MasterScope SystemManager G Ver8.0
Hypervisor Monitor Option for VMware
User's Guide

July 2018

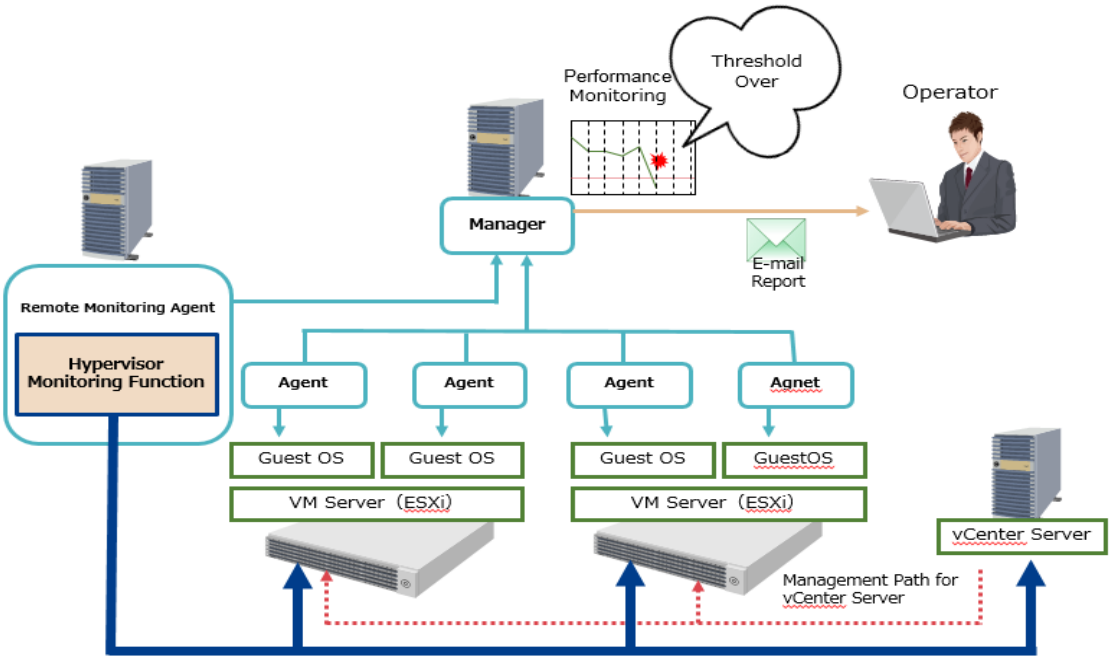
NEC Corporation

1) Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States and other countries.
In addition, Microsoft product names included in this guide are registered trademarks of Microsoft Corporation in the United States and other countries.
2) VMware and the VMware logo are registered trademarks of VMware, Inc. in the United States of America and other countries.
3) Other product names, company names, and proper nouns mentioned in this document are trademarks or registered trademarks of their respective companies.
4) The TM and ® marks are not included in the text or figures of this document.
5) The specifications or designs of windows shown in this manual are subject to change without notice to improve the product.

Table of Contents

1. About This Document

This document describes setting procedure for monitoring VMware ESXi and vCenter Server (Windows) and vCenter Server Appliance by MasterScope SystemManager G.



2. Hypervisor Monitor Option

The hypervisor monitor option provides the following functions:

- ESXi Server monitoring function
  Monitors the status of VMware ESXi Server in the system.
  When ESXi Server is to be included as a monitoring target, the VM of the ESXi Server must be registered as a remote host.

- vCenter Server (Windows) monitoring function
  Monitors the status of VMware vCenter Server in the system.
  When vCenter Server, running under Windows, is to be included as a monitoring target, the host on which the vCenter Server is installed must be registered as a remote host.

  * In this procedure manual, vCenter Server, running under Windows, is expressed as "vCenter Server". (vCenter Server Appliance is expressed as "Appliance".)

- vCenter Server (Appliance) monitoring function
  Monitors the status of VMware vCenter Appliance in the system.
  When vCenter Server Appliance is to be included as a monitoring target, the VM of the vCenter Server Appliance must be registered as a remote host.

  * In this procedure manual, vCenter Server Appliance is expressed as "Appliance".

1. **Performance Monitoring**
   For detailed monitoring items, see “Appendix A. List of Monitoring Objects”.
2. **Event Monitoring**
   Monitor Events on ESXi or vCenter Server or Appliance. If event matches message filter, notify the event to Message View.

[Notes]

- ✓ To use this option, purchase “Hypervisor Monitor Option for VMware” license.
- ✓ Performance information might not be collected at the specified interval depending on the number of registered hypervisors (ESXi Server and vCenter Server and Appliance) and the load status.

3. System Requirements

1. **Windows manager**

This is compatible with the manager of Windows environments supported by SystemManager G.

This is not used with the HP-UX and Linux managers.

2. **Windows remote monitoring agent**

Supported platforms

- Windows Server 2008 R2 (x64)
- Windows Server 2012 (x64)
- Windows Server 2012 R2 (x64)
- Windows Server 2016 (x64)

Required software

One of the following versions of .Net Framework must be installed:

- Microsoft .Net Framework 2.0
- Microsoft .Net Framework 3.0
- Microsoft .Net Framework 3.5

System Requirements

For the required system resources, see "System Requirements" in MasterScope SystemManager G release memo.

3. **Monitoring targets**

Version	ESXi	vCenter Server (Windows)	vCenter Server Appliance
5.0	○	○	-
5.1	○	○	-
5.5	○	○	-
6.0	○	○	-
6.5	○	○	○

It's possible to monitor less than 20 targets of ESXi by 1 remote monitoring agent, but it depends on your environment.

4. Installation

4.1 Installing Remote Monitoring Agent

Install the remote monitoring agent bedore performing the settings described in this guide.
For information on how to install this product, refer to the MasterScope Media release memo (relmemo.pdf).

4.2 Registering License

Register “Hypervisor Monitor Option for VMware” license key. For information how to register license key, see chapter of “Manage the license” in help manual.

If the license is not registered, the "vCenter/ESX" tab is not displayed in Account setting detail dialog(*).

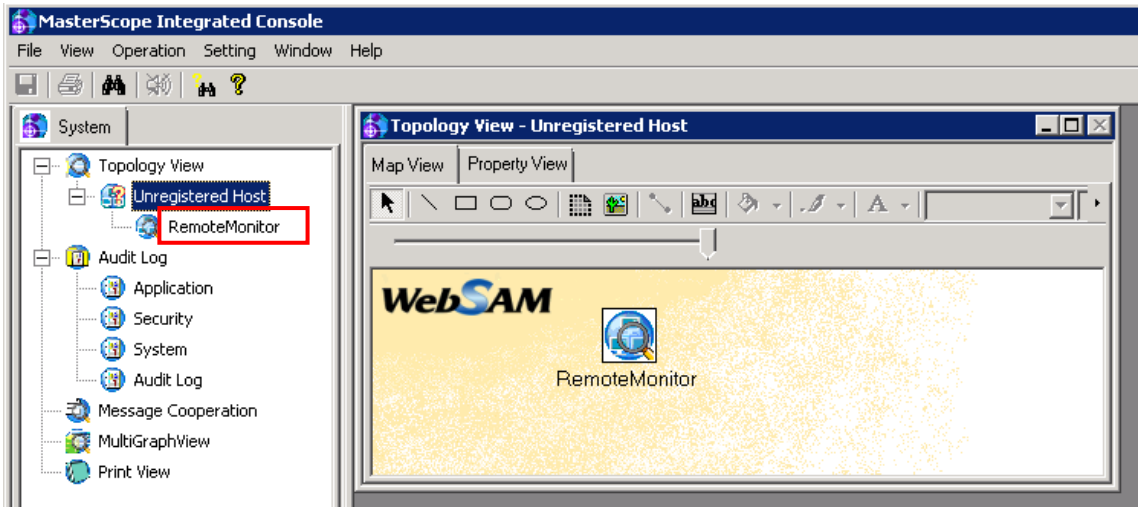
*See "5.2 Specifying the authentication information of ESXi Server/vCenter Server/Appliance“.

5. Setting up monitoring

This operation should be executed after shifting into the Configuration mode.
Select menu [Setting] > [Configuration Mode].

5.1 Adding remote monitoring agent

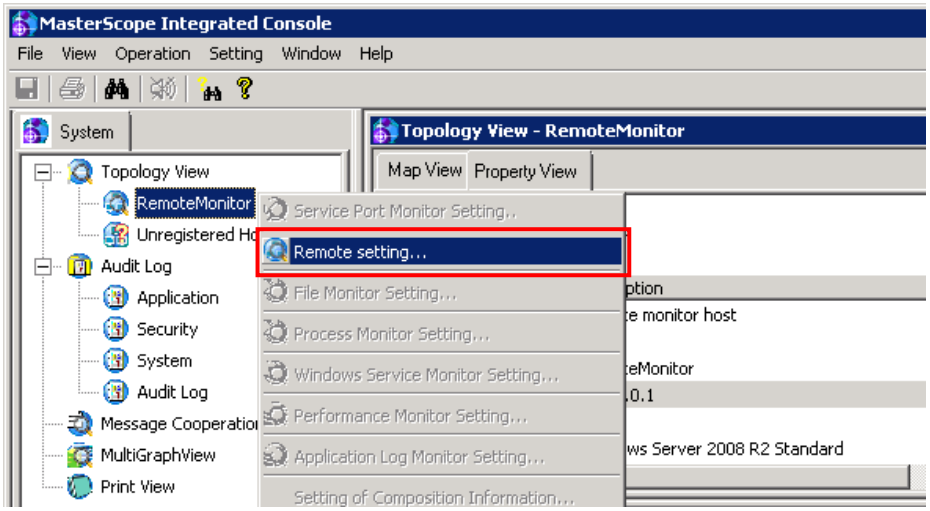
Open the monitoring view and add the remote monitoring agent to the Topology View tree.
A new remote monitoring agent connected to the manager is automatically registered under the [Unregistered Host] group directly under the root node (Topology View node).
Note that the remote host cannot be defined while the remote monitoring agent is registered in the [Unregistered Host] group. The remote monitoring agent must therefore be moved directly under the root node (topology view node) or to a defined host group. Once this is done, the remote host can be defined.



