Deploy the ExtraHop Discover Appliance in AWS

Introduction

This guide explains how to launch the ExtraHop Discover AMI to monitor your Amazon Web Services (AWS) environment. You must have administrative access to launch a third-party AMI and an ExtraHop product key to complete these procedures.

Creating the ExtraHop Instance in AWS

To create the ExtraHop instance in AWS, complete the following steps:

1. Sign in to AWS with your username and password.
2. Click **EC2**.
3. In the left navigation panel, under Images, click **AMIs**.
4. Above the table of AMIs, change the **Filter** from **Owned by Me** to **Public Images**.
5. In the filter box, type `ExtraHop` and then press enter.
6. Select the checkbox next to the appropriate ExtraHop Discover Appliance AMI and click **Launch**.
7. Select a supported instance type for the product you are installing, using the following table.

Product	**Supported Instance Types**
EH1000v	m3.large, c3.xlarge, c4.xlarge
EH2000v	m3.xlarge, c3.2xlarge, c4.2xlarge
EH6100v	c3.8xlarge, c4.8xlarge

> **Note:** C3 instance types deployed in a VPC will take advantage of Enhanced Networking capabilities. M3 instance types do not support Enhanced Networking.

8. Click **Next: Configure Instance Details**.
9. Click the **Network** drop-down list and select **Launch into EC2-Classic** or one of your organization's VPCs.

> **Note:** ExtraHop C3 instances deployed in a VPC will take advantage of advantage of Amazon's Enhanced Networking capabilities. If you launch into **EC2-Classic**, you will not get support for Enhanced Networking.

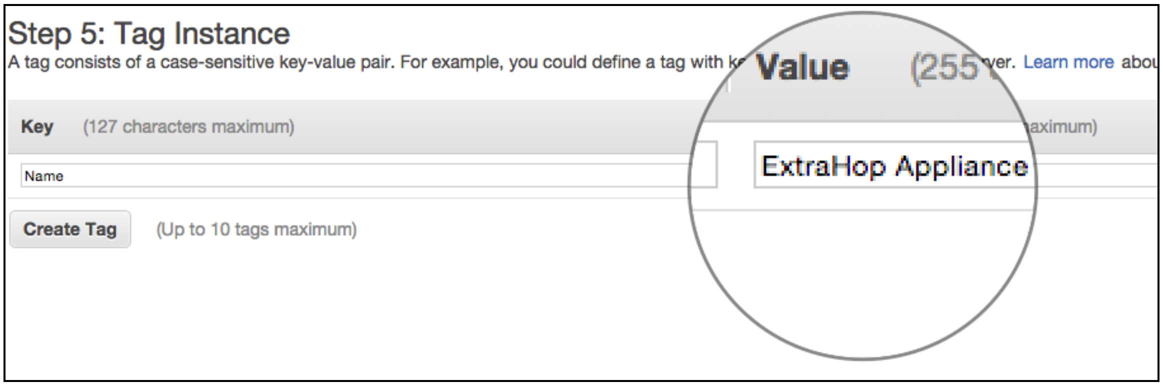
10. From the **Shutdown behavior** drop-down list, select **Stop**.
11. Click the **Protect against accidental termination** checkbox.
12. (Optional) Click the **IAM role** drop-down list and select an IAM role.
13. (Optional) If you launched into a VPC and want to use more than one interface, scroll down to the **Network Interfaces** section and click **Add Device** to add additional interfaces to the instance.

> **Note:** If you use more than one interface, make sure that each interface is on a different subnet.

14. On the **Configure Instance Details** page, click **Next: Add Storage**.

> **Note:** If you want to add a disk to enable packet capture, finish this procedure and then refer to Appendix D.

15. Accept the default storage settings and click **Next: Tag Instance**.
16. In the **Value** field, enter a name for the instance.



Step 5: Tag Instance

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with k ver. Learn more abou

Key (127 characters maximum)	Value (255 aximum)
Name	ExtraHop Appliance

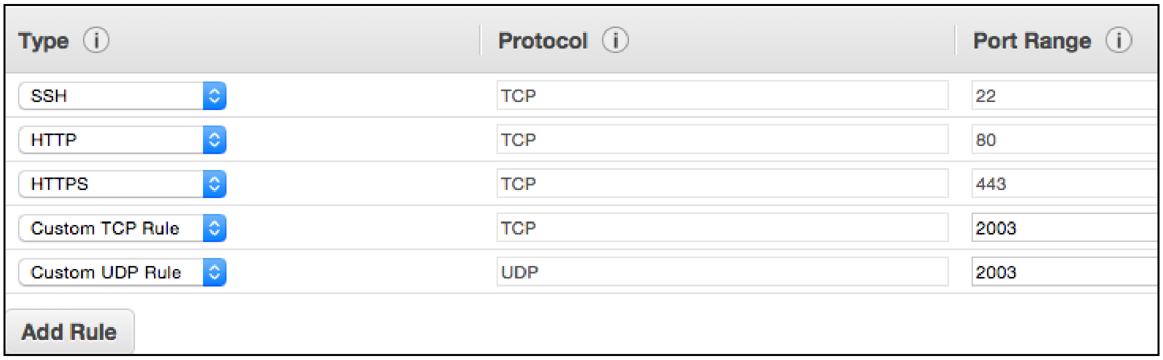
17. Click **Next: Configure Security Group**.
18. On the **Configure Security Group** page, use the procedure below and the table that follows to create a new security group or add ports to an existing group. If you already have a security group with the required ports for ExtraHop, you can skip this step.
    a. Select either **Create a *new* security group** or **Select an *existing* security group**. If you choose to edit an existing group, select the group you want to edit. If you choose to create a new group, enter a **Security group** name and **Description**.
    b. Click the **Type** drop-down list, and select a protocol type. Type the port number in the **Port Range** field.
    c. For each additional port needed, click the **Add Rule** button. Then click the **Type** drop-down list, select a protocol type, and type the port number in the **Port Range** field.

