HP Operations Smart Plug-in for Virtualization Infrastructure

For the Windows ®, HP-UX, Linux, and Solaris operating systems

Software Version: 11.12

User Guide

Document Release Date: June 2013

Software Release Date: June 2013

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

http://h20230.www2.hp.com/selfsolve/manuals

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

Visit the HP Software Support Online web site at:

http://www.hp.com/go/hpsoftwaresupport

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Contents

User Guide 1

Contents 5

Conventions Used in this Document 10

Introduction 11

VI SPI Monitoring Solution for Virtualization Technologies 11

Monitoring HPVM 12

Monitoring IBM AIX LPAR and WPAR 12

Monitoring Microsoft Hyper-V Servers 14

Monitoring Oracle Solaris Zones 15

Monitoring VMware ESX/ESXi Servers 16

Monitoring KVM or Xen 17

Virtualization Infrastructure SPI Components 19

Map View on HPOM for Windows 19

Map View on HPOM for UNIX 20

Tools 21

Policies 21

Graphs 22

Reports 22

Getting Started 24

On HPOM for Windows 25

Starting the VI SPI 25

Plan the Virtualized Infrastructure 25

Prerequisites for Installing VI SPI Policies 25

Running the Discovery Policies 27

Deploying Quick Start Policies from HPOM for Windows 28

On HPOM for UNIX 29

Running the Discovery Policies on the Virtualized Infrastructure 29

Deploying Quick Start Policies from HPOM for UNIX 29
Viewing Reports and Graphs 31
Integrating HP Performance Manager with HPOM for UNIX 31
Updating Reports after Upgrading the SPI 31
Data Collection for Reports 32
Virtualization Infrastructure SPI Policies and Tools 33
Virtualization Infrastructure SPI Policies 33
Auto Discovery Policy 34
Availability Policies 35
Performance Agent Processes Monitor Policy 35
State Monitor Policy for HPVM Guests 36
State Monitor Policy for IBM Frame and LPAR 37
State Monitor Policy for IBM WPAR 39
State Monitor Policy for Microsoft Hyper-V Guests 40
State Monitor Policy for Oracle Solaris Zones 41
State Monitor Policy for VMware ESX or ESXi Servers 42
State Monitor Policy for KVM or Xen Guests 43
Host Service Monitor Policy for Microsoft Hyper-V 44
Process Monitoring Policy for HPVM 45
Process Monitoring Policies for Oracle Solaris Zones 45
Data Collector Policy for IBM HMC 46
State Monitor Policy for VMware vCenter 47
Capacity Policies 48
VMFS Utilization Monitor Policy for VMware ESX or ESXi Servers 48
Memory Usage Monitor Policy for VMware ESX or ESXi Servers 50
Host Disk Usage Monitor Policy for VMware ESX or ESXi Servers 52
Event Monitoring Policies 54
Event Type Policy for VMware ESX or ESXi Servers 54
Event Type Policy for VMware vCenter 55
Event Monitoring Policy for VMware ESX or ESXi Servers 56
Event Monitoring Policy for VMware vCenter 56
Hardware Monitoring Policies 57

Hardware Data Collector Policy for VMware Datacenter 57
Host Ethernet Port Health Monitor Policy for VMware ESX or ESXi Servers 58
Host Sensor Health Monitor Policy for VMware ESX or ESXi Servers 59
Host Chassis Health Monitor Policy for VMware ESX or ESXi Servers 60
Host Processor Health Monitor Policy for VMware ESX or ESXi Servers 61
Host Fan Health Monitor Policy for VMware ESX or ESXi Servers 62
Host Physical Memory Health Monitor Policy for VMware ESX or ESXi Servers ... 63
Log Monitoring Policies 63
Image Management Service Administration Logfile Monitoring Policy 64
Image Management Service Operational Logfile Monitoring Policy for Microsoft Hyper-V 64
Hypervisor Administration Logfile Monitoring Policy for Microsoft Hyper-V 64
Hypervisor Operational Logfile Monitoring Policy for Microsoft Hyper-V 65
VMMS Administration Logfile Monitoring Policy for Microsoft Hyper-V 65
VMMS Operational Logfile Monitoring Policy for Microsoft Hyper-V 67
Hypervisor Worker Administration Logfile Monitoring Policy for Microsoft Hyper-V .69
Hypervisor Worker Operational Logfile Monitoring Policy for Microsoft Hyper-V 70
Performance Policies 70
Host CPU Utilization Monitor Policy for HPVM 71
Host CPU Utilization Monitor Policy for IBM LPAR 72
Host CPU Utilization Monitor Policy for Microsoft Hyper-V 73
Host CPU Utilization Monitor Policy for Oracle Solaris Zones 74
Total VM CPU Utilization Monitor Policy for VMware ESX or ESXi Servers 75
Host CPU Utilization Monitor Policy for VMware ESX or ESXi Servers 77
Host CPU Utilization (by Virtual Machines) Monitor Policy for VMware ESX or ESXi Servers 78
Host CPU Utilization Monitor for VMware vCenter 80
Total Frame CPU Utilization Monitor Policy for IBM LPAR 81
CPU Entitlement Utilization Monitor Policy for HPVM 83
CPU Entitlement Utilization Monitor Policy for IBM LPAR 85
CPU Entitlement Utilization Monitor Policy for IBM WPAR 87
CPU Entitlement Utilization Monitor Policy for Microsoft Hyper-V 90
CPU Entitlement Utilization Monitor Policy for Oracle Solaris Zones 92

CPU Entitlement Utilization Monitor Policy for VMware ESX or ESXi Servers 94
CPU Saturation Monitor Policy for VMware vCenter 96
Memory Entitlement Utilization Monitor Policy for IBM LPAR 98
Memory Entitlement Utilization Monitor Policy for IBM WPAR 100
Memory Entitlement Utilization Monitor Policy for Oracle Solaris Zones 102
Network Interface In-Byte Rate Monitor Policy for VMware ESX or ESXi Servers 104
Network Interface Out-Byte Rate Monitor Policy for VMware ESX or ESXi Servers 106
Network Interface Card Monitor Policy for VMware ESX or ESXi Servers 109
Memory Performance Monitor Policy for VMware ESX or ESXi Servers 110
Host Memory Health Monitor Policy for VMware ESX or ESXi Servers 111
Host Memory Utilization (by Virtual Machines) Monitor Policy for VMware ESX or ESXi Servers 113
Memory Utilization (by Virtual Machines) Monitor Policy for VMware ESX or ESXi Servers 115
Memory Utilization Monitor policy for VMware vCenter 116
Total Memory Utilization (by Virtual Machines) Monitor Policy for VMware ESX or ESXi Servers 118
Frame Memory Utilization Monitor Policy for IBM LPAR 119
Physical Memory Utilization Monitor Policy for Oracle Solaris Zones 120
Swap Utilization Monitor Policy for Oracle Solaris Zones 121
Data Collector Policy for VMware Datacenter 123
CPU Utilization Monitor Policy for VMware Datacenter 124
Memory Utilization Monitor Policy for VMware Datacenter 125
Datastore Utilization Monitor Policy for VMware Datacenter 126
Datastore SpaceUtilization Monitor Policy for VMware vCenter 127
VMFS Utilization Data Collector Policy for VMware ESX or ESXi Servers 128
VMFS Read Latency Monitor Policy for VMware ESX or ESXi Servers 129
VMFS Write Latency Monitor Policy for VMware ESX or ESXi Servers 131
Guest Latency Monitor Policy for VMware vCenter 132
Disk Error Monitor Policy for VMware ESX or ESXi Servers 133
Disk Throughput Monitor Policy for VMware ESX or ESXi Servers 134
Vifp Target Check Policy for VMware ESX or ESXi Servers 136
Host CPU Utilization Monitor Policy for KVM or Xen 136

Guest CPU Utilization Monitor Policy for KVM or Xen 137
Physical Disk Byte Rate Baseline Policy for KVM or Xen 138
Net Byte Rate Baseline Policy for KVM or Xen 141
Guest Total CPU Utilization Monitor Policy for KVM or Xen 143
Memory Utilization Monitor Policy for KVM or Xen Host 145
Memory Performance Monitor Policy for KVM or Xen 147
Memory Usage Policy for KVM or Xen 148
Trending Based Alert Mechanism 150
Deploying VI SPI Policies from HPOM for UNIX Management Server 159
Virtualization Infrastructure SPI Tools 159
Host Information Tool 160
Guest Information Tool 160
List of Suspended Virtual Machines Tool 160
List of Virtual Machines Tool 161
Resource Pool Information Tool 161
Overall Status for VMware vMA Tool 161
Virtualization Infrastructure SPI Reports and Graphs 162
Virtualization Infrastructure SPI Reports 162
Virtualization Infrastructure SPI Graphs 166
Troubleshooting 170
Discovery 170
Policies 171
VI SPI Scripts 176
HP Operations Agent 176
A) Virtualization Infrastructure SPI Metrics 178
Metrics Collected by VI-VMwareVMFSDataCollector Policy 178
Metrics Collected by VI-VMwareDCDataCollector Policy 180
Metrics Collected by VI-VMwareHardwareHealthCollector Policy 180
Metrics Collected by VI-IBMHMCDataCollector Policy 183
Policies which work on ESX, ESXi, or vCenter 184
Additional Monitoring Features Supported for ESX/ESXi or vCenter 187

Chapter 1

Conventions Used in this Document

The following conventions are used in this document.

Convention	Description
HPOM for UNIX	HPOM for UNIX is used in the document to imply HPOM on HP-UX, Linux, and Solaris. Wherever required distinction is made for a specific operating system as: • HPOM on HP-UX • HPOM on Linux • HPOM on Solaris
Infrastructure SPIs	HP Operations Smart Plug-ins for Infrastructure. The software suite includes three Smart Plug-ins: • HP Operations Smart Plug-in for Systems Infrastructure • HP Operations Smart Plug-in for Virtualization Infrastructure • HP Operations Smart Plug-in for Cluster Infrastructure
SI SPI	HP Operations Smart Plug-in for Systems Infrastructure
VI SPI	HP Operations Smart Plug-in for Virtualization Infrastructure
CI SPI	HP Operations Smart Plug-in for Cluster Infrastructure

Chapter 2

Introduction

The HP Operations Smart Plug-in for Virtualization Infrastructure (VI SPI) enables you to manage and monitor virtual infrastructure on various technologies from an HP Operations Manager (HPOM) console. VI SPI adds monitoring capabilities otherwise unavailable to HPOM. For more information about HPOM, see the *HP Operations Manager for UNIX Concepts Guide.*

The VI SPI monitors the performance, capacity, utilization, availability, and resource consumption of the host machines, virtual machines, and resource pools.

For information about which vendor versions are supported by the VI SPI, see the *HP Operations Smart Plug-in for Virtualization Infrastructure Release Notes*.

The VI SPI is a part of the HP Operations Smart Plug-ins for Infrastructure suite (Infrastructure SPIs). The other components in the suite include the Systems Infrastructure Smart Plug-ins (SI SPI), the Cluster Infrastructure Smart Plug-ins (CI SPI), the Report pack and the Graph pack. Installation of SI SPI is mandatory while installing other components from the Infrastructure SPIs media.

Note: HP Reporter 4.0 is supported on 64-bit Windows operating system.

The VI SPI also integrates with other HPOM products such as HP Performance Manager, HP Performance Agent, and HP Reporter.

VI SPI Monitoring Solution for Virtualization Technologies

Virtualization Infrastructure Smart Plug-ins 11.12 supports virtualization technologies from the following vendors:

- HP Integrity Virtual Machines (HPVM)
- IBM LPAR and WPAR
- Microsoft Hyper-V
- Oracle Solaris Zones
- VMware ESX/ESXi servers
- Kernel-based Virtual Machines (KVM) or Xen

To monitor these technologies, ensure that the following software is installed on the node (host/monitoring system):

- HP Operations agent 11.xx
- (Optional) HP Performance Manager 8.20 (or higher) if you want to view graphs
- (Optional) HP Reporter 3.80 (or higher) if you want to view reports

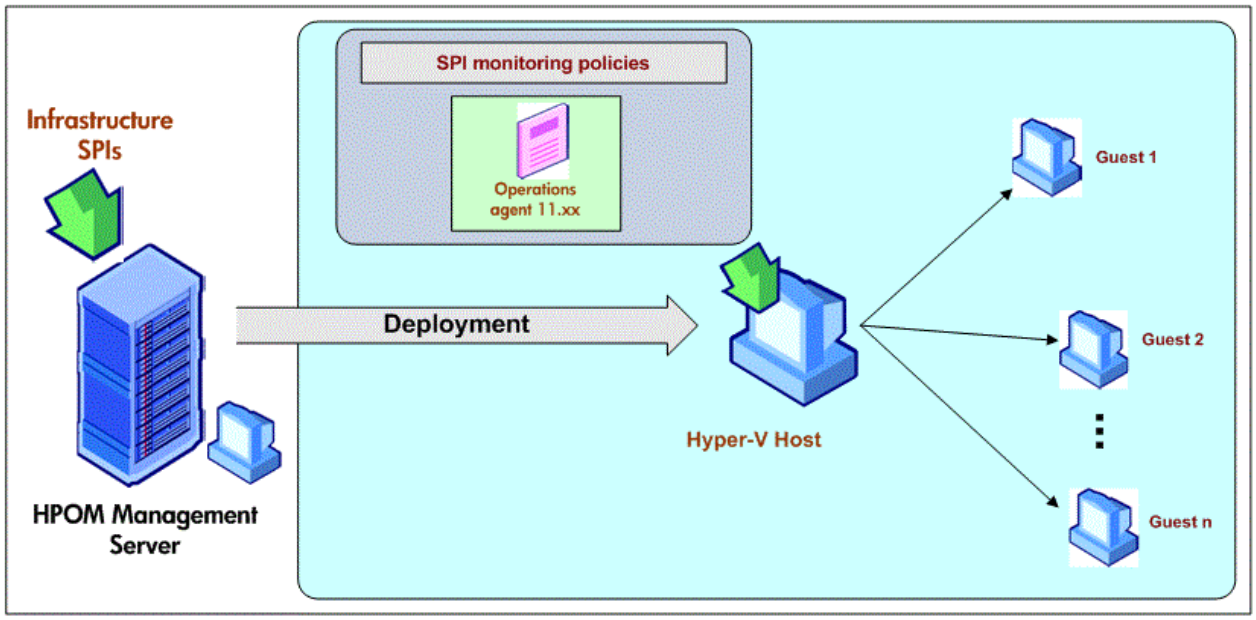
Monitoring HPVM

You must deploy VI SPI, for the HPVM environment, on the HPVM host. VI SPI enables you to monitor the availability and performance of HPVM hosts and the guest machines running on the hosts.

VI SPI sends alert messages to the HPOM console based on the threshold values set in the HPVM specific policies.

HP Operations agent 11.xx and the VI SPI are deployed on the HPVM host.

The following illustration shows a typical HPVM environment with VI SPI deployed on an HPVM host:



Monitoring IBM AIX LPAR and WPAR

VI SPI, for IBM AIX LPARs, is deployed on an LPAR within a frame. This LPAR can be called as a monitoring LPAR because it monitors other LPARS within the frame. Each frame must contain at least one monitoring LPAR. If you want to monitor the availability of all the LPARs and Frames in a Hardware Monitoring Console (HMC) environment, make one monitor LPAR as Configuration LPAR.

VI SPI sends alerts to the HPOM console based on the threshold values set in the IBM Frame, LPAR, and WPAR specific policies.

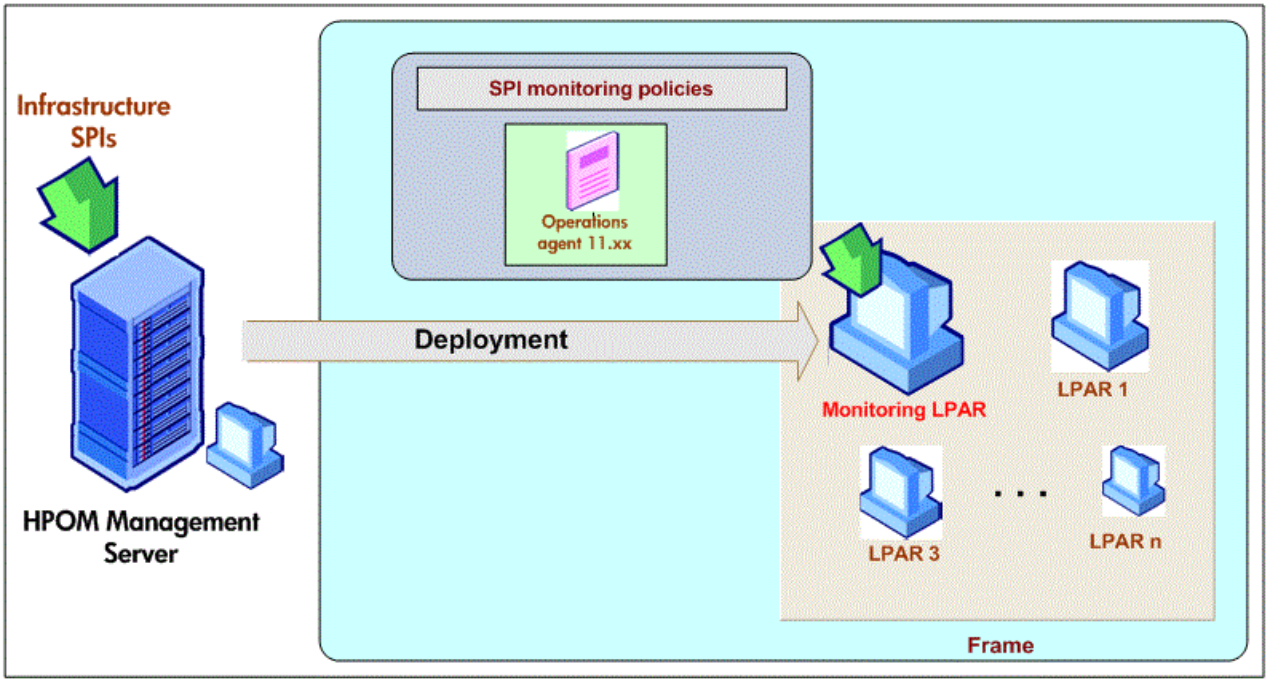
You can also configure VI SPI to monitor the HMCs connected with the frames.

Scenario 1: Monitoring the LPARs, Frame, and WPARs

VI SPI, deployed on the monitoring LPAR, monitors the availability and performance of the monitoring LPAR. VI SPI also enables you to monitor the availability and performance of the frame, other LPARs within the frame, and the WPARs running on the monitoring LPAR (VI SPI monitors only the WPARs created on the monitoring LPAR.)

HP Operations agent 11.xx and the VI SPI are deployed on the monitoring LPAR.

The following illustration shows a typical AIX LPAR environment with the monitoring solution deployed on an LPAR within a frame:



Scenario 2: Monitoring the LPARs, Frame, WPARs, and HMCs

You can configure VI SPI to collect state related (of LPARs and frames) and configuration metrics from the HMCs connected to frames. The information gathered from the HMC is used for reporting and graphing. It is also used for state monitoring.

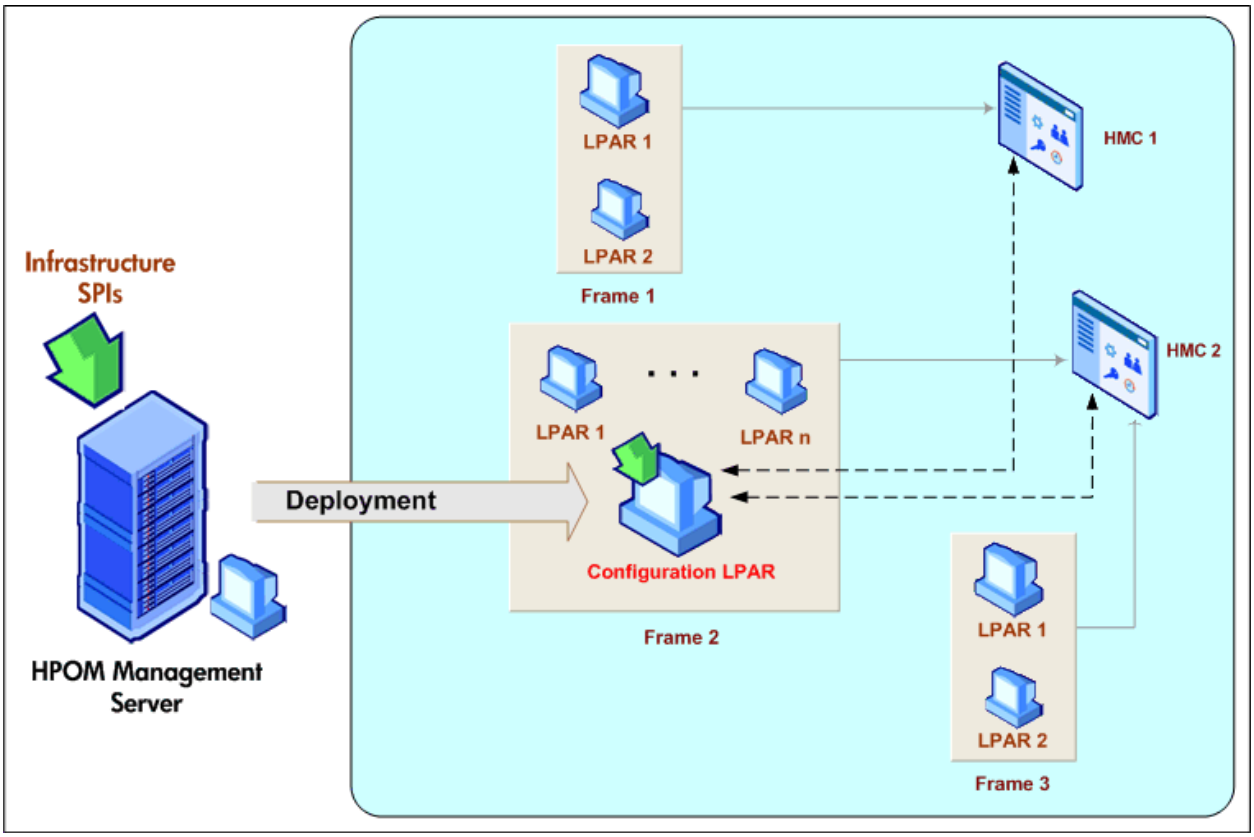
VI SPI is deployed on the LPAR to which the HMCs are connected. This LPAR can be called as a configuration LPAR. The configuration LPAR monitors:

- The WPARs running within the configuration LPAR.
- The state of all the frames and LPARs connected to the HMCs.
- Configuration information of all the frames and LPARs connected to the HMCs.

After deploying the VI SPI, run the *getSSHAuthentication.pl* script on the monitor/configuration LPAR connected to the HMC. This script is located under the */var/opt/OV/bin/instrumentation* directory on the LPAR.

The *getSSHAuthentication.pl* script provides you password-less authentication to access the configuration information on the HMC.

The following illustration shows a typical setup where different frames are managed by HMCs. These HMCs are in turn connected to the configuration LPAR.



Monitoring Microsoft Hyper-V Servers

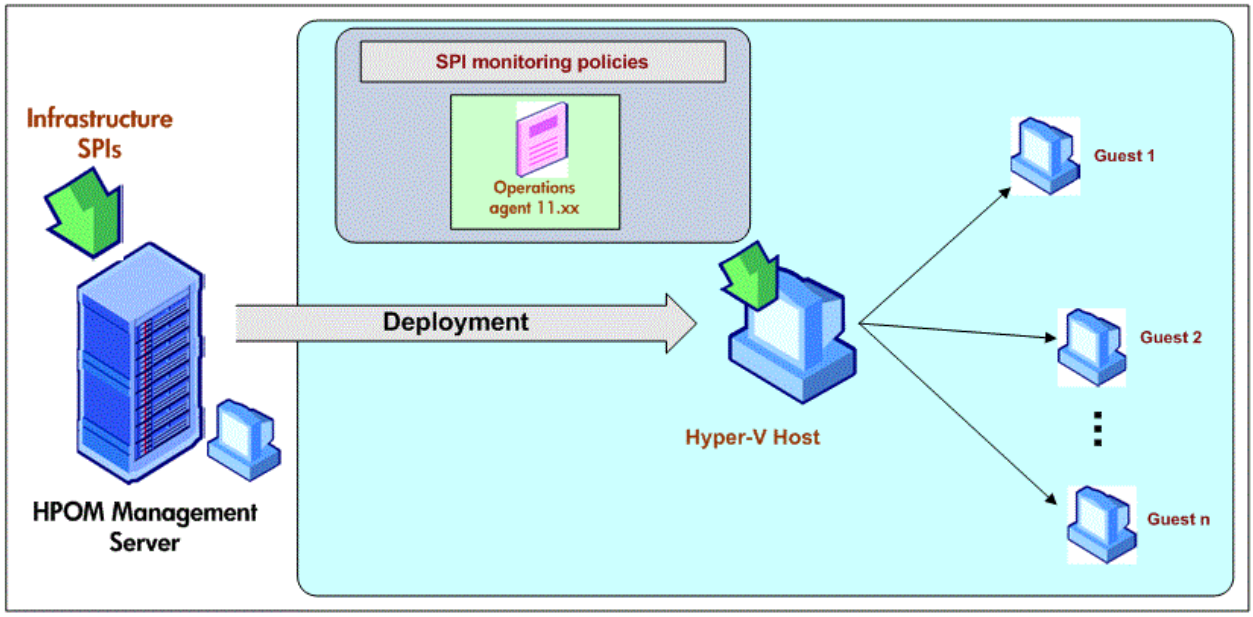
You must deploy VI SPI, for the Hyper-V environment, on the Hyper-V host. VI SPI enables you to:

- Monitor the availability and performance of Hyper-V hosts, and the guest systems running on the hosts.
- Monitor events.

VI SPI sends alert messages to the HPOM console based on the threshold values set in the Hyper-V specific policies.

HP Operations agent 11.xx and the VI SPI are deployed on the Hyper-V host.

The following illustration shows a typical Hyper-V environment with VI SPI deployed on a Hyper-V host:



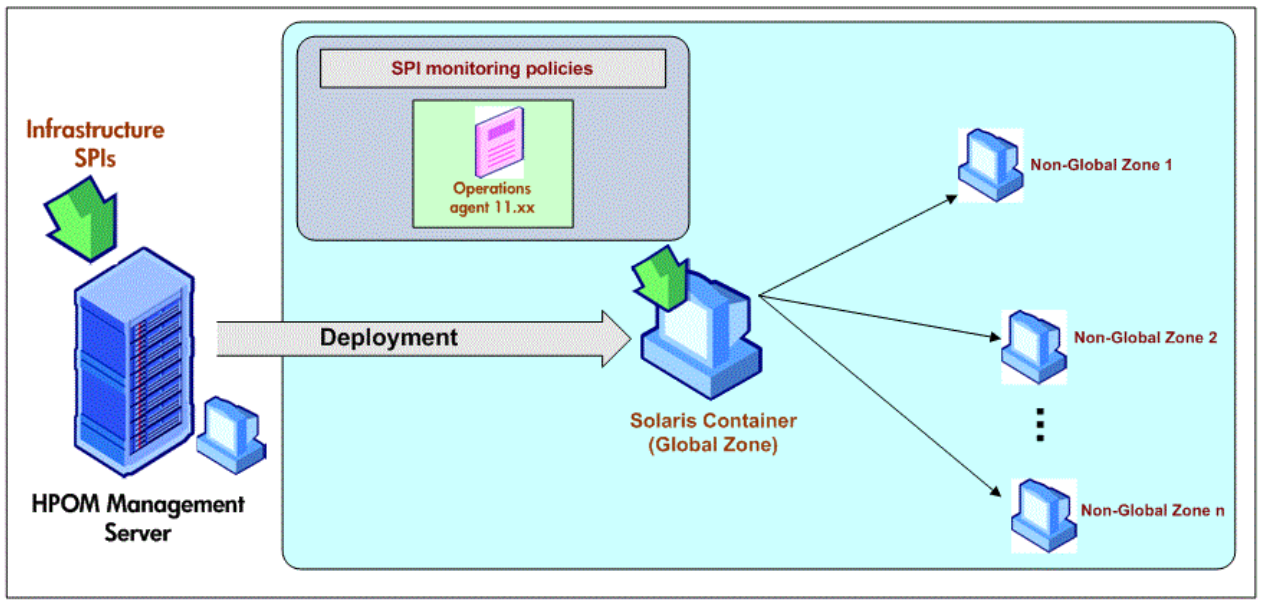
Monitoring Oracle Solaris Zones

You must deploy VI SPI, for the Solaris Zones environment, on the Solaris global zone. VI SPI enables you to monitor the availability and performance of the global zone, and the local zones running on the global zone.

VI SPI sends alert messages to the HPOM console based on the threshold values set in the Oracle Solaris Zones specific policies.

HP Operations agent 11.xx and the VI SPI are also deployed on the Solaris container.

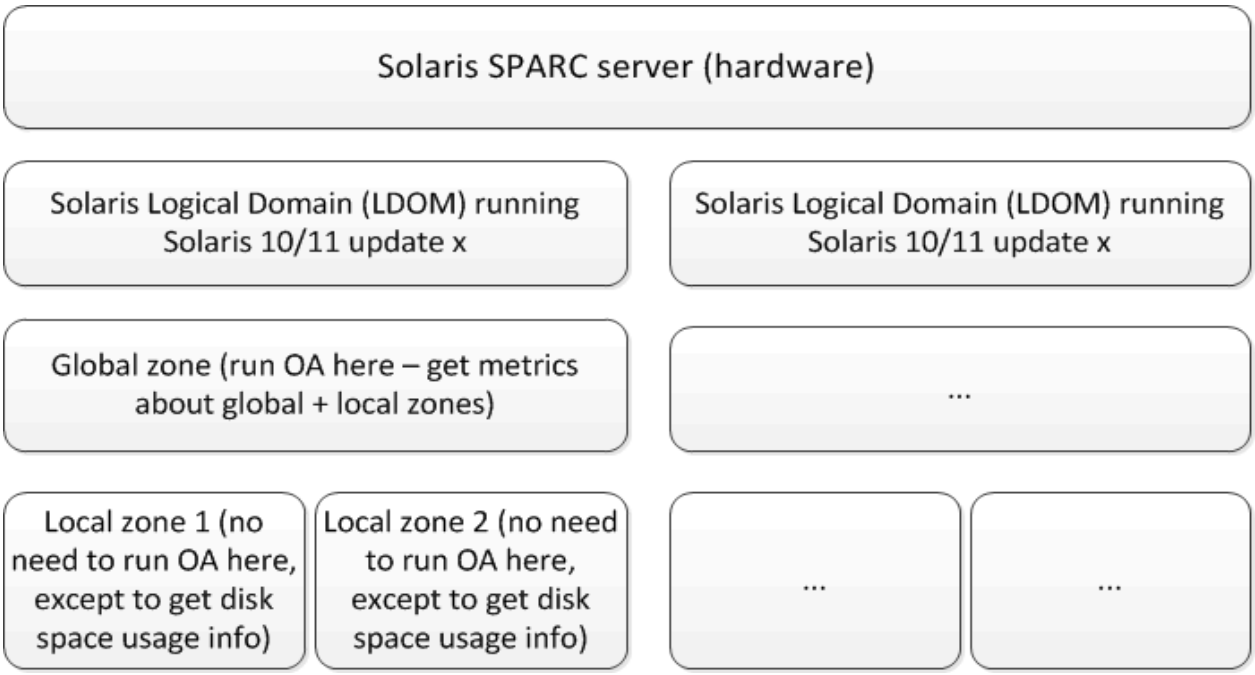
The following illustration shows a typical Solaris Zones environment with VI SPI deployed on a global zone:



VI SPI installation is only supported on global zone. The installation discovers and monitors only the global and non-global zones associated with it.

Note: VI SPI is not aware of LDOMs.

The following illustration shows VI SPI policies deployed on a global zone on a LDOM server.



Monitoring VMware ESX/ESXi Servers

You must deploy VI SPI, for the VMware environment, on a vMA machine. VI SPI enables you to:

- Gather the availability and capacity information of multiple VMware ESX/ESXi hosts, guests, and resource pools associated with the hosts.
- Monitor the performance of VMware ESX/ESXi hosts and guests.
- Monitor events.

HP Operations agent 11.xx and the VI SPI are deployed on a vMA, which is a virtual machine hosted on a VMware ESX/ESXi host. It is used to perform most of the tasks performed in the ESX/ESXi service console.

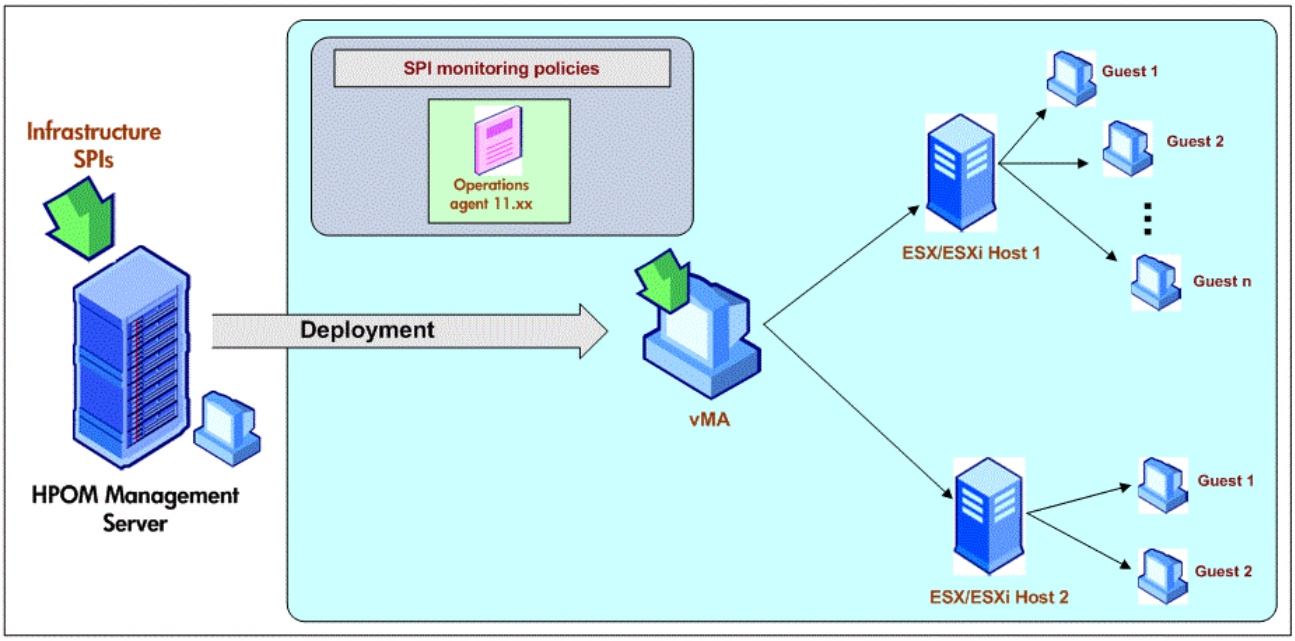
vMA is a standard VM used to run scripts or agents that manage VMware ESX/ESXi hosts and guests. A single vMA installation can manage events and performance data for multiple VMware ESX/ESXi hosts, associated guests, and resource pools.