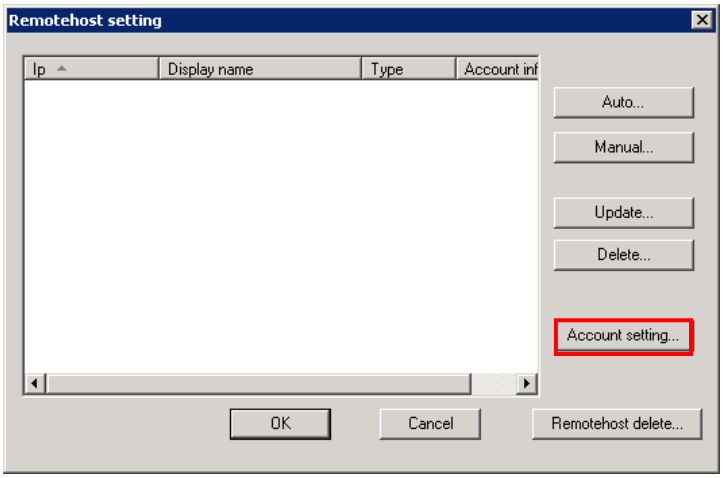
5.2 Specifying the authentication information of ESXi Server/vCenter Server/Appliance

To monitor ESXi Server and vCenter Server and Appliance, authentication information must be specified when adding a remote host.

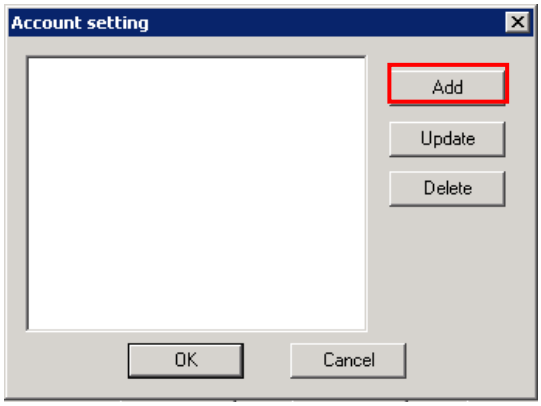
1. Right-click the remote monitoring agent in the topology view to open the pop-up menu and select [Remote setting].



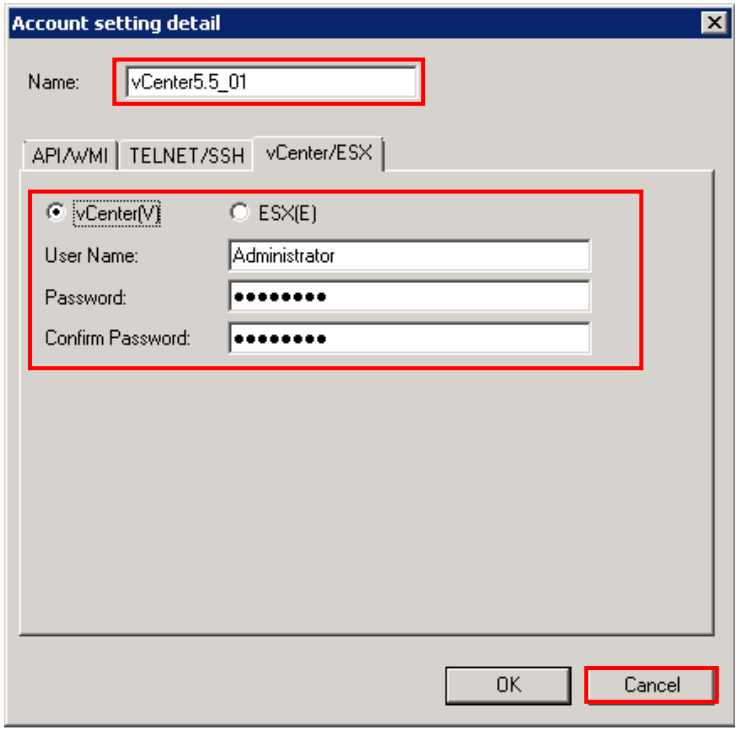
2. When the [Remote setting] dialog opens, click [Account setting].



3. When the [Account setting] dialog opens, click [Add].



4. When the [Account setting detail] dialog opens, select the [vCenter/ESX] tab, enter the required items, and click the [OK] button. The [vCenter/ESX] tab is added to the [Account setting] dialog box when the license for the hypervisor monitoring function is registered.



- Name

  Specify an arbitrary name for the authentication setting.

- vCenter or ESX

  Select [vCenter] or [ESX] as the login target.

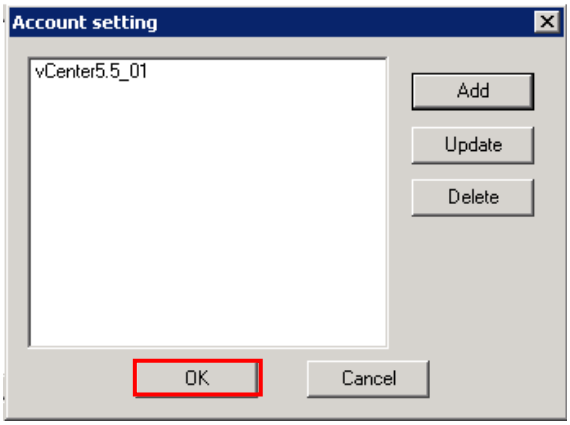
Select vCenter for Appliance, also.

- User Name

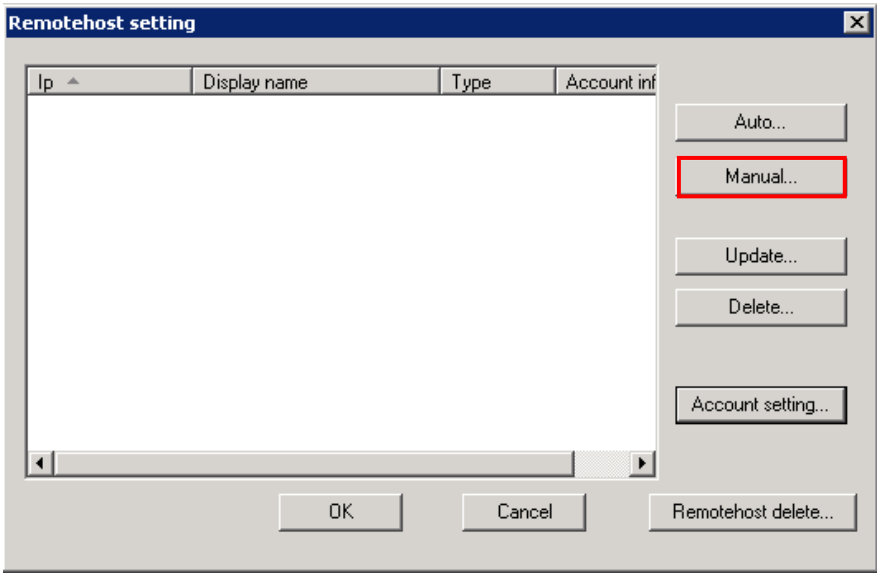
  Specify the login user name for monitoring target. Register a user with administrator authority as the login user.
- Password and Confirm Password

  Specify the login password for monitoring target.

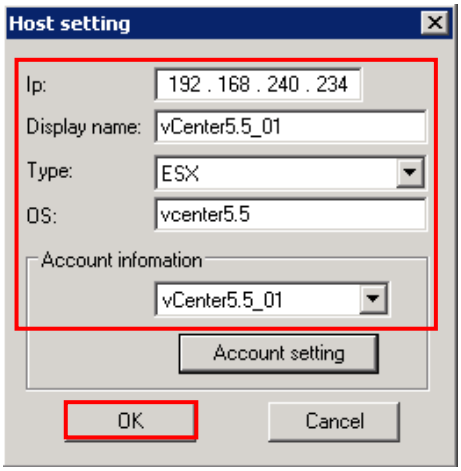
5. When the [Account setting] dialog opens, click the [OK] button.



6. When the [Remotehost setting] dialog opens, click the [Manual] button.



7. When the [Host setting] window opens, enter the connection information for monitoring target to be monitored and click the [OK] button.



- Ip

  Specify the IP address of monitoring target to be monitored. Only IPv4 can be specified.

- Display name

  Specify the node name displayed in the topology view by using up to 64 characters. This item must be specified. You can use one-byte alphanumeric characters, hyphens (-), underscores (_), at marks (@), and periods (.).

  [Notes]

  - ✓ A node name that is already registered to the topology view cannot be used.
  - ✓ The same IP address as one that is registered to another remote monitoring agent can be registered. However, an IP address that is already registered to the same remote monitoring agent cannot be registered in duplicate.
  - ✓ If a character string reserved by the system or a character string that is not recognized as a file or directory is specified in [Display name], monitoring may not be performed properly.

- Type

  Select "ESX" from the pull-down list.

- OS

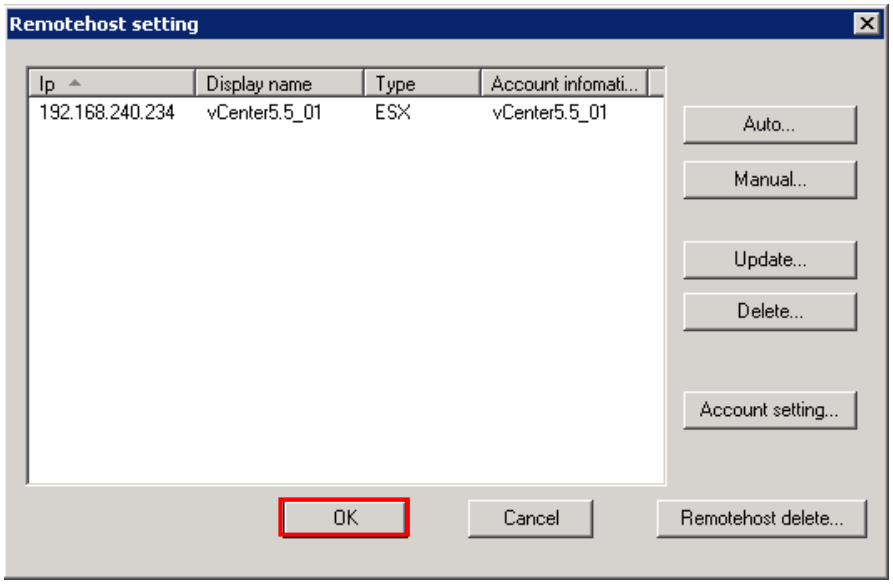
  Specify the OS name by using up to 128 characters. This item is optional.

