Packet Capture on the EH1000v/2000v with VMware

This guide describes how to use packet capture on the EH1000v/2000v virtual appliances with VMware. The guide assumes experience administering VMware ESX and ESXi environments. Users must have access to the ExtraHop Admin UI and write permission to the ExtraHop Web UI in order to complete the steps in this guide.

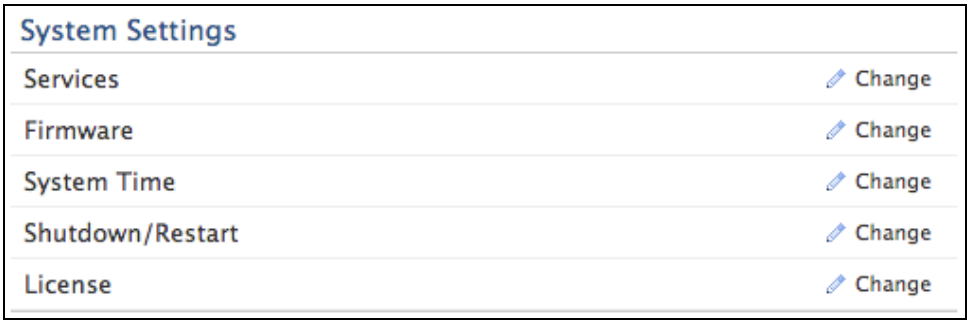
Best practices:

- Use a storage partition on a local machine.
- Use a minimum disk size of 1 GB

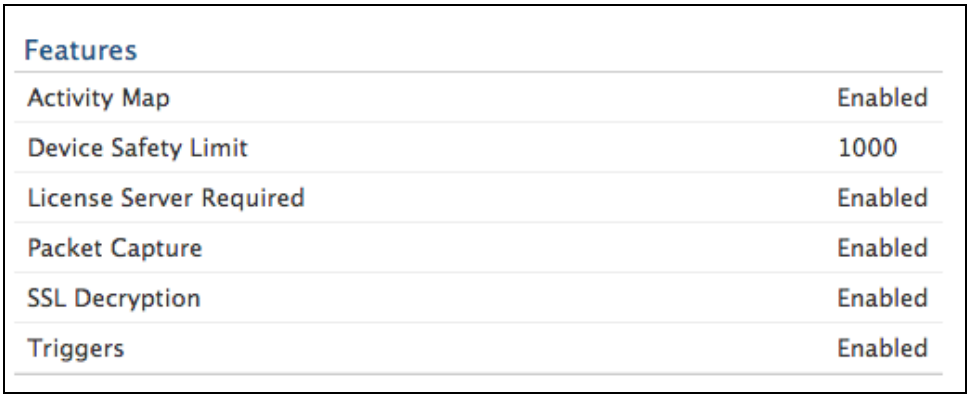
Enabling Packet Capture

Ensure that your ExtraHop license has packet capture enabled.

1. In the Admin UI, go to **System Settings** and click **License**.



2. Go to the**Features** section and verify that packet capture is enabled. If packet capture is enabled, go to the next section. If your license does not have packet capture enabled, go to the next step.



