Monitoring VMware Systems

VMware: vSphere Base Pack PowerPack version 207

Table of Contents

Chapter 1

Introduction

Overview

For the ScienceLogic platform to discover and collect information from a VMware vCenter Server, you must ensure that the platform can communicate with the vCenter Server. This manual describes how to configure VMware vCenter Servers and ESX/ESXi servers for communication with the ScienceLogic platform.

The ScienceLogic platform can use the data collected from VMware vCenter Servers to create device records for all components managed by that vCenter server, such as datastores and guest VMs. This manual describes how to configure the platform to create component devices for VMware systems.

This manual describes:

- *Configuring a vCenter Server*
- *Discovering a vCenter Server*
- Configuring SNMP on *ESXi 4.x & 5.x* and *ESX 4.x*
- *Dashboards for VMware devices*

NOTE: Before you read this manual or use the ScienceLogic platform to monitor VMware, you might want to familiarize yourself with the terminology used by VMware. The VMware Master Glossary is available at: http://www.vmware.com/pdf/master_glossary.pdf

NOTE: ScienceLogic provides this documentation for the convenience of ScienceLogic customers. Some of the configuration information contained herein pertains to third-party vendor software that is subject to change without notice to ScienceLogic. ScienceLogic makes every attempt to maintain accurate technical information and cannot be held responsible for defects or changes in third-party vendor software. There is no written or implied guarantee that information contained herein will work for all third-party variants. See the End User License Agreement (EULA) for more information.

What is VMware vSphere?

vSphere is VMware's cloud virtualization platform that enables users to deploy and manage VMware cloud-based resources using a suite of components, including the vCenter Server centralized management application and ESX/ESXi host servers.

What Does the VMware: vSphere Base Pack PowerPack Monitor?

To monitor VMware virtual infrastructure using the ScienceLogic platform, you must install the *VMware: vSphere Base Pack* PowerPack. This PowerPack enables you to discover, model, and collect data about VMware virtual devices.

The *VMware: vSphere Base Pack* PowerPack includes:

- Two example credentials you can use as templates to create SOAP/XML credentials to connect to the VMware devices you want to monitor
- Dynamic Applications to discover, model, and monitor performance metrics and/or collect configuration data for VMware devices.
- Device Classes for each of the VMware devices the ScienceLogic platform monitors
- A Device Template that enables you to easily align multiple Dynamic Applications to VMware devices
- Event Policies and corresponding alerts that are triggered when VMware devices meet certain status criteria
- Device dashboards for several of the discoverable VMware component devices

NOTE: The *VMware: vSphere Dashboards* PowerPack contains additional dashboards that display data collected from VMware systems. To view these dashboards, you must install the *VMware: vSphere Dashboards* PowerPack on your ScienceLogic system. (For more information, see the chapter on *VMware Dashboards*.)

Installing the VMware: vSphere Base Pack PowerPack

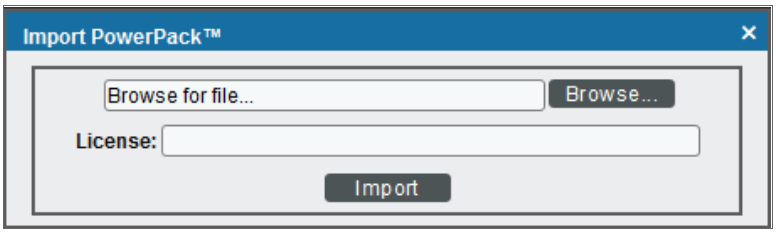
Before completing the steps in this manual, you must import and install version 207 of the *VMware: vSphere Base Pack* PowerPack.

NOTE: To install version 207 of the *VMware: vSphere Base Pack* PowerPack, your ScienceLogic system must be upgraded to the 8.2.0 or later release. The Dynamic Applications in version 207 of the *VMware: vSphere Base Pack* PowerPack support VMware vCenter Servers running versions 4.x, 5.x, and 6.x, and ESX/ESXi servers running versions 4.x and 5.x.

To download and install a PowerPack:

TIP: By default, installing a new version of a PowerPack overwrites all content in that PowerPack that has already been installed on the target system. You can use the ***Enable Selective PowerPack Field Protection*** setting in the **Behavior Settings** page (System > Settings > Behavior) to prevent new PowerPacks from overwriting local changes for some commonly customized fields. (For more information, see the ***System Administration*** manual.)

1. Download the PowerPack from the ScienceLogic Customer Portal.
2. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).
3. In the **PowerPack Manager** page, click the **[Actions]** button, then select *Import PowerPack*.
4. The **Import PowerPack** dialog box appears:



5. Click the **[Browse]** button and navigate to the PowerPack file.
6. When the **PowerPack Installer** modal page appears, click the **[Install]** button to install the PowerPack.

NOTE: If you exit the **PowerPack Installer** modal page without installing the imported PowerPack, the imported PowerPack will not appear in the **PowerPack Manager** page. However, the imported PowerPack will appear in the **Imported PowerPacks** modal page. This page appears when you click the **[Actions]** menu and select *Install PowerPack*.

Version Requirements and Limitations

The following limitations and requirements apply to specific functionality in the *VMware: vSphere Base Pack* PowerPack:

- To collect I/O and latency metrics for datastores, you must enable Storage I/O Control. For information about Storage I/O Control, see the VMware knowledge base.
- Datastore Storage Performance Statistics are available only from vCenter systems running vSphere API 4.1.2 or later. The ScienceLogic platform will not collect Datastore Storage Performance Statistics if the Dynamic Applications that use Dynamic Component Mapping are used to monitor ESX or ESXi servers directly.
- Datastore Performance Statistics are unavailable for NFS datastores.
- If VMware Tools is not installed on a guest VM, the ScienceLogic platform cannot collect all performance statistics for that guest VM.
- Because no truly unique identifier is provided by the VMware vSphere API, it is possible that duplicate component devices could be created in the ScienceLogic platform when a virtual machine vMotions between separately monitored ESX/ESXi servers. (This issue does not affect vMotion events that occur within the same component tree, such as between two ESX/ESXi servers that are monitored through the same vCenter server.) Therefore, ScienceLogic recommends monitoring VMware servers through vCenter. In addition to accommodating vMotion events, monitoring through vCenter prevents performance issues on ESX/ESXi servers caused by API use.
- If you want to delete and reinstall version 203 or higher of the *VMware: vSphere Base Pack* PowerPack, you should first delete any existing copies of the Device Template included in the PowerPack and then create new versions of them after reinstalling the PowerPack. Doing so ensures that any copies of the Device Template included in the PowerPack will work properly after reinstallation. You should then assign the new Device Template(s) to any existing Discovery Sessions that were linked to the previous versions of the template(s).

Chapter 2

Configuring VMware vCenter Server for Monitoring

Overview

The following sections describe how to configure VMware vCenter resources for monitoring by the ScienceLogic platform using the *VMware: vSphere Base Pack* PowerPack:

Prerequisites

Before performing the steps for configuring a vCenter server, you must have:

- Installed and configured a VMware vCenter server that monitors your ESX and ESXi servers.
- Installed the VMware vCenter web service. The VMware vCenter web service is installed by default on VMware vCenter servers. For more information about the installation of the VMware vCenter web service, see the Web Service FAQs page on the VMware website.
- Created a user account that the platform can use to access the web service. For vCenter 5.0 and earlier, the VMware vCenter web service uses the user groups and/or active directory users configured on the Windows Server on which vCenter is installed. For vCenter 5.1, the VMware vCenter web service uses the user groups and/or active directory users configured on the VMware SSO server. You might want to create a user account that is used by only the ScienceLogic platform. This chapter includes instructions on how to grant read-only

permissions to a vCenter user.

- Access to the vCenter server using the vSphere client.

Ensuring the VMware vCenter Web Service is Running

Using the default VMware configuration, the VMware vCenter Web Service is automatically started on VMware vCenter servers.

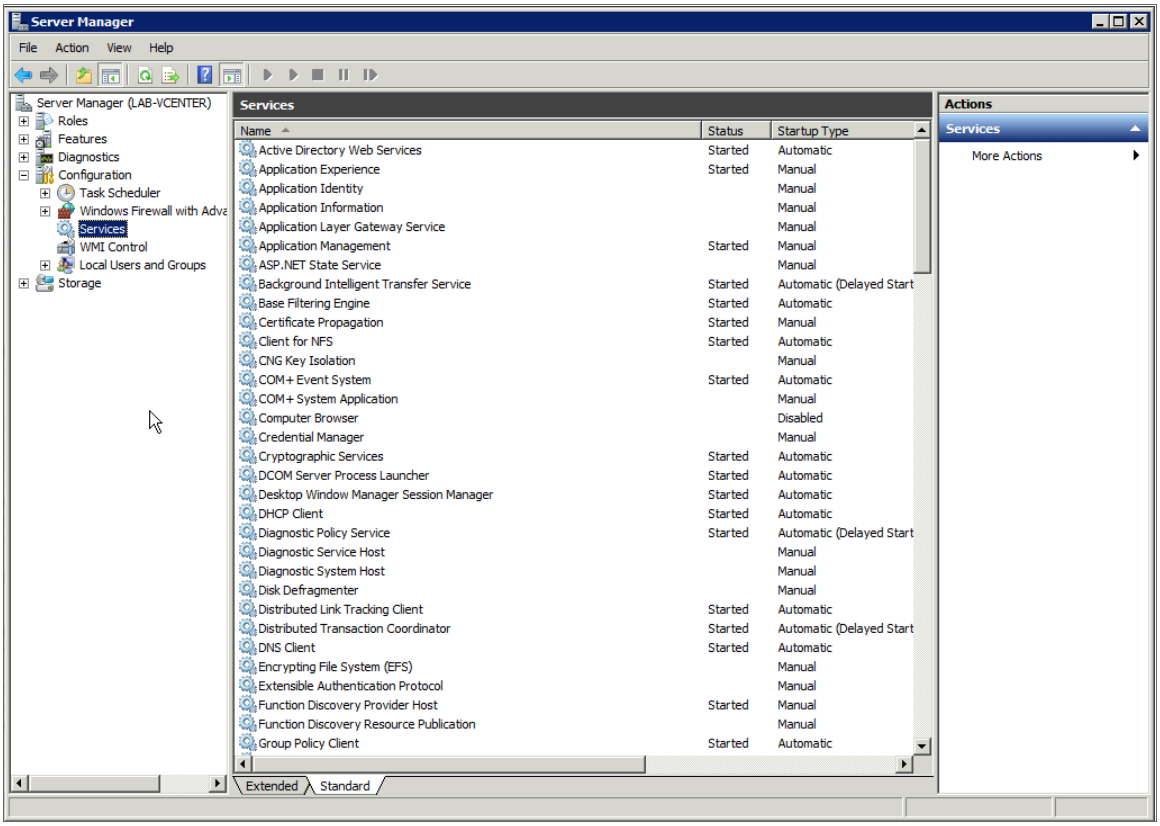
To verify that the web service is available, navigate to the following URL in a browser window:

```
https://ip-address-of-vcenter-server/sdk/vimService.wsdl
```

- If the web service is running, an XML document will be returned.
- If a connection error is displayed, the web service might not be running.

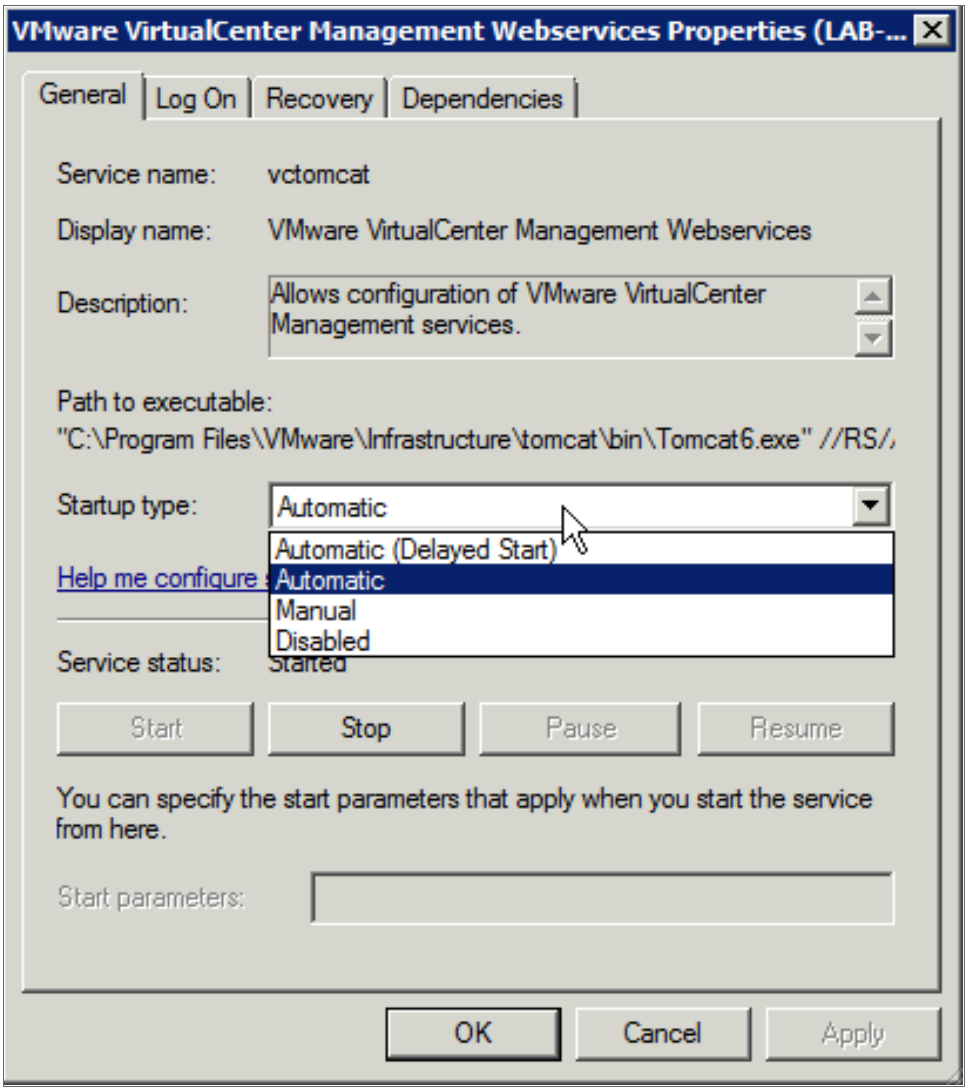
To verify the web service is running:

1. Log in to the Windows Server that hosts vCenter Server.
2. Open the ***Server Manager***.
3. In the left pane, expand the ***Configuration*** entry and select ***Services***.



4. Locate the *VMware VirtualCenter Management Webservices* service. If the web service is configured and started correctly, the ***Status*** should be *Started* and the ***Startup Type*** should be *Automatic*.

5. If the ***Status*** is not *Started*, right click on the *VMware vCenter Management Webservices* service, then select *Start*.
6. If the ***Startup Type*** is not *Automatic*, right click on the *VMware vCenter Management Webservices* service, then select *Properties*. The general properties for the service are displayed.



7. In the ***Startup type*** drop-down list, select *Automatic* and then click the **[OK]** button.

After the web service starts, try navigating to the URL again. If a connection error is still displayed, your network's firewall may be blocking access to port 443 (HTTPS), which is required to use the VMware vCenter web service.

If the computer on which you navigated to the URL does not have access to port 443 on the ESX server, but the Data Collector responsible for monitoring the ESX server does, you can verify connectivity from the console of the Data Collector. Issue the following command from the console of the Data Collector:

```
curl -k "https://ip-address-of-vcenter-server/sdk/vimService.wsdl"
```

If the web service is running and the port is not blocked by a firewall, an XML document will be returned.

