

Install the EH1000v/2000v with Hyper-V

Contents

Install the EH1000v/2000v with Hyper-V	1
Introduction	3
Feedback	4
Related Documentation	4
How Mirroring Works	5
Network-Based Mirroring	5
Host-Based Mirroring	6
Installation Requirements	8
Disk Requirements and Recommendations	8
System Requirements: 1000v	9
System Requirements: 2000v	10
Installing the ExtraHop VM	11
Installing the Files for Hyper-V	12
Applying the ExtraHop License	23
Configuring a Static IP Address	27
Mirror Wire Data	28
Mirroring Internal and External Traffic	29
Software Tap	35

Introduction

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 using intra-VM traffic.

This guide explains how to install these products:

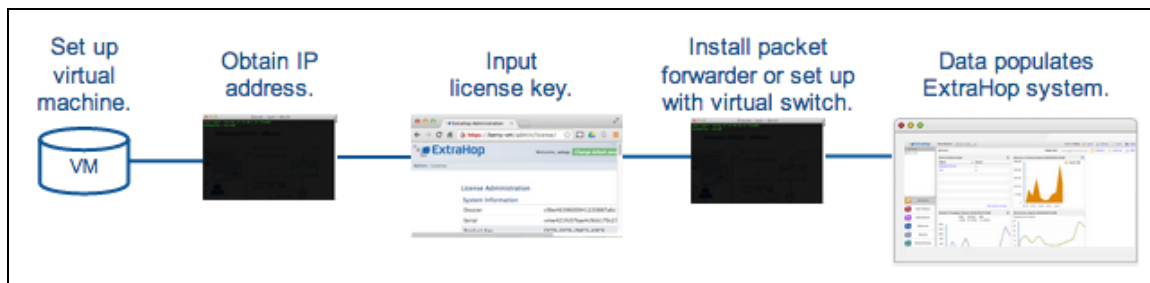
- EH1000v (Monitors up to 250 devices)
- EH2000v (Monitors up to 1000 devices)

On these platforms:

- Hyper-V (Microsoft)

We assume you have some experience administering your hypervisor product.

The following diagram shows the high-level steps to install and use the ExtraHop virtual appliance. Installation time is approximately 15 minutes.



Feedback

We are working hard to improve our product, and with your feedback we can better meet your needs. As a valued ExtraHop customer, we appreciate all feedback you can provide. Please email feedback to the following addresses:

- **Feature requests:** pm@extrahop.com
- **Defects:** support@extrahop.com
- **Documentation:** documentation@extrahop.com
- **Other:** support@extrahop.com

Related Documentation

Use the following documentation to assist you with the procedures in this guide:

- **ExtraHop Admin UI Users Guide:** <https://docs.extrahop.com/current/admin-ui-users-guide/>

How Mirroring Works

ExtraHop is a passive system.

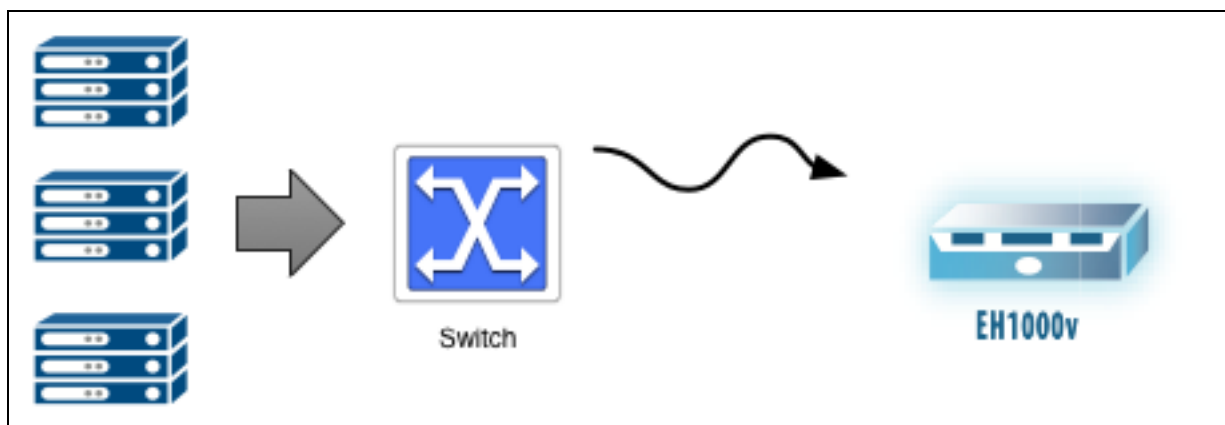
Its wire data feed comes entirely from mirrored traffic. This is an improvement from traditional methods of collecting wire data with packet analyzers. With ExtraHop, the traffic is mirrored directly into the appliance and then reassembled into full per-client sessions and transaction streams, offering you the entire transaction payload in real time to analyze. There are two ways to mirror traffic into ExtraHop: network-based mirroring and host-based mirroring. This topic discusses the differences between the two.

Network-Based Mirroring

The big advantage with network based mirroring is that you can set it up at the network level, capturing traffic from multiple hosts with a minimum amount of configuration. There are different types of network-based mirroring, each designed for mirroring traffic to a target in a particular situation. The big challenge with all the network-based mirroring strategies is that they rely heavily on the capabilities of the hardware on your network (physical or virtual). If you're running a virtual ExtraHop appliance, the hypervisor you're running (and even the version of hypervisor) also plays into the equation. That said, if you can take advantage of network-based mirroring you'll probably want to because once it's set up, it requires less administrative effort to maintain.

There are three main types of network-based mirroring.

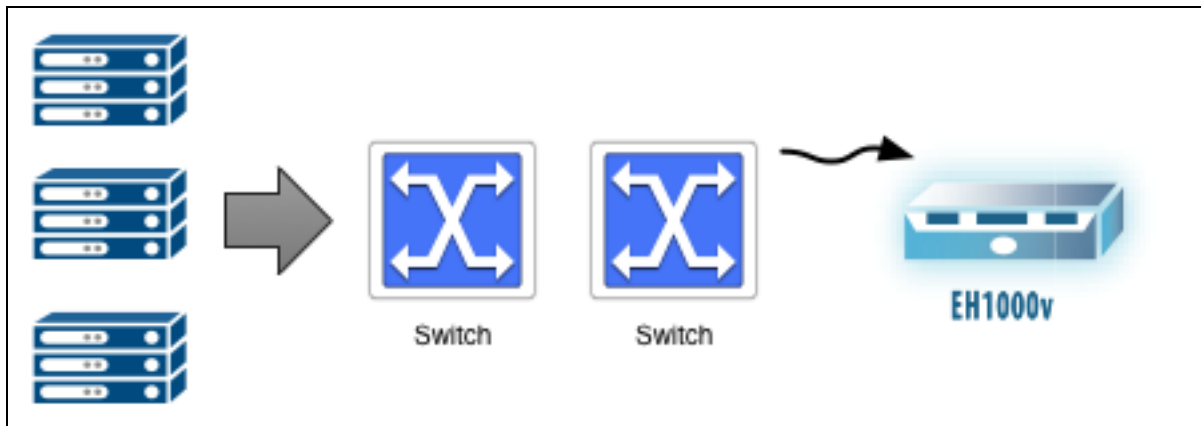
SPAN



The SPAN port is the name of the port on Cisco switches that mirrors traffic. SPAN stands for Switched Port ANalyzer (SPAN). Different vendors use different names, but spanning has become synonymous for a port on a switch that mirrors traffic. The key thing about a SPAN is that it's all local traffic. You can configure any of the ports on the switch to mirror traffic to an ExtraHop appliance that has access to the SPAN port.

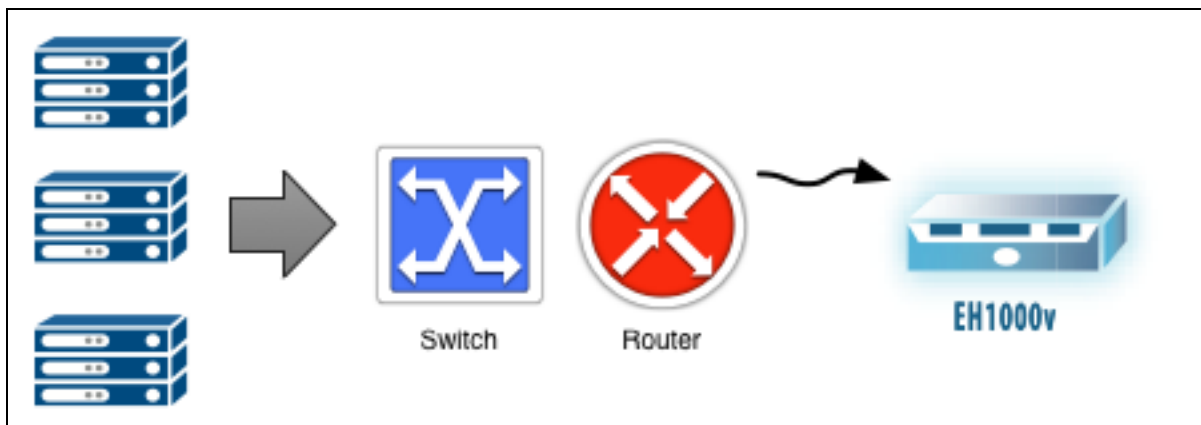
Promiscuous mode is similar to SPAN, but instead of mirroring only select local port traffic to the SPAN port, promiscuous mode mirrors all the traffic from every port. Any traffic that comes through the switch is mirrored to your ExtraHop appliance.

RSPAN



RSPAN is useful if the traffic you’re interested in mirroring is more than one switch away from where you can attach your ExtraHop appliance. The “R” in RSPAN stands for remote. You’re spanning all the traffic from one switch through any number of additional switches to your target ExtraHop appliance using a dedicated mirroring VLAN. Each switch in the path needs to be configured to carry the dedicated VLAN that contains the mirror traffic.

ERSPAN

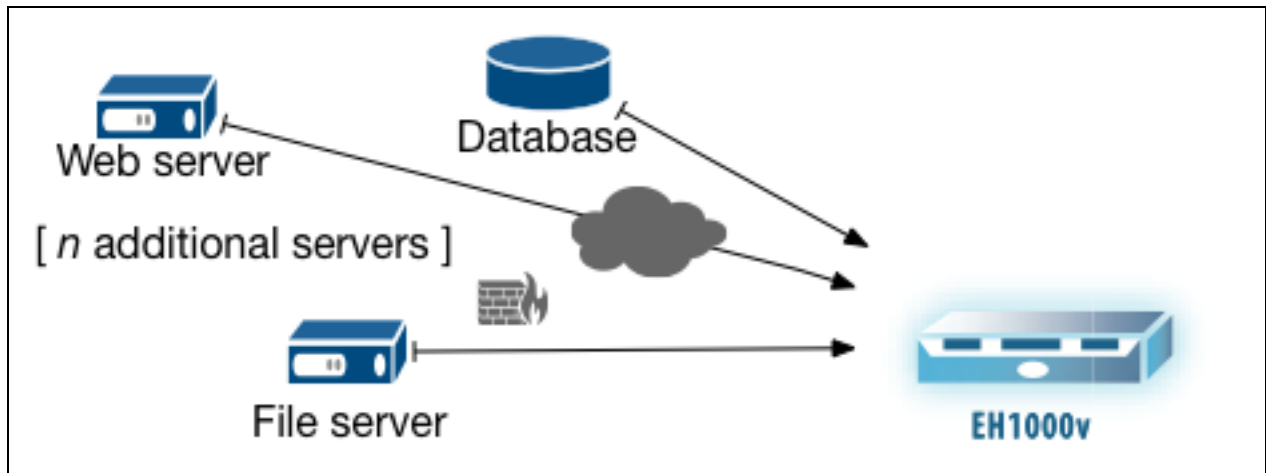


If a Layer 3 (L3) boundary (such as a Router, Firewall, or Layer 3 Switch) sits between the traffic you’re interested in mirroring and where you can attach your ExtraHop appliance, ERSPAN may be helpful to you. To cross the Layer 3 boundary, ERSPAN encapsulates the mirror traffic in a GRE tunnel addressed to the IP address of a capture interface on the ExtraHop appliance. The encapsulated mirror traffic navigates the network just as any other packet would.

Host-Based Mirroring

If network-based mirroring won’t work for you, then host-based mirroring is a reliable way to get traffic into ExtraHop.

Software Tap



Host-based mirroring requires that you install a software tap on each host you want to monitor. The big advantage of the software tap is that it works with any type of network gear you have. It works independent of the type or version of hypervisor you're running. Host-based mirroring is a way of configuring the adapter on a host to duplicate and forward all traffic to ExtraHop. You can install it on Windows or Linux hosts.

The software tap (also called RPCAP and a packet forwarder) is analogous to a network tap, which is an unobtrusive hardware device for mirroring traffic from a network.

Installation Requirements

This section includes hardware and software requirements for the host on which you are installing the ExtraHop virtual appliance.

Disk Requirements and Recommendations

To ensure proper functionality of the virtual appliance:

- Do not change the default disk size on initial installation. Using 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 changing it.
- 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.

System Requirements: 1000v

Installation of the EH1000v has the following requirements:

- An existing installation of Hyper-V on Windows Server 2012
- A Hyper-V Manager client

The following server hardware is required for the EH1000v:

- **Processor:** 2 processing cores with hyper-threading support, VT-x technology, and 64-bit architecture
To use SSL decryption, three processing cores are required. Refer to *ExtraHop Guide: Adding a CPU Core to the EH1000v with Hyper-V* for more information.
- **Memory:** 4 GB or higher
- **Disk:** 46 GB or higher (thick-provisioned)
- **Network:** You can configure the EH1000v to monitor intra-VM or external traffic.
 - **Intra-VM:** One 1-Gbps Ethernet network port is required (for management). The management port must be accessible on port 443.
 - **External:** Two 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. While it is possible to use 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.
- **Registration:** For registration purposes, the EH1000v requires outbound DNS connectivity on UDP port 53 unless managed by the ExtraHop Central Manager (ECM).

System Requirements: 2000v

Installation of the EH1000v has the following requirements:

- An existing installation of Hyper-V on Windows Server 2012
- A Hyper-V Manager client

The following server hardware is required for the EH2000v:

- **Processor:** 6 processing cores with hyperthreading support, VT-x technology, and 64-bit architecture
To use SSL decryption, three processing cores are required. Refer to *ExtraHop Guide: Adding a CPU Core to the EH1000v with Hyper-V* for more information.
- **Memory:** 6 GB or higher
- **Disk:** 255 GB or higher (thick-provisioned)
- **Network:** You can configure the EH2000v to monitor intra-VM or external traffic.
 - **Intra-VM:** One 1-Gbps Ethernet network port is required (for management). The management interface must be accessible on port 443.
 - **External:** 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. While it is possible to use 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.
- **Registration:** For registration purposes, the EH2000v requires outbound DNS connectivity on UDP port 53 unless managed by the ExtraHop Central Manager (ECM).