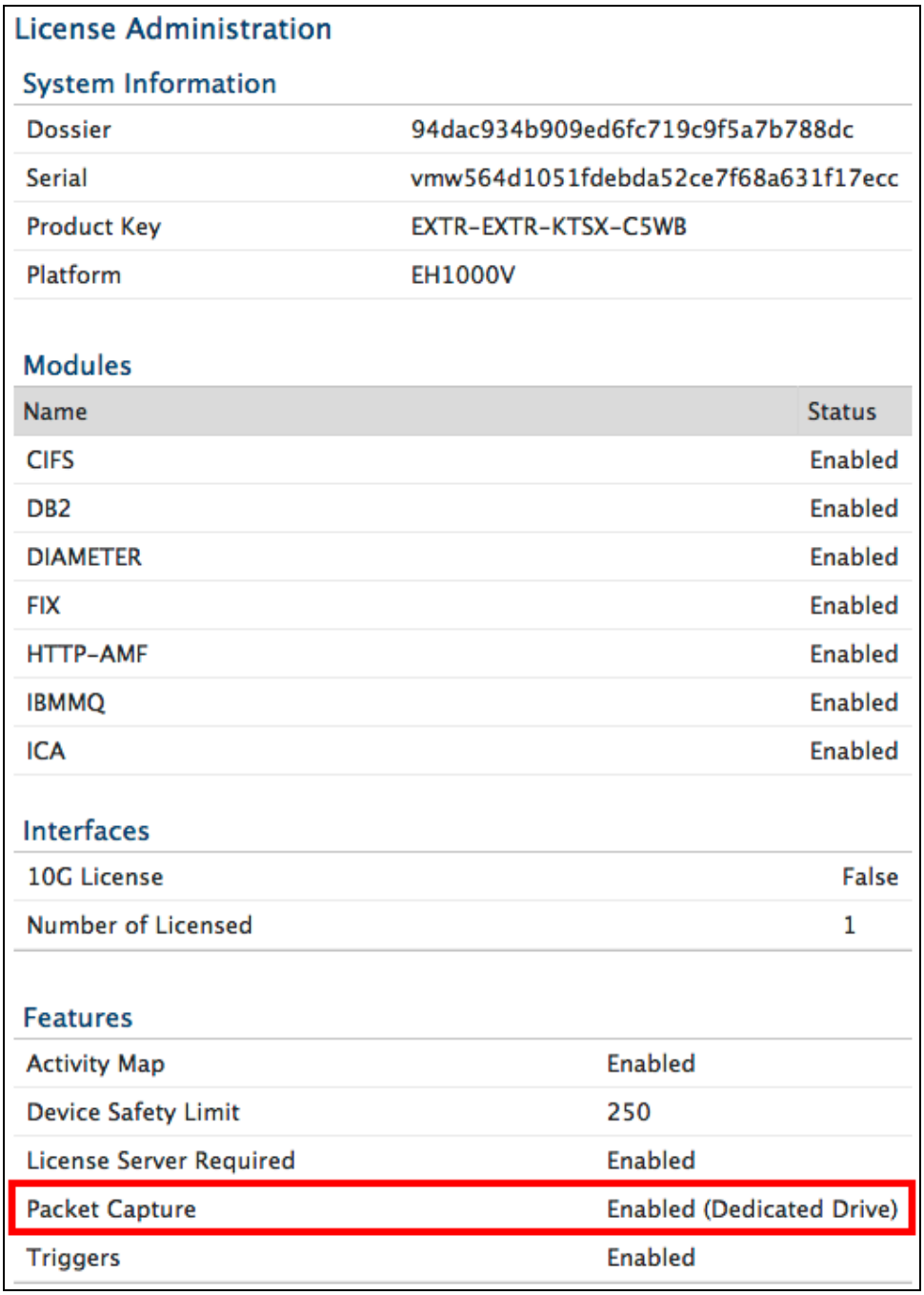
3. The ExtraHop requires a product key and a license in order to use packet capture. Contact ExtraHop Support (support@extrahop.com) to obtain your product key.

a. Go to **Manage License** and click **Register** to enter the product key.

b. 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.

c. Refresh your browser to see the updated license.

The following example shows a properly licensed ExtraHop with packet capture on the **License Administration** page of the Admin UI:



License Administration

System Information

Dossier	94dac934b909ed6fc719c9f5a7b788dc
Serial	vmw564d1051fdebda52ce7f68a631f17ecc
Product Key	EXTR-EXTR-KTSX-C5WB
Platform	EH1000V

Modules

Name	Status
CIFS	Enabled
DB2	Enabled
DIAMETER	Enabled
FIX	Enabled
HTTP-AMF	Enabled
IBMMQ	Enabled
ICA	Enabled

