vSphere Monitoring and Performance

Update 1
vSphere 5.0
vCenter Server 5.0
ESXi 5.0

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-000800-00

vmware®

You can find the most up-to-date technical documentation on the VMware Web site at:

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About vSphere Monitoring and Performance

VMware provides several tools to help you monitor your virtual environment and to locate the source of potential issues and current problems.

Performance charts in the vSphere Web Client and the vSphere Client	Allow you to see performance data on a variety of system resources including CPU, Memory, Storage, and so on.
Performance monitoring command-line utilities	Allow you to access detailed information on system performance through the command line.
Host health	Allows you to quickly identify which hosts are healthy and which are experiencing problems.
Storage maps and charts	Provide an in-depth look at your storage resources.
Events, alerts, and alarms in the vSphere Web Client and the vSphere Client	Allow you configure alerts and alarms and to specify the actions the system should take when they are triggered.

Intended Audience

The content in this section is intended for vSphere administrators who are perform the following tasks:

- Monitor the health and performance of physical hardware backings for the virtual environment.
- Monitor the health and performance of virtual devices in the virtual environment.
- Troubleshoot problems in the system.
- Configure alarms.
- Configure SNMP messages.

Virtual machine administrators also might find the section on Chapter 2, “Monitoring Guest Operating System Performance,” on page 23 helpful.

Monitoring Inventory Objects with Performance Charts 1

The vSphere statistics subsystem collects data on the resource usage of inventory objects. Data on a wide range of metrics is collected at frequent intervals, processed, and archived in the vCenter Server database. You can access statistical information through command-line monitoring utilities or by viewing performance charts in the vSphere Client and the vSphere Web Client. Your client must be connected to a vCenter Server to view charts.

Counters and Metric Groups

vCenter Server systems and hosts use data counters to query for statistics. A data counter is a unit of information relevant to a given inventory object or device. Each counter collects data for a different statistic in a metric group. For example, the disk metric group includes separate data counters to collect data for disk read rate, disk write rate, and disk usage. Statistics for each counter are rolled up after a specified collection interval and are displayed in a performance chart. Each data counter consists of several attributes that are used to determine the statistical value collected.

For a complete list and description of performance metrics, see the *vSphere API Reference*.

Note Data for hosts with versions of ESXi prior to 5.0 is not included in results collected by counters that are introduced in ESXi 5.0. See the VMware Knowledge Base for details.

Collection Levels and Collection Intervals

Collection levels determine the number of counters for which data is gathered during each collection interval. Collection intervals determine the time period during which statistics are aggregated, calculated, rolled up, and archived in the vCenter Server database. Together, the collection interval and collection level determine how much statistical data is collected and stored in your vCenter Server database .

Data Availability

Real-time data appears in the performance charts only for hosts and virtual machines that are powered on. Historical data appears for all supported inventory objects, but might be unavailable during certain circumstances.

This chapter includes the following topics:

Performance Chart Types

Performance metrics are displayed in different types of charts, depending on the metric type and object.

Table 1-1. Performance Chart Types

Chart Type	Description
Line chart	Displays metrics for a single inventory object. The data for each performance counter is plotted on a separate line in the chart. For example, a network chart for a host can contain two lines: one showing the number of packets received, and one showing the number of packets transmitted.
Bar chart	Displays storage metrics for datastores in a selected datacenter. Each datastore is represented as a bar in the chart. Each bar displays metrics based on the file type: virtual disks, snapshots, swap files, and other files.
Pie chart	Displays storage metrics for a single object, based on the file types or virtual machines. For example, a pie chart for a datastore can display the amount of storage space occupied by the virtual machines taking up the largest space.
Stacked chart	Displays metrics for the child objects that have the highest statistical values. All other objects are aggregated, and the sum value is displayed with the term **Other**. For example, a host's stacked CPU usage chart displays CPU usage metrics for the five virtual machines on the host that are consuming the most CPU. The **Other** amount contains the total CPU usage of the remaining virtual machines. The metrics for the host itself are displayed in separate line charts. Stacked charts are useful in comparing resource allocation and usage across multiple hosts or virtual machines. By default, the five child objects with the highest data counter values are displayed.

Data Counters

Each data counter includes several attributes that are used to determine the statistical value collected. See the *vSphere API Reference* for a complete list and description of supported counters.

Table 1-2. Data Counter Attributes

Attribute	Description
Unit of Measurement	Standard in which the statistic quantity is measured. ■ Kilobytes (KB) – 1024 bytes ■ Kilobytes per second (KBps) – 1024 bytes per second ■ Kilobits (kb) – 1000 bits ■ Kilobits per second (kbps) – 1000 bits per second ■ Megabytes (MB) ■ megabytes per second (MBps) ■ megabits (Mb), megabits per second (Mbps) ■ megahertz (MHz) ■ microseconds (µs) ■ milliseconds (ms) ■ number (#) ■ percent (%) ■ seconds (s)
Description	Text description of the data counter.

Table 1-2. Data Counter Attributes (Continued)

Attribute	Description
Statistics Type	Measurement used during the statistics interval. Related to the unit of measurement. ■ Rate – Value over the current statistics interval ■ Delta – Change from previous statistics interval. ■ Absolute – Absolute value (independent of the statistics interval).
Rollup Type	Calculation method used during the statistics interval to roll up data. Determines the type of statistical values that are returned for the counter. ■ Average – Data collected during the interval is aggregated and averaged. ■ Minimum – The minimum value is rolled up. ■ Maximum – The maximum value is rolled up. The Minimum and Maximum values are collected and displayed only in statistics level 4. Minimum and maximum rollup types are used to capture peaks in data during the interval. For real-time data, the value is the current minimum or current maximum. For historical data, the value is the average minimum or average maximum. For example, the following information for the CPU usage chart shows that the average is collected at statistics level 1 and the minimum and maximum values are collected at statistics level 4. ■ Counter: usage ■ Unit: Percentage (%) ■ Rollup Type: Average (Minimum/Maximum) ■ Collection Level: 1 (4) ■ Summation – Data collected is summed. The measurement displayed in the chart represents the sum of data collected during the interval. ■ Latest – Data collected during the interval is a set value. The value displayed in the performance charts represents the current value.
Collection level	Number of data counters used to collect statistics. Collection levels range from 1 to 4, with 4 having the most counters.

Metric Groups

The performance data collection subsystem for vSphere collects performance data on a variety of inventory items and their devices. Data counters define individual performance metrics. Performance metrics are organized into logical groups based on the object or object device. Statistics for one or more metrics can be displayed in a chart.

Table 1-3. Metric Groups

Metric group	Description
Cluster Services	Performance statistics for clusters configured by using VMware DRS (distributed resource scheduler), VMware HA (high availability), or both.
CPU	CPU utilization per host, virtual machine, resource pool, or compute resource.
Storage Pods and Datastores	Statistics for datastore utilization
Disk	Disk utilization per host, virtual machine, or datastore. Disk metrics include I/O performance (such as latency and read/write speeds), and utilization metrics for storage as a finite resource.
Management Agent	Memory swap statistics per COS.

Table 1-3. Metric Groups (Continued)

Metric group	Description
Memory	Memory utilization per host, virtual machine, resource pool, or compute resource. The value obtained is one of the following: ■ For virtual machines, memory refers to guest physical memory. Guest physical memory is the amount of physical memory presented as a virtual-hardware component to the virtual machine, at creation time, and made available when the virtual machine is running. ■ For hosts, memory refers to machine memory. Machine memory is the RAM that is installed in the hardware that comprises the host system.
Network	Network utilization for both physical and virtual network interface controllers (NICs) and other network devices, such as the virtual switches (vSwitch) that support connectivity among all components (hosts, virtual machines, VMkernel, and so on).
Power	Energy usage statistics per host.
Storage Adapter	Data traffic statistics per HBA.
Storage Path	Data traffic statistics per path.
System	Overall system availability, such as system heartbeat and uptime. These counters are available directly from hosts and from vCenter Server.
Virtual Machine Operations	Virtual machine power and provisioning operations in a cluster or datacenter.

Data Collection Intervals

Collection intervals determine the duration for which statistics are aggregated, calculated, rolled up, and archived. Together, the collection interval and collection level determine how much statistical data is gathered and stored in your vCenter Server database.

Table 1-4. Collection Intervals

Collection Interval/Archive Length	Collection Frequency	Default Behavior
1 Day	5 Minutes	Real-time statistics are rolled up to create one data point every 5 minutes. The result is 12 data points every hour and 288 data points every day. After 30 minutes, the six data points collected are aggregated and rolled up as a data point for the 1 Week time range. You can change the interval duration and archive length of the 1 Day collection interval by configuring the statistics settings.
1 Week	30 Minutes	1 Day statistics are rolled up to create one data point every 30 minutes. The result is 48 data points every day and 336 data points every week. Every 2 hours, the 12 data points collected are aggregated and rolled up as a data point for the 1 Month time range. You cannot change the default settings of the 1 Week collection interval.
1 Month	2 Hours	1 Week statistics are rolled up to create one data point every 2 hours. The result is 12 data points every day and 360 data points every month (assuming a 30-day month). After 24 hours, the 12 data points collected are aggregated and rolled up as a data point for the **1 Year** time range. You cannot change the default settings of the 1 Month collection interval.
1 Year	1 Day	1 Month statistics are rolled up to create one data point every day. The result is 365 data points each year. You can change the interval duration and archive length of the 1 Year collection interval by configuring the statistics settings.

Data Collection Levels

Each collection interval has a default collection level that determines the amount of data gathered and which counters are available for display in charts. Collection levels are also refered to as statistics levels.

Table 1-5. Statistics Levels

Level	Metrics	Best Practice
Level 1	■ Cluster Services (VMware Distributed Resource Scheduler) – all metrics ■ CPU – cpuentitlement, totalmhz, usage (average), usagemhz ■ Disk – capacity, maxTotalLatency, provisioned, unshared, usage (average), used ■ Memory – consumed, mementitlement, overhead, swapinRate, swapoutRate, swapused, totalmb, usage (average), vmmemctl (balloon) ■ Network – usage (average) ■ System – heartbeat, uptime ■ Virtual Machine Operations – numChangeDS, numChangeHost, numChangeHostDS	Use for long-term performance monitoring when device statistics are not required. Level 1 is the default Collection Level for all Collection Intervals.
Level 2	■ Level 1 metrics ■ CPU – idle, reservedCapacity ■ Disk – All metrics, excluding numberRead and numberWrite. ■ Memory – All metrics, excluding memUsed and maximum and minimum rollup values. ■ Virtual Machine Operations – All metrics	Use for long-term performance monitoring when device statistics are not required but you want to monitor more than the basic statistics.
Level 3	■ Level 1 and Level 2 metrics ■ Metrics for all counters, excluding minimum and maximum rollup values. ■ Device metrics	Use for short-term performance monitoring after encountering problems or when device statistics are required. Because of the large quantity of troubleshooting data retrieved and recorded, use level 3 for the shortest time period (Day or Week collection interval).
Level 4	All metrics supported by the vCenter Server, including minimum and maximum rollup values.	Use for short-term performance monitoring after encountering problems or when device statistics are required. Because of the large quantity of troubleshooting data retrieved and recorded, use level 4 for the shortest amount of time.

View Charts

The vCenter Server statistics settings, the type of object selected, and the features that are enabled on the selected object determine the amount of information displayed in charts. Charts are organized into views. You can select a view to see related data together on one screen. You can also specify the time range, or data collection interval. The duration extends from the selected time range to the present time.

Prerequisites

You must have a vSphere Web Client or a vSphere Client connected to a vCenter Server.

Procedure

1 Select an inventory object.

2 Navigate to the performance charts for your client.

Option	Description
vSphere Client	Select the **Performance** tab > **Overview** or **Advanced** subtab. Overview charts display multiple data sets in one panel to easily evaluate different resource statistics, display thumbnail charts for child objects, and display charts for a parent and a child object. Advanced charts display more information than overview charts, are configurable, and can be printed or exported to a spreadsheet file.
vSphere Web Client	Select the **Monitor** tab > **Performance** subtab. Advanced charts are available only in the vSphere Client.

3 Select a view.

4 Specify a time range.

Performance Charts View Menu Options

Options under the View menu for performance charts vary depending upon the object selected and the properties of the object.

For example, the **Virtual Machines** view is available when you view host performance charts only if there are virtual machines on the selected host. Likewise, the **Fault Tolerance** view for virtual machine performance charts is available only when that feature is enabled for the selected virtual machine.

Table 1-6. Performance Chart Views by Inventory Object

Object	View list items	
Datacenter	**Clusters**	Thumbnail CPU and memory charts for each cluster, and stacked charts for total CPU and memory usage in the datacenter. This view is the default.
	Storage	Space utilization charts for datastores in the datacenter, including space by file type and storage space used by each datastore in the datacenter.
Datastore/Data store Cluster	**Space**	Space utilization charts for the datastore: space by file type, space by virtual machine, and space usage.
	Performance	Performance charts for the datastore/datastore cluster and for virtual machine disks on the resource.
	NOTE: The Performance view for datastores is only available when all hosts that are connected to the datastores are ESX/ESXi 4.1 or greater. The Performance view for datastore clusters is only available when the Storage DRS is enabled.	
Cluster	**Home**	CPU and memory charts for the cluster.
	Resource Pools & Virtual Machines	Thumbnail charts for resource pools and virtual machines, and stacked charts for total CPU and memory usage in the cluster.
	Hosts	Thumbnail charts for each host in the cluster, and stacked charts for total CPU, memory, disk usage, and network usage.
Host	**Home**	CPU, memory, disk, and network charts for the host.
	Virtual Machines	Thumbnail charts for virtual machines, and stacked charts for total CPU usage and total memory usage on the host.

Table 1-6. Performance Chart Views by Inventory Object (Continued)

Object	View list items	
Resource Pool/vApps	**Home**	CPU and memory charts for the resource pool.
	Resource Pools & Virtual Machines	Thumbnail charts for resource pools, and virtual machines and stacked charts for CPU and memory usage in the resource pool or vApp.
Virtual Machine	**Home**	CPU, memory, network, host (thumbnail charts), and disk usage charts for the virtual machine.
	Storage	Space utilization charts for the virtual machine: space by file type, space by datastore, and total gigabytes.
	Fault Tolerance	CPU and memory charts that display comparative metrics for the fault-tolerant primary and secondary virtual machines.

Create Custom Charts

Use advanced charts, or create your own custom charts, to see more performance data. Advanced charts can be useful when you are aware of a problem but need more statistical data to pinpoint the source of the trouble.

Advanced charts include the following features:

- More information. Hover over a data point in a chart and details about that specific data point are displayed.
- Customizable charts. Change chart settings. Save custom settings to create your own charts.
- Export to spreadsheet.
- Save to image file or spreadsheet.

View Advanced Performance Charts

Advanced charts support data counters that are not supported in other performance charts.

When connected directly to a host, the advanced performance charts display only real-time statistics and past day statistics.

Prerequisites

You must have a vSphere Client connected to a vCenter Server.

Procedure

1 Select an inventory object.

2 Click the **Performance** tab.

3 Click **Advanced**.

4 (Optional) To view a different chart, select an option from the **Switch to** list.

The amount of historical data displayed in a chart depends on the collection interval and statistics level set for vCenter Server.

5 (Optional) To view the chart in its own window, click the pop-up chart button. You can view additional charts while keeping this chart open.

Set Advanced Performance Charts as the Default

You can configure the vSphere Client to display the advanced performance charts by default when you open the **Performance** tab. The default is to display the overview performance charts.

Prerequisites

You must have a vSphere Client connected to a vCenter Server.

Procedure

1 Select **Edit > Client Settings**.

2 In the **Tabs** section of the Client Settings dialog box, select **Default to Advanced Performance Charts**.

3 Click **OK**.

Change Advanced Chart Settings

You can customize a performance chart by specifying the objects to monitor, the counters to include, the time range, and chart type. You can customize preconfigured chart views and create new chart views.

Prerequisites

You must have a vSphere Client connected to a vCenter Server.

Procedure

1 Select an inventory object and click the **Performance** tab.

2 Click **Advanced**.

3 Click **Chart Options**.

4 Select a metric group for the chart.

5 Select a time range for the metric group.

If you choose **Custom**, do one of the following.

- Select **Last** and set the number of hours, days, weeks, or months for the amount of time to monitor the object.
- Select **From** and select the beginning and end dates.

You can also customize the time range options by customizing the statistics collection interval setting.

6 Select the chart type.

When selecting the stacked graph option, consider the following.

- You can select only one item from the list of measurements.
- Per-virtual-machine stacked graphs are available only for hosts.
- Click a counter description name to display information about the counter's function and whether the selected metric can be stacked for per-virtual-machine graphs.

7 In Objects, select the inventory objects to display in the chart.

You can also specify the objects using the **All** or **None** buttons.

8 In Counters, select the data counters to display in the chart.

You can also specify counters using the **All** or **None** buttons.

Click a counter name to display information about the counter in the Counter Description panel.

9 Click **Apply**.

Changes to chart settings take effect immediately after they are applied.

10 Click **OK**.

Create a Custom Advanced Chart

You can create your own charts by saving customized chart settings. New charts are added to the **Switch to** menu and will appear there only when charts for the selected object are being displayed.

Prerequisites

You must have a vSphere Client connected to a vCenter Server.

Procedure

1 Customize chart settings as described in "Change Advanced Chart Settings," on page 14

2 Click **Save Chart Settings**.

3 Enter a name for your settings.

4 Click **OK**.

The chart settings are saved and an entry for your chart is added to the **Switch to** menu.