- Account infomation

  Select the registered authentication information to be used for remote host monitoring.

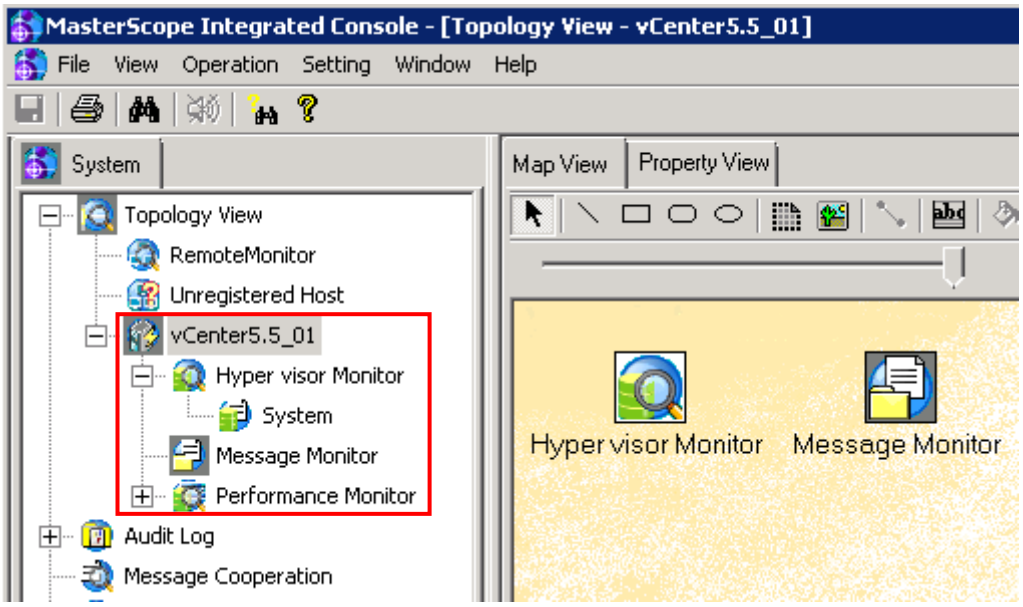
  Select the authentication information you created in step 4.

8. When the [Remotehost setting] dialog opens, click the [OK] button.



5.3 Adding monitoring target

Following successful authentication, the monitoring target is connected under the unregistered host node in the topology view. It is therefore necessary to move the monitoring target directly under the Topology View

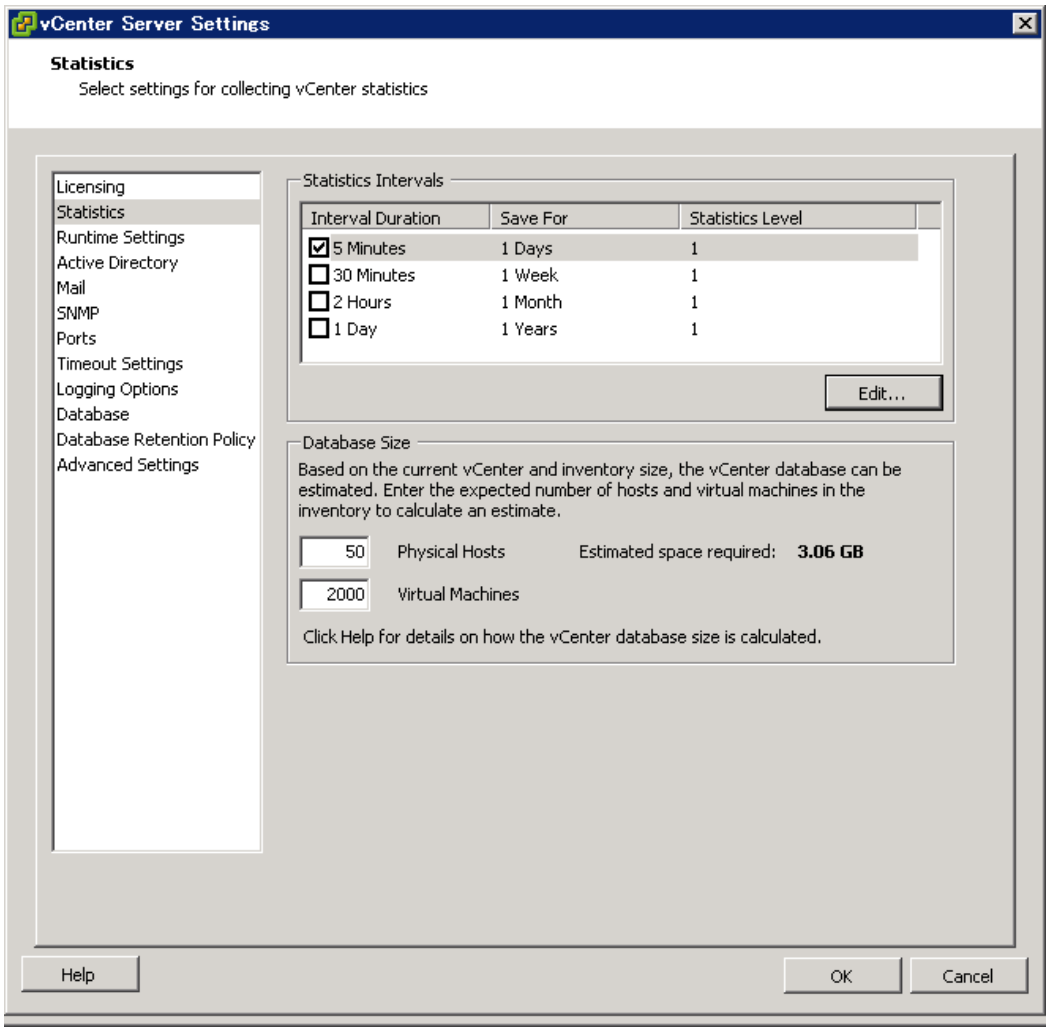


5.4 Configuring performance monitoring

5.4.1 Specifying the statistical information of vCenter Server/Appliance

When monitor vCenter Server or Appliance, specify the statistical information settings in vCenter Server/Appliance.

Select [Administration] > [vCenter Server Settings] > [Statistics].

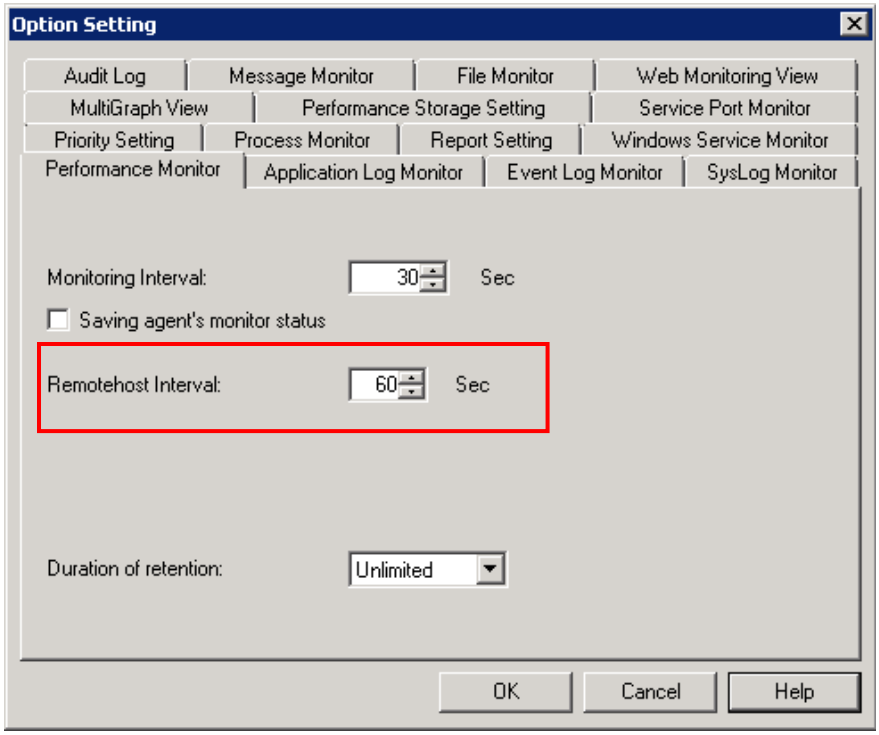


Select the [5 Minutes] check box in [Statistics Intervals].

5.4.2 Changing the performance monitoring interval

The hypervisor performance monitoring interval is coordinated with the performance monitoring interval on the remote host.

To change the performance monitoring interval, open the [Option Setting] window from [Option] on the [Setting] menu in the monitoring window and select the [Performance Monitor] tab.



➢ Remotehost Interval

Specify the performance monitoring interval on the remote host in seconds.

When using hypervisor performance monitoring, must be set to 60 seconds.

[Note]

The performance monitoring interval is changed on other remote hosts at the same time.