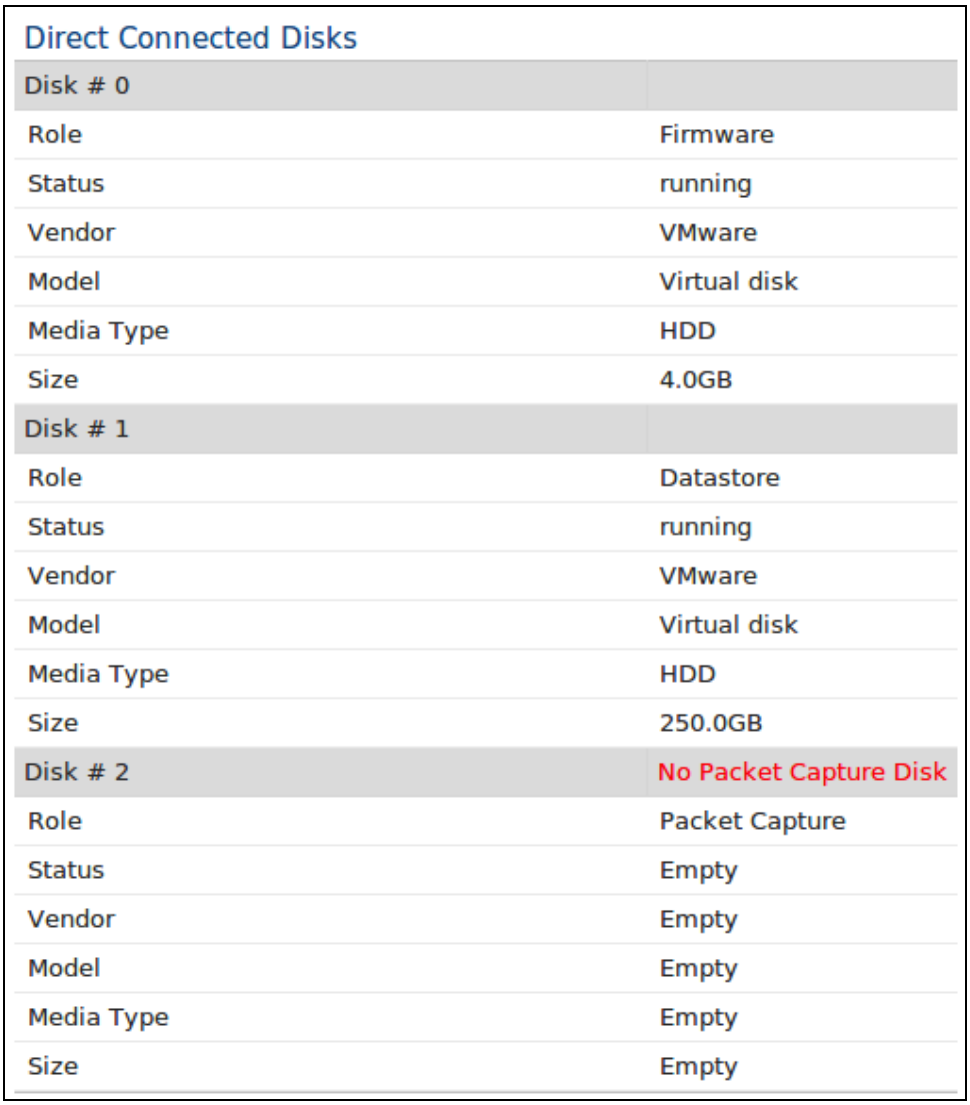
Interfaces

10G License	False
Number of Licensed	1

Features

Activity Map	Enabled
Device Safety Limit	250
License Server Required	Enabled
Packet Capture	Enabled (Dedicated Drive)
Triggers	Enabled

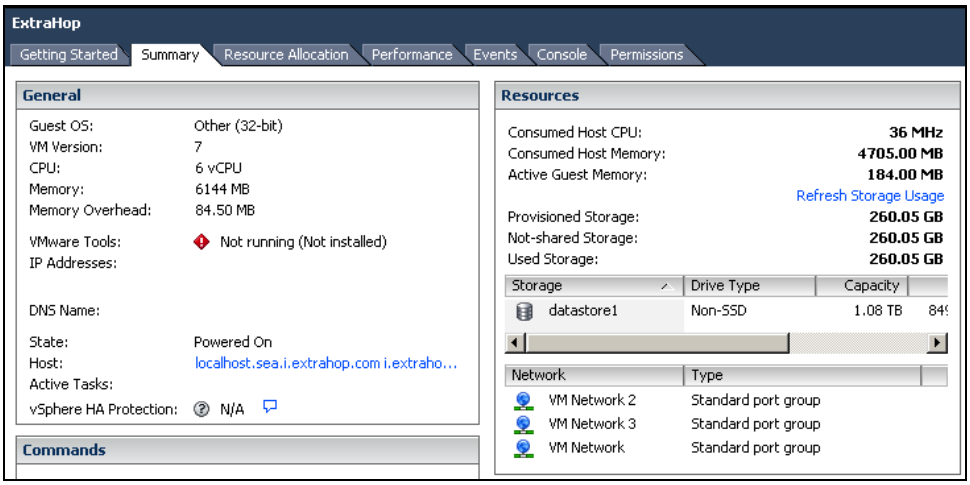
4. In the Admin UI, go to **System Settings** and click **Disk**. The Drive Map shows the **No Packet Capture Disk** message.