VI SPI sends alert messages to the HPOM console based on the threshold values set in the VMware specific policies.

Note: VI SPI does not require any VMware SDK to monitor VMware ESX/ESXi hosts and

guests. VMware SDK packages are available on vMA after the vMA is created. You need not install these packages separately unless vMA installation was erroneous.

The following illustration shows a typical VMware environment with VI SPI deployed on a vMA:



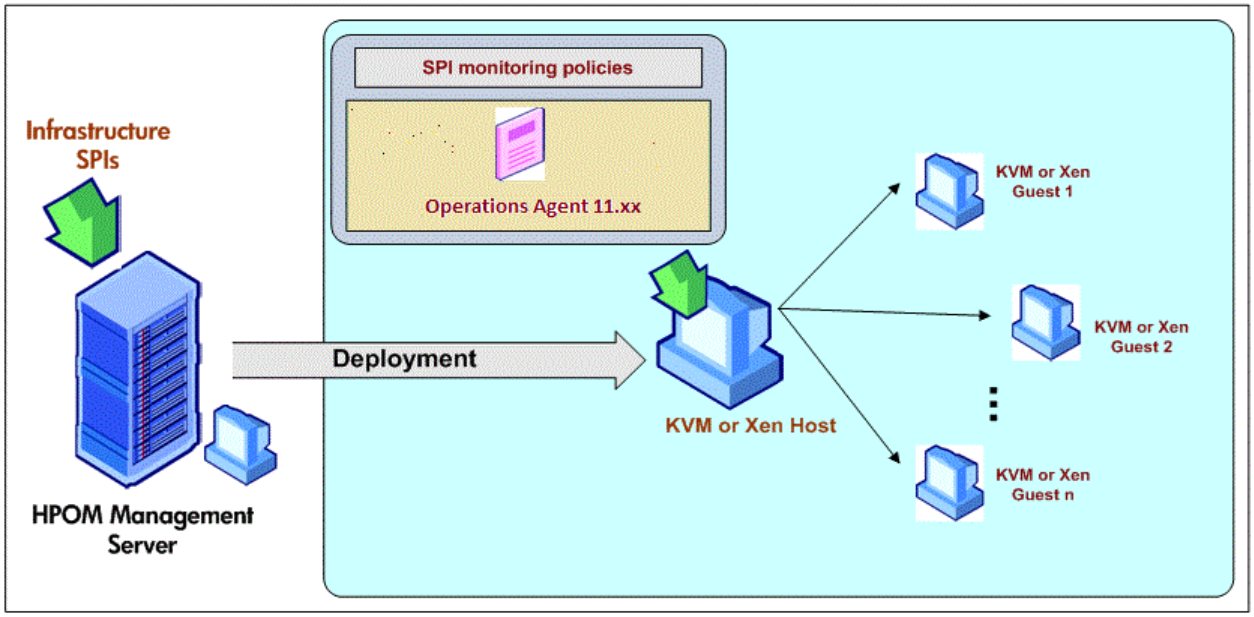
Monitoring KVM or Xen

You must deploy VI SPI, for the KVM or Xen environment, on the KVM or Xen host. VI SPI enables you to monitor the availability and performance of KVM or Xen hosts, and the guest machines running on the hosts.

VI SPI sends alert messages to the HPOM console based on the threshold values set in the KVM or Xen specific policies.

HP Operations agent 11.xx and the VI SPI are deployed on the KVM or Xen host.

The following illustration shows a typical KVM or Xen environment with VI SPI deployed on an KVM or Xen host:


SPI monitoring policies
Operations Agent 11.xx
Infrastructure SPIs
HPOM Management Server
Deployment
KVM or Xen Host
KVM or Xen Guest 1
KVM or Xen Guest 2
KVM or Xen Guest n

Chapter 3

Virtualization Infrastructure SPI Components

The Virtualization Infrastructure SPI provides preconfigured policies and tools for monitoring the operations, availability, and performance of host servers, virtual machines, and resource pools. These policies and tools, along with discovery, enable you to quickly gain control of the essential elements of your virtual IT infrastructure.

Map View on HPOM for Windows

After installing VI SPI, if you add nodes to the HPOM server with the *AutoDeployConfig* turned `on`, the Systems Infrastructure SPI (SI SPI) service discovery policy is automatically deployed to the node.

Note: If you added the nodes before installing the VI SPI, you must manually deploy the SI SPI service discovery to the nodes.

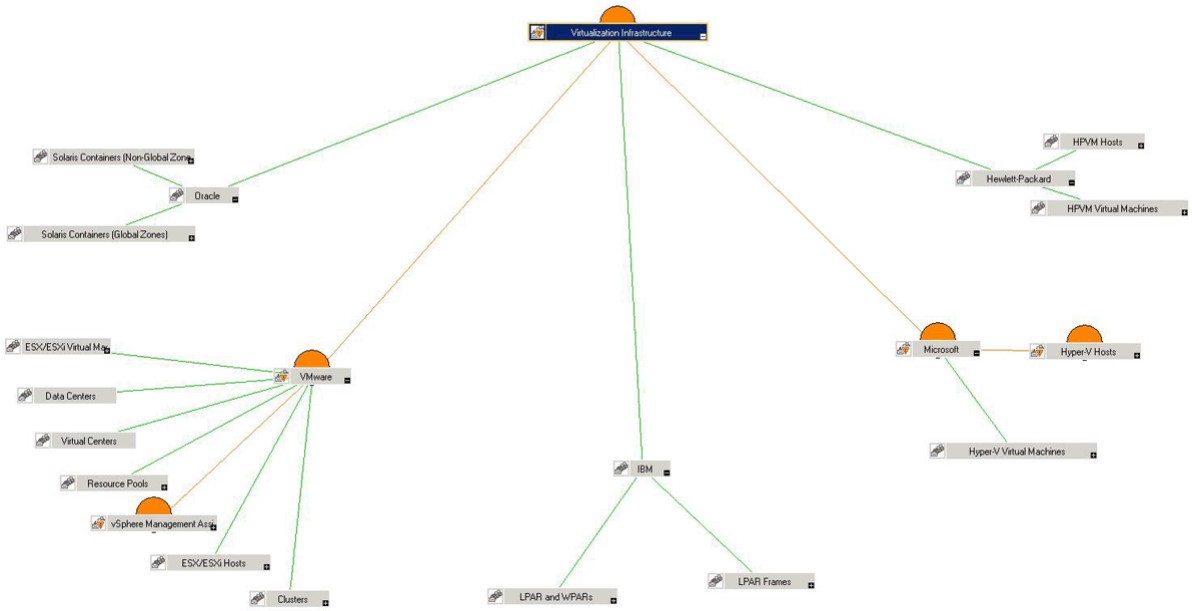
Before the discovery policy identifies the node, read the *Starting the VI SPI* section of the *HP Operations Infrastructure Smart Plug-ins Installation Guide*. This section describes about the prerequisites for deploying the VI SPI policies.

After the discovery policy identifies the node as a HPVM host, Solaris container, AIX frame, VMware vMA or Hyper-V host, it triggers the auto-deployment of the VI SPI discovery policy. The VI SPI discovery adds discovered information to the HPOM Services area. This information is used to populate the VI SPI map view for the managed nodes.

The map view displays the real-time status of your infrastructure environment. To see the map view select **Services** from the console tree and click **Virtualization Infrastructure.** The map view graphically represents the structural view of your virtualization infrastructure or node hierarchy in the infrastructure environment.

The graphical representation of discovered elements in the service views enables speedy diagnosis of problems on your virtualized systems.

- To see the root cause of any problem indicated in your message browser, click **View** → **Root Cause**.
- To display the services and system components affected by a problem, click **View** → **Impacted**.



The icons and lines in your map are color-coded to indicate the severity levels of items in the map and to show status propagation. Use the map view to drill down to the level in your node or service hierarchy where a problem is occurring.

Map View on HPOM for UNIX

Before the discovery policy identifies the node, read the *Starting the VI SPI* section of the *HP Operations Infrastructure Smart Plug-ins Installation Guide*. This section describes about the prerequisites for deploying the VI SPI policies.

The map view displays the real-time status of your virtual infrastructure environment. To ensure that the operator can see the service map in the HPOM for UNIX (HP-UX, Linux, and Solaris) Operational interface, run the following commands on the management server:

```
opcservice -assign <operator name> AutoDiscovery
```

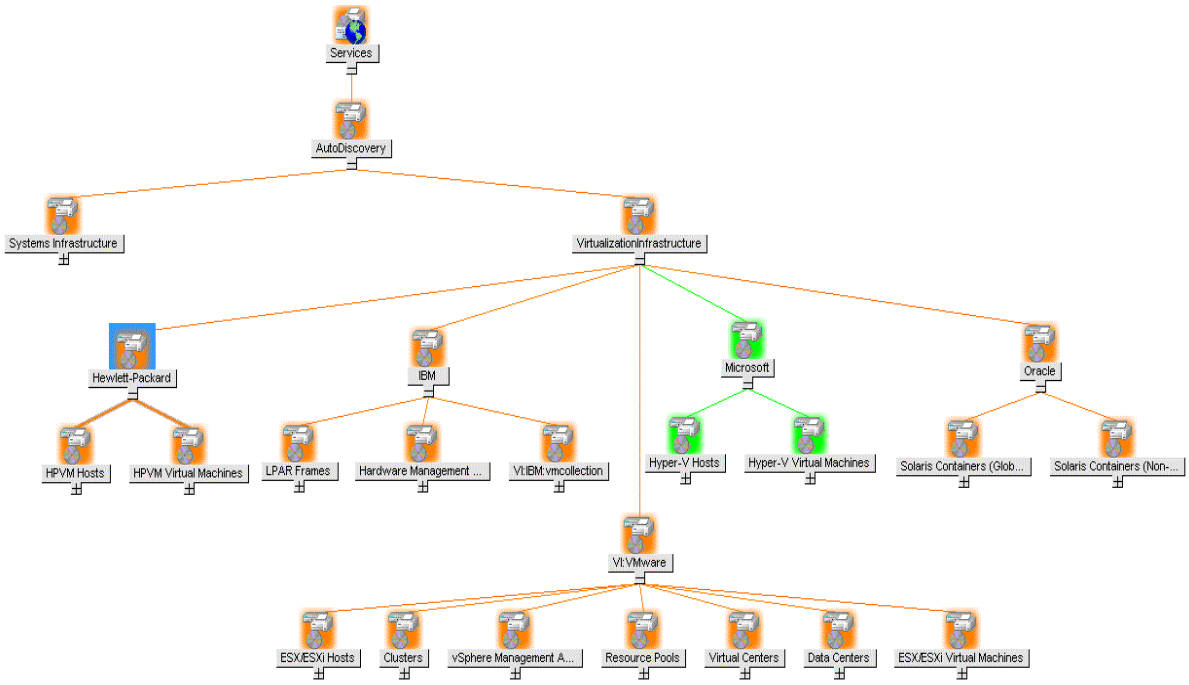
In this instance, `<operator name>` is the operator (for example, opc_adm or opc_op) to which you want to assign the service.

The service discovery policy does not automatically deploy policies to the nodes. You can manually deploy them.

The map view displays the real-time status of your virtual infrastructure environment.

To see the map view, follow these steps:

1. Launch the HPOM Operational interface.
2. Log on using your user name and password.
3. Select **Services** → **Virtualization Infrastructure** → **Show Graph**, to see the map view.



The map view graphically represents the structural view of your virtualization infrastructure hierarchy in the infrastructure environment.

Tools

You can access Virtualization Infrastructure SPI tools at: **Tools → Virtualization Infrastructure.** These tools display data collected for a particular managed node. For more information about the tools provided by Virtualization Infrastructure SPI, see "Virtualization Infrastructure SPI Tools" on page 159.

Policies

On HPOM for Windows, several default policies are automatically deployed on the supported managed nodes during installation. These can be used as-is to begin receiving virtualized infrastructure related data and messages from the environment. You can choose to turn off automatic deployment of policies when services are discovered. In addition, you can modify and save preconfigured policies with new names to create custom policies for your own specialized purposes. For information about deploying policies from the management server, see "Deploying VI SPI Policies from HPOM for Windows Management Server" on page 157.

On HPOM for UNIX (HP-UX, Linux, or Solaris) the discovery policy does not automatically deploy policies to the nodes. You can manually deploy them. For information about deploying policies from the management server, see "Deploying VI SPI Policies from HPOM for UNIX Management Server" on page 159.

The policy types are as follows:

- **Service/Process Monitoring policies** provide a means for monitoring system services and processes.

- **Logfile Entry policies** capture status or error messages generated by the system nodes and resource groups application.
- **Measurement Threshold policies** define conditions for each metric so that the collected metric values can be interpreted and alert messages can be displayed in the message browser. Each measurement threshold policy compares the actual metric value against the specified/auto threshold. If the actual value meets or exceeds the threshold, it generates message and instruction text that help you resolve a situation.
- **Scheduled Task policies** determine when and what metric values are to be collected and defines the collection interval. The collection intervals can be 5 minutes, 15 minutes, one hour, or one day. The collection interval indicates how often data is collected for a specific group. The scheduled task policy has two functions: to run the collector/analyzer at each collection interval on a node and to collect data for all metrics listed within the polices **Command** text box.
- **Service Discovery policy** discovers individual system nodes and resource group instances and builds a map view for all Virtualization Infrastructure SPI discovered instances.
- **Config Policies** provide a means for user-defined metrics.

The Virtualization Infrastructure SPI provides a set of pre-configured policies to help the system administrators efficiently monitor the virtual infrastructure. The VI SPI policies begin with **VI** for easy identification and modification.

These policies can be customized to suit specific needs. For information about the policies provided by Virtualization Infrastructure SPI, see "Virtualization Infrastructure SPI Policies" on page 33.

Graphs

The VI SPI enables you to see and trace out the root cause of any discrepancy in the normal behavior of an element being monitored. HPOM is integrated with HP Performance Manager, a web-based analysis tool that helps you to see, evaluate, and compare performance between virtual systems. Using HP Performance Manager you can see any of the following:

- Graphs such as line, bar or area
- Tables for data such as process details
- Baseline graphs
- Dynamic graphs in Java format that allow you to turn off display of individual metrics or hover over a point on a graph and see the values displayed

You can see the data represented graphically, for quick and easy analysis of a serious or critical error message reported. For more information about the graphs provided by Virtualization Infrastructure SPI, see "Virtualization Infrastructure SPI Graphs" on page 166.

Reports

You can integrate the VI SPI by installing the HP Reporter to generate web-based reports on metric data.

If HP Reporter is installed on the HPOM management server for Windows, you can view reports from the console. To see a report, expand **Reports** in the console tree, and then double-click individual reports.

If HP Reporter is installed on a separate system connected to the HPOM management server (for Windows, UNIX, Linux, or Solaris operating system), you can see the reports on HP Reporter system. For more information about integration of HP Reporter with HPOM, see *HP Reporter Installation and Special Configuration Guide*.

For information about the reports provided by Virtualization Infrastructure SPI, see "Virtualization Infrastructure SPI Reports" on page 162.

Chapter 4

Getting Started

After you install the infrastructure SPIs on the HPOM for Windows management server or HPOM for UNIX management server, you must complete the tasks required to manage your infrastructure.

The deployment checklist summarizes the tasks that you must complete before you start deploying the policies.

Deployment Checklist

Complete (Y/N)	Tasks
	Verify that you have installed HPOM 9.10 on the management server. In addition, verify that HP Operations Agent version 11.00 or above is installed. Make sure that you have installed all the available patches and hotfixes for HPOM and HP Operations agent.
	Verify that you have Performance Manager and HP Reporter installed to generate the graphs and reports.
	If you use VI SPI to monitor VMware environment, make sure vMA appliance is created and the recommended resource configuration is used.
	If you use VI SPI to monitor VMware environment, make sure ESX/ESXi hosts and vCenter servers are added to vMA.
	Make sure that you give sufficient time to HP Operations agent to collect the metrics before you start deploying the monitoring policies.

On HPOM for Windows

Follow the steps to getting started on HPOM for Windows.

Starting the VI SPI

To get started with discovering the virtualized infrastructure, the first step is to run the SI SPI discovery.

Plan the Virtualized Infrastructure

For monitoring VMware environment, follow these steps:

1. Add the ESX/ESXi hosts as targets to the vMA.

   Run the command vifp addserver <ESX host>.

2. To monitor events from vCenter, add vCenter as target to vMA.

   Run the command vifp addserver <vCenter>.

Note: For a single vMA, HP Operations agent can monitor the maximum of 20 ESX hosts and 400 instances (ESX/ESXi ,VMs, resource pools, VCenter).

Note: For information about configuring vMA 5.0.0.2 with vi admin user, see the section Configure the Agent User during Installation in the *Operation Agent User Guide*.

Prerequisites for Installing VI SPI Policies

Before deploying the VI SPI policies, ensure the following:

- Install the latest HPOM patches. Make sure to check if you have installed OMW_000120 or higher patches.
- HP Operation agent 11.xx is installed and running.
- *logicalsystem* is appended to the `parm` file on vMA and HyperV host. Follow these steps:
  a. *On UNIX hosts,*

     go to the directory `/var/opt/perf` and open the `parm` file.

     On Windows hosts,

     go to the directory `%ovdatadir%` and open the `parm` file.

  b. *On Windows, Linux, UNIX or Solaris*

     Append the text **logicalsystem** at the end of the following line:

     ```
     application process device=disk,cpu,filesystem
     transaction
     ```
     logicalsystem

Note: Logical system is supported on Solaris 10 or above.

On AIX

Append the text **logicalsystems** at the end of the following line:

```
application process device=disk,cpu,filesystem
transaction
```
logicalsystems

For enabling LPAR logging, set `logicalsystems=lpar`

For enabling WPAR logging, set `logicalsystems=wpar`

For enabling both LPAR and WPAR logging, set

`logicalsystems=lpar,wpar` or `logicalsystems=wpar,lpar` or `logicalsystems=all`

Note: Logical system is supported for LPAR on AIX 5L V5.3 ML3 or above and WPAR on AIX 6.1 TL2 global environment only.

c. For VMware, modify the settings in the `viserver.properties` file on vMA.

```
jvmArgs=-Xms512m -Xmx1024m -classpath ........
```

```
kill -9 <pid of viserver>
```

go to directory `/var/opt/perf`

```
rm –rf .viserver.lock
```

d. Restart HP Operations agent 11.xx. Run the following command:

On Windows

```
%ovinstalldir%bin\ovpacmd REFRESH COL
```

On HP-UX, Linux, or Solaris

```
/opt/perf/bin/ovpa -restart scope
```

On AIX

```
/usr/lpp/perf/bin/ovpa -restart scope
```

Wait for 10 to 15 minutes for collection to start.

Run the following command to check if BYLS data is being collected:

On Windows

```
ovcodautil -dumpds scope | findstr BYLS
```

On UNIX

```
ovcodautil -dumpds scope | grep BYLS
```

e. On the node, run the command to update the instance deletion threshold value :

```
ovconfchg -ns agtrep -set
```

```
INSTANCE_DELETION_THRESHOLD 3

ovconfchg -ns agtrep -set

RESEND_RELATIONSHIP_INSTANCES TRUE
```

By default, the threshold value is set to 5.

f. On the server, to update and increase the action agent timeout value, run the following command:

```
ovconfchg -ns eaagt -set OPC_KILL_AUTO_ACTION_TIMEOUT 4000
```

By default, the value is set to 600.

For more information about the commands, see *HPOM Online Help*.

- The Agent settings available under **Infrastructure Management → Settings and Thresholds** are deployed on the virtualized nodes (hypervisors and managed proxies.)
- Infrastructure SPI messages from the messages policy groups are deployed on the virtualized nodes (hypervisors and managed proxies.)
- Make sure that HP Performance Manager is installed (to view graphs) on the HPOM server.

Tip: It is recommended that you install VMware Tools on all guest machines to enhance the performance of virtual machine's guest operating system. VMware tools give you the ability to shutdown guest operating system, synchronize time between guest and host operating system, and so on. It also sends heartbeat to VMware Server.

Although a guest operating system can run without VMware Tools, you lose important capabilities and convenience to use the virtual machine.

Running the Discovery Policies

After the SI SPI discovery has identified a node as a virtualization node, the VI SPI discovery is auto-deployed. The virtual machines running on those nodes are added under the respective Virtualization Infrastructure node group and the vendor specific QuickStart policies are auto-deployed on those nodes.

The discovered managed nodes are regrouped in the console tree under the following Node folders:

- **Nodes→ InfraSPI Managed Nodes→ Hypervisor Hosts and Proxies**
- **Nodes→Virtualization→** *<vendor name>*

The VI SPI discovery policy adds the discovered elements to the HPOM service map. Select **Services→ Virtualization Infrastructure**, to view the VI SPI service map.

Note: If the discovery map for virtualization is not appearing, see Problem: Discovery map for VI SPI is not appearing.

Deploying Quick Start Policies from HPOM for Windows

After the SI SPI discovery runs successfully, the discovered nodes are automatically added to the relevant Infrastructure SPI node groups.

By default, QuickStart policies are assigned to these node groups. When a node is added to the node group, these QuickStart policies get automatically deployed to the managed nodes (if policy autodeployment is enabled).

After the infrastructure is discovered and the service map is populated on the HPOM for Windows management server, the QuickStart policies are automatically deployed to the managed nodes (if policy autodeployment is enabled). Available for all three Infrastructure SPIs, QuickStart policies get you started immediately without having to spend much time customizing settings. Autodeployment of policies is enabled by default. You can choose to turn off automatic deployment of policies when services are discovered. In addition, you can modify and save preconfigured policies with new names to create custom policies for your own specialized purposes.

The advanced policies are used in specific scenarios. You can manually deploy these policies as required.

If you turned off autodeployment of policies, you can manually deploy the QuickStart policies by accessing either of the two policies grouping provided by the Infrastructure SPIs. The groupings are based on monitored aspects and vendor and operating system. The monitored aspects based grouping helps you to access and deploy policies to monitor performance, availability, capacity, logs, and security aspects across multiple operating systems.

The **Policies grouped by Vendor** help you to quickly access the policies relevant to your operating system at one place. For example, to access VI-VMwareEventMonitor policy for deploying it on a managed node, expand:

Infrastructure Management→<*language*>→Virtualization Infrastructure→ Policies grouped by Vendor → VMware ESX - QuickStart. → VI-VMwareEventMonitor

On HPOM for UNIX

Follow the steps for getting started with the Infrastructure SPIs on HPOM for UNIX (HP-UX, Linux, and Solaris).

Before you start, make sure that you have installed the latest patches and hotfixes.

List of the Patches

HPOM for HP-UX	HPOM for Linux	HPOM for Solaris
PHSS_43123	OML_00057	ITOSOL_00779

Running the Discovery Policies on the Virtualized Infrastructure

To get started with discovering the virtualized infrastructure, the first step is to deploy the SI-SystemDiscovery policy on the nodes. As VI SPI discovery policies are not auto deployed, one or more auto messages are sent to HPOM. These messages include the auto action to add the nodes to InfraSPI node groups. For example, for VMware, the Auto-Add messages add the virtualization nodes (eg, ESX/ESXi hosts, vCenter, and vMA) to Virtualization node group. The node is added as VI-VMwareESX Hosts, VI-VMware vCenter, and so on.

The vendor specific QuickStart policies are auto-assigned on those nodes. After the nodes are added to these node groups, you have to deploy the auto-assigned policies on the nodes. Also, deploy VI discovery policy on the node. The virtual machines running on those nodes are added under the respective Virtualization Infrastructure node group.

The discovered managed nodes are regrouped in the console tree as **Nodes→Virtualization→** *<vendor name>.*

The VI SPI discovery policy adds the discovered elements to the HPOM service map. The service map graphically represents the discovered virtual infrastructure.

Note: If the discovery map for virtualization is not appearing, see Problem: Discovery map for VI SPI is not appearing.

Deploying Quick Start Policies from HPOM for UNIX

After the SI SPI discovery runs successfully, the discovered nodes are automatically added to the relevant Infrastructure SPI node groups.

By default, QuickStart policies are assigned to these node groups. When a node is added to the node group, these QuickStart policies get assigned to the node automatically. You must then deploy these policies manually on the node by selecting **Deploy Configuration** from the **Actions** menu in the Admin GUI.

Available for all three Infrastructure SPIs, QuickStart policies get you started immediately without having to spend much time customizing settings. Automatic assignment of policies is enabled by default.

The groupings are based on *monitored aspects* and *operating systems/vendor*. The monitored aspects based grouping helps you to access and deploy policies to monitor performance, availability, capacity, logs, and security aspects across multiple operating systems.

The policies grouped by operating system and vendor help you to quickly access the policies relevant to your operating system at one place. For example, to access VI-VMwareEventMonitor policy for deploying it on a managed node, select:

/ Policy Bank / Infrastructure Management / en / Virtualization Infrastructure / Policies grouped by Vendor / VMware ESX - QuickStart

Policies grouped by operating system include two sub groups: QuickStart and Advanced. The QuickStart group includes the policies that are used most often. The advanced policies like the disk utilization policy and the disk capacity monitor policy are used in specific scenarios. The following figure shows the policies grouped by vendor and the subgroups for QuickStart and Advanced policies.

Viewing Reports and Graphs

To generate and view reports and graphs from data collected by the Infrastructure SPIs, you must use HP Reporter and HP Performance Manager, respectively, in conjunction with HPOM. The Infrastructure SPIs collect and store reporting and graphing data in a data store. The data store can be CODA (HP Operations agent's data store—also known as embedded performance component) or HP Performance Agent.

For VI SPI reporting and graphing, HP Performance Agent must be installed on the managed node.

To view graphs on HPOM for HP-UX, Linux, or Solaris you need to first integrate HP Performance Manager with the HPOM management server.

Integrating HP Performance Manager with HPOM for UNIX

To integrate HPOM for UNIX (HP-UX, Linux, or Solaris) server with HP Performance Manager, follow these steps:

- If HP Performance Manager is installed on the HPOM server, run the following command:

/opt/OV/contrib/OpC/OVPM/install_OVPM.sh

install_OVPM.sh <nodename>:<port>

Example: install_OVPM.sh test.ovtest.com:8081

- If HP Performance Manager is installed on a remote system connected to the HPOM server, follow these steps:

1. Copy the graph templates from the remote system where HP Performance Manager is installed to the HPOM server. To learn about the graph types and their location on the system, see *HP Performance Manager Administrator Guide*.
2. Run the following command on the HPOM server:

/opt/OV/contrib/OpC/OVPM/install_OVPM.sh

install_OVPM.sh <nodename>:<port>

Example: install_OVPM.sh test.ovtest.com:8081

These steps set the host system configuration for HP Performance Manager, that is used when launching graphs from events in the HPOM operator GUI.

Updating Reports after Upgrading the SPI

After the upgrade, the existing report files are replaced with the new report files. Run the following command to update the reports.

1. Go to the **Start** menu.
2. Select **Run**.
3. At the prompt, type the command **repcrys** and click **Ok**.

Confirm that all the reports on the management server are in sync with the reports on the HP Reporter GUI. Click the **Reporter Status** tab in the Reporter GUI to check for the number reports sent to the console and also for any error message.

Data Collection for Reports

With the VI SPI, data collection for reports does not depend on policy deployment. The data is collected by the HP Operations Agent deployed on the managed nodes.

The following table lists the reports and policies that are required to be deployed on the managed node to collect data for corresponding reports.

Reports	Policies	Managed Node Platform	SPI
Hyper-V Configuration	HP Performance Agent metrics	Microsoft Hyper-V	VI SPI
Hyper-V CPU Utilization	HP Performance Agent metrics	Microsoft Hyper-V	VI SPI
vMA Host-Guest Configuration	HP Performance Agent metrics	VMware vMA	VI SPI
vMA CPU Utilization	HP Performance Agent metrics	VMware vMA	VI SPI
vMA Memory Utilization	HP Performance Agent metrics	VMware vMA	VI SPI
vMA Ready Utilization	HP Performance Agent metrics	VMware vMA	VI SPI
vMA Top Busy CPU	HP Performance Agent metrics	VMware vMA	VI SPI
vMA Top Busy Disk	HP Performance Agent metrics	VMware vMA	VI SPI
vMA Top Busy Memory	HP Performance Agent metrics	VMware vMA	VI SPI
vMA Availability	HP Performance Agent metrics	VMware vMA	VI SPI

To view reports for the Infrastructure SPIs from HPOM for Windows, expand **Reports** **Infrastructure Management** → **Virtualization Infrastructure** in the console tree. To display a report, select the desired report on the HPOM console, right-click, and then select **Show report**.

Chapter 5

Virtualization Infrastructure SPI Policies and Tools

The Virtualization Infrastructure SPI (VI SPI) provides a wide range of policies and tools to help manage your infrastructure. The policies help you monitor systems in virtualized environments and the tools display data collected for these systems.

Virtualization Infrastructure SPI Policies

A policy is a rule or set of rules that helps you automate monitoring. The VI SPI policies help you monitor in Windows and UNIX environments. Most policies are common to all environments, but there are some policies that are relevant only to a particular environment and must be deployed only on the relevant platform. Deployment of policy to an unsupported platform may lead to an unexpected behavior or cause the policy to fail.

The folder Infrastructure Management group contains a subgroup arranged according to language. For example, the subgroup for English policies is **en,** for Japanese language is **ja,** and for Simplified Chinese language is **zh**.

In the console tree, the VI SPI policies are listed at the following location:

Policy management → Policy groups → Infrastructure Management → *<language>* → Virtualization Infrastructure.

For information about deploying policies from the management server, see "Deploying VI SPI Policies from HPOM for Windows Management Server" on page 157.

For HPOM for UNIX (HP-UX, Linux, or Solaris), the policy group on the console/ Administration interface is:

Policy Bank → Infrastructure Management → *<language>* → Virtualization Infrastructure

For information about deploying policies from the management server, see "Deploying VI SPI Policies from HPOM for UNIX Management Server" on page 159.

The VI SPI policies available for vMA and VA solution are given below:

HPOM for Windows (Infrastructure Management → <language> → Virtualization Infrastructure → <Policy Group>)	HPOM for UNIX (Policy Bank → Infrastructure Management → <language> → Virtualization Infrastructure → <Policy Group>)	vMA based solution	VA based solution
Auto Discovery	Auto Discovery	Yes	Yes
Availability → VMware ESX	Availability → VMware ESX	Yes	No

HPOM for Windows (Infrastructure Management → <language> → Virtualization Infrastructure → <Policy Group>)	HPOM for UNIX (Policy Bank → Infrastructure Management → <language> → Virtualization Infrastructure → <Policy Group>)	vMA based solution	VA based solution
Capacity → VMware ESX	Capacity → VMware ESX	Yes	No
Events → VMware ESX	Events → VMware ESX	Yes	No
Hardware → VMware ESX	Hardware → VMware ESX	Yes	No
Performance → VMware ESX	Performance → VMware ESX	Yes	No
Policies grouped by Vendor → VMware ESX - QuickStart	Policies grouped by Vendor → VMware ESX - QuickStart	Yes	No
Policies grouped by Vendor → VMware ESX - Advanced	Policies grouped by Vendor → VMware ESX - Advanced	Yes	No
Availability → VMware vCenter	Availability → VMware vCenter	No	Yes
Events → VMware vCenter	Events → VMware vCenter	No	Yes
Performance → VMware vCenter	Performance → VMware vCenter	No	Yes
Policies grouped by Vendor → VMware vCenter - QuickStart	Policies grouped by Vendor → VMware vCenter - QuickStart	No	Yes
Policies grouped by Vendor → VMware vCenter - Advanced	Policies grouped by Vendor → VMware vCenter - Advanced	No	Yes

Auto Discovery Policy

The Virtualization Infrastructure SPI discovers virtual machines and resource pools that are available on host server nodes and automatically configures the service hierarchy. After you add a node to the HPOM server **with auto deployment enabled**, the Systems Infrastructure SPI service discovery policy is automatically deployed to the nodes. Once the Systems Infrastructure SPI discovery identifies the system as a node that hosts virtual machines or a vMA, it automatically triggers the auto-deployment of the VI-Discovery policy. The Virtualization Infrastructure SPI discovery adds discovered information to the HPOM Services area.

Note: The Service Discovery policy is auto-deployed only on HPOM for Windows. This policy must be manually assigned and deployed to the nodes on HPOM for UNIX (HP-UX, Linux and Solaris).

Discovering Services Manually

In the console tree, the auto discovery policy is listed at the following location:

Infrastructure Management → ***<language>*** → **Virtualization Infrastructure** → **Auto Discovery**.

To deploy the Discovery policy manually, follow these steps:

1. Select the **VI-Discovery** policy.
2. Right-click and select **All tasks → Deploy on...**
3. Select the nodes on which you want to deploy the policy.
4. Click **OK**.

Note: The *VI-Discovery* policy does not automatically deploy the preconfigured policies. You must manually deploy the policies.

Availability Policies

Availability monitoring helps to ensure adequate availability of resources. The availability policies compute and compare current load on virtualized infrastructure with threshold levels and sends an alert message to HPOM console if there is any shortfall in resource availability.

In the console tree, the Availability policies are listed at the following location:

Infrastructure Management → <*language*> → Virtualization Infrastructure → Availability.

Performance Agent Processes Monitor Policy

VI-PerfAgentProcessMonitor

The VI-PerfAgentProcessMonitor policy is a measurement threshold policy that monitors the performance agent processes running on the nodes. It first checks if *CODA* (for HP Operations agent) or *SCOPE* (for HP Performance Agent) are enabled on the node and then checks their status.

In addition to monitoring the status of Scope and CODA, the VI-PerfAgentProcessMonitor policy also monitors the status of the *VISERVER* process in case of VMware and the status of the *LSDAEMON* process in case of AIX.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → <*language*> → Virtualization Infrastructure → Availability**.
- **Infrastructure Management → <*language*> → Virtualization Infrastructure → Policies Grouped by Vendor → <*platform*> - QuickStart**.

If any of the performance agent processes stop running, this policy sends an alert message of severity `Major` to the HPOM console. This policy has an automatic action associated with it that starts the process internally. After the process starts and the *start* command for the services is successful, the alert message is moved to the Acknowledge message window.

If all the services are up and running, the alert message gets acknowledged with a Normal alert message during the next run of the policy.

The default polling interval for this policy is 5 minutes. You can modify the polling interval based on your requirements.

Note: Ensure that you do *not* set the polling interval below 30 seconds or the policy will not work.

State Monitor Policy for HPVM Guests

VI-HPVMStateMonitor

The VI-HPVMStateMonitor policy monitors and reports on the state of HPVM guests. It sends alert messages of severity `Major` or `Warning` to the HPOM console based on the state of the virtual machine being monitored.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Availability → HPVM**.
- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor HPVM - QuickStart**.