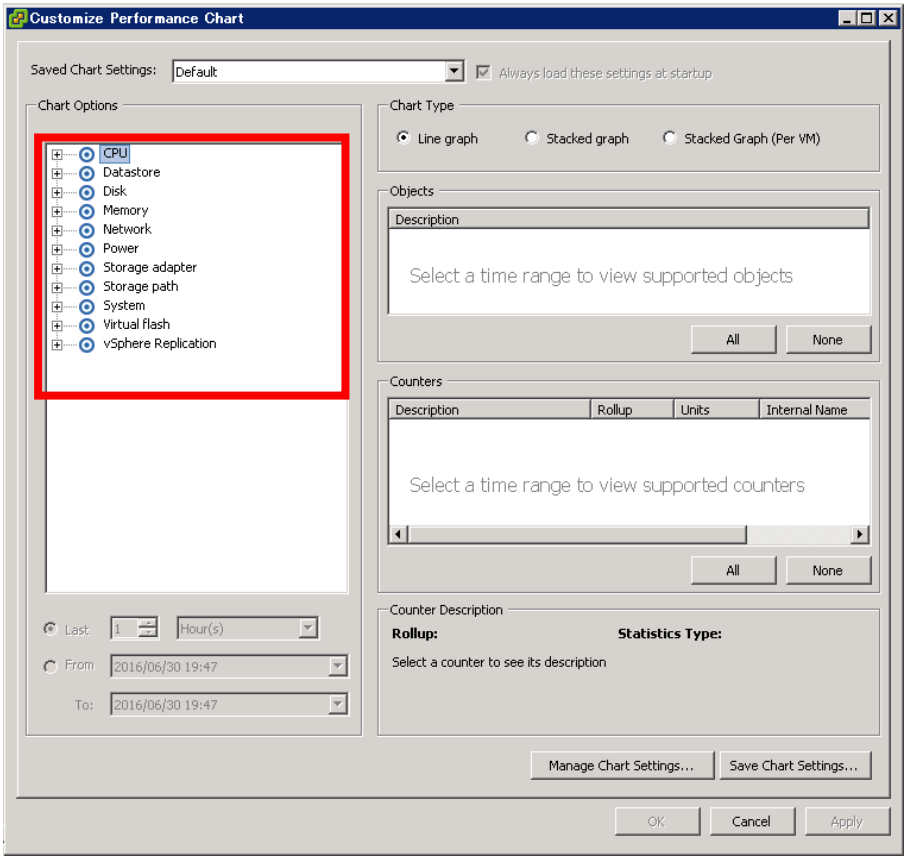
5.4.3 Configuring the performance monitoring settings

Specify the monitoring objects (resources, instances and counters) in the same way as for the performance monitoring settings for remote host monitoring.

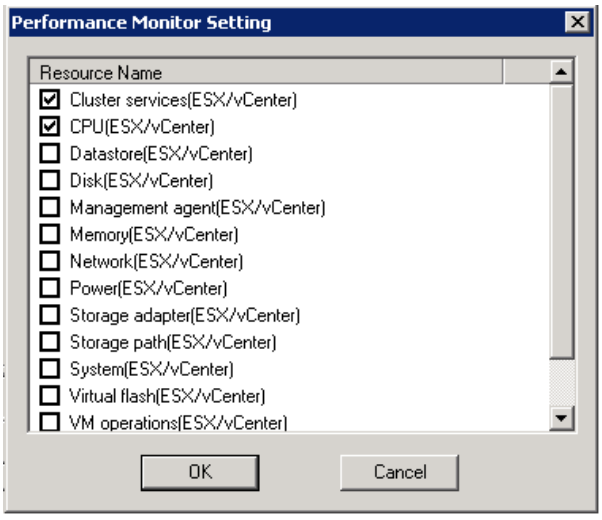
For how to operate the window, see “About performance monitoring” in the SystemManager help.

Resources:

This corresponds to [Customize Performance Chart] > [Chart options] in monitoring target.

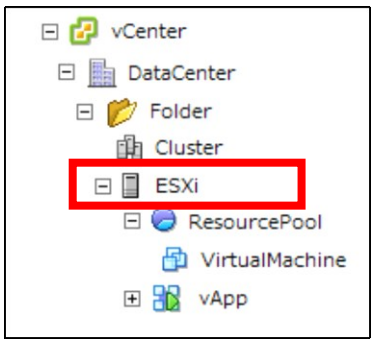


The resource settings window is shown below. Select the check boxes for the resources to be monitored.

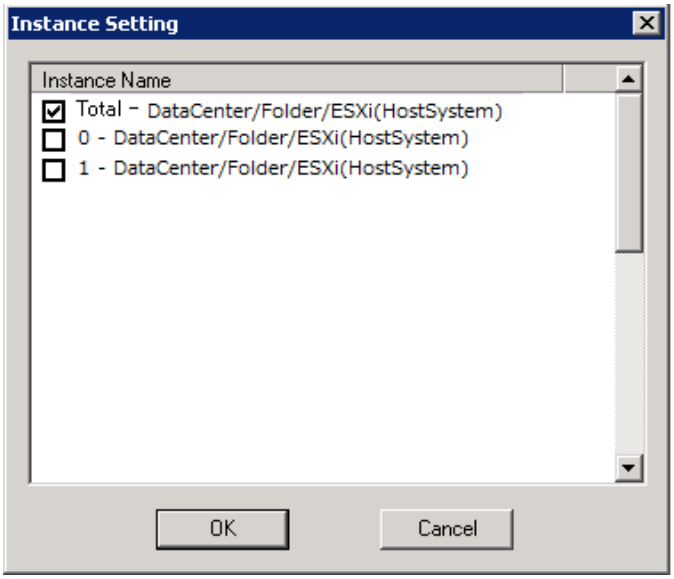


Instances:

This corresponds to settings in the tree in monitoring target.



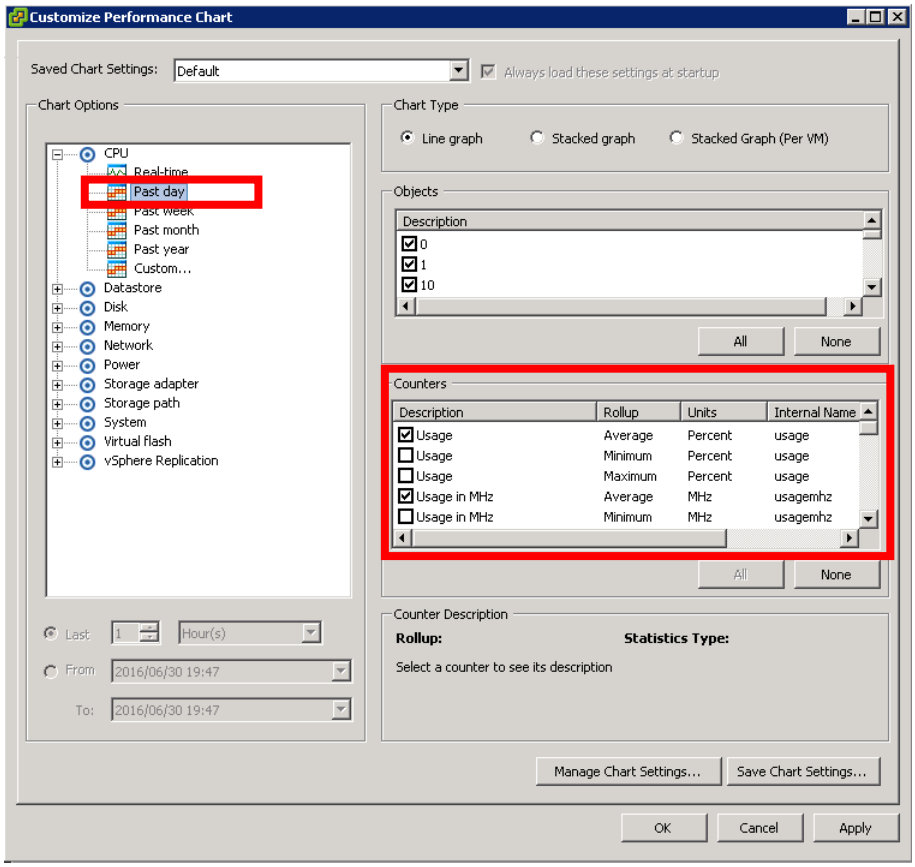
If the vSphere client has the tree structure as shown in the above figure, the instance names of ESXi (number of CPUs: 2) are displayed as follows.



The text in parentheses indicates Managed Object Type. HostSystem, ClusterComputeResource, ResourcePool or VirtualApp is displayed.

Counters:

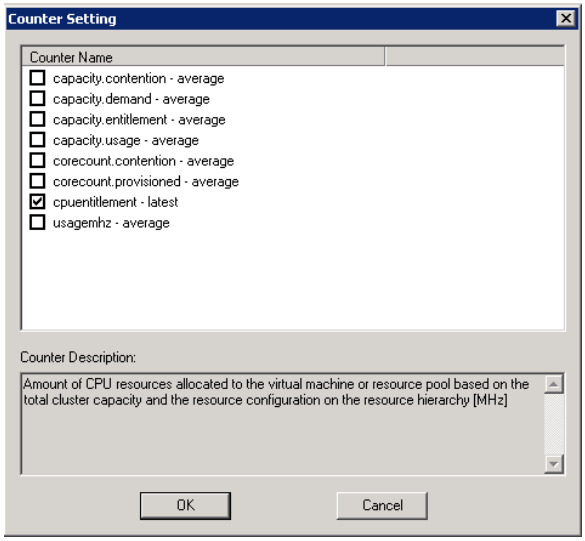
This corresponds to [Customize Performance Chart] > [Counters] in monitoring target.



When vCenter Server/Appliance is monitored, the counter displayed in [Past day] can be monitored.

When ESXi is monitored, the counter displayed in [Real-time] can be monitored.

The [Counter Setting] dialog box is displayed as follows.



For details about the monitoring counters, see "Appendix A. List of Monitored Objects".

5.4.4 Notes

- About instance and counter setting
  - ✓ Some instances and counters are not displayed depending on the version of the hypervisor being used or Statistics Intervals of vCenter Server.
  - ✓ Instance names consisting of more than 128 characters are not displayed in the [Instance Setting] dialog box. If you want to check the performance value, make sure that instant names are within 128 characters by flattening hierarchies or shortening the name in the tree.

- About acquired performance value
  - ✓ When monitoring ESXi, the performance value is fixing for 1 minute.
  - ✓ When monitoring vCenter Server/Appliance, the performance value is fixing for 5 minutes.
  - ✓ When the Managed Object Type is ClusterComputeResource, ResourcePool, or VirtualApp in monitoring vCenter Server/Appliance, the performance value is fixing for 5 minutes, but its interval is fixed to 30 minutes.

- When performance value can't be acquired in monitoring vCenter Server

1. Check vCenter Server setting, web.xml file.

```
<context-param>
    <description>Specify the maximum query size (number of metrics)for a single
    report. Non-positive values are ignored.</description>
    <param-name>maxQuerySize</param-name>
    <param-value>64</param-value>
</context-param>
```

   For details, see following url.
   http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2107096

2. When <param-value> is greater than 64, configure following file.
   `%INSTALL_DATA%\OperationsRemote\Agent\sg\VMHostPrb\VMHostPrb.ini`
   (`%INSTALL_DATA%` is a folder in the data area specified when the remote monitoring

agentis installed.)

```
[Perf]
VCenterMaxQueryMetrics=<param-value>
```

Set <*param-value*> to `VCenterMaxQueryMetrics`.