Installing the ExtraHop VM

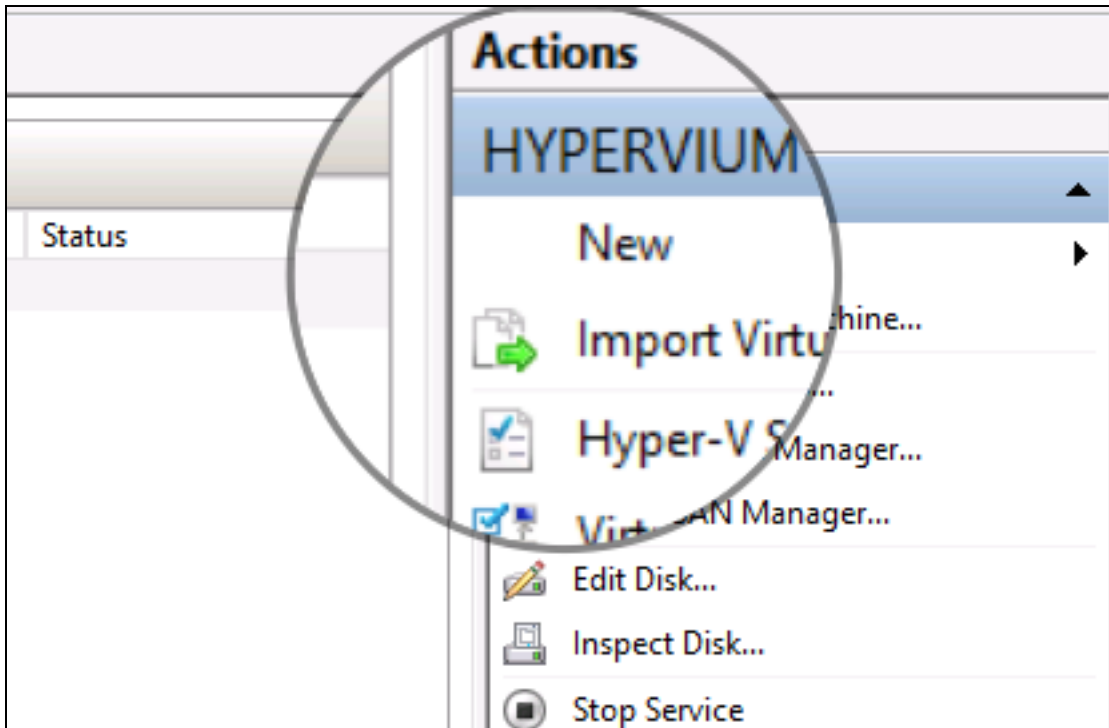
Before you install the ExtraHop virtual appliance, ensure the following:

- You have downloaded the file for the ExtraHop virtual appliance (this is an OVA file for OVA-aware hypervisor products). If you have not downloaded the file, contact support@extrahop.com.
- You have the ExtraHop virtual appliance license key provided by ExtraHop. If you do not have a license key, contact support@extrahop.com.
- You have an existing installation of one of the following virtualization products:
 - Microsoft Hyper-V
- Your host system meets the minimum hardware requirements, and you understand the disk requirements for setting up an ExtraHop appliance.
- If you are using a software tap, you have administrative access to servers you want to monitor, and you are running a 64-bit operating system (Linux/Windows). If you are using Windows, you must be using Windows Server 2008 R2 or Windows Server 2012.
- If you want to use Port Mirroring mode, you have administrative access to any physical or virtual switches that require configuration.

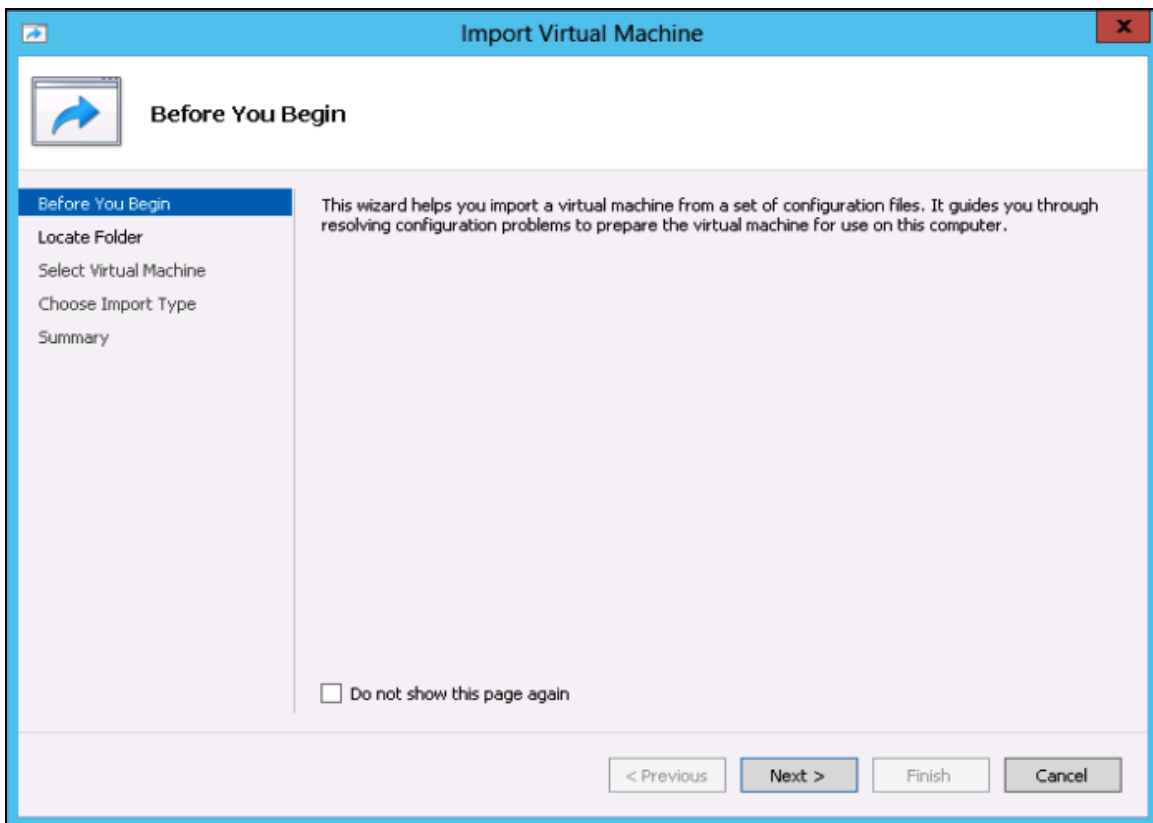
Installing the Files for Hyper-V

To install the files to run the ExtraHop virtual appliance with Hyper-V, complete the following steps.

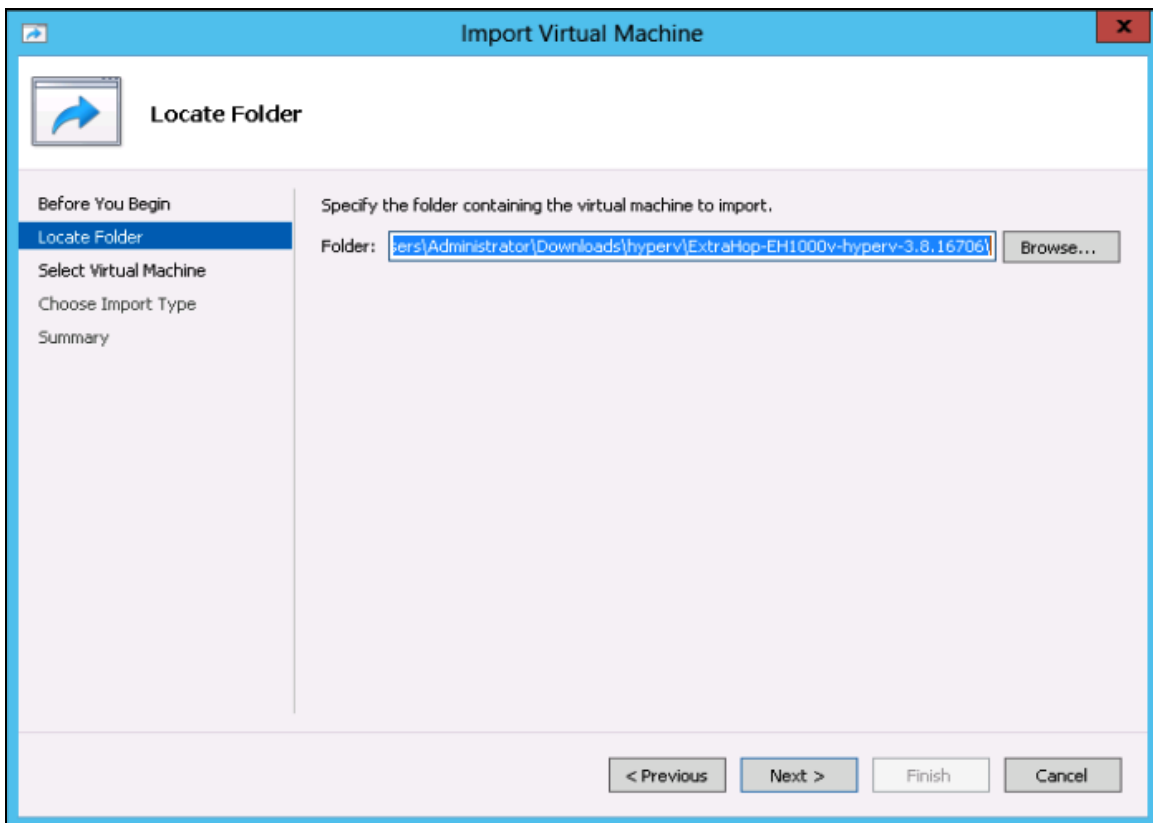
1. Go to the **Start** menu and open the **Hyper-V Manager**.
2. In the right pane of the Hyper-V Manager, click **New** and select **Import Virtual Machine...**



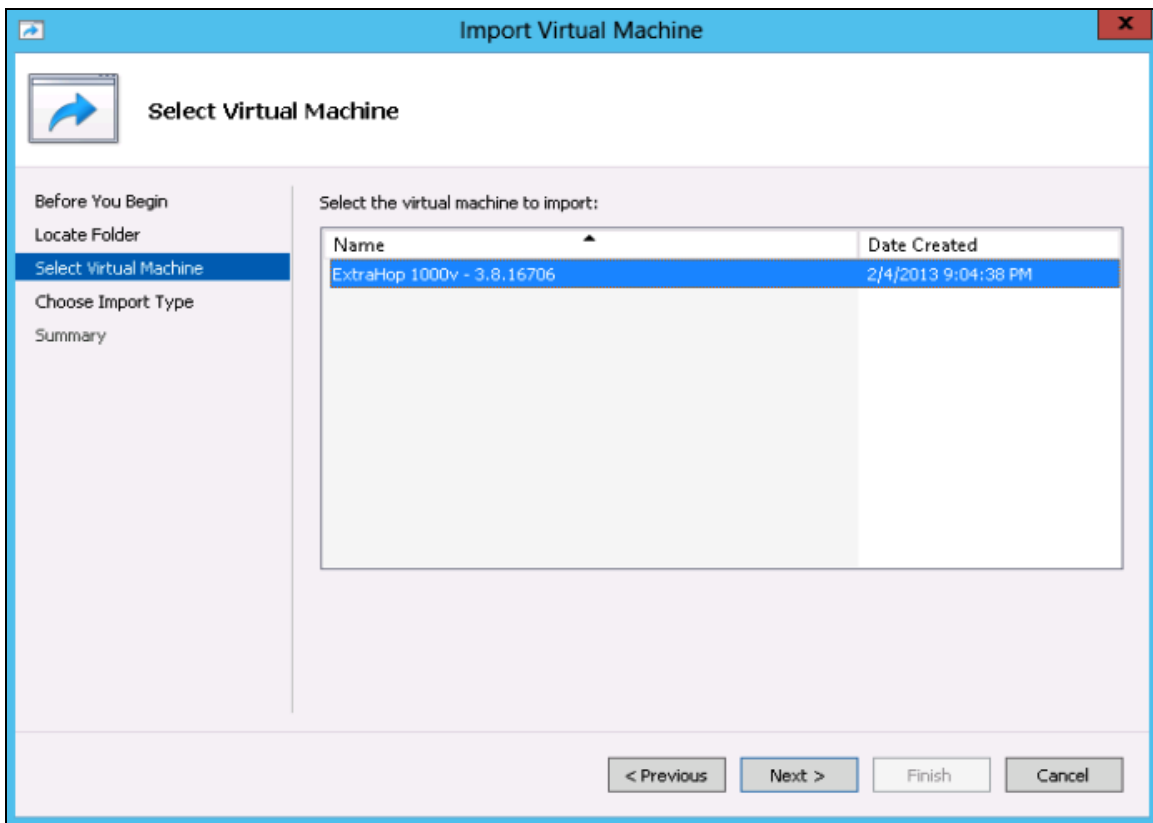
3. In the Import Virtual Machine Wizard, click **Next**.