The following ports need to be open for the ExtraHop AWS instance:

- **TCP ports 22, 80, and 443 inbound to the ExtraHop system:** These ports are used to download the installer and administer the ExtraHop system. If you cannot open port 80, you can copy the installer to each instance manually. Refer to *Installing the Software Tap on a Linux Instance* or *Installing the Software Tap on a Windows Instance.*
- **TCP/UDP ports inbound to the ExtraHop system:** Depending on the ExtraHop product, you must open a port (or a range of ports) for the software tap. See the following table for the default ports required for each product. You can use alternate port numbers, but you must add them to the security group. For the best performance, keep the port ranges for each product intact.

Product	TCP/UDP ports	Range
EH1000v	2003	1
EH2000v	2003-2006	4
EH6100v	2003-2010	8

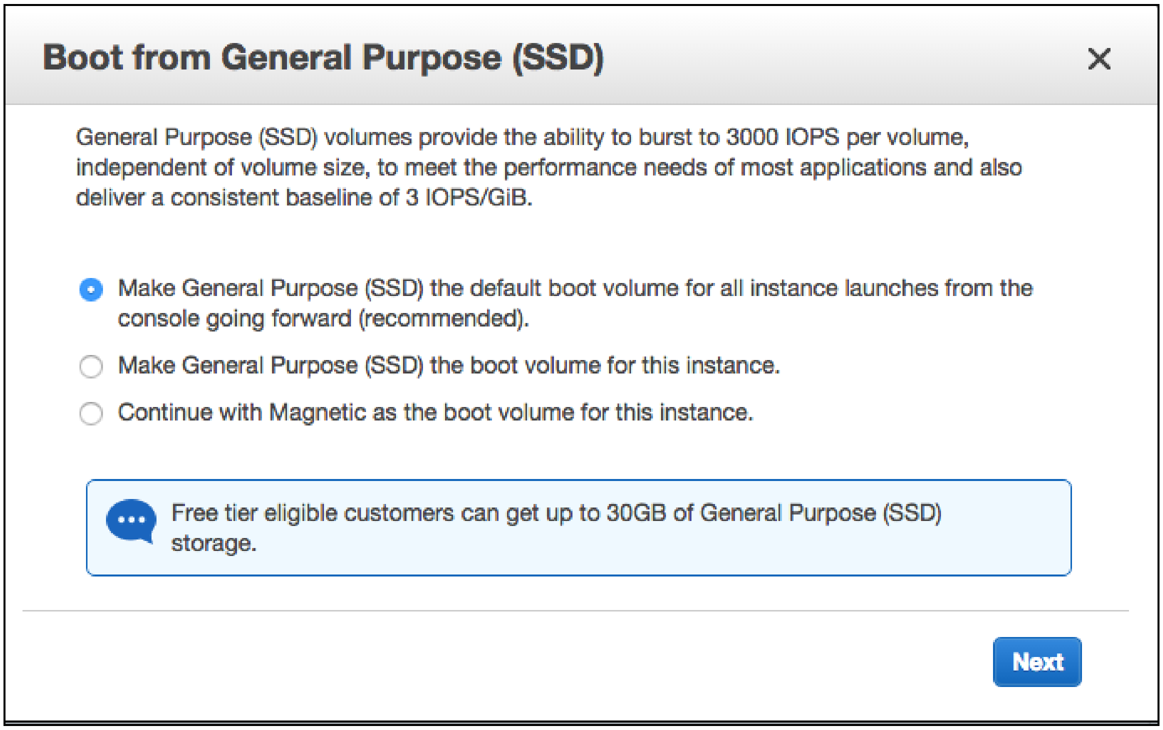
> **Note:** The image below depicts the security groups configuration for an EH1000v listening on port 2003 for UPD or TCP traffic from the software tap.



Type	Protocol	Port Range
SSH	TCP	22
HTTP	TCP	80
HTTPS	TCP	443
Custom TCP Rule	TCP	2003
Custom UDP Rule	UDP	2003

19. Click **Review and Launch**.

20. Select **Make General Purpose (SSD)** and click **Next**.



Boot from General Purpose (SSD)

General Purpose (SSD) volumes provide the ability to burst to 3000 IOPS per volume, independent of volume size, to meet the performance needs of most applications and also deliver a consistent baseline of 3 IOPS/GiB.

● Make General Purpose (SSD) the default boot volume for all instance launches from the console going forward (recommended).

○ Make General Purpose (SSD) the boot volume for this instance.