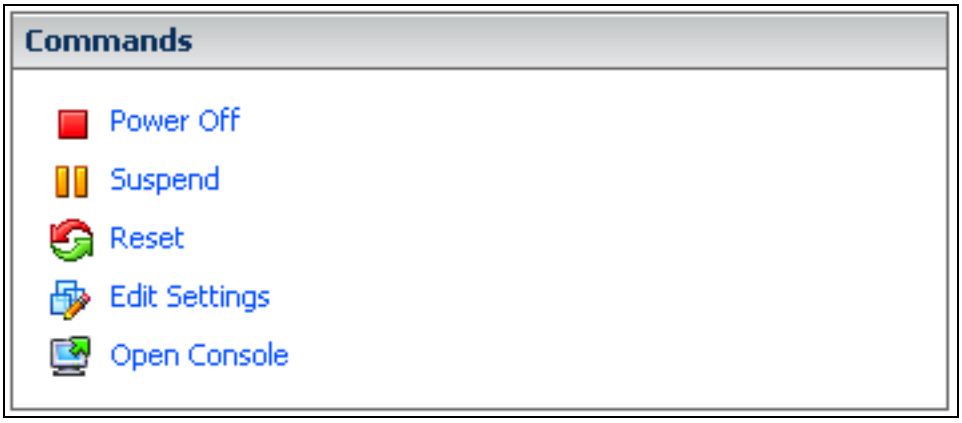
Direct Connected Disks

Disk # 0	
Role	Firmware
Status	running
Vendor	VMware
Model	Virtual disk
Media Type	HDD
Size	4.0GB
Disk # 1	
Role	Datastore
Status	running
Vendor	VMware
Model	Virtual disk
Media Type	HDD
Size	250.0GB
Disk # 2	No Packet Capture Disk
Role	Packet Capture
Status	Empty
Vendor	Empty
Model	Empty
Media Type	Empty
Size	Empty

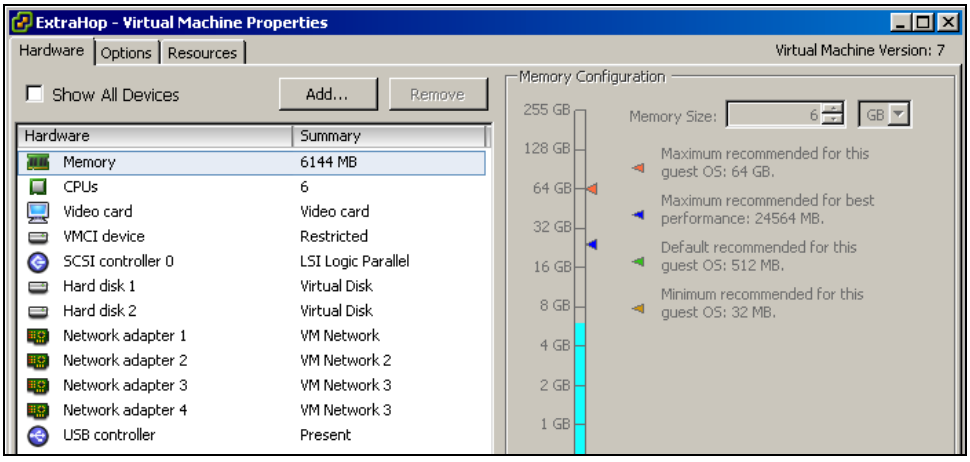
5. Log in to VMware and click the **Summary** tab.



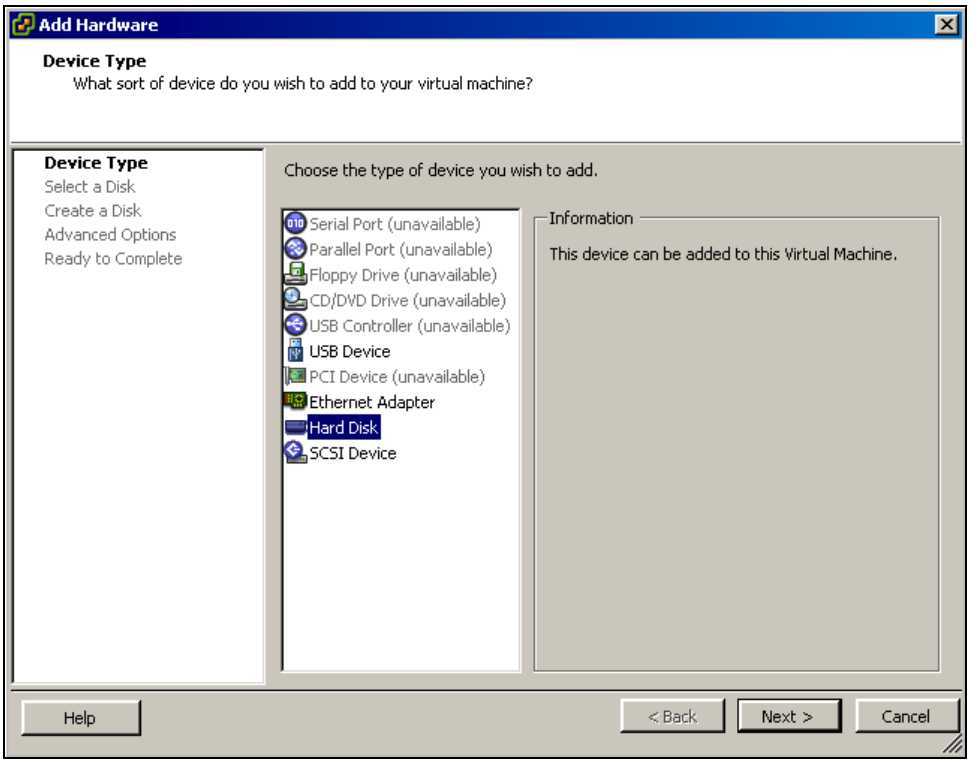
6. Click **Edit Settings**.



