VMware Monitoring in Foglight® Evolve Cloud 5.8.2

User and Reference Guide

owners.

Legend

■   **WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.**

❗   **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

ℹ️   **IMPORTANT NOTE**, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.

Contents

Using VMware Monitoring in Foglight Evolve Cloud

This chapter introduces you to the VMware® virtual infrastructure and provides you with essential foundational information.

For more detailed information about VMware virtualization products and solutions, consult the appropriate VMware documentation.

- Introducing the virtual infrastructure
- Navigation basics
- Interacting with VMware Monitoring in Foglight Evolve Cloud
- VMware Performance Agent configuration

Introducing the virtual infrastructure

VMware® vSphere® provides an innovative mechanism for organizing and viewing any virtual infrastructure built on its platform. Using a unique combination of physical and logical components, this mechanism effectively and efficiently fulfills the VMware vision of the modern virtual infrastructure.

VMware Monitoring in Foglight® Evolve Cloud accommodates customers of all sizes that leverage the VMware virtualization platform by examining and enhancing eminently knowledgeable VMware view of the virtual world.

The following figure highlights the components or objects that make up a typical vSphere implementation. The figure makes a clear distinction between objects that exist in the physical world and those that are considered to be virtual.

Figure 1. VMware vCenter Server infrastructure
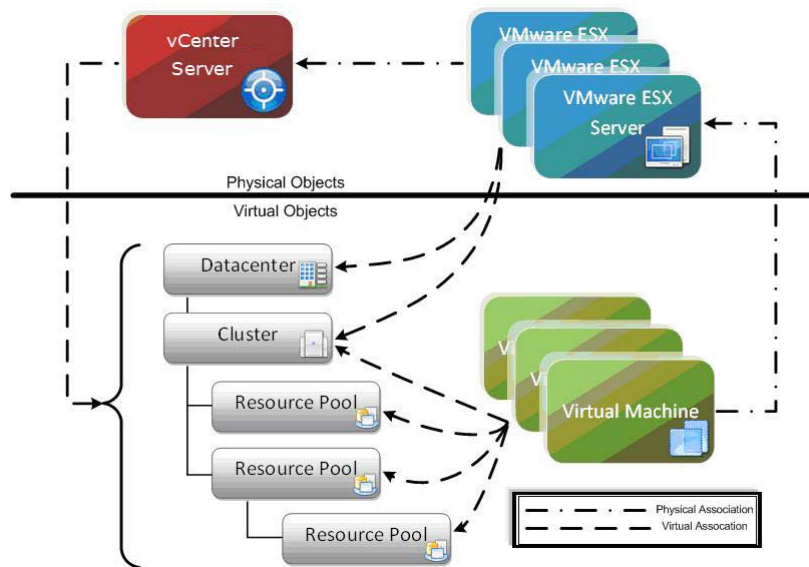
VMware vCenter® allows for the configuration of a hierarchical organizational structure that resides primarily within the virtual domain. This enables an organization to easily configure physical VMware ESX® Servers and virtual machines to reside in logical groups that dictate the various aspects of the virtual infrastructure (like physical object location, resource allocations and limitations for virtual machines, and high availability settings for physical and virtual components).

Object roles

Before we get too far into discussing the layout and capabilities of VMware Monitoring in Foglight® Evolve Cloud, we must understand the different roles the various physical and virtual objects play within the overall virtual infrastructure.

The vCenter® Server and VMware® ESX® Servers provide the physical foundation for the vSphere® infrastructure.

Virtual machines on the other hand are classified as virtual components for the purpose of management and monitoring, even though they have many of the same characteristics (like direct network and storage access) as physical systems. At any given time, a virtual machine must be contained within a single VMware ESX Server. The particular ESX Server in which a given virtual machine is contained may change of course over the lifetime of the virtual machine through the use of unique VMware technologies such as VMware vSphere® vMotion® or VMware vSphere® High Availability (VMware HA).

Physical objects

The physical objects within the VMware® virtual infrastructure are those with which you can physically interact. The virtual components or objects that make up the virtual environment cannot exist without the presence of underlying physical components.

A VMware ESX® Server is an example of a physical component.

To have VMware Monitoring in Foglight® Evolve Cloud monitor a virtual infrastructure, the virtual infrastructure must consist of at least one vCenter Server that is used to manage the virtual infrastructure and at least one ESX Server that is used to run virtual machines.

> **i** | **NOTE:** Each ESX Server that is used to run virtual machines must have its own managing vCenter Agent installed on it.

ESX Server Hosts

An ESX Server Host is the single physical component required to begin building a virtual infrastructure. An ESX Server provides a hypervisor based architecture for controlling and managing resources for the virtual machines that run on it. The virtual machines running on the host share the resources it provides. Should resources become over-committed, the ESX Server hypervisor determines which virtual machines have priority access to the shared resources (based on manual virtual machine configurations) and distributes the available resources accordingly.

Each ESX Server is managed by a single vCenter Server instance, and can be configured to exist logically within either a datacenter or cluster virtual object within the overall virtual infrastructure.

VMware vCenter Server

Although a vCenter Server can technically exist as a virtual machine, it is considered a physical component within the VMware virtual infrastructure.

VMware vCenter is the software tool used to manage virtual environments that are built on the VMware virtualization platform. vCenter creates a hierarchical structure of virtual objects that enables a system administrator to logically lay out his virtual infrastructure configuration. vCenter also introduces other advanced VMware functionality such as Distributed Resource Scheduling (DRS), VMotion, and High Availability (HA) that can be used to enhance the benefits of a virtual infrastructure.

vCenter provides a robust WSDL that VMware Monitoring in Foglight Evolve Cloud leverages to capture and manipulate key characteristics and performance metrics of the various object types and objects found within the virtual infrastructure configuration. Each vCenter instance that is to be monitored using this product must have a VMware Performance Agent configured for it that points to the Web service interface. As mentioned in the *Managing Storage in Virtual Environments Installation and Configuration Guide*, this agent can be installed on the vCenter Server itself because all of the required components for the proper operation of the agent come pre-configured.

A single vCenter Server can monitor approximately 100 VMware ESX Servers and 1500 virtual machines before performance and scalability challenges demand the introduction of a second vCenter Server. Multiple vCenter instances can be disbursed geographically to localize the management of large, distributed vSphere implementations.

Virtual objects

Virtual objects can exist only within the confines of the virtual infrastructure. With the exception of virtual machines, virtual objects are logical and are used for organizing VMware ESX Servers and virtual machines, either geographically or by function. In addition, virtual objects allow for the advanced configuration of resource management and of high availability settings.

Virtual machines

The creation and subsequent use of virtual machines is the primary purpose for building and maintaining a virtual infrastructure. Virtual machines share many of the characteristics of physical systems (like storage and network interaction), but they do not have direct access to the hardware that is used to process their information and they are considered virtual components within the virtual infrastructure.

A virtual machine encompasses more than just a guest operating system like Microsoft Windows. A virtual machine also contains specific configurations that help to define it, such as the number of processors and the amount of memory it can leverage.

All of the resource utilization for a particular virtual machine on a VMware ESX Server is scheduled through that Server's hypervisor. The efficient tracking and analysis of this scheduling of resources at both the virtual machine and the ESX Server Host level is a key function provided by VMware Monitoring in Foglight Evolve Cloud.

At any given time a virtual machine must reside on a single VMware ESX Server, but it can be moved across physical ESX Servers, typically without downtime, through the use of key vCenter functionality called VMotion. VMotion provides a method for proactively moving a virtual machine from one ESX Server to another while avoiding the downtime that can arise from having to perform actions like patching a physical host server. VMotion also provides a manual method a system administrator can use to better balance virtual machine workloads based on resource utilization trends.

VMware Monitoring in Foglight Evolve Cloud also provides a mechanism that tracks the life cycle of the virtual machines within the virtual infrastructure. This enables you to quickly and easily view a history of a virtual machine's performance metrics and a history of its logical location within the virtual infrastructure.

VMware vCenter offers some additional valuable features that customers may wish to use including the VMware Distributed Resource Scheduling (DRS) feature for automating the process of balancing VMware ESX Server utilization and the VMware High Availability (HA) feature for recovering from host failure within a cluster.

Datacenters

A datacenter is the topmost virtual object within a vCenter Server implementation and is required before any VMware ESX Server Hosts can be added to a vCenter. A datacenter is most commonly used to identify the physical boundaries within which an ESX Server Host can exist. In most implementations these boundaries constitute a single physical location that contains a large number of ESX Server Hosts. There is no hard and fast rule stating that a datacenter must exist entirely at just one physical location, but other datacenter implementations are atypical of most virtual infrastructures.

Within the boundaries of a datacenter, objects of the same type cannot have the same name. For example, it is not possible to configure two ESX Server Hosts with the same name to reside within the same datacenter. The same goes for virtual machines, clusters, resource pools and any other objects that can be created and configured to reside within a datacenter. Objects of the same type can have identical names as long as they are located in different datacenters.

Datastores

The management of datastores is carried out at the both the datacenter and the ESX Server levels.

Each datastore is contained within a datacenter and must be uniquely named within its containing datacenter.

A datastore represents a storage location for virtual machine files. The storage location can be a local file system path, a Virtual Machine File System Storage (VMFS) volume, or a Network Attached Storage directory.

ESX Server Hosts can be configured to mount a set of network drives (or datastores). For each storage location within a datacenter there is only one datastore, so multiple hosts may be configured to point to the same datastore. Whenever an ESX Server Host accesses a virtual machine or file within a datacenter it must use the appropriate datastore path.

Each datastore object keeps a record of ESX Server Hosts that have mounted it, and a datastore object can be removed only if no hosts are currently mounting that datastore.

Datastores are host-independent and platform-independent. Therefore, they do not change in any way when the virtual machines contained within them are moved from one ESX Server to another.

VSAN datastores

Virtual SAN (VSAN) is a software component running on the ESXi hypervisor. It collects storage resources associated with a cluster and creates a storage pool that is accessible to all hosts on the cluster. When Virtual SAN is enabled on a cluster, a VSAN datastore is created in your environment. VSAN datastores are collections of storage elements that are available to the hosts.

Clusters

A cluster object is a group of VMware ESX Servers that share common storage resources and network configurations. A cluster represents a pool of the combined resources of all of the ESX Server Hosts assigned to the cluster. For example, if four ESX Servers are added to a cluster and each ESX Server has 2x2 GHz processors with 4 GB of memory, the cluster represents a pool of 16 GHz of CPU processing power and 16 GB of memory that is available for use by virtual machines.

A cluster also serves as the boundary for virtual machine migration activity through the VMware vMotion or VMware HA features. When using either of these technologies for virtual machine migration it is critical that the participating ESX Server Hosts have identical storage resource and network configurations, and this is guaranteed within a cluster by the very definition of a cluster.

vApp

A vApp is a group of virtual machines that can be managed as a single object. vApps simplify management of complex, multi-tiered applications that run on multiple interdependent virtual machines. vApps have the same basic operations as virtual machines and resource pools. With vApps, you can set the order in which the virtual machines in the vApp power on, automatically assign IP addresses to virtual machines in the vApp, and provide application level customization.

vApps offer:

- Container for multiple virtual machines.

- Resource controls for the VMs inside the container.

- Network configurations contained inside.

- Portability of the vApp such that everything can be contained and transferred to another virtual infrastructure.

- Entire vApps can be powered on, powered off, suspended, or shutdown.

- Entire vApps can be cloned.

Resource pools

Resource pools enable an administrator to fine tune resource allocations within a cluster. A resource pool can be configured to leverage a portion of the overall available resources within a cluster and then virtual machines can be assigned to that resource pool. This enables an administrator to prioritize virtual machines—to either limit or guarantee certain resources to a particular virtual machine or group of virtual machines.

Resource pools can be configured in many ways, from simple to complex. For a simple example, two resource pools are configured within a cluster; one is named Production Virtual Machines and the other is named Development Virtual Machines. The Production resource pool is configured with a "High" share priority and the Development resource pool is configured with the default "Normal" share priority. In this case any virtual machine residing in the Production resource pool is automatically given twice the priority, in terms of access to system resources during periods of contention, of any virtual machine residing in the Development resource pool.

To better demonstrates the true potential of using resource pools, the following is an advanced example. Four ESX Servers are added to a cluster and each ESX Server has 2x2 GHz processors with 4 GB of memory. The cluster therefore represents a pool of 16 GHz of CPU processing power and 16 GB of memory that is available for use by virtual machines. The figure below illustrates that the Production Cluster resource that resides in the Chicago datacenter has 16 GHz of processing power and 16 GB of memory. A resource pool is created for a CRM Application that has access to 8 GHz of the cluster's total CPU resources and 6 GB of the cluster's total memory. By drilling down further from there you see that within the CRM Application resource pool there are two more resource pools (Database and Web). The existence of the Database resource pool ensures that key database virtual machines have access to the resources necessary to perform their highly transactional operations. The web servers have access to a smaller portion of the overall resources—just enough to provide the necessary end-user responsiveness from a web transaction perspective without impacting the key backend database infrastructure.

Figure 2. Resource pool example
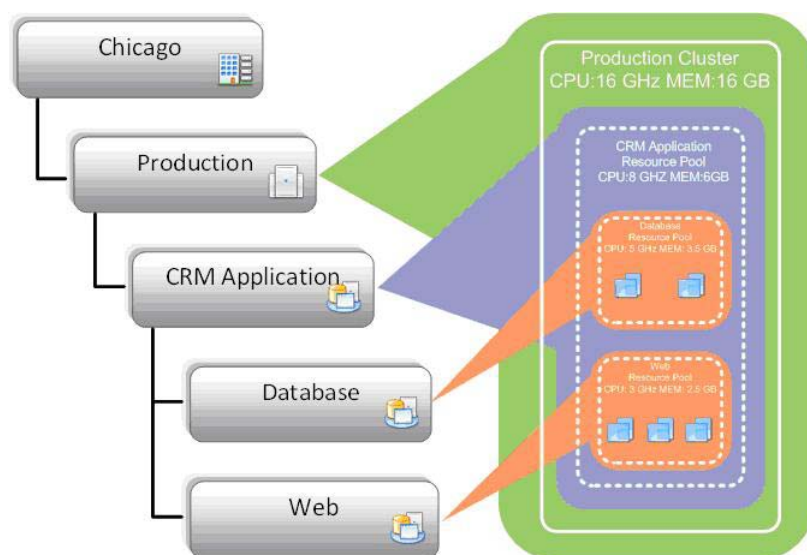
To assist with the understanding of these nested relationships of virtualized objects, VMware Monitoring in Foglight Evolve Cloud provides both a Topological and a Hierarchical view of the entire virtual infrastructure as well as resource pool mapping functionality for maximum flexibility in tracking advanced virtual infrastructure configurations.

Virtual switches

Your VMware environment uses virtual switches to distribute network traffic. A stand-alone ESX host typically uses a *standard virtual switch* to manage network traffic to and from virtual machines running on that host. *Distributed virtual switches* manage configuration of proxy switches, enabling communication between a virtual machine using the distributed switch and any of these components:

• any other virtual machines on any ESX hosts that use the same distributed switch

• virtual machines that use a standard virtual switch

• remote systems on a physical network connected to the same ESX host

In addition to standard and distributed virtual switches, your monitored environment may also include one or more *Cisco virtual switches*. A Cisco virtual switch is a third-party distributed virtual switch that manages network traffic between virtual machines and other components in your integrated virtual infrastructure. For more information about virtual switches, see your VMware documentation.

Folders

Folders are hierarchical components that exist within a vCenter and they enable an administrator to more easily organize the virtual environment for manageability. There are three different types of folders that can exist within the various layers of the virtual infrastructure hierarchy.

The following table lists the available types of folders, and explains the levels at which they can exist and the objects they can contain.

Table 1. Folder Types

Folder Type	Level at Which It Can Exist	Objects It Can Contain
Datacenter	vCenter Root	Datacenters
Virtual Machine	Datacenter	Virtual Machines and Templates
Compute Resources	Datacenter	Hosts and Clusters

Folders may contain nested folders of the same type, but not of other types. It is not possible, for example, to create a virtual machine folder within a datacenter folder.

Folders are provided strictly for organizational and management purposes. They offer a way for an administrator to classify objects that is not tied to (and therefore bound by) the virtual/physical relationship framework. For example, two datacenter folders are created at a vCenter root; one folder is labeled Primary Datacenters and the other is labeled Disaster Recovery Datacenters. An administrator can configure multiple primary datacenters containing production ESX Servers, place those datacenters in the Primary Datacenters folder, and then assign the necessary permissions to that folder to allow standard users to perform management tasks for the entire primary virtual infrastructure. The administrator can then configure multiple disaster recovery datacenters containing disaster recovery ESX Servers, place those datacenters in the Disaster Recovery Datacenters folder, and assign a different set of permissions to that folder. This prevents standard users from building virtual machines that may take over resources that are necessarily dedicated to HA-configured disaster failover virtual infrastructure components.

Using VMware Monitoring in Foglight Evolve Cloud, you can observe either a Topology view that does not use folders and presents a logical breakdown of the virtual infrastructure by component, or a Hierarchy view that uses folders and presents the familiar interface that is found within the vCenter management server.

Navigation basics

This section describes the basic VMware Monitoring in Foglight® Evolve Cloud navigation techniques necessary for using VMware Monitoring in Foglight Evolve Cloud.

For information about navigation in the browser interface, see Interacting with VMware Monitoring in Foglight Evolve Cloud on page 15.

VMware Monitoring in Foglight Evolve Cloud browser interface elements

Depending on your user roles, you may see either the contents of the first bookmark (the Welcome page is the default) listed under Bookmarks, or a home page. For further details, see the *Foglight Evolve Cloud User Guide*.

Typically, the browser interface is divided into three panels: the navigation panel on the left, the display area in the middle, and the action panel on the right.

Figure 3. VMware Monitoring in Foglight Evolve Cloud Browser Interface
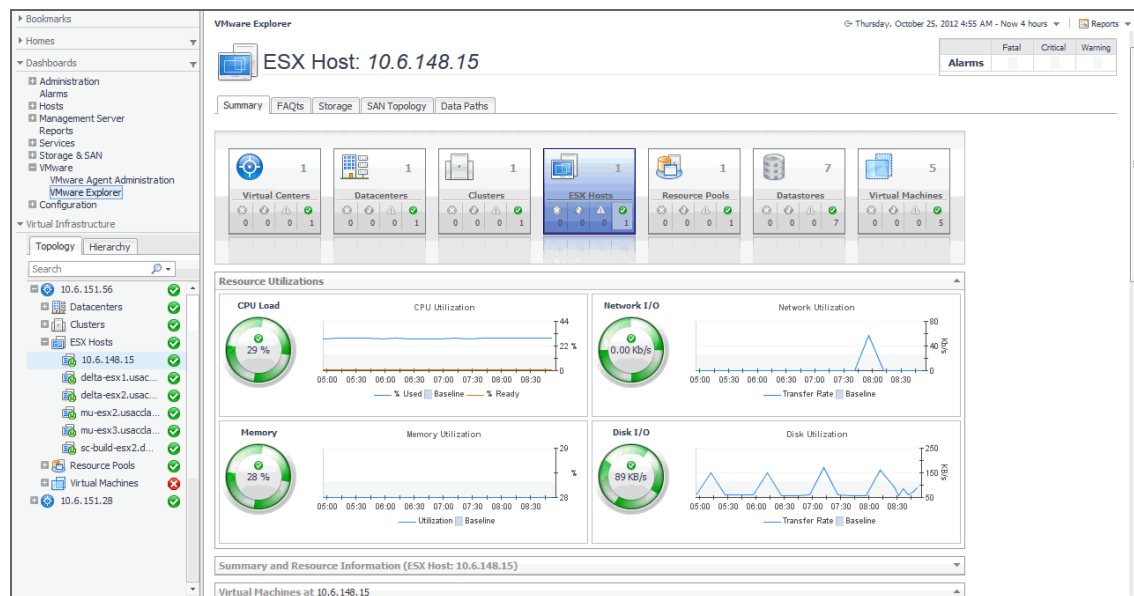
Navigation panel

The navigation panel operates like a drawer. Its default state is open. To close the navigation panel, click the arrow at the far left of the VMware Monitoring in Foglight Evolve Cloud browser interface. Click that arrow again to open the navigation panel.

The navigation panel lists all of the dashboards that are available to the current user for viewing. You can use the navigation panel to select a dashboard to view in the display area. To access a specific dashboard, open the appropriate module (the Virtual module, for example).

The navigation panel also provides access to the VMware Monitoring in Foglight Evolve Cloud Administration and Configuration areas, and may provide access to some product-specific navigational views (for example, the Virtual Infrastructure view for the VMware Explorer dashboard).

If you do not see any dashboards in the navigation panel, the user id with which you signed in may not have been assigned to a group. For details, see the *VMware Monitoring in Foglight Evolve Cloud User Help*.

Display area

The display area is used to view current dashboards and reports, as well as to create new dashboards and reports. You can increase the size of this area by resizing the navigation panel, or, if the action panel is open, by closing the action panel.

Action panel

The action panel operates like a drawer. Its default state is closed. To open the action panel, click the arrow at the far right of the VMware Monitoring in Foglight Evolve Cloud browser interface. Click that arrow again to close the action panel.

The action panel contains the various actions and tasks you can perform with the current dashboard. It also contains views and data that you can add to a dashboard or report you are creating and provides access to the online help files.

Breadcrumbs

If you drill down into various levels across dashboards within VMware Monitoring in Foglight® Evolve Cloud, a trail of breadcrumbs is left at the top of the current dashboard. This trail provides you with context. It also provides you with the name of the level you are currently viewing and with a simple mechanism for returning to any of its related parent levels.

The following breadcrumb trail was created while drilling down from the Virtual Environment Summary dashboard into the VMware Explorer dashboard. Each item within a breadcrumb trail is a hyper link to a previously viewed parent level.

Figure 4. Breadcrumb trail

| 土 VMware Environment > **VMware Explor** |

For more specific information about the Virtual Environment Summary dashboard or the VMware Explorer dashboard, see .

Time Range

The default behavior of VMware Monitoring in Foglight® Evolve Cloud is to display metrics, alerts, and messages that have occurred within the last four hours. This time range, however, is configurable.

To configure the Time Range, use the Time Range popup, which you can access from the upper right corner of the VMware Monitoring in Foglight Evolve Cloud browser interface.

Figure 5. Time Range popup
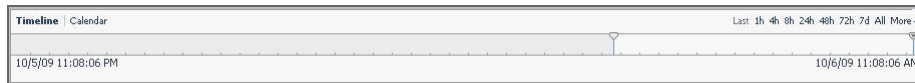
Using the Time Range popup, you can select from predefined time ranges or you can specify a custom range using either a sliding time bar or calendar precision controls to specify dates and times. When you modify the time range for a dashboard or view, it adjusts the range for all of the views contained within and drill-downs accessed from that dashboard or view. It does not adjust the time range for any parent views.

For more information about modifying the time range, see the *Foglight Evolve Cloud User Guide.*

Sortable lists

In certain VMware Monitoring in Foglight® Evolve Cloud dashboards, some levels of views contain sortable lists. An example of this is the VMware Explorer dashboard Related Objects view displayed below.

Figure 6. Sortable lists

It is possible to sort this list by column using any of the column headings. Click a column heading once to sort the list in ascending order. The list is redrawn according to your specification. Click the column heading again to re-sort the list in descending order.

This is handy when you want to have an organized view of virtual machines or host objects sorted by name, status, or some other criterion.

Alarms and their status indicators

VMware Monitoring in Foglight® Evolve Cloud uses status indicators to show the alarm states of the objects within the virtual infrastructure. Four status indicators (fatal, critical, warning, and normal), similar to those displayed in the following image, are used throughout the VMware Monitoring in Foglight Evolve Cloud dashboards.

Figure 7. Alarm indicators
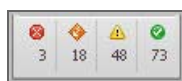
The VMware Monitoring in Foglight Evolve Cloud alarm types respond to thresholds that are defined within the VMware Monitoring in Foglight Evolve Cloud rules. As metrics change and move through thresholds, alarms are raised. As a metric moves through thresholds, the severity of an alarm changes, which causes the associated status indicator to change.

For detailed information about the rules included with the product, see Rules on page 84.

It is important to note that any events that trigger an alarm for an object do not trigger an alarm for any of the object's parents. For example, a single virtual machine running at a high CPU utilization does not trigger an alarm for its parent ESX® Server. An alarm would only be triggered for the parent ESX Server if the server itself was running at a high CPU utilization.

Mouse-over actions

Many items within the VMware Monitoring in Foglight® Evolve Cloud dashboards display additional information when you hover the cursor over them. For example, when you hover the cursor over a graph you are likely to see a specific value or values that correspond) to the position of the cursor. When you hover the cursor over an individual metric, you are likely to see a small descriptive popup.

Interacting with VMware Monitoring in Foglight Evolve Cloud

When you deploy VMware Monitoring in Foglight® Evolve Cloud, a set of predefined dashboards enables you to view the performance of your virtual system at a glance. They allow you to ensure consistent application performance by drilling down for details from higher-level components such as clusters, hosts, and virtual machines, to viewing detailed specifics about each component, such as CPU utilization and network I/O.

First, familiarize yourself with roles needed to access different parts of the browser interface included with the product (see Exploring the VMWare Agent Administration Dashboard). Then, ensure your monitored agents are configured for data collection. You do that by navigating to the VMware Agent Administration dashboard. This dashboard lists the available agents and shows their status, and provides access to other administrative tasks. For more information, see Exploring the VMWare Agent Administration Dashboard on page 15 and Configuring monitoring agents for data collection on page 18.

Start by navigating to the VMware Explorer. Use this dashboard to see specific performance details related to a specific component, such as its CPU load, network I/O, total memory, or consumed disk space. For more information, see Investigating performance metrics on page 24.

Next, review the alarms that are generated against your environment and, if required, set their sensitivity level. The VMware Agent Administration dashboard enables you to configure the level of alarm sensitivity. The alarm sensitivity reflects the level of alarms the system stores and displays.

To read about additional features, such as creating OS mapping rules, or reviewing topology object instances and expired data, see Additional features on page 33.

Exploring the VMWare Agent Administration Dashboard

The VMWare Agent Administration dashboard allows you to deploy remote agents, configure rules, and set advanced platform options.

This dashboard consists of the Rule Configuration tab, Advanced Options tab, User Level Access tab, and the Agents view.

Figure 8. VMware Agent Administration dashboard
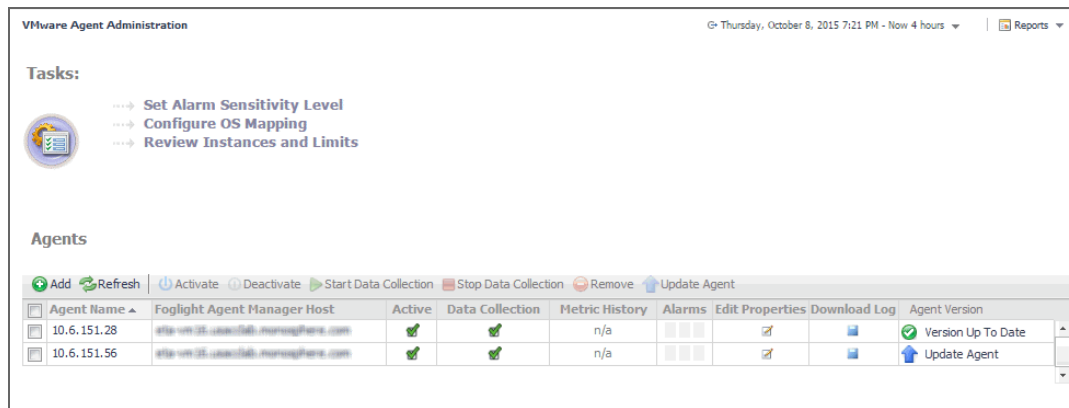
Rule Configuration tab

The **Rule Configuration** tab contains links to administrative tasks that you can initiate from this tab:

- **Set Alarm Sensitivity Level:** Sets the level of alarms that the system generates, stores, and displays. For more information, see Setting the alarm sensitivity level on page 33.

Figure 9. VMware Agent Administration dashboard
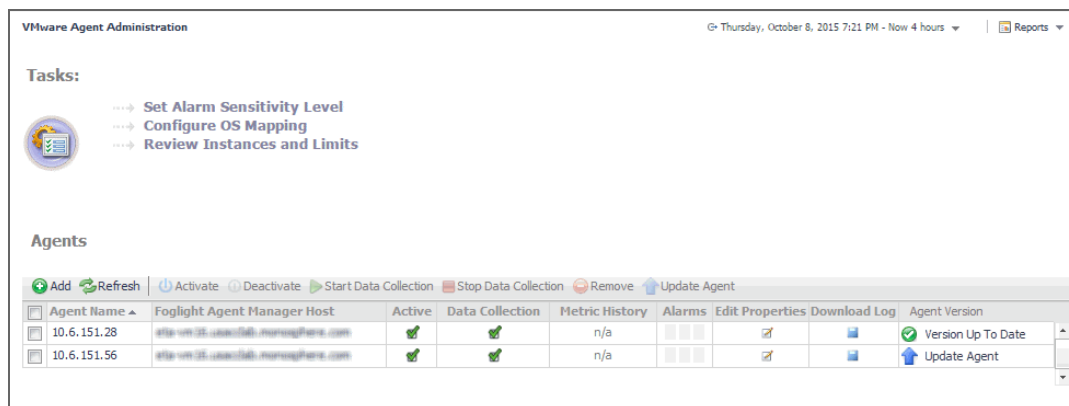
Advanced Options tab

The **Advanced Options** tab contains links to administrative tasks that you can initiate from this tab:

- **Configure OS Mapping:** Associates different versions of an operating system with a common OS name. For more information, see Creating OS mapping rules on page 33.

- **Review Instances and Limits:** View existing VMware object instances. For more information, see Reviewing object instances and limits on page 35.

- **Metrics Collection Management:** Configure the metrics collect by agent. For more information, see Configure Metrics Collection on page 36.

User Level Access tab

The **User Level Access** tab is used to filter which resources are accessible to Foglight users or Foglight user groups.

VMware Monitoring in Foglight Evolve Cloud 5.8.2 User and Reference Guide
Using VMware Monitoring in Foglight Evolve Cloud

16

Prerequisites

Before assigning resources to be accessed by certain users or user groups, make sure to assign only the "*Dashboard User*" and "*VMware Operator User*" roles to the specified users or user groups.

> **i** | **NOTE:** Ensure that the specified users or user groups only have the "*Dashboard User*" and "*VMware Operator User*" roles.

To configure the resources to be accessed by the user (or user group):

1   On the navigation panel, under **Dashboards**, choose **VMware > VMware Agent Administration**.

2   Select the user (or user group), and then click the button in the *Configure* column.

3   In the **Authorization Dialog**, select the resources from the left table, and then click **>>** to move them to the right table, and then click **save**.

   The Save Configuration dialog box appears, showing the configuration of User Level access has been saved successful.

Agents view

The **Agents** view shows a list of existing agent instances and a set of agent management buttons at the top of the list. The following buttons are available:

- **Add:** Starts a workflow for creating new agent instances. For more information, see Configuring monitoring agents for data collection on page 18.

- **Refresh:** Refreshes the list of agent instances and their states.

- **Activate:** Activates one or more selected agent instances. Activating an agent instance starts the agent process on the machine on which the agent is installed.

- **Deactivate:** Deactivates one or more selected agent instances. Deactivating an agent stops the agent process on the machine on which the agent is installed.

- **Start Data Collection:** Starts the data collection for one or more selected agent instances. Starting an agent's data collection causes the agent to begin monitoring a Virtual Center, and to send the collected metrics back to the Management Server.

- **Stop Data Collection:** Stops the data collection for one or more selected agent instances. Stopping an agent's data collection causes the agent to stop monitoring the Virtual Center.

- **Edit Properties:** Starts a workflow for editing the properties of one or more selected agent instances. Each agent comes with a set of properties that it uses to configure its correct running state. For more information, see Setting the Configuration properties on page 40.

- **Remove:** Deletes the selected agent instance.

- **Update Agent**: Updates the agent package to the latest version.

To perform an agent management command, select the one or more check boxes in the left-most column and click the appropriate button. For example, to start an agent's data collection, select the check box in the agent row and click **Start Data Collection**.

The table in the **Agents** area lists the existing VMware Performance Agent instances. For more details about the data appearing in this table, see Agents view on page 79.

Accessing the VMware Agent Administration Dashboard

To access the VMware Agent Administration dashboard:

1   Log in to the Foglight Evolve Cloud browser interface.

2   Ensure that the navigation panel is open.

   To open the navigation panel, click the right-facing arrow ▶ on the left.

On the navigation panel, under **Dashboards**, choose **VMware > VMware Agent Administration**.

The VMware Agent Administration dashboard appears in the display area.

Figure 10. VMware Agent Administration dashboard
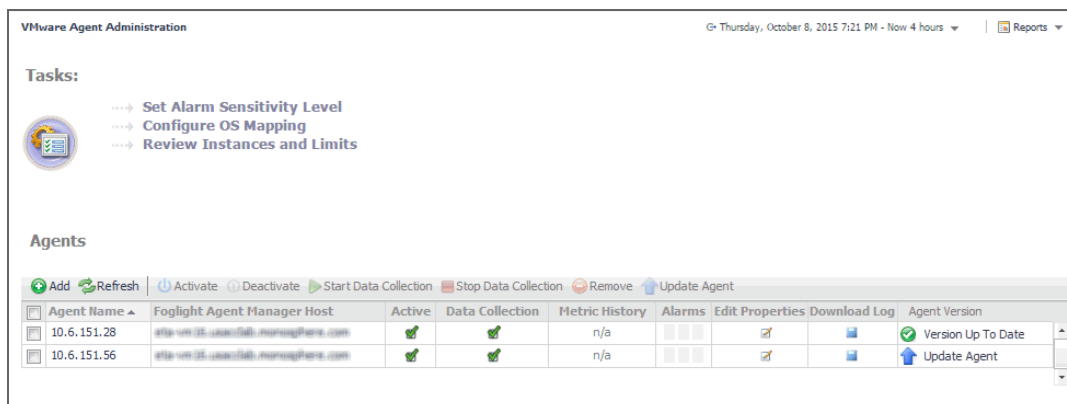
Configuring monitoring agents for data collection

VMware Monitoring in Foglight® Evolve Cloud uses the VMware Performance Agent to collect information from monitored environments. Creating a VMware Performance Agent instance creates the agent process on the Agent Manager host. Activating the VMware Performance Agent starts that agent process while starting an agent instance's data collection enables the agent to start collecting data from the monitored vCenter® and to send it to VMware Monitoring in Foglight Evolve Cloud.

When the VMware Performance Agent package is successfully deployed, create one or more agent instances, activate them, and start their data collection. To perform these steps in a single operation for one or more monitored hosts, use the **Agents** view on the **Administration** tab.

Each VMware Performance Agent monitors a single Virtual Center. When you create a VMware Performance Agent instance and the Agent Setup wizard determines that the Virtual Center was not previously monitored by this Foglight Evolve Cloud instance, it starts importing historical data into Foglight Evolve Cloud. This data is not immediately available as it takes some time to collect it. This process can import data collected over 30 days or less, depending on the amount of data available in the Virtual Center. This allows you to explore VMware metrics as soon as the data is imported, instead for waiting for the agent to collect some data from the Virtual Center. The **Metric History** column in the **Agents** table indicates the progress of the historical data import. Historical data is intended for charting, trending, and general presentation purposes. It does not cause any alarms to fire.