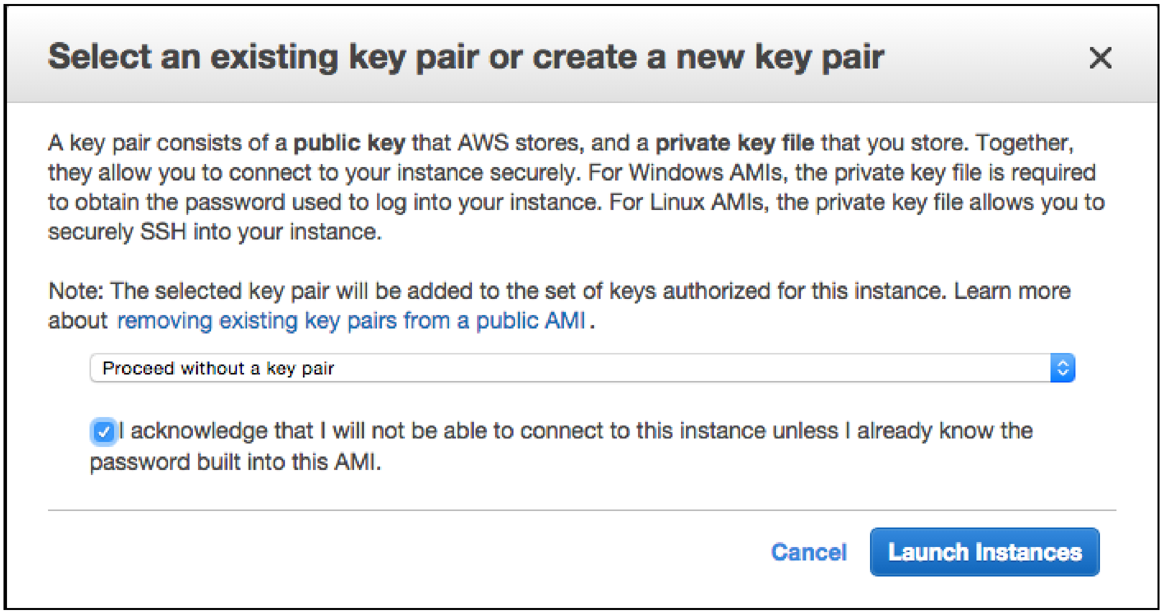
○ Continue with Magnetic as the boot volume for this instance.

Free tier eligible customers can get up to 30GB of General Purpose (SSD) storage.

> **Note:** If you select **Make General Purpose (SSD)...**, then you will not see this step on subsequent instance launches.

21. Scroll down to review the AMI details, instance type, and security group information, and then click **Launch**.
22. In the pop-up window, click the first drop-down list and select **Proceed without a key pair**.

23. Click the **I acknowledge...** checkbox and then click **Launch Instance**.



Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

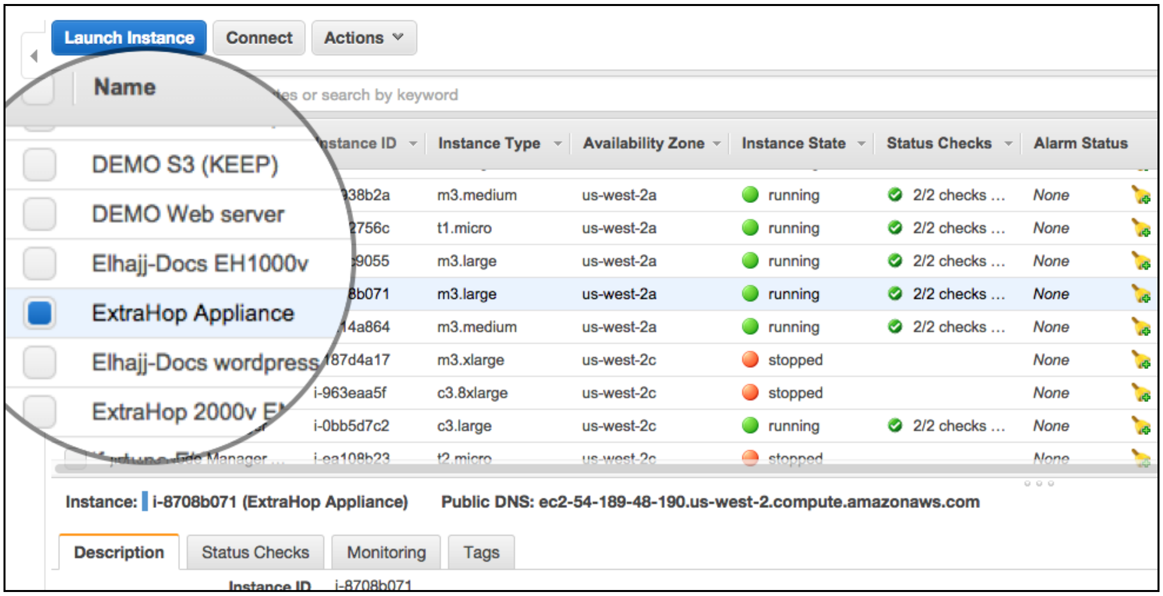
Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.

Proceed without a key pair

☑ I acknowledge that I will not be able to connect to this instance unless I already know the password built into this AMI.

24. Click **View Instances** to return to the AWS Management Console.

From the AWS Management Console, you can view your instance on the **Initializing** screen.