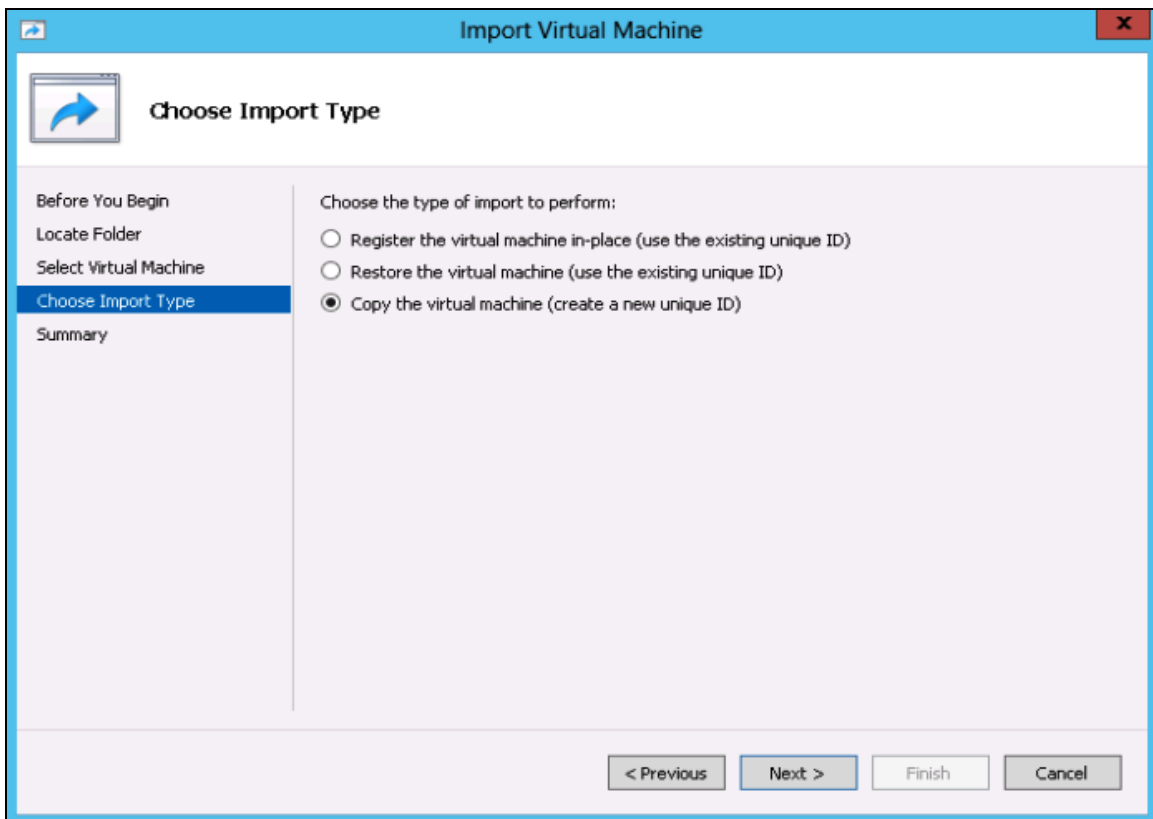
4. Browse to the folder with the extracted files and click **Next**.



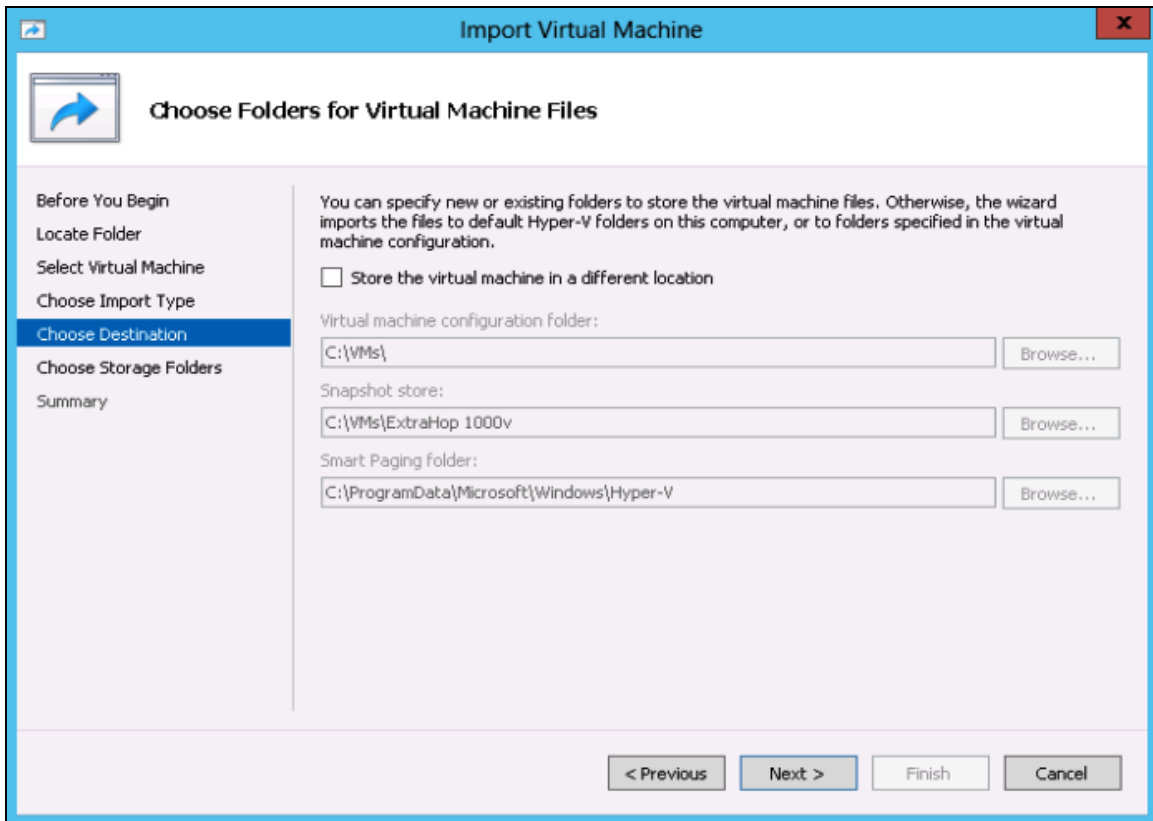
5. On **Select Virtual Machine**, click **Next**.



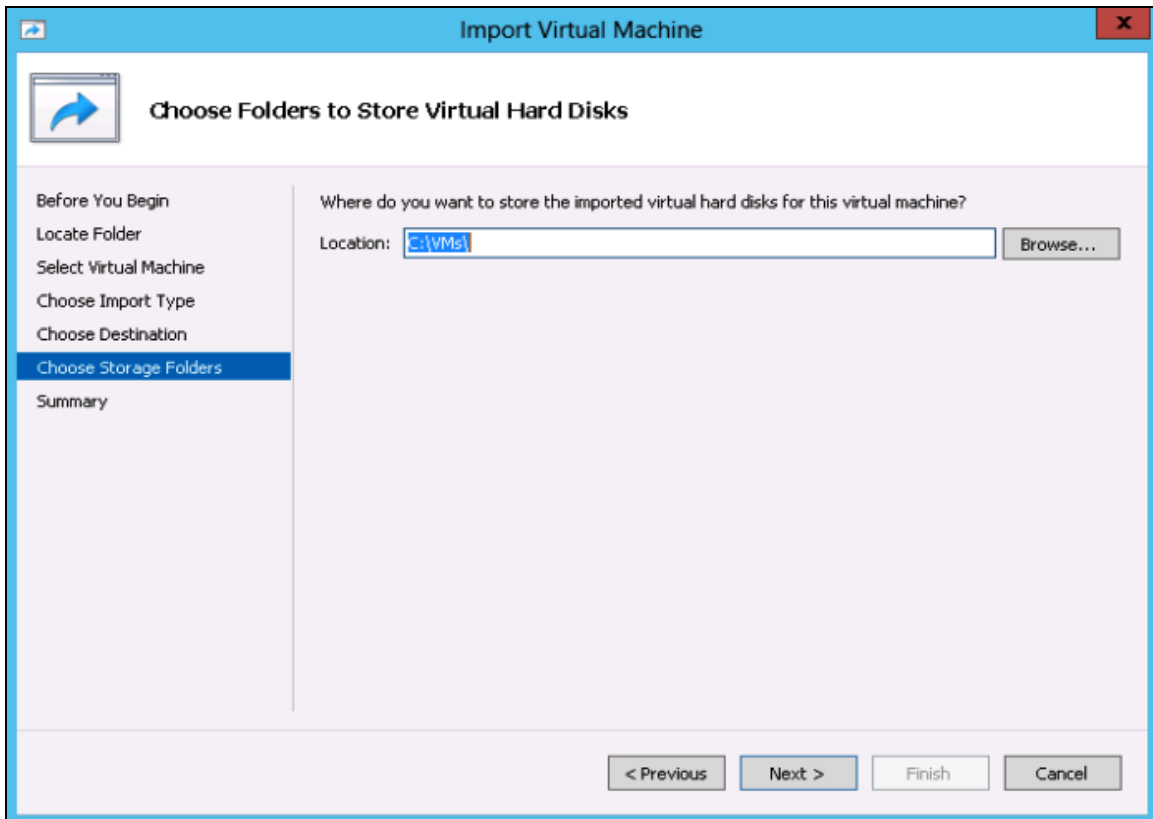
6. Select **Copy the virtual machine** and click **Next**.



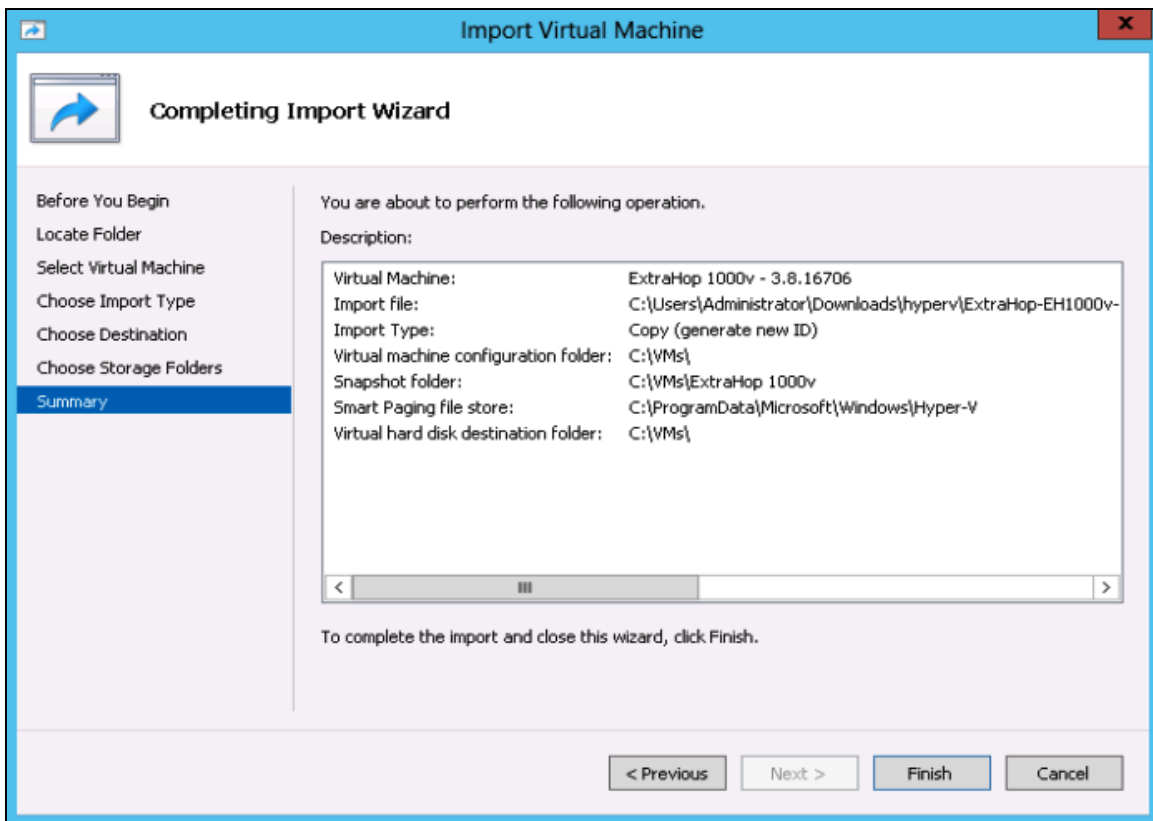
7. On **Choose Folders for Virtual Machine Files**, select the location to store the configuration of the VM and click **Next**.



- On **Choose Storage Folders to Store Virtual Hard Disks**, select a location to store the virtual hard disks and click **Next**.