To import vCenter historical data, the minimum recommended vCenter Statistics Levels must be at least 2 in the samples that are collected for one month for the agent to populate 30 days of historic collections. The following table lists the minimum Statistics Levels for all collection frequencies. For more information about vCenter Statistics levels, see your VMware® documentation.

Table 2. Statistics Levels for all collection frequencies

Collection Interval	Collection Frequency	Statistics Level
1 Day	5 Minutes	1
1 Week	30 Minutes	1
1 Month	**2 Hours**	**2**
1 Year	1 Day	1

IMPORTANT: Before creating your first VMware Performance agent, you must configure a Virtual Center user with sufficient privileges. For more information, see "Enabling VMware Performance Agents to Collect Data from a Virtual Center" in the Foglight for VMware *Installation Guide*.

NOTE: In FIPS-compliant mode, you need to import the CA certificate or the self-signed certificate to the KeyStore of FglAM. For more information, see Managing certificates.

To create, activate VMware Performance Agent instances, and start their data collection:

1   Log in to the Foglight Evolve Cloud browser interface.

2   On the navigation panel, under **Dashboards**, choose **VMware > VMware Agent Administration**.

Figure 11. VMware Agent Administration dashboard
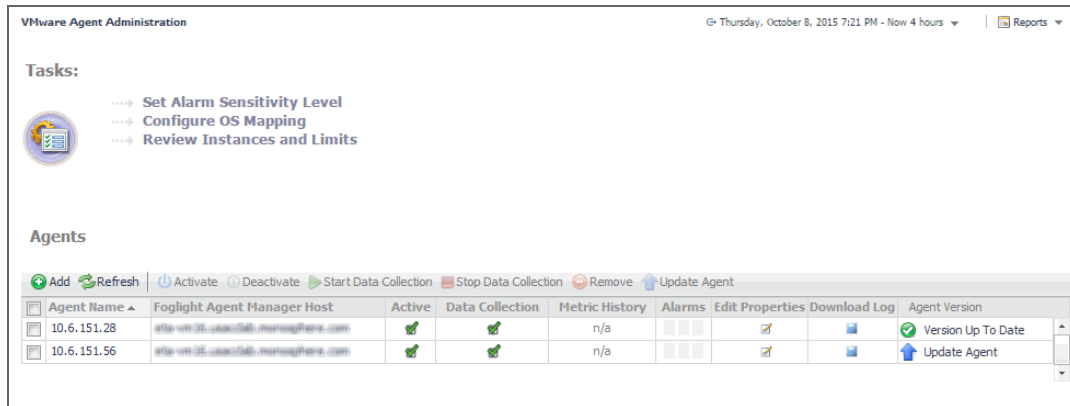
3   Launch the **Agent Setup Wizard**. In the **Agents** area, click **Add**.

The **Agent Setup Wizard** appears with the **Select an Agent Host** page open.
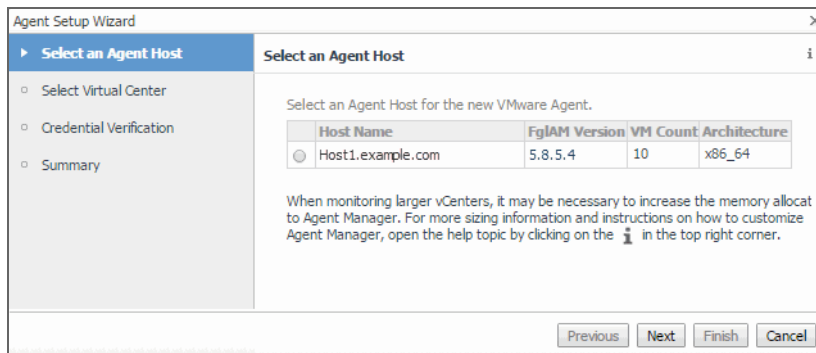
4   Select the host machine running the Agent Manager that you want to manage the VMware Performance Agent you are about to create, and click **Next**.

The **Agent Setup Wizard** refreshes, showing the **Select Virtual Center** page.
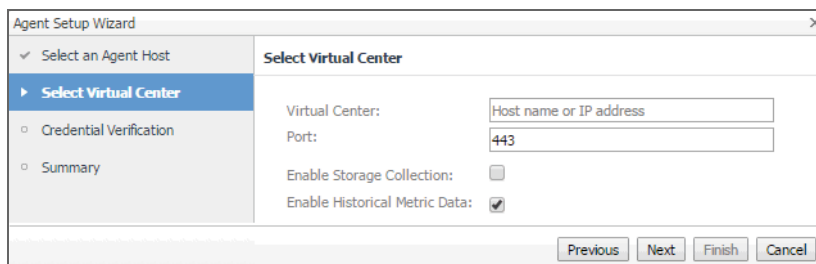
5 Specify the Virtual Center that you want to monitor.

   a   In the **Virtual Center** box, type the fully qualified name of the host on which the Virtual Center is running.

   b   In the **Port** box, type the port number of the host running the Virtual Center that will be used by the VMware Performance Agent to connect to the Virtual Center.

   c   If you want to enable the VMware Performance Agent to collect the Foglight Evolve Cloud Storage data, select the **Enable Storage Collection** check box. Foglight Evolve Cloud Storage can help you optimize the VMware environment by monitoring virtual storage and its underlying physical storage components. For more information about this product, see the *Managing Foglight Manager Storage User and Reference Guide*.

   d   If you want to import historical data, select the **Enable Historical Metric Data** check box. This data is not immediately available as it takes some time to collect it. This process can import data collected over 30 days or less, depending on the amount of data available in the Virtual Center. Selecting this option allows you to explore VMware metrics as soon as the data is imported, instead for waiting for the agent to collect some data from the Virtual Center.

   e   Click **Next**.

The **Agent Setup Wizard** refreshes, showing the **Credential Verification** page.

6 Specify user credentials the VMware Performance Agent needs to log into tho Virtual Center host. Select one of the following options:

> **i** | **IMPORTANT:** The Virtual Center user account must have sufficient privileges. For more information, see "Enabling VMware Performance Agents to Collect Data from a Virtual Center" in the VMware Monitoring in Foglight Evolve Cloud *User and Reference Guide*.

   ▪   **Add vCenter(s) to a new credential**: Select this option if you want to create a new credential for the selected vCenter. Click **Next** and continue to Step 7.

   ▪   **Add vCenter(s) to an existing credential**: Select this option if you want to use an existing credential for the selected vCenter. This option is suitable if an existing credential has the information needed to access the vCenter. Click **Next and** continue to Step 8.

For complete information about Foglight Evolve Cloud credentials, see the *Administration and Configuration Help*.

7 **Creating a new credential only**.

a   Specify the following information:

    ▫   **Credential Name**: Type a name that uniquely identifies the credential.

    ▫   **User**: Type the vCenter user name.

    ▫   **Password**: Type the vCenter password.

    ▫   **Confirm Password**: Type the vCenter password.

b   Select a lockbox in which you want to keep the credential. A lockbox can be used to group credentials for access and/or security. In smaller Foglight Evolve Cloud installations, you can use the default **System** lockbox.

c   Click **Next**.

The **Summary** page appears.

d   Click **Finish**.

The **Agent Setup Wizard** closes, and the **Agents** area refreshes, showing a newly created VMware Performance agent instance.

8   **Using an existing credential only**.
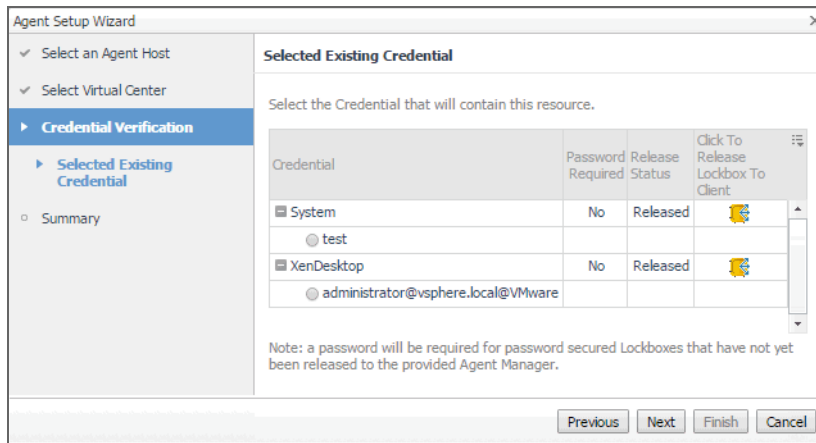
    a   Select an existing credential that you want to use to access the vCenter.

    b   Click **Next**.

        The **Summary** page appears.
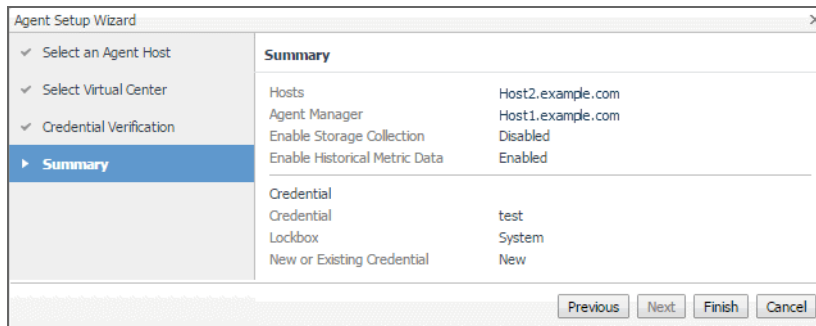
    c   Click **Finish**.

The **Agent Setup Wizard** closes, and the Agents area refreshes, showing a newly created VMware Performance agent instance.

Managing certificates

Syntax Conventions

In order to successfully make use of the Foglight commands in your monitoring environment, review the syntax conventions before getting started. The syntax conventions are as follows:

- Generic examples follow the UNIX path structure that uses forward slashes '/' to separate directories.

- Platform-specific examples follow standard platform conventions. For example, UNIX-specific examples use forward slashes '/' as directory delimiters, while Windows examples use backslashes '\'.

- *<foglight_home>* is a placeholder that represents the path to the Foglight Management Server installation.

- *<foglight_agent_mgr_home>* is a placeholder that represents the path to the Foglight Agent Manager installation. This can be the location of the Foglight Agent Manager installation on a monitored host, or the home directory of the Foglight Agent Manager that comes embedded with the Foglight Management Server. For example:

Path to the Foglight Agent Manager installation on a monitored host (Windows):

C:\Quest\Foglight_Agent_Manager

Path to the embedded Foglight Agent Manager installation (Windows):

C:\Quest\Foglight\fglam

- Unless otherwise specified, Foglight commands are case-sensitive.

Managing certificates for FglAM

Foglight Evolve agents use Foglight Agent Manager (FglAM) to manage certificates for SSL encryption connection.

Prerequisite

All the certificate-related command line options require that FglAM be **up and running**.

Add a certificate

```
bin/fglam --add-certificate "user alias 1"=/path/to/certificate/file
```

- Validate the certificate and ensure the following:

    - It is not expired.

    - It is an X.509 format.

    - FglAM requires the Base64 format. To verify if the certificate file is encoded with Base64, open the certificate with a notepad and the certificate should be similar to the following example:
      ```
      -----BEGIN CERTIFICATE-----
      XXXXXXXX=
      -----END CERTIFICATE-----
      ```
      > **i** | **NOTE:** If the certificate is not Base64 format, use openssl command to convert the certificate file into a Base64 file. Use either of the following commands depending on the source form:
      > ```
      > openssl x509 -inform DER -in xxx.cer -out xxx.crt
      > ```
      > or
      > ```
      > openssl x509 -inform PEM -in xxx.cer -out xxx.crt
      > ```

- The `alias` is required and is used in the list and delete operations to refer to the certificate. It can be anything.

List installed certificates

```
bin/fglam --list-certificates
```

Print out a list of certificates and the aliases that refer to them.

Refer to the example output below:

```
List of installed certificates:

  Alias               Certificate Info

  -----               ---------------

  user alias 1        XXXX
```

Delete a certificate

Remove a certificate referred to by an `alias`.

```
bin/fglam --delete-certificate "user alias 1"
```

A full example for managing certificate for FglAM

- Add an example certificate into FglAM certificate store

```
C:\Quest\Foglight\fglam\bin>fglam.exe --add-certificate "Evolve-test"="D:/Evolve-
test.crt"

...

2020-02-27 16:31:01.000 INFO  [native] Certificate added: Certificate from

   D:\Evolve-test.crt added as Evolve-test
```

- List the example certificate in the FglAM certificate store

```
C:\Quest\Foglight\fglam\bin>fglam.exe --list-certificate

...

  Alias                      Certificate

  -----                      -----------

  Evolve-test                          Issuer:

                             CN: XXX
```

- Delete the example certificate from the FglAM certificate store

```
C:\Quest\Foglight\fglam\bin>fglam.exe --delete-certificate "Evolve-test"

...

2020-02-27 16:28:21.000 INFO  [native] Certificate deleted: Certificate

   Evolve-test deleted
```

Investigating performance metrics

The VMware Explorer allows you to monitor a wide range of elements in your virtual infrastructure. It contains a number of informative views through which you can quickly and easily access detailed information about any of the available components (physical or virtual) within the infrastructure. Its hierarchical interface includes drilldown capabilities that display various performance metrics and alarms within the virtual infrastructure.

Figure 12. VMware Explorer
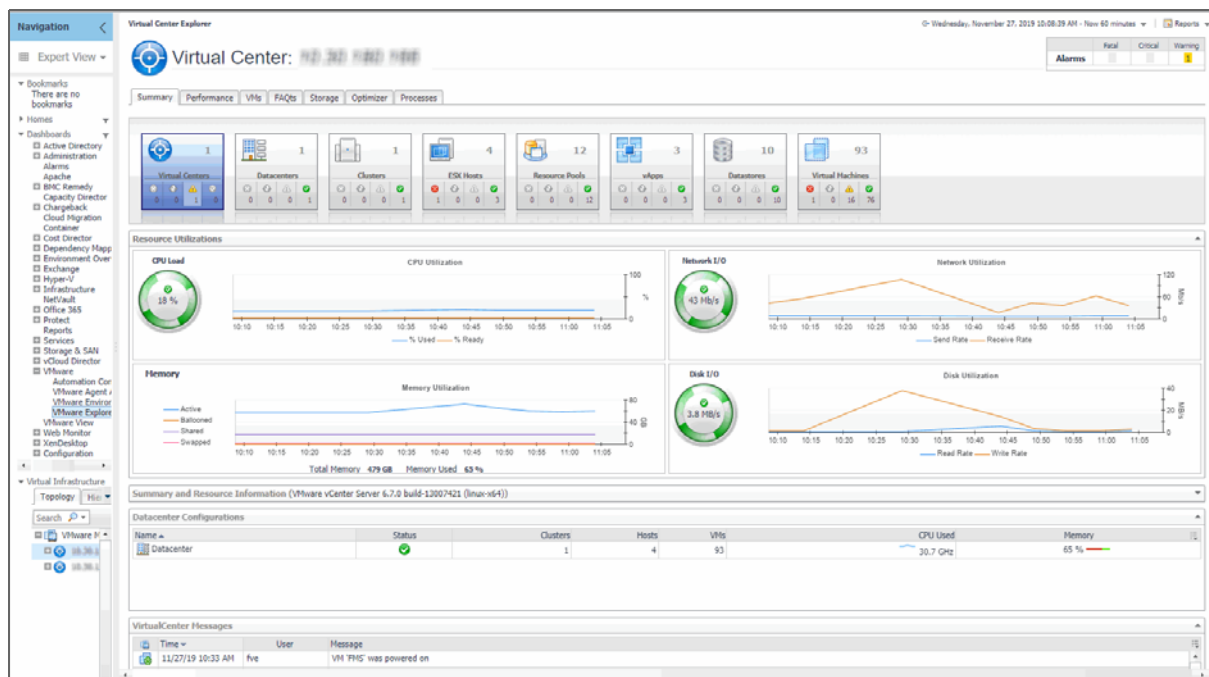
i | **NOTE:** The VMware Explorer dashboard is inventory-based. The VMware Explorer dashboard counts all virtual machines (VMs), including template VMs, for each vCenter. The Virtual Environment Summary dashboard is service-based. The VMware service created by VMware Monitoring in Foglight® Evolve Cloud for a particular vCenter does not contain template VMs. Therefore, the number of VMs for a particular vCenter is different when you view it through the VMware Explorer dashboard than the number that appears when you view it through the Virtual Environment Summary dashboard.

To access this dashboard, from the navigation panel, under Dashboards, click **VMware > VMware Explorer**. For complete reference about the data appearing on this dashboard, see VMware Explorer views on page 46.

The Virtual Infrastructure view contains a navigation tree on the Topology tab that represents the various virtual infrastructure objects: Virtual Centers, Datacenters, Clusters, ESX Hosts, Resource Pools, and Virtual Machines. For each individual object or group of objects, a status indicator appears, showing the alarm of highest severity that is outstanding for the that object or objects. For example, there are 25 virtual machines configured for a vCenter. Twenty of the virtual machines have a normal status, three have a warning status, and two have a critical status. In the Topology view, the virtual machines container for that vCenter displays a critical status indicator to show that at least one of the virtual machines associated with the vCenter has an outstanding critical alarm.

Figure 13. Topology tab
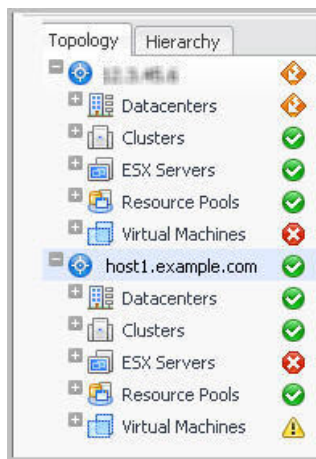
The Hierarchy tab shows the logical layout of vCenter management servers.

Figure 14. Hierarchy tab
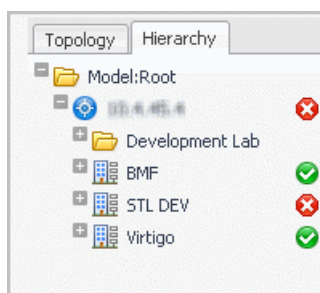
Hovering over an object in the Virtual Infrastructure view, you see a popup that provides a summary of the present state of that object.

Figure 15. Object summary dwell
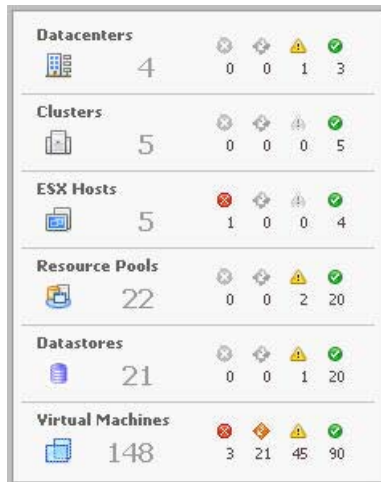
Selecting an object or group of objects on either tab of the Virtual Infrastructure view displays performance details about your selection in the VMware Explorer Primary view. The VMware Explorer Primary view takes up the entire display area of the VMware Monitoring in Foglight Evolve Cloud browser interface. This view provides significant value to administrators who leverage VMware Monitoring in Foglight Evolve Cloud to monitor their virtual infrastructure.

Figure 16. VMware Explorer
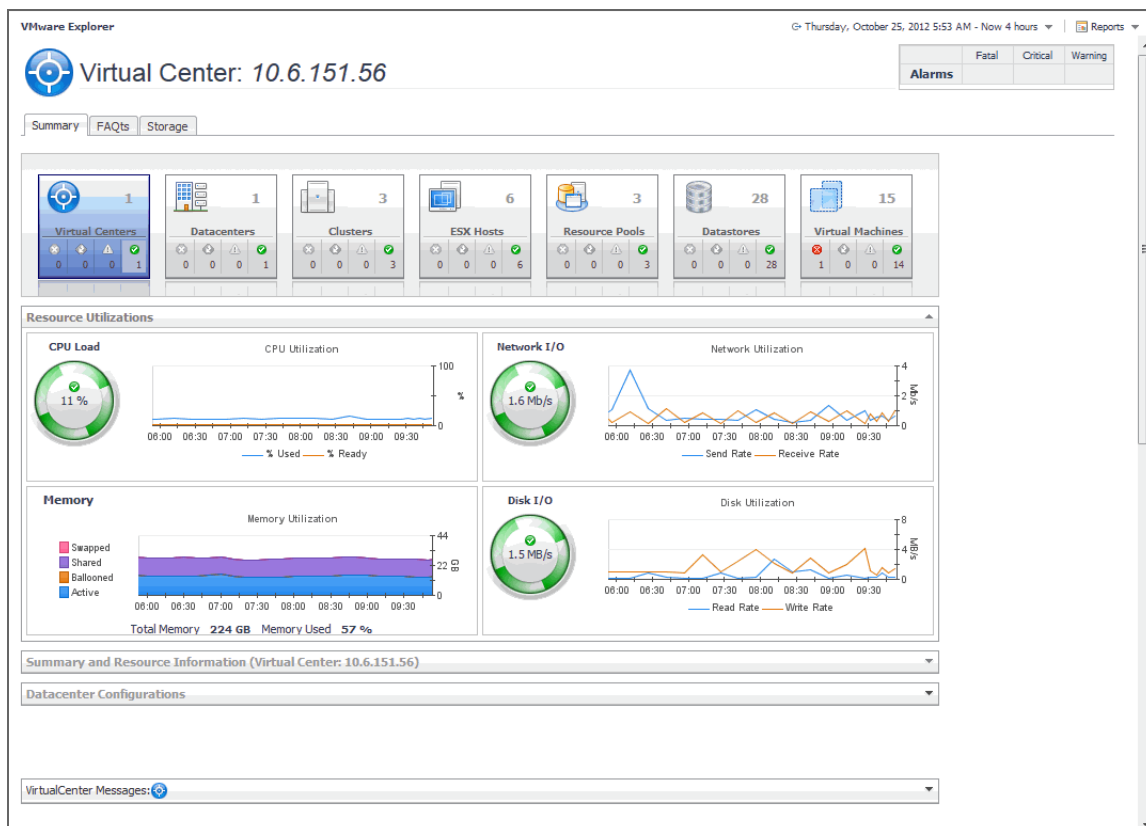
The alarm summary in the top-right shows the number of alarms at each severity level that are outstanding for the selected object. Clicking an alarm count lists the active alarms for the object.

A set of tiles displayed along the top indicate the type of the selected object or objects, and the related alarm counts.

Additionally, a collection of navigation tabs appears in this view. These navigation tabs vary from object to object, but generally contain a tab to an object summary (typically the default view), a tab to an object performance overview, and one or more tabs to other relevant information.

The display area changes in appearance and content, depending on the selected object or group of objects. For example, if you select an object type container from the Topology view, the Summary tab displays a consumption graph and a table that are representative of the group of objects within that container.

Figure 17. VMware Explorer Summary tab
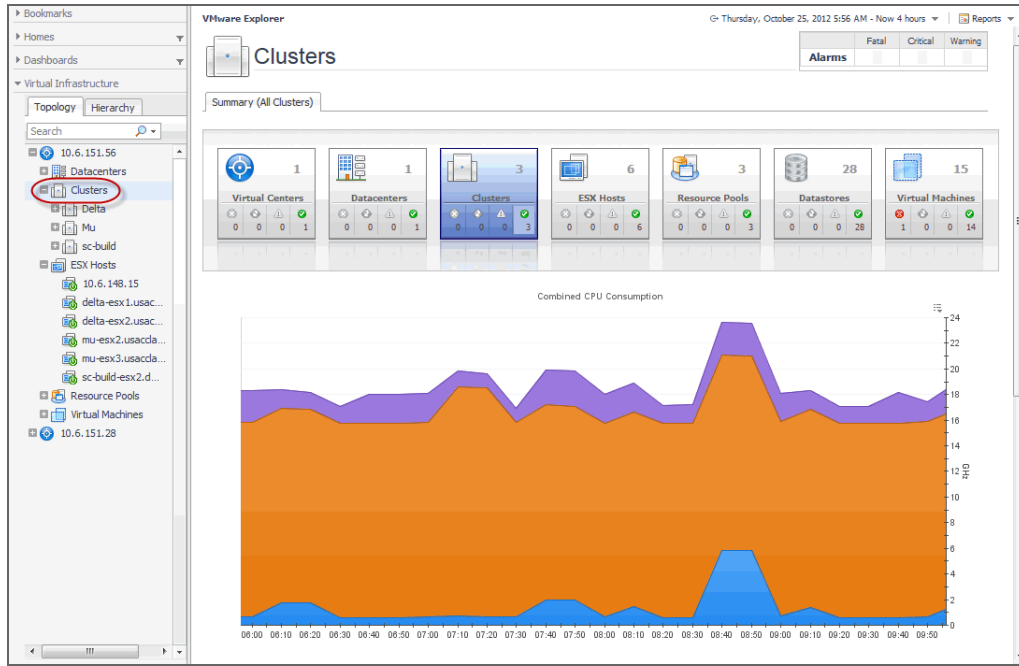
However, selecting a Resource Pool container from the Topology tab displays a Resource Pools Relationship Tree on the Summary tab. This tree contains every resource pool that belongs to the clusters within the associated vCenter. This is useful if you want to see how those resource pools are laid out, or if you want to take a look at the utilization statistics for each configured resource pool on the vCenter.

Figure 18. Resource Pool tree
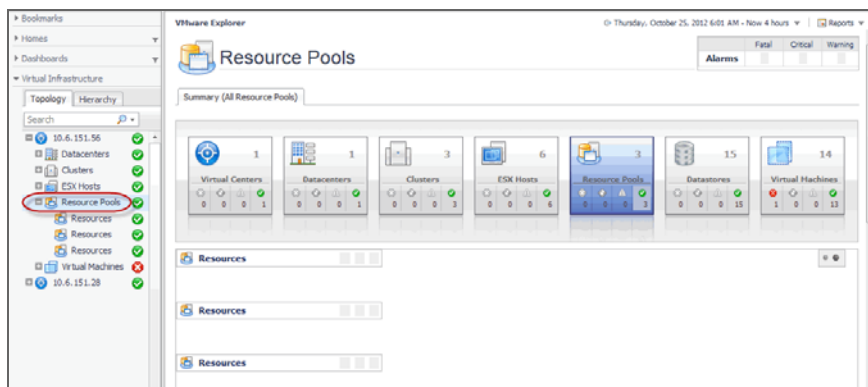
If you select an individual resource pool from the Virtual Infrastructure view, the Summary displays summary and utilization information for that resource pool. This is typically the type of information you see on the Summary tab when you select any individual object from the Virtual Infrastructure view.

Figure 19. Resource Pool Summary
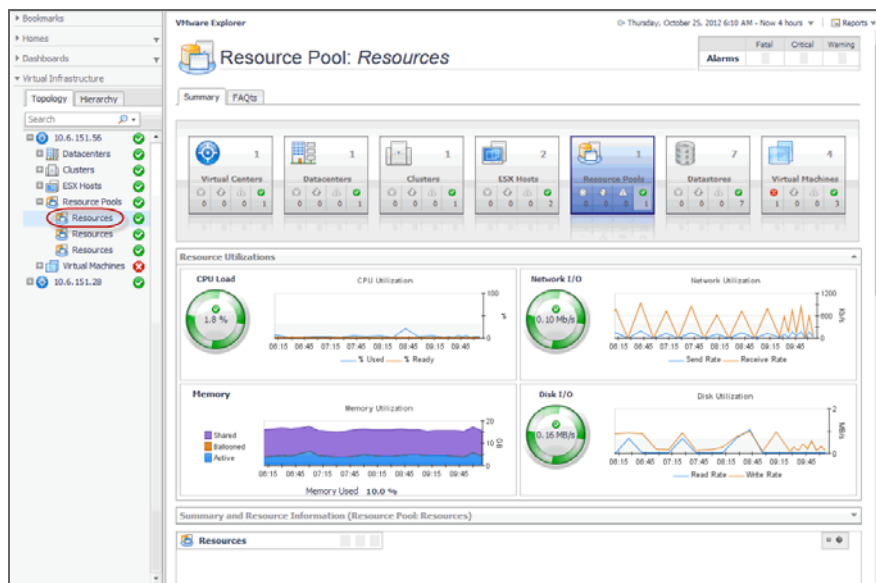
The metrics and the amount of detail displayed in the display area vary depending on the type of the selected object. For example, in the image below, the tiles indicate that the selected object is the *New Datacenter* datacenter, and that it is connected to one vCenter, one cluster, two ESX® Hosts, and so on.

Figure 20. Datacenter Summary

VMware Monitoring in Foglight Evolve Cloud 5.8.2 User and Reference Guide
Using VMware Monitoring in Foglight Evolve Cloud

28
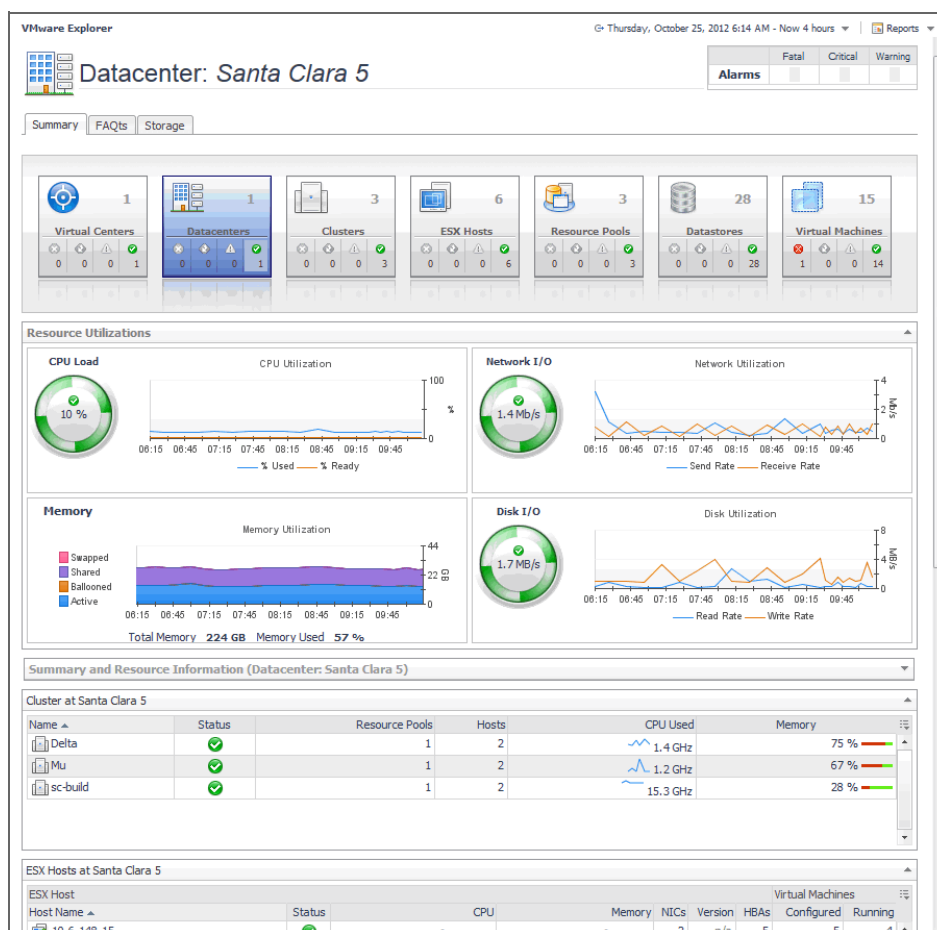
The Utilizations view, typically located across the center of the display area tab, provides numerical and graphical representations of utilization metrics associated with the selected object or group of objects. For example, selecting a single resource pool from the Virtual Infrastructure view and opening the Performance tab in the display area, displays four graphs in the Utilizations view, showing CPU, memory, disk, and network resource utilizations for the selected resource pool.

Figure 21. Resource Utilization views
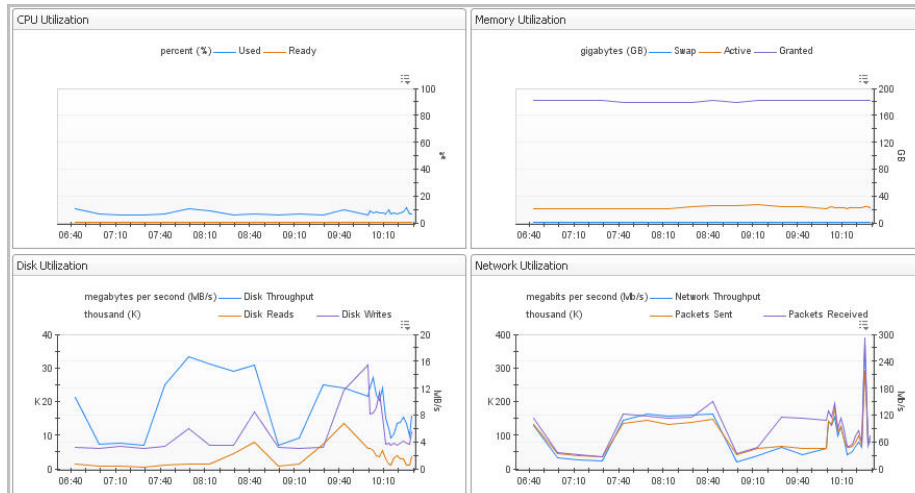
From there, clicking a graph or a spinner shows a larger view of the graph with descriptive text about each metric appearing in the graph.

Figure 22. Resource Pools, CPU Utilization drilldown
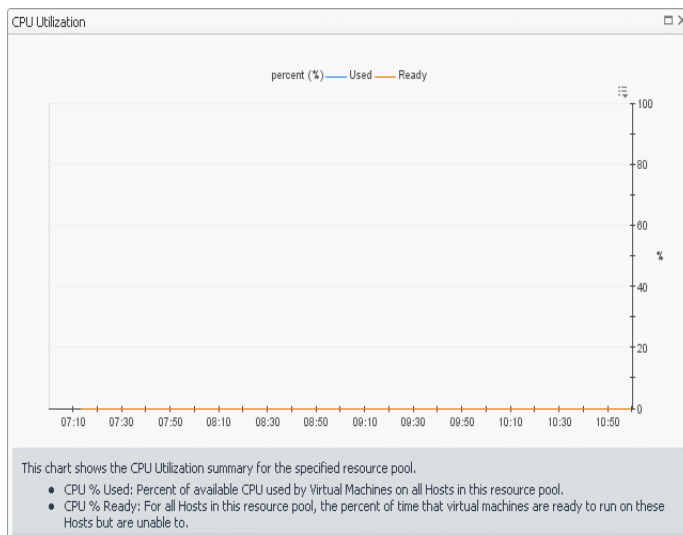
If you open the **VMs** tab for that same resource pool, the Utilizations view displays one graph illustrating the percent-used and percent-ready CPU utilization for the virtual machines of the resource pool.