Name	nstance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status
DEMO S3 (KEEP)	38b2a	m3.medium	us-west-2a	● running	✓ 2/2 checks ...	None
DEMO Web server	2756c	t1.micro	us-west-2a	● running	✓ 2/2 checks ...	None
Elhajj-Docs EH1000v	9055	m3.large	us-west-2a	● running	✓ 2/2 checks ...	None
ExtraHop Appliance	8b071	m3.large	us-west-2a	● running	✓ 2/2 checks ...	None
	14a864	m3.medium	us-west-2a	● running	✓ 2/2 checks ...	None
Elhajj-Docs wordpress	187d4a17	m3.xlarge	us-west-2c	● stopped		None
ExtraHop 2000v E	i-963eaa5f	c3.8xlarge	us-west-2c	● stopped		None
	i-0bb5d7c2	c3.large	us-west-2c	● running	✓ 2/2 checks ...	None
[illegible] Manager ...	i-ea108b23	t2.micro	us-west-2c	● stopped		None

Instance: i-8708b071 (ExtraHop Appliance) Public DNS: ec2-54-189-48-190.us-west-2.compute.amazonaws.com

Instance ID i-8708b071

Under the table, on the **Description** tab, you can find an IP or hostname for the ExtraHop appliance that is accessible from your environment.

Licensing the ExtraHop System

To license the ExtraHop system, complete the following steps:

1. Once the instance has booted, browse to the ExtraHop appliance (https://<*extrahop_management_ip*>/admin).
2. Review the license agreement, select **I Agree**, and click **Submit**.
3. In the **Login** screen, enter the default user name and password:
   - For user name, type `setup`.
   - For password, type the instance ID. You can find the Instance ID on the **Description** tab of an instance selected on the Initlizing screen. Use the string of characters that follow **i-** (but not **i-** itself).
4. Click **ExtraHop Administration**.
5. Under **Manage License**, click **Register** to enter the product key.
6. Enter the product key and then click **Register**.

   The ExtraHop system will contact the license server and validate the product key. After the product key is validated, the license is downloaded.

7. Click **Done**.

The ExtraHop system is now able to receive traffic from software taps.

Monitoring Instances With RPCAP

Remote packet capture (RPCAP) forwards traffic from any server to the ExtraHop virtual appliance. RPCAP is conceptually similar to a physical network tap, but implemented in software. ExtraHop refers to this configuration as a software tap, or packet forwarder.

To monitor instances with RPCAP, you must do the following:

- Install the software tap on the instances sending traffic.
- Analyze wire data in the ExtraHop Web UI.

> **Note:** For ExtraHop AWS instances with one interface, the target and the management IP addresses are the same. All EC2-Classic instances have one interface.

Installing the Software Tap on an Instance Sending Traffic

(Linux) You must run the software tap command on each instance to be monitored in order to forward packets to the ExtraHop system.

1. In the ExtraHop Admin UI, go to the **System Configuration** section, click **Capture**, and then click **Software Tap**.
2. Go to the section that matches the Linux distribution you are running, and copy and paste the commands for installing and setting up the software into your terminal.

> **Note:** Amazon bases its Linux distributions on Red Hat. If you want to install the software tap on an Amazon distribution, follow the **RPM-Based Systems** instructions.

(Windows) You must run the software tap command on each instance to be monitored in order to forward packets to the ExtraHop system. You must have Administrator privileges on the Windows server to use this procedure.

1. In the ExtraHop Admin UI, go to the **System Configuration** section, click **Capture**, and then click **Software Tap**.

2. Click the Windows rpcapd installer to begin the download.

3. Follow the prompts to run the software tap.

Managing the Software Tap

Linux: Run the following commands to manage the software tap.

- To start, stop, restart, reload, or check the status of the software tap:

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

- To view software tap messages:

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

- To run the software tap manually for debugging purposes only:

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

  Replace `<extrahop_rpcap_target_ip>` with the IP Address of the ExtraHop appliance you want to receive this data.

  Replace `<extrahop_rpcapd_port>`with the port number the ExtraHop appliance is listening on.

  For example, if your ExtraHop appliance is at IP address 10.0.0.2, listening for packets on port 2003, you would enter: `10.0.0.2,2003`.

For information on running the software tap on servers with multiple interfaces, refer to *Appendix C.*

Windows PowerShell: Run the following commands to manage the software tap.

- To set the PowerShell execution policy back to the default:

  ```
  set-executionpolicy restricted
  ```

- To start, stop, restart, or check the status of the software tap:

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

To view software tap messages:

1. Open the Event Viewer, click **Windows Logs**, and select **Application**.
2. In the Application panel, sort by source and scroll down to rpcapd.