When the Managed Object Type is ClusterComputeResource, select smaller value from 10 and <*param-value*>.
Set selected value to `VCenterMaxQueryMetrics`.

3. Restart remote monitoring agent

- The performance information might not be collected at the specified interval depending on the number of registered hypervisors (ESXi Server and vCenter Server and Appliance) and the load status.

5.5 Configureing event monitoring

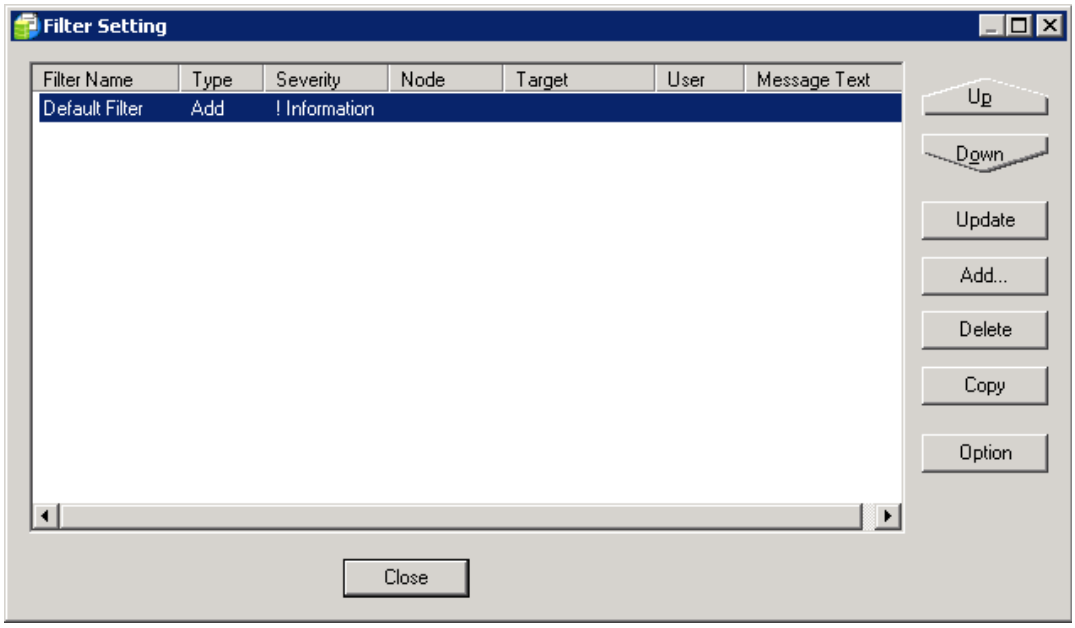
This product provide function to monitor events on ESXi Server/vCenter Server/Appliance, and notify message to Message View.
Set up the filter in the same way as for the event log monitoring settings for remote host monitoring.

[Notes]

- ✓ [Default Filter] is defined to filter logs whose importance in the event log is not “information”, and to report a message when these logs are output.
- ✓ When monitoring event logs, monitoring processing logins and logouts are registered to the log of the hypervisor. For this reason, reporting logs whose importance is “information” is disabled by the default filter.

5.5.1 Defining filter

Define a filter to extract the events output on ESXi Server/vCenter Server/Appliance.
Right-click the event log node (System) in the tree view and select [Filter Setting] from the displayed pop-up menu to display the [Filter Setting] dialog box.
For each filter, define the message extraction conditions and the information to add when extracting the messages.



In list of filters, extraction conditions and severity of each filter are displayed. Filtering is processed from the top to the bottom of the list sequentially, and the operation is performed based on the filter definition whose condition is matched first. Subsequent filtering processes after the first matched filter

definition are not performed. Moreover, no message is reported when none of the filters match the condition.

- [Up] and [Down] buttons
  Change the execution order of the selected filter.
  [Up] button switches the position of the selected filter to right above.
  [Down] button switches the position of the selected filter to right below.

- [Update] button
  Edit the definition details of the currently selected filter. Edit can also be performed by double-clicking a filter on the list.

- [Add] button
  Add a new filter at the position of the currently selected filter. When the [Add] button is clicked without selecting a filter, a new filter is added to the bottom of the list.

- [Delete] button
  Delete the currently selected filter.

- [Copy] button
  Copy the currently selected filter, and add a filter with the same extraction conditions and severity to add (except the filter name) to the selected position.

- [Option] button
  Open the [Filter Option Setting] dialog box to specify the options for the event log monitoring function.

[Note]
[Default Filter] is defined for all event logs immediately after remote host registration. [Default Filter] is defined to filter logs whose importance in the event log is not “information”, and to report a message when these logs are output.

5.5.2 Defining extraction conditions for event log monitoring

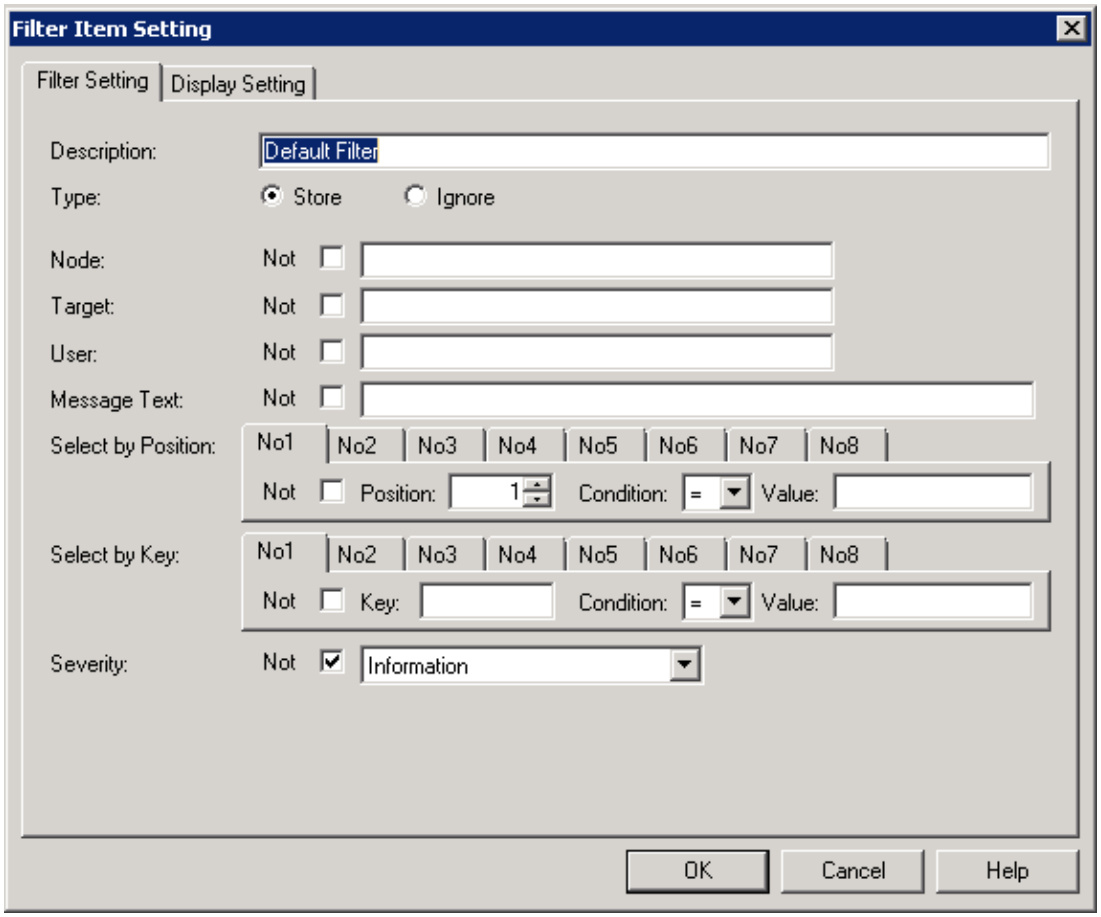
Define the conditions to extract logs to be reported to the Message View from the output event.

The filter extraction conditions are defined in the [Filter Item Setting] dialog box. To display the [Filter Item Setting] dialog box, perform the following operation:

1. Click the [Add] button in the [Filter Setting] dialog box.
2. Select the filter to edit in the [Filter Setting] dialog box, and then click the [Update] button.
3. Double-click the filter to edit in the [Filter Setting] dialog box.

When the [Filter Item Setting] dialog box is displayed, enter the extraction conditions on the [Filter Setting] tab, and then click the [OK] button.

[Notes]
When a conditions is omitted, that condition is not applied (all messages are targeted).
To extract messages, the message content must match all the conditions specified here.
Commas (,) and double quotation marks (“) cannot be used in this dialog box.



- Description

Specify the filter name by using up to 256 characters. The character string specified here is displayed as the filter name in the [Filter Setting] dialog box. [Description] cannot be omitted.

- Type

  Specify the filter type. When [Store] is selected, messages matching this filter are stored based on their category. When [Ignore] is selected, no message is reported for a log matching this filter, and the filtering processing of subsequent filters is not performed.

- Node (name of the node that output the message)

  Specify the filter condition for the node by using up to 256 characters in regular expression format. If a negative condition is specified, messages that do not match the regular expression condition are selected.

  [Note]

  The maximum length of node names for this product is 256 characters. If text longer than 256 characters is used, only the first 256 characters are valid.

- Target (name of the target that was the source of the message)

  Specify the filter condition for the target by using up to 128 characters in regular expression format. If a negative condition is specified, messages that do not match the regular expression condition are selected.

  [Note]

  The maximum length of node names for this product is 128 characters. If text longer than 256 characters is used, only the first 256 characters are valid.

- User (name of the user who was logged in when the message was output)

  Specify the filter condition for the user by using up to 128 characters in regular expression format. If a negative condition is specified, messages that do not match the regular expression condition are selected.

  [Note]

  The maximum length of node names for this product is 128 characters. If text longer than 256 characters is used, only the first 256 characters are valid.

- Message Text (body of message)

  Specify the filter condition for the message text by using up to 1,024 characters in regular expression format. If a negative condition is specified, messages that do not match the regular expression condition are selected.

