HP Operations Smart Plug-in for Virtualization Infrastructure

for HP Operations Manager for Windows®, UNIX®, and Linux operating systems

Software Version: 1.50

User Guide

Document Release Date: September 2009
Software Release Date: September 2009

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 Notices

Trademark Notices

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

UNIX® is a registered trademark of The Open Group.

Motif® is a registered trademark of the Open Software Foundation in the U.S. and other countries.

Adobe®, Acrobat® and PostScript® are trademarks of Adobe Systems Incorporated.

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:

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

1 Introduction

The HP Operations Smart Plug-in for Virtualization Infrastructure (Virtualization Infrastructure SPI) is a software application that integrates with HP Operations Manager (HPOM) and extends HPOM's management scope to include monitoring for the enterprise-wide distributed virtual infrastructure on Microsoft Windows and Linux operating systems.

The SPI monitors the performance, capacity, utilization, availability, and resource consumption of the host machines, virtual machines, and resource pools. For more information on which operating-system versions are supported by the Virtualization Infrastructure SPI, see the *HP Operations Smart Plug-in for Virtualization Infrastructure Release Notes*.

The Virtualization Infrastructure SPI is configured such that it can be used by other HP Operations Smart Plug-ins. It is integrated with the Systems Infrastructure SPI to provide infrastructure discovery feature in virtualized and single system environments. The Virtualization Infrastructure SPI integrates with other HPOM products such as HP Performance Manager, HP Performance Agent, and HP Reporter.

2 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.

The Virtualization Infrastructure SPI helps you monitor virtualization platforms running on Windows, or Linux operating system. The SPI installation/configuration adds the following components to the HPOM console.

Map View on HPOM for Windows

After you add a node to the HPOM server, the Systems Infrastructure SPI service discovery policy is automatically deployed to the nodes. Once the discovery policy identifies the node as a VMware vMA or Hyper-V node, it triggers the autodeployment of the Virtualization Infrastructure SPI discovery policy. The Virtualization Infrastructure SPI discovery adds discovered information to the HPOM Services area. This information is used to populate the Virtualization Infrastructure SPI map view for the managed nodes.

The map view displays the real-time status of your infrastructure environment. To view 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. You can see the cause of any problem indicated in your message browser through the Root Cause view, or display the services and system components affected by a problem through the Impacted Services view.

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/Linux

The map view displays the real-time status of your virtual infrastructure environment. To ensure that the operator can view the service map in the HPOM for UNIX and HPOM for Linux Operational UI, run the following commands on the management:

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

where 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 these.

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

To view the map view:

1. Launch the HPOM Operational UI.
2. Log on using your user name and password.

3 Select **Services** → **Virtualization Infrastructure** → **Show Graph**, to view 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.

Policies

In case of 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. In case of HPOM for UNIX/Linux, the discovery policy does not automatically deploy policies to the nodes. You can manually deploy them.

The Virtualization Infrastructure SPI policies begin with VI for easy identification and modification. 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 to collect and defines the collection interval. The collection intervals can occur at 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 mean for entering user-defined metrics.

The Virtualization Infrastructure SPI provides a set of pre-configured policies to help the system administrators efficiently monitor the virtual infrastructure. These policies can easily be customized to suit specific needs. For information about the policies provided by Virtualization Infrastructure SPI, see Virtualization Infrastructure SPI Policies

Graphs

The Virtualization Infrastructure SPI enables you to view 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 view, 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 view 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.

Reports

You can integrate the Virtualization Infrastructure 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 view 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, or Linux operating system), you can view the reports on HP Reporter system. For more information on 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.

3 Virtualization Infrastructure SPI Policies and Tools

The Virtualization Infrastructure 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 Virtualization Infrastructure SPI helps you monitor in Windows and Linux 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 unexpected behavior or cause the policy to fail

The folder SPI for Infrastructure group contains a subgroup *en* arranged according to the language English.

For HPOM for Windows, the policy group on the console is:

Policy management → Policy groups → SPI for Infrastructure → en → Virtualization Infrastructure

For HPOM for UNIX/ Linux, the policy group on the console/ Administration UI is:

Policy Bank → SPI for Infrastructure → en → Virtualization Infrastructure

Auto Discovery Policy

The Virtualization Infrastructure SPI discovers virtual machines and resource pools that are available on Hyper-V, ESX, or ESXi host server nodes and automatically configures the service hierarchy. After you add a node to the HPOM server, the Systems Infrastructure SPI service discovery policy is automatically deployed to the nodes. Once the Systems Infrastructure SPI discovery identifies the node as a VMware vMA or Hyper-V node that hosts virtual machines, it automatically triggers the auto-deployment of the VI-Discovery policy.

The virtual machines are not added in the HPOM node bank by default during virtualization discovery although messages to add guests hosted by the ESX and ESXi systems are generated. You can ignore these messages. The auto-addition of virtual machines in the node bank is disabled to prevent a large number of virtual machines getting added in batch causing poor performance at the time of discovery. By default the XPL configuration setting on the HPOM management server `infraspi.AutoAdd_Guests` is set to `false`. You can set the value to `true` and re-run the action to enable the auto-addition feature. A convenient time may be chosen for running the auto-action.

The Virtualization Infrastructure SPI discovery adds discovered information to the HPOM Services area.