> **Note:** 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 software tap manually for debugging purposes only, run the following command:

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

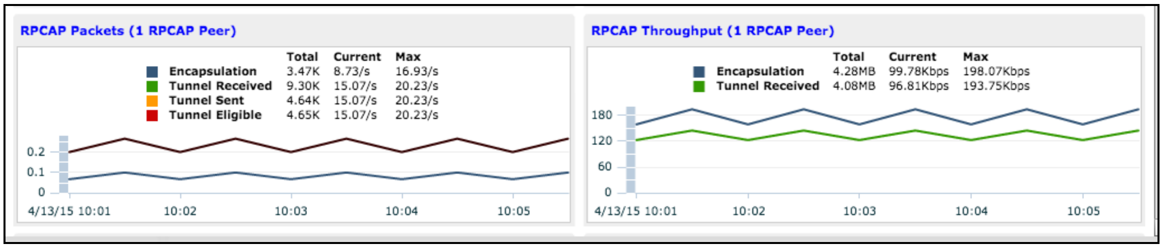
- Replace `<extrahop_rpcap_target_ip>` with the IP Address of the ExtraHop appliance you want to receive this data.
- Replace `<extrahop_rpcapd_port>`with the port number the EXtraHop appliance is listening on.
- If your ExtraHop appliance was at IP address 10.0.0.2, listening for packets on port 2003, you would enter: `10.0.0.2,2003`.

For information on running the software tap on servers with multiple interfaces, refer to *Appendix C.*

Analyzing Wire Data from a Software Tap

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

1. Log in to the ExtraHop Web UI and click the System Settings icon.
2. Click **System Health** to get more information about the forwarded data. This page displays a Packets and Throughput graph for each software tap connected to the ExtraHop system.



RPCAP Packets (1 RPCAP Peer)

	Total	Current	Max
■ Encapsulation	3.47K	8.73/s	16.93/s
🟩 Tunnel Received	9.30K	15.07/s	20.23/s
🟧 Tunnel Sent	4.64K	15.07/s	20.23/s
🟥 Tunnel Eligible	4.65K	15.07/s	20.23/s

RPCAP Throughput (1 RPCAP Peer)

	Total	Current	Max
■ Encapsulation	4.28MB	99.78Kbps	198.07Kbps
🟩 Tunnel Received	4.08MB	96.81Kbps	193.75Kbps

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.

If the ExtraHop system is receiving and processing all the packets sent by the server, then the **Tunnel Eligible**, **Tunnel Sent**, and **Tunnel Received** values are equal. If they are not, use the following guidelines for troubleshooting:

- If **Tunnel Sent** is less than **Tunnel Eligible**, the server is not able to forward out all the traffic. This might indicate that the software tap requires more processing or outbound bandwidth resources on the instance. 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 instance. This might be due to network congestion or insufficient resources on the ExtraHop system. If you suspect it is the latter, contact ExtraHop Support.

Appendix A: Configuring RPCAP Settings

By default, the ExtraHop system accepts RPCAP 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.

The default user name and password are as follows:

- User name: `setup` (for Web UI) or `shell` (for shell access)
- Password: The instance ID, which consists of the string of characters that follow **i-**.

Updating the RPCAP Configuration on the ExtraHop System

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

1. Go to the **Network Settings** section and click **Connectivity**.
2. Go to the **RPCAP Settings** section and click **Change**.
3. 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 can 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.

   > **Note:** You must specify either 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.

Updating the RPCAP Configuration on the Instance

If the instances using the software tap are not already connecting to the port configured on the ExtraHop system, you must update the port used in the software tap command on each monitored instance.

Run the following command:

```
curl --connect-timeout 10 --fail -k \
'https://<extrahop_management_ip>/tools/install-rpcapd.sh' > \
install-rpcapd.sh && sudo sh ./install-rpcapd.sh \
<extrahop_rpcap_target_ip> <extrahop_rpcapd_port>
```

Where *`<extrahop_management_ip>`* is the ExtraHop system's management IP, and *`<extrahop_rpcapd_port>`* is the port you configured on the ExtraHop system.

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

If the software tap is already running, run the following command:

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

Note: If you configure a new port, you must ensure that your AWS firewall allows inbound traffic from that port.

Appendix B: Using Additional RPCAP Installation Commands

Linux

To download the software tap manually, complete the following steps.

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

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

Windows

To download the software tap manually, complete the following steps.

1. Go to https://<*extrahop_management_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_rpcap_target_ip> -RpcapPort
<extrahop_rpcapd_port>
```

Appendix C: Monitoring Multiple Interfaces

For servers with multiple interfaces, the software tap 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 software tap, open the configuration file on the instance: `/opt/extrahop/etc/rpcapd.ini`

   After installation, the configuration file contains text similar to the following:

   ```
   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_management_ip>, <extrahop_rpcapd_port>, ifname=<interface_name>
   ```

   or

   ```
   ActiveClient = <extrahop_management_ip>, <extrahop_rpcapd_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>` might 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. Run the following command to save the configuration file and restart the software tap:

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

   To reinstall the software tap after changing the configuration file, run the installation command and replace `<extrahop_management_ip>` and `<extrahop_rpcapd_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 software tap, open the configuration file on the instance: `C:\Program Files\rpcapd\rpcapd.ini`

   After installation, the file contains this text similar to the following:

   ```
   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_management_ip>, <extrahop_rpcapd_port>, ifname=<interface_address>
   ```

   or

   ```
   ActiveClient = <extrahop_management)ip>, <extrahop_rpcapd_port>, ifaddr=<interface_name>
   ```

   `<interface_address>` specifies the IP address of the interface from which the packets are forwarded. `<interface_address>` might 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 file and restart the software tap by running the `restart-service rpcapd` command.