Creating a Read-Only User Account

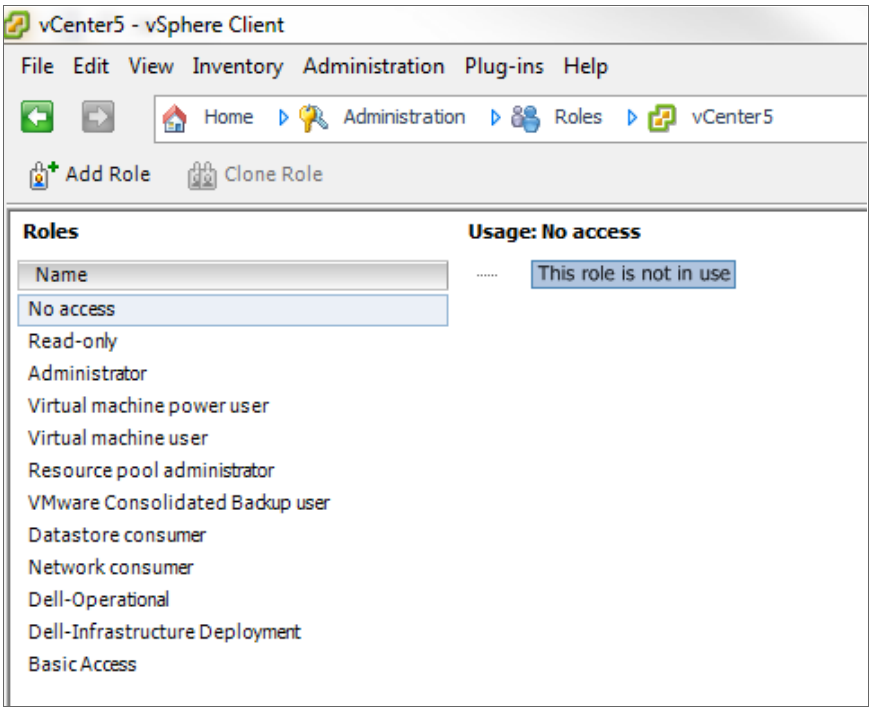
For vCenter 5.0 and earlier, the VMware vCenter web service uses the user groups and/or active directory users configured on the Windows Server on which vCenter is installed.

For vCenter 5.1, the VMware vCenter web service uses the user groups and/or active directory users configured on the VMware SSO server.

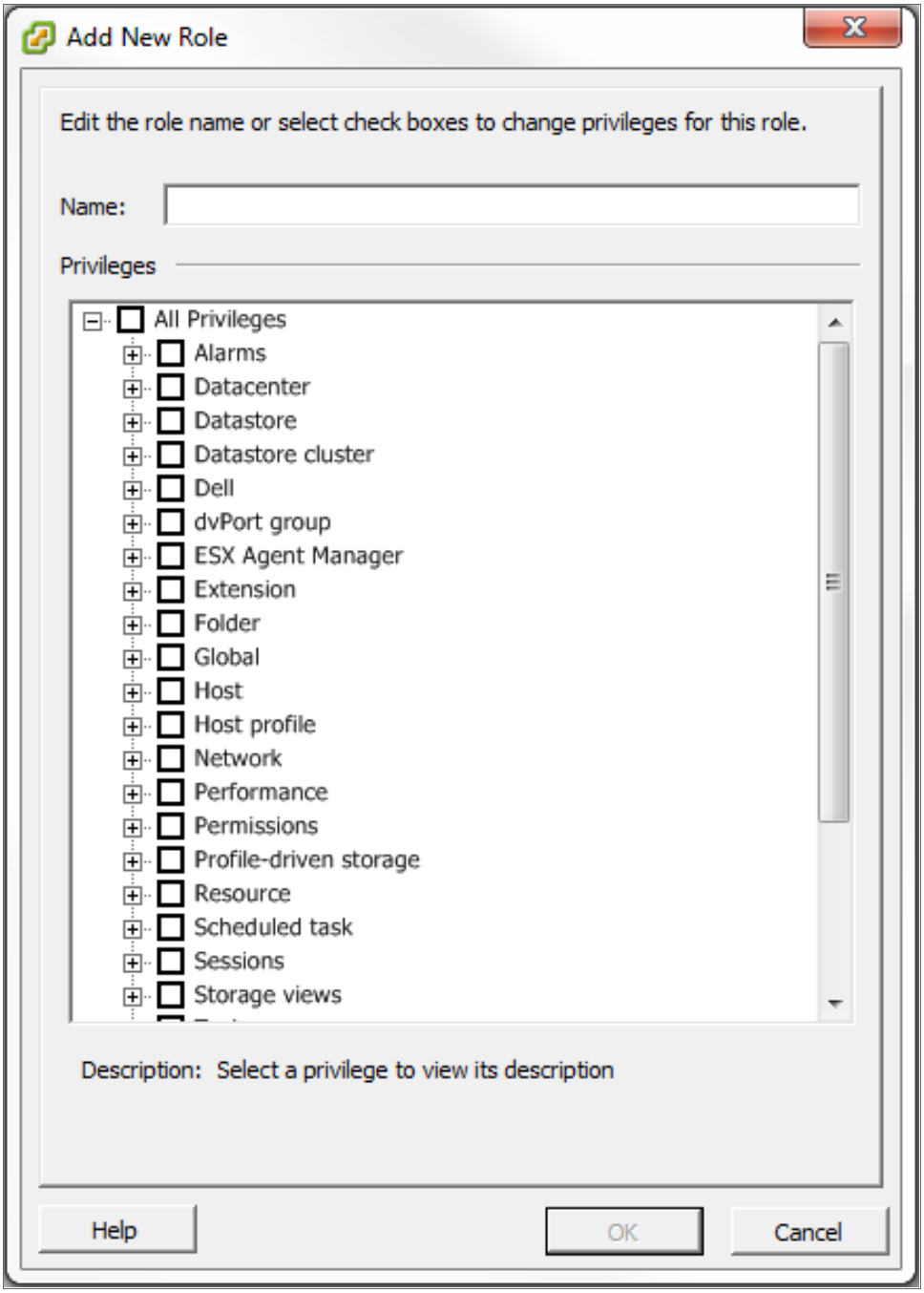
Administrative users are the only default user type that have the level of access the ScienceLogic platform requires to collect data from the VMware vCenter web service. If you do not want to use the username and password of an administrative user in the SOAP/XML credential, you can set up a custom user role with the specific read-only access the ScienceLogic platform requires to the VMware vCenter web service.

To create a custom user role that grants the read-only access the ScienceLogic platform requires, perform the following steps:

1. Log in to the vCenter server as an administrator using the VMware vSphere client.
2. In the menu at the top of the page, click View > Administration > Roles. The **Roles** page appears:



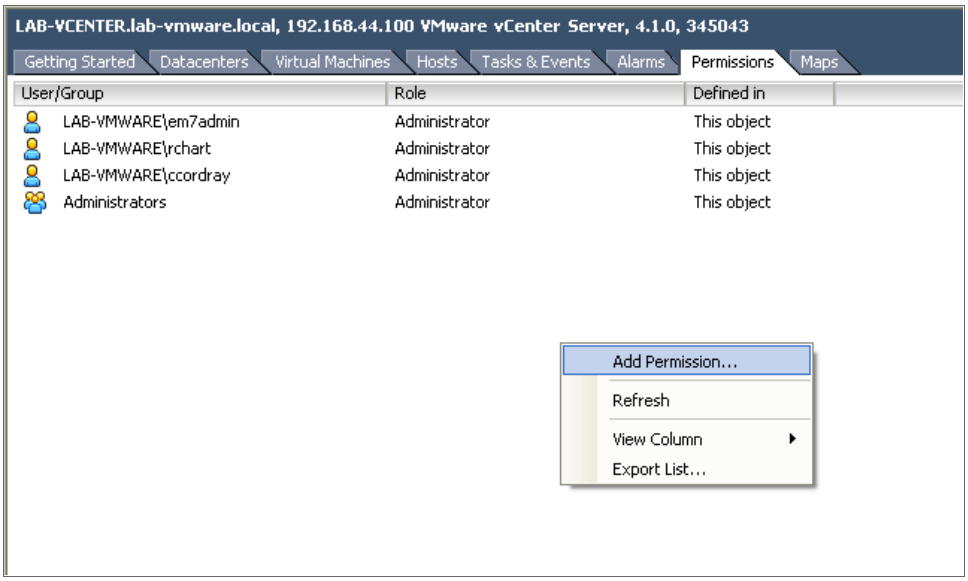
3. Click the **[Add Role]** button. The **Add New Role** page appears:



4. Enter "ScienceLogic" in the ***Name*** field.
5. Expand the ***Storage views*** section in the **Privileges** pane and select the ***View*** checkbox.
6. Click the **[OK]** button.

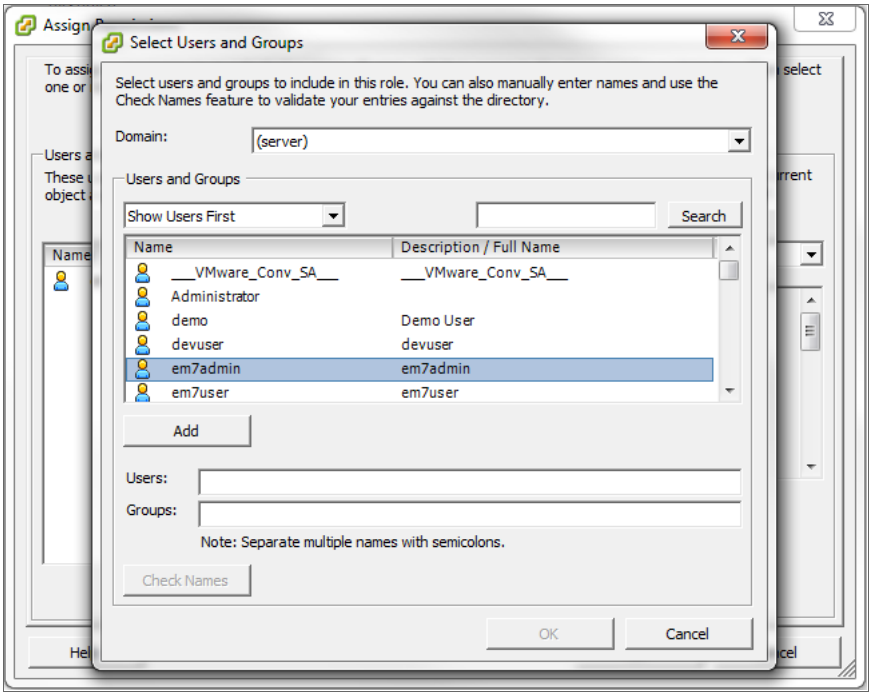
To assign the custom role to a user account, perform the following steps:

1. Log in to the vCenter server as an administrator using the VMware vSphere client.
2. In the vSphere client, ensure the vCenter server is selected in the left pane.
3. Click the **[Permissions]** tab in the main pane.

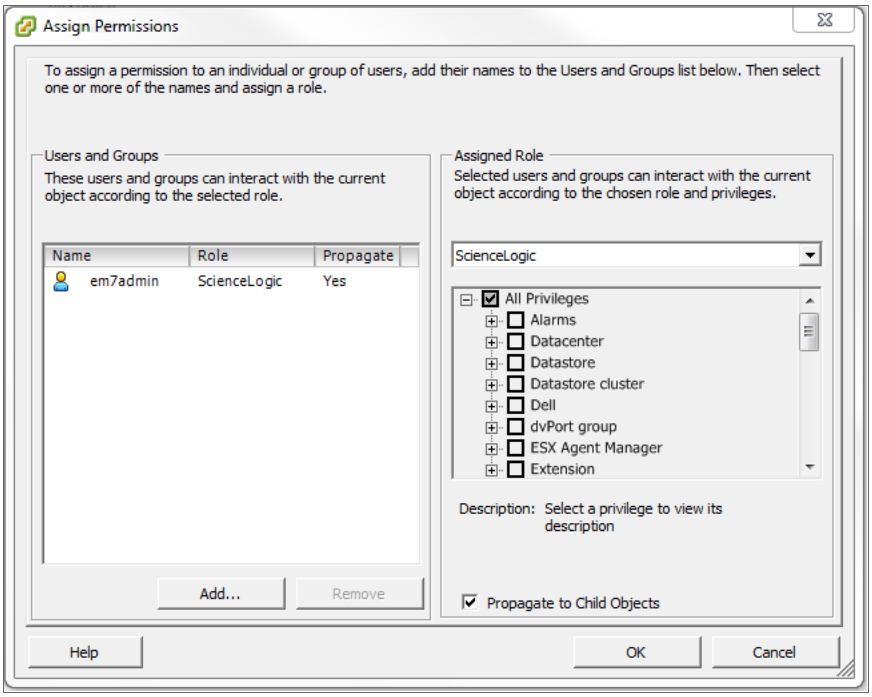


4. Right click in the main pane, then select *Add Permission…*. The **Assign Permissions** window appears.

5. In the ***Assigned Role*** drop-down list, select the *ScienceLogic* role that you created in the previous section. Click the **[Add]** button. The **Select Users and Groups** window appears.



6. From the list of users, select the user or group you want to assign the required permissions to, then click the **[Add]** button, followed by the **[OK]** button. The **Select Users and Groups** pop-up window closes.



7. In the **Assign Permissions** pop-up window, ensure that the user or group you selected is highlighted in the ***Users and Groups*** select list, and that the ***Propagate to Child Objects*** checkbox is checked.
8. Click the **[OK]** button.

To test that the user that you configured works with the VMware web service, navigate to the following URL in a browser window:

```
https://ip-address-of-vmware-server/mob
```

When prompted, enter the username and password you created for the platform to access the VMware Web Service. If the user is configured correctly, the following page appears:

If the user is not configured correctly, you will be prompted again for a username and password.

Configuring a SOAP/XML Credential

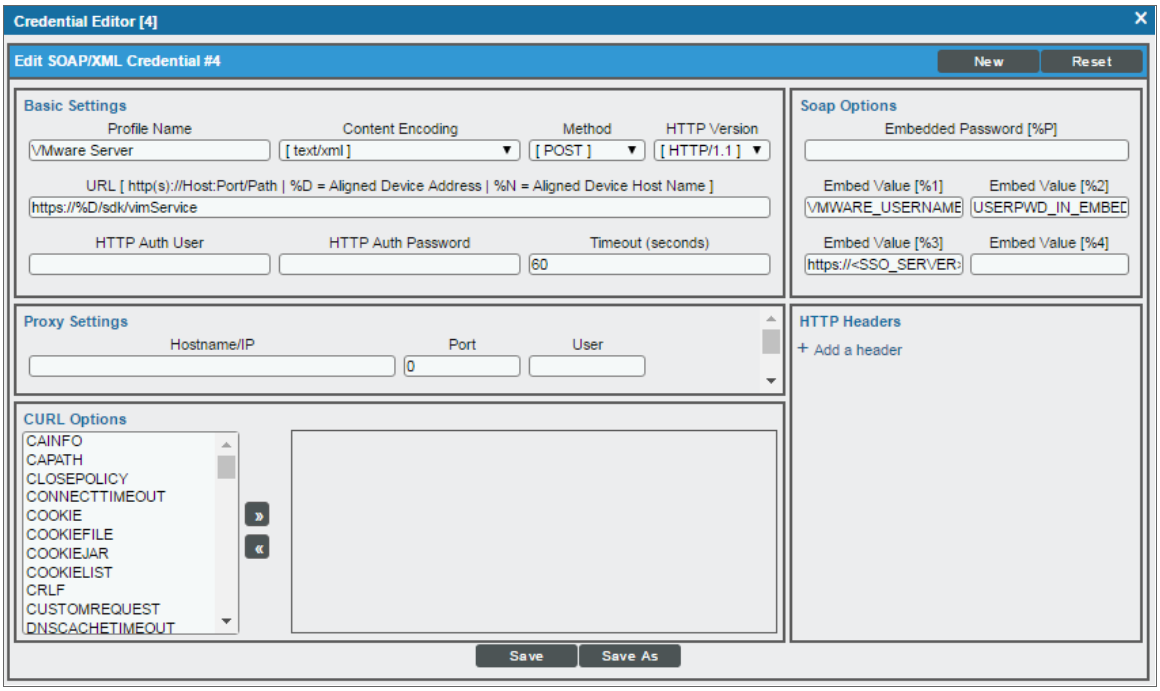
To use the Dynamic Applications in the *VMware: vSphere Base Pack* PowerPack, you must configure a SOAP/XML credential for the VMware web service. The *VMware: vSphere Base Pack* PowerPack includes the following templates for SOAP/XML credentials that you can edit for use with your vCenter server:

- VMware Server (for use with vCenter Server versions 4.x and 5.x)
- VMware Server vCenter 6 (for use with vCenter Server version 6.x)

To modify either of the templates, perform the following steps:

1. Go to the **Credential Management** page (System > Manage > Credentials).

2. Click the wrench icon ( ) for the "VMware Server" or "VMware Server vCenter 6" credential. The **Credential Editor** modal page appears:



3. Supply values in the following fields:

   - ***Profile Name***. Enter a new name for the credential.
   - ***Embed Value [%1]***. Enter the username the platform will use to connect to the VMware web service.
   - ***Embedded Password [%P]***. Enter the password the platform will use to connect to the VMware web service.
   - ***Embed Value [%3]***. Do one of the following, based on the vCenter system that you want to monitor:
     - If you are monitoring a vCenter 6.x system that uses SSO for authentication, enter "https://<sso-server ip-address>/sts/STSService/vc6.local" in this field, replacing "<sso-server ip-address>" with the IP address of the SSO server used by the vCenter system.
     - If you are monitoring a vCenter 5.x system that uses SSO for authentication, enter "https://<sso-server ip-address>:7444/ims/STSService" in this field, replacing "<sso-server ip-address>" with the IP address of the SSO server used by the vCenter system.
     - If you are monitoring a vCenter 5.x system and want to use the traditional, non-SSO authentication method, do not enter a value in this field.

