Install the ExtraHop Discovery Edition with Hyper-V

Introduction

The ExtraHop Discovery Edition will help you to discover the performance of your applications across the network, web, VDI, database, and storage tiers. The ExtraHop Discovery Edition can monitor up to 50 systems in a Hyper-V deployment or a single server using a high-speed packet forwarder.

In a typical production deployment, the ExtraHop system operates in Port Mirroring mode, where it receives a copy of the network traffic through a SPAN or network tap. For testing and demonstration purposes, this guide also provides instructions to use the ExtraHop Discovery Edition in RPCAP mode. In this mode, you can send traffic to the ExtraHop system by installing a lightweight high-speed packet forwarder on any server you wish to monitor.

This guide explains how to install the ExtraHop Discovery Edition using the Hyper-V Manager running on a Windows Server 2012 machine. The guide assumes experience administering Hyper-V environments.

Installation Requirements

To ensure proper functionality of the virtual appliance:

- Do not change the default disk size on initial installation.
- Do not migrate the VM.
- Do not create a snapshot of the ExtraHop Discovery Edition, or you will be unable to change the disk size later.

Pre-Installation Checklist

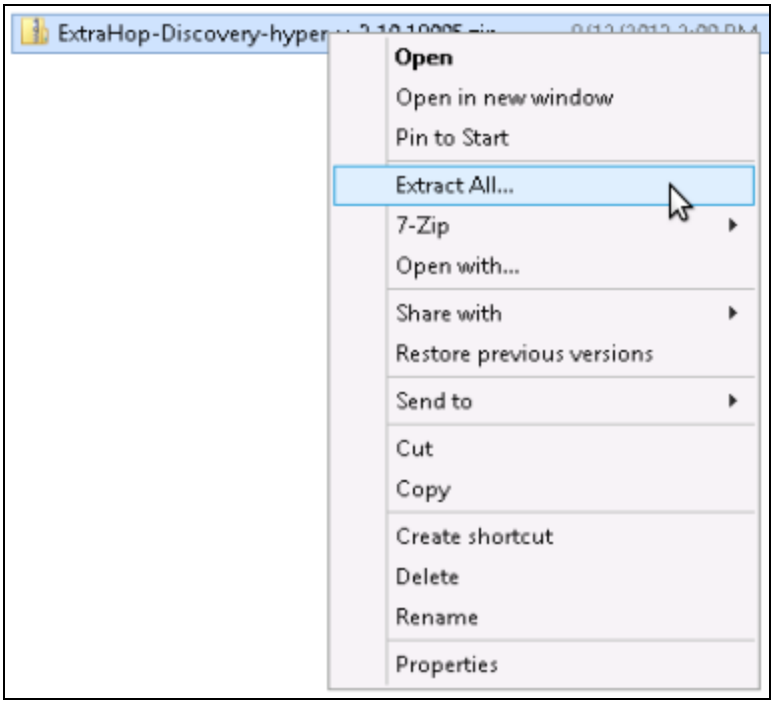
Before you install the ExtraHop Discovery Edition, ensure the following:

- You have downloaded the Hyper-V package for the ExtraHop Discovery Edition. If you have not downloaded the package, please contact support@extrahop.com
- You have the ExtraHop Discovery Edition license key provided by ExtraHop. Again, if you do not have a license key, please contact support@extrahop.com
- You have an existing installation of Hyper-V on Windows Server 2012 or later.
- Your Hyper-V server meets the minimum hardware requirements, and you understand ExtraHop's installation guidelines. Refer to *Appendix A* for more information.
- If you are using RPCAP mode, you have administrative access to the servers you want to monitor. If you want to use Port Mirroring mode, you have administrative access to the physical switches.
- If you are using RPCAP mode, you are running a 64-bit Linux or Windows OS. If you are using Windows, you are using Windows Server 2008 R2 or 2012.

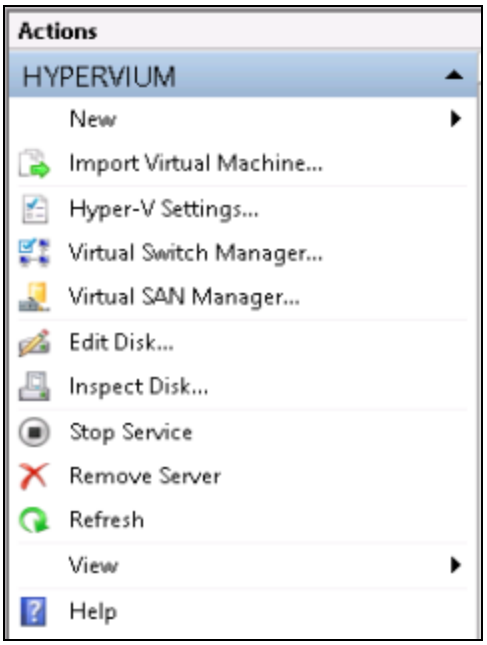
Installing the ExtraHop Discovery Edition Hyper-V Package

To install the ExtraHop Discovery Edition Hyper-V package, complete the following steps.

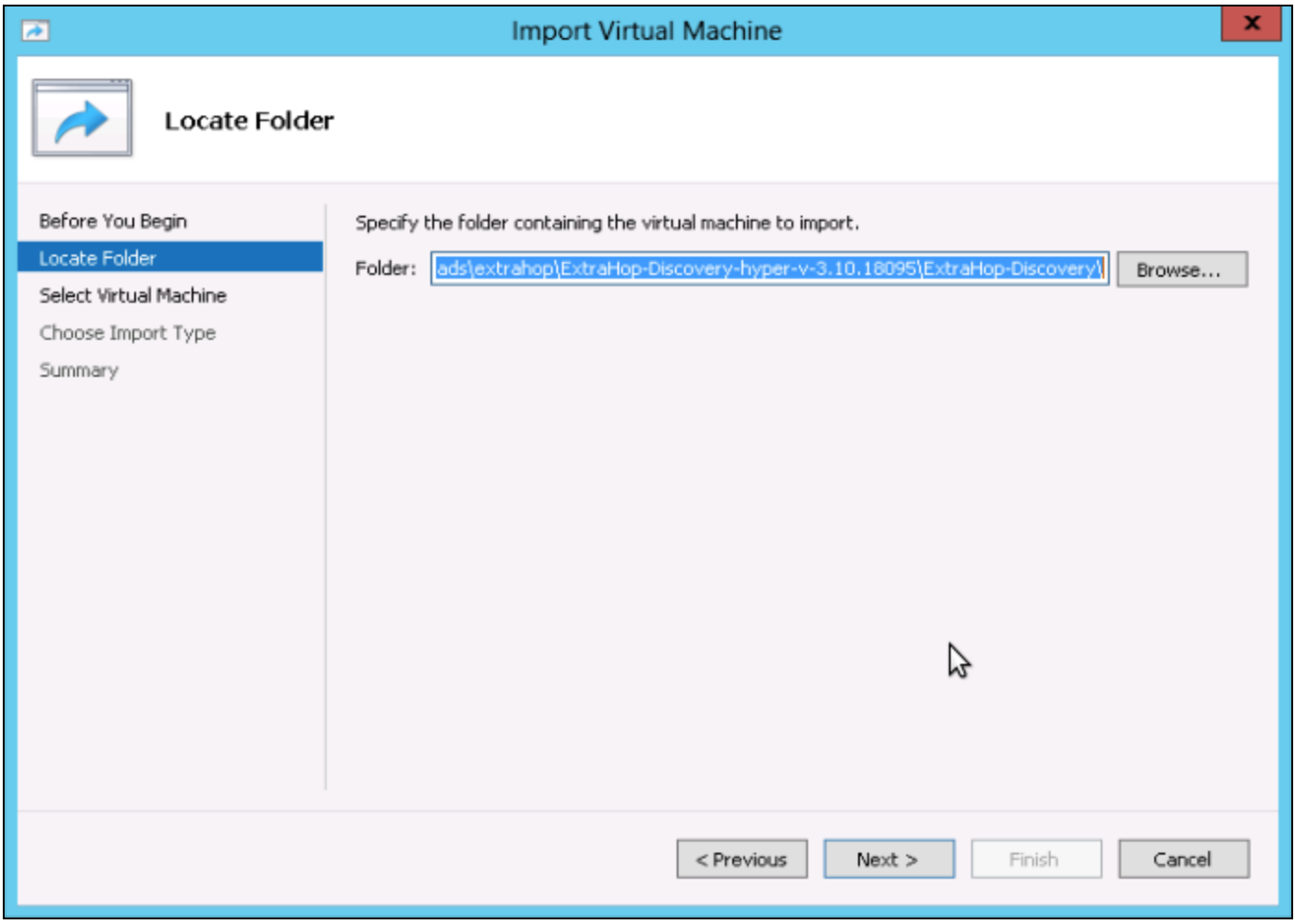
1. Unzip the ExtraHop Discovery Edition Hyper-V package provided by ExtraHop. Right-click the folder and click **Extract All**.