Delete a Custom Advanced Chart View

You can delete custom chart views from the vSphere Client.

Prerequisites

You must have a vSphere Client connected to a vCenter Server.

Procedure

1 Select any object in the datacenter to enable the **Performance** tab.

2 Click the **Performance** tab and click **Advanced**.

3 Click **Chart Options**.

4 Click **Manage Chart Settings**.

5 Select a chart and click **Delete**.

The chart is deleted, and it is removed from the **Switch to** menu.

6 Click **OK**.

Save Chart Data to a File

You can save data from the Advanced performance charts to a file in various graphics formats or in Microsoft Excel format.

Prerequisites

You must have a vSphere Client connected to a vCenter Server.

Procedure

1 In the **Performance** tab, click **Advanced**.

2 Click **Save**.

3 In the Save Performance Chart dialog box, navigate to the location to save the file.

4 Enter a name for the file.

5 Select a file type.

6 Click **Save**.

The file is saved to the location and format you specified.

Export Performance Data to a Spreadsheet

You can export performance data from the Advanced charts to a Microsoft Office Excel file.

Prerequisites

You must have a vSphere Client connected to a vCenter Server.

Procedure

1 Select the object in the inventory.

2 Select **File > Report > Performance**.

If performance data is not available for the selected inventory object, the Export Performance option is not available.

3 Enter a filename and location.

4 Select the date and time range for the chart.

5 In **Chart Options**, select the chart type.

6 Select the metric groups to display in the chart.

You can also specify the objects by selecting **All** or **None**.

7 (Optional) To customize the options, click **Advanced**, select the objects and counters to include in the chart, and click **OK**.

8 Specify the size of the chart in the exported file.

9 Click **OK** to export the data.

Troubleshoot and Enhance Performance

This section presents tips for identifying and solving performance problems.

The suggestions in this section are not meant to be a comprehensive guide to diagnosing and troubleshooting problems in the virtual environment. It is meant to provide information about some common problems that can be solved without contacting VMware Technical Support.

Solutions for Consistently High CPU Usage

Temporary spikes in CPU usage indicate that you are making the best use of CPU resources. Consistently high CPU usage might indicate a problem. You can use the vSphere Client CPU performance charts to monitor CPU usage for hosts, clusters, resource pools, virtual machines, and vApps.

Problem

- Host CPU usage constantly is high. A high CPU usage value can lead to increased ready time and processor queuing of the virtual machines on the host.
- Virtual machine CPU usage is above 90% and the CPU ready value is above 20%. Application performance is impacted.

Cause

The host probably is lacking the CPU resources required to meet the demand.

Solution

- Verify that VMware Tools is installed on every virtual machine on the host.
- Compare the CPU usage value of a virtual machine with the CPU usage of other virtual machines on the host or in the resource pool. The stacked bar chart on the host's **Virtual Machine** view shows the CPU usage for all virtual machines on the host.
- Determine whether the high ready time for the virtual machine resulted from its CPU usage time reaching the CPU limit setting. If so, increase the CPU limit on the virtual machine.
- Increase the CPU shares to give the virtual machine more opportunities to run. The total ready time on the host might remain at the same level if the host system is constrained by CPU. If the host ready time doesn't decrease, set the CPU reservations for high-priority virtual machines to guarantee that they receive the required CPU cycles.
- Increase the amount of memory allocated to the virtual machine. This action decreases disk and or network activity for applications that cache. This might lower disk I/O and reduce the need for the host to virtualize the hardware. Virtual machines with smaller resource allocations generally accumulate more CPU ready time.
- Reduce the number of virtual CPUs on a virtual machine to only the number required to execute the workload. For example, a single-threaded application on a four-way virtual machine only benefits from a single vCPU. But the hypervisor's maintenance of the three idle vCPUs takes CPU cycles that could be used for other work.
- If the host is not already in a DRS cluster, add it to one. If the host is in a DRS cluster, increase the number of hosts and migrate one or more virtual machines onto the new host.
- Upgrade the physical CPUs or cores on the host if necessary.
- Use the newest version of hypervisor software, and enable CPU-saving features such as TCP Segmentation Offload, large memory pages, and jumbo frames.

Solutions for Memory Performance Problems

Host machine memory is the hardware backing for guest virtual memory and guest physical memory. Host machine memory must be at least slightly larger than the combined active memory of the virtual machines on the host. A virtual machine's memory size must be slightly larger than the average guest memory usage. Increasing the virtual machine memory size results in more overhead memory usage.

Problem

- Memory usage is constantly high (94% or greater) or constantly low (24% or less).
- Free memory consistently is 6% or less and swapping frequently occurs.

Cause

- The host probably is lacking the memory required to meet the demand. The active memory size is the same as the granted memory size, which results in memory resources that are not sufficient for the workload. Granted memory is too much if the active memory is constantly low.
- Host machine memory resources are not enough to meet the demand, which leads to memory reclamation and degraded performance.
- The active memory size is the same as the granted memory size, which results in memory resources that are not sufficient for the workload.

Solution

- Verify that VMware Tools is installed on each virtual machine. The balloon driver is installed with VMware Tools and is critical to performance.
- Verify that the balloon driver is enabled. The VMkernel regularly reclaims unused virtual machine memory by ballooning and swapping. Generally, this does not impact virtual machine performance.
- Reduce the memory space on the virtual machine, and correct the cache size if it is too large. This frees up memory for other virtual machines.
- If the memory reservation of the virtual machine is set to a value much higher than its active memory, decrease the reservation setting so that the VMkernel can reclaim the idle memory for other virtual machines on the host.
- Migrate one or more virtual machines to a host in a DRS cluster.
- Add physical memory to the host.

Solutions for Storage Performance Problems

Datastores represent storage locations for virtual machine files. A storage location can be a VMFS volume, a directory on Network Attached Storage, or a local file system path. Datastores are platform-independent and host-independent.

Problem

- Snapshot files are consuming a lot of datastore space.
- The datastore is at full capacity when the used space is equal to the capacity. Allocated space can be larger than datastore capacity, for example, when you have snapshots and thin-provisioned disks.

Solution

- Consider consolidating snapshots to the virtual disk when they are no longer needed. Consolidating the snapshots deletes the redo log files and removes the snapshots from the vSphere Client user interface.
- You can provision more space to the datastore if possible, or you can add disks to the datastore or use shared datastores.

Solutions for Disk Performance Problems

Use the disk charts to monitor average disk loads and to determine trends in disk usage. For example, you might notice a performance degradation with applications that frequently read from and write to the hard disk. If you see a spike in the number of disk read/write requests, check if any such applications were running at that time.

Problem

- The value for the kernelLatency data counter is greater than 4ms.
- The value for the deviceLatency data counter is greater than 15ms indicates there are probably problems with the storage array.
- The queueLatency data counter measures above zero.
- Spikes in latency.
- Unusual increases in read/write requests.

Cause

- The virtual machines on the host are trying to send more throughput to the storage system than the configuration supports.

- The storage array probably is experiencing internal problems.
- The workload is too high and the array cannot process the data fast enough.

Solution

- The virtual machines on the host are trying to send more throughput to the storage system than the configuration supports. Check the CPU usage, and increase the queue depth.
- Move the active VMDK to a volume with more spindles or add disks to the LUN.
- Increase the virtual machine memory. This should allow for more operating system caching, which can reduce I/O activity. Note that this may require you to also increase the host memory. Increasing memory might reduce the need to store data because databases can utilize system memory to cache data and avoid disk access.
- Check swap statistics in the guest operating system to verify that virtual machines have adequate memory. Increase the guest memory, but not to an extent that leads to excessive host memory swapping. Install VMware Tools so that memory ballooning can occur.
- Defragment the file systems on all guests.
- Disable antivirus on-demand scans on the VMDK and VMEM files.
- Use the vendor's array tools to determine the array performance statistics. When too many servers simultaneously access common elements on an array, the disks might have trouble keeping up. Consider array-side improvements to increase throughput.
- Use Storage VMotion to migrate I/O-intensive virtual machines across multiple hosts.
- Balance the disk load across all physical resources available. Spread heavily used storage across LUNs that are accessed by different adapters. Use separate queues for each adapter to improve disk efficiency.
- Configure the HBAs and RAID controllers for optimal use. Verify that the queue depths and cache settings on the RAID controllers are adequate. If not, increase the number of outstanding disk requests for the virtual machine by adjusting the `Disk.SchedNumReqOutstanding` parameter.
- For resource-intensive virtual machines, separate the virtual machine's physical disk drive from the drive with the system page file. This alleviates disk spindle contention during periods of high use.
- On systems with sizable RAM, disable memory trimming by adding the line `MemTrimRate=0` to the virtual machine's .VMX file.
- If the combined disk I/O is higher than a single HBA capacity, use multipathing or multiple links.
- For ESXi hosts, create virtual disks as preallocated. When you create a virtual disk for a guest operating system, select **Allocate all disk space now**. The performance degradation associated with reassigning additional disk space does not occur, and the disk is less likely to become fragmented.
- Use the most current hypervisor software.

Solutions for Poor Network Performance

Network performance is dependent on application workload and network configuration. Dropped network packets indicate a bottleneck in the network. Slow network performance can be a sign of load-balancing problems.

Problem

Network problems can manifest in many ways:

- Packets are being dropped.
- Network latency is high.
- Data receive rate is low.

Cause

Network problems can have several causes:

- Virtual machine network resource shares are too few.
- Network packet size is too large, which results in high network latency. Use the VMware AppSpeed performance monitoring application or a third-party application to check network latency.
- Network packet size is too small, which increases the demand for the CPU resources needed for processing each packet. Host CPU, or possibly virtual machine CPU, resources are not enough to handle the load.

Solution

- Determine whether packets are being dropped by using `esxtop` or the advanced performance charts to examine the `droppedTx` and `droppedRx` network counter values. Verify that VMware Tools is installed on each virtual machine.
- Check the number of virtual machines assigned to each physical NIC. If necessary, perform load balancing by moving virtual machines to different vSwitches or by adding more NICs to the host. You can also move virtual machines to another host or increase the host CPU or virtual machine CPU.
- If possible, use vmxnet3 NIC drivers, which are available with VMware Tools. They are optimized for high performance.
- If virtual machines running on the same host communicate with each other, connect them to the same vSwitch to avoid the cost of transferring packets over the physical network.
- Assign each physical NIC to a port group and a vSwitch.
- Use separate physical NICs to handle the different traffic streams, such as network packets generated by virtual machines, iSCSI protocols, VMotion tasks.
- Ensure that the physical NIC capacity is large enough to handle the network traffic on that vSwitch. If the capacity is not enough, consider using a high-bandwidth physical NIC (10Gbps) or moving some virtual machines to a vSwitch with a lighter load or to a new vSwitch.
- If packets are being dropped at the vSwitch port, increase the virtual network driver ring buffers where applicable.
- Verify that the reported speed and duplex settings for the physical NIC match the hardware expectations and that the hardware is configured to run at its maximum capability. For example, verify that NICs with 1Gbps are not reset to 100Mbps because they are connected to an older switch.
- Verify that all NICs are running in full duplex mode. Hardware connectivity issues might result in a NIC resetting itself to a lower speed or half duplex mode.
- Use vNICs that are TSO-capable, and verify that TSO-Jumbo Frames are enabled where possible.

Why are my charts empty?

The following table lists the scenarios in which performance charts are empty with the label "No data available." Each scenario assumes that the default rollup configuration for the vCenter Server system has not changed. Metrics introduced in ESXi 5.0 are not available for hosts running earlier versions; "No data available" will be displayed when users attempt to view new metrics on older hosts.

Table 1-7. Scenarios for Unavailable Performance Data

Chart Time Range	Behavior
Real time	Real-time statistics are not available for disconnected hosts or powered off virtual machines. The charts are empty with the label "No data available."
1 day	The real-time statistics are collected on hosts and aggregated every 5 minutes. After six data points are collected (30 minutes), they are rolled up to the vCenter Server database to create the 1 Day statistics. 1 Day statistics might not be available for 30 minutes after the current time, depending on when the sample period began. The charts are empty with the label "No data available."
1 week	The 1 Day statistics are rolled up to create one data point every 30 minutes. If there is a lag in the rollup operation, the 1 Week statistics might not be available for 1 hour after the current time (30 minutes for the 1 Week collection interval + 30 minutes for the 1 Day collection interval). The charts are empty with the label "No data available."
1 month	The 1 Week statistics are rolled up to create one data point every 2 hours. If there is a lag in the rollup operations, the 1 Month statistics might not be available for 3 hours (2 hours for the 1 Month collection interval + 1 hour for the 1 Week collection interval). The charts are empty with the label "No data available."
1 year	The 1 Month statistics are rolled up to create one data point every day. If there is a lag in the rollup operations, the statistics might not be available for 1 day and 3 hours (1 day for the past year collection interval + 3 hours for the past month collection interval). During this time, the charts are empty with the label "No data available."

Monitoring Guest Operating System Performance 2

This section describes how to install and view VMware-specific performance data for virtual machines that run Microsoft Windows operating systems. VMware provides performance counters that enable you to view data on many aspects of guest operating system performance for the Microsoft Windows Perfmon utility.

Some virtualization processes dynamically allocate available resources depending on the status, or utilization rates, of virtual machines in the environment. This can make obtaining accurate information about the resource utilization (CPU utilization, in particular) of individual virtual machines, or applications running within virtual machines, difficult. VMware now provides virtual machine-specific performance counter libraries for the Windows Perfmon utility that enable application administrators to access accurate virtual machine resource utilization statistics from within the Windows Perfmon utility.

This chapter includes the following topics:

Enable Statistics Collection for Guest Operating System Performance Analysis

VMware-specific performance objects are loaded into Microsoft Windows Perfmon and enabled when VMware Tools is installed.

To display a performance chart for any performance object, you must add counters. See "View Performance Statistics for Windows Guest Operating Systems," on page 23

View Performance Statistics for Windows Guest Operating Systems

You can display VMware specific statistics in the Microsoft Windows Perfmon utility.

Prerequisites

Verify that a virtual machine with a Microsoft Windows operating system and VMware Tools is installed.

Procedure

1 Open a console to the virtual machine and log in.

2 Select **Start > Run**.

3 Enter **Perfmon** and press **Enter**.

4 In the Performance dialog box, click **Add** .

5 In the Add Counters dialog box, select **Use local computer counters**.

6 Select a virtual machine performance object.

   Virtual machine performance object names begin with **VM**.

7 Select the counters that you want to display for that object.

8 If the performance object has multiple instances, select the instances you want to display.

9 Click **Add**.

   The Performance dialog box displays data for the selected performance object.

10 Click **Close** to close the Add Counter dialog box and return to the Performance dialog box.

Monitoring Host Health Status 3

You can use the vSphere Client to monitor the state of host hardware components, such as CPU processors, memory, fans, and other components.

The host health monitoring tool allows you to monitor the health of a variety of host hardware components including:

- CPU processors
- Memory
- Fans
- Temperature
- Voltage
- Power
- Network
- Battery
- Storage
- Cable/Interconnect
- Software components
- Watchdog
- Other

The host health monitoring tool presents data gathered using Systems Management Architecture for Server Hardware (SMASH) profiles. The information displayed depends on the sensors available on your server hardware. SMASH is an industry standard specification providing protocols for managing a variety of systems in the datacenter. For more information, see http://www.dmtf.org/standards/smash.

You can monitor a host's health status either by connecting the vSphere Client directly to a host, or by connecting to a vCenter Server system. You can also set alarms to trigger when the host health status changes.

This chapter includes the following topics:

Monitor Health Status When Directly Connected to a Host

When you connect the vSphere Client directly to a host, you can view the health status from the host's **Configuration** tab.

When you are connected to a host through vCenter Server, you must use the **Hardware Status** tab to monitor the host health.

Procedure

1 Log in to the host using the vSphere Client, and display the inventory.

2 Click the **Configuration** tab, and click **Health Status**.

If a component is functioning normally, the status indicator is green. The status indicator changes to yellow or red if a system component violates a performance threshold or is not functioning properly. Generally, a yellow indicator signifies degraded performance. A red indicator signifies that a component stopped operating or exceeded the highest threshold. If the status is blank, then the health monitoring service cannot determine the status of the component.

The **Reading** column displays the current values for the sensors. For instance, the column displays rotations per minute (RPM) for fans and degrees Celsius for temperature.

Monitor Health Status When Connected to vCenter Server

When you connect the vSphere Client to vCenter Server, you can view the health status from the **Hardware Status** tab.

When you are connected to a host through vCenter Server, you must use the **Hardware Status** tab to monitor the host health.

Prerequisites

Ensure that the vCenter Hardware Status plug-in is enabled.

Procedure

1 Log in to a vCenter Server system using the vSphere Client.

2 Select the host in the inventory and click the **Hardware Status** tab.

3 From the **View** drop-down menu, select the type of information to view.

Option	Description
Sensors	Displays all sensors arranged in a tree view. If the status is blank, the health monitoring service cannot determine the status of the component. ■ Click **Show all sensors** to expand the tree view to show all sensors under each group. ■ Click **Show all details** to expand the tree view to show descriptive details for every sensor. ■ Click **Hide all** to collapse the tree view to show only the sensor groups.
Alerts and warnings	Displays only alerts and warnings.
System event log	Displays the system event log. Click **Reset event log** to clear the event log. CAUTION Resetting the event log clears all log data. Download a support bundle or export the log data before resetting the log if you need to preserve existing log information for troubleshooting.