Figure 23. Resource Pools, VM CPU Utilization drilldown
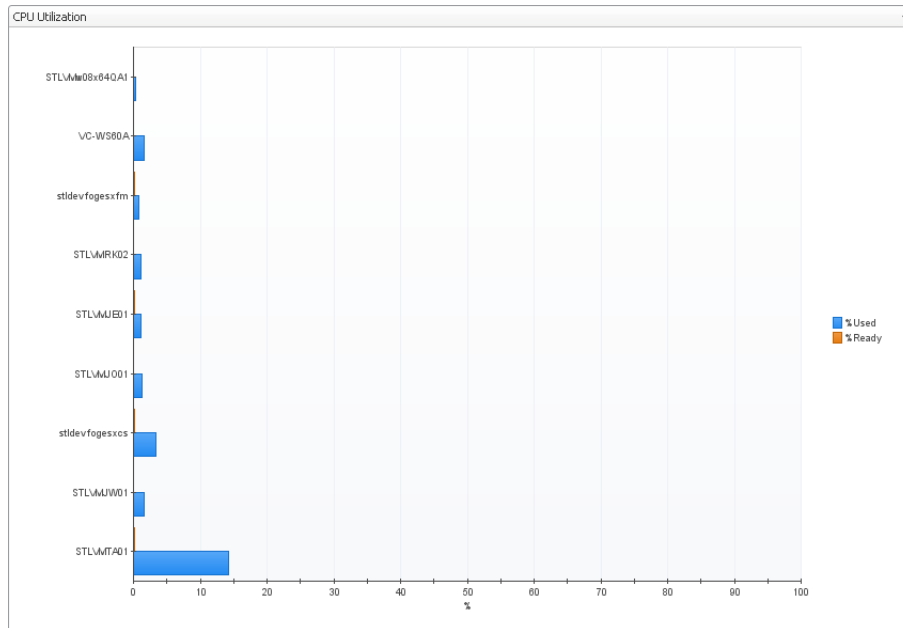
If, however, you select a collection of ESX Hosts from the Virtual Infrastructure view and you open the Summary tab, an informative graph appears in place of a Utilizations view. Selecting a collection of objects in the Virtual Infrastructure view always shows a composite view displaying information about all object instances contained in that collection.

Figure 24. Combined CPU Consumption
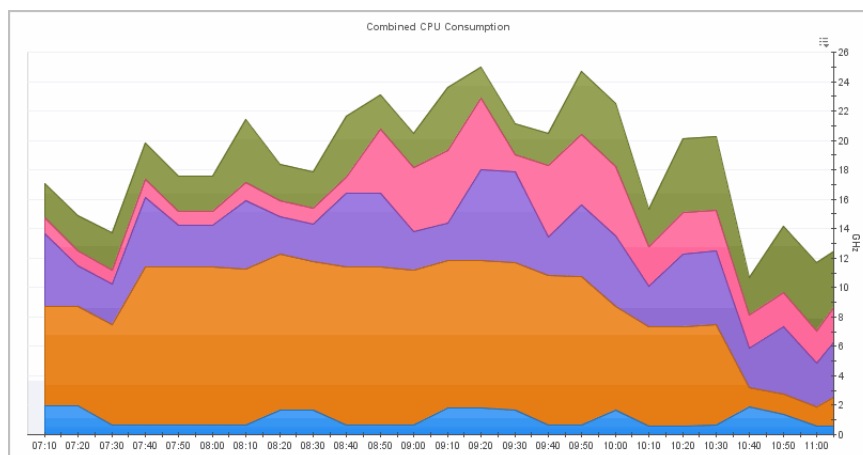
In addition to the Utilizations view, one or more Related Objects views may appear at the bottom of the display area. These views take the form of tables and list either the parent or child objects or both (whichever are applicable) of the object being viewed, and provide pertinent details about each one. Their appearance depends on the type and range of objects selected in the Virtual Infrastructure view.

For example, if you select a single cluster, two Related Objects views appear: one displaying the ESX hosts that belong to their cluster, and another listing the virtual machines running on those hosts. The views also display the performance metrics associated with each list item.

Figure 25. Related Objects views
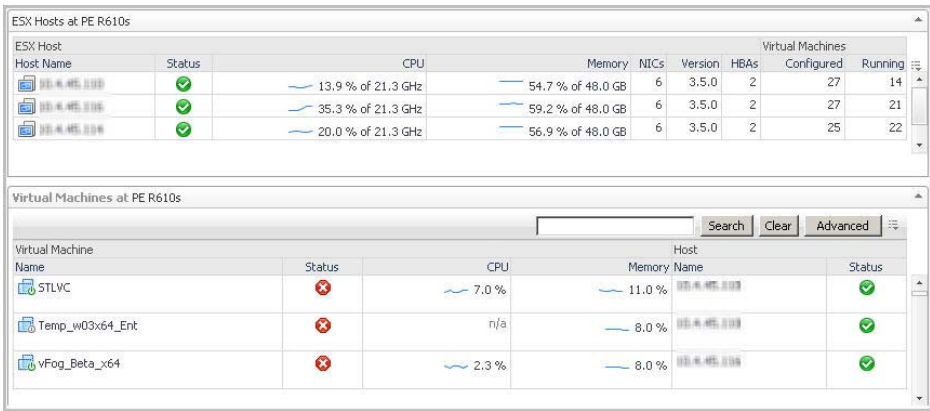
However, when you select a cluster container, the **Summary** tab shows a Related Objects view that lists all of the clusters in that container and provides pertinent details about each one.

Figure 26. Cluster details
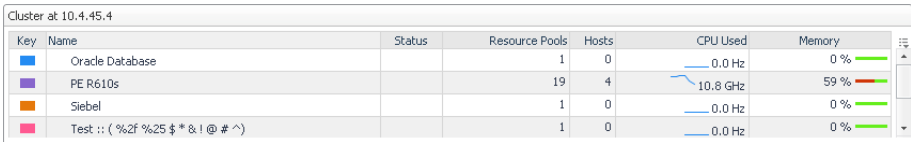
Viewing baseline ranges

Foglight Evolve Cloud can estimate system performance by comparing metric values against a baseline range. A baseline establishes expected data patterns during a given time period. This feature is only available when your Foglight Evolve Cloud system includes a baseline cartridge with applicable metric definitions. VMware Monitoring in Foglight Evolve Cloud uses the capabilities of the IntelliProfile cartridge, which enables the appearance of baseline data for ESX hosts and virtual machines on the VMware Environment and VMware Explorer dashboards.

Figure 27. Resource Utilization views
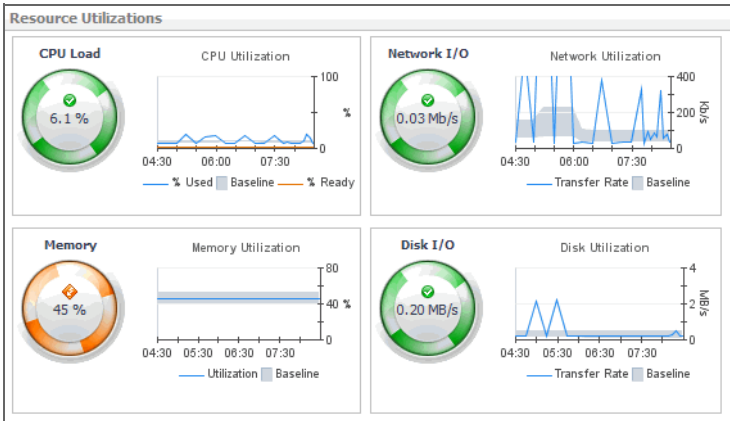
Baseline data can also be displayed on custom dashboards and views for the following metric properties.

Table 3. Topology types and the related metric properties

Topology Type	Metric Property
HostCPUs	utilization
Memory	utilization

Table 3. Topology types and the related metric properties

Topology Type	Metric Property
HostStorage	`diskTransferRate`
HostNetwork	`transferRate`
VMWVirtualMachineMemory	`active`
VMWVirtualMachineMemory	`consumed`
VMWESXServerMemory	`active`
VMWESXServerMemory	`consumed`

Start creating a custom dashboard by clicking **Create dashboard** on the action panel. From there, create a view and add one or more of the data elements listed above. For complete information about custom dashboards and how to get started, refer to the *Foglight Evolve Cloud User Help* and the *Creating Custom Dashboards* learning video.

Before finishing, edit the view properties and enable the appearance of the baseline minimum and maximum values by selecting one or more of the **Show baseline min/max as** check boxes.

Figure 28. Add View dialog box
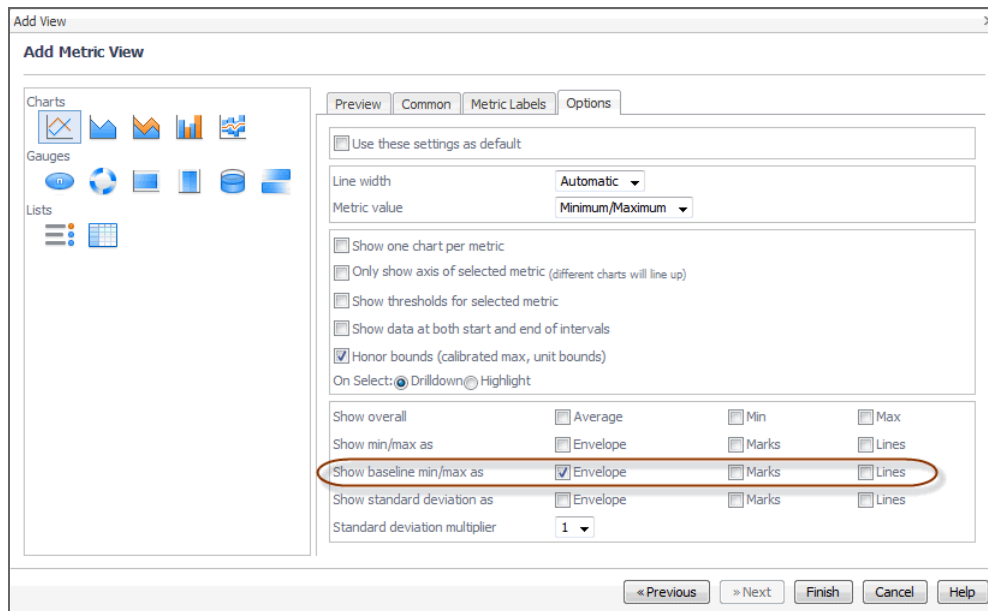
When you finish creating the custom dashboard, the blue line in the chart indicates metric values over time, while the grey shaded area represents the baseline range for the selected metric.

Figure 29. Baseline range for a view
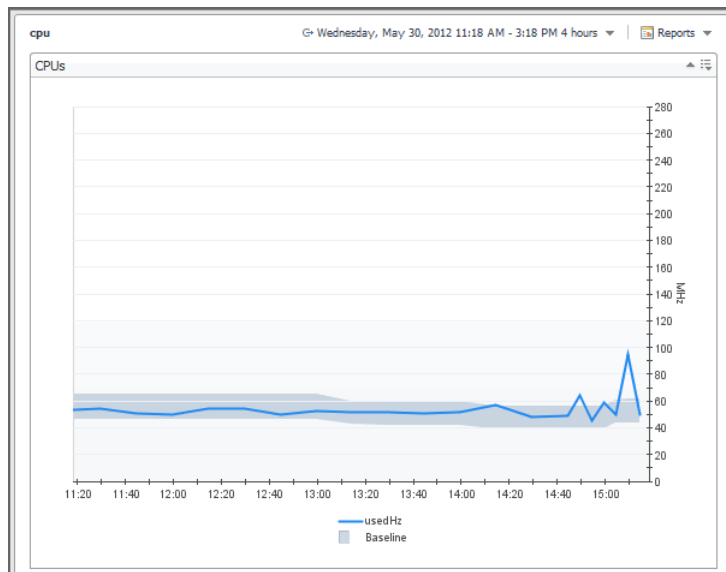
Setting the alarm sensitivity level

The VMware Agent Administration dashboard enables you to configure the level of alarm sensitivity. The VMware Monitoring in Foglight® Evolve Cloud alarm sensitivity reflects the level of alarms the system stores and displays.

To configure the level of alarm sensitivity:

1   On the VMware Agent Administration dashboard click **Set Alarm Sensitivity Level**.

   The **Set Alarm Sensitivity Level** dialog box appears.
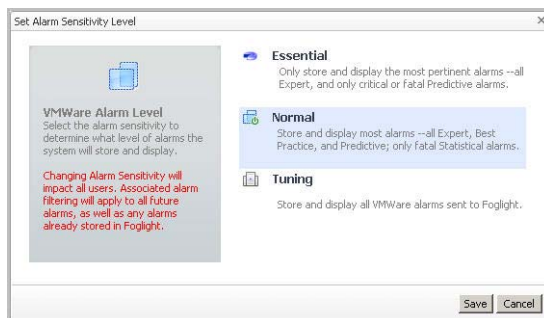
2   On the dialog box, click one of the alarm sensitivity levels to select it. Normal is the default level.

3   Click **Save**.

Additional features

Creating OS mapping rules

OS mapping involves associating various versions and editions of a particular operating system with a common OS name. You configure OS mapping rules using the **Administration** tab on the VMware Environment dashboard. This helps VMware Monitoring in Foglight Evolve Cloud map the OS names reported by VMware

Monitoring in Foglight Evolve Cloud to those reported by physical OS monitoring, so that you can view all Windows machines, all Linux machines, and so on.

For reference information about this view, see OS Mapping view on page 81.

To configure OS mapping rules:

• On the VMware Agent Administration dashboard, click **Configure OS Mapping**.

   The **OS Mapping** view appears.
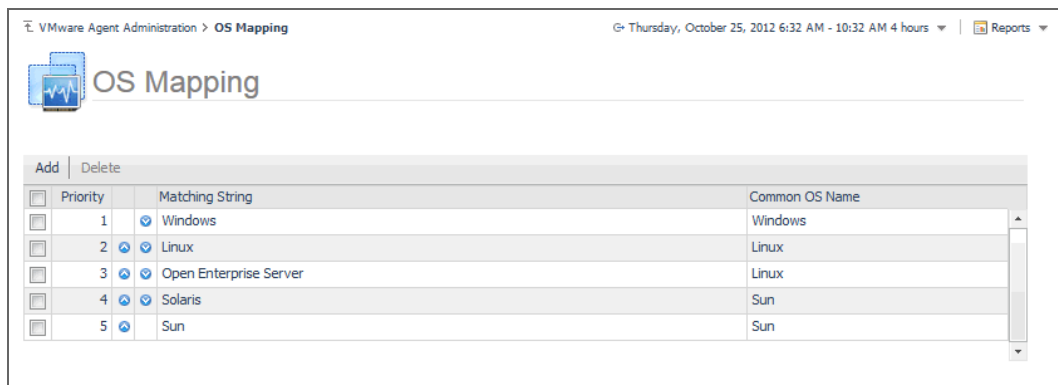
To add an OS mapping rule:

1 In the **OS Mapping** view, click **Add**.

   The **Add OS Mapping Rule** dialog box appears.
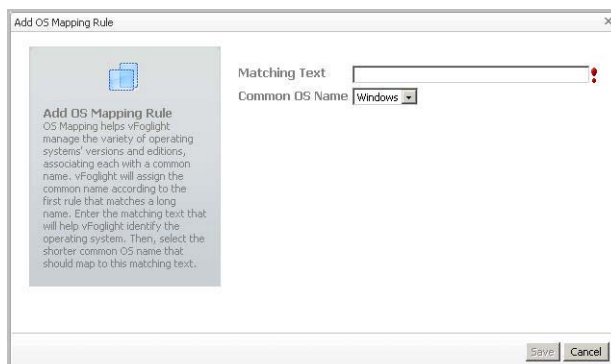
2 In the **Add OS Mapping Rule** dialog box, in the **Matching Text** box, type the OS name with its edition and/or version number to help VMware Monitoring in Foglight Evolve Cloud identify the operating system.

3 In the **Common OS Name** list, select the shorter common OS name.

4 Click **Save**.

   VMware Monitoring in Foglight Evolve Cloud matches the shorter common OS name with the text you provided in Step 2.

To delete an OS mapping rule:

1 In the **OS Mapping** view, select an OS mapping rule by clicking the associated check box in the left column.

2 Click **Delete**.

3 Click **Save**.

To configure the priority of an OS mapping rule:

- In the **OS Mapping** view, move a rule one level up by clicking the up arrow in the rule's row.

- Move a rule one level down by clicking the down arrow in the rule's row.
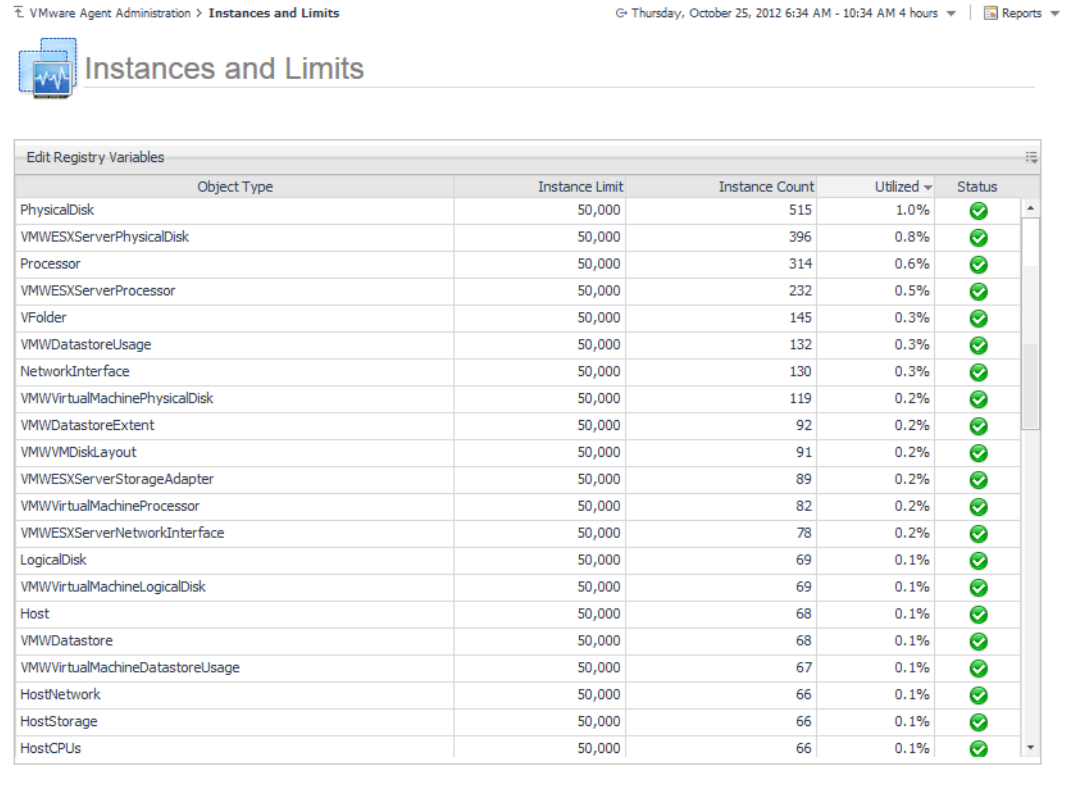
Reviewing object instances and limits

Foglight Evolve Cloud collects data from monitored environments and creates a data model in real-time. The resulting topology model consists of nodes where each node is an object instance of a particular object type. Each type of monitoring environment can have a unique set of object types. VMware Monitoring in Foglight Evolve Cloud includes a set of topology object types and their definitions. When Foglight Evolve Cloud collects data from your VMware environment, it builds the topology model that consists of the instances of the object types defined by VMware Monitoring in Foglight Evolve Cloud. By default, a monitored environment can result in up to 50,000 object instances being created by a single object type. This value is controlled by the `foglight.limit.instances` registry variable.

Registry variables have a global default value and type-specific scoped values. This means that different object types can have different instance limits.

Explore the **Instances and Limits** view to see the existing VMware object types. To access this view, on the VMware Agent Administration dashboard, click **Review Instances and Limits**.

Figure 30. Instances and Limits

The **Instances and Limits** view displays the list of the existing VMware object types, and for each type it shows the type name, instance limit, instance count, instance limit utilization, and the current status given as a highest severity level associated with an instance of that type. This information can give you insight into the size of your database and whether additional adjustments are required to improve your system performance. For example, if an object type results in a high number of object instances, this may result in performance bottlenecks. To prevent them, check if any of these are updated recently and, if not, delete them from the database.

To view the list of existing registry variables or to edit them, click **Edit Registry Variable** in the top-left corner. For complete information about registry variables, see the *Administration and Configuration Help*.

For reference information about this view, see

Configure Metrics Collection

VMware agent has collect total 99 metrics from vCenter, but some metrics are not used to VMware dashboard and relate products (Capacity Director, Optimizer and so on), so the user can disable the collection of these metrics at this view.

For reference information about this view, see

To configure the metrics collection:

1 On the navigation panel, under **Dashboards**, choose **VMware > VMware Environment**.

2 On the VMware Environment dashboard that appears in the display area, choose **Administration > Advanced Options**, click **Metrics Collection Management**.

3 Select the agent, click the button **Collect Metrics For Dashboard Only** or **Restore The Default Setting**, and then click the button **Save Edited Configuration**. The default setting is collect all metrics.

> **i** | **NOTE:** User can also select/deselect the **Collecting** checkbox, but we wouldn't recommend it because some metrics have been used for conversion of other metrics.

Generating reports

VMware Monitoring in Foglight Evolve Cloud includes a report generation ability. This allows you to create reports using a set of predefined templates to report on the various aspects of your virtual environment. VMware Monitoring in Foglight Evolve Cloud includes a collection of predefined report templates.

You can generate, copy, and edit reports using the Reports dashboard included with the Management Server.

Available report templates

The following templates are available with VMware Monitoring in Foglight Evolve Cloud.

Table 4. VMware Monitoring in Foglight Evolve Cloud report templates

Report Template Name	Object Type	This template can be used to generate a report that…
Datastore Reclamation and Addition	Service	Shows the capacity of the selected datastores and lists the ESX hosts and virtual machines that are connected to them. Information about the logical and physical disks on the virtual machines is also displayed in this report.
Storage Reclamation And Addition By ESX Hosts	Datastore	Shows the datastore usage per ESX host.
Storage Reclamation And Addition by Virtual Machines	Service	Shows the capacity and usage of logical and physical disks on the selected virtual machines.
Virtual Machines Disk Space Addition - Detail	Service	Shows relevant details for all virtual machines with a given percentage (or less) free storage available.
Virtual Machines Disk Space Addition - Summary	Service	Summarizes relevant details for all virtual machines with a given percentage (or less) free storage available.
Virtual Machines Disk Space Reclamation - Detail	Service	Shows relevant details for all virtual machines with a given percentage (or less) free storage available.
Virtual Machines Disk Space Reclamation - Summary	Service	Summarizes relevant details for all virtual machines with a given percentage (or less) free storage available.

VMware Performance Agent configuration

The VMware Performance Agent collects data from the virtual infrastructure and sends it to the <Product Name>™ Management Server. The agent keeps track of resource utilization metrics and alerts you when certain pre-defined thresholds are reached.

VMware Performance Agent and Agent Manager configuration

On 64-bit hosts meeting the minimum system requirements, the embedded Agent Manager can be used to run VMware Performance Agents to monitor up to 500 virtual machines. If the total number of virtual machines to be monitored from a single agent host is greater than 500, an Agent Manager should be installed on a separate host.

> **i** | **IMPORTANT:** Foglight Evolve Virtual Appliance comes pre-configured to support up to 4,000 virtual machines. If you are using this product, there is no need to follow the configuration procedure described in this section.

If additional cartridges and agents are added to the environment, product performance should be monitored and agents moved off of the embedded Agent Manager to reduce the load.

Table 5. Foglight VMware Performance Agent host system requirements

	Minimum CPU	Minimum Memory	Total Monitored VMs
Windows 64-bit	2[1]	4 GB	2000
Linux 64-bit	2[1]	4 GB	2000

[1] Additional CPUs may be required for larger environments.

Monitoring more than 4000 virtual machines from a single agent host

The Agent Manager JVM usually requires additional memory to monitor more than 4000 virtual machines. The total number of virtual machines is the total from all vCenters that will be monitored from all VMware Performance agents running on the Agent Manager.

The following calculations are guidelines, not hard and fast rules. Memory requirements can vary greatly from installation to installation with similar VM counts. If insufficient memory is configured, the failure mode is easily recognizable: all agents on the Agent Manager host will go into a broken state after the agent(s) were activated for a short period of time, usually within 24 hours. In addition, the Agent Manager log will contain a line similar to the following:

```
Caused by: java.lang.OutOfMemoryError: Java heap space
```

If this is the case, add memory greater than what is shown in the calculations below, in increments of 512 MB until the agents stabilize.

JVM memory requirements for VMware Performance agents are calculated using the following formula:

```
512 MB + 0.5 MB/VM
```

According to the above formula, monitoring 4000 virtual machines requires 2560 MB of memory:

```
512 MB + 2048 MB = 2560 MB
```

This is the default setting for agents deployed on 64-bit systems.

Similarly, monitoring 8000 virtual machines requires 4608 MB of memory:

```
512 MB + 4096 MB = 4608 MB
```

This requires a change in the default Agent Manager settings.

To change the JVM memory settings:

1 Determine the amount of *additional* memory required. This will be the total from the last step above minus the default value of 2560 MB. In the example above, this is 4608 MB – 2560 MB = *2048 MB*.

2 On the agent machine, open the *baseline.jvmargs.config* file for editing. The file is located in the *<Agent_Manager_home>/state/default/config* directory.

3 Add the following lines to the `memory settings` section:

```
vmparameter.0 = "-Xms2048m";
vmparameter.1 = "-Xmx2048m";
```

> **i** | **NOTE:** If this file has been previously edited have been made to this file, increment the numeric parameters accordingly.

4 Delete the existing deployed negotiation configuration settings directory:

<Agent_Manager_home>/state/default/config/deployments

5 Restart the Agent Manager for these settings to take effect.

Host system recommendations

Dedication

When monitoring larger vCenters, the Agent Manager machine hosting the VMware Performance agents should be dedicated to this task. No other Foglight agent types should run on the host and the host should not run any other applications.

Memory

Regardless of the values set for JVM memory above, Agent Manager never allocates more than 80% of system memory. So the machine hosting the Agent Manager and VMware Performance Agents must have sufficient memory. Beyond the memory requirements of the Agent Manager, a minimum of 2 GB should be free for the operating system. In the example above for 8000 VMs and an Agent Manager memory requirement of 4608 MB, the host should have a minimum of 6656 MB - the greater of:

```
1.25 x 4608 MB = 5760 MB
```

Or:

```
2048 + 4608 MB = 6656 MB
```

If the Agent Manager is configured on a virtual machine, it is recommended that the VM use a memory reservation to ensure maximum performance.

CPU

CPU usage on the Agent Manager host is relatively low most of the time. However, usage peaks dramatically during the performance metric collection. This is normal and expected. CPU utilization consistently over 50% is an indication that additional processing power is required. As with memory, usage can vary between different installations with similar numbers of virtual machines. The following guidelines should be followed.

Table 6. CPU usage guidelines

Up to 1000 VMs	2 CPUs

Table 6. CPU usage guidelines

1000 – 4000 VMs	4 CPUs
4000+ VMs	add 1 CPU per 1000 VMs – round up when necessary

When the Agent Manager and VMware Performance agents are running on a virtual machine, the VM should be configured with CPU reservation whenever possible to ensure best performance. Lack of processing power on the Agent Manager manifests in missed collections and gaps in the data usually noticeable in various graphs throughout the Foglight for VMware dashboards.

Configuring agent properties

When an agent connects to <Product Name>™, it is provided with sets of properties that it uses to configure its correct running state. Each agent is provided with a combination of two types of properties: agent properties and shareable properties.

Default versions of these properties are installed with VMware Monitoring in Foglight Evolve Cloud. However, you can edit the default shareable and agent properties, configure agent properties that apply only to a specific agent instance, and create edited clones of shareable properties that are used by a subset of agents of a certain type.

There are two ways to access the VMware Performance Agent properties:

- On the VMware Environment dashboard, on the **Administration** tab, select an agent instance and click **Edit Properties** (see Configuring monitoring agents for data collection on page 18). This method only provides access to the Configuration properties, but not the Black List and Data Collection Scheduler properties.

- On the Agent Status dashboard, select an agent instance and click **Edit Properties**. This method provides access to the full set of VMware Performance Agent properties, and is described in this topic.

For more information about working with agent properties, see the *Administration and Configuration Guide.*

To modify agent properties:

1 Log in to the Foglight Evolve Cloud browser interface.

2 Ensure that the navigation panel is open.

   To open the navigation panel, click the right-facing arrow ▶ on the left.

3 Navigate to the VMware Performance Agent properties. An agent instance can have a combination of global and private properties. Global properties apply to all instances of the agent type, while private properties apply only to specific agent instances.

   a On the navigation panel, under **Dashboards**, choose **Administration > Agents > Agent Status**.

   > **ℹ** | **IMPORTANT:** Another way of editing the VMware Performance Agent properties is through the Agent Properties dashboard. The properties you specify on this dashboard apply to all instances of the VMware Performance Agent type. To be certain that you are editing properties for a particular agent instance, without overwriting any properties of other VMware Performance instances, use the Agent Status dashboard instead of the Agent Properties dashboard.

   b On the Agent Status dashboard, select the instance of the VMware Performance Agent whose properties you want to modify and click **Edit > Edit Properties**.

   c Click **Modify the private properties for this agent** to indicate that you want to edit the properties of the selected VMware Performance Agent instance.

   A list of agent properties appears in the display area.

The configuration of agent properties described in this section include:

- Setting the Configuration properties on page 40
- Setting the FileCollector properties on page 41
- Setting the vSwitchCollector properties on page 42
- Setting the Duplicate VM List properties on page 43
- Setting the Black List properties on page 43
- Setting the Data Collection Scheduler properties on page 45

Setting the Configuration properties

The **Configuration** properties point the VMware Performance Agent to the machine on which the Virtual Center is running, and provide some additional configuration settings.

To set the Configuration properties:

1 Locate the VMware Performance Agent's **Configuration** properties.

2 Set the **Configuration** properties as follows:

- **Host Name**: The fully qualified host name of the machine on which the Virtual Center is running.

- **Host Port**: The port number of the machine on which the Virtual Center is running that will be used by the VMware Performance Agent to connect to that machine in order to collect data from the monitored Virtual Center.

- **Performance request threads**: The number of threads in a performance request.

- **Cisco switch collection threads**: The number of threads in a Cisco switch collection.

- **Storage Collection Enabled**: If you are running <Product Name>™ for Storage Management and want to enable the VMware Performance Agent to collect the Foglight Evolve Cloud Storage data,

select **True**, otherwise, set this property to **False**. Foglight Evolve Cloud for Storage Management can help you optimize the VMware environment virtual storage and its underlying physical storage components. For more information about this product, see your Foglight Evolve Cloud for Storage Management documentation.

- **VMWare Request Timeout (sec)**: The amount of time in seconds after which a VMware request times out.

- **Default performance request timeout (sec)**. **Increased as needed**: The amount of time in seconds after which a default performance request times out.

- **Property request timeout (sec)**: The amount of time in seconds after which a property request times out.

- **Update request timeout (sec)**: The amount of time in seconds after which an update request times out.

- **Login/open/close timeout (sec)**: The amount of time in seconds after which login, open, or close requests times out.

- **Cisco switch connection timeout (sec)**: The amount of time in seconds after which a Cisco switch connection times out.

- **Cisco switch timeout (sec) for performing a single SSH command**: The amount of time in seconds after which an attempt to perform a single SSH command on a Cisco switch times out.

- **Request Timeout for HA operation (sec)**: The amount of time in seconds after which an HA operation request times out.

- **Request Timeout for move vm operation (min)**: The amount of time in minutes after which a request for an operation to move a virtual machine times out.

- **Alarms Collection Enabled**: If you want to collect VMware alarms from the monitored system, set this to **True**. Otherwise, select **False**.

- **Performance request batch size (10-50)**: The size of a performance request batch.

- **Performance submission batch size**: The size of a performance submission batch.

3 Click **Save**.

Setting the FileCollector properties

A file collector is a component that captures metrics from specific files on the monitoring system. The **FileCollector** properties instruct the VMware Performance Agent which datastores, file directories, and files to exclude from monitoring.

To set the FileCollector properties:

1 Locate the VMware Performance Agent's **FileCollector** properties.

2 Set the **FileCollector** properties as follows:

- **Excluded Datastores**: Select a list in which you want to specify the datastores that you want to exclude from monitoring. You can select or clone an existing list, and edit it, as required. The default list is `excludedDatastoresList`. Lists can be shared between multiple agent instances. For more information about list properties, see the *Administration and Configuration Help*.

    For each datastore entry in the list, set its properties as follows:

    - **Datastore Name**: The name of one or more datastores that you want to exclude from monitoring. To specify multiple datastores, you must use regular expressions.

    - **Regex Flag**: Indicates if the **Datastore Name** contains a regular expressions.

- **Excluded Folders**: Select a list in which you want to specify the file directories that you want to exclude from monitoring. You can select or clone an existing list, and edit it, as required. The default

list is `hiddenFolders`. Lists can be shared between multiple agent instances. For more information about list properties, see the *Administration and Configuration Help*.

For each directory entry in the list, set its properties as follows:

- **Folder Name**: The path to one or more directories that you want to exclude from monitoring. To specify multiple directories, you must use regular expressions.
- **Regex Flag**: Indicates if the **Folder Name** contains a regular expressions.

- **Excluded Files**: Select a list in which you want to specify the files that you want to exclude from monitoring. You can select or clone an existing list, and edit it, as required. The default list is `vmwareSrmFiles`. Lists can be shared between multiple agent instances. For more information about list properties, see the *Administration and Configuration Help*.

For each directory entry in the list, set its **File Name Regex** property to a regular expression that points to one or more files that you want to exclude from monitoring.

3 Click **Save**.

Setting the vSwitchCollector properties

A vSwitch collector is a component that captures metrics from virtual switches on the monitoring system. The **vSwitchCollector** properties instruct the VMware Performance Agent which virtual switches to monitor.

To set the vSwitchCollector properties:

1 Locate the VMware Performance Agent's **vSwitchCollector** properties.

2 Set the **vSwitchCollector** properties as follows:

- **Monitoring Switches**: Select a list in which you want to specify the VMware virtual switches that you want to monitor. You can select or clone an existing list, and edit it, as required. The default list is `monitoredSwitchList`. Lists can be shared between multiple agent instances. For more information about list properties, see the *Administration and Configuration Help*.

  For each switch entry in the list, set its properties as follows:

  - **DVS Managed Object Reference**: The managed object reference of the distributed virtual switch.
  - Switch IP: The IP address of the virtual switch.
  - Fglam IP: The IP address of the Agent Manager associated with this VMware Performance Agent instance.
  - Listening Port: The port number the virtual switch uses.
  - End Date: The date after which the virtual switch will no longer be in use.
  - Enable Data Collect: An indicator of whether this VMware Performance Agent instance collects the data about this virtual switch.

- **Other Switches (Non-VMware)**: Select a list in which you want to specify the non-VMware virtual switches that you want to monitor. You can select or clone an existing list, and edit it, as required. The default list is `monitoredSwitchList`. Lists can be shared between multiple agent instances. For more information about list properties, see the *Administration and Configuration Help*.

  For each switch entry in the list, set its properties as follows:

  - **DVS Managed Object Reference**: The managed object reference of the distributed virtual switch.
  - Switch IP: The IP address of the virtual switch.