NOTE: In some cases, the SSO server IP address will be the same as the vCenter server.

4. Click the **[Save As]** button to save your changes as a new credential.

Chapter 3

Discovering a vCenter Server

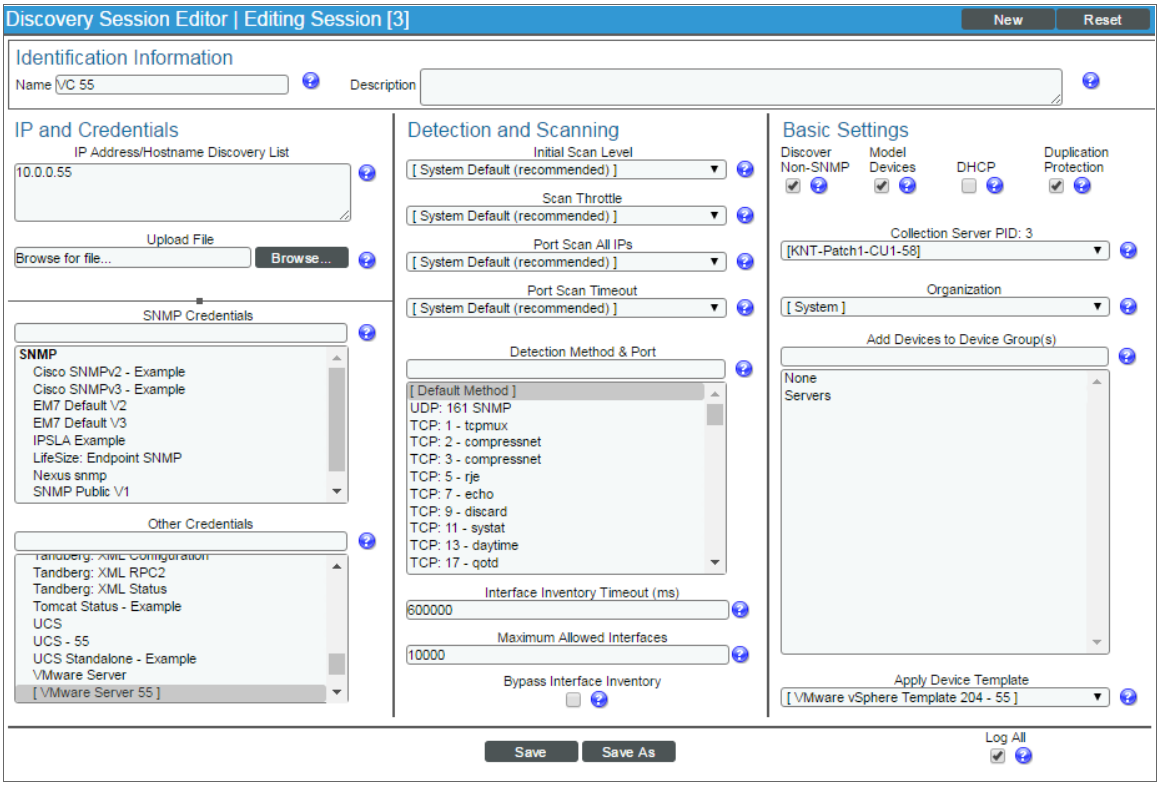
Overview

The following sections describe the steps required to discover a vCenter Server and component devices in the ScienceLogic platform:

Discovering a vCenter Server

To create and run a discovery session that will discover a vCenter server, perform the following steps:

1. Go to the **Discovery Control Panel** page (System > Manage > Discovery).
2. Click the **[Create]** button to create a new discovery session. The **Discovery Session Editor** modal page appears:



3. Enter values in the following fields:

   - ***IP Address Discovery List***. Enter the IP address for the vCenter server.
   - ***SNMP Credentials***. If the Windows server that hosts the vCenter server is SNMP-enabled, select the SNMP credential for the vCenter server in this field. If you do not select an SNMP credential in this field, you must select the ***Discover Non-SNMP*** checkbox.
   - ***Other Credentials***. If you want to discover the vCenter server using a device template, select the *SOAP/XML credential you created* in this field. If you do so, you will also need to make a selection in the ***Apply Device Template*** field. Alternatively, you can leave both of these fields blank and *manually align the necessary Dynamic Applications to the vCenter server* instead.
   - ***Discover Non-SNMP***. If the Windows server that hosts the vCenter server is not SNMP-enabled, you must select this checkbox.

- ***Apply Device Template***. If you selected a SOAP/XML credential in the ***Other Credentials*** field, then select the *VMware vSphere Template* from the drop-down list.

4. Optionally, you can enter values in the other fields on this page. For more information about the other fields on this page, see the ***Discovery & Credentials*** manual.
5. Click the **[Save]** button and then close the **Discovery Session Editor** modal page.
6. The discovery session you created will appear at the top of the **Discovery Control Panel** page. Click its lightning-bolt icon () to run the discovery session.
7. The **Discovery Session** window appears. When the vCenter server is discovered, click its device icon () to view the **Device Properties** page for the vCenter server.

Manually Aligning Dynamic Applications to a vCenter Server

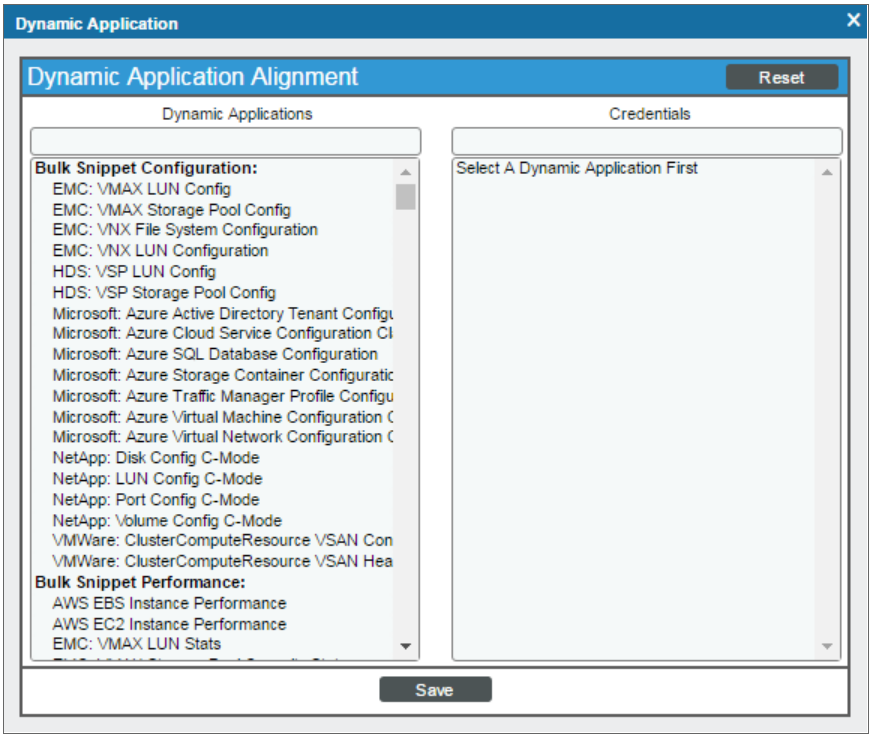
If you did not apply a device template when creating the vCenter server discovery session, then you must discover the VMware vSphere component devices by manually aligning the appropriate Dynamic Applications to the vCenter server.

To align the Dynamic Applications to a vCenter server, perform the following steps:

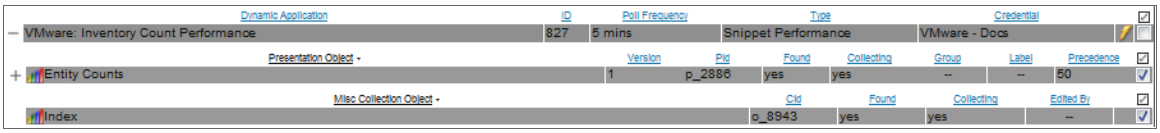
> **NOTE:** Use these steps if you want to check how many component device records will be created before starting the discovery of component devices. If you do not need to check the number of component devices, you can *align the Dynamic Applications via device template*.

1. From the **Device Properties** page (Registry > Devices > wrench icon) for the vCenter server, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.

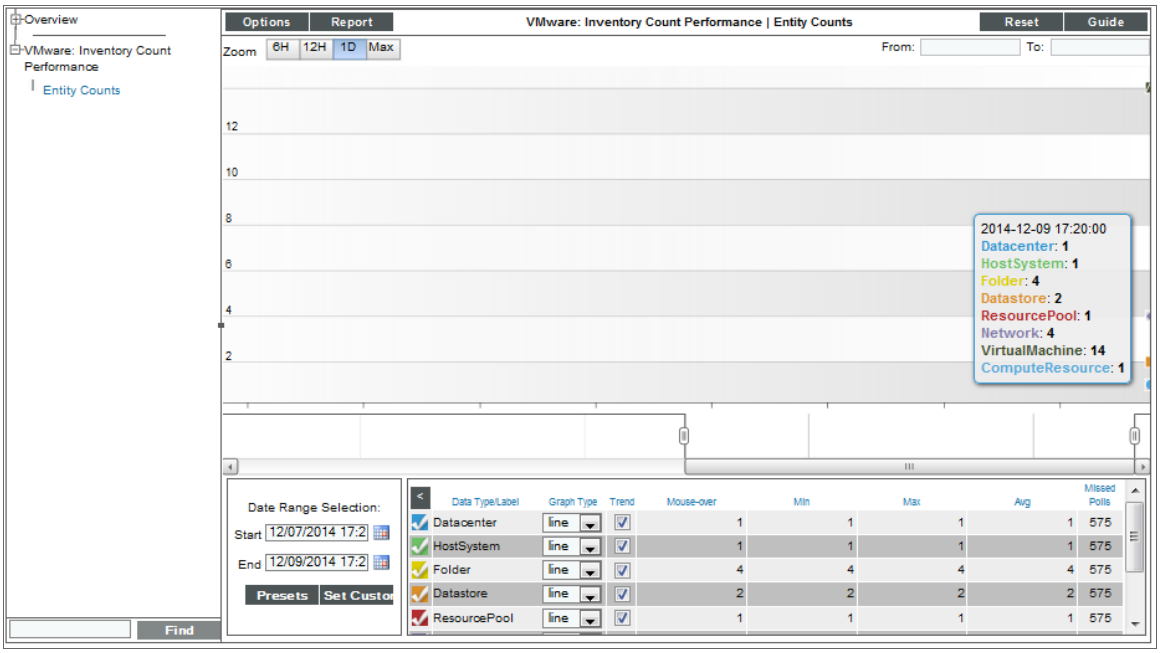
2. Click the **[Action]** button and then select *Add Dynamic Application*. The **Dynamic Application Alignment** page appears:



3. In the ***Dynamic Applications*** field, select the "VMware: Inventory Cache" Dynamic Application.
4. In the ***Credentials*** field, select the *SOAP/XML credential you created*.
5. Click the **[Save]** button.
6. Repeat steps 2–5 for the "VMware: Performance Cache" and "VMware: QuickStats Cache" Dynamic Applications.
7. If you want to check that your ScienceLogic system has enough capacity for all components managed by the vCenter server, repeat steps 2–5 for the "VMware: Inventory Count Performance" Dynamic Application.
8. After aligning the "VMware: Inventory Count Performance" Dynamic Application, click the **[Reset]** button and then click the plus icon (+) for the "VMware: Inventory Count Performance" Dynamic Application. If collection for the Dynamic Application was successful, the graph icons ( ) for the "VMware: Inventory Count Performance" Dynamic Application are enabled:



9. Click a graph icon ( ) for the "Entity Counts" presentation object to view the collected data. The **Device Performance** page will display the number of components of each type managed by the vCenter server:



10. Leave the **Dynamic Application Collections** page and the **Device Performance** page open and go to the **Appliance Manager** page (System > Settings > Appliances) in your main browser window.
11. In the **Appliance Manager** page, locate the row for the primary Database Server or All-In-One Appliance. Verify that the difference between the ***Capacity*** and ***Allocation*** values for the primary Database Server or All-In-One Appliance is greater than the total number of components displayed in the **Configuration Report** page. If the difference between the ***Capacity*** and ***Allocation*** values is less than the total number of components, the platform will not be able to discover all the components managed by the vCenter server.
12. After you have verified that your ScienceLogic system has enough capacity for all components managed by the vCenter server, repeat steps 2–5 for the following Dynamic Applications:
    - VMware: ComponentCount Configuration
    - VMware: Events
    - VMware: Inventory Cache Meta Performance
    - VMware: LicenseManager RootDevice Configuration
    - VMware: Performance Counter Lookup Configuration
    - VMware: Perf Metadata Performance
    - VMware: QuickStats Cache Meta Performance
    - VMware: RetrieveServiceContent Metadata Performance
    - VMware: RootFolder Datacenter Discovery

- VMware: RootFolder Folder Discovery

13. If you want to collect VMware events, repeat steps 2–5 for the "VMware: Events" Dynamic Application.

Aligning Dynamic Applications to a VMware Device via Device Template

If you do not need to check how many component device records will be created before starting the discovery of component devices, you can align all applicable Dynamic Applications using the VMware vSphere Template device template. To apply the VMware vSphere Template device template to a device, perform the following steps:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
2. Select the checkbox for the VMware device that you want to monitor.
3. In the ***Select Action*** drop-down list, select *Modify By Template*.
4. Click the **[Go]** button.
5. In the ***Template*** drop-down list, select *VMware vSphere Template*.
6. Click the **[Apply]** button.
7. In the confirmation page, click the **[Confirm]** button.
8. Click the wrench icon () for the VMware device.
9. Click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
10. Select the checkboxes for the following Dynamic Applications:

    - VMware: ComponentCount Configuration
    - VMware: Events
    - VMware: Inventory Cache
    - VMware: Inventory Cache Meta Performance
    - VMware: Inventory Count Performance
    - VMware: LicenseManager RootDevice Configuration
    - VMware: Performance Cache
    - VMware: Performance Counter Lookup Configuration
    - VMware: Perf Metadata Performance
    - VMware: QuickStats Cache
    - VMware: QuickStats Cache Meta Performance
    - VMware: RetrieveServiceContent Metadata Performance
    - VMware: RootFolder Datacenter Discovery
    - VMware: RootFolder Folder Discovery

11. In the ***Select Action*** drop-down list, select the *SOAP/XML credential you created*.
12. Click the **[Go]** button.
13. Perform the additional configuration steps for the *VMware: Events Dynamic Application*.

Configuring the "VMware: Events" Dynamic Application

The "VMware: Events" Dynamic Application is designed to insert all VMware events into the device log of the aligned vCenter server.

For the platform to insert VMware events into the device log, the Data Collector that monitors the vCenter server must be configured to process API events. For instructions on how to configure a Data Collector to process API events, see the ***Global Settings*** chapter in the ***System Administration*** manual.

You can configure the "VMware: Events" Dynamic Application to ignore specific types of VMware events. To do this:

1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
2. Click the wrench icon () for the "VMware: Events" Dynamic Application. The **Dynamic Applications Properties Editor** page appears.
3. Click the **[Snippets]** tab. The **Dynamic Applications Snippet Editor & Registry** page appears.
4. Click wrench icon () for the "VMware Event Collection" snippet.
5. Locate the section that looks like this:

```
event_dict = {
  "AlarmStatusChangedEvent": {"count": 0, "countAll": 0, "collect": True},
  "ClusterStatusChangedEvent": {"count": 0, "countAll": 0, "collect": True},
  "HostStatusChangedEvent": {"count": 0, "countAll": 0, "collect": True},
  "UserLoginSessionEvent": {"count": 0, "countAll": 0, "collect": True},
  "UserLogoutSessionEvent": {"count": 0, "countAll": 0, "collect": True},
  "VmEvent": {"count": 0, "countAll": 0, "collect": True},
  "VmMigratedEvent": {"count": 0, "countAll": 0, "collect": True},
  "other": {"count": 0, "countAll": 0, "collect": True},
}
```

   For each event type you want the platform to ignore, change the "collect" value to "False". For example, to disable the User Login Session Event, you would change the "UserLoginSessionEvent" line to:

```
"UserLoginSessionEvent": {"count": 0, "countAll": 0, "collect": False},
```

6. Click the **[Save]** button.

If you have edited the "VMware Events" Dynamic Application, you must remove the Dynamic Application from the *VMware: vSphere Base Pack* PowerPack. If you do not remove the Dynamic Application from the PowerPack, your changes will be overwritten the next time the PowerPack is installed.