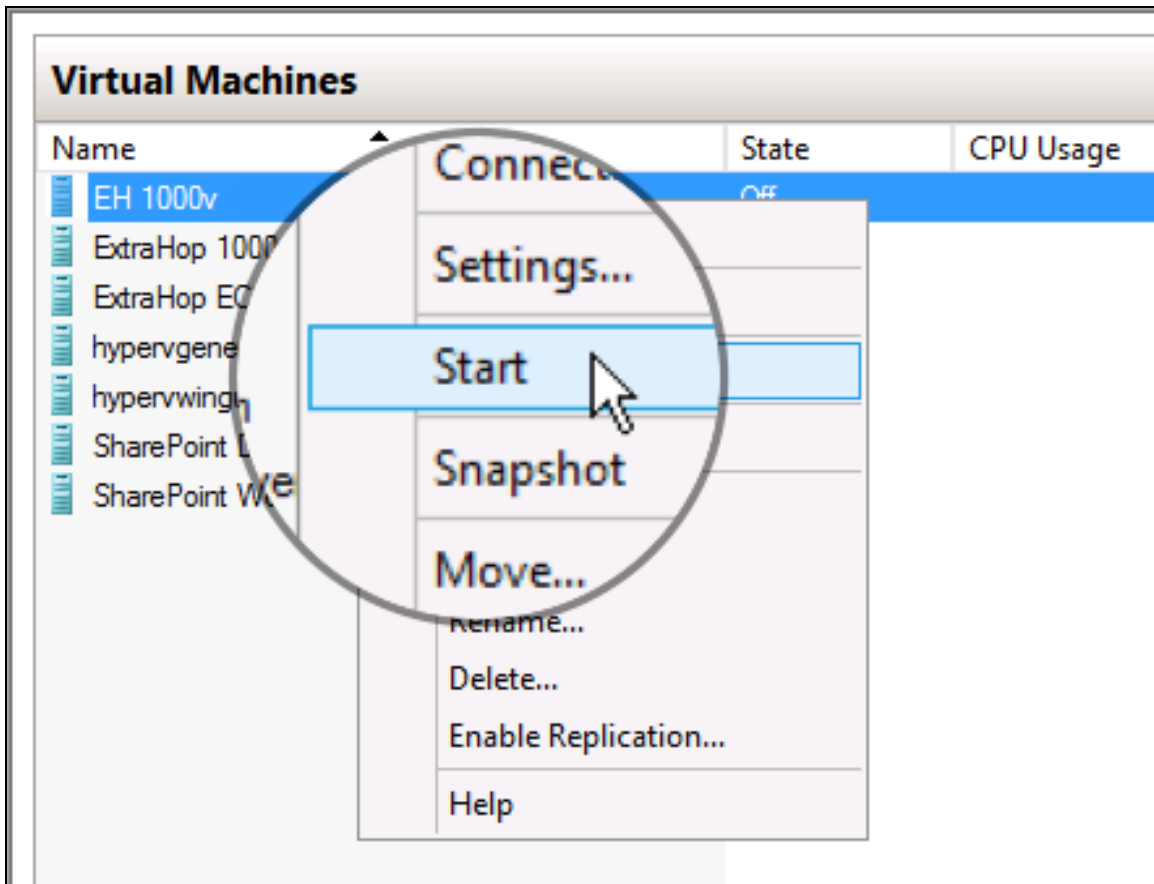


9. On the summary screen review your choices and then click **Finish**.

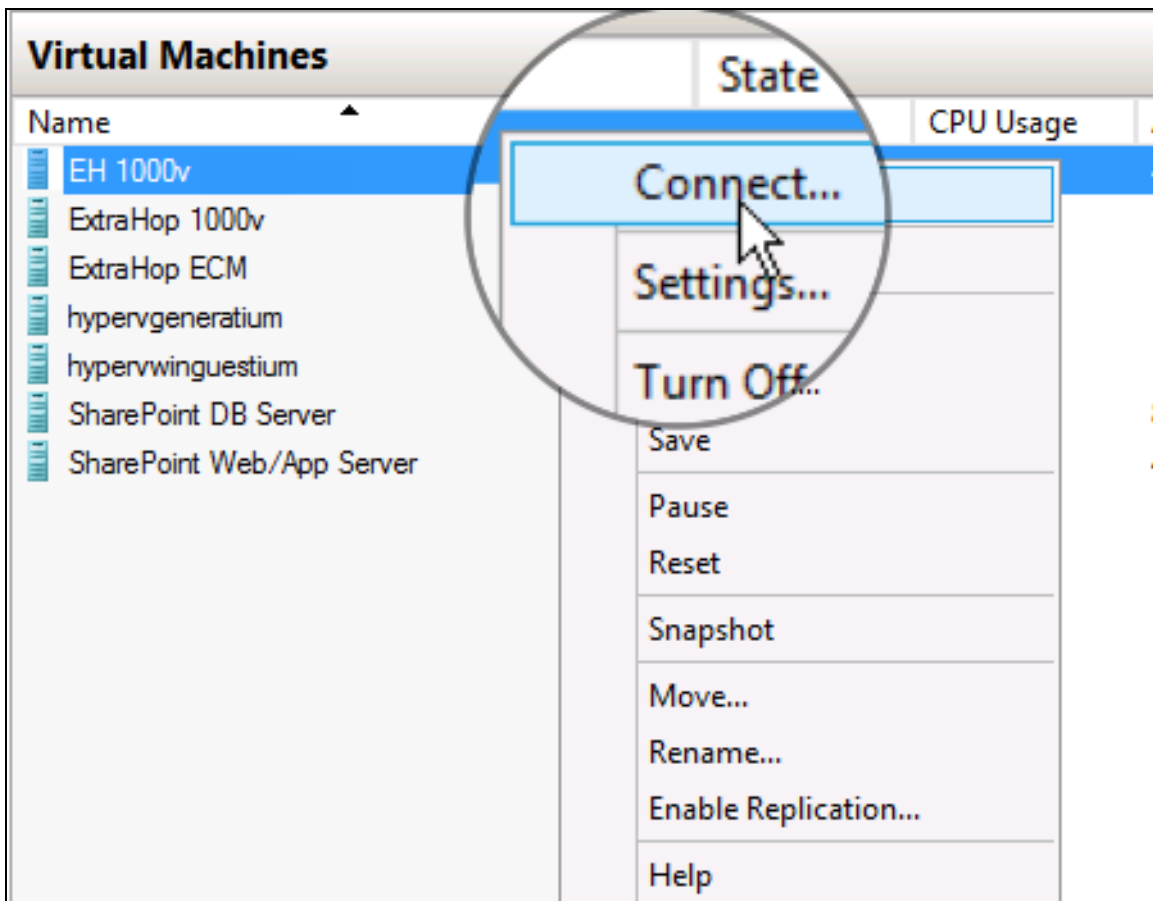


10. Wait several minutes for the files to copy.

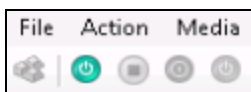
11. In the Virtual Machines list, right-click the virtual machine and select **Start**.



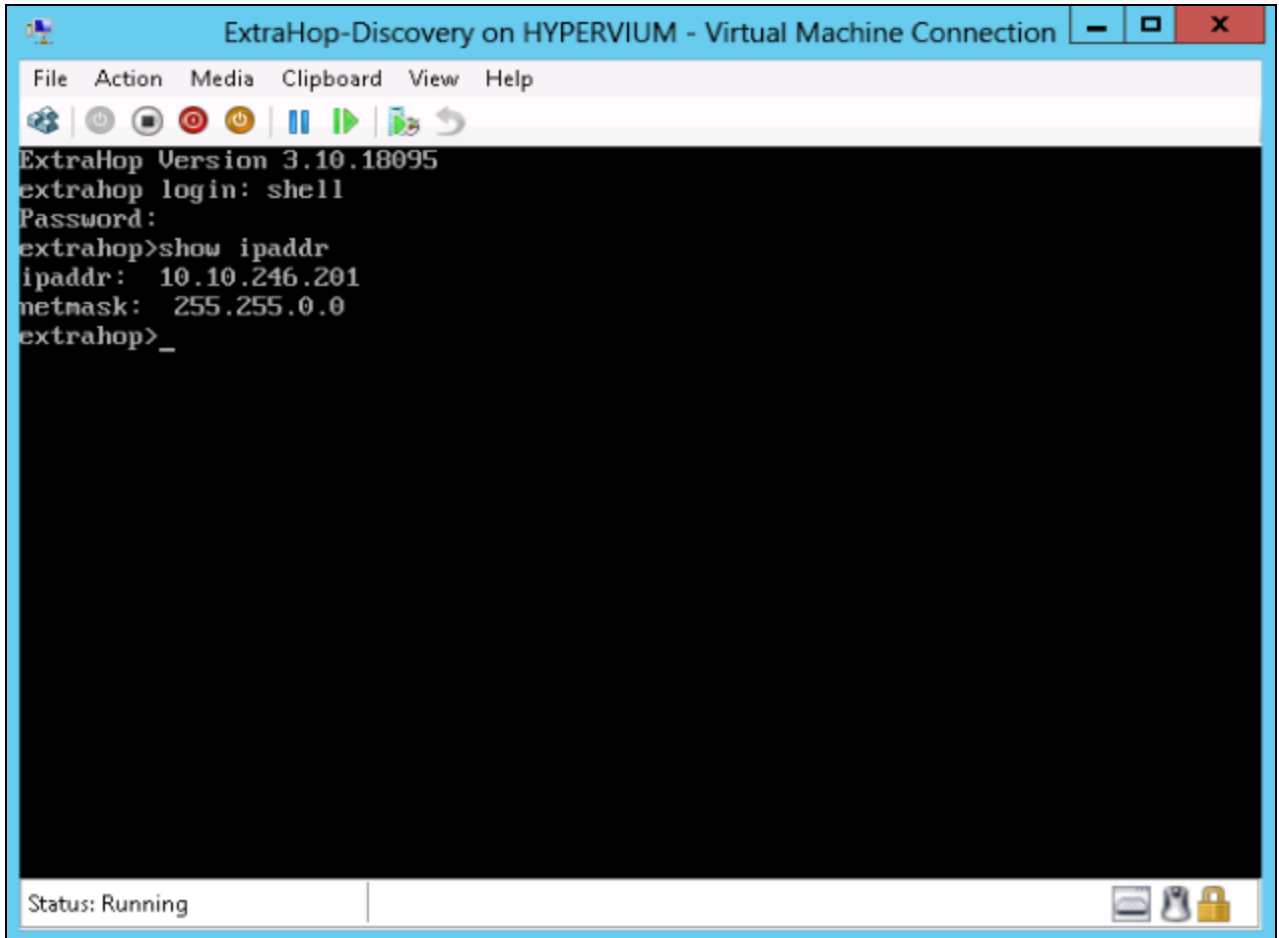
- Right-click the virtual machine again and select **Connect**.



- Click the green start button at the top of the screen and wait for the login prompt.



- Run the `show ipaddr` command to display the IP address of the ExtraHop Discovery Edition.



If your network does not support DHCP, refer to *Appendix: Configuring a Static IP Address* to set a static IP address.

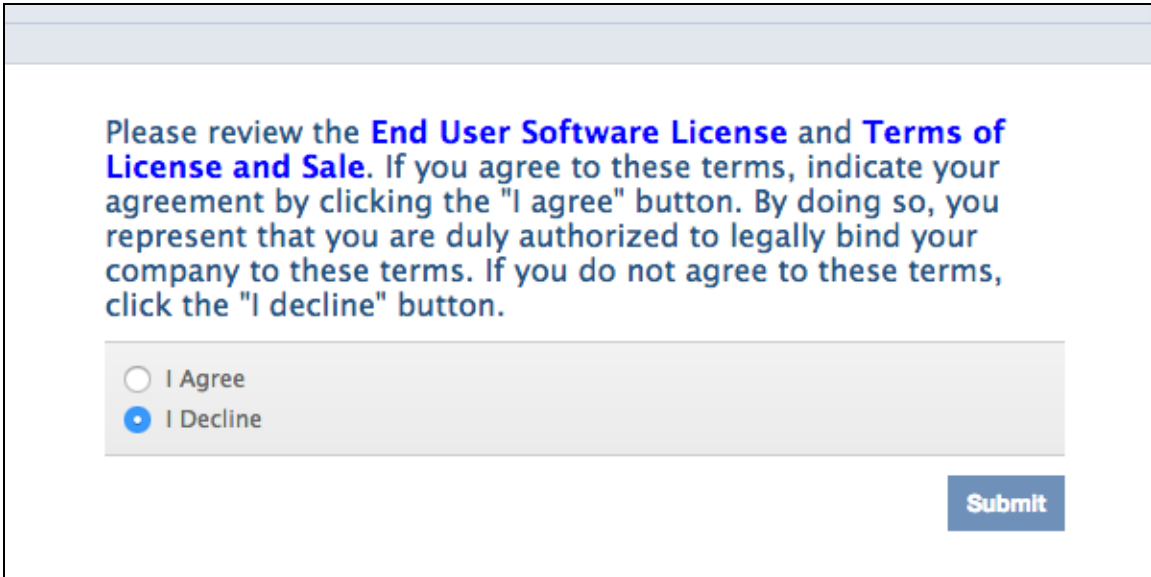
The default time server setting is `pool.ntp.org`. To configure the time servers manually, refer to the System Settings section of the *ExtraHop Admin UI Users Guide*.

15. You'll need the IP address to apply the ExtraHop license in the next procedure.

Applying the ExtraHop License

The ExtraHop virtual appliance requires a product key and a license in order to function.

1. Browse to the ExtraHop appliance: (https://<extrahop_management_ip>/admin)



Please review the **End User Software License** and **Terms of License and Sale**. If you agree to these terms, indicate your agreement by clicking the "I agree" button. By doing so, you represent that you are duly authorized to legally bind your company to these terms. If you do not agree to these terms, click the "I decline" button.

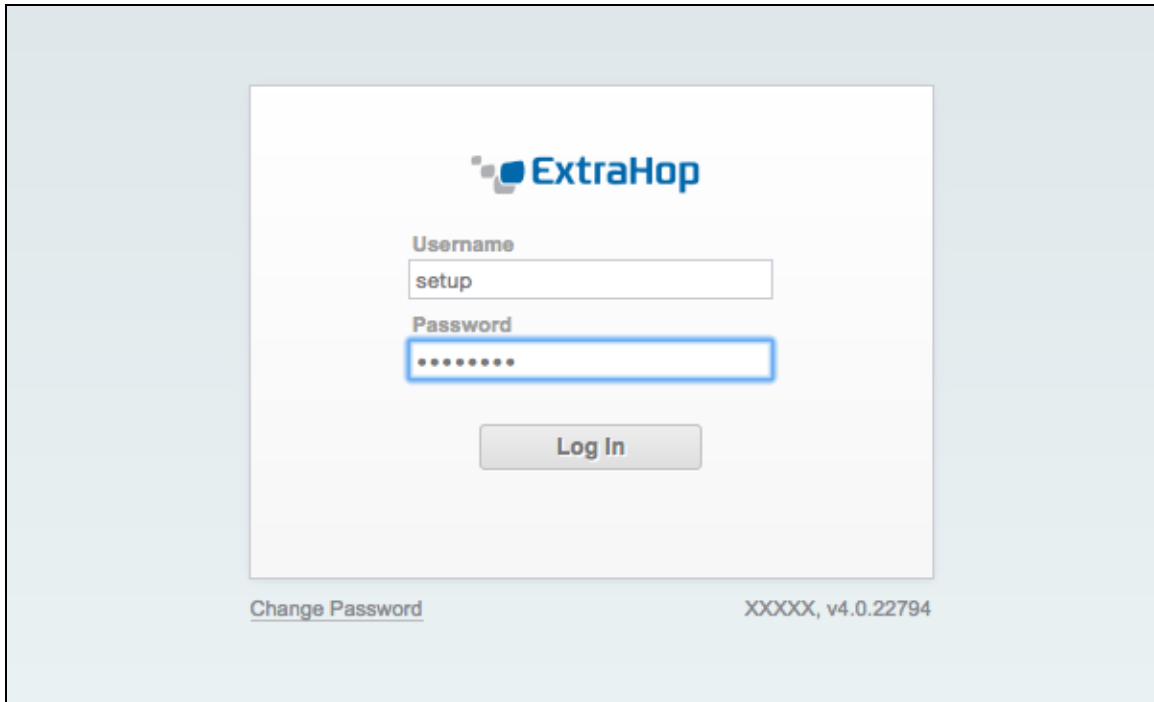
I Agree
 I Decline

Submit

If your browser prompts you about security certificates, ignore the warning and proceed.