Discovering services manually

The default policy group for the autodiscovery policy is:

SPI for Infrastructure → **en** → **Virtualization Infrastructure** → **Auto Discovery** on the console tree.

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**.

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. The default policy group for the availability policies is:

SPI for Infrastructure → **en** → **Virtualization Infrastructure** → **Availability**

VM State Monitor Policy

VI-StateMonitor

This policy can be deployed on the Microsoft Hyper-V and VMware vMA servers. The policy monitors and reports the state of the host servers and the guest virtual machines configured on them. It sends following message alerts:

- Major alert message if the virtual machine is in any of the following states:
  - Stuck
  - Crash
  - Hung
- Warning (issue) alert message if the virtual machine is in any of the following states:
  - Unknown
  - Deleted
- Warning (non-issue) alert message if the virtual machine is in any of the following states:
  - Disabled
  - Paused
  - Suspended

  To receive warning alert messages for these states, enable the monitoring by setting the script parameter **`AlertOnPlannedOutage=True`**. By default the value is false.

- Warning (Transient-states) alert message if the virtual machine state is in any of the following states:
  - Starting
  - Snapshoting
  - Migrating
  - Saving
  - Stopping
  - Pausing
  - Resuming

  The VM state monitor policy checks for these states. If it finds a virtual machine in any of these states for more than 60 minutes, it will send out an alert.
- Normal
  - Enabled

Metrics Used	BYLS_LS_ROLE BYLS_LS_STATE BYLS_LS_NAME BYLS_DISPLAY_NAME BYLS_LS_UUID
Supported Platforms	Microsoft Hyper-V VMware vMA
Script-Parameter	**Description**
AlertOnPlannedOutage	The value for this parameter can be **`true`**, **`false`**, or *a specified time range*. • Set the value to **`true`**, to start monitoring if the VMs are in suspended, on, off, enabled, or disabled state. The policy monitors when a VM goes into suspended state and sends and alert message to the HPOM console. • Set the value to **`false`**, to disable monitoring state change for VMs. • Set to **`hh:mm:ss-hh:mm:ss`** format for time bound alerting. In other words, set a time range for monitoring the virtual machines. For example, set **`09:00:00-20:00:00`**, if you want the policy to check for VM state change between 9:00:00 hours to 20:00:00 hours. Specify the time range as per the local time of the vMA or Hyper-V server.
MessageGroup	Enter an appropriate value that will help you identify the messages sent by this policy to the HPOM console.
Debug	Set a non-zero value to start receiving debug messages. These messages are displayed on the console with normal severity.

Host Service Monitor Policy

VI-MSHyperVHostServiceMonitor

This policy monitors the availability of services on the host operating system of the Microsoft Hyper-V server. 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 any service is not running, an alert 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.

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. The default policy group for the policy is:

SPI for Infrastructure → en → Virtualization Infrastructure → Capacity → VMware vMA

VMFS Utilization Monitor Policy

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 uses APIs provided by VMware to retrieve information such as:

- Storage device connected to a particular host
- HBA Device number
- UUID of the host

- Space utilization
- Maximum capacity
- Available space

Supported Platforms	VMware vMA
Script-Parameter	**Description**
SpaceUtilCriticalThreshold	If the disk space utilization is above the specified threshold value, the policy generates a critical severity message.
SpaceUtilMajorThreshold	If the disk space utilization is above the specified threshold value, the policy generates a major severity message.
SpaceUtilMinorThreshold	If the disk space utilization is above the specified threshold value, the policy generates a minor severity message.
SpaceUtilWarningThreshold	If the disk space utilization is above the specified threshold value, the policy generates a warning severity message.
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 a non-zero value to start receiving debug messages. These messages are displayed on the console with normal severity.

Virtual Machine Memory Usage Monitor Policy

VI-VMwareVMMemoryUsage-AT

This policy monitors how much memory is being used by the guest virtual machines and resource pools in MBs. 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 send out 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_MEM_USED BYLS_LS_UUID BYLS_LS_ROLE BYLS_DISPLAY_NAME
Supported Platforms	VMware vMA
Script-Parameter	**Description**
MessageApplication	Enter 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	Enter 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 form normal, at which the policy will send 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 will send 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 will send 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 a non-zero value to start receiving debug messages. These messages are displayed on the console with normal severity.
MessageGroup	Displays the message group for outgoing messages.
MemUsageCutOff	Set a value below which you do not want to monitor the memory usage for virtual guest machines.

Host Disk Usage Monitor Policy

VI-VMwareHostDiskUtilization-AT

The VI-VMwareHostDiskUtilization-AT policy monitors how much of the host operating system disk space is being used by the guest virtual machines and resource pools in MBs. The policy uses a multi-instance baseline for monitoring the disk space 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 policy 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_DISK_UTIL BYLS_LS_UUID BYLS_LS_ROLE BYLS_LS_HOSTNAME
Supported Platforms	VMware vMA
Script-Parameter	**Description**
MessageApplication	Enter 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	Enter 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 form normal, at which the policy will send 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 will send 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 will send 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.
DebugLevel	Set a non-zero value to start receiving debug messages. These messages are displayed on the console with normal severity.
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.

Performance Policies

Performance monitoring helps to preempt performance disruption and identify when the infrastructure issues can threaten service quality. You can use the collected performance data to correlate events across the virtualized infrastructure in order to identify the root cause of a developing performance issue.