To remove the Dynamic Application from the PowerPack:

1. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).

2. Click the wrench icon () for the *VMware: vSphere Base Pack* PowerPack. The **Editing PowerPack** window appears.
3. In the left NavBar, click **Dynamic Applications**. The **Embedded/AvailableDynamic Applications** page appears.
4. In the **Embedded Dynamic Applications** pane, click the bomb icon () for the "VMware: Events" Dynamic Application.

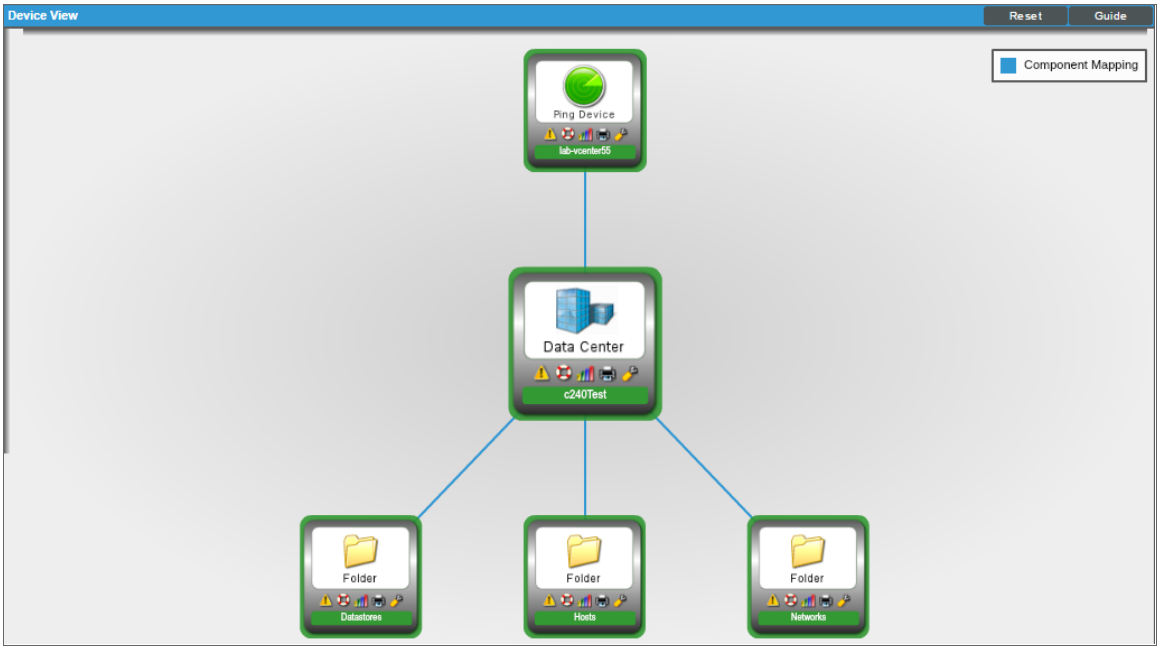
Viewing Component Devices

When the platform performs collection for the "VMware: RootFolder Datacenter Discovery" Dynamic Application, the platform will create component devices for the components managed by the vCenter server and align other Dynamic Applications to those component devices. Some of the Dynamic Applications aligned to the component devices are also used to create additional component devices. All component devices appear on the **Device Manager** page.

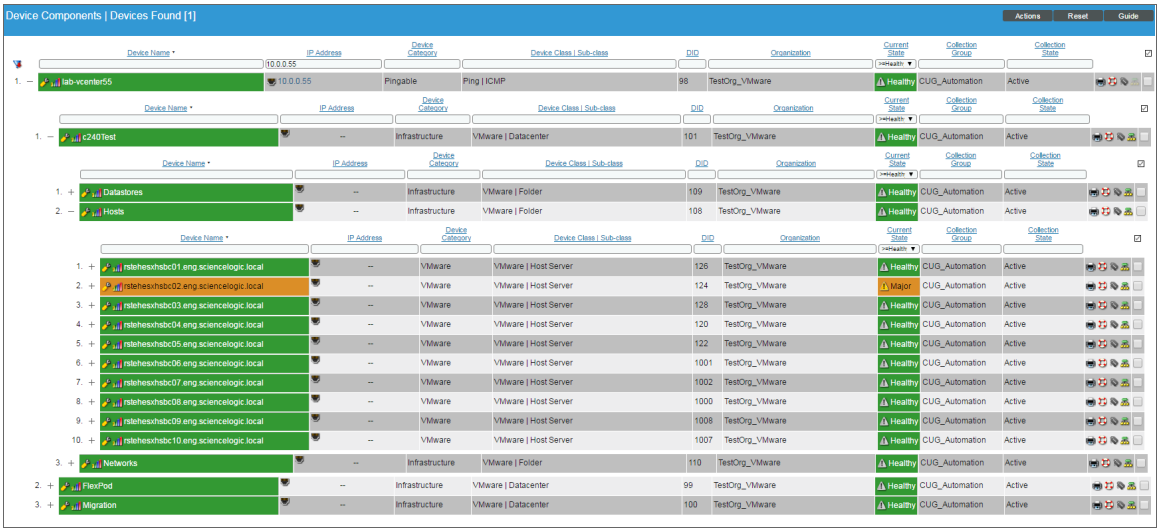
NOTE: During initial discovery, the ScienceLogic platform requests information about 200 devices per poll period until all component devices are discovered. After initial discovery, the ScienceLogic platform requests only the changes from the previously collected topology. If you have a large VMware infrastructure, it can take several collection cycles after the initial collection of the "VMware: RootFolder Datacenter Discovery" Dynamic Application for all component devices to be discovered.

In addition to the **Device Manager** page, you can view the vCenter server and all associated component devices in the following places in the user interface:

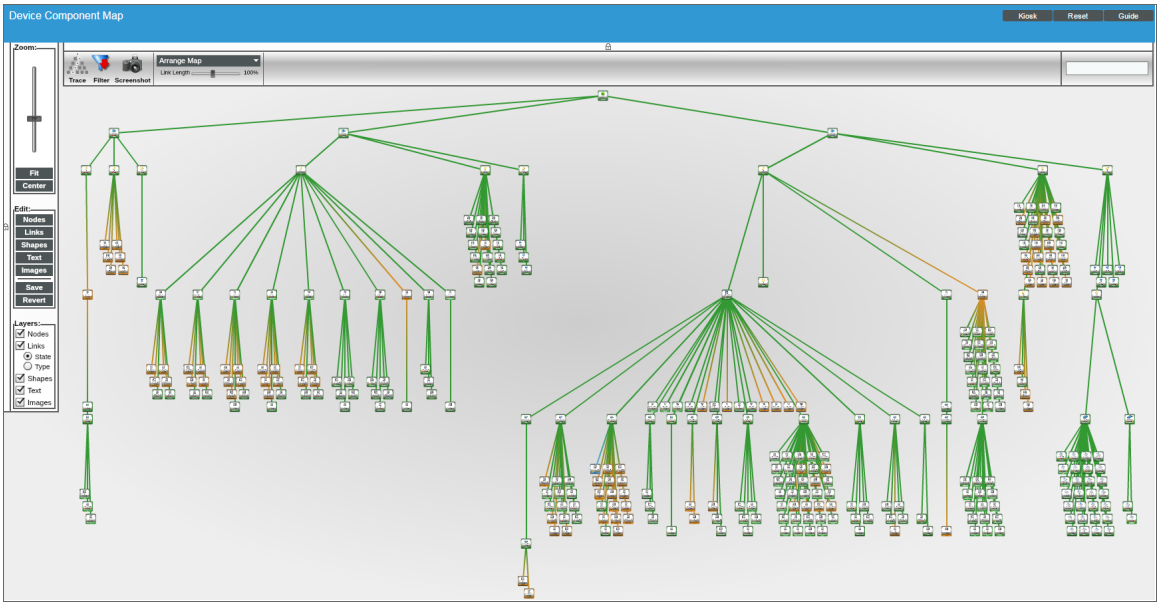
- The **Device View** modal page (click the bar-graph icon [] for a device, then click the **Topology** tab) displays a map of a particular device and all of the devices with which it has parent-child relationships. Double-clicking any of the listed devices reloads the page to make the selected device the primary device:



- The **Device Components** page (Registry > Devices > Device Components) displays a list of all root devices and component devices discovered by the platform. The **Device Components** page displays all root devices and component devices in an indented view, so you can easily view the hierarchy and relationships between child devices, parent devices, and root devices. To view the component devices associated with a vCenter server, find the vCenter server and click its plus icon (+):



- The **Component Map** page (Views > Device Maps > Components) allows you to view devices by root node and view the relationships between root nodes, parent components, and child components in a map. This makes it easy to visualize and manage root nodes and their components. The ScienceLogic platform automatically updates the **Component Map** as new component devices are discovered. The platform also updates each map with the latest status and event information. To view the map for a vCenter server, go to the **Component Map** page and select the map from the list in the left NavBar. To learn more about the **Component Map** page, see the ***Views*** manual.



Relationships with Other Types of Component Devices

In addition to the parent/child relationships between component devices, the following relationships are automatically created by the Dynamic Applications in the *VMware: vSphere Base Pack* PowerPack:

- VMware Virtual Machines and VMware Datastores
- VMware Virtual Machines and VMware Networks
- VMware Virtual Machines and Cisco Cloud Center
- VMware VirtualApps and VMware Networks
- VMware Hosts and VMware Datastores
- VMware Hosts and VMware Networks
- VMware Hosts and VMware Virtual Machines
- VMware Datastore Clusters and VMware Virtual Machines
- VMware Datastore Clusters and VMware Host Clusters
- VMware Datastore Clusters and VMware Hosts

The ScienceLogic platform can also automatically build relationships between VMware component devices and other associated devices. If you discover one or more of the following:

- An EMC VNX device using the Dynamic Applications in the *EMC: VNX* PowerPack
- A NetApp device using the Dynamic Applications in the *NetApp Base Pack* PowerPack
- A UCS device using the Dynamic Applications in the *Cisco: UCS* PowerPack

The platform automatically creates relationships between the following types of component devices, where appropriate:

- EMC VNX LUNs and VMware Datastores
- NetApp LUNs and VMware Datastores
- NetApp Volumes and VMware Datastores
- VMware Hosts and UCS Service Profiles

Determining Availability for Component Devices

The Dynamic Applications that discover the component devices managed by a vCenter server include collection objects that define the availability status of those component devices.

The following types of component devices are considered unavailable if a vCenter server reports that the power state is off:

- Compute Resource

- Host Server (i.e., ESX and ESXi Servers)
- Virtual Machine

The following types of component devices are considered unavailable if a vCenter server loses its connection to an ESXi hypervisor host server:

- Host Server
- Virtual Machine

The following types of component devices are considered unavailable if a vCenter server does not include information about those components in the appropriate response:

- Distributed Virtual Switch
- Distributed Virtual Portgroup
- Folder
- Network
- Resource Pool

The following types of component devices are considered unavailable based on other conditions:

- ***Datastore***. A datastore is considered unavailable if it is not accessible. A datastore is not accessible if no hosts have successfully mounted the datastore volume.
- ***Cluster***. A cluster is considered unavailable if no hosts are associated with the cluster or all hosts associated with the cluster are powered off.

When a VMware device is shut down, an event is created to alert the user that the device is unavailable. If you turn off VMware devices intentionally, you can suppress these availability events.

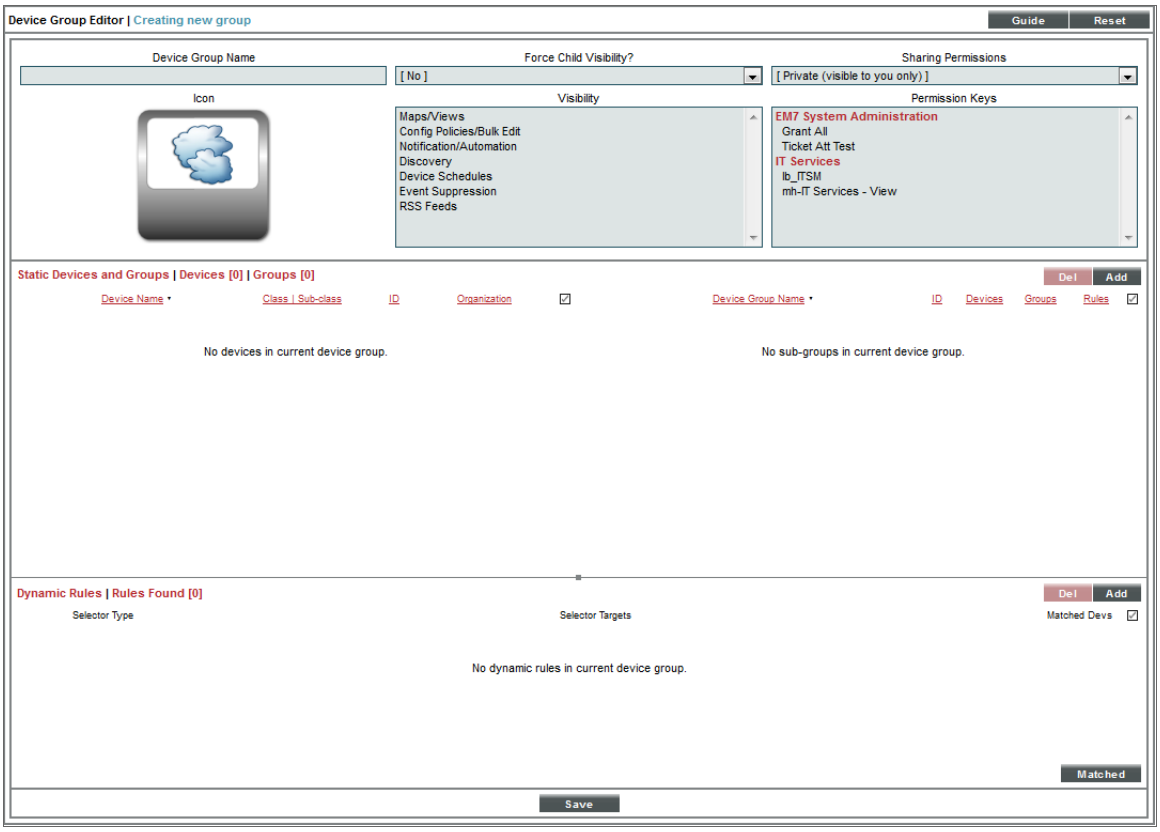
To suppress these events:

- Create a device group that contains the VMware devices for which you want to suppress availability events.
- Suppress that device group in the relevant Event Policies.

