ExtraHop Standard Management Pack for VROPS User Guide

Rev 8/18/2016

1 Overview

The ExtraHop Standard Management Pack for vRealize Operations Management (VROPS) provides visibility into a wealth of wire data analytics through the ExtraHop platform. With ExtraHop, metrics associated with more than 50 protocols from L2 to L7 are available. The metrics provided by ExtraHop are available for use in your own custom VROPS dashboards, reports, and alerts. The management pack provides 5 default dashboards and 26 views based on metrics from the ExtraHop platform.

2 Installation

2.1 Requirements

The ExtraHop Standard Management Pack for VROPS requires an installation of VMware's vRealize Operation Manager 6.2 or higher and an ExtraHop Discover appliance running version 5.3 or later.

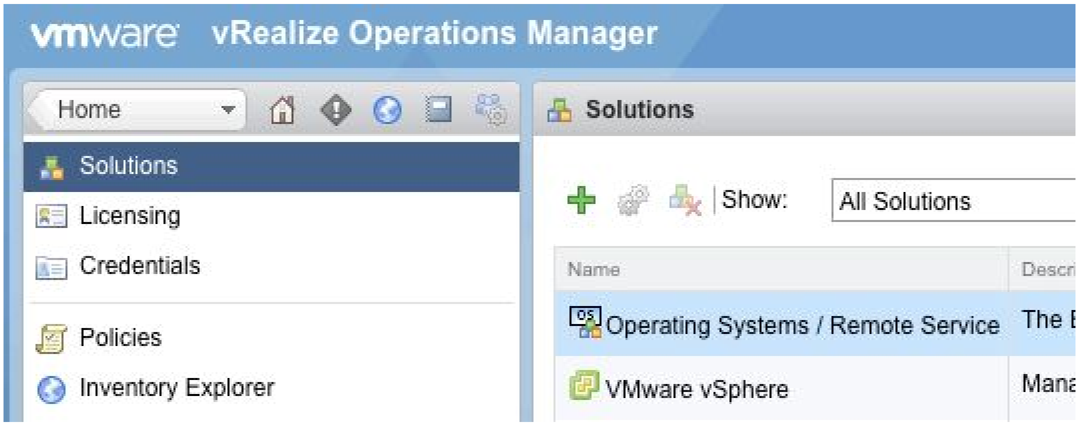
2.2 Obtain the ExtraHop Standard Management Pack for VROPS

The ExtraHop Standard Management Pack for VROPS is a .pak archive that can be downloaded from the link in your welcome email.

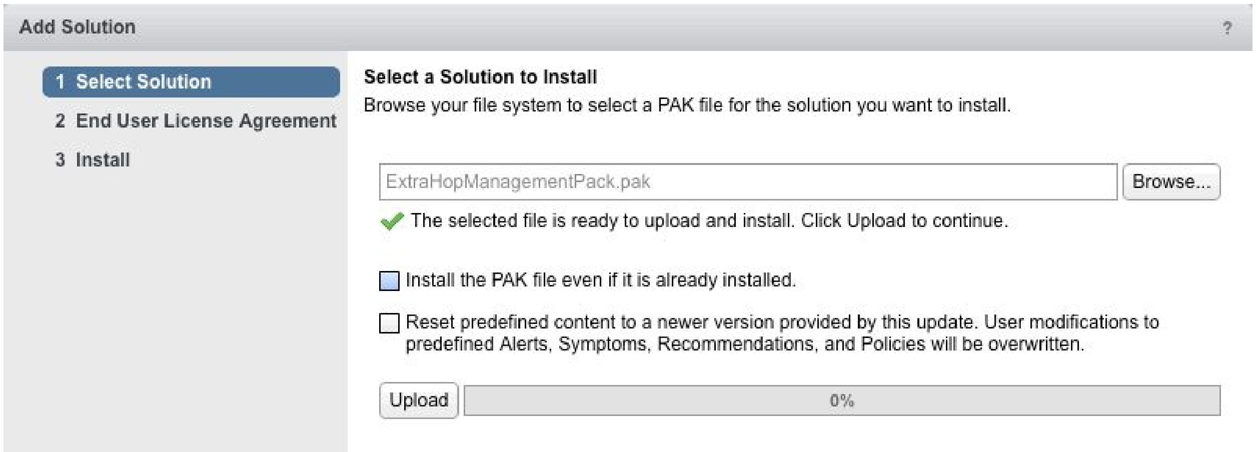
2.3 Install the ExtraHop Standard Management Pack for VROPS

After you download the management pack, complete the following steps to install the .pak file.

1. Log into the vRealize Operation Manager UI.
2. Click on **Administration**.
3. Click on **Solutions**.



4. Click the **+** symbol to begin installation of the management pack.
5. Browse to the management pack location.
6. Click **Upload** to upload the management pack.



Select a Solution to Install

Browse your file system to select a PAK file for the solution you want to install.

ExtraHopManagementPack.pak

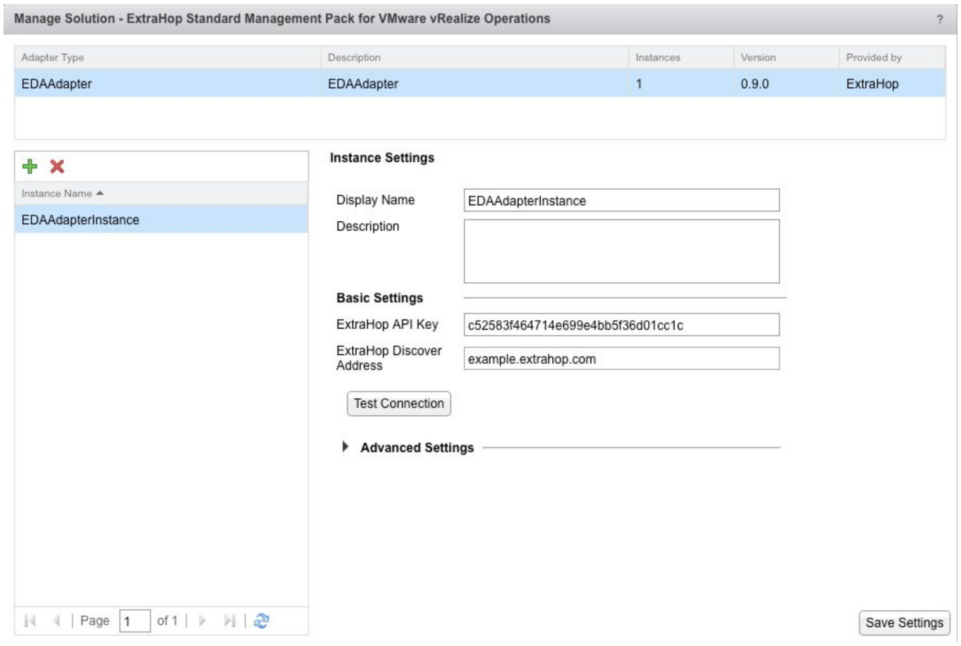
✓ The selected file is ready to upload and install. Click Upload to continue.