Virtualization Infrastructure SPI provides performance policies for Microsoft Hyper-V and VMware vMA platforms.

Host CPU Utilization Monitor Policy for vMA

VI-VMwareHostsCPUUtilizationMonitor

The VI-VMwareHostsCPUUtilizationMonitor 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 out an alert in case of any violations. The default policy group for the policy is:

SPI for Infrastructure → en → Virtualization Infrastructure → Performance → VMware vMA.

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 Platforms	VMware vMA
Script-Parameter	**Description**

MessageGroup	Message group for outgoing messages.
CPUUtilWarningThreshold	Set the threshold value for minimum CPU utilization on the host machine, at which you want to receive a warning severity message.
CPUUtilMinorThreshold	Set the threshold value (greater than the value for *CPUUtilWarningThreshold)* for minimum CPU utilization on the host machine, at which you want to receive a minor severity message.
CPUUtilMajorThreshold	Set the threshold value (greater than the value for *CPUUtilMinorThreshold)* for minimum CPU utilization on the host machine, at which you want to receive a major severity message.
CPUUtilCriticalThreshold	Set the threshold value (greater than the value for *CPUUtilMajorThreshold)* for minimum CPU utilization on the host machine, at which you want to receive a critical severity message.
CPUReadyTimeCriticalThreshold	Set the threshold value for minimum CPU ready time, to the value at which you want to receive a critical severity message.
CPUReadyTimeMajorThreshold	Set the threshold value for minimum CPU ready time, to the value at which you want to receive a major severity message.
CPUReadyTimeMinorThreshold	Set the threshold value for minimum CPU ready time, to the value at which you want to receive a minor severity message.
CPUReadyTimeWarningThreshold	Set the threshold value for minimum CPU ready time, to the value at which you want to receive a warning severity message.
Debug	Set a non-zero value to start receiving debug messages. These messages are displayed on the console with normal severity.
Trace	Set a non-zero value to enable tracing.

Host CPU Utilization Monitor Policy for Hyper-V

VI-HostCPUUtilizationMonitor

The VI-HostCPUUtilizationMonitor policy monitors and maintains information about the CPUs on the Hyper-V host server (managed node). This policy monitors CPU utilization along with ready utilization on the host machine and sends an alert in case of any violation. The default policy group for the policy is:

Metrics Used	BYLS_LS_ROLE BYLS_LS_UUID BYLS_DISPLAY_NAME BYLS_CPU_PHYS_READY_UTIL BYLS_CPU_PHYS_TOTAL_UTIL BYLS_LS_HOST_HOSTNAME BYLS_LS_HOSTNAME BYLS_LS_TYPE
Supported Platforms	Microsoft Hyper-V
Script-Parameter	**Description**
MessageGroup	Message group for outgoing messages.
CPUUtilWarningThreshold	Set the threshold value for minimum CPU utilization on the host machine, at which you want to receive a warning severity message.
CPUUtilMinorThreshold	Set the threshold value (greater than the value for *CPUUtilWarningThreshold)* for minimum CPU utilization on the host machine, at which you want to receive a minor severity message.
CPUUtilMajorThreshold	Set the threshold value (greater than the value for *CPUUtilMinorThreshold)* for minimum CPU utilization on the host machine, at which you want to receive a major severity message.
CPUUtilCriticalThreshold	Set the threshold value (greater than the value for *CPUUtilMajorThreshold)* for minimum CPU utilization on the host machine, at which you want to receive a critical severity message.
RunQueueLengthCriticalThreshold	The threshold is expressed as the process queue length. In other words it is the number of processes waiting for CPU time. Set the threshold value for minimum number of processes in the queue at which you want to receive a critical severity message.
RunQueueLengthMajorThreshold	Set the threshold value for minimum number of processes in the queue at which you want to receive a major severity message
RunQueueLengthMinorThreshold	Set the threshold value for minimum number of processes in the queue at which you want to receive a minor severity message

RunQueueLengthWarningThreshold	Set the threshold value for minimum number of processes in the queue at which you want to receive a warning severity message
Debug	Set a non-zero value to start receiving debug messages. These messages are displayed on the console with normal severity.
Trace	Set a non-zero value to enable tracing.

CPU Entitlement Utilization Monitor Policy

VI-VMCpuEntitlementUtilizationMonitor-AT

This policy calculates (as a percentage) the current CPU utilization and compares it to the minimum CPU entitlement utilization of virtual machines. The policy uses automatic threshold determination to automatically calculate threshold values according to the memory utilization of the virtual machines on previous days. The default policy group for the policy is:

SPI for Infrastructure → en → Virtualization Infrastructure → Performance

Metrics Used	BYLS_CPU_ENTL_UTIL BYLS_LS_NAME BYLS_LS_UUID BYLS_LS_STATE BYLS_DISPLAY_NAME
Supported Platforms	Microsoft Hyper-V VMware vMA
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	Enter 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 minimum value of the CPU utilization as indicated by the metric.
WarningDeviations	Displays the number of standard deviation away form normal, at which the policy will send 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 will send 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 will send 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 a non-zero value to start receiving debug messages. These messages are displayed on the console with normal severity.
Trace	Set a non-zero value to enable tracing.

