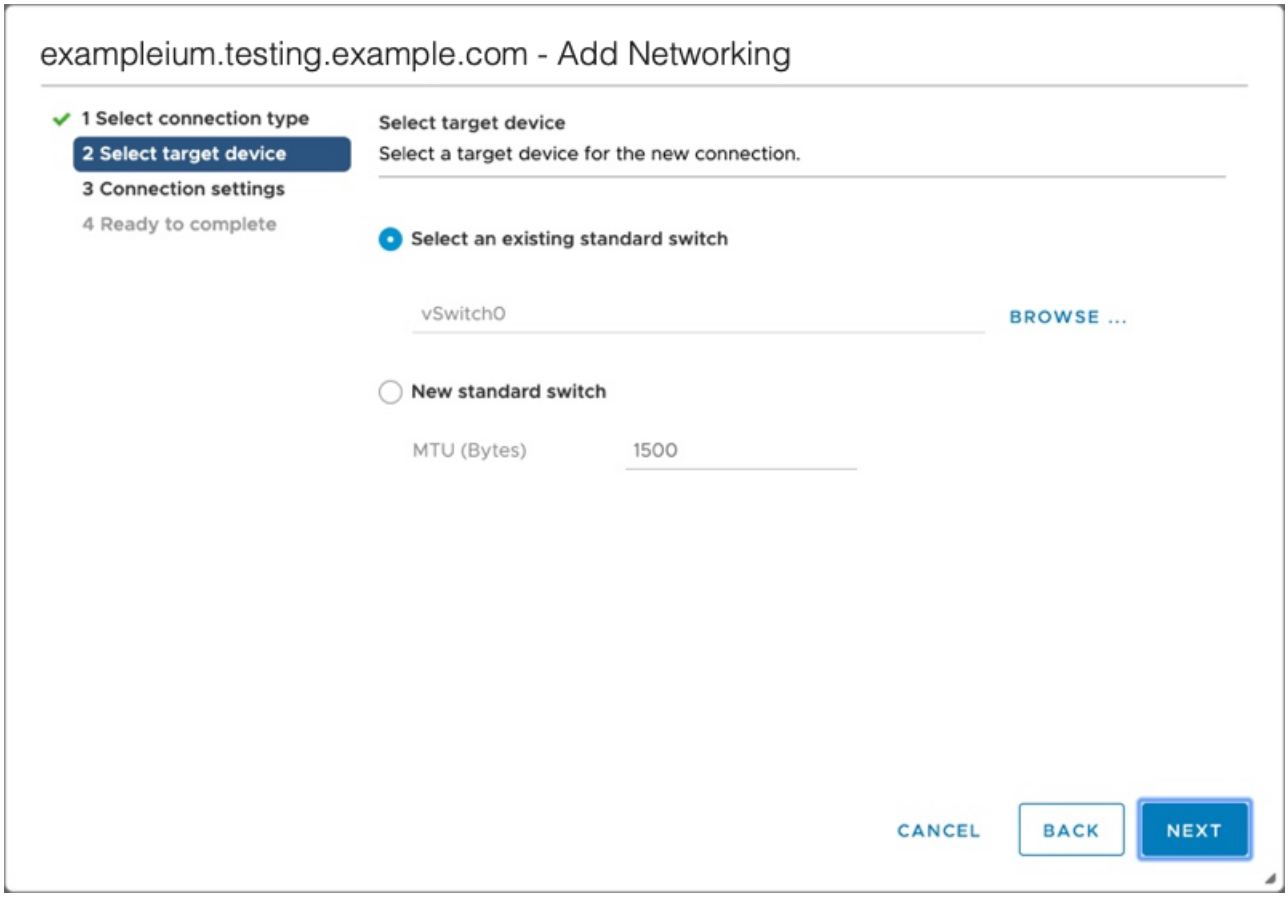
1. Start the VMware vSphere client and connect to your ESX server.
2. Select the ESX host at the top of the tree control in the left panel and then click the **Configure** tab.
3. In the **Networking** section, click Virtual Switches.



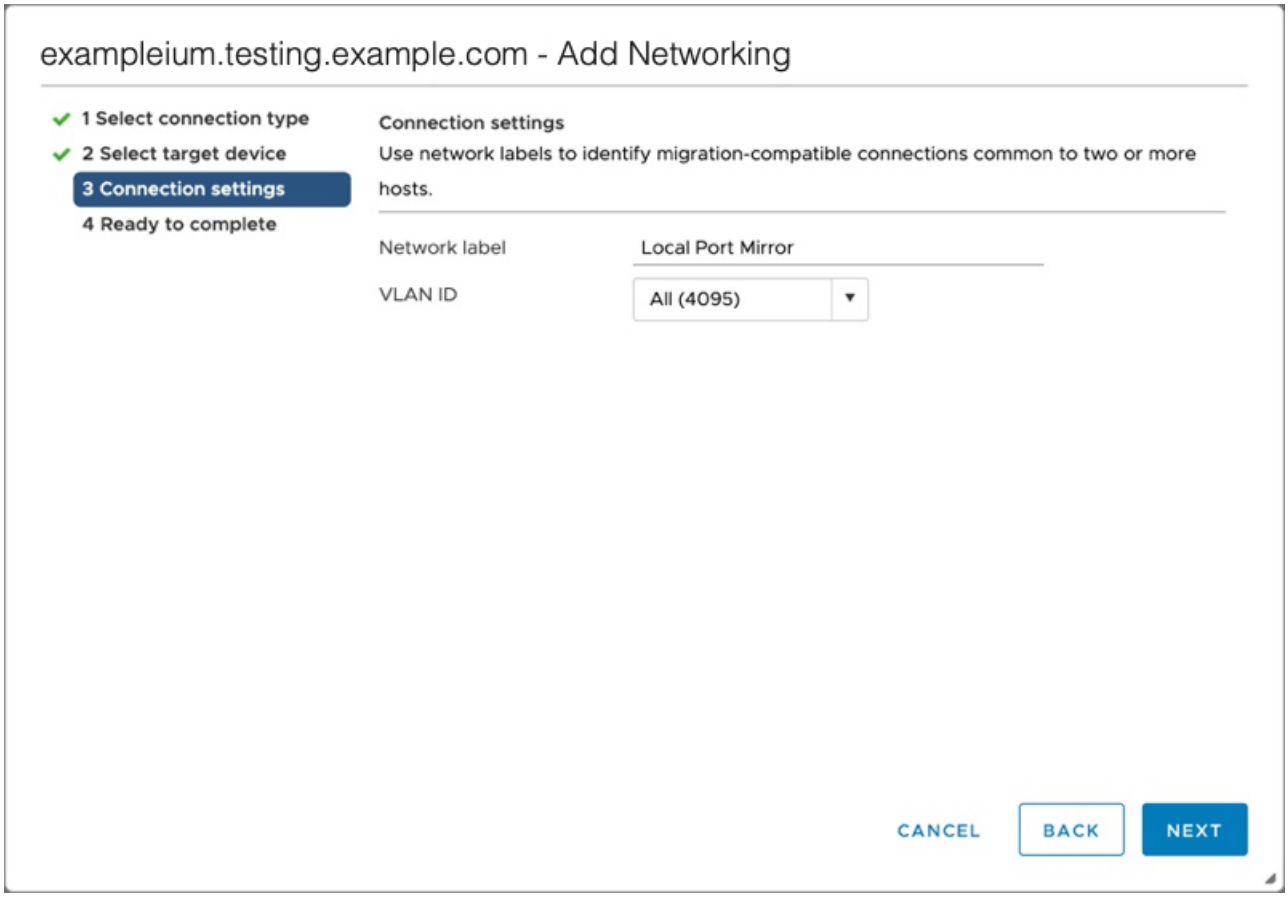
4. To add a port group to the vSwitch0, click **Add Networking**.
   The Add Networking window appears.
5. Select **Virtual Machine Port Group for a Standard Switch** as the connection type and then click **Next**.