To create the device group:

1. Go to the **Device Groups** page (Registry > Devices > Device Groups).

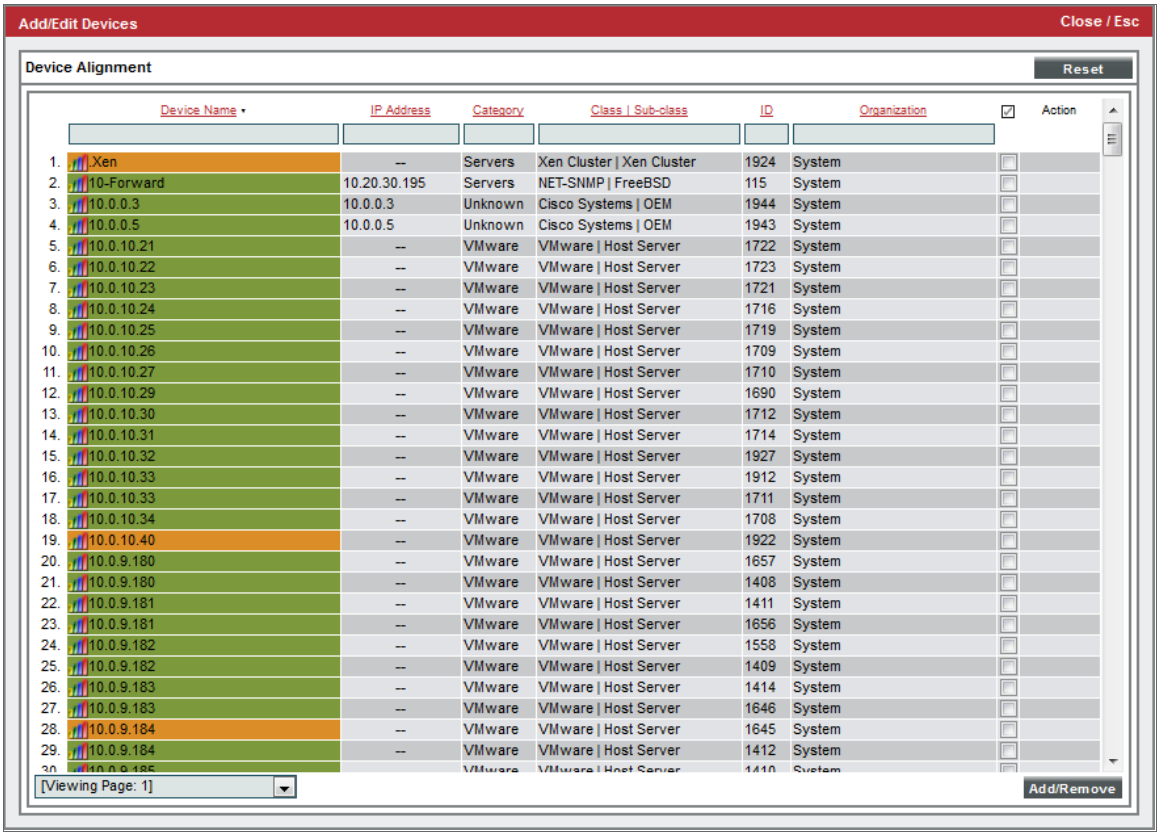
2. Click the **[Create]** button. The **Device Group Editor** page appears:



3. Enter values in the following fields:

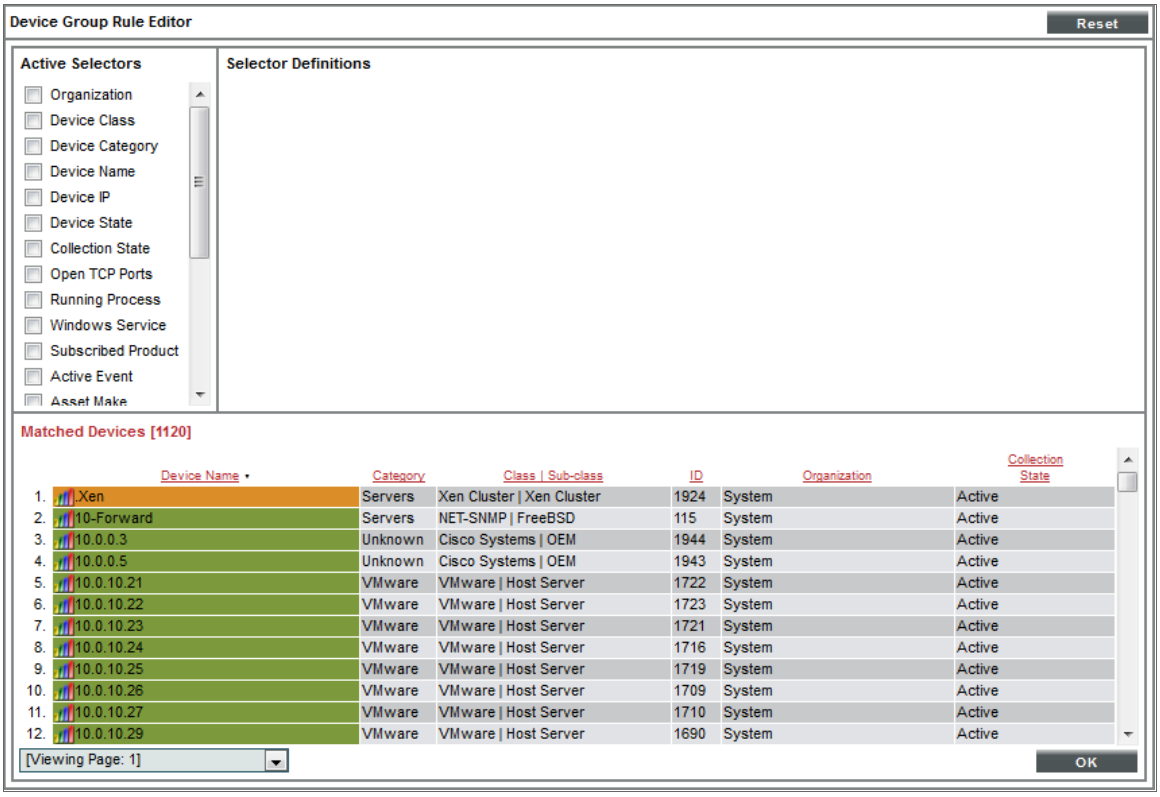
   - ***Device Group Name***. In this field you can enter a customized Device Group Name. For example, "Event Suppressed VMs".
   - ***Visibility***. Select *Event Suppression*.

4. If you want to suppress one or a few individual devices, click the **[Add]** button under the **Static Devices and Groups** pane and select *Add Devices*. The **Device Alignment** modal page appears:



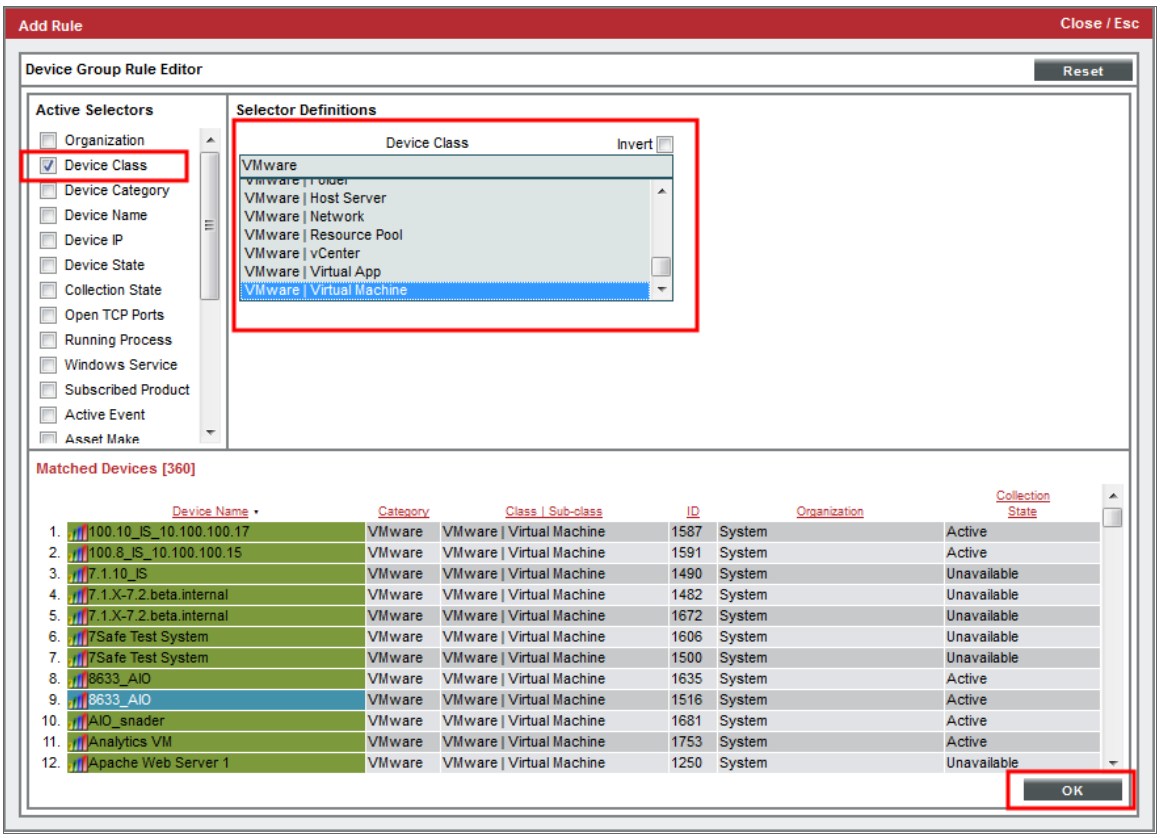
5. In the **Device Alignment** modal page, perform a search in the ***Class | Sub-class*** column for "Virtual Machine" to bring up the available VMware devices.
6. Find the device(s) for which you want to suppress availability events and select their checkbox ( ).
7. Click the **[Add/Remove]** button to add the device(s).

8. To add all VM devices to the device group, click the **[Add]** button in the **Dynamic Rules** pane of the **Device Group Editor** page. The **Device Group Rule Editor** page appears:



9. In the **Device Group Rule Editor** page, select the checkbox (☑) for ***Device Class*** in the **Active Selectors** pane.

10. In the **Selector Definitions** pane, the ***Device Class*** field appears. Perform a search for "VMware" in the ***Device Class*** field, and select *VMware | Virtual Machine*. All virtual machines will appear in the **Matched Devices** pane:

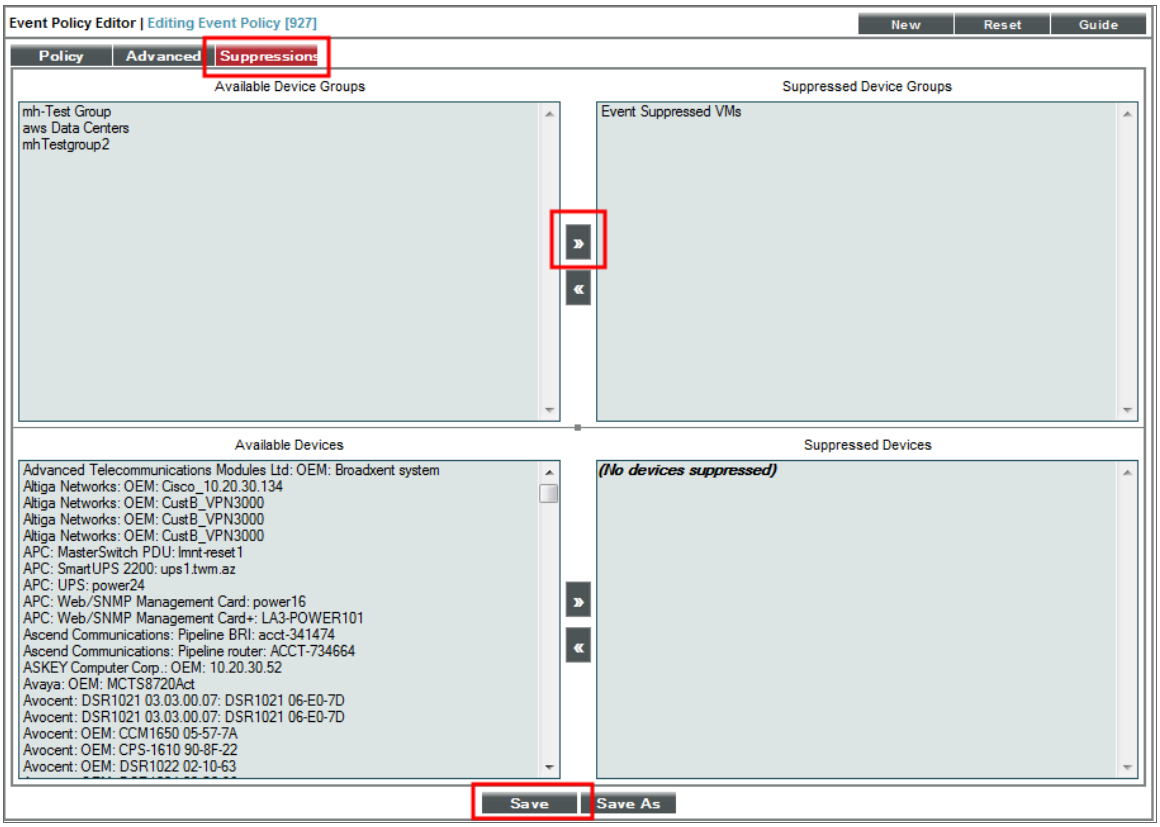


11. Click the **[OK]** button. The Device Class will appear in the **Dynamic Rules** pane.

Next, you need to suppress two Event Policies for this Device Group. To do this:

1. Go to the **Event Policy Manager** page (Registry > Events > Event Manager).
2. Perform a search in the ***Event Policy Name*** column for "Availability".

3. Click the wrench icon ( ) for the **Poller: Availability Check Failed** policy. The **Event Policy Editor** page appears:



4. Click the **[Suppressions]** tab in the **Event Policy Editor** page.
5. In the ***Available Device Groups*** field, select the device group you created. In this example, you would select *Event Suppressed VMs*.
6. Click the right arrow button, **[>>]**, and the device group moves to the ***Suppressed Device Groups*** field.
7. Click the **[Save]** button.
8. Repeat these steps for the **Poller: Availability Healthy** event policy to suppress events that will occur when a VMware device is turned back on again.

Chapter 4

VMware Dashboards

Overview

The ScienceLogic platform includes the *VMware: vSphere Dashboards* PowerPack. The *VMware: vSphere Dashboards* PowerPack contains two dashboards that display data collected from VMware systems:

- *VMware Host Performance*. Displays information about monitored ESX and ESXi host servers.
- *VMware vCenter Overview*. Displays information about guest VMs that consume the most system resources.

In addition, the *VMware: vSphere Base Pack* PowerPack includes device dashboards that provide summary information for VMware component devices. The following device dashboards in the *VMware: vSphere Base Pack* PowerPack are aligned as the default device dashboard for the equivalent device class:

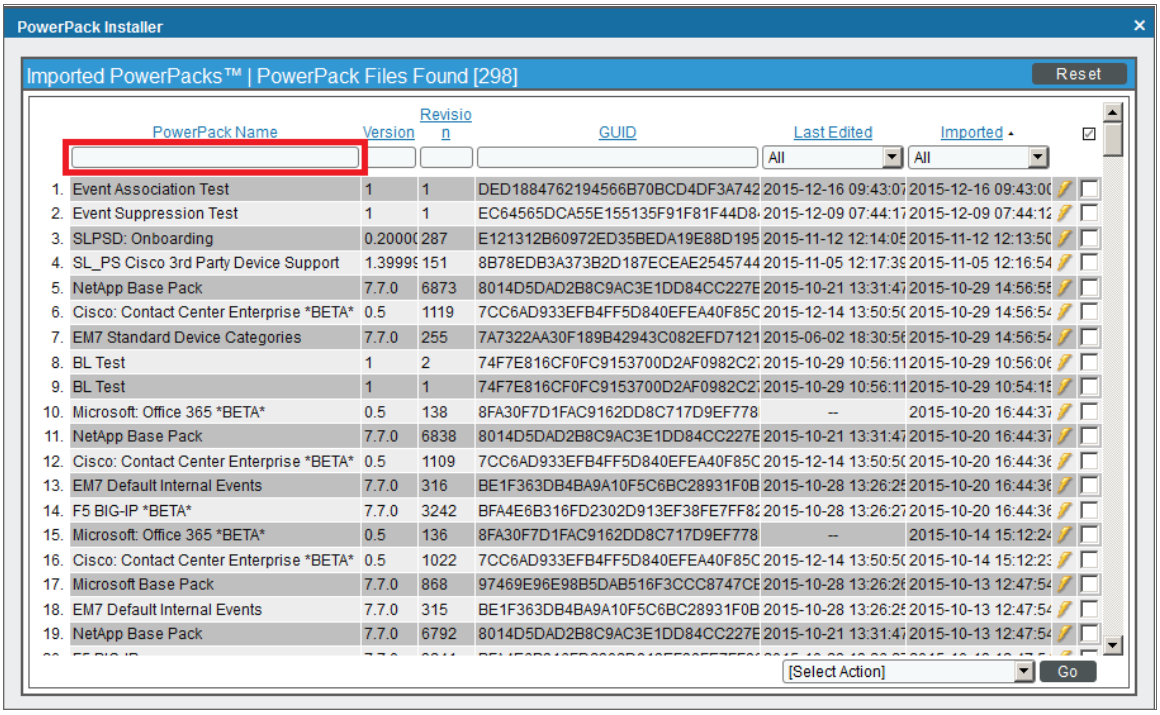
- *VMware: Cluster*
- *VMware: Datastore*
- *VMware: Datastore Cluster*
- *VMware: Host*
- *VMware: Resource Pool*
- *VMware: Virtual App*
- *VMware: Virtual Machine*

This chapter describes how to install these dashboards and includes a description of each.