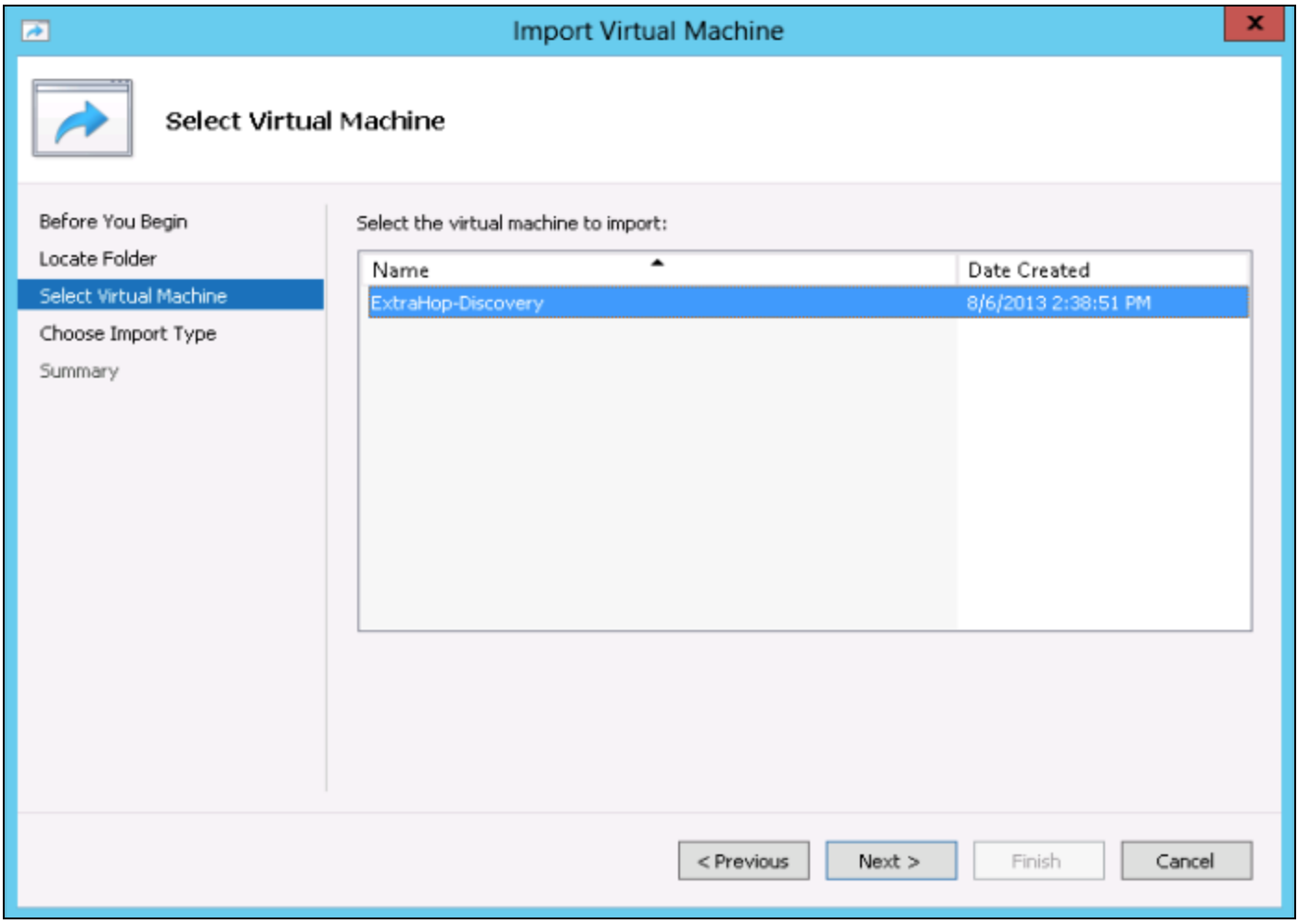
2. Click **Next** and wait approximately 5 minutes for the files to open.
3. Open the Hyper-V Manager.
4. In the Hyper-V Manager, go to the **Actions** panel in the right side of the screen and click **Import Virtual Machine**.



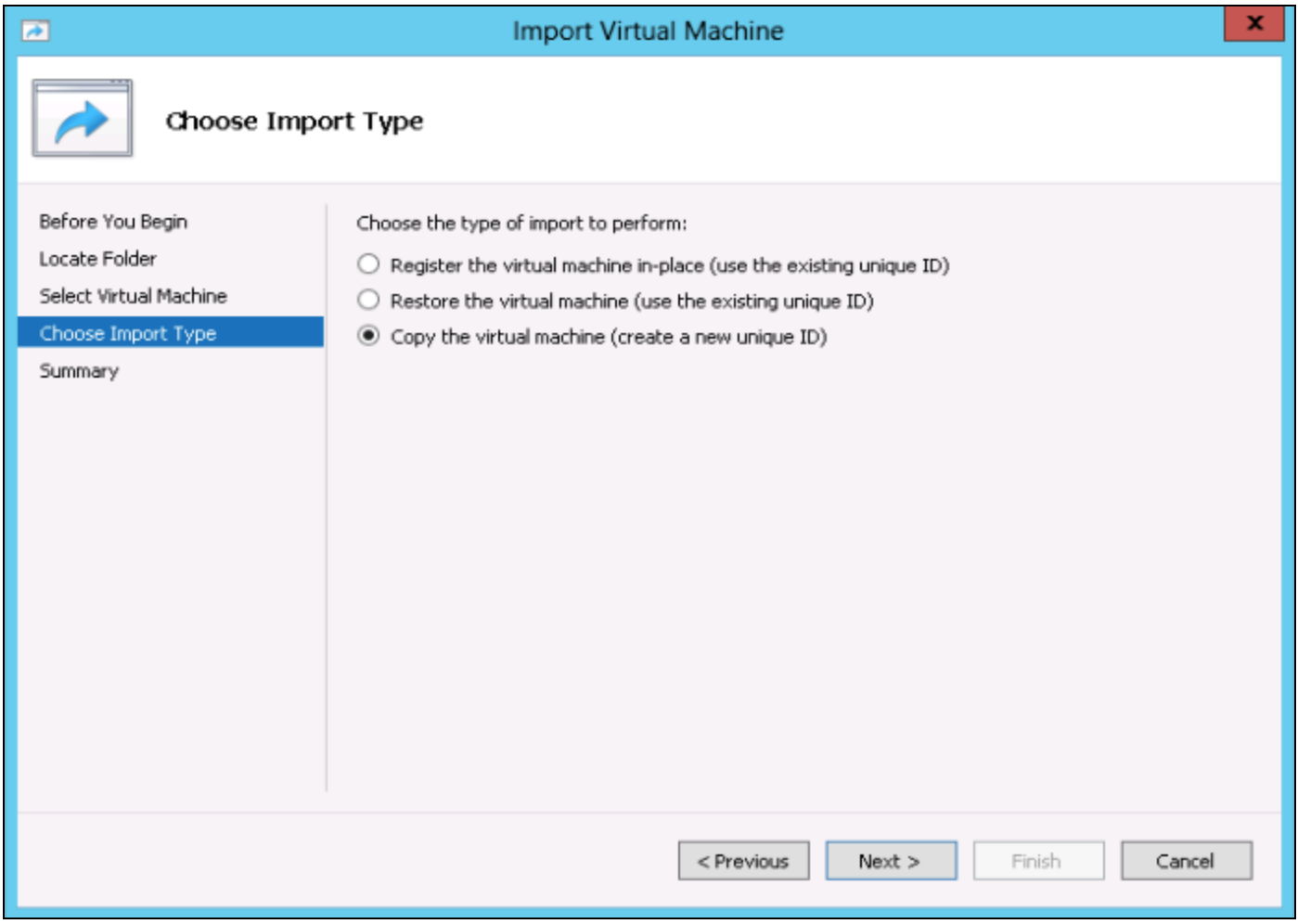
5. On the **Before You Begin** screen, click **Next**.
6. On the **Locate Folder** screen, browse to the ExtraHop-Discovery folder you just extracted.