☐ Install the PAK file even if it is already installed.

☐ Reset predefined content to a newer version provided by this update. User modifications to predefined Alerts, Symptoms, Recommendations, and Policies will be overwritten.

0%

7. After the upload is complete, click **Next**.
8. Accept the ExtraHop EULA and then click **Next** to begin the installation.
9. When the installation is complete, select the configure icon to configure the adapter instance.
10. Specify the **ExtraHop API Key** and the **ExtraHop Discover Address**. The **ExtraHop API Key** can be obtained from the ExtraHop Discover administration menu under the **API Access** menu item.
11. Test the connection and then click **Save Settings**.



Manage Solution - ExtraHop Standard Management Pack for VMware vRealize Operations
?
Page 1 of 1
Test Connection
Advanced Settings
Save Settings

Adapter Type	Description	Instances	Version	Provided by
EDAAdapter	EDAAdapter	1	0.9.0	ExtraHop

Instance Name
EDAAdapterInstance

Instance Settings

Display Name: EDAAdapterInstance

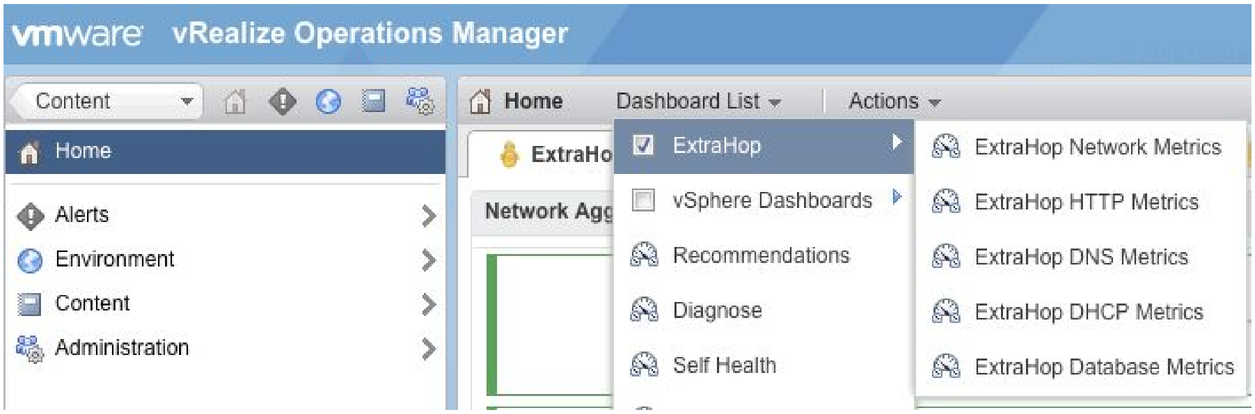
Description:

Basic Settings

ExtraHop API Key: c52583f464714e699e4bb5f36d01cc1c

ExtraHop Discover Address: example.extrahop.com

12. Return to the vRealize Operations Manager Home page.
13. Verify that the ExtraHop dashboard group and dashboards appear in the **Dashboard List**.



3 Available Metrics and Visualizations

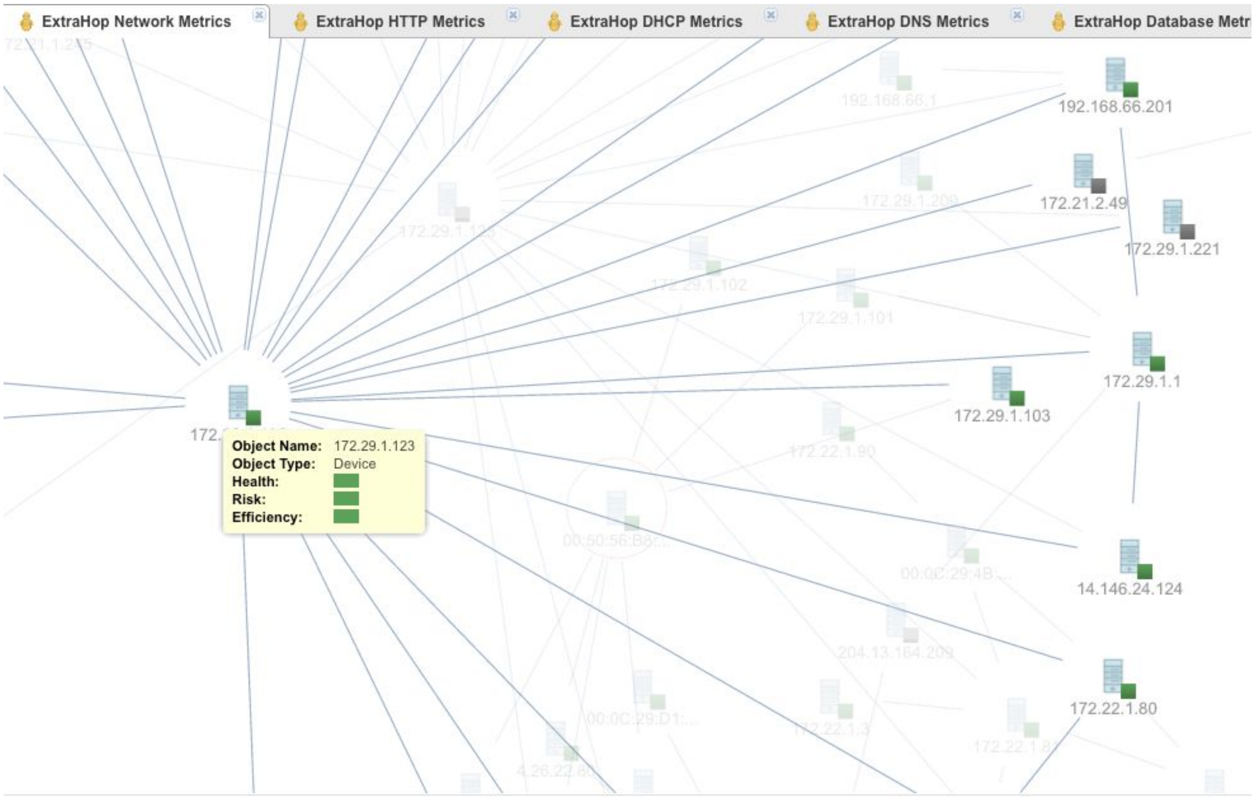
3.1 Network Analytics

3.1.1 Network Metrics

The following network metrics are provided with the ExtraHop Standard Management Pack (listed by object, metric group, and metric name):