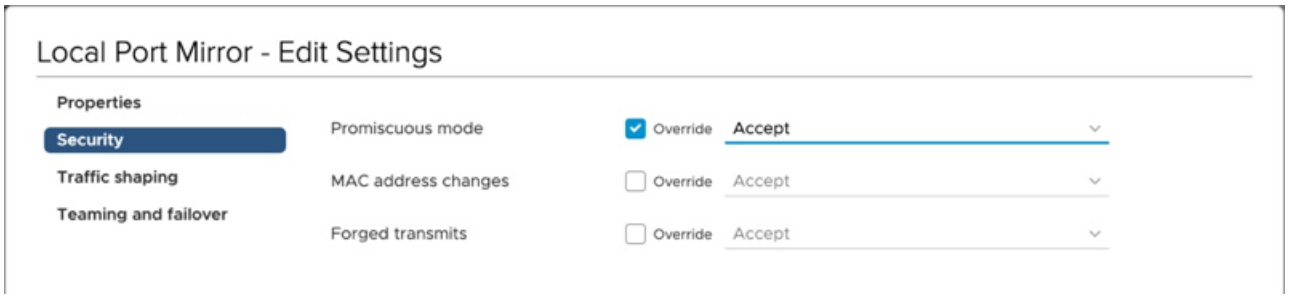
6. In the Select target device step, choose **Select an existing standard switch** and then click **Next**. The default switch is vSwitch0.



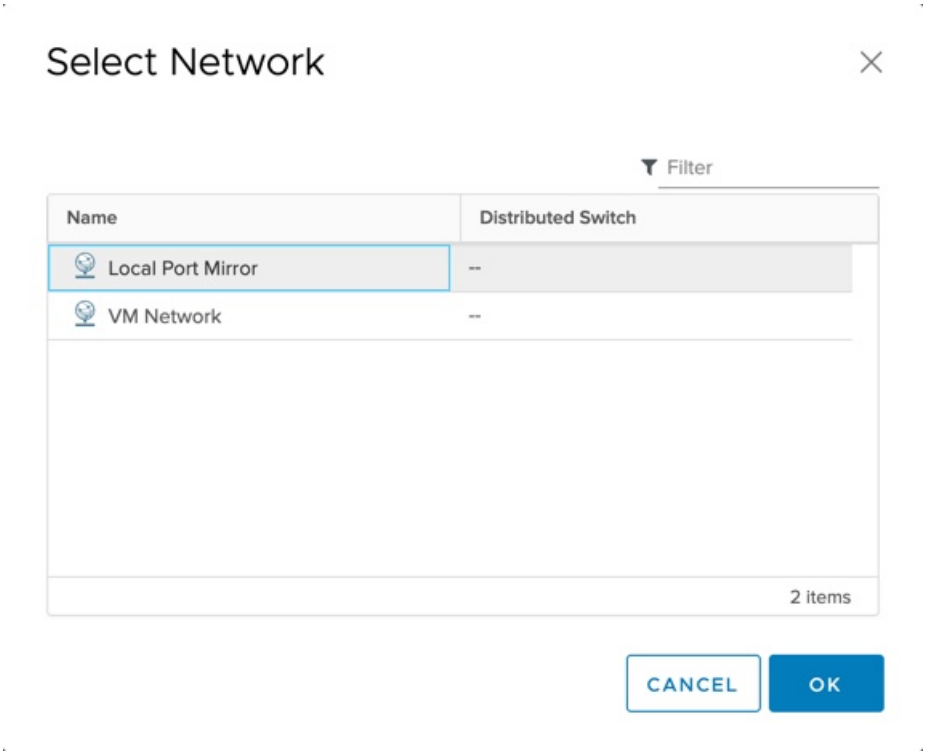
7. In the Connection settings step, assign a unique name to the new port group, click the **VLAN ID** drop-down menu, and select **All (VLAN 4095)**.



8. Click **Next**.
9. Click **Finish**.
10. Set the Remote Port Mirror to Promiscuous Mode as follows.
    a) In the vSwitch0 section, click the edit menu icon ... next to the new port group and click **Edit**.
    b) Click **Security**.
    c) Select the override checkbox next to Promiscuous mode set the Promiscuous Mode to **Accept**, and then click **OK**.



11. Click **VMs** from the top menu.
12. Right-click the name of the Discover appliance virtual machine and click **Edit Settings**.
13. Click **Network Adapter 2**.
14. Select **Browse** from the drop-down menu.
15. Click **Local Port Mirror**, and then click **OK**.