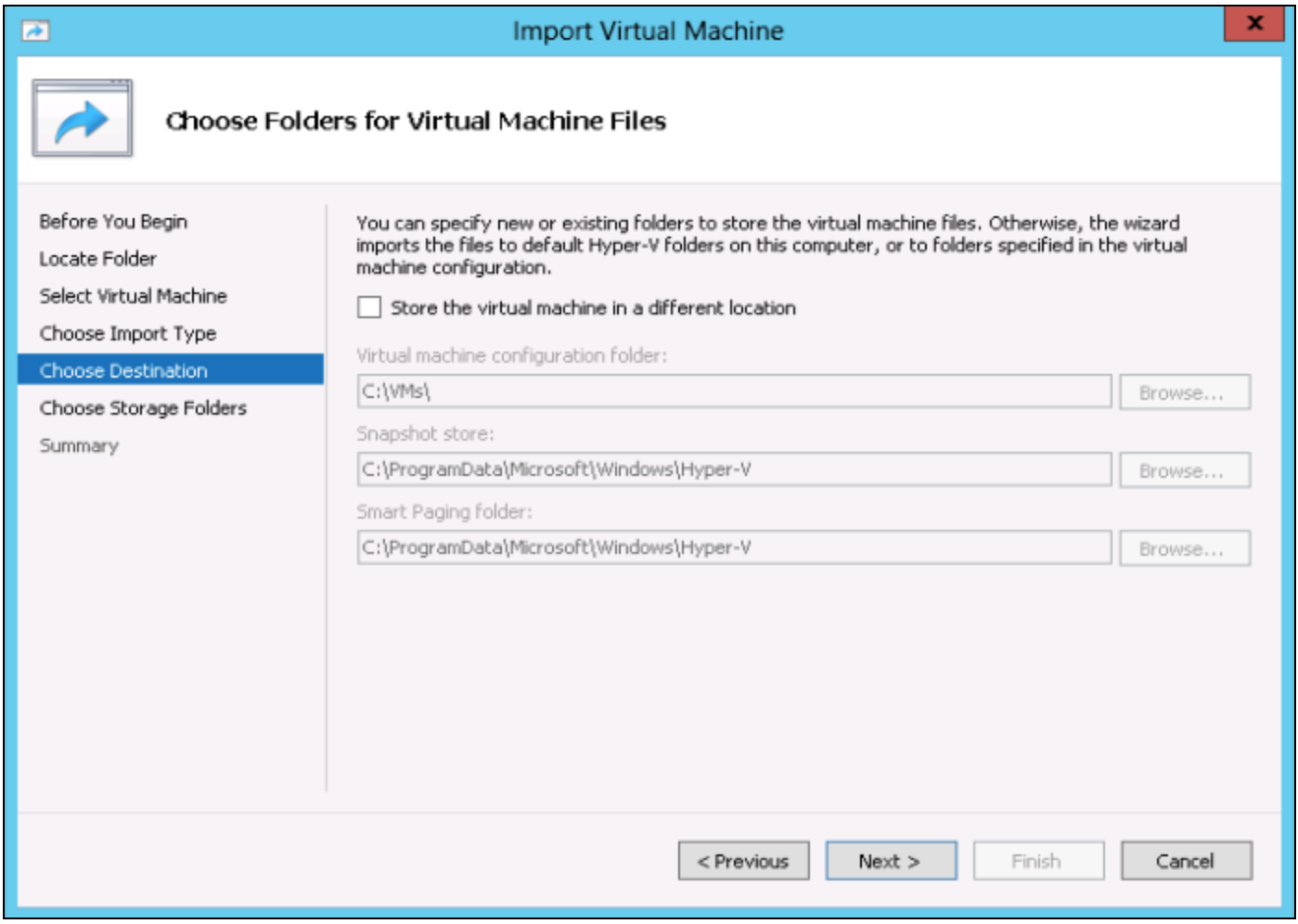
7. On the **Select Virtual Machine** screen, click **Next**.



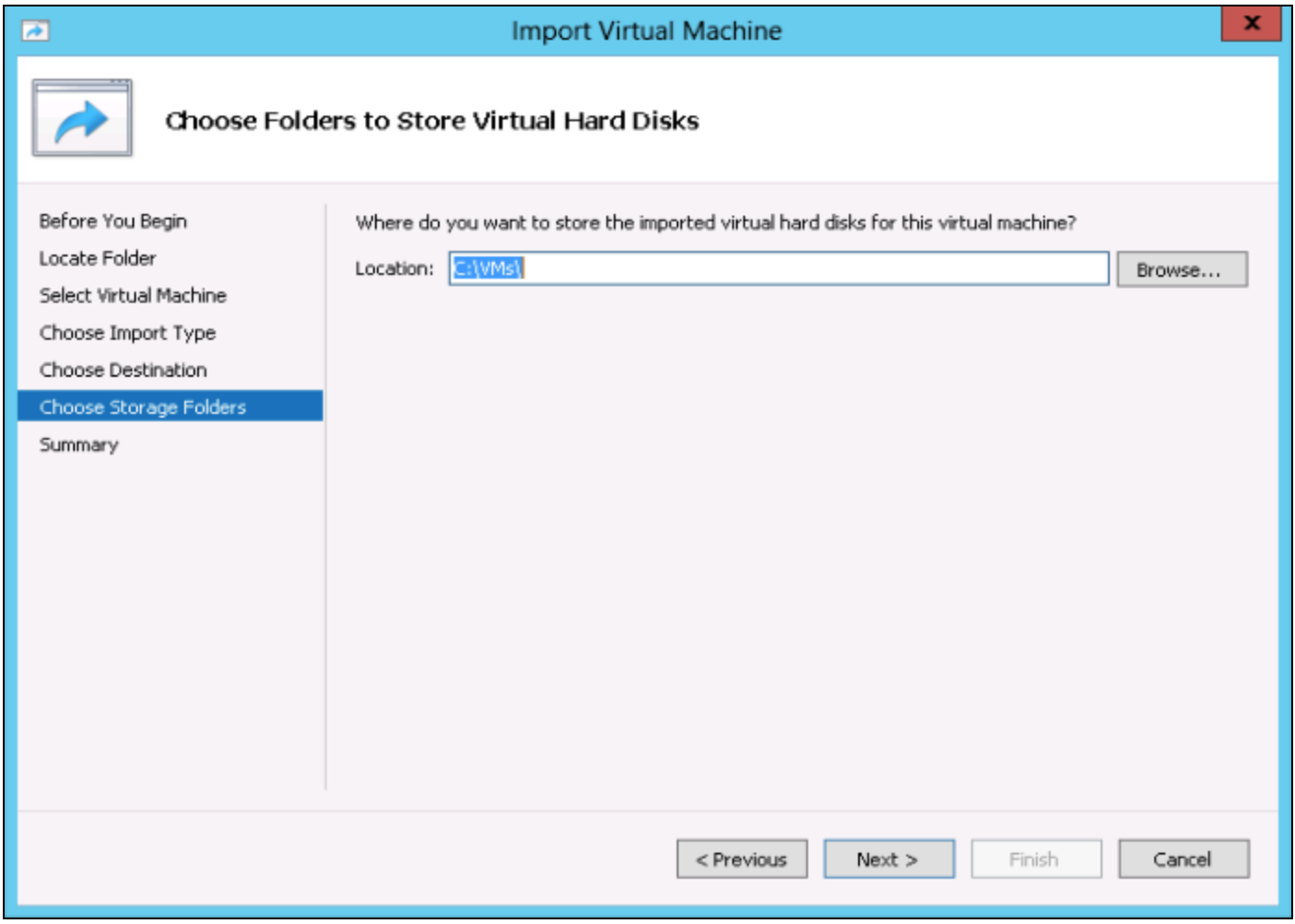
8. On the **Choose Import Type** screen, select **Copy the virtual machine** and click **Next**.