VM Network Interface In-Byte Rate Policy

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. The default policy group for the policy is:

SPI for Infrastructure → en → Virtualization Infrastructure → Performance → VMware vMA

Metrics Used	BYLS_NET_IN_BYTE BYLS_NET_IN_PACKET
Supported Platforms	VMware vMA
Script-Parameter	**Description**
MessageApplication	Enter 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	Enter 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 will send 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 will send 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 will send 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.
DebugLevel	Set a non-zero value to start receiving debug messages. These messages are displayed on the console with normal severity.
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.
Trace	Set a non-zero value to enable tracing.

VM Network Interface Out-Byte Rate Policy

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. The default policy group for the policy is:

SPI for Infrastructure → en → Virtualization Infrastructure → Performance → VMware vMA

Metrics Used	BYLS_NET_OUT_BYTE BYLS_NET_OUT_PACKET
Supported Platforms	VMware vMA
Script-Parameter	**Description**

MessageApplication	Enter 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	Enter 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 will send 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 will send 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 will send 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 a non-zero value to start receiving debug messages. These messages are displayed on the console with normal severity.
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.
Trace	Set a non-zero value to enable tracing.

Virtual Machine Memory Performance Monitor Policy

VI-VMwareVMMemoryPerformanceMonitor

The VI-VMMemoryPerformanceMonitor 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 sends out an alert to the HPOM console. The message severity can be major, minor, or warning depending upon the level of threshold violated. The default policy group for the policy is:

Metrics Used	BYLS_DISPLAY_NAME BYLS_MEM_USED BYLS_LS_UUID BYLS_LS_ROLE BYLS_MEM_BALLOON_USED BYLS_MEM_ENTL_MIN BYLS_MEM_ENTL BYLS_LS_HOSTNAME
Supported Platforms	VMware vMA
Script-Parameter	**Description**
VMSwapUtilWarningThreshold	Displays the swap utilization level for the virtual machines. Set the threshold value for minimum swap memory utilization on the virtual machine, at which you want to receive a warning severity message.
VMSwapUtilMinorThreshold	Displays the swap utilization level for the virtual machines. Set the threshold value (greater than the value of *VMSwapUtilWarningThreshold)* for minimum swap memory utilization on the virtual machine, at which you want to receive a minor severity message.
VMSwapUtilMajorThreshold	Displays the swap utilization level for the virtual machines. Set the threshold value (greater than the value of *VMSwapUtilMinorThreshold)* for minimum swap memory utilization on the virtual machine, at which you want to receive a major severity message.
DebugLevel	Set a non-zero value to start receiving debug messages. These messages are displayed on the console with normal severity.

Host Memory Health Monitor Policy

VI-VMwareHostMemoryHealthMonitor

The VI-HostMemoryHealthMonitor policy monitors the health of the host machines on VMware vMA 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 VI-VMwareHostMemoryHealthMonitor sends out an alert to the HPOM console. The message severity can be major, minor, or warning depending upon the level of threshold violated The default policy group for the policy is:

SPI for Infrastructure → en → Virtualization Infrastructure → Performance → VMware vMA.

Metrics Used	BYLS_DISPLAY_NAME BYLS_LS_UUID BYLS_MEM_PHYS_UTIL BYLS_LS_ROLE BYLS_MEM_HEALTH BYLS_LS_HOSTNAME
Supported Platforms	VMware vMA
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.
HostMemHealthWarningThreshold	Displays the host memory utilization level. Set the threshold value in percentage for minimum memory utilization on the host machine, at which you want to receive a warning severity message.
HostMemHealthMinorThreshold	Displays the host memory utilization level. Set the threshold value in percentage (greater than the value of *HostMemHealthWarningThreshold)* for minimum memory utilization on the host machine, at which you want to receive a minor severity message.
HostMemHealthMajorThreshold	Displays the host memory utilization level. Set the threshold value in percentage (greater than the value of *HostMemHealthMinorThreshold)* for minimum memory utilization on the host machine, at which you want to receive a major severity message.
DebugLevel	Set a non-zero value to start receiving debug messages. These messages are displayed on the console with normal severity.

Event Monitoring Policies

The event monitoring policies monitor the crucial system events for the hosts managed by vMA. These policies can be broadly classified into event collector policy & event monitor policies. The event collector policy reads critical virtual machine events and records them into a logfile `vmeventlist.log`. The event monitor policies read the logfile `vmeventlist.log` and look for specific patterns that are of user's interest.

The default policy group for event monitoring policies is:

Event Collector Policy

VI-VMEventCollector

This policy reads the VMware APIs for information regarding critical virtual machine events and records them into a logfile `vmeventlist.log`. The policy records the events from multiple hosts managed by vMA. This logfile is used as an input for event monitor policies.

The event collection happens for the collection interval set in the policy. The default collection interval is 15 minutes. For the first interval the policy reads and records all events from the beginning of that day. Subsequently it records data from the last polled time.

After deploying event collector policy, wait for at least one collection interval before deploying other event monitor policies. This is to let the event collector policy create the vmeventlist.log file.

If you deploy the event monitor policies before the first interval of collector policy is over, the following message is generated: `Logfile /var/opt/OV/tmp/vispi/vmeventlist.log doesn't exist. Treating as empty. (OpC30-108)`. You can ignore this message. From subsequent intervals the message will not be generated.

VMware Event Type Policy

VI-VMwareEventTypes

You can use this policy to define specific events for monitoring. The events within this policy are commented implying that the VI-VMEventCollector policy collects all events by default. If you want to monitor specific events, you can enable it by un-commenting the appropriate lines. The collector policy reads the configuration file and collect events of selected event types.