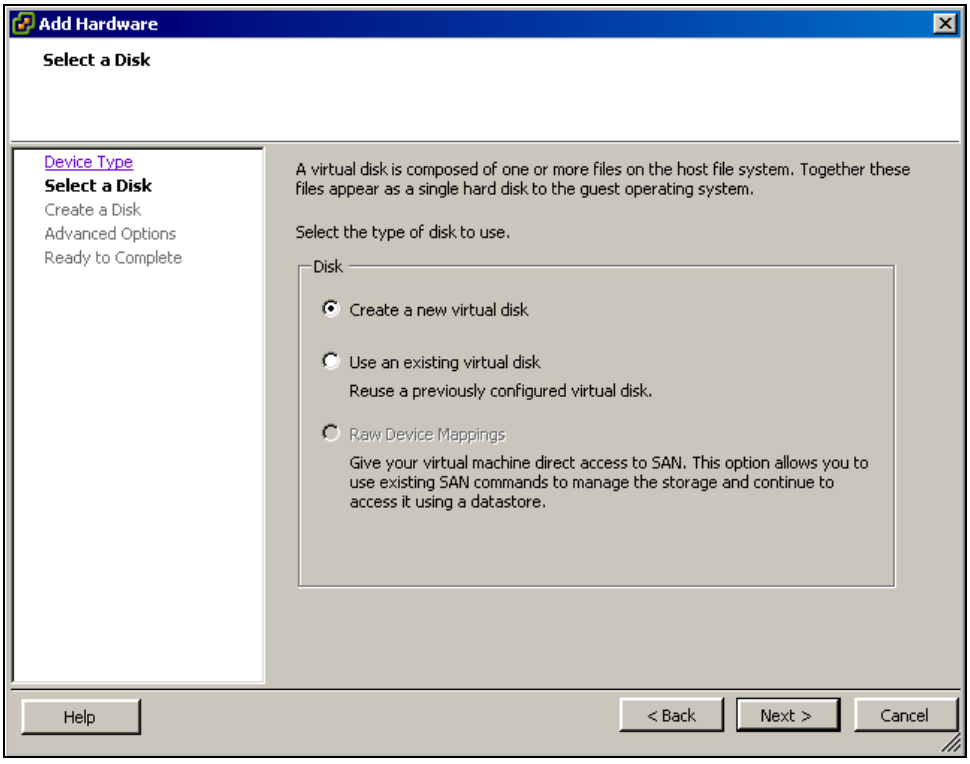
7. Click **Add**.