The VI-HPVMStateMonitor policy alerts on the following states:

Major Alert	**Warning Alert**		**Normal Alert**
Critical States	Warning States	Down States	Normal State
• Hung • Crash	• Unknown • Invalid • Other	• Down • Boot • Shutdown	• Up

The VI-HPVMStateMonitor policy alerts on transient states only if the virtual machine is in transient state for more than 30 minutes. This policy does not report on the state of the host machines.

Metrics Used	BYLS_LS_STATE BYLS_LS_NAME BYLS_DISPLAY_NAME GBL_LS_TYPE
Supported Platforms	HPVM
Script-Parameter	**Description**
AlertOnPlannedOutage	The value of AlertOnPlannedOutage is set to `FALSE` by default. You can change it to `TRUE` or `hh:mm:ss-hh:mm:ss` format for time-bound alerting. To receive alerts for all the states listed under the Down category, set the value to TRUE or the specified time format.
MessageGroup	Message group for outgoing messages.

Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 5 minutes. You can modify the polling interval based on your requirements.

State Monitor Policy for IBM Frame and LPAR

VI-IBMFrameAndLPARStateMonitor

The VI-IBMFrameAndLPARStateMonitor policy monitors IBM Frames and LPARs on those Frames. It sends alert messages of severity `Major` or `Warning` to the HPOM console based on the state of the Frames and LPARs being monitored.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → *<language>*→ Virtualization Infrastructure → Availability → IBM LPAR**
- **Infrastructure Management → *<language>*→ Virtualization Infrastructure → Policies Grouped by Vendor → IBM LPAR - Advanced**.

This policy collects the following information about the frames and LPARs and logs it in CODA under two classes: FRAME and LPAR

- *FRAME Class:*
  - HMC Name
  - Frame Name
  - Frame State
- *LPAR Class:*
  - HMC Name
  - Frame Name
  - LPAR ID
  - LPAR Name
  - LPAR State

The policy alerts on the following Frame states:

Major Alert	**Warning Alert**			**Normal Alert**
Critical States	*Warning State*	*Down State*	*Transient States*	*Normal State*
• Error • Error - Dump in Progress • Error - Terminated	• Incomplete • Failed Authentication • Pending Authentication -	• Power off	• Initializing	• Operating

Major Alert	Warning Alert			Normal Alert
	Password Updates Required • Recovery • No Connection • On Demand Recovery			

The VI-IBMFrameAndLPARStateMonitor policy alerts on the following LPAR states:

Major Alert	Warning Alert			Normal Alert
Critical States	*Warning State*	*Down State*	*Transient States*	*Normal State*
• Not Available	• Error	• Not Activated	• Starting • Migrating - Running • Shutting Down • Hardware Discovery • Migrating - Not Activated	• Running

This policy alerts on transient states only if the virtual machine is in transient state for more than 30 minutes. It does not report on the state of the host machines.

Supported Platforms	IBM Frame and LPAR
Script-Parameter	**Description**
Aler-tOnPlannedOutage	The value of *AlertOnPlannedOutage* is set to `FALSE` by default. You can change it to `TRUE` or `hh:mm:ss-hh:mm:ss` format for time-bound alerting. To receive alerts for all the states listed under the Down category, set the value to `TRUE` or the specified time format.
MessageGroup	Message group for outgoing messages.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 5 minutes. You can modify the polling interval based on your requirements.

State Monitor Policy for IBM WPAR

VI-IBMWPARStateMonitor

The VI-IBMWPARStateMonitor policy monitors and reports on the state of IBM WPARs. It sends alert messages of severity `Major` or `Warning` to the HPOM console based on the state of the WPARs being monitored.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Availability → IBM LPAR**.
- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor → IBM LPAR - QuickStart**.

The VI-IBMWPARStateMonitor policy alerts on the following states:

Major Alert	Warning Alert			Normal Alert
Critical States	*Warning State*	*Down State*	*Transient States*	*Normal State*
• Broken • Error	• Frozen	• Paused	• Transitional • Defined • Loaded	• Active

The VI-IBMWPARStateMonitor policy alerts on transient states only if the virtual machine is in transient state for more than 30 minutes. This policy does not report on the state of the host machines.

Metrics Used	BYLS_LS_STATE BYLS_LS_NAME BYLS_DISPLAY_NAME GBL_LS_TYPE
Supported Platforms	IBM WPAR
Script-Parameter	**Description**
AlertOnPlannedOutage	The value of *AlertOnPlannedOutage* is set to `FALSE` by default. You can change it to `TRUE` or `hh:mm:ss-hh:mm:ss` format for time-bound alerting. To receive alerts for all the states listed under the Down category, set the value to `TRUE` or the specified time format.
MessageGroup	Message group for outgoing messages.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 5 minutes. You can modify the polling interval based on your requirements.

State Monitor Policy for Microsoft Hyper-V Guests

VI-MSHyperVStateMonitor

The VI-MSHyperVStateMonitor policy monitors and reports on the state of the Microsoft Hyper-V guest machines. It sends alert messages of severity `Warning` to the HPOM console based on the state of the virtual machine being monitored.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Availability → MS Hyper-V**.
- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor → MS Hyper-V - QuickStart**.

The VI-MSHyperVStateMonitor policy alerts on the following states:

Warning Alert			**Normal Alert**
Warning States	*Down States*	*Transient States*	*Normal State*
• Unknown • Deleted	• Suspended • Paused • Disabled	• Starting • Snapshoting • Migrating • Saving • Stopping • Pausing • Resuming	• Enabled

The VI-MSHyperVStateMonitor policy alerts on transient states only if the virtual machine is in transient state for more than 30 minutes. This policy does not report on the state of the host machines.

Metrics Used	BYLS_LS_STATE BYLS_LS_NAME BYLS_DISPLAY_NAME GBL_LS_TYPE
Supported Platforms	Microsoft Hyper-V
Script-Parameter	**Description**
AlertOnPlannedOutage	The value of *AlertOnPlannedOutage* is set to `FALSE` by default.

	You can change it to `TRUE` or `hh:mm:ss-hh:mm:ss` format for time-bound alerting. To receive alerts for all the states listed under the Down category, set the value to `TRUE` or the specified time format.
MessageGroup	Message group for outgoing messages.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 5 minutes. You can modify the polling interval based on your requirements.

State Monitor Policy for Oracle Solaris Zones

VI-OracleSolarisStateMonitor

The VI-OracleSolarisStateMonitor policy monitors and reports on the state of Solaris zones. It sends alert messages of severity `Warning` to the HPOM console based on the state of the zones being monitored.

In the console tree, the policy is listed at the following locations:

Infrastructure Management → *<language>* → Virtualization Infrastructure → Availability → Oracle Containers.

Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor → Oracle Containers - QuickStart.

The VI-OracleSolarisStateMonitor policy alerts on the following states:

Warning Alert		**Normal Alert**
Down State	*Transient States*	*Normal State*
• Down	• Configured • Incomplete • Installed • Ready • Shutting • Mounted	• Running,

The VI-OracleSolarisStateMonitor policy alerts on transient states only if the virtual machine is in transient state for more than 30 minutes. This policy does not report on the state of the host machines.

Metrics Used	• BYLS_LS_STATE

	• BYLS_LS_NAME • BYLS_DISPLAY_NAME • GBL_LS_TYPE
Supported Platforms	Oracle Solaris Zones
Script-Parameter	**Description**
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.
AlertOnPlannedOutage	The value of *AlertOnPlannedOutage* is set to `FALSE` by default. You can change it to `TRUE` or `hh:mm:ss-hh:mm:ss` format for time-bound alerting. To receive alerts for all the states listed under the Down category, set the value to `TRUE` or the specified time format.

The default polling interval for this policy is 5 minutes. You can modify the polling interval based on your requirements.

State Monitor Policy for VMware ESX or ESXi Servers

VI-VMWareStateMonitor

The VI-VMWareStateMonitor policy monitors and reports on the state of the guest machines on VMware ESX or ESXi servers. It sends alert messages of severity `Warning` to the HPOM console based on the state of the virtual machine being monitored.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → <*language*> → Virtualization Infrastructure → Availability → VMware ESX**.
- **Infrastructure Management → <*language*> → Virtualization Infrastructure → Policies Grouped by Vendor → VMware ESX - QuickStart**.

For VI-VMWareStateMonitor policy alerts on the following states:

Warning Alert	**Normal Alert**
Down States	*Normal State*
Off Suspended	On

The VI-VMWareStateMonitor policy alerts on transient states only if the virtual machine is in transient state for more than 30 minutes. This policy does not report on the state of the host machines.

Metrics Used	• BYLS_LS_STATE • BYLS_LS_NAME • BYLS_LS_ROLE • BYLS_LS_TYPE • BYLS_DISPLAY_NAME
Supported Platforms	VMware ESX or ESXi
Script-Parameter	**Description**
AlertOnPlannedOutage	The value of *AlertOnPlannedOutage* is set to `FALSE` by default. You can change it to `TRUE` or `hh:mm:ss-hh:mm:ss` format for time-bound alerting. To receive alerts for all the states listed under the Down category, set the value to `TRUE` or the specified time format.
MessageGroup	Message group for outgoing messages.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 5 minutes. You can modify the polling interval based on your requirements.

State Monitor Policy for KVM or Xen Guests

VI-LinuxVirtStateMonitor

The VI-LinuxVirtStateMonitor policy monitors and reports the state of KVM or Xen logical systems. It sends alert messages of severity `Major` or `Warning` to the HPOM console based on the state of the virtual machine being monitored.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → *<language>*→ Virtualization Infrastructure → Availability → LinuxVirt**.
- **Infrastructure Management → *<language>*→ Virtualization Infrastructure → Policies Grouped by Vendor → LinuxVirt - QuickStart**.

The VI-LinuxVirtStateMonitor policy alerts on the following states:

Major Alert	**Warning Alert**			**Normal Alert**
Critical State	*Warning State*	*Down States*	*Transient States*	*Normal State*
Crashed	Paused	• Shutdown • Shutoff	• Run/Idle • No state	Running

The VI-LinuxVirtStateMonitor policy alerts on transient states only if the virtual machine is in transient state for more than 30 minutes. This policy does not report the state of the host machines.

Supported Platforms	KVM or Xen
Script-Parameter	**Description**
AlertOnPlannedOutage	The value of *AlertOnPlannedOutage* is set to `FALSE` by default. You can change it to `TRUE` or `hh:mm:ss-hh:mm:ss` format for time-bound alerting. To receive alerts for all the states listed under the Down category, set the value to `TRUE` or the specified time format.
MessageGroup	Message group for outgoing messages.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 5 minutes. You can modify the polling interval based on your requirements.

Host Service Monitor Policy for Microsoft Hyper-V

VI-MSHyperVHostServiceMonitor

This policy monitors the availability of services on the host operating system of the Microsoft Hyper-V server.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Availability → MS Hyper-V**.
- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor → MS Hyper-V - QuickStart**.

The policy monitors the following services:

- Hyper-V Virtual Machine Management

Service name: *vmms*

This service is responsible for managing the state of all guest virtual machines. It is used for creation, deletion, and modification of virtual machines.

- Hyper-V Networking Management Service

Service name: *nvspwmi*

This service is used to manage networking resources in virtualization environment such as virtual switches.

- Hyper-V Image Management Service

Service name: *vhdsvc*

This service is used to manage virtual media for virtual machines. It is used to collect information about virtual hard disk operations.

If one of the services is not running, an alert message is sent to the HPOM management server with an associated operator-initiated action to start the affected service. The message severity by default is Major for all services.

The default polling interval for this policy is 5 minutes. You can modify the polling interval based on your requirements.

Process Monitoring Policy for HPVM

VI-HPVMDaemonsMonitor

The VI-HPVMDaemonsMonitor policy monitors the processes/daemons running on HPVM and sends Minor alert messages when any of the processes or daemons stop.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Availability → HPVM**.
- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor → HPVM - QuickStart**.

This VI-HPVMDaemonsMonitor policy monitors the following HPVM processes/daemons:

Daemon Name	Function
hpvmmonlogd	Copies the monitor output from the driver memory to the *hpvm_mon_log* file and rotates the log files as required.
hpvmctrld	Manages distributed guests.
hpvmamrd	Automatically reallocates memory for guests.
hpvmapp	Is associated with the individual VMs.
hpvmnetd	Manages a specified virtual switch.
vm_fssagt	Computes fair shares for virtual machines.

The alert messages are automatically acknowledged when the processes/daemons start.

The default polling interval for this policy is 5 minutes. You can modify the polling interval based on your requirements.

Process Monitoring Policies for Oracle Solaris Zones

VI-OracleSolarisRcapdProcessMonitor

The VI-OracleSolarisRcapdProcessMonitor policy monitors the **resource capping daemon (rcapd)** running on Solaris zones and sends an alert message with severity `Minor` to the HPOM console when rcapd stops.

If you have configured the zones with memory caps, the rcapd enables you to regulate physical memory consumption by the zones. When the resident set size (RSS) of a collection of processes exceeds its cap, rcapd reduces the RSS of the collection.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → <*language*> → Virtualization Infrastructure → Availability → Oracle Containers**.
- **Infrastructure Management → <*language*> → Virtualization Infrastructure → Policies Grouped by Vendor → Oracle Containers - Advanced**.

The alert messages are automatically acknowledged when rcapd starts.

The default polling interval for this policy is 5 minutes. You can modify the polling interval based on your requirements.

VI-OracleSolarisFmdProcessMonitor

The VI-OracleSolarisFmdProcessMonitor policy monitors the **fault manager daemon (fmd)** running on Solaris zones and sends an alert message with severity `Minor` to the HPOM console when fmd stops.

The fmd diagnoses and pro-actively resolves (for example, by disabling faulty components) any system software problem on the Solaris system on which it is running.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → <*language*> → Virtualization Infrastructure → Availability → Oracle Containers**.
- **Infrastructure Management → <*language*> → Virtualization Infrastructure → Policies Grouped by Vendor → Oracle Containers - QuickStart**.

The alert messages are automatically acknowledged when fmd starts.

The default polling interval for this policy is 5 minutes. You can modify the polling interval based on your requirements.

Data Collector Policy for IBM HMC

VI-IBMHMCDataCollector

The VI-IBMHMCDataCollector policy collects configuration information from the HMCs and logs it in CODA. You can modify the default logging interval based on your requirements.

This policy collects and logs the following configuration information in CODA under two classes: FRAME_CONFIGURATION and LPAR_CONFIGURATION.

- HMC Name
- Frame name
- Frame Serial number
- Frame Model type
- Configurable Memory in Frame
- Available Memory in Frame after assigning to every LPAR

- Configurable Processing units in Frame
- Available Processing units in Frame after assigning to every LPAR
- Frame IP address
- LPAR Name
- Assigned Memory to the particular LPAR
- Assigned Processing unit to the particular LPAR

Before deploying this policy, run the *getSSHAuthentication.pl* script to connect to the HMC. This script is located under the */var/opt/OV/bin/instrumentation* directory on the node (frame).

The *getSSHAuthentication.pl* script provides you password-less access to the configuration information on the HMC.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → <*language*>→ Virtualization Infrastructure → Availability → IBM LPAR**.
- **Infrastructure Management → <*language*> → Virtualization Infrastructure → Policies Grouped by Vendor → IBM LPAR - Advanced**.

The default logging interval for this policy is 30 minutes. You can modify the logging interval in the policy depending on your requirements.

State Monitor Policy for VMware vCenter

VI-VMwareVCGuestStateMonitor

The VI-VMwareVCGuestStateMonitor policy monitors the state of all logical systems in the VMware environment. It sends an alert of severity `Warning` to the HPOM console based on the state of the guests being monitored.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management > en > Virtualization Infrastructure > Availability > VMware vCenter**
- **Infrastructure Management > en > Virtualization Infrastructure > Policies grouped by vendor > VMware vCenter - Quick Start**

The VI-VMwareVCGuestStateMonitor policy alerts on the following states:

Warning Alert		**Normal Alert**
Down State	*Warning States*	*Normal State*
• Off • Suspended	• Unknown	• On

The VI-VMwareVCGuestStateMonitor policy alerts on transient states only if the virtual machine is in transient state for more than 30 minutes. This policy does not report on the state of the host machines.

Metrics Used	• SystemState • LSName • SystemRole • SystemName • SystemHostHostName
Supported Platforms	VMware vCenter
Script-Parameter	**Description**
AlertOnPlannedOutage	The value of *AlertOnPlannedOutage* is set to `FALSE` by default. You can change it to `TRUE` or `hh:mm:ss-hh:mm:ss` format for time-bound alerting. To receive alerts for all the states listed under the Down category, set the value to `TRUE` or the specified time format.
MessageGroup	Message group for outgoing messages.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 5 minutes. You can modify the polling interval based on your requirements.

Capacity Policies

Capacity monitoring helps to identify the under-utilized and over-utilized resources. Capacity monitoring policies monitor the capacity utilization of the resources in virtualization environment.

In the console tree, the Capacity policies are listed at the following location:

Infrastructure Management → ***<language>*** → **Virtualization Infrastructure** → **Capacity**.

VMFS Utilization Monitor Policy for VMware ESX or ESXi Servers

VI-VMwareVMFSUtilizationMonitor

This policy monitors the disk space utilization on the Virtual Machine File System (VMFS). VMFS represents the data storage volumes on which the VMware guest disk files are stored. This policy is deployed on the vMA system. The policy alerts on the information collected by the **VI-VMwareVMFSDataCollector** (see "VMFS Utilization Data Collector Policy for VMware ESX or ESXi Servers" on page 128**)**.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management** → ***<language>*** → **Virtualization Infrastructure** → **Capacity** → **VMware ESX**.
- **Infrastructure Management** → ***<language>*** → **Virtualization Infrastructure** → **Policies Grouped by Vendor** → **VMware ESX - Advanced**.

Metrics Used	VMFS_UUID VMFS_HOSTNAME VMFS_DEVNAME VMFS_DEVNO VMFS_DIRNAME VMFS_SPACE_UTIL
Supported Platform	VMware ESX or ESXi

Script-Parameter	Description
SpaceUtilCriticalThreshold	If the disk space utilization is more than the specified threshold value, the policy generates an alert message with severity `Critical`.
SpaceUtilMajorThreshold	If the disk space utilization is more than the specified threshold value, the policy generates an alert message with severity `Major`.
SpaceUtilMinorThreshold	If the disk space utilization is more than the specified threshold value, the policy generates an alert message with severity `Minor`.
SpaceUtilWarningThreshold	If the disk space utilization is more than the specified threshold value, the policy generates an alert message with severity `Warning`.
Assign-MessageToRemoteHost	Set the value to **1** to display the source of the alert message as the remote host. By default the messages are assigned to the managed node from which the message is sent out.
MessageGroup	Message group for outgoing messages.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 5 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

Memory Usage Monitor Policy for VMware ESX or ESXi Servers

VI-VMwareVMMemoryUsage-AT

This policy monitors the amount of memory being used by the guest virtual machines and resource pools in MBs.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Capacity → VMware ESX**.
- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor → VMware ESX - Advanced**.

The policy uses a multi-instance baseline for monitoring the memory usage for virtual machines and resource pools. It uses automatic threshold determination to automatically calculate the threshold values. The threshold values are calculated according to the host memory usage by guest virtual machines and resource pools on previous days. When the threshold values are reached or exceeded, the VI-VMwareVMMemoryUsage-AT sends an alert to the HPOM console. The message severity can be major, minor, or warning depending upon the level of threshold violated.

Metrics Used	BYLS_DISPLAY_NAME BYLS_LS_HOSTNAME BYLS_MEM_USED BYLS_LS_UUID BYLS_LS_ROLE
Supported Platform	VMware ESX or ESXi
Script-Parameter	**Description**
MessageApplication	Type an appropriate value that will help you identify the messages sent by this policy to the HPOM console.
DataSource	Displays the data source name as SCOPE.
DataObject	Displays the data object name as LOGICAL.
DataMetric	Displays the metric name as BYLS_MEM_USED.
BaselinePeriod	Type the time period you want to define as a baseline period. For example, if you specify 3600 as the parameter value, the most recent 3600-second (1-hour) period becomes the current baseline period.
MinimumValue	Displays the minimum value of the memory consumption as indicated by the metric.

MaximumValue	Displays the maximum value of the memory consumption as indicated by the metric.
WarningDeviations	Displays the number of standard deviation away from normal, at which the policy sends a warning alert to HPOM console. Set an appropriate value for the parameter. To disable the parameter, set the value as *5*.
MinorDeviations	Displays the number of standard deviation away from normal, at which the policy sends a minor message to HPOM console. Set an appropriate value for the parameter greater than the specified value for *WarningDeviations*. To disable the parameter, set value as *5*.
MajorDeviations	Displays the number of standard deviation away from normal, at which the policy sends a major message to HPOM console. Set an appropriate value for the parameter greater than the specified value for *MinorDeviations*. To disable the parameter, set value as *5*.
WarningHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
WarningLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
InstanceSource	Do not rename the policy name. The policy uses its name to retrieve the source.

Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.
MessageGroup	Message group for outgoing messages.
MemUsageCutOff	Set a value below which you do not want to monitor the memory usage for virtual guest machines.

The default polling interval for this policy is 30 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

After the values return within normal levels, the alert messages are automatically acknowledged.

Host Disk Usage Monitor Policy for VMware ESX or ESXi Servers

VI-VMwareHostDiskUtilization-AT

The VI-VMwareHostDiskUtilization-AT policy monitors the duration for which the physical disks are utilized for input/output.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → <*language*> → Virtualization Infrastructure → Capacity → VMware ESX**.
- **Infrastructure Management → <*language*> → Virtualization Infrastructure → Policies Grouped by Vendor → VMware ESX - Advanced**.

The policy uses a multi-instance baseline for monitoring the disk input/output utilization. It uses automatic threshold determination to automatically calculate the threshold values. The threshold values are calculated based on the average percentage of disk utilization for the input/output operations on the previous days. When the threshold values are reached or exceeded, the policy sends an alert message to the HPOM console. The message severity can be major, minor, or warning depending upon the level of threshold violated.

Metrics Used	BYLS_DISPLAY_NAME BYLS_DISK_UTIL BYLS_LS_UUID BYLS_LS_ROLE BYLS_LS_HOSTNAME
Supported Platform	VMware ESX or ESXi
Script-Parameter	**Description**
MessageApplication	Type an appropriate value that will help you identify the messages sent by this policy to the HPOM console.

DataSource	Displays the data source name as SCOPE.
DataObject	Displays the data object name as LOGICAL.
DataMetric	Displays the metric name as BYLS_DISK_UTIL.
BaselinePeriod	Type the time period you want to define as a baseline period. For example, if you specify 3600 as the parameter value, the most recent 3600-second (1-hour) period becomes the current baseline period.
MinimumValue	Displays the minimum value of the disk space as indicated by the metric.
MaximumValue	Displays the maximum value of the disk space as indicated by the metric.
WarningDeviations	Displays the number of standard deviation away from normal, at which the policy sends a warning message to HPOM console. Set an appropriate value for the parameter. To disable the parameter, set value as *5*.
MinorDeviations	Displays the number of standard deviation away from normal, at which the policy sends a minor message to HPOM console. Set an appropriate value for the parameter greater than the specified value for *WarningDeviations*. To disable the parameter, set value as *5*.
MajorDeviations	Displays the number of standard deviation away from normal, at which the policy sends a major message to HPOM console. Set an appropriate value for the parameter greater than the specified value for *MinorDeviations*. To disable the parameter, set value as *5*.
WarningHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
WarningLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.

MinorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
InstanceSource	Do not rename the parameter name. The policy uses its name to retrieve the source.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.
MessageGroup	Displays the message group for outgoing messages.
HostDiskUtilCutOff	Set a value below which you do not want to monitor the disk usage for the host machine.

The default polling interval for this policy is 30 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

After the values return within normal levels, the alert messages are automatically acknowledged.

Event Monitoring Policies

The event monitoring policies monitor crucial events from the ESX or ESXi hosts or vCenter managed by vMA. This group contains a monitoring policy and a configuration policy. The configuration policy lists all events that VI SPI monitors and also provides you the capability of adding the events you want to monitor in the list.

Note: To avoid getting duplicate messages and to capture all VI SPI events accurately, ensure that the ESX or ESXi hosts, vCenter, and vMA machines are accurately time synced.

The monitoring policy monitors the events listed in the configuration policy and sends alert messages to the HPOM console, as and when events are raised. All events are logged under */var/opt/OV/log/vispi.txt* for analysis.

In the console tree, the Event policies are listed at the following location:

Infrastructure Management → **<*language*>** → **Virtualization Infrastructure** → **Events**.

Event Type Policy for VMware ESX or ESXi Servers

VI-VMwareEventTypes

VI-VMwareEventTypes policy a configuration policy. It defines the events that the VI SPI monitors. The following event types are defined in this policy:

Note: You can see these events in the Data tab of the policy windows. Complementary events like a crucial event and its corrective event are separated with a colon in that order.

- VmSuspendedEvent:VmResumingEvent
- VmPoweredOffEvent:VmPoweredOnEvent
- DrsEnteredStandbyModeEvent:DrsExitedStandbyModeEvent
- DrsDisabledEvent:DrsEnabledEvent
- VmRenamedEvent
- VmRemovedEvent
- DrsVmPoweredOnEvent
- DrsVmMigratedEvent
- NotEnoughResourcesToStartVmEvent
- VmBeingHotMigratedEvent
- VmFailedMigrateEvent
- VmMigratedEvent
- VmDiskFailedEvent
- VmFailoverFailed
- VmNoNetworkAccessEvent
- VmUuidChangedEvent
- VmUuidConflictEvent
- VmOrphanedEvent
- HostRemovedEvent
- HostShutdownEvent

To monitor other events (apart from the ones mentioned above) using the VI-VMwareEventMonitor policy, add the event in the Config file (Data tab) of the VI-VMwareEventTypes policy.

By default, the newly added event will send alert messages of severity `Warning`.

In the console tree, the VI-VMwareEventTypes policy is listed at the following locations:

- **Infrastructure Management** → ***<language>*** → **Virtualization Infrastructure** → **Events** → **VMware ESX**.
- **Infrastructure Management** → ***<language>*** → **Virtualization Infrastructure** → **Policies Grouped by Vendor** → **VMware ESX- QuickStart**.

Event Type Policy for VMware vCenter

VI-VMwareVCEventTypes

The VI-VMwareVCEventTypes policy is a configuration policy. It defines the events that the VI SPI monitors.

In the console tree, the VI-VMwareEventTypes policy is listed at the following locations:

- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Events → VMware vCenter**.
- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor → VMware vCenter- QuickStart**.

Event Monitoring Policy for VMware ESX or ESXi Servers

VI-VMwareEventMonitor

The VI-VMwareEventMonitor policy monitors the events defined in the VI-VMwareEventTypes policy and sends an alert message to the HPOM console in case an event of a defined type occurs.

Supported Platform	VMware ESX or ESXi
Script-Parameter	**Description**
MessageGroup	Message group for outgoing messages.
EventSource	Collects events from either ESX/vCenter. By default it collects events from ESX servers.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 15 minutes. If your environment has a large number of monitored instances, to collect data accurately, increase the policy's polling interval to an appropriate value.

In the console tree, this policy is listed at the following locations:

- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Events → VMware ESX**.
- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor → VMware ESX- QuickStart**.

Event Monitoring Policy for VMware vCenter

VI-VMwareVCEventMonitor

The VI-VMwareVCEventMonitor policy enables you to monitor events from ESX vCenter server.

In the console tree, this policy is listed at the following locations:

- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Events → VMware vCenter**.
- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor → VMware vCenter- QuickStart**.

Metrics Used	EventSource
Supported Platforms	VMware vCenter
Script-Parameter	**Description**
MessageGroup	Message group for outgoing messages.
EventSource	Collects events from vCenter host.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 1 minute, as the default collection interval of agent is 1 minute. You can modify the polling interval based on your requirements.

Note: If the agent collection interval is changed to 300 seconds, you have to change the polling interval of *VI-VMwareVCEventMonitor* policy to 5 minutes.

Hardware Monitoring Policies

Hardware monitoring policies enable you to monitor the health and status of your VMware ESX or ESXi host servers. These measurement threshold policies monitor the health of the hardware components of the VMware ESX or ESXi host servers and send alert messages to the HPOM console if the health is not normal.

These policies obtain data from the VMware CIM SMASH/Server Management APIs. For information about the CIM SMASH APIs, see the VMware documentation at http://www.vmware.com/support.

Note:
1. The VI SPI hardware monitoring policies monitor and alert on only those properties that are exposed by the individual hardware vendors.

2. ESX 35 U4 or higher or ESXi servers are required for VI SPI hardware monitoring policies.

In the console tree, the Hardware policies are listed at the following location:

Infrastructure Management → *<language>* → **Virtualization Infrastructure** → **Hardware** → **VMware ESX**.

Hardware Data Collector Policy for VMware Datacenter

VI-VMwareHardwareHealthCollector

The VI-VMwareHardwareHealthCollector policy collects data about the health of the processor, memory, fan, chassis, ethernet port, and sensor of the host machines for the VMware datacenters and logs it in CODA. The default logging interval is 30 minutes. You can modify the logging interval based on your requirements.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management** → ***<language>*** → **Virtualization Infrastructure** → **Hardware** → **VMware ESX**.

Policies grouped under Health Collector policy	VMWARE_HOST_PROCESSOR_HEALTH_MONITOR VMWARE_HOST_PHYSICAL_MEMORY_HEALTH_ MONITOR VMWARE_HOST_ETHERNETPORT_HEALTH_MONITOR VMWARE_HOST_FAN_HEALTH_MONITOR VMWARE_HOST_CHASSIS_HEALTH_MONITOR VMWARE_HOST_SENSOR_HEALTH_MONITOR
Supported Platform	vCenter
Script-Parameter	**Description**
MessageGroup	Message group for outgoing messages.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The VI-VMwareHostProcessorHealthMonitor, VI-VMwareHostPhysicalMemoryHealth Monitor, VI-VMwareHostEthernetPortHealthMonitor, VI-VMwareHostFanHealthMonitor, VI-VMwareHostChassisHealthMonitor, and VI-VMwareHostSensorHealthMonitor policies send alert messages based on the data collected and logged by the VI-VMwareHardware HealthCollector policy.

The default polling interval of this policy is 30 minutes. If your environment has a large number of monitored instances, to collect data accurately, increase the policy's polling interval to an appropriate value.

Host Ethernet Port Health Monitor Policy for VMware ESX or ESXi Servers

VI-VMwareHostEthernetPortHealthMonitor

The VI-VMwareHostEthernetPortHealthMonitor policy monitors the health of the ethernet port on VMware ESX or ESXi host servers. It sends an alert message to the HPOM console if the health of the port is not normal.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management** → ***<language>*** → **Virtualization Infrastructure** → **Hardware** → **VMware ESX**.
- **Infrastructure Management** → ***<language>*** → **Virtualization Infrastructure** → **Policies Grouped by Vendor** → **VMware ESX - Advanced**.

Metrics Used	VMWARE_ETHERNETPORT_HOST_NAME VMWARE_ETHERNETPORT_HOST_UUID VMWARE_ETHERNETPORT_ELEMENT_NAME VMWARE_ETHERNETPORT_DESCRIPTION VMWARE_ETHERNETPORT_NETWORK_ADDRESSES VMWARE_ETHERNETPORT_ENABLED_STATE VMWARE_ETHERNETPORT_HEALTH_STATE VMWARE_ETHERNETPORT_OPERATIONAL_STATUS
Supported Platform	VMware ESX or ESXi
Script-Parameter	**Description**
MessageGroup	Message group for outgoing messages.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 5 minutes. If your environment has a large number of monitored instances, to collect data accurately, increase the policy's polling interval to an appropriate value.

Host Sensor Health Monitor Policy for VMware ESX or ESXi Servers

VI-VMwareHostSensorHealthMonitor

The VI-VMwareHostSensorHealthMonitor policy monitors the health of the sensors associated with all the devices on VMware ESX or ESXi host servers. It sends an alert message to the HPOM console if the health of any sensor is not normal.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management** → **<*language*>** → **Virtualization Infrastructure** → **Hardware** → **VMware ESX**.
- **Infrastructure Management** → **<*language*>** → **Virtualization Infrastructure** → **Policies Grouped by Vendor** → **VMware ESX - Advanced**.

Metrics Used	VMWARE_SENSOR_HOST_NAME VMWARE_SENSOR_HOST_UUID VMWARE_SENSOR_PART_COMPONENT VMWARE_SENSOR_SENSOR_NAME

	VMWARE_SENSOR_SENSOR_TYPE VMWARE_SENSOR_HEALTH_STATE VMWARE_SENSOR_OPERATIONAL_STATUS VMWARE_SENSOR_CURRENT_READING
Supported Platform	VMware ESX or ESXi
Script-Parameter	**Description**
MessageGroup	Message group for outgoing messages.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 5 minutes. If your environment has a large number of monitored instances, to collect data accurately, increase the policy's polling interval to an appropriate value.

Host Chassis Health Monitor Policy for VMware ESX or ESXi Servers

VI-VMwareHostChassisHealthMonitor

The VI-VMwareHostChassisHealthMonitor policy monitors the health of the VMware ESX or ESXi host server's chassis. It sends an alert message to the HPOM console if the health of the chassis is not normal.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management** → **<*language*>** → **Virtualization Infrastructure** → **Hardware** → **VMware ESX**.
- **Infrastructure Management** → **<*language*>** → **Virtualization Infrastructure** → **Policies Grouped by Vendor** → **VMware ESX - Advanced**.

Metrics Used	VMWARE_CHASSIS_HOST_NAME VMWARE_CHASSIS_HOST_UUID VMWARE_CHASSIS_ELEMENT_NAME VMWARE_CHASSIS_DESCRIPTION VMWARE_CHASSIS_UUID VMWARE_CHASSIS_MANUFACTURER VMWARE_CHASSIS_MODEL VMWARE_CHASSIS_POWERON_STATUS

	VMWARE_CHASSIS_HEALTH_STATE VMWARE_CHASSIS_OPERATIONAL_STATUS
Supported Platform	VMware ESX or ESXi
Script-Parameter	**Description**
MessageGroup	Message group for outgoing messages.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 5 minutes. If your environment has a large number of monitored instances, to collect data accurately, increase the policy's polling interval to an appropriate value.

Host Processor Health Monitor Policy for VMware ESX or ESXi Servers

VI-VMwareHostProcessorHealthMonitor

The VI-VMwareHostProcessorHealthMonitor policy monitors the health of the processors running on the VMware ESX or ESXi host servers. It sends an alert message to the HPOM console if the health of any processor is not normal.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management** → **<*language*>** → **Virtualization Infrastructure** → **Hardware** → **VMware ESX**.
- **Infrastructure Management** → **<*language*>** → **Virtualization Infrastructure** → **Policies Grouped by Vendor** → **VMware ESX - Advanced**.