[Note]

The maximum length of the message text for this product is 1,024 characters. If text longer than 1,024 characters is used, only the first 1,024 characters are valid.

- Select by Position

Specify up to 8 search conditions by specifying a position in the message text. If a negative condition is specified, messages that do not match the condition are selected.

- Position

  Specify the comparison start position (character number) in the message text in a range of 1 to 1,024.

- Condition

  Specify the comparison condition.

- Value

  Specify a value to compare by using up to 64 characters. The regular expression format cannot be used for specifying a comparison value.

  [Example] To extract messages in which the 10th character in the message text is “Error”, specify as shown below.

  Position: 10
  Condition: =
  Value: Error

- Select by Key

Specify up to 8 search conditions by specifying a key in the log content. If a negative condition is specified, messages that do not match the condition are selected.

- Key

  Specify the key in the log content by using up to 64 characters.

- Condition

  Specify the comparison condition. When [=] is specified, a regular expression is applied as the comparison value. When a condition other than [=] is specified, a binary comparison with the character string specified for the comparison value is performed.

- Value

  Specify the value to compare. When [=] is specified for [Condition], specify [Value] using a regular expression.

  [Example] To extract logs in which error_number is 4 or less when the log content includes

a character string “error_number = 5” (“5” is variable), specify as shown below.

Key: error_number
Condition: <=
Value: 4

[Key] and [Value] used for [Select by Key] must be enclosed in separators in the log content. Recognizable separators are one-byte spaces, (,), [,], {, }, < and >. A character string containing one or more two-byte spaces cannot be specified for the key value.

Example:
(error_number=1)

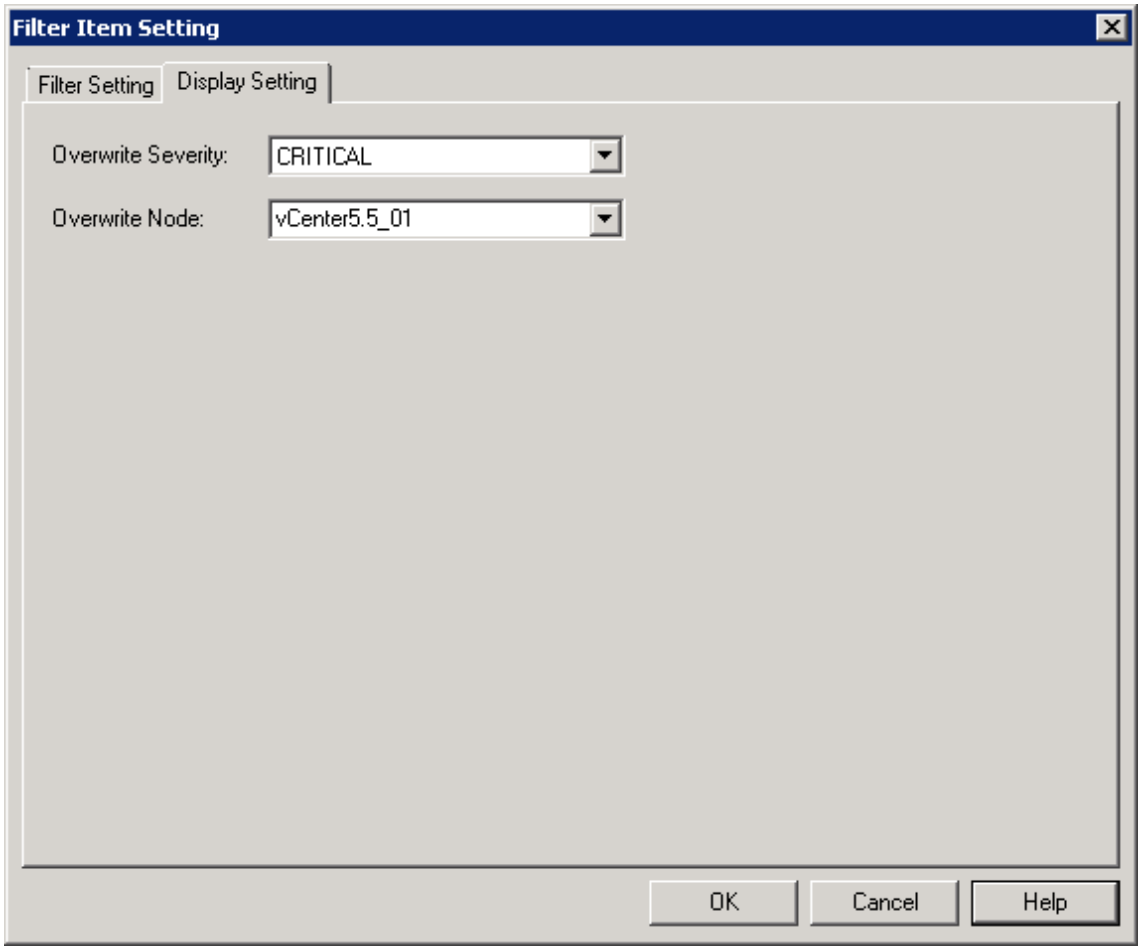
Note that spaces between the key, “=” and the value are ignored.

- Severity
  Select a search condition for items corresponding to [Severity] event logs. If a negative condition is specified, messages that do not match the selected condition are targeted.

5.5.3 Defining the information added to reported event log

Define the information to add when reporting a message for an extracted log.

Enter the information to add on the [Display Setting] tab in the [Filter Item Setting] dialog box and then click the [OK] button.



- Overwrite Severity

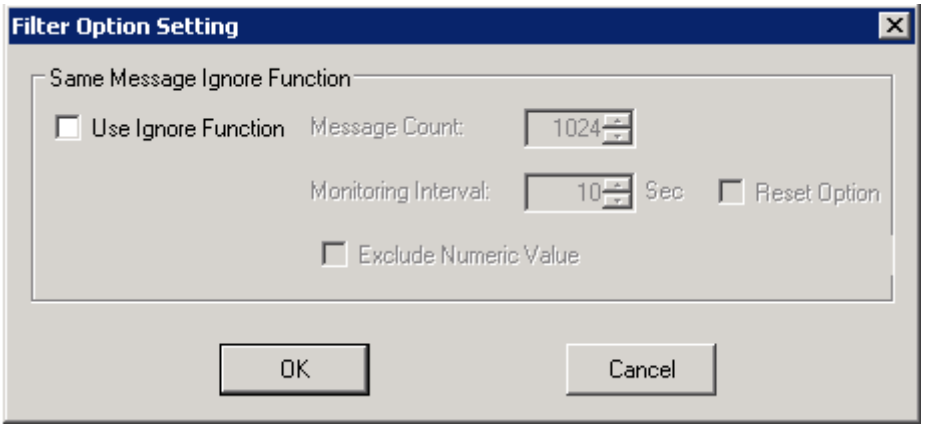
  Change the importance of messages matching the filter condition to the specified importance. A user mark cannot be used for importance that can be changed by using Overwrite Severity.

- Overwrite Node

  Change the message node name of messages matching the filter condition to a node name specified by using up to 256 characters.

5.5.4 Specifying options for event log monitoring

To define options for event log monitoring, click the [Option] button in the [Filter Setting] dialog. After configuring the settings, click the [OK] button.



【Same Message Ignore Function】

- Use Ignore Function

  Select whether or not to report a message when identical logs are output in a short period of time. Select the check box of [Use Ignore Function] to suppress the number of messages by not reporting a message for an identical log generated in the specified period of time.

- Message Count

  Specify the maximum number of log categories for which to suppress message reporting for each event log. Specify a value from 256 to 4,096. The default value is 1,024.

  When the number of logs for which to suppress message reporting exceeds the value specified here, logs are excluded from suppression starting with the oldest log (the log that has not been output for the longest time).

- Monitoring Interval

  Specify the period for suppressing messages after a log is output. Specify a value in the range of 1 to 3,600 seconds. The default value is 10 seconds.

  [Example] Whether or not to report a message and the reporting operation when the monitoring interval is 1 minute (60 seconds) and the following log is output is shown below.

Time (Seconds)	Log	Reporting	Operation
000	LOG001	Sent	LOG001 is added as a suppression target (up to 60 seconds).
010	LOG002	Sent	LOG002 is added as a suppression target (up to 70 seconds).

020	LOG003	Sent	LOG003 is added as a suppression target (up to 80 seconds).
030	LOG004	Sent	LOG004 is added as a suppression target (up to 90 seconds).
040	LOG001	Not sent	A message is not reported because the log is specified as a suppression target.
050	LOG002	Not sent	A message is not reported because the log is specified as a suppression target.
060	LOG004	Not sent	A message is not reported because the log is specified as a suppression target. LOG001 is excluded from the suppression targets.
070	LOG001	Sent	LOG001 is added as a suppression target (up to 130 seconds). LOG002 is excluded from the suppression targets.
080	LOG001	Not sent	A message is not reported because the log is specified as a suppression target. LOG003 is excluded from the suppression targets.
090	LOG003	Sent	LOG003 is added as a suppression target (up to 150 seconds). LOG004 is excluded from the suppression targets.

- Reset Option

  Specify whether or not to reset the period to suppress reporting of messages when identical logs are output. When the check box is selected, the suppression period is reset every time an identical log is output.

  [Example] Whether or not a message is reported and the reporting operation when the monitoring interval is 1 minute (60 seconds), resetting the suppression period is specified, and the following log is output is shown below.

Time (Seconds)	Log	Reporting	Operation
000	LOG001	Sent	LOG001 is added as a suppression target (up to 60 seconds).
010	LOG002	Sent	LOG002 is added as a suppression target (up to 70 seconds).

020	LOG003	Sent	LOG003 is added as a suppression target (up to 80 seconds).
030	LOG004	Sent	LOG004 is added as a suppression target (up to 90 seconds).
040	LOG001	Not sent	A message is not reported because the log is specified as a suppression target. The suppression period for LOG001 is reset (up to 100 seconds).
050	LOG002	Not sent	A message is not reported because the log is specified as a suppression target. The suppression period for LOG002 is reset (up to 110 seconds).
060	LOG004	Not sent	A message is not reported because the log is specified as a suppression target. The suppression period for LOG004 is reset (up to 120 seconds).
070	LOG001	Not sent	A message is not reported because the log is specified as a suppression target. The suppression period for LOG001 is reset (up to 130 seconds).
080	LOG001	Not sent	A message is not reported because the log is specified as a suppression target. The suppression period for LOG001 is reset (up to 140 seconds). LOG003 is excluded from the suppression targets.
090	LOG003	Sent	LOG003 is added as a suppression target (up to 150 seconds).