   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_management_ip> -KeepConfig
   ```

   or

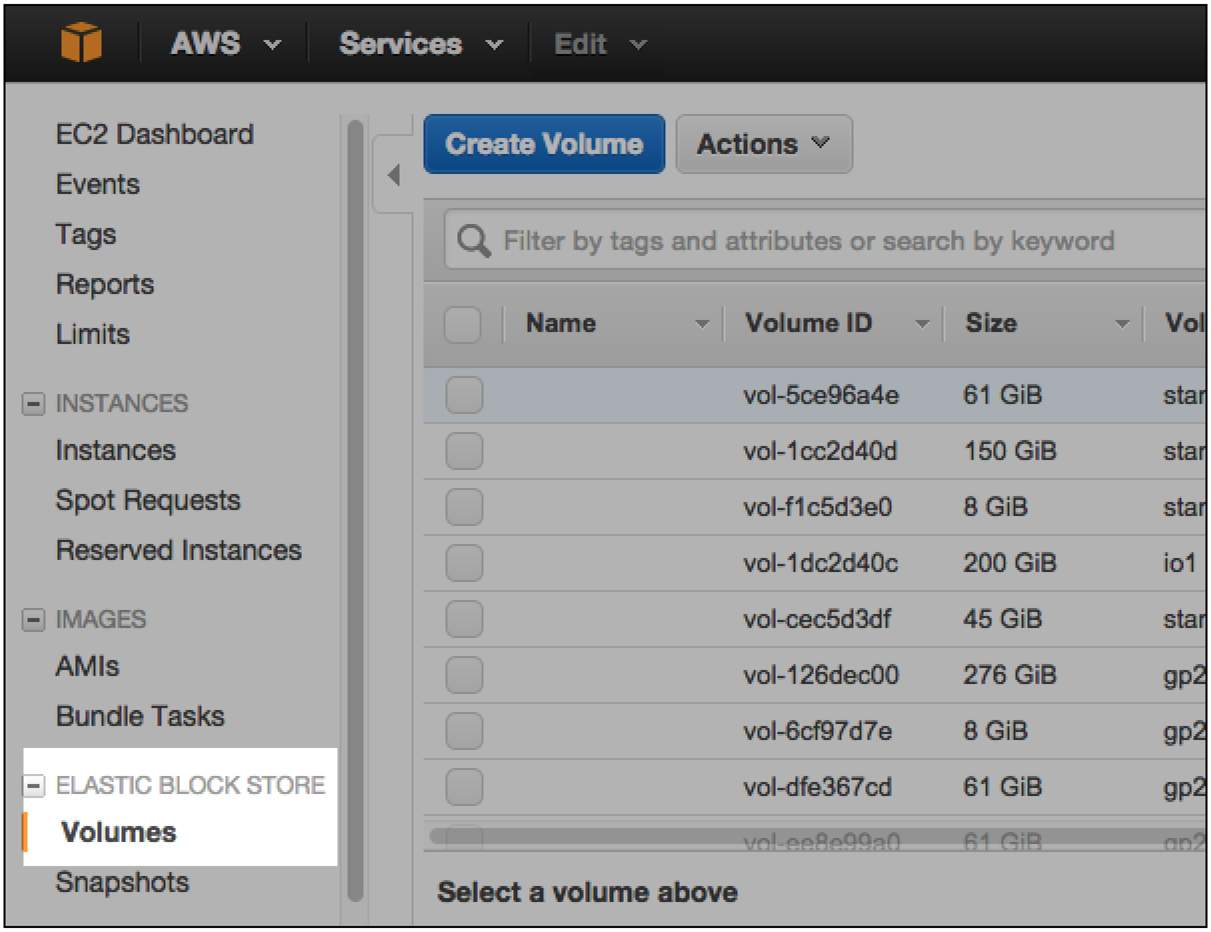
   ```
   .\install-rpcapd.ps1 -InputDir . -KeepConfig
   ```

Appendix D: Installing a Disk for Packet Capture

With ExtraHop firmware version 4.1 and later, you can run packet capture with your ExtraHop system deployed with AWS.

To run packet capture with the ExtraHop system, complete the following steps:

1. In the ExtraHop Admin UI, go to the System Settings section and click **License**. Go to the Features section and verify that **Packet Capture** is set to **Enabled**.
2. Go to the System Settings section and click **Shutdown/Restart**.
3. In the System section, click **Shutdown**.
4. Click **Halt**.
5. Click **Done**.
6. In the left panel of the AWS console, go to the Elastic Block Store section and click **Volumes**.

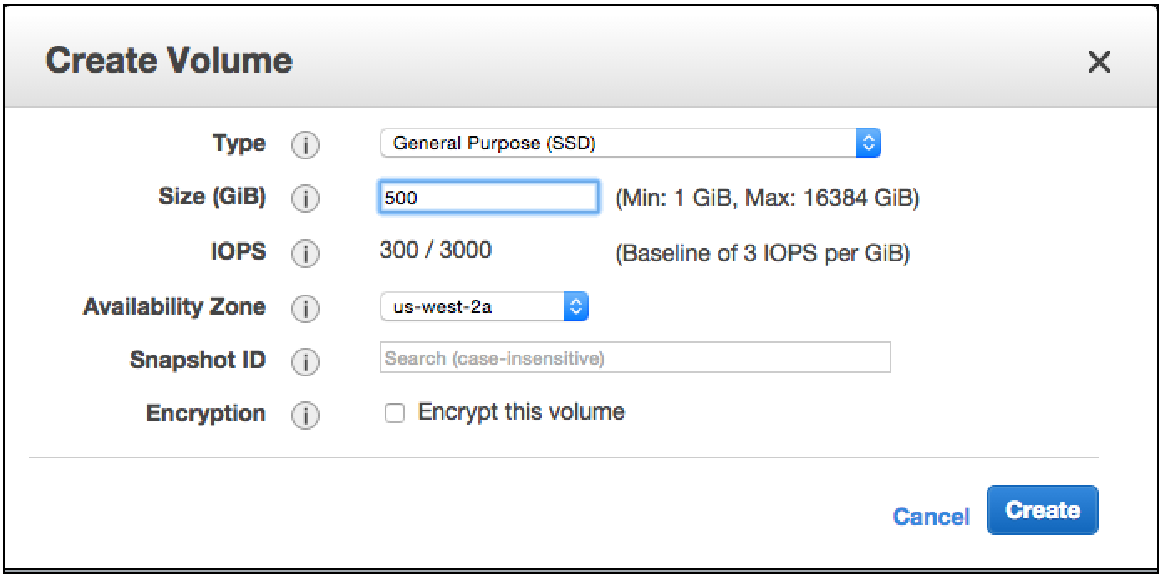


Name	Volume ID	Size	Vol
	vol-5ce96a4e	61 GiB	star
	vol-1cc2d40d	150 GiB	star
	vol-f1c5d3e0	8 GiB	star
	vol-1dc2d40c	200 GiB	io1
	vol-cec5d3df	45 GiB	star