Reset Hardware Sensors When Directly Connected to a Host

Some host hardware sensors display data that is cumulative over time. You can reset these sensors to clear the data in them and begin collecting new data.

Prerequisites

If you need to preserve sensor data for troubleshooting or other purposes, take a screenshot, export the data, or download a support bundle before resetting sensors.

Procedure

1 On the host **Configuration** tab, click **Health Status**.

2 Click **Reset Sensors**.

Reset Health Status Sensors When Connected to vCenter Server

Some host hardware sensors display data that is cumulative over time. You can reset these sensors to clear the data in them and begin collecting new data.

If you need to preserve sensor data for troubleshooting or other purposes, take a screenshot, export the data, or download a support bundle before resetting sensors.

Prerequisites

Ensure that the vCenter Hardware Status plug-in is enabled.

Procedure

1 Log in to a vCenter Server system using the vSphere Client, and display the **Hosts and Clusters** view in the inventory.

2 Select the host in the inventory and click the **Hardware Status** tab.

3 Click **Reset sensors**.

Troubleshoot the Hardware Health Service

The Hardware Health service is a vCenter Server extension that uses an Internet Explorer Web browser control to display information about host hardware health. Use the information in this topic to troubleshoot problems with Hardware Health.

Procedure

- Take the appropriate action based on the observed problem.

Problem	Action
The Hardware Status tab is not visible in the vSphere Client.	Select **Plug-ins > Plug-in Manager** and verify that the Hardware Status plug-in is enabled.
The Hardware Status tab displays the following error message: `the remote name could not be resolved` *`SERVER_NAME`* where *`SERVER_NAME`* is the domain name of the vCenter Server system.	This error appears when the client system is unable to resolve the domain name of the vCenter Server system. Either fix the domain name resolution problem, or edit the file `C:\Program Files\VMware\Infrastructure\VirtualCenter Server\extensions\cim-ui\extensions.xml` on the vCenter Server system and replace the vCenter Server domain name with its IP address.
The Hardware Status tab displays a security alert.	Your Internet Explorer security settings are set too high. To change the security settings: a Launch Internet Explorer. b Select **Tools > Internet Options**. c Click the **Security** tab. d Select the **Local intranet** Web content zone. e Click **Custom Level**. f Underneath **Allow scripting of Internet Explorer Web browser control**, select **Enable**. g Click **OK** to close the Security Settings dialog box, and click **OK** to close the Internet Options dialog box.

Monitoring Storage Resources 4

If you use vCenter Server to manage your hosts, you can review information on storage usage and visually map relationships between all storage entities that are available in vCenter Server.

In the vSphere Client, for any inventory object except networking, the storage usage data appears in the **Storage Views** tab. To view this tab, you must have the vCenter Storage Monitoring plug-in, which is generally installed and enabled by default.

You can display storage information as reports or storage topology maps.

Reports Reports display relationship tables that provide insight about how an inventory object is associated with storage entities. They also offer summarized storage usage data for the object's virtual and physical storage resources. Use the **Reports** view to analyze storage space utilization and availability, multipathing status, and other storage properties of the selected object and items related to it.

If you use arrays that support storage vendor providers developed through Storage APIs - Storage Awareness, the Reports view offers additional information about storage arrays, storage processors, ports, LUNs or file systems, and so on. For more information about vendor providers, see the *vSphere Storage* documentation.

Maps Storage topology maps visually represent relationships between the selected object and its associated virtual and physical storage entities.

This chapter includes the following topics:

Working with Storage Reports

You monitor storage information through the **Reports** view on the vSphere Client **Storage Views** tab.

For the object you select in the Inventory, a list of categories associated with the object is available. You can display and review statistics for each category of items on the list depending on the inventory object.

For example, if the inventory object is a datastore, you can display information for all virtual machines that reside on the datastore, all hosts that have access to the datastore, a LUN or LUNs, on which the datastore is deployed, and so on. In addition, if your storage supports vendor providers developed through the Storage APIs - Storage Awareness, you can also see information about physical arrays. For information on vendor providers, see the *vSphere Storage* documentation.

When you display the reports tables, the default column headings depend on the inventory object you select. You can customize the tables by adding or removing columns. Reports are automatically updated every 30 minutes. You can manually update the reports by clicking the **Update** link.

You can search for specific information you need to see by filtering reports tables based on storage attributes and keywords.

Display Storage Reports

You can view storage reports in the vSphere Client.

You can display storage reports to review storage information for any inventory object except networking. For example, if the inventory object is a virtual machine, you can review datastores and LUNs that the virtual machine uses, status of paths to the LUNs, adapters that the host uses to access the LUNs, and so on.

Procedure

1 Start the vSphere Client, and log in to the vCenter Server system.

2 Select the appropriate inventory object.

3 Click **Storage Views > Reports**.

4 Select **View > Filtering** to display the **Show all [Category of Items]** and search fields.

5 Click **Show all [Category of Items]** and select a category from the list to display information about that category.

6 Move the cursor over the column heading to see the description of each column.

Filter Storage Reports

To search for specific information you need, you can filter reports tables based on storage attributes you select and keywords you enter in the search field.

Procedure

1 Start the vSphere Client, and log in to the vCenter Server system.

2 Select the appropriate inventory object.

3 Click **Storage Views > Reports**.

4 Select **View > Filtering** to display the **Show all [Category of Items]** and search fields.

5 Click **Show all [Category of Items]** and select a category from the list to display information about that category.

6 Click the search field arrow and select the attributes to include in the search.

7 Type a keyword into the box and press Enter.

The table is updated based on your search criteria. For example, if you are reviewing reports for datastores in a datacenter, you can display information for only those datastores that have NFS format by selecting the **File System Type** attribute and entering NFS as a key word. Filtering is persistent for the user session.

Customize Storage Reports

When you display the reports tables, the default column headings depend on the inventory object you select. You can customize the tables by adding or removing columns.

Procedure

1 Start the vSphere Client, and log in to the vCenter Server system.

2 Select the appropriate inventory object.

3 Click **Storage Views > Reports**.

4 Select **View > Filtering** to display the **Show all [Category of Items]** and search fields.

5 Click **Show all [Category of Items]** and select a category from the list to display information about that category.

6 Customize the report by adding or hiding columns.

- To add a column, right-click any column heading and select an item to display from the list.
- To hide a column, right-click the column heading and deselect it in the list.

Export Storage Reports

You can export storage usage data from a report to a file in various formats, including XML, HTML, or Microsoft Excel.

Procedure

1 Start the vSphere Client, and log in to the vCenter Server system.

2 Select the appropriate inventory object.

3 Click **Storage Views > Reports**.

4 Select **View > Filtering** to display the **Show all [Category of Items]** and search fields.

5 Click **Show all [Category of Items]** and select a category from the list to display information about that category.

6 Right-click below the table and select **Export List**.

7 Specify a file name, type, and location.

8 Click **Save**.

Working with Storage Maps

The Maps view on the vSphere Client **Storage Views** tab helps you visually represent and understand the relationships between an inventory object and all virtual and physical storage resources available for this object. Maps are object-centric and display only items relevant to the specific object.

Maps are automatically updated every 30 minutes. You can manually update the maps by clicking the **Update** link.

You can customize a map view by selecting or deselecting options in the Show area, or by hiding specific items or changing their position on the map.

You can reposition the map by dragging it, and zoom in or out of the map or a section.

Display Storage Maps

You can view storage maps in the vSphere Client.

For any inventory object except networking, you can display storage maps that graphically represent the relationships between the object, for example, a virtual machine, and all resources, such as datastores, LUNs, hosts, and so on, available for this object.

Procedure

1 Start the vSphere Client, and log in to the vCenter Server system.

2 From the vSphere Client, select the appropriate inventory object.

3 Click **Storage Views > Maps**.

Move Items on Storage Maps

You can move individual items on the storage map to make the map visually clearer.

Procedure

1 Start the vSphere Client, and log in to the vCenter Server system.

2 From the vSphere Client, select the appropriate inventory object.

3 Click **Storage Views > Maps**.

4 Select an item you want to move.

Hold the CTRL key to select multiple items.

5 Reposition the selected item by dragging it.

Hide Items on Storage Maps

You can hide items when you view a storage map.

Procedure

1 Start the vSphere Client, and log in to the vCenter Server system.

2 From the vSphere Client, select the appropriate inventory object.

3 Click **Storage Views > Maps**.

4 Right-click the item you want to hide and select **Hide Node** from the menu.

Export Storage Maps

Use the vSphere Client to export maps to various graphic file types, including `jpeg`, `tiff`, and `gif`.

Procedure

1 Start the vSphere Client, and log in to the vCenter Server system.

2 From the vSphere Client, select the appropriate inventory object.

3 Click **Storage Views > Maps**.

4 Right-click the map and select **Export Map**.

5 Specify a file name, type, and location.

6 Click **Save**.

The image file is saved to the format and directory you specified.

Monitoring Events, Alarms, and Automated Actions

5

vSphere includes a user-configurable events and alarms subsystem. This subsystem tracks events happening throughout vSphere and stores the data in log files and the vCenter Server database. This subsystem also enables you to specify the conditions under which alarms are triggered. Alarms can change state from mild warnings to more serious alerts as system conditions change, and can trigger automated alarm actions. This functionality is useful when you want to be informed, or take immediate action, when certain events or conditions occur for a specific inventory object, or group of objects.

Events

Events are records of user actions or system actions that occur on objects in vCenter Server or on a host. Actions that might be recordered as events include, but are not limited to, the following examples:

- A license key expires
- A virtual machine is powered on
- A user logs in to a virtual machine
- A host connection is lost

Event data includes details about the event such as who generated it, when it occured, and what type of event it is. There are three types of events:

- Information
- Warning
- Error

Event data is displayed in **Tasks and Events** tab for the selected inventory object. See "View Events," on page 34

Alarms

Alarms are notifications that are activated in response to an event, a set of conditions, or the state of an inventory object. An alarm definition consists of the following elements:

- Name and description - Provides an identifying label and description.
- Alarm type - Defines the type of object that will be monitored.
- Triggers - Defines the event, condition, or state that will trigger the alarm and defines the notification severity.
- Tolerance thresholds (Reporting) - Provides additional restrictions on condition and state triggers thresholds that must be exceeded before the alarm is triggered.

- Actions - Defines operations that occur in response to triggered alarms. VMware provides sets of predefined actions that are specific to inventory object types.

Alarms have the following severity levels:

- Normal – green
- Warning – yellow
- Alert – red

Alarm definitions are associated with the object selected in the inventory. An alarm monitors the type of inventory objects specified in its definition.

For example, you might want to monitor the CPU usage of all virtual machines in a specific host cluster. You can select the cluster in the inventory, and add a virtual machine alarm to it. When enabled, that alarm will monitor all virtual machines running in the cluster and will trigger when any one of them meets the criteria defined in the alarm. If you want to monitor a specific virtual machine in the cluster, but not others, you would select that virtual machine in the inventory and add an alarm to it. One easy way to apply the same alarms to a group of objects is to place those objects in a folder and define the alarm on the folder.

NOTE You can enable, disable, and modify alarms only from the object in which the alarm is defined. For example, if you defined an alarm in a cluster to monitor virtual machines, you can only enable, disable, or modify that alarm through the cluster; you can not make changes to the alarm at the individual virtual machine level.

Alarm Actions

Alarm actions are operations that occur in response to the trigger. For example, you can have an email notification sent to one or more administrators when an alarm is triggered.

NOTE Default alarms are not preconfigured with actions. You must manually set what action occurs when the triggering event, condition, or state occurs.

This chapter includes the following topics:

View Events

You can view events associated with a single object or view all vSphere events. The events list for a selected inventory object includes events associated with child objects.

Prerequisites

You must have a vSphere Web Client or a vSphere Client connected to a vCenter Server.

Required privilege: **Read-only**

Procedure

- Perform the actions that correspond with the client interface you are using.

In this interface...	Do this...
vSphere Client	■ To see a list of all events in the system, select **Home > Management > Events**. ■ To see a list of events associated with a selected inventory object and its child objects, select the **Tasks & Events** tab and click **Events**.
vSphere Web Client	■ To see a list of all events in the system, select **Monitor > Event Console** from the Console Launcher. ■ To see a list of events associated with a selected inventory object and its child objects, perform the following actions: 1 Open the **vCenter Management** console. 2 Select an inventory object. 3 Select the **Monitor** tab. 4 Click **Events**.
Both clients	■ Select an event to see event details. ■ Use the filter controls above the list to filter the list. ■ Click a column heading to sort the list.

View System Logs

vSphere records events in the vCenter Server database. System log entries include such information as who generated the event, when the event was created, and the type of event.

Prerequisites

You must have a vSphere Client connected to a vCenter Server.

Required privilege:**Global. Diagnostics** privilege.

Procedure

1 To view system log entries, select **Home > Administration > System Logs**.

2 From the drop-down menu, select the log.

3 (Optional) Click **Show All** or **Show next#lines** to see additional log entries.

4 (Optional) Filter the log entries.

   a Select **View > Filtering**.

   b Type the filter criteria in the filter box.

Export Events Data

You can export all or part of the events data stored in the vCenter Server database.

Prerequisites

You must have a vSphere Web Client or a vSphere Client connected to a vCenter Server.

Required Privilege: **Read-only**

Procedure

- Perform the actions that correspond with the client interface you are using.

Option	Description
vSphere Client	a Select **File > Export > Export Events**. b (Linked-mode only) In the**vCenter Server** list, select the server where the events occurred. c Specify Events, Time, and Limits attributes for the events you want to export. d Specify a file name and location. e Click **OK**.
vSphere Web Client	a Switch console views to the Event Console view and click **Export**. b Specify Events, Time, and Limits attributes for the events you want to export. c Click **Proceed**. d Click **Export**. e Specify a file name and location. f Click **OK**.

vCenter Server creates the file in the specified location. The file contains the **Type**, **Time**, and **Description** of the events.

View Triggered Alarms and Alarm Definitions

Triggered alarms are visible in several locations throughout the vSphere Client and vSphere Web Client. Alarm definitions are accessible only through the vSphere Client.

Prerequisites

You must have a vSphere Web Client or a vSphere Client connected to a vCenter Server.

Procedure

- Perform the following actions for the client you are using:

Option	Description
vSphere Client	■ To view all triggered alarms, click **Alarms** in the status bar. ■ To view alarms triggered on an selected inventory object, select the **Alarms** tab **> Triggered Alarms**. ■ To view a list of alarms associated with a selected inventory object, select the **Alarms** tab **> Definitions**. The **Defined In** column indicates the object on which the alarm was set.
vSphere Web Client	■ To view all triggered alarms, click **All** in the Alarms sidebar. ■ To view only newly triggered alarms, click **New** in the Alarms sidebar. ■ To view acknowledged alarms, click **Ack'd** in the Alarms sidebar. ■ To view alarms triggered on an selected inventory object, select **Monitor > Alarms** tab.

Acknowledge Triggered Alarms

Acknowledging an alarm lets other users know that you are taking ownership of the issue. After an alarm is acknowledged, its alarm actions are discontinued. For example, a host has an alarm set on it that monitors CPU usage and that sends an email to an administrator when the alarm is triggered. The host CPU usage spikes, triggering the alarm which sends an email to the host's administrator. The administrator acknowledges the triggered alarm to let other administrators know he is working on the problem, and to prevent the alarm from sending more email messages. The alarm, however, is still visible in the system. Alarms are neither cleared, nor reset when acknowledged.

Prerequisites

You must have a vSphere Web Client or a vSphere Client connected to a vCenter Server.

Required privilege: **Alarm.Alarm Acknowledge**

Procedure

- Perform the following actions for the client you are using:

Option	Description
vSphere Client	a Display the inventory panel. b If necessary, select **View > Status Bar** to display the status pane. c In the status bar, click **Alarms** to display the Triggered Alarms panel. d Right-click the alarm and select **Acknowledge Alarm**. e To acknowledge multiple alarms at one time, shift-click each alarm to select it, right-click the selection, and select **Acknowledge Alarm**.
vSphere Web Client	a Select an inventory object. b Select **Monitor > Alarms**. c Select the alarms you want to acknowledge. Use Shift+Click or Ctrl+Click to select multiple alarms. d Click **Acknowledge**. Alternative methods: ■ Click **Acknowledge** in Alarm Details. ■ Right-click an alarm in the Alarm sidebar and select **Acknowledge**.

Reset Triggered Event Alarms

An alarm triggered by an event might not reset to a normal state if vCenter Server does not retrieve the event that identifies the normal condition. In such cases, reset the alarm manually to return it to a normal state.

Prerequisites

You must have a vSphere Web Client or a vSphere Client connected to a vCenter Server.

Required privilege: **Alarm.Set Alarm Status**

Procedure

- Perform the following actions for the client you are using:

Option	Description
vSphere Client	a Locate the triggered alarm in the Triggered Alarms panel or on the **Alarms** tab for the object. b Right-click the alarm and select **Reset Alarm to Green**.
vSphere Web Client	a Select an inventory object. b Select **Monitor > Alarms**. c Select the alarms you want to reset. Use Shift+Click or Ctrl+Click to select multiple alarms. d Click **Reset to Green**. Alternative methods: ■ Click **Reset to green** in Alarm Details. ■ Right-click an alarm in the Alarm sidebar and select **Reset to green**.

Identify Disabled Alarm Actions

If you are experiencing problems with alarm actions for a specific inventory object, ensure that alarm actions are enabled for that object.