Installing the VMware: vSphere Dashboards PowerPack

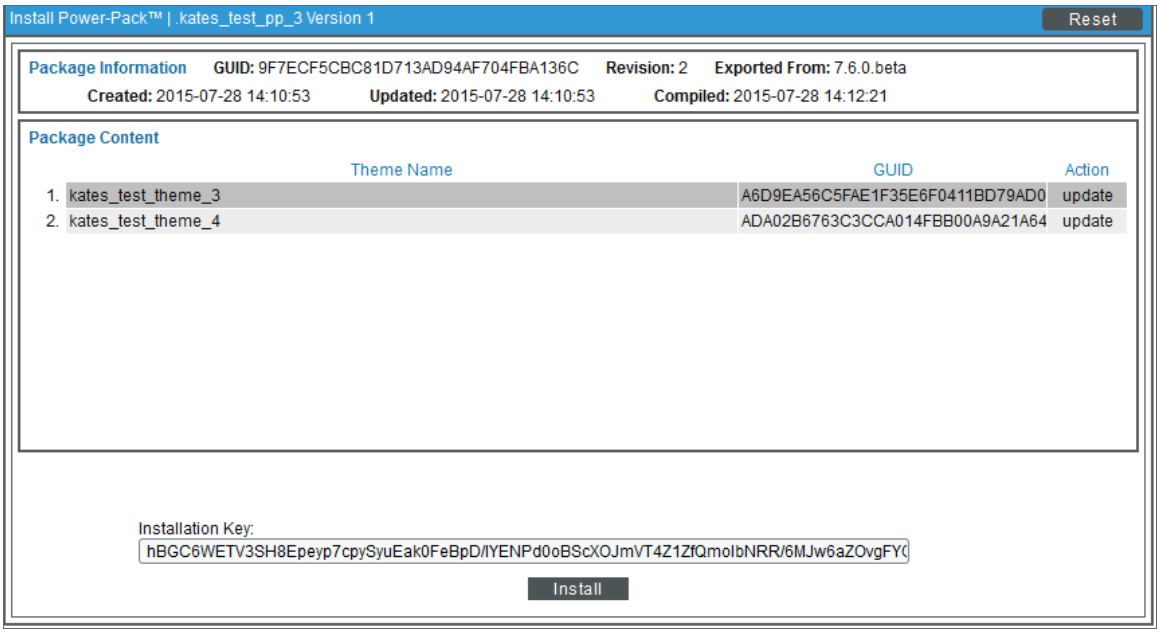
Before you can view the VMware Host Performance or VMware vCenter Overview dashboards in the ScienceLogic platform, you must first install the *VMware: vSphere Dashboards* PowerPack. To do so:

1. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).
2. Click the **[Actions]** button, then select *Install PowerPack*. The **Imported PowerPacks** modal page appears.
3. Use the search filter in the ***PowerPack Name*** column heading to locate the PowerPack you want to install. To do so, enter text to match, including special characters, and the **Imported PowerPacks** modal page displays only PowerPacks that have a matching name.



4. Click the lightning-bolt icon ( ) for the PowerPack that you want to install.

5. The **Install PowerPack** modal page appears. To install the PowerPack, click **[Install]**.

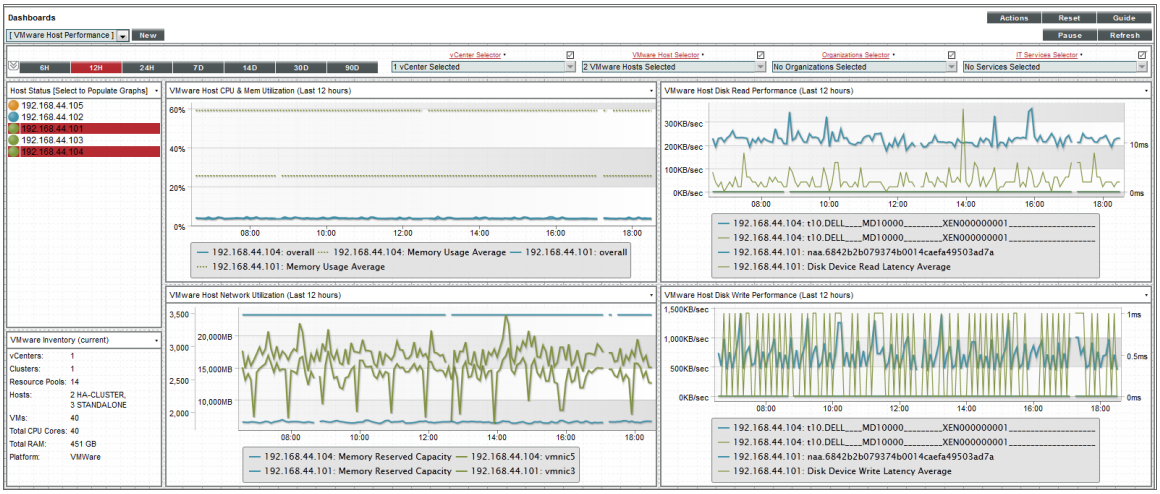


6. The PowerPack now appears in the **PowerPack Manager** page. The contents of the PowerPack are automatically installed in your ScienceLogic system.

VMware Host Performance Dashboard

The VMware Host Performance dashboard allows service providers to monitor VMware hosts and diagnose problems with those hosts. The dashboard can include data from up to four hosts in each graph. This allows users to find correlations between hosts in data drops or spikes, making it easier for users to identify and diagnose issues.

The dashboard displays the following widgets:



Context Quick Selector. This widget is located along the top of the dashboard and contains:

- *Time span presets*. Users select the time span over which they want to view data. Selections range from 6 hours to 90 days.
- *vCenter Selector*. If a user has multiple vCenters, this drop-down list allows the user to select one or several vCenters for which they want to view data.
- *Organizations Selector*. This drop-down list allows a user to select specific organizations for which they want to view data.
- *IT Services Selector*. If a user has an ITSM service (for example, for e-commerce), the IT Services Selector drop-down list allows them to select an IT service for which they want to view data.

Host Status. Displays the IP address of each VMware ESX/ESXi server and its status with a color-coded "traffic light" icon. When you select one or more VMware ESX/ESXi server, the four performance widgets are populated with data from that host server(s). The status of each host is indicated as follows:

- Critical. Host has a serious problem that requires immediate attention.
- Major. Host has a problem that requires immediate attention.
- Minor. Host has a less-serious problem.
- Notice. Host has an informational event associated with it.
- Healthy. Host is running with no problems.

> **NOTE**: More than four hosts can be selected in the ***Host Status*** widget, but the dashboard will only display data from the first four that have been selected.

VMware Inventory. This widget displays information based on the user's credentials. The widget displays inventory information about the following:

- vCenters
- Clusters
- Resource Pools
- Hosts
- VMs
- Total CPU Cores
- Total RAM
- Platform

The following four widgets measure different aspects of VMware performance. Select one or more hosts in the ***Host Status*** widget to view data in these widgets:

- ***VMware Host CPU & Memory Utilization***. Displays overall and average CPU and Memory Utilization in percent. Displays a line graph with a line each for CPU Utilization and Memory Utilitization over the time period selected in the Context Quick Selector by percent.

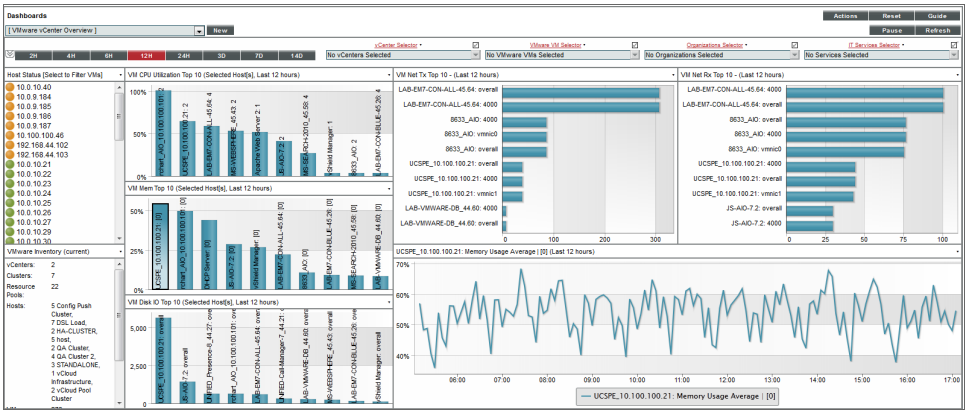
- ***VMware Host Disk Read Performance***. Displays the Disk Read Performance of the selected host in a line graph.
- ***VMware Host Network Utilization***. Displays the Network Utilization of the selected host in a line graph.
- ***VMware Host Disk Write Performance***. Displays the Disk Write Performance of the selected host in a line graph.

Each of the four performance widgets has the following features:

- The X-axis of each widget displays time selected in the Context Quick Selector by hours or days.
- For the selected VMware ESX/ESXi server, the Y-axis displays either performance or utilization by percentage or in a format that is auto-converted to the most consumable value based on the server.
- You can hide a data series by selecting the label in the legend that appears at the bottom of the widget. To show a hidden data series, select the label again.
- You can zoom in on a section of the graph by clicking, holding, and dragging your mouse across the section you want to view. If you are zoomed in on a section of the graph, you can revert to the original time span by selecting *Reset zoom* in the top-right corner of the graph.
- Hovering the cursor over a single line reveals details about specific data points. If you select a data point, the **Device Performance** page will open in a separate window with the graph for the selected metric displayed.

VMware vCenter Overview Dashboard

The VMware vCenter Overview dashboard allows users to have visibility into their VMware environment. Users can view how their VMs and hosts are performing over a given period of time. The dashboard allows diagnostics with its overlay capability. By selecting up to four hosts, the usage average of those devices and hosts can reveal correlations in spikes or drops in data, allowing the user to quickly diagnose issues.



Context Quick Selector. This widget contains the time span presets buttons, vCenter Selector, VMware VM Selector, Organizations Selector, and IT Services Selector.

- *Time span presets*. Users select the time span over which they want to view data. Selections range from 6 hours to 90 days.

- *vCenter Selector*. If a user has multiple vCenters, this drop-down list allows the user to select one or several vCenters for which they want to view data
- *VMware Host Selector*. This drop-down list allows a user to select up to four VMware Hosts for which they want to view data.
- *Organizations Selector*. This drop-down list allows a user to select specific organizations for which they want to view data
- *IT Services Selector*. If a user has an ITSM service for e-commerce, for example, the IT Services Selector drop-down list allows them to select an IT service for which they want to view data.

Host Status. Displays the IP address of each VMware server and its status with a color-coded "traffic light" icon. When one or more are selected, the graphs will be populated with data from that host server(s). The status of each host is indicated as follows:

- Critical. Host has a serious problem that requires immediate attention.
- Major. Host has a problem that requires immediate attention.
- Minor. Host has a less-serious problem.
- Notice. Host has an informational event associated with it.
- Healthy. Host is running with no problems.

> **NOTE**: More than four hosts can be selected in the ***Host Status*** widget, but the dashboard will only display data from the first four that have been selected. It is recommended that you select VMware devices from the ***VMware VM Selector*** drop-down list in the ***Quick Context Selector*** widget.

VMware Inventory. This widget displays information based on the user's credentials. The widget displays inventory information about the following:

- vCenters
- Clusters
- Resource Pools
- Hosts
- VMs
- Total CPU Cores
- Total RAM
- Platform

VM CPU Utilization. Displays the 10 guest VMs with the highest average CPU utilization over the selected time period. The widget displays a bar graph with percentage utilized as the Y-axis.

VM Memory Top 10. Displays the 10 guest VMs with the highest average memory utilization over the selected time period. The widget displays a bar graph with percentage utilized as the Y-axis.

VM Disk IO Top 10. Displays the 10 guest VMs with the highest average disk usage over the selected time period. The widget displays a bar graph with disk utilization as the Y-axis.

VM Network Transmit Top 10. Displays the 10 guest VMs with the highest average outbound network utilization over the selected time period. The widget displays a bar graph with outbound network utilization as the Y-axis.

VM Network Receive Top 10. Displays the 10 guest VMs with the highest average inbound network utilization over the selected time period. The widget displays a bar graph with inbound network utilization as the Y-axis.

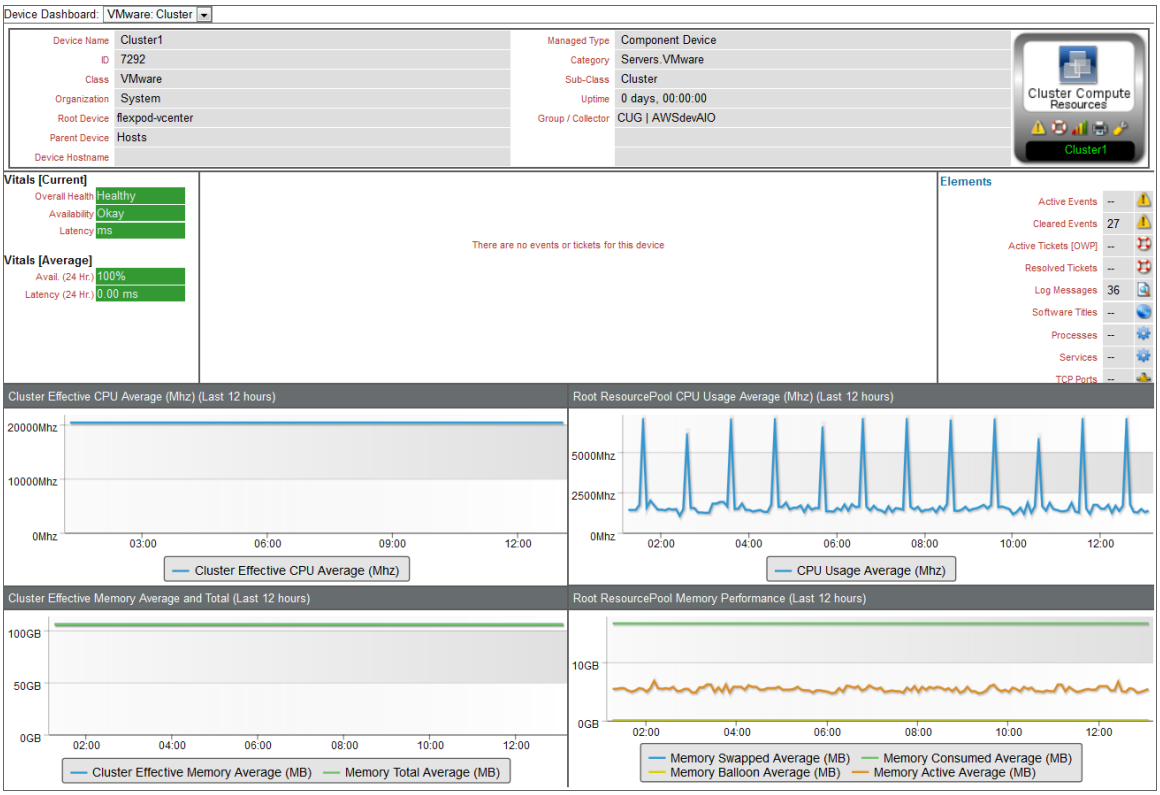
Detailed Performance Graph. The widget in the bottom-right of the dashboard displays data when a bar on any of the other graphs in this dashboard is selected. When a bar is selected, it displays the selected metric over time. You can select up to eight metrics to display in this graph by holding down the **<Ctrl>** key when you select each bar.