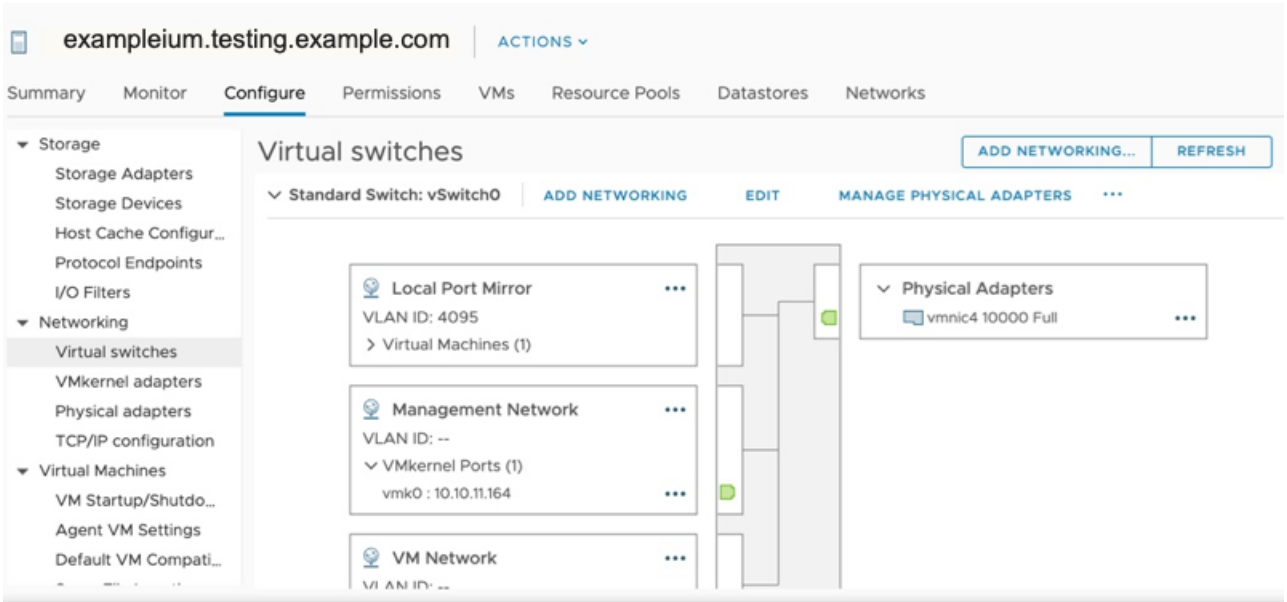


16. Verify that Local Port Mirror appears next to Network Adapter 2 in the Edit Settings window, and then click **OK**.
17. Restart the Discover virtual appliance to activate the new adapter setting.

Monitoring external mirrored traffic to the VM

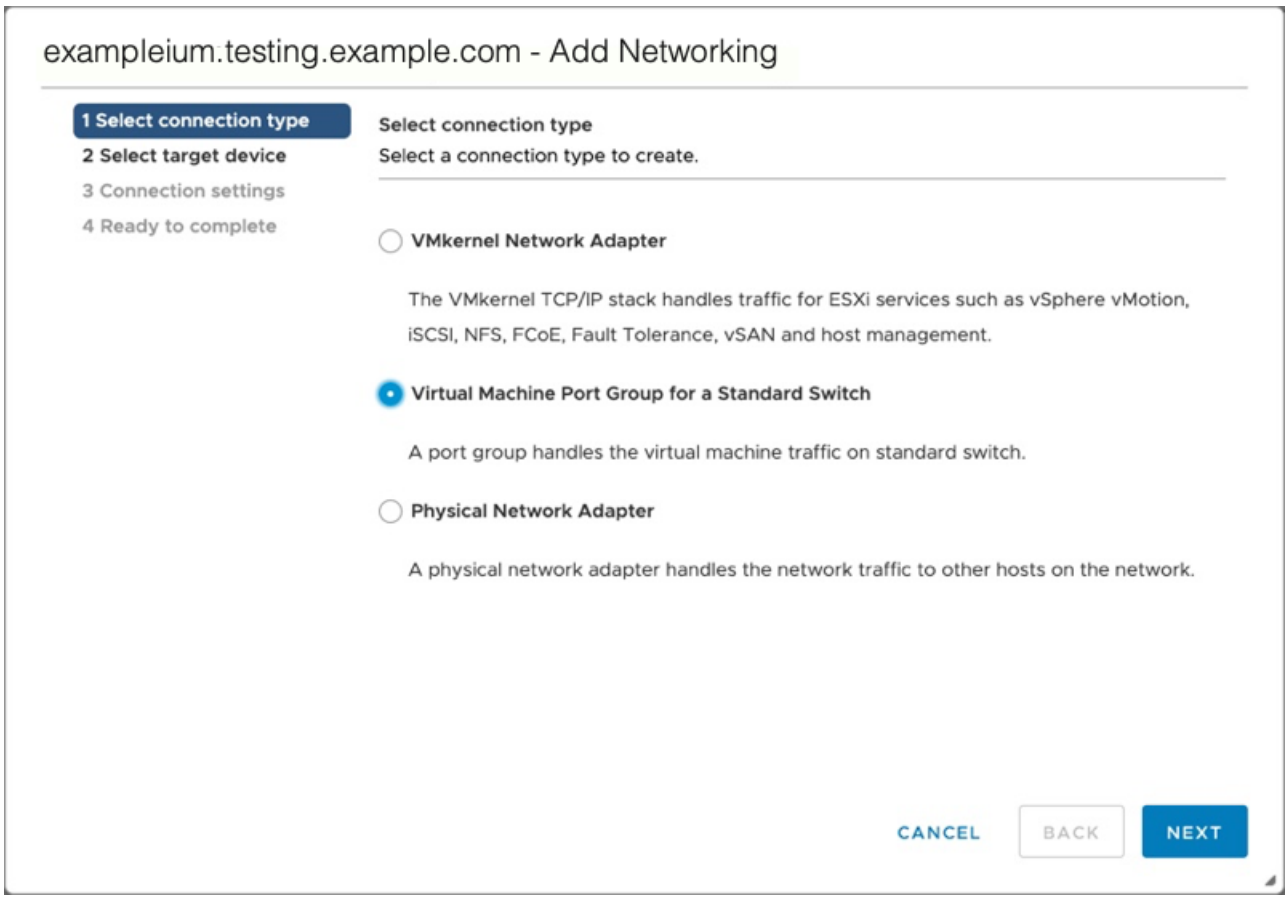
This scenario requires a second physical network interface and the creation of a second vSwitch associated with that NIC. This NIC then connects to a mirror, tap, or aggregator that copies traffic from a switch. This setup is useful for monitoring the intranet of an office.

1. Start the VMware vSphere client and connect to your ESX server.
2. Select the ESX host at the top of the tree control in the left panel and then click the **Configure** tab.
3. Click **Networking**.

