Deploy the ExtraHop Discover Appliance with Hyper-V

Published: 2018-10-10

The following procedures explain how to deploy the ExtraHop Discover EDA 1000v and EDA 2000v virtual appliance on the Microsoft Hyper-V platform. You must have experience administering your hypervisor product to complete these procedures.

Virtual machine requirements

You must have an existing installation of Hyper-V on Windows Server 2012 (or later) capable of hosting the Discover virtual appliance. In addition, you need Hyper-V Manager to manage the virtual machine.

The following table provides the server hardware requirements for each Discover model.

EDA 1000v	EDA 2000v
2 CPUs with hyper-threading support, VT-x technology, and 64-bit architecture. If you want to enable SSL decryption, 3 CPUs are required. For more information, see Add a CPU Core to the EDA 1000v with Hyper-V.	6 CPUs with hyper-threading support, VT-x technology, and 64-bit architecture.
4 GB RAM or higher	6 GB RAM or higher
46 GB or higher disk (thick-provisioned)	255 GB or higher disk (thick-provisioned)

To ensure proper functionality of the virtual appliance:

- Do not change the default disk size on initial installation. Keeping 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.
- 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.

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

For both the EDA 1000v and EDA 2000v, you can 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. One for the physical port mirror and one for management. The physical 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.

Note: All of the virtual NICs are configured in trunk mode by default. If you need to assign a specific VLAN to your management interface, you must modify the interface through PowerShell to change the management interface to access mode.

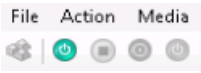
© 2018 ExtraHop Networks, Inc. All rights reserved.

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

Install the files for Hyper-V

Before you begin
If you have not already done so, download the ExtraHop Discover firmware file for Hyper-V from the ExtraHop Customer Portal and extract the contents from the `.zip` file to your Windows Server machine.

1. On your Windows Server machine, 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. If the Before You Begin screen appears, click **Next**. Otherwise, continue to the next step.
4. Browse to the folder with the extracted files and click **Next**.
5. Select the virtual machine to import and 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**.
8. 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**.
12. Right-click the virtual machine again and select **Connect**.
13. Click the green start button at the top of the screen and wait for the login prompt.



14. At the login prompt, type `shell` and then press ENTER.
15. At the password prompt, type `default`, and then press ENTER.
16. Run the `show ipaddr` command to display the IP address and netmask of the Discover appliance. You need the IP address to apply the ExtraHop license in the next procedure.

> **Note:** If your network does not support DHCP, see Configure a Static IP Address to set a static IP address.

Configure a static IP address through the CLI

The ExtraHop appliance 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.

1. Establish a console connection to the ExtraHop appliance.
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 Web UI 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 appliance.

After the appliance 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 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 specifies Network Adapter 1 as the management interface.

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

Monitoring intra-VM traffic

The Discover appliance can be configured to monitor network traffic of another VM on the same host by choosing **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.