DRS Event Policy

VI-VMwareDRSEvent

The policy monitors the log file `/var/opt/OV/tmp/vispi/vmeventlist.log` and alerts in case of any occurrence of DRS related events. The default polling interval is 5 minutes.

This policy checks for the following conditions:

Condition	Description
DRS entered standby mode event	Checks for error conditions that match the *DRS put <@.server> into standby mode* pattern in the log file. If any matches are found, the policy sets the node in outage mode and sends a message with warning severity to the HPOM console with the appropriate message attributes.
DRS entering standby mode event	Checks for error conditions that match the *DRS is putting <@.server> into standby mode* pattern in the log file. If any matches are found, the policy sends a message with normal severity to the HPOM console with the appropriate message attributes.

DRS VM powered on event	Checks for error conditions that match the *DRS powered On <@.vm> on <@.server> in <@.datacenter>* pattern in the log file. If any matches are found, the policy sends a message with normal severity to the HPOM console with the appropriate message attributes.
DRS exiting standby mode event	Checks for error conditions that match the *DRS is moving <@.hostname> out of standby mode* pattern in the log file. If any matches are found, the policy sends a message with normal severity to the HPOM console with the appropriate message attributes.
DrsExitedStandbyModeEvent	Checks for error conditions that match the *DRS moved <@.server> out of standby mode* pattern in the log file. If any matches are found, the policy sends a message with normal severity to the HPOM console with the appropriate message attributes.
DRS disabled event	Checks for error conditions that match the *Disabled DRS on cluster <@.cluster> in datacenter <@.datacenter>* pattern in the log file. If any matches are found, the policy sends a message with minor severity to the HPOM console with the appropriate message attributes.
DRS enabled event	Checks for error conditions that match the *Enabled DRS on <@.cluster> with automation level <@.level> in <@.datacenter>* pattern in the log file. If any matches are found, the policy sends a message with normal severity to the HPOM console with the appropriate message attributes.
DRS VM migrate event	Checks for error conditions that match the *DRS migrated <@.vm> from <@.sourcehost> to <@.desthost> in cluster <@.cluster> in <@.datacenter>* pattern in the log file. If any matches are found, the policy sends a message with normal severity to the HPOM console with the appropriate message attributes.

Rename Event Policy

VI-VMwareRenameEvent

This policy monitors the log file `/var/opt/OV/tmp/vispi/vmeventlist.log` and alerts in case of any rename events. The default polling interval is 5 minutes.

This policy checks for the following conditions:

Condition	Description
VM renamed event	Checks for error conditions that match the *Renamed <@.vm> from <@.oldName> to <@.newName> in <@.datacenter>* pattern in the log file. If any matches are found, this condition sends a message with warning severity to the HPOM console with the appropriate message attributes.

VM Creation or Removal Event Policy

VI-VMwareVMCreationRemovalEvent

This policy monitors the log file `/var/opt/OV/tmp/vispi/vmeventlist.log` and alerts whenever a VM is created or removed. The default polling interval is 5 minutes.

This policy checks for the following conditions:

Condition	Description
VM created event	Checks for error conditions that match the *Created <@.vm> on <@.server> in <@.datacenter>* pattern in the log file. If any matches are found, this condition sends a message with normal severity to the HPOM console with the appropriate message attributes.
VM removed event	Checks for error conditions that match the *Removed <@.vm> on <@.server> from <@.datacenter>* pattern in the log file. If any matches are found, this condition sends a message with minor severity to the HPOM console with the appropriate message attributes.

VM Powered On or Powered Off Event Policy

VI-VMwareVMPoweredOnOffEvent

This policy monitors the log file `/var/opt/OV/tmp/vispi/vmeventlist.log` and alerts whenever a VM is powered on or powered off. The default polling interval is 5 minutes.

This policy checks for the following conditions:

Condition	Description
VM powered on event	Checks for error conditions that match the *<@.VM> on <@.Server> in <@.Datacenter> is powered on* pattern in the log file. If any matches are found, this condition sends a message with normal severity to the HPOM console with the appropriate message attributes.
VM powered off event	Checks for error conditions that match the *<@.VM> on <@.Server> in <@.Datacenter> is powered off* pattern in the log file. If any matches are found, this condition sends a message with warning severity to the HPOM console with the appropriate message attributes.

VM Suspended and Resumed Event Policy

VI-VMwareVMSuspendedResumeEvent

This policy monitors the log file `/var/opt/OV/tmp/vispi/vmeventlist.log` and alerts whenever a VM is suspended or resumed. The default polling interval is 5 minutes.

This policy checks for the following conditions:

Condition	Description
VM suspend event	Checks for error conditions that match the *<@.vm> on <@.server> in <@.datacenter> is suspended* pattern in the log file. If any matches are found, this condition sends a message with warning severity to the HPOM console with the appropriate message attributes.
VM resume event	Checks for error conditions that match the *<@.VM> on <@.Server> in <@.Datacenter> is resumed* pattern in the log file. If any matches are found, this condition sends a message with normal severity to the HPOM console with the appropriate message attributes.

Log Monitoring Policies

The Logfile policies monitor the crucial system logs for the Hyper-V hosts managed. The default policy group for these policies is:

SPI for Infrastructure → en → Virtualization Infrastructure → Logs → MS Hyper-V

Hypervisor Administration Logfile Monitoring Policy

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.