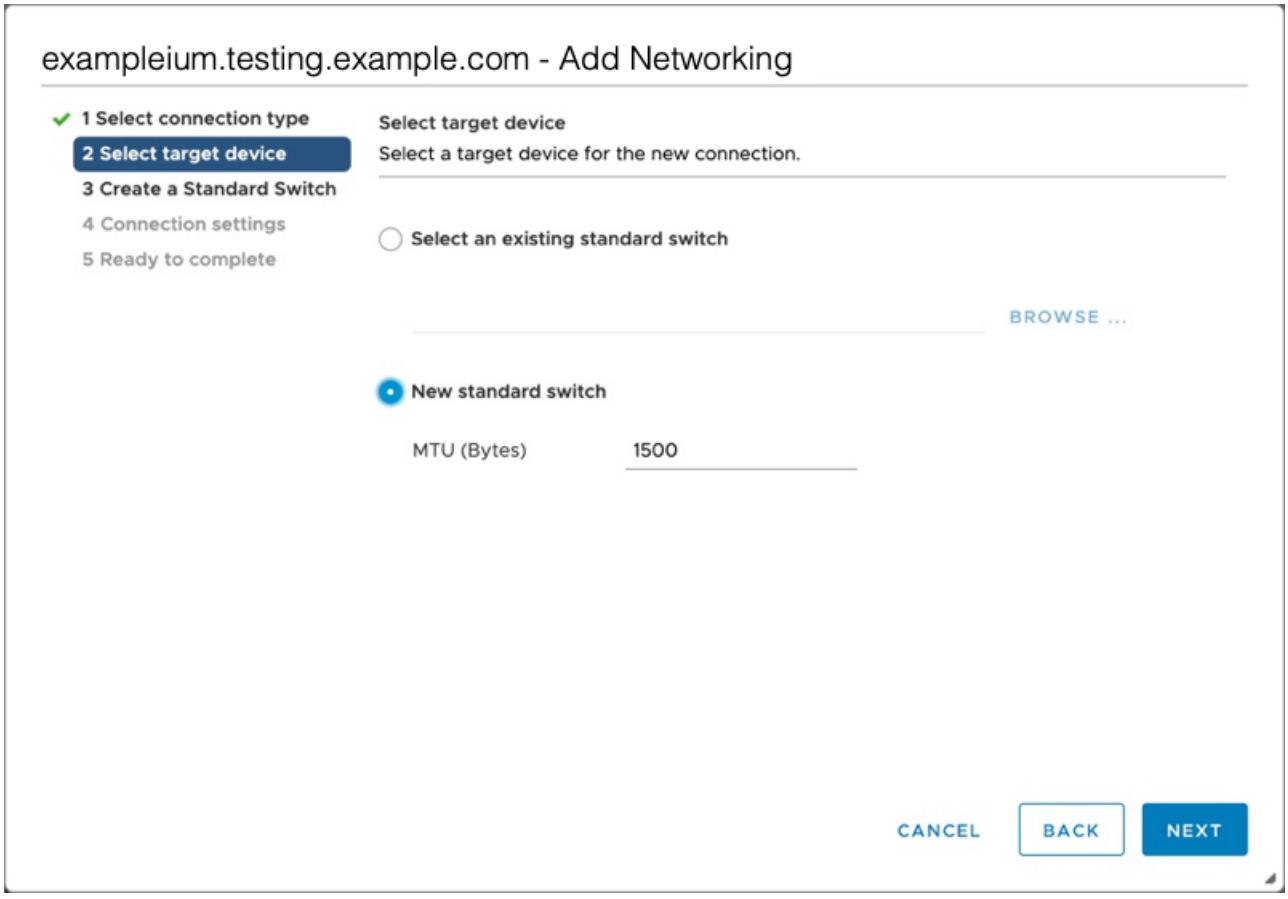


This view shows how the virtual switch is configured. It displays the physical NIC to which the vSwitch is tied (vmnic4 is eth0) and which networking components are connected to that vSwitch.

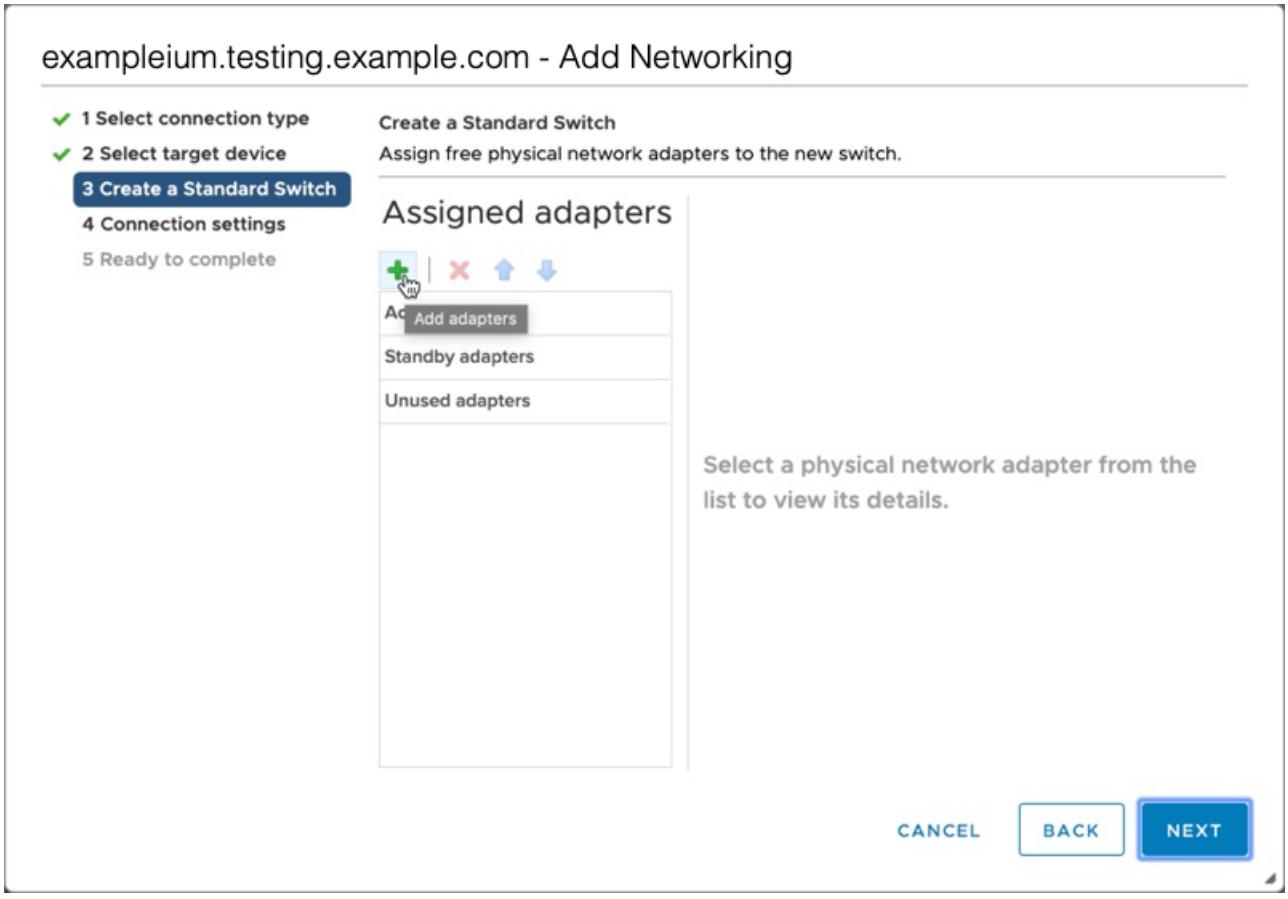
4. To add a second vSwitch, click **Add Networking**. The Add Network Wizard window appears.
5. Select **Virtual Machine Port Group for a Standard Switch** as the connection type and then click **Next**.