Prerequisites

You must have a vSphere Web Client or a vSphere Client connected to a vCenter Server.

Procedure

1 Select a parent object, depending on the scope of objects you want to examine.

- vCenter Server
- Datacenter
- Cluster
- Host
- Virtual Switch
- Datastore Cluster

2 Select the tab that corresponds to the child objects you want to examine.

For example, if the selected inventory object is a datacenter, you might select the Hosts tab.

3 Locate the **Alarm Actions** column..

You might need to scroll horizontally to bring the column into view.

The value in the **Alarm Actions** column indicates whether alarm actions are enabled or disabled on the listed objects.

Monitoring Solutions with the vCenter Solutions Manager 6

A vSphere administrator uses the vCenter Solutions Manager to view the installalled solutions, view detailed information about the solutions, and monitor the solution health status.

You can monitor and manage vSphere solutions from the vSphere Client that displays an inventory of vSphere solutions and details about each solution.

A solution is an extension of the vCenter Server that adds new functions to a vCenter Server instance. For example, vSphere ESX Agent Manager is a standard vCenter solution provided by VMware that allows you to manage ESX host agents that add new capabilities to ESX hosts. Another standard solution that vSphere provides is vService Manager. VMware products that integrate with vCenter Sever are also considered solutions. You can install a solution to add functionality from third-party technologies to the standard functions of vCenter Server. Solutions typically are delivered as OVF packages. You can install and deploy solutions from vSphere Client. Solutions can be integrated into the vCenter Solutions Manager.

If a virtual machine or vApp is running a solution, a custom icon appears next to it in the inventory view of the vSphere Client. When you power on or power off a virtual machine or vApp, you are notified that you are performing this operation on an entity that is managed by the solution manager.

Each solution registers a unique icon to identify that the virtual machine or vApp is being managed by that solution. The icons show the power states (powered on, paused, powered off).

The solutions display more than one type of icon if they manage more than one type of virtual machine or vApp.

When you attempt an operation on a virtual machine or a vApp that is managed by a solution, an informational warning message appears.

For more information, see the *Developing and Deploying vSphere Solutions, vServices, and ESX Agents* documentation.

This chapter includes the following topics:

Viewing Solutions

You can deploy, monitor, and interact with solutions that are installed in a vCenter Server instance with the vCenter Solutions Manager. The Solutions Manager displays information about the health of a solution.

You can navigate to the Solutions Manager from the home page of the vSphere Client. The Solutions Manager view displays information about the solution:

- Solution name

- Solution health
- vService providers

Procedure

1 Click the Solutions Manager icon from vSphere Client home.

2 Navigate through the tabs in the Solutions Manager.

   - **Summary** tab. Lists the number of installed solutions and a brief health overview for each of the solutions.
   - **Solutions** tab. Lists each managed solution.
   - **Health** tab. Provides the health status of the vCenter services. It also shows alerts or warnings for each of the services.

3 In the Solutions Manager inventory, click one of the solutions.

   - **Summary** tab. Lists information about the solution, including a link to the product and vendor Web sites, a link to launch the management UI in a separate window, and a link to the virtual machine or vApp running this solution.

     Selecting the vendor Web site link takes you to the Summary page of the virtual machine or vApp. A link under "Managed by" returns you to the solution.
   - **Virtual Machines** tab. Lists all the virtual machines belonging to the solution
   - **vServices Providers** tab.
   - **Management** tab or any other tabs the solution specified.

Monitoring Agents

The vCenter Solutions Manager displays the vSphere ESX Agent Manager agents that you use to deploy and manage related agents on ESX hosts.

An administrator uses the solutions manager to keep track of whether a solution's agents are working as expected. Outstanding issues are reflected by the solution's ESX Agent Manager status and a list of issues.

When a solution's state changes, the solutions manager updates the ESX Agent Manager's summary status and state. Administrators use this status to track whether the goal state is reached.

The agency's health status is indicated by a specific color:

- Red. The solution must intervene for the ESX Agent Manager to proceed. For example, if a virtual machine agent is powered off manually on a compute resource and the ESX Agent Manager does not attempt to power on the agent. The ESX Agent Manager reports this action to the solution. The solution alerts the administrator to power on the agent.
- Yellow. The ESX Agent Manager is actively working to reach a goal state. The goal state can be enabled, disabled, or uninstalled. For example, when a solution is registered, its status is yellow until the ESX Agent Manager deploys the solutions agents to all the specified compute resources. A solution does not need to intervene when the ESX Agent Manager reports its ESX Agent Manager health status as yellow.
- Green. A solution and all its agents reached the goal state.

Monitoring vServices

A vService is a service or function that a solution provides to virtual machines and vApps. A solution can provide one or more vServices. These vServices integrate with the platform and are able to change the environment in which the vApp or virtual machine runs.

A vService is a type of service for a virtual machine and a vApp provided by a vCenter extension. Virtual machines and vApps can have dependencies on vServices. Each dependency is associated with a vService type. The vService type must be bound to a particular vCenter extension that implements that vService type. This vService type is similar to a virtual hardware device. For example, a virtual machine can have a networking device that at deployment must be connected to a particular network.

The vService Manager allows a solution to connect to operations related to OVF templates:

- Importing OVF templates. Receive a callback when OVF templates with a vService dependancy of a certain type is imported.
- Exporting OVF templates. Inserts OVF sections when a virtual machine is exported.
- OVF environment generation. Inserts OVF sections into the OVF environment at the power-on instance.

The **vService Provider** tab in the solution manager provides details for each vCenter extension. This information allows you to monitor vService providers and list the virtual machines or vApps to which they are bound.

Performance Monitoring Utilities: resxtop and esxtop 7

The resxtop and esxtop command-line utilities provide a detailed look at how ESXi uses resources in real time. You can start either utility in one of three modes: interactive (default), batch, or replay.

The fundamental difference between resxtop and esxtop is that you can use resxtop remotely, whereas you can start esxtop only through the ESXi Shell of a local ESXi host.

This chapter includes the following topics:

Using the esxtop Utility

You can run the esxtop utility using the ESXi Shell to communicate with the ESXi host's management interface. You must have root user privileges.

Type the command, using the options you want:

```
esxtop [-] [h] [v] [b] [s] [a] [c filename] [R vm-support_dir_path]  [d delay] [n iter]
```

The esxtop utility reads its default configuration from .esxtop50rc on the ESXi system. This configuration file consists of nine lines.

The first eight lines contain lowercase and uppercase letters to specify which fields appear in which order on the CPU, memory, storage adapter, storage device, virtual machine storage, network, interrupt, and CPU power panels. The letters correspond to the letters in the Fields or Order panels for the respective esxtop panel.

The ninth line contains information on the other options. Most important, if you saved a configuration in secure mode, you do not get an insecure esxtop without removing the s from the seventh line of your .esxtop50rc file. A number specifies the delay time between updates. As in interactive mode, typing c, m, d, u, v, n, I, or p determines the panel with which esxtop starts.

NOTE Do not edit the .esxtop50rc file. Instead, select the fields and the order in a running esxtop process, make changes, and save this file using the W interactive command.

Using the resxtop Utility

The resxtop utility is a vSphere CLI command.

Before you can use any vSphere CLI commands, you must either download and install a vSphere CLI package or deploy the vSphere Management Assistant (vMA) to your ESXi host or vCenter Server system.

After it is set up, start resxtop from the command line. For remote connections, you can connect to a host either directly or through vCenter Server.

The command-line options listed in the following table are the same as for esxtop (except for the R option) with additional connection options.

NOTE resxtop does not use all the options shared by other vSphere CLI commands.

Table 7-1. resxtop Command-Line Options

Option	Description
[server]	Name of the remote host to connect to (required). If connecting directly to the ESXi host, use the name of that host. If your connection to the ESXi host is indirect (that is, through vCenter Server), use the name of the vCenter Server system for this option.
[vihost]	If you connect indirectly (through vCenter Server), this option should contain the name of the ESXi host you connect to. If you connect directly to the host, this option is not used. Note that the host name needs to be the same as what appears in the vSphere Client.
[portnumber]	Port number to connect to on the remote server. The default port is 443, and unless this is changed on the server, this option is not needed.
[username]	User name to be authenticated when connecting to the remote host. The remote server prompts you for a password.

You can also use resxtop on a local ESXi host by omitting the server option on the command line. The command defaults to localhost.

Using esxtop or resxtop in Interactive Mode

By default, resxtop and esxtop run in interactive mode. Interactive mode displays statistics in different panels.

A help menu is available for each panel.

Interactive Mode Command-Line Options

You can use various command-line options with esxtop and resxtop in interactive mode.

Table 7-2. Interactive Mode Command-Line Options

Option	Description
h	Prints help for resxtop (or esxtop) command-line options.
v	Prints resxtop (or esxtop) version number.
s	Calls resxtop (or esxtop) in secure mode. In secure mode, the –d command, which specifies delay between updates, is disabled.
d	Specifies the delay between updates. The default is five seconds. The minimum is two seconds. Change this with the interactive command s. If you specify a delay of less than two seconds, the delay is set to two seconds.
n	Number of iterations. Updates the display n times and exits. Default value is 10000.
server	The name of the remote server host to connect to (required for resxtop only).

Table 7-2. Interactive Mode Command-Line Options (Continued)

Option	Description
`vihost`	If you connect indirectly (through vCenter Server), this option should contain the name of the ESXi host you connect to. If you connect directly to the ESXi host, this option is not used. Note that the host name needs to be the same as what is displayed in the vSphere Client.
`portnumber`	The port number to connect to on the remote server. The default port is 443, and unless this is changed on the server, this option is not needed. (`resxtop` only)
`username`	The user name to be authenticated when connecting to the remote host. The remote server prompts you for a password, as well (`resxtop` only).
`a`	Show all statistics. This option overrides configuration file setups and shows all statistics. The configuration file can be the default ~/.esxtop50rc configuration file or a user-defined configuration file.
`c` *filename*	Load a user-defined configuration file. If the -c option is not used, the default configuration filename is ~/.esxtop50rc. Create your own configuration file, specifying a different filename, using the `W` single-key interactive command.

Common Statistics Description

Several statistics appear on the different panels while `resxtop` (or `esxtop`) is running in interactive mode. These statistics are common across all four panels.

The Uptime line, found at the top of each of the four `resxtop` (or `esxtop`) panels, displays the current time, time since last reboot, number of currently running worlds and load averages. A world is an ESXi VMkernel schedulable entity, similar to a process or thread in other operating systems.

Below that the load averages over the past one, five, and fifteen minutes appear. Load averages take into account both running and ready-to-run worlds. A load average of 1.00 means that there is full utilization of all physical CPUs. A load average of 2.00 means that the ESXi system might need twice as many physical CPUs as are currently available. Similarly, a load average of 0.50 means that the physical CPUs on the ESXi system are half utilized.

Statistics Columns and Order Pages

You can define the order of fields displayed in interactive mode.

If you press `f`, `F`, `o`, or `O`, the system displays a page that specifies the field order on the top line and short descriptions of the field contents. If the letter in the field string corresponding to a field is uppercase, the field is displayed. An asterisk in front of the field description indicates whether a field is displayed.

The order of the fields corresponds to the order of the letters in the string.

From the Field Select panel, you can:

- Toggle the display of a field by pressing the corresponding letter.
- Move a field to the left by pressing the corresponding uppercase letter.
- Move a field to the right by pressing the corresponding lowercase letter.

Interactive Mode Single-Key Commands

When running in interactive mode, `resxtop` (or `esxtop`) recognizes several single-key commands.

All interactive mode panels recognize the commands listed in the following table. The command to specify the delay between updates is disabled if the `s` option is given on the command line. All sorting interactive commands sort in descending order.

Table 7-3. Interactive Mode Single-Key Commands

Key	Description
h or ?	Displays a help menu for the current panel, giving a brief summary of commands, and the status of secure mode.
space	Immediately updates the current panel.
^L	Erases and redraws the current panel.
f or F	Displays a panel for adding or removing statistics columns (fields) to or from the current panel.
o or O	Displays a panel for changing the order of statistics columns on the current panel.
#	Prompts you for the number of statistics rows to display. Any value greater than 0 overrides automatic determination of the number of rows to show, which is based on window size measurement. If you change this number in one `resxtop` (or `esxtop`) panel, the change affects all four panels.
s	Prompts you for the delay between updates, in seconds. Fractional values are recognized down to microseconds. The default value is five seconds. The minimum value is two seconds. This command is not available in secure mode.
W	Write the current setup to an esxtop (or resxtop) configuration file. This is the recommended way to write a configuration file. The default filename is the one specified by -c option, or `~/.esxtop50rc` if the -c option is not used. You can also specify a different filename on the prompt generated by this W command.
q	Quit interactive mode.
c	Switch to the CPU resource utilization panel.
p	Switch to the CPU Power utilization panel.
m	Switch to the memory resource utilization panel.
d	Switch to the storage (disk) adapter resource utilization panel.
u	Switch to storage (disk) device resource utilization screen.
v	Switch to storage (disk) virtual machine resource utilization screen.
n	Switch to the network resource utilization panel.
i	Switch to the interrupt panel.

CPU Panel

The CPU panel displays server-wide statistics as well as statistics for individual world, resource pool, and virtual machine CPU utilization.

Resource pools, virtual machines that are running, or other worlds are at times called groups. For worlds belonging to a virtual machine, statistics for the virtual machine that is running are displayed. All other worlds are logically aggregated into the resource pools that contain them.

Table 7-4. CPU Panel Statistics

Line	Description
PCPU USED(%)	A PCPU refers to a physical hardware execution context. This can be a physical CPU core if hyperthreading is unavailable or disabled, or a logical CPU (LCPU or SMT thread) if hyperthreading is enabled. PCPU USED(%) displays the following percentages: ■ percentage of CPU usage per PCPU ■ percentage of CPU usage averaged over all PCPUs CPU Usage (%USED) is the percentage of PCPU nominal frequency that was used since the last screen update. It equals the total sum of %USED for Worlds that ran on this PCPU. **NOTE** If a PCPU is running at frequency that is higher than its nominal (rated) frequency, then PCPU USED(%) can be greater than 100%. If a PCPU and its partner are busy when hyperthreading is enabled, each PCPU accounts for half of the CPU usage.
PCPU UTIL(%)	A PCPU refers to a physical hardware execution context. This can be a physical CPU core if hyperthreading is unavailable or disabled, or a logical CPU (LCPU or SMT thread) if hyperthreading is enabled. PCPU UTIL(%) represents the percentage of real time that the PCPU was not idle (raw PCPU utilization) and it displays the percentage CPU utilization per PCPU, and the percentage CPU utilization averaged over all PCPUs. **NOTE** PCPU UTIL(%) might differ from PCPU USED(%) due to power management technologies or hyperthreading.
ID	Resource pool ID or virtual machine ID of the resource pool or virtual machine of the world that is running, or world ID of the world that is running.
GID	Resource pool ID of the resource pool or virtual machine of the world that is running.
NAME	Name of the resource pool or virtual machine of the world that is running, or name of the world that is running.
NWLD	Number of members in the resource pool or virtual machine of the world that is running. If a Group is expanded using the interactive command `e`, then NWLD for all the resulting worlds is 1.
%STATE TIMES	Set of CPU statistics made up of the following percentages. For a world, the percentages are a percentage of one physical CPU core.
%USED	Percentage of physical CPU core cycles used by the resource pool, virtual machine, or world. %USED might depend on the frequency with which the CPU core is running. When running with lower CPU core frequency, %USED can be smaller than %RUN. On CPUs which support turbo mode, CPU frequency can also be higher than the nominal (rated) frequency, and %USED can be larger than %RUN.
%SYS	Percentage of time spent in the ESXi VMkernel on behalf of the resource pool, virtual machine, or world to process interrupts and to perform other system activities. This time is part of the time used to calculate %USED.
%WAIT	Percentage of time the resource pool, virtual machine, or world spent in the blocked or busy wait state. This percentage includes the percentage of time the resource pool, virtual machine, or world was idle.
%VMWAIT	The total percentage of time the Resource Pool/World spent in a blocked state waiting for events.
%IDLE	Percentage of time the resource pool, virtual machine, or world was idle. Subtract this percentage from %WAIT to see the percentage of time the resource pool, virtual machine, or world was waiting for some event. The difference, %WAIT- %IDLE, of the VCPU worlds can be used to estimate guest I/O wait time. To find the VCPU worlds, use the single-key command `e` to expand a virtual machine and search for the world NAME starting with "vcpu". (The VCPU worlds might wait for other events in addition to I/O events, so this measurement is only an estimate.)
%RDY	Percentage of time the resource pool, virtual machine, or world was ready to run, but was not provided CPU resources on which to execute.
%MLMTD (max limited)	Percentage of time the ESXi VMkernel deliberately did not run the resource pool, virtual machine, or world because doing so would violate the resource pool, virtual machine, or world's limit setting. Because the resource pool, virtual machine, or world is ready to run when it is prevented from running in this way, the %MLMTD (max limited) time is included in %RDY time.