3 Click **Save**.

Setting the Duplicate VM List properties

A duplicated virtual machine is a copy or clone of an existing VM in your environment. The **Duplicate VM List** properties indicate to the VMware Performance Agent which virtual machines are duplicates or clones of the existing VMs.

To set the Duplicate VM List properties:

1   Locate the VMware Performance Agent's **Duplicate VM List** properties.

2   Set the **Duplicate VM List** properties as follows:

   ▪   **Duplicate VM List MOR**: Select a list in which you want to specify the duplicated virtual machines. You can select or clone an existing list, and edit it, as required. The default list is `duplicateVMListList.` Lists can be shared between multiple agent instances. For more information about list properties, see the *Administration and Configuration Help*.

      For each directory entry in the list, set its **Duplicate VM Item** property to contain the managed

3   Click **Save**.

Setting the Black List properties

In some rare cases, the VMware Performance Agent can encounter ESX® hosts and virtual machines for which it cannot collect data. To prevent these problems, the VMware Performance Agent detects these entities, excludes them from data collection, and adds them to the agent black list.

Any metrics associated with these objects are not included in roll up performance metrics. When an entity is added to the agent black list, an agent message and alarm are generated makes you aware of the problem so that you can investigate it further in the monitored VMware® environment. When the issue with the entity is resolved, it can be removed from the agent black list. The next available performance collection includes this entity in the data collection request.

In addition to the list that is populated by the agent, there is a user-populated black list. You populate this list by adding ESX hosts and virtual machines that you want to exclude from data collection. This feature enables Foglight Evolve Cloud administrators to disable data collection for certain ESX hosts and virtual machines, which also prevents their performance metrics from being submitted to Foglight Evolve Cloud.

> **!** | **CAUTION: Black listing an ESX host disables data collection for that ESX host, including the collection of virtual machine, storage, and network metrics for that host.**

Any metrics associated with these objects are submitted as part of roll up metrics. For example, if a virtual machine that appears on the user-populated black list is part of a resource pool, the virtual machine performance metrics are included with the performance metrics of other virtual machines from the same resource pool. This resource pool performance data is collected and submitted to Foglight Evolve Cloud. At the same time, the black-listed virtual machine object will not appear to have any performance metrics stored for this object. ESX hosts are handled the same way in terms of rolling up performance data for clusters, datacenters, or the Virtual Center.

Each ESX host or virtual machine entry in the user black list should include the Managed Object Reference (MOR) value. The MOR value is assigned to monitored objects in the monitored VMware environment and is collected by VMware Monitoring in Foglight Evolve Cloud. This value is stored in the `Managed Object Reference` property of ESX host and virtual machine objects. You can use the Data Browser to find out the MOR values for those ESX hosts or virtual machines that you want to exclude from data collection.

The agent checks both lists during data collection. You can remove entities from either list, as required. For example, if you resolve an issue with a virtual machine that causes data collection problems, you can remove the virtual machine from the black list.

For any ESX hosts or virtual machines that you want to exclude from data collection an entry should exist in the agent or user black lists. While you can add entries to the user lists, agent black lists should only be populated by the VMware Performance Agent. Any ESX hosts or virtual machines for which you want to enable data collection must have their entries removed from either black lists.

Every VMware Performance Agent instance is associated with an agent and a user black list. Each agent instance should maintain a unique pair of these lists. Because list properties in Foglight Evolve Cloud (also known as secondary properties) are shareable properties, meaning that they are accessible to all agent instances of the type in which they are defined, you should clone an agent and a user black list for each agent instance and give them unique names.

Entities included in these lists are not included in the collection of performance metrics. Other collections are not affected by their contents.

To set the black list properties:

1 Locate the VMware Performance Agent's **BlackList** properties.

2 Associate this agent instance with a user black list.

    a Choose the user black list that you want to use for this agent instance. Click the **User BlackListed MORs** list, and select the black list. The default list is `userBlackList`.

    b Clone the selected list to create a unique user black list for this agent instance. Click **Clone** on the right.

       The **Clone userBlackList** dialog box appears.
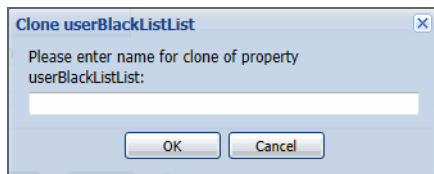
    c In the **Clone userBlackList** dialog box, type the name of the user black list. It is recommended to use a syntax that makes the list name unique and easily associated with this agent instance. For example: <*list_name*>_<*agent_name*>

    d Click **OK** to close the **Clone userBlackList** dialog box.

       The newly cloned user black list is now associated with this agent instance.

3 Edit the user black list to disable or enable data collection for particular ESX hosts or virtual machines.

    i | **IMPORTANT:** For any ESX hosts or virtual machines that you want to exclude from data collection, an entry should exist in the agent or user black lists. While you can add entries to the user lists, agent black lists should only be populated by the VMware Performance Agent. Any ESX hosts or virtual machines for which you want to enable data collection must have their entries removed from either black lists.

    a Click **Edit** on the right of the **User BlackListed MORs** list.

       The **VMwarePerformance - userBlackList** dialog box appears.
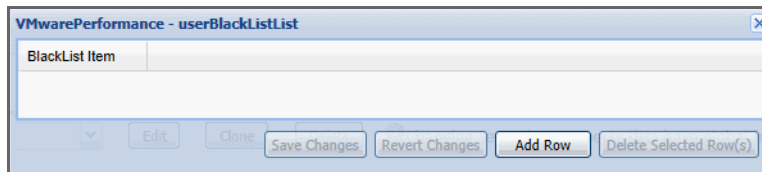
    b To disable data collection for an ESX host or virtual machine, add it to the list.

       i | **IMPORTANT:** Black listing an ESX host disables data collection for that ESX host, including the collection of virtual machine, storage, and network metrics for that host.

       To black list an ESX host or virtual machine, click **Add Row**, and in the new row that appears, in the **BlackList Item** column, specify the ESX host or virtual machine using the following syntax:

       <**host**|**vm**>-<*MOR*>

       Where:

- **host**: Indicates that the black list item is an ESX host.

- **vm**: Indicates that the black list item is a virtual machine.

- *MOR*: The value of the Managed Object Reference property of the ESX host or virtual machine that you want to exclude from data collection.

  For example: `vm-20123`

  > **i** | **TIP:** You can use the Data Browser to find out the MOR values for those ESX hosts or virtual machines that you want to exclude from data collection.

c To enable data collection for an ESX host or virtual machine, remove it from the list. Select the ESX host or virtual machine entry in the list, and click **Delete Selected Row(s)**.

The list refreshes, no longer showing the deleted entry.

4 Click **Save**.

Setting the Data Collection Scheduler properties

Use the Data Collection Scheduler properties to adjust how frequently the VMware Performance Agent collects data from the monitored server.

To set the data collection properties:

1 Locate the VMware Performance Agent's **Data Collection Scheduler** properties.

2 Set the **Data Collection Scheduler** properties as follows:

a Select a collection configuration list. You can select or clone an existing collection configuration list, and edit it, as required.

b Add, remove, or edit collectors in the list.

c For each collector, set its properties as follows:

- **Collector Name**: The name of the collector. A collector is a component that captures specific type of metrics. Existing collectors are: **Relationship And Hierarchy Data**, **Inventory Entity Properties**, **Performance Metrics**, and **Events Collection**.

- **Default Collection Interval**: Contains the length of the default collection interval. The default collection intervals for the existing collectors are:

  Relationship and Hierarchy: 2 minutes

  Inventory Entity Properties: 5 minutes

  Performance Metrics: 5 minutes

  Events Collection: 3 minutes

- **Time Unit**: Contains the time unit for measuring the default collection interval: milliseconds, seconds, minutes, hours, or days.

- **Fast-Mode Collection Interval**: Contains the length of the collection interval when the agent is running in fast mode.

- **Fast-Mode Time Unit**: Contains the length of the collection interval when the agent is running in fast mode.

- **Fast-Mode Max Count**: Contains the maximum count of entries when the agent is running in fast mode.

Reference

This chapter contains reference information about views, rules, and data tables that are included with VMware Monitoring in Foglight® Evolve Cloud. Read this chapter to find out details about these components.

- Views
- Rules

Views

VMware Monitoring in Foglight® Evolve Cloud ships with predefined views to help you monitor your application server environment. This chapter provides quick reference information about each view.

VMware Monitoring in Foglight Evolve Cloud displays monitoring data in views that group, format, and display data. The main types are described below.

Dashboards are top-level views that do not receive data from other views. Dashboards usually contain a number of lower-level views. The dashboards supplied with VMware Monitoring in Foglight Evolve Cloud, as well as those created by users, are available in the navigation panel.

Lower-level views in VMware Monitoring in Foglight Evolve Cloud can be added to dashboards or can be accessed by drilling down from a dashboard. They receive and display data directly from the VMware Monitoring in Foglight Evolve Cloud Management Server or from other views. Some views filter or select data that appears in other views in the same dashboard. Some are tree views with expandable nodes for selecting servers, applications, or data.

VMware Monitoring in Foglight Evolve Cloud ships with several dashboards that allow you to monitor and configure your virtual environment. Each of these dashboards contains a number of views. This section describes these views in more detail. For more information about the VMware dashboards, see Interacting with VMware Monitoring in Foglight Evolve Cloud.

VMware Monitoring in Foglight Evolve Cloud includes the following groups of views:

- VMware Explorer views
- VMware Agent Administration views

VMware Explorer views

The VMware Explorer dashboard contains the following views:

- FAQts tab
- Resource Pools Relationship Tree view
- Storage tab (Cluster)
- Storage tab (Datacenter)
- Storage tab (ESX Host)
- Storage tab (Virtual Machine)
- Summary tab

- Summary (All Clusters) tab

- Summary (All Datacenters) tab

- Summary (All Resource Pools) tab

- Summary (All Servers) tab

- Summary (All Virtual Machines) tab

- Virtual Infrastructure view

ℹ️ | **NOTE:** The Administration tab is only available in Foglight Pro, when the Virtual-VMware-Admin and Virtual-HyperV cartridges are installed. It is not included with Foglight SE. In Foglight Pro, this tab is accessible if your Foglight user account includes the VMware Automation User role.

FAQts tab

Purpose

Through three embedded views (the Categories, Question, and Answer views), the **FAQts** tab enables you to ask VMware Monitoring in Foglight Evolve Cloud questions and provides the answers to those questions.

Figure 31. FAQts tab
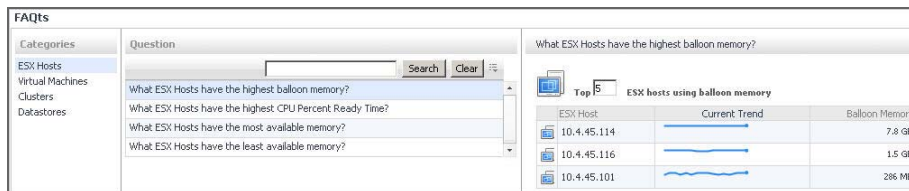
How to Get Here

The **FAQts** view appears on both the Virtual Environment Summary and VMware Explorer dashboards as a navigation tab.

Description of Embedded Views

The FAQts view is made up of the following embedded views:

- Answer

- Categories

- Questions

Answer

This view provides an answer to the question selected in the Questions view. The answer appears in the following form:

Top *x* *<objects of category>…*

where *x* is the number of objects of the category you provided in the Categories view.

Specify *x* by entering a number. The answer is relative to the subset of the infrastructure you are viewing in the dashboard. For example, the top 5 datastores are different for each individual cluster in the infrastructure.

Categories

This view lists the categories for which questions can be answered for you by VMware Monitoring in Foglight Evolve Cloud.

Click a category in the list to select it.

Questions

This view lists the questions, for the category selected in the Categories, that can be answered for you by VMware Monitoring in Foglight Evolve Cloud.

Click a question in the list to select it.

If the list of questions is long and you want to narrow it down, search for a particular text string using the **Search** box.

Resource Pools Relationship Tree view

Purpose

The Resource Pools Relationship Tree view is provided in the VMware Explorer dashboard. If you select a Resource Pool container from the Topology view on the Virtual Infrastructure view and click the Summary navigation tab within the VMware Explorer Primary view, a Resource Pools Relationship Tree view is displayed in the Primary view. A Resource Pools Relationship Tree contains every resource pool that belongs to the clusters within the associated VirtualCenter.

For more information about the VMware Explorer dashboard, see Investigating performance metrics on page 24.

The Resource Pools Relationship Tree view is useful if you want to see how the resource pools within the clusters are laid out or if you want to take a look at the utilization statistics for each configured resource pool on the VirtualCenter.

Figure 32. Resource Pools Relationship Tree view
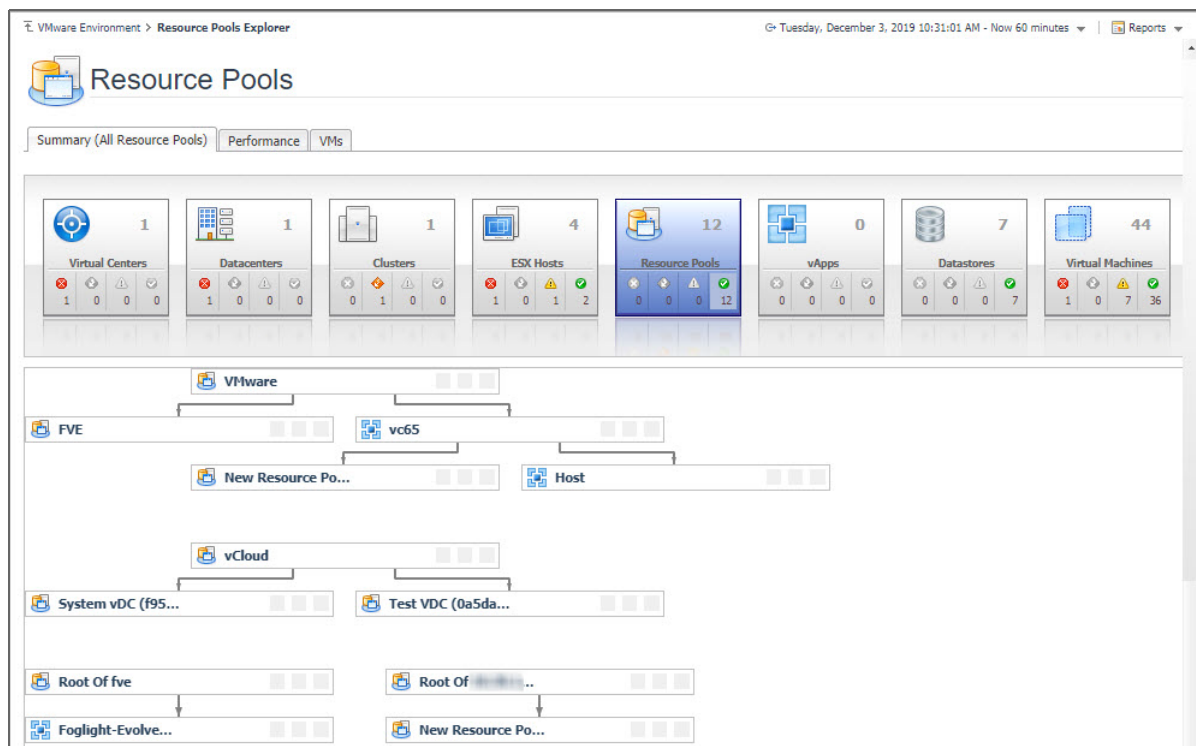
The default Resource Pools Relationship Tree simply displays the names of the various resource pools and their parent/child relationships.

You can use the Normal Zoom Level button on the mini map at the top right of the Relationship Tree to zoom into a more detailed version of the Tree. You can use the Minimized Zoom Level button on the mini map to zoom back out again.

You can browse through a Relationship Tree by clicking and dragging the rectangular shadow provided on the mini map.

Storage tab (Cluster)

Purpose

The VMware Explorer's **Storage** tab displays the disk storage capacity associated with the selected component. Selecting a cluster and opening this tab displays the storage metrics associated with the selected cluster.

Figure 33. Storage tab (Cluster)
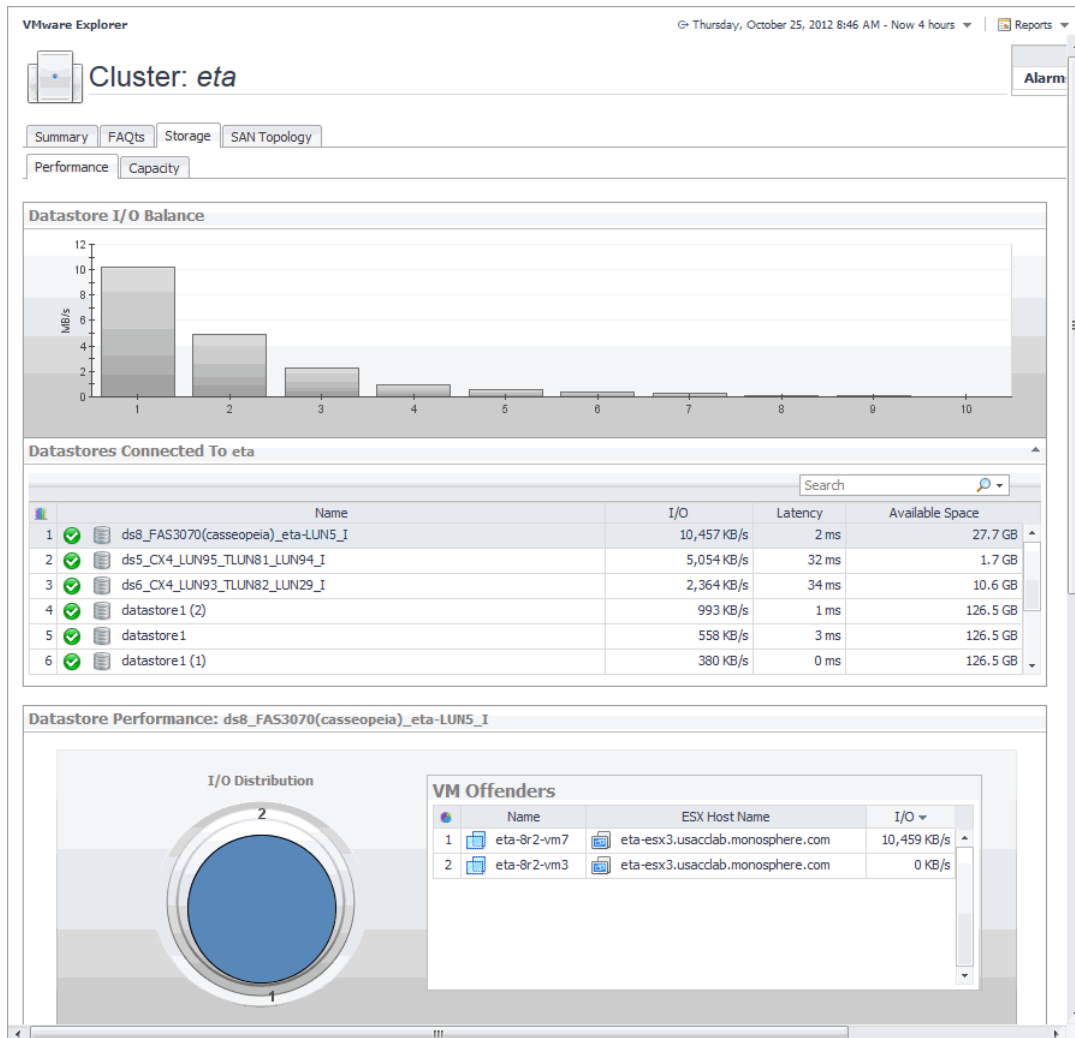
How to Get Here

1   Open the VMware Explorer.

2   On the Virtual Infrastructure view, that appears on the navigation panel, select a cluster.

3   In the VMware Explorer, open the **Storage** tab.

Description of Embedded Views

This view is made up of the following embedded views:

- Capacity: Datastore (Capacity tab)

- Datastore Capacity Balance (Capacity tab)

- Datastore I/O Balance (Performance tab)

- Datastores Connected to Cluster (Performance and Capacity tabs)

- ESX Hosts (Performance tab)

- ESX I/O Balance (Performance tab)

- Performance: Datastore (Performance tab)

Table 7. Capacity: Datastore (Capacity tab)

Description	This view contains information about the selected datastore data capacity.
Data displayed	• **Datastore, In Use**. The percentage of disk space in use.
	• **Most Available, Available Space**. The disk space available on the datastore.
	• **Most Available, Name**. The name of the datastore.
	• **VMs On Datastore, Allocated**. The amount of memory allocated to the virtual machine.
	• **VMs On Datastore, In Use**. The amount of memory used by the virtual machine.
	• **VMs On Datastore, Name**. The name of the virtual machine associated with the datastore.

Table 8. Datastore Capacity Balance (Capacity tab)

Description	This view shows the datastore capacity for each datastore connected to the selected cluster.

Table 9. Datastore I/O Balance (Performance tab)

Description	This view shows the data transfer rates for each datastore connected to the selected cluster.

Table 10. Datastores Connected to Cluster (Performance and Capacity tabs)

Description	This view lists the datastores connected to the selected cluster and shows performance metrics associated with each datastore.
Data displayed	• **Available Space**. The amount of available space on the datastore.
	• **I/O**. The datastore data transfer rates.
	• **Latency**. The datastore latency.
	• **Name**. The datastore name and its alarm status.

Table 11. ESX Hosts (Performance tab)

Description	This view lists the ESX hosts belonging to the selected cluster and associated with the selected datastore, and shows performance metrics associated with each ESX host.
Data displayed	• **Name**. The ESX host name or IP address.
	• **Read**. The ESX host data read rates.
	• **Read Latency**. The ESX host read latency.
	• **Write**. The ESX host data write rates.
	• **Write Latency**. The ESX host write latency.

Table 12. ESX I/O Balance (Performance tab)

Description	This view shows the data transfer rates each ESX host belonging to the selected cluster and associated with the selected datastore.

Table 13. Performance: Datastore (Performance tab)

Description	This view shows the amount I/O resources used by the virtual machines associated with the selected datastore.
Data displayed	• **I/O Distribution**. A pie chart indicating how much the individual virtual machines contributed to the use of I/O resources. • **VM Offenders, Name**. The name of the virtual machine. • **VM Offenders, ESX Host Name**. The name of the ESX host on which the ESX machine is running. • **VM Offenders, I/O**. The data transfer rate for the virtual machine.

Storage tab (Datacenter)

Purpose

The VMware Explorer's **Storage** tab displays the disk storage capacity associated with the selected component. Selecting a data center and opening this tab displays storage metrics for all Datastores associated with the selected Datacenter.

Figure 34. Storage tab (Datacenter)
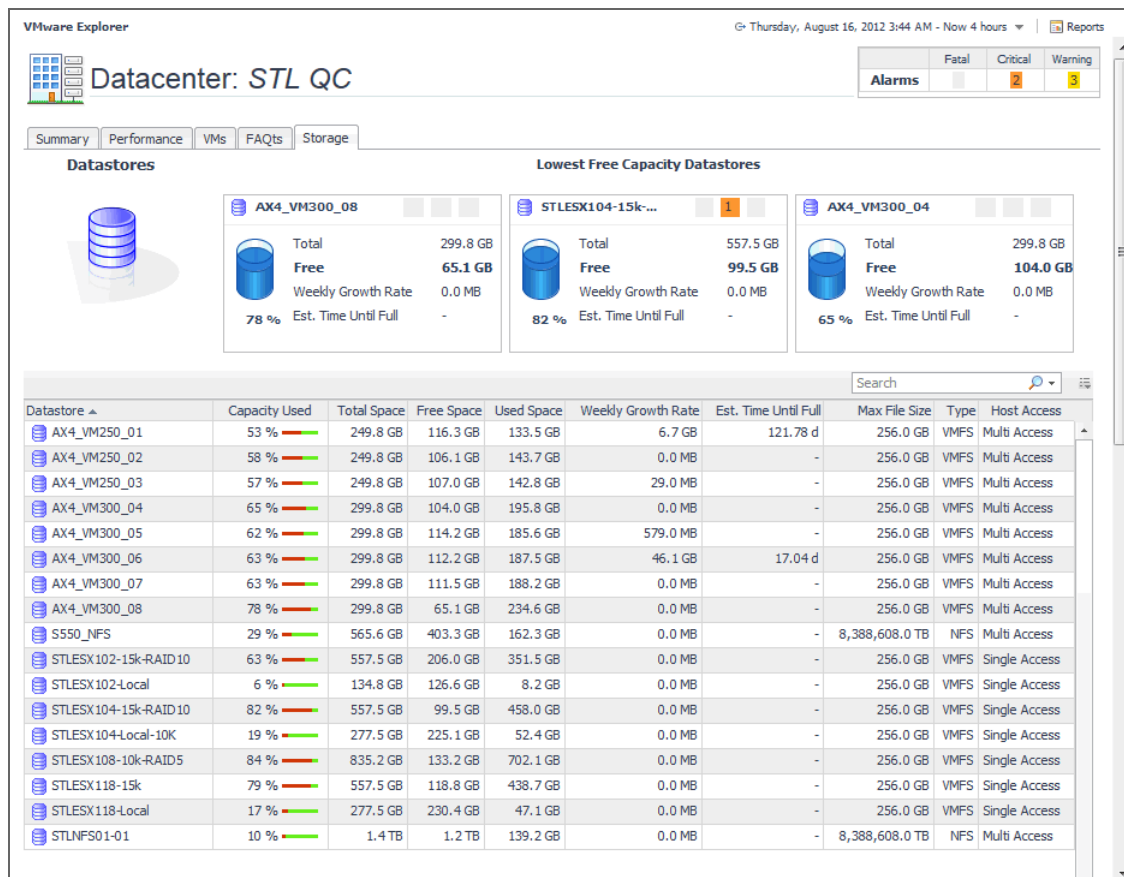
How to Get Here

1   Open the VMware Explorer.

2   On the Virtual Infrastructure view, that appears on the navigation panel, select a Datacenter.

3   In the VMware Explorer, open the **Storage** tab.

Description of Embedded Views

This view is made up of the following embedded views:

* Lowest Free Capacity Datastores

* Datastores

Table 14. Lowest Free Capacity Datastores

Description	The **Storage** tab displays three tiles, identifying the datastores with the lowest amount of free space.
	This view contains information about the used, free, and total space of the selected components' datastores, along with projected short-term estimates, given the current growth patterns.
Data displayed	• **Datastore**. The name of the selected datastore, followed by the related alarm counts.
	• **Est. Time Until Full**. The estimated amount of time until which this datastore will become full.
	• **Free**. The amount of free space for this datastore.
	• **Total**. The total amount of space for this datastore.
	• **Weekly Growth Rate**. The average amount of space the datastore expands every week.

Table 15. Datastores

Description	Lists the datastores associated with the selected datacenter, and shows storage metrics associated with each datastore.
Data displayed	• **Capacity Used**. The current percentage of the used disk space.
	• **Datastore**. The datastore name.
	• **Est. Time Until Full**. The estimated time after which the disk will be full.
	• **Free Space**. The amount of disk space that is free.
	• **Host Access**. The host access type.
	• **Max File Size**. The maximum file size.
	• **Total Space**.The total disk space, including used and free space.
	• **Type**. The file system type.
	• **Used Space**. The amount of used disk space.
	• **Weekly Growth Rate**. The estimated growth pattern of the used disk space.

Storage tab (ESX Host)

Purpose

The VMware Explorer's **Storage** tab displays the disk storage capacity associated with the selected component. Selecting an ESX host and opening this tab displays the storage metrics associated with the selected ESX host.

Figure 35. Storage tab (ESX Host)
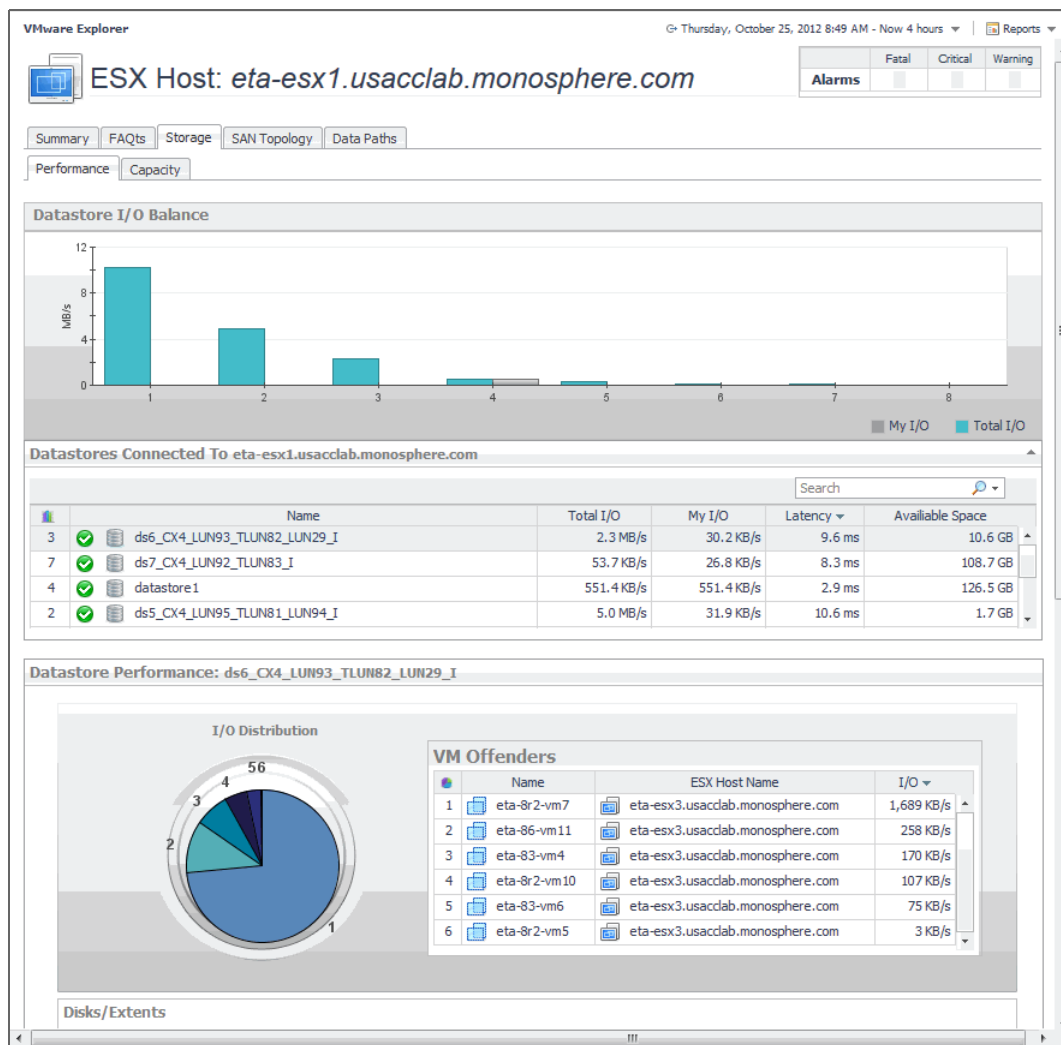
How to Get Here

1. Open the VMware Explorer.

2. On the Virtual Infrastructure view, that appears on the navigation panel, select an ESX host.

3. In the VMware Explorer, open the **Storage** tab.

Description of Embedded Views

This view is made up of the following embedded views:

- Datastore Capacity (Capacity tab)

- Datastore Capacity Balance (Capacity tab)

- Datastore I/O Balance (Performance tab)

- Datastore Performance (Performance tab)

- Datastores Connected to ESX Host (Performance and Capacity tabs)

- Storage Adaptor Utilization (Performance tab)

- Storage Adaptors (Performance tab)

Table 16. Datastore Capacity (Capacity tab)

Description	This view contains information about the selected datastore data capacity.
Data displayed	• **Datastore, In Use**. The percentage of disk space in use. • **Most Available, Available Space**. The disk space available on the datastore. • **Most Available, Name**. The name of the datastore. • **VMs On Datastore, Allocated**. The amount of memory allocated to the virtual machine. • **VMs On Datastore, In Use**. The amount of memory used by the virtual machine. • **VMs On Datastore, Name**. The name of the virtual machine associated with the datastore.

Table 17. Datastore Capacity Balance (Capacity tab)

Description	This view shows the datastore capacity for each datastore connected to the selected ESX host.

Table 18. Datastore I/O Balance (Performance tab)

Description	This view shows the data transfer rates for each datastore connected to the selected ESX host.

Table 19. Datastore Performance (Performance tab)

|	
Description	This view shows a the amount I/O resources used by the virtual machines associated with the selected datastore.
Data displayed	• **Disks/Extents, Name** (VMFS and NFS datastores only). The name of the disk associated with the datastore. For more information about VMFS and NFS datastores, see Datastores on page 9. • **Disks/Extents, Read** (VMFS and NFS datastores only). The rate at which the data is read from the disk. • **Disks/Extents, Read Latency** (VMFS and NFS datastores only). The read latency of the disk. • **Disks/Extents, Write** (VMFS and NFS datastores only). The rate at which the data is written to the disk • **Disks/Extents, Write Latency** (VMFS and NFS datastores only). The write latency of the disk. • **I/O Distribution**. A pie chart indicating how much the individual virtual machines contributed to the use of I/O resources. • **VM Offenders, Name**. The name of the virtual machine. • **VM Offenders, ESX Host Name**. The name of the ESX host on which the ESX machine is running.

Table 19. Datastore Performance (Performance tab)

> - **VM Offenders, I/O**. The data transfer rate for the virtual machine.
> - **Vsan Disks** (VSAN datastores only). Click **Explore Physical Disks** view to display the more information about physical disks.

> For more information about VSAN datastores, see VSAN datastores on page 9.

Table 20. Datastores Connected to ESX Host (Performance and Capacity tabs)

Description	This view lists the datastores connected to the selected ESX host and shows performance metrics associated with each datastore.
Data displayed	• **Available Space**. The amount of available space on the datastore.
	• **Latency**. The datastore latency.
	• **My I/O**. The datastore data transfer rates associated with the selected ESX host.
	• **Name**. The datastore name and its alarm status.
	• **Total I/O**. The total datastore data transfer rate.

Table 21. Storage Adaptor Utilization (Performance tab)

Description	This view shows the data transfer rates for each storage adaptor associated with the selected ESX host.

Table 22. Storage Adaptors (Performance tab)

Description	This view lists the storage adaptors associated with the selected ESX host, and shows performance metrics for each adaptor.
Data displayed	• **Name**. The storage adaptor name.
	• **Read**. The storage adaptor data read rates.
	• **Read Latency**. The storage adaptor read latency.
	• **Write**. The storage adaptor data write rates.
	• **Write Latency**. The storage adaptor write latency.

Storage tab (Virtual Machine)

Purpose

The VMware Explorer's **Storage** tab displays the disk storage capacity associated with the selected component. Selecting a virtual machine and opening this tab displays the storage metrics associated with the selected virtual machine.