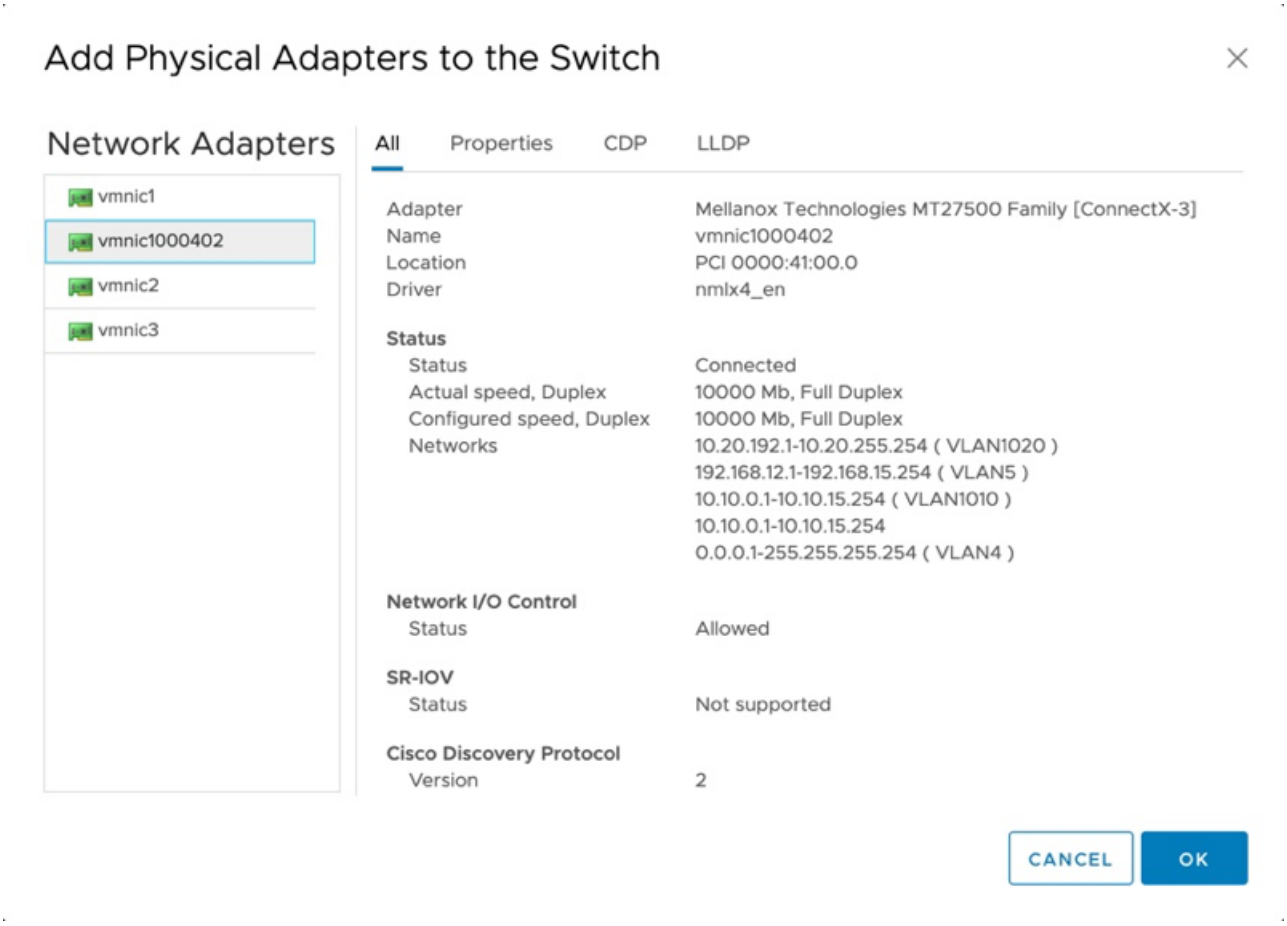
6. In the Select target device step, select **New standard switch**, and then click **Next**.