Table 7-4. CPU Panel Statistics (Continued)

Line	Description
%SWPWT	Percentage of time a resource pool or world spends waiting for the ESXi VMkernel to swap memory. The %SWPWT (swap wait) time is included in the %WAIT time.
EVENT COUNTS/s	Set of CPU statistics made up of per second event rates. These statistics are for VMware internal use only.
CPU ALLOC	Set of CPU statistics made up of the following CPU allocation configuration parameters.
AMIN	Resource pool, virtual machine, or world attribute Reservation.
AMAX	Resource pool, virtual machine, or world attribute Limit. A value of -1 means unlimited.
ASHRS	Resource pool, virtual machine, or world attribute Shares.
SUMMARY STATS	Set of CPU statistics made up of the following CPU configuration parameters and statistics. These statistics apply only to worlds and not to virtual machines or resource pools.
AFFINITY BIT MASK	Bit mask showing the current scheduling affinity for the world.
HTSHARING	Current hyperthreading configuration.
CPU	The physical or logical processor on which the world was running when `resxtop` (or `esxtop`) obtained this information.
HTQ	Indicates whether the world is currently quarantined or not. N means no and Y means yes.
TIMER/s	Timer rate for this world.
%OVRLP	Percentage of system time spent during scheduling of a resource pool, virtual machine, or world on behalf of a different resource pool, virtual machine, or world while the resource pool, virtual machine, or world was scheduled. This time is not included in %SYS. For example, if virtual machine A is currently being scheduled and a network packet for virtual machine B is processed by the ESXi VMkernel, the time spent appears as %OVRLP for virtual machine A and %SYS for virtual machine B.
%RUN	Percentage of total time scheduled. This time does not account for hyperthreading and system time. On a hyperthreading enabled server, the %RUN can be twice as large as %USED.
%CSTP	Percentage of time a resource pool spends in a ready, co-deschedule state. **NOTE** You might see this statistic displayed, but it is intended for VMware use only.
POWER	Current CPU power consumption for a resource pool (in Watts).
%LAT_C	Percentage of time the resource pool or world was ready to run but was not scheduled to run because of CPU resource contention.
%LAT_M	Percentage of time the resource pool or world was ready to run but was not scheduled to run because of memory resource contention.
%DMD	CPU demand in percentage. It represents the average active CPU load in the past minute.

You can change the display using single-key commands.

Table 7-5. CPU Panel Single-Key Commands

Command	Description
e	Toggles whether CPU statistics are displayed expanded or unexpanded. The expanded display includes CPU resource utilization statistics broken down by individual worlds belonging to a resource pool or virtual machine. All percentages for the individual worlds are percentage of a single physical CPU. Consider these examples: ■ If the %Used by a resource pool is 30% on a two-way server, the resource pool is utilizing 30 percent of one physical core. ■ If the %Used by a world belonging to a resource pool is 30 percent on a two-way server, that world is utilizing 30% of one physical core.
U	Sorts resource pools, virtual machines, and worlds by the resource pool's or virtual machine's %Used column. This is the default sort order.
R	Sorts resource pools, virtual machines, and worlds by the resource pool's or virtual machine's %RDY column.
N	Sorts resource pools, virtual machines, and worlds by the GID column.
V	Displays virtual machine instances only.
L	Changes the displayed length of the NAME column.

CPU Power Panel

The CPU Power panel displays CPU Power utilization statistics.

On the CPU Power panel, statistics are arranged per PCPU. A PCPU is a physical hardware execution context -- a physical CPU core if hyper-threading is unavailable or disabled, or a logical CPU (LCPU or SMT thread) if hyper-threading is enabled.

Table 7-6. CPU Power Panel Statistics

Line	Description
Power Usage	Current total power usage (in Watts).
Power Cap	Total power cap (in Watts).
PSTATE MHZ	Clock frequency per state.
%USED	Percentage of PCPU nominal frequency used since the last screen update. It is the same as PCPU USED(%) shown in the CPU Screen.
%UTIL	Raw PCPU utilization, that is the percentage of real time that PCPU was not idle. It is the same as PCPU UTIL(%) shown in the CPU Screen.
%Cx	Percentage of time the PCPU spent in C-State 'x'.
%Px	Percentage of time the PCPU spent in P-State 'x'. On systems with Processor Clocking Control, P-states are not directly visible to ESXi, so `esxtop` instead shows the percentage of time spent at full speed under the heading 'P0' and the percentage of time spent at any lower speed under 'P1'.
%Tx	Percentage of time the PCPU spent in T-State 'x'.

Memory Panel

The Memory panel displays server-wide and group memory utilization statistics. As on the CPU panel, groups correspond to resource pools, running virtual machines, or other worlds that are consuming memory.

The first line, found at the top of the Memory panel displays the current time, time since last reboot, number of currently running worlds, and memory overcommitment averages. The memory overcommitment averages over the past one, five, and fifteen minutes appear. Memory overcommitment of 1.00 means a memory overcommitment of 100 percent.

Table 7-7. Memory Panel Statistics

Field	Description	
PMEM (MB)	Displays the machine memory statistics for the server. All numbers are in megabytes.	
	total	Total amount of machine memory in the server.
	vmk	Amount of machine memory being used by the ESXi VMkernel.
	other	Amount of machine memory being used by everything other than the ESXi VMkernel.
	free	Amount of machine memory that is free.
VMKMEM (MB)	Displays the machine memory statistics for the ESXi VMkernel. All numbers are in megabytes.	
	managed	Total amount of machine memory managed by the ESXi VMkernel.
	min free	Minimum amount of machine memory that the ESXi VMkernel aims to keep free.
	rsvd	Total amount of machine memory currently reserved by resource pools.
	ursvd	Total amount of machine memory currently unreserved.
	state	Current machine memory availability state. Possible values are high, soft, hard and low. High means that the machine memory is not under any pressure and low means that it is.
NUMA (MB)	Displays the ESXi NUMA statistics. This line appears only if the ESXi host is running on a NUMA server. All numbers are in megabytes. For each NUMA node in the server, two statistics are displayed: ■ The total amount of machine memory in the NUMA node that is managed by ESXi. ■ The amount of machine memory in the node that is currently free (in parentheses).	
PSHARE (MB)	Displays the ESXi page-sharing statistics. All numbers are in megabytes.	
	shared	Amount of physical memory that is being shared.
	common	Amount of machine memory that is common across worlds.
	saving	Amount of machine memory that is saved because of page sharing.
SWAP (MB)	Displays the ESXi swap usage statistics. All numbers are in megabytes.	
	curr	Current swap usage.
	rclmtgt	Where the ESXi system expects the reclaimed memory to be. Memory can be reclaimed by swapping or compression.
	r/s	Rate at which memory is swapped in by the ESXi system from disk.
	w/s	Rate at which memory is swapped to disk by the ESXi system.
ZIP (MB)	Displays the ESXi memory compression statistics. All numbers are in megabytes.	
	zipped	Total compressed physical memory.
	saved	Saved memory by compression.

Table 7-7. Memory Panel Statistics (Continued)

Field	Description	
MEMCTL (MB)	Displays the memory balloon statistics. All numbers are in megabytes.	
	curr	Total amount of physical memory reclaimed using the `vmmemctl` module.
	target	Total amount of physical memory the ESXi host attempts to reclaim using the `vmmemctl` module.
	max	Maximum amount of physical memory the ESXi host can reclaim using the `vmmemctl` module.
AMIN	Memory reservation for this resource pool or virtual machine.	
AMAX	Memory limit for this resource pool or virtual machine. A value of -1 means Unlimited.	
ASHRS	Memory shares for this resource pool or virtual machine.	
NHN	Current home node for the resource pool or virtual machine. This statistic is applicable only on NUMA systems. If the virtual machine has no home node, a dash (-) appears.	
NRMEM (MB)	Current amount of remote memory allocated to the virtual machine or resource pool. This statistic is applicable only on NUMA systems.	
N% L	Current percentage of memory allocated to the virtual machine or resource pool that is local.	
MEMSZ (MB)	Amount of physical memory allocated to a resource pool or virtual machine.	
GRANT (MB)	Amount of guest physical memory mapped to a resource pool or virtual machine. The consumed host machine memory is equal to GRANT - SHRDSVD.	
SZTGT (MB)	Amount of machine memory the ESXi VMkernel wants to allocate to a resource pool or virtual machine.	
TCHD (MB)	Working set estimate for the resource pool or virtual machine.	
%ACTV	Percentage of guest physical memory that is being referenced by the guest. This is an instantaneous value.	
%ACTVS	Percentage of guest physical memory that is being referenced by the guest. This is a slow moving average.	
%ACTVF	Percentage of guest physical memory that is being referenced by the guest. This is a fast moving average.	
%ACTVN	Percentage of guest physical memory that is being referenced by the guest. This is an estimation. (You might see this statistic displayed, but it is intended for VMware use only.)	
MCTL?	Memory balloon driver is installed or not. **N** means no, **Y** means yes.	
MCTLSZ (MB)	Amount of physical memory reclaimed from the resource pool by way of ballooning.	
MCTLTGT (MB)	Amount of physical memory the ESXi system attempts to reclaim from the resource pool or virtual machine by way of ballooning.	
MCTLMAX (MB)	Maximum amount of physical memory the ESXi system can reclaim from the resource pool or virtual machine by way of ballooning. This maximum depends on the guest operating system type.	
SWCUR (MB)	Current swap usage by this resource pool or virtual machine.	
SWTGT (MB)	Target where the ESXi host expects the swap usage by the resource pool or virtual machine to be.	
SWR/s (MB)	Rate at which the ESXi host swaps in memory from disk for the resource pool or virtual machine.	
SWW/s (MB)	Rate at which the ESXi host swaps resource pool or virtual machine memory to disk.	
LLSWR/s (MB)	Rate at which memory is read from the host cache.	
LLSWW/s (MB)	Rate at which memory is written to the host cache from various sources.	

Table 7-7. Memory Panel Statistics (Continued)

Field	Description
CPTRD (MB)	Amount of data read from checkpoint file.
CPTTGT (MB)	Size of checkpoint file.
ZERO (MB)	Resource pool or virtual machine physical pages that are zeroed.
SHRD (MB)	Resource pool or virtual machine physical pages that are shared.
SHRDSVD (MB)	Machine pages that are saved because of resource pool or virtual machine shared pages.
OVHD (MB)	Current space overhead for resource pool.
OVHDMAX (MB)	Maximum space overhead that might be incurred by resource pool or virtual machine.
OVHDUW (MB)	Current space overhead for a user world. (You might see this statistic displayed, but it is intended for VMware use only.)
GST_NDx (MB)	Guest memory allocated for a resource pool on NUMA node x. This statistic is applicable on NUMA systems only.
OVD_NDx (MB)	VMM overhead memory allocated for a resource pool on NUMA node x. This statistic is applicable on NUMA systems only.
TCHD_W (MB)	Write working set estimate for resource pool.
CACHESZ (MB)	Compression memory cache size.
CACHEUSD (MB)	Used compression memory cache.
ZIP/s (MB/s)	Compressed memory per second.
UNZIP/s (MB/s)	Decompressed memory per second.

Table 7-8. Memory Panel Interactive Commands

Command	Description
M	Sort resource pools or virtual machines by MEMSZ column. This is the default sort order.
B	Sort resource pools or virtual machines by Group Memctl column.
N	Sort resource pools or virtual machines by GID column.
V	Display virtual machine instances only.
L	Changes the displayed length of the NAME column.

Storage Adapter Panel

Statistics in the Storage Adapter panel are aggregated per storage adapter by default. Statistics can also be viewed per storage path.

Table 7-9. Storage Adapter Panel Statistics

Column	Description
ADAPTR	Name of the storage adapter.
PATH	Storage path name. This name is only visible if the corresponding adapter is expanded. See interactive command `e` in Table 7-10.
NPTH	Number of paths.
AQLEN	Current queue depth of the storage adapter.
CMDS/s	Number of commands issued per second.
READS/s	Number of read commands issued per second.
WRITES/s	Number of write commands issued per second.

Table 7-9. Storage Adapter Panel Statistics (Continued)

Column	Description
MBREAD/s	Megabytes read per second.
MBWRTN/s	Megabytes written per second.
RESV/s	Number of SCSI reservations per second.
CONS/s	Number of SCSI reservation conflicts per second.
DAVG/cmd	Average device latency per command, in milliseconds.
KAVG/cmd	Average ESXi VMkernel latency per command, in milliseconds.
GAVG/cmd	Average virtual machine operating system latency per command, in milliseconds.
QAVG/cmd	Average queue latency per command, in milliseconds.
DAVG/rd	Average device read latency per read operation, in milliseconds.
KAVG/rd	Average ESXi VMkernel read latency per read operation, in milliseconds.
GAVG/rd	Average guest operating system read latency per read operation, in milliseconds.
QAVG/rd	Average queue latency per read operation, in milliseconds.
DAVG/wr	Average device write latency per write operation, in milliseconds.
KAVG/wr	Average ESXi VMkernel write latency per write operation, in milliseconds.
GAVG/wr	Average guest operating system write latency per write operation, in milliseconds.
QAVG/wr	Average queue latency per write operation, in milliseconds.
FCMDS/s	Number of failed commands issued per second.
FREAD/s	Number of failed read commands issued per second.
FWRITE/s	Number of failed write commands issued per second.
FMBRD/s	Megabytes of failed read operations per second.
FMBWR/s	Megabytes of failed write operations per second.
FRESV/s	Number of failed SCSI reservations per second.
ABRTS/s	Number of commands aborted per second.
RESETS/s	Number of commands reset per second.
PAECMD/s	The number of PAE (Physical Address Extension) commands per second.
PAECP/s	The number of PAE copies per second.
SPLTCMD/s	The number of split commands per second.
SPLTCP/s	The number of split copies per second.

The following table displays the interactive commands you can use with the storage adapter panel.

Table 7-10. Storage Adapter Panel Interactive Commands

Command	Description
`e`	Toggles whether storage adapter statistics appear expanded or unexpanded. Allows you to view storage resource utilization statistics broken down by individual paths belonging to an expanded storage adapter. You are prompted for the adapter name.
`r`	Sorts by READS/s column.
`w`	Sorts by WRITES/s column.
`R`	Sorts by MBREAD/s read column.

Table 7-10. Storage Adapter Panel Interactive Commands (Continued)

Command	Description
T	Sorts by MBWRTN/s written column.
N	Sorts first by ADAPTR column, then by PATH column. This is the default sort order.

Storage Device Panel

The storage device panel displays server-wide storage utilization statistics.

By default, the information is grouped per storage device. You can also group the statistics per path, per world, or per partition.

Table 7-11. Storage Device Panel Statistics

Column	Description
DEVICE	Name of the storage device.
PATH	Path name. This name is visible only if the corresponding device is expanded to paths. See the interactive command `p` in Table 7-12.
WORLD	World ID. This ID is visible only if the corresponding device is expanded to worlds. See the interactive command `e` in Table 7-12. The world statistics are per world per device.
PARTITION	Partition ID. This ID is visible only if the corresponding device is expanded to partitions. See interactive command `t` in Table 7-12.
NPH	Number of paths.
NWD	Number of worlds.
NPN	Number of partitions.
SHARES	Number of shares. This statistic is applicable only to worlds.
BLKSZ	Block size in bytes.
NUMBLKS	Number of blocks of the device.
DQLEN	Current device queue depth of the storage device.
WQLEN	World queue depth. This is the maximum number of ESXi VMkernel active commands that the world is allowed to have. This is a per device maximum for the world. It is valid only if the corresponding device is expanded to worlds.
ACTV	Number of commands in the ESXi VMkernel that are currently active. This statistic applies to only worlds and devices.
QUED	Number of commands in the ESXi VMkernel that are currently queued. This statistic applies to only worlds and devices.
%USD	Percentage of the queue depth used by ESXi VMkernel active commands. This statistic applies to only worlds and devices.
LOAD	Ratio of ESXi VMkernel active commands plus ESXi VMkernel queued commands to queue depth. This statistic applies to only worlds and devices.
CMDS/s	Number of commands issued per second.
READS/s	Number of read commands issued per second.
WRITES/s	Number of write commands issued per second.
MBREAD/s	Megabytes read per second.
MBWRTN/s	Megabytes written per second.
DAVG/cmd	Average device latency per command in milliseconds.
KAVG/cmd	Average ESXi VMkernel latency per command in milliseconds.
GAVG/cmd	Average guest operating system latency per command in milliseconds.

Table 7-11. Storage Device Panel Statistics (Continued)

Column	Description
QAVG/cmd	Average queue latency per command in milliseconds.
DAVG/rd	Average device read latency per read operation in milliseconds.
KAVG/rd	Average ESXi VMkernel read latency per read operation in milliseconds.
GAVG/rd	Average guest operating system read latency per read operation in milliseconds.
QAVG/rd	Average queue read latency per read operation in milliseconds.
DAVG/wr	Average device write latency per write operation in milliseconds.
KAVG/wr	Average ESXi VMkernel write latency per write operation in milliseconds.
GAVG/wr	Average guest operating system write latency per write operation in milliseconds.
QAVG/wr	Average queue write latency per write operation in milliseconds.
ABRTS/s	Number of commands aborted per second.
RESETS/s	Number of commands reset per second.
PAECMD/s	Number of PAE commands per second. This statistic applies to only paths.
PAECP/s	Number of PAE copies per second. This statistic applies to only paths.
SPLTCMD/s	Number of split commands per second. This statistic applies to only paths.
SPLTCP/s	Number of split copies per second. This statistic applies to only paths.

The following table displays the interactive commands you can use with the storage device panel.