Metrics Used	VMWARE_PROCESSOR_HOST_NAME VMWARE_PROCESSOR_HOST_UUID VMWARE_PROCESSOR_ELEMENT_NAME VMWARE_PROCESSOR_FAMILY VMWARE_PROCESSOR_MODEL VMWARE_PROCESSOR_CURRENT_CLOCK_SPEED VMWARE_PROCESSOR_MAX_CLOCK_SPEED VMWARE_PROCESSOR_EXTERNAL_BUS_CLOCK_SPEED VMWARE_PROCESSOR_STEPPING VMWARE_PROCESSOR_NUM_ENABLED_CORES

	VMWARE_PROCESSOR_HEALTH_STATE VMWARE_PROCESSOR_OPERATIONAL_STATUS
Supported Platform	VMware ESX or ESXi
Script-Parameter	**Description**
MessageGroup	Message group for outgoing messages.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 5 minutes. If your environment has a large number of monitored instances, to collect data accurately, increase the policy's polling interval to an appropriate value.

Host Fan Health Monitor Policy for VMware ESX or ESXi Servers

VI-VMwareHostFanHealthMonitor

The VI-VMwareHostFanHealthMonitor policy monitors the health of the fans on VMware ESX or ESXi host servers. It sends an alert message to the HPOM console if the health of any fan is not normal.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management** → **<*language*>** → **Virtualization Infrastructure** → **Hardware** → **VMware ESX**.
- **Infrastructure Management** → **<*language*>** → **Virtualization Infrastructure** → **Policies Grouped by Vendor** → **VMware ESX - Advanced**.

Metrics Used	VMWARE_FAN_HOST_NAME VMWARE_FAN_HOST_UUID VMWARE_FAN_ELEMENT_NAME VMWARE_FAN_HEALTH_STATE VMWARE_FAN_OPERATIONAL_STATUS
Supported Platform	VMware ESX or ESXi
Script-Parameter	**Description**
MessageGroup	Message group for outgoing messages.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 5 minutes. If your environment has a large number of monitored instances, to collect data accurately, increase the policy's polling interval to an appropriate value.

Host Physical Memory Health Monitor Policy for VMware ESX or ESXi Servers

VI-VMwareHostPhysicalMemoryHealthMonitor

The VI-VMwareHostPhysicalMemoryHealthMonitor policy monitors the health of the physical memory associated with the VMware ESX or ESXi host servers. It sends an alert message to the HPOM console if the health of the physical memory is not normal.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management** → **<*language*>** → **Virtualization Infrastructure** → **Hardware** → **VMware ESX**.
- **Infrastructure Management** → **<*language*>** → **Virtualization Infrastructure** → **Policies Grouped by Vendor** → **VMware ESX - Advanced**.

Metrics Used	VMWARE_MEMORY_HOST_NAME VMWARE_MEMORY_HOST_UUID VMWARE_MEMORY_ELEMENT_NAME VMWARE_MEMORY_CAPACITY VMWARE_MEMORY_MAX_MEMORY_SPEED VMWARE_MEMORY_HEALTH_STATE VMWARE_MEMORY_OPERATIONAL_STATUS
Supported Platform	VMware ESX or ESXi
Script-Parameter	**Description**
MessageGroup	Message group for outgoing messages.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 5 minutes. If your environment has a large number of monitored instances, to collect data accurately, increase the policy's polling interval to an appropriate value.

Log Monitoring Policies

The Logfile policies monitor the crucial system logs for the Hyper-V hosts.

In the console tree, the Log policies are listed at the following location:

Infrastructure Management → **<*language*>** → **Virtualization Infrastructure** → **Logs**.

Image Management Service Administration Logfile Monitoring Policy

VI-MSHyperV_ImageAdminWarnError

This policy monitors the log file and forwards the Image Management Service administration event log entries to the HPOM console with severity level of warning or error.

In the console tree, these policies are listed at the following locations:

- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Logs → MS Hyper-V**.
- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor → MS Hyper-V- QuickStart**.

The policy looks for the following error recorded in the log file:

The Hyper-V Image Management Service failed to start.

For example: This error appears in the Events Viewer. To see the error message in the HPOM for Windows server, go to **Run** and type *eventvwr*. The Event Viewer interface opens. If this error has occurred, the message appears under **Windows Logs → Security** or **Windows Logs → System**.

Image Management Service Operational Logfile Monitoring Policy for Microsoft Hyper-V

VI-MSHyperV_ImageOperationalWarnError

This policy monitors the log file and forwards the Image Management Service operational event log entries to the HPOM console with severity level of warning or error.

In the console tree, these policies are listed at the following locations:

- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Logs → MS Hyper-V**.
- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor → MS Hyper-V- QuickStart**.

The policy looks for the following error recorded in the log file:

The Hyper-V Image Management Service failed to start

Hypervisor Administration Logfile Monitoring Policy for Microsoft Hyper-V

VI-MSHyperV_HyperVisorAdminWarnError

This policy monitors the log file and forwards the virtual machine hypervisor administration event log entries to the HPOM console with severity level of warning or error.

In the console tree, these policies are listed at the following locations:

- **Infrastructure Management → *<language>*→ Virtualization Infrastructure → Logs → MS Hyper-V**.
- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor → MS Hyper-V- QuickStart**.

The policy looks for the following errors recorded in the log file:

- Hyper-V launch aborted due to auto-launch being disabled in the registry
- Hyper-V launch failed
- Hyper-V launch failed; No-execute (NX) or DEP not enabled on processor

Hypervisor Operational Logfile Monitoring Policy for Microsoft Hyper-V

VI-MSHyperV_HyperVisorOperationalWarnError

This policy monitors the log file and forwards the virtual machine hypervisor operational event log entries to the HPOM console with severity level of warning or error.

In the console tree, these policies are listed at the following locations:

- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Logs → MS Hyper-V**.
- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor → MS Hyper-V- QuickStart**.

The policy looks for the following errors recorded in the log file:

- Hyper-V launch aborted due to auto-launch being disabled in the registry
- Hyper-V launch failed
- Hyper-V launch failed; No-execute (NX) or DEP not enabled on processor

VMMS Administration Logfile Monitoring Policy for Microsoft Hyper-V

VI-MSHyperV_VMMSAdminWarnError

This policy monitors the log file and forwards the virtual machine VMMS admin event log entries to the HPOM console with severity level of warning or error.

In the console tree, these policies are listed at the following locations:

- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Logs → MS Hyper-V**.
- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor → MS Hyper-V- QuickStart**.

The policy looks for the following errors recorded in the log file:

- Hyper-V Virtual Machine Management service is shutting down while some virtual machines are running
- Hyper-V Virtual Machine Management service failed to start
- Virtual Machine is about to run out of disk space
- Virtual network switch name was not found
- Unable to find virtual hard disk file
- The WMI provider failed to start
- Virtual Machine Management service failed to register
- Virtual Machine Management service did not find the virtual machine
- The virtual network switch was not found
- Virtual Machine Management service failed to verify the running state of the virtual machine
- Virtual Machine Management service failed to start the virtual machine
- Error occurred while identifying the Hyper-V VSS writer
- Failed to register domain name
- Failed to create a new virtual machine
- Virtual Machine Bus (VMBus) cannot start
- The virtual machine bus is not running
- Cannot load a snapshot configuration because it is corrupt
- The network adapter is not configured correctly
- Failed to open virtual disk
- Automatic restart has been disabled for virtual machine
- Failed to pause Virtual machine
- Failed to Resume Virtual machine
- Snapshot is corrupted
- The physical device could not be found
- Error while attempting to start the virtual machine
- The Hyper-V Virtual Machine Management service encountered an unexpected error
- Hyper-V Virtual Machine Management service failed to start
- Hyper-V Virtual Machine Management service started successfully
- Cannot attach storage media to controller
- Cannot change the media
- Cannot change the virtual hard disk path
- Background disk merge has been interrupted
- Cannot open virtual disk

- Cannot open handle to Hyper-V storage provider
- Cannot access Hyper-V storage provider.
- Invalid MAC address.
- Virtual Machine failed to remove security identifier
- Failed to perform the operation. The virtual machine is not in a valid state to perform the operation
- Virtual machine failed to turn off
- Virtual machine timed out waiting for worker process to exit
- Cannot take snapshot
- Cannot modify the numeric lock when the virtual machine is online
- Cannot change or send keys when the virtual machine is not running
- Virtual machine cannot find a usable certificate
- Cannot modify the boot order when the virtual machine is online
- Failed to initialize the virtual machine during reset

VMMS Operational Logfile Monitoring Policy for Microsoft Hyper-V

VI-MSHyperV_VMMSOperationalWarnError

This policy monitors the log file and forwards virtual machine VMMS operational event log entries to the HPOM console with severity level of warning or error.

In the console tree, these policies are listed at the following locations:

- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Logs → MS Hyper-V**.
- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor → MS Hyper-V- QuickStart**.

The policy looks for the following errors recorded in the log file:

- Hyper-V Virtual Machine Management service is shutting down while some virtual machines are running
- Hyper-V Virtual Machine Management service failed to start
- Virtual Machine is about to run out of disk space
- Virtual network switch name was not found
- Unable to find virtual hard disk file
- The WMI provider failed to start
- Virtual Machine Management service failed to register
- Virtual Machine Management service did not find the virtual machine

- The virtual network switch was not found
- Virtual Machine Management service failed to verify the running state of the virtual machine
- Virtual Machine Management service failed to start the virtual machine
- Error occurred while identifying the Hyper-V VSS writer
- Failed to register domain name
- Failed to create a new virtual machine
- Virtual Machine Bus (VMBus) cannot start
- The virtual machine bus is not running
- Cannot load a snapshot configuration because it is corrupt
- The network adapter is not configured correctly
- Failed to open virtual disk
- Automatic restart has been disabled for virtual machine
- Failed to pause Virtual machine
- Failed to Resume Virtual machine
- Snapshot is corrupted
- The physical device could not be found
- Error while attempting to start the virtual machine
- The Hyper-V Virtual Machine Management service encountered an unexpected error
- Hyper-V Virtual Machine Management service failed to start
- Hyper-V Virtual Machine Management service started successfully
- Cannot attach storage media to controller
- Cannot change the media
- Cannot change the virtual hard disk path
- Background disk merge has been interrupted
- Cannot open virtual disk
- Cannot open handle to Hyper-V storage provider
- Cannot access Hyper-V storage provider.
- Invalid MAC address.
- Virtual Machine failed to remove security identifier
- Failed to perform the operation. The virtual machine is not in a valid state to perform the operation
- Virtual machine failed to turn off
- Virtual machine timed out waiting for worker process to exit
- Cannot take snapshot

- Cannot modify the numeric lock when the virtual machine is online
- Cannot change or send keys when the virtual machine is not running
- Virtual machine cannot find a usable certificate
- Cannot modify the boot order when the virtual machine is online
- Failed to initialize the virtual machine during reset

Hypervisor Worker Administration Logfile Monitoring Policy for Microsoft Hyper-V

VI-MSHyperV_WorkerAdminWarnError

This policy monitors the log file and forwards virtual machine event log for the source Microsoft-Windows-Hyper-V-Worker-Admin to the HPOM console with severity level of warning or error.

In the console tree, these policies are listed at the following locations:

- **Infrastructure Management → <*language*> → Virtualization Infrastructure → Logs → MS Hyper-V**.
- **Infrastructure Management → <*language*> → Virtualization Infrastructure → Policies Grouped by Vendor → MS Hyper-V- QuickStart**.

The policy looks for the following errors recorded in the log file:

- Unsupported static MAC address
- No available MAC address for virtual machines
- Could not open file
- The virtual machine could not be started because the hypervisor is not running
- Cannot modify the GUID, serial number, base board serial number or chassis asset tag when the virtual machine is online
- An unrecoverable internal error has occurred
- Failed to power on virtual machine
- Virtual machine failed to start after reset
- Error while opening file during ethernet device startup
- Virtual machine Out of Memory Error
- The network adapter is not configured correctly
- The virtual machine cannot be started
- error while attempting to start the virtual
- The physical device could not be found
- Failed to open virtual disk
- Error while opening file during ethernet device startup
- Failed to initialize the virtual machine

Hypervisor Worker Operational Logfile Monitoring Policy for Microsoft Hyper-V

VI-MSHyperV_WorkerOperationalWarnError

This policy monitors the log file and forwards virtual machine event log for the source Microsoft-Windows-Hyper-V-Worker-Operational to the HPOM console with severity level of warning or error.

In the console tree, these policies are listed at the following locations:

- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Logs → MS Hyper-V**.
- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor → MS Hyper-V- QuickStart**.

The policy looks for the following errors recorded in the log file:

- Unsupported static MAC address
- No available MAC address for virtual machines
- Could not open file
- The virtual machine could not be started because the hypervisor is not running
- Cannot modify the GUID, serial number, base board serial number or chassis asset tag when the virtual machine is online
- An unrecoverable internal error has occurred
- Failed to power on virtual machine
- Virtual machine failed to start after reset
- Error while opening file during ethernet device startup
- Virtual machine Out of Memory Error
- The network adapter is not configured correctly
- The virtual machine cannot be started
- error while attempting to start the virtual
- The physical device could not be found
- Failed to open virtual disk
- Error while opening file during ethernet device startup
- Failed to initialize the virtual machine

Performance Policies

Performance monitoring helps to identify potential performance disruptions and take pro-active steps to resolve them before they threaten service quality.

In the console tree, the Performance policies are listed at the following location:

Infrastructure Management → *<language>* → Virtualization Infrastructure → Performance

You can use performance data to correlate events across the virtualized infrastructure in order to identify the root cause of a developing performance issue.

Host CPU Utilization Monitor Policy for HPVM

VI-HPVMHostCPUUtilMonitor

The VI-HPVMHostCPUUtilMonitor policy monitors the CPUs on the host servers (managed nodes) for HPVMs and sends an alert message in case the performance goes below the set threshold.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Performance → HPVM**.
- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor → HPVM - QuickStart**.

The VI-HPVMHostCPUUtilMonitor policy provides information about the following:

- Host level CPU utilization
- VMs utilizing the maximum CPU (in descending order)

Metrics Used	GBL_SYSTEM_ID GBL_LS_TYPE GBL_CPU_TOTAL_UTIL BYLS_CPU_PHYS_TOTAL_UTIL BYLS_DISPLAY_NAME
Supported Platform	HPVM
Script-Parameter	**Description**
MessageGroup	Message group for outgoing messages.
CPUUtilMajorThreshold	If the CPU utilization on the host machine is more than the specified threshold value, the policy generates an alert message with severity `Major`.
CPUUtilMinorThreshold	If the CPU utilization on the host machine is more than the specified threshold value, the policy generates an alert message with severity `Minor`.
CPUUtilWarningThreshold	If the CPU utilization on the host machine is more than the specified threshold value, the policy generates an alert message with severity `Warning`.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The alert messages are generated based on the values of the script parameters mentioned in the above table. The alert messages are automatically acknowledged when the values of host CPU utilization reach normal.

The default polling interval for this policy is 5 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

Host CPU Utilization Monitor Policy for IBM LPAR

VI-IBMLPARFrameCPUUtilMonitor

The VI-IBMLPARFrameCPUUtilMonitor policy monitors the CPUs on the frames (managed nodes) for IBM AIX LPARs and sends an alert message in case the performance goes below the set threshold.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Performance → IBM LPAR**
- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor → IBM LPAR - QuickStart**.

The VI-IBMLPARFrameCPUUtilMonitor policy provides information about the following:

- Frame level CPU utilization
- LPARs utilizing the maximum CPU (in descending order)

The policy calculates the frame level CPU utilization with respect to the available CPU's in a frame. However, when generating the list of LPARs utilizing the maximum CPU, the policy calculates the CPU utilization of the LPARs based on BYLS_CPU_PHYS_TOTAL_UTIL metric. This metric provides the CPU utilization information based on the CPUs available in the pool to which the LPAR belongs.

Note: You must deploy this policy on the host machine.

Metrics Used	GBL_SYSTEM_ID GBL_LS_TYPE BYLS_CPU_PHYS_TOTAL_UTIL BYLS_DISPLAY_NAME BYLS_CPU_PHYSC
Supported Platform	IBM LPAR
Script-Parameter	**Description**
MessageGroup	Message group for outgoing messages.

CPUUtilMajorThreshold	If the CPU utilization on the host machine is more than the specified threshold value, the policy generates an alert message with severity `Major`.
CPUUtilMinorThreshold	If the CPU utilization on the host machine is more than the specified threshold value, the policy generates an alert message with severity `Minor`.
CPUUtilWarningThreshold	If the CPU utilization on the host machine is more than the specified threshold value, the policy generates an alert message with severity `Warning`.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The alert messages are generated based on the values of the script parameters mentioned in the above table. The alert messages are automatically acknowledged when the values of host CPU utilization reach normal.

The default polling interval for this policy is 5 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

Host CPU Utilization Monitor Policy for Microsoft Hyper-V

VI-MSHyperVHostCPUUtilMonitor

The VI-MSHyperVHostCPUUtilMonitor policy monitors the CPUs on the host servers (managed nodes) for Microsoft Hyper-V and sends an alert message in case the performance goes below the set threshold.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → <*language*> → Virtualization Infrastructure → Performance → MS Hyper-V**.
- **Infrastructure Management → <*language*> → Virtualization Infrastructure → Policies Grouped by Vendor → MS Hyper-V - QuickStart**.

The VI-MSHyperVHostCPUUtilMonitor policy provides information about the following:

- Host level CPU utilization
- VMs utilizing the maximum CPU (in descending order)

Metrics Used	GBL_SYSTEM_ID GBL_LS_TYPE GBL_CPU_TOTAL_UTIL BYLS_CPU_PHYS_TOTAL_UTIL BYLS_DISPLAY_NAME

Supported Platform	Microsoft Hyper-V
Script-Parameter	**Description**
MessageGroup	Message group for outgoing messages.
CPUUtilMajorThreshold	If the CPU utilization on the host machine is more than the specified threshold value, the policy generates an alert message with severity `Major`.
CPUUtilMinorThreshold	If the CPU utilization on the host machine is more than the specified threshold value, the policy generates an alert message with severity `Minor`.
CPUUtilWarningThreshold	If the CPU utilization on the host machine is more than the specified threshold value, the policy generates an alert message with severity `Warning`.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The alert messages are generated based on the values of the script parameters mentioned in the above table. The alert messages are automatically acknowledged when the values of host CPU utilization reach normal.

The default polling interval for this policy is 5 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

Host CPU Utilization Monitor Policy for Oracle Solaris Zones

VI-OracleSolarisHostCPUUtilMonitor

The VI-OracleSolarisHostCPUUtilMonitor policy monitors the CPUs on the host servers (managed nodes) for Solaris zones and sends an alert message in case the performance goes below the set threshold.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Performance → Oracle Containers**
- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor → Oracle Containers - QuickStart**.

The VI-OracleSolarisHostCPUUtilMonitor policy provides information about the following:

- Host level CPU utilization
- Zones utilizing the maximum CPU (in descending order)

Metrics Used	GBL_SYSTEM_ID

	GBL_LS_TYPE GBL_CPU_TOTAL_UTIL BYLS_CPU_PHYS_TOTAL_UTIL BYLS_DISPLAY_NAME
Supported Platform	Oracle Solaris Zones
Script-Parameter	**Description**
MessageGroup	Message group for outgoing messages.
CPUUtilMajorThreshold	If the CPU utilization on the host machine is more than the specified threshold value, the policy generates an alert message with severity `Major`.
CPUUtilMinorThreshold	If the CPU utilization on the host machine is more than the specified threshold value, the policy generates an alert message with severity `Minor`.
CPUUtilWarningThreshold	If the CPU utilization on the host machine is more than the specified threshold value, the policy generates an alert message with severity `Warning`.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The alert messages are generated based on the values of the script parameters mentioned in the above table. The alert messages are automatically acknowledged when the values of host CPU utilization reach normal.

The default polling interval for this policy is 5 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

Total VM CPU Utilization Monitor Policy for VMware ESX or ESXi Servers

VI-VMwareTotalVMCPUUtilMonitor

The VI-VMwareTotalVMCPUUtilMonitor policy monitors and maintains information about the CPUs on the VMware host server (managed node). The policy monitors CPU utilization and ready utilization of all virtual machines on a particular host managed by a vMA and sends an alert message to the HPOM console in case of any violations.

In the console tree, the policy is listed at the following location:

- **Infrastructure Management** → ***<language>*** → **Virtualization Infrastructure** → **Performance** → **VMware ESX**.
- **Infrastructure Management** → ***<language>*** → **Virtualization Infrastructure** → **Policies Grouped by Vendor** → **VMware ESX - Advanced**.

The VI-VMwareTotalCPUUtilMonitor policy provides information about the following:

- Host level CPU utilization
- VMs utilizing the maximum CPU (in descending order)

Metrics Used	BYLS_LS_ROLE BYLS_LS_UUID BYLS_LS_NAME BYLS_LS_HOSTNAME BYLS_LS_STATE BYLS_LS_PARENT_UUID BYLS_CPU_PHYS_READY_UTIL BYLS_CPU_PHYS_TOTAL_UTIL BYLS_DISPLAY_NAME
Supported Platform	VMware ESX or ESXi
Script-Parameter	**Description**
MessageGroup	Message group for outgoing messages.
CPUUtilMajorThreshold	If the CPU utilization on the host machine is more than the specified threshold value, the policy generates an alert message with severity `Major`.
CPUUtilMinorThreshold	If the CPU utilization on the host machine is more than the specified threshold value, the policy generates an alert message with severity `Minor`.
CPUUtilWarningThreshold	If the CPU utilization on the host machine is more than the specified threshold value, the policy generates an alert message with severity `Warning`.
CPUReadyTimeMajorThreshold	If the value for minimum CPU ready time is more than the specified threshold value, the policy generates an alert message with severity `Major`.
CPUReadyTimeMinorThreshold	If the value for minimum CPU ready time is more than the specified threshold value, the policy generates an alert message with severity `Minor`.
CPUReadyTimeWarningThreshold	If the value for minimum CPU ready time is more than the specified threshold value, the policy generates an alert message with severity `Warning`.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 5 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

After the values return within normal levels, the alert messages are automatically acknowledged.

Host CPU Utilization Monitor Policy for VMware ESX or ESXi Servers

VI-VMwareHostsCPUUtilMonitor

The VI-VMwareHostsCPUUtilMonitor policy calculates the CPU utilization of the active VMs under the host VMware ESX or ESXi servers.

When the threshold values are reached or exceeded, the policy sends an alert message to the HPOM console. The message severity can be major, minor, or warning depending upon the level of threshold violated.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management** → ***<language>*** → **Virtualization Infrastructure** → **Performance** → **VMware ESX**.
- **Infrastructure Management** → ***<language>*** → **Virtualization Infrastructure** → **Policies Grouped by Vendor** → **VMware ESX - Advanced**.

Metrics Used	BYLS_LS_ROLE BYLS_LS_UUID BYLS_LS_STATE BYLS_MACHINE_MODEL BYLS_CPU_PHYS_TOTAL_UTIL BYLS_LS_HOSTNAME
Supported Platform	VMware ESX or ESXi
Script-Parameter	**Description**
HostsCpuUtilCriticalThreshold	If the CPU utilization on the host machine is more than the critical threshold value, the policy generates an alert message with severity `Critical`.
HostsCpuUtilMajorThreshold	If the CPU utilization on the host machine is more than the major threshold value, the policy generates an alert message with severity `Major`.
HostsCpuUtilMinorThreshold	If the CPU utilization on the host machine is more than the minor threshold value, the policy generates an alert message with severity `Minor`.
HostsCpuUtilWarningThreshold	If the CPU utilization on the host machine is more than the warning threshold value, the policy generates an alert

	message with severity `Warning`.
MessageGroup	Message group for outgoing messages.
MessageApplication	Application for outgoing messages.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 5 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

After the values return within normal levels, the alert messages are automatically acknowledged.

Host CPU Utilization (by Virtual Machines) Monitor Policy for VMware ESX or ESXi Servers

VI-VMwareHostsCPUUtilMonitor-AT

The VI-VMwareHostsCPUUtilMonitor-AT policy calculates the total host CPU utilization (including the Service Console's CPU usage) of the active VMs under the host VMware ESX or ESXi servers

The threshold values for this policy are automatically calculated based on the previous CPU utilization records.

When the threshold values are reached or exceeded, the policy sends an alert message to the HPOM console. The message severity can be major, minor, or warning depending upon the level of threshold violated.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → <*language*> → Virtualization Infrastructure → Performance → VMware ESX**.
- **Infrastructure Management → <*language*> → Virtualization Infrastructure → Policies Grouped by Vendor → VMware ESX - Advanced**.

Metrics Used	BYLS_LS_ROLE BYLS_LS_HOSTNAME BYLS_CPU_PHYS_TOTAL_UTIL
Supported Platform	VMware ESX or ESXi
Script-Parameter	**Description**
MessageObject	Application for outgoing messages.
DataSource	Displays the data source name as SCOPE.
DataObject	Displays the data object name as LOGICAL.

DataMetric	Displays the metric name as BYLS_CPU_ENTL_UTIL.
BaselinePeriod	Type the time period you want to define as a baseline period, such as '3600 seconds'. This period moves with the current time. The most recent 3600-second (1-hour) period becomes the current baseline period.
MinimumValue	Displays the minimum value of the CPU utilization as indicated by the metric.
MaximumValue	Displays the maximum value of the CPU utilization as indicated by the metric.
WarningDeviations	Displays the number of standard deviation away from normal, at which the policy sends a warning message to HPOM console. Set an appropriate value for the parameter. To disable the parameter, set value as *5*.
MinorDeviations	Displays the number of standard deviation away from normal, at which the policy sends a minor message to HPOM console. Set an appropriate value for the parameter greater than the specified value for *WarningDeviations*. To disable the parameter, set value as *5*.
WarningHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
WarningLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in

	MinorDeviations. To disable the parameter, set value as *none*.
MajorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
MessageGroup	Message group for outgoing messages.
HostCPUUtilCutOff	Set a value below which you do not want to monitor CPU utilization.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 5 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

After the values return within normal levels, the alert messages are automatically acknowledged.

Host CPU Utilization Monitor for VMware vCenter

VI-VMwareVCHostCPUUtilMonitor

The VI-VMwareVCHostCPUUtilMonitor policy monitors the CPU utilization for ESX or ESX/i host.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Performance → VMware vCenter**.
- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor → VMware vCenter - Advanced**.

Metrics Used	• SystemRole • SystemState • CPUPhysTotalUtil • SystemName
Supported Platforms	VMware vCenter
Script-Parameter	**Description**
HostCpuUtilCriticalThreshold	If the CPU Utilization for a Host Esx/i is more than the specified threshold value, the policy generates an alert message with severity `Critical`.
HostCpuUtilMajorThreshold	If the CPU Utilization for a Host Esx/i is more than the specified

	threshold value, the policy generates an alert message with severity `Major`.
HostCpuUtilMinorThreshold	If the CPU Utilization for a Host Esx/i is more than the specified threshold value, the policy generates an alert message with severity `Minor`.
HostCpuU-tilWarningThreshold	If the CPU Utilization for a Host Esx/i is more than the specified threshold value, the policy generates an alert message with severity `Warning`.
MessageGroup	Message group for outgoing messages.
MessageApplication	Application for outgoing messages
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 5 minutes. You can modify the polling interval based on your requirements.

Total Frame CPU Utilization Monitor Policy for IBM LPAR

VI-IBMLPARFrameCPUUtilMonitor-AT

The VI-IBMLPARFrameCPUUtilMonitor-AT policy calculates the total CPU utilization of all active LPARS within a frame.

The threshold values for this policy are automatically calculated based on the previous CPU utilization by the LPARs.

When the threshold values are reached or exceeded, the policy sends an alert message to the HPOM console. The message severity can be major, minor, or warning depending upon the level of threshold violated.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management** → **<*language*>** → **Virtualization Infrastructure** → **Performance** → **IBM LPAR**.
- **Infrastructure Management** → **<*language*>** → **Virtualization Infrastructure** → **Policies Grouped by Vendor** → **IBM LPAR - Advanced**.

Metrics Used	FRAME_CPU_UTIL GBL_LS_TYPE
Supported Platform	IBM LPAR
Script-Parameter	**Description**
MessageObject	Application for outgoing messages.

DataSource	Displays the data source name as SCOPE.
DataObject	Displays the data object name as LOGICAL.
DataMetric	Displays the metric name as FRAME_CPU_UTIL.
BaselinePeriod	Type the time period you want to define as a baseline period, such as '3600 seconds'. This period moves with the current time. The most recent 3600-second (1-hour) period becomes the current baseline period.
MinimumValue	Displays the minimum value of the CPU utilization as indicated by the metric.
MaximumValue	Displays the maximum value of the CPU utilization as indicated by the metric.
WarningDeviations	Displays the number of standard deviation away from normal, at which the policy sends a warning message to HPOM console. Set an appropriate value for the parameter. To disable the parameter, set value as *5*.
MinorDeviations	Displays the number of standard deviation away from normal, at which the policy sends a minor message to HPOM console. Set an appropriate value for the parameter greater than the specified value for *WarningDeviations*. To disable the parameter, set value as *5*.
MajorDeviations	Displays the number of standard deviation away from normal, at which the policy sends a major message to HPOM console. Set an appropriate value for the parameter greater than the specified value for *MinorDeviations*. To disable the parameter, set value as *5*.
WarningHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
WarningLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.

MinorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
MessageGroup	Message group for outgoing messages.
LPARFrameCPUUtilCutOff	Set a value below which you do not want to monitor CPU utilization.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 30 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

After the values return within normal levels, the alert messages are automatically acknowledged.

Note: The **VI-IBMLPARFrameCPUUtilMonitor-AT** policy is dependent on the **VI-IBMLPARFrameMemoryUtilMonitor** policy as the **FRAME_CPU_UTIL** metric is collected in the **VI-IBMLPARFrameMemoryUtilMonitor** policy

CPU Entitlement Utilization Monitor Policy for HPVM

VI-HPVMGuestCPUEntlUtilMonitor-AT

The VI-HPVMCPUEntlUtilMonitor-AT policy calculates the current CPU utilization (in percentage) of HPVM guests. It indicates the logical system's CPU utilization against the minimum entitled CPU. Entitled CPU is the number of guaranteed processing units allocated to a logical system.

The threshold values for this policy are automatically calculated based on the previous CPU utilization by the guests.

When the threshold values are reached or exceeded, the policy sends an alert message to the HPOM console. The message severity can be major, minor, or warning depending upon the level of threshold violated.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → <*language*> → Virtualization Infrastructure → Performance → HPVM**.
- **Infrastructure Management → <*language*> → Virtualization Infrastructure → Policies Grouped by Vendor → HPVM - Advanced**.

Metrics Used	BYLS_CPU_ENTL_UTIL BYLS_LS_NAME BYLS_DISPLAY_NAME GBL_LS_TYPE
Supported Platform	HPVM
Script-Parameter	**Description**
MessageObject	Application for outgoing messages.
DataSource	Displays the data source name as SCOPE.
DataObject	Displays the data object name as LOGICAL.
DataMetric	Displays the metric name as BYLS_CPU_ENTL_UTIL.
BaselinePeriod	Type the time period you want to define as a baseline period, such as '3600 seconds'. This period moves with the current time. The most recent 3600-second (1-hour) period becomes the current baseline period.
MinimumValue	Displays the minimum value of the CPU utilization as indicated by the metric.
MaximumValue	Displays the maximum value of the CPU utilization as indicated by the metric.
WarningDeviations	Displays the number of standard deviation away from normal, at which the policy sends a warning message to HPOM console. Set an appropriate value for the parameter. To disable the parameter, set value as *5*.
MinorDeviations	Displays the number of standard deviation away from normal, at which the policy sends a minor message to HPOM console. Set an appropriate value for the parameter greater than the specified value for *WarningDeviations*. To disable the parameter, set value as *5*.
MajorDeviations	Displays the number of standard deviation away from normal, at which the policy sends a major message to HPOM console. Set an appropriate value for the parameter greater than the specified value for *MinorDeviations*. To disable the parameter, set value as *5*.
WarningHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorHighSeverity	Displays the severity of the alert messages to be sent to HPOM

	console in case the current data meets or exceeds the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
WarningLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
MessageGroup	Message group for outgoing messages.
CPUEntlUtilCutOff	Set a value below which you do not want to monitor CPU utilization.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 30 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

After the values return within normal levels, the alert messages are automatically acknowledged.

CPU Entitlement Utilization Monitor Policy for IBM LPAR

VI-IBMLPARCPUEntlUtilMonitor-AT

This policy calculates the current CPU utilization (in percentage) of AIX LPARs. It indicates the logical system's CPU utilization against the minimum entitled CPU. Entitled CPU is the number of guaranteed processing units allocated to a logical system.

The threshold values for this policy are automatically calculated based on the previous CPU utilization by the LPARs.

When the threshold values are reached or exceeded, the policy sends an alert message to the HPOM console. The message severity can be major, minor, or warning depending upon the level of threshold violated.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Performance → IBM LPAR**.
- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor → IBM LPAR - Advanced**.

Note: This policy does not monitor the WPARs running on the LPAR. To monitor the WPARs deploy the VI-IBMWPARCPUEntlUtilMonitor-AT policy. See "CPU Entitlement Utilization Monitor Policy for IBM WPAR" on next page.

Metrics Used	BYLS_CPU_ENTL_UTIL BYLS_LS_NAME BYLS_DISPLAY_NAME BYLS_LS_TYPE
Supported Platform	IBM LPAR
Script-Parameter	**Description**
MessageObject	Application for outgoing messages.
DataSource	Displays the data source name as SCOPE.
DataObject	Displays the data object name as LOGICAL.
DataMetric	Displays the metric name as BYLS_CPU_ENTL_UTIL.
BaselinePeriod	Type the time period you want to define as a baseline period, such as '3600 seconds'. This period moves with the current time. The most recent 3600-second (1-hour) period becomes the current baseline period.
MinimumValue	Displays the minimum value of the CPU utilization as indicated by the metric.
MaximumValue	Displays the maximum value of the CPU utilization as indicated by the metric.
WarningDeviations	Displays the number of standard deviation away from normal, at which the policy sends a warning message to HPOM console. Set an appropriate value for the parameter. To disable the parameter, set value as *5*.
MinorDeviations	Displays the number of standard deviation away from normal, at which the policy sends a minor message to HPOM console. Set an appropriate value for the parameter greater than the specified value for *WarningDeviations*. To disable the parameter, set value as *5*.

MajorDeviations	Displays the number of standard deviation away from normal, at which the policy sends a major message to HPOM console. Set an appropriate value for the parameter greater than the specified value for *MinorDeviations*. To disable the parameter, set value as *5*.
WarningHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
WarningLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
MessageGroup	Message group for outgoing messages.
CPUEntlUtilCutOff	Set a value below which you do not want to monitor CPU utilization.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 30 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

After the values return within normal levels, the alert messages are automatically acknowledged.