Figure 36. Storage tab (Virtual Machine)
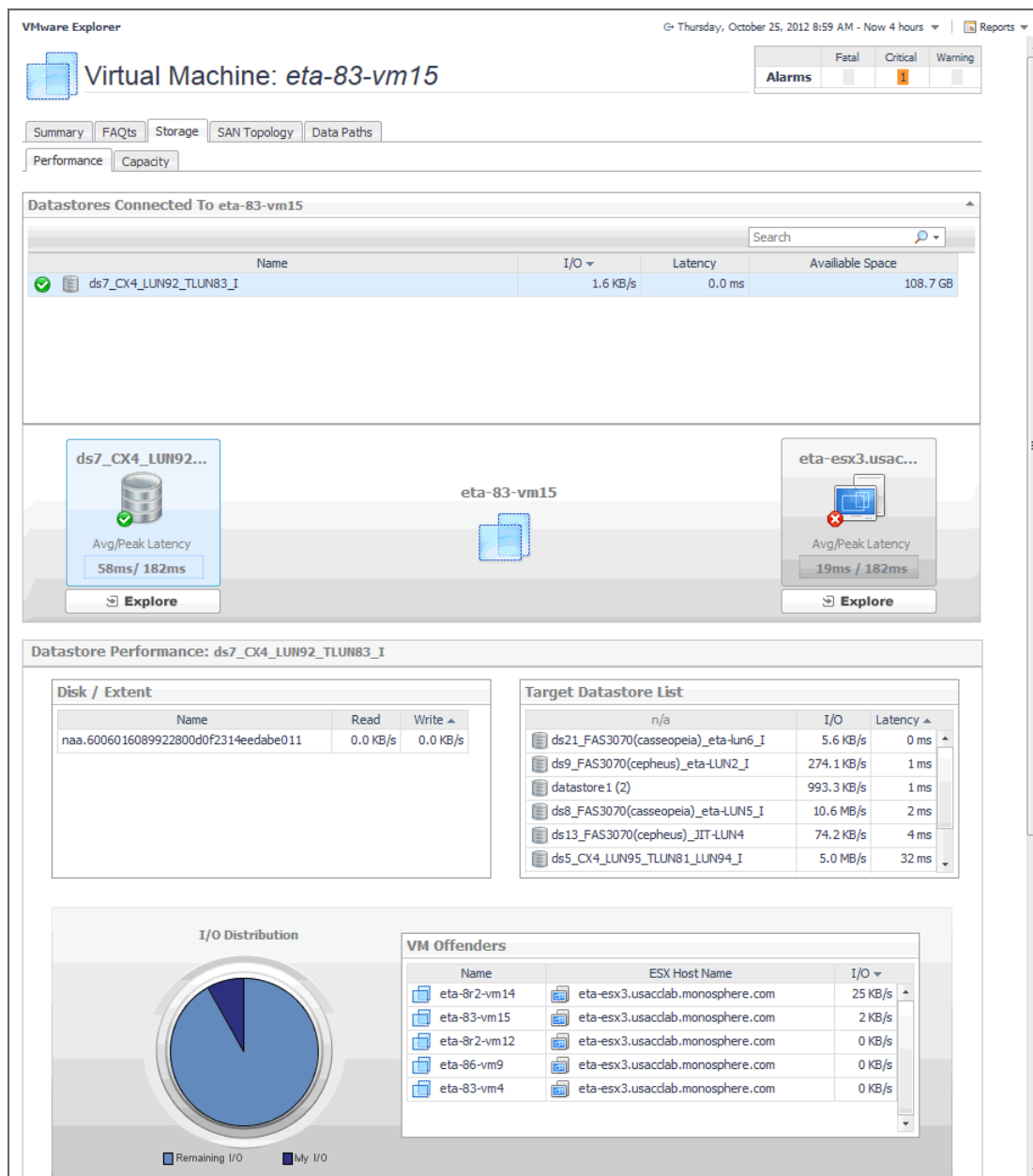
How to Get Here

1   Open the VMware Explorer.

2   On the Virtual Infrastructure view, that appears on the navigation panel, select a virtual machine.

3   In the VMware Explorer, open the **Storage** tab.

Description of Embedded Views

This view is made up of the following embedded views:

• Datastore Capacity (Capacity tab)

• Datastore Performance (Performance tab)

• Datastores Connected to Virtual Machine (Performance and Capacity tabs)

- Virtual Machine Capacity (Capacity tab)

Table 23. Datastore Capacity (Capacity tab)

Description	This view contains information about the selected datastore and virtual machine data capacity.
Data displayed	• **Datastore, Current Utilization, Allocated**. The amount and percentage of disk space allocated to the datastore.
	• **Datastore, Current Utilization, Available Space**. The disk space available on the datastore.
	• **Datastore, Current Utilization, Capacity**. The total disk space on the datastore.
	• **Datastore, Current Utilization, In Use**. The amount and percentage of disk space the datastore uses.
	• **Datastore, In Use**. The percentage of disk space in use by the datastore.
	• **Virtual Machine, Current Utilization, Allocated**. The amount and percentage of disk space allocated to the virtual machine.
	• **Virtual Machine, Current Utilization, In Use**. The amount and percentage of disk space the virtual machine uses.
	• **Virtual Machine, In Use**. The percentage of disk space in use by the virtual machine.

Table 24. Datastore Performance (Performance tab)

Description	This view shows the amount of I/O resources used by the datastore associated with the selected virtual machine.
Data displayed	• **Disk/Extent, Name**. The name of the disk associated with the datastore.
	• **Disk/Extent, Read**. The read rate of the disk associated with the datastore.
	• **Disk/Extent, Write**. The write rate of the disk associated with the datastore.
	• **I/O Distribution**. A pie chart indicating how much the selected virtual machines contributes to the overall use of I/O resources.
	• **Target Datastore List, I/O**. The data transfer rate of the target datastore.
	• **Target Datastore List, Latency**. The data transfer latency of the target datastore.
	• **Target Datastore List, Name**. The name of the target datastore.
	• **VM Offenders, ESX Host Name**. The name of the ESX host on which the ESX machine is running.
	• **VM Offenders, I/O**. The data transfer rate for the virtual machine.
	• **VM Offenders, Name**. The name of the virtual machine.

Table 25. Datastores Connected to Virtual Machine (Performance and Capacity tabs)

Description	This view lists the datastores connected to the selected virtual machine and shows performance metrics associated with each datastore.
Data displayed	• **Available Space**. The amount of available space on the datastore.
	• **Datastore, Avg/Peak Latency**. The average and peak latency rates for the selected datastore.
	• **ESX Host, Avg/Peak Latency**. The average and peak latency rates for the ESX host associated with the selected virtual machine.
	• **Latency**. The datastore latency.
	• **I/O**. My I/O. The datastore data transfer rates associated with the selected ESX host.
	• **Name**. The datastore name and its alarm status.
	• **Total I/O**. The total datastore data transfer rate.

Table 26. Virtual Machine Capacity (Capacity tab)

Description	This view lists the logical disks associated with the selected virtual machines and shows their performance metrics.
Data displayed	• **Available Space**. The space currently available on the logical disk.
	• **Capacity**. The logical disk capacity.
	• **In Use**. The amount of disk space used by the logical disk.
	• **Logical Disk**. The name of the logical disk.
	• **Time To Full**. The estimated time after which the disk will be full.
	• **Total Space**. The total space allocated to the logical disk.
	• **Weekly Growth Rate**. The estimated growth pattern of the used disk space.

Summary tab

Purpose

The Summary view provides a hierarchical inventory, in the form of tiles, of the objects that are related to the object or group of objects selected.

Figure 37. Summary tab
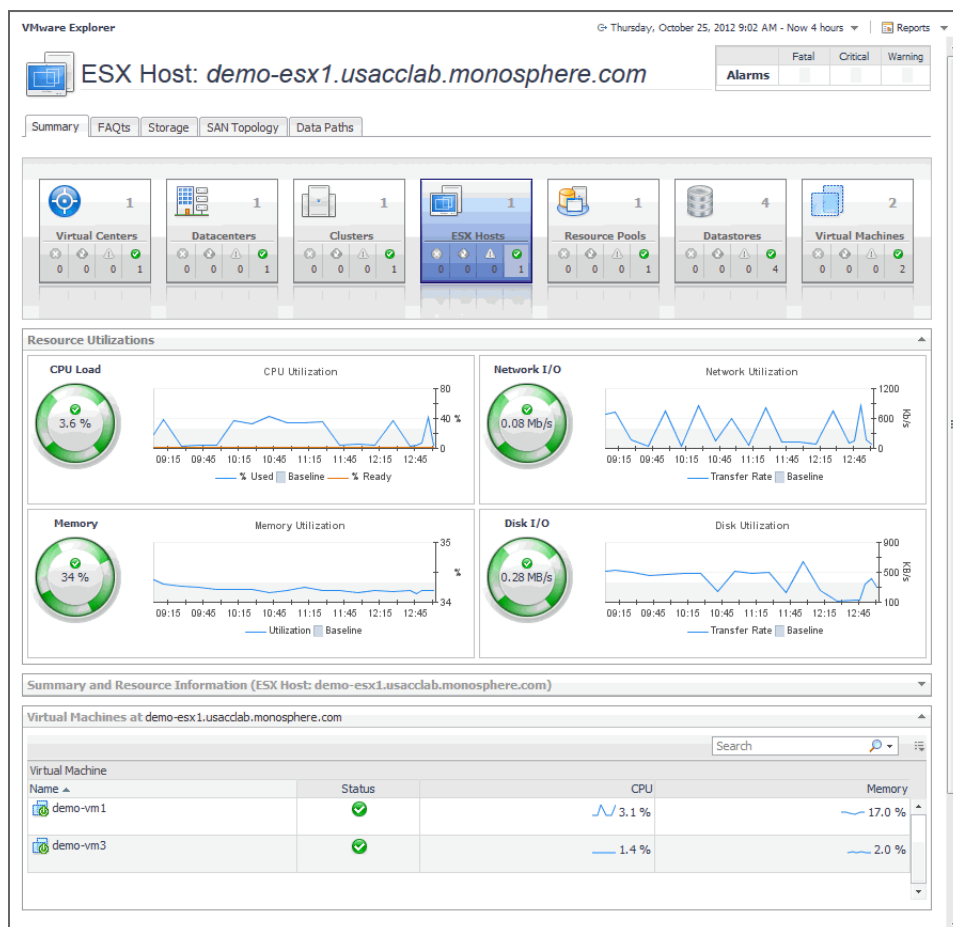
Each tile shows the number of instances of the corresponding object type, as well as the counts of objects of that type in each of the alarm states (Normal, Warning, Critical, Fatal).

More detailed information for the selected object or objects is displayed in the collapsible views below the Summary view.

On a tile, click the object type icon, the object type name, or the object count, to view a popup that lists all objects of the corresponding type, along with their respective states. Click a column header on the popup to change the sort order. Click an object in the popup list to view details for that object in the VMware Explorer dashboard.

On a tile, click an alarm state icon or the number below it to view a popup that shows the outstanding alarms of that state for the corresponding object type.

If an alarm state has a count of zero, then you can not select that alarm state. When you click a normal state icon or count, the VMware Explorer page is refreshed, but you do not see an alarm popup because there are no alarms associated with the normal state.

How to Get Here

1   Open the VMware Explorer.

2   In the Virtual Infrastructure view, select a Virtual Center, datacenter, cluster, ESX host, resource pool, or a virtual machine.

    The Summary tab is the first tab you see open in the display area.

Description of Embedded Views

This view is made up of the following embedded views:

* Cluster

* ESX Hosts

* Notes

* Resource Pool

* Resource Utilizations

* Servers

* Summary and Resource Information

* Virtual Environment

* Virtual Machines

* Virtual Machine and Resource Pool Changes

Table 27. Cluster

Description	Shows a list of clusters associated with the selected datacenter. **NOTE:** This view only appears when viewing datacenter details.
Data displayed	• **CPU Used**. The amount of CPU processing power used by all ESX hosts associated with the cluster and the selected datacenter. • **Hosts**. The number of ESX hosts associated with the cluster and the selected datacenter. • **Memory**. The percentage of total memory used by all ESX hosts associated with the cluster and the selected datacenter. • **Name**. The cluster name. • **Resource Pools**. The number of resource pools associated with the cluster and the selected datacenter. • **Status**. The status of the cluster, associated with any alarms raised against that virtual machine. If no alarms are fired, the status appears as Normal. Otherwise, the status is set to the alarm severity (Warning, Critical, or Fatal).
Where to go next	Drill down on any cluster entry. The Summary tab refreshes, showing the cluster details

Table 28. ESX Hosts

Description	Shows a list of ESX hosts associated with the selected cluster or datacenter. **NOTE:** This view only appears when viewing cluster or datacenter details.
Data displayed	• **ESX Host, CPU**. The amount of CPU processing power used by the ESX host. • **ESX Host, HBAs**. The number of host adapters that exist on the ESX host. • **ESX Host, Memory**. The percentage of total memory used by the ESX host. • **ESX Host, Name**. The virtual machine name. • **ESX Host, NICs**. The number of network interface cards that exist on the ESX host. • **ESX Host, Status**. The status of the virtual machine, associated with any alarms raised against that virtual machine. If no alarms are fired, the status appears as Normal. Otherwise, the status is set to the alarm severity (Warning, Critical, or Fatal). • **ESX Host, Version**. The version of the VMware ESX Server application installed on the host. • **Virtual Machines, Configured**. The number of virtual machines that are configured to run on the ESX host. • **Virtual Machines, Running**. The number of virtual machines currently running on the host.
Where to go next	Drill down on any ESX host entry. The Summary tab refreshes, showing the ESX host details.

Table 29. Notes

Description	Shows additional notes about the selected virtual machine. **NOTE:** This view only appears when viewing virtual machine details.

Table 30. Resource Pool

Description	For complete information about this view, see Resource Pools Relationship Tree view on page 48.

Table 31. Resource Utilizations

Description	Shows the resource consumption for the selected cluster, server, or virtual machine broken down into four simple views.
Data displayed	• **CPU Load**. The current percentage of the selected component's (cluster, server, or virtual machine) CPU load, used to execute system code and user programs, based on the total CPU capacity available to that component. • **CPU Utilization, % Used**. The percentage of the selected component's (cluster, server, or virtual machine) CPU utilization spent on executing system code and user programs during the selected time period. • **CPU Utilization, % Ready**. The percentage of the selected component's (cluster, server, or virtual machine) CPU resources that are ready to execute system code and user programs during the selected time period. • **CPU Utilization, Baseline**. An envelope indicating the expected CPU utilization range based on historical data. **NOTE:** This information is only available when exploring ESX hosts or virtual machines. • **Datastore I/O**. The current datastore I/O rate for the selected ESX host. **NOTE:** This information is only available when exploring ESX hosts.

Table 31. Resource Utilizations

- **Datastore Utilization, Baseline**. An envelope indicating the expected datastore utilization range based on historical data.

  NOTE: This information is only available when exploring ESX hosts.

- **Datastore Utilization, Transfer Rate**. The rate at which data was read from and written to the datastore of the selected ESX host during the specified time period.

  NOTE: This information is only available when exploring ESX hosts.

- **Datastore Utilization, Write Rate**. The rate at which data was written to the datastore of the selected component during the specified time period.

  NOTE: This information is only available when exploring ESX hosts.

- **Datastore I/O**. The current datastore I/O rate for the selected server or cluster.

  NOTE: This information is only available when exploring ESX hosts.

- **Disk Utilization, Baseline**. An envelope indicating the expected disk utilization range based on historical data.

  NOTE: This information is only available when exploring datacenters, clusters, resource pools, virtual machines, or virtual centers.

- **Disk Utilization, Transfer Rate**. The rate at which data was read from and written to the disks of the selected component during the specified time period.

  NOTE: This information is only available when exploring datacenters, clusters, resource pools, virtual machines, or virtual centers.

- **Disk Utilization, Write Rate**. The rate at which data was written to the disks of the selected component during the specified time period.

  NOTE: This information is only available when exploring datacenters, clusters, resource pools, virtual machines, or virtual centers.

- **Disk I/O**. The current disk I/O rate for the selected server or cluster.

  NOTE: This information is only available when exploring datacenters, clusters, resource pools, virtual machines, or virtual centers.

- **Memory Usage**. The current percentage of the average memory usage by the selected component (server or cluster).

- **Memory Utilization, Baseline**. An envelope indicating the expected memory utilization range based on historical data.

  NOTE: This information is only available when exploring ESX hosts or virtual machines.

- **Memory Utilization, Utilization**. The percentage of the available memory that the selected component (server or cluster) uses during the specified time period.

- **Network I/O**. The current rate at which the selected component (cluster, server, or virtual machine) transfers data from and to the network.

- **Network Utilization, Baseline**. An envelope indicating the expected network utilization range based on historical data.

  NOTE: This information is only available when exploring ESX hosts or virtual machines.

- **Network Utilization, Transfer Rate**. The rate at which the selected component (cluster, server, or virtual machine) receives and sends data to the network during the selected time period.

Where to go next   Drill down on:

Table 31. Resource Utilizations

- **CPU Load** spinner. Displays the **CPU Load** dialog box.
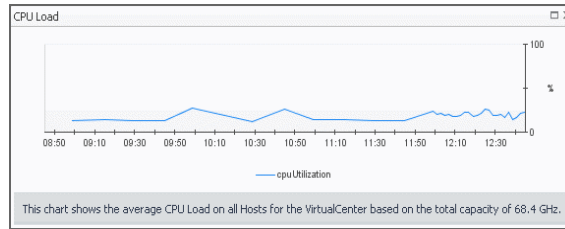
- **CPU Utilization** graph. Displays the **CPU Utilization** dialog box.
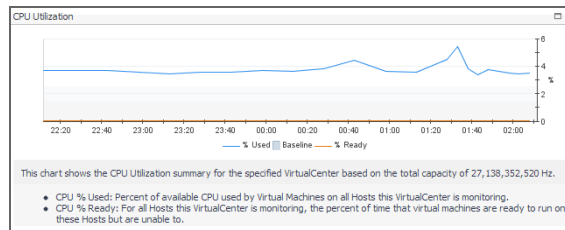
- **Disk I/O** spinner. Displays the **Disk I/O** dialog box.
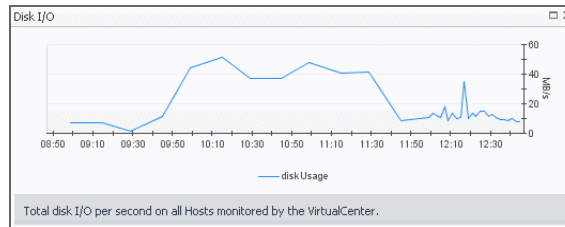
NOTE: This drilldown is only available when viewing server or cluster details in the VMware Explorer.

- **Disk Utilization** graph. Displays the **Disk Utilization** dialog box.
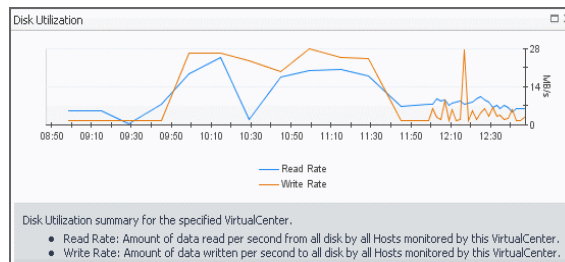
NOTE: This drilldown is only available when viewing server or cluster details in the VMware Explorer.

- **Memory Usage** spinner. Displays the **Memory Usage** dialog box.
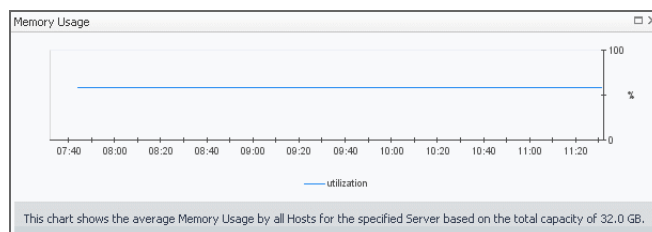
NOTE: This drilldown is only available when viewing server or cluster details in the VMware Explorer.

Table 31. Resource Utilizations

  • **Memory Utilization** graph. Displays the **Memory Utilization** dialog box.
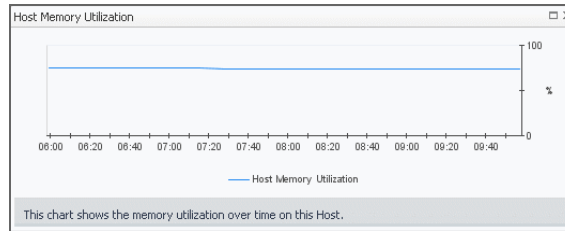
> **NOTE:** This drilldown is only available when viewing server or cluster details in the VMware Explorer.

  • **Network I/O** spinner. Displays the **Network I/O** dialog box.
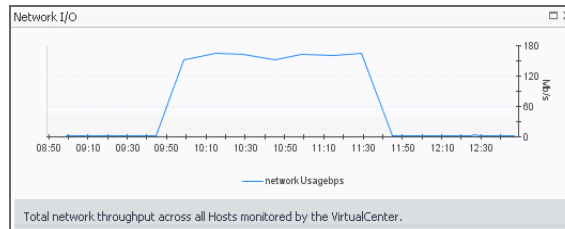
  • **Network Utilization** graph. Displays the **Network Utilization** dialog box.
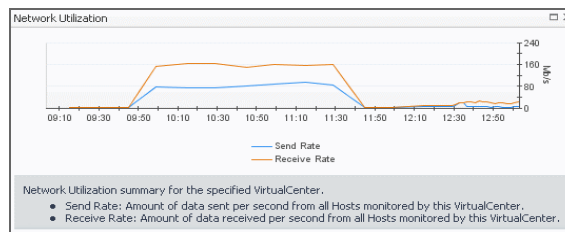
Table 32. Servers

Description	Shows a list of servers that belong to the selected cluster. **NOTE:** This view only appears when viewing cluster details.
Data displayed	• **Server, CPU**. The current percentage of the server's CPU load, used to execute system code and user programs, based on the total CPU capacity. • **Server, Memory**. The current percentage of the server's memory usage by the selected component. • **Server, NICs**. The number of network interface cards that the server uses. • **Server, Server Name**. The server name. • **Server, Status**. The server status, associated with any alarms raised against that server. If no alarms are fired, the status appears as Normal. Otherwise, the status is set to the alarm severity (Warning, Critical, or Fatal). • **Server,** Version. The operating system version. • **Virtual Machines, Configured**. The number of virtual machines that exist on the server. • **Virtual Machines, Running**. The number of virtual machines that are currently running on the server.
Where to go next	Drill down on any server entry. The VMware Explorer dashboard appears, showing the server details on the Summary tab.

Table 33. Summary and Resource Information

Description	Shows physical configuration details for the selected server or virtual machine.
Data displayed	**Data appearing when viewing cluster details:**

- **Datacenter**. The name of the datacenter associated with the cluster.
- **Datastores**. The number of datastores associated with the selected cluster.
- **ESX Hosts**. The number of ESX hosts that belong to the selected cluster.
- **Memory Capacity**. The combined memory capacity of the servers that belong to the selected cluster.
- **Network Interfaces**. The number of network interface cards used by the servers that belong to the selected cluster.
- **Processing Power**. The CPU speed available to the selected cluster.
- **Resource Pools**. The number of resource pools associated with the cluster.
- **Virtual Center**. The IP address of the Virtual Center to which the cluster belongs.
- **Virtual Machines Hosted**. The number of virtual machines hosted in the selected cluster.

Data appearing when viewing ESX host details:

- **Cluster**. The name of the cluster to which the selected ESX host belongs.
- **Computing Capacity**. The CPU processing power available to the ESX host.
- **Connection Status**. The ESX host's connection status.
- **Current Status**. The current status of the selected ESX host: `Turned off` or `Powered On`.
- **Datastores**. The number of datastores associated with the ESX host.
- **DNS Name**. The fully qualified DNS name of the host.
- **ESX Software Version**. The VMware application version.
- **Memory Capacity**. The memory capacity of the selected ESX host.
- **Network Interfaces**. The number of network interface cards that exist on the ESX host.
- **Processors**. The number of CPUs used by the selected server.
- **Virtual Machines Count**. The number of virtual machines running on the selected server.
- **VM's Powered On Count**. The number of virtual machines that exist on the host that are currently powered on.

Data appearing when viewing virtual machine details:

- **Cluster**. The name of the cluster to which the selected virtual machine belongs.
- **Connection Status**. The virtual machine's connection status.
- **Current Status**. The current status of the selected virtual machine: `Turned off` or `Powered On`.
- **Datacenter**. The name of the datacenter associated with the virtual machine.
- **DNS Name**. The fully qualified DNS name of the virtual machine.
- **ESX Host**. The IP address of the ESX host on which the virtual machine is running.
- **IP address**. The IP address of the virtual machine.
- **Memory Capacity**. The amount of memory resources allocated to the virtual machine.
- **Network Interfaces**. The number of network interface cards used by the selected virtual machine.
- **OS**. The name of the operating system used by the selected virtual machine.
- **Processors**. The number of CPUs used by the selected virtual machine and the number of the CPU shares.

Table 33. Summary and Resource Information

- **Resource Pools**. The name of the resource associated with the virtual machine.
- **Storage Devices**. The number of physical and logical disks associated with the virtual machine.
- **Uptime**. The percentage of time during which the virtual machine is running.
- **Virtual Center**. The IP address of the Virtual Center to which the virtual machine belongs.
- **Vmware Tools**. The name of VMware applications used to manege the virtual machine.

Data appearing when viewing datacenter details:

- **Clusters**. The number of clusters associated with the datacenter.
- **Combined Processing**. The combined CPU processing power available to the datacenter.
- **Datastores**. The number of datastores associated with the datacenter.
- **ESX Hosts**. The number of ESX hosts associated with the datacenter.
- **Memory Capacity**. The combined memory capacity available to the datacenter.
- **Network Interfaces**. The number of network interface cards available to the datacenter.
- **Resource Pools**. The number of resource pools associated with the datacenter.
- **Virtual Machines Hosted**. The number of virtual machines associated with the datacenter.

Data appearing when viewing resource pool details:

- **CPU Limit**. The maximum CPU processing power allocated to the datacenter.
- **CPU Reservation**. The CPU processing power allocated to the datacenter.
- **CPU Shares**. The state of CPU shares associated with the datacenter.
- **Memory Limit**. The maximum memory resources allocated to the datacenter.
- **Memory Reserved**. The memory resources allocated to the datacenter.
- **Memory Shares**. The state of memory shares associated with the datacenter.
- **Nested Resource Pool(s)**. The number of child resource pools.
- **Parent**. The host name or IP address of the resource pool parent element.
- **Virtual Machines**. The number of virtual machines associated with the resource pool.

Table 34. Virtual Environment

Description	The VMware Explorer's Virtual Environment view displays a high-level overview of your virtual environment. The view has a tile for each object type: **Virtual Centers**, **Datacenters**, **Clusters**, **ESX Hosts**, **Resource Pools**, **Datastores**, and **Virtual Machines**. Each tile shows the number of the corresponding object instances in your virtual infrastructure, as well as the count of objects of that type in each of the alarm states (Normal, Warning, Critical, Fatal).
Data displayed	• **Alarm counts**. The total counts of alarms associated with the clusters, servers, or virtual machines, broken down by alarm types (Normal, Warning, Critical, Fatal). • **Cluster count**. The number of clusters in the Virtual Center. • **Datacenter count**. The number of datacenters in the Virtual Center. • **Datastore count**. The number of datastores in the Virtual Center. • **ESX Host count**. The number of ESX hosts in the Virtual Center. • **Resource Pools**. The number of resource pools in the Virtual Center.

Table 34. Virtual Environment

- **Virtual Machine count**. The number of virtual machines in the Virtual Center

- **Virtual Center count**. There can be only one Virtual Center in each model.

Where to go next   Drill down on:

- **Cluster**. Displays the **Clusters Inventory** dwell, showing the names and states of one or more clusters associated with the selected component.

Clusters Inventory	
Name ▲	State
Oracle Database	✓

- **Datacenter**. Displays the **Datacenters Inventory** dwell, showing the names and states of one or more datacenters associated with the selected component.

Datacenters Inventory	
Name ▲	State
Virtual VMWare	✓

- **Datastores**. Displays the **Datastores Inventory** dwell, showing the names and states of one or more datastores associated with the selected component.

Datastores Inventory	
Name ▲	State
AX4_VM250_01	✓
AX4_VM250_02	✓
AX4_VM250_03	✓
AX4_VM250_04	✓
AX4_VM300_50	◈
datastore1 (1)	◈
datastore1-with	✓
datastore2-10k	✓
datastore3-10k	✓
datastore4-15k	◈
Extent_test	✓

- **ESX Hosts**. Displays the **ESX Hosts Inventory** dwell, showing the names and states of one or more ESX hosts associated with the selected component.

ESX Hosts Inventory	
Name ▲	State
10.4.45.100	✓
10.4.45.102	✕
10.4.45.104	◈
10.4.45.106	⚠
10.4.45.108	✓
10.4.45.118	✕

- **Resource Pools**. Displays the **Resource Pools Inventory** dwell, showing the names and states of one or more resource pools associated with the selected component.

Resource Pools Inventory	
Name ▲	State
chadrootrp	✓
chadtest1	✓
chadtest2	✓
chadtest3	✓
LabMan	✓
Performance Tes	⚠
Resources	✓
Resources	⚠
Resources	✓
TestRP10	✓
TestRP11	✓

Table 34. Virtual Environment

- **Virtual Center**. Displays the **Virtual Centers Inventory** dwell, showing the name and state of the virtual center containing the selected component.
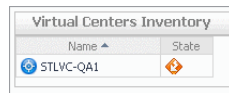
- **Virtual Machines**. Displays the **Virtual Machines Inventory** dwell, showing the names and states of one or more virtual machines associated with the selected component.
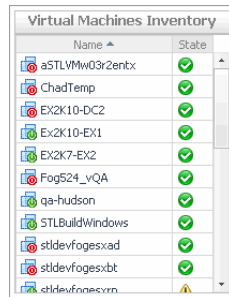
Table 35. Virtual Machines

Description	Shows a list of virtual machines associated with the selected cluster or ESX host. **NOTE:** This view only appears when viewing cluster or ESX host details.
Data displayed	• **Name**. The virtual machine name. • **Status**. The status of the virtual machine, associated with any alarms raised against that virtual machine. If no alarms are fired, the status appears as Normal. Otherwise, the status is set to the alarm severity (Warning, Critical, or Fatal).
Where to go next	Drill down on any virtual machine entry. The Summary tab refreshes, showing the virtual machine details.

Table 36. Virtual Machine and Resource Pool Changes

Description	Shows a list of asset tracking changes associated with the selected virtual machine and its resource pool. **NOTE:** This view only appears when viewing virtual machine details.
Data displayed	• **Change**. The change description. • **Time**. The date and time at which the change occurred. • **Details**. Additional details about the change.

Summary (All Clusters) tab

Purpose

The **Summary (All Clusters)** tab shows a summary of system resources for all available clusters in a Virtual Center.

Figure 38. Summary (All Clusters) tab
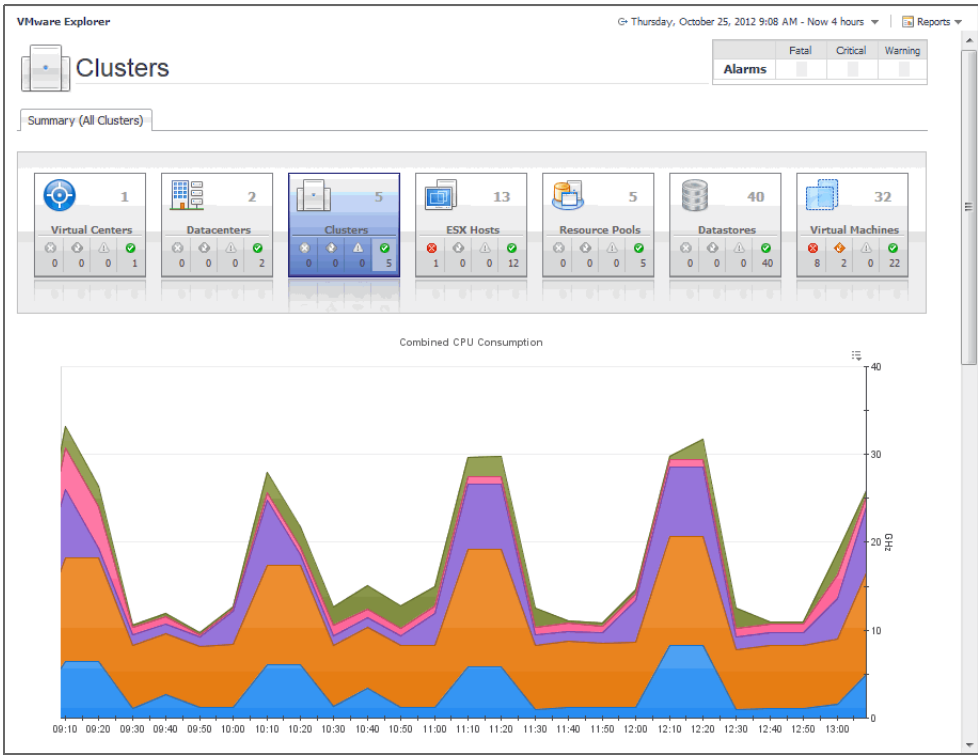
How to Get Here

1 Open the VMware Explorer.

2 In the Virtual Infrastructure view, that appears on the navigation panel, select the **Clusters** node.

   The VMware Explorer refreshes in the display area with the Summary (All Clusters) tab open.

Description of Embedded Views

This view is made up of the following embedded views:

- Clusters at Virtual Center
- Combined CPU Consumption
- Virtual Environment

Table 37. Clusters at Virtual Center

Description	This tabular view lists the clusters that exist in the Virtual Center.
Data displayed	• **CPU Used**. The current amount of the CPU speed used by the ESX hosts in the cluster. • **Hosts**. The number of ESX hosts in the cluster. • **Key**. The color used in the Combined CPU Consumption chart to represent the cluster. • **Memory**. The current percentage of memory used by all servers in the cluster. • **Name**. Cluster name. • **Resource Pools**. The number of resource pools in the cluster.

Table 37. Clusters at Virtual Center

> • **Status**. The status of the cluster, associated with any alarms raised against that cluster. If no alarms are fired, the status appears as Normal. Otherwise, the status is set to the highest alarm severity (Warning, Critical, or Fatal).

Where to go next	Drill down on any cluster entry. The VMware Explorer refreshes, showing the cluster details on the Summary tab.

Table 38. Combined CPU Consumption

Description	Shows the combined percentage of the CPU usage for all clusters in the Virtual Center.
Data displayed	• **Combined CPU Consumption, %**. The combined percentage of the CPU utilization used by all ESX hosts in all clusters to execute system code and user programs during the selected time period.
Where to go next	Drill down on:

> • **Combined CPU Consumption %**. Displays the **Combined CPU Consumption** dialog box.

Table 39. Virtual Environment

Description	The VMware Explorer's Virtual Environment view displays a high-level overview of your virtual environment. The view has a tile for each object type: **Clusters**, **Servers**, and **Virtual Machines**. Each tile shows how many of the corresponding object instances there are in your virtual infrastructure, as well as the count of objects of that type in each of the alarm states (Normal, Warning, Critical, Fatal).
Data displayed	• **Alarm counts**. The total counts of alarms associated with the clusters, servers, or virtual machines, broken down by alarm types (Normal, Warning, Critical, Fatal).
	• **Cluster count**. The number of clusters in your virtual environment.
	• **Server count**. The number of physical servers in your virtual environment.
	• **Virtual Machine count**. The number of virtual machines in your environment.
Where to go next	Drill down on:

> • **Cluster**. Displays the **Clusters Inventory** dwell, showing the names and states of all clusters that exist in the Virtual Center.