VMware Device Dashboards

In addition, the *VMware: vSphere Base Pack* PowerPack includes device dashboards that provide summary information for VMware component devices. The following device dashboards in the *VMware: vSphere Base Pack* PowerPack are aligned as the default device dashboard for the equivalent device class:

- *VMware: Cluster*
- *VMware: Datastore*
- *VMware: Datastore Cluster*
- *VMware: Host*
- *VMware: Resource Pool*
- *VMware: Virtual App*
- *VMware: Virtual Machine*

VMware: Cluster

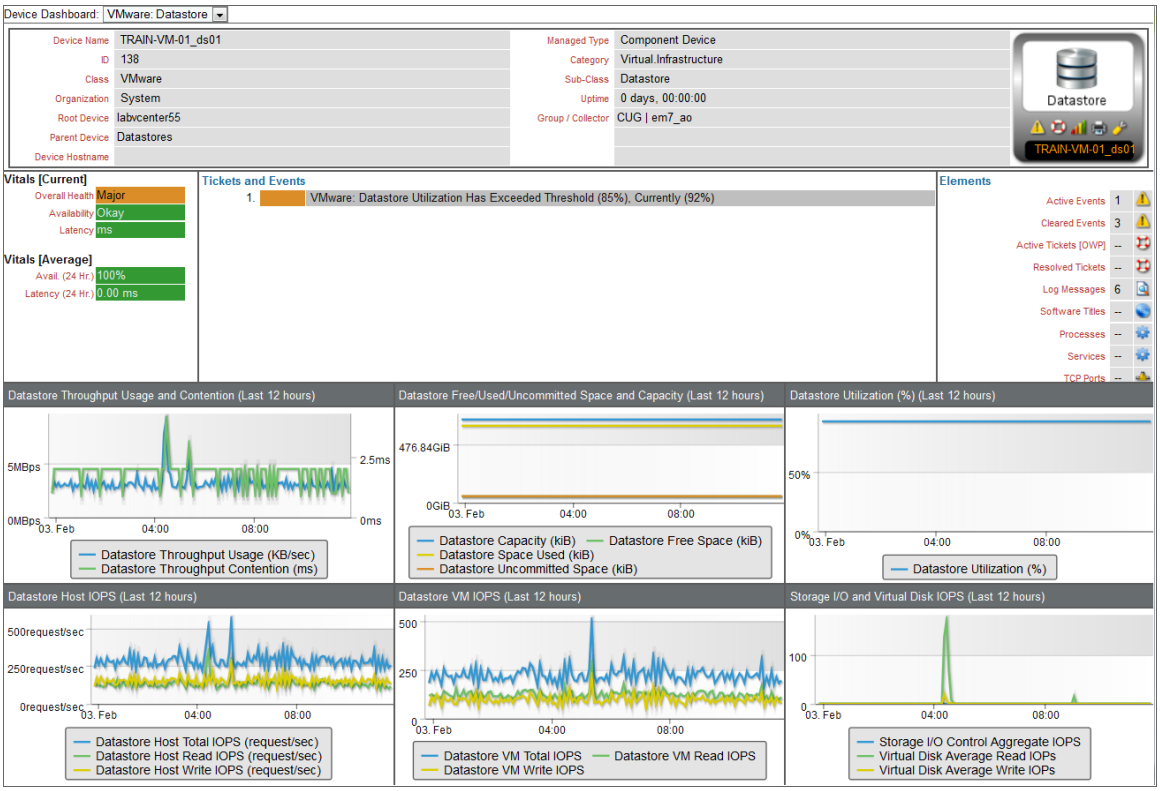


The VMware: Cluster device dashboard displays the following information:

- The basic information about the cluster
- The current health, availability, and latency for the cluster
- A list of active events and open tickets associated with the cluster
- A count of, and links to, the elements associated with the cluster
- Four instances of the Multi-series Performance Widget that display the following metrics trended over the last 12 hours:
    - Cluster Effective CPU Average
    - CPU Usage Average
    - Cluster Effective Memory Average
    - Memory Total Average
    - Memory Swapped Average
    - Memory Consumed Average

- Memory Balloon Average
- Memory Active Average

VMware: Datastore

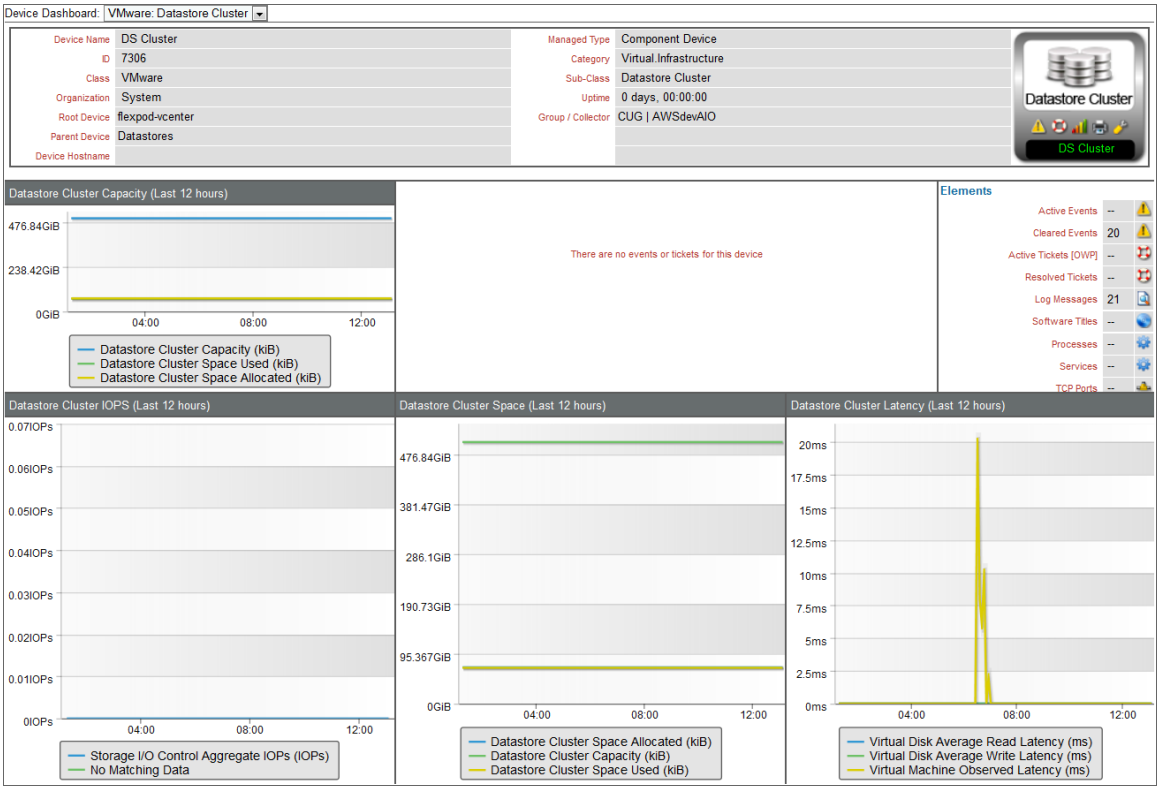


The VMware: Datastore device dashboard displays the following information:

- The basic information about the datastore
- The current health, availability, and latency for the datastore
- A list of active events and open tickets associated with the datastore
- A count of, and links to, the elements associated with the datastore
- Six instances of the Multi-series Performance Widget that display the following metrics trended over the last 12 hours:
    - Datastore Throughput Usage
    - Datastore Throughput Contention
    - Datastore Capacity
    - Datastore Free Space
    - Datastore Space Used
    - Datastore Uncommitted Space

- Datastore Utilization
- Datastore Host Total IOPS
- Datastore Host Read IOPS
- Datastore Host Write IOPS
- Datastore VM Total IOPS
- Datastore VM Read IOPS
- Datastore VM Write IOPS
- Storage I/O Control Aggregate IOPS
- Virtual Disk Average Read IOPS
- Virtual Disk Average Write IOPS

VMware: Datastore Cluster

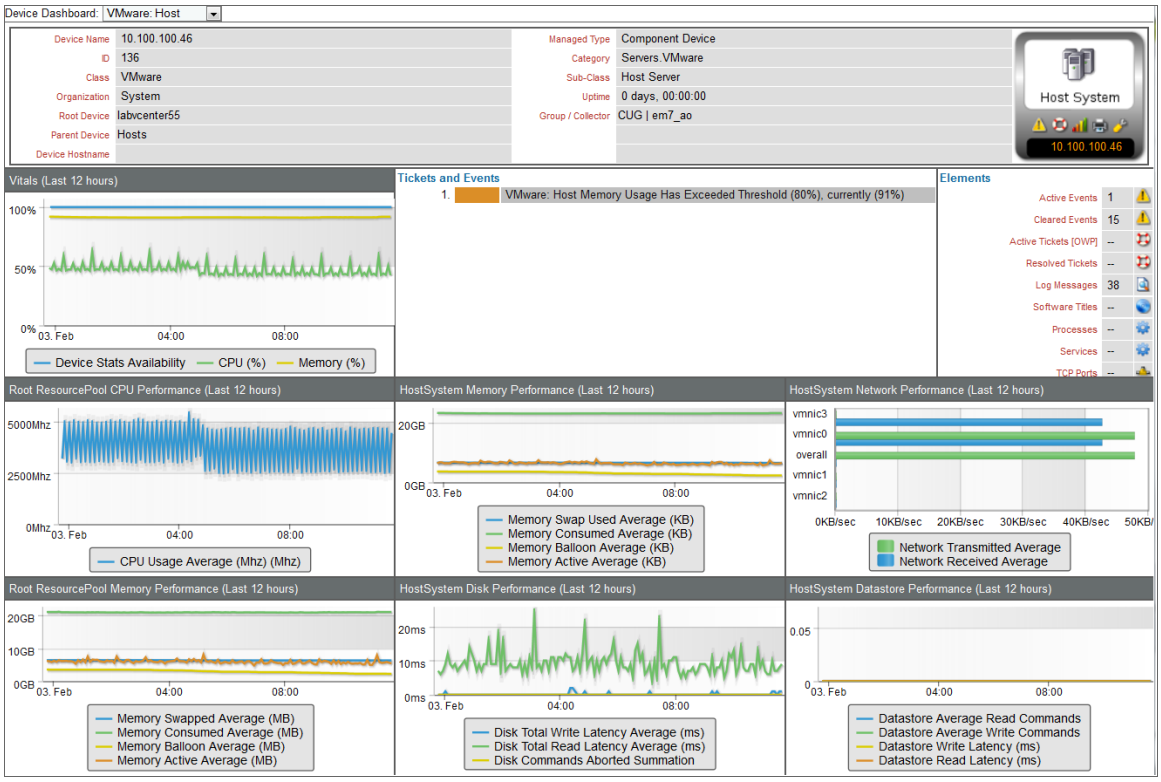


The VMware: Datastore Cluster device dashboard displays the following information:

- The basic information about the datastore cluster
- A list of active events and open tickets associated with the datastore cluster
- A count of, and links to, the elements associated with the datastore cluster

- Four instances of the Multi-series Performance Widget that display the following metrics trended over the last 12 hours:
    - Datastore Cluster Capacity
    - Datastore Cluster Space Used
    - Datastore Cluster Space Allocated
    - Storage I/O Control Aggregate IOPS
    - Virtual Disk Average Read Latency
    - Virtual Disk Average Write Latency
    - Virtual Machine Observed Latency

VMware: Host

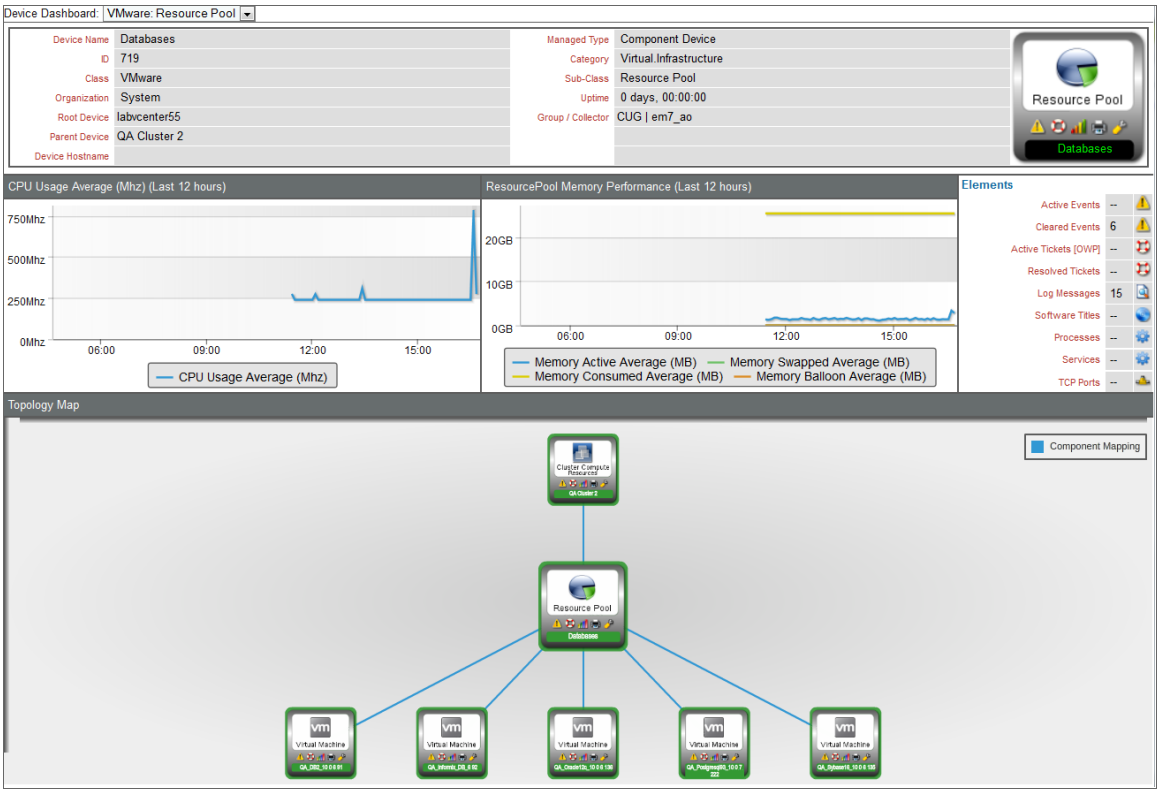


The VMware: Host device dashboard displays the following information:

- The basic information about the host
- A list of active events and open tickets associated with the host
- A count of, and links to, the elements associated with the host
- Seven instances of the Multi-series Performance Widget that display the following metrics trended over the last 12 hours:
    - Availability

- CPU (%)
- Memory (%)
- CPU Usage Average
- Memory Swap Used Average
- Memory Consumed Average
- Memory Balloon Average
- Memory Active Average
- Network Transmitted Average
- Network Received Average
- Disk Total Write Latency Average
- Disk Total Read Latency Average
- Disk Commands Aborted Summation
- Datastore Average Read Commands
- Datastore Average Write Commands
- Datastore Write Latency
- Datastore Read Latency

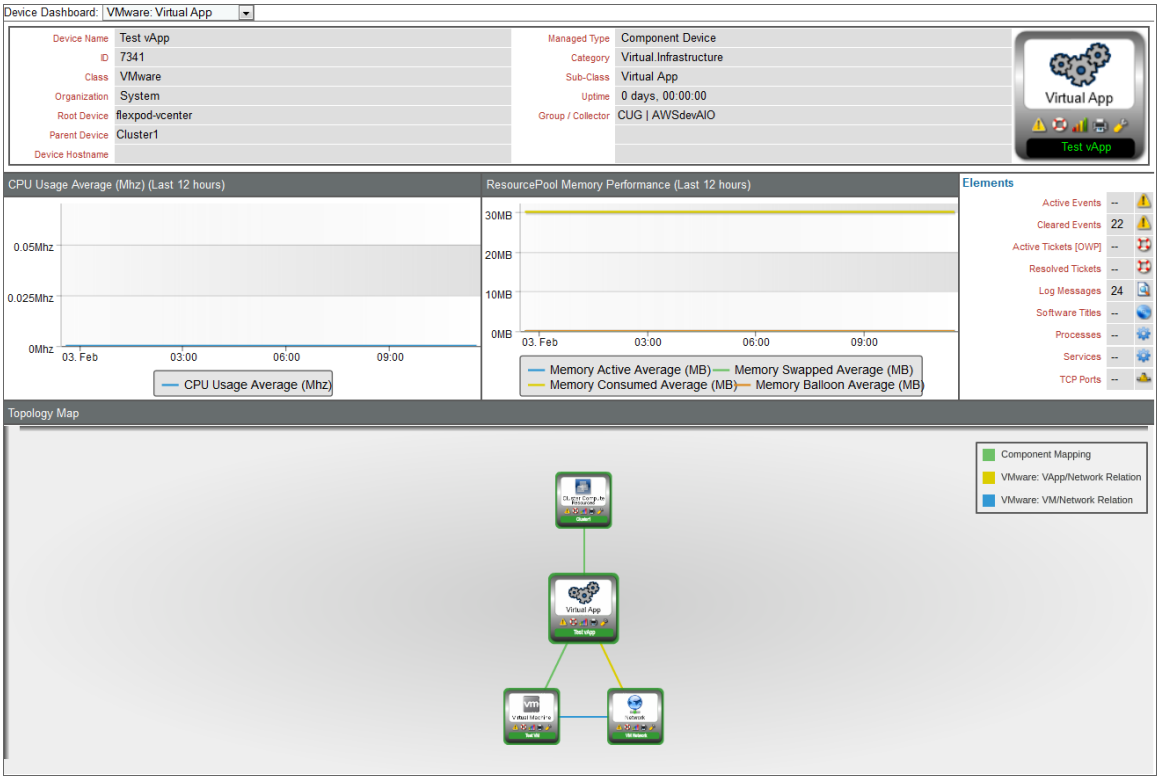
VMware: Resource Pool



The VMware: Resource Pool device dashboard displays the following information:

- The basic information about the resource pool
- A count of, and links to, the elements associated with the resource pool
- Two instances of the Multi-series Performance Widget that display the following metrics trended over the last 12 hours:
    - CPU Usage Average
    - Memory Active Average
    - Memory Swap Used Average
    - Memory Consumed Average
    - Memory Balloon Average
- A topology map that shows the devices that are directly related to the resource pool