CPU Entitlement Utilization Monitor Policy for IBM WPAR

VI-IBMWPARCPUEntlUtilMonitor-AT

This policy calculates the current CPU utilization (in percentage) of AIX WPARs. It indicates the logical system's CPU utilization against the minimum entitled CPU. Entitled CPU is the number of guaranteed processing units allocated to a logical system.

The threshold values for this policy are automatically calculated based on the previous CPU utilization by the WPARs.

When the threshold values are reached or exceeded, the policy sends an alert message to the HPOM console. The message severity can be major, minor, or warning depending upon the level of threshold violated.

Note: The VI-IBMWPARCPUEntlUtilMonitor-AT policy monitors only the WPARs that are created in an LPAR on which PA 5.0 is running.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management** → **<*language*>** → **Virtualization Infrastructure** → **Performance** → **IBM LPAR**.
- **Infrastructure Management** → **<*language*>** → **Virtualization Infrastructure** → **Policies Grouped by Vendor** → **IBM LPAR - Advanced**.

Metrics Used	BYLS_CPU_ENTL_UTIL BYLS_LS_NAME BYLS_DISPLAY_NAME BYLS_LS_TYPE
Supported Platform	IBM WPAR
Script-Parameter	**Description**
MessageObject	Application for outgoing messages.
DataSource	Displays the data source name as SCOPE.
DataObject	Displays the data object name as LOGICAL.
DataMetric	Displays the metric name as BYLS_CPU_ENTL_UTIL.
BaselinePeriod	Type the time period you want to define as a baseline period, such as '3600 seconds'. This period moves with the current time. The most recent 3600-second (1-hour) period becomes the current baseline period.
MinimumValue	Displays the minimum value of the CPU utilization as indicated by the metric.
MaximumValue	Displays the maximum value of the CPU utilization as indicated by the metric.
WarningDeviations	Displays the number of standard deviation away form normal, at

	which the policy sends a warning message to HPOM console. Set an appropriate value for the parameter. To disable the parameter, set value as *5*.
MinorDeviations	Displays the number of standard deviation away form normal, at which the policy sends a minor message to HPOM console. Set an appropriate value for the parameter greater than the specified value for *WarningDeviations*. To disable the parameter, set value as *5*.
MajorDeviations	Displays the number of standard deviation away form normal, at which the policy sends a major message to HPOM console. Set an appropriate value for the parameter greater than the specified value for *MinorDeviations*. To disable the parameter, set value as *5*.
WarningHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
WarningLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
MessageGroup	Message group for outgoing messages.
CPUEntlUtilCutOff	Set a value below which you do not want to monitor CPU utilization.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 30 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

After the values return within normal levels, the alert messages are automatically acknowledged.

CPU Entitlement Utilization Monitor Policy for Microsoft Hyper-V

VI-MSHyperVGuestCPUEntlUtilMonitor-AT

This policy calculates the current CPU utilization (in percentage) of Microsoft Hyper-V. It indicates the logical system's CPU utilization against the minimum entitled CPU. Entitled CPU is the number of guaranteed processing units allocated to a logical system.

The threshold values for this policy are automatically calculated based on the previous CPU utilization by Microsoft Hyper-V.

When the threshold values are reached or exceeded, the policy sends an alert to the HPOM console. The message severity can be major, minor, or warning depending upon the level of threshold violated.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → <*language*> → Virtualization Infrastructure → Performance → MS Hyper-V**.
- **Infrastructure Management → <*language*> → Virtualization Infrastructure → Policies Grouped by Vendor → MS Hyper-V - Advanced**.

Metrics Used	BYLS_CPU_ENTL_UTIL BYLS_LS_NAME BYLS_DISPLAY_NAME GBL_LS_TYPE
Supported Platform	Microsoft Hyper-V
Script-Parameter	**Description**
MessageObject	Application for outgoing messages.
DataSource	Displays the data source name as SCOPE.
DataObject	Displays the data object name as LOGICAL.
DataMetric	Displays the metric name as BYLS_CPU_ENTL_UTIL.
BaselinePeriod	Type the time period you want to define as a baseline period, such as '3600 seconds'. This period moves with the current time. The most recent 3600-second (1-hour) period becomes the current baseline period.

MinimumValue	Displays the minimum value of the CPU utilization as indicated by the metric.
MaximumValue	Displays the maximum value of the CPU utilization as indicated by the metric.
WarningDeviations	Displays the number of standard deviation away form normal, at which the policy sends a warning message to HPOM console. Set an appropriate value for the parameter. To disable the parameter, set value as *5*.
MinorDeviations	Displays the number of standard deviation away form normal, at which the policy sends a minor message to HPOM console. Set an appropriate value for the parameter greater than the specified value for *WarningDeviations*. To disable the parameter, set value as *5*.
MajorDeviations	Displays the number of standard deviation away form normal, at which the policy sends a major message to HPOM console. Set an appropriate value for the parameter greater than the specified value for *MinorDeviations*. To disable the parameter, set value as *5*.
WarningHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
WarningLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.

MessageGroup	Message group for outgoing messages.
CPUEntlUtilCutOff	Set a value below which you do not want to monitor CPU utilization.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 30 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

After the values return within normal levels, the alert messages are automatically acknowledged.

CPU Entitlement Utilization Monitor Policy for Oracle Solaris Zones

VI-OracleSolarisZoneCPUEntlUtilMonitor-AT

This policy calculates the current CPU utilization (in percentage) of Solaris zones. It indicates the logical system's CPU utilization against the minimum entitled CPU. Entitled CPU is the number of guaranteed processing units allocated to a logical system.

The threshold values for this policy are automatically calculated based on the previous CPU utilization by the zones.

When the threshold values are reached or exceeded, the policy sends an alert message to the HPOM console. The message severity can be major, minor, or warning depending upon the level of threshold violated.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Performance → Oracle Containers**.
- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor → Oracle Containers - Advanced**.

Metrics Used	BYLS_CPU_ENTL_UTIL BYLS_LS_NAME BYLS_DISPLAY_NAME GBL_LS_TYPE
Supported Platform	Oracle Solaris Zones
Script-Parameter	**Description**
MessageObject	Application for outgoing messages.
DataSource	Displays the data source name as SCOPE.

DataObject	Displays the data object name as LOGICAL.
DataMetric	Displays the metric name as BYLS_CPU_ENTL_UTIL.
BaselinePeriod	Type the time period you want to define as a baseline period, such as '3600 seconds'. This period moves with the current time. The most recent 3600-second (1-hour) period becomes the current baseline period.
MinimumValue	Displays the minimum value of the CPU utilization as indicated by the metric.
MaximumValue	Displays the maximum value of the CPU utilization as indicated by the metric.
WarningDeviations	Displays the number of standard deviation away form normal, at which the policy sends a warning message to HPOM console. Set an appropriate value for the parameter. To disable the parameter, set value as *5*.
MinorDeviations	Displays the number of standard deviation away form normal, at which the policy sends a minor message to HPOM console. Set an appropriate value for the parameter greater than the specified value for *WarningDeviations*. To disable the parameter, set value as *5*.
MajorDeviations	Displays the number of standard deviation away form normal, at which the policy sends a major message to HPOM console. Set an appropriate value for the parameter greater than the specified value for *MinorDeviations*. To disable the parameter, set value as *5*.
WarningHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
WarningLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.

MinorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
MessageGroup	Message group for outgoing messages.
CPUEntlUtilCutOff	Set a value below which you do not want to monitor CPU utilization.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 30 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

After the values return within normal levels, the alert messages are automatically acknowledged.

CPU Entitlement Utilization Monitor Policy for VMware ESX or ESXi Servers

VI-VmWareGuestCPUEntlUtilMonitor-AT

This policy calculates the current CPU utilization (in percentage) of VMware ESX or ESXi servers. It indicates the logical system's CPU utilization against the minimum entitled CPU. Entitled CPU is the number of guaranteed processing units allocated to a logical system.

The threshold values for this policy are automatically calculated based on the previous CPU utilization by the ESX or ESXi servers.

When the threshold values are reached or exceeded, the policy sends an alert message to the HPOM console. The message severity can be major, minor, or warning depending upon the level of threshold violated.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → <*language*> → Virtualization Infrastructure → Performance → VMware ESX**.
- **Infrastructure Management → <*language*> → Virtualization Infrastructure → Policies Grouped by Vendor → VMware ESX - Advanced**.

Metrics Used	BYLS_CPU_ENTL_UTIL BYLS_LS_NAME

	BYLS_DISPLAY_NAME GBL_LS_TYPE
Supported Platform	VMware ESX or ESXi
Script-Parameter	**Description**
MessageObject	Application for outgoing messages.
DataSource	Displays the data source name as SCOPE.
DataObject	Displays the data object name as LOGICAL.
DataMetric	Displays the metric name as BYLS_CPU_ENTL_UTIL.
BaselinePeriod	Type the time period you want to define as a baseline period, such as '3600 seconds'. This period moves with the current time. The most recent 3600-second (1-hour) period becomes the current baseline period.
MinimumValue	Displays the minimum value of the CPU utilization as indicated by the metric.
MaximumValue	Displays the maximum value of the CPU utilization as indicated by the metric.
WarningDeviations	Displays the number of standard deviation away form normal, at which the policy sends a warning message to HPOM console. Set an appropriate value for the parameter. To disable the parameter, set value as *5*.
MinorDeviations	Displays the number of standard deviation away form normal, at which the policy sends a minor message to HPOM console. Set an appropriate value for the parameter greater than the specified value for *WarningDeviations*. To disable the parameter, set value as *5*.
MajorDeviations	Displays the number of standard deviation away form normal, at which the policy sends a major message to HPOM console. Set an appropriate value for the parameter greater than the specified value for *MinorDeviations*. To disable the parameter, set value as *5*.
WarningHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.

MajorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
WarningLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
MessageGroup	Message group for outgoing messages.
CPUEntlUtilCutOff	Set a value below which you do not want to monitor CPU utilization.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 30 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

After the values return within normal levels, the alert messages are automatically acknowledged.

CPU Saturation Monitor Policy for VMware vCenter

VI-VMwareVCHostCPUSaturationMonitor

The VI-VMwareVCHostCPUSaturationMonitor policy monitors the consumption of host CPUs by virtual machines. The alert message lists the virtual machines that continuously use a significant amount of the CPU resource.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Performance → VMware vCenter**.
- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor → VMware vCenter - Advanced**.

Metrics Used	• SystemRole

	• SystemID • SystemState • CPUPhysTotalUtil • SystemName
Supported Platforms	VMware vCenter
Script-Parameter	**Description**
HostCpuUtilCriticalThreshold	If the CPU utilization on the host machine is more than the critical threshold value, the policy generates an alert message with severity `Critical`.
HostCpuUtilMajorThreshold	If the CPU utilization on the host machine is more than the major threshold value, the policy generates an alert message with severity `Major`.
HostCpuUtilMinorThreshold	If the CPU utilization on the host machine is more than the minor threshold value, the policy generates an alert message with severity `Minor`.
HostCpuUtilWarningThreshold	If the CPU utilization on the host machine is more than the warning threshold value, the policy generates an alert message with severity `Warning`.
VMCPUReadyPercentThreshold	The ready utilization of a CPU for a virtual machine should be less than 20 percent.
VMCPUUtilMaxThreshold	The maximum CPU utilization for a virtual machine.
VMCPUUtilMinThreshold	The minimum CPU utilization for a virtual machine.
HighCPUU-tilVMCountPercentThreshold	The threshold count of high CPU utilization of the virtual machines for the host.
HighCPU-ReadyVMCountPercentThreshold	The threshold count of high CPU ready utilization of the virtual machines for the host.
MessageGroup	Message group for outgoing messages.
MessageApplication	Application for outgoing messages.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 5 minutes. You can modify the polling interval based on your requirements.

Memory Entitlement Utilization Monitor Policy for IBM LPAR

VI-IBMLPARMemoryEntlUtilMonitor-AT

The VI-IBMLPARMemoryEntlUtilMonitor-AT policy calculates the current memory utilization (in percentage) of all IBM LPARs in ACTIVE state. It indicates the LPAR's memory utilization against the minimum entitled memory.

Entitled memory is the amount of guaranteed memory allocated to a logical system.

The threshold values for this policy are automatically calculated based on the previous memory utilization by the LPARs.

When the threshold values are reached or exceeded, the policy sends an alert message to the HPOM console. The message severity can be major, minor, or warning depending upon the level of threshold violated.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Performance → IBM LPAR**.
- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor → IBM LPAR - Advanced**.

Metrics Used	BYLS_MEM_ENTL_UTIL BYLS_LS_NAME BYLS_LS_STATE BYLS_DISPLAY_NAME GBL_LS_TYPE
Supported Platform	IBM LPAR
Script-Parameter	**Description**
MessageObject	Application for outgoing messages.
DataSource	Displays the data source name as SCOPE.
DataObject	Displays the data object name as LOGICAL.
DataMetric	Displays the metric name as BYLS_MEM_ENTL_UTIL.
BaselinePeriod	Type the time period you want to define as a baseline period, such as '3600 seconds'. This period moves with the current time. The most recent 3600-second (1-hour) period becomes the current baseline period.
MinimumValue	Displays the minimum value of the entitled memory utilization as indicated by the metric.

MaximumValue	Displays the maximum value of the entitled memory utilization as indicated by the metric.
WarningDeviations	Displays the number of standard deviation away form normal, at which the policy sends a warning message to HPOM console. Set an appropriate value for the parameter. To disable the parameter, set value as *5*.
MinorDeviations	Displays the number of standard deviation away form normal, at which the policy sends a minor message to HPOM console. Set an appropriate value for the parameter greater than the specified value for *WarningDeviations*. To disable the parameter, set value as *5*.
MajorDeviations	Displays the number of standard deviation away form normal, at which the policy sends a major message to HPOM console. Set an appropriate value for the parameter greater than the specified value for *MinorDeviations*. To disable the parameter, set value as *5*.
WarningHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
WarningLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
MessageGroup	Message group for outgoing messages.

MEMEntlUtilCutOff	Set a value below which you do not want to monitor memory utilization.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 30 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

After the values return within normal levels, the alert messages are automatically acknowledged.

Memory Entitlement Utilization Monitor Policy for IBM WPAR

VI-IBMWPARMemoryEntlUtilMonitor-AT

The VI-IBMWPARMemoryEntlUtilMonitor-AT policy calculates the current memory utilization (in percentage) of IBM WPARs (running on the monitoring LPAR) in ACTIVE state. It indicates the WPAR's memory utilization against the minimum entitled memory.

Entitled memory is the amount of guaranteed memory allocated to a logical system.

The threshold values for this policy are automatically calculated based on the previous memory utilization by the WPARs.

When the threshold values are reached or exceeded, the policy sends an alert message to the HPOM console. The message severity can be major, minor, or warning depending upon the level of threshold violated.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → <*language*> → Virtualization Infrastructure → Performance → IBM LPAR**.
- **Infrastructure Management → <*language*> → Virtualization Infrastructure → Policies Grouped by Vendor → IBM LPAR - Advanced**.

Metrics Used	BYLS_MEM_ENTL_UTIL BYLS_LS_NAME BYLS_LS_STATE BYLS_DISPLAY_NAME GBL_LS_TYPE
Supported Platform	IBM WPAR
Script-Parameter	**Description**

MessageObject	Application for outgoing messages.
DataSource	Displays the data source name as SCOPE.
DataObject	Displays the data object name as LOGICAL.
DataMetric	Displays the metric name as BYLS_MEM_ENTL_UTIL.
BaselinePeriod	Type the time period you want to define as a baseline period, such as '3600 seconds'. This period moves with the current time. The most recent 3600-second (1-hour) period becomes the current baseline period.
MinimumValue	Displays the minimum value of the entitled memory utilization as indicated by the metric.
MaximumValue	Displays the maximum value of the entitled memory utilization as indicated by the metric.
WarningDeviations	Displays the number of standard deviation away form normal, at which the policy sends a warning message to HPOM console. Set an appropriate value for the parameter. To disable the parameter, set value as *5*.
MinorDeviations	Displays the number of standard deviation away form normal, at which the policy sends a minor message to HPOM console. Set an appropriate value for the parameter greater than the specified value for *WarningDeviations*. To disable the parameter, set value as *5*.
MajorDeviations	Displays the number of standard deviation away form normal, at which the policy sends a major message to HPOM console. Set an appropriate value for the parameter greater than the specified value for *MinorDeviations*. To disable the parameter, set value as *5*.
WarningHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
WarningLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample

	data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
MessageGroup	Message group for outgoing messages.
MEMEntlUtilCutOff	Set a value below which you do not want to monitor memory utilization.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 30 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

After the values return within normal levels, the alert messages are automatically acknowledged.

Memory Entitlement Utilization Monitor Policy for Oracle Solaris Zones

VI-OracleSolarisMemoryEntlUtilMonitor-AT

The VI-OracleSolarisMemoryEntlUtilMonitor-AT policy calculates the current memory utilization (in percentage) of all Solaris zones in RUNNING state. It indicates the zone's memory utilization against the minimum entitled memory.

Entitled memory is the amount of guaranteed memory allocated to a logical system.

The threshold values for this policy are automatically calculated based on the previous memory utilization by the zones.

When the threshold values are reached or exceeded, the policy sends an alert message to the HPOM console. The message severity can be major, minor, or warning depending upon the level of threshold violated.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → <*language*> → Virtualization Infrastructure → Performance → Oracle Containers**.
- **Infrastructure Management → <*language*> → Virtualization Infrastructure → Policies Grouped by Vendor → Oracle Containers - Advanced**.

Metrics Used	BYLS_MEM_ENTL_UTIL (This is calculated against capped memory value if zone is capped and against total physical memory if zone is uncapped.) BYLS_LS_NAME BYLS_LS_STATE BYLS_DISPLAY_NAME GBL_LS_TYPE
Supported Platform	Oracle Solaris Zones

Script-Parameter	Description
MessageObject	Application for outgoing messages.
DataSource	Displays the data source name as SCOPE.
DataObject	Displays the data object name as LOGICAL.
DataMetric	Displays the metric name as BYLS_MEM_ENTL_UTIL.
BaselinePeriod	Type the time period you want to define as a baseline period, such as '3600 seconds'. This period moves with the current time. The most recent 3600-second (1-hour) period becomes the current baseline period.
MinimumValue	Displays the minimum value of the entitled memory utilization as indicated by the metric.
MaximumValue	Displays the maximum value of the entitled memory utilization as indicated by the metric.
WarningDeviations	Displays the number of standard deviation away form normal, at which the policy sends a warning message to HPOM console. Set an appropriate value for the parameter. To disable the parameter, set value as *5*.
MinorDeviations	Displays the number of standard deviation away form normal, at which the policy sends a minor message to HPOM console. Set an appropriate value for the parameter greater than the specified value for *WarningDeviations*. To disable the parameter, set value as *5*.
MajorDeviations	Displays the number of standard deviation away form normal, at which the policy sends a major message to HPOM console. Set an appropriate value for the parameter greater than the specified value for *MinorDeviations*. To disable the parameter, set value as *5*.
WarningHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *WarningDeviations*. To

	disable the parameter, set value as *none*.
MinorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
WarningLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
MessageGroup	Message group for outgoing messages.
MEMEntlUtilCutOff	Set a value below which you do not want to monitor memory utilization.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

Note: For a zone with memory cap there is a slight deviation between the values generated by the metrics and that of the value given by system command **prstat -Z**.

The default polling interval for this policy is 30 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

After the values return within normal levels, the alert messages are automatically acknowledged.

Network Interface In-Byte Rate Monitor Policy for VMware ESX or ESXi Servers

VI-VMwareNetifInbyteBaseline-AT

The VI-VMwareNetifInbyteBaseline-AT policy monitors the network interface in-byte or in-packet rate for a network interface in a given interval. It collectively monitors all instances of the incoming

bytes or packets on each network interface on the managed node. The policy uses the automatic threshold determination to automatically calculate the threshold values according to the network interface in-byte rate on previous days.

This policy relies on historical data. For accurate results, deploy the policy only after 4 weeks of data has been collected by the HP Performance Agent.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management** → ***<language>*** → **Virtualization Infrastructure** → **Performance** →
  VMware ESX
- **Infrastructure Management** → ***<language>*** → **Virtualization Infrastructure** → **Policies Grouped by Vendor** → **VMware ESX - Advanced**.

Metrics Used	BYLS_NET_IN_BYTE BYLS_NET_IN_PACKET
Supported Platform	VMware ESX or ESXi
Script-Parameter	**Description**
MessageApplication	Type an appropriate value that will help you identify the messages sent by the VI-VMwareNetifInbyteBaseline-AT policy to the management console.
DataSource	Displays the data source name as SCOPE.
DataObject	Displays the data object name as LOGICAL.
DataMetric	Displays the metric name as BYLS_NET_IN_BYTE.
UsePacketNumbers	Set the value to *true* if you want to monitor Net Out packet numbers in place of bytes for the following parameters. By default the value is set to false.
BaselinePeriod	Type the time period you want to define as a baseline period, such as '3600 seconds'. This period moves with the current time. The most recent 3600-second (1-hour) period becomes the current baseline period.
MinimumValue	Displays the minimum value of the in-byte rate as indicated by the metric.
MaximumValue	Displays the maximum value of the in-byte rate as indicated by the metric.
WarningDeviations	Displays the number of standard deviation away form normal, at which the policy sends a warning message to HPOM console. Set an appropriate value for the parameter. To disable the parameter, set value as *5*.
MinorDeviations	Displays the number of standard deviation away form normal, at

	which the policy sends a minor message to HPOM console. Set an appropriate value for the parameter greater than the specified value for *WarningDeviations*. To disable the parameter, set value as *5*.
MajorDeviations	Displays the number of standard deviation away form normal, at which the policy sends a major message to HPOM console. Set an appropriate value for the parameter greater than the specified value for *MinorDeviations*. To disable the parameter, set value as *5*.
MinorHighSeverity	If the *MinorDeviations* is violated above normal, the policy generates a minor high severity message.
MajorHighSeverity	If the *MajorDeviations* is violated above normal, the policy generates a major high severity message.
WarningLowSeverity	If the *WarningDeviations* is violated below normal, the policy generates a warning low severity message.
MinorLowSeverity	If the *MinorDeviations* is violated below normal, the policy generates a minor low severity message.
MajorLowSeverity	If the *MajorDeviations* is violated below normal, the policy generates a major low severity message.
InstanceSource	Do not rename the policy name. The policy uses its name to retrieve the source.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.
MessageGroup	Message group for outgoing messages.
HostNetifInbyteCutOff	Set the value below which you do not want to monitor the network interfaces on the host server.

The default polling interval for this policy is 30 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

After the values return within normal levels, the alert messages are automatically acknowledged.

Network Interface Out-Byte Rate Monitor Policy for VMware ESX or ESXi Servers

VI-VMwareNetifOutbyteBaseline-AT

The VI-VMwareNetifOutbyteBaseline-AT policy monitors the network interface out-byte or out-packet rate for a network interface in a given interval. It collectively monitors all instances of the outgoing bytes or packets on each network interface on the managed node. The policy uses

automatic threshold determination to automatically calculate the threshold values according to the network interface out-byte rate on previous days.

This policy relies on historical data. For accurate results, deploy the policy only after 4 weeks of data has been collected by the HP Performance Agent.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Performance → VMware ESX**.
- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor → VMware ESX - Advanced**.

Metrics Used	BYLS_NET_OUT_BYTE BYLS_NET_OUT_PACKET
Supported Platform	VMware ESX or ESXi
Script-Parameter	**Description**
MessageApplication	Type an appropriate value that will help you identify the messages sent by the VI-VMwareNetifOutbyteBaseline-AT policy to the management console.
DataSource	Displays the data source name as SCOPE.
DataObject	Displays the data object name as LOGICAL.
DataMetric	Displays the metric name as BYLS_NET_OUT_BYTE.
UsePacketNumbers	Set the value to `true` if you want to monitor Net Out packet numbers in place of bytes for the following parameters. By default the value is set to `false`.
BaselinePeriod	Type the time period you want to define as a baseline period, such as '3600 seconds'. This period moves with the current time. The most recent 3600-second (1-hour) period becomes the current baseline period.
MinimumValue	Displays the minimum value of the out-byte rate as indicated by the metric.
MaximumValue	Displays the maximum value of the out-byte rate as indicated by the metric.
WarningDeviations	Displays the number of standard deviation away form normal, at which the policy sends a warning message to HPOM console. Set an appropriate value for the parameter. To disable the parameter, set value as *5*.
MinorDeviations	Displays the number of standard deviation away form normal, at which the policy sends a minor message to HPOM console. Set

	an appropriate value for the parameter greater than the specified value for *WarningDeviations*. To disable the parameter, set value as *5*.
MajorDeviations	Displays the number of standard deviation away form normal, at which the policy sends a major message to HPOM console. Set an appropriate value for the parameter greater than the specified value for *MinorDeviations*. To disable the parameter, set value as *5*.
WarningHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
WarningLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
InstanceSource	Do not rename the policy name. The policy uses its name to retrieve the source.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.
MessageGroup	Message group for outgoing messages.
HostNetifOutbyteCutOff	Set the value below which you do not want to monitor the network interfaces on the host server.

The default polling interval for this policy is 30 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

After the values return within normal levels, the alert messages are automatically acknowledged.

Network Interface Card Monitor Policy for VMware ESX or ESXi Servers

VI-VMwareHostNICMonitor

The VI-VMwareHostNICMonitor policy monitors the performance of the Network Interface Cards installed on each ESX or ESXi server.

When the threshold values are reached or exceeded, the VI-VMwareHostNICMonitor policy sends an alert message to the HPOM console. The message severity can be major, minor, or warning depending upon the level of threshold violated.

Note: By default, critical alerts are masked. However, if you wish to receive critical alerts for this policy, open the policy and modify the values set in the *NICByteRateCriticalThreshold* and the *NICPktRateCriticalThreshold* script parameters depending on your requirements.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management** → <*language*> → **Virtualization Infrastructure** → **Performance** → **VMware ESX**
- **Infrastructure Management** → <*language*> → **Virtualization Infrastructure** → **Policies Grouped by Vendor** → **VMware ESX - Advanced**.

Metrics Used	BYNETIF_IN_BYTE_RATE BYNETIF_OUT_BYTE_RATE BYNETIF_IN_PACKET_RATE BYNETIF_OUT_PACKET_RATE BYNETIF_NAME BYNETIF_ID BYNETIF_NET_TYPE
Supported Platform	VMware ESX or ESXi
Script-Parameter	**Description**
NICByteRateMajorThreshold	If the average number of bytes transferred per second from the interface is more than the specified value, the policy generates an alert message with severity `Major`.
NICByteRateMinorThreshold	If the average number of bytes transferred per second from the interface is more than the specified value, the policy generates an alert message with severity `Minor`.

NICByteRateWarningThreshold	If the average number of bytes transferred per second from the interface is more than the specified value, the policy generates an alert message with severity `Warning`.
NICPktRateMajorThreshold	If the average number of packets transferred per second from this interface is more than the specified value, the policy generates an alert message with severity `Major`.
NICPktRateMinorThreshold	If the average number of packets transferred per second from this interface is more than the specified value, the policy generates an alert message with severity `Minor`.
NICPktRateWarningThreshold	If the average number of packets transferred per second from this interface is more than the specified value, the policy generates an alert message with severity `Warning`.
UsePktInfo	Set this variable if you want this policy to monitor the packet transmission rate.
MessageGroup	Message group for outgoing messages.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 5 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

Memory Performance Monitor Policy for VMware ESX or ESXi Servers

VI-VMwareVMMemoryPerformanceMonitor

The VI-VMwareVMMemoryPerformanceMonitor policy monitors the memory performance of the virtual machines. It compares the memory utilized by the virtual machine against the amount of virtual memory entitled to it.

The memory utilized by a virtual machine is calculated by taking the difference between the amount of actual memory used by the virtual machine (for running processes, applications, and services) and amount of memory held by the host operating system for ballooning. The ballooning technique is used by the host operating system to expand and contract the memory allocated to a guest virtual machine for controlling the overall memory usage by the guest virtual machines.

When the threshold values are reached or exceeded, the VI-VMwareVMMemoryPerformanceMonitor policy sends an alert message to the HPOM console. The message severity can be major, minor, or warning depending upon the level of threshold violated.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management** → ***<language>*** → **Virtualization Infrastructure** → **Performance** →
  VMware ESX.

- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor → VMware ESX - QuickStart**.

Metrics Used	BYLS_LS_ROLE BYLS_LS_UUID BYLS_MEM_SWAPOUT BYLS_MEM_USED BYLS_MEM_PHYS_UTIL BYLS_MEM_ENTL BYLS_MEM_BALLOON_UTIL BYLS_MEM_ENTL_MIN BYLS_MEM_ENTL_MAX BYLS_MEM_BALLOON_USED BYLS_LS_TYPE
Supported Platform	VMware ESX or ESXi
Script-Parameter	**Description**
VMSwapUtilMajorThreshold	If the swap utilization level for the virtual machines is more than the specified value, the policy generates an alert message with severity `Major`.
VMSwapUtilMinorThreshold	If the swap utilization level for the virtual machines is more than the specified value, the policy generates an alert message with severity `Minor`.
VMSwapUtilWarningThreshold	If the swap utilization level for the virtual machines is more than the specified value, the policy generates an alert message with severity `Warning`.
Debuglevel	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 5 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

Host Memory Health Monitor Policy for VMware ESX or ESXi Servers

VI-VMwareHostMemoryHealthMonitor

The VI-VMwareHostMemoryHealthMonitor policy monitors the health of the host machines on VMware ESX or ESXi servers in terms of memory utilization. It can be used to monitor the availability or utilization of the memory on the host machine.

When the threshold values are reached or exceeded, the policy sends an alert message to the HPOM console. The message severity can be major, minor, or warning depending upon the level of threshold violated.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Performance → VMware ESX**.
- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor → VMware ESX - Advanced**.

Metrics Used	BYLS_DISPLAY_NAME BYLS_LS_UUID BYLS_MEM_PHYS_UTIL BYLS_LS_ROLE BYLS_MEM_HEALTH BYLS_LS_HOSTNAME
Supported Platform	VMware ESX or ESXi
Script-Parameter	**Description**
UseMemoryHealthMetric	Displays a flag value of true or false indicating the use of metric `BYLS_MEM_HEALTH`. Set the value to `true` if you want to monitor the amount of memory available on the host machine. If set to `true`, the following parameters will be used to monitor the available memory on the host. If set to `false` the parameters will be used to monitor the percentage of memory used on the host.
HostMemHealthMajorThreshold	If the host memory utilization level for the virtual machines is more than the specified value, the policy generates an alert message with severity `Major`.
HostMemHealthMinorThreshold	If the host memory utilization level for the virtual machines is more than the specified value, the policy generates an alert message with severity `Minor`.
HostMemHealthWarningThreshold	If the host memory utilization level for the virtual machines is more than the specified value, the policy generates an alert message with severity `Warning`.

Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 5 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

Host Memory Utilization (by Virtual Machines) Monitor Policy for VMware ESX or ESXi Servers

VI-VMwareHostsMemoryUtilMonitor-AT

The VI-VMwareHostsMemoryUtilMonitor-AT policy calculates the total host memory utilization (including Service Console's memory utilization) by all active VMs under the host VMware ESX or ESXi servers.

The threshold values for this policy are automatically calculated based on the previous host memory utilization records.

When the threshold values are reached or exceeded, the policy sends an alert message to the HPOM console. The message severity can be major, minor, or warning depending upon the level of threshold violated.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management** → **<*language*>** → **Virtualization Infrastructure** → **Performance** → **VMware ESX**.
- **Infrastructure Management** → **<*language*>** → **Virtualization Infrastructure** → **Policies Grouped by Vendor** → **VMware ESX - Advanced**.

Metrics Used	BYLS_LS_ROLE BYLS_LS_HOSTNAME BYLS_MEM_PHYS_UTIL
Supported Platform	VMware ESX or ESXi
Script-Parameter	**Description**
MessageObject	Application for outgoing messages.
DataSource	Displays the data source name as SCOPE.
DataObject	Displays the data object name as LOGICAL.
DataMetric	Displays the metric name as BYLS_MEM_PHYS_UTIL.
BaselinePeriod	Type the time period you want to define as a baseline period, such as '3600 seconds'. This period moves with the current time. The most recent 3600-second (1-hour) period becomes the current baseline period.

MinimumValue	Displays the minimum value of host memory utilization as indicated by the metric.
MaximumValue	Displays the maximum value of host memory utilization as indicated by the metric.
WarningDeviations	Displays the number of standard deviation away form normal, at which the policy sends a warning message to HPOM console. Set an appropriate value for the parameter. To disable the parameter, set value as *5*.
MinorDeviations	Displays the number of standard deviation away form normal, at which the policy sends a minor message to HPOM console. Set an appropriate value for the parameter greater than the specified value for *WarningDeviations*. To disable the parameter, set value as *5*.
WarningHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
WarningLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as

	none.
MessageGroup	Message group for outgoing messages.
HostMemUtilCutOff	Set a value below which you do not want to monitor the memory utilization.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 30 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

After the values return within normal levels, the alert messages are automatically acknowledged.

Memory Utilization (by Virtual Machines) Monitor Policy for VMware ESX or ESXi Servers

VI-VMwareVMMemoryUtilMonitor

The VI-VMwareVMMemoryUtilMonitor policy monitors the memory utilization (in percentage) by all the active VMs on a VMware ESX or ESXi server.