Enable port mirroring mode in the Hyper-V manager

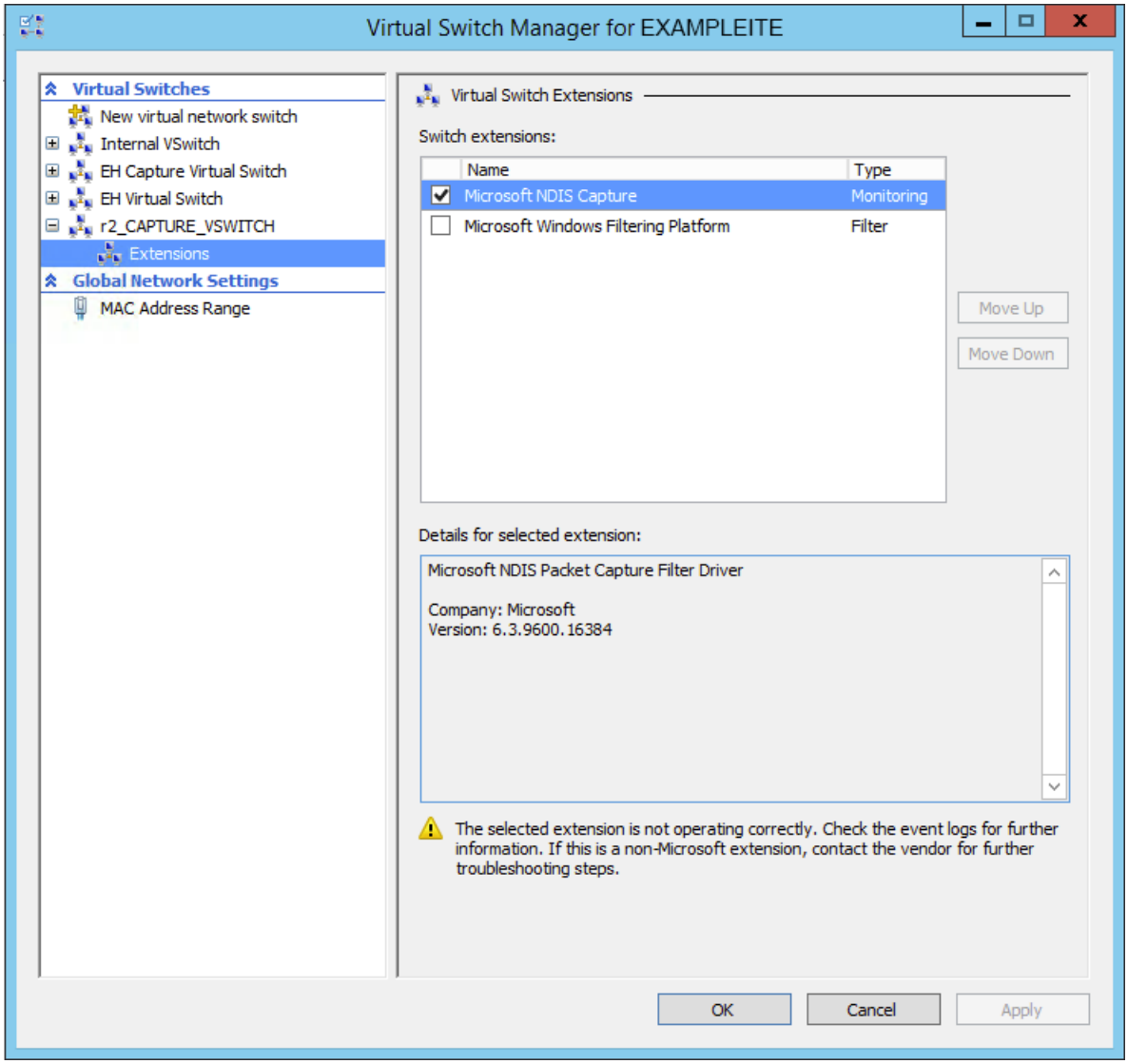
1. Right-click the ExtraHop Discover VM and select **Settings**.
2. Expand **Network Adapter** and click **Advanced Features**.
3. In the Port mirroring section, click the Mirroring mode drop-down list and select **Source**.
4. Make note of the source network and ensure the capture interface on the ExtraHop VM is on the same network.

5. Click **Apply**.
6. Click **OK**.
7. 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 Discover 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 **Destination**.
4. Click **Apply**.
5. Click **OK**.
6. Expand the virtual switch associated with the external data feed and enable the **Microsoft NDIS Capture** switch. You can ignore the warning that the selected extension is not operating correctly.



7. Click **Apply**, and then click **OK**.
8. Start Windows PowerShell with administrator privileges.

9. Configure the external port of the virtual switch by running the following commands:
   a) Store the `FeatureName` parameter in a variable:

```
$portFeature=Get-VMSystemSwitchExtensionPortFeature -FeatureName
 "Ethernet Switch Port Security Settings"
```

   b) Change the monitor mode of the virtual switch to Source:

```
$portFeature.SettingData.MonitorMode = 2
```

   c) Add an external port to the virtual switch that includes the `FeatureName` parameter specified in step 9a:

```
add-VMSwitchExtensionPortFeature -ExternalPort -SwitchName
 <name_of_switch> -VMSwitchExtensionFeature $portFeature
```

   Where <*name_of_switch*> is the name of the virtual switch.
10. Optional: To receive mirrored traffic from multiple VLANs, set the VM NIC to trunk mode and specify a list of allowed VLAN IDs by running the following command:

```
Set-VMNetworkAdapterVlan -VMName <destination_vm> -Trunk -
AllowedVlanIdList <id_list> -NativeVlanId <vlan_id>
```

    Where <*destination_vm*> is the name of the Discover VM, <*id_list*> is the list of allowed VLAN IDs, and <*vlan_id*> is the ID of the default VLAN.