	vol-126dec00	276 GiB	gp2
	vol-6cf97d7e	8 GiB	gp2
	vol-dfe367cd	61 GiB	gp2
	vol-ee8e99a0	61 GiB	gp2

Select a volume above

7. Click the **Create Volume** button.

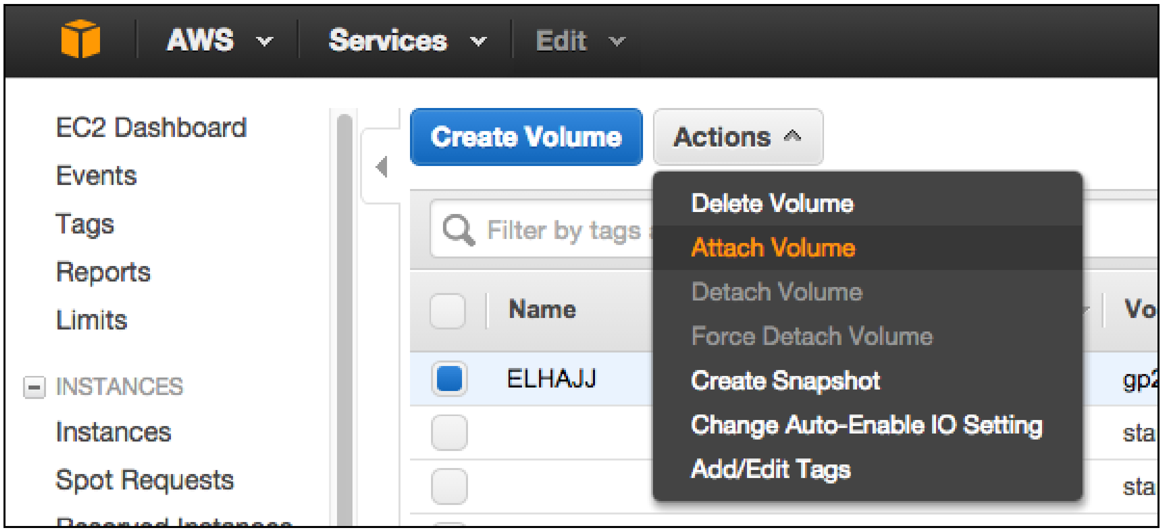
8. Select a size up to 500 G.



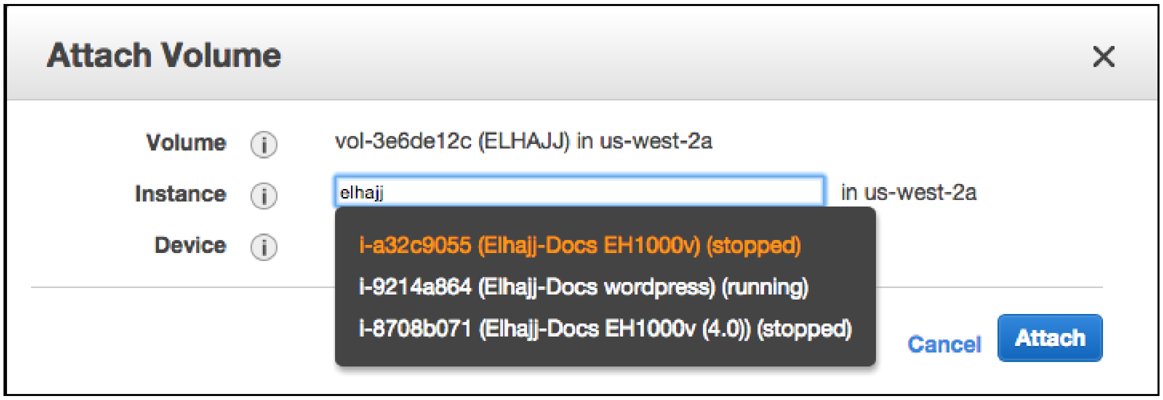
Create Volume

Type	General Purpose (SSD)
Size (GiB)	500 (Min: 1 GiB, Max: 16384 GiB)
IOPS	300 / 3000 (Baseline of 3 IOPS per GiB)
Availability Zone	us-west-2a
Snapshot ID	Search (case-insensitive)
Encryption	□ Encrypt this volume

9. Select an availability zone. Ensure the volume is in the same availability zone as the AWS instance.
10. Leave **Snapshot ID** blank.
11. Click **Create**.
12. Your volume appears in the list. Select the volume.
13. Click **Actions** and select **Attach Volume**.



14. In the Attach Volume pop-up window, click the **Instance** field and search for your instance.



Attach Volume

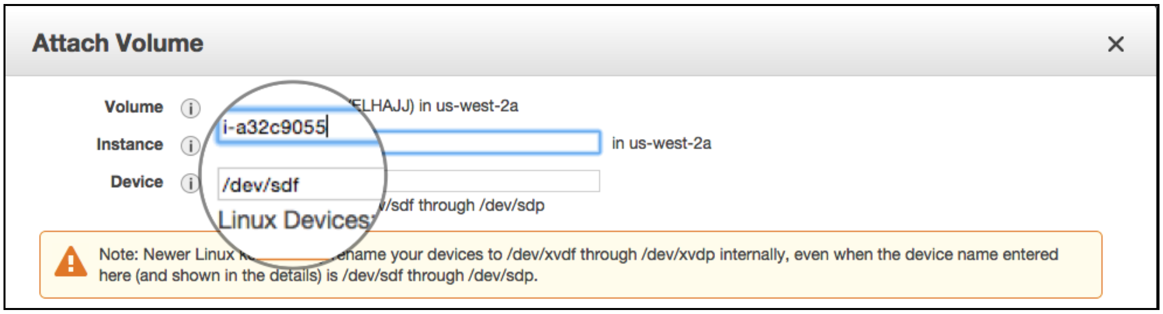
Volume: vol-3e6de12c (ELHAJJ) in us-west-2a

Instance: elhajj in us-west-2a

Device

i-a32c9055 (Elhajj-Docs EH1000v) (stopped)