- Network Aggregate Stats
    - Network Metrics
        - Request L2 Bytes
        - Request Packets
        - Request Nagle
        - Request Receive Throttle
        - Request RTOs
        - Request Zero Windows
        - Response L2 Bytes
        - Response Packets
        - Response Nagle
        - Response Receive Throttle
        - Response RTOs
        - Response Zero Windows
- Device
    - Device Metrics
        - Round Trip Time
        - RTOs In
        - RTOs Out
        - Zero Windows In
        - Zero Windows Out
        - Bytes In
        - Bytes Out
        - Packets In
        - Packets Out

3.1.2 Network Metrics Visualizations



Object Name: 172.29.1.123
Object Type: Device
Health: 🟩
Risk: 🟩
Efficiency: 🟩

Network Activity Map

The following network metrics visualizations are provided with the ExtraHop Standard Management Pack:

- Network Aggregate Metrics
- Network Aggregate Trends
- Highest Latencies
- Network Devices and Metrics
- Network Activity Map
- Network Device Round Trip
- Network Device Bytes In/Out
- Network Device Packets In/Out
- Network Device Stalls RTOs In/Out
- Network Device Stalls Zero Windows In/Out

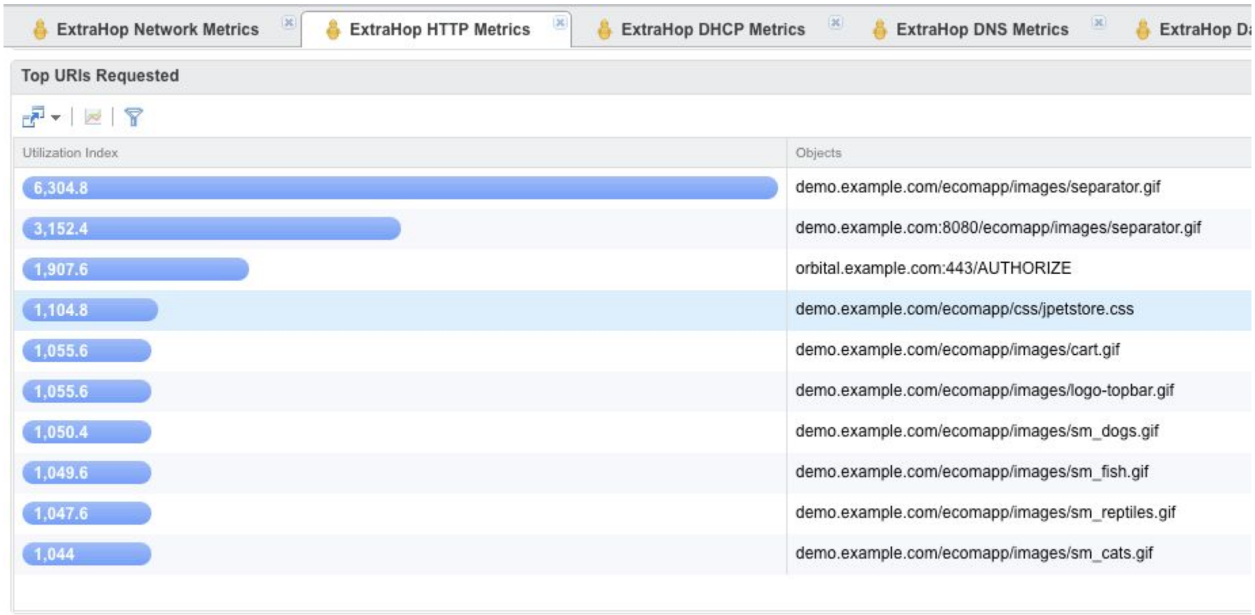
3.2 HTTP Analytics

3.2.1 HTTP Metrics

The following HTTP metrics are provided with the ExtraHop Standard Management Pack (listed by object, metric group and metric name):

- HTTP Aggregate Stats
    - HTTP Metrics
        - Requests
        - Request L2 Bytes
        - Request Packets
        - Request RTOs
        - Request Zero Windows
        - Request Aborts
        - Responses
        - Response L2 Bytes
        - Response Packets
        - Response RTOs
        - Response Zero Windows
        - Response Aborts
        - Response Errors
- HTTP Client
    - HTTP Client Metrics
        - Requests
        - Request Aborts
        - Responses
        - Response Aborts
        - Response Errors
        - Server Processing Time
- HTTP Server
    - HTTP Server Metrics
        - Requests
        - Request Aborts
        - Responses
        - Response Aborts
        - Response Errors
        - Server Processing Time
- HTTP Status Code Record
    - Counts
- URI Record
    - Counts
- URI Error Record
    - Counts

3.2.2 HTTP Metrics Visualizations



Top URIs Requested

Utilization Index	Objects
6,304.8	demo.example.com/ecomapp/images/separator.gif
3,152.4	demo.example.com:8080/ecomapp/images/separator.gif
1,907.6	orbital.example.com:443/AUTHORIZE
1,104.8	demo.example.com/ecomapp/css/jpetstore.css
1,055.6	demo.example.com/ecomapp/images/cart.gif
1,055.6	demo.example.com/ecomapp/images/logo-topbar.gif
1,050.4	demo.example.com/ecomapp/images/sm_dogs.gif
1,049.6	demo.example.com/ecomapp/images/sm_fish.gif
1,047.6	demo.example.com/ecomapp/images/sm_reptiles.gif
1,044	demo.example.com/ecomapp/images/sm_cats.gif

Top URIs Requested

The following HTTP metrics visualizations are provided with the ExtraHop Standard Management Pack:

- HTTP Aggregate Metrics
- HTTP Aggregate Trends
- Top Clients (Requests)
- Top Servers (Responses)
- Top Servers for Processing Time
- Top Response Codes
- Top URIs Requested
- Top URI Errors
- HTTP Servers and Metrics
- HTTP Server Activity Map
- HTTP Server Response Processing Time
- HTTP Server Requests/Responses
- HTTP Server Response Errors
- HTTP Clients and Metrics
- HTTP Client Requests/Responses
- HTTP Client Response Errors

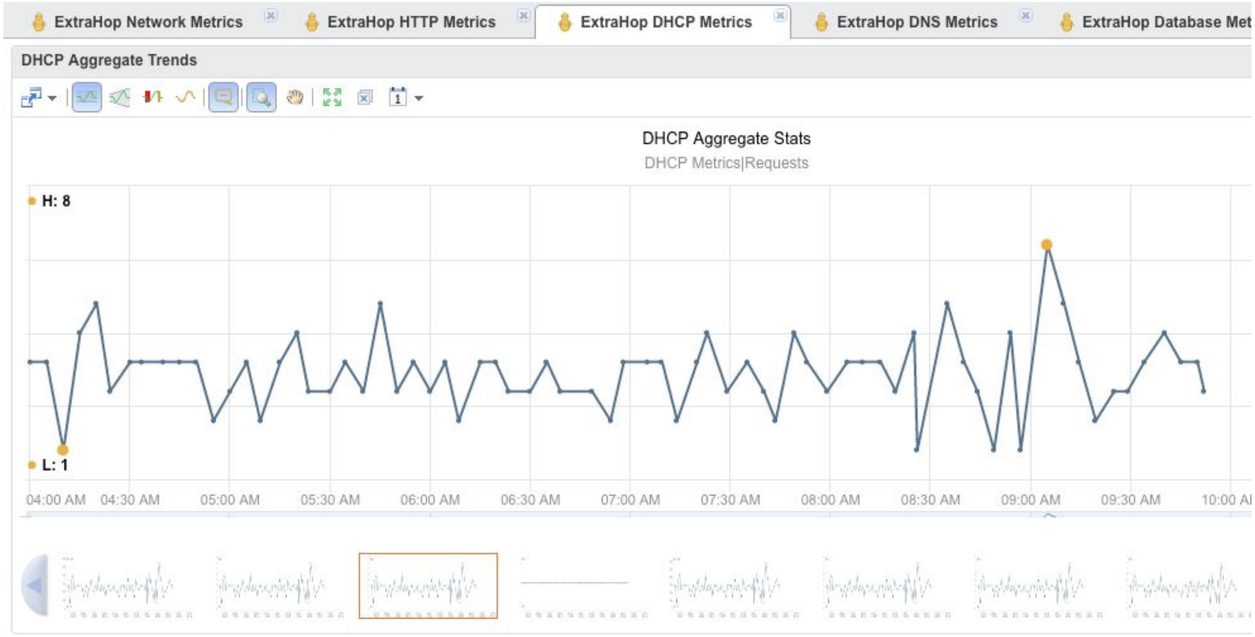
3.3 DHCP Analytics

3.3.1 DHCP Metrics

The following DHCP metrics are provided with the ExtraHop Standard Management Pack (listed by object, metric group and metric name):

- DHCP Aggregate Stats
  - DHCP Metrics
    - Requests
    - Request L2 Bytes
    - Request Packets
    - Responses
    - Response L2 Bytes
    - Response Packets
    - Response Errors
  - DHCP Message Type Metrics (Counts)
    - DHCPDISCOVER
    - DHCPOFFER
    - DHCPREQUEST
    - DHCPACK
    - DHCPNACK
    - DHCPDECLINE
    - DHCPRELEASE
    - DHCPINFORM
- DHCP Client
  - DHCP Client Metrics
    - Requests
    - Responses
    - Response Errors
    - Server Processing Time
- DHCP Server
  - DHCP Server Metrics
    - Requests
    - Responses
    - Response Errors
    - Server Processing Time

3.3.2 DHCP Metrics Visualizations



DHCP Aggregate Trends

The following DHCP metrics visualizations are provided with the ExtraHop Standard Management Pack:

- DHCP Aggregate Metrics
- DHCP Aggregate Trends
- Top Servers (Responses)
- Top Servers for Processing Time
- DHCP Servers and Metrics
- DHCP Server Activity Map
- DHCP Server Requests/Responses
- DHCP Server Response Errors
- DHCP Clients and Metrics
- DHCP Client Requests/Responses
- DHCP Client Response Errors