    For example:

```
Set-VMNetworkAdapterVlan -VMName EDA1000v -Trunk -AllowedVlanIdList 1-100
 -NativeVlanId 10
```

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 implement 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 (Windows Server 2008 R2 or 2012).

To ensure proper functionality of the ExtraHop virtual appliance:

- Ensure RPCAP is enabled on the ExtraHop virtual appliance. See the Configuring additional RPCAP settings section 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://<discover_ip_address>/admin/capture/rpcapd/linux/`. The bottom of the ExtraHop Admin UI page contains links to automatically download the software tap.

Download and install on Debian-based systems

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

1. Download the software tap on the server by running one of the following commands:

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

   Where `<extrahop_ip_address>` is the Interface 1 (management) IP address and `<extrahop_firmware_version>` is the firmware version.
2. Run the software tap on the server by running the following command:

   ```
   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: Verify the ExtraHop system is receiving traffic by running the following commands:

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

   ```
   sudo service rpcapd status
   ```
5. Optional: To change the ExtraHop IP address, port number, or arguments to the service, run the following command.

   ```
   sudo dpkg-reconfigure rpcapd
   ```

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

1. Download the software tap on the server by running on of the following commands:

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

   Where `<extrahop_ip_address>` is the IP address for interface 1 (management), and `<extrahop_firmware_version>` is the firmware version.
2. Install and run the software tap on the server by running the following command:

   ```
   sudo rpm -i rpcapd-<extrahop_firmware_version>.x86_64.rpm
   ```
3. Open and edit the `rpcapd.ini` file in a text editor by running one of the following commands:

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

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

   Example output:

   ```
   #ActiveClient = <TARGETIP>,<TARGETPORT>
   NullAuthPermit = YES
   ```

   Replace `<TARGETIP>` with the IP address of the Discover appliance, and `<TARGETPORT>` with `2003`. In addition, uncomment the line by deleting the number sign (#) at the beginning of the line.

For example:

```
ActiveClient = 10.10.10.10,2003
NullAuthPermit = YES
```

4. Start sending traffic to the ExtraHop system by running the following command:

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

5. Optional: Verify the ExtraHop system is receiving traffic by running the following command:

```
sudo service rpcapd status
```

Download and install on other Linux systems

1. Download the software tap on the server by running one of the following commands:
   - ```
     wget --no-check-certificate 'https://<extrahop_ip_address>/tools/
     rpcapd-<extrahop_firmware_version>.tar.gz'
     ```
   - ```
     curl -Ok 'https://<extrahop_ip_address>/tools/rpcapd-
     <extrahop_firmware_version>.tar.gz'
     ```

   Where `<extrahop_ip_address>` is the IP address for Interface 1 (management), and `<extrahop_firmware_version>` is the firmware version.
2. Install and run the software tap on the server by running the following commands:
   a) Extract the software tap files from the archive file:

   ```
   tar xf rpcapd-<extrahop_firmware_version>.tar.gz
   ```

   b) Change to the `rpcapd` directory:

   ```
   cd rpcapd
   ```

   c) Run the installation script:

   ```
   sudo ./install.sh <extrahop_ip> 2003
   ```
3. Optional: Verify the ExtraHop system is receiving traffic by running the following command:

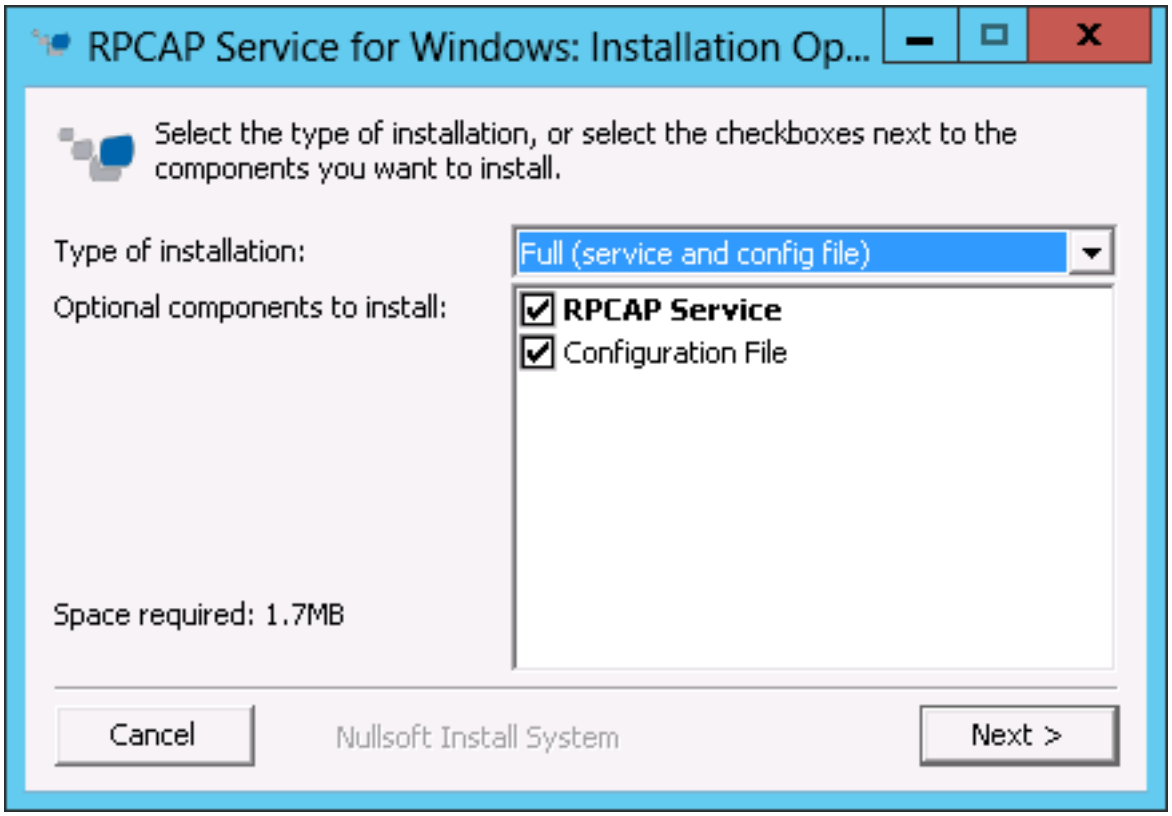
```
sudo /etc/init.d/rpcapd status
```

To run the software tap on servers with multiple interfaces, See Monitoring multiple interfaces on a Linux server.

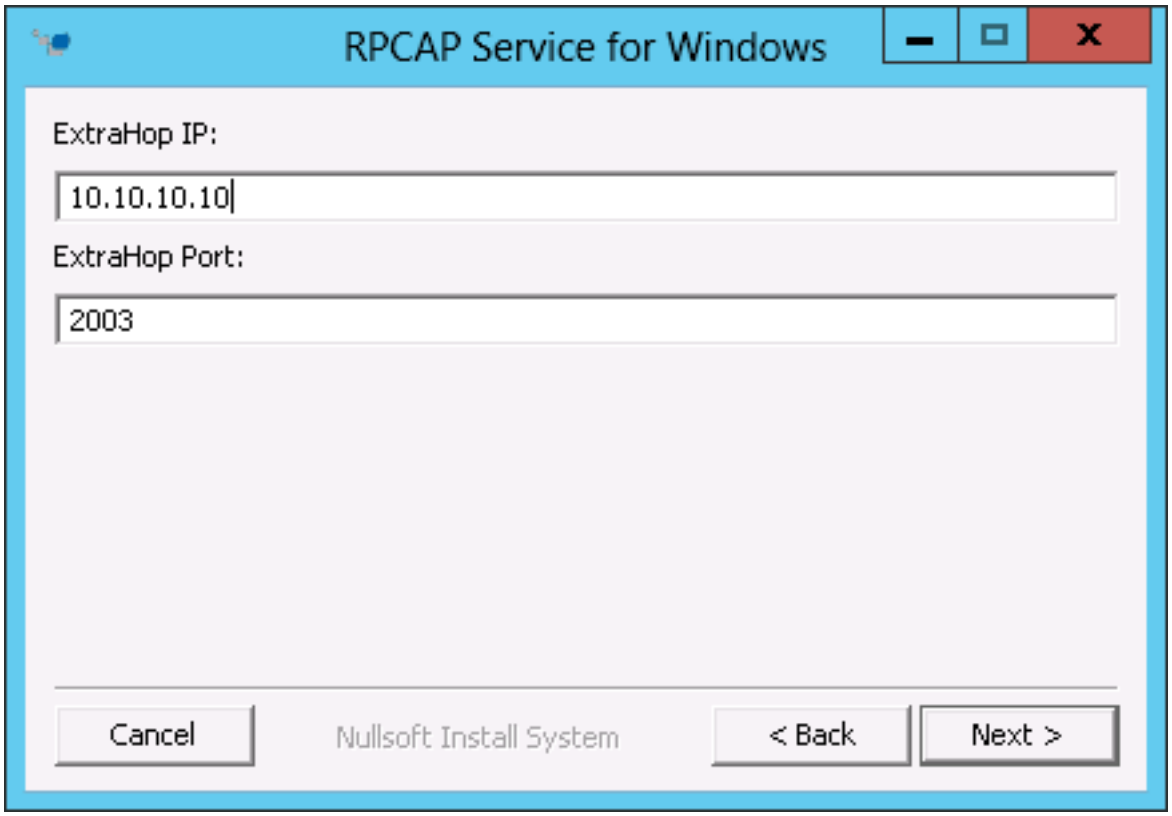
Install the software tap on a Windows server

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

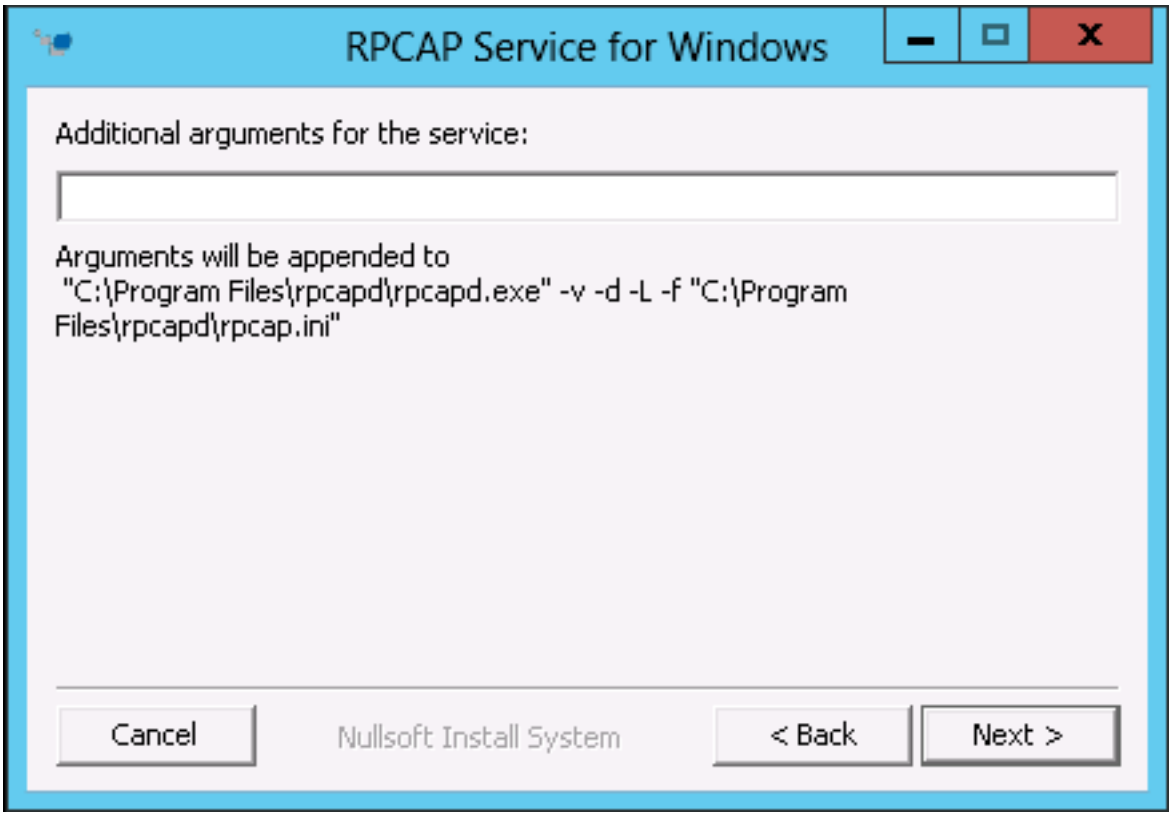