The default polling interval is 1 minute. 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

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.

The default polling interval is 1 minute. 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 Logfile Monitoring Policy

VI-MSHyperV_HyperVisorWarnError

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

The default polling interval is 1 minute. The policy looks for all hypervisor error events recorded in the log file.

VMMS Administration Logfile Monitoring Policy

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.

The default polling interval is 1 minute. The policy looks for the following errors recorded in the log file:

- 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.
- An error occurred because the snap shot is corrupted.
- 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.
- Failed to initialize the virtual machine during reset.
- Cannot modify the boot order when the virtual machine is online.
- 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.

VMMS Operational Logfile Monitoring Policy

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.

The default polling interval is 1 minute. The policy looks for the following errors recorded in the log file:

- 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.
- An error occurred because the snap shot is corrupted.
- 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.
- Failed to initialize the virtual machine during reset.
- Cannot modify the boot order when the virtual machine is online.
- 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.

VMMS Logfile Monitoring Policy

VI-MSHyperV_VMMSWarnError

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

The default polling interval is 1 minute. The policy looks for all VMMS error events recorded in the log file.

Hypervisor Worker Administration Logfile Monitoring Policy

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.

The default polling interval is 1 minute. 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.

Hypervisor Worker Operational Logfile Monitoring Policy

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.

The default polling interval is 1 minute. 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.

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.

Launching Tools on HPOM for Windows

Go to **Tools** → **Virtualization Infrastructure** → **VMware** in the console tree. To launch the tool, follow these steps:

1. Double-click the tool.

   Select where to launch this tool window opens.
2. Under the Select one or more nodes/node group/service section, select the host server node to launch the tool.
3. Click **Launch**.

This Edit Parameters page appears.

4 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.

5 Click **Launch**.

The Tool Status windows appears. It displays the list of launched tools and tool output.

Launching Tools on HPOM for UNIX and HPOM for Linux

On HPOM for UNIX server, you can find the tools under **Tool Bank** → **Virtualization Infrastructure** in the Administration UI.

Follow the steps to launch the tool:

1 Right-click the **VMware Host Info** tool, select **Start Customized**.

Start Tool - Customized Wizard window opens.

2 Under the nodes list, select the host server node to launch the tool.

3 On the wizard, click **Get Selections.**

The node is added to the Selected Nodes list.

4 Click **Next.**

5 On the page Specify additional information needed to run the tool, you can specify the additional information or leave the fields blank.

6 Click **Finish**.

The tool output is displayed.

The following tools are provided on HP Operations Manager for Windows and UNIX operating systems:

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.

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.

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.

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 pools hosted on a single system as well. This *Edit Parameters* page does not appear for this tool.

4 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

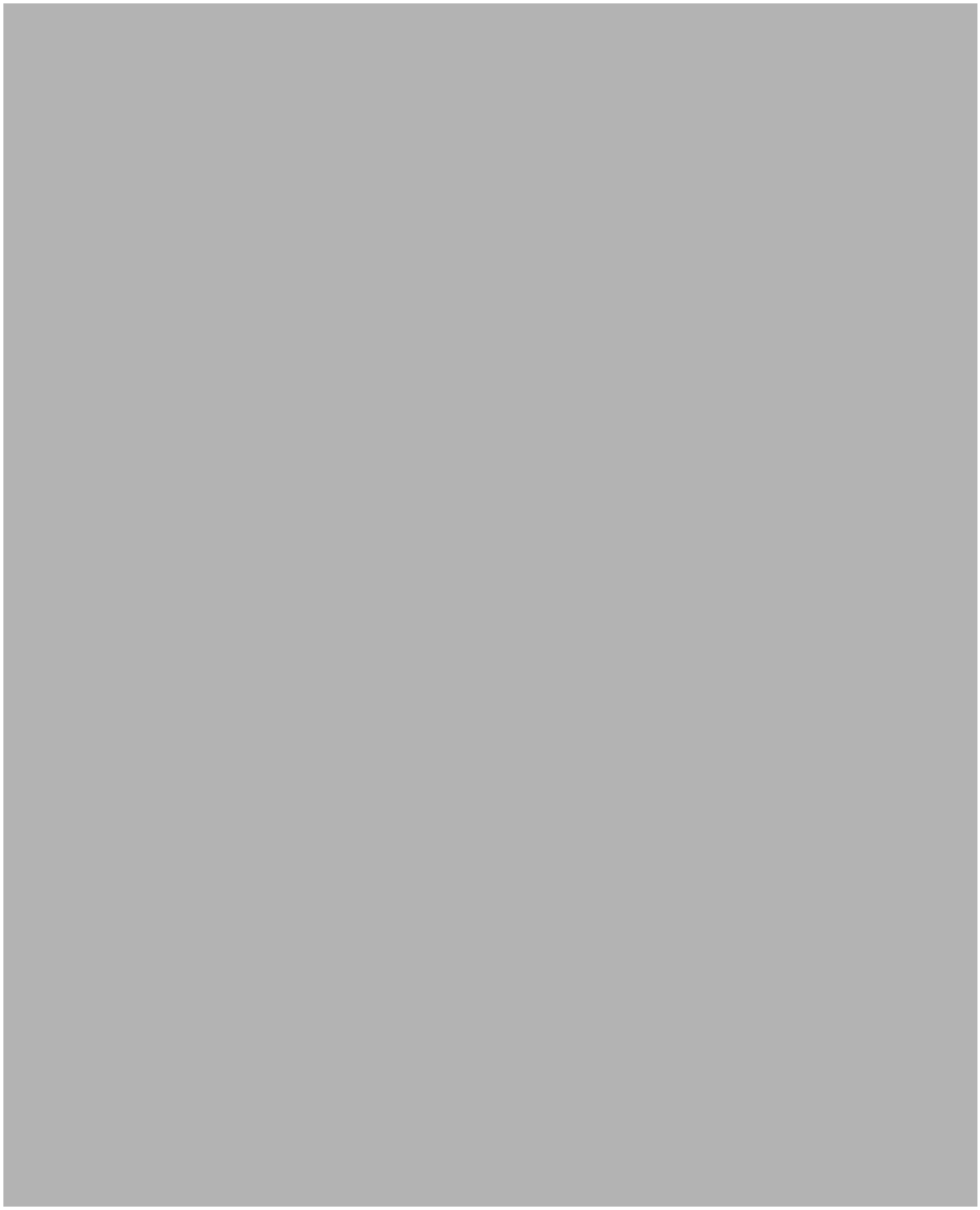
You can access Virtualization Infrastructure SPI reports from the HPOM console. To install HP Reporter package, see the *Infrastructure SPI Installation Guide*.