> • **Datacenter**. Displays the **Datacenters Inventory** dwell, showing the names and states of all datacenters that exist in the Virtual Center.

Table 39. Virtual Environment

- **Datastores**. Displays the **Datastores Inventory** dwell, showing the names and states of all datastores that exist in the Virtual Center.

- **ESX Hosts**. Displays the **ESX Hosts Inventory** dwell, showing the names and states of all ESX hosts that exist in the Virtual Center.

- **Resource Pools**. Displays the **Resource Pools Inventory** dwell, showing the names and states of all resource pools that exist in the Virtual Center.

- **Virtual Center**. Displays the **Virtual Centers Inventory** dwell, showing the name and state of the selected Virtual Center.

- **Virtual Machines**. Displays the **Virtual Machines Inventory** dwell, showing the names and states of all resource pools that exist in the Virtual Center.

Summary (All Datacenters) tab

Purpose

The **Summary (All Datacenters)** tab shows a summary of system resources for all datacenters that currently exist in a selected Virtual Center.

Figure 39. Summary (All Datacenters) tab
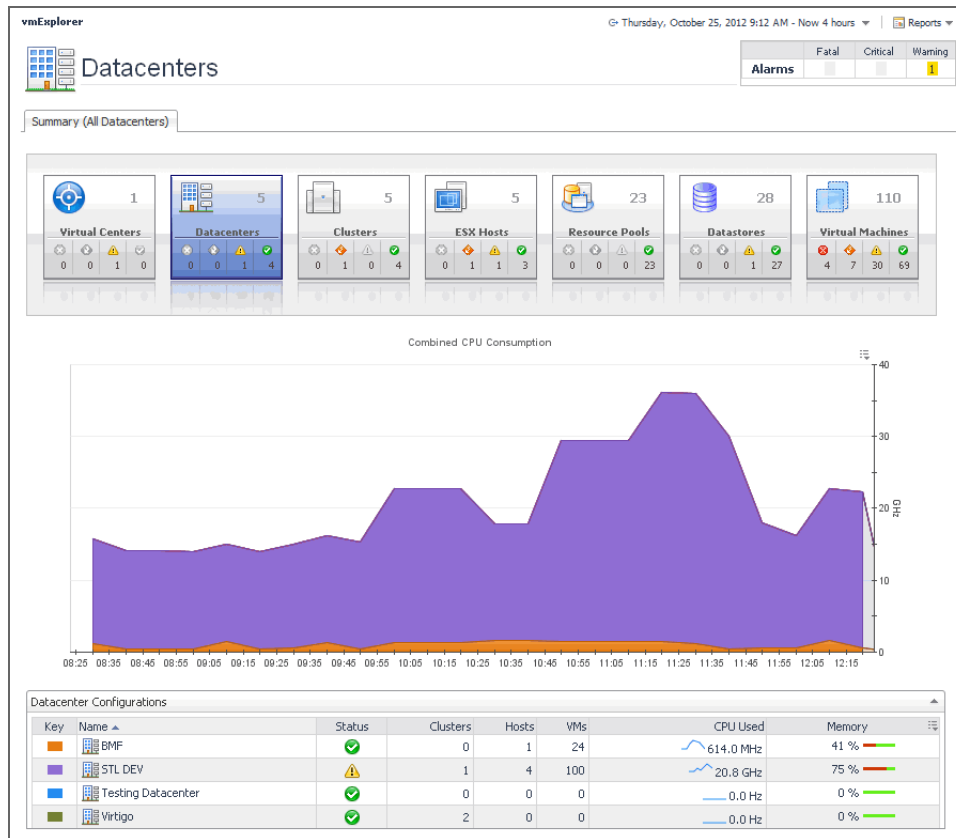
How to Get Here

1 Open the VMware Explorer.

2 On the Virtual Infrastructure view, that appears on the navigation panel, select the **Datacenters** node.

   The VMware Explorer refreshes in the display area, showing the Summary (All Datacenters) tab.

Description of Embedded Views

This view is made up of the following embedded views:

- Combined CPU Consumption
- Datacenter Configurations
- Virtual Environment

Table 40. Combined CPU Consumption

Description	Shows the combined percentage of the CPU usage for all ESX hosts in the system.
Data displayed	• **Combined CPU Consumption %**. The combined percentage of the CPU utilization used by all ESX hosts to execute system code and user programs during the selected time period.
Where to go next	Drill down on:

• **Combined CPU Consumption %**. Displays the **Combined CPU Consumption** dialog box.

Table 41. Datacenter Configurations

Description	This tabular view lists all datacenters that exist in a Virtual Center configuration.
Data displayed	• **Clusters**. The number of clusters associated with the datacenter.
	• **CPU Used**. The current amount of the CPU speed that is used by the ESX hosts associated with the datacenter.
	• **Hosts**. The number of ESX hosts associated with the datacenter.
	• **Key**. The color used in the Combined CPU Consumption chart to represent the datacenter.
	• **Memory**. The current percentage of memory that is used by the ESX host.
	• **Name**. The datacenter name.
	• **Status**. The datacenter status, associated with any alarms raised against it. If no alarms are fired, the status appears as Normal. Otherwise, the status is set to the highest alarm severity (Warning, Critical, or Fatal).
	• **VMs**. The number of virtual machines associated with the datacenter.
Where to go next	Drill down on any datacenter entry. The VMware Environment dashboard appears, showing the datacenter details on the Summary tab.

Table 42. Virtual Environment

Description	This embedded view shows the same information as the Virtual Environment view appearing on the Summary (All Clusters) tab. See page 69 for complete information.

Summary (All Resource Pools) tab

Purpose

The **Summary (All Resource Pools)** tab shows a summary of system resources for all resource pools that currently exist in a selected Virtual Center.

Figure 40. Summary (All Resource Pools) tab
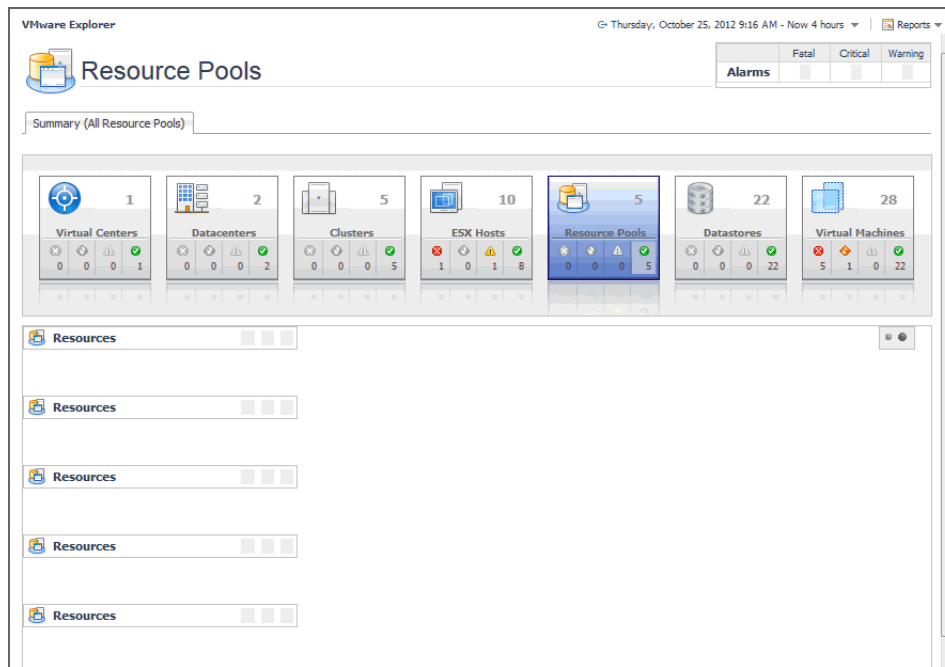
How to Get Here

1 Open the VMware Explorer.

2 On the Virtual Infrastructure view, that appears on the navigation panel, select the **Resource Pools** node.

   The VMware Explorer refreshes in the display area, showing the Summary (All Resource Pools) tab.

Description of Embedded Views

This view is made up of the following embedded views:

• Resource Pool

• Virtual Environment

Resource Pool

For complete information about this view, see Resource Pools Relationship Tree view on page 48.

Virtual Environment

This embedded view shows the same information as the Virtual Environment view appearing on the Summary (All Clusters) tab. See page 69 for complete information.

Summary (All Servers) tab

Purpose

The **Summary (All Servers)** tab shows a summary of system resources for all ESX hosts that currently exist in a selected Virtual Center.

Figure 41. Summary (All Servers) tab
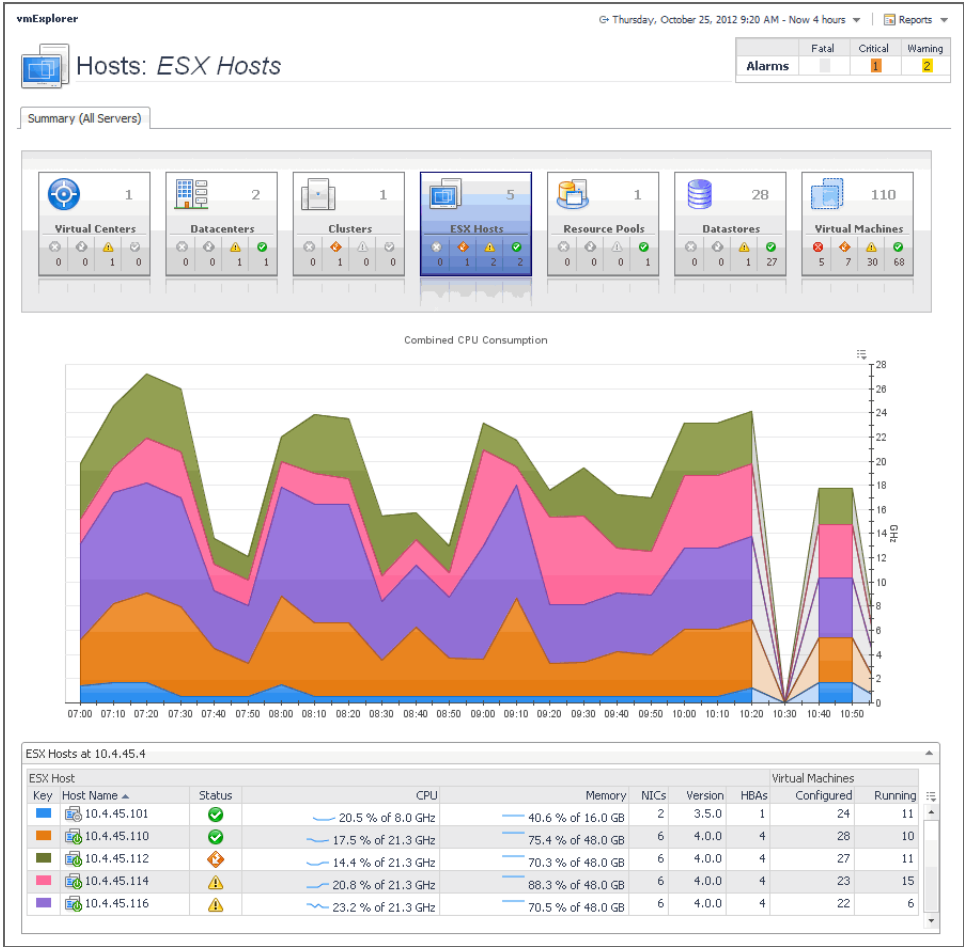
How to Get Here

1 Open the VMware Explorer.

2 On the Virtual Infrastructure view, that appears on the navigation panel, select the **ESX Hosts** node.

   The VMware Explorer refreshes in the display area, showing the Summary (All Servers) tab.

Description of Embedded Views

This view is made up of the following embedded views:

*   Combined CPU Consumption

*   ESX hosts

*   Virtual Environment

Table 43. Combined CPU Consumption

Description	Shows the combined percentage of the CPU usage for all ESX hosts in the system.
Data displayed	• **Combined CPU Consumption %**. The combined percentage of the CPU utilization used by all ESX hosts to execute system code and user programs during the selected time period.

Table 43. Combined CPU Consumption

Where to go next	Drink down on:

- **Combined CPU Consumption %**. Displays the **Combined CPU Consumption** dialog box.
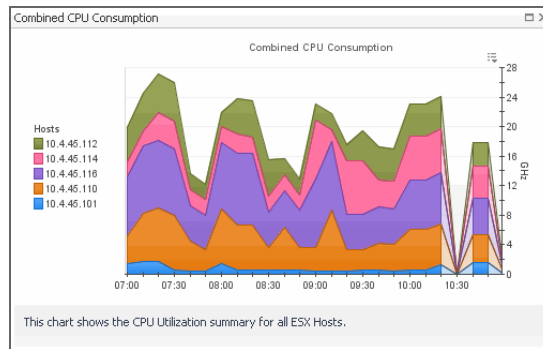
Table 44. ESX hosts

Description	This tabular view lists all ESX hosts that exist in your environment.
Data displayed	

- **ESX host, CPU**. The current amount of the CPU speed that is used by the ESX host.
- **ESX host, Key**. The color used in the Combined CPU Consumption chart to represent the ESX host.
- **ESX host, Memory**. The current percentage of memory that is used by the ESX host.
- **ESX host, NICs**. The number of network interface cards used by the ESX host.
- **ESX host, ESX host Name**. ESX host name.
- **ESX host, Status**. The ESX host status, associated with any alarms raised against it. If no alarms are fired, the status appears as Normal. Otherwise, the status is set to the highest alarm severity (Warning, Critical, or Fatal).
- **ESX host, Version**. The version number of the Windows OS running on the ESX host.
- **Virtual Machines, Configured**. The number of virtual machines that exist on the ESX host.
- **Virtual Machines, Running**. The number of virtual machines that are running on the ESX host.

Where to go next	Drink down on any ESX host entry. The VMware Environment dashboard appears, showing the ESX host details on the Summary tab.

Table 45. Virtual Environment

Description	This embedded view shows the same information as the Virtual Environment view appearing on the Summary (All Clusters) tab. See page 69 for complete information.

Summary (All Virtual Machines) tab

Purpose

The **Summary (All Virtual Machines)** tab shows a summary of system resources for all virtual machines that currently exist in the selected Virtual Center.

Figure 42. Summary (All Virtual Machines) tab
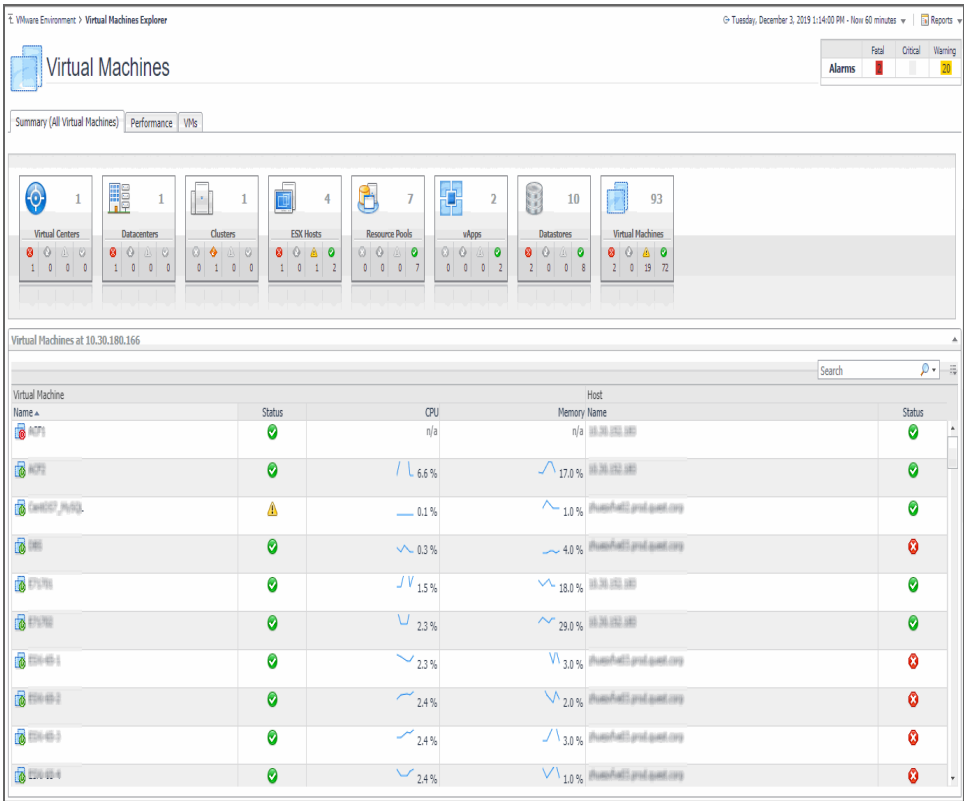
How to Get Here

1   Open the VMware Explorer.

2   On the Virtual Infrastructure view, select a **Virtual Machines** node.

The VMware Explorer refreshes in the display area, showing the Summary (All Virtual Machines) tab.

Description of Embedded Views

This view is made up of the following embedded views:

-   Virtual Environment
-   Virtual Machines

Table 46. Virtual Environment

Description	This embedded view shows the same information as the Virtual Environment view appearing on the Summary (All Clusters) tab. See page 69 for complete information.

Table 47. Virtual Machines

Description	This tabular view lists all virtual machines that exist in the selected Virtual Center.
Data displayed	**•** **Virtual Machine, Name**. The name of the server on which the virtual machine is running.
	• **Virtual Machine, Status**. The status of the server on which the virtual machine is running, associated with any alarms raised against it. If no alarms are fired, the status appears as Normal. Otherwise, the status is set to the highest alarm severity (Warning, Critical, or Fatal).

Table 47. Virtual Machines

- **Virtual Machine, CPU**. The percentage of the virtual machine's CPU utilization spent on executing system code and user programs.
- **Virtual Machine, Name**. The virtual machine name.
- **Virtual Machine, Status**. The virtual machine status, associated with any alarms raised against it. If no alarms are fired, the status appears as Normal. Otherwise, the status is set to the highest alarm severity (Warning, Critical, or Fatal).
- **Virtual Machine, Memory**. The total amount of memory allocated to the virtual machine.

Where to go next   Drill down on any virtual machine entry. The VMware Environment dashboard appears, showing the server details on the Summary tab.

Virtual Infrastructure view

Purpose

The Virtual Infrastructure view provides an organized view of the various virtual infrastructure objects that are monitored by VMware Monitoring in Foglight Evolve Cloud. It serves as a navigation tool, and it also presents pertinent alarm information.
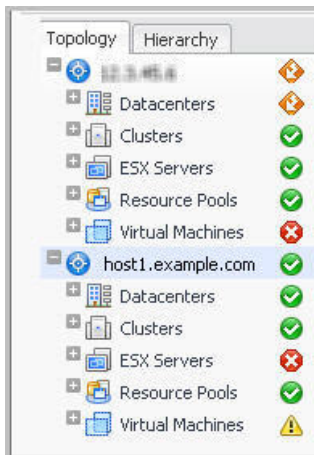
When you select an object from the Virtual Infrastructure view, all of the views in the VMware Explorer dashboard are updated with information pertaining to that object.

How to Get Here

- Open the VMware Explorer.

  The Virtual Infrastructure view appears on the navigation panel.

Description of Embedded Views

The Virtual Infrastructure view is made up of the following embedded views:

- Topology Tab
- Hierarchy Tab
- Mouse-over Status Popups

Topology Tab

The Topology view is organized into a tree using object type (or topology type) containers for branches.

Within the Topology view, all of the virtual infrastructure objects are organized into a tree using object type (or topology type) containers for branches. The top-level objects in the Topology view are always the vCenters.

The top-level objects in the Topology view are always the VirtualCenters.

Each VirtualCenter in the Topology view contains several object type containers, and each object type container contains every object of that particular type that is managed by the parent VirtualCenter.

Each object type container, as well as each object, has a representative icon that is displayed to the left, as shown in the following table.

Table 48. Virtual Infrastructure View Object Icons

Icon	Object	Object Name
	VirtualCenter	VMWVirtualCenter
	Datacenter	VMWDatacenter
	Cluster	VMWCluster
	ESX Server	VMWESXServer
	Resource Pool	VMWResourcePool
	Virtual Machine	VMWVirtualMachine
	Datastore	VMWDatastore

At the right, the Topology view displays status indicators. For an individual object, the status indicator represents the alarm of highest severity that is outstanding for that object. For an object type container, the status indicator represents the alarm of highest severity that is outstanding for all objects of that type.

> **i** | **NOTE:** A single virtual machine running at a high CPU utilization does not trigger an alarm for its parent ESX Server. An alarm is only triggered for the parent ESX Server if the server itself is running at a high CPU utilization.

Hierarchy Tab

The Hierarchy view represents the logical layout of VirtualCenter management servers, so it is not organized into groups of common objects.

Within the Hierarchy view, each VirtualCenter object is organized into a tree that has the same hierarchical structure as the VirtualCenter and displays the objects (datacenters, clusters, resource pools, virtual machines, folders, etc.) within the VirtualCenter as branches.

In the Hierarchy view, each VirtualCenter object is organized into a tree that has the same hierarchical structure as the corresponding VirtualCenter, displaying the objects (for example, datacenters, clusters, resource pools, virtual machines, and folders) within the VirtualCenter as branches.

Each object in the Hierarchy view has a representative icon that is displayed at the left of the object's name. These icons are shown in the table in Topology Tab on page 77.

At the right, the Hierarchy view displays status indicators. Each status indicator represents the alarm of highest severity that is outstanding for the corresponding object.

Mouse-over Status Popups

When you hover the cursor over an object in the Virtual Infrastructure view, you see a popup that provides a summary of the present state of that object.

The following image shows the popup you see when you hover the cursor over a VirtualCenter object in the Virtual Infrastructure view.
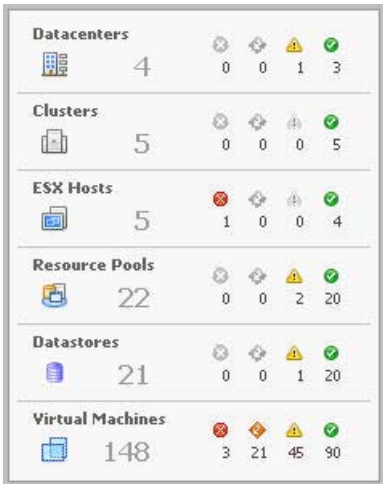
VMware Agent Administration views

The VMware Environment dashboard contains the following views:

- Agents view
- Instances and Limits view
- OS Mapping view
- Metrics Collection Management View

Agents view

Purpose

This view displays a list of the existing VMware Performance Agent instances and shows their status. Use it to verify that your agents are collecting data from the monitored environment.

Figure 43. Agents view
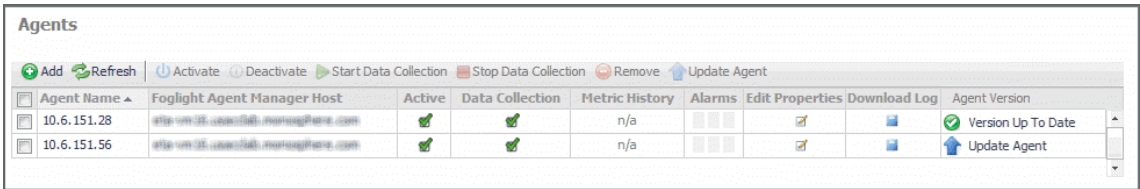
How to Get Here

1   On the VMware Environment dashboard, open the **Administration** tab.

The Agents view appears at the bottom of the **Administration** tab.

Description of the View

Data displayed
- **Active**. Indicates if the VMware Performance Agent process is running.
- **Agent Name**. The name of the VMware Performance Agent instance.

Description of the View

- **Agent Version**. Indicates if the agent is running the latest version of the agent package (✅ Version Up To Date), or it needs to be updated (⬆ Update Agent).
- **Alarms**. The total numbers of Warning, Critical, and Fatal alarms.
- **Data Collection**. Indicates if the VMware Performance Agent is collecting data from the monitored environment.
- **Download Log**. Allows you to download the agent log file.
- **Edit Properties**. Allows you to edit the agent's properties.
- **Foglight Agent Manager Host**. The name of the machine on which the Agent Manager and the VMware Performance Agent process are running.
- **Metric History**. The progress of the import of historical data. Each VMware Performance Agent monitors a single Virtual Center. When you create a VMware Performance Agent instance and the Agent Setup wizard determines that the Virtual Center was not previously monitored by this Foglight Evolve Cloud instance, it starts importing historical data into Foglight Evolve Cloud. This data is not immediately available as it takes some time to collect it. This process can import data collected over 30 days or less, depending on the amount of data available in the Virtual Center. This allows you to explore VMware metrics as soon as the data is imported, instead for waiting for the agent to collect some data from the Virtual Center. Historical data is intended for charting, trending, and general presentation purposes. It does not cause any alarms to fire.

  Click this column to start a metric history import, or to see its progress. When the import is in progress, you have an option to cancel it, if needed.

10.4.33.151	✕
Last Updated:	10/5/15 4:36 PM Cancel
Process Started:	10/5/15 4:36 PM
Process Resumed:	10/5/15 4:36 PM
Processed To Date:	n/a
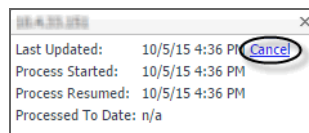
  Click **Cancel** in the dwell to cancel the import. You can resume it at a later time.

  When the metric history import is completed, this is indicated in the dwell.

10.4.45.84	✕
Last Updated:	5/6/15 10:56 AM Finished
Process Started:	5/6/15 9:23 AM
Process Resumed:	5/6/15 9:23 AM
Processed To Date:	4/6/15 9:23 AM
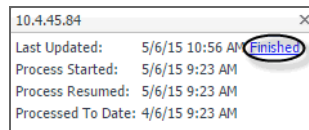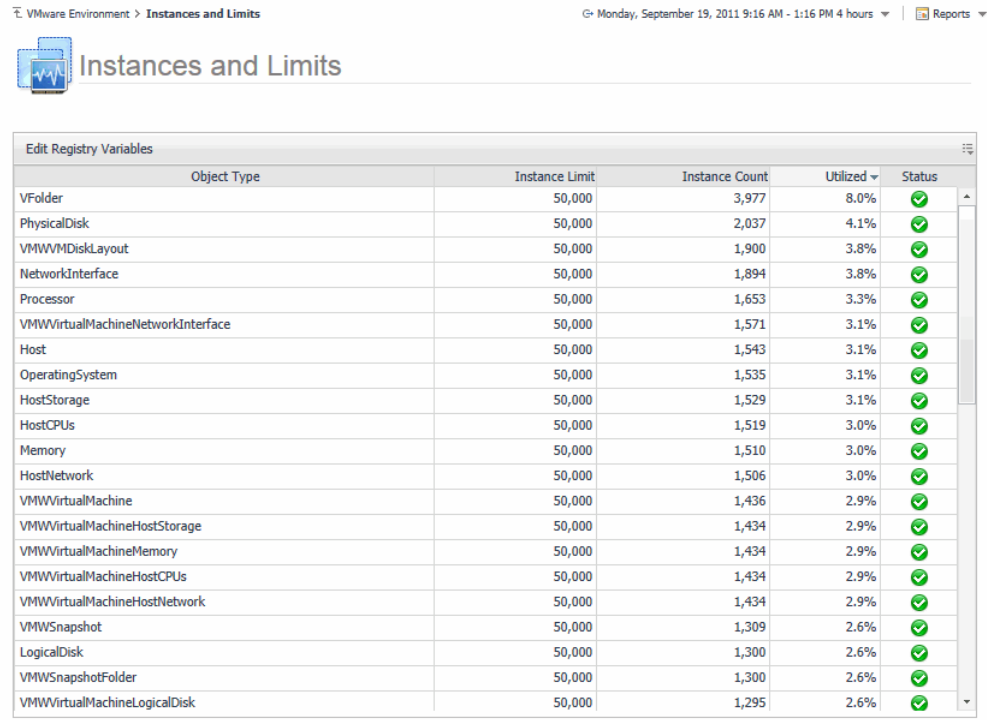
Instances and Limits view

Purpose

This view displays the list of the existing VMware object types. This information can give you insight into the size of your database and whether additional adjustments are required to improve your system performance.

Figure 44. Instances and Limits view

How to Get Here

- On the VMware Environment dashboard, on the **Administration** tab, click **Review Instances and Limits**.

  The Instances and Limits view appears in the display area.

Table 49. Description of the View
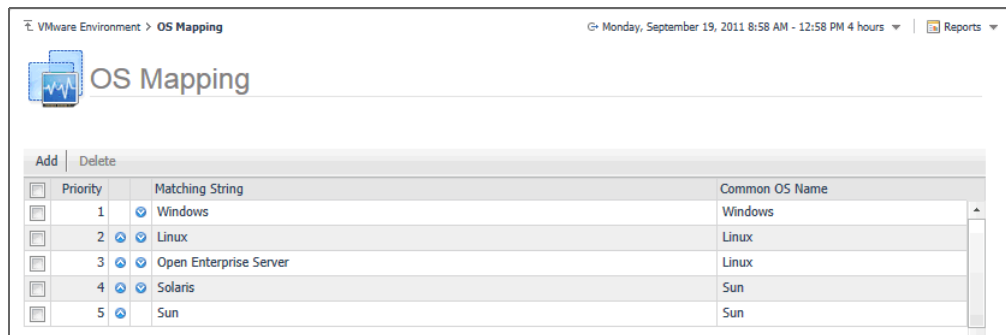
Data displayed	• **Instance Count**. The current number of object instances of this type.
	• **Instance Limit**. The maximum number of object instances of this type that can be instantiated.
	• **Object Type**. The type of the topology object.
	• **Status**. The current status representing the highest severity level associated with an instance of that type.
	• **Utilized**. The percentage of the object limit instance that is currently utilized.

OS Mapping view

Purpose

You configure OS mapping rules using the OS Mapping view. OS mapping is the mapping of the various versions and editions of a particular operating system to a common OS name. This helps VMware Monitoring in Foglight Evolve Cloud manage the variety of versions and editions of each OS.

Figure 45. OS Mapping view

How to Get Here

- On the VMware Environment dashboard, on the **Administration** tab, click **Configure OS Mapping**.

  The OS Mapping view appears in the display area.

Table 50. Description of the View

Data displayed	• **Common OS Name**. The OS name.
	• **Matching String**. The OS name to be matched against existing OS names.
	• **Priority**. The matching priority. Selecting a mapping and clicking ◎ or ◎ allows you to edit the priority sequence.

Metrics Collection Management View

Purpose

The Metrics Collection Management view is used to configure the metrics collect by agent. VMware agent has collect total 99 metrics from vCenter, but some metrics are not used to VMware dashboard and relate products (Capacity Director, Optimizer and so on), less metrics collection can reduce the pressure of collection from vCenter and improve performance for agent on large environment. This view is for this purpose and user can disable the collection of these metrics at this view.

- **Please select agent:** select the agent which need configure.

- **Collect Metrics For Dashboard Only:** Configure the agent just collect the metrics used for dashboard only.

- **Restore The Default Setting:** Configure the agent to collect all metrics of VMware by default.

- **Save Edited Configuration:** After editing these settings, click the Save Edited Collection Information button to save your configuration.

How to Get Here

- On the VMware Environment dashboard, on the Administration tab, on the Advanced Options sub tab, click Metrics Collection Management. The Metrics Collection Management View in the display area.

Figure 46. VMware Metrics Collection Management view

Data displayed

- **Name:** The metrics name.

- **Collecting:** Agent collect this metric or not, agent collect it when it selected.

- **Description:** The description of metric.

Table 51. Summary and Resource Information

Description	Lists the summary and resource information of the selected virtual machine.
Data displayed	• **Current Status**. The current status of the selected virtual machine: `Turned off` or `Powered On.` • **Processors**. The number of CPUs used by the selected virtual machine. • **Uptime**. The percentage of time during which the virtual machine is running. • **Memory Capacity**. The amount of memory resources allocated to the selected virtual machine. • **Powered on Date.** The date on which the selected virtual machine is powered. • **Network Interface.** The number of network interface cards that exist on the selected virtual machine. • **OS Reboot Date**. The date when rebooting the operating system. • **Storage Devices**. The number of physical and logical disks associated with the virtual machine. • **DNS Name**. The fully qualified DNS name of the selected virtual machine. • **Virtual Center**. The IP address of the Virtual Center to which the virtual machine belongs. • **Connection Status**. The virtual machine's connection status. • **Datacenter**. The name of the datacenter associated with the virtual machine. • **IP Address**. The IP address of the virtual machine. • **Cluster**. The name of the cluster associated with the virtual machine. • **Vmware Tools**. The name of VMware applications used to manage the virtual machine. • **Resource Pool**. The name of resource pools associated with the virtual machine. • **OS**. The name of the operating system used by the selected virtual machine. • **ESX Host**. The IP address of the ESX host on which the virtual machine is running. • **Managed Object Reference**. Identifies the virtual switch in your monitored environment.

Rules

VMware Monitoring in Foglight® Evolve Cloud allows you to create flexible rules that can be applied to complex, interrelated data from multiple sources within your distributed system. You can associate several different actions with a rule, configure a rule so that it does not fire repeatedly, and associate a rule with schedules to define when it should and should not be evaluated.

Different types of data can be used in rules, including registry variables, raw metrics, derived metrics, and topology object properties.

There are two types of rules in VMware Monitoring in Foglight Evolve Cloud: simple rules and multiple-severity rules. A simple rule has a single condition, and can be in one of three states: *Fire*, *Undefined*, or *Normal*. A multiple-severity rule can have up to five severity levels: *Undefined*, *Fatal*, *Critical*, *Warning*, and *Normal*.

Rule conditions are regularly evaluated against monitoring data (metrics and topology object properties collected from your monitored environment and transformed into a standard format). Therefore, the state of the rule can change if the data changes. For example, if a set of monitoring data matches a simple rule's condition, the rule enters the *Fire* state. If the next set does not match the condition, the rule exits the *Fire* state and enters the *Normal* state.

A rule condition is a type of expression that can be true or false. When it evaluates to true, the rule is said to fire, causing any actions that are associated with the rule or severity level to be performed. You can configure a rule to perform one or more actions upon entering or exiting each state. When a multiple-severity rule fires, an alarm also appears in VMware Monitoring in Foglight Evolve Cloud.

For more information see the *VMware Monitoring in Foglight Evolve Cloud Administration and Configuration Help.*

VMware Monitoring in Foglight Evolve Cloud provides an effective monitoring solution for the VMware infrastructure. The rules included in VMware Monitoring in Foglight Evolve Cloud alert you to virtual infrastructure problems.

When service degradations are detected, VMware Monitoring in Foglight Evolve Cloud sends alerts to the event console. Optionally, VMware Monitoring in Foglight Evolve Cloud can be configured to send emails, pager messages, or perform other actions you define. Performance data can be viewed, analyzed and reported using VMware Monitoring in Foglight Evolve Cloud.

VMware Monitoring in Foglight Evolve Cloud includes a number of predefined rules that capture the expert knowledge of our virtualization specialists and are used to monitor the health of your virtual infrastructure. VMware Monitoring in Foglight Evolve Cloud allows you to modify these rules or create your own flexible rules that can be applied to complex, interrelated data from multiple sources within your distributed system.

In this chapter, rule descriptions are organized into logical groupings. To see a rule description, select the appropriate grouping from the sections listed below.