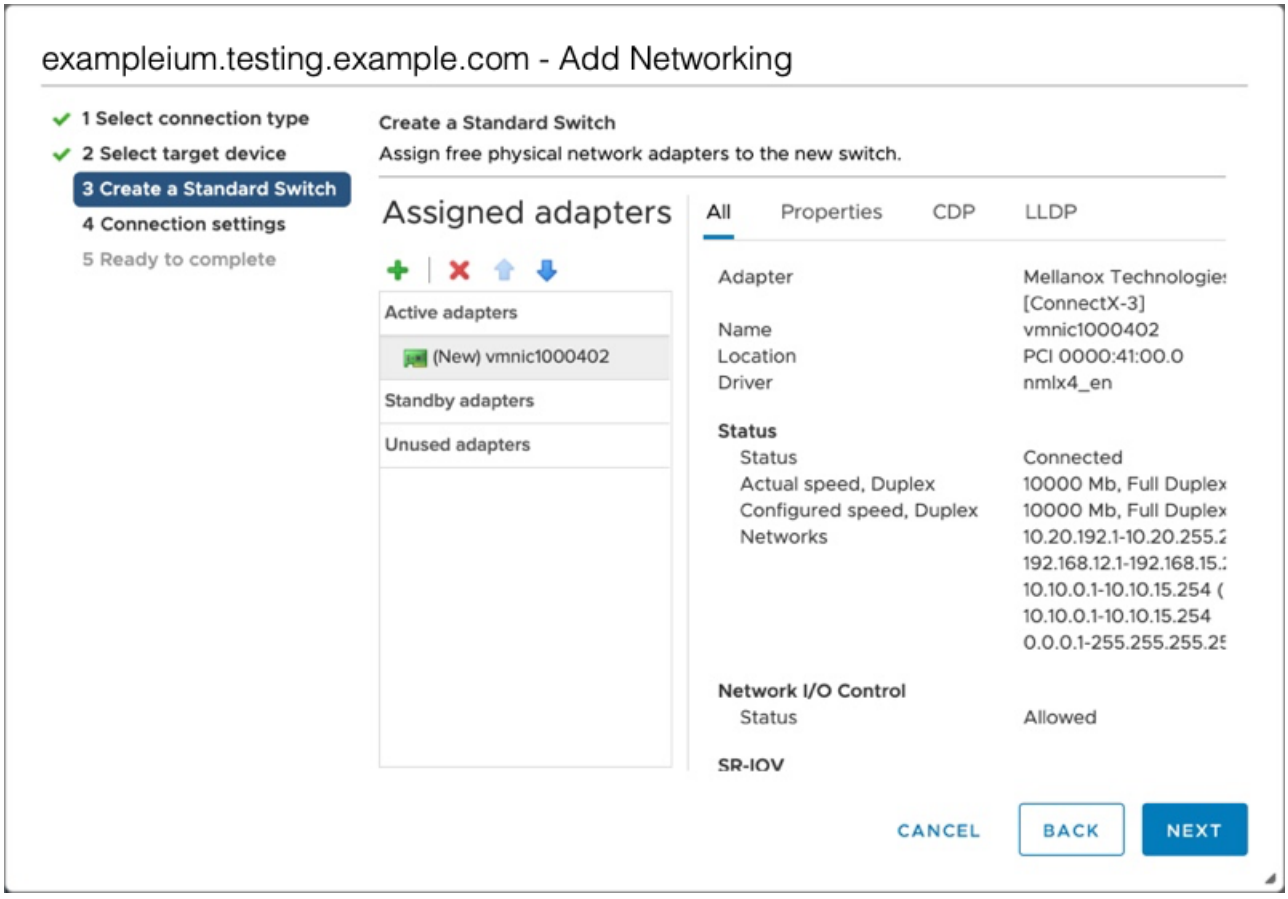
7. In the Create a Standard Switch step, click the Add adapters icon (**+**).



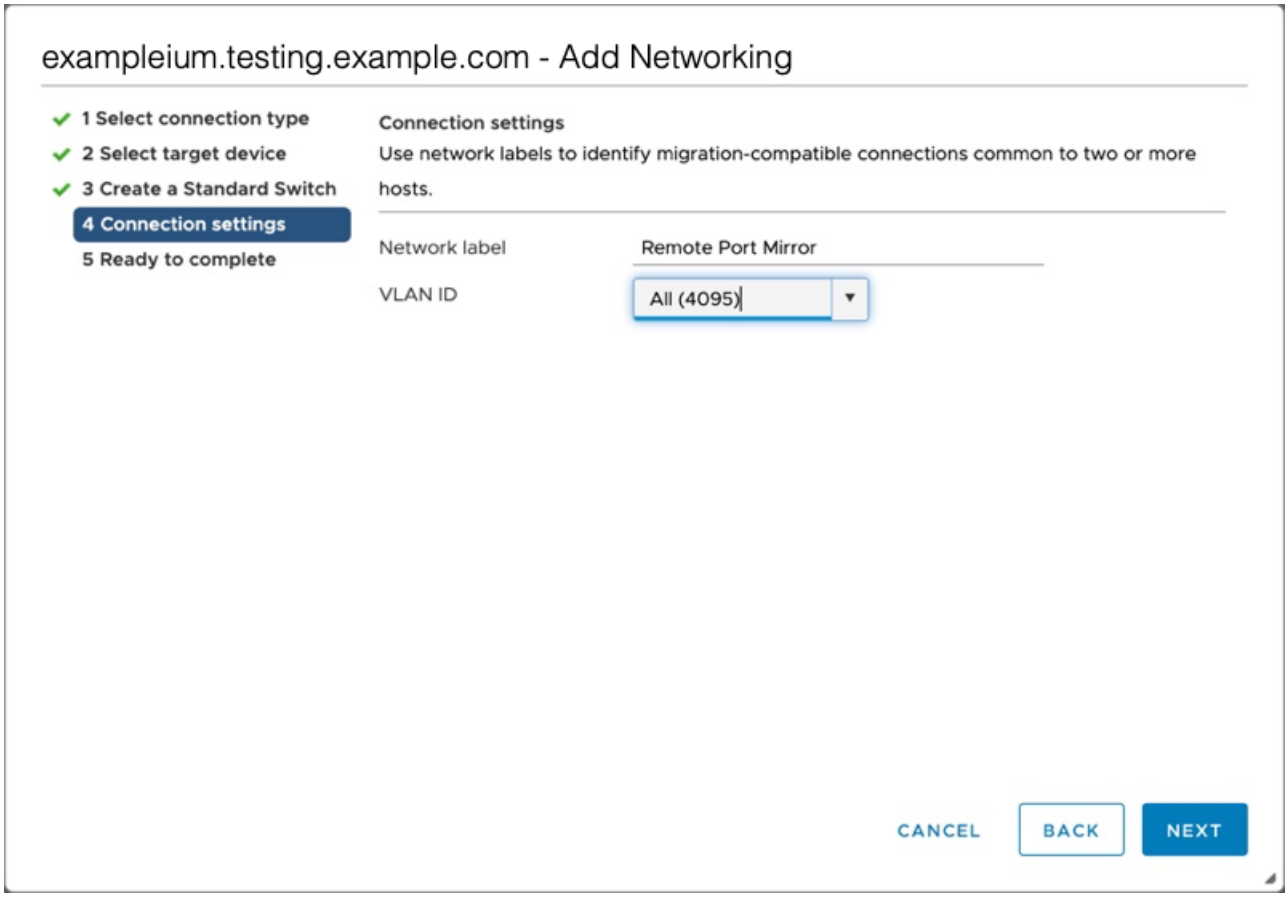
8. Select the NIC interface for external traffic mirroring, and then click **OK**.