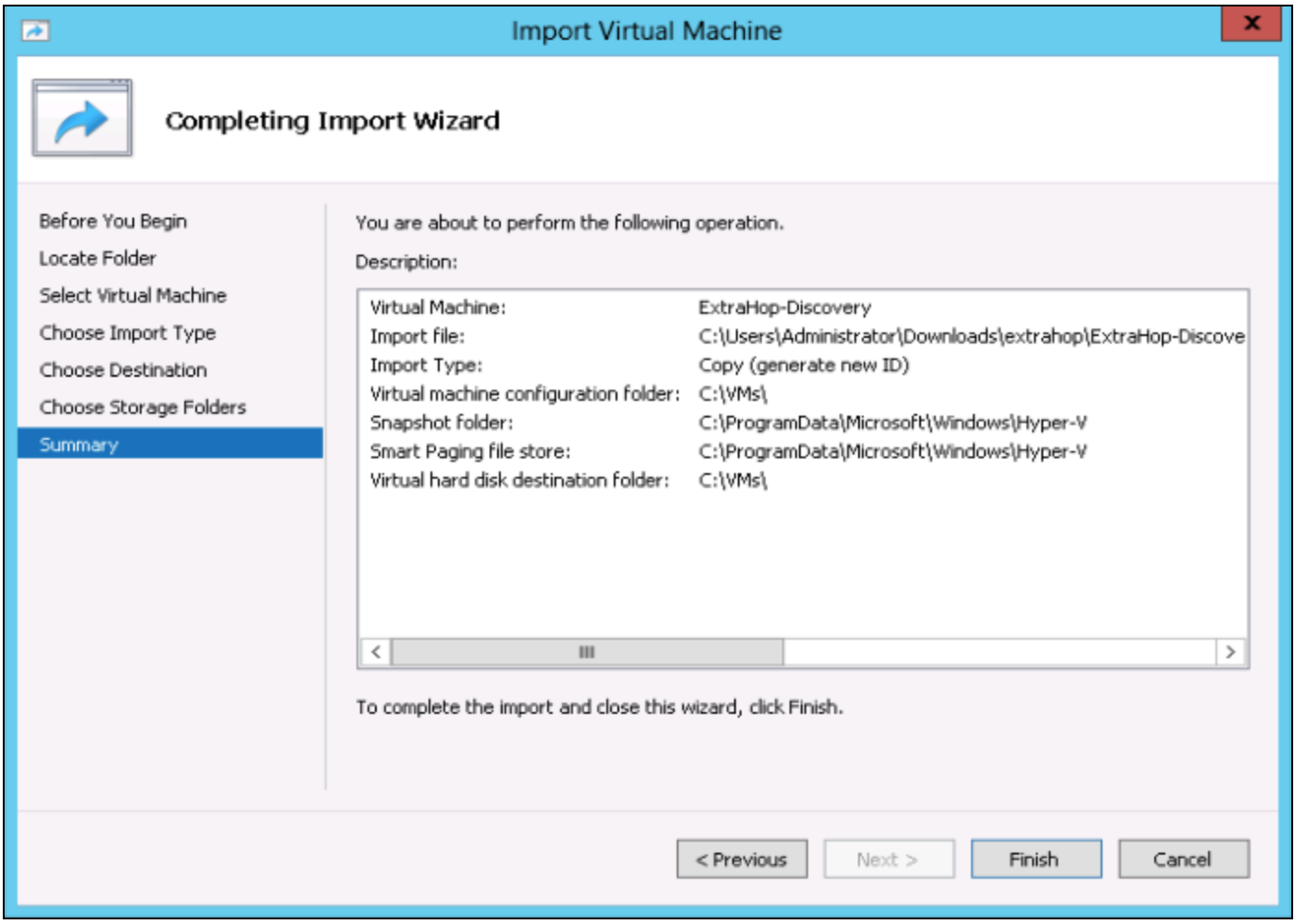
9. On the **Choose Destination** screen, select the location to store the configuration of the VM and click **Next**.



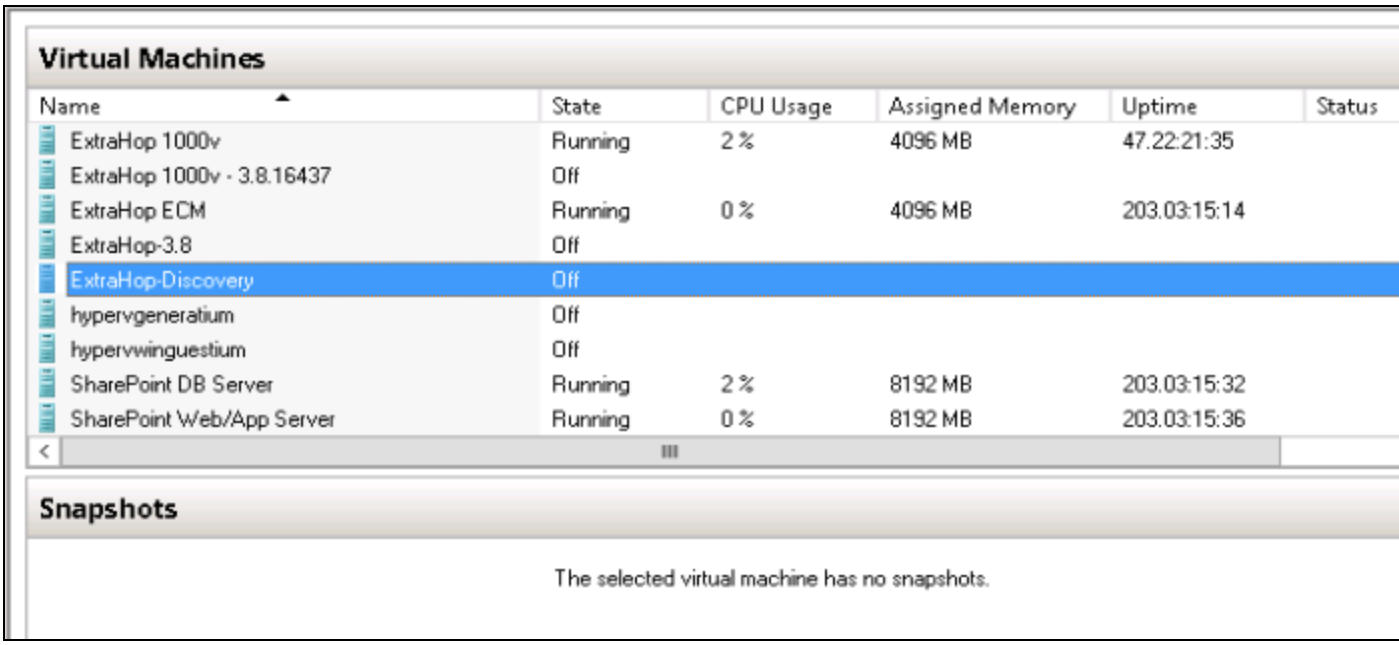
10. On the **Choose Storage Folders** screen, select the location to store the VM hard disks and click **Next**.



11. On the Summary screen, ensure you have made the correct selections and click **Finish** and wait approximately 10 minutes for the hard disks to copy.