Many of the rules listed and described in this chapter have thresholds (standard deviations, utilization percentages, etc.) defined within them. Those thresholds are default values predefined in the registry.

VMware Monitoring in Foglight Evolve Cloud includes the following groups of rules:

- Cluster Rules
- Datacenter Rules
- Datastore Rules
- Resource Pool Rules
- ESX Server Rules
- VirtualCenter Rules
- Virtual Machine Rules
- Virtual Switch Rules

i | **NOTE:** Unless otherwise noted, the following views display alarms triggered by most rules included with VMware Monitoring in Foglight Evolve Cloud:
  - Summary tab on page 58
  - Virtual Infrastructure view on page 77

Cluster Rules

This section describes the cluster rule:

- VMW Cluster Disk IO on page 85

VMW Cluster Disk IO

Purpose

This rule monitors for spikes and dramatic drops in disk IO for a cluster. This rule is disabled by default, and can be enabled as required.

Scope

VMWCluster

Table 52. Rule Definition

Conditions	State	Action
The disk usage is no more than 2.2 standard deviations (NumSTDevs) from the mean disk usage.	Normal	None
The disk usage is more than 2.2 but no more than 2.8 standard deviations from the mean disk usage.	Warning	None
The disk usage is more than 2.8 standard deviations from the mean disk usage.	Critical	None

Datacenter Rules

This section describes the datacenter rule. This rule is disabled by default, and can be enabled as required.

VMW Datacenter Disk IO

Purpose

This rule monitors for spikes and dramatic drops in disk IO for a datacenter.

Scope

VMWDatacenter

Table 53. Rule Definition

Conditions	State	Action
The disk usage is no more than 2.2 standard deviations (NumSTDevs) from the mean disk usage.	Normal	None
The disk usage is more than 2.2 but no more than 2.8 standard deviations from the mean disk usage.	Warning	None
The disk usage is more than 2.8 standard deviations from the mean disk usage.	Critical	None

Datastore Rules

This section describes datastore rules.

Rules in this section:

VMW Datastore Estimated Fill Time

Purpose

This rule determines when the datastore is likely to reach its capacity, based on its present growth rate.

Scope

VMWDatastore

Table 54. Rule Definition

Conditions	State	Action
At the present growth rate, the datastore will not reach its capacity within 90 days.	Normal	None
At the present growth rate, the datastore will reach its capacity in 90 days or less.	Warning	None
At the present growth rate, the datastore will reach its capacity in 30 days or less.	Critical	Send email to VMware administrator
At the present growth rate, the datastore will reach its capacity in 7 days or less.	Fatal	Send email to VMware administrator

VMW Datastore Inactive

Purpose

This rule detects when a datastore becomes inactive in vSphere.

Scope

VMWDatastore

Table 55. Rule Definitions

Conditions	State	Action
The datastore is currently active.	Normal	None
The datastore is currently inactive.	Warning	None

Resource Pool Rules

This section describes the resource pool rule:

-

VMW Resource Pool Disk IO

Purpose

This rule monitors for spikes and dramatic drops in disk IO for a resource pool.

Scope

VMWResourcePool

Table 56. Rule Definition

Conditions	State	Action
The disk usage is no more than 2.2 standard deviations (NumSTDevs) from the mean disk usage.	Normal	None

Table 56. Rule Definition

The disk usage is more than 2.2 but no more than 2.8 standard deviations from the mean disk usage.	Warning	None
The disk usage is more than 2.8 standard deviations from the mean disk usage.	Critical	None

Views Displaying Alarms Based on this Rule

The views listed in Rules on page 84, in addition to the Resource Pools Relationship Tree view on page 48.

ESX Server Rules

This section lists and describes the ESX Server rules.

Rules in this section:

- VMW ESX Server Disk IO on page 88
- VMW ESX Server Queue Latency on page 88
- VMW ESX Server Queue Latency Deviation on page 89
- VMW ESX Server Total Latency on page 89
- VMW ESX Server Total Latency Deviation on page 90

VMW ESX Server Disk IO

Purpose

This rule monitors for spikes and drops in disk IO for an ESX Server.

Scope

VMWESXServerStorage

Table 57. Rule Definition

Conditions	State	Action
The disk usage is no more than 2.2 standard deviations (NumSTDevs) from the mean disk usage.	Normal	None
The disk usage is more than 2.2 but no more than 2.8 standard deviations from the mean disk usage.	Warning	None
The disk usage is more than 2.8 standard deviations from the mean disk usage.	Critical	None

VMW ESX Server Queue Latency

Purpose

This rule fires when the Queue Command Latency for a physical disk in a VMware ESX Server exceeds the normal operating range. The Queue Command Latency for a collection interval is the time spent, per SCSI command, in the VM kernel queue.

Scope

VMWESXServerPhysicalDisk

Table 58. Rule Definition

Conditions	State	Action
The Queue Command Latency for a physical disk on all monitored ESX hosts does not exceed the number of milliseconds set by the `VMW:diskQueueLatency.warning` registry variable. The global default value of this variable is 25.	Normal	None
The Queue Command Latency for a physical disk on a monitored ESX host has exceeded the number of milliseconds set by the `VMW:diskQueueLatency.warning` registry variable. The global default value of this variable is 25.	Warning	None
The Queue Command Latency for a physical disk on a monitored ESX host has exceeded the number of milliseconds set by the `VMW:diskQueueLatency.critical` registry variable. The global default value of this variable is 35.	Critical	Send email to VMware administrator
The Queue Command Latency for a physical disk on a monitored ESX host has exceeded the number of milliseconds set by the `VMW:diskQueueLatency.fatal` registry variable. The global default value of this variable is 40.	Fatal	Send email to VMware administrator

VMW ESX Server Queue Latency Deviation

Purpose

This rule fires when the Queue Command Latency for a physical disk in a VMware ESX Server exceeds the normal operating range, using the standard deviation. The Queue Command Latency for a collection interval is the time spent, per SCSI command, in the VM kernel queue.

Scope

VMWESXServerPhysicalDisk

Table 59. Rule Definition

Conditions	State	Action
The Queue Command Latency for a physical disk on all monitored ESX is within the normal operating range.	Normal	None
The Queue Command Latency for a physical disk on a monitored ESX host has entered the Warning state, when calculated using the standard deviation.	Warning	None
The Queue Command Latency for a physical disk on a monitored ESX host has entered the Critical state, when calculated using the standard deviation.	Critical	Send email to VMware administrator

VMW ESX Server Total Latency

Purpose

This rule fires when the total command latency (that is, the time taken during the collection interval to process a SCSI command issued by the guest OS to the virtual machine or the sum of kernelLatency and deviceLatency, based on data from the seven days prior to yesterday) of an ESX Server physical disk exceeds the normal operating range.

Scope

VMWESXServerPhysicalDisk

Table 60. Rule Definition

Conditions	State	Action
The total command latency is less than 25 milliseconds.	Normal	None
The total command latency is 25 milliseconds or greater, but no greater than 34 milliseconds.	Warning	None
The total command latency is 35 milliseconds or greater, but no greater than 39 milliseconds.	Critical	Send email to VMware administrator
The total command latency is 40 milliseconds or greater.	Fatal	Send email to VMware administrator

VMW ESX Server Total Latency Deviation

Purpose

This rule fires when the total command latency (that is, the time taken during the collection interval to process a SCSI command issued by the guest OS to the virtual machine or the sum of kernelLatency and deviceLatency, based on data from the seven days prior to yesterday) of an ESX Server physical disk exceeds the normal operating range, using deviation.

Scope

VMWESXServerPhysicalDisk

Table 61. Rule Definition

Conditions	State	Action
The total command latency is no more than 2.2 standard deviations from the mean total command latency.	Normal	None
The total command latency is more than 2.2 but no more than 2.8 standard deviations from the mean total command latency.	Warning	None
The total command latency is more than 2.8 standard deviations from the mean total command latency.	Critical	Send email to VMware administrator

VirtualCenter Rules

This section describes the VirtualCenter rule. This rule is disabled by default, and can be enabled as required:

VMW VirtualCenter Disk IO

Purpose

This rule monitors for spikes and dramatic drops in disk IO for a VirtualCenter.

Scope

VMWVirtualCenter

Table 62. Rule Definition

Conditions	State	Action
The disk usage is no more than 2.2 standard deviations (NumSTDevs) from the mean disk usage.	Normal	None
The disk usage is more than 2.2 but no more than 2.8 standard deviations from the mean disk usage.	Warning	None
The disk usage is more than 2.8 standard deviations from the mean disk usage.	Critical	None

Views Displaying Alarms Based on this Rule

Virtual Machine Rules

This section lists and describes the virtual machine rules.

Rules in this section:

VMW Virtual Machine Disk Command Aborts

Purpose

This rule monitors for situations in which a disk command has been aborted because these may be an indication of hardware problems.

Scope

VMWVirtualMachineHostStorage

Table 63. Rule Definition

Conditions	State	Action
There are no disk command aborts to report.	Normal	None
A disk command abort has occurred.	Critical	Send email to VMware administrator

VMW Virtual Machine Disk IO

Purpose

This rule monitors for spikes and dramatic drops in disk IO for a virtual machine.

Scope

VMWVirtualMachineHostStorage

Table 64. Rule Definition

Conditions	State	Action
The disk usage is no more than 2.2 standard deviations (NumSTDevs) from the mean disk usage.	Normal	None
The disk usage is more than 2.2 but no more than 2.8 standard deviations from the mean disk usage.	Warning	None
The disk usage is more than 2.8 standard deviations from the mean disk usage.	Critical	None

VMW Virtual Machine Logical Drive Estimated Fill Time

Purpose

This rule determines when the virtual machine logical drive is likely to reach its capacity, based on its present growth rate.

Scope

VMWVirtualMachineLogicalDisk

Table 65. Rule Definition

Conditions	State	Action
At the present growth rate, the logical drive will not reach its capacity within 90 days.	Normal	None
At the present growth rate, the logical drive will reach its capacity in 90 days or less.	Warning	None
At the present growth rate, the logical drive will reach its capacity in 30 days or less.	Critical	Send email to VMware administrator
At the present growth rate, the logical drive will reach its capacity in 7 days or less.	Fatal	Send email to VMware administrator

VMW Virtual Machine Logical Drive Utilization

Purpose

This rule monitors disk utilization and fires when the disk utilization reaches 90 percent or greater.

Scope

VMWVirtualMachineLogicalDisk

Table 66. Rule Definition

Conditions	State	Action
The disk utilization is less than 90 percent.	Normal	None
The disk utilization is 90 percent or greater, but less than 95 percent.	Warning	None
The disk utilization is 95 percent or greater, but less than 99 percent.	Critical	Send email to VMware administrator
The disk utilization is 99 percent or greater.	Fatal	Send email to VMware administrator

VMW Virtual Machine Memory Swapping

Purpose

This rule monitors for the swapping in and out of virtual machine memory.

Scope

VMWVirtualMachineMemory

Table 67. Rule Definition

Conditions	State	Action
The virtual machine has not moved any of its memory from its physical pages to the VMware swap file within the ESX Server.	Normal	None
The virtual machine has moved some of its memory from its physical pages to the VMware swap file within the ESX Server. This may adversely affect the virtual machine's performance.	Critical	None
The virtual machine is actively using memory that it has moved to the VMware swap file. This will adversely affect the virtual machine's performance.	Fatal	None

Virtual Switch Rules

This section lists and describes the virtual switch rules.

Rules in this section:

VMW Distributed Virtual Switch Available Ports

Purpose

This rule checks for available ports on VMware distributed virtual switches.

Scope

VMWDistributedVirtualSwitch

Table 68. Rule Definition

Conditions	State	Action
The number of available ports on a distributed virtual switch is greater than the value set by the `VMW:DistributedVirtualSwitchAvailablePorts.warning` registry variable. The global default value of this variable is 20, meaning that in a default installation each of the monitored distributed virtual switches has more than 20 available ports.	Normal	None

Table 68. Rule Definition

The number of available ports on a distributed virtual switch reached the value set by the `VMW:DistributedVirtualSwitchAvailablePorts.warning` registry variable. The global default value of this variable is 20, meaning that in a default installation a Warning alarm is generated if a distributed virtual switch has 20 or fewer available ports.	Warning	None
The number of available ports on a distributed virtual switch reached the value set by the `VMW:DistributedVirtualSwitchAvailablePorts.critical` registry variable. The global default value of this variable is 10, meaning that in a default installation a Critical alarm is generated if a distributed virtual switch has 10 or fewer available ports.	Critical	None
The number of available ports on a distributed virtual switch reached the value set by the `VMW:DistributedVirtualSwitchAvailablePorts.fatal` registry variable. The global default value of this variable is 5, meaning that in a default installation a Fatal alarm is generated if a distributed virtual switch has 5 or fewer available ports.	Fatal	None

VMW Distributed Virtual Switch Network Utilization

Purpose

This rule checks the levels of network utilization on VMware distributed virtual switches.

Scope

VMWDistributedVirtualSwitch

Table 69. Rule Definition

Conditions	State	Action
The levels of network utilization on all monitored distributed virtual switches is below the percentage set by the `VMW:DistributedVirtualSwitchNetwork.warning` variable. The global default value of this variable is 75, meaning that in a default installation the network utilization of each of the monitored distributed virtual switches is lower than 75%.	Normal	None
The level of network utilization of a distributed virtual switch reached the percentage set by the `VMW:DistributedVirtualSwitchNetwork.warning` variable. The global default value of this variable is 75, meaning that in a default installation a Warning alarm is generated if the network utilization of a distributed virtual switch is 75% or higher.	Warning	None
The level of network utilization of a distributed virtual switch reached the percentage set by the `VMW:DistributedVirtualSwitchNetwork.critical` variable. The global default value of this variable is 85, meaning that in a default installation a Critical alarm is generated if the network utilization of a distributed virtual switch is 85% or higher.	Critical	None
The level of network utilization of a distributed virtual switch reached the percentage set by the `VMW:DistributedVirtualSwitchNetwork.fatal` variable. The global default value of this variable is 95, meaning that in a default installation a Fatal alarm is generated if the network utilization of a distributed virtual switch is 95% or higher.	Fatal	None

VMW Distributed Virtual Switch Packet Loss

Purpose

This rule checks the levels of packet loss on VMware distributed virtual switches.

Scope

VMWDistributedVirtualSwitch

Table 70. Rule Definition

Conditions	State	Action
The levels of packet loss on all monitored distributed virtual switches matches the percentage set by the `VMW:DistributedVirtualSwitchPacketLoss.warning` variable. The global default value of this variable is 0, meaning that in a default installation the packet loss on each of the monitored distributed virtual switches is 0%.	Normal	None
The level of packet loss of a distributed virtual switch is higher than the percentage set by the `VMW:DistributedVirtualSwitchPacketLoss.warning` variable. The global default value of this variable is 0 meaning that in a default installation a Warning alarm is generated if the packet loss on a distributed virtual switch is higher than 0%	Warning	None
The level of packet loss of a distributed virtual switch reached the percentage set by the `VMW:DistributedVirtualSwitchPacketLoss.critical` variable. The global default value of this variable is 85, meaning that in a default installation a Critical alarm is generated if the packet loss of a distributed virtual switch is higher than 10%.	Critical	None
The level of packet loss of a distributed virtual switch reached the percentage set by the `VMW:DistributedVirtualSwitchPacketLoss.fatal` variable. The global default value of this variable is 95, meaning that in a default installation a Fatal alarm is generated if the packet loss of a distributed virtual switch is higher than 20%.	Fatal	None

VMW Standard Virtual Switch Available Ports

Purpose

This rule checks for available ports on VMware standard virtual switches.

Scope

VMWHostVirtualSwitch

Table 71. Rule Definition

Conditions	State	Action
The number of available ports on a standard virtual switch is greater than the value set by the `VMW:StandardVirtualSwitchAvailablePorts.warning` registry variable. The global default value of this variable is 20, meaning that in a default installation each of the monitored standard virtual switches has more than 20 available ports.	Normal	None
The number of available ports on a standard virtual switch reached the value set by the `VMW:StandardVirtualSwitchAvailablePorts.warning` registry variable. The global default value of this variable is 20, meaning that in a default installation a Warning alarm is generated if a standard virtual switch has 20 or fewer available ports.	Warning	None
The number of available ports on a standard virtual switch reached the value set by the `VMW:DistributedVirtualSwitchAvailablePorts.critical` registry variable. The global default value of this variable is 10, meaning that in a default installation a Critical alarm is generated if a standard virtual switch has 10 or fewer available ports.	Critical	None
The number of available ports on a standard virtual switch reached the value set by the `VMW:StandardVirtualSwitchAvailablePorts.fatal` registry variable. The global default value of this variable is 5, meaning that in a default installation a Fatal alarm is generated if a standard virtual switch has 5 or fewer available ports.	Fatal	None

VMW Standard Virtual Switch Network Packet Loss

Purpose

This rule checks the levels of packet loss on VMware standard virtual switches.

Scope

VMWHostVirtualSwitch

Table 72. Rule Definition

Conditions	State	Action
The levels of packet loss on all monitored distributed virtual switches matches the percentage set by the `VVMW:StandardVirtualSwitchPacketLoss.warning` variable. The global default value of this variable is 0, meaning that in a default installation the packet loss on each of the monitored distributed virtual switches is 0%.	Normal	None
The level of packet loss of a distributed virtual switch is higher than the percentage set by the `VMW:StandardVirtualSwitchPacketLoss.warning` variable. The global default value of this variable is 0 meaning that in a default installation a Warning alarm is generated if the packet loss on a distributed virtual switch is higher than 0%	Warning	None
The level of packet loss of a distributed virtual switch reached the percentage set by the `VMW:StandardVirtualSwitchPacketLoss.critical` variable. The global default value of this variable is 85, meaning that in a default installation a Critical alarm is generated if the packet loss of a distributed virtual switch is higher than 10%.	Critical	None
The level of packet loss of a distributed virtual switch reached the percentage set by the `VMW:StandardVirtualSwitchPacketLoss.fatal` variable. The global default value of this variable is 95, meaning that in a default installation a Fatal alarm is generated if the packet loss of a distributed virtual switch is higher than 20%.	Fatal	None

VMW Standard Virtual Switch Network Utilization

Purpose

This rule checks the levels of network utilization on VMware standard virtual switches.

Scope

VMWHostVirtualSwitch

Table 73. Rule Definition

Conditions	State	Action
The levels of network utilization on all monitored standard virtual switches is below the percentage set by the `VMW:StandardVirtualSwitchNetwork.warning` variable. The global default value of this variable is 75, meaning that in a default installation the network utilization of each of the monitored standard virtual switches is 75% or lower.	Normal	None
The level of network utilization of a standard virtual switch reached the percentage set by the `VMW:StandardVirtualSwitchNetwork.warning` variable. The global default value of this variable is 75, meaning that in a default installation a Warning alarm is generated if the network utilization of a standard virtual switch is higher than 75%.	Warning	None
The level of network utilization of a standard virtual switch reached the percentage set by the `VMW:StandardVirtualSwitchNetwork.critical` variable. The global default value of this variable is 85, meaning that in a default installation a Critical alarm is generated if the network utilization of a standard virtual switch is higher than 85%.	Critical	None
The level of network utilization of a standard virtual switch reached the percentage set by the `VMW:StandardVirtualSwitchNetwork.fatal` variable. The global default value of this variable is 95, meaning that in a default installation a Fatal alarm is generated if the network utilization of a standard virtual switch is higher than 95%.	Fatal	None

VMW Virtual Switch Credentials Invalid

Purpose

This rule monitors the accuracy of virtual switch credentials.

Scope

VMWVirtualSwitch.alerts

Table 74. Rule Definition

Conditions	State	Action
All monitored virtual switches have valid credentials.	Normal	None
The credentials for a virtual switch are invalid which prevents data collections for the configurations associated with that switch.	Fatal	None

Appendix: Alarm Messages

This appendix describes the alarm messages generated by the VMware Performance Agent, and suggests possible solutions.

An error has occurred while attempting to connect to the vCenter. Please review the credentials used by the agent for accessing the vCenter.

Possible solutions:

- Ensure the VMware Performance Agent properties contain a valid user name and password.

The user account configured for the agent does not have sufficient permissions to perform its collections. Please review the agent configuration and ensure the correct account is being used and that this account has the necessary permissions in the VMware environment.

Possible solutions:

- Ensure the VMware Performance Agent credentials are configured to grant sufficient user permissions.
- Ensure the user has sufficient permissions on the Virtual Center.

The agent was unable to connect to the vCenter. Please review the Host Name and Host Port in the agent configuration. If these are correct there may be issues in your network preventing the connection to the vCenter.

Possible solutions:

- Incorrect host name
    - Ensure the VMware Performance Agent properties contain a valid host name.
- Incorrect port number
    - Ensure the VMware Performance Agent properties contain a valid port number.
- The specified host name does not resolve in DNS
    - Correct any DNS issues.
- The specified IP address not reachable
    - Correct any network issues.

The agent was unable to connect to the vCenter. Please review the Host Name and Host Port in the agent configuration. If these are correct there may be an issue with the vCenter causing it to refuse connections. Please contact the administrator of the VMware environment to ensure the vCenter is operating normally.

Possible solutions:

- Incorrect host name
    - Ensure the VMware Performance Agent properties contain a valid host name.
- Incorrect port number
    - Ensure the VMware Performance Agent properties contain a valid port number.

An invalid Host Port value has been used in one or more attempts to connect to the vCenter. Please review your agent configuration to ensure proper connection information has been entered.

Possible solutions:

- Incorrect port number
    - Ensure the VMware Performance Agent properties contain a valid port number.

The vCenter defined in the agent configuration is running a version that is not supported by this product. Please review the Host Name and Host Port in the agent configuration to ensure the connection settings point to the intended system. You may also need to contact your VMware administrator to ensure it is on one of the supported versions.

Possible solutions:

- Update the vCenter to a supported version.

The agent is unable to find a route through the network to communicate with the vCenter. Please contact your network administrator to ensure that the Foglight, Agent (if separate), and vCenter systems are able to communicate or

to resolve other network issues that may be resulting in this issue.

Possible solutions:

- Incorrect host name

    - Ensure the VMware Performance Agent properties contain a valid host name.

- Incorrect port number

    - Ensure the VMware Performance Agent properties contain a valid port number.

- The specified host name does not resolve in DNS

    - Correct any DNS issues.

- The specified IP address not reachable

    - Correct any network issues.

A problem occurred connecting to the vCenter. Please review your agent configuration to ensure proper connection information has been entered.

Possible solutions:

- Incorrect host name

    - Ensure the VMware Performance Agent properties contain a valid host name.

- The specified host name does not resolve in DNS

    - Correct any DNS issues.

- The specified IP address is not reachable

    - Correct any network issues.

The agent was unable to construct a valid URL from the connection information provided. Please review your agent configuration to ensure proper connection information has been entered.

Possible solutions:

- Incorrect host name

    - Ensure the VMware Performance Agent properties contain a valid host name.

An unexpected error occurred while connecting to the vCenter. Please review your agent configuration to ensure proper connection information has been entered.

Possible solutions:

- Incorrect host name

    - Ensure the VMware Performance Agent properties contain a valid host name.

- Incorrect credentials

- Ensure the VMware Performance Agent properties contain a correct user name and password.
- Incorrect port number
    - Ensure the VMware Performance Agent properties contain a valid port number.
- The specified host name does not resolve in DNS
    - Correct any DNS issues.
- The specified IP address not reachable.
    - Correct any network issues.

The agent has entered an invalid state and is unable to proceed with normal operation. This situation may be self-correcting. However, if you continue to see this message, please deactivate the agent and then reactivate it one or two minutes after deactivation completed. If the situation continues please contact Quest Support.

Possible solutions:

- If alarm reoccurs, contact Quest Support

The agent was unable to establish a secure SSL connection to the vCenter. Please review your agent configuration to ensure proper connection information has been entered.

Possible solutions:

- Incorrect connection settings
    - Ensure the VMware Performance Agent properties contain a valid host name and port number.
- vCenter not accepting SSL connections
    - Enable SSL Connections in your Virtual Center.

An unexpected error occurred while connecting to the vCenter. Please review your agent configuration to ensure proper connection information has been entered.

Possible solutions:

- Incorrect host name
    - Ensure the VMware Performance Agent properties contain a valid host name.
- Incorrect credentials
    - Ensure the VMware Performance Agent properties contain a correct user name and password
- Incorrect port number
    - Ensure the VMware Performance Agent properties contain a valid port number.
- The specified host name does not resolve in DNS.
    - Correct any DNS issues.

- The specified IP address not reachable.
    - Correct any network issues.

Collecting performance data for one or more specific entities has caused the performance data request to the vCenter to fail. No further performance data will be collected for these entities. Please review the status of these entities in the VMware Environment and address any serious issues that may have occurred. Once the entities are operating normally, they can be removed from the Agent-Managed Blacklisted Entities list and performance data collections will resume for the entities. Consult the VMware Monitoring in Foglight Evolve Cloud documentation for the procedure for removing an entity from the Agent-Managed Blacklisted Entities list.

Possible solutions:

- Resolve any errors with these entities in the virtual environment.

Collecting performance data for 25 or more specific entities has caused the performance data request to the vCenter to fail. Due to the size of this number it is likely that an issue with the virtual environment is the root cause and these entities are not specifically at fault. Please resolve any known environment issues. If the situation continues, please contact Quest Support.

Possible solutions:

- Resolve any known environment issues.

An unexpected issue occurred during data collection from the vCenter. Please review your environment to ensure that data collection has resumed in a normal fashion. If there is a persistent problem or this message recurs regularly please contact Quest Support.

Possible solutions:

- Confirm that the VMware data collection resumed after the issue was encountered by the agent. If the Foglight Evolve Cloud installation is not receiving VMware monitoring data or this message occurs regularly, contact Quest Support.

Appendix: Metrics

This appendix lists what metrics are collected by the VMware Performance Agent, and explains the collected metrics.

Virtual machine metrics

Table 75. Virtual machine metrics

Topology	Metric name	Description
host.cpus.processor	usedHz	CPU usage, as measured in hertz, during the interval
host.cpus.processor	percentSystemTime	Amount of time spent on system processes on each virtual CPU in the virtual machine
host.cpus.processor	Utilization	CPU usage as a percentage during the interval
host.cpus	usedHz	CPU usage, as measured in hertz, during the interval
host.cpus	percentSystemTime	The percent of time spent on system processes on each virtual CPU in the virtual machine
host.cpus	Utilization	CPU usage as a percentage during the interval
cpus.processor	percentReadyTime	The percent of time that the virtual machine was ready, but could not get scheduled to run on the physical CPU during last measurement interval
cpus.processor	swapWaitPercent	The percent of CPU time spent waiting for memory swap-in
cpus.processor	maxlimited	The percent of time the virtual machine is ready to run, but is not running because it has reached its maximum CPU limit setting
cpus.processor	coStopPercent	The percent of time the virtual machine is ready to run, but is unable to run due to co-scheduling constraints
cpus	percentReadyTime	The percent of time that the virtual machine was ready, but could not get scheduled to run on the physical CPU during last measurement interval
cpus	summedPercentReady	Sum of all vCPU's percentReadyTime
cpus	swapWait	CPU time spent waiting for memory swap-in
cpus	swapWaitPercent	The percent of CPU time spent waiting for memory swap-in
cpus	maxlimited	The percent of time the virtual machine is ready to run, but is not running because it has reached its maximum CPU limit setting
cpus	coStop	Time the virtual machine is ready to run, but is unable to run due to co-scheduling constraints
cpus	coStopPercent	The percent of time the virtual machine is ready to run, but is unable to run due to co-scheduling constraints
cpus	demand	The amount of CPU resources a virtual machine would use if there were no CPU contention or CPU limit

Table 75. Virtual machine metrics

cpus	latency	Percent of time the virtual machine is unable to run because it is contending for access to the physical CPU(s)
cpus	shares	The priority of CPU resource allocation
cpus	reservation	Amount of CPU resource reserved for virtual machine
cpus	limit	Max of CPU resource can be allocated to VM due to limit setting
host.memory	consumed	Amount of host physical memory consumed by host
host.memory	utilization	Memory usage as percentage of total configured or available memory
host.memory	capacity	Amount of configured memory
memory	active	Amount of memory that is actively used, as estimated by VMkernel based on recently touched memory pages
memory	allocated	Amount of configured memory
memory	balloon	Amount of memory allocated by the virtual machine memory control driver
memory	balloonTarget	Target value set by VMkernal for the virtual machine's memory balloon size
memory	capacity	Amount of configured memory
memory	granted	Amount of host physical memory or physical memory that is mapped for a virtual machine
memory	limit	Max of physical memory can be allocated to virtual machine due to limit setting
memory	overhead	Host physical memory consumed by the virtualization infrastructure for running the virtual machine
memory	reservation	Amount of memory resource reserved for virtual machine
memory	shared	Amount of guest physical memory that is shared with other virtual machines
memory	shares	The priority of memory resource allocation
memory	swapIn	Amount swapped-in to memory from disk
memory	swapOut	Amount of memory swapped-out to disk
memory	swapped	Current amount of guest physical memory swapped out to the virtual machine swap file by the Vmkernel
memory	swapTarget	Target size for the virtual machine swap file
memory	vmSwapInRate	Rate at which memory is swapped from disk into active memory during the interval
memory	vmSwapOutRate	Rate at which memory is being swapped from active memory to disk during the current interval
host.network.interface	inboundPacketsDropped	Number of received packets dropped during the collection interval
host.network.interface	outboundPacketsDropped	Number of transmitted packets dropped during the collection interval
host.network.interface	packetsReceived	Packets received per second during the interval
host.network.interface	packetsSent	Packets transmitted per second during the interval
host.network.interface	receiveRate	Average amount of data received per second during the interval
host.network.interface	sendRate	Average amount of data transmitted per second during the interval
host.network	packetsReceived	Sum of packetsReceived of all NICs

Table 75. Virtual machine metrics

host.network	packetsSent	Sum of packetsSent of all NICs
host.network	receiveRate	Sum of receiveRate of all NICs
host.network	sendRate	Sum of sendRate of all NICs
host.network	transferRate	Sum of transferRate of all NICs
network.interface	networkPacketLoss	percent of dropped packets
network.interface	utilization	deprecated metric
network	networkPacketLoss	average percent of dropped packets of all NICs
network	utilization	deprecated metric
host.storage.physical Disk	bytesRead	Average bytes read from the disk each second during the collection interval.
host.storage.physical Disk	bytesWritten	Average bytes written to disk each second during the collection interval
host.storage.physical Disk	reads	Average number of read commands issued per second from the disk during the collection interval.
host.storage.physical Disk	writes	Average number of write commands issued per second to the disk during the collection interval.
host.storage.logicalDi sk	capacityAvailable	Percent of available capacity of the logical disk
host.storage.logicalDi sk	capacityUsed	Percent of used capacity of the logical disk
host.storage.logicalDi sk	spaceAvailable	Available space of the logical disk
host.storage.logicalDi sk	spaceUsed	Used space of the logical disk
host.storage.logicalDi sk	totalSpace	Total space of the logical disk
host.storage	diskBytesRead	Sum of bytesRead of all physical disks
host.storage	diskBytesWritten	Sum of bytesWritten of all physical disks
host.storage	diskTransferRate	Sum of transferRate of all physical disks (diskBytesRead + diskBytesWritten)
host.storage	diskReads	Sum of reads of all physical disks
host.storage	diskWrites	Sum of writes of all physical disks
host.storage	diskUtilization	Percent of used capacity of all logical disks
host.storage	spaceAvailable	Sum of spaceAvailable of all logical disks
host.storage	spaceUsed	Sum of spaceUsed of all logical disks
storage.physicalDisk	commandAbortsRate	Number of SCSI commands aborted per second during the collection interval.
storage.physicalDisk	commandsIssuedRate	Number of SCSI commands issued per second during the collection interval.
storage.physicalDisk	bytesTotal	Average bytes transfer of disk each second during the collection interval. (bytesRead + bytesWritten)
storage.datastore(VM WDatastoreUsage)	read	Average bytes read from the datastore each second during the collection interval.
storage.datastore(VM WDatastoreUsage)	write	Average bytes written to datastore each second during the collection interval
storage.datastore(VM WDatastoreUsage)	transferRate	Average transferRate of the datastore each second during the collection interval. (read + write)

Table 75. Virtual machine metrics

storage.datastore(VMWDatastoreUsage)	readCommands	Average number of read commands issued per second from the datastore during the collection interval.
storage.datastore(VMWDatastoreUsage)	writeCommands	Average number of write commands issued per second to the datastore during the collection interval.
storage.datastore(VMWDatastoreUsage)	iops	Average number of commands issued per second to the datastore during the collection interval. (readCommands + writeCommands)
storage.datastore(VMWDatastoreUsage)	readLatency	Average amount of time for a read operation from the datastore
storage.datastore(VMWDatastoreUsage)	writeLatency	Average amount of time for a write operation to the datastore
storage.datastore(VMWDatastoreUsage)	averageLatency	Average amount of time for a I/O operation to the datastore
storage.virtualDisk	busResets	Number of SCSI-bus reset commands issued during the collection interval.
storage.virtualDisk	commandsAborted	Number of SCSI commands aborted during the collection interval.
storage.virtualDisk	iops	Average number of commands issued per second to the virtual disk during the collection interval
storage.virtualDisk	numberReadAveraged	Average number of read commands issued per second to the virtual disk during the collection interval
storage.virtualDisk	numberWriteAveraged	Average number of write commands issued per second to the virtual disk during the collection interval
storage.virtualDisk	read	Rate of reading data from the virtual disk
storage.virtualDisk	write	Rate of writing data to the virtual disk
storage.virtualDisk	throughput	Rate of data throughput of the virtual disk. (read + write)
storage.virtualDisk	totalReadLatency	Average amount of time for a read operation from the virtual disk
storage.virtualDisk	totalWriteLatency	Average amount of time for a write operation to the virtual disk
storage.virtualDisk	totalCommandLatency	Average amount of time for a I/O operation to the virtual disk
storage.virtualDisk	readLoadMetric	Storage DRS virtual disk metric for the read workload model
storage.virtualDisk	writeLoadMetric	Storage DRS virtual disk metric for the write workload model
storage.virtualDisk	readOIO	Average number of outstanding read requests to the virtual disk during the collection interval
storage.virtualDisk	writeOIO	Average number of outstanding write requests to the virtual disk during the collection interval.
storage	datastoreRead	Sum of read of all datastores
storage	datastoreWrite	Sum of write of all datastores
storage	datastoreTransferRate	Sum of transferRate of all datastores
storage	datastoreReadCommands	Sum of readCommands of all datastores
storage	datastoreWriteCommands	Sum of writeCommands of all datastores
storage	datastoreIops	Sum of iops of all datastore
storage	diskCommandAbortsRate	Sum of commandAbortsRate of all physical disks
storage	diskCommandsIssuedRate	Sum of commandsIssuedRate of all physical disks