When the threshold values are reached or exceeded, the policy sends an alert message to the HPOM console. The message severity can be major, minor, or warning depending upon the level of threshold violated.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Performance → VMware ESX**.
- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor → VMware ESX - Advanced.**

Metrics Used	BYLS_LS_UUID BYLS_LS_ROLE BYLS_LS_STATE BYLS_MEM_SWAPOUT BYLS_MEM_ENTL_MIN BYLS_MEM_ENTL_MAX BYLS_LS_HOST_HOSTNAME
Supported Platform	VMware ESX or ESXi
Script-Parameter	**Description**

VMSwapOutCriticalThreshold	If the memory swap out for a virtual machine is more than the critical threshold value, the policy generates an alert message with severity `Critical`.
VMSwapOutMajorThreshold	If the memory swap out for a virtual machine is more than the major threshold value, the policy generates an alert message with severity `Major`.
VMSwapOutMinorThreshold	If the memory swap out for a virtual machine is more than the minor threshold value, the policy generates an alert message with severity `Minor`.
VMSwapOutWarningThreshold	If the memory swap out for a virtual machine is more than the warning threshold value, the policy generates an alert message with severity `Warning`.
VMMemUtilCriticalThreshold	If the memory utilization percent for a virtual machine is more than the critical threshold value, the policy generates an alert message with severity `Critical`.
VMMemUtilMajorThreshold	If the memory utilization percent for a virtual machine is more than the major threshold value, the policy generates an alert message with severity `Major`.
VMMemUtilMinorThreshold	If the memory utilization percent is for a virtual machine is more than the minor threshold value, the policy generates an alert message with severity `Minor`.
VMMemUtilWarningThreshold	If the memory utilization percent for a virtual machine is more than the warning threshold value, the policy generates an alert message with severity `Warning`.
MessageGroup	Message group for outgoing messages.
MessageApplication	Application for outgoing messages.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 5 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

Memory Utilization Monitor policy for VMware vCenter

VI-VMwareVCHostMemUtilMonitor

The VI-VMwareVCHostMemUtilMonitor policy monitors the memory pressure utilization of ESX/ESXi hosts.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Performance → VMware vCenter**.
- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor → VMware vCenter - Advanced.**

Metrics Used	• SystemID • SystemRole • SystemState • SystemName • MemPhysUtil • MemOverallHealth • MemPhys
Supported Platforms	VMware vCenter

Script-Parameter	Description
HostMemUtilCriticalThreshold	If the memory utilization for a Host Esx/i is more than the critical threshold value, the policy generates an alert message with severity `Critical`.
HostMemUtilMajorThreshold	If the memory utilization for a Host Esx/i is more than the major threshold value, the policy generates an alert message with severity `Major`.
HostMemUtilMinorThreshold	If the memory utilization for a Host Esx/i is more than the minor threshold value, the policy generates an alert message with severity `Minor`.
HostMemUtilWarningThreshold	If the memory utilization for a Host Esx/i is more than the warning threshold value, the policy generates an alert message with severity `Warning`.
VMMemSwapUtilThreshold	If the swap utilization for a virtual machine as indicated by the metric is more than the threshold value, the policy generates an alert message.
VMMemBalloonUtilThreshold	If the balloon utilization for a virtual machine as indicated by the metric is more than the threshold value, the policy generates an alert message.
MemOverCommitmentThreshold	If the memory over commitment for a host that is the memory allocated on virtual machines is greater than the actual physical memory available on the host machine, the policy generates an alert message.
High-MemS-wapUtilVMCountPercentThreshold	If the percentage of virtual machines with high swap utilization in a host is more than the threshold value, the policy generates an alert message.

High-Mem-BalloonUtilVMCountPercentThreshold	If the percentage of virtual machines with high balloon utilization in a host is more than the threshold value, the policy generates an alert message.
BalloonUtilAndSwapUtilCheck	Set the value to `true` to monitor the swap utilization and balloon utilization of each virtual machine in the host else set to `false` to monitor the memory utilization. By default the value is set to false.
MessageGroup	Message group for outgoing messages.
MessageApplication	Application for outgoing messages.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 5 minutes. You can modify the polling interval based on your requirements.

Total Memory Utilization (by Virtual Machines) Monitor Policy for VMware ESX or ESXi Servers

VI-VMwareTotalVMMemoryUtilMonitor

The VI-VMwareTotalVMMemoryUtilMonitor policy monitors the total memory utilization (in percentage) by all the active VMs on a VMware ESX or ESXi server.

When the threshold values are reached or exceeded, the policy sends an alert message to the HPOM console. The message severity can be major, minor, or warning depending upon the level of threshold violated.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management →*<language>*→ Virtualization Infrastructure → Performance →**
  VMware ESX.
- **Infrastructure Management →*<language>*→ Virtualization Infrastructure → Policies Grouped by Vendor → VMware ESX - Advanced.**

Metrics Used	BYLS_LS_PARENT_UUID BYLS_MEM_PHYS_UTIL BYLS_DISPLAY_NAME BYLS_LS_ROLE BYLS_LS_UUID

	BYLS_LS_NAME BYLS_LS_HOSTNAME BYLS_LS_STATE
Supported Platform	VMware ESX or ESXi
Script-Parameter	**Description**
MessageGroup	Message group for outgoing messages.
MemUtilMajorThreshold	If the total memory utilization percent is more than the specified threshold value, the policy generates an alert message with severity `Major`.
MemUtilMinorThreshold	If the total memory utilization percent is more than the specified threshold value, the policy generates an alert message with severity `Minor`.
MemUtilWarningThreshold	If the total memory utilization percent is more than the specified threshold value, the policy generates an alert message with severity `Warning`.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 5 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

Frame Memory Utilization Monitor Policy for IBM LPAR

VI-IBMLPARFrameMemoryUtilMonitor

The VI-IBMLPARFrameMemoryUtilMonitor policy monitors the memory utilization of the IBM AIX frames and alerts on any abnormal growth in physical memory utilization of AIX frames.

When the threshold values are reached or exceeded, the policy sends an alert message to the HPOM console. The message severity can be major, minor, or warning depending upon the level of threshold violated. The alert message contains the following information:

- Names of the LPARs in the frame.
- The amount of memory assigned to the LPAR (in megabytes.)
- The amount of memory used by the LPAR (in megabytes.)
- The percentage of memory utilized by the LPAR with respect to the frame.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management** → ***<language>*** → **Virtualization Infrastructure** → **Performance** →
  IBM LPAR.

- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor → IBM LPAR- QuickStart**.

Metrics Used	BYLS_MEM_ENTL_UTIL BYLS_MEM_ENTL GBL_LS_TYPE GBL_SYSTEM_ID BYLS_DISPLAY_NAME BYLS_LS_TYPE BYLS_LS_NAME
Supported Platform	IBM AIX Frames

Script-Parameter	Description
MessageGroup	Message group for outgoing messages.
MemUtilMajorThreshold	If the memory utilization is more than the specified threshold value, the policy generates an alert message with severity `Major`.
MemUtilMinorThreshold	If the memory utilization is more than the specified threshold value, the policy generates an alert message with severity `Minor`.
MemUtilWarningThreshold	If the memory utilization is more than the specified threshold value, the policy generates an alert message with severity `Warning`.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 5 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

Physical Memory Utilization Monitor Policy for Oracle Solaris Zones

VI-OracleSolarisHostMemoryUtilMonitor

The VI-OracleSolarisHostMemoryUtilMonitor policy monitors the memory utilization on Solaris zones. When the threshold values are reached or exceeded, the policy sends an alert message to the HPOM console. The message severity can be major, minor, or warning depending upon the level of threshold violated.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Performance → Oracle Containers**.
- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor → Oracle Containers- QuickStart**.

Metrics Used	GBL_MEM_UTIL GBL_MEM_FREE BYLS_MEM_ENTL_UTIL BYLS_MEM_ENTL BYLS_DISPLAY_NAME
Supported Platform	Oracle Solaris Zones
Script-Parameter	**Description**
MessageGroup	Message group for outgoing messages.
MemUtilMajorThreshold	If the memory utilization is more than the specified threshold value and the free memory available (in megabytes) is less than the specified threshold value, the policy generates an alert message with severity `Major`.
FreeMemAvailMajorThreshold	
MemUtilMinorThreshold	If the memory utilization is more than the specified threshold value and the free memory available (in megabytes) is less than the specified threshold value, the policy generates an alert message with severity `Minor`.
FreeMemAvailMinorThreshold	
MemUtilWarningThreshold	If the memory utilization is more than the specified threshold value and the free memory available (in megabytes) is less than the specified threshold value, the policy generates an alert message with severity `Warning`.
FreeMemAvailWarningThreshold	
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 5 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

Swap Utilization Monitor Policy for Oracle Solaris Zones

VI-OracleSolarisZoneSwapUtilMonitor-AT

The VI-OracleSolarisZoneSwapUtilMonitor policy monitors the swap utilization on Solaris zones. When the threshold values are reached or exceeded, the policy sends an alert message to the

HPOM console. The message severity can be major, minor, or warning depending upon the level of threshold violated.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → <*language*> → Virtualization Infrastructure → Performance → Oracle Containers**.
- **Infrastructure Management → <*language*> → Virtualization Infrastructure → Policies Grouped by Vendor → Oracle Containers- Advanced**.

Metrics Used	BYLS_LS_NAME BYLS_MEM_SWAP_UTIL
Supported Platform	Oracle Solaris Zones
Script-Parameter	**Description**
MessageObject	Application for outgoing messages.
DataSource	Displays the data source name as SCOPE.
DataObject	Displays the data object name as LOGICAL.
DataMetric	Displays the metric name as BYLS_MEM_SWAP_UTIL.
BaselinePeriod	Type the time period you want to define as a baseline period, such as '3600 seconds'. This period moves with the current time. The most recent 3600-second (1-hour) period becomes the current baseline period.
MinimumValue	Displays the minimum value of the swap utilization as indicated by the metric.
MaximumValue	Displays the maximum value of the swap utilization as indicated by the metric.
WarningDeviations	Displays the number of standard deviation away form normal, at which the policy sends a warning message to HPOM console. Set an appropriate value for the parameter. To disable the parameter, set value as *5*.
MinorDeviations	Displays the number of standard deviation away form normal, at which the policy sends a minor message to HPOM console. Set an appropriate value for the parameter greater than the specified value for *WarningDeviations*. To disable the parameter, set value as *5*.
MajorDeviations	Displays the number of standard deviation away form normal, at which the policy sends a major message to HPOM console. Set an appropriate value for the parameter greater than the specified value for *MinorDeviations*. To disable the parameter, set value as *5*.

WarningHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
WarningLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
MessageGroup	Message group for outgoing messages.
SwapUtilCutOff	Set a value below which you do not want to monitor CPU utilization.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 30 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

After the values return within normal levels, the alert messages are automatically acknowledged.

Data Collector Policy for VMware Datacenter

VI-VMwareDCDataCollector

The VI-VMwareDCDataCollector policy collects data about the CPU, memory, and datastore performance data for the VMware datacenters and logs it in CODA.

Metrics Logged in CODA	VMWARE_VC_NAME VMWARE_DC_NAME VMWARE_DC_CPU_UTIL VMWARE_DC_CPU_USED VMWARE_DC_CPU_TOTAL VMWARE_DC_MEMORY_UTIL VMWARE_DC_MEMORY_USED VMWARE_DC_MEMORY_TOTAL VMWARE_DC_DATASTORE_UTIL VMWARE_DC_DATASTORE_FREE VMWARE_DC_DATASTORE_TOTAL
Supported Platform	VMware ESX or ESXi

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management** → ***<language>*** → **Virtualization Infrastructure** → **Performance** →
  VMware ESX.
- **Infrastructure Management** → ***<language>*** → **Virtualization Infrastructure** → **Policies Grouped by Vendor** → **VMware ESX- QuickStart**.

The VI-VMwareDCCPUUtilMonitor policy, VI-VMwareDCMemoryUtilMonitor policy, and the VI-VMwareDCDataStoreUtilMonitor policies alert based on the data collected and logged by the VI-VMwareDCDataCollector policy.

The default polling interval of this policy is 30 minutes. If your environment has a large number of monitored instances, to collect data accurately, increase the policy's polling interval to an appropriate value.

CPU Utilization Monitor Policy for VMware Datacenter

VI-VMwareDCCPUUtilMonitor

Note: You must deploy this policy **30 minutes** after deploying the VI-VMwareDCDataCollector policy because this policy depends on the data collected by VI-VMwareDCDataCollector (see "Hardware Data Collector Policy for VMware Datacenter" on page 57.)

The VI-VMwareDCCPUUtilMonitor policy monitors the aggregate CPU utilization at the VMware datacenter level. Based on the data logged in CODA by the VI-VMwareDCDataCollector policy, the VI-VMwareDCCPUUtilMonitor policy sends alert messages to the HPOM console.

Metrics Used	VMWARE_DC_CPU_UTIL VMWARE_DC_NAME VMWARE_VC_NAME
Supported Platform	VMware ESX or ESXi
Script-Parameter	**Description**
DCCPUUtilMajorThreshold	If the CPU utilization at the datacenter level is more than the specified threshold value, the policy generates an alert message with severity `Major`.
DCCPUUtilMinorThreshold	If the CPU utilization at the datacenter level is more than the specified threshold value, the policy generates an alert message with severity `Minor`.
DCCPUUtilWarningThreshold	If the CPU utilization at the datacenter level is more than the specified threshold value, the policy generates an alert message with severity `Warning`.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Performance → VMware ESX**.
- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor → VMware ESX- Advanced**.

The default polling interval for this policy is 5 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

Memory Utilization Monitor Policy for VMware Datacenter

VI-VMwareDCMemoryUtilMonitor

Note: You must deploy this policy **30 minutes** after deploying the VI-VMwareDCDataCollector policy because this policy depends on the data collected by VI-VMwareDCDataCollector (see "Hardware Data Collector Policy for VMware Datacenter" on page 57.)

The VI-VMwareDCMemoryUtilMonitor policy monitors the aggregate memory utilization at the VMware datacenter level. Based on the data logged in CODA by the VI-VMwareDCDataCollector policy, the VI-VMwareDCMemoryUtilMonitor policy sends alert messages to the HPOM console.

Metrics Used	VMWARE_DC_MEMORY_UTIL VMWARE_DC_NAME VMWARE_VC_NAME
Supported Platform	VMware ESX or ESXi
Script-Parameter	**Description**
DCMemoryUtilMajorThreshold	If the memory utilization at the datacenter level is more than the specified threshold value, the policy generates an alert message with severity `Major`.
DCMemoryUtilMinorThreshold	If the memory utilization at the datacenter level is more than the specified threshold value, the policy generates an alert message with severity `Minor`.
DCMemoryUtilWarningThreshold	If the memory utilization at the datacenter level is more than the specified threshold value, the policy generates an alert message with severity `Warning`.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Performance → VMware ESX**.
- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor → VMware ESX- Advanced**.

The default polling interval for this policy is 5 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

Datastore Utilization Monitor Policy for VMware Datacenter

VI-VMwareDCDataStoreUtilMonitor

Note: You must deploy this policy **30 minutes** after deploying the VI-VMwareDCDataCollector policy because this policy depends on the data collected by VI-VMwareDCDataCollector (see "Hardware Data Collector Policy for VMware Datacenter" on page 57.)

The VI-VMwareDCDataStoreUtilMonitor policy monitors the aggregate data store (disk space) utilization at the VMware datacenter level. Based on the data logged in CODA by the VI-VMwareDCDataCollector policy, the VI-VMwareDCDataStoreUtilMonitor policy sends alert messages to the HPOM console.

Metrics Used	VMWARE_VC_NAME VMWARE_DC_NAME VMWARE_DC_DATASTORE_UTIL
Supported Platform	VMware ESX or ESXi
Script-Parameter	**Description**
DCDataStoreUtilMajorThreshold	If the datastore (disk space) utilization at the datacenter level is more than the specified threshold value, the policy generates an alert message with severity `Major`.
DCDataStoreUtilMinorThreshold	If the datastore (disk space) utilization at the datacenter level is more than the specified threshold value, the policy generates an alert message with severity `Minor`.
DCDataStoreUtilWarningThreshold	If the datastore (disk space) utilization at the datacenter level is more than the specified threshold value, the policy generates an alert message with severity `Warning`.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management** → ***<language>*** → **Virtualization Infrastructure** → **Performance** → **VMware ESX**.
- **Infrastructure Management** → ***<language>*** → **Virtualization Infrastructure** → **Policies Grouped by Vendor** → **VMware ESX- Advanced**.

The default polling interval for this policy is 5 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

Datastore SpaceUtilization Monitor Policy for VMware vCenter

VI-VMwareVCDatastoreSpaceUtilizationMonitor

The VI-VMwareVCDatastoreSpaceUtilizationMonitor policy monitors the space utilization of each VMware datastore.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Performance → VMware vCenter**.
- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor → VMware vCenter- Advanced**.

Metrics Used	AvailableSpace Capacity Name ID
Supported Platform	VMware vCenter
Script-Parameter	**Description**
DatastoreUtilCriticalThreshold	If the datastore (disk space) utilization is more than the specified threshold value, the policy generates an alert message with severity `Critical`.
DatastoreUtilMajorThreshold	If the datastore (disk space) utilization is more than the specified threshold value, the policy generates an alert message with severity `Major`.
DataStoreUtilMinorThreshold	If the datastore (disk space) utilization is more than the specified threshold value, the policy generates an alert message with severity `Minor`.
DataStoreUtilWarningThreshold	If the datastore (disk space) utilization is more than the specified threshold value, the policy generates an alert message with severity `Warning`.
MessageGroup	Message group for outgoing messages.
MessageApplication	Application for outgoing messages.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 5 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

VMFS Utilization Data Collector Policy for VMware ESX or ESXi Servers

VI-VMwareVMFSDataCollector

The VI-VMwareVMFSDataCollector policy collects data about the disk space utilization, LUN latency, and disk throughput on the Virtual Machine File System (VMFS) and logs it in CODA.

VMFS represents the data storage volumes on which the VMware guest disk files are stored.

The policy uses APIs provided by VMware to retrieve the following information:

- Storage device connected to a particular host
- HBA Device number
- Host name
- UUID of the host
- Location of the host
- File system
- Space utilization
- Maximum capacity
- Available space
- Used percent
- Total read latency
- Total write latency
- Device read latency
- Device write latency
- Kernel read latency
- Kernel write latency
- Number of commands issued
- Number of commands aborted
- Number of bus resets
- Read throughput
- Write throughput

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management** → ***<language>*** → **Virtualization Infrastructure** → **Performance** → **VMware ESX**.
- **Infrastructure Management** →***<language>*** → **Virtualization Infrastructure** → **Policies Grouped by Vendor** → **VMware ESX - QuickStart**.

The default logging interval for this policy is 30 minutes. If your environment has a large number of monitored instances, to collect data accurately, increase the policy's polling interval to an appropriate value.

VMFS Read Latency Monitor Policy for VMware ESX or ESXi Servers

VI-VMFSReadLatencyMonitor

Note: You must deploy this policy **30 minutes** after deploying the VI-VMwareVMFSDataCollector policy because this policy depends on the data collected by VI-VMwareVMFSDataCollector (see "VMFS Utilization Data Collector Policy for VMware ESX or ESXi Servers" on page 128.)

The VI-VMFSReadLatencyMonitor policy monitors the following:

- VMFS read latency
- VMFS device read latency
- VMFS kernel read latency

Based on the data logged in CODA by the VI-VMwareVMFSDataCollector policy (see "VMFS Utilization Data Collector Policy for VMware ESX or ESXi Servers" on page 128), the VI-VMFSReadLatencyMonitor policy sends alert messages to the HPOM console.

Supported Platform	VMware ESX or ESXi
Script-Parameter	**Description**
ReadLatencyMajorThreshold	If the read latency is more than the specified threshold value, the policy generates an alert message with severity `Major`.
ReadLatencyMinorThreshold	If the read latency is more than the specified threshold value, the policy generates an alert message with severity `Minor`.
ReadLatencyWarningThreshold	If the read latency is more than the specified threshold value, the policy generates an alert message with severity `Warning`.
AssignMessageToRemoteHost	Set the value to **1** to display the source of the alert message as the remote host. By default, the messages are assigned to the managed node from which the message is sent out.
MessageGroup	Message group for outgoing messages.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management** → ***<language>*** → **Virtualization Infrastructure** → **Performance** → **VMware ESX**.
- **Infrastructure Management** → ***<language>*** → **Virtualization Infrastructure** → **Policies Grouped by Vendor** → **VMware ESX- Advanced**.

The default polling interval for this policy is 5 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

VMFS Write Latency Monitor Policy for VMware ESX or ESXi Servers

VI-VMFSWriteLatencyMonitor

Note: You must deploy this policy **30 minutes** after deploying the VI-VMwareVMFSDataCollector policy because this policy depends on the data collected by VI-VMwareVMFSDataCollector (see "VMFS Utilization Data Collector Policy for VMware ESX or ESXi Servers" on page 128.)

The VI-VMFSWriteLatencyMonitor policy monitors the following:

- VMFS write latency
- VMFS device write latency
- VMFS kernel write latency

Based on the data logged in CODA by the VI-VMwareVMFSDataCollector policy (see "VMFS Utilization Data Collector Policy for VMware ESX or ESXi Servers" on page 128), the VI-VMFSWriteLatencyMonitor policy sends alert messages to the HPOM console.

Supported Platform	VMware ESX or ESXi
Script-Parameter	**Description**
WriteLatencyMajorThreshold	If the write latency is more than the specified threshold value, the policy generates an alert message with severity `Major`.
WriteLatencyMinorThreshold	If the write latency is more than the specified threshold value, the policy generates an alert message with severity `Minor`.
WriteLatencyWarningThreshold	If the write latency is more than the specified threshold value, the policy generates an alert message with severity `Warning`.
AssignMessageToRemoteHost	Set the value to **1** to display the source of the alert message as the remote host. By default the messages are assigned to the managed node from which the message is sent out.
MessageGroup	Message group for outgoing messages.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Performance → VMware ESX**.
- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor → VMware ESX- Advanced**.

The default polling interval for this policy is 5 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

Guest Latency Monitor Policy for VMware vCenter

VI-VMwareVCGuestLatencyMonitor

The VI-VMwareVCGuestLatencyMonitor policy monitors the latency of guest systems (virtual machines). Latency of a virtual machine leads to performance problems.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Performance → VMware vCenter**.
- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor → VMware vCenter- Advanced**.

Metrics Used	• SystemID • SystemRole • SystemState • SystemName • DiskWriteLatency • DiskReadLatency • SystemHostHostName
Supported Platforms	VMware vCenter

Script-Parameter	Description
DiskReadLatencyCriticalThreshold	If the disk read latency for a guest is more than the specified threshold value, the policy generates an alert message with severity `Critical`.
DiskReadLatencyMajorThreshold	If the disk read latency for a guest is more than the specified threshold value, the policy generates an alert message with severity `Major`.
DiskReadLatencyMinorThreshold	If the disk read latency for a guest is more than the specified threshold value, the policy generates an alert message with severity `Minor`.

DiskReadLatencyWarningThreshold	If the disk read latency for a guest is more than the specified threshold value, the policy generates an alert message with severity `Warning`.
DiskWriteLatencyCriticalThreshold	If the disk write latency for a guest is more than the specified threshold value, the policy generates an alert message with severity `Critical`.
DiskWriteLatencyMajorThreshold	If the disk write latency for a guest is more than the specified threshold value, the policy generates an alert message with severity `Major`.
DiskWriteLatencyMinorThreshold	If the disk write latency for a guest is more than the specified threshold value, the policy generates an alert message with severity `Minor`.
DiskWriteLatencyWarningThreshold	If the disk write latency for a guest is more than the specified threshold value, the policy generates an alert message with severity `Warning`.
MessageGroup	Message group for outgoing messages.
MessageApplication	Application for outgoing messages.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 5 minutes. You can modify the polling interval based on your requirements.

Disk Error Monitor Policy for VMware ESX or ESXi Servers

VI-VMwareDiskErrorMonitor

Note: You must deploy this policy **30 minutes** after deploying the VI-VMwareVMFSDataCollector policy because this policy depends on the data collected by VI-VMwareVMFSDataCollector (see "VMFS Utilization Data Collector Policy for VMware ESX or ESXi Servers" on page 128.)

The VI-VMwareDiskErrorMonitor policy monitors the number of disk bus resets and number of disk commands that quit. Based on the data logged in CODA by the VI-VMwareVMFSDataCollector policy (see "VMFS Utilization Data Collector Policy for VMware ESX or ESXi Servers" on page 128), the VI-VMwareDiskErrorMonitor policy sends alert messages to the HPOM console.

Supported Platform	VMware ESX or ESXi
Script-Parameter	**Description**

DiskBusResetMajorThreshold	If the number of disk bus resets is more than the specified threshold value, the policy generates an alert message with severity `Major`.
DiskBusResetMinorThreshold	If the number of disk bus resets is more than the specified threshold value, the policy generates an alert message with severity `Minor`.
DiskBusResetWarningThreshold	If the number of disk bus resets is more than the specified threshold value, the policy generates an alert message with severity `Warning`.
DiskCommandsAbortedMajorThreshold	If the number of disk commands that quit is more than the specified threshold value, the policy generates an alert message with severity `Major`.
DiskCommandsAbortedMinorThreshold	If the number of disk commands that quit is more than the specified threshold value, the policy generates an alert message with severity `Minor`.
DiskCommandsAbortedWarningThreshold	If the disk commands that quit is more than the specified threshold value, the policy generates an alert message with severity `Warning`.
AssignMessageToRemoteHost	Set the value to **1** to display the source of the alert message as the remote host. By default the messages are assigned to the managed node from which the message is sent out.
MessageGroup	Message group for outgoing messages.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Performance → VMware ESX**.
- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor → VMware ESX- Advanced**.

The default polling interval for this policy is 5 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

Disk Throughput Monitor Policy for VMware ESX or ESXi Servers

VI-VMwareDiskThroughput Monitor

Note: You must deploy this policy **30 minutes** after deploying the VI-VMwareVMFSDataCollector policy because this policy depends on the data collected by VI-VMwareVMFSDataCollector (see "VMFS Utilization Data Collector Policy for VMware ESX or ESXi Servers" on page 128.)

The VI-VMwareDiskThroughputMonitor policy monitors the disk read throughput rate and the disk write throughput rate.

Based on the data logged in CODA by the VI-VMwareVMFSDataCollector policy (see "VMFS Utilization Data Collector Policy for VMware ESX or ESXi Servers" on page 128), the VI-VMwareDiskThroughputMonitor policy sends alert messages to the HPOM console.

Supported Platform	VMware ESX or ESXi
Script-Parameter	**Description**
DiskReadThroughputMajorThreshold	If the read throughput rate of the disk is more than the specified threshold value, the policy generates an alert message with severity `Major`.
DiskReadThroughputMinorThreshold	If the read throughput rate of the disk is more than the specified threshold value, the policy generates an alert message with severity `Minor`.
DiskReadThroughputWarningThreshold	If the read throughput rate of the disk is more than the specified threshold value, the policy generates an alert message with severity `Warning`.
DiskWriteThroughputMajorThreshold	If the write throughput rate of the disk is more than the specified threshold value, the policy generates an alert message with severity `Major`.
DiskWriteThroughputMinorThreshold	If the write throughput rate of the disk is more than the specified threshold value, the policy generates an alert message with severity `Minor`.
DiskWriteThroughputWarningThreshold	If the write throughput rate of the disk is more than the specified threshold value, the policy generates an alert message with severity `Warning`.
AssignMessageToRemoteHost	Set the value to **1** to display the source of the alert message as the remote host. By default the messages are assigned to the managed node from which the message is sent out.
MessageGroup	Message group for outgoing messages.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management** → ***<language>*** → **Virtualization Infrastructure** → **Performance** → **VMware ESX**.
- **Infrastructure Management** → ***<language>*** → **Virtualization Infrastructure** → **Policies Grouped by Vendor** → **VMware ESX- Advanced**.

The default polling interval for this policy is 5 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

Vifp Target Check Policy for VMware ESX or ESXi Servers

VI-VMwareVifpTargetCheck

The VI-VMwareVifpTargetCheck policy monitors the connectivity of VMware vMA target servers on the managed node by using vifp commands. Based on the connectivity issue, the policy sends alert messages to the HPOM console.

Supported Platform	VMware ESX or ESXi
Script-Parameter	**Description**
MessageGroup	Message group for outgoing messages.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

In the console tree, the policy is listed at the following location:

- **Infrastructure Management** → ***<language>*** → **Virtualization Infrastructure** → **Policies Grouped by Vendor** → **VMware ESX- QuickStart**.

The default polling interval for this policy is 15 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

Host CPU Utilization Monitor Policy for KVM or Xen

VI-LinuxVirtHostCPUUtilMonitor

The VI-LinuxVirtHostCPUUtilMonitor policy monitors the CPUs on the host servers (managed nodes) for KVM or Xen and sends an alert message in case the performance goes below the set threshold.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management** → ***<language>*** → **Virtualization Infrastructure** → **Performance** → **LinuxVirt**.

- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor → LinuxVirt - QuickStart**.

The VI-LinuxVirtHostCPUUtilMonitor policy provides information about the following:

- Host level CPU utilization
- VMs utilizing the maximum CPU (in descending order)

Metrics Used	GBL_CPU_TOTAL_UTIL GBL_SYSTEM_ID GBL_LS_TYPE
Supported Platform	KVM or Xen

Script-Parameter	Description
MessageGroup	Message group for outgoing messages.
CPUUtilCriticalThreshold	If the CPU utilization on the host machine is more than the critical threshold value, the policy generates an alert message with severity `Critical`.
CPUUtilMajorThreshold	If the CPU utilization on the host machine is more than the major threshold value, the policy generates an alert message with severity `Major`.
CPUUtilMinorThreshold	If the CPU utilization on the host machine is more than the minor threshold value, the policy generates an alert message with severity `Minor`.
CPUUtilWarningThreshold	If the CPU utilization on the host machine is more than the warning threshold value, the policy generates an alert message with severity `Warning`.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The alert messages are generated based on the values of the script parameters mentioned in the above table. The alert messages are automatically acknowledged when the values of host CPU utilization reach normal.

The default polling interval for this policy is 5 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

Guest CPU Utilization Monitor Policy for KVM or Xen

VI-LinuxVirtGuestCPUUtilMonitor

The VI-LinuxVirtGuestCPUUtilMonitor policy monitors the CPUs on the guest servers (managed nodes) for KVM or Xen and sends an alert message in case the performance goes below the set threshold.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → <*language*> → Virtualization Infrastructure → Performance → LinuxVirt**.
- **Infrastructure Management → <*language*> → Virtualization Infrastructure → Policies Grouped by Vendor → LinuxVirt - QuickStart**.

The VI-LinuxVirtGuestCPUUtilMonitor policy provides information about the following:

- Host level CPU utilization
- VMs utilizing the maximum CPU (in descending order)

Metrics Used	BYLS_LS_ROLE BYLS_CPU_TOTAL_UTIL BYLS_DISPLAY_NAME BYLS_LS_UUID BYLS_LS_STATE BYLS_LS_HOST_HOSTNAME
Supported Platform	KVM or Xen
Script-Parameter	**Description**
VMCPUUtilMajorThreshold	If the CPU utilization on the host machine is more than the major threshold value, the policy generates an alert message with severity `Major`.
VMCPUUtilMinorThreshold	If the CPU utilization on the host machine is more than the minor threshold value, the policy generates an alert message with severity `Minor`.
VMCPUUtilWarningThreshold	If the CPU utilization on the host machine is more than the warning threshold value, the policy generates an alert message with severity `Warning`.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The alert messages are generated based on the values of the script parameters mentioned in the above table. The alert messages are automatically acknowledged when the values of guest CPU utilization reach normal.

The default polling interval for this policy is 5 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

Physical Disk Byte Rate Baseline Policy for KVM or Xen

VI-LinuxVirtDiskPhysByteRateBaseline-AT

The VI-LinuxVirtDiskPhysByteRateBaseline-AT policy uses an instance baseline for monitoring the average number of bytes transferred per second from and to the physical disk for KVM or Xen and sends an alert message in case the performance goes below the set threshold.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → <*language*> → Virtualization Infrastructure → Performance → LinuxVirt**.
- **Infrastructure Management → <*language*> → Virtualization Infrastructure → Policies Grouped by Vendor → LinuxVirt - Advanced**.

Metrics Used	BYLS_DISK_PHYS_BYTE_RATE BYLS_LS_ROLE BYLS_LS_NAME BYLS_LS_UUID BYLS_DISPLAY_NAME
Supported Platform	KVM or Xen
Script-Parameter	**Description**
MessageApplication	Application for incoming messages.
DataSource	Displays the data source name as SCOPE.
DataObject	Displays the data object name as LOGICAL.
DataMetric	Displays the metric name as BYLS_DISK_PHYS_ BYTE_RATE.
UsePacketNumbers	Monitors the net packet numbers when set to TRUE.
BaselinePeriod	Type the time period you want to define as a baseline period, such as '3600 seconds'. This period moves with the current time. The most recent 3600-second (1-hour) period becomes the current baseline period.
MinimumValue	Displays the minimum value of bytes transferred as indicated by the metric.
MaximumValue	Displays the maximum value of bytes transferred as indicated by the metric.
WarningDeviations	Displays the number of standard deviation away form normal, at which the policy sends a warning message to HPOM console. Set an appropriate value for the parameter. To disable the parameter, set value as *5*.
MinorDeviations	Displays the number of standard deviation away form normal, at which the policy sends a minor message to HPOM console. Set an appropriate value for the

	parameter greater than the specified value for *WarningDeviations*. To disable the parameter, set value as *5*.
MajorDeviations	Displays the number of standard deviation away form normal, at which the policy sends a major message to HPOM console. Set an appropriate value for the parameter greater than the specified value for *MinorDeviations*. To disable the parameter, set value as *5*.
WarningHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
WarningLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
InstanceSource	Do not rename the policy name. The policy uses its name to retrieve the source.
DebugLevel	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log

	the messages in the trace file on the managed node.
MessageGroup	Message group for outgoing messages.
DiskPhysbyteCutOff	Set a Putbyte rate value below DiskPhysbyteCutOff which you do not want to monitor.

The default polling interval for this policy is 30 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

After the values return within normal levels, the alert messages are automatically acknowledged.

Net Byte Rate Baseline Policy for KVM or Xen

VI-LinuxVirtNetByteRateBaseline-AT

The VI-LinuxVirtNetByteRateBaseline-AT policy uses instance baseline for monitoring the net byte rate for KVM or Xen and sends an alert message in case the performance goes below the set threshold.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → <*language*>→ Virtualization Infrastructure → Performance → LinuxVirt**.
- **Infrastructure Management → <*language*> → Virtualization Infrastructure → Policies Grouped by Vendor → LinuxVirt - Advanced**.

Metrics Used	BYLS_NET_BYTE_RATE BYLS_LS_ROLE BYLS_DISPLAY_NAME BYLS_LS_UUID
Supported Platform	KVM or Xen
Script-Parameter	**Description**
MessageApplication	Application for incoming messages.
DataSource	Displays the data source name as SCOPE.
DataObject	Displays the data object name as LOGICAL.
DataMetric	Displays the metric name as BYLS_NET_BYTE_ RATE.
UsePacketNumbers	Monitors the net packet numbers when set to TRUE.
BaselinePeriod	Type the time period you want to define as a baseline period, such as '3600 seconds'. This period moves with the current time. The most recent 3600-second (1-hour)

	period becomes the current baseline period.
MinimumValue	Displays the minimum value of the net byte rate as indicated by the metric.
MaximumValue	Displays the maximum value of the net byte rate as indicated by the metric.
WarningDeviations	Displays the number of standard deviation away form normal, at which the policy sends a warning message to HPOM console. Set an appropriate value for the parameter. To disable the parameter, set value as *5*.
MinorDeviations	Displays the number of standard deviation away form normal, at which the policy sends a minor message to HPOM console. Set an appropriate value for the parameter greater than the specified value for *WarningDeviations*. To disable the parameter, set value as *5*.
MajorDeviations	Displays the number of standard deviation away form normal, at which the policy sends a major message to HPOM console. Set an appropriate value for the parameter greater than the specified value for *MinorDeviations*. To disable the parameter, set value as *5*.
WarningHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
WarningLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorLowSeverity	Displays the severity of the alert messages to be sent to

	HPOM console in case the current data meets or falls below the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
InstanceSource	Do not rename the policy name. The policy uses its name to retrieve the source.
DebugLevel	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.
MessageGroup	Message group for outgoing messages.
NetbyteRateCutOff	Set a `Putbyte` rate value below `NetbyteRateCutOff` which you do not want to monitor.