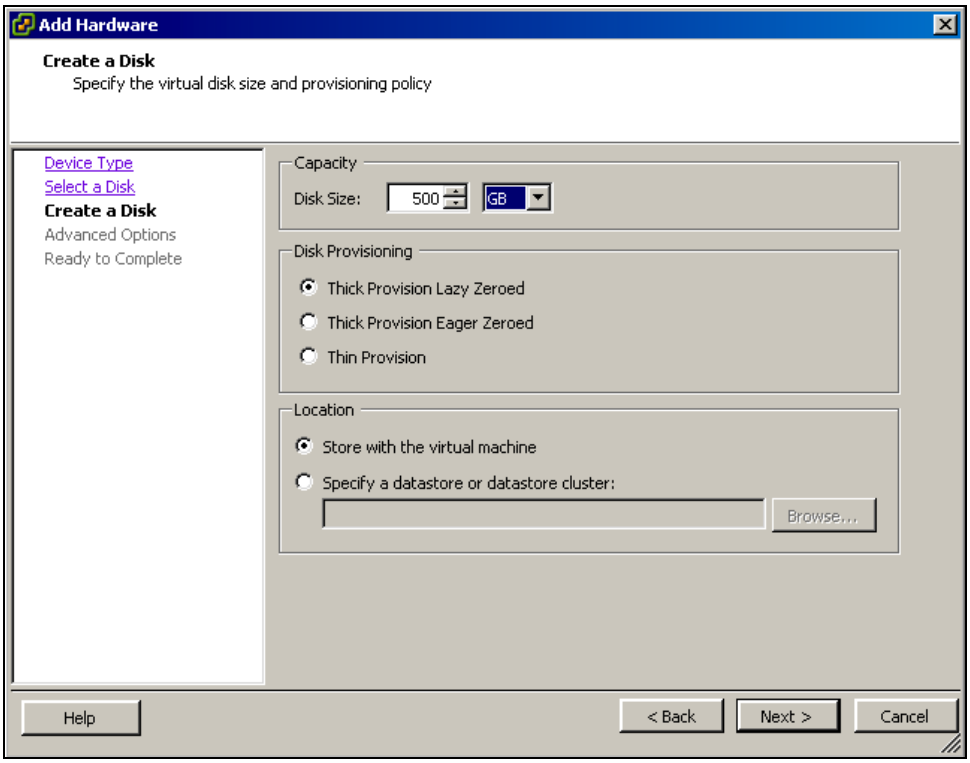
8. Select **Hard Disk** and click **Next**.



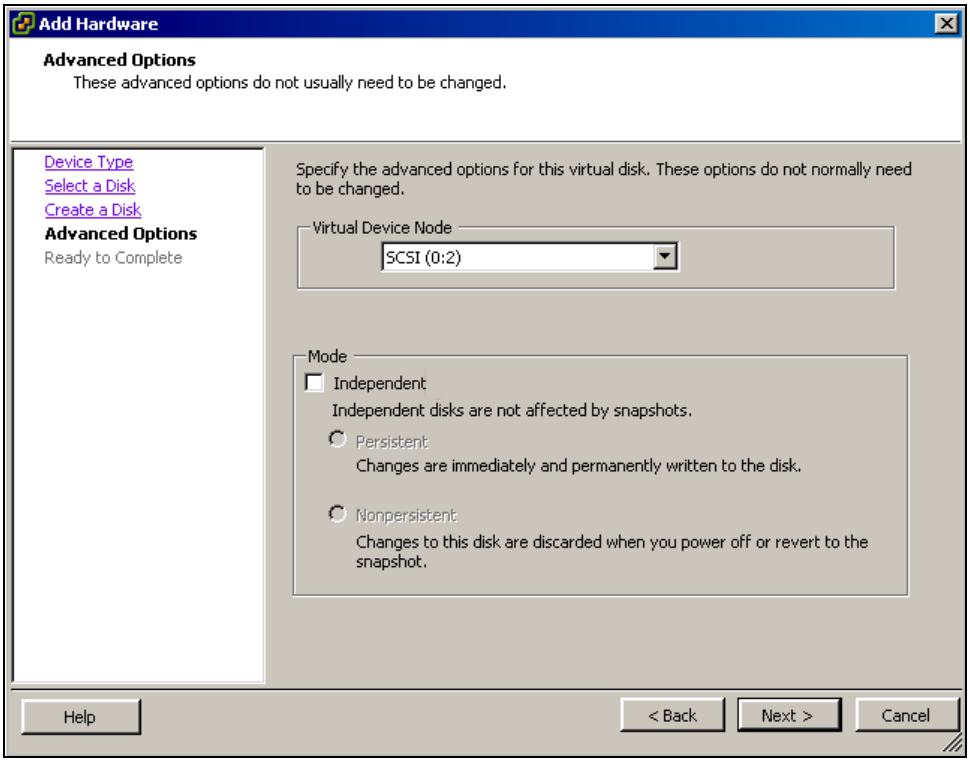
9. Select the **Create a new virtual disk** radio button and click **Next**.