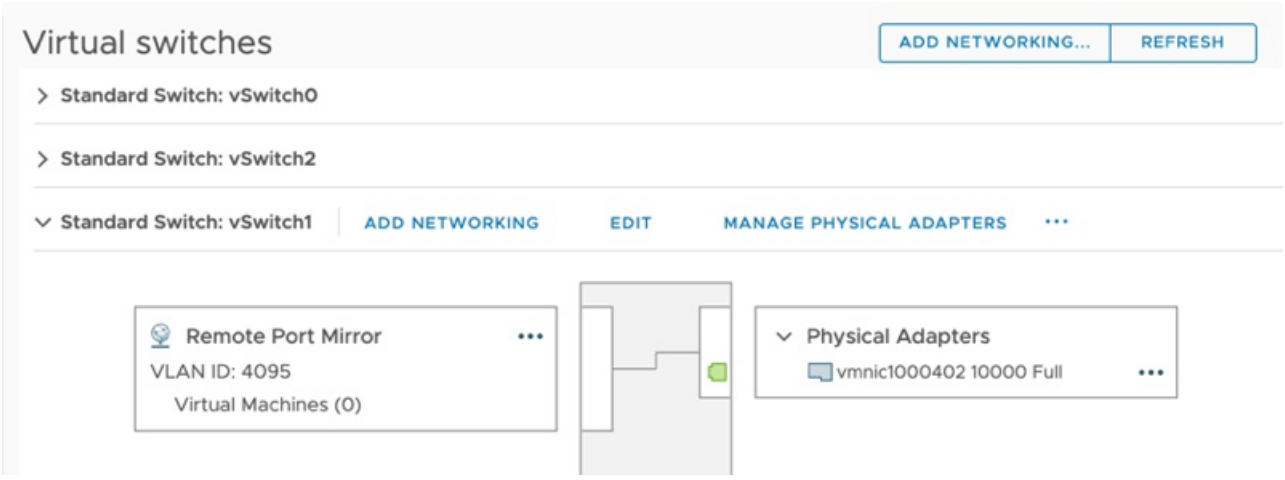
9. Verify the assigned adapter and then click **Next**.



10. In the Connection settings step, type a unique name in the Network label field, select **All (VLAN 4095)** from the VLAN ID drop-down menu, and then click **Next**.

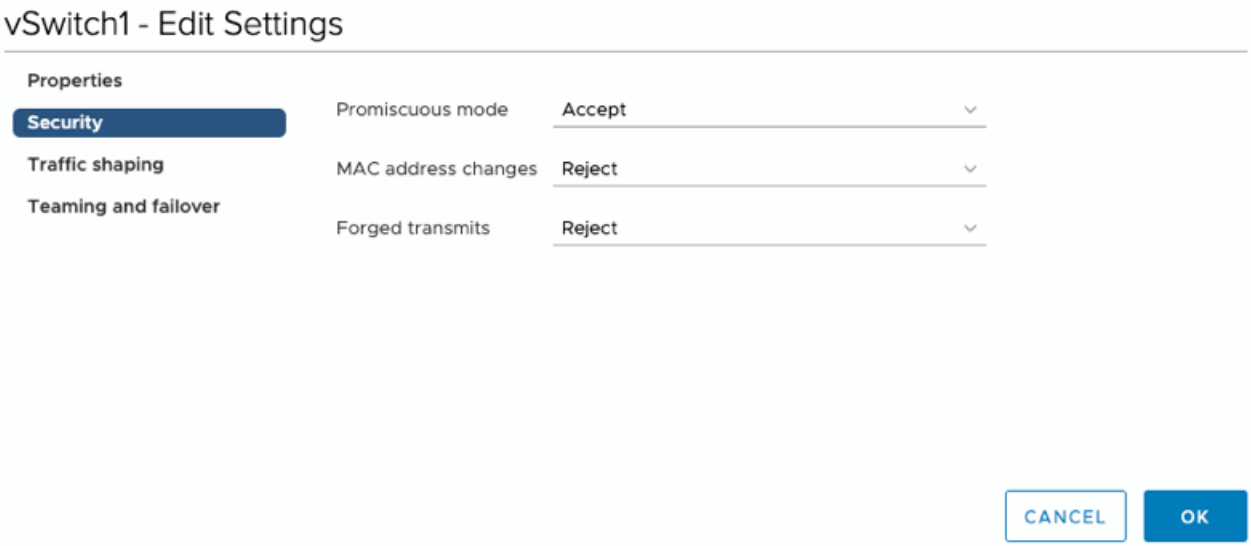


11. Review your settings and then click **Finish**.
12. Set the Remote Port Mirror to Promiscuous Mode as follows.
    a) Click **Edit** next to vSwitch1.

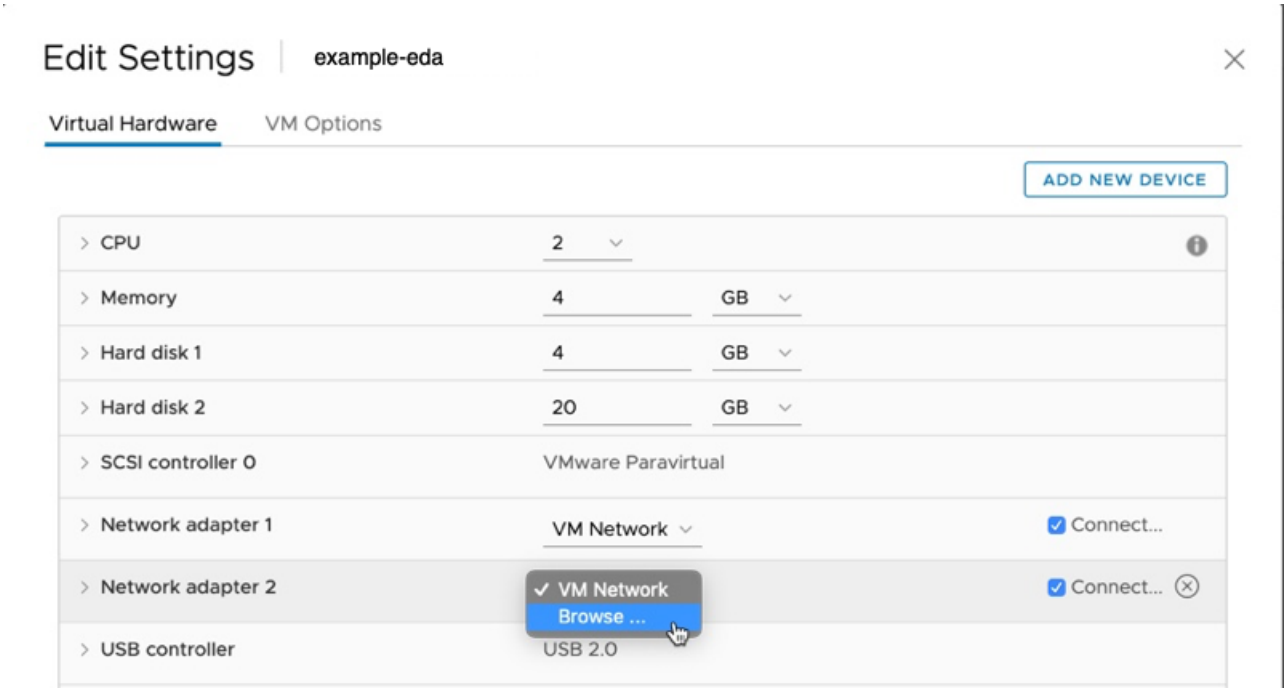


    b) Click the **Security** tab, set the Promiscuous Mode to **Accept**, and then click **OK**.

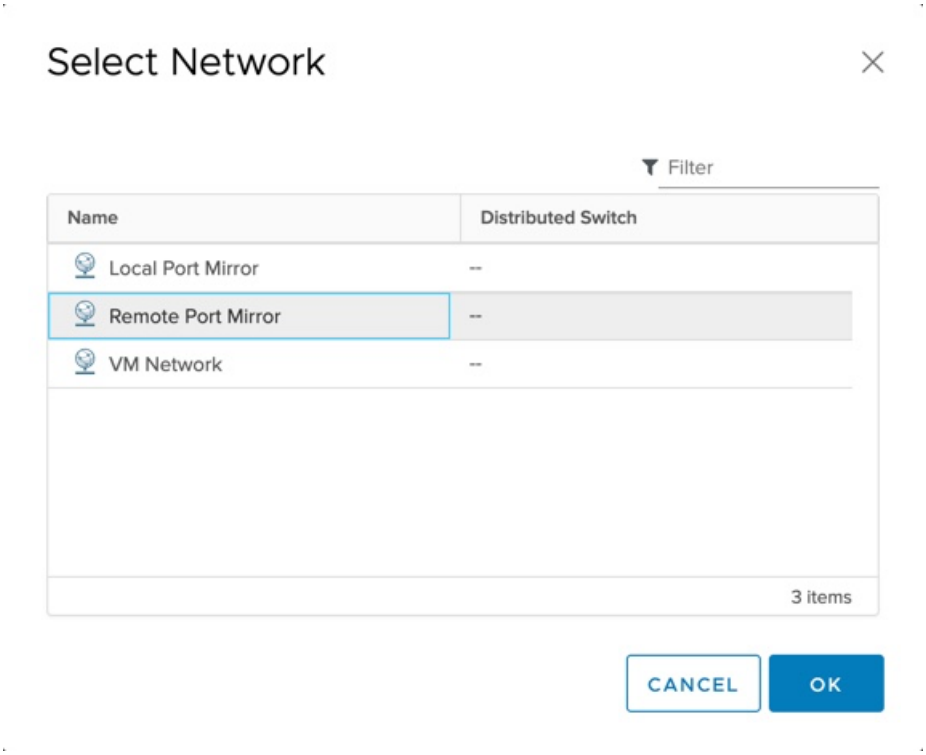
> **Note:** Mac address changes and Forged transmits are set to **Accept** by default. You can change these settings to **Reject** if required for your environment.



13. In the left panel, select the ExtraHop virtual appliance.
14. Click the **Actions** drop-down menu and then select **Edit Settings...**.
15. Click **Network Adapter 2** and then click **Browse...** from the drop-down menu.



16. Click **Remote Port Mirror**, and then click **OK**.



17. Restart the ExtraHop VM to activate the new adapter setting.

Monitoring external mirrored traffic to the VM (EDA 2000v or EDA 6100v)

In this scenario, you must create a third and fourth physical network interface and two more vSwitches associated with those NICs. These NICs then connect to a mirror, tap, or aggregator that copies traffic from a switch.

1. Start the VMware vSphere client and connect to your ESX server.
2. Select the ESX host at the top of the navigation tree in the left panel and then click the **Configure** tab.
3. Click **Networking** and then click **Add Networking**.
4. Select **Virtual Machine Port Group for a Standard Switch** as the connection type and then click **Next**.
5. In the Select target device step, choose **Select an existing standard switch** and then click **Next**. The default switch is vSwitch0.
6. In the Connection settings step, assign a unique name to the new port group (`Remote Port Mirror` 2, for example), click the **VLAN ID** drop-down menu, and select **All (VLAN 4095)**.
7. Click **Next** and then click **Finish**.
8. Set the Remote Port Mirror to Promiscuous Mode as follows.
   a) Click **Edit** next to vSwitch2.
   b) Click the **Security** tab, set the Promiscuous Mode to **Accept**, and then click **OK**.

   Note: Mac address changes and Forged transmits are set to **Accept** by default. You can change these settings to **Reject** if required for your environment.
9. In the left panel, select the ExtraHop virtual appliance.
10. Click the **Actions** drop-down menu and then select **Edit Settings...**.
11. Click **Network Adapter 3** and then click **Browse...** from the drop-down menu.
12. Click **Remote Port Mirror 2**, and then click **OK**.
13. Repeat steps 3 through 10 to add a fourth vSwitch.
14. Restart the ExtraHop VM to activate the new adapter setting.

Monitoring both intra-VM and external mirrored traffic to the VM (EDA 2000v or EDA 6100v)

In this scenario, you can monitor a mix of intra-VM and external mirrored traffic on up to three virtual interfaces.

1. To monitor intra-VM traffic on one or more virtual interfaces, create a VM port group on the default virtual switch of the ESX host for each interface as described in Monitoring Intra-VM Traffic.
2. To monitor external mirrored traffic on one or more virtual interfaces, create a physical network interface and corresponding vSwitch for each interface as described in Monitoring External Mirrored Traffic to the VM.
3. Click **Network Adapter x** and select an option from the **Network label** drop-down list for each interface.

Mirroring VLANs

To mirror VLANs, you must either set the destination port on the port mirror configuration to VLAN Trunking or set the exact VLAN ID on the ports of the VLANS you are mirroring.

Related documentation

For information about configuring RSPAN, ERSPAN, and RPCAP to monitor remote devices, see the following topics.

- Configure RSPAN with VMware
- Configure ERSPAN with VMware
- Configure ERSPAN with the Nexus 1000V
- Packet Forwarding with RPCAP