The default polling interval for this policy is 30 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

After the values return within normal levels, the alert messages are automatically acknowledged.

Guest Total CPU Utilization Monitor Policy for KVM or Xen

VI-LinuxVirtGuestCPUTotalUtilMonitor-AT

The VI-LinuxVirtGuestCPUUtilMonitor policy uses the multi-instance baseline for monitoring the total CPU utilization of the guest machines for KVM or Xen and sends an alert message in case the performance goes below the set threshold.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → <*language*> → Virtualization Infrastructure → Performance → LinuxVirt**.
- **Infrastructure Management → <*language*> → Virtualization Infrastructure → Policies Grouped by Vendor → LinuxVirt - Advanced**.

Metrics Used	BYLS_CPU_TOTAL_UTIL BYLS_LS_NAME BYLS_LS_UUID

	BYLS_DISPLAY_NAME BYLS_LS_ROLE
Supported Platform	KVM or Xen
Script-Parameter	**Description**
MessageObject	Application for outgoing messages.
DataSource	Displays the data source name as SCOPE.
DataObject	Displays the data object name as LOGICAL.
DataMetric	Displays the metric name as BYLS_CPU_TOTAL_ UTIL.
BaselinePeriod	Type the time period you want to define as a baseline period, such as '3600 seconds'. This period moves with the current time. The most recent 3600-second (1-hour) period becomes the current baseline period.
MinimumValue	Displays the minimum value of CPU utilization as indicated by the metric.
MaximumValue	Displays the maximum value of CPU utilization as indicated by the metric.
WarningDeviations	Displays the number of standard deviation away form normal, at which the policy sends a warning message to HPOM console. Set an appropriate value for the parameter. To disable the parameter, set value as *5*.
MinorDeviations	Displays the number of standard deviation away form normal, at which the policy sends a minor message to HPOM console. Set an appropriate value for the parameter greater than the specified value for *WarningDeviations*. To disable the parameter, set value as *5*.
MajorDeviations	Displays the number of standard deviation away form normal, at which the policy sends a major message to HPOM console. Set an appropriate value for the parameter greater than the specified value for *MinorDeviations*. To disable the parameter, set value as *5*.
WarningHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.

MinorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
WarningLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
InstanceSource	Do not rename the policy name. The policy uses its name to retrieve the source.
MessageGroup	Message group for outgoing messages.
CPUTotUtilCutOff	Set the CPU Utilization level below CPUTotUtilCutOff which you do not want to monitor.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 30 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

After the values return within normal levels, the alert messages are automatically acknowledged.

Memory Utilization Monitor Policy for KVM or Xen Host

VI-LinuxVirtHostMemoryUtilMonitor

The VI-LinuxVirtHostMemoryUtilMonitor policy monitors memory utilization of the host machines for KVM or Xen and sends an alert message in case the performance goes below the set threshold.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Performance → LinuxVirt**.
- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor → LinuxVirt - Advanced**.

Metrics Used	GBL_MEM_UTIL GBL_MEM_FREE GBL_LS_TYPE
Supported Platform	KVM or Xen

Script-Parameter	Description
MemUtilCriticalThreshold	If the memory utilization on the host machine is more than the critical threshold value, the policy generates an alert message with severity `Critical`.
MemUtilMajorThreshold	If the memory utilization on the host machine is more than the major threshold value, the policy generates an alert message with severity `Major`.
MemUtilMinorThreshold	If the memory utilization on the host machine is more than the minor threshold value, the policy generates an alert message with severity `Minor`.
MemUtilWarningThreshold	If the memory utilization on the host machine is more than the warning threshold value, the policy generates an alert message with severity `Warning`.
FreeMemAvailCriticalThreshold	If the free memory available in Mbs on the host machine is more than the critical threshold value, the policy generates an alert message with severity `Critical`.
FreeMemAvailMajorThreshold	If the free memory available in Mbs on the host machine is more than the major threshold value, the policy generates an alert message with severity `Major`.
FreeMemAvailMinorThreshold	If the free memory available in Mbs on the host machine is more than the minor threshold value, the policy generates an alert message with severity `Minor`.
FreeMemAvailWarningThreshold	If the free memory available in Mbs on the host machine is more than the warning threshold value, the policy generates an alert message with severity `Warning`.
MessageGroup	Message group for outgoing messages.

Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The alert messages are generated based on the values of the script parameters mentioned in the above table. The alert messages are automatically acknowledged when the values of host memory utilization reach normal.

The default polling interval for this policy is 5 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

Memory Performance Monitor Policy for KVM or Xen

VI-LinuxVirtVMMemoryPerformanceMonitor

The VI-LinuxVirtVMMemoryPerformanceMonitor policy monitors the memory performance of the KVM or Xen virtual machines and sends an alert message in case the performance goes below the set threshold.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Performance → LinuxVirt**.
- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor → LinuxVirt - Advanced**.

Metrics Used	BYLS_LS_ROLE BYLS_LS_TYPE BYLS_LS_UUID BYLS_MEM_USED BYLS_MEM_PHYS_UTIL BYLS_MEM_ENTL BYLS_LS_HOST_HOSTNAME BYLS_DISPLAY_NAME BYLS_MEM_SWAPOUT
Supported Platform	KVM or Xen
Script-Parameter	**Description**
VMSwapOutMajorThreshold	If the memory swap out for a virtual machine is more than the major threshold value, the policy generates an alert message with severity `Major`.
VMSwapOutMinorThreshold	If the memory swap out for a virtual machine is more than the minor threshold value, the policy generates an

	alert message with severity `Minor`.
VMSwapOutWarningThreshold	If the memory swap out for a virtual machine is more than the warning threshold value, the policy generates an alert message with severity `Warning`.
VMMemUtilMajorThreshold	If the memory utilization on the virtual machine is more than the major threshold value, the policy generates an alert message with severity `Major`.
VMMemUtilMinorThreshold	If the memory utilization on the virtual machine is more than the minor threshold value, the policy generates an alert message with severity `Minor`.
VMMemUtilWarningThreshold	If the memory utilization on the virtual machine is more than the warning threshold value, the policy generates an alert message with severity `Warning`.
Debuglevel	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The alert messages are generated based on the values of the script parameters mentioned in the above table. The alert messages are automatically acknowledged when the values of host memory utilization reach normal.

The default polling interval for this policy is 5 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

Memory Usage Policy for KVM or Xen

VI-LinuxVirtVMMemoryUsage-AT

The VI-LinuxVirtVMMemoryUsage-AT policy monitors how much memory is being used by the guest virtual machines and resource pools in MBs.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → <*language*> → Virtualization Infrastructure → Performance → LinuxVirt**.
- **Infrastructure Management → <*language*> → Virtualization Infrastructure → Policies Grouped by Vendor → LinuxVirt - Advanced**.

The policy uses a multi-instance baseline for monitoring the memory usage for virtual machines. It uses automatic threshold determination to automatically calculate the threshold values. The threshold values are calculated according to the host memory usage by guest virtual machines on previous days. When the threshold values are reached or exceeded, the VI-LinuxVirtVMMemoryUsage-AT sends an alert to the HPOM console. The message severity can be major, minor, or warning depending upon the level of threshold violated.

Metrics Used	BYLS_DISPLAY_NAME

	BYLS_MEM_USED BYLS_LS_UUID BYS_LS_ROLE
Supported Platform	KVM or Xen
Script-Parameter	**Description**
MessageApplication	Application for outgoing messages.
DataSource	Displays the data source name as SCOPE.
DataObject	Displays the data object name as LOGICAL.
DataMetric	Displays the metric name as BYLS_MEM_USED.
BaselinePeriod	Type the time period you want to define as a baseline period, such as '3600 seconds'. This period moves with the current time. The most recent 3600-second (1-hour) period becomes the current baseline period.
MinimumValue	Displays the minimum value of memory used as indicated by the metric.
MaximumValue	Displays the maximum value of memory used as indicated by the metric.
WarningDeviations	Displays the number of standard deviation away form normal, at which the policy sends a warning message to HPOM console. Set an appropriate value for the parameter. To disable the parameter, set value as *5*.
MinorDeviations	Displays the number of standard deviation away form normal, at which the policy sends a minor message to HPOM console. Set an appropriate value for the parameter greater than the specified value for *WarningDeviations*. To disable the parameter, set value as *5*.
MajorDeviations	Displays the number of standard deviation away form normal, at which the policy sends a major message to HPOM console. Set an appropriate value for the parameter greater than the specified value for *MinorDeviations*. To disable the parameter, set value as *5*.
WarningHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.

MinorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
WarningLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
InstanceSource	Do not rename the policy name. The policy uses its name to retrieve the source.
DebugLevel	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.
MessageGroup	Message group for outgoing messages.
MemUsageCutOff	Set a value below which you do not want to monitor the memory usage for virtual guest machines.

The default polling interval for this policy is 30 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

After the values return within normal levels, the alert messages are automatically acknowledged.

Trending Based Alert Mechanism

The existing policies generate an alert whenever the utilization factor is greater than the threshold value. The utilization factor is not constant and may vary in the next interval. In a fluctuating

system, the policy generates an alert based on the spike. To overcome this limitation trending based alert mechanism is introduced.

Trending mechanism uses last 30 samples to find out the trend of the system. Using the trend value, the policy calculates the time taken to reach the saturation value that is the `HardStopThreshold`.

Trending feature has been implemented in the following policies:

- VI-VMwareVCGuestCPUPerformanceMonitor
- VI-VMwareVCGuestMemoryPerformanceMonitor
- VI-VMwareVCClusterCPUPerformanceMonitor
- VI-VMwareVCClusterMemoryPerformanceMonitor

The parameters used with respect to the trending feature is:

- **TrendingCheckFlag**: This flag is used to switch the trending feature **On** or **Off**.
- **HardStopThreshold**: The trending feature will not be applicable above this value.

Cluster CPU Performance Monitor Policy for VMware vCenter

VI-VMwareVCClusterCPUPerformanceMonitor

The VI-VMwareVCClusterCPUPerformanceMonitor policy monitors the CPU utilization of the cluster along with the vmotion count in the cluster.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Performance → VMware vCenter.**
- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor → VMware vCenter - Advanced.**

Metrics Used	• SystemRole • ID • Name • CPUTotalUtil • TotalVmMotions • Type • ParentUUID • CPUPhysTotalUtil • SystemHostName
Supported Platform	VMware vCenter
Script-Parameter	**Description**
ClusterCpuUtilMajorThreshold	If the CPU utilization for a cluster is more than the

	specified threshold value, the policy generates an alert message with severity `Major`.
ClusterCpuUtilMinorThreshold	If the CPU utilization for a cluster is more than the specified threshold value, the policy generates an alert message with severity `Minor`.
ClusterCpuUtilWarningThreshold	If the CPU utilization for a cluster is more than the specified threshold value, the policy generates an alert message with severity `Warning`.
TrendingCheckFlag	Set the value to `On` if you want to enable the trending feature. If you want to disable the trending feature set the value to `Off`. The default value is `Off`.
HardStopThreshold	If the CPU utilization for a virtual machine is more than the specified threshold value without any trending feature, the policy generates an alert message with severity `Major`. This flag is applicable only if the *TrendingCheckFlag* is set to `On`.
MessageGroup	Message group for outgoing messages.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 30 seconds. You can modify the threshold settings and polling interval in the policy depending on your requirements.

Cluster Memory Performance Monitor Policy for VMware vCenter

VI-VMwareVCClusterMemoryPerformanceMonitor

The VI-VMwareVCClusterMemoryPerformanceMonitor policy monitors the memory utilization of the cluster along with the vmotion count in the cluster.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Performance → VMware vCenter.**
- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor → VMware vCenter - Advanced.**

Metrics Used	• SystemRole • ID • Name • MemTotalUtil • TotalVmMotions

	• Type • ParentUUID • MemPhysUtil • MemEntl • MemUsed • MemFree
Supported Platform	VMware vCenter
Script-Parameter	**Description**
ClusterMemUtilMajorThreshold	If the memory utilization for a cluster is more than the specified threshold value, the policy generates an alert message with severity `Major`.
ClusterMemUtilMinorThreshold	If the memory utilization for a cluster is more than the specified threshold value, the policy generates an alert message with severity `Minor`.
ClusterMemUtilWarningThreshold	If the memory utilization for a cluster is more than the specified threshold value, the policy generates an alert message with severity `Warning`.
TrendingCheckFlag	Set the value to `On` if you want to enable the trending feature. If you want to disable the trending feature set the value to `Off`. The default value is `Off`.
HardStopThreshold	If the CPU utilization for a virtual machine is more than the specified threshold value without any trending feature, the policy generates an alert message with severity `Major`. This flag is applicable only if *TrendingCheckFlag* is set to `On`.
MessageGroup	Message group for outgoing messages.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 10 seconds. You can modify the threshold settings and polling interval in the policy depending on your requirements.

Guest CPU Performance Monitor Policy for VMware vCenter

VI-VMwareVCGuestCPUPerformanceMonitor

The VI-VMwareVCGuestCPUPerformanceMonitor policy monitors the CPU utilization of the guest systems and sends an alert message in case the performance level goes below the set threshold.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Performance → VMware vCenter.**
- **Infrastructure Management → *<language>* → Virtualization Infrastructure → Policies Grouped by Vendor → VMware vCenter - Advanced.**

Metrics Used	• SystemRole • SystemID • CPUTotalUtil • SystemName • SystemState • CPUPhysReadyUtil • NumCPU • SystemHostHostName • SystemHostName • CPUEntlMin • CPUEntlMax • CPUSharesPrio • GuestToolsStatus
Supported Platform	VMware vCenter
Script-Parameter	**Description**
VMCpuUtilMajorThreshold	If the CPU utilization for a virtual machine is more than the specified threshold value, the policy generates an alert message with severity `Major`.
VMCpuUtilMinorThreshold	If the CPU utilization for a virtual machine is more than the specified threshold value, the policy generates an alert message with severity `Minor`.
VMCpuUtilWarningThreshold	If the CPU utilization for a virtual machine is more than the specified threshold value, the policy generates an alert message with severity `Warning`.
VMReadyUtilMajorThreshold	If the ready utilization for a virtual machine is more than the specified threshold value, the policy generates an alert message with severity `Major`.
VMReadyUtilMinorThreshold	If the ready utilization for a virtual machine is more than the specified threshold value, the policy generates an alert message with severity `Minor`.
VMReadyUtilWarningThreshold	If the ready utilization for a virtual machine is more than the specified threshold value, the policy generates an

	alert message with severity `Warning`.
TrendingCheckFlag	Set the value to `On` if you want to enable the trending feature. If you want to disable the trending feature set the value to `Off`. The default value is `Off`
HardStopThreshold	If the CPU utilization for a virtual machine is more than the specified threshold value without any trending feature, the policy generates an alert message with severity `Major`. This flag is applicable only if *TrendingCheckFlag* is set to `On`.
MessageGroup	Message group for outgoing messages.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 20 seconds. You can modify the threshold settings and polling interval in the policy depending on your requirements.

Guest Memory Performance Monitor Policy for VMware vCenter

VI-VMwareVCGuestMemoryPerformanceMonitor

The VI-VMwareVCGuestMemoryPerformanceMonitor policy monitors the memory performance of the guest systems. High memory utilization for a long period of time or high memory swap and balloon utilization can impact the performance of virtual machines.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → <*language*> → Virtualization Infrastructure → Performance → VMware vCenter**
- **Infrastructure Management → <*language*> → Virtualization Infrastructure → Policies Grouped by Vendor → VMware vCenter - Advanced**.

Metrics Used	• SystemRole • SystemID • MemUsed • SystemName • SystemState • MemEntl • MemBalloonUtil • MemSwapUtil • SystemHostHostName • SystemHostName

	• MemEntlMin • MemEntlMax • MemSharesPrio • GuestToolsStatus
Supported Platform	VMware vCenter
Script-Parameter	**Description**
VMMemUtilMajorThreshold	If the memory utilization for a virtual machine is more than the specified threshold value, the policy generates an alert message with severity `Major`.
VMMemUtilMinorThreshold	If the memory utilization for a virtual machine is more than the specified threshold value, the policy generates an alert message with severity `Minor`.
VMMemUtilWarningThreshold	If the memory utilization for a virtual machine is more than the specified threshold value, the policy generates an alert message with severity `Warning`.
VMMemBalloonUtilThreshold	If the balloon utilization for a virtual machine is more than the specified threshold value, the policy generates an alert message with severity `Minor`.
VMMemSwapUtilThreshold	If the swap utilization for a virtual machine is more than the specified threshold value, the policy generates an alert message with severity `Major`.
TrendingCheckFlag	Set the value to `On` if you want to enable the trending feature. If you want to disable the trending feature set the value to `Off`. The default value is `Off`
HardStopThreshold	If the memory utilization for a virtual machine is more than the specified threshold value, the policy generates an alert message with severity `Major`. This flag is applicable only if *TrendingCheckFlag* is set to `On`.
MessageGroup	Message group for outgoing messages.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 5 minutes 30 seconds. You can modify the threshold settings and polling interval in the policy depending on your requirements.

Resource Pool CPU Utilization Monitor Policy for VMware vCenter

VI-VMwareVCRespoolCPUUtilMonitor

The VI-VMwareVCRespoolCPUUtilMonitor policy monitors the CPU utilization of Resource pool. High CPU utilization creates performance problems at Virtual machines. The alert message lists the virtual machines that use a significant amount of the CPU resource.

In the console tree, the policy is listed at the following locations:

- **Infrastructure Management → <*language*> → Virtualization Infrastructure → Performance → VMware vCenter**
- **Infrastructure Management → <*language*> → Virtualization Infrastructure → Policies Grouped by Vendor → VMware vCenter - Advanced**.

Metrics Used	• LSName • BelongsToDatacenter • ClusterName • CPUPhysUtil • ID • Name
Supported Platform	VMware vCenter
Script-Parameter	**Description**
RespoolCpuUtilCriticalThreshold	If the CPU utilization for a resource pool is more than the specified threshold value, the policy generates an alert message with severity `Critical`.
RespoolCpuUtilMajorThreshold	If the CPU utilization for a resource pool is more than the specified threshold value, the policy generates an alert message with severity `Major`.
RespoolCpuUtilMinorThreshold	If the CPU utilization for a resource pool is more than the specified threshold value, the policy generates an alert message with severity `Minor`.
RespoolCpuUtilWarningThreshold	If the CPU utilization for a resource pool is more than the specified threshold value, the policy generates an alert message with severity `Warning`.
MessageGroup	Message group for outgoing messages.
MessageApplication	Application for outgoing messages.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node.

The default polling interval for this policy is 30 minutes. You can modify the threshold settings and polling interval in the policy depending on your requirements.

Deploying VI SPI Policies from HPOM for Windows Management Server

To enable auto deployment of policies, follow these steps:

1. To enable auto deployment on the server, run the following command:

   /opt/OV/contrib/OpC/autogranting/enableAutoGranting.sh

2. To enable auto deployment for Infra SPI using XPL config change, run the following command:

   ovconfchg -ns infraspi -set AUTODEPLOYMENT true

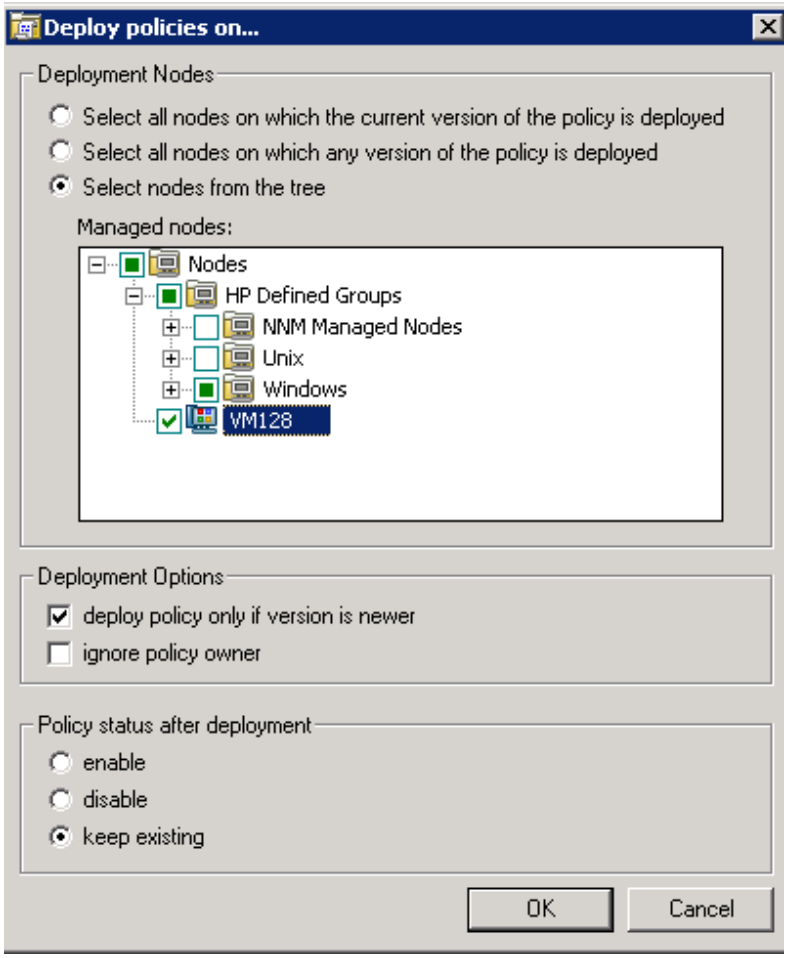
3. To activate the node, run the following command on the management server:

   opcactivate -srv <HPOM Server> -cert_srv <HPOM Server> -f

4. Grant the certificates.
5. Add the node to the SI-Deployment node group.
6. Deploy configuration.
7. Check whether the node is added to the appropriate node group.
8. Verify auto deployment of policies to the node.

To manually deploy policies from the management server, follow these steps:

1. Right-click the policy you want to deploy.
2. From the menu, select **All Tasks**.
3. Select **Deploy on**. The Deploy policies on dialog box opens.



4. Select the option **Select nodes from the tree**. From the list of managed nodes, select the nodes where you want to deploy the policy.
5. Click **OK**.

Deploying VI SPI Policies from HPOM for UNIX Management Server

Before you deploy policies, make sure that the nodes have been added to the management server and have HP Operations Agent software installed. For more information about how to add nodes to the management server, see *HP Operations Manager for Unix Online Help*.

To deploy policies from the management server for HPOM for UNIX (HP-UX, Linux, or Solaris) follow these steps:

Task 1: Assign Policy or Policy group

1. Log on to HPOM as the administrator. The HPOM Administration interface appears.
2. Click **Policy Bank** under the Objects Bank category. The Policy Bank window opens.
3. In the Policy Bank window, select the policy or policy groups you want to assign to a node or a node group.
4. Select **Assign to Node/Node group...** from the **Choose an Action** drop-down box and click submit. The select window opens.
5. Select the node or the node groups and click **OK**. The selected policies are assigned to the nodes.

Task 2: Deploy Policies

1. From the HPOM Administration interface, click **Node Bank** under the Objects Bank category. The Node Bank window opens.
2. In the Node Bank window, select the nodes or node groups on which you want to deploy policies.
3. Select **Deploy Configuration...** from the **Choose an Action** drop-down box and click submit. The selector window opens.
4. Select the **Distribute Policies** check box and click **OK**. The policies are deployed on the selected nodes.

Virtualization Infrastructure SPI Tools

The Virtualization Infrastructure SPI provides a number of pre-configured tools that help you manage the virtualized infrastructure. These tools are supported on VMware ESX and ESXi servers managed by VMware vMA.

To launch a tool from the HPOM for Windows management server, follow these steps:

1. From the console tree **Tools** folder, select the **Virtualization Infrastructure** folder.
2. Double-click the tool. The **Select where to launch this tool** window opens.

3. Under the Select one or more nodes/node group/service section, select the host server node to launch the tool.
4. Click **Launch**. The Edit Parameters page appears.
5. Leave the Parameters text box blank to see the information about all hosts managed by vMA or enter the host name to see information about that specific host.
6. Click **Launch**. The Tool Status windows appears. It displays the list of launched tools and tool output.

To launch a tool from the HPOM for UNIX management server, follow these steps:

1. Go to **Tool Bank** → **Virtualization Infrastructure** in the Administration interface.
2. Right-click the **VMware Host Info** tool, select **Start Customized**. The Start Tool - Customized Wizard window opens.
3. Under the nodes list, select the host server node to launch the tool.
4. On the wizard, click **Get Selections.** The node is added to the Selected Nodes list.
5. Click **Next**.
6. On the page Specify Additional Information Needed to Run the Tool, you can specify the additional information or leave the fields blank.
7. Click **Finish**. The tool output appears.

Host Information Tool

VMware Host Info

This tool lists the information about the host systems that are managed by VMware vMA. It displays information such as boot time, file system, host status, and memory usage. By default it displays information about each host managed by vMA. You can display the information about a single system as well.

Guest Information Tool

LinuxVirt Guest Info

This tool lists the information about the guest systems that are managed by KVM or Xen. It displays information such as CPU time, guest status, and memory usage. By default it displays information about each guest managed by KVM or Xen irrespective of the state of the guest system. You can display the information about a single guest system as well by passing the guest system name as a parameter while running the tool.

List of Suspended Virtual Machines Tool

VMware List Suspended VMs

This tool lists all virtual machines managed by vMA that are suspended or powered off. By default it displays information about the virtual machines hosted on the servers managed by vMA. You can display the information about virtual machines hosted on a single server as well.

LinuxVirt List Suspended VMs

This tool lists all virtual machines configured on LinuxVirt servers that are suspended or powered off. You can display the information about virtual machines hosted on a single server as well.

List of Virtual Machines Tool

VMware List VMs

This tool lists all virtual machines managed by vMA. By default it lists the virtual machines hosted on the servers managed by vMA. You can display the list of virtual machines hosted on a single server as well.

LinuxVirt List VMs

This tool lists all the active virtual machines for the selected KVM or Xen host. You need not pass any parameters while running this tool.

Resource Pool Information Tool

VMware Resource Pool Info

This tool lists the information about the resource pools that are managed by VMware vMA. It displays information such as guaranteed minimum CPU units configured, reserved amount of memory, and minimum processor capacity. By default the tool displays information about each resource pool hosted on the servers managed by vMA. You can display the information about a resource pool hosted on a single system as well. The *Edit Parameters* page does not appear for this tool.

Overall Status for VMware vMA Tool

VMware vMA OverAll Status

This tool lists the overall information about VMware vMA. It displays information with respect to Operations agent, such as the version of Operations agent installed and status of the main components of Operations agent. It also displays vMA related information, such as the vMA version of the node, vMA resource allocation and utilization, status of the target nodes connected to vMA, allowed number of instances on vMA 4.0 or 4.1 or 5.0. No parameters are required to be passed for this tool.

Chapter 6

Virtualization Infrastructure SPI Reports and Graphs

You can integrate the Virtualization Infrastructure SPI with HP Reporter to generate reports based on collected metric data from the managed nodes. The reports provide an overall picture of virtual resources. You can also generate graphs to analyze the metric data collected. To generate and view reports and graphs from data collected by the Virtualization Infrastructure SPI, use HP Reporter and HP Performance Manager with HPOM.

Virtualization Infrastructure SPI Reports

The reports provide an overall picture of virtual resources. You can integrate the Virtualization Infrastructure SPI with HP Reporter to generate reports based on collected metric data from the managed nodes.

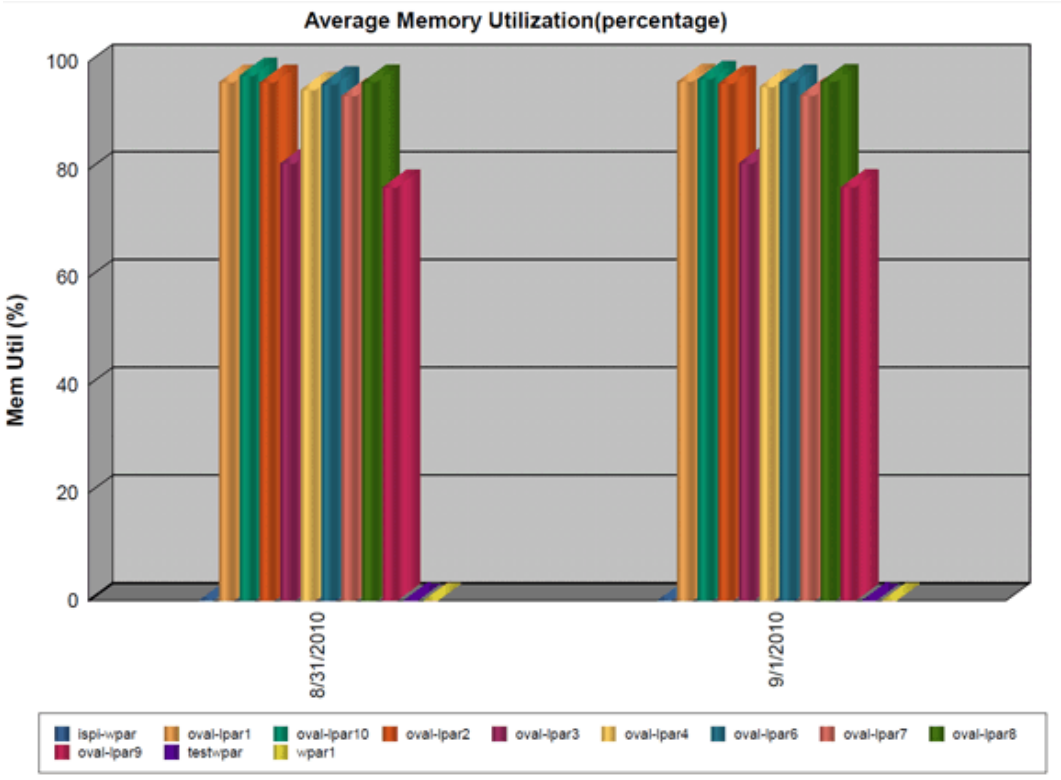
You can access Virtualization Infrastructure SPI reports from the HPOM console. To install HP Reporter package, see *Infrastructure SPI Installation Guide*.

To view reports for Virtualization Infrastructure SPI from HPOM for Windows, expand **Reports** → **Virtualization Infrastructure** in the console tree. To display a report, select the desired report, right-click, and then select **Show report**.

The Virtualization Infrastructure SPI Reports folder is not created until data is collected on nodes and the Service Reporter consolidation process has run, which is usually 24 hours after a node becomes managed.

If HP Reporter is installed on a separate system connected to the HPOM management server (for Windows, UNIX, Linux, Solaris operating system), you can view the reports on HP Reporter system. For more information about integration of HP Reporter with HPOM, see *HP Reporter Installation and Special Configuration Guide*.

Figure 1: Sample Report



The SPI for Virtualization Infrastructure provides the following reports:

Table 1: Virtualization Infrastructure SPI Reports

Report/ Report Title	Purpose	Platform
HPVM Configuration	This report displays the configuration information of the HPVM hosts. You can use this report to view and compare the configuration details for HPVM hosts.	HPVM
HPVM CPU Utilization	This report displays the physical CPU utilization details of the HPVM hosts. You can use this report to view and compare the CPU utilization of the HPVM hosts.	HPVM
IBM LPAR Configuration	This report displays the configuration information of the IBM LPARs. You can use this report to view and compare the configuration details for IBM LPARs.	IBM LPAR
IBM LPAR CPU Utilization	This report displays the physical CPU utilization details of the IBM LPARs. You can use this report to view and compare the CPU utilization of the IBM LPARs.	IBM LPAR

Report/ Report Title	Purpose	Platform
IBM LPAR Memory Utilization	This report displays the physical memory utilization information of IBM LPARs. You can use this report to view and compare the physical memory utilization of IBM LPARs.	IBM LPAR
Infra SPI Active HPOM Message Severity	This report displays the severity of the active Infrastructure SPIs error messages on the HPOM server that were not acknowledged at the time of data collection.	Microsoft Hyper-V
Infra SPI Active HPOM Messages - Top 20	This report displays the top 20 active error messages on the HPOM server that were not acknowledged at the time of data collection.	Microsoft Hyper-V
Infra SPI History HPOM Message Severity	This report displays the severity of Infrastructure SPIs error messages that were sent to the HPOM server and were acknowledged.	Microsoft Hyper-V
Infra SPI History HPOM Messages - Top 20	This report displays the top 20 Infrastructure SPIs error messages that were sent to the HPOM server and were not acknowledged.	Microsoft Hyper-V
Oracle Containers Configuration	This report displays the configuration information of Oracle Containers. You can use this report to view and compare the configuration details for Oracle Containers.	Oracle Solaris Zones
Oracle Containers CPU Utilization	This report displays the physical CPU utilization details of Oracle Containers. You can use this report to view and compare the CPU utilization of Oracle Containers.	Oracle Solaris Zones
VMware Configuration	This report displays the configuration information of the the host ESX/ESXi servers and the guest virtual machines configured on them. You can use this report to view and compare the configuration details for the host and guest machines.	VMware ESX/ESXi
VMware CPU Utilization	This report displays the physical CPU utilization details of the vMA and the host ESX/ESXi servers managed by it. It also displays the resource pools and the guest virtual machines configured on the hosts. You can use this report to view and compare the physical CPU utilization of host and guest machines.	VMware ESX/ESXi
VMware Memory Utilization	This report displays the physical memory	VMware ESX/ESXi

Report/ Report Title	Purpose	Platform
	utilization information of the vMA and the host ESX/ESXi servers managed by it. You can use this report to view and compare the physical memory utilization of ESX/ESXi host machines and the guest virtual machines configured on them.	
VMware DataCenter CPU Utilization	This report displays the details of aggregate physical CPU utilization at the VMware DataCenter level.	VMware ESX/ESXi
VMware DataCenter Memory Utilization	This report displays the details of aggregate memory utilization at the VMware DataCenter level.	VMware ESX/ESXi
VMware DataCenter Datastore Utilization	This report displays the details of aggregate datastore utilization at the VMware DataCenter level.	VMware ESX/ESXi
Infra SPI Active HPOM Message Severity	This report displays the severity of the active Infrastructure SPIs error messages on the HPOM server that were not acknowledged at the time of data collection.	VMware ESX/ESXi
Infra SPI Active HPOM Messages - Top 20	This report displays the top 20 active error messages on the HPOM server that were not acknowledged at the time of data collection.	VMware ESX/ESXi
Infra SPI History HPOM Message Severity	This report displays the severity of Infrastructure SPIs error messages that were sent to the HPOM server and were acknowledged.	VMware ESX/ESXi
Infra SPI History HPOM Messages - Top 20	This report displays the top 20 Infrastructure SPIs error messages that were sent to the HPOM server and were not acknowledged.	VMware ESX/ESXi
LinuxVirt Host-Guest CPU Utilization	This report displays the average percentage of the total CPU cycles consumed by the Host and Guest systems within a time interval.	KVM or Xen
LinuxVirt Host-Guest Disk Phys Read Byte Rate	This report displays the number of bytes read from the disk between the previous refresh operation and the current refresh operation of LinuxVirt Host and Guest systems within a time interval.	KVM or Xen
LinuxVirt Host-Guest Disk Phys Write Byte Rate	This report displays the number of bytes written to the disk between the previous refresh operation and the current refresh	KVM or Xen

Report/ Report Title	Purpose	Platform
	operation of LinuxVirt Host and Guest systems within a time interval.	
LinuxVirt Host-Guest Net In Packet Rate	This report displays the average rate at which data is received between the previous refresh cycle and the current refresh cycle of LinuxVirt Host and Guest systems.	KVM or Xen
LinuxVirt Host-Guest Net Out Packet Rate	This report displays the average rate at which data is transmitted between the previous refresh cycle and the current refresh cycle of LinuxVirt Host and Guest systems.	KVM or Xen

Virtualization Infrastructure SPI Graphs

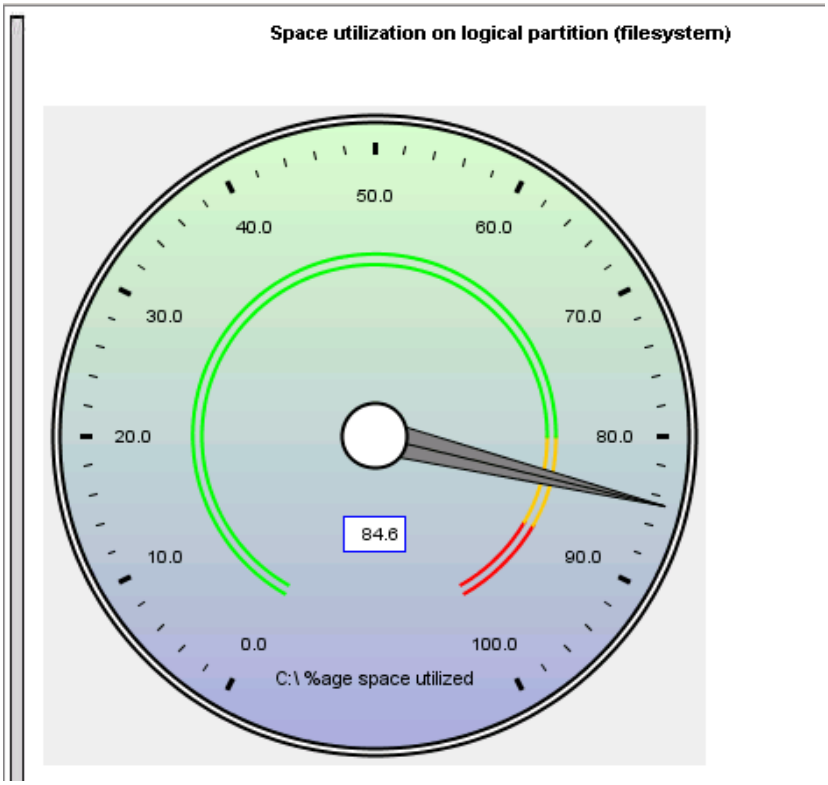
You can generate graphs to analyze the metric data collected. To generate and view graphs from data collected by the Virtualization Infrastructure SPI, use HP Performance Manager with HPOM. HP Performance Manager generates graphs from near real-time data gathered from the managed nodes. You can access these graphs from the HPOM console if you install HP Performance Manager on an HPOM management server.