Table 7-12. Storage Device Panel Interactive Commands

Command	Description
`e`	Expand or roll up storage world statistics. This command allows you to view storage resource utilization statistics separated by individual worlds belonging to an expanded storage device. You are prompted for the device name. The statistics are per world per device.
`P`	Expand or roll up storage path statistics. This command allows you to view storage resource utilization statistics separated by individual paths belonging to an expanded storage device. You are prompted for the device name.
`t`	Expand or roll up storage partition statistics. This command allows you to view storage resource utilization statistics separated by individual partitions belonging to an expanded storage device. You are prompted for the device name.
`r`	Sort by READS/s column.
`w`	Sort by WRITES/s column.
`R`	Sort by MBREAD/s column.
`T`	Sort by MBWRTN column.
`N`	Sort first by DEVICE column, then by PATH, WORLD, and PARTITION column. This is the default sort order.
`L`	Changes the displayed length of the DEVICE column.

Virtual Machine Storage Panel

This panel displays virtual machine-centric storage statistics.

By default, statistics are aggregated on a per-resource-pool basis. One virtual machine has one corresponding resource pool, so the panel displays statistics on a per-virtual-machine basis. You can also view statistics on per-VSCSI-device basis.

Table 7-13. Virtual Machine Storage Panel Statistics

Column	Description
ID	Resource pool ID or VSCSI ID of VSCSI device.
GID	Resource pool ID.
VMNAME	Name of the resource pool.
VSCSINAME	Name of the VSCSI device.
NDK	Number of VSCSI devices
CMDS/s	Number of commands issued per second.
READS/s	Number of read commands issued per second.
WRITES/s	Number of write commands issued per second.
MBREAD/s	Megabytes read per second.
MBWRTN/s	Megabytes written per second.
LAT/rd	Average latency (in milliseconds) per read.
LAT/wr	Average latency (in milliseconds) per write.

The following table lists the interactive commands you can use with the virtual machine storage panel.

Table 7-14. Virtual Machine Storage Panel Interactive Commands

Command	Description
`e`	Expand or roll up storage VSCSI statistics. Allows you to view storage resource utilization statistics broken down by individual VSCSI devices belonging to a group. You are prompted to enter the group ID. The statistics are per VSCSI device.
`r`	Sort by READS/s column.
`w`	Sort by WRITES/s column.
`R`	Sort by MBREAD/s column.
`T`	Sort by MBWRTN/s column.
`N`	Sort first by VMNAME column, and then by VSCSINAME column. This is the default sort order.

Network Panel

The Network panel displays server-wide network utilization statistics.

Statistics are arranged by port for each virtual network device configured. For physical network adapter statistics, see the row in the table that corresponds to the port to which the physical network adapter is connected. For statistics on a virtual network adapter configured in a particular virtual machine, see the row corresponding to the port to which the virtual network adapter is connected.

Table 7-15. Network Panel Statistics

Column	Description
PORT-ID	Virtual network device port ID.
UPLINK	Y means the corresponding port is an uplink. N means it is not.
UP	Y means the corresponding link is up. N means it is not.
SPEED	Link speed in Megabits per second.
FDUPLX	Y means the corresponding link is operating at full duplex. N means it is not.
USED-BY	Virtual network device port user.
DTYP	Virtual network device type. H means HUB and S means switch.

Table 7-15. Network Panel Statistics (Continued)

Column	Description
DNAME	Virtual network device name.
PKTTX/s	Number of packets transmitted per second.
PKTRX/s	Number of packets received per second.
MbTX/s	MegaBits transmitted per second.
MbRX/s	MegaBits received per second.
%DRPTX	Percentage of transmit packets dropped.
%DRPRX	Percentage of receive packets dropped.
TEAM-PNIC	Name of the physical NIC used for the team uplink.
PKTTXMUL/s	Number of multicast packets transmitted per second.
PKTRXMUL/s	Number of multicast packets received per second.
PKTTXBRD/s	Number of broadcast packets transmitted per second.
PKTRXBRD/s	Number of broadcast packets received per second.

The following table displays the interactive commands you can use with the network panel.

Table 7-16. Network Panel Interactive Commands

Command	Description
`T`	Sorts by Mb Tx column.
`R`	Sorts by Mb Rx column.
`t`	Sorts by Packets Tx column.
`r`	Sorts by Packets Rx column.
`N`	Sorts by PORT-ID column. This is the default sort order.
`L`	Changes the displayed length of the DNAME column.

Interrupt Panel

The interrupt panel displays information about the use of interrupt vectors.

Table 7-17. Interrupt Panel Statistics

Column	Description
VECTOR	Interrupt vector ID.
COUNT/s	Total number of interrupts per second. This value is cumulative of the count for every CPU.
COUNT_x	Interrupts per second on CPU x.
TIME/int	Average processing time per interrupt (in microseconds).
TIME_x	Average processing time per interrupt on CPU x (in microseconds).
DEVICES	Devices that use the interrupt vector. If the interrupt vector is not enabled for the device, its name is enclosed in angle brackets (< and >).

Using Batch Mode

Batch mode allows you to collect and save resource utilization statistics in a file.

After you prepare for batch mode, you can use `esxtop` or `resxtop` in this mode.

Prepare for Batch Mode

To run in batch mode, you must first prepare for batch mode.

Procedure

1 Run `resxtop` (or `esxtop`) in interactive mode.

2 In each of the panels, select the columns you want.

3 Save this configuration to a file (by default `~/.esxtop50rc`) using the `W` interactive command.

You can now use `resxtop` (or `esxtop`) in batch mode.

Use esxtop or resxtop in Batch Mode

After you have prepared for batch mode, you can use `esxtop` or `resxtop` in this mode.

Procedure

1 Start `resxtop` (or `esxtop`) to redirect the output to a file.

For example:

```
esxtop –b > my_file.csv
```

The filename must have a `.csv` extension. The utility does not enforce this, but the post-processing tools require it.

2 Process statistics collected in batch mode using tools such as Microsoft Excel and Perfmon.

In batch mode, `resxtop` (or `esxtop`) does not accept interactive commands. In batch mode, the utility runs until it produces the number of iterations requested (see command-line option `n`, below, for more details), or until you end the process by pressing Ctrl+c.

Batch Mode Command-Line Options

You can use batch mode with command-line options.

Table 7-18. Command-Line Options in Batch Mode

Option	Description
`a`	Show all statistics. This option overrides configuration file setups and shows all statistics. The configuration file can be the default `~/.esxtop50rc` configuration file or a user-defined configuration file.
`b`	Runs `resxtop` (or `esxtop`) in batch mode.
`c` *filename*	Load a user-defined configuration file. If the `–c` option is not used, the default configuration filename is ~/.esxtop41rc. Create your own configuration file, specifying a different filename, using the `W` single-key interactive command.
`d`	Specifies the delay between statistics snapshots. The default is five seconds. The minimum is two seconds. If a delay of less than two seconds is specified, the delay is set to two seconds.
`n`	Number of iterations. `resxtop` (or `esxtop`) collects and saves statistics this number of times, and then exits.
`server`	The name of the remote server host to connect to (required, `resxtop` only).
`vihost`	If you connect indirectly (through vCenter Server), this option should contain the name of the ESXi host you connect to. If you connect directly to the ESXi host, this option is not used. Note that the host name needs to be the same as what appears in the vSphere Client.

Table 7-18. Command-Line Options in Batch Mode (Continued)

Option	Description
portnumber	The port number to connect to on the remote server. The default port is 443, and unless this is changed on the server, this option is not needed. (resxtop only)
username	The user name to be authenticated when connecting to the remote host. You are prompted by the remote server for a password, as well (resxtop only).

Using Replay Mode

In replay mode, esxtop replays resource utilization statistics collected using vm-support.

After you prepare for replay mode, you can use esxtop in this mode. See the vm-support man page.

In replay mode, esxtop accepts the same set of interactive commands as in interactive mode and runs until no more snapshots are collected by vm-support to be read or until the requested number of iterations are completed.

Prepare for Replay Mode

To run in replay mode, you must prepare for replay mode.

Procedure

1 Run vm-support in snapshot mode in the ESXi Shell.

Use the following command.

```
vm-support -S -d duration -I interval
```

2 Unzip and untar the resulting tar file so that esxtop can use it in replay mode.

You can now use esxtop in replay mode.

Use esxtop in Replay Mode

You can use esxtop in replay mode.

Replay mode can be run to produce output in the same style as batch mode (see the command-line option b, below).

NOTE Batch output from esxtop cannot be played back by resxtop.

Snapshots collected by vm-supported can be replayed by esxtop. However, vm-support output generated by ESXi can be replayed only by esxtop running on the same version of ESXi.

Procedure

- To activate replay mode, enter the following at the command-line prompt.

```
esxtop -R vm-support_dir_path
```

Replay Mode Command-Line Options

You can use replay mode with command-line options.

The following table lists the command-line options available for esxtop replay mode.

Table 7-19. Command-Line Options in Replay Mode

Option	Description
`R`	Path to the vm-support collected snapshot's directory.
`a`	Show all statistics. This option overrides configuration file setups and shows all statistics. The configuration file can be the default `~/.esxtop50rc` configuration file or a user-defined configuration file.
`b`	Runs `esxtop` in Batch mode.
`c` *filename*	Load a user-defined configuration file. If the `–c` option is not used, the default configuration filename is ~/.esxtop50rc. Create your own configuration file and specify a different filename using the `W` single-key interactive command.
`d`	Specifies the delay between panel updates. The default is five seconds. The minimum is two seconds. If a delay of less than two seconds is specified, the delay is set to two seconds.
`n`	Number of iterations `esxtop` updates the display this number of times and then exits.

Monitoring Networked Devices with SNMP and vSphere

8

Simple Network Management Protocol (SNMP) allows management programs to monitor and control a variety of networked devices.

Managed systems run SNMP agents, which can provide information to a management program in at least one of the following ways:

- In response to a `GET` operation, which is a specific request for information from the management system.
- By sending a trap, which is an alert sent by the SNMP agent to notify the management system of a particular event or condition.

Optionally, you can configure ESXi hosts to convert CIM indications to SNMP traps, allowing this information to be received by SNMP monitoring systems.

Management Information Base (MIB) files define the information that can be provided by managed devices. The MIB files contain object identifiers (OIDs) and variables arranged in a hierarchy.

vCenter Server and ESXi have SNMP agents. The agent provided with each product has differing capabilities.

This chapter includes the following topics:

Using SNMP Traps with vCenter Server

The SNMP agent included with vCenter Server can be used to send traps when the vCenter Server system is started and when an alarm is triggered on vCenter Server. The vCenter Server SNMP agent functions only as a trap emitter and does not support other SNMP operations, such as `GET`.

The traps sent by vCenter Server are typically sent to other management programs. You must configure your management server to interpret the SNMP traps sent by vCenter Server.

To use the vCenter Server SNMP traps, configure the SNMP settings on vCenter Server and configure your management client software to accept the traps from vCenter Server.

The traps sent by vCenter Server are defined in `VMWARE-VC-EVENT-MIB.mib`. See "VMWARE-VC-EVENT-MIB," on page 76.

Configure SNMP Settings for vCenter Server

To use SNMP with vCenter Server, you must configure SNMP settings using the vSphere Client.

Prerequisites

To complete the following task, the vSphere Client must be connected to a vCenter Server. In addition, you need the DNS name and IP address of the SNMP receiver, the port number of the receiver, and the community identifier.

Procedure

1 Select **Administration > vCenter Server Settings**.

2 If the vCenter Server is part of a connected group, in **Current vCenter Server**, select the appropriate server.

3 Click **SNMP** in the navigation list.

4 Enter the following information for the **Primary Receiver** of the SNMP traps.

Option	Description
Receiver URL	The DNS name or IP address of the SNMP receiver.
Receiver port	The port number of the receiver to which the SNMP agent sends traps. If the port value is empty, vCenter Server uses the default port, **162**.
Community	The community identifier.

5 (Optional) Enable additional receivers in the **Enable Receiver 2**, **Enable Receiver 3**, and **Enable Receiver 4** options.

6 Click **OK**.

The vCenter Server system is now ready to send traps to the management system you have specified.

What to do next

Configure your SNMP management software to receive and interpret data from the vCenter Server SNMP agent. See "Configure SNMP Management Client Software," on page 65.

Configure SNMP for ESXi

ESXi includes an SNMP agent embedded in hostd that can both send traps and receive polling requests such as `GET` requests. This agent is referred to as the embedded SNMP agent.

By default, the embedded SNMP agent is disabled. To enable it, you must configure it using the vSphere CLI command `vicfg-snmp`.

Prerequisites

SNMP configuration for ESXi requires the vSphere Command-Line Interface. See *Getting Started with vSphere Command-Line Interfaces*.

Procedure

1 Configure SNMP Communities on page 63

Before you enable the ESXi embedded SNMP agent, you must configure at least one community for the agent.

2 Configure the SNMP Agent to Send Traps on page 63

You can use the ESXi embedded SNMP agent to send virtual machine and environmental traps to management systems. To configure the agent to send traps, you must specify a target address and community.

3 Configure the SNMP Agent for Polling on page 64

If you configure the ESXi embedded SNMP agent for polling, it can listen for and respond to requests from SNMP management client systems, such as `GET` requests.

4 Configure the Source used by the SNMP Agent for Hardware Events on page 64

You can configure the ESXi embedded SNMP agent to receive hardware events either from IPMI sensors or CIM indications.

5 Configure the SNMP Agent to Filter Traps on page 65

You can configure the ESXi embedded SNMP agent to filter out traps if you don't want your SNMP management software to receive those traps.

6 Configure SNMP Management Client Software on page 65

After you have configured a vCenter Server system or a host to send traps, you must configure your management client software to receive and interpret those traps.

Configure SNMP Communities

Before you enable the ESXi embedded SNMP agent, you must configure at least one community for the agent.

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

Prerequisites

SNMP configuration for ESXi requires the vSphere Command-Line Interface. See *Getting Started with vSphere Command-Line Interfaces*.

Procedure

- From the vSphere CLI, type
  `vicfg-snmp.pl --server hostname --username username --password password -c com1`.

  Replace *com1* with the community name you wish to set. Each time you specify a community with this command, the settings you specify overwrite the previous configuration. To specify multiple communities, separate the community names with a comma.

  For example, to set the communities public and internal on the host host.example.com, you might type **`vicfg-snmp.pl --server host.example.com --username user --password password -c public, internal`**.

Configure the SNMP Agent to Send Traps

You can use the ESXi embedded SNMP agent to send virtual machine and environmental traps to management systems. To configure the agent to send traps, you must specify a target address and community.

To send traps with the SNMP agent, you must configure the target (receiver) address, community, and an optional port. If you do not specify a port, the SNMP agent sends traps to UDP port 162 on the target management system by default.

Prerequisites

SNMP configuration for ESXi requires the vSphere Command-Line Interface. See *Getting Started with vSphere Command-Line Interfaces*.

Procedure

1 From the vSphere CLI, type
vicfg-snmp.pl --server *hostname* --username *username* --password *password* -t *target_address@port/community*.

Replace *target_address*, *port*, and *community* with the address of the target system, the port number to send the traps to, and the community name, respectively. Each time you specify a target with this command, the settings you specify overwrite all previously specified settings. To specify multiple targets, separate them with a comma.

For example, to send SNMP traps from the host host.example.com to port 162 on target.example.com using the public community, type
vicfg-snmp.pl --server host.example.com --username user --password password -t target.example.com@162/public.

2 (Optional) If the SNMP agent is not enabled, enable it by typing
vicfg-snmp.pl --server *hostname* --username *username* --password *password* --enable.

3 (Optional) Send a test trap to verify that the agent is configured correctly by typing
vicfg-snmp.pl --server *hostname* --username *username* --password *password* --test.

The agent sends a `warmStart` trap to the configured target.

Configure the SNMP Agent for Polling

If you configure the ESXi embedded SNMP agent for polling, it can listen for and respond to requests from SNMP management client systems, such as `GET` requests.

By default, the embedded SNMP agent listens on UDP port 161 for polling requests from management systems. You can use the `vicfg-snmp` command to configure an alternative port. To avoid conflicting with other services, use a UDP port that is not defined in `/etc/services`.

Prerequisites

SNMP configuration for ESXi requires the vSphere Command-Line Interface. See *Getting Started with vSphere Command-Line Interfaces*.

Procedure

1 From the vSphere CLI, type
vicfg-snmp.pl --server *hostname* --username *username* --password *password* -p *port*.

Replace *port* with the port for the embedded SNMP agent to use for listening for polling requests.

2 (Optional) If the SNMP agent is not enabled, enable it by typing
vicfg-snmp.pl --server *hostname* --username *username* --password *password* --enable.

Configure the Sourceused by the SNMP Agentfor Hardware Events

You can configure the ESXi embedded SNMP agent to receive hardware events either from IPMI sensors or CIM indications.

IPMI sensors were used for hardware monitoring in ESX/ESXi 4.x and earlier. The conversion of CIM indications to SNMP notifications is newly available in ESXi 5.0.

Prerequisites

SNMP configuration for ESXi requires the vSphere Command-Line Interface. See *Getting Started with vSphere Command-Line Interfaces*.

Procedure

1 From the vSphere CLI, configure the source for hardware events.

Option	Command
IPMI sensors	`vicfg-snmp.pl --server hostname --username username --password password -y sensors`
CIM indications	`vicfg-snmp.pl --server hostname --username username --password password -y indications`

2 (Optional) If the SNMP agent is not enabled, enable it by typing
`vicfg-snmp.pl --server hostname --username username --password password --enable`.

Configure the SNMP Agent to Filter Traps

You can configure the ESXi embedded SNMP agent to filter out traps if you don't want your SNMP management software to receive those traps.