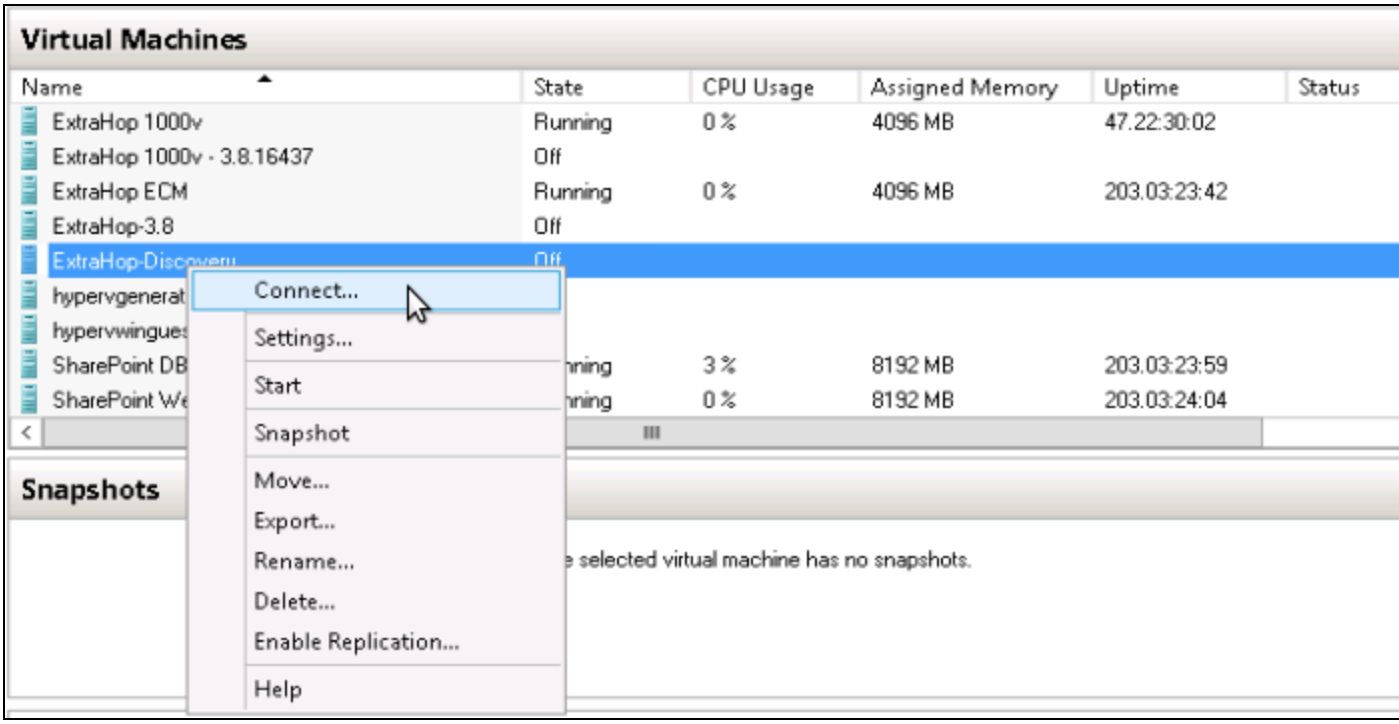


12. Go to the Virtual Machines list and find the ExtraHop-Discovery VM.

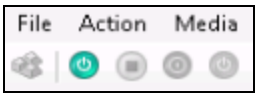


Powering On the ExtraHop Discovery Edition for the First Time

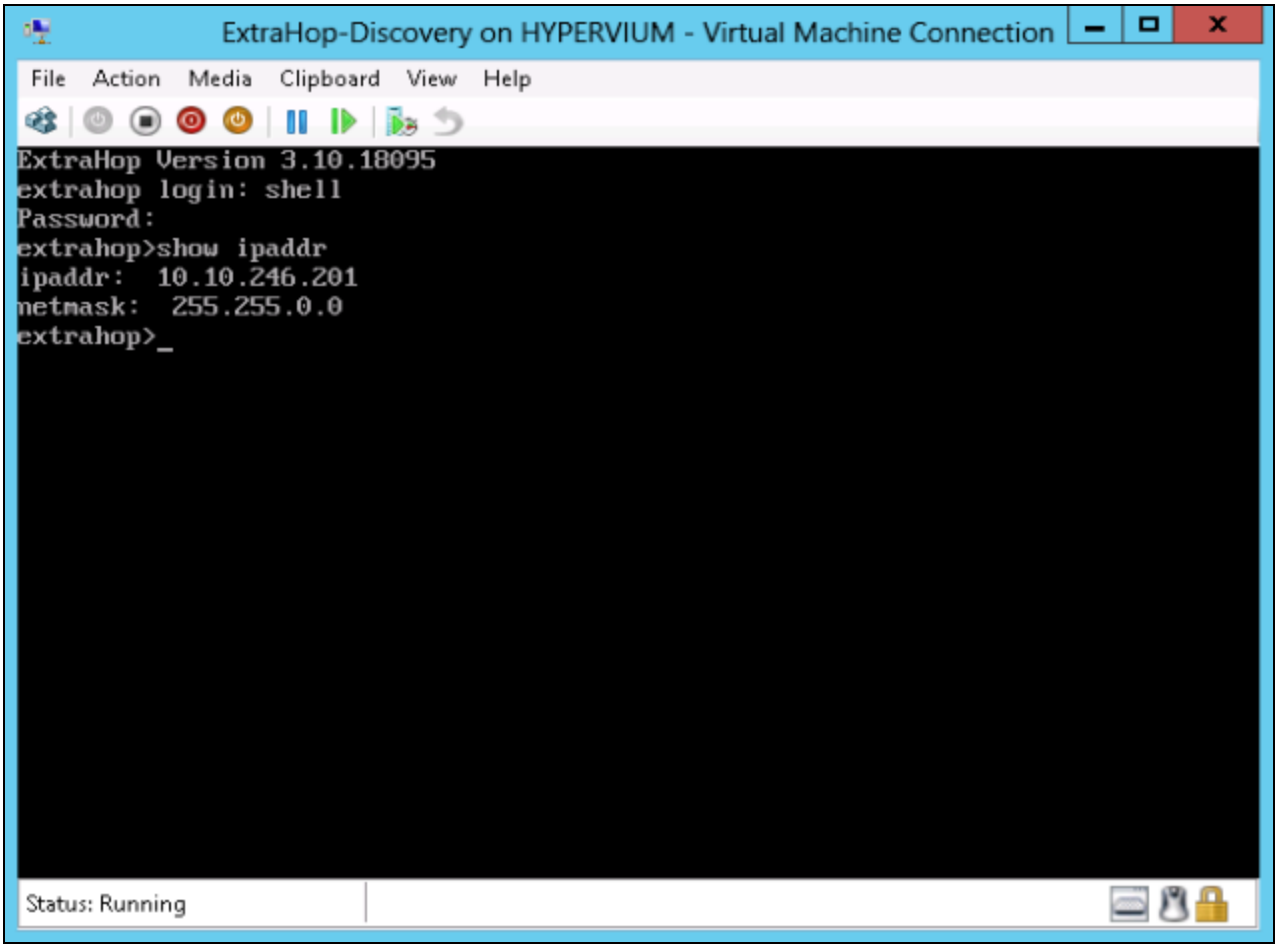
1. In the Virtual Machines list, right-click **ExtraHop-Discovery** and select **Connect**.



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



3. Log in with the `shell` user account and the password `default`.
4. Run the `show ipaddr` command to display the IP address of the ExtraHop Discovery Edition.



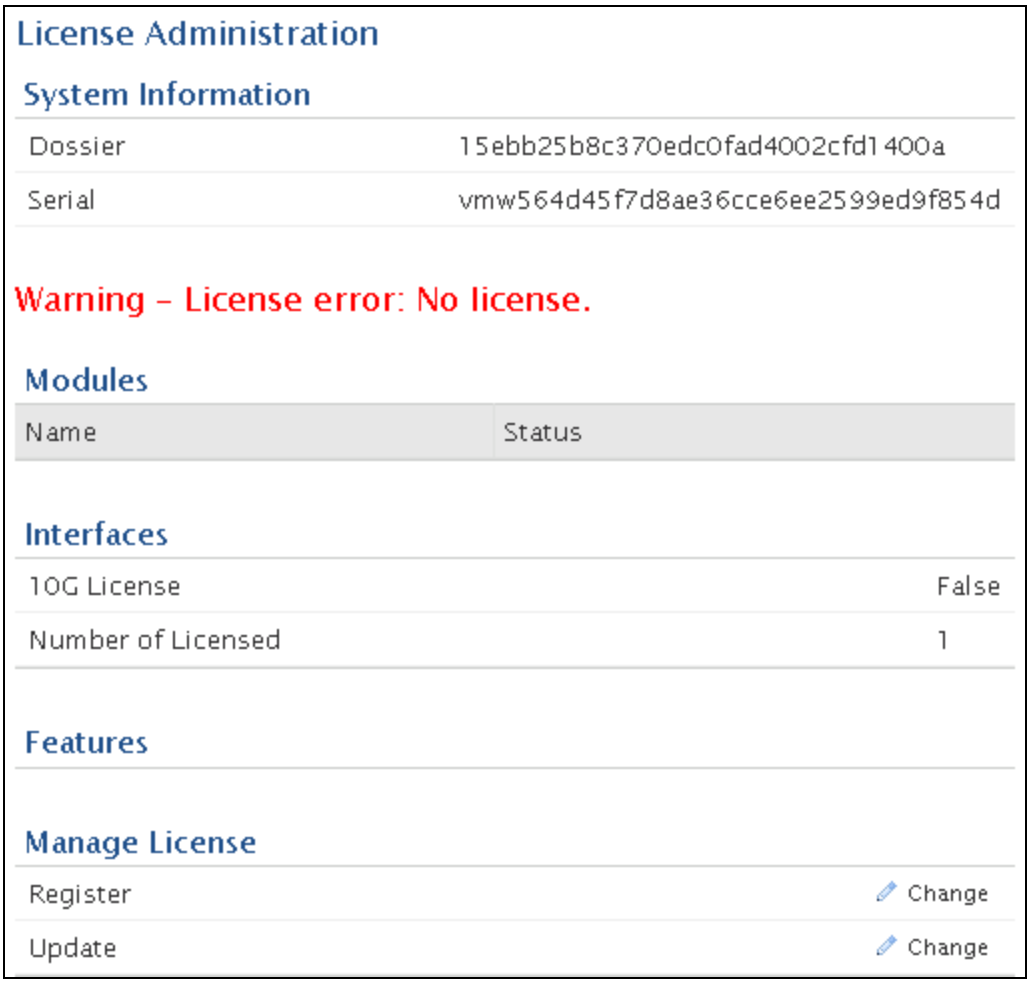
If your network does not support DHCP, refer to *Appendix B* to set a static IP address.

> 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.*

5. Go to your browser and type the IP address discovered above.
6. Review the End User Software License, select **I Agree**, and click **Submit**.
7. This VM requires a product key and a license in order to function. Log in to the Administration UI (https://ipaddress/admin) with the setup user account and the password `default`.