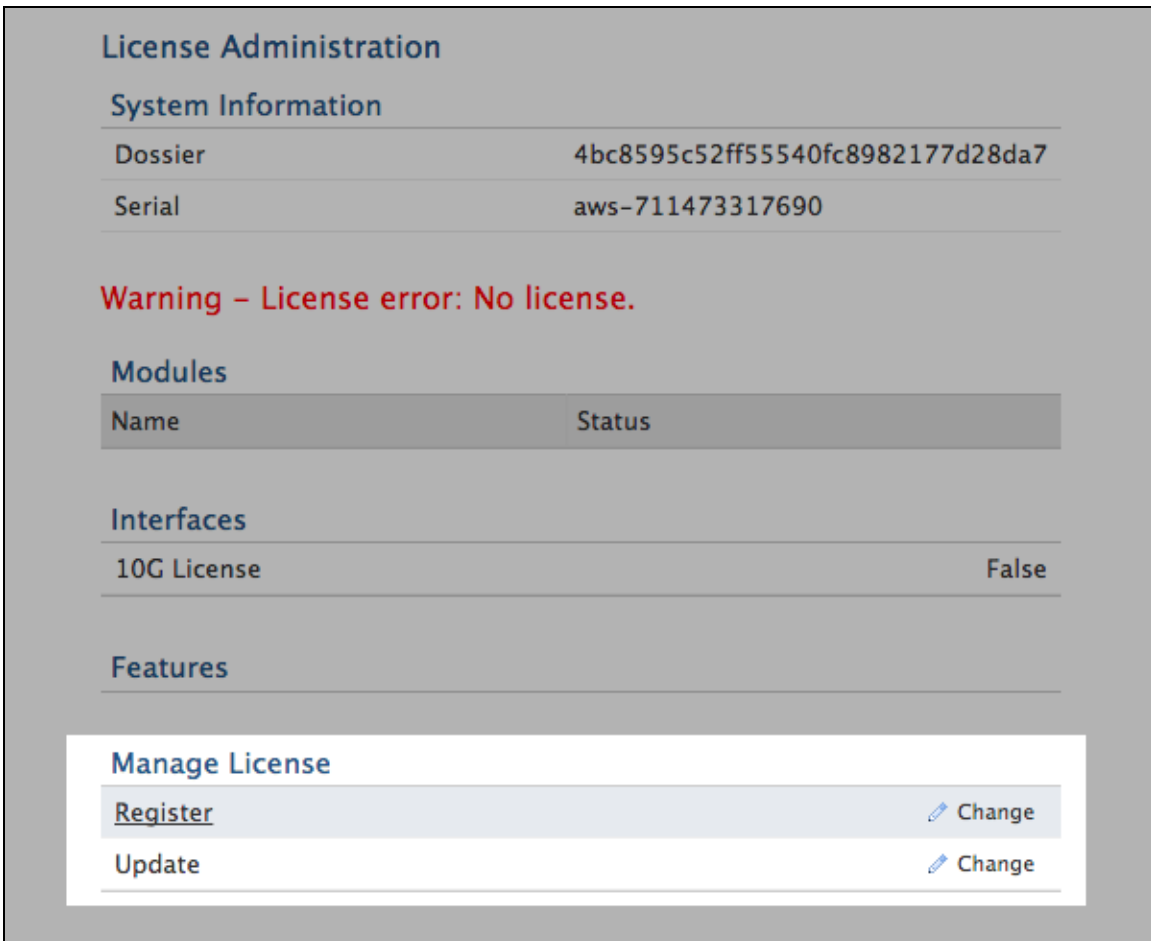
2. Review the license agreement, select **I Agree**, and click **Submit**.

3. On the login screen, enter the default user name and password:
 - **Username:** setup
 - **Password:** default



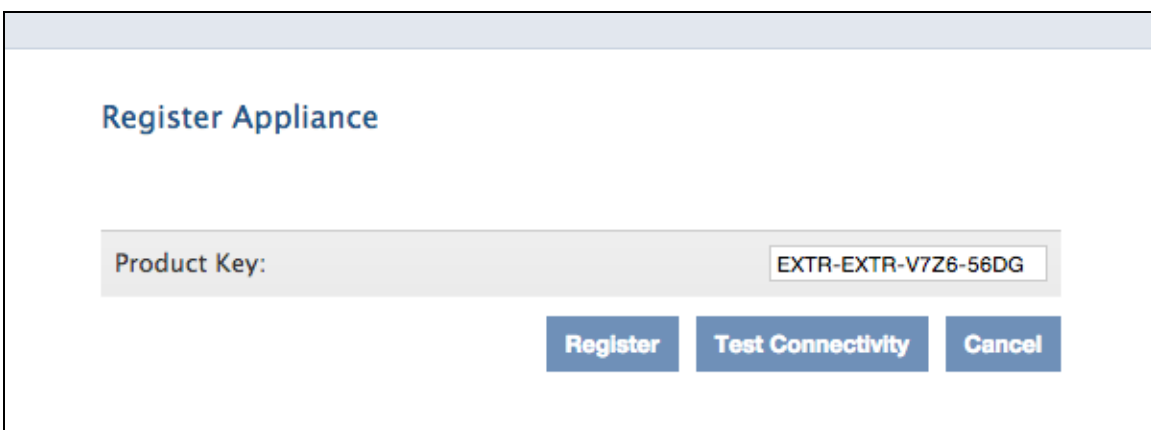
4. Click **ExtraHop Administration**.

5. Under **Manage License**, click **Register** to enter the product key.



The screenshot shows the 'License Administration' section of the ExtraHop interface. It includes a 'System Information' table with fields for 'Dossier' (4bc8595c52ff55540fc8982177d28da7) and 'Serial' (aws-711473317690). A red warning message states 'Warning - License error: No license.' Below this are sections for 'Modules' (with a table header for Name and Status), 'Interfaces' (showing '10G License' with a status of 'False'), and 'Features'. At the bottom, a 'Manage License' panel contains two options: 'Register' and 'Update', each with a 'Change' link.

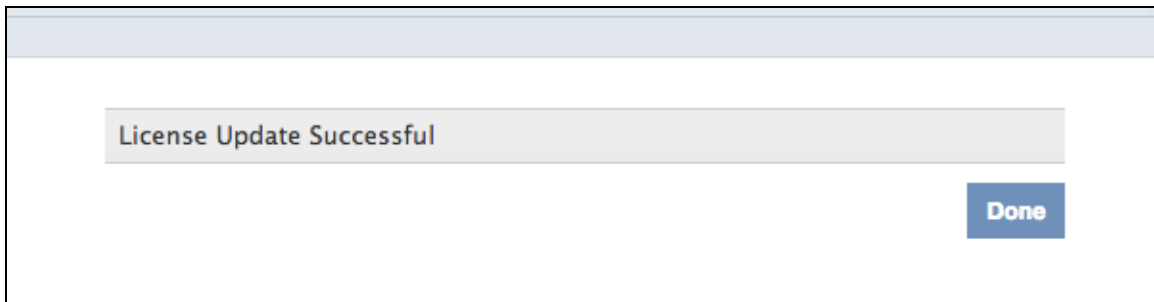
6. Enter the product key and then click **Register**.



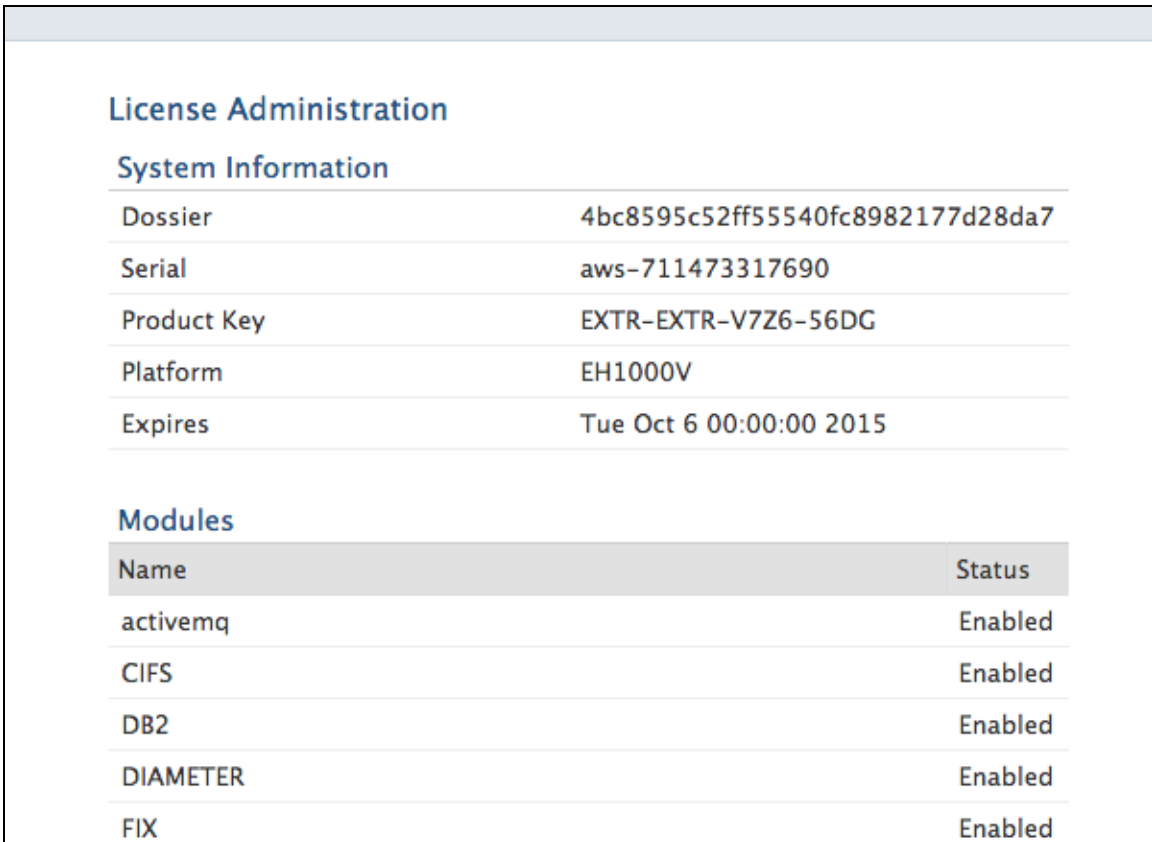
The screenshot shows the 'Register Appliance' dialog box. It features a 'Product Key:' label followed by a text input field containing the key 'EXTR-EXTR-V7Z6-56DG'. Below the input field are three buttons: 'Register', 'Test Connectivity', and 'Cancel'.

The ExtraHop system contacts the license server and validates the product key. After the product key is validated, the license is downloaded.

7. Click **Done**.



This is an example of the License Administration page showing a properly licensed ExtraHop system:



The screenshot shows the 'License Administration' page. It has a title 'License Administration' and a sub-section 'System Information'. Below this is a table with system details. Another sub-section 'Modules' contains a table listing various modules and their status.

License Administration	
System Information	
Dossier	4bc8595c52ff55540fc8982177d28da7
Serial	aws-711473317690
Product Key	EXTR-EXTR-V7Z6-56DG
Platform	EH1000V
Expires	Tue Oct 6 00:00:00 2015
Modules	
Name	Status
activemq	Enabled
CIFS	Enabled
DB2	Enabled
DIAMETER	Enabled
FIX	Enabled

The ExtraHop system is now licensed and able to receive mirrored traffic.

Configuring a Static IP Address

The ExtraHop virtual appliance is delivered with DHCP enabled. If your network does not support DHCP, no IP address would be acquired, and you must configure a static address manually. To configure a static IP address, complete the following steps:

1. Log in to the console. Use the user account named *shell* and the password default.
2. Enable the privilege commands.

```
extrahop>enable
Password:default
extrahop#
```

3. Enter the configuration section.

```
extrahop#config
extrahop(config)#
```

4. Enter the interface section.

```
extrahop(config)#int
extrahop(config-if)#
```

5. Set the IP address and DNS using this syntax: `ip ipaddr IP_ADDRESS NETMASK GATEWAY DNS`.

```
extrahop(config-if)#ip ipaddr 10.10.10.10 255.255.0.0 10.10.1.254 8.8.8.8
```

6. Save the running config.

```
extrahop(config-if)#exit
extrahop(config) * #running_config save
Would you like to write configuration changes to default config [Y/n]?: y
extrahop(config)#
```

The full set of commands is as follows:

```
extrahop>enable
Password:
extrahop#config
extrahop(config)#int
extrahop(config-if)#ip ipaddr 10.10.10.10 255.255.0.0 10.10.1.254 8.8.8.8
Changing IP address. Please wait...
.Done
extrahop(config-if)# exit
extrahop(config) * #running_config save
Would you like to write configuration changes to default config [Y/n]?: y
extrahop(config)#
```

Note: The default time server setting is `pool.ntp.org`. To configure the time servers manually, refer to the **System Settings** section of the *ExtraHop Admin UI Users Guide*.

Mirror Wire Data

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

Mirroring Internal and External Traffic

The ExtraHop virtual appliance can be configured to monitor network traffic in the following network configuration examples. Each example requires a modification to the network configuration of its hypervisor host and uses Network Adapter 1 as the management interface.

- on page 1
- Monitoring External Mirrored Traffic to the VM (EH1000v)

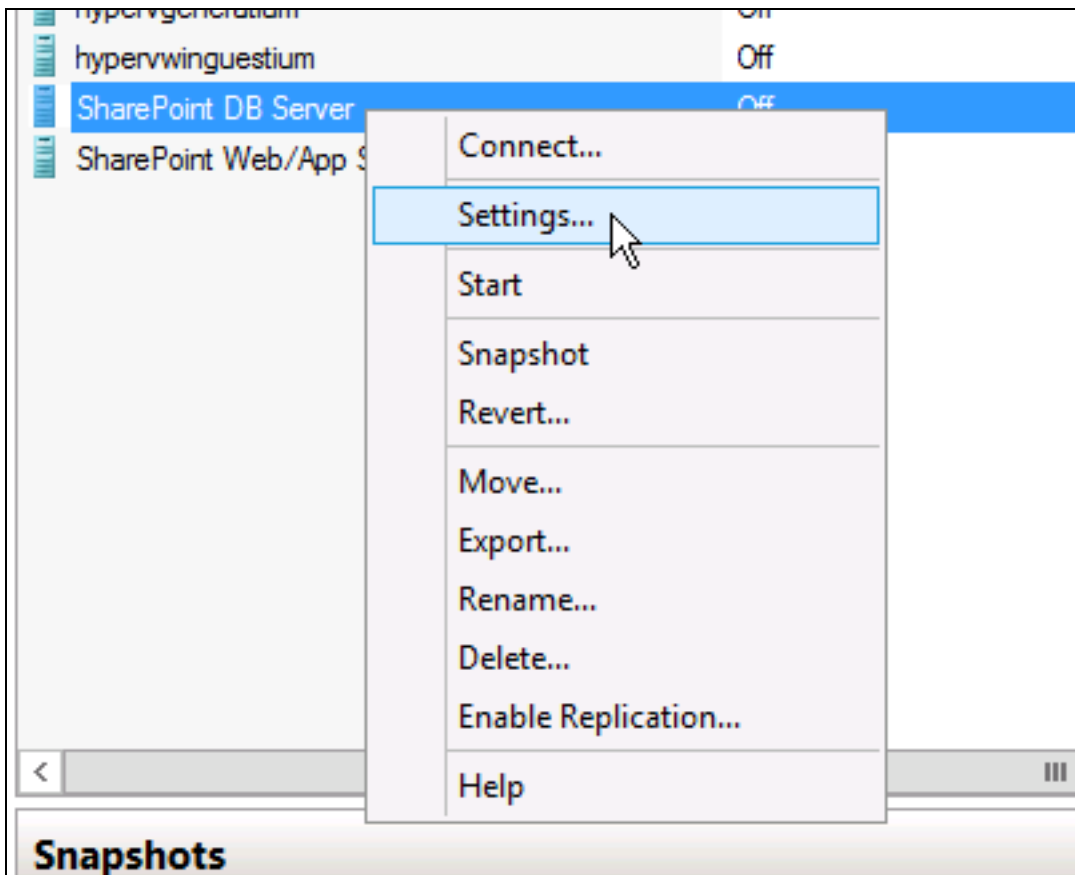
Note: Monitoring external network-mirrored traffic requires an external NIC and an associated virtual switch.

Monitoring Intra-VM Traffic

The ExtraHop Discovery Edition can be configured to monitor network traffic of another VM on the same host using Port Mirroring mode in the Hyper-V Manager. An ExtraHop virtual machine running in port mirroring mode can only monitor another virtual machine running on the same virtual switch.

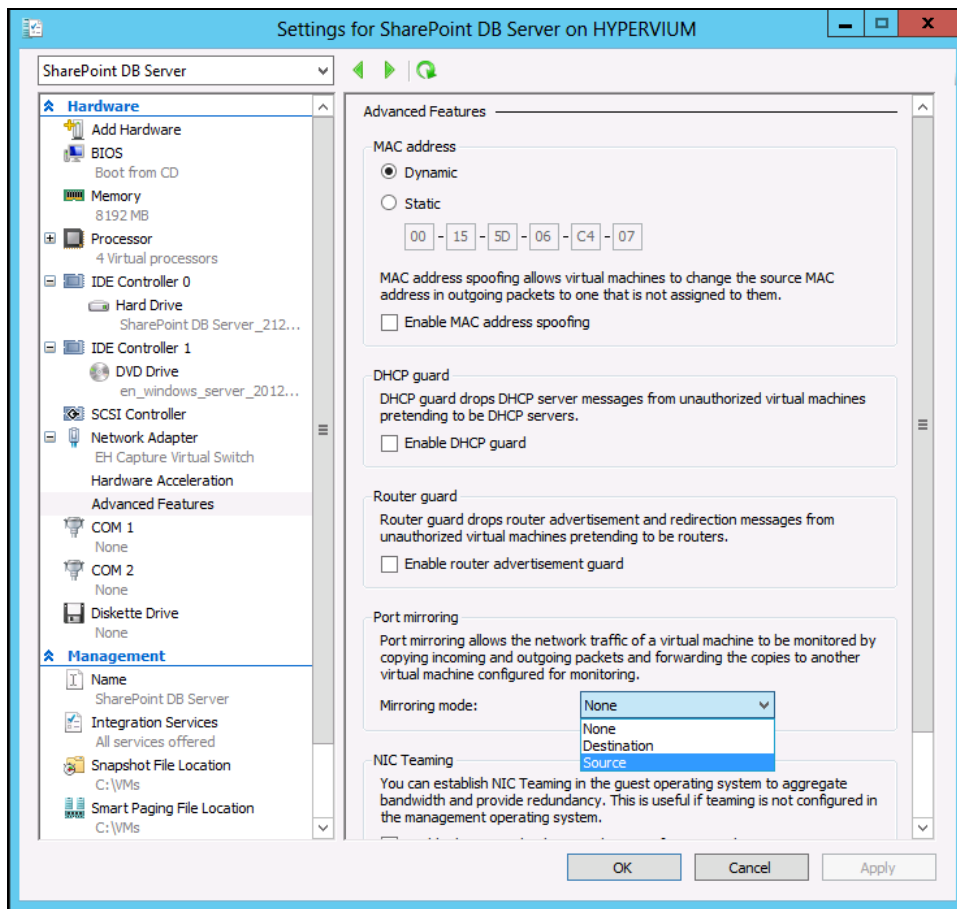
Enabling Port Mirroring Mode in the Hyper-V Manager

1. Right-click the ExtraHop-Discovery VM and select **Settings**.



2. Expand **Network Adapter** and click **Advanced Features**.

- In the Port mirroring section, click the **Mirroring mode** drop-down list and select **Source**.

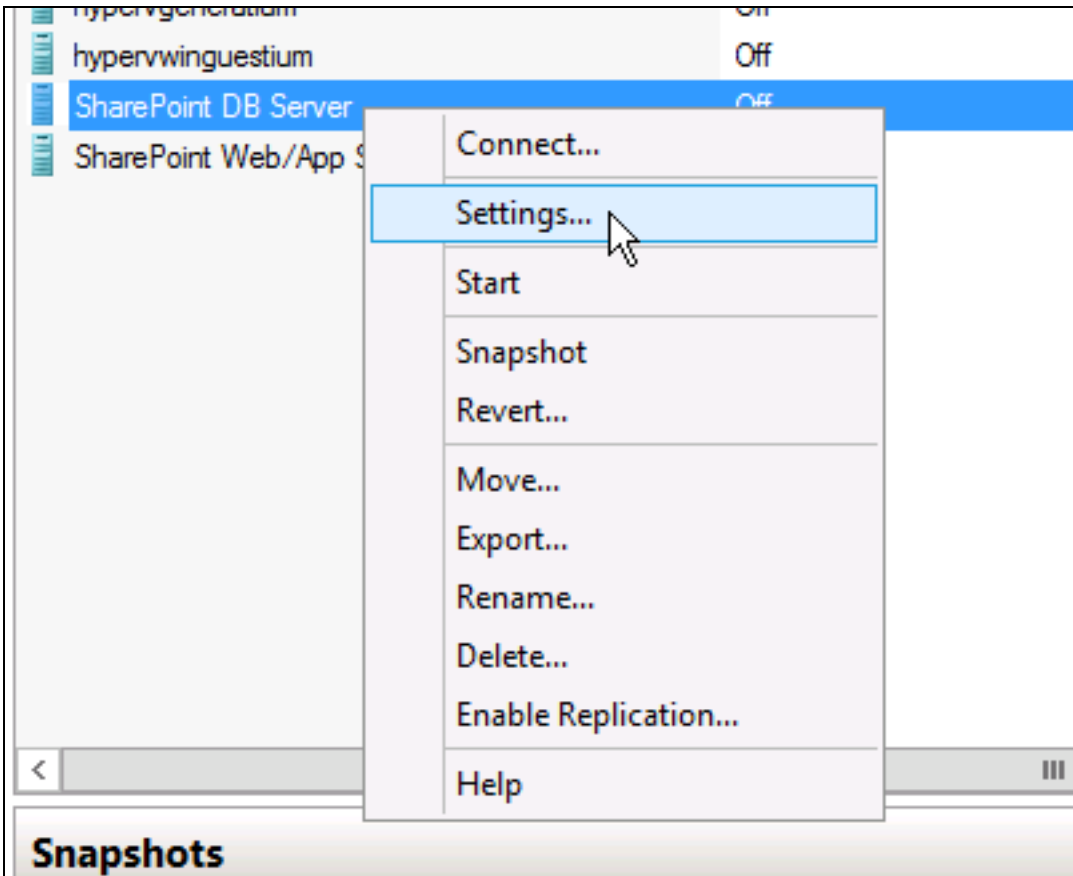


- Make note of the source network and ensure the ExtraHop system's capture interface is on the same network.
- Click the **Apply** button.
- Click **OK**.
- Repeat these steps for all the VMs you want to monitor, excluding the first VM you created in this procedure.

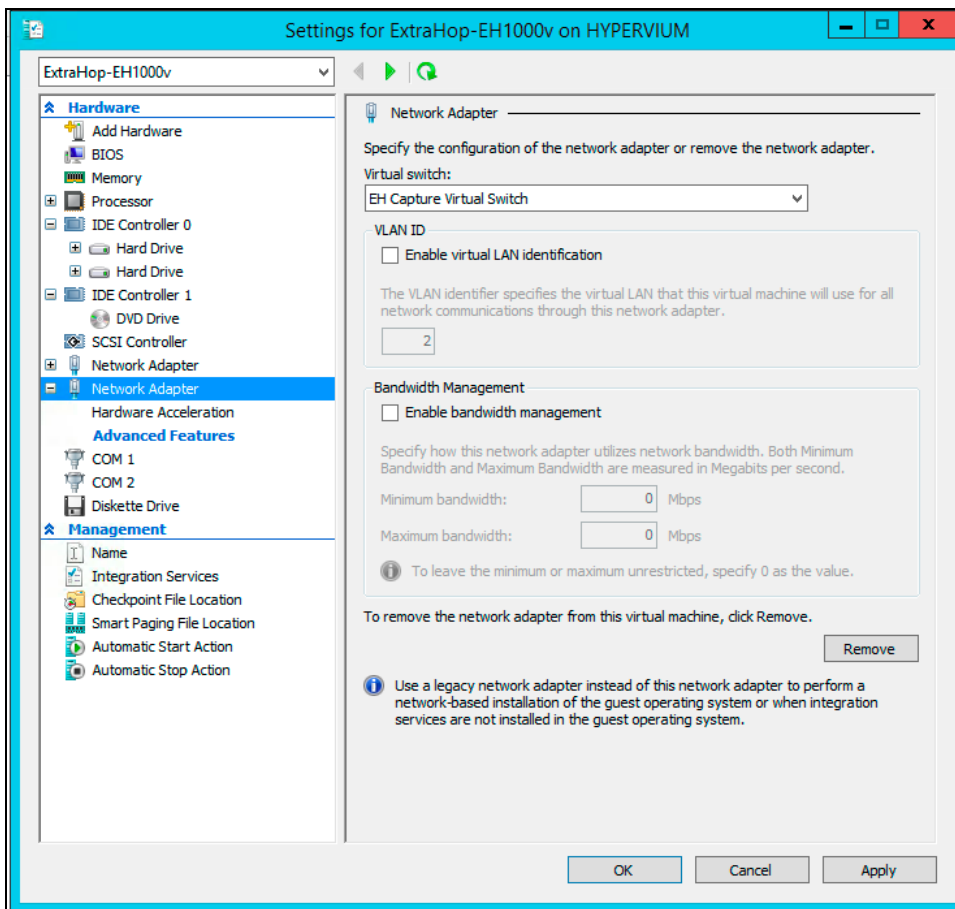
Monitoring External Mirrored Traffic to the VM

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.

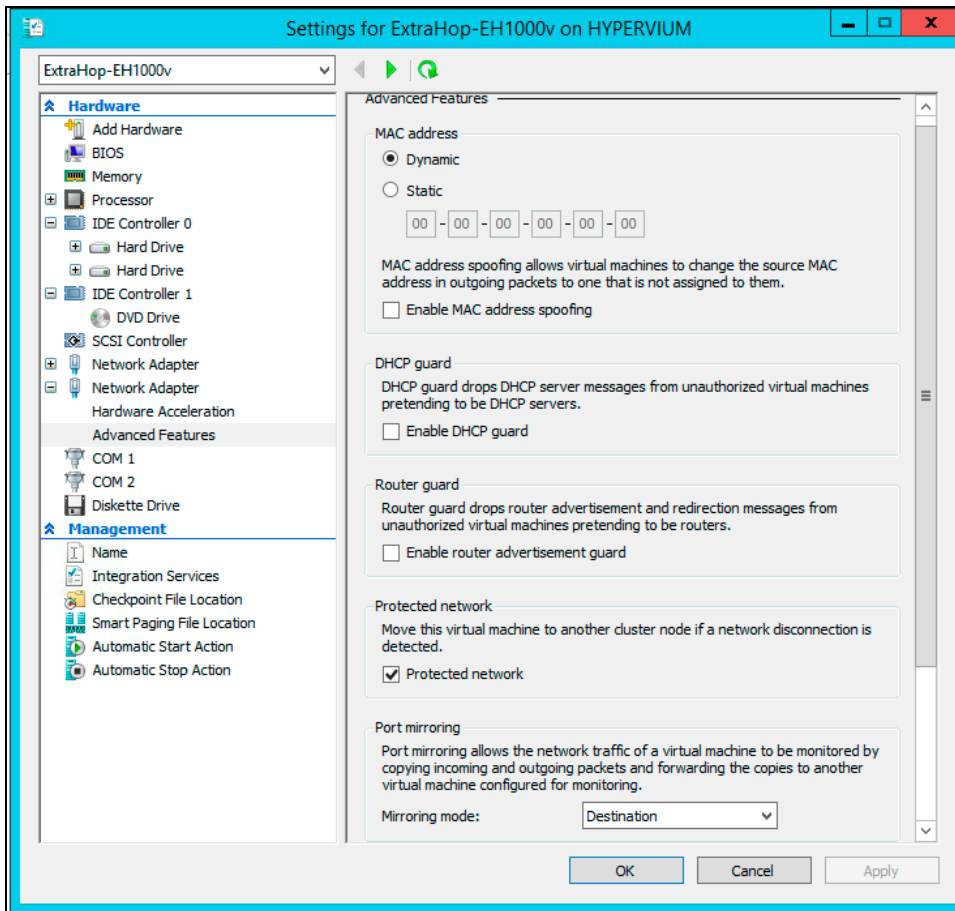
1. Right-click the ExtraHop-Discovery VM and select **Settings**.



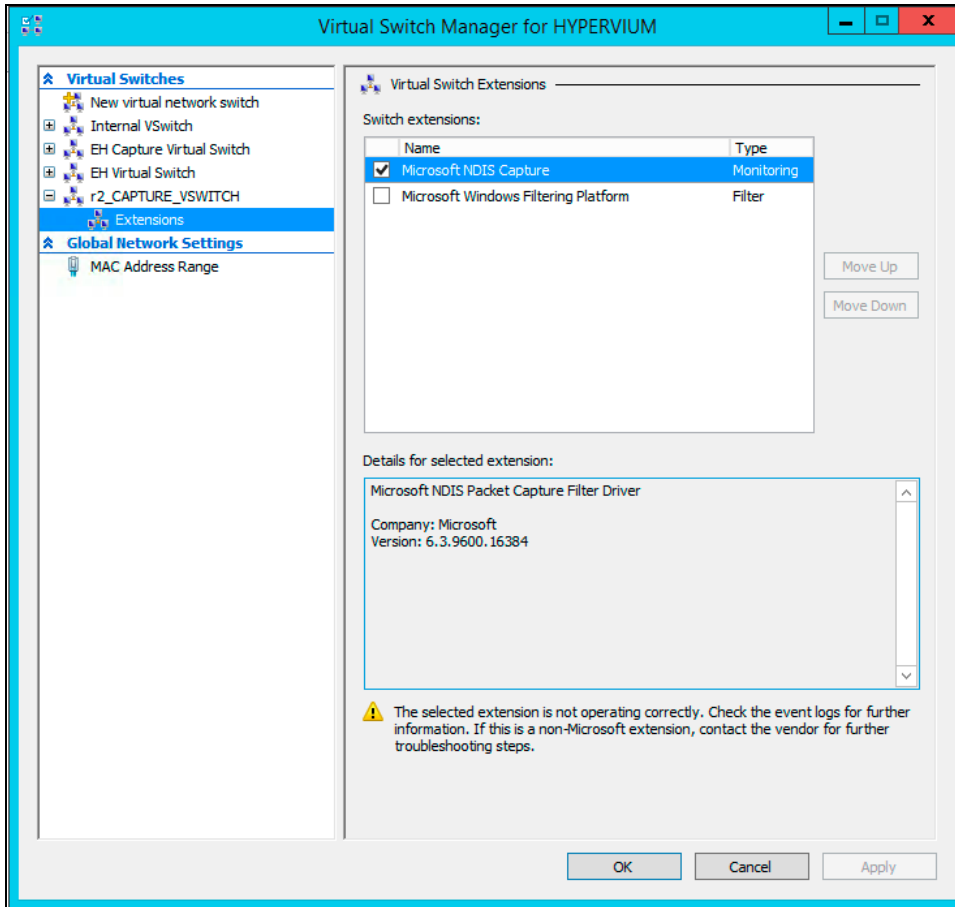
2. Expand **Network Adapter** and click **Advanced Features**.



- In the Port mirroring section, click the **Mirroring mode** drop-down list and select **Destination**.



- Click the **Apply** button.
- Click **OK**.
- Expand the virtual switch associated with the external data feed and enable the **Microsoft NDIS Capture** switch. Don't worry about the warning. The PowerShell command in the next step will get it to work.



7. Click the **Apply** button.
8. Click **OK**.
9. Open a PowerShell prompt and enter the following commands:

```
$a = Get-VMSwitchExtensionPortFeature -FeatureId 776e0ba7-94a1-41c8-8f28-951f524251b5
$a.SettingData.MonitorMode = 2
add-VMSwitchExtensionPortFeature -ExternalPort -SwitchName <name of the switch> -
VMSwitchExtensionFeature $a
```

This technical reference for this procedure comes from [this blog post](#) on the Networking Blog at Technet.

Software Tap

A software tap forwards traffic from any host to ExtraHop. A software tap is conceptually similar to a physical network tap, but implemented in software. In these topics and the industry, this software is alternately referred to as a packet forwarder, or sometimes RPCAP, which stands for Remote Packet CAPture.

To use the software tap, ensure the following:

- You have administrative access to servers you want to monitor.
- You are running a 64-bit Linux or Windows OS. If you are using Windows, you are using Windows Server 2008 R2 or 2012.

To ensure proper functionality of the ExtraHop virtual appliance:

- Ensure RPCAP is enabled on the ExtraHop virtual appliance. Refer to **Configuring Additional RPCAP Settings** for optional settings.
- Install the software tap on the servers sending traffic.
- Analyze traffic in the ExtraHop Web UI.

Install the Software Tap on a Linux Server

You must install the software tap on each server to be monitored in order to forward packets to the ExtraHop system. You can retrieve the commands from the procedures in this section or the ExtraHop Admin UI: https://<extrahop_ip>/admin/capture/rpcapd/linux/. The bottom of the ExtraHop Admin UI page contains links to automatically download the software tap.

Debian-Based Systems

To download and install the software tap on Debian-based systems:

1. Run one of the following commands to download the software tap on the server:

```
wget --no-check-certificate 'https://<extrahop_ip>/tools/rpcapd_<extrahop_firmware_version>_amd64.deb'  
curl -Ok 'https://<extrahop_ip>/tools/rpcapd_<extrahop_firmware_version>_amd64.deb'
```

Replace <extrahop_ip> with the ExtraHop system's interface 1 (management) IP address.

Replace <extrahop_firmware_version> with the ExtraHop system's firmware version.

2. Run the following command to install and run the software tap on the server:

```
sudo dpkg -i rpcapd_<extrahop_firmware_version>_amd64.deb
```

3. At the prompt, enter the ExtraHop IP address, confirm the default connection to port 2003, and press Enter.
4. (Optional) Run the following commands to verify the ExtraHop system is receiving traffic:

```
sudo dpkg --get-selections | grep rpcapd  
sudo service rpcapd status
```

5. (Optional) Run the following command to change the ExtraHop IP address, port number, or arguments to the service:

```
sudo dpkg-reconfigure rpcapd
```

RPM-Based Systems

To download and install the software tap on RPM-based systems:

1. Run one of the following commands to download the software tap on the server:

```
wget --no-check-certificate 'https://<extrahop_ip>/tools/rpcapd-<extrahop_firmware_version>.x86_64.rpm'  
curl -Ok 'https://<extrahop_ip>/tools/rpcapd-<extrahop_firmware_version>.x86_64.rpm'
```

Replace <extrahop_ip> with the ExtraHop system's interface 1 (management) IP address.

Replace <extrahop_firmware_version> with the ExtraHop system's firmware version.

2. Run the following command to install and run the software tap on the server:

```
sudo rpm -i rpcapd-<extrahop_firmware_version>.x86_64.rpm
```

3. Run one of the following configuration commands:

```
vim /opt/extrahop/etc/rpcapd.ini  
nano /opt/extrahop/etc/rpcapd.ini
```

Example output:

```
cat /opt/extrahop/etc/rpcapd.ini  
#ActiveClient = <TARGETIP>,<TARGETPORT>  
NullAuthPermit = YES
```

Replace <TARGETIP> with your ExtraHop system's IP address and <TARGETPORT> with 2003, and uncomment the line.

Example output:

```
cat /opt/extrahop/etc/rpcapd.ini  
ActiveClient = 10.10.10.10,2003  
NullAuthPermit = YES
```

4. Run the following command to start sending traffic to the ExtraHop system:

```
sudo /etc/init.d/rpcapd start
```

5. (Optional) Run the following command to verify the ExtraHop system is receiving traffic:

```
sudo service rpcapd status
```

Generic/Other Linux Systems

To download and install the software tap on another Linux system:

1. Run one of the following commands to download the software tap on the server:

```
wget --no-check-certificate 'https://<extrahop_ip>/tools/rpcapd-<extrahop_firmware_<br>version>.tar.gz'  
curl -Ok 'https://<extrahop_ip>/tools/rpcapd-<extrahop_firmware_version>.tar.gz'
```

Replace <extrahop_ip> with the ExtraHop system's interface 1 (management) IP address.

Replace <extrahop_firmware_version> with the ExtraHop system's firmware version.

2. Run the following commands to install and run the software tap on the server:

```
tar xf rpcapd-<extrahop_firmware_version>.tar.gz  
cd rpcapd  
sudo ./install.sh <extrahop_ip> 2003
```

3. (Optional) Run the following command to verify the ExtraHop system is receiving traffic:

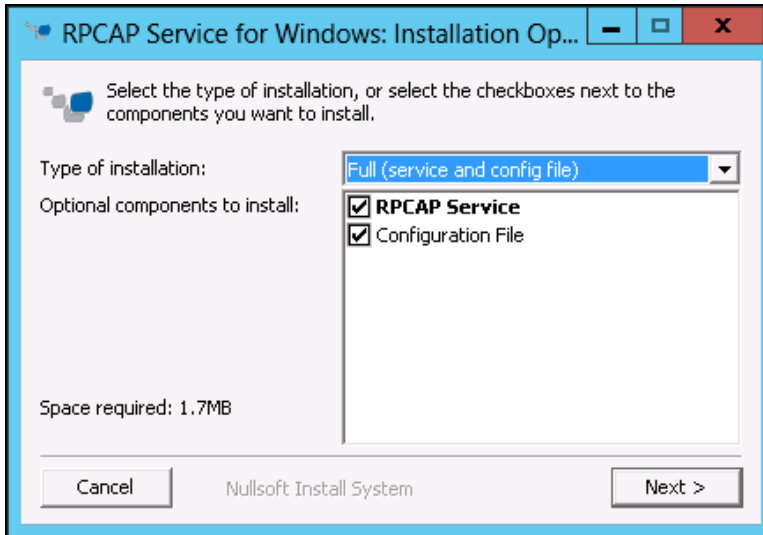
```
sudo /etc/init.d/rpcapd status
```

To run the software tap on servers with multiple interfaces, refer to **Monitoring Multiple Interfaces on a Linux Server**.

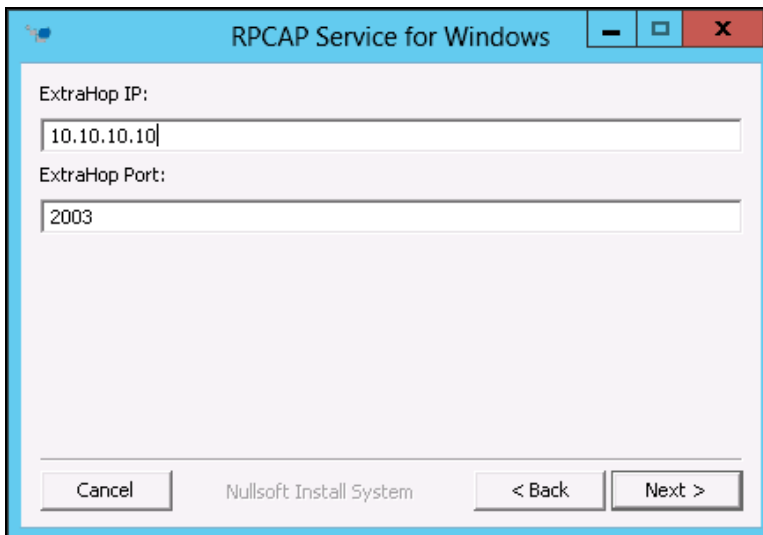
Install the Software Tap on a Windows Server

You must install the software tap on each server to be monitored in order to forward packets to the ExtraHop system. To download and install the software tap:

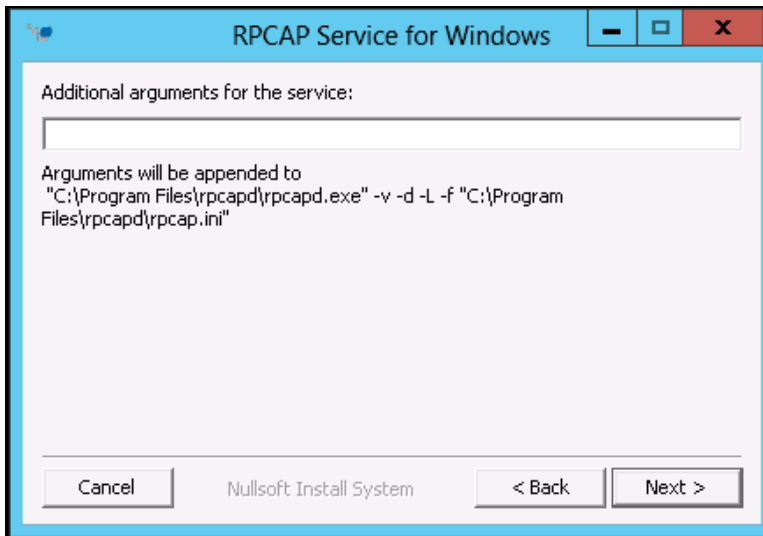
1. Go to https://<extrahop_ip>/admin/capture/rpcapd/windows/ to download the RPCAP Service for Windows installer file.
2. When the file is finished downloading, click it to open the installer.
3. In the wizard, select the components to install.



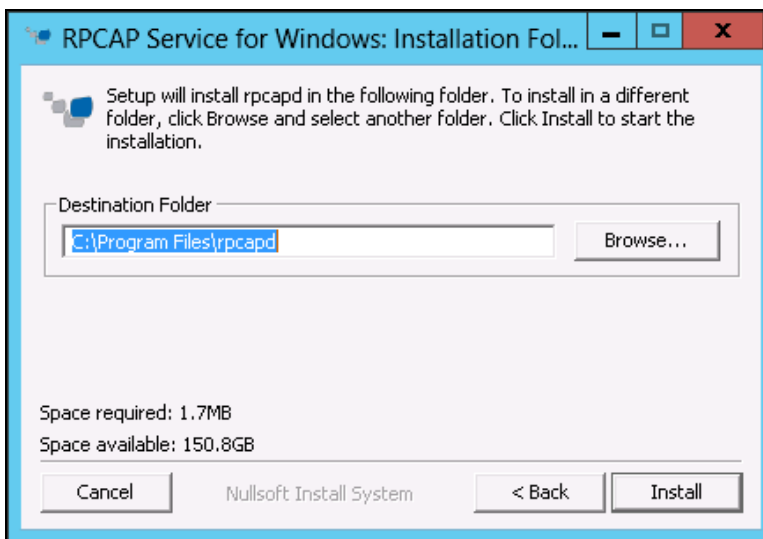
4. Complete the **ExtraHop IP** and **ExtraHop Port** fields and click **Next**. The default port is 2003.



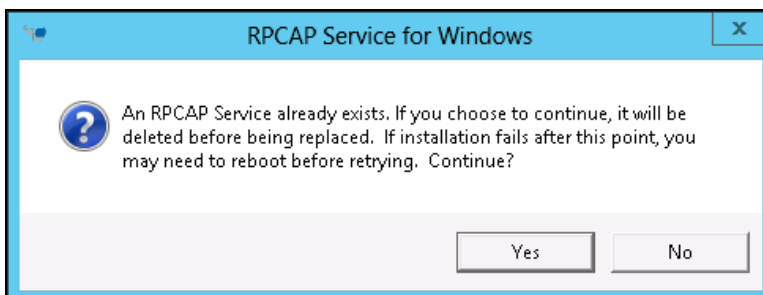
5. (Optional) Enter additional arguments in the text box and click **Next**.



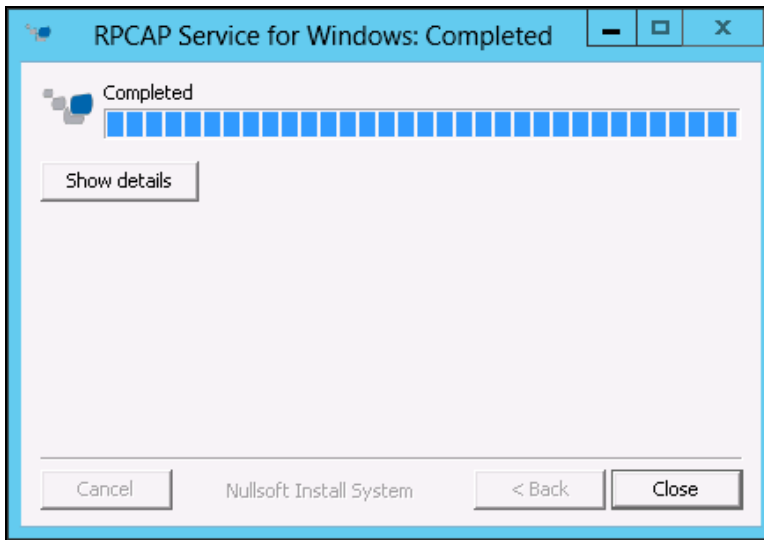
6. Browse to and select the destination folder to install RPCAP Service.