3.4 DNS Analytics

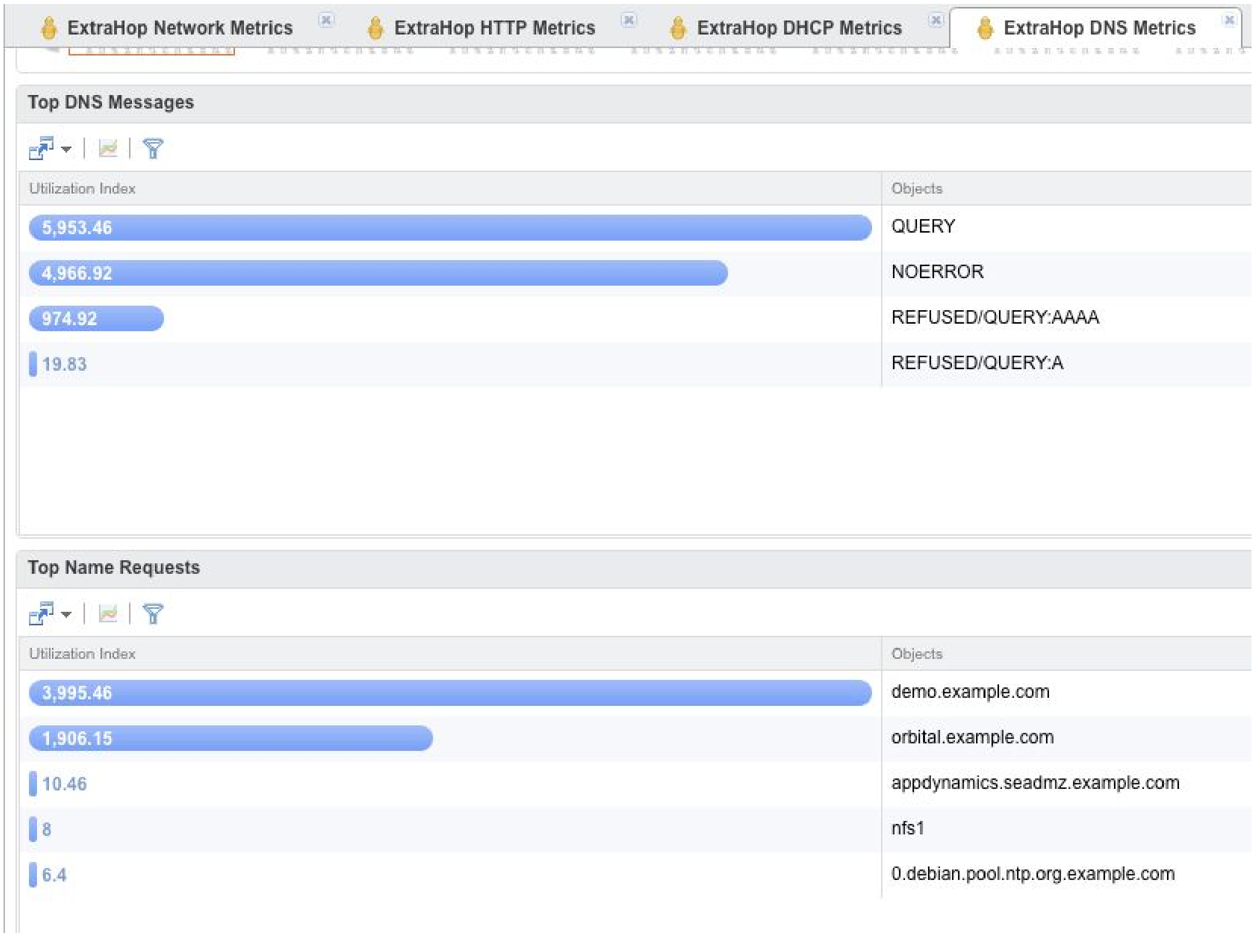
3.4.1 DNS Metrics

The following DNS metrics are provided with the ExtraHop Standard Management Pack (listed by object, metric group and metric name):

- DNS Aggregate Stats
    - DNS Metrics
        - Requests
        - Request L2 Bytes

    - Request Packets
    - Request Timeouts
    - Responses
    - Response L2 Bytes
    - Response Packets
    - Response Errors
- DNS Client
  - DNS Client Metrics
    - Requests
    - Request Timeouts
    - Responses
    - Response Errors
    - Server Processing Time
- DNS Server
  - DNS Server Metrics
    - Requests
    - Request Timeouts
    - Responses
    - Response Errors
    - Server Processing Time
- DNS Message Record
    - Counts
- DNS QNAME Record
    - Counts
- DNS QNAME Error Record
    - Counts

3.4.2 DNS Metrics Visualizations



Top DNS Messages

Utilization Index	Objects
5,953.46	QUERY
4,966.92	NOERROR
974.92	REFUSED/QUERY:AAAA
19.83	REFUSED/QUERY:A

Top Name Requests

Utilization Index	Objects
3,995.46	demo.example.com
1,906.15	orbital.example.com
10.46	appdynamics.seadmz.example.com
8	nfs1
6.4	0.debian.pool.ntp.org.example.com

Top DNS Messages and Top Name Requests

The following DNS metrics visualizations are provided with the ExtraHop Standard Management Pack:

- DNS Aggregate Metrics
- DNS Aggregate Trends
- Top DNS Messages
- Top Name Requests
- Top Name Errors
- Top Clients (Requests)
- Top Servers (Responses)
- Top Servers for Processing Time
- DNS Servers and Metrics
- DNS Server Activity Map
- DNS Server Processing Time
- DNS Server Requests/Responses
- DNS Server Response Errors
- DNS Clients and Metrics
- DNS Client Requests/Responses

- DNS Client Response Errors

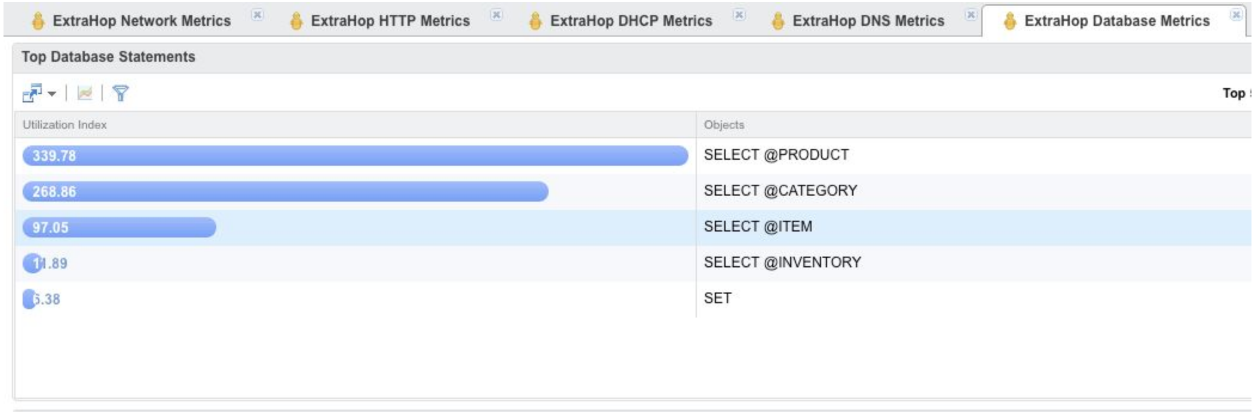
3.5 Database Analytics

3.5.1 Database Metrics

The following database metrics are provided with the ExtraHop Standard Management Pack (listed by object, metric group and metric name):

- Database Aggregate Stats
    - Database Metrics
        - Requests
        - Request Bytes
        - Request L2 Bytes
        - Request Packets
        - Request RTOs
        - Request Zero Windows
        - Responses
        - Response Bytes
        - Response L2 Bytes
        - Response Packets
        - Response Errors
        - Response RTOs
        - Response Zero Windows
- Database Client
    - Database Client Metrics
        - Requests
        - Request Aborts
        - Responses
        - Response Aborts
        - Response Errors
        - Server Processing Time
- Database Server
    - Database Server Metrics
        - Requests
        - Request Aborts
        - Responses
        - Response Aborts
        - Response Errors
        - Server Processing Time
- Database Statement Record
        - Counts

3.5.2 Database Metrics Visualizations



Utilization Index	Objects
339.78	SELECT @PRODUCT
268.86	SELECT @CATEGORY
97.05	SELECT @ITEM
11.89	SELECT @INVENTORY
6.38	SET

Top Database Statements

The following database metrics visualizations are provided with the ExtraHop Standard Management Pack:

- Database Aggregate Metrics
- Database Aggregate Trends
- Top Database Statements
- Top Clients (Requests)
- Top Servers (Responses)
- Top Servers for Processing Time
- Database Servers and Metrics
- Database Activity Map
- Database Server Processing Time
- Database Server Requests/Responses
- Database Server Response Errors
- Database Clients and Metrics
- Database Clients Requests/Responses
- Database Client Response Errors

4 Creating Alerts through the ExtraHop Standard Management Pack Metrics

You can create VROPS alerts for your virtual environment through ExtraHop metrics. These can be quickly created within the VROPS user interface. These alerts can then warn you when issues arise and provide recommendations and actions to resolve issues.