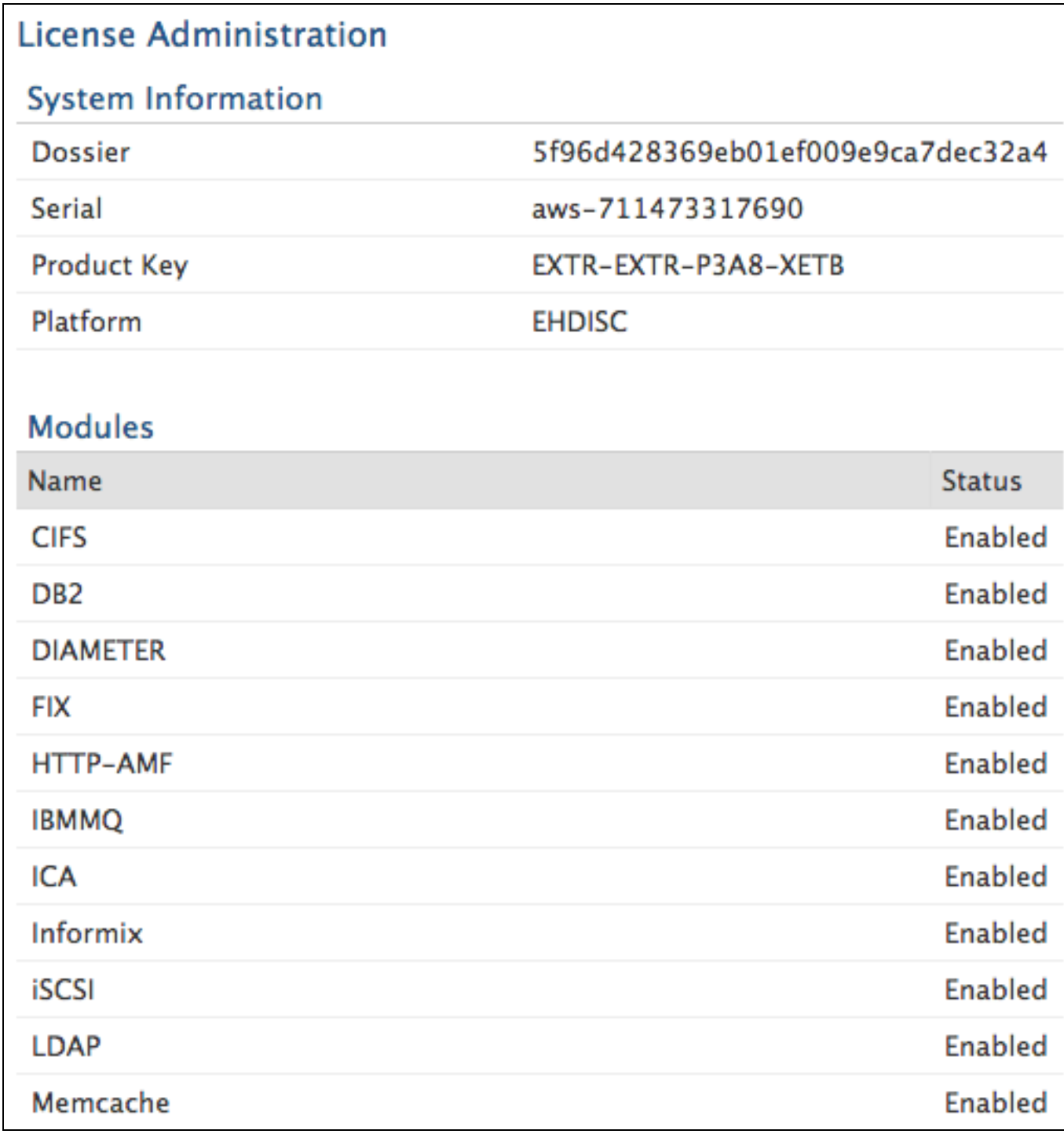
a. Click **Please apply license to Admin UI**.

b. Click **Register** to enter the product key.



c. Enter the product key and then click **Register**. The ExtraHop system now contacts the license server and validates the product key. After the product key is validated, the license is downloaded.

The following example shows a properly licensed ExtraHop Discovery Edition in the ExtraHop Admin UI:



License Administration

System Information

Dossier	5f96d428369eb01ef009e9ca7dec32a4
Serial	aws-711473317690
Product Key	EXTR-EXTR-P3A8-XETB
Platform	EHDISC

Modules

Name	Status
CIFS	Enabled
DB2	Enabled
DIAMETER	Enabled
FIX	Enabled
HTTP-AMF	Enabled
IBMMQ	Enabled
ICA	Enabled
Informix	Enabled
iSCSI	Enabled
LDAP	Enabled
Memcache	Enabled

Setting Up the ExtraHop Discovery Edition in RPCAP Mode

To monitor servers using RPCAP, you must do the following:

- Ensure the high-speed packet forwarder is enabled on the ExtraHop appliance. Refer to Appendix C for optional settings.
- Install the high-speed packet forwarder on the servers sending traffic.
- Analyze packet-forwarding traffic in the ExtraHop Web UI.

Installing the High-Speed Packet Forwarder on the Server Sending Traffic

(Linux) You must run the packet forwarder command on each server to be monitored in order to forward packets to the ExtraHop system.

1. Run the following command to download the packet forwarder on the server:

```
curl --connect-timeout 10 --fail -k \

'http://<extrahop_ip>/tools/install-rpcapd.sh' > \

install-rpcapd.sh
```

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

   > Some PDF viewers may add extra newlines when copying and pasting commands. Ensure the text has copied correctly before running the command.

2. Run the following command to install and run the packet forwarder on the instance:

```
sudo sh ./install-rpcapd.sh <extrahop_rpcap_target_ip>
<extrahop_rpcapd_port>
```

   Replace `<extrahop_rpcap_target_ip>` with the IP address of the interface on the ExtraHop system that is listening for the remote packet capture. This may be the same as the management IP if the server has only one interface. You can look up IP addresses in two ways:

   - Run the CLI command `show ip interface` on the ExtraHop system.
   - In the Admin UI, go to N**etwork Settings** and click **Connectivity**.

     Replace `<extrahop_rpcapd_port>` with the port used for the packet forwarder, which is port 2003 by default.

Example Output:

```
user@server:~$ sudo ./rpcapd-linux-64bit -n -v -S -a
"myextrahop,2003"

Press CTRL + C to stop the server...

Connecting to host myextrahop, port 2003, using protocol Unspecified

Opening 'rpcap://eth0'

pcap_set_buffer_size(16777216)

Connecting UDP packet data socket to 10.1.2.3:2003

setting IP_RECVERR to 1
```

```
   IP_RECVERR is set to 1

Ready to forward packets in single-threaded mode

ifrecv=17 (17) TotCapt=17 (17) krnldrop=0 0% (0 0%) ifdrop=0 (0)

sent=1 (1) sentbytes=1274 (1274) eagain=0 (0 sleep) enobufs=0 (0
sleep) senderr=0

   max_dispatch=1 max_caplen=66 read_timeout=0

ifrecv=61 (78) TotCapt=61 (78) krnldrop=0 0% (0 0%) ifdrop=0 (0)

sent=5 (6) sentbytes=5444 (6718) eagain=0 (0 sleep) enobufs=0 (0
sleep) senderr=0

   max_dispatch=10 max_caplen=253 read_timeout=1

ifrecv=2 (80) TotCapt=2 (80) krnldrop=0 0% (0 0%) ifdrop=0 (0)

sent=0 (6) sentbytes=0 (6718) eagain=0 (0 sleep) enobufs=0 (0 sleep)
senderr=0

   max_dispatch=1 max_caplen=60 read_timeout=1
```

Notes:

To start, stop, restart, reload, or check the status of the packet forwarder, run the command

```
sudo /etc/init.d/rpcapd {start|stop|status|restart|force-reload}
```

To view packet forwarder messages, run the command

```
tail /var/log/messages or tail /var/log/syslog
```

To run the packet forwarder manually for debugging purposes only, run the command

```
sudo /opt/extrahop/sbin/rpcapd -a <extrahop_rpcap_target_
ip>,<extrahop_rpcapd_port> -n -v
```

To run the packet forwarder on servers with multiple interfaces, refer to *Appendix E.*

(Windows) You must run the packet forwarder command on each server to be monitored in order to forward packets to the ExtraHop system.