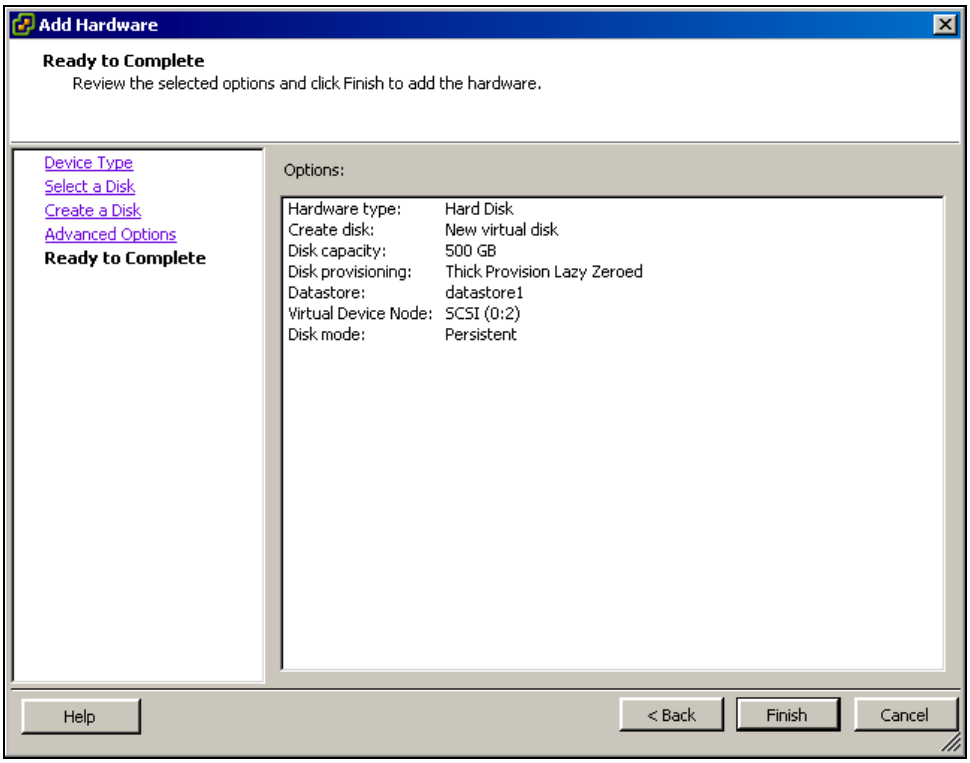
10. Set the **Disk Size** to 500 GB, select the **Thick Provision Lazy Zero** radio button and click **Next**.



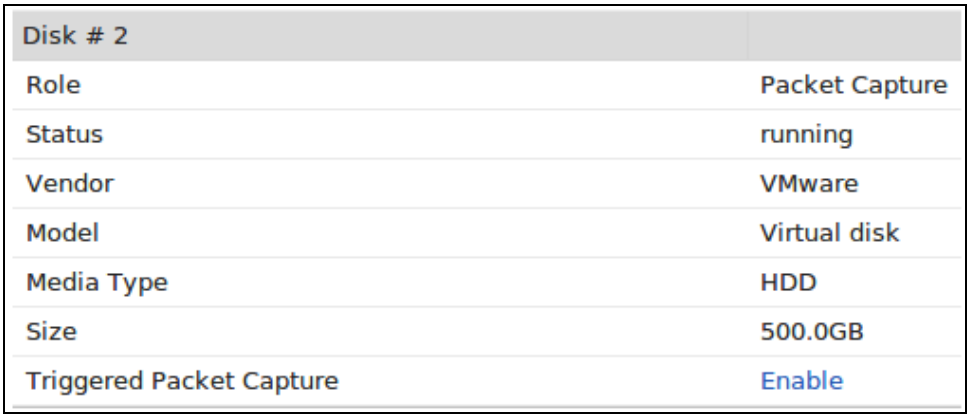
11. In the **Advanced Options** window, use the default settings and click **Next**.



12. Click **Finish**.



13. Click **OK**.
14. Refresh the Admin UI. The drive is now allotted for packet capture.
15. Next to **Triggered Packet Capture**, click **Enable**.