Table 75. Virtual machine metrics

storage	diskReadRequestsRate	Sum of reads of all physical disks
storage	diskWriteRequestsRate	Sum of writes of all physical disks
VMWVsanObject	read	Rate of reading data from the vSAN object (A virtual disk is a vSAN object)
VMWVsanObject	write	Rate of writing data from the vSAN object
VMWVsanObject	transferRate	Rate of data transferRate of the vSAN object (read + write)
VMWVsanObject	readCommands	Average number of read commands issued per second to the vSAN object during the collection interval
VMWVsanObject	writeCommands	Average number of write commands issued per second to the vSAN object during the collection interval
VMWVsanObject	iops	Average number of commands issued per second to the vSAN object during the collection interval
VMWVsanObjectContent	read	Rate of reading data from the vSAN Content(A vSAN object may store on several contents(phisical disk), depends on vSAN policy)
VMWVsanObjectContent	write	Rate of writing data from the vSAN Content
VMWVsanObjectContent	transferRate	Rate of data transferRate of the vSAN Content (read + write)
VMWVsanObjectContent	readCommands	Average number of read commands issued per second to the vSAN Content during the collection interval
VMWVsanObjectContent	writeCommands	Average number of write commands issued per second to the vSAN Content during the collection interval
VMWVsanObjectContent	iops	Average number of commands issued per second to the vSAN Content during the collection interval

ESXi host metrics

Table 76. ESXi host metrics

Topology	Metric name	Description
host.cpus.processor	usedHz	CPU usage, as measured in hertz, during the interval
host.cpus.processor	Utilization	CPU usage as a percentage during the interval
host.cpus	usedHz	CPU usage, as measured in hertz, during the interval
host.cpus	Utilization	CPU usage as a percentage during the interval
host.cpus	totalHz	Total amount of CPU resources is equal to the frequency of the processors multiplied by the number of cores.
cpus	percentReadyTime	average of averages from child VM percentReadyTime
cpus	demand	The amount of CPU resources a virtual machine would use if there were no CPU contention or CPU limit
host.memory	consumed	Amount of host physical memory consumed by host
host.memory	utilization	Memory usage as percentage of total configured or available memory
host.memory	capacity	Amount of configured memory
memory	active	Amount of memory that is actively used, as estimated by VMkernel based on recently touched memory pages

Table 76. ESXi host metrics

memory	balloon	Amount of memory allocated by the virtual machine memory control driver
memory	capacity	Amount of configured memory
memory	consumed	Amount of host physical memory consumed by a virtual machine
memory	granted	Amount of host physical memory or physical memory that is mapped for a virtual machine
memory	heap	VMkernel virtual address space dedicated to VMkernel main heap and related data
memory	heapFree	Free address space in the VMkernel main heap.Varies based on number of physical devices and configuration options
memory	overhead	Host physical memory consumed by the virtualization infrastructure for running the virtual machine
memory	reservedCapacity	Total amount of memory reservation used by powered-on virtual machines and vSphere services on the host
memory	serverSwapInRate	Rate at which memory is swapped from disk into active memory during the interval
memory	serverSwapOutRate	Rate at which memory is being swapped from active memory to disk during the current interval
memory	sharedCommon	Amount of machine memory that is shared by all powered-on virtual machines and vSphere services on the host
memory	shared	Sum of all shared metrics for all powered-on virtual machines, plus amount for vSphere services on the host
memory	swapIn	Sum of swapin values for all powered-on virtual machines on the host.
memory	swapOut	Sum of swapout metrics from all powered-on virtual machines on the host.
memory	swapUsed	Current amount of guest physical memory swapped out to the virtual machine swap file by the Vmkernel
memory	unreserved	Amount of memory that is unreserved
memory	vmKernel	Amount of memory used by vmKernel
memory	zero	Memory that contains 0s only.Included in shared amount, Host: Sum of zero metrics for all powered-on virtual machines, plus vSphere services on the host.
host.network.interface	packetsReceived	Packets received per second during the interval.
host.network.interface	packetsSent	Packets transmitted per second during the interval.
host.network.interface	receiveRate	Average amount of data received per second during the interval.
host.network.interface	sendRate	Average amount of data transmitted per second during the interval.
host.network.interface	bandwidth	bandwidth of the NIC
host.network.interface	inboundPacketsDropped	Number of received packets dropped during the collection interval.
host.network.interface	outboundPacketsDropped	Number of transmitted packets dropped during the collection interval.
host.network	packetsReceived	Sum of packetsReceived of all NICs
host.network	packetsSent	Sum of packetsSent of all NICs
host.network	receiveRate	Sum of receiveRate of all NICs
host.network	sendRate	Sum of endRate of all NICs

Table 76. ESXi host metrics

host.network	transferRate	Sum of transferRate of all NICs
network.interface	ftusage	Average pNic I/O rate for FT
network.interface	hbrusage	Average pNic I/O rate for HBR
network.interface	iscsiusage	Average pNic I/O rate for iSCSI
network.interface	nfsusage	Average pNic I/O rate for NFS
network.interface	usage	The current network usage for the NIC
network.interface	utilization	The current network percent usage for the NIC
network.interface	vmotionusage	Average pNic I/O rate for vMotion
network.interface	vmusage	Average pNic I/O rate for VMs
network.switch	ftTrafficUtilization	FT traffic utlization for the vSwitch
network.switch	hbrTrafficUtilization	HBR traffic utlization for the vSwitch
network.switch	iscsiTrafficUtilization	iSCSI traffic utlization for the vSwitch
network.switch	networkPacketLoss	Percent of packet loss for the vSwitch
network.switch	networkThroughput	Throughput for the vSwitch
network.switch	networkUtilization	bandwidth Utilization for the vSwitch
network.switch	nfsTrafficUtilization	NFS traffic utlization for the vSwitch
network.switch	sumThroughput	ftusage + hbrusage + iscsiusage + nfsusage + vmotionusage + vmusage of All attached NICs
network.switch	vmotionTrafficUtilization	vMotion traffic utlization for the vSwitch
network.switch	vmTrafficUtilization	VMs traffic utlization for the vSwitch
network	bandwidth	bandwidth of all available pNICs on the host
host.storage.physicalDisk	bytesRead	Average number of bytes read from the disk each second during the collection interval.
host.storage.physicalDisk	bytesWritten	Average number of bytes written to disk each second during the collection interval
host.storage.physicalDisk	reads	Average number of read commands issued per second from the disk during the collection interval.
host.storage.physicalDisk	writes	Average number of write commands issued per second to the disk during the collection interval.
host.storage	diskBytesRead	Sum of bytesRead of all physical disks
host.storage	diskBytesWritten	Sum of bytesWritten of all physical disks
host.storage	diskTransferRate	Sum of transferRate of all physical disks (diskBytesRead + diskBytesWritten)
host.storage	diskReads	Sum of reads of all physical disks
host.storage	diskWrites	Sum of writes of all physical disks
storage.physicalDisk	commandAbortsRate	Number of SCSI commands aborted per second during the collection interval.
storage.physicalDisk	commandsIssuedRate	Number of SCSI commands issued per second during the collection interval.
storage.physicalDisk	deviceReadLatency	Average amount of time, in milliseconds, to read from the physical device
storage.physicalDisk	kernelReadLatency	Average amount of time, in milliseconds, spent by VMkernel to process each SCSI read command
storage.physicalDisk	totalReadLatency	Average amount of time taken during the collection interval to process a SCSI read command issued from the guest OS to the virtual machine

Table 76. ESXi host metrics

storage.physicalDisk	queueReadLatency	Average amount of time spent in the VMkernel queue, per SCSI read command, during the collection interval
storage.physicalDisk	deviceWriteLatency	Average amount of time, in milliseconds, to write to the physical device
storage.physicalDisk	kernelWriteLatency	Average amount of time, in milliseconds, spent by VMkernel to process each SCSI write command
storage.physicalDisk	totalWriteLatency	Average amount of time taken during the collection interval to process a SCSI write command issued by the guest OS to the virtual machine
storage.physicalDisk	queueWriteLatency	Average amount of time spent in the VMkernel queue, per SCSI write command, during the collection interval
storage.physicalDisk	deviceCommandLatency	Average amount of time taken during the collection interval to process a SCSI write command issued by the guest OS to the virtual machine
storage.physicalDisk	kernelCommandLatency	Average amount of time, in milliseconds, spent by VMkernel to process each SCSI command
storage.physicalDisk	totalCommandLatency	Average amount of time taken during the collection interval to process a SCSI command issued by the guest OS to the virtual machine
storage.physicalDisk	queueCommandLatency	Average amount of time spent in the VMkernel queue, per SCSI command, during the collection interval.
storage.physicalDisk	bytesTotal	Average bytes transfer of disk each second during the collection interval. (bytesRead + bytesWritten)
storage.storageAdapter(VMWESXStorageAdapter)	read	Rate of reading data by the storage adapter
storage.storageAdapter(VMWESXStorageAdapter)	write	Rate of writing data by the storage adapter
storage.storageAdapter(VMWESXStorageAdapter)	readCommands	Average number of read commands issued per second by the storage adapter during the collection interval
storage.storageAdapter(VMWESXStorageAdapter)	writeCommands	Average number of write commands issued per second by the storage adapter during the collection interval
storage.storageAdapter(VMWESXStorageAdapter)	totalCommands	Average number of commands issued per second by the storage adapter during the collection interval
storage.storageAdapter(VMWESXStorageAdapter)	readLatency	Average amount of time for a read operation by the storage adapter.
storage.storageAdapter(VMWESXStorageAdapter)	writeLatency	Average amount of time for a write operation by the storage adapter.
storage.datastore(VMWDatastoreUsage)	read	Average bytes read from the datastore each second during the collection interval.
storage.datastore(VMWDatastoreUsage)	write	Average bytes written to datastore each second during the collection interval
storage.datastore(VMWDatastoreUsage)	transferRate	Average bytes transferRate of datastore each second during the collection interval (read + write)
storage.datastore(VMWDatastoreUsage)	readCommands	Average number of read commands issued per second from the datastore during the collection interval.

Table 76. ESXi host metrics

storage.datastore(VMWDatastoreUsage)	writeCommands	Average number of write commands issued per second to the datastore during the collection interval.
storage.datastore(VMWDatastoreUsage)	datastoreIops	Average number of commands issued per second to the datastore during the collection interval.
storage.datastore(VMWDatastoreUsage)	readLatency	Average amount of time for a read operation from the datastore
storage.datastore(VMWDatastoreUsage)	writeLatency	Average amount of time for a write operation to the datastore
storage.datastore(VMWDatastoreUsage)	averageLatency	Average amount of time for a I/O operation to the datastore
storage.datastore(VMWDatastoreUsage)	iops	Average number of write commands issued per second to the datastore during the collection interval.
storage.datastore(VMWDatastoreUsage)	datastoreMaxQueueDepth	The maximum number of I/Os that can be outstanding at a given time
storage	datastoreIops	Sum of iops of all datastores
storage	datastoreRead	Sum of read of all datastores
storage	datastoreReadCommands	Sum of readCommands of all datastores
storage	datastoreTransferRate	Sum of transferRate of all datastores
storage	datastoreWrite	Sum of write of all datastores
storage	datastoreWriteCommands	Sum of writeCommands of all datastore
storage	diskCommandAbortsRate	Sum of commandAbortsRate of all physical disks
storage	diskCommandsIssuedRate	Sum of commandsIssuedRate of all physical disks
storage	diskReadRequestsRate	Sum of reads of all physical disks
storage	diskWriteRequestsRate	Sum of writes of all physical disks
VMWVsanDisk	spaceReserved	Reserved space of the vSAN disk
VMWVsanDisk	spaceUsed	Used space of the vSAN disk
VMWVsanDisk	totalSpace	Total space of the vSAN disk

Datastore metrics

Table 77. Datastore metrics

Topology	Metric name	Description
VMWDatastore	read	Average number of bytes read from the datastore each second during the collection interval (sum from attached ESX Host VMWDatastoreUsage objects)
VMWDatastore	write	Average number of bytes written to datastore each second during the collection interval (sum from attached ESX Host VMWDatastoreUsage objects)
VMWDatastore	readwriteTotal	read + write
VMWDatastore	readLatency	Average amount of time for a read operation from the datastore

Table 77. Datastore metrics

VMWDatastore	writeLatency	Average amount of time for a write operation to the datastore
VMWDatastore	averageLatency	Average amount of time for a I/O operation to the datastore
VMWDatastore	capacityAvailable	Percent of available capacity for the datastore
VMWDatastore	capacityUsed	Percent of used capacity for the datastore
VMWDatastore	totalSpace	Total space of the datastore
VMWDatastore	uncommitted	Uncommitted space of the datastore
VMWDatastore	spaceAvailable	Available space of the datastore
VMWDatastore	spaceUsed	Used space of the datastore
VMWVirtualStorage	capacityAvailable	Percent of available capacity for the datastore
VMWVirtualStorage	capacityUsed	Percent of used capacity for the datastore
VMWVirtualStorage	totalSpace	Total space of the datastore
VMWVirtualStorage	uncommitted	Uncommitted space of the datastore
VMWVirtualStorage	spaceAvailable	Available space of the datastore
VMWVirtualStorage	spaceUsed	Used space of the datastore

Datastore cluster metrics

Table 78. Datastore cluster metric

Topology	Metric name	Description
VMWDatastoreCluster	read	Average number of bytes read from the datastore cluster each second during the collection interval (sum of child datastores)
VMWDatastoreCluster	write	Average number of bytes written to datastore cluster each second during the collection interval (sum of child datastores)
VMWDatastoreCluster	readwriteTotal	read + write
VMWDatastoreCluster	readLatency	Average amount of time for a read operation from the datastore cluster
VMWDatastoreCluster	writeLatency	Average amount of time for a write operation to the datastore cluster
VMWDatastoreCluster	averageLatency	Average amount of time for a I/O operation to the datastore cluster
VMWDatastoreCluster	capacityAvailable	Percent of available capacity for the datastore cluster (sum of child datastores)
VMWDatastoreCluster	capacityUsed	Percent of used capacity for the datastore cluster (sum of child datastores)
VMWDatastoreCluster	totalSpace	Total space of the datastore cluster (sum of child datastores)
VMWDatastoreCluster	uncommitted	Uncommitted space of the datastore cluster (sum of child datastores)
VMWDatastoreCluster	spaceAvailable	Available space of the datastore cluster (sum of child datastores)
VMWDatastoreCluster	spaceUsed	Used space of the datastore cluster (sum of child datastores)

Resource pool metrics

Table 79. Resource pool metric

Topology	Metric name	Description
VMWResourcePool	avgDiskReadRequestsRate	Average disk read request rate of VMs under the resource pool
VMWResourcePool	avgDiskWriteRequestsRate	Average disk write request rate of VMs under the resource pool
VMWResourcePool	avgNetworkPacketsReceivedRate	Average network packet received rate of VMs under the resource pool
VMWResourcePool	avgNetworkPacketsTransmittedRate	Average network packet transmitted rate of VMs under the resource pool
VMWResourcePool	avgNetworkReceiveRatebps	Average network received rate of VMs under the resource pool
VMWResourcePool	avgNetworkTransmitRatebps	Average network transmitted rate of VMs under the resource pool
VMWResourcePool	cpuLimit	Max of CPU resource can be allocated to VMs under the resource pool
VMWResourcePool	cpuPercentReady	Average CPU PercentReady of VMs under the resource pool
VMWResourcePool	cpuReservation	Amount of CPU resource reserved for the resource pool
VMWResourcePool	cpuShares	The priority value of CPU resource allocation
VMWResourcePool	cpuUsedHz	Sum of usedHz from all VMs under the resource pool
VMWResourcePool	cpuUtilization	Average CPU utilization of VMs under the resource pool
VMWResourcePool	diskReadRate	Sum of disk bytesRead from all VMs under the resource pool
VMWResourcePool	diskReadRequestsRate	Sum of diskReadRequestsRate from all VMs under the resource pool
VMWResourcePool	diskUsage	sum of disk.usage.average from all VMs under the resource pool
VMWResourcePool	diskWriteRate	Sum of disk bytesWrite from all VMs under the resource pool
VMWResourcePool	diskWriteRequestsRate	Sum of diskWriteRequestsRate from all VMs under the resource pool
VMWResourcePool	memoryActive	Sum of active memory from all VMs under the resource pool
VMWResourcePool	memoryBalloon	Sum of balloon memory from all VMs under the resource pool
VMWResourcePool	memoryConsumed	Sum of consumed memory from all VMs under the resource pool
VMWResourcePool	memoryGranted	Sum of granted memory from all VMs under the resource pool
VMWResourcePool	memoryLimit	Max of physical memory resource can be allocated to VMs under the resource pool
VMWResourcePool	memoryOverhead	Sum of overhead memory from all VMs under the resource pool

Table 79. Resource pool metric

VMWResourcePool	memoryReservation	Amount of physical memory resource reserved for the resource pool
VMWResourcePool	memoryShared	Sum of shared memory from all VMs under the resource pool
VMWResourcePool	memoryShares	The priority value of cpu resource allocation
VMWResourcePool	memorySwapIn	Sum of active memory from all VMs under the resource pool
VMWResourcePool	memorySwapOut	Sum of active memory from all VMs under the resource pool
VMWResourcePool	memoryUtilization	Sum of active memory from all VMs under the resource pool
VMWResourcePool	memoryZero	Sum of active memory from all VMs under the resource pool
VMWResourcePool	networkPacketsReceivedRate	Sum of network packetsReceived from all VMs under the resource pool
VMWResourcePool	networkPacketsSentRate	Sum of network packetsSent from all VMs under the resource pool
VMWResourcePool	networkReceiveRate	Sum of network receiveRate from all VMs under the resource pool
VMWResourcePool	networkSendRate	Sum of network sendRate from all VMs under the resource pool
VMWResourcePool	networkUsagebps	sum of net.usage.average from all VMs under the resource pool

vApp metrics

Table 80. vApp metrics

Topology	Metric name	Description
VMWvApp	avgDiskReadRequestsRate	Average disk read request rate of VMs under the vApp
VMWvApp	avgDiskWriteRequestsRate	Average disk write request rate of VMs under the vApp
VMWvApp	avgNetworkPacketsReceivedRate	Average network packet received rate of VMs under the vApp
VMWvApp	avgNetworkPacketsTransmittedRate	Average network packet transmitted rate of VMs under the vApp
VMWvApp	avgNetworkReceiveRatebps	Average network received rate of VMs under the vApp
VMWvApp	avgNetworkTransmitRatebps	Average network transmitted rate of VMs under the vApp
VMWvApp	cpuLimit	Max of CPU resource can be allocated to VMs under the resource pool
VMWvApp	cpuPercentReady	Average cpuPercentReady of VMs under the vApp
VMWvApp	cpuReservation	Amount of CPU resource reserved for the resource pool
VMWvApp	cpuShares	The priority value of CPU resource allocation

Table 80. vApp metrics

VMWvApp	cpuUsedHz	Sum of usedHz from all VMs under the vApp
VMWvApp	cpuUtilization	Average cpu utilization of VMs under the vApp
VMWvApp	diskReadRate	Sum of disk bytesRead from all VMs under the vApp
VMWvApp	diskReadRequestsRate	Sum of diskReadRequestsRate from all VMs under the vApp
VMWvApp	diskUsage	sum of disk.usage.average from all VMs under the vApp
VMWvApp	diskWriteRate	Sum of disk bytesWrite from all VMs under the vApp
VMWvApp	diskWriteRequestsRate	Sum of diskWriteRequestsRate from all VMs under the vApp
VMWvApp	memoryActive	Sum of active memory from all VMs under the vApp
VMWvApp	memoryBalloon	Sum of balloon memory from all VMs under the vApp
VMWvApp	memoryConsumed	Sum of consumed memory from all VMs under the vApp
VMWvApp	memoryGranted	Sum of granted memory from all VMs under the vApp
VMWvApp	memoryLimit	Max of physical memory resource can be allocated to VMs under the resource pool
VMWvApp	memoryOverhead	Sum of overhead memory from all VMs under the vApp
VMWvApp	memoryReservation	Amount of physical memory resource reserved for the resource pool
VMWvApp	memoryShared	Sum of shared memory from all VMs under the vApp
VMWvApp	memoryShares	The priority value of cpu resource allocation
VMWvApp	memorySwapIn	Sum of active memory from all VMs under the vApp
VMWvApp	memorySwapOut	Sum of active memory from all VMs under the vApp
VMWvApp	memoryUtilization	Average memory utilization of VMs under the vApp
VMWvApp	memoryZero	Sum of active memory from all VMs under the vApp
VMWvApp	networkPacketsReceivedRate	Sum of network packetsReceived from all VMs under the vApp
VMWvApp	networkPacketsSentRate	Sum of network packetsSent from all VMs under the vApp
VMWvApp	networkReceiveRate	Sum of network receiveRate from all VMs under the vApp
VMWvApp	networkSendRate	Sum of networr sendRate from all VMs under the vApp
VMWvApp	networkUsagebps	sum of net.usage.average from all VMs under the vApp

Cluster metrics

Table 81. Cluster metrics

Topology	Metric name	Description
VMWCluster	avgDiskReadRate	Average disk read rate of ESX Hosts under the cluster
VMWCluster	avgDiskReadRequestsRate	Average disk read request rate of ESX Hosts under the cluster
VMWCluster	avgDiskWriteRate	Average disk write rate of ESX Hosts under the cluster
VMWCluster	avgDiskWriteRequestsRate	Average disk write request rate of ESX Hosts under the cluster
VMWCluster	avgNetworkPacketsReceivedRate	Average network packet received rate of ESX Hosts under the cluster
VMWCluster	avgNetworkPacketsTransmittedRate	Average network packet transmitted rate of ESX Hosts under the cluster
VMWCluster	avgNetworkReceiveRatebps	Average network received rate of ESX Hosts under the cluster
VMWCluster	avgNetworkTransmitRatebps	Average network transmitted rate of ESX Hosts under the cluster
VMWCluster	cpuDemand	Sum of CPU demand from all ESX Hosts under the cluster
VMWCluster	cpuUsedHz	Sum of CPU usedHz from all ESX Hosts under the cluster
VMWCluster	cpuUtilization	Average CPU Utilization of ESX Hosts under the cluster
VMWCluster	cpuPercentReady	Average CPU percentReady of ESX Hosts under the cluster
VMWCluster	totalHz	Sum of CPU totalHz from all ESX Hosts under the cluster
VMWCluster	diskReadRate	Sum of disk bytesRead from all ESX Hosts under the cluster
VMWCluster	diskWriteRate	Sum of disk bytesWritten from all ESX Hosts under the cluster
VMWCluster	diskReadRequestsRate	Sum of disk diskReadRequestsRate from all ESX Hosts under the cluster
VMWCluster	diskWriteRequestsRate	Sum of disk diskWriteRequestsRate from all ESX Hosts under the cluster
VMWCluster	diskUsage	Sum of disk.usage.average from all ESX Hosts under the cluster
VMWCluster	memoryActive	Sum of active memory from all ESX Hosts under the cluster
VMWCluster	memoryBalloon	Sum of balloon memory from all ESX Hosts under the cluster
VMWCluster	memoryConsumed	Sum of consumed memory from all ESX Hosts under the cluster
VMWCluster	memoryGranted	Sum of granted memory from all ESX Hosts under the cluster

Table 81. Cluster metrics

VMWCluster	memoryHeap	Sum of heap memory from all ESX Hosts under the cluster
VMWCluster	memoryHeapFree	Sum of heapFree memory from all ESX Hosts under the cluster
VMWCluster	memoryOverhead	Sum of Overhead memory from all ESX Hosts under the cluster
VMWCluster	memoryReservedCapacity	Sum of ReservedCapacity memory from all ESX Hosts under the cluster
VMWCluster	memoryShared	Sum of shared memory from all ESX Hosts under the cluster
VMWCluster	memorySharedCommon	Sum of sharedCommon memory from all ESX Hosts under the cluster
VMWCluster	memoryState	Sum of state memory from all ESX Hosts under the cluster
VMWCluster	memorySwapIn	Sum of swapIn memory from all ESX Hosts under the cluster
VMWCluster	memorySwapOut	Sum of swapOut memory from all ESX Hosts under the cluster
VMWCluster	memorySwapUsed	Sum of swapUsed memory from all ESX Hosts under the cluster
VMWCluster	memoryUnreserved	Sum of unreserved memory from all ESX Hosts under the cluster
VMWCluster	memoryUtilization	Average memory utlization of the Cluster
VMWCluster	memoryZero	Sum of zero memory from all ESX Hosts under the cluster
VMWCluster	vmKernelMemory	Sum of vmKernel memory from all ESX Hosts under the cluster
VMWCluster	totalMemory	Sum of total memory from all ESX Hosts under the cluster
VMWCluster	networkPacketsSentRate	Sum of network packetsSent from all ESX Hosts under the cluster
VMWCluster	networkPacketsReceivedRate	Sum of network packetsReceived from all ESX Hosts under the cluster
VMWCluster	networkSendRate	Sum of network sendRate from all ESX Hosts under the cluster
VMWCluster	networkReceiveRate	Sum of network receiveRate from all ESX Hosts under the cluster
VMWCluster	networkUsagebps	Sum of network net.usage.average from all ESX Hosts under the cluster

Datacenter metrics

Table 82. Datacenter metrics

Topology	Metric name	Description
VMWDatacenter	avgDiskReadRate	Average disk read rate of ESX Hosts under the datacenter
VMWDatacenter	avgDiskReadRequestsRate	Average disk read request rate of ESX Hosts under the datacenter
VMWDatacenter	avgDiskWriteRate	Average disk write rate of ESX Hosts under the datacenter
VMWDatacenter	avgDiskWriteRequestsRate	Average disk write request rate of ESX Hosts under the datacenter
VMWDatacenter	avgNetworkPacketsReceivedRate	Average network packet received rate of ESX Hosts under the datacenter
VMWDatacenter	avgNetworkPacketsTransmittedRate	Average network packet transmitted rate of ESX Hosts under the datacenter
VMWDatacenter	avgNetworkReceiveRatebps	Average network received rate of ESX Hosts under the datacenter
VMWDatacenter	avgNetworkTransmitRatebps	Average network transmitted rate of ESX Hosts under the datacenter
VMWDatacenter	cpuUsedHz	Sum of CPU usedHz from all ESX Hosts under the datacenter
VMWDatacenter	cpuUtilization	Average CPU Utilization of ESX Hosts under the datacenter
VMWDatacenter	cpuPercentReady	Average CPU percentReady of ESX Hosts under the datacenter
VMWDatacenter	totalHz	Sum of CPU totalHz from all ESX Hosts under the datacenter
VMWDatacenter	diskReadRate	Sum of disk bytesRead from all ESX Hosts under the datacenter
VMWDatacenter	diskWriteRate	Sum of disk bytesWritten from all ESX Hosts under the datacenter
VMWDatacenter	diskReadRequestsRate	Sum of disk diskReadRequestsRate from all ESX Hosts under the datacenter
VMWDatacenter	diskWriteRequestsRate	Sum of disk diskWriteRequestsRate from all ESX Hosts under the datacenter
VMWDatacenter	diskUsage	Sum of disk.usage.average from all ESX Hosts under the datacenter
VMWDatacenter	memoryActive	Sum of active memory from all ESX Hosts under the datacenter
VMWDatacenter	memoryBalloon	Sum of balloon memory from all ESX Hosts under the datacenter
VMWDatacenter	memoryConsumed	Sum of consumed memory from all ESX Hosts under the datacenter
VMWDatacenter	memoryGranted	Sum of granted memory from all ESX Hosts under the datacenter
VMWDatacenter	memoryHeap	Sum of heap memory from all ESX Hosts under the datacenter
VMWDatacenter	memoryHeapFree	Sum of heapFree memory from all ESX Hosts under the datacenter

Table 82. Datacenter metrics

VMWDatacenter	memoryOverhead	Sum of Overhead memory from all ESX Hosts under the datacenter
VMWDatacenter	memoryReservedCapacity	Sum of ReservedCapacity memory from all ESX Hosts under the datacenter
VMWDatacenter	memoryShared	Sum of shared memory from all ESX Hosts under the datacenter
VMWDatacenter	memorySharedCommon	Sum of sharedCommon memory from all ESX Hosts under the datacenter
VMWDatacenter	memoryState	Sum of state memory from all ESX Hosts under the datacenter
VMWDatacenter	memorySwapIn	Sum of swapIn memory from all ESX Hosts under the datacenter
VMWDatacenter	memorySwapOut	Sum of swapOut memory from all ESX Hosts under the datacenter
VMWDatacenter	memorySwapUsed	Sum of swapUsed memory from all ESX Hosts under the datacenter
VMWDatacenter	memoryUnreserved	Sum of unreserved memory from all ESX Hosts under the datacenter
VMWDatacenter	memoryUtilization	Average memory utlization of the Cluster
VMWDatacenter	memoryZero	Sum of zero memory from all ESX Hosts under the datacenter
VMWDatacenter	vmKernelMemory	Sum of vmKernel memory from all ESX Hosts under the datacenter
VMWDatacenter	totalMemory	Sum of total memory from all ESX Hosts under the datacenter
VMWDatacenter	networkPacketsSentRate	Sum of network packetsSent from all ESX Hosts under the datacenter
VMWDatacenter	networkPacketsReceivedRate	Sum of network packetsReceived from all ESX Hosts under the datacenter
VMWDatacenter	networkSendRate	Sum of network sendRate from all ESX Hosts under the datacenter
VMWDatacenter	networkReceiveRate	Sum of network receiveRate from all ESX Hosts under the datacenter
VMWDatacenter	networkUsagebps	Sum of network net.usage.average from all ESX Hosts under the datacenter

vCenter metrics

Table 83. vCenter metric

Topology	Metric name	Description
VMWVirtualCenter	avgDiskReadRate	Average disk read rate of ESX Hosts under the vCenter
VMWVirtualCenter	avgDiskReadRequestsRate	Average disk read request rate of ESX Hosts under the vCenter
VMWVirtualCenter	avgDiskWriteRate	Average disk write rate of ESX Hosts under the vCenter

Table 83. vCenter metric

VMWVirtualCenter	avgDiskWriteRequestsRate	Average disk write request rate of ESX Hosts under the vCenter
VMWVirtualCenter	avgNetworkPacketsReceivedRate	Average network packet received rate of ESX Hosts under the vCenter
VMWVirtualCenter	avgNetworkPacketsTransmittedRate	Average network packet transmitted rate of ESX Hosts under the vCenter
VMWVirtualCenter	avgNetworkReceiveRatebps	Average network received rate of ESX Hosts under the vCenter
VMWVirtualCenter	avgNetworkTransmitRatebps	Average network transmitted rate of ESX Hosts under the vCenter
VMWVirtualCenter	cpuUsedHz	Sum of CPU usedHz from all ESX Hosts under the vCenter
VMWVirtualCenter	cpuUtilization	Average CPU Utilization of ESX Hosts under the vCenter
VMWVirtualCenter	cpuPercentReady	Average CPU percentReady of ESX Hosts under the vCenter
VMWVirtualCenter	totalHz	Sum of CPU totalHz from all ESX Hosts under the vCenter
VMWVirtualCenter	diskReadRate	Sum of disk bytesRead from all ESX Hosts under the vCenter
VMWVirtualCenter	diskWriteRate	Sum of disk bytesWritten from all ESX Hosts under the vCenter
VMWVirtualCenter	diskReadRequestsRate	Sum of disk diskReadRequestsRate from all ESX Hosts under the vCenter
VMWVirtualCenter	diskWriteRequestsRate	Sum of disk diskWriteRequestsRate from all ESX Hosts under the vCenter
VMWVirtualCenter	diskUsage	Sum of disk.usage.average from all ESX Hosts under the vCenter
VMWVirtualCenter	memoryActive	Sum of active memory from all ESX Hosts under the vCenter
VMWVirtualCenter	memoryBalloon	Sum of balloon memory from all ESX Hosts under the vCenter
VMWVirtualCenter	memoryConsumed	Sum of consumed memory from all ESX Hosts under the vCenter
VMWVirtualCenter	memoryGranted	Sum of granted memory from all ESX Hosts under the vCenter
VMWVirtualCenter	memoryHeap	Sum of heap memory from all ESX Hosts under the vCenter
VMWVirtualCenter	memoryHeapFree	Sum of heapFree memory from all ESX Hosts under the vCenter
VMWVirtualCenter	memoryOverhead	Sum of Overhead memory from all ESX Hosts under the vCenter
VMWVirtualCenter	memoryReservedCapacity	Sum of ReservedCapacity memory from all ESX Hosts under the vCenter
VMWVirtualCenter	memoryShared	Sum of shared memory from all ESX Hosts under the vCenter
VMWVirtualCenter	memorySharedCommon	Sum of sharedCommon memory from all ESX Hosts under the vCenter
VMWVirtualCenter	memoryState	Sum of state memory from all ESX Hosts under the vCenter

Table 83. vCenter metric

VMWVirtualCenter	memorySwapIn	Sum of swapIn memory from all ESX Hosts under the vCenter
VMWVirtualCenter	memorySwapOut	Sum of swapOut memory from all ESX Hosts under the vCenter
VMWVirtualCenter	memorySwapUsed	Sum of swapUsed memory from all ESX Hosts under the vCenter
VMWVirtualCenter	memoryUnreserved	Sum of unreserved memory from all ESX Hosts under the vCenter
VMWVirtualCenter	memoryUtilization	Average memory utlization of the Cluster
VMWVirtualCenter	memoryZero	Sum of zero memory from all ESX Hosts under the vCenter
VMWVirtualCenter	vmKernelMemory	Sum of vmKernel memory from all ESX Hosts under the vCenter
VMWVirtualCenter	totalMemory	Sum of total memory from all ESX Hosts under the vCenter
VMWVirtualCenter	networkPacketsSentRate	Sum of network packetsSent from all ESX Hosts under the vCenter
VMWVirtualCenter	networkPacketsReceivedRate	Sum of network packetsReceived from all ESX Hosts under the vCenter
VMWVirtualCenter	networkSendRate	Sum of network sendRate from all ESX Hosts under the vCenter
VMWVirtualCenter	networkReceiveRate	Sum of network receiveRate from all ESX Hosts under the vCenter
VMWVirtualCenter	networkUsagebps	Sum of network net.usage.average from all ESX Hosts under the vCenter

DvSwitch metrics

Table 84. DvSwitch metrics

Topology	Metric name	Description
VMWDistributedVirtualSwitch	ftTrafficUtilization	FT traffic utlization for the vSwitch
VMWDistributedVirtualSwitch	hbrTrafficUtilization	HBR traffic utlization for the vSwitch
VMWDistributedVirtualSwitch	iscsiTrafficUtilization	iSCSI traffic utlization for the vSwitch
VMWDistributedVirtualSwitch	networkPacketLoss	Percent of packet loss for the vSwitch
VMWDistributedVirtualSwitch	networkThroughput	Throughput for the vSwitch
VMWDistributedVirtualSwitch	networkUtilization	bandwidth Utilization for the vSwitch
VMWDistributedVirtualSwitch	nfsTrafficUtilization	NFS traffic utlization for the vSwitch
VMWDistributedVirtualSwitch	sumThroughput	ftusage + hbrusage + iscsiusage + nfsusage + vmotionusage + vmusage of All attached NICs
VMWDistributedVirtualSwitch	vmotionTrafficUtilization	vMotion traffic utlization for the vSwitch
VMWDistributedVirtualSwitch	vmTrafficUtilization	VMs traffic utlization for the vSwitch

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation™.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece—you—to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit https://www.quest.com/company/contact-us.aspx or call +1-949-754-8000.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request.
- View Knowledge Base articles.
- Sign up for product notifications.
- Download software and technical documentation.
- View how-to-videos.
- Engage in community discussions.
- Chat with support engineers online.
- View services to assist you with your product.