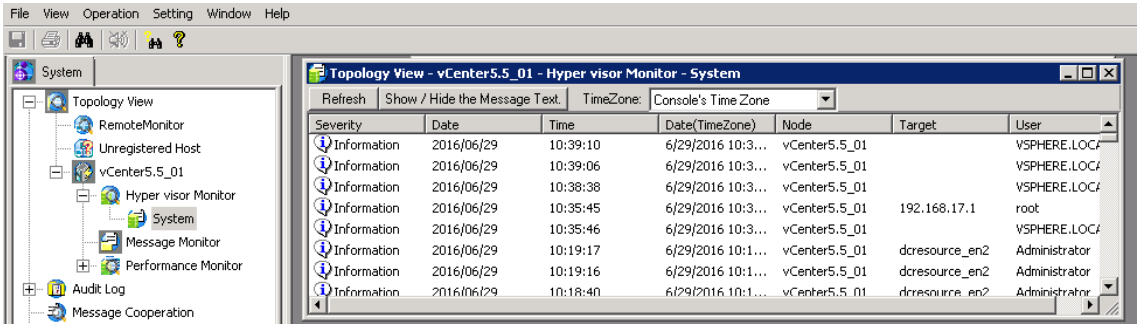
- Exclude Numeric Value

  When this check box is selected, a log that differs from others only in terms of numerical value is recognized as an identical log and is suppressed. This option is useful when the log contents include occurrence times, etc.

  [Example] When comparing “2000/12/12 error = 0” and “2000/5/12 error = 1”, both become “// error =” after excluding the numeric values, and thus they are recognized as an identical message.

5.5.5 Displaying current event log contents

Load the event log and display its contents. To display the log contents, double-click the event log node in the tree view.



- [Refresh] button

  Update the displayed contents to the latest contents after the log contents have been updated.

- [Show/Hide the Message Text] button

  Show or hide the pane to display the message text of the selected log at the bottom of the log list.

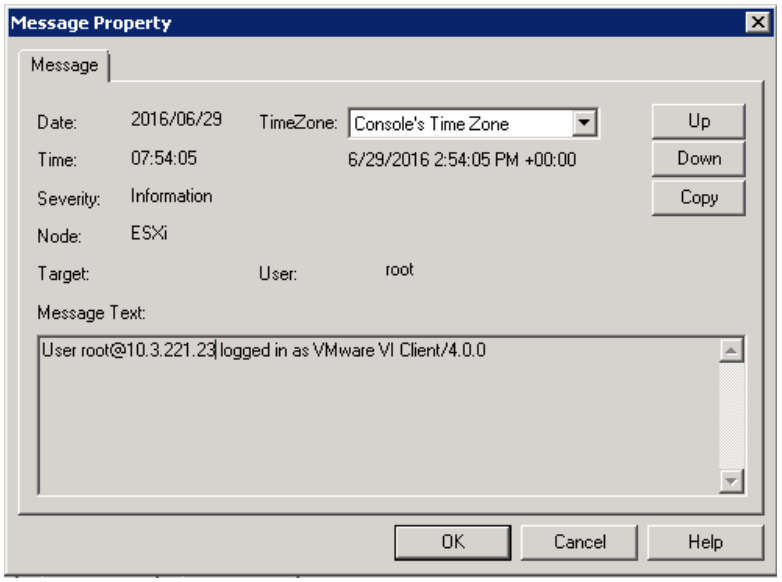
- Time zone

  The time zone of the date/time displayed in the [Date(TimeZone)] column can be specified.

  ・ Console's Time Zone: Displays the time zone of the machine that is displaying the monitoring window.

  ・ Manager's Time Zone: Displays the time zone of the machine that is running the manager service.

  In addition, an event log in the list can be double-clicked to display the [Message Property] dialog box.



- Time Zone

  The time zone of the date/time displayed in the [Date(TimeZone)] column can be specified.

  - Console's Time Zone: Displays the time zone of the machine that is displaying the monitoring window.
  - Manager's Time Zone: Displays the time zone of the machine that is running the manager service.

- [Up] and [Down] buttons

  Switch the log whose properties are displayed. Click the [Up] button to display one log above in the list, and the [Down] button to display one log below in the list.

- [Coyp] button

  Click this to copy the log details to the clipboard.

[Notes]

- ✓ The event log display function displays all event logs regardless of the event log filter settings.
- ✓ If the number of monitored event logs exceeds 1,000, the latest 1,000 logs are displayed.
- ✓ The contents displayed by the event log display function are the contents of the log file; not the contents of the actually reported message. The contents of the actually reported message can be confirmed by using the message monitoring function.

5.6 Importing and exporting hypervisor monitoring definitions

You can import and export performance monitoring settings and event log monitoring settings for hypervisor monitoring in the same way as when using the normal agent.
For details about the procedure, see the following sections in the SystemManager help:
- Import the definition for monitored agents
- Export the definition for the monitored agents and generate the definition file

When exported, definition files are output under the names shown below.

Service name	Definition file name
Topology	Topology.txt
Message monitoring	MessageView.txt
Performance Monitor	Performance.txt
Hypervisor Monitor	VMEventLog.txt

[Note]

- ✓ When performing performance monitoring by using the hypervisor, the instance name information includes the host name and other information. Exported information cannot be applied to other remote agents. To import information to other remote agents, clear the check box for the performance Monitor service in the import selection dialog box.

6. Notes

6.1 Creating authentication information

Use the authentication information created after “Hypervisor Monitor Option for VMware” license was enabled.(for the procedure, see 5.2 Specifying the authentication information of ESXi Server/vCenter Server/Appliance.)
If you use authentication information created before license is enabled, that information is not saved correctly.
[Workaround]
After enabling the license (the license is displayed on the [vCenter/ESXi] tab), create new authentication information.

6.2 Changing the time setting in ESXi Server or vCenter Server or Appliance

When using the "save the history to a file" performance monitoring function, if you set the time back on an ESXi or vCenter server or Appliance whose performance is being monitored by the hypervisor, the performance value of the past time is stored, making performance data invalid.
Execute [Initialize] and delete performance information by using the following procedure.
(This operation deletes the history data.)

To set the time back in monitoring target, perform the following operations on the console:

1. Stop the remote monitoring agent service.
2. Delete the *IP address* _result.csv file for the IP of the monitoring target server to be monitored from the following folder in the remote monitoring agent:
   `%INSTALL%\OperationsRemote\Agent\sg\VMHostPrb\`*`IP address`*`_result.csv`
   (`%INSTALL%` is the installation path of the remote monitoring agent.)

   The default path is as shown below.
   `C:\Program Files\NEC\UMF\OperationsRemote\Agent\sg\VMHostPrb\`*`IP address`*`_result.csv`

3. Update the time in the monitoring target server to be monitored.
4. Start the remote monitoring agent service.
5. Right-click the Performance Monitor tree in the target server and execute [Initialize] from the displayed pop-up menu to delete existing information.

Appendix A. List of Monitored Objects

This appendix describes the objects and instances whose information can be monitored.

[Note]

Some instances and counters are not displayed depending on whether the server is vCenter or ESXi, or Appliance and the version to be monitored.

CPU (ESX/vCenter) object

Counter name	Description of counter
coreUtilization	CPU utilization of the corresponding core (if hyper-threading is enabled) as a percentage during the interval (A core is utilized, if either or both of its logical CPUs are utilized) [%]
cpuentitlement	Amount of CPU resources allocated to the virtual machine or resource pool based on the total cluster capacity and the resource configuration on the resource hierarchy [MHz]
idle	Total time that the CPU spent in an idle state [ms]
reservedCapacity	Total CPU capacity reserved by virtual machines [MHz]
totalCapacity	Total CPU capacity reserved by and available for virtual machines [MHz]
totalmhz	Total amount of CPU resources of all hosts in the cluster [MHz]
usage	CPU usage as a percentage during the interval [%]
usagemhz	CPU usage, as measured in megahertz, during the interval [MHz]
used	Total CPU usage [ms]
utilization	CPU utilization as a percentage during the interval (CPU usage and CPU utilization may be different due to power management technologies or hyper-threading) [%]
ready	Time that the virtual machine was ready but could not get scheduled to run on the physical CPU during last measurement interval [ms]
readiness	Percentage of time that the virtual machine was ready but could not get scheduled to run on the physical CPU [%]

Cluster service (ESX/vCenter) object

Counter name	Description of counter
cpufairness	Fairness of distributed CPU resource allocation [number]
effectivecpu	Total available CPU resources of all hosts within a cluster [MHz]
effectivemem	Aggregate available memory resources of all the hosts within a cluster [number]
failover	VMware HA Number of failures that can be tolerated [number]
memfairness	Aggregate available memory resources of all the hosts within a cluster [number]

System (ESX/vCenter) object

Counter name	Description of counter
diskUsage	Amount of disk space usage for each mount point [%]
resourceCpuAct1	CPU active average over 1 minute of the system resource group [%]
resourceCpuAct5	CPU active average over 5 minutes of the system resource group [%]
resourceCpuAllocMax	CPU allocation limit (in MHZ) of the system resource group [MHz]
resourceCpuAllocMin	CPU allocation reservation (in MHZ) of the system resource group [MHz]
resourceCpuAllocShares	CPU allocation shares of the system resource group [number]
resourceCpuMaxLimited1	CPU maximum limited over 1 minute of the system resource group [%]
resourceCpuMaxLimited5	CPU maximum limited over 5 minutes of the system resource group [%]
resourceCpuRun1	CPU running average over 1 minute of the system resource group [%]
resourceCpuRun5	CPU running average over 5 minutes of the system resource group [%]

resourceCpuUsage	Amount of CPU used during the interval by the Service Console and other applications [MHz]
resourceMemAllocMax	Memory allocation limit (in KB) of the system resource group [KB]
resourceMemAllocMin	Memory allocation reservation (in KB) of the system resource group [KB]
resourceMemAllocShares	Memory allocation shares of the system resource group [number]
resourceMemCow	Memory shared by the system resource group [KB]
resourceMemMapped	Memory mapped by the system resource group [KB]
resourceMemOverhead	Overhead memory consumed by the system resource group [KB]
resourceMemShared	Memory saved due to sharing by the system resource group [KB]
resourceMemSwapped	Memory swapped out by the system resource group [KB]
resourceMemTouched	Memory touched by the system resource group [KB]
resourceMemZero	Zero filled memory used by the system resource group [KB]
uptime	Total time elapsed