4.1 Developing the Alert

Before creating an alert in VROPS, determine the following aspects of your alert:

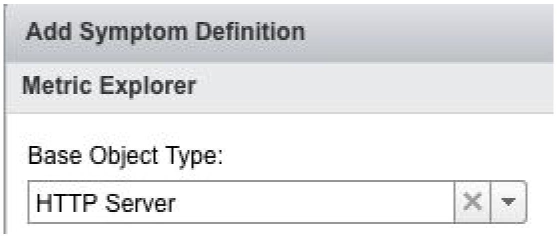
- Determine which ExtraHop metric to monitor (see Section 3 for a list of metrics).
- Determine the threshold level that will trigger the alert for the symptom definition.

- Determine recommendations for further investigation by an administrator.
- If appropriate, determine the actions that might resolve the issue, such as powering off a virtual machine. Available actions can be found under **Content** > **Actions**.

4.2 Create the Symptom Definition

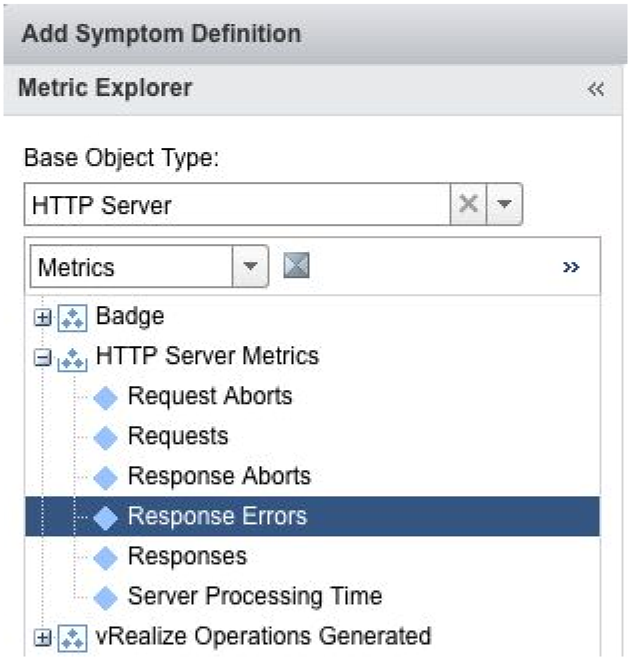
Follow the next steps to create the symptom definition for your alert.

1. Go to **Content** > **Symptom Definitions**.
2. Select **Metric / Property Symptom Definitions**.
3. Click the plus symbol + to add a new symptom definition.
4. Under **Base Object Type**, select the object associated with the metric (see section 3).



Base Object Type: HTTP Server

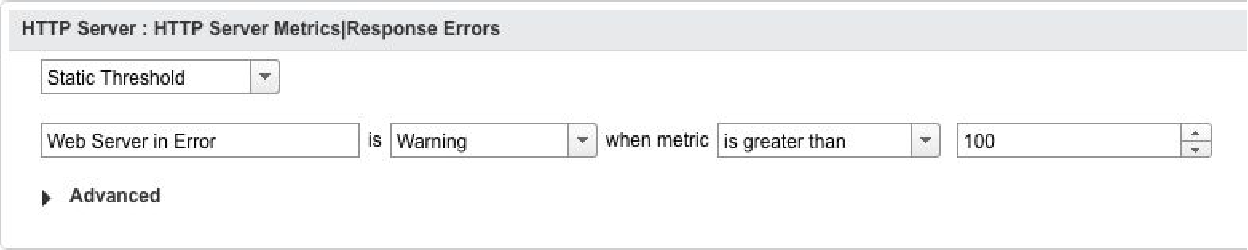
5. Next, double-click the metric that you would like to create a threshold for. This step creates a symptom definition entry to the right.



Base Object Type: HTTP Server

6. Complete the following information for the symptom definition entry:
   a. A name
   b. Threshold type
   c. Alert type

    d. Threshold evaluation
7. Click the question mark in the upper right corner of the dialog for more details about the symptom definition.

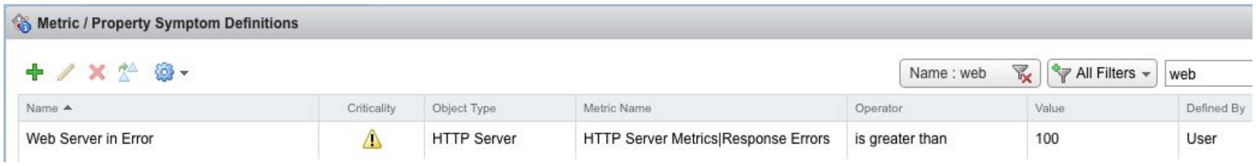


HTTP Server : HTTP Server Metrics|Response Errors

Static Threshold

Web Server in Error is Warning when metric is greater than 100

8. Click **Save** to save the symptom definition. The symptom will appear in the symptom definitions list.



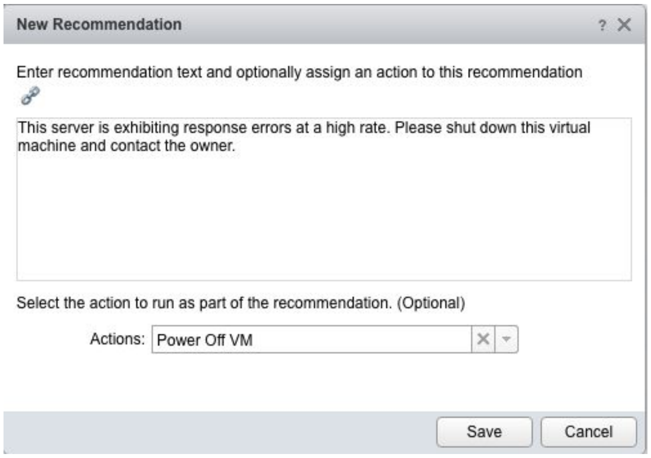
Metric / Property Symptom Definitions

Name ▲	Criticality	Object Type	Metric Name	Operator	Value	Defined By
Web Server in Error	⚠	HTTP Server	HTTP Server Metrics|Response Errors	is greater than	100	User

4.3 Create the Recommendation

Complete the following steps to create the recommendation for an alert.