VMware: Virtual App

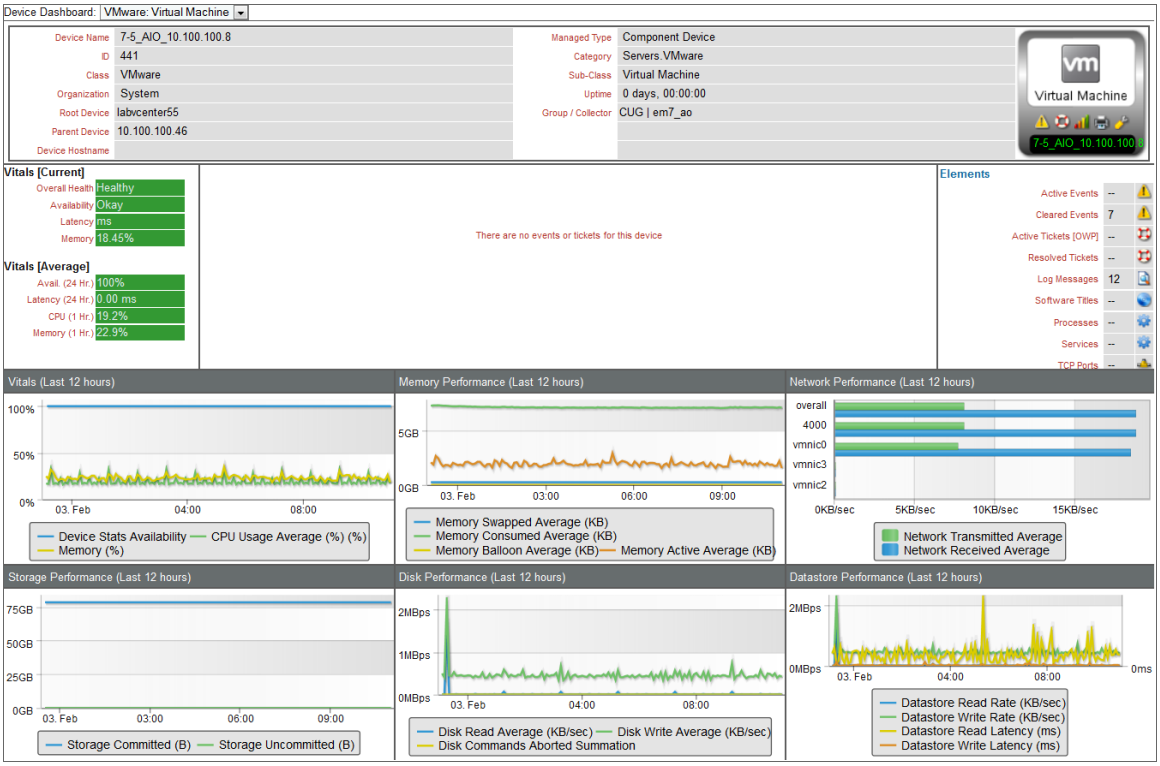


The VMware: Virtual App device dashboard displays the following information:

- The basic information about the virtual app
- A count of, and links to, the elements associated with the virtual app

- Two instances of the Multi-series Performance Widget that display the following metrics trended over the last 12 hours:
    - CPU Usage Average
    - Memory Active Average
    - Memory Swap Used Average
    - Memory Consumed Average
    - Memory Balloon Average
- A topology map that shows the devices that are directly related to the virtual app

VMware: Virtual Machine



The VMware: Virtual Machine device dashboard displays the following information:

- The basic information about the virtual machine
- The current health, availability, latency, CPU, and memory for the virtual machine
- A list of active events and open tickets associated with the virtual machine
- A count of, and links to, the elements associated with the virtual machine
- Six instances of the Multi-series Performance Widget that display the following metrics trended over the last 12 hours:
    - Availability

- CPU (%)
- Memory (%)
- Memory Swapped Average
- Memory Consumed Average
- Memory Balloon Average
- Memory Active Average
- Network Transmitted Average
- Network Received Average
- Storage Committed
- Storage Uncommitted
- Disk Read Average
- Disk Write Average
- Disk Commands Aborted Summation
- Datastore Read Rate
- Datastore Write Rate
- Datastore Read Latency
- Datastore Write Latency

Appendix

A

Configuring SNMP on ESXi 4.x and 5.x

Overview

To configure an ESXi server for communication via SNMP, you must perform the following tasks:

1. Locally, install the vSphere Command-Line Interface so you can communicate with the ESXi server.
2. On the ESXi server, assign the server at least one SNMP community.
3. On the ESXi server, configure SNMP Traps.
4. On the ESXi server, configure SNMP Polling.
5. On the ESXi server, enable the SNMP agent.

This chapter describes how to perform these tasks on

- VMware ESXi 4.x
- VMware ESXi 5.x

CAUTION: The free versions of ESXi do not support SNMP.

Installing the vSphere Command-Line Interface

The vSphere Command-Line Interface allows you to communicate with an ESXi server directly from your desktop. The vSphere Command-Line Interface allows you to open a shell session or command-line session on your desktop and communicate with an ESXi server.

NOTE: For details on the commands available with the vSphere Command-Line Interface (including details on the ***vicfg_snmp*** commands), see http://www.vmware.com/pdf/vsphere4/r40_u1/vsp_40_u1_vcli.pdf .

To download the vSphere Command-Line Interface, go to the following page: http://www.vmware.com/support/developer/vcli/ .

- The **Downloads** link at the top of the page allows you to download the vSphere Command-Line Interface.
- The **Documentation** links at the bottom of the page allow you to read instructions on downloading and installing vSphere Command-Line Interface.

Assigning an SNMP Community

To use SNMP on an ESXi server, you must configure at least one community for the SNMP agent on that server.

An SNMP community defines a group of devices and management systems. Only devices and management systems that are members of the same community can exchange SNMP messages. A device or management system can be a member of multiple communities.

NOTE: In the ScienceLogic platform, the SNMP community is called the ***community string*** and is used in credentials for SNMP v1 and SNMP v2 to authenticate communication with the ESXi server.

To define a community for the ESXi server, open a shell session or a command line session and enter the following at the command prompt:

```
vicfg-snmp.pl --server <hostname or IP address of the ESXi server> --username <your username on the ESXi server> --password <your password on the ESXi server> -c <one or more communities to assign to the ESXi server>
```

For example:

```
vicfg-snmp.pl --server 192.168.10.10 --username root --password esxadmin -c public,servers
```

This example:

- connects to the ESXi server at 192.168.10.10
- connects as user "root" with password "esxadmin". This is the account name and password for the ESXi server.
- assigns the ESXi server to two communities: public and servers

Configuring SNMP Traps

Traps are unsolicited messages that are sent to the ScienceLogic platform from a device that the platform is monitoring. Before an EXSi server can send traps to the platform, you must tell the ESXi server where to send traps and assign the ScienceLogic appliance to the same community as the ESXi server.

To do this, open a shell session or a command line session and enter the following at the command prompt:

```
vicfg-snmp.pl --server <hostname or IP address of the ESXi server> --username <your username on the ESXi server> --password <your password on the ESXi server> -t <hostname or IP address of an EM7 All-In-One Appliance, Data Collector, or Message Collector>@<port>/<community>.
```

For example:

```
vicfg-snmp.pl --server 192.168.10.10 --username root --password esxadmin -t 192.168.9.100@162/public
```

This example:

- connects to the ESXi server at 192.168.10.10
- connects as user "root" with password "esxadmin". This is the account name and password for the ESXi server.
- tells the ESXi server to send traps to 192.168.9.100, to the port 162. The All-In-One Appliance, Data Collector, or Message Collector is assigned the community "public".

Configuring SNMP Polling

You must configure the SNMP agent on an ESXi server to listen for communications from the platform. The platform will retrieve data from the ESXi server by sending SNMP GET requests (also known as "polling").

To configure an ESXi server for polling, open a shell session or a command line session and enter the following at the command prompt:

```
vicfg-snmp.pl --server <hostname or IP address of the ESXi server> --username <your username on the ESXi server> --password <your password on the ESXi server> -p <port for incoming SNMP GET requests>
```

For example:

```
vicfg-snmp.pl --server 192.168.10.10 --username root --password esxadmin -p 161
```

This example:

- connects to the ESXi server at 192.168.10.10
- connects as user "root" with password "esxadmin". This is the account name and password for the ESXi server.

- tells the ESXi server to use port 161 to listen for SNMP GET requests from the platform. Port 161 is the default port.

Enabling the SNMP Agent

The SNMP agent on each ESXi server provides the platform with information in response to the SNMP GET requests sent by the platform. By default, the SNMP agent on each ESXi server is disabled. You must enable the SNMP agent on the ESXi server before the platform can retrieve information from the ESXi server.

To enable the SNMP agent on the ESXi server, open a shell session or a command line session and enter the following at the command prompt:

```
vicfg-snmp.pl --server <hostname or IP address of the ESXi server> --username <your username on the ESXi server> --password <your password on the ESXi server> --enable
```

For example:

```
vicfg-snmp.pl --server 192.168.10.10 --username root --password esxadmin --enable
```

This example:

- connects to the ESXi server at 192.168.10.10
- connects as user "root" with password "esxadmin". This is the account name and password for the ESXi server.
- starts the SNMP agent on the ESXi server

Testing Traps

The vSphere Command-Line Interface includes a command for testing traps. You can use this command to send a test trap from the ESXi server to the platform.

To do this:

1. In the platform, discover the ESXi server. When creating a credential for the ESXi server, use the **community** specified earlier in this chapter. For details on discovering a device in the ScienceLogic platform, see the ***Discovery and Credentials*** manual.
2. After the ESXi server has been successfully discovered in the platform, go to your desktop. Don't exit the user interface session.
3. Open a shell session or a command-line session. At the prompt, enter the following:

   ```
   vicfg-snmp.pl --server <hostname or IP address of the ESXi server> --username <your username on the ESXi server> --password <your password on the ESXi server> --test
   ```

   For example:

   ```
   vicfg-snmp.pl --server 192.168.10.10 --username root --password esxadmin --test
   ```

This example:

- connects to the ESXi server at 192.168.10.10
- connects as user "root" with password "esxadmin". This is the account name and password for the ESXi server.
- sends a "test" trap, specifically a "warmstart" trap. The platform will receive this trap and store it in the device log for the ESXi server.

NOTE: The --test option sends a "warmstart" trap.

6. In the user interface, go to the **Device Manager** page (Registry > Devices > Device Manager) and find the ESXi server. Click its wrench icon ().
7. Click the **[Logs]** tab. In the **Device Logs & Messages** page, you should see the "warmstart" trap message.

Appendix

B

Configuring SNMP on ESX 4.x

Overview

The configuration steps in the Configuring SNMP on ESXi 4.x & 5.x appendix can be used to configure SNMP on an ESX 4.x server; however, to allow the platform access to the largest amount of data, ScienceLogic recommends you use the configuration described in this chapter. VMware ESX 4.x servers have two SNMP agents available:

- ***UCD-SNMP***. Reports information on interfaces, file systems, memory, and other components common to networked devices.
- ***VMware***. Reports information specific to VMware ESX servers, such as configuration of Guest VMs.

Configuring SNMP Polling & SNMP Traps

The following configuration will allow both agents to run simultaneously. All SNMP requests on the standard port, 161, will be handled by the UCD-SNMP agent. If the UCD-SNMP agent receives a request for an OID in the VMware enterprise tree (.1.3.6.1.4.1.6876), it will act as a proxy to the VMware agent running on port 171. To configure both agents to run together, perform the following steps:

1. Log in to the ESX 4.x server as root at the console or using SSH.
2. Open /etc/vmware/snmp.xml using your preferred text editor. ESX 4.x servers have nano and vi installed.
3. Edit the values contained in the following XML tags:
    - ***<communities>***. Enter the community string for the VMware agent. You can enter multiple community strings, separated by commas.
    - ***<enable>***. Enter "true".
    - ***<port>***. Enter "171".

- ***<targets>***. Enter the IP address of the ScienceLogic appliance that handles traps for your ScienceLogic system (either an All-In-One Appliance, Message Collector, or Data Collector), followed by "@162", a space, then the community string to use for SNMP traps. For example:

  ```
  192.168.9.100@162 public
  ```

  This tells the ESX server to send traps to 192.168.9.100, to the port 162 using the community string "public".

4. Save your changes to the snmp.xml file and exit the text editor.
5. Issue the following command to stop the UCD-SNMP agent:

   ```
   service snmpd stop
   ```

6. Open /etc/snmp/snmpd.conf using your preferred text editor.

> **NOTE:** These instructions provide a basic configuration using a single community string, v1- and v2c-only authentication, and access to the entire MIB tree used by the UCD-SNMP and VMware agents. You might want to make further changes to this file based on the security policies for your enterprise. The snmpd.conf file used by the UCD-SNMP agent uses syntax common to most linux-based systems.

7. Enter the community string at the end of the *com2sec notConfigUser default* line. For example:

   ```
   com2sec notConfigUser default public
   ```

   Specifies the community string "public".

8. Add the following line to the *view* section of the file:

   ```
   view systemview included .1
   ```

9. Add the following line to the end of the file, replacing *community-string* with one of the community strings you specified in the ***<communities>*** tag in the snmp.xml file:

   ```
   proxy -v 1 -c community-string 127.0.0.1:171 .1.3.6.1.4.1.6876
   ```

10. Save your changes to the snmpd.conf file and exit the text editor.
11. Issue the following two commands to restart the VMware and UCD-SNMP agents:

    ```
    service mgmt-vmware restart
    service snmpd restart
    ```

12. To ensure that the UCD-SNMP agent starts when the ESX server is rebooted, issue the following command:

    ```
    chkconfig --add snmpd
    ```

13. To ensure the ESX server firewall allows SNMP requests, issue the following command:

    ```
    esxcfg-firewall -e snmpd
    ```

14. To test that your settings are correct, issue the following command, replacing *community-string* with the community string you entered in the snmpd.conf file:

    ```
    snmpwalk -v 2c -c community-string localhost .1.3.6.1.4.1.6876 | grep 6876.1
    ```

    If the settings are configured correctly, the UCD-SNMP agent will respond with three lines: "VMware ESX", the ESX version number, and the build number the ESX server is running.

Testing Traps

You can test that the ESX server is correctly configured to send traps by restarting the mgmt-vmware service. Restarting this service will make the ESX server send a "warmstart" trap.

To do this:

1. In the platform, discover the ESX server. When creating a credential for the ESX server, use the **community string** specified earlier in this chapter. For details on discovering a device in the ScienceLogic platform, see the ***Discovery and Credentials*** manual.
2. After the ESX server has been successfully discovered in the platform, issue the following command from the console of the ESX server:

    ```
    service mgmt-vmware restart
    ```

3. In the user interface, go to the **Device Manager** page (Registry > Devices > Device Manager) and find the ESX server. Click its wrench icon ().
4. Click the **[Logs]** tab. In the **Device Logs & Messages** page, you should see the "warmstart" trap message.

© 2003 - 2018, ScienceLogic, Inc.

All rights reserved.

LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

ALL INFORMATION AVAILABLE IN THIS GUIDE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. SCIENCELOGIC™ AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.

Although ScienceLogic™ has attempted to provide accurate information on this Site, information on this Site may contain inadvertent technical inaccuracies or typographical errors, and ScienceLogic™ assumes no responsibility for the accuracy of the information. Information may be changed or updated without notice. ScienceLogic™ may also make improvements and / or changes in the products or services described in this Site at any time without notice.

Copyrights and Trademarks

ScienceLogic, the ScienceLogic logo, and EM7 are trademarks of ScienceLogic, Inc. in the United States, other countries, or both.

Below is a list of trademarks and service marks that should be credited to ScienceLogic, Inc. The ® and ™ symbols reflect the trademark registration status in the U.S. Patent and Trademark Office and may not be appropriate for materials to be distributed outside the United States.

- ScienceLogic™
- EM7™ and em7™
- Simplify IT™
- Dynamic Application™
- Relational Infrastructure Management™

The absence of a product or service name, slogan or logo from this list does not constitute a waiver of ScienceLogic's trademark or other intellectual property rights concerning that name, slogan, or logo.

Please note that laws concerning use of trademarks or product names vary by country. Always consult a local attorney for additional guidance.

Other

If any provision of this agreement shall be unlawful, void, or for any reason unenforceable, then that provision shall be deemed severable from this agreement and shall not affect the validity and enforceability of any remaining provisions. This is the entire agreement between the parties relating to the matters contained herein.

In the U.S. and other jurisdictions, trademark owners have a duty to police the use of their marks. Therefore, if you become aware of any improper use of ScienceLogic Trademarks, including infringement or counterfeiting by third parties, report them to Science Logic's legal department immediately. Report as much detail as possible about the misuse, including the name of the party, contact information, and copies or photographs of the potential misuse to: legal@sciencelogic.com

800-SCI-LOGIC (1-800-724-5644)

International: +1-703-354-1010