To view reports for Virtualization Infrastructure SPI from HPOM for Windows, expand **Reports** → **SPI for Infrastructure** → **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. The following is an example report.

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

Figure 1 Example report for Virtualization Infrastructure SPI



The SPI for Virtualization Infrastructure provides the following reports:

Report/ Report Title	Purpose	Platform
Hyper-V Configuration	This report displays the configuration information of the Hyper-V hosts. You can use this report to view and compare the configuration details for Hyper-v hosts.	Microsoft Hyper-V
Hyper-V CPU Utilization	This report displays the physical CPU utilization details of the Hyper-V hosts. You can use this report to view and compare the CPU utilization of the Hyper-v hosts.	Microsoft Hyper-V
vMA Host-Guest 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 vMA
vMA 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 vMA
vMA Memory Utilization	This report displays the physical memory 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 vMA

Report/ Report Title	Purpose	Platform
vMA Ready Utilization	This report displays the ready utilization information of the vMA and the ESX/ESXi servers managed by it. You can use this report to view and compare the ready utilization of ESX/ESXi host machines and the guest virtual machines configured on them.	VMware vMA
vMA Top Busy CPU	This report displays a list of top ten CPU according to the usage. The report sorts and displays the top systems according to the CPU cycles consumed by them during the reporting interval.	VMware vMA
vMA Top Busy Disk	This report displays a list of top ten host machines according to the disk cycles consumed by them during the reporting interval.	VMware vMA
vMA Top Busy Memory	This report displays a list of top ten virtual machines that are reaching the threshold in terms of memory usage. The report sorts and displays the top systems according to the memory cycles consumed by them during the reporting interval.	VMware vMA
vMA Availability	This report displays a list of top ten virtual machines according to the percentage of machine availability or the machine up-time during the reporting interval. It also provides information about the up-time and down-time hours for these machines.	VMware vMA