1. Go to `https://<extrahop_ip_address>/admin/capture/rpcapd/windows/` to download the RPCAP Service for Windows installer file.
2. When the file is finished downloading, double-click the file to start the installer.
3. In the wizard, select the components to install.



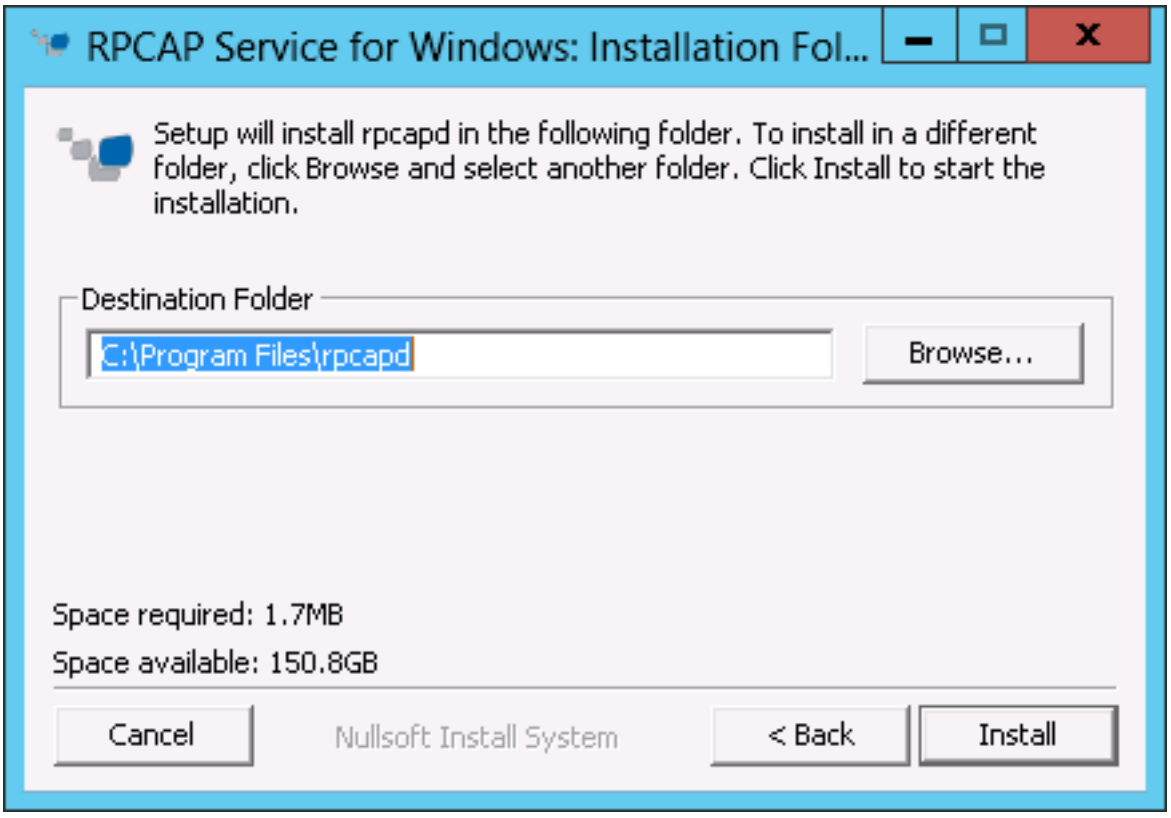
4. Complete the **ExtraHop IP** and **ExtraHop Port** fields and click **Next**. The default port is 2003.



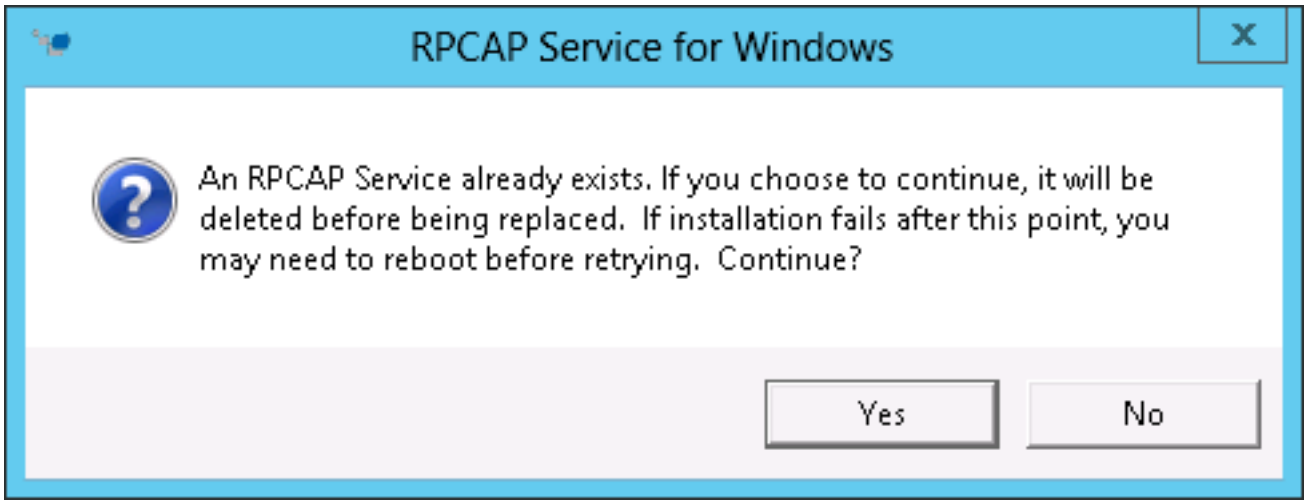
5. Optional: Enter additional arguments in the text box and click **Next**.



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



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



8. 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, `/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>
   ```