Storage adapter (ESX/vCenter) object

Counter name	Description of counter
commandsAveraged	Average number of commands issued per second by the storage adapter during the collection interval [number]
numberReadAveraged	Average number of read commands issued per second by the storage adapter during the collection interval [number]
numberWriteAveraged	Average number of write commands issued per second by the storage adapter during the collection interval [number]
read	Rate of reading data by the storage adapter [Kbps]
totalReadLatency	The average time a read by the storage adapter takes [ms]
totalWriteLatency	The average time a write by the storage adapter takes

	[ms]
write	Rate of writing data by the storage adapter [Kbps]

Storage path (ESX/vCenter) object

Counter name	Description of counter
commandsAveraged	Average number of commands issued per second on the storage path during the collection interval [number]
numberReadAveraged	Average number of read commands issued per second on the storage path during the collection interval [number]
numberWriteAveraged	Average number of write commands issued per second on the storage path during the collection interval [number]
read	Rate of reading data on the storage path [Kbps]
totalReadLatency	The average time a read issued on the storage path takes [ms]
totalWriteLatency	The average time a write issued on the storage path takes [ms]
write	Rate of writing data on the storage path [Kbps]

Disk (ESX/vCenter) object

Counter name	Description of counter
busResets	Number of SCSI-bus reset commands issued during the collection interval [number]
commands	Number of SCSI commands issued during the collection interval [number]
commandsAborted	Number of SCSI commands aborted during the collection interval [number]
commandsAveraged	Average number of SCSI commands issued per second during the collection interval [number]
deviceLatency	Average amount of time, in milliseconds, to complete a SCSI command from the physical device [ms]
deviceReadLatency	Average amount of time, in milliseconds, to complete read from the physical device [ms]
deviceWriteLatency	Average amount of time, in milliseconds, to write to the

	physical device [ms]
kernelLatency	Average amount of time, in milliseconds, spent by VMkernel processing each SCSI command [ms]
kernelReadLatency	Average amount of time, in milliseconds, spent by VMKernel processing each SCSI read command [ms]
kernelWriteLatency	Average amount of time, in milliseconds, spent by VMKernel processing each SCSI write command [ms]
maxQueueDepth	Maximum queue depth [number]
maxTotalLatency	Highest latency value across all disks used by the host [ms]
numberRead	Number of disk reads during the collection interval [number]
numberReadAveraged	Average number of disk reads per second during the collection interval [number]
numberWrite	Number of disk writes during the collection interval [number]
numberWriteAveraged	Average number of disk writes per second during the collection interval [number]
queueLatency	Average amount of time spent in the VMkernel queue
queueReadLatency	Average amount of time taken during the collection interval per SCSI read command in the VMKernel queue [ms]
queueWriteLatency	Average amount time taken during the collection interval per SCSI write command in the VMKernel queue [ms]
read	Average number of kilobytes read from the disk each second during the collection interval [Kbps]
totalLatency	Average amount of time taken during the collection interval to process a SCSI command issued by the Guest OS to the virtual machine [ms]
totalReadLatency	Average amount of time taken during the collection interval to process a SCSI read command issued from the Guest OS to the virtual machine [ms]
totalWriteLatency	Average amount of time taken during the collection interval to process a SCSI write command issued by the Guest OS to the virtual machine [ms]
usage	Aggregated disk I/O rate. For hosts

write	Average number of kilobytes written to disk each second during the collection interval [Kbps]

Datastore (ESX/vCenter) object

Counter name	Description of counter
datastoreIops	Storage I/O Control aggregated IOPS [number]
numberReadAveraged	Average number of read commands issued per second to the datastore during the collection interval [number]
numberWriteAveraged	Average number of write commands issued per second to the datastore during the collection interval [number]
read	Rate of reading data from the datastore [Kbps]
sizeNormalizedDatastoreLatency	Storage I/O Control size-normalized I/O latency [us]
totalReadLatency	The average time a read from the datastore takes [ms]
totalWriteLatency	The average time a write to the datastore takes [ms]
write	Rate of writing data to the datastore [Kbps]

Network (ESX/vCenter) object

Counter name	Description of counter
droppedRx	Number of receives dropped [number]
droppedTx	Number of transmits dropped [number]
packetsRx	Number of packets received during the interval [number]
packetsTx	Number of packets transmitted during the interval [number]
received	Average rate at which data was received during the interval [Kbps]
transmitted	Average rate at which data was transmitted during the interval [Kbps]
usage	Network utilization (combined transmit- and receive-rates) during the interval [Kbps]

Memory (ESX/vCenter) object

Counter name	Description of counter
active	Amount of memory that is actively used, as estimated by VMkernel based on recently touched memory pages [KB]
activewrite	Amount of memory actively being written to by the VM [KB]
compressed	Amount of memory compressed by ESX [KB]
compressionRate	Rate of memory compression for the VM [Kbps]
consumed	Amount of memory consumed by a virtual machine, host, or cluster [KB]
decompressionRate	Rate of memory decompression for the VM [Kbps]
granted	Amount of machine memory or physical memory that is mapped for a virtual machine or a host [KB]
heap	VMkernel virtual address space dedicated to VMkernel main heap and related data [KB]
heapfree	Free address space in the VMkernel's main heap [KB]
mementitlement	Memory allocation as calculated by the VMkernel scheduler based on current estimated demand and reservation, limit, and shares policies set for all virtual machines and resource pools in the host or cluster [MB]
overhead	Memory (KB) consumed by the virtualization infrastructure for running the VM [KB]
reservedCapacity	Total amount of memory reservation used by powered-on virtual machines and vSphere services on the host [MB]
shared	Amount of guest memory that is shared with other virtual machines, relative to a single virtual machine or to all powered-on virtual machines on a host [KB]
sharedcommon	Amount of machine memory that is shared by all powered-on virtual machines and vSphere services on the host [KB]
state	One of four threshold levels representing the percentage of free memory on the host. The counter value determines swapping and ballooning behavior for memory reclamation. [number]
swapin	Amount swapped-in to memory from disk [KB]
swapinRate	Rate at which memory is swapped from disk into active

	memory during the interval [Kbps]
swapout	Amount of memory swapped-out to disk [KB]
swapoutRate	Rate at which memory is being swapped from active memory to disk during the current interval [Kbps]
swapped	Current amount of guest physical memory swapped out to the virtual machine's swap file by the VMkernel [KB]
swapused	Amount of memory that is used by swap [KB]
sysUsage	Amount of machine memory used by VMkernel for core functionality, such as device drivers and other internal uses [KB]
totalCapacity	Total amount of memory reservation used by and available for powered-on virtual machines and vSphere services on the host [MB]
totalmb	Total amount of machine memory of all hosts in the cluster that is available for virtual machine memory (physical memory for use by the Guest OS) and virtual machine overhead memory [MB]
unreserved	Amount of memory that is unreserved [KB]
usage	Memory usage as percentage of total configured or available memory [%]
vmmemctl	Amount of memory allocated by the virtual machine memory control driver (vmmemctl), which is installed with VMware Tools [KB]
zero	Memory that contains 0s only [KB]
vmfs.pbc.capMissRatio	Trailing average of the ratio of capacity misses to compulsory misses for the VMFS PB Cache [%]
vmfs.pbc.overhead	Amount of VMFS heap used by the VMFS PB Cache [KB]
vmfs.pbc.size	Space used for holding VMFS Pointer Blocks in memory [MB]
vmfs.pbc.sizeMax	Maximum size the VMFS Pointer Block Cache can grow to [MB]
vmfs.pbc.workingSet	Amount of file blocks whose addresses are cached in the VMFS PB Cache [TB]
vmfs.pbc.workingSetMax	Maximum amount of file blocks whose addresses are cached in the VMFS PB Cache [TB]

Virtual flash (ESX/vCenter) object

Counter name	Description of counter
numActiveVMDKs	Number of caches controlled by the virtual flash module [number]

Management agent (ESX/vCenter) object

Counter name	Description of counter
memUsed	Amount of total configured memory that is available for use [KB]
swapIn	Amount of memory that is swapped in for the Service Console [Kbps]
swapOut	Amount of memory that is swapped out for the Service Console [Kbps]
swapUsed	Sum of the memory swapped by all powered-on virtual machines on the host [KB]

Virtual machine operation (ESX/vCenter) object

Counter name	Description of counter
numChangeDS	Number of virtual machine power on operations [number]
numChangeHost	Number of datastore change operations for powered-off and suspended virtual machines [number]
numChangeHostDS	Number of host change operations for powered-off and suspended VMs [number]
numClone	Number of host and datastore change operations for powered-off and suspended virtual machines [number]
numCreate	Number of virtual machine clone operations [number]
numDeploy	Number of virtual machine create operations [number]
numDestroy	Number of virtual machine template deploy operations [number]
numPoweroff	Number of virtual machine delete operations [number]
numPoweron	Number of virtual machine power off operations [number]
numRebootGuest	Number of virtual machine guest reboot operations [number]
numReconfigure	Number of virtual machine reconfigure operations [number]

numRegister	Number of virtual machine register operations [number]
numReset	Number of virtual machine reset operations [number]
numShutdownGuest	Number of virtual machine guest shutdown operations [number]
numStandbyGuest	Number of virtual machine standby guest operations [number]
numSuspend	Number of virtual machine suspend operations [number]
numSVMotion	Number of migrations with Storage vMotion (datastore change operations for powered-on VMs) [number]
numUnregister	Number of virtual machine unregister operations [number]
numVMotion	Number of migrations with vMotion (host change operations for powered-on VMs) [number]
numXVMotion	Number of host and datastore change operations for powered-on and suspended virtual machines [number]

Power supply (ESX/vCenter) object

Counter name	Description of counter
energy	Total energy used since last stats reset [J]
power	Current power usage [W]
powerCap	Maximum allowed power usage [W]

- End -