1. Open a PowerShell shell with *Administrator* privileges on the Windows server.
2. Run the following installation command to change the PowerShell execution policy:

```
set-executionpolicy unrestricted
```

3. Run the following command to download the packet forwarder on the server:

```
(new-object system.net.webclient).downloadfile
("http://<extrahop_ip>/tools/install-rpcapd.ps1", "install-
rpcapd.ps1");
```

Some PDF viewers may add extra newlines when copying and pasting commands. Ensure the text has copied correctly before running the command.

4. Run the following command to install the packet forwarder on the server:

```
.\install-rpcapd.ps1 -MgmtIp <extrahop_ip> -RpcapIp <extrahop_
rpcap_target_ip> -RpcapPort <extrahop_rpcapd_port>
```

   Replace `<extrahop_ip>` with the ExtraHop system's interface 1 IP.

   Replace `<extrahop_rpcap_target_ip>` with the IP address of the interface on the ExtraHop system that is listening for the remote packet capture. This may be the same as the management IP if the server has only one interface. You can look up IP addresses in two ways:

   - Run the CLI command show ip interface on the ExtraHop system.
   - In the Admin UI, go to **Network Settings** and click **Connectivity**.

   Replace `<extrahop_rpcapd_port>` with the port used for the packet forwarder, most commonly port 2003.

Notes:

To set the PowerShell execution policy back to the default, run the command

```
set-executionpolicy restricted
```

To start, stop, restart, or check the status of the packet forwarder, run the command

```
{start-service|stop-service|restart-service|get-service} rpcapd
```

To view packet forwarder messages, open the Event Viewer, click **Windows Logs**, and select **Application**. In the Application panel, sort by source and scroll down to **rpcapd**.

When reinstalling rpcapd, if a message appears that rpcapd is being used by another process, make sure the Event Viewer is closed.

To run the packet forwarder manually for debugging purposes only, run the command

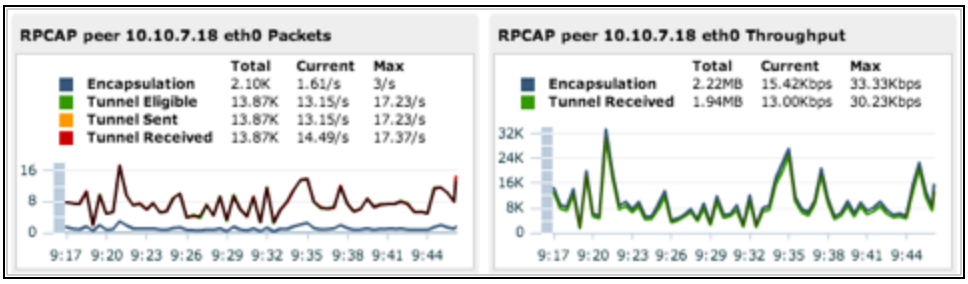
```
"C:\Program Files\rpcapd\rpcapd" -a <extrahop_rpcap_target_
ip>,<extrahop_rpcapd_port> -n -v
```

To run the packet forwarder on servers with multiple interfaces, refer to *Appendix E.*

Analyzing Packet Forwarding Traffic in the ExtraHop Web UI

To find out how much forwarded traffic the ExtraHop system is receiving, complete the following steps.

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



The RPCAP Packet 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, use the following reference for troubleshooting:

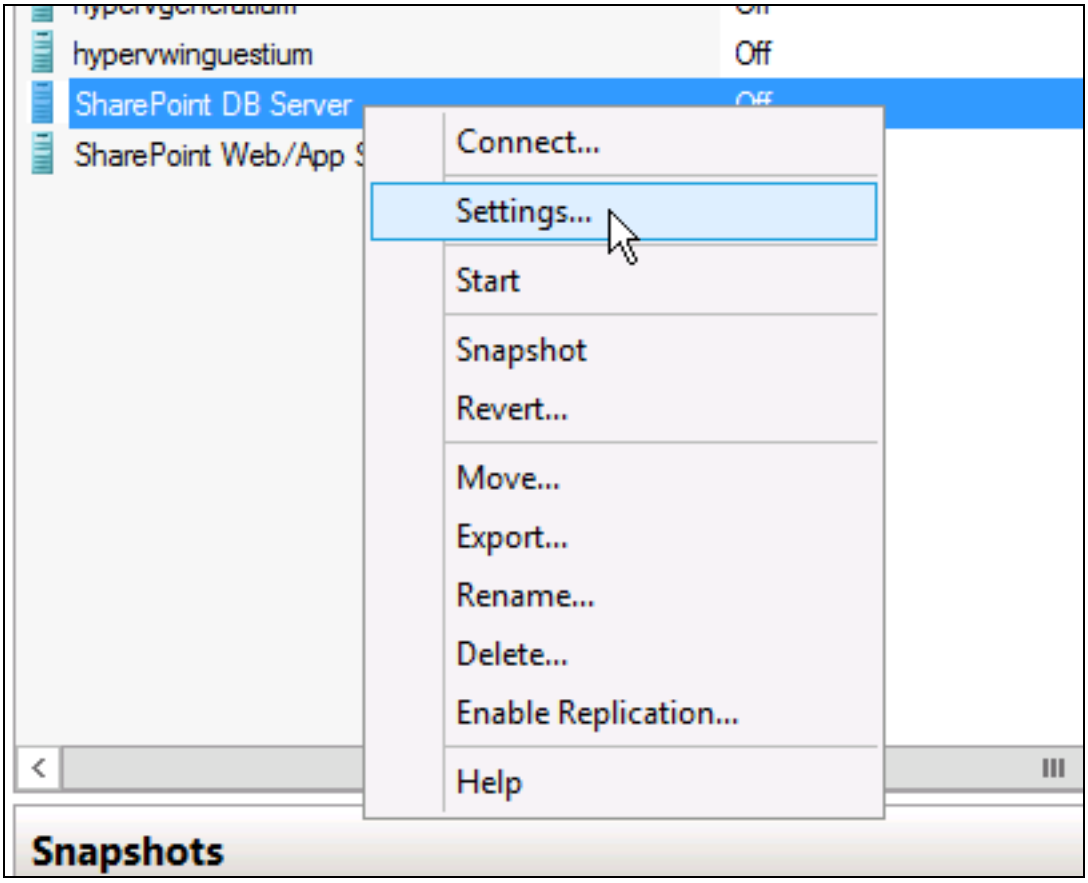
- If **Tunnel Sent** is less than **Tunnel Eligible**, the server is not able to forward out all the traffic. This may indicate that packet forwarding requires more processing or outbound bandwidth resources on the server. Consider separating the forwarding process onto a separate CPU or allocating a 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 may be due to network congestion or insufficient resources on the ExtraHop system. If you suspect it is the latter, contact ExtraHop Support.

Setting Up the ExtraHop Discovery Edition in Port Mirroring Mode

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.