   Where *<interface_name>* is the name of the interface from which you want to forward packets, and *<interface_address>* is the IP address of the interface from which the packets are forwarded. The *<interface_address>* variable can 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 by 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 by 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.

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

   Where <*interface_address*> is the IP address of the interface from which the packets are forwarded and <*interface_address*> can 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.

   or

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

   Where <*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 with 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 with 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 with 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 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.

To specify another port, complete the following steps.

1. Go to the RPCAP Settings section and click **2003**.
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 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

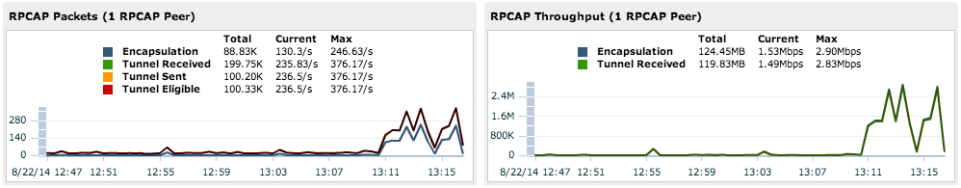
Specifies the traffic to forward using Berkeley Packet Filter syntax. For example, `TCP port 80` forwards only TCP traffic on port 80, and `not TCP port 80` forwards only non-TCP traffic on port 80.

3. Click **Save**.

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 into the ExtraHop Web UI (`https://<extrahop_ip>/extrahop`) and click the **System Settings** icon.
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

Run the following commands:

- 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.
- 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
```

- 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**.