16. Wait approximately 10 minutes. When the progress indicator disappears, your VM is ready to use packet capture.

Using Triggers to Define the Packet Capture

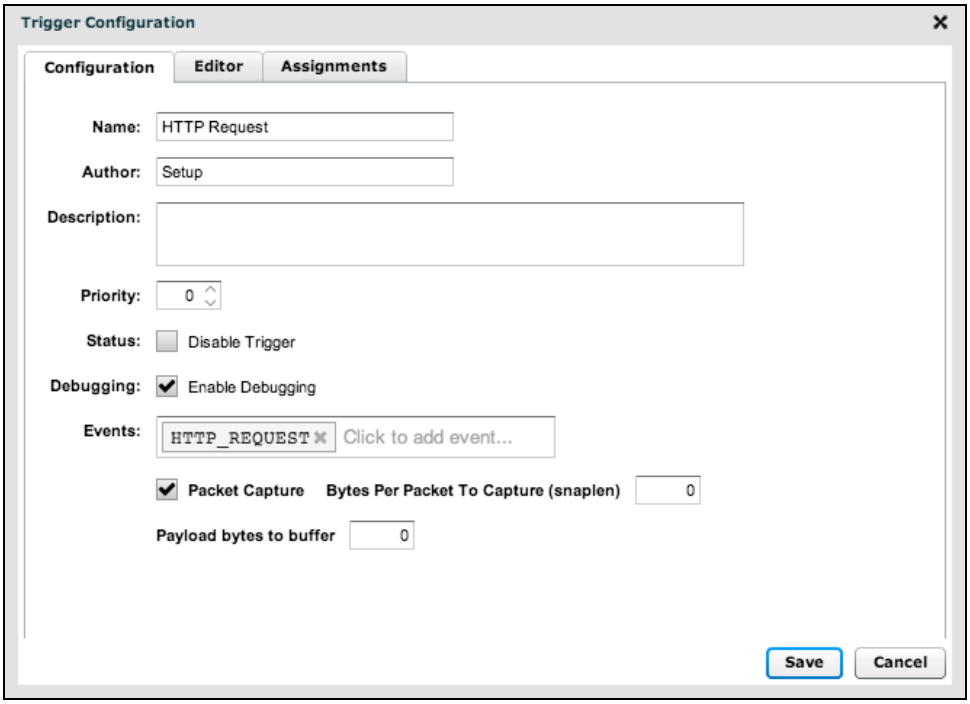
The ExtraHop system uses Application Inspection Triggers to gather custom metrics. These metrics are stored internally and can be used by other features, such as packet capture. Triggers are user-defined scripts that perform additional actions during well-defined events.

For information about writing triggers, refer to the following related documentation:

- *ExtraHop Guide: Getting Started with Application Inspection Triggers*.
- *ExtraHop Application Inspection Triggers API*

To create a trigger, complete the following steps:

1. In the Web UI, click **Settings**, click **Triggers**,and then click **New**.
2. Enter a name for the trigger, select the event that will activate the trigger, and click the **Packet Capture** checkbox.

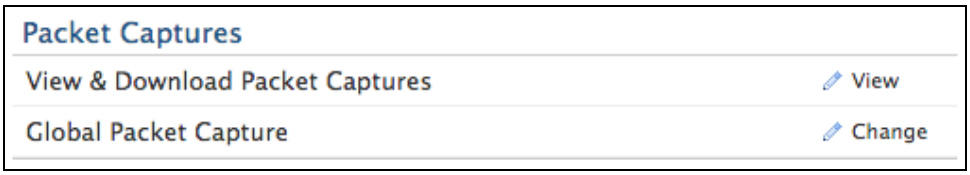


> Once you have tested the trigger to ensure it works, uncheck **Enable Debugging** to avoid excessive debug messages in the Runtime Log.

3. Click the **Editor** tab, enter your trigger source code, and click **Save**.
4. Click the **Assignments** tab and assign the trigger to a device or group of devices.

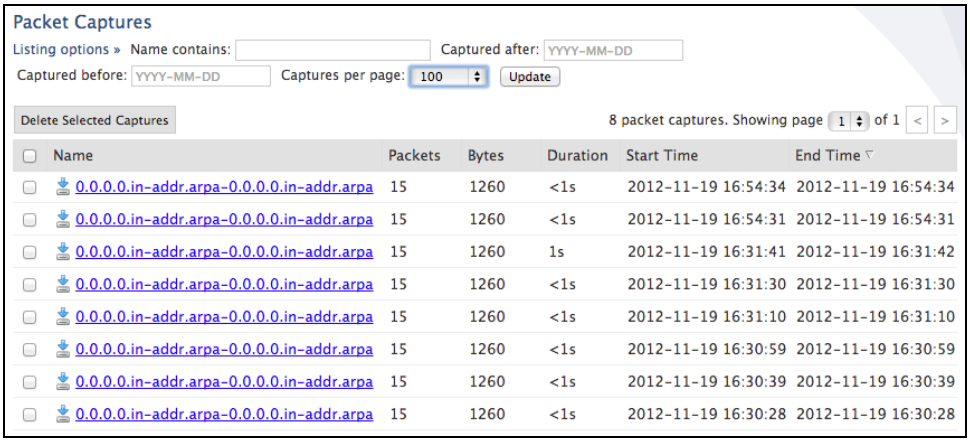
Viewing the Packet Capture Results

1. In the Admin UI, go to the **Packet Captures** section and click **View & Download Packet Captures**.



2. On the **Packet Captures** page, select a packet capture to download to your workstation. You can filter

packet captures by name and the date of capture.



3. Open the downloaded packet capture in a packet analyzer such as Wireshark.