i-9214a864 (Elhajj-Docs wordpress) (running)
i-8708b071 (Elhajj-Docs EH1000v (4.0)) (stopped)
Cancel
Attach

15. The **Device** field populates with the file system location where the volume will be mounted.



Attach Volume

Volume: (ELHAJJ) in us-west-2a

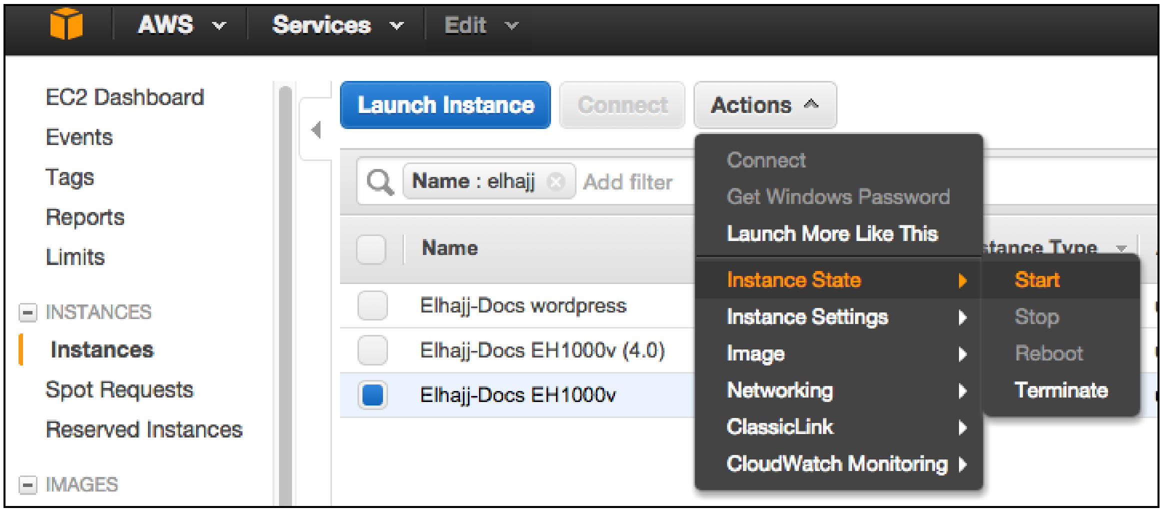
Instance: i-a32c9055 in us-west-2a

Device: /dev/sdf

Linux Devices: /dev/sdf through /dev/sdp

Note: Newer Linux k… rename your devices to /dev/xvdf through /dev/xvdp internally, even when the device name entered here (and shown in the details) is /dev/sdf through /dev/sdp.

16. Click **Attach**.
17. In the left panel, click **Instances** and then select your instance.
18. From the **Action** button, point to **Instance State** and then click **Start**.



Note: The public IP might change when you relaunch an instance.

19. You are prompted to confirm you want to start the instance. Click **Yes, Start**.
20. In the ExtraHop Admin UI, go to the **System Settings** section and click **Disk** to ensure Disk #1 has the role, **Packet Capture**.