7. (Optional) If RPCAP Service was previously installed, click **Yes** to delete the previous service.



- When the installation is complete, click **Close**.



Monitoring Multiple Interfaces on a Linux Server

For servers with multiple interfaces, you can configure the software tap to forward packets from a particular interface or from multiple interfaces by editing its configuration file on the server.

To edit the configuration file, complete the following steps.

1. After installing the software tap, open the configuration file on the server: `/opt/extrahop/etc/rpcapd.ini`

The configuration file contains this text or similar:

```
ActiveClient = 10.0.0.100,2003
NullAuthPermit = YES
```

2. Modify the existing ActiveClient line and create an ActiveClient line for each additional interface to be monitored. Specify each interface by its interface name or IP address.

```
ActiveClient = <extrahop_ip>, <extrahop_port>, ifname=<interface_name>
```

or

```
ActiveClient = <extrahop_ip>, <extrahop_port>, ifaddr=<interface_address>
```

`<interface_name>` is the name of the interface from which you want to forward packets.

`<interface_address>` specifies the IP address of the interface from which the packets are forwarded.

`<interface_address>` may be either the IP address itself, such as 10.10.1.100, or a CIDR specification (network IP address/subnet prefix length) that contains the IP address, such as 10.10.1.0/24.

For every ActiveClient line, the software tap independently forwards packets from the interface specified in the line.

The following is an example of the configuration file specifying two interfaces using the interface name:

```
ActiveClient = 10.10.6.45, 2003, ifname=eth0
ActiveClient = 10.10.6.45, 2003, ifname=eth1
NullAuthPermit = YES
```

The following is an example of the configuration file specifying two interfaces using the interface IP address:

```
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.1.100
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.2.100
NullAuthPermit = YES
```

The following is an example of the configuration file specifying two interfaces using CIDR specifications that contain the interface IP address:

```
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.1.0/24
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.2.0/24
NullAuthPermit = YES
```

3. Save the configuration file. Make sure to save the file in ASCII format to prevent errors.

4. Restart the software tap by running the command

```
sudo /etc/init.d/rpcapd restart
```

Note: To reinstall the software tap after changing the configuration file, run the installation command and replace `<extrahop_ip>` and `<extrahop_port>` with the `-k` flag in order to preserve the modified configuration file. For example:

```
sudo sh ./install-rpcapd.sh -k
```

Monitoring Multiple Interfaces on a Windows Server

For servers with multiple interfaces, you can configure the software tap to forward packets from a particular interface or from multiple interfaces by editing its configuration file on the server.

To edit the configuration file, complete the following steps.

1. After installing the software tap, on the server, open the configuration file: C:\Program Files\rpcapd\rpcapd.ini

The configuration file contains this text or similar:

```
ActiveClient = 10.0.0.100,2003
NullAuthPermit = YES
```

2. Modify the existing ActiveClient line and create an ActiveClient line for each additional interface to be monitored. Specify each interface by its interface name or IP address. For every ActiveClient line, the software tap will independently forward packets from the interface specified in the line:

```
ActiveClient = <extrahop_ip>, <extrahop_port>, ifname=<interface_address>
```

or

```
ActiveClient = <extrahop_ip>, <extrahop_port>, ifaddr=<interface_name>
```

<interface_address> specifies the IP address of the interface from which the packets are forwarded. <interface_address> may be either the IP address itself, such as 10.10.1.100, or a CIDR specification (network IP address/subnet prefix length) that contains the IP address, such as 10.10.1.0/24.

<interface_name> is the name of the interface from which the packets are forwarded. The name is formatted as \Device\NPF_{<GUID>}, where <GUID> is the globally unique identifier (GUID) of the interface. For example, if the interface GUID is 2C2FC212-701D-42E6-9EAE-BEE969FEFB3F, the interface name is \Device\NPF_{2C2FC212-701D-42E6-9EAE-BEE969FEFB3F}.

The following is an example of the configuration file specifying two interfaces using the interface IP address:

```
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.1.100
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.2.100
NullAuthPermit = YES
```

The following is an example of the configuration file specifying two interfaces using CIDR specifications that contain the interface IP address:

```
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.1.0/24
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.2.0/24
NullAuthPermit = YES
```

The following is an example of the configuration file specifying two interfaces using the interface name:

```
ActiveClient = 10.10.6.45, 2003, ifname=\Device\NPF_{2C2FC212-701D-42E6-9EAE-BEE969FEFB3F}
ActiveClient = 10.10.6.45, 2003, ifname=\Device\NPF_{3C2FC212-701D-42E6-9EAE-BEE969FEFB3F}
NullAuthPermit = YES
```

3. Save the configuration (.ini) file. Make sure to save the file in ASCII format to prevent errors.

4. Restart the software tap by running the command

```
restart-service rpcapd
```

Note: To reinstall the software tap after changing the configuration file, run the installation command and replace `-RpcapIp` and `-RpcapPort` with the `-KeepConfig` flag in order to preserve the modified configuration file. For example:

```
.\install-rpcapd.ps1 -MgmtIp <extrahop_ip> -KeepConfig
```

or

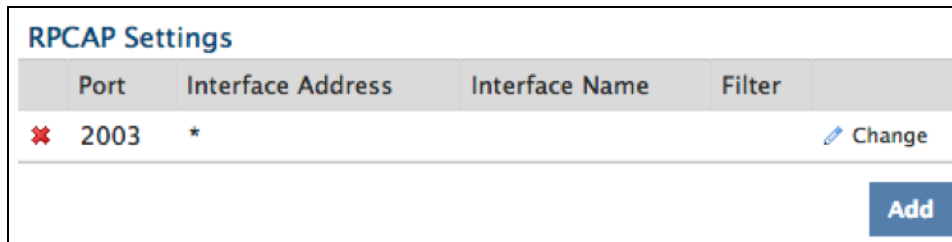
```
.\install-rpcapd.ps1 -InputDir . -KeepConfig
```

Configuring Additional RPCAP Settings

By default, the ExtraHop system accepts forwarded packets on port 2003. The servers using the software tap are directed to forward all traffic as denoted by the wildcard (*) in the Interface Address column.

(Optional) To specify another port, complete the following steps.

1. Go to the RPCAP Settings section and click **Change**.



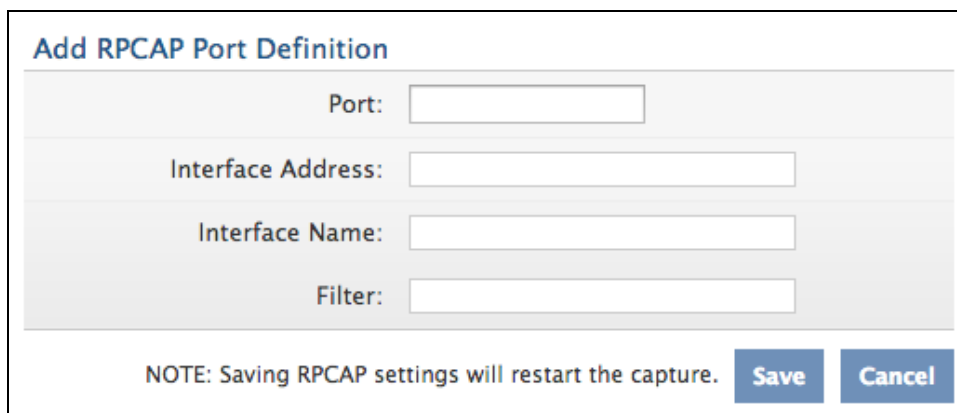
The screenshot shows the 'RPCAP Settings' section of a web interface. It contains a table with the following columns: Port, Interface Address, Interface Name, and Filter. The first row has a red 'X' icon, the value '2003' in the Port column, and a '*' in the Interface Address column. To the right of this row is a 'Change' button with a pencil icon. Below the table is an 'Add' button.

Port	Interface Address	Interface Name	Filter
✖ 2003	*		

[Change](#)

[Add](#)

2. Change and modify the settings on the Add RPCAP Port Definition page.



The screenshot shows the 'Add RPCAP Port Definition' form. It has four input fields: Port, Interface Address, Interface Name, and Filter. Below the fields is a note: 'NOTE: Saving RPCAP settings will restart the capture.' and two buttons: 'Save' and 'Cancel'.

Port:

Interface Address:

Interface Name:

Filter:

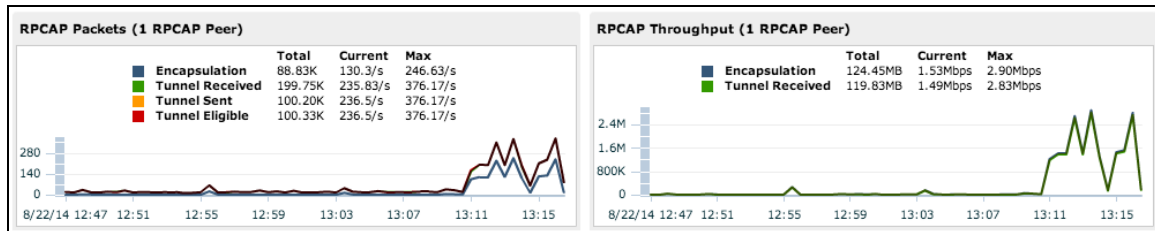
NOTE: Saving RPCAP settings will restart the capture. [Save](#) [Cancel](#)

- **Port:** Specifies the listening port on the ExtraHop system. Each port must be unique for each interface subnet on the same server. Different subnets across servers are able to use the same port.
- **Interface Address:** Specifies a subnet on the packet-forwarding server. If the server has multiple interfaces that match the interface address, the first interface on the server sends traffic to the ExtraHop system unless the interface name is specified.
- **Interface Name:** Indicates the interface on the packet-forwarding server from which to forward packets.
Note: You must specify an interface address or an interface name. If you specify both, then both criteria will apply.
- **Filter:** Specifies the traffic to forward using Berkeley Packet Filter syntax. For example, TCP port 80 forwards only TCP traffic on port 80, and not TCP port 80 forwards only non-TCP traffic on port 80.

Analyzing Wire Data from a Software Tap

To find out how much wire data the ExtraHop system is receiving from the software tap:

1. Log in to the ExtraHop Web UI (https://<extrahop_ip>/extrahop) and click the **Settings** button.
2. Click **System Health** to get more information about the forwarded traffic. This page displays a Packets and Throughput graph for each software tap connected to the ExtraHop system.



The RPCAP Packets and Throughput graphs contain four metrics:

- **Encapsulation**: The total number of RPCAP encapsulation packets received by the ExtraHop system.
- **Tunnel Eligible**: Total number of packets eligible to be forwarded to the ExtraHop system.
- **Tunnel Sent**: Total number of RPCAP-tunneled packets forwarded to the ExtraHop system.
- **Tunnel Received**: Total number of RPCAP-tunneled packets received by the ExtraHop system.

The tunnel eligible, tunnel sent, and tunnel received values are equal if the ExtraHop system is receiving and processing all the packets sent by the server. If they are not equal, use the following reference for troubleshooting:

- If **Tunnel Sent** is less than **Tunnel Eligible**, the server is not able to forward all of the traffic. This behavior may indicate that packet forwarding requires more processing or outbound bandwidth resources on the server. Consider separating the forwarding process onto a separate CPU or allocating a dedicated interface for forwarding traffic.
 - If **Tunnel Received** is less than **Tunnel Sent**, the ExtraHop system is not receiving all the traffic forwarded by the server. This behavior may be due to network congestion or insufficient resources on the ExtraHop system. If you suspect it is the latter, contact ExtraHop Support.
3. Once you have verified that the ExtraHop system is receiving traffic, exit the **System Health** page and view metrics in the ExtraHop Web UI.

Removing the Software Tap from a Linux Server

To remove the software tap, run the commands in one of the following sections.

Debian-Based Systems

To stop and remove the software tap from a Debian-based Linux server, run the following commands:

```
sudo service rpcapd stop
sudo dpkg -r rpcapd
sudo dpkg --get-selections | grep rpcapd
```

You can also set the `-P` flag to completely remove the package from your system.

RPM-Based Systems

To stop and remove the software tap from a RPM-based Linux server, run the following commands:

```
service rpcapd stop
rpm -e rpcapd-<extrahop_firmware_version>.x86_64
```

Generic/Other Linux Systems

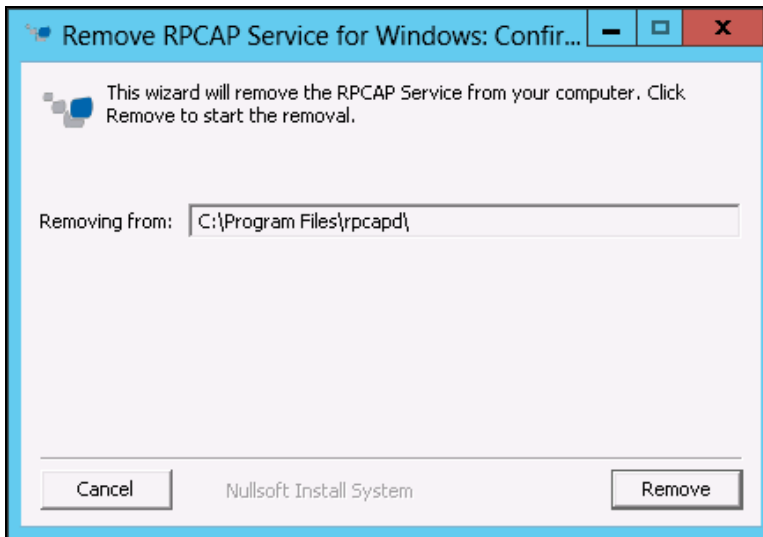
To stop and remove the software tap from another Linux server, run the following commands:

```
sudo /etc/init.d/rpcapd stop
sudo update-rc.d -f rpcapd remove
sudo rm -rf /opt/extrahop
sudo rm -f /etc/init.d/rpcapd
```

Removing the Software Tap from a Windows Server

To remove the software tap from a Windows server or your Windows desktop:

1. Go to the **Start Menu** and select **Control Panel**.
2. Select **Uninstall a program**.
3. Select **RPCAP Service for Windows**.
4. In the pop-up dialog box, click **Remove**.



5. When the removal is complete, click **Close**.