Prerequisites

SNMP configuration for ESXi requires the vSphere Command-Line Interface. See *Getting Started with vSphere Command-Line Interfaces*.

Procedure

1 From the vSphere CLI,
`vicfg-snmp.pl --server hostname --username username --password password -n oid_list`

oid_list is a list of OIDs for the traps to filter, separated by commas. This list replaces any OIDs that were previously specificed using this command.

For example, to filter out coldStart (OID 1.3.6.1.4.1.6876.4.1.1.0) and warmStart (OID 1.3.6.1.4.1.6876.4.1.1.1) traps, type
`vicfg-snmp.pl --server hostname --username username --password password -n 1.3.6.1.4.1.6876.4.1.1.0,1.3.6.1.4.1.6876.4.1.1.1` .

2 (Optional) If the SNMP agent is not enabled, enable it by typing
`vicfg-snmp.pl --server hostname --username username --password password --enable`.

The traps identified by the specified OIDs are filtered out of the output of the SNMP agent, and are not sent to SNMP management software.

What to do next

To clear all trap filters,
type`vicfg-snmp.pl --server hostname --username username --password password -n reset`.

Configure SNMP Management Client Software

After you have configured a vCenter Server system or a host to send traps, you must configure your management client software to receive and interpret those traps.

To configure your management client software, specify the communities for the managed device, configure the port settings, and load the VMware MIB files. See the documentation for your management system for specific instructions for these steps.

Prerequisites

To complete this task, download the VMware MIB files from the VMware Web site: http://communities.vmware.com/community/developer/managementapi.

Procedure

1 In your management software, specify the vCenter Server or host as an SNMP-based managed device.

2 Set up appropriate community names in the management software.

These names must correspond to the communities set for the SNMP agent on the vCenter Server system or host.

3 (Optional) If you configured the SNMP agent to send traps to a port on the management system other than the default UDP port 162, configure the management client software to listen on the port you configured.

4 Load the VMware MIBs into the management software so you can view the symbolic names for the vCenter Server or host variables.

To prevent lookup errors, load the MIB files in the following order:

a `VMWARE-ROOT-MIB.mib`

b `VMWARE-TC-MIB.mib`

c `VMWARE-PRODUCTS-MIB.mib`

d `VMWARE-SYSTEM-MIB.mib`

e `VMWARE-ENV-MIB.mib`

f `VMWARE-RESOURCES-MIB.mib`

g `VMWARE-VMINFO-MIB.mib`

h `VMWARE-OBSOLETE-MIB.mib` (for use with versions of ESX/ESXi prior to 4.0)

i `VMWARE-AGENTCAP-MIB.mib`

j `VMWARE-VC-EVENT-MIB.mib`

The management software can now receive and interpret traps from vCenter Server or hosts.

SNMP Diagnostics

You can use SNMP tools to diagnose configuration problems.

- Type **`vicfg-snmp.pl --server`** ***`hostname`*** **`--username`** ***`username`*** **`--password`** ***`password`*** **`--test`** at the vSphere command-line interface to prompt the embedded SNMP agent to send a test `warmStart` trap.
- Type **`vicfg-snmp.pl --server`** ***`hostname`*** **`--username`** ***`username`*** **`--password`** ***`password`*** **`--show`** to display the current configuration of the embedded SNMP agent.
- The `SNMPv2-MIB.mib` file provides a number of counters to aid in debugging SNMP problems. See "SNMPv2 Diagnostic Counters," on page 79.
- The `VMWARE-AGENTCAP-MIB.mib` file defines the capabilities of the VMware SNMP agents by product version. Use this file to determine if the SNMP functionality that you want to use is supported.

Using SNMP with Guest Operating Systems

You can use SNMP to monitor guest operating systems or applications running in virtual machines.

The virtual machine uses its own virtual hardware devices. Do not install agents in the virtual machines that are intended to monitor physical hardware.

Procedure

- Install the SNMP agents you normally would use for that purpose in the guest operating systems.

VMware MIB Files

VMware MIB files define the information provided by ESXi hosts and vCenter Server to SNMP management software.

You can download these MIB files from http://communities.vmware.com/community/developer/forums/managementapi#http://communities.vmware.com/community/developer/forums/managementapi/SNMP-MIB.

Table 8-1 lists the MIB files provided by VMware and describes the information that each file provides.

Table 8-1. VMware MIB Files

MIB File	Description
VMWARE-ROOT-MIB.mib	Contains VMware's enterprise OID and top level OID assignments.
VMWARE-AGENTCAP-MIB.mib	Defines the capabilities of the VMware agents by product versions.
VMWARE-CIMOM-MIB.mib	Defines variables and trap types used to report on the state of the CIM Object Management subsystem.
VMWARE-ENV-MIB.mib	Defines variables and trap types used to report on the state of physical hardware components of the host computer. Enables conversion of CIM indications to SNMP traps.
VMWARE-OBSOLETE-MIB.mib	Defines OIDs that have been made obsolete to maintain backward compatibility with earlier versions of ESX/ESXi. Includes variables formerly defined in the files VMWARE-TRAPS-MIB.mib and VMWARE-VMKERNEL-MIB.mib.
VMWARE-PRODUCTS-MIB.mib	Defines OIDs to uniquely identify each SNMP agent on each VMware platform by name, version, and build platform.
VMWARE-RESOURCES-MIB.mib	Defines variables used to report information on resource usage of the VMkernel, including physical memory, CPU, and disk utilization.
VMWARE-SYSTEM-MIB.mib	The VMWARE-SYSTEM-MIB.mib file is obsolete. Use the SNMPv2-MIB to obtain information from sysDescr.0 and sysObjec ID.0.
VMWARE-TC-MIB.mib	Defines common textual conventions used by VMware MIB files.
VMWARE-VC-EVENTS-MIB.mib	Defines traps sent by vCenter Server. Load this file if you use vCenter Server to send traps.
VMWARE-VMINFO-MIB.mib	Defines variables for reporting information about virtual machines, including virtual machine traps.

Table 8-2 lists MIB files included in the VMware MIB files package that are not created by VMware. These can be used with the VMware MIB files to provide additional information.

Table 8-2. Other MIB Files

MIB File	Description
HOST-RESOURCES-MIB.mib	Defines objects that are useful for managing host computers.
HOST-RESOURCES-TYPES.mib	Defines storage, device, and filesystem types for use with HOST-RESOURCES-MIB.mib.
IF-MIB.mib	Defines attributes related to physical NICs on the host system.
SNMPv2-CONF.mib	Defines conformance groups for MIBs.
SNMPv2-MIB.mib	Defines the SNMP version 2 MIB objects.
SNMPv2-SMI.mib	Defines the Structure of Managment Information for SNMP version 2.
SNMPv2-TC.mib	Defines textual conventions for SNMP version 2.

VMWARE-ROOT-MIB

The VMWARE-ROOT-MIB.mib file defines the VMware enterprise OID and top level OID assignments.

Table 8-3 lists the identification mapping defined in VMWARE-ROOT-MIB.mib.

Table 8-3. Definition Mapping for VMWARE-ROOT-MIB.mib

Label	Identification Mapping
vmware	enterprises 6876
vmwSystem	vmware 1
vmwVirtMachines	vmware 2
vmwResources	vmware 3
vmwProductSpecific	vmware 4
vmwLdap	vmware 40
vmwTraps	vmware 50
vmwOID	vmware 60
vmwareAgentCapabilities	vmware 70
vmwExperimental	vmware 700
vmwObsolete	vmware 800

VMWARE-CIMOM-MIB

The VMWARE-CIMOM-MIB.mib file defines traps for reporting information about the CIM object manager subsystem.

Table 8-4 lists the traps defined in VMWARE-CIMOM-MIB.mib.

Table 8-4. VMWARE-CIMOM-MIB Trap Definitions

Trap	Description
vmwCimOmHeartbeat	This notification, if the agent is so configured, will be sent periodically to indicate that CIM object manager indication delivery is functioning.

VMWARE-ENV-MIB

The VMWARE-ENV-MIB.mib defines variables and trap types used to report on the state of physical components of the host computer.

This file also includes definitions that allow indications from CIM providers on ESXi hosts to be converted to SNMP traps.

Table 8-5 lists the traps defined in VMWARE-ENV-MIB.mib.

Table 8-5. Traps Defined in VMWARE-ENV-MIB

Trap	Description
vmwEnvHardwareEvent	This trap is sent when an ESXi host has detected a material change in the physical condition of the hardware. This trap has been deprecated.
vmwESXEnvHardwareEvent	This trap is sent when an ESX host has detected a material change in the physical condition of the hardware. This trap has been deprecated.

Table 8-5. Traps Defined in VMWARE-ENV-MIB (Continued)

Trap	Description
vmwESXEnvHardwareAlert	A hardware alert as received from the Common Infrastructure Management (CIM) subsystem on this system.
vmwESXEnvBatteryAlert	A battery alert as received from the Common Infrastructure Management (CIM) subsystem on this system.
vmwESXEnvChassisAlert	A chassis alert as received from the Common Infrastructure Management (CIM) subsystem on this system.
vmwESXEnvThermalAlert	A cooling/thermal alert as received from the Common Infrastructure Management (CIM) subsystem on this system.
vmwESXEnvDiskAlert	A disk drive alert as received from the Common Infrastructure Management (CIM) subsystem on this system.
vmwESXEnvPowerAlert	A power suppply alert as received from the Common Infrastructure Management (CIM) subsystem on this system.
vmwESXEnvProcessorAlert	An IPMI processor alert as received from the Common Infrastructure Management (CIM) subsystem on this system.
vmwESXEnvMemoryAlert	An IPMI memory alert as received from the Common Infrastructure Management (CIM) subsystem on this system.
vmwESXEnvBIOSAlert	A BIOS System Event Log alert as received from the Common Infrastructure Management (CIM) subsystem on this system.

Table 8-6 lists the variables defined in `VMWARE-ENV-MIB.mib`.

Table 8-6. Variable Definitions in VMWARE-ENV-MIB

Variable	ID Mapping	Description
vmwEnv	vmwProductSpecific 20	Defines the OID root for this MIB module.
vmwESXNotifications	vmwESX 0	Parent of all ESXi-specific notifications.
vmwEnvNumber	vmwEnv 1	Number of conceptual rows in `vmwEnvTable`.
vmwEnvLastChange	vmwEnv 2	The value of `sysUptime` when a conceptual row was last added to or deleted from `vmwEnvTable`.
vmwEnvTable	vmwEnv 3	This table is populated by monitoring subsystems such as IPMI.
vmwEnvEntry	vmwEnvTable 1	One entry is created in the table for each physical component reporting its status toESXi.
vmwEnvIndex	vmwEnvEntry 1	A unique identifier for the physical component. This identifier does not persist across management restarts.
vmwSubsystemType	vmwEnvEntry 2	The type of hardware component that is reporting its environmental state.
vmwHardwareStatus	vmwEnvEntry 3	The last reported status of the component.
vmwEventDescription	vmwEnvEntry 4	A description of the last reported event for this hardware component.
vmwEnvHardwareTime	vmwEnvEntry 5	The value of `sysUptime` when `vmwHardwareStatus` was reported.
vmwEnvSource	vmwEnv 100	The source used to obtain the hardware state.

Table 8-6. Variable Definitions in VMWARE-ENV-MIB (Continued)

Variable	ID Mapping	Description
vmwEnvInIndications	vmwEnv 101	The number of HTTP POST msgs containing CIM Indications in XML as received by the agent.
vmwEnvLastIn	vmwEnv 102	The value of sysUptime when the agent last received an indication.
vmwEnvOutNotifications	vmwEnv 103	The number of traps sent that originated as CIM indications.
vmwEnvInErrs	vmwEnv 104	The number of CIM indications that agent did not complete receipt of.
vmwEnvIndOidErrs	vmwEnv 105	The number of CIM indications having a MappingString qualifier for which the value was not a valid OID.
vmwEnvCvtValueErrs	vmwEnv 106	The number of CIM indication properties having a MappingString qualifier for which the CIM value for the given CIM type could not be converted.
vmwEnvCvtSyntaxErrs	vmwEnv 107	The number of CIM indication properties having a MappingString qualifier for which the CIM type could not be converted to SMI syntax.
vmwEnvCvtOidErrs	vmwEnv 108	The number of CIM indication properties having a MappingString qualifier for which the the OID was not valid.
vmwEnvGetClassErrs	vmwEnv 109	The number of CIM GetClass operations over a given CIM indication class and namespace could not be completed (timeout) or returned error.
vmwEnvPropertySkips	vmwEnv 110	Number of CIM indications having properties which do not have a MappingString qualifier in the class definition and were not converted.
vmwEnvIndicationSkips	vmwEnv 111	Number of CIM indications recieved for which GetClass reported no MappingStrings qualifier and were not converted to a notification.
vmwEnvCIM	vmwProductSpecific 30	Defines root object for notifications from CIM indcations.
vmwEnvDescription	vmwEnvCIM 1	A short description of the CIM indication.
vmwEnvEventTime	vmwEnvCIM 2	The time and date that the underlying event was first detected.
vmwEnvIndicationTime	vmwEnvCIM 3	The time and date that the indication received by the SNMP agent was created.
vmwEnvPerceivedSeverity	vmwEnvCIM 4	An enumerated value that describes the serverity of the indication from the notifier's point of view.
vmwEnvAlertType	vmwEnvCIM 5	The primary classification of the indication.

Table 8-6. Variable Definitions in VMWARE-ENV-MIB (Continued)

Variable	ID Mapping	Description
vmwEnvSysCreationClassName	vmwEnvCIM 6	The scoping system's CreationClassName for the provider generating this indication.
vmwEnvAlertingElement	vmwEnvCIM 7	The identifying information of the entity for which this notification was generated.
vmwEnvAlertingFormat	vmwEnvCIM 8	The format of the AlertingManagedElement property is interpretable based upon the value of this property.
vmwEnvSystemName	vmwEnvCIM 9	The scoping system's name for the provider generating this message.
vmwEnvProviderName	vmwEnvCIM 10	The name of the CIM provider, a software module loaded into the CIM subsystem, generating this message.

VMWARE-OBSOLETE-MIB

The VMWARE–OBSOLETE–MIB.mib file contains all previously published managed objects that have been made obsolete. This file is provided to maintain compatibility with older versions of ESX/ESXi.

The variables defined in this file were originally defined in previous versions of the VMWARE–RESOURCES–MIB.mib and VMWARE–TRAPS–MIB.mib files. Table 8-7 lists the variables defined in VMWARE–OBSOLETE–MIB.mib.

Table 8-7. Variables Defined in VMWARE-OBSOLETE-MIB

Variable	ID Mapping	Description
Obsolete variables originally from VMWARE-RESOURCES-MIB		
vmwResources	vmware 3	
vmwCPU	vmwResources 1	Defines the root OID for the subtree of variables used to report CPU information.
vmwCpuTable	vmwCPU 2	A table of CPU usage by each virtual machine.
vmwCpuEntry	vmwCpuTable 1	An entry in cpuTable that records CPU usage for a single virtual machine.
vmwCpuVMID	vmwCpuEntry 1	The identification number allocated to the virtual machine by the VMkernel.
vmwCpuShares	vmwCpuEntry 2	The share of the CPU allocated to the virtual machine by the VMkernel.
vmwCpuUtil	vmwCpuEntry 3	Amount of time the virtual machine has been running on the CPU (in seconds).
vmwMemTable	vmwMemory 4	A table of memory usage by each virtual machine.
vmwMemEntry	vmwMemTable 1	An entry in memTable that records memory usage by a single virtual machine.
vmwMemVMID	vmwMemEntry 1	The identification number allocated to the virtual machine by the VMkernel.
vmwMemShares	vmwMemEntry 2	The shares of memory allocated to the virtual machine by the VMkernel.

Table 8-7. Variables Defined in VMWARE-OBSOLETE-MIB (Continued)

Variable	ID Mapping	Description
vmwMemConfigured	vmwMemEntry 3	The amount of memory the virtual machine was configured with (in KB).
vmwMemUtil	vmwMemEntry 4	The amount of memory currently used by the virtual machine (in KB).
vmwHBATable	vmwResources 3	A table used for reporting disk adapter and target information.
vmwHBAEntry	vmwHBATable 1	A record for a single HBA connected to the host machine.
vmwHbaIdx	vmwHBAEntry 1	Index for the HBA table.
vmwHbaName	vmwHBAEntry 2	A string describing the disk. Format: <devname#>:<tgt>:<lun>.
vmwHbaVMID	vmwHBAEntry 3	The identification number allocated to the running virtual machine by the VMkernel.
vmwDiskShares	vmwHBAEntry 4	Share of disk bandwidth allocated to this virtual machine.
vmwNumReads	vmwHBAEntry 5	Number of reads to this disk since the disk module was loaded.
vmwKbRead	vmwHBAEntry 6	Kilobytes read from this disk since the disk module was loaded.
vmwNumWrites	vmwHBAEntry 7	Number of writes to this disk since the disk module was loaded.
vmwKbWritten	vmwHBAEntry 8	Number of kilobytes written to this disk since the disk module was loaded.
vmwNetTable	vmwResources 4	A table used for reporting network adapter statistics.
vmwNetEntry	vmwNetTable 1	A record for a single network adapter on the virtual machine.
vmwNetIdx	vmwNetEntry 1	Index for the network table.
vmwNetName	vmwNetEntry 2	A string describing the network adapter.
vmwNetVMID	vmwNetEntry 3	The identification number allocated to the running virtual machine by the VMkernel.
vmwNetIfAddr	vmwNetEntry 4	The MAC address of the virtual machine's virtual network adapter.
vmwNetShares	vmwNetEntry 5	Share of network bandwidth allocate d to this virtual machine. This object has not been implemented.
vmwNetPktsTx	vmwNetEntry 6	The number of packets transmitted on this network adapter since the network module was loaded. Deprecated in favor of vmwNetHCPktsTx.
vmwNetKbTx	vmwNetEntry 7	The number of kilobytes sent from this network adapter since the network module was loaded. Deprecated in favor of vmwNetHCKbTx.