Virtualization Infrastructure SPI Graphs

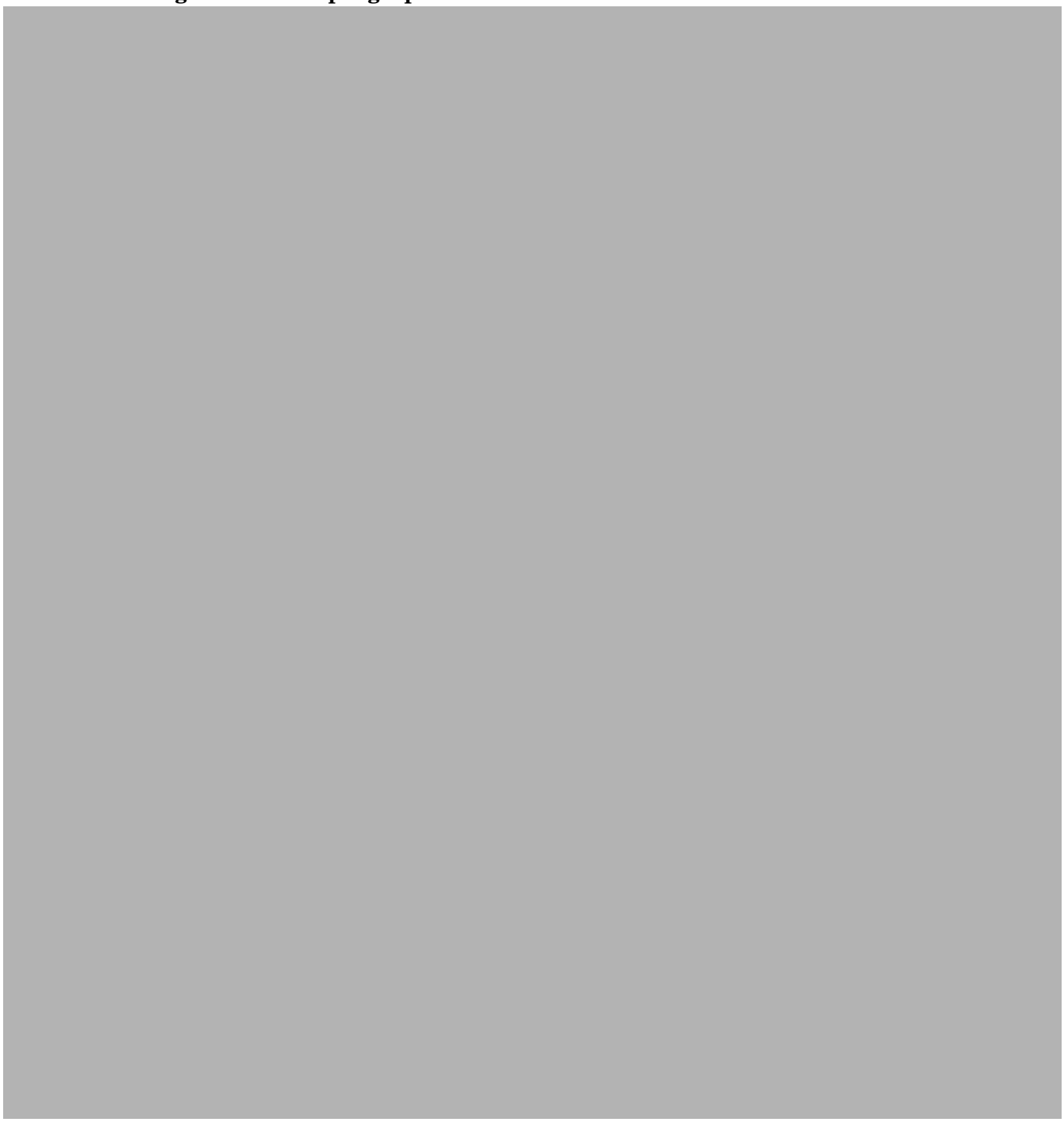
HP Performance Manager generates graphs from near real-time data gathered from the managed nodes. You can access these graphs from the HPOM console if you install HP Performance Manager on an HPOM management server.

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→ InfraSPI → Virtualization.**

To access the graphs on HPOM for UNIX/ Linux, 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 Example graph for Virtualization Infrastructure SPI



The SPI for Virtualization Infrastructure provides the following graphs:

Table 1 Virtualization Infrastructure SPI graphs

Graph/ Graph Title	Purpose
Host Memory Utilization Baseline	This graph shows the host memory utilized by the guest virtual machines.
CPU Entitlement Utilization Baseline	This graph shows the CPU entitlement utilization by the guest virtual machines configured on the host machine.
Guest Memory Utilization	This graph shows the memory utilization for the guest virtual machines.
Host memory utilization	This graph shows the memory utilization for the host machines.
Host disk utilization	This graph shows the disk utilization for the host machines.
CPU Utilization - VMware	This graph shows the CPU utilization for the VMware ESX/ ESXi host machines and the guest virtual machines hosted on them.
Host CPU Utilization - Hypervisor	This graph shows the memory utilization for the Microsoft Hyper-V host machines.
ESX/ ESXi Host - Inward data (MB)	This graph shows the network interface in-bytes or packets on the host machine.
ESX/ ESXi Host - Outward data (MB)	This graph shows the network interface out-bytes or packets on the host machine.
CPU Utilization across ESX, ESXi Hosts	This graph shows the CPU utilization across the VMware ESX/ ESXi host machines.
CPU Utilization across Resource Pools	This graph shows the CPU utilization across the resource pools.
CPU Utilization across Guests	This graph shows the CPU utilization across the guest virtual machines.

5 Troubleshooting

This chapter offers an overview of the Virtualization Infrastructure SPI limitations and issues and covers basic troubleshooting for them.

Advanced Monitoring policies modified in HPOM for UNIX Administrator GUI fail to run after deployment to managed nodes.

Cause: When advanced monitoring policies are edited in GUI mode in HPOM for UNIX policy editor, syntax errors are induced into the perl code module. This causes the policy to fail to execute. 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 for UNIX.

Solution: To edit the settings in the Measurement Threshold policy, use 'Edit in Raw mode' feature of the HPOM for UNIX Administrator GUI to change the policy contents. This requires you to know the syntax of the policy data file.

Discovery procedures and data collection gives error with non-English names.

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 error as they are not recognized by the StoreCollection OvPerl APIs in HP Operations Agent.

Time-out function for VM event collector policy

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.

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.

The Virtualization Discovery does not automatically add nodes

The virtual machines are not added in the HPOM node bank by default during virtualization discovery although messages to add guests hosted by the ESX and ESXi systems are generated. You can ignore these messages. The auto-addition of virtual machines in the node bank is disabled to prevent a large number of virtual machines getting added in batch causing poor performance at the time of discovery. By default the XPL configuration setting on the HPOM management server `infraspi.AutoAdd_Guests` is set to `false`. You can set the value to `true` and re-run the action to enable the auto-addition feature. A convenient time may be chosen for running the auto-action.

Virtualization Infrastructure SPI scripts take longer time to run depending on the retry level set on the vMA system

VMware vMA tries to connect to the host servers added to 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. 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 Certificates not installing 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 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 on port 383 and how to enable it, see *HP Operations Manager Firewall Concepts and Configuration Guide*.