1. Go to **Content** > **Recommendations**.
2. Click the plus symbol ✚ to add a recommendation.
3. In the dialog box, enter descriptive text for the recommendation and optionally select an **Action** to resolve the issue.



New Recommendation

Enter recommendation text and optionally assign an action to this recommendation

This server is exhibiting response errors at a high rate. Please shut down this virtual machine and contact the owner.

Select the action to run as part of the recommendation. (Optional)

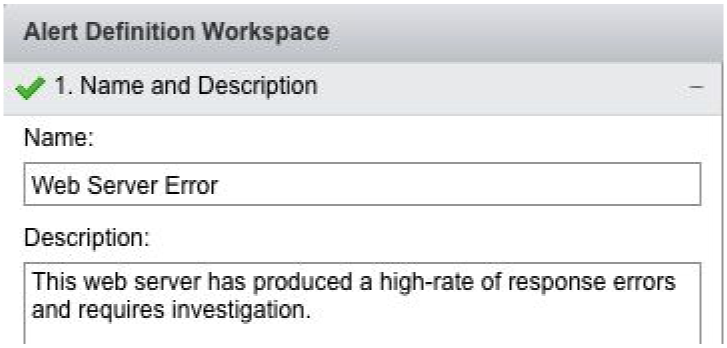
Actions: Power Off VM

4. Click **Save** to save the recommendation. The recommendation will appear in the recommendations list.

4.4 Create the Alert

After you have defined a symptom and a recommendation, you can create the alert. Complete the following steps to create the alert.

1. Go to **Content** > **Alert Definitions**.
2. Click the plus symbol ✚ to add an alert.
3. Specify a name and a description for the alert.



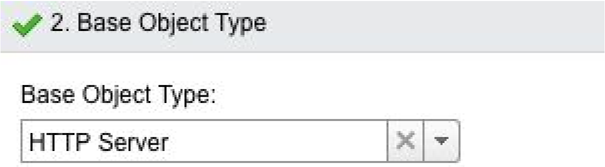
Alert Definition Workspace

✓ 1. Name and Description

Name: Web Server Error

Description: This web server has produced a high-rate of response errors and requires investigation.

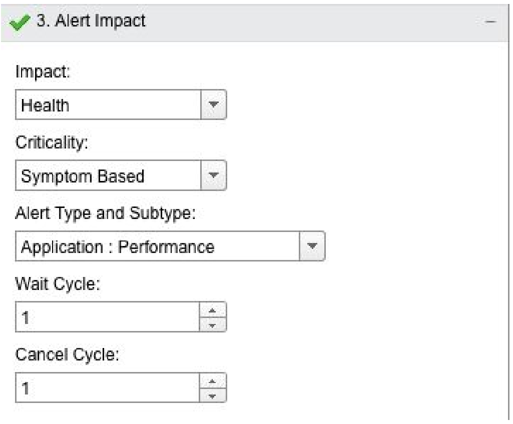
4. Choose the **Base Object Type**. Select the same object that you defined in the symptom.



✓ 2. Base Object Type

Base Object Type: HTTP Server

5. For the **Alert Impact**, select the type of impact.



✓ 3. Alert Impact

Impact: Health

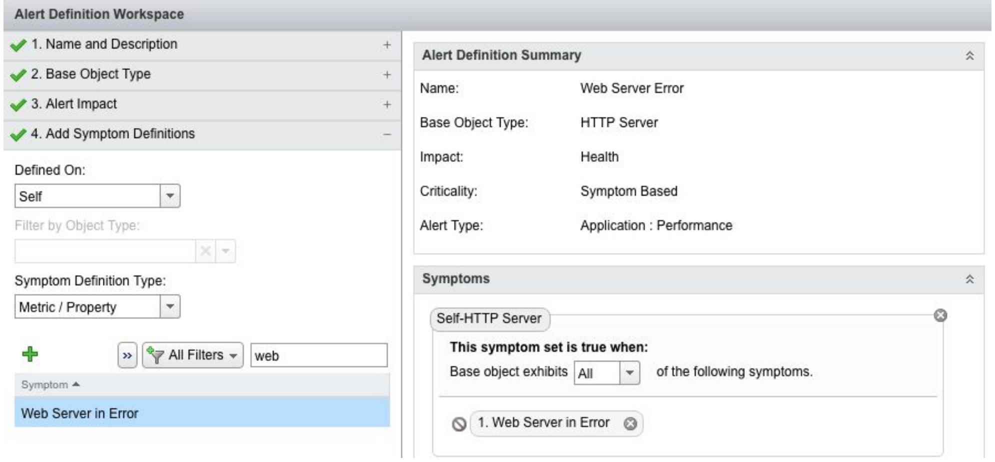
Criticality: Symptom Based

Alert Type and Subtype: Application : Performance

Wait Cycle: 1

Cancel Cycle: 1

6. For **Add Symptom Definitions**, drag the symptom definition to the right.



Alert Definition Workspace

1. Name and Description
2. Base Object Type
3. Alert Impact
4. Add Symptom Definitions

Defined On: Self

Filter by Object Type:

Symptom Definition Type: Metric / Property

All Filters: web

Symptom

Web Server in Error

Alert Definition Summary

Name: Web Server Error
Base Object Type: HTTP Server
Impact: Health
Criticality: Symptom Based
Alert Type: Application : Performance