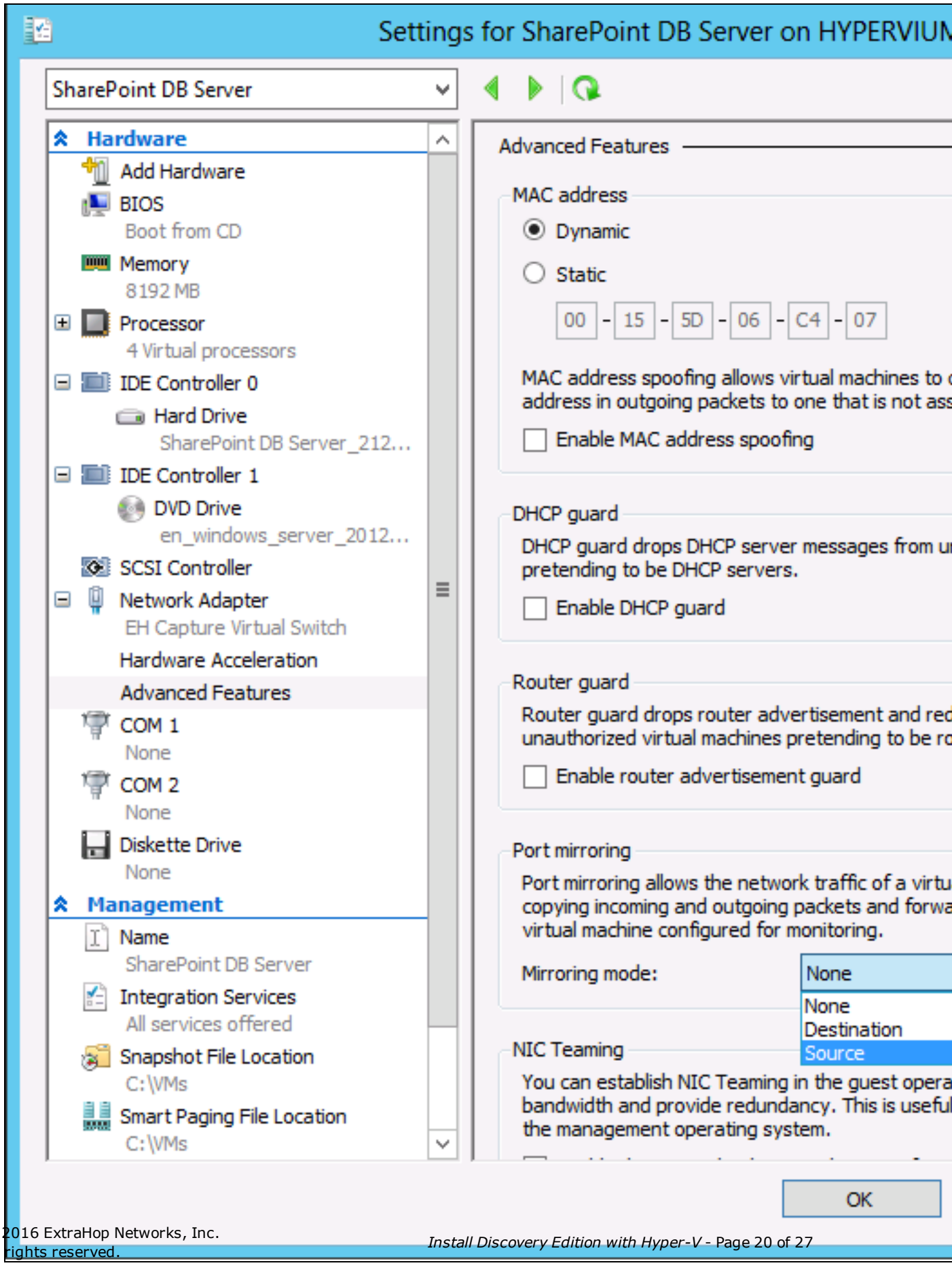
Enabling Port Mirroring Mode in the Hyper-V Manager

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



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

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



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

Appendix A: System Requirements

Installation of the ExtraHop Discovery Edition has the following requirements:

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

Hardware Requirements

The following Hyper-V server hardware is required:

- **Processor**: Two Intel processing cores with hyper-threading support, VT-x technology, 64-bit architecture, and processing speed 2.5GHz or higher
- **Memory**: 4GB or larger
- **Disk**: 16GB or larger
- **Network**: If the ExtraHop Discovery Edition is monitoring traffic on a single server or intra-VM traffic only, one 1Gbps Ethernet network port is required (for management). The management interface must be accessible on port 443.

  If the ExtraHop Discovery Edition is monitoring the intranet network traffic, two 1Gbps 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 Hyper-V server must support network interface drivers.

  If the ExtraHop Discovery Edition is using the RPCAP packet forwarder, the packet-forwarding interface must be accessible on TCP ports 443 and 80 to download the file and UDP/TCP port 2003 to use packet forwarding. To avoid opening port 443, refer to Appendix D: Using Additional RPCAP Installation Commands on page 22 to download the file manually.
- **Registration**: For registration purposes, the ExtraHop Discovery Edition requires outbound DNS connectivity on UDP port 53.

  The preconfigured virtual appliance has the following default settings:
- Two CPUs
- 4GB RAM
- One 4GB disk
- One 12GB disk
- Two network interfaces

- One bridged network interface for management
- (Optional) One network interface for port mirroring or capturing traffic from the VM switch

Appendix B: Configuring a Static IP Address

The ExtraHop Discovery Edition 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, perform the following steps:

1. Log in to the console with the shell user account 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 10.10.2.14 255.255.0.0
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 10.10.2.14 255.255.0.0 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)#
```

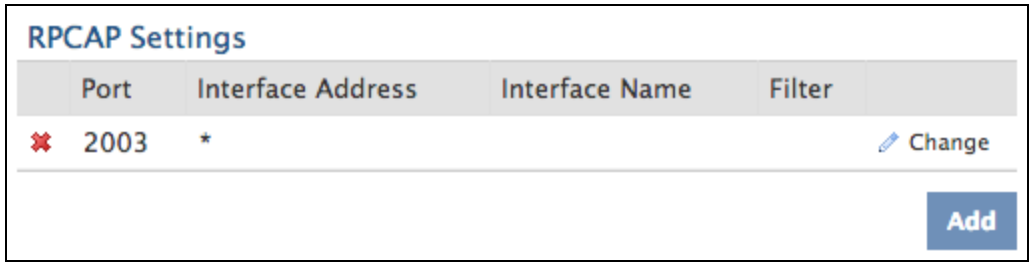
The default time server setting is pool.ntp.org. To configure the time servers manually, refer to the *System Settings* section of the *ExtraHop Admin UI Users Guide.*

Appendix C: Configuring Additional RPCAP Settings

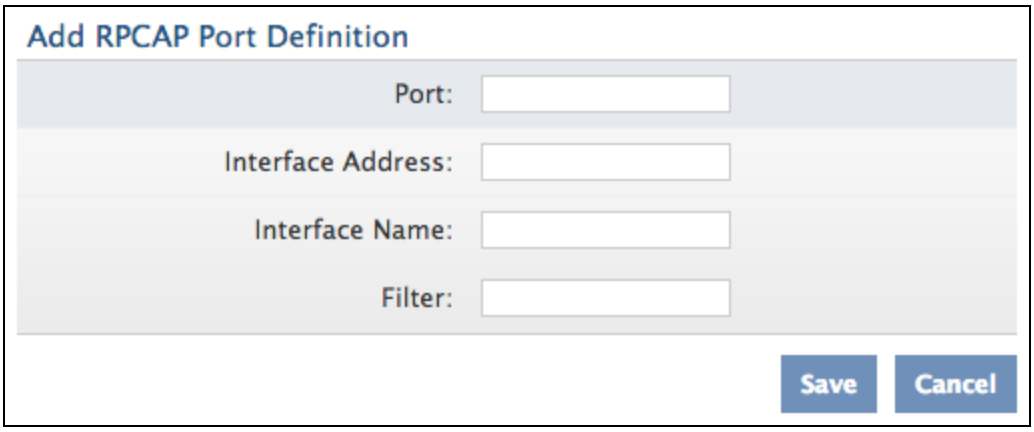
By default, the ExtraHop system accepts RPCAP forwarded packets on port 2003. The servers using the packet forwarder are directed to forward all traffic as denoted by the wildcard in the **Interface Address** column.

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

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



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



- **Port:** Specifies the listening port on the ExtraHop system. Each port must be unique for each interface subnet on the same device. Different subnets across servers are able to use the same port.
- **Interface Address:** Specifies a subnet to choose the interface from which to forward packets. If the server has multiple interfaces that match the interface address, the first interface on the server sends traffic to the ExtraHop system.
- **Interface Name:** Indicates the interface on the packet-forwarding server from which to forward packets.

  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.

Appendix D: Using Additional RPCAP Installation Commands

Linux

To download the packet forwarder manually, complete the following steps.

1. Go to https://<extrahop_ip>/tools.
2. Download the rpcapd file for Linux.
3. Install it on the server by running the command

```
sudo sh ./install-rpcapd.sh <extrahop_ip> <extrahop_port>
```

Windows

To download the packet forwarder manually, complete the following steps.

1. Go to `https://<extrahop_ip>/tools`.
2. Download and unzip the rpcapd file for Windows.
3. Open PowerShell and navigate to the directory containing the unzipped files.

4. Run the command `./install-rpcapd.ps1 -InputDir . -RpcapIp <extrahop_ip> -RpcapPort <extrahop_port>`

Appendix E: Monitoring Multiple Interfaces

For servers with multiple interfaces, the packet forwarder can be configured to forward packets from a particular interface or from multiple interfaces by editing its configuration file on the server.

Linux

To edit the configuration file, complete the following steps.

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

   After installation, 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 packet forwarder 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 and restart the packet forwarder. Run the command

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

> To reinstall the packet forwarder 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
> ```

Windows

To edit the configuration file, complete the following steps.

1. After installing the packet forwarder, open the configuration file on the server: `C:\Program Files\rpcapd\rpcapd.ini`

   After installation, the 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 packet forwarder 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 and restart the packet forwarder by running the command `restart-service rpcapd`

> To reinstall the packet forwarder 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
```

Appendix F: Setting Up Automatic Restart

It is best practice to enable the VM to automatically restart in case of power failure. To set up automatic restart, complete the following steps.

1. Right click **ExtraHop-Discovery** and click **Settings**.
2. Click **Automatic Start Action**.
3. Click the **Automatically start...** and click **OK**.