Table 8-7. Variables Defined in VMWARE-OBSOLETE-MIB (Continued)

Variable	ID Mapping	Description
vmwNetPktsRx	vmwNetEntry 8	The number of packets received on this network adapter since the network module was loaded. Deprecated in favor of vmwNetHCPktsRx.
vmwNetKbRx	vmwNetEntry 9	The number of kilobytes received on this network adapter since the network module was loaded. Deprecated in favor of vmwNetHCKbRx
vmwNetHCPktsTx	vmwNetEntry 10	The number of packets transmitted on this network adapter since the network module was loaded. This counter is the 64-bit version of vmwNetPktsTx.
vmwNetHCKbTx	vmwNetEntry 11	The number of kilobytes sent from this network adapter since the network module was loaded. This counter is the 64-bit version of vmwNetKbTx.
vmwNetHCPktsRx	vmwNetEntry 12	The number of packets received on this network adapter since the network module was loaded. This counter is the 64-bit version of vmwNetPktsRx.
vmwNetHCKbRx	vmwNetEntry 13	The number of kilobytes received on this network adapter since the network module was loaded. This counter is the 64-bit version of vmwNetKbRx.
Obsolete variables originally defined in VMWARE-TRAPS-MIB		
vmID	vmwTraps 101	The ID of the affected virtual machine generating the trap. If there is no virtual machine ID (for example, if the virtual machine has been powered off), the vmID is -1.
vmConfigFile	vmwTraps 102	The configuration file of the virtual machine generating the trap.
vpxdTrapType	vmwTraps 301	The trap type of the vCenter Server trap.
vpxdHostName	vmwTraps 302	The name of the affected host.
vpxdVMName	vmwTraps 303	The name of the affected virtual machine.
vpxdOldStatus	vmwTraps 304	The prior status.
vpxdNewStatus	vmwTraps 305	The new status.
vpxdObjValue	vmwTraps 306	The object value.

Table 8-8 lists the traps defined in VMWARE–OBSOLETE–MIB.mib. These traps were originally defined in VMWARE–TRAPS–MIB.mib.

Table 8-8. Traps Defined in VMWARE-OBSOLETE-MIB

Trap	Description
ESX/ESXi Traps	
vmPoweredOn	This trap is sent when a virtual machine is powered on from a suspended or powered off state.
vmPoweredOff	This trap is sent when a virtual machine is powered off.

Table 8-8. Traps Defined in VMWARE-OBSOLETE-MIB (Continued)

Trap	Description
vmHBLost	This trap is sent when a virtual machine detects a loss in guest heartbeat. VMware Tools must be installed in the guest operating system in order for this value to be valid.
vmHBDetected	This trap is sent when a virtual machine detects or regains the guest heartbeat. VMware Tools must be installed in the guest operating system in order for this value to be valid.
vmSuspended	This trap is sent when a virtual machine is suspended.
vCenter Server Traps	
vpxdTrap	This trap is sent when an entity status has changed.

VMWARE-PRODUCTS-MIB

The VMWARE-PRODUCTS-MIB.mib file defines OIDs to uniquely identify each SNMP agent on each VMware platform.

Table 8-9 lists identification mappings defined in VMWARE-PRODUCTS-MIB.mib.

Table 8-9. Identification Mappings for VMWARE-PRODUCTS-MIB.mib

Label	Identification Mapping
oidESX	vmwOID 1
vmwESX	vmwProductSpecific 1
vmwDVS	vmwProductSpecific 2
vmwVC	vmwProductSpecific 3
vmwServer	vmwProductSpecific 4

VMWARE-RESOURCES-MIB

The VMWARE-RESOURCES-MIB.mib file defines variables used to report information on resource usage.

Table 8-10 lists the identification mappings defined in VMWARE-RESOURCES-MIB.mib.

Table 8-10. Identification Mappings for VMWARE-RESOURCES-MIB

Variable	ID Mapping	Description
CPU Subtree		
vmwCPU	vmwResources 1	Defines the root OID for the subtree of variables used to report CPU information.
vmwNumCPUs	vmwCPU 1	The number of physical CPUs present on the system.
Memory Subtree		
vmwMemory	vmwResources 2	Defines the root OID for the subtree of variables used to report memory information.
vmwMemSize	vmwMemory 1	Amount of physical memory present on the host (in KB).
vmwMemCOS	vmwMemory 2	Amount of physical memory allocated to the service console (in KB). This variable does not apply to ESXi hosts, which do not have a service console.
vmwMemAvail	vmwMemory 3	The amount of memory available to run virtual machines and to allocate to the hypervisor. It is computed by subtracting vmwMemCOS from vmwMemSize.

Table 8-10. Identification Mappings for VMWARE-RESOURCES-MIB (Continued)

Variable	ID Mapping	Description
Storage Subtree		
vmwStorage	vmwResources 5	Defines the root OID for the subtree of variables used to report memory information.
vmwHostBusAdapterNumber	vmwStorage 1	The number of entries in the vmwHostBusAdapterTable.
vmwHostBusAdapterTable	vmwStorage 2	A table of Host Bus Adapters found in this host.
vmwHostBusAdapterEntry	vmwHostBusAdapterTable 1	An entry in the Host Bus Adapter table holding details for a particular adapter.
vmwHostBusAdapterIndex	vmwHostBusAdapterEntry 1	An arbitrary index assigned to this adapter.
vmwHbaDeviceName	vmwHostBusAdapterEntry 2	The system device name for this adapter.
vmwHbaBusNumber	vmwHostBusAdapterEntry 3	The host bus number. For unsupported adapters, returns -1.
vmwHbaStatus	vmwHostBusAdapterEntry 4	The operational status of the adapter.
vmwHbaModelName	vmwHostBusAdapterEntry 5	The model name of the adapter.
vmwHbaDriverName	vmwHostBusAdapterEntry 6	The name of the adapter driver.
vmwHbaPci	vmwHostBusAdapterEntry 7	The PCI ID of the adapter.

VMWARE-SYSTEM-MIB

The `VMWARE-SYSTEM-MIB.mib` file provides variables for identifying the VMware software running on a managed system by product name, version number, and build number.

Table 8-11 lists the variables defined in `VMWARE-SYSTEM-MIB.mib`.

Table 8-11. Variables Defined in VMWARE-SYSTEM-MIB

Variable	ID Mapping	Description
vmwProdName	vmwSystem 1	The product name.
vmwProdVersion	vmwSystem 2	The product version number, in the format *Major.Minor.Update*.
vmwProdBuild	vmwSystem 4	The product build number.

VMWARE-TC-MIB

The `VMWARE-TC-MIB.mib` file provides common textual conventions used by VMware MIB files.

`VMWARE-TC-MIB.mib` defines the following integer values for `VmwSubsystemTypes`:

- unknown(1)
- chassis(2)
- powerSupply(3)
- fan(4)
- cpu(5)
- memory(6)
- battery(7)
- temperatureSensor(8)

- raidController(9)
- voltage(10)

VMWARE-TC-MIB.mib defines the following integer values for VmwSubsystemStatus:

- unknown(1)
- normal(2)
- marginal(3)
- critical(4)
- failed(5)

VMWARE-VC-EVENT-MIB

The VMWARE-VC-EVENT-MIB.mib file provides definitions for traps sent by vCenter Server. These definitions were provided by VMWARE-TRAPS-MIB.mib in earlier versions of VirtualCenter Server.

Table 8-12 lists the traps defined for vCenter Server.

Table 8-12. Alarms Defined in VMWARE-VC-EVENT-MIB

Trap	ID Mapping	Description
vpxdAlarm	vmwVCNotifications 201	The vCenter Server SNMP agent sends this trap when an entity's alarm status changes.
vpxdDiagnostic	vmwVCNotifications 202	The vCenter Server SNMP agent sends this trap when vCenter Server starts or is restarted, or when a test notification is requested. vCenter Server can be configured to send this trap periodically at regular intervals.

Table 8-13 lists the variables defined for the vCenter Server traps.

Table 8-13. Variables Defined in VMWARE-VC-EVENT-MIB

Variable	ID Mapping	Description
vmwVpxdTrapType	vmwVC 301	The trap type of the vCenter Server trap.
vmwVpxdHostName	vmwVC 302	The name of the affected host.
vmwVpxdVMName	vmwVC 303	The name of the affected virtual machine.
vmwVpxdOldStatus	vmwVC 304	The prior status.
vmwVpxdNewStatus	vmwVC 305	The new status.
vmwVpxdObjValue	vmwVC 306	The object value.

VMWARE-VMINFO-MIB

The VMWARE-VMINFO-MIB.mib file defines variables and traps for reporting virtual machine information.

Table 8-14 lists the variables defined in VMWARE-VMINFO-MIB.mib.

Table 8-14. Identification Mappings for VMWARE-VMINFO-MIB

Variable	ID Mapping	Description
Virtual Machine Variables		
vmwVmTable	vmwVirtMachines 1	A table containing information on the virtual machines that have been configured on the system.

Table 8-14. Identification Mappings for VMWARE-VMINFO-MIB (Continued)

Variable	ID Mapping	Description
vmwVmEntry	vmwVmTable 1	The record for a single virtual machine.
vmwVmIdx	vmwVmEntry 1	An index for the virtual machine entry.
vmwVmDisplayName	vmwVmEntry 2	The display name for the virtual machine.
vmwVmConfigFile	vmwVmEntry 3	The path to the configuration file for this virtual machine.
vmwVmGuestOS	vmwVmEntry 4	The guest operating system running on the virtual machine.
vmwVmMemSize	vmwVmEntry 5	The memory (in MB) configured for this virtual machine.
vmwVmState	vmwVmEntry 6	The virtual machine power state (on or off).
vmwVmVMID	vmwVmEntry 7	An identification number assigned to running virtual machines by the VMkernel. Powered-off virtual machines to not have this ID.
vmwVmGuestState	vmwVmEntry 8	The state of the guest operating system (on or off).
vmwVmCpus	vmwVmEntry 9	The number of virtual CPUs assigned to this virtual machine.
Virtual Machine HBA Variables		
vmwVmHbaTable	vmwVirtMachines 2	A table of HBAs visible to a virtual machine.
vmwVmHbaEntry	vmwVmHbaTable 1	Record for a single HBA.
vmwHbaVmIdx	vmwVmHbaEntry 1	A number corresponding to the virtual machine's index in the vmwVmTable.
vmwVmHbaIdx	vmwVmHbaEntry 2	Uniquely identifies a given HBA in this VM. May change across system reboots.
vmwHbaNum	vmwVmHbaEntry 3	The name of the HBA as it appears in the virtual machine settings.
vmwHbaVirtDev	vmwVmHbaEntry 4	The HBA hardware being emulated to the guest operating system.
vmwHbaTgtTable	vmwVirtMachines 3	The table of all virtual disks configure for virtual machines in vmwVmTable.
vmwHbaTgtEntry	vmwHbaTgtTable 1	A record for a specific storage disk. May change across reboots.
vmwHbaTgtVmIdx	vmwHbaTgtEntry 1	A number corresponding to the virtual machine's index (vmwVmIdx) in the vmwVmTable.
vmwHbaTgtIdx	vmwHbaTgtEntry 2	This value identifies a particular disk.
vmwHbaTgtNum	vmwHbaTgtEntry 3	Identifies the disk as seen from the host bus controller.
Virtual Machine Network Variables		
vmwVmNetTable	vmwVirtMachines 4	A table of network adapters for all virtual machines in vmwVmTable.
vmwVmNetEntry	vmwVmNetTable 1	Identifies a unique network adapter in this table.
vmwVmNetVmIdx	vmwVmNetEntry 1	A number corresponding to the virtual machine's index in the vmwVmTable.
vmwVmNetIdx	vmwVmNetEntry 2	Identifies a unique network adapter in this table. May change across sytem reboots.
vmwVmNetNum	vmwVmNetEntry 3	The name of the network adapter as it appears in the virtual machine settings.

Table 8-14. Identification Mappings for VMWARE-VMINFO-MIB (Continued)

Variable	ID Mapping	Description
vmwVmNetName	vmwVmNetEntry 4	Identifies what the network adapter is connected to.
vmwVmNetConnType	vmwVmNetEntry 5	Obsolete. Do not use.
vmwVmNetConnected	vmwVmNetEntry 6	Reports true if the ethernet virtual device is connected to the virtual machine.
vmwVmMAC	vmwVmNetEntry 7	Reports the configured virtual hardware MAC address. If VMware Tools is not running, the value is zero or empty.
Virtual Floppy Device Variables		
vmwFloppyTable	vmwVirtMachines 5	A table of floppy drives for all virtual machines in vmwVmTable.
vmwFloppyEntry	vmwFloppyTable 1	Identifies a single floppy device. May change across system reboots.
vmwFdVmIdx	vmwFloppyEntry 1	A number corresponding to the virtual machine's index in the vmwVmTable.
vmwFdIdx	vmwFloppyEntry 2	Identifies a specific virtual floppy device.
vmwFdName	vmwFloppyEntry 3	The file or device that this virtual floppy device is connected to.
vmwFdConnected	vmwFloppyEntry 4	Reports true if the floppy device is connected.
Virtual DVD or CD-ROM Variables		
vmwCdromTable	vmwVirtMachines 6	A table of DVD or CD-ROM drives for all virtual machines in vmwVmTable.
vmwCdromEntry	vmwCdromTable 1	Identifies a specific CD-ROM or DVD drive. May change across system reboots.
vmwCdVmIdx	vmwCdromEntry 1	A number corresponding to the virtual machine's index in the vmwVmTable.
vmwCdromIdx	vmwCdromEntry 2	Identifies the specific DVD or CD-ROM drive.
vmwCdromName	vmwCdromEntry 3	The file or device that the virtual DVD or CD-ROM drive has been configured to use.
vmwCdromConnected	vmwCdromEntry 4	Reports true the CD-ROM device is connected.
Virtual Machine Trap Variables		
vmwVmID	vmwTraps 101	Holds the same value as vmwVmVMID of the affected virtual machine generating the trap, to allow polling of the affected virtual machine in vmwVmTable.
vmwVmConfigFilePath	vmwTraps 102	The configuration file of the virtual machine generating the trap.

Table 8-15 lists the traps defined in VMWARE-VMINFO-MIB.mib. These traps were formely defined in VMWARE-TRAPS-MIB.mib.

Table 8-15. Traps Defined in VMWARE-VMINFO-MIB

Trap	ID Mapping	Description
vmwVmPoweredOn	vmwVmNotifications 1	This trap is sent when a virtual machine is powered on from a suspended or powered off state.
vmwVmPoweredOff	vmwVmNotifications 2	This trap is sent when a virtual machine is powered off.

Table 8-15. Traps Defined in VMWARE-VMINFO-MIB (Continued)

Trap	ID Mapping	Description
vmwVmHBLost	vmwVmNotifications 3	This trap is sent when a virtual machine detects a loss in guest heartbeat. VMware Tools must be installed in the guest operating system in order for this value to be valid.
vmwVmHBDetected	vmwVmNotifications 4	This trap is sent when a virtual machine detects or regains the guest heartbeat. VMware Tools must be installed in the guest operating system in order for this value to be valid.
vmwVmSuspended	vmwVmNotifications 5	This trap is sent when a virtual machine is suspended.

SNMPv2 Diagnostic Counters

The SNMPv2-MIB.mib file provides a number of counters to aid in debugging SNMP problems.

Table 8-16 lists some of these diagnostic counters.

Table 8-16. Diagnostic Counters from SNMPv2-MIB

Variable	ID Mapping	Description
snmpInPkts	snmp 1	The total number of messages delivered to the SNMP entity from the transport service.
snmpInBadVersions	snmp 3	The total number of SNMP messages that were delivered to the SNMP entity and were for an unsupported SNMP version.
snmpInBadCommunityNames	snmp 4	The total number of community-based SNMP messages delivered to the SNMP entity that used an invalid SNMP community name.
snmpInBadCommunityUses	snmp 5	The total number of community-based SNMP messages delivered to the SNMP entity that represented an SNMP operation that was not allowed for the community named in the message.
snmpInASNParseErrs	snmp 6	The total number of ASN.1 or BER errors encountered by the SNMP entity when decoding received SNMP messages.
snmpEnableAuthenTraps	snmp 30	Indicates whether the SNMP entity is permitted to generate authenticationFailure traps. The value of this object overrides any configuration information. It therefore provides a means of disabling all authenticationFailure traps.
snmpSilentDrops	snmp 31	The total number of Confirmed Class PDUs delivered to the SNMP entity that were silently dropped because the size of a reply containing an alternate Response Class PDU with an empty variable-bindings field was greater than either a local constraint or the maximum message size associated with the originator of the request.
snmpProxyDrops	snmp 32	The total number of Confirmed Class PDUs delivered to the SNMP entity that were silently dropped because the transmission of the message to a proxy target failed in a manner other than a time-out such that no Response Class PDU could be returned.

Index