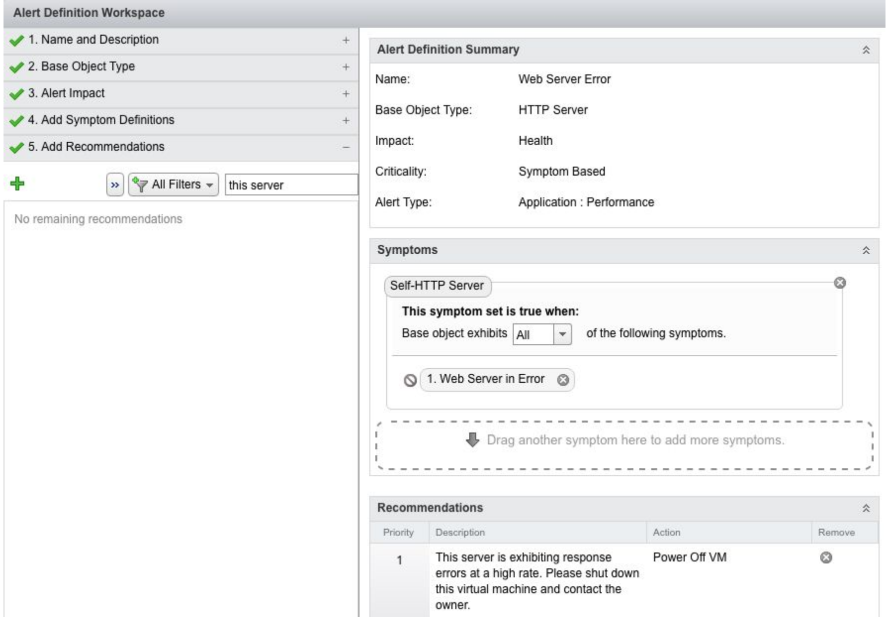
Symptoms

Self-HTTP Server

This symptom set is true when:
Base object exhibits All of the following symptoms.

1. Web Server in Error

7. For **Add Recommendations**, drag the recommendation to the right.



Alert Definition Workspace

1. Name and Description
2. Base Object Type
3. Alert Impact
4. Add Symptom Definitions
5. Add Recommendations

All Filters: this server

No remaining recommendations

Alert Definition Summary

Name: Web Server Error
Base Object Type: HTTP Server
Impact: Health
Criticality: Symptom Based
Alert Type: Application : Performance

Symptoms

Self-HTTP Server

This symptom set is true when:
Base object exhibits All of the following symptoms.

1. Web Server in Error

Drag another symptom here to add more symptoms.

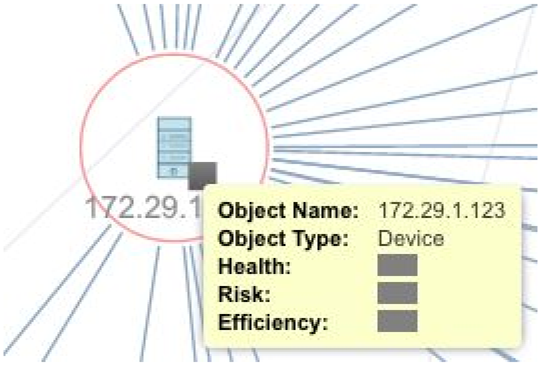
Recommendations

Priority	Description	Action	Remove
1	This server is exhibiting response errors at a high rate. Please shut down this virtual machine and contact the owner.	Power Off VM	⊗

8. Click **Save** to save and enable the alert. The alert will appear in the alerts list.

5 Updating Object Health, Risk or Efficiency Status through ExtraHop Standard Management Pack Metrics

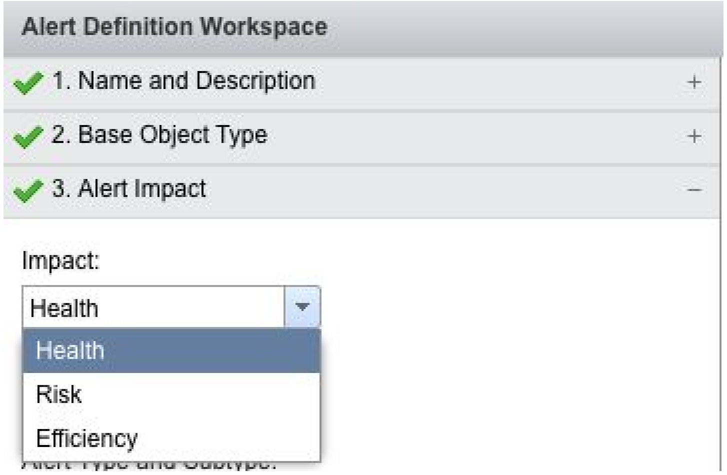
ExtraHop metrics can set the health, risk, or efficiency status of an object. This setting can provide quick visual identification of the status of an object. This is achieved through the creation of an alert. Refer to section 4 for how to create an alert.



Object Name: 172.29.1.123
Object Type: Device
Health: ▨
Risk: ▨
Efficiency: ▨

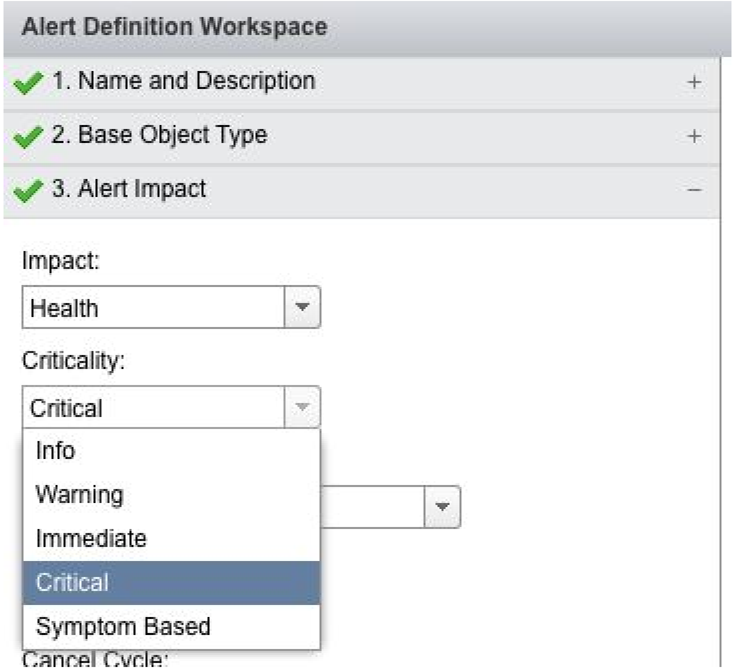
5.1 Setting Health, Risk, or Efficiency Status While Creating an Alert

To set a Health, Risk, or Efficiency status, create an alert as described in section 4. While creating the alert (section 4.4), set an **Impact** through the **Alert Impact** setting.



Impact: Health

After you specify the **Impact**, set the **Criticality**.



Impact: Health

Criticality: Critical

You have now set the object status as determined by this alert.