The Virtualization Infrastructure SPI comes with a set of pre-configured graphs. They are located on the HPOM console tree in the Graphs folders. You can access this Graphs folder only if you install HP Performance Manager on the HPOM management server. The following is an example graph.

To access the graphs on HPOM for Windows, select **Graphs→ Infrastructure Performance → Virtualization**.

To access the graphs on HPOM for UNIX (HP-UX, Linux, and Solaris), select the active message, open the Message Properties window, and click **Actions.** Under the Operator initiated action section, click **Perform**. Alternatively you can, right-click active message, select **Perform/Stop Action** and click **Perform Operator-Initiated Action**.

Figure 2: Sample Graph



The SPI for Virtualization Infrastructure provides the following graphs:

- Global History
- Global Run Queue Baseline
- Global Details
- Multiple Global Forecasts
- CPU Summary
- CPU Utilization Summary
- CPU Utilization Baseline
- Individual CPUs
- CPU Comparison
- CPU Gauges
- CPU Details
- Global CPU Forecast
- Seasonal CPU Forecast
- Disk Summary
- Disk Throughput
- Disk Space
- Disk Space (Pie Chart)

- Disk Details
- Disk Utilization
- Swap Space Utilization
- Network Summary
- Individual Networks
- Network Interface Details
- Memory Summary
- Physical Memory Utilization
- System Configuration
- Configuration Details
- Transaction Health
- Transaction History
- Transaction Details
- Transaction Response Forecasts
- Filesystem Details
- Application CPU Gauges
- Application CPU Forecasts
- Application History
- Application Details
- Process Details
- Virtualization Configuration
- VM Status
- CPU Entitlement by Logical Systems
- Percentage Utilization of CPU Entitlement by Logical Systems
- Percentage Utilization of Total Physical CPU by Logical Systems
- Percentage Utilization of Physical CPU by LPAR Frame
- LPAR Frame Memory Utilization
- CPU Details of Logical System
- CPU Summary by Logical Systems
- Percentage Utilization of Memory Entitlement by Logical Systems
- Memory Summary by Logical Systems
- CPU Entitlement Utilization Baseline
- Percentage Utilization of Swap by Zones

- Percentage Utilization of Memory by Zones
- VMware ESX/ESXi Host Memory Utilization
- VMware ESX/ESXi Host Memory Utilization Baseline
- VMware ESX/ESXi Host Disk Utilization
- VMware ESX/ESXi Host - Network MB
- VMware ESX/ESXi - CPU Utilization across Resource Pools
- Solaris Container Host CPU Utilization
- MSHyper-V Host CPU Utilization
- HPVM Host CPU Utilization
- LPAR Frame level CPU Utilization
- LPAR Frame CPU Utilization
- Guests - CPU entitlement Utilization
- VMware Datacenter - CPU and Memory aggregate usage)
- VMware Data Center - Percentage Utilization of CPU
- VMware Data Center - Percentage Utilization of Memory
- VMware Data Center - Percentage Utilization of Datastore
- LinuxVirt Network Byte Rate Baseline
- LinuxVirt Physical Disk Byte Rate Baseline
- Percentage Utilization of Total CPU by Logical Systems
- CPU Summary by Logical Systems
- LinuxVirt Host CPU Utilization
- Percentage Utilization of Memory by VMs on LinuxVirt

Chapter 7

Troubleshooting

This chapter offers an overview of the Virtualization Infrastructure SPI limitations and issues and covers basic troubleshooting information.

Discovery

Problem	VI Discovery does not work. Service map does not appear on the HPOM server and auto-addition of VMs is not triggered.
Solution	Restart the discovery agent on the node. Type the following command at the command prompt: `ovc -restart agtrep`

Problem	Discovery procedures and data collection gives error with non-English names.
Cause	The virtual infrastructure configurations with non-English machine names and resource group names are not supported by Virtualization Infrastructure SPI. The Virtualization Infrastructure SPI can be deployed successfully on a non-English HP Operations Manager. However, using non-English names for virtual systems gives an error as they are not recognized by the StoreCollection OvPerl APIs in the HP Operations agent.

Problem	Some guest machines do not appear under **Nodes** → **Virtualization** → **ESX/ESXi Virtual machines**.
Cause	This happens when the guest machines are in Powered Off state.
Solution	Power on the guest machines. The performance agent will collect data about the machines and add them in the node group.

Problem	Messages to add guests hosted by the ESX and ESXi

	servers are generated during virtualization discovery but these actions fail by default.
Cause	This happens because the XPL configuration setting on the HPOM management server *infraspi.AutoAdd_Guests* is set to false by default. You can set the value to true and again run the action to add guests.
Solution	The action does not run automatically by default to prevent a large number of virtual machines getting added in batch causing poor performance of the HPOM console. A convenient time may be chosen for running the auto-action. To enable the Auto-addition feature, follow these steps: In the HPOM console, go to **Infrastructure Management → Settings and Thresholds → Agent Settings**. 1. Double-click the **AUTO_ADDITION_SETTINGS** policy. The policy window opens. 2. Set *AutoAdd_Guests* to **true**. 3. Click **Save and Close**. 4. Deploy the AUTO_ADDITION_SETTINGS policy on the node.

Policies

Problem	Advanced Monitoring policies modified in HPOM for UNIX Administrator interface fail to run after deployment on the managed nodes.
Cause	When advanced monitoring policies are edited in interface mode in HPOM for UNIX policy editor, syntax errors are induced into the Perl code module. This causes the policy to fail to run. Errors such as the following appear: *An error occurred in the processing of the policy 'SI-LinuxSshdProcessMonitor'. Please check the following errors and take corrective actions. (OpC30-797)* *Error during evaluation of threshold level "Processes - Fill Instance list" (OpC30-728)* *Execution of instance filter script failed. (OpC30-714)* *Perl Script execution failed: syntax error at PerlScript line 11, near "1*

	#BEGIN_PROCESSES_LIST *#ProcName=/usr/sbin/sshd* *#Params=* *#Params=* *#MonMode=>=* *#ProcNum=1* *#END_PROCESSES_LIST* *@ProcNames"* *Missing right curly or square bracket at PerlScript line 17, within string* *syntax error at PerlScript line 17, at EOF* *. (OpC30-750)* The un-edited advanced monitoring policies (Measurement Threshold type) work fine when deployed from HPOM on UNIX.
Solution	To edit the settings in the Measurement Threshold policy, use 'Edit in Raw mode' feature of the HPOM for UNIX Administrator interface to change the policy contents. This requires you to know the syntax of the policy data file.

Problem	VM event collector policy times out
Cause	The VM event collector policy is scheduled to run every 15 minutes by default. The event collecting script (of VM event collector policy) is allowed to run for a maximum of 10 minutes by default after which it times out the event collection.
Solution	In case, you want to change the schedule interval for the event collector policy, make sure the time-out interval is set to be less than the schedule interval of collector policy.

Problem	Warning/error messages on the HPOM console:

	Check the following errors and take corrective actions. (OpC30-797) Error during evaluation of threshold level "CPU Spikes level Critical" (OpC30-728) Execution of threshold script failed. (OpC30-712) Perl Script execution failed: Can't locate OvTrace.pm in @INC (@INC contains: /usr/lpp/OV\lbin\eaagt\perl /usr/lpp/OV/lbin/eaagt/perl /var/opt/OV/bin/instrumentation /usr/lpp/OV/nonOV/perl/a/lib/5.8.8/aix-thread-multi /usr/lpp/OV/nonOV/perl/a/lib/5.8.8 /usr/lpp/OV/nonOV/perl/a/lib/site_perl/5.8.8/aix-thread-multi /usr/lpp/OV/nonOV/perl/a/lib/site_perl/5.8.8 /usr/lpp/OV/nonOV/perl/a/lib/site_perl .) at PerlScript line 136. *BEGIN failed--compilation aborted (in cleanup) Can't locate OvTrace.pm in @INC (@INC contains: /usr/lpp/OV\lbin\eaagt\perl /usr/lpp/OV/lbin/eaagt/perl /var/opt/OV/bin/instrumentation /usr/lpp/OV/nonOV/perl/a/lib/5.8.8/aix-thread-multi /usr/lpp/OV/nonOV/perl/a/lib/5.8.8 /usr/lpp/OV/nonOV/perl/a/lib/site_perl/5.8.8/aix-thread-multi /usr/lpp/OV/nonOV/perl/a/lib/site_perl/5.8.8 /usr/lpp/OV/nonOV/perl/a/lib/site_perl .) at PerlScript line 136.* *BEGIN failed--compilation aborted at PerlScript line 136.* *. (OpC30-750)*
Cause	This error occurs on any policy and any *.pm file when the instrumentation is not deployed on the node correctly.
Solution	Forcefully deploy the instrumentation on the node.

Problem	Metrics are not displayed for collector policies.
Solution	There are two collector policies in VI SPI for data collection. Follow these steps to check whether metrics are logged for each of these policies: 1. Deploy VI-VMwareVMFSDataCollector and VI-VMwareDCDataCollector policies on the node. These policies collect information and store it in CODA. 2. Type the command: `ovcodautil -obj` 3. After running the commands, check the metrics listed under the following class and object for both the

	policies: **Policy Name**: VI-VMwareVMFSDataCollector **Class**: VISPI **Object**: VMFS **Metrics**: • VMFS_HOSTNAME • VMFS_DEVNAME • VMFS_DEVNO • VMFS_DIRNAME • VMFS_TYPE • VMFS_MAX_SIZE • VMFS_SPACE_AVAIL • VMFS_SPACE_UTIL • VMFS_TOTAL_READ_LATENCY • VMFS_TOTAL_WRITE_LATENCY • VMFS_DEVICE_READ_LATENCY • VMFS_DEVICE_WRITE_LATENCY • VMFS_KERNEL_READ_LATENCY • VMFS_KERNEL_WRITE_LATENCY • VMFS_DISK_BUS_RESETS • VMFS_DISK_COMMANDS_ISSUED • VMFS_DISK_COMMANDS_ABORTED • VMFS_DISK_READ_THROUGHPUT • VMFS_DISK_WRITE_THROUGHPUT • VMFS_UUID • VMFS_HOSTNAME • VMFS_DEVNAME • VMFS_DEVNO • VMFS_DIRNAME • VMFS_TYPE • VMFS_MAX_SIZE • VMFS_SPACE_AVAIL • VMFS_SPACE_UTIL

	• VMFS_TOTAL_READ_LATENCY • VMFS_TOTAL_WRITE_LATENCY • VMFS_DEVICE_READ_LATENCY • VMFS_DEVICE_WRITE_LATENCY • VMFS_KERNEL_READ_LATENCY • VMFS_KERNEL_WRITE_LATENCY • VMFS_DISK_BUS_RESETS • VMFS_DISK_COMMANDS_ISSUED • VMFS_DISK_COMMANDS_ABORTED • VMFS_DISK_READ_THROUGHPUT • VMFS_DISK_WRITE_THROUGHPUT **Policy Name**: VI-VMwareDCDataCollector **Class**: VISPI **Object**: DC **Metrics**: • VMWARE_VC_NAME • VMWARE_DC_NAME • VMWARE_DC_CPU_UTIL • VMWARE_DC_CPU_USED • VMWARE_DC_CPU_TOTAL • VMWARE_DC_MEMORY_UTIL • VMWARE_DC_MEMORY_USED • VMWARE_DC_MEMORY_TOTAL • VMWARE_DC_DATASTORE_UTIL • VMWARE_DC_DATASTORE_FREE • VMWARE_DC_DATASTORE_TOTAL If the metrics is not listed, then the policy you had deployed is not working.

Problem	Data is not logged against each metrics for collector policies.
Solution	There are two collector policies in VI SPI for data collection. Follow these steps to check whether data is

	logged for each of these policies: 1. Deploy VI-VMwareVMFSDataCollector and VI-VMwareDCDataCollector policies on the node. 2. Check if metrics are collected for both the policies. For more information about the list of metrics, see *Metrics are not displayed for collector policies on page 121*. 3. Type the command: `ovcodautil -dumpds VISPI` After you run the command, the data appears for each metrics for both the policies. If you do not see any data listed against each metrics, then data is not logged for that policy.

VI SPI Scripts

Problem	Virtualization Infrastructure SPI scripts take longer time to run depending on the retry level set on the vMA system.
Cause	VMware vMA tries to connect to the host servers registered on it many times, till it succeeds. Due to this reason, the Virtualization Infrastructure SPI scripts may take longer time to run depending on the retry level set on the vMA system.

Solution	Run the following commands on the vMA system to reduce the number of retries to 1:
	`#sysctl -w net.ipv4.tcp_syn_retries=1`
	`net.ipv4.tcp_syn_retries = 1`
	#service network restart

HP Operations Agent

Problem	HP Operations agent certificates are not getting installed on the vMA system
Cause	The iptable firewall runs on the vMA system by default blocking the communication over the network.
Solution	Follow these steps for installing the HP Operations agent Certificates on the vMA system: 1. Open the TCP port (383) for HTTPS communication both ways (inward and outward).

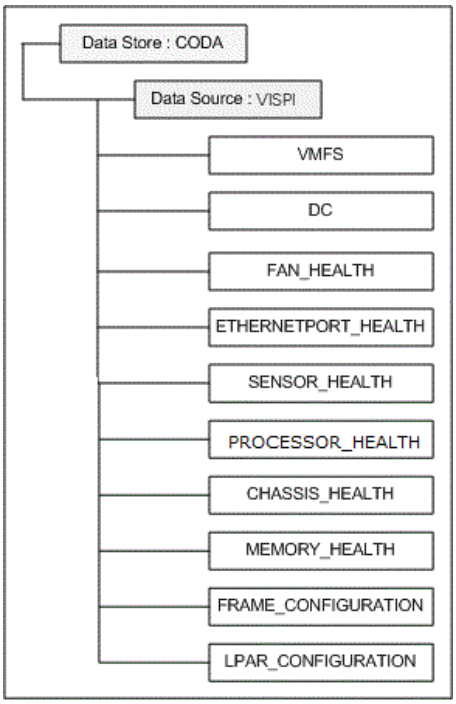
	2. Re-run the request to get certificates (**ovcert –certreq**) and bestow the certificate from the server. For more information about port 383 and how to enable it, see *HP Operations Manager Firewall Concepts and Configuration Guide*.

Appendix A

A) Virtualization Infrastructure SPI Metrics

VISPI provides performance based monitoring policies along with the metrics provided by SCOPE (for HP Performance Agent). VI SPI uses Infrastructure SPI metrics. These metrics are collected and logged in CODA (for HP Operations Agent) which is the default data store. For more information about Performance Agent metrics, see *HP Performance Agent for Windows Dictionary of Operating System Performance Metrics*.

Collection Objects



The following policies collect Infrastructure SPI metrics:

- VI-VMwareVMFSDataCollector
- VI-VMwareDCDataCollector
- VI-VMwareHardwareHealthCollector
- VI-IBMHMCDataCollector

Metrics Collected by VI-VMwareVMFSDataCollector Policy

The following metrics are related to the virtual machine's file system.

CODA\\VISPI\\VMFS

Metric Name	Description
VMFS_UUID	Universally Unique Identifier of the file system.
VMFS_HOSTNAME	Host name of the file system.
VMFS_DEVNAME	User friendly name of the VMFS volume.
VMFS_DEVNO	Device number.
VMFS_DIRNAME	Directory name of the file system.
VMFS_TYPE	Type of the file system.
VMFS_MAX_SIZE	Maximum size of the file system
VMFS_SPACE_AVAIL	Total space available on the file system.
VMFS_SPACE_UTIL	Total file system space utilized
VMFS_TOTAL_READ_LATENCY	The amount of time a read takes from the perspective of a guest operating system. This is the sum of kernel read latency and physical device read latency.
VMFS_TOTAL_WRITE_LATENCY	The amount of time a write takes from the perspective of a guest operating system. This is the sum of the kernel write latency and the physical device write latency.
VMFS_DEVICE_READ_LATENCY	Average amount of time, in milliseconds, to complete read from the physical device.
VMFS_DEVICE_WRITE_LATENCY	Average amount of time, in milliseconds, to write to the physical device (LUN).
VMFS_KERNEL_READ_LATENCY	Average amount of time, in milliseconds, spent by VMKernel processing each SCSI read command.
VMFS_KERNEL_WRITE_LATENCY	Average amount of time, in milliseconds, spent by VMKernel processing each SCSI write command.
VMFS_DISK_BUS_RESETS	Number of SCSI-bus reset commands issued during the collection interval by the file system.
VMFS_DISK_COMMANDS_ISSUED	Number of SCSI commands issued during the collection interval.
VMFS_DISK_COMMANDS_ABORTED	Number of SCSI commands aborted during the collection interval.
VMFS_DISK_READ_THROUGHPUT	Read throughput of the physical disk.
VMFS_DISK_WRITE_THROUGHPUT	Write throughput of the physical disk.

Metrics Collected by VI-VMwareDCDataCollector Policy

The following metrics are related to the VMware datacenter.

CODA\\VISPI\\DC

Metric Name	Description
VMWARE_VC_NAME	Name of the vCenter
VMWARE_DC_NAME	Name of the datacenter
VMWARE_DC_CPU_UTIL	Summarized CPU utilization for data center
VMWARE_DC_CPU_USED	Summarized CPU usage for data center in MHz
VMWARE_DC_MEMORY_UTIL	Summarized memory utilization for data center
VMWARE_DC_MEMORY_USED	Summarized memory usage for data center in GB
VMWARE_DC_MEMORY_TOTAL	Summarized total memory of data center in GB
VMWARE_DC_DATASTORE_UTIL	Summarized datastore utilization for data center
VMWARE_DC_DATASTORE_FREE	Summarized free disk space of data center in GB
VMWARE_DC_DATASTORE_TOTAL	Summarized total disk space of data center in GB

Metrics Collected by VI-VMwareHardwareHealthCollector Policy

The following collection of metrics are related to the hardware health of the host machine.

CODA\\VISPI\\FAN_HEALTH

Metric Name	Description
VMWARE_FAN_HOST_NAME	Name of the host machine
VMWARE_FAN_HOST_UUID	Universally Unique Identifier of the host machine.
VMWARE_FAN_ELEMENT_NAME	User-friendly name of the fan
VMWARE_FAN_HEALTH_STATE	Current health of the fan
VMWARE_FAN_OPERATIONAL_STATUS	Current statuses of the fan.

CODA\\VISPI\\ETHERNETPORT_HEALTH

Metric Name	Description
VMWARE_ETHERNETPORT_HOST_ NAME	Name of the host machine
VMWARE_ETHERNETPORT_HOST_ UUID	Universally Unique Identifier of the host machine.
VMWARE_ETHERNETPORT_ELEMENT_ NAME	User-friendly name of the ethernet port.
VMWARE_ETHERNETPORT_ DESCRIPTION	Textual description of the ethernet port
VMWARE_ETHERNETPORT_NETWORK_ ADDRESSES	Ethernet/802.3 MAC addresses formatted as twelve hexadecimal digits (for example, `010203040506`), with each pair representing one of the six octets of the MAC address in *canonical* bit order.
VMWARE_ETHERNETPORT_ENABLED_ STATE	Enabled and disabled states of the ethernet port
VMWARE_ETHERNETPORT_HEALTH_ STATE	Current health of the ethernet port
VMWARE_ETHERNETPORT_ OPERATIONAL_STATUS	Current statuses of the ethernet port.

CODA\\VISPI\\SENSOR_HEALTH

Metric Name	Description
VMWARE_SENSOR_HOST_NAME	Name of the host machine.
VMWARE_SENSOR_HOST_UUID	Universally Unique Identifier of the host machine.
VMWARE_SENSOR_PART_ COMPONENT	No description available.
VMWARE_SENSOR_SENSOR_NAME	Label by which the sensor is known
VMWARE_SENSOR_SENSOR_TYPE	Type of the sensor, e.g. voltage or temperature sensor.
VMWARE_SENSOR_HEALTH_STATE	Current health of the sensor.
VMWARE_SENSOR_OPERATIONAL_ STATUS	Current statuses of the sensor.
VMWARE_SENSOR_CURRENT_ READING	Current readings by the sensor.

CODA\\VISPI\\PROCESSOR_HEALTH

Metric Name	Description
VMWARE_PROCESSOR_HOST_NAME	Name of the host machine.
VMWARE_PROCESSOR_HOST_UUID	Universally Unique Identifier of the host machine.
VMWARE_PROCESSOR_ELEMENT_NAME	User-friendly name of the processor.
VMWARE_PROCESSOR_FAMILY	Processor family type.
VMWARE_PROCESSOR_MODEL	General name (model type) of the processor.
VMWARE_PROCESSOR_CURRENT_CLOCK_SPEED	Current speed (in MHz) of the processor.
VMWARE_PROCESSOR_MAX_CLOCK_SPEED	Maximum speed (in MHz) of the processor.
VMWARE_PROCESSOR_EXTERNAL_BUS_CLOCK_SPEED	Speed (in MHz) of the external bus interface (also known as the front side bus).
VMWARE_PROCESSOR_STEPPING	Revision level of the processor within the processor family.
VMWARE_PROCESSOR_NUM_ENABLED_CORES	Number of processor cores enabled for the processor.
VMWARE_PROCESSOR_HEALTH_STATE	Current health of the processor.
VMWARE_PROCESSOR_OPERATIONAL_STATUS	Current statuses of the processor.

CODA\\VISPI\\MEMORY_HEALTH

Metric Name	Description
VMWARE_MEMORY_HOST_NAME	Name of the host machine.
VMWARE_MEMORY_HOST_UUID	Universally Unique Identifier of the host machine.
VMWARE_MEMORY_ELEMENT_NAME	User-friendly name of the physical memory.
VMWARE_MEMORY_CAPACITY	Total capacity of the physical memory, in byte
VMWARE_MEMORY_MAX_MEMORY_SPEED	Maximum speed of the physical memory, in nanoseconds.
VMWARE_MEMORY_HEALTH_STATE	Current health of the physical memory.
VMWARE_MEMORY_OPERATIONAL_STATUS	Current statuses of the physical memory.

CODA\\VISPI\\CHASSIS_HEALTH

Metric Name	Description
VMWARE_CHASSIS_HOST_NAME	Name of the host machine.
VMWARE_CHASSIS_HOST_UUID	Universally Unique Identifier of the host machine.
VMWARE_CHASSIS_ELEMENT_NAME	User-friendly name of the chassis.
VMWARE_CHASSIS_DESCRIPTION	Textual description of the chassis.
VMWARE_CHASSIS_UUID	UUID of the chassis.
VMWARE_CHASSIS_MANUFACTURER	Name of the company that manufactured the chassis.
VMWARE_CHASSIS_MODEL	General name (model type) of the chassis.
VMWARE_CHASSIS_POWERON_ STATUS	Power On status of the chassis.
VMWARE_CHASSIS_HEALTH_STATE	Current health of the chassis.
VMWARE_CHASSIS_OPERATIONAL_ STATUS	Current statuses of the chassis.

Metrics Collected by VI-IBMHMCDataCollector Policy

The metrics are related to the AIX Frames.

CODA\\VISPI\\FRAME_CONFIGURATION

Metric Name	Description
HMC_NAME	Name of the HMC
FRAME_NAME	Name of the frame.
FRAME_SERIAL_NO	Serial number of the frame.
FRAME_MODEL_TYPE	Hardware model type of the frame.
FRAME_IP	IP address of the frame.
FRAME_MEM_CONFIG	Total amount of configurable memory available on the frame.
FRAME_MEM_AVAIL	Total amount of unassigned memory available on the frame.
FRAME_PROC_CONFIG	Total number of configurable processing units available on the frame.
FRAME_PROC_AVAIL	Total number of unassigned processing units available on the frame.

The following metrics are related to the LPARs

CODA\\VISPI\\LPAR_CONFIGURATION

Metric Name	Description
HMC_NAME	Name of the HMC
FRAME_NAME	Name of the frame.
FRAME_SERIAL_NO	Serial number of the frame.
FRAME_MODEL_TYPE	Hardware model type of the frame.
LPAR_NAME	Name of the LPAR.
LPAR_MEM_CONFIG	Total amount of memory assigned to the LPAR.
LPAR_PROC_CONFIG	Total number of processing units assigned to the LPAR.

Policies which work on ESX, ESXi, or vCenter

The following table lists the policies which work on ESX, ESXi, or vCenter.

Note: It is mandatory to deploy the dependent policy first and then the actual policy on the node.

Policy Name	Target node type to be set on vMA	Description	Dependent Policy
Performance Policies			
VI-VMware DCDataCollector	vCent-er	This policy collects data about the CPU, memory, and datastore performance data for the VMware datacenters and logs it in CODA.	None
VI-VMware DCCPUUtilMonitor	vCent-er	This policy monitors the aggregate CPU utilization at the VMware datacenter level based on the data logged in CODA by the VI-VMwareDCDataCollector policy.	VI-VMware DCDataCollector
VI-VMware DCMe-moryUtilMonitor	vCent-er	This policy monitors the aggregate memory utilization at the VMware datacenter level based on the data logged in CODA by the VI-VMwareDCDataCollector policy.	VI-VMware DCDataCollector

Policy Name	Target node type to be set on vMA	Description	Dependent Policy
VI-VMware DCDa-taStoreUtilMonitor	vCent-er	This policy monitors the aggregate data store (disk space) utilization at the VMware datacenter level based on the data logged in CODA by the VI-VMwareDCDataCollector policy.	VI-VMware DCDataCollector
VI-VmWareGuest CPUEntlUtilMonitor-AT	ESX or ESXi	This policy calculates the current CPU utilization (in percentage) of VMware ESX/ESXi servers.	None
VI-VMwareNetif InbyteBaseline-AT	ESX or ESXi	This policy monitors the network interface in-byte or in-packet rate for a network interface in a given interval.	None
VI-VMwareNetif OutbyteBaseline-AT	ESX or ESXi	This policy monitors the network interface out-byte or out-packet rate for a network interface in a given interval.	None
VI-VMware HostNICMonitor	ESX or ESXi	This policy monitors the performance of the Network Interface Cards installed on each ESX/ESXi server.	None
VI-VMwareVMMemory PerformanceMonitor	ESX or ESXi	This policy monitors the memory performance of the virtual machines. It compares the memory utilized by the virtual machine against the amount of virtual memory entitled to it.	None
VI-VMwareHostMemory HealthMonitor	ESX or ESXi	This policy monitors the health of the host machines on VMware ESX/ESXi servers in terms of memory utilization. It can be used to monitor the availability or utilization of the memory on the host machine.	None
VI-VMware-HostsMemory UtilMonitor-AT	ESX or ESXi	This policy calculates the total host memory utilization (including Service Console's memory utilization) by all active VMs under the host VMware ESX/ESXi servers.	None
VI-VMwareTotal VMMe-moryUtilMonitor	ESX or ESXi	This policy monitors the total memory utilization (in percentage) by all the active VMs on VMware ESX/ESXi server.	None
VI-VMwareVMFS	ESX	This policy collects data about the disk	None

Policy Name	Target node type to be set on vMA	Description	Dependent Policy
DataCollector	or ESXi	space utilization, LUN latency, and disk throughput on the Virtual Machine File System (VMFS) and logs it in CODA.	
VI-VMFSRead LatencyMonitor	ESX or ESXi	This policy sends alert messages to the HPOM console based on the data logged in CODA by the VI-VMwareVMFSDataCollector policy.	VI-VMware VMFSDa-taCollector
VI-VMFSWrite LatencyMonitor	ESX or ESXi	This policy sends alert messages to the HPOM console based on the data logged in CODA by the VI-VMwareVMFSDataCollector policy.	VI-VMware VMFSDa-taCollector
VI-VMware-DiskErrorMonitor	ESX or ESXi	This policy monitors the number of disk bus resets and number of disk commands that quit. It sends alert messages to the HPOM console based on the data logged in CODA by the VI-VMwareVMFSDataCollector policy.	None
VI-VMwareDisk ThroughputMonitor	ESX or ESXi	This policy monitors the disk-read throughput rate and the disk- write throughput rate. It sends alert messages to the HPOM console based on the data logged in CODA by the VI-VMwareVMFSDataCollector policy.	None
Hardware Monitoring Policies			
VI-VMwareHost Pro-cessorHealthMonitor	vCent-er	This policy monitors the health of the host machine's processor based on the data logged in CODA by the VI-VMwareHardwareHealthCollector policy.	VI-VMware-Hardware HealthCollector
VI-VMwareHostPhysical MemoryHealthMonitor	vCent-er	This policy monitors the health of the host machine's physical memory based on the data logged in CODA by the VI-VMwareHardwareHealthCollector policy.	VI-VMware-Hardware HealthCollector
VI-VMwareHostEthernet PortHealthMonitor	vCent-er	This policy monitors the health of the host machine's ethernet port based on the data logged in CODA by the VI-VMwareHardwareHealthCollector policy.	VI-VMware-Hardware HealthCollector
VI-VMwareHost	vCent-	This policy monitors the health of the host	VI-

Policy Name	Target node type to be set on vMA	Description	Dependent Policy
FanHealthMonitor	er	machine's fan based on the data logged in CODA by the VI-VMwareHardwareHealthCollector policy.	VMware-Hardware HealthCollector
VI-VMwareHost ChassisHealthMonitor	vCent-er	This policy monitors the health of the host machine's chassis based on the data logged in CODA by the VI-VMwareHardwareHealthCollector policy.	VI-VMware-Hardware HealthCollector
VI-VMwareHost SensorHealthMonitor	vCent-er	This policy monitors the health of the host machine's sensor based on the data logged in CODA by the VI-VMwareHardwareHealthCollector policy.	VI-VMware-Hardware HealthCollector
Event Monitoring Policy			
VI-VMware EventMonitor	ESX or ESXi or vCent-er	This policy monitors crucial events from the ESX/ESXi hosts or vCenter managed by vMA.	VI-VMware EventTypes

Note: In case of Collector policies, the data is stored under the DataSource VISPI and not under SCOPE.

Additional Monitoring Features Supported for ESX/ESXi or vCenter

The following table summarizes the additional monitoring features supported by VISPI with respect to ESX/ESXi or vCenter.

Additional features supported by VISPI	ESX/ESXi	vCenter
Event Monitoring	VmSuspendedEvent:VmResumingEvent VmPoweredOffEvent:Vm	DrsEnteredStandbyModeEvent:DrsExitedStandbyModeEvent DrsDisabledEvent:Drs

Additional features supported by VISPI	ESX/ESXi	vCenter
	PoweredOnEvent VmRenamedEvent VmRemovedEvent NotEnoughResources ToStartVmEvent VmBeingHotMigratedEvent VmDiskFailedEvent VmNoNetworkAccessEvent VmUuidChangedEvent VmUuidConflictEvent VmOrphanedEvent	EnabledEvent DrsVmPoweredOnEvent DrsVmMigratedEvent HostRemovedEvent HostShutdownEvent VmFailoverFailed VmFailedMigrateEvent VmMigratedEvent The operations carried out from the vCenter can be monitored by adding vCenter to the vMA and deploying the Event Monitor policy on the node.
Data Center Monitoring	Need not deploy if the environment has only ESX/ESXi configured.	It monitors the individual VMware datacenter level CPU, memory, and datastore performance-data, as there can be multiple datacenters under a single vCenter.

We appreciate your feedback!

If an email client is configured on this system, by default an email window opens when you click on the bookmark “Comments”.

In case you do not have the email client configured, copy the information below to a web mail client, and send this email to **docfeedback@hp.com**

Product name:

Document title:

Version number:

Feedback: