

HP OMi Management Pack for Infrastructure

Software Version: 1.12

HP Operations Manager i for Linux and Windows® operating systems

User Guide

Document Release Date: June 2015
Software Release Date: May 2015



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

© Copyright 2013-2015 Hewlett-Packard Development Company, L.P.

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.

This product includes an interface of the 'zlib' general purpose compression library, which is Copyright © 1995-2002 Jean-loup Gailly and Mark Adler.

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: <https://softwaresupport.hp.com/group/softwaresupport/search-result?keyword=>.

This site requires an HP Passport account. If you do not have one, click the **Create an account** button on the HP Passport Sign in page.

Support

Visit the HP Software Support web site at: <https://softwaresupport.hp.com>

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

HP Software 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 <https://softwaresupport.hp.com> and click **Register**.

To find more information about access levels, go to: <https://softwaresupport.hp.com/web/softwaresupport/access-levels>

HP Software Solutions & Integrations and Best Practices

Visit HP Software Solutions Now at <https://h20230.www2.hp.com/sc/solutions/index.jsp> to explore how the products in the HP Software catalog work together, exchange information, and solve business needs.

Visit the Cross Portfolio Best Practices Library at <https://hpln.hp.com/group/best-practices-hpsw> to access a wide variety of best practice documents and materials.

Contents

Chapter 1: OMi Management Pack for Infrastructure	7
Chapter 2: Getting Started	8
Task 1: Adding Nodes to the BSM 9.2x or OMi 10.x Console	8
Task 2: Deploying the Infrastructure Discovery Aspect	8
Task 3: Verifying the Discovery	10
Task 4: Deploying the Infrastructure Management Templates or Discovery Aspects	10
Data Collection	11
Task 4a: Identifying and Deploying Infrastructure Management Template	11
Task 4b: Deploying Infrastructure Aspects	12
Task 5: Updating the Management Templates and Aspects to a Newer Version	13
Topology Synchronization for Smart Plug-in for Infrastructure	16
Chapter 3: Components of OMi MP for Infrastructure	18
Infrastructure Management Templates	18
Overview of Infrastructure Management Templates	19
How to Access Infrastructure Management Templates	19
How to Deploy Infrastructure Management Templates	20
How to Automatically Assign Management Templates & Aspects	20
Essential Cluster Management Template	22
How to Access the Essential Cluster Management Template	22
Essential IBM Power Management Template	23
How to Access the Essential IBM Power Management Template	23
Essential KVM Management Template	24
How to Access the Essential KVM Management Template	24
Essential Oracle Solaris Management Template	24
How to Access the Essential Oracle Solaris Management Template	25
Essential System Management Template	25
How to Access the Essential System Management Template	25
Essential VMware vSphere Management Template	26
How to Access the Essential VMware vSphere Management Template	26
Essential XEN Management Template	27
How to Access Essential XEN Management Template	27
Extensive IBM Power Management Template	27

How to Access Extensive IBM Power Management Template	28
Extensive KVM Management Template	28
How to Access the Extensive KVM Management Template	28
Extensive Oracle Solaris Management Template	29
How to Access the Extensive Oracle Solaris Management Template	29
Extensive System Management Template	30
How to Access the Extensive System Management Template	30
Extensive VMware vSphere Management Template	31
How to Access the Extensive VMware vSphere Management Template	31
Extensive XEN Management Template	31
How to Access the Extensive XEN Management Template	32
Infrastructure Aspects	32
How to Access the Infrastructure Aspects	33
How to Create Infrastructure Aspects	33
How to Deploy Infrastructure Aspects	35
Systems Infrastructure Aspects	36
User Interface Reference	36
Bandwidth Utilization and Network IOPS	37
CPU Performance	37
General System Services Availability	38
Key System Services Availability	50
Memory and Swap Utilization	55
Remote Disk Space Utilization	55
Resource Bottleneck Diagnosis	56
Server Hardware Fault	58
Space Availability and Disk IOPS	60
System Infrastructure Discovery	61
System Fault Analysis	61
User Logins	66
Virtualization Infrastructure Aspects	69
User Interface Reference	70
IBM Power Guest Health	70
IBM Power Guest Performance	71
IBM Power Host Health	72
KVM Guest Health	73
KVM Guest Performance	74
KVM Host Health	74
Oracle Solaris Guest Health	75
Oracle Solaris Guest Performance	75

Oracle Solaris Host Health	77
VMware Cluster Performance	78
VMware Datastore Performance	80
VMware Host Health	81
VMware Resource Pool Monitor	82
VMware Guest Health	83
VMware vSphere Events	85
Virtual Infrastructure Discovery	86
Xen Guest Health	86
Xen Guest Performance	87
Xen Host Health	87
Cluster Infrastructure Aspects	88
User Interface Reference	88
Cluster Infrastructure Discovery	89
Cluster Strength and Status	89
Parameters	91
Types of Parameters	92
Parameter Flags	92
Infrastructure Parameters	92
Tuning of Parameters	105
Configuration Items and Configuration Item Types	106
CI Types Mapped in OMi	106
Run Time Service Model (RTSM) Views	107
How to Access the RTSM Views	107
Event Type Indicators	119
How to Access the Event Type Indicators (ETIs)	119
Health Indicators	120
How to Access Health Indicators (HIs)	120
Topology Based Event Correlation (TBEC) Rules	129
How to Access the Correlation Rules	129
Mapping Rules	135
Operations Orchestration (OO) Flows	137
Tools	139
How to Access Tools	139
Chapter 4: Customizing OMi MP for Infrastructure	143
Creating Infrastructure Management Templates	143

Editing Infrastructure Management Templates	145
Editing Parameters - Changing the Default Values	145
Editing Aspects - Deleting an Aspect	146
Chapter 5: Troubleshooting	147
Appendix: Graph Templates	148
Systems Infrastructure Graph Templates	148
Virtualization Infrastructure Graph Templates	165
Send Documentation Feedback	178

Chapter 1: OMi Management Pack for Infrastructure

The HP OMi Management Pack for Infrastructure (OMi MP for Infrastructure) works with HP Operations Manager i (OMi) and enables you to seamlessly monitor the various systems operating in a data center environment. It includes Indicators - Health Indicators (HIs), Event Type Indicators (ETIs), and Topology Based Event Correlation (TBEC) Rules that analyze and categorize the events occurring in the systems and report the health status of the systems. It also includes Management Templates for monitoring the availability, health, and performance of individual systems, clusters, and virtual nodes. These Management Templates consists of a wide range of Aspects which enable monitoring the system components.

The Management Templates can be seamlessly deployed by administrators for monitoring the systems in any environment. The Management Templates can also be easily customized by subject matter experts (SMEs) and developers to suit different monitoring requirements.

OMi MP for Infrastructure works with OMi and provides the following salient features:

- Ready-to-deploy, management solutions to suit different monitoring requirements.
- Aspects for creating customized solutions.
- Infrastructure element based deployment and configuration.

Chapter 2: Getting Started

The following section provides step-by-step instructions on how to get started using OMi Management Pack for Infrastructure:


Task 1: Adding Nodes to the BSM 9.2x or OMi 10.x Console

Note: If the Node already exists in Run-time Service Model (RTSM), you can skip this step and proceed to [Task 2](#).

Before you begin monitoring, you need to add the nodes:

1. Open the Monitored Nodes pane from Administration:

On BSM 9.2x, click **Admin > Operations Management > Setup > Monitored Nodes**.

On OMi 10.x, click **Administration > Setup and Maintenance > Monitored Nodes**.
2. In the Node Views pane, click **Predefined Node Filters > Monitored Nodes** and then click  and then click **Computer > <select the OS Type>**. The Create New Monitored Nodes dialog box appears.
3. Specify the Primary DNS Name, IP Address, Operating System, and Processor Architecture of the node and click **OK**.

The newly created node is saved as a CI instance in RTSM.

Note: The node with HP Operations Agent needs to be connected to the HP OMi server and certificate needs to be granted.

Task 2: Deploying the Infrastructure Discovery Aspect

The OMi MP for Infrastructure has three Discovery Aspects and they are: System Infrastructure Discovery, Virtual Infrastructure Discovery, and Cluster Infrastructure Discovery. Depending on the type of node, you can deploy one or a combination of these Aspects.


Type of Node	Aspects to be Deployed
Standalone Node (Windows)	Deploy the System Infrastructure Discovery Aspect.
Standalone Node (Linux)	Deploy the System Infrastructure Discovery Aspect.
Cluster Node	Deploy the System Infrastructure Discovery Aspect first and then deploy the Cluster Infrastructure Discovery Aspect.
ESX Host (Virtual Appliance (VA))	Deploy the Virtual Infrastructure Discovery Aspect.


To discover the CIs on the added managed nodes, you must deploy the Infrastructure Discovery Aspect.

1. Open the Management Templates & Aspects pane:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Management Templates & Aspects**.

On OMi 10.x, click **Administration > Monitoring > Management Templates & Aspects**.

2. In the Configuration Folders pane, click **Configuration Folders > Infrastructure Management**.
3. In the Management Templates & Aspects pane, right-click the respective Infrastructure Discovery Aspect, and then click  **Assign and Deploy Item**. The Assign and Deploy Wizard opens.
4. In the **Configuration Item** tab, click the CI to which you want to deploy the Discovery aspect and then click **Next**.
5. In the **Required Parameters** tab, all mandatory parameters are listed in the management template that do not have a value.
6. In the **All Parameters** tab on BSM 9.2x or **Parameter Summary** tab on OMi 10.x, you can change the default values of the parameters.

Note: In the **All Parameters** tab on BSM 9.2x or **Parameter Summary** tab on OMi 10.x, you can override the default values of any parameter. You can specify a value for each parameter at the Aspect level. By default, parameters defined as expert parameters are not displayed. To display expert parameters, click  **Show Expert Parameters**.

7. (Optional). If you do not want to enable the assignment immediately, clear the **Enable Assigned Objects** check box on BSM 9.2x or **Enable Assignment(s)** check box on OMi 10.x. You can then enable the assignment later using the Assignments & Tuning pane.
8. Click **Finish**.

Note:

- After the Infrastructure Discovery Aspect is deployed, a message stating the Assignment and deployment jobs created appears. To check the status of the deployment jobs:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Deployment Jobs**.

On OMi 10.x, click **Administration > Monitoring > Deployment Jobs**.
- For monitoring VMware vSphere virtualization, IBM Power, and Oracle Solaris zones environment, see *Monitoring using OMi MP for Infrastructure* section in the *OMi Management Pack for Infrastructure Installation Guide*.

Task 3: Verifying the Discovery

After you deploy the Infrastructure Discovery Aspect, you must verify if the CIs are populated in the Top View.

1. Open the Event Perspective pane:

On BSM 9.2x, click **Applications > Operations Management > Event Perspective**.

On OMi 10.x, click **Workspaces > Operations Console > Event Perspective**.

2. In the **Browse Views** tab, select the **HACluster_Infrastructure**, **Sol_Zones_Infrastructure**, **Virtual_Infrastructure** or **Systems_Infrastructure** view.

The CIs are populated in Browse Views.

Note: For more information about the Views, see [Run Time Service Model \(RTSM\) Views](#).

Task 4: Deploying the Infrastructure Management Templates or Discovery Aspects

Note: If you are using the **Monitoring Automation (9.2x) for Composite Applications** license, you can either deploy the Infrastructure Management Templates or Infrastructure Aspects to the CIs. For more information about deploying the Infrastructure Management Template, see [Task 4a: Identifying and Deploying Infrastructure Management Template](#).

Note: If you are using the **Monitoring Automation for Servers** license, you can deploy the Infrastructure Aspects. For more information about deploying the Infrastructure Aspects, see [Task 4b: Deploying Infrastructure Aspects](#).

Data Collection

Frequency (polling interval) at which each Aspect must be monitored is predefined with a default value in a specific frequency parameter. Frequency parameter is an expert parameter that is defined for each of the metrics regardless of whether they are for generating events or not.

Following are the four predefined frequency parameters:

Parameter	Frequency
Very High	5 mins
High	15 mins
Medium	1 hour
Low	24 hours

After Management Templates and Aspects are deployed, the collector is triggered based on the predefined frequency parameter in a specific Aspect. You can modify the default value of the parameter at the following levels:

- During deployment of the Management Template or Aspects using the Management Templates & Aspects pane.
- After deployment using the Assignments & Tuning pane.

For more information about how to modify the parameter values, see [Tuning Parameters](#).


Task 4a: Identifying and Deploying Infrastructure Management Template


You must deploy the Infrastructure Discovery Aspect even if the CIs are already populated by any other source such as SiteScope, DDM and so on. For more information on deploying the Discovery Aspect, see [Task 2: Deploying the Infrastructure Discovery Aspect](#).

To deploy the Infrastructure Management Templates to the CIs, follow these steps:

1. Open the Management Templates & Aspects pane:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Management Templates & Aspects**.

On OMi 10.x, click **Administration > Monitoring > Management Templates & Aspects**.
2. In the Configuration Folders pane, click **Configuration Folders > Infrastructure Management > Infrastructure Management Templates**.
3. In the Management Templates & Aspects pane, click the Management Template that you want to deploy, and then click  **Assign and Deploy Item**. The Assign and Deploy wizard opens.
4. In the **Configuration Item** tab, click the CI to which you want to assign the Management Template, and then click **Next**.
5. In the **Required Parameters** tab, all mandatory parameters are listed in the Management Template that do not have a value.
6. Click **Next** to go to **All Parameters** tab on BSM 9.2x or **Parameter Summary** tab on OMi 10.x.

Note: In the **All Parameters** tab on BSM 9.2x or **Parameter Summary** tab on OMi 10.x, you can override the default values of any parameter. You can specify a value for each parameter at the Aspect level. By default, parameters defined as expert parameters are not displayed. To display expert parameters, click  **Show Expert Parameters**.

7. Click **Next**.
8. *(Optional)*. If you do not want to enable the assignment immediately, clear the **Enable Assigned Objects** check box on BSM 9.2x or **Enable Assignment(s)** check box on OMi 10.x. You can then enable the assignment later using the Assignments & Tuning pane.
9. Click **Finish**.


Task 4b: Deploying Infrastructure Aspects

You **must** deploy the Infrastructure Discovery Aspect even if the CIs are already populated by any other source such as SiteScope, DDM, and so on. For more information on deploying the Discovery Aspect, see [Task 2: Deploying the Infrastructure Discovery Aspect](#).

Note: If you are using the **Monitoring Automation for Composite Applications** license and have assigned the Infrastructure Management Templates to the CI, you can skip this task.

1. Open the Management Templates & Aspects pane:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Management Templates & Aspects**.

On OMi 10.x, click **Administration > Monitoring > Management Templates & Aspects**.
2. In the Configuration Folders pane, click **Configuration Folders > Infrastructure Management**.
3. In the Management Templates & Aspects pane, select the Aspect you want to deploy, and then click  **Assign and Deploy Item**. The Assign and Deploy wizard opens.
4. In the **Configuration Item** tab, select the CI to which you want to assign the Aspect and then click **Next**.
5. In the **Required Parameters** tab, all mandatory parameters are listed in the management template that do not have a value.
6. In the **All Parameters** tab on BSM 9.2x or the **Parameter Summary** tab on OMi 10.x, you can change the default values of the parameters.
7. Click **Next**.
8. *(Optional)*. If you do not want to enable the assignment immediately, clear the **Enable Assigned Objects** check box on BSM 9.2x or **Enable Assignment(s)** check box on OMi 10.x. You can then enable the assignment later using the Assignments & Tuning pane.
9. Click **Finish**.

Task 5: Updating the Management Templates and Aspects to a Newer Version

You can update the existing deployed Management Templates and Aspects to the latest version. The following are two scenarios when you need to update the Management Templates or Aspects:

Use Case 1: You have already deployed Infrastructure Aspects and/or Management Templates to the managed nodes before installing OMi MP for Infrastructure 1.12. We recommend you to use the latest version of Aspects or Management Templates on those nodes.


To update to the latest version, select the Management Templates or Aspects on the managed nodes. Perform the following steps for each Management Template and Aspect assignment on each of the managed nodes:

For BSM 9.2x:

1. Open the Management Templates & Aspects pane and click **Admin > Operations Management > Monitoring > Management Templates & Aspects**.

2. Select 1.100 Infrastructure Aspects and/or Management Templates that has been deployed to nodes.
3. Edit the parameters and redeploy to each of the Node CIs.

For OMi 10.x:


1. Open the Assignments & Tuning pane and click **Administration > Monitoring > Assignments & Tuning**.
2. In the Browse Views pane, select the **Infrastructure_Common** view and select each Node CI where version update is required.
3. Click  **Show Assignments That Require an Update**.

All the Management Templates and Aspects that requires an update are listed.

4. Select each of the Management Templates and Aspects and click  **Update Assigned Item**.

The Update Assigned Item dialog box appears.

5. In the **Update Options** tab, follow these steps:
 - Select the latest version from the **Update to Version** drop down list.
 - If you select **Use parameter values from existing assignments**, only the new mandatory parameters that do not have a default value are listed.
 - If you select **Use default parameter values from version selected above**, all mandatory parameters from the selected Management Template or Aspect version that do not have a default value are displayed. These parameters must be edited before proceeding to the next step of the wizard.
6. Click **Next** to go to **Required Parameters**.

To change a parameter, double-click or select the parameter from the list and click  **Edit**.

The Edit Parameter dialog opens. If there are no mandatory parameters that require editing for this assignment, you are automatically taken to the **All Parameters** tab on BSM 9.2x or the **Parameter Summary** tab on OMi 10.x.

7. Click **Next** to go to the **All Parameters** tab on BSM 9.2x or the **Parameter Summary** tab on OMi 10.x or click **Finish** to save the changes and close the wizard.
8. Click **Finish** to save the changes and close the wizard. The assigned item is updated to the specified Management Template or Aspect version.

Use Case 2: You are using a Management Pack that internally uses the OMi MP for Infrastructure Aspects and you need to update the Infrastructure Aspects to the latest version. For example, OMi MP

for Oracle Database, OMi MP for Oracle WebLogic, OMi MP for Microsoft Exchange Server, OMi MP for SAP, and so on use Infrastructure Aspects to monitor Infrastructure performance such as Resource Bottleneck Diagnosis, System Fault Analysis and so on.

To update all items in a Management Template on BSM 9.2x and OMi 10.x Servers, do the following:

1. Open the Management Templates & Aspects pane:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Management Templates & Aspects**.

On OMi 10.x, click **Administration > Monitoring > Management Templates & Aspects**.

2. Select each Management Template that contains the Infrastructure Aspects.

3. Click  **Update to Latest**.

The Update to Latest Wizard appears.

4. In the **Options** tab, click **Next**.

5. In the **Preview** tab, a preview of the update is shown as an expanded tree view of the Aspect, where items that will be updated are labeled "*(old version > new version)*", and items that will not be updated are labeled "*(current version)*".


6. Click **Finish** to apply the update as shown in the preview.

To update the Management Templates to latest on the managed nodes:


For BSM 9.2x:

1. Click **Admin > Operations Management > Monitoring > Management Templates & Aspects**.
2. Select each of the application Management Templates of latest version which includes updated Infrastructure Aspects.
3. Edit the parameters and redeploy to each of the CIs.

For OMi 10.x:


1. Click **Administration > Monitoring > Assignments & Tuning**.
2. In the Browse Views pane, select the specific application view and select each CI where version update is required.
3. Click  **Show Assignments That Require an Update**.

All the Management Templates and Aspects that requires an update are listed.

4. Select each Management Templates and click  **Update Assigned Item**.

The Update Assigned Item dialog box appears.

5. In the **Update Options** tab, follow these steps:
 - Select the latest version from the **Update to Version** drop down list.
 - If you select **Use parameter values from existing assignments**, only the new mandatory parameters that do not have a default value are listed.
 - If you select **Use default parameter values from version selected above**, all mandatory parameters from the selected Management Template or Aspect version that do not have a default value are displayed. These parameters must be edited before proceeding to the next step of the wizard.
6. Click **Next** to go to **Required Parameters**.

To change a parameter, double-click or select the parameter from the list and click  **Edit**.

The Edit Parameter dialog opens. If there are no mandatory parameters that require editing for this assignment, you are automatically taken to the **All Parameters** tab on BSM 9.2x or the **Parameter Summary** tab on OMi 10.x.


7. Click **Next** to go to **All Parameters** tab on BSM 9.2x or the **Parameter Summary** tab on OMi 10.x or **Finish** to save the changes and close the wizard.
8. Click **Finish** to save the changes and close the wizard. The assigned item is updated to the specified Management Template or Aspect version.

Topology Synchronization for Smart Plug-in for Infrastructure

Note: It is recommended to check the Topology Synchronization settings if a Node or a CI is monitored by HP Operations Manager.

If you use Smart Plug-in for Infrastructure with HP Operations Manager, perform the following steps to forward topology data from the HPOM server to the BSM or OMi Server. For more information about Topology Synchronization, see the *HP Operations Manager i Administration Guide*.

1. Open the Infrastructure Settings from Administration:
 - On BSM 9.2x, click **Admin > Platform > Setup and Maintenance > Infrastructure Settings**.
 - On OMi 10.x, click **Administration > Setup and Maintenance > Infrastructure Settings**.

2. In the Infrastructure Settings pane, select **Applications > Operations Management**.
3. To verify if the topology synchronization package to be synced is added, click **Operations Management - HPOM Topology Synchronization Settings**.
4. If the package is not added, in **Packages for Topology Sync**, click  **Edit**.
5. In **Value**, add **default;nodegroups;operations-agent;HPOprSys;HPOprClu;HPOprVir** and click **Save**.

Chapter 3: Components of OMi MP for Infrastructure

The OMi MP for Infrastructure includes the following components for monitoring the availability, health and performance of individual systems, clusters, and virtual nodes.

- [Infrastructure Management Templates](#)
- [Infrastructure Aspects](#)
- [Parameters](#)
- [Configuration Items and Configuration Item Types](#)
- [Run Time Service Model \(RTSM\) Views](#)
- [Event Type Indicators](#)
- [Health Indicators](#)
- [Policies Setting HIs/ETIs](#)
- [Topology Based Event Correlation \(TBEC\) Rules](#)
- [Mapping Rules](#)
- [Tools](#)

Infrastructure Management Templates

The Infrastructure Management Templates provide a complete management solution for monitoring the health and performance of individual systems, virtual, and clusters in a datacenter environment.

By default, OMi MP for Infrastructure consists of a set of Infrastructure Management Templates with predefined settings to monitor the systems in an environment. You can deploy the Infrastructure Management Templates with the default parameters and seamlessly monitor the systems in your environment. These Infrastructure Management Templates comprises several Aspects which enable you to monitor the systems.

Based on the monitoring requirements, you can also customize the Infrastructure Management Templates or create Infrastructure Management Templates to monitor the systems in your environment.

Overview of Infrastructure Management Templates

OMi MP for Infrastructure comprises the following Infrastructure Management Templates:

- [Essential Cluster Management Template](#)
- [Essential IBM Power Management Template](#)
- [Essential KVM Management Template](#)
- [Essential Oracle Solaris Management Template](#)
- [Essential System Management Template](#)
- [Essential VMware vSphere Management Template](#)
- [Essential XEN Management Template](#)
- [Extensive IBM Power Management Template](#)
- [Extensive KVM Management Template](#)
- [Extensive Oracle Solaris Management Template](#)
- [Extensive System Management Template](#)
- [Extensive VMware vSphere Management Template](#)
- [Extensive XEN Management Template](#)

How to Access Infrastructure Management Templates

1. Open the Management Templates & Aspects pane:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Management Templates & Aspects**.

On OMi 10.x, click **Administration > Monitoring > Management Templates & Aspects**.

2. Click **Configuration Folders > Infrastructure Management > Infrastructure Management Templates**.

Note: The version number of OMi MP for Infrastructure is 1.12, whereas the version number of Management Templates and Aspects is 1.1 and the version number of the Policy Templates is 1.1000.

How to Deploy Infrastructure Management Templates

For more information about deploying Infrastructure Management Templates, see [Task 4b: Identifying and Deploying Infrastructure Management Template](#).


How to Automatically Assign Management Templates & Aspects

1. Open the Automatic Assignment Rules window:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Automatic Assignment Rules**.

On OMi 10.x, click **Administration > Monitoring > Automatic Assignment Rules**.

The screen consists of the Auto-Assignment Rules pane at the top, and a parameter list at the bottom.


2. Click  **New Assignment** in the toolbar of the Auto-Assignment Rules pane and select the appropriate option. The Create Auto-Assignment Rule wizard appears.
3. In the **Select Target View** tab, select an Infrastructure view containing the CIs for which you want to create an automatic assignment, and click **Next**.
4. In the **Select Item to Assign** tab, click the Infrastructure management template or aspect that you want to automatically assign to all CIs with a CI type appearing in the selected view.

The latest version of the management template or aspect that you want to assign is selected by default. Click **Next**.
5. In the **Required Parameters** tab, all mandatory parameters are listed in the management template that do not yet have a value. As they are mandatory, however, all listed parameters must be given a value before the management template can be deployed.

If all required values are specified, you can choose one of the following actions:

- Click **Finish** to assign the configuration object to the selected CI and close the wizard or dialog.
- Click **Next** to go to **All Parameters** tab on BSM 9.2x or **Parameter Summary** tab on OMi 10.x, where you can override the default value of any parameter, including those that are not required.

Note: To access the **Configure Options** tab, click **Next** in this step, and **Next** again in the **All Parameters** tab on BSM 9.2x or **Parameter Summary** tab on OMi 10.x.

To change a parameter, double-click it, or select it in the list and click  **Edit**.


- For standard parameters, the Edit Parameter dialog opens.

Click **Value**, specify the value, and then click **OK**.

- For instance parameters, the Edit Instance Parameter dialog opens.

Add instance values, and then for each instance value, specify dependent parameter values. After you specify the instances and dependent parameter values, click **OK**.

6. (Optional). In the **All Parameters** tab on BSM 9.2x or **Parameter Summary** tab on OMi 10.x, specify a value for each parameter that needs to be monitored against a different value than the default value.

To change a parameter, double-click it, or select it in the list and click  **Edit**.

- For standard parameters, the Edit Parameter dialog opens.

Click **Value**, specify the value, and then click **OK**.

- For instance parameters, the Edit Instance Parameter dialog opens.

Add instance values, and then for each instance value, specify dependent parameter values. After you specify the instances and dependent parameter values, click **OK**.

Click **Next** to go to the **Configure Options** tab, or **Finish** to save the assignment and close the wizard.

7. (Optional). In the **Configure Options** tab, clear the **Enable Assigned Objects** check box on BSM 9.2x and **Enable Assignment(s)** check box on OMi 10.x if you do not want to activate the assignment rule immediately.

You can activate automatic assignment rules later using the Automatic Assignment Rules pane at:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Automatic Assignment Rules**.

On OMi 10.x, click **Administration > Monitoring > Automatic Assignment Rules**.

8. Click **Finish** to save the changes and close the wizard. The assignment rule is added to the list of auto-assignment rules.

An assignment may trigger an event to be sent to OMi if one of the following situations applies:

- A deployment job fails.
- An auto-assignment fails.
- An auto-assignment succeeds. This behavior can be configured in the Infrastructure Settings.

You can check if the automatic assignment rule successfully created the expected assignments as follows:

1. Open the Assignments & Tuning pane:


On BSM 9.2x, click **Admin > Operations Management > Monitoring > Assignments & Tuning**.

On OMi 10.x, click **Administration > Monitoring > Assignments & Tuning**.
2. In the **Browse Views** tab, select the view you identified when creating your automatic assignment rule.
3. Expand the view, and select a node that corresponds to the root CI type of the assigned item. Assignments created as a result of Automatic Assignment Rules are shown in the list of assignments at the top of the right pane, and have the value Auto-Assignment in the column **Assigned By**.

You can consider the following options for tuning the assignment:

- Use the Auto-Assignment Rules pane to tune the parameter values for all assignments triggered by the automatic assignment rule.
- Use the Assignments pane to tune, redeploy, delete, and enable or disable individual assignments.

How to Display an Assignment Report for a Management Template

1. Select the Management Template you want to create the report for.
2. Click  **Generate Assignment Report** in the Management Templates & Aspects pane.

The pre-configured Assignment Report is displayed.

You can display additional types of reports from the Assignments & Tuning pane.

Essential Cluster Management Template

The Essential Cluster Management Template monitors the high availability (HA) components such as the cluster strength, nodes and resource pool availability in a clustered environment. It monitors the single point of failure (SPOF), quorum conditions and node strength of the components in a clustered environment. The Essential Cluster Management Template comprises of specific Aspects for monitoring these features.

How to Access the Essential Cluster Management Template

1. Open the Management Templates & Aspects pane:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Management Templates & Aspects**.

On OMi 10.x, click **Administration > Monitoring > Management Templates & Aspects**.

2. Click **Configuration Folders > Infrastructure Management > Infrastructure Management Templates > Essential Cluster Management**.

Management Template - Aspects

The Essential Cluster Management Template consists of the following Aspects:

- [Cluster Strength and Status](#)
- [Cluster Infrastructure Discovery](#)

Essential IBM Power Management Template

The Essential IBM Power Management Template manages the health and availability of IBM Power virtualization environment. It monitors the basic functionality of the Virtualized IBM LPAR environment - Guest availability, memory and CPU utilization of Frame and discovers the virtual components such as hypervisor host, guest, and resource pool. The Essential IBM Power Management Template comprises specific Aspects to monitor these features.

How to Access the Essential IBM Power Management Template

1. Open the Management Templates & Aspects pane:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Management Templates & Aspects**.

On OMi 10.x, click **Administration > Monitoring > Management Templates & Aspects**.

2. Click **Configuration Folders > Infrastructure Management > Infrastructure Management Templates > Essential IBM Power Management**.

Management Template - Aspects

The Essential IBM Power Management Template consists of the following Aspects:

- [IBM Power Host Health](#)
- [IBM Power Guest Health](#)

Essential KVM Management Template

The Essential KVM Management Template manages the health and availability of KVM Virtualization Environment in a Datacenter. It monitors the basic functionalities of Virtualized KVM environment - resource usage for KVM host and individual Guest, Guest availability and resources, and discovers the virtual components like hypervisor host, guest, and resource pool. The Essential KVM Management Template comprises specific Aspects to monitor these features.

How to Access the Essential KVM Management Template

1. Open the Management Templates & Aspects pane:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Management Templates & Aspects**.

On OMi 10.x, click **Administration > Monitoring > Management Templates & Aspects**.

2. Click **Configuration Folders > Infrastructure Management > Infrastructure Management Templates > Essential KVM Management**.

Note: You can deploy Essential KVM Management Template *only* on the host.

Management Template - Aspects

The Essential KVM Management Template consists of the following Aspects:

- [Virtual Infrastructure Discovery](#)
- [KVM Guest Health](#)
- [KVM Host Health](#)

Essential Oracle Solaris Management Template

The Essential Oracle Solaris Management Template manages the health and availability of Oracle Solaris Virtualization Environment. It monitors the basic functionality of the Oracle Solaris Zones environment - Guest resources, Host Resource Utilization and discovers the virtual components such as hypervisor host, guest, and resource pool. The Essential Oracle Solaris Management Template comprises of specific Aspects to monitor these features.

How to Access the Essential Oracle Solaris Management Template

1. Open the Management Templates & Aspects pane:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Management Templates & Aspects**.

On OMi 10.x, click **Administration > Monitoring > Management Templates & Aspects**.

2. Click **Configuration Folders > Infrastructure Management > Infrastructure Management Templates > Essential Oracle Solaris Management**.

Note: You can deploy Essential Oracle Solaris Management Template *only* on the host.

Management Template - Aspects

The Essential Oracle Solaris Management Template consists of the following Aspects:

- [Oracle Solaris Host Health](#)
- [Oracle Solaris Guest Health](#)
- [Virtual Infrastructure Discovery](#)

Essential System Management Template

The Essential System Management Template monitors the health of all the systems - individual, clusters, and virtual in a data center environment. It monitors the basic functionalities - availability of system services and processes, software resources (CPU, memory, network, and disk), checks for system downtime risks by tracking congestion and bottlenecks in system resources and failed logins and last logins on your system. The Essential System Management Template comprises of specific Aspects to monitor these features.

How to Access the Essential System Management Template

1. Open the Management Templates & Aspects pane:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Management Templates & Aspects**.

On OMi 10.x, click **Administration > Monitoring > Management Templates & Aspects**.

2. Click **Configuration Folders > Infrastructure Management > Infrastructure Management Templates > Essential System Management**.

Management Template - Aspects

The Essential System Management Template consists of the following Aspects:

- [Resource Bottleneck Diagnosis](#)
- [Key System Services Availability](#)
- [System Fault Analysis](#)
- [User Logins](#)
- [System Infrastructure Discovery](#)

Essential VMware vSphere Management Template

The Essential VMware vSphere Management Template monitors the health, availability and status of hosts or guests in a VMware vSphere Environment. It monitors the basic functionality in a virtualized VMware vSphere environment - Datastore utilization, Guest availability and resources, resource usage for individual hosts and virtual machines from vCenter and discovers the virtual components such as hypervisor host, guest, and resource pool. The Essential VMware vSphere Management Template comprises of specific Aspects to monitor these features.

How to Access the Essential VMware vSphere Management Template

1. Open the Management Templates & Aspects pane:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Management Templates & Aspects**.

On OMi 10.x, click **Administration > Monitoring > Management Templates & Aspects**.

2. Click **Configuration Folders > Infrastructure Management > Infrastructure Management Templates > Essential VMware vSphere Management**.

Management Template - Aspects

The Essential VMware vSphere Management consists of the following Aspects:

- [VMware Host Health](#)
- [VMware Guest Health](#)
- [VMware Datastore Performance](#)
- [VMware vSphere Events](#)

Essential XEN Management Template

The Essential XEN Management Template monitors the resource usage for XEN host and individual guest systems. It monitors the basic functionalities of XEN virtualization environment - Guest availability and resources, Host resource utilization and discovers the virtual components like hypervisor host, guest, and resource pool. The Essential XEN Management Template comprises specific Aspects to monitor these features.

How to Access Essential XEN Management Template

1. Open the Management Templates & Aspects pane:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Management Templates & Aspects**.

On OMi 10.x, click **Administration > Monitoring > Management Templates & Aspects**.

2. Click **Configuration Folders > Infrastructure Management > Infrastructure Management Templates > Essential XEN Management**.

Note: You can deploy Essential XEN Management Template *only* on the host.

Management Template - Aspects

The Essential XEN Management Template consists of the following Aspects:

- [Xen Guest Health](#)
- [Xen Host Health](#)
- [Virtual Infrastructure Discovery](#)

Extensive IBM Power Management Template

The Extensive IBM Power Management Template monitors the performance and health of IBM Power virtualization environment. It monitors the Guest performance as an advanced feature in addition to the basic functionality - Guest availability, memory and CPU utilization of Frame and discovers the virtual components such as hypervisor host, guest, and resource pool. The Extensive IBM Power Management Template comprises of specific Aspects to monitor these features.

How to Access Extensive IBM Power Management Template

1. Open the Management Templates & Aspects pane:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Management Templates & Aspects**.

On OMi 10.x, click **Administration > Monitoring > Management Templates & Aspects**.

2. Click **Configuration Folders > Infrastructure Management > Infrastructure Management Templates > Essential XEN Management**.

Management Template - Aspects

The Extensive IBM Power Management Template consists of the following Aspects:

- [IBM Power Host Health](#)
- [IBM Power Guest Health](#)
- [IBM Power Guest Performance](#)

Extensive KVM Management Template

The Extensive KVM Management Template monitors the performance and health of host and guest systems in a KVM Virtualization Environment. It monitors the Guest performance as an advanced feature in addition to the basic functionalities - resource usage for KVM host and individual Guest, Guest availability and resources, and discovers the virtual components like hypervisor host, guest, and resource pool. The Extensive KVM Management Template comprises of specific Aspects to monitor these features.

How to Access the Extensive KVM Management Template

1. Open the Management Templates & Aspects pane:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Management Templates & Aspects**.

On OMi 10.x, click **Administration > Monitoring > Management Templates & Aspects**.

2. Click **Configuration Folders > Infrastructure Management > Infrastructure Management Templates > Extensive KVM Management**.

Note: You can deploy Extensive KVM Management Template *only* on the host.

Management Template - Aspects

The Extensive KVM Management Template consists of the following Aspects:

- [Virtual Infrastructure Discovery](#)
- [KVM Guest Health](#)
- [KVM Guest Performance](#)
- [KVM Host Health](#)

Extensive Oracle Solaris Management Template

The Extensive Oracle Solaris Management Template monitors the performance and health of Oracle Solaris Virtualization Environment. It monitors the Guest performance as an advanced feature in addition to the basic functionalities of Oracle Solaris Zones environment - Guest resources, Host Resource Utilization and discovers the virtual components such as hypervisor host, guest, and resource pool. The Extensive Oracle Solaris Management Template comprises of specific Aspects to monitor these features.

How to Access the Extensive Oracle Solaris Management Template

1. Open the Management Templates & Aspects pane:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Management Templates & Aspects**.

On OMi 10.x, click **Administration > Monitoring > Management Templates & Aspects**.

2. Click **Configuration Folders > Infrastructure Management > Infrastructure Management Templates > Extensive Oracle Solaris Management**.

Note: You can deploy Extensive Oracle Solaris Management Template *only* on the host.

Management Template - Aspects

The Extensive Oracle Solaris Management Template consists of the following Aspects:

- [Oracle Solaris Guest Health](#)
- [Oracle Solaris Guest Performance](#)

- [Oracle Solaris Host Health](#)
- [Virtual Infrastructure Discovery](#)

Extensive System Management Template

The Extensive System Management Template monitors the in-depth performance of a system by analyzing availability and performance of individual system resources. It monitors the advanced features - network I/O operations and performance, CPU performance and statistics, memory performance, space utilization of remote disk, health and status of HP ProLiant servers and the basic functionalities - availability of system services and processes, software resources (CPU, memory, network, and disk), checks for system downtime risks by tracking congestions and bottlenecks in system resources and failed logins and last logins on your system. The Extensive System Management Template comprises of specific Aspects to monitor these features.

How to Access the Extensive System Management Template

1. Open the Management Templates & Aspects pane:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Management Templates & Aspects**.

On OMi 10.x, click **Administration > Monitoring > Management Templates & Aspects**.

2. Click **Configuration Folders > Infrastructure Management > Infrastructure Management Templates > Extensive System Management**.

Management Template - Aspects

The Extensive System Management Template consists of the following Aspects:

- [Bandwidth Utilization and Network IOPS](#)
- [CPU Performance](#)
- [Memory and Swap Utilization](#)
- [Remote Disk Space Utilization](#)
- [Resource Bottleneck Diagnosis](#)
- [Space Availability and Disk IOPS](#)
- [System Infrastructure Discovery](#)

Extensive VMware vSphere Management Template

The Extensive VMware vSphere Management Template monitors the health, availability, and status of hosts or guests in a VMware vSphere Environment. It monitors the advanced features such as the CPU and memory Utilization for VMware clusters and resource pools. It also monitors the basic functionality such as Datastore utilization, Guest availability and resources, resource usage for individual hosts and virtual machines from vCenter and discovers the virtual components such as hypervisor host, guest, and resource pool. The Extensive VMware vSphere Management Template comprises of specific Aspects to monitor these features.

How to Access the Extensive VMware vSphere Management Template

1. Open the Management Templates & Aspects pane:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Management Templates & Aspects**.

On OMi 10.x, click **Administration > Monitoring > Management Templates & Aspects**.

2. Click **Configuration Folders > Infrastructure Management > Infrastructure Management Templates > Extensive VMware vSphere Management**.

Management Template - Aspects

The Extensive VMware vSphere Management consists of the following Aspects:

- [VMware Host Health](#)
- [VMware Cluster Performance](#)
- [VMware Guest Health](#)
- [VMware Datastore Performance](#)
- [VMware Resource Pool Monitor](#)
- [VMware vSphere Events](#)

Extensive XEN Management Template

The Extensive XEN Management Template monitors the performance and health of host and guest systems in a XEN Virtualization Environment. It monitors Guest Performance as an advanced feature in addition to the basic functionalities - Guest availability and resources, Host resource utilization and discovers the virtual components like hypervisor host, guest, and resource pool. The Extensive XEN Management Template comprises of specific Aspects to monitor these features.

How to Access the Extensive XEN Management Template

1. Open the Management Templates & Aspects pane:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Management Templates & Aspects**.

On OMi 10.x, click **Administration > Monitoring > Management Templates & Aspects**.

2. Click **Configuration Folders > Infrastructure Management > Infrastructure Management Templates > Extensive XEN Management**.

Note: You can deploy Extensive XEN Management Template *only* on the host.

Management Template - Aspects

The Extensive XEN Management Template consists of the following Aspects:

- [XEN Guest Health](#)
- [XEN Guest Performance](#)
- [XEN Host Health](#)
- [Virtual Infrastructure Discovery](#)

Infrastructure Aspects

Infrastructure Aspects monitor the system resources operating in a data center environment. The systems can be stand-alone, virtual, or clustered systems. Each Infrastructure Aspect consists of policy templates, instrumentation, and parameters for monitoring the health and performance of the systems. Each Aspect provides the ability to monitor a Computer, VMware VirtualCenter, and FailoverCluster CI.

Grouping of Infrastructure Aspects

The Infrastructure Aspects are grouped as follows:

- [Systems Infrastructure Aspects](#)
- [Virtualization Infrastructure Aspects](#)
- [Cluster Infrastructure Aspects](#)

How to Access the Infrastructure Aspects

1. Open the Management Templates & Aspects pane:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Management Templates & Aspects**.

On OMi 10.x, click **Administration > Monitoring > Management Templates & Aspects**.

2. Click **Configuration Folders > Infrastructure Management > <aspect folder>**.

Note: The version number of OMi MP for Infrastructure is 1.12, whereas the version number of Management Templates and Aspects is 1.1 and the version number of the Policy Templates is 1.1000.

How to Create Infrastructure Aspects






1. Open the Management Templates & Aspects pane:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Management Templates & Aspects**.



On OMi 10.x, click **Administration > Monitoring > Management Templates & Aspects**.

2. In the Configuration Folders pane:


Configuration Folders > Infrastructure Management

3. In the Configuration Folders pane, click the configuration folder in which you want to create the new Aspect. If you need to create a new configuration folder, click the .
4. In the Management Templates & Aspects pane, click the , and then click . The Create Aspect wizard opens.
5. In the **General** tab, type a unique **Name** for the new Aspect. Click **Next**.
6. Each Aspect enables you to manage one feature or characteristic of one or more types of configuration item. In the **CI Types** tab, select one or more **Available CI Type(s)** to which this Aspect can be assigned, and then click  to add them to the list of assigned CI types. (Press **CTRL** to select several CI types). Click **Next**.
7. In the **Instrumentation** tab, click  to add instrumentation to the Aspect. The Add

Instrumentation dialog box opens, which enables you to select the instrumentation that you want to add. Click **Next**.

8. (Optional). In the **Aspects** tab, click , and then click . The Add Existing Aspect dialog box opens, which enables you to select an existing Aspect that you want to nest within this Aspect. Click an Aspect, and then click **OK**.

If suitable Aspects do not exist, click , and then click  to create a new Aspect. Click **Next**.



9. In the **Policy Templates** tab, click  Add Policy Templates on BSM 9.2x and Add Policy Templates From Liston OMi 10.x.

The Add Policy Template to Aspect dialog box opens. Select the policy templates that you want to add, and then click **OK**. (Press **CTRL** to select several policy templates.)

If suitable policy templates do not exist, click , and then click  to create a policy template.

10. In the **Policy Templates** tab, select the **Version** of the policy templates that you want to add.

Each modification to a policy template is stored in the database as a separate version. Aspects contain specific versions of policy templates. If a new version of a policy template becomes available later, you have to update the Aspect to include the latest version.

11. (Optional). In the **Policy Templates** tab, click the policy template to which you want to add a deployment condition, click , and then click .


The Edit Deployment Condition dialog box opens, which enables you to specify deployment conditions for the selected policy template.

Set the condition and then click **OK**.

In the **Policy Templates** tab, click **Next**.

12. In the **Parameters** tab, the list of all the parameters added to this Aspect from the policy templates is displayed.


To combine parameters:

- a. Press **CTRL** and click the parameters that you want to combine.
- b. Click . The Edit/Combine Parameters dialog box opens.
- c. Type a **Name** for the combined parameters.
- d. (Optional). Specify a **Description**, **Default Value**, and whether the combined parameter is **Read Only**, an **Expert Setting**, or **Hidden**.

You can either set a specific default value, or you can click **From CI Attribute** and then browse for a CI attribute. When you specify a CI attribute, Operations Management sets the parameter value automatically during deployment of the policy templates, using the actual value of this attribute from the CI. You can also set conditional parameter values here.

Note: Read Only prevents changes to the parameter value when the Aspect is assigned to a configuration item. Hidden also prevents changes, but additionally makes the parameter invisible. Users can choose whether to show expert settings when they make an assignment.

- e. Click **OK**.

You can also edit the parameters without combining them, to override the defaults in the policy template. Click one parameter, and then click . The Edit/Combine Parameters dialog box opens.

13. In the Create Aspect wizard, click **Finish** to save the Aspect and close the wizard. The new Aspect appears in the Management Templates & Aspects pane.

How to Deploy Infrastructure Aspects


1. Open the Management Templates & Aspects pane:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Management Templates & Aspects**.


On OMi 10.x, click **Administration > Monitoring > Management Templates & Aspects**.



2. In the Configuration Folders pane:


Configuration Folders > Infrastructure Management

3. In the Management Templates & Aspects pane, click the Aspect that you want to deploy, and then click . The Assign and Deploy wizard opens.
4. In the **Configuration Item** tab, click the configuration item to which you want to assign the Aspect, and then click **Next**.
5. In the **Required Parameters** tab, all mandatory parameters are listed in the management template that do not have a value.

If all required values are specified, click **Next** to go to the **All Parameters** tab on BSM 9.2x **Parameter Summary** tab on OMi 10.x.

To change a parameter, double-click it, or click .

- a. Select the Instance parameter in the list, and then click . The Edit Parameter Value dialog box opens.
 - b. Click **Value**, specify the value, and then click **OK**.
 - c. Select the Dependent Parameters and specify the value. Click **Next**.
6. Click **Next** to go to the **All Parameters** tab on BSM 9.2x **Parameter Summary** tab on OMi 10.x. To change the default values of the parameters, you can select the parameter and then click . The Edit Parameter dialog box opens. Click **Value**, specify the value, and then click **OK**.

Note: In the **All Parameters** tab on BSM 9.2x or **Parameter Summary** tab on OMi 10.x, you can override the default values of any parameter. You can specify a value for each parameter at the Management Template level. By default, parameters defines as expert parameters are not shown. To show expert parameters, click  **Show Expert Parameters**.

Click **Next**.

7. *(Optional)*. If you do not want to enable the assignment immediately, clear the **Enable Assigned Objects** check box on BSM 9.2x or **Enable Assignment(s)** check box on OMi 10.x. You can then enable the assignment later using the Assignments & Tuning pane.
8. Click **Finish**.

Systems Infrastructure Aspects

Systems Infrastructure Aspects manage the health of every single system in the environment. Each system will have its own set of resources, hardware and software that needs to be managed for the system to be healthy. It also monitors the performance of all system resources such as CPU, Memory, Disk, FileSystem, Network Interface, System process and services, Security, System logging and so on. Systems Infrastructure Aspects monitors the Computer CI types.

User Interface Reference

General	Provides an overview of the general attributes of the Systems Infrastructure Aspects.
CI Type	The type of CIs that can be assigned to the Aspect. This is the type of CI which is assigned to the Management Template. The Systems Infrastructure Aspects contain the Computer CI types.
Instrumentation	Provides an overview of the programs deployed to the CI types which contains the System Infrastructure Aspect.

Aspects	Provides an overview of any Aspects that contain the Systems Infrastructure Aspect. You can expand each item in the list to see more details about the nested Aspect.
Policy Templates	Provides an overview of the policy templates that contain the Systems Infrastructure Aspect. You can expand each item in the list to see more details about the policy template.

The Systems Infrastructure Aspects consists of the following:

Bandwidth Utilization and Network IOPS

This Aspect monitors IO operations, and performance of the systems in the network. It monitors the network IO operations and performance based on the bandwidth used, outbound queue length and average bytes transferred per second. This Aspect contains the following policy template:

CI Type	Policy Template	Policy Description	Policy Type
Computer	Sys_ NetworkUsageAndPerformance	Monitors the network usage of the systems and shows error rates and collisions to identify potential network bottlenecks. It also monitors the physical NICs of only the vMA machines. It does not monitor performance data for package collision on Windows as the BYNETIF_COLLISION metric is not available on Windows operating systems.	Measurement Threshold Template

CPU Performance

This Aspect monitors the overall CPU performance such as the CPU utilization percentage and spike in CPU usage. Individual CPU performance monitoring is based on total CPU utilization, CPU utilization in user mode, CPU utilization in system mode and interrupt rate. This Aspect contains the following policy template:

CI Type	Policy Template	Indicator	Policy Description	Policy Type
Computer	Sys_ CPUSpikeCheck	CPUUsageLevel	Monitors the variation in processor performance. A system experiences CPU spike when there is a sharp rise in the CPU usage immediately followed by a decrease in usage. It also monitors the CPU time spent in user mode and system mode. It also monitors the total CPU time when the CPU is busy.	Measurement Threshold Template

General System Services Availability

This Aspect monitors the availability of system services and processes. This Aspect monitors the following system services and processes:

- **HP-UX:** Bootpd, Cron, and Network File System (NFS)
- **Linux:** Dynamic Host Configuration Protocol (DHCP), Named, NFS, Sendmail, Cron, and Server Message Block (Smb)
- **Windows:** Distributed File System (DFS), DHCP, Domain Name system (DNS), File Transfer Protocol (FTP), Firewall, Fax, NFS, Remote Procedure Call (RPC), RRA, Print, Simple Network Management Protocol (SNMP), Terminal server, Web Management Tools, and Web Server Service.
- **AIX:** Cron, DHCP, Named, NFS, Portmap, Sendmail, and Webserver
- **Solaris:** DHCP, Named, NFS, Sendmail, Cron, and SNMP
- **Debian:** Apache, Cron, Exim, Internet Service Daemon (InetD), Named, Nfs, NetBIOS Message Block Daemon (Nmbd), Samba, and Single Sided High Density (Sshd).

This Aspect consists of the following policy templates:

CI Type	Policy Template	Indicator	Policy Description	Policy Type
Computer	Sys_AIXCronProcessMonitor	BatchJobService	Monitors the Cron daemon processes running on the AIX operating systems.	Service/Process Monitoring Template
	Sys_AIXDHCPPProcessMonitor	DHCPService	Monitors the DHCP server daemon processes running on AIX operating systems.	
	Sys_AIXNamedProcessMonitor	DNSService	Monitors the Named processes running on the AIX operating systems.	
	Sys_AIXNfsServerProcessMonitor	FileServerService	Monitors the NFS server related processes running on the AIX operating systems.	

CI Type	Policy Template	Indicator	Policy Description	Policy Type
	Sys_AIXPortmapProcessMonitor	RPCService	Converts the RPC program numbers into Internet port numbers running on the AIX operating systems.	
	Sys_AIXQdaemonProcessMonitor	PrintService	Monitors the job requests and the resources required to complete the jobs running on AIX operating systems.	
	Sys_AIXSendmailProcessMonitor	EmailService	Monitors the Sendmail daemon processes running on the AIX operating systems.	
	Sys_AIXWebserverProcessMonitor	WebServerService	Monitors the httpd daemon processes running on the AIX operating systems.	

CI Type	Policy Template	Indicator	Policy Description	Policy Type
	Sys_HPUXBootpdProcessMonitor	DHCPService	Monitors the Bootpd daemon processes running on the HP-UX operating systems.	
	Sys_HPUXCronProcessMonitor	BatchJobService	Monitors the Cron daemon processes on the HP-UX operating systems.	
	Sys_HPUXNfsServerProcessMonitor	FileServerService	Monitors the state of NFS daemon processes running on the HP-UX operating systems.	
	Sys_LinuxDHCPPProcessMonitor	DHCPService	Monitors the DHCP daemon processes running on Linux operating systems.	

CI Type	Policy Template	Indicator	Policy Description	Policy Type
	Sys_LinuxNamedProcessMonitor	DNSService	Monitors the Named daemon processes running on Linux operating systems.	
	Sys_LinuxNfsServerProcessMonitor	FileServerService	Monitors the state of NFS daemon processes running on Linux operating systems.	
	Sys_LinuxSendmailProcessMonitor	EmailService	Monitors the Sendmail daemon processes running on the Linux operating systems.	
	Sys_LinuxSmbServerProcessMonitor	FileServerService	Monitors SMB daemon processes running on the Linux operating systems.	

CI Type	Policy Template	Indicator	Policy Description	Policy Type
	Sys_MSWindowsDFSRoleMonitor	NA	Monitors the availability of system services required for the DFS role service.	
	Sys_MSWindowsDHCPserverRoleMonitor	DHCPserverService	Monitors the availability of system services required for the DHCP server role service.	
	Sys_MSWindowsDNSServerRoleMonitor	DNSService	Monitors the availability of system services required for the DNS server role service.	
	Sys_MSWindowsFTPServerRoleMonitor	FTPServerService	Monitors the availability of system services required for the FTP publishing service role service.	

CI Type	Policy Template	Indicator	Policy Description	Policy Type
	Sys_ MSWindowsFaxServerRoleMonitor	NA	Monitors the availability of system services required for the fax server role service.	
	Sys_ MSWindowsFirewallRoleMonitor	FirewallService	Monitors the availability of system services required for the Windows firewall.	
	Sys_MSWindowsNFSRoleMonitor	NA	Monitors the availability of system services required for the NFS role service.	
	Sys_ MSWindowsPrintServiceRoleMonitor	PrintService	Monitors the availability of system services required for print services role service.	

CI Type	Policy Template	Indicator	Policy Description	Policy Type
	Sys_MSWindowsRRAServicesRoleMonitor	NA	Monitors the availability of system services required for routing and remote access services role service.	
	Sys_MSWindowsRpcRoleMonitor	RPCService	Monitors the availability of system services required for RPC.	
	Sys_MSWindowsSnmpProcessMonitor	NA	Monitors the SNMP service on Windows operating systems.	
	Sys_MSWindowsTSGatewayRoleMonitor	NA	Monitors the availability of system services required for Terminal Services (TS) gateway role service.	

CI Type	Policy Template	Indicator	Policy Description	Policy Type
	Sys_MSWindowsTSLicensingRoleMonitor	NA	Monitors the availability of system services required for TS licensing role service.	
	Sys_MSWindowsTSWebAccessRoleMonitor	NA	Monitors the availability of system services required for TS web access role service.	
	Sys_MSWindowsTerminalServerRoleMonitor	MSTerminalService	Monitors the availability of system services required for terminal server role service.	
	Sys_MSWindowsWebMgmtToolsRoleMonitor	NA	Monitors the availability of system services required for web management tools role service.	

CI Type	Policy Template	Indicator	Policy Description	Policy Type
	Sys_MSWindowsWebServerRoleMonitor	WebServerService	Monitors the availability of system services required for web server role service.	
	Sys_OpenSshdProcessMonitor	SecureLoginService	Monitors SSH daemon processes running on the system	
	Sys_RHELCronProcessMonitor	BatchJobService	Monitors Cron daemon processes running on RHEL operating systems.	
	Sys_SLESCronProcessMonitor	BatchJobService	Monitors Cron daemon processes running on SLES operating systems.	
	Sys_SunSolarisCronProcessMonitor	BatchJobService	Monitors Cron daemon processes running on Sun Solaris operating systems.	

CI Type	Policy Template	Indicator	Policy Description	Policy Type
	Sys_SunSolarisDHCPProcessMonitor	DHCPService	Monitors DHCP daemon processes running on Sun Solaris operating systems.	
	Sys_SunSolarisNamedProcessMonitor	DNSService	Monitors Named daemon processes running on Sun Solaris operating systems.	
	Sys_SunSolarisNfsProcessMonitor	FileServerService	Monitors NFS processes running on Sun Solaris operating systems.	
	Sys_SunSolarisSendmailProcessMonitor	EmailService	Monitors the Sendmail daemon processes running on Sun Solaris operating systems.	
	Sys_UnixSnmpdProcessMonitor	NA	Monitors the SNMP processes running on Linux and Unix operating systems.	

CI Type	Policy Template	Indicator	Policy Description	Policy Type
	Sys_DebianApacheProcessMonitor	WebServerService	Monitors the Apache processes running on Debian operating systems.	
	Sys_DebianCronProcessMonitor	BatchJobService	Monitors the Cron daemon processes running on Debian operating systems.	
	Sys_DebianEximProcessMonitor	EmailService	Monitors Exim processes running on the Debian operating systems.	
	Sys_DebianInetdProcessMonitor	NA	Monitors the Inetd processes running on the Debian operating systems.	
	Sys_DebianNamedProcessMonitor	DNSService	Monitors the Named processes running on Debian operating systems.	

CI Type	Policy Template	Indicator	Policy Description	Policy Type
	Sys_DebianNfsServerProcessMonitor	FileServerService	Monitors the Nfs processes running on Debian operating systems.	
	Sys_DebianNmbdProcessMonitor	FileServerService	Monitors the Nmbd processes running on Debian operating systems.	
	Sys_DebianSambaProcessMonitor	FileServerService	Monitors the Samba processes running on Debian operating systems.	
	Sys_DebianSshdProcessMonitor	NA	Monitors the SSH daemon processes running on Debian operating systems.	

Key System Services Availability

This Aspect monitors the key processes that run in the background to support the different tasks required for the operating system or application. This Aspect monitors availability of following processes and services:

- **HPUX, Linux, Solaris:** Syslog and SSH daemon (Sshd)
- **AIX:** Syslog

- **Windows:** Event log, Fileserver, Network policy server, task scheduler and Windows Server 2003 (Win2k3) file services.

This Aspect consists of the following policy templates:

CI Type	Policy Template	Indicator	Policy Description	Policy Type
Computer	Sys_AIXSyslogProcessMonitor	NA	This policy template monitors the Syslog processes running on AIX operating systems.	Service/Processes Monitoring Template
	Sys_HPUSshdProcessMonitor	NA	This policy template monitors the SSH daemon processes running on HP-UX operating systems.	
	Sys_HPUSyslogProcessMonitor	NA	This policy template monitors the Syslog daemon processes running on HP-UX operating systems.	

CI Type	Policy Template	Indicator	Policy Description	Policy Type
	Sys_LinuxSshdProcessMonitor	NA	This policy template monitors the SSH daemon processes running on Linux operating systems	
	Sys_MSWindowsEventLogRoleMonitor	NA	This policy template monitors the availability of system services required for event log role service.	
	Sys_MSWindowsFileServerRoleMonitor	NA	This policy template monitors the availability of system services required for files server role service.	

CI Type	Policy Template	Indicator	Policy Description	Policy Type
	Sys_ MSWindowsNetworkPolicyServerRoleMonitor	NA	This policy template monitors the availability of system services required for network policy server role service.	
	Sys_ MSWindowsTaskSchedulerRoleMonitor	NA	This policy template monitors the availability of system services required for task scheduler role service.	
	Sys_ MSWindowsWin2k3FileServicesRoleMonitor	NA	This policy template monitors the availability of system services required for Win2k3 files services role service.	

CI Type	Policy Template	Indicator	Policy Description	Policy Type
	Sys_RHELSyslogProcessMonitor	NA	This policy template monitors the Syslog daemon processes running on RHEL operating systems.	
	Sys_SLESSyslogProcessMonitor	NA	This policy template monitors the Syslog daemon processes running on SLES operating systems.	
	Sys_SunSolarisSshdProcessMonitor	NA	This policy template monitors the SSH daemon processes running on Sun Solaris operating systems.	
	Sys_SunSolarisSyslogProcessMonitor	NA	This policy template monitors the system log processes running on Sun Solaris operating systems.	

Memory and Swap Utilization

The Memory and Swap Utilization Aspect monitors memory performance of the system. Memory performance monitoring is based on Memory utilization (in percentage), Swap space utilization (in percentage), Free memory available (in MBs), and Free swap space available (in MBs). This Aspect consists of the following policy templates:

CI Type	Policy Template	Indicator	Policy Description	Policy Type
Computer	Sys_MemoryUsageAndPerformance	MemoryUsageLevel	Monitors the memory usage of the system and shows error rates and collisions to identify potential memory bottlenecks.	Measurement Threshold Template
	Sys_SwapCapacityMonitor	SwapUsageLevel	Monitors the swap space utilization of the system.	

Remote Disk Space Utilization

The Remote Disk Space Utilization Aspect monitors space utilization of remote disk. This Aspect consists of the following policy templates:

CI Type	Policy Template	Indicator	Policy Description	Policy Type
Computer, FileSystem	Sys_LinuxCifsUtilizationMonitor	NetworkFileShareUsageLevel	Monitors space utilization level for CIFS remote filesystems on Linux platforms.	Measurement Threshold Template

CI Type	Policy Template	Indicator	Policy Description	Policy Type
	Sys_LinuxNfsUtilizationMonitor	NetworkFileShareUsageLevel	Monitors space utilization level for NFS remote filesystems on Linux platforms.	

Resource Bottleneck Diagnosis

This Aspect identifies congestions and bottleneck conditions for system resources like the CPU, memory, network, and disk. CPU bottleneck monitoring is based on global CPU utilization and load average (Run Queue Length) Memory bottleneck monitoring is based on memory utilization, free memory available, and memory swap out rate. Filesystem monitoring is based on space utilization level for busiest filesystem on the node. Network monitoring is based on Packet collision rate, packet error rate, and outbound queue length. This Aspect contains the following policy templates:

CI Type	Policy Template	Indicator	Policy Description	Policy Type
Computer	Sys_CPUBottleneckDiagnosis	CPULoad	<p>Detects CPU bottlenecks such as exceeding the thresholds for CPU utilization percentage, processor queue length, and total number of CPUs running on an operating system.</p> <p>For example, if the threshold for CPU utilization is violated along with threshold for number of processes in the</p>	Measurement Threshold Template

CI Type	Policy Template	Indicator	Policy Description	Policy Type
			<p>queue waiting for CPU time, the policy sends an alert. The message also displays a list of the top ten CPU utilization processes.</p>	
	Sys_DiskPeakUtilMonitor	DiskUsageLevel	<p>Monitors the utilization level of the disk on the system. It checks whether the utilization level is full.</p>	
	Sys_MemoryBottleneckDiagnosis	MemoryLoad	<p>Monitors the physical memory utilization and the bottlenecks. Memory bottleneck condition occurs when the memory utilization is high and the available memory is very low. It causes the system to slow down affecting overall performance. High memory consumption results in excessive page outs, high page scan rate, swap-out byte rate, and page request rate, eventually slowing down the system. The</p>	

CI Type	Policy Template	Indicator	Policy Description	Policy Type
			message also displays a list of top ten memory utilization processes.	
	Sys_NetworkInterfaceErrorDiagnosis	SESSION	Monitors the network usage of the system and checks for potential network bottlenecks or errors.	

Server Hardware Fault

This Aspect monitors the health and status of the HP ProLiant servers. These policies monitor the Simple Network Management Protocol SNMP traps generated by the SIM Agent and send alert messages to the HPOM console. All these policies are of the type SNMP Interceptor. This Aspect consists of the following policy templates:

CI Type	Policy Template	Indicator	Policy Description	Policy Type
Computer	Sys_HPProLiant_BladeType2Traps	NA	This policy intercepts SNMP traps related to Blade Type 2.	SNMP Interceptor Template
	Sys_HPProLiant_CPQCLUSTraps	NA	This policy intercepts SNMP traps related to clusters in terms of the state of the battery, monitor, Hot Plug Slot Board, memory, and hood.	

CI Type	Policy Template	Indicator	Policy Description	Policy Type
	Sys_HPProLiant_CPQCMCTraps	NA	This policy intercepts SNMP traps related to the health of the Console Management Controller (CMC) in terms of power consumption, smoke, humidity, temperature, and fan.	
	Sys_HPProLiant_CPQHLTHTraps	NA	This policy intercepts SNMP traps related to the health of the server.	
	Sys_HPProLiant_CPQNICTraps	NA	This policy intercepts SNMP traps related to the performance and availability of the Network Interface Card (NIC).	
	Sys_HPProLiant_CPQRackTraps	NA	This policy intercepts SNMP traps related to rack information in terms of temperature, power, and status.	
	Sys_HPProLiant_CPQRCTraps	NA	This policy intercepts SNMP traps related to the performance and availability of the RAID Controller.	
	Sys_HPProLiant_CPQRPMTraps	NA	This policy intercepts SNMP traps related to Rack Power Manager.	

CI Type	Policy Template	Indicator	Policy Description	Policy Type
	Sys_HPProLiant_CPQSSTraps	NA	This policy intercepts SNMP traps related to storage systems in terms of fan status, temperature, and power supply.	
	Sys_HPProLiant_CPQSysInfoTraps	NA	This policy intercepts SNMP traps related to system information in terms of the state of the battery, monitor, Hot Plug Slot Board, memory, and hood.	
	Sys_HPProLiant_CPQUPSTraps	NA	This policy intercepts SNMP traps related to Uninterrupted Power Supply (UPS) in terms of status, battery, and actions initiated by UPS.	
	Sys_HPProLiant_FwdDriveArrayTraps	NA	This policy intercepts SNMP traps related to Compaq's Intelligent Drive Array.	
	Sys_HPProLiant_VCDomainTraps	NA	This policy intercepts SNMP traps related to virtual connect domain.	
	Sys_HPProLiant_VCModuleTraps	NA	This policy intercepts the SNMP trap related to virtual connect module.	

Space Availability and Disk IOPS

This Aspect monitors the disk IO operations and space utilization of the system. This Aspect consists of the following policy template:

CI Type	Policy Template	Indicator	Policy Description	Policy Type
Computer	Sys_FileSystemUtilizationMonitor	DiskUsageLevel	Monitors the utilization of the file systems on the node.	Measurement Threshold Template

System Infrastructure Discovery

This Aspect discovers and gathers information regarding the system resources, operating system, and applications on a managed node. This Aspect contains the following policy templates:

CI Type	Policy Template	Indicator	Policy Description	Policy Type
Computer	OPC_PERL_INCLUDE_INSTR_DIR	NA	Is used for setting OPC_PERL_INCLUDE_INSTR_DIR in the HP Operations Agent xp1 config namespace. Set the value to TRUE for Infrastructure SPI policies to work.	Node Info Template
	Sys_SystemDiscovery	NA	Gathers service information from the managed nodes such as hardware resources, operating system attributes, and applications.	Service Auto-Discovery Template

System Fault Analysis

This Aspect monitors the kernel log file, boot log file, and event log file for critical error conditions and instructions. This Aspect contains the following policy templates:

CI Type	Policy Template	Indicator	Policy Description	Policy Type
Computer	Sys_LinuxKernelLog	NA	This policy template monitors the kernel log file /var/log/ and alerts in case of any kernel service failure. It checks for error conditions that match the <*> kernel: <@.service>: <*.msg> failed pattern in the kernel log file. If any matches are found, this condition sends an alert with minor severity.	Logfile Entry Template
Computer	Sys_LinuxBootLog	NA	This policy template monitors the boot log file /var/log/boot.log and alerts in case of any system boot errors. It	

CI Type	Policy Template	Indicator	Policy Description	Policy Type
			<p>checks for the following conditions:</p> <ul style="list-style-type: none"> • Service startup failed - Checks for error conditions that match the <*> <@.service>: <@.daemon> startup failed pattern in the boot log file. If any matches are found, this condition sends an alert with minor severity. • Service failed - Checks for error conditions that match the <*> <@.service>: <*.msg> failed pattern in the log file. If any matches are found, this condition sends an alert with critical severity. 	
Computer	Sys_LinuxSecureLog	NA	<p>This policy template alerts the user in case of any secure login failure. It checks for the error conditions that match the <*> sshd : Failed password for <@.user> from <*.host> port <#> ssh2 pattern. If any matches are found, this condition sends an alert with warning severity.</p>	
Computer	Sys_AIXErrptLog	NA	<p>This policy template monitors the errpt log file /var/opt/OV/tmp/sispi/errpt.log and generates an error report from entries in an error log. It checks for error conditions that match <@.errcode> <2#.mo><2#.dd><2#.hh><2#.mm><2#.yy> <@> <@> <@.object> <*.msgtext> each column in the errpt log file. If any matches are found, this condition sends an alert with warning severity.</p>	

CI Type	Policy Template	Indicator	Policy Description	Policy Type
Computer	Sys_MSWindowsServer_DNSWamError	NA	<p>This policy template monitors the log file for the Microsoft DNS server service and its corresponding process and forwards the error log entries with a warning, or error severity. The policy looks for the following errors recorded in the DNS log file:</p> <ul style="list-style-type: none"> • The DNS server could not allocate memory for the resource record. • The DNS server was unable to service a client request due a shortage of available memory. • The DNS server could not create a zone transfer thread. • The DNS server encountered an error while writing to a file. • The DNS server could not initialize the remote procedure call (RPC) service. 	Windows Event Log Template
Computer	Sys_MSWindowsServer_DHCPWamError	NA	<p>This policy template monitors the DHCP event logs and forwards the event log entries with warning, or error severity. The policy looks for the following errors:</p> <ul style="list-style-type: none"> • lashlpr cannot contact the NPS service. • There are no IP addresses available for BOOTP clients in the scope or superscope. • The DHCP server is unable to reach the NPS server for determining the client's NAP access state. • There are no IP addresses available for lease in the scope or superscope. 	

CI Type	Policy Template	Indicator	Policy Description	Policy Type
			<ul style="list-style-type: none"> • The DHCP service failed to initialize the audit log. • The DHCP/BINL service on the local computer has determined that it is not authorized to start. • The DHCP/BINL service on this workgroup server has encountered another server with IP Address. • The DHCP service failed to restore the DHCP registry configuration. • The DHCP service was unable to read the global BOOTP file name from the registry. • The DHCP service is not servicing any clients because there are no active interfaces. • There is no static IP address bound to the DHCP server. • The DHCP Server service failed to register with Service Controller. • The DHCP Server service failed to initialize its registry parameters. 	

CI Type	Policy Template	Indicator	Policy Description	Policy Type
Computer	Sys_MSWindowsServer_NFSWarnError	NA	This policy template monitors the NFS event logs and forwards the event log entries with warning, or error severity. The policy looks for the following errors: <ul style="list-style-type: none"> • Server for NFS detected a low disk space condition and has stopped recording audits. • The audit log has reached its maximum file size. • Server for NFS could not register with RPC Port Mapper. • The Server for NFS received a failure from the NFS driver during phase 2 initialization. 	
Computer	Sys_MSWindowsServer_TerminalServiceWarnError	NA	This policy template forwards the terminal service event logs entries with warning, or error severity. The policy looks for the following errors: <ul style="list-style-type: none"> • A connection request was denied because the terminal server is currently configured to not accept connections. • Autoreconnect failed to reconnect user to session because authentication failed. • Terminal Service start failed. • The terminal server received large number of incomplete connections. 	
Computer	Sys_MSWindowsServer_WindowsLogonWarnError	NA	This policy template monitors the Windows logon and initialization event logs and forwards the error log entries with warning, or error severity. The policy looks for the following errors recorded in the Windows log file: <ul style="list-style-type: none"> • Windows license is invalid. 	

CI Type	Policy Template	Indicator	Policy Description	Policy Type
			<ul style="list-style-type: none"> Windows license activation failed. The Windows logon process has failed to switch the desktop. The Windows logon process has unexpectedly terminated. The Windows logon process has failed to spawn a user application. The Windows logon process has failed to terminate currently logged on user's processes. The Windows logon process has failed to disconnect the user session. 	

User Logins

This Aspect checks the number of failed logins and last logins on your system. This Aspect consists of the following policy templates:

CI Type	Policy Template	Indicator	Policy Description	Policy Type
Computer	Sys_MSWindowsFailedLoginsCollector	NA	This policy checks for the number of: <ul style="list-style-type: none"> Failed login attempts on Microsoft Windows. Invalid logins, either due to unknown username or incorrect password on the managed node. 	Scheduled Task Template

CI Type	Policy Template	Indicator	Policy Description	Policy Type
			<ul style="list-style-type: none"> ■ The policy logs individual instances of failed login into the GBL_NUM_FAILED_LOGINS metric in EPC. By default, the time interval is 1 hour. 	
	Sys_ MSWindowsLastLogonsCollector	NA	This policy template performs the following tasks: <ul style="list-style-type: none"> • Checks for the logon details of all the active local user accounts on Microsoft Windows. • Logs individual instances of user logon into the SECONDS_SINCE_LASTLOGIN metric in EPC. By default, the time interval is 1 hour. 	

CI Type	Policy Template	Indicator	Policy Description	Policy Type
	Sys_UNIXFailedLoginsCollector	NA	This policy checks for the number of: <ul style="list-style-type: none"> • Failed login attempts on RHEL and SLES Linux systems, HP-UX, AIX, and Solaris operating systems. • Invalid logins, either due to unknown username or incorrect password on the managed node. <ul style="list-style-type: none"> ■ The policies log individual instances of failed login into the GBL_NUM_FAILED_LOGINS metric in EPC. By default, the time interval is 1 hour. 	
	Sys_LinuxLastLogonsCollector	NA	This policy checks for the logon details of all the active local user accounts on RHEL and SLES	

CI Type	Policy Template	Indicator	Policy Description	Policy Type
			Linux operating systems. The policy logs individual instances of user logon into the SECONDS_SINCE_LASTLOGIN metric in EPC. By default, the time interval is 1 hour.	

Note: You must have the following pre-requisites for the Sys_UNIXFailedLoginsCollector policy to function correctly when deployed on the Solaris node:

- Set the following variables in **/etc/default/login** file

```
SYSLOG=YES
```

```
SYSLOG_FAILED_LOGINS=1
```

- In **/etc/syslog.conf** file, check if the following line is present:

```
auth.notice ifdef(LOGHOST', /var/log/authlog, @loghost)
```

- Refresh syslogd using the following command:

```
svcadm refresh system/system-log
```

Sys_UNIXFailedLoginsCollector policy is deployed in the following paths:

On Solaris nodes: /var/log/authlog

On Linux nodes: lastb command

On HP-UX nodes: lastb command

On AIX nodes: /etc/security/failedlogin log

Virtualization Infrastructure Aspects

Virtualization Infrastructure Aspects monitors the resource usage and availability of host, guests or virtual machines. It includes the virtualization discovery which discovers all the elements in a virtualized environment. It ensures the environment is healthy and available. Virtualization Infrastructure Aspects monitor the VMware VirtualCenter CI types.

User Interface Reference

General	Provides an overview of the general attributes of the Virtualization Infrastructure Aspects.
CI Type	The type of CIs that can be assigned to the Aspect. This is the type of CI which is assigned to the Management Template. The Virtualization Infrastructure Aspects contain the Computer CI types.
Instrumentation	Provides an overview of the programs deployed to the CI types which contains the Aspect.
Aspects	Provides an overview of any Aspects that contain the Virtualization Infrastructure Aspect. You can expand each item in the list to see more details about the nested aspect.
Policy Templates	Provides an overview of the policy templates that contain the Virtualization Infrastructure Aspect. You can expand each item in the list to see more details about the policy template.

The Virtualization Infrastructure Aspects consists of the following:

IBM Power Guest Health

The IBM Power Guest Health Aspect monitors Guest availability in a Virtualized IBM LPAR Environment. This Aspect consists of the following policy templates:

CI Type	Policy Template	Indicator	Policy Description	Policy Type
Computer	Virt_IBMFrameAndLPARStateMonitor	NodeStatus	Monitors the IBM Frames and LPAR states.	Measurement Threshold Template
	Virt_IBMWPARStateMonitor	NodeStatus	Monitors and reports on the state of IBM WPARs.	

Note: Before deploying **Virt_IBMFrameAndLPARStateMonitor** 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.

IBM Power Guest Performance

The IBM Power Guest Performance Aspect monitors Guest performance in a Virtualized IBM LPAR Environment. This Aspect consists of the following policy templates:

CI Type	Policy Template	Indicator	Policy Description	Policy Type
Computer	Virt_IBMLPARCpuEntlUtilMonitor-AT	CPULoad	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.	Measurement Threshold Template
	Virt_IBMLPARMemoryEntlUtilMonitor-AT	MEMLoad	Calculates the current memory utilization (in percentage) of all IBM LPARs on AIX in ACTIVE state. It indicates the LPARs memory utilization against the minimum entitled memory.	

CI Type	Policy Template	Indicator	Policy Description	Policy Type
	Virt_ IBMWPARCpuEntlUtilMonitor-AT	CPUload	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.	
	Virt_ IBMWPARMemoryEntlUtilMonitor-AT	MEMLoad	Calculates the current memory utilization (in percentage) of IBM WPARs (running on the monitoring LPAR) in ACTIVE state. It indicates the WPARs memory utilization against the minimum entitled memory.	

IBM Power Host Health

The IBM Power Host Health Aspect monitors Frame memory and CPU Utilization in a Virtualized IBM LPAR environment. This Aspect consists of the following policy templates:

CI Type	Policy Template	Indicator	Policy Description	Policy Type
IBM Frame	Virt_IBMLPARFrameCPUUtilMonitor	CPUload	Monitors the LPAR Frame CPU utilization for IBM LPAR virtual infrastructure.	Measurement Threshold Template
	Virt_IBMLPARFrameMemoryUtilMonitor	MemoryLoad	Monitors the LPAR Frame Memory utilization for IBM LPAR Frame virtual infrastructure.	

KVM Guest Health

The KVM Guest Health Aspect monitors the guest availability and resources in a virtualized KVM environment. This Aspect consists of the following policy templates:

CI Type	Policy Template	Indicator	Policy Description	Policy Type
Computer (Virtualization Layer Software)	Virt_LinuxHV_GuestCPUUtilMonitor	CPUload	Monitors the CPU utilization of VMs within a host. The CPU utilization of each VM is checked against the threshold limits. In case of any violation, alerts are raised with the list of VMs on that host.	Measurement Threshold Template
	Virt_LinuxHV_StateMonitor	NodeStatus	Monitors and evaluates the KVM and Xen logical system which has any one of the states such as nostate, running, run/idle, paused, shutdown, crashed, and shut off.	

KVM Guest Performance

The KVM Guest Performance Aspect monitors the guest performance in a virtualized KVM environment. This Aspect consists of the following policy templates:

CI Type	Policy Template	Indicator	Policy Description	Policy Type
Computer (Virtualization Layer Software)	Virt_LinuxHV_DiskPhysByteRateBaseline-AT	InterfaceUtilization	Uses an instance baseline for monitoring the average number of bytes transferred per second from and to the physical disk.	Measurement Threshold Template
	Virt_LinuxHV_GuestCPUTotalUtilMonitor-AT	CPULoad	Uses the multi-instance baseline for monitoring the total CPU utilization of the guest machines.	
	Virt_LinuxHV_NetByteRateBaseline-AT	InterfaceUtilization	Uses the instance baseline for monitoring the net byte rate.	

KVM Host Health

The KVM Host Health Aspect monitors the host resource utilization in a virtualized KVM environment. This Aspect consists of the following policy templates:

CI Type	Policy Template	Indicator	Policy Description	Policy Type
Computer	Virt_LinuxHV_HostCPUUtilMonitor	CPUload	This policy template monitors the host CPU utilization for KVM and Xen systems in a virtualized environment.	Measurement Threshold Template
	Virt_LinuxHV_HostMemoryUtilMonitor	MemoryUsageLevel	This policy template monitors the host physical memory utilization for KVM and Xen systems in a virtualized environment.	

Oracle Solaris Guest Health

The Oracle Solaris Guest Health Aspect monitors guest resources in Oracle Solaris zones environment. This Aspect consists of the following policy template:

CI Type	Policy Template	Indicator	Policy Description	Policy Type
Unix	Virt_OracleSolarisStateMonitor	NodeStatus	Checks the logical system state and raises an alert for Oracle Solaris containers.	Measurement Threshold Template

Oracle Solaris Guest Performance

The Oracle Solaris Guest Performance Aspect monitors guest Performance in a virtualized Oracle Solaris environment. This Aspect consists of the following policy templates:

CI Type	Policy Template	Indicator	Policy Description	Policy Type
Unix	Virt_OracleSolarisMemoryEntUtilMonitor-AT	MemoryEntitlementUsageLevel	Calculates the current memory utilization (in	Measurement Threshold Template

CI Type	Policy Template	Indicator	Policy Description	Policy Type
			percentage) of all Solaris zones in RUNNING state. It indicates the zone's memory utilization against the minimum entitled memory.	
	Virt_OracleSolarisZoneCPUEntUtilMonitor-AT	CPUEntitlementUsageLevel	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.	

CI Type	Policy Template	Indicator	Policy Description	Policy Type
	Virt_ OracleSolarisZoneSwapUtilMonitor-AT	SwapUsageLevel	Monitors the swap utilization on Solaris zones.	

Oracle Solaris Host Health

The Oracle Solaris Host Health Aspect monitors the host resource utilization in a virtualized Oracle Solaris zones environment. This Aspect consists of the following policy templates:

CI Type	Policy Template	Indicator	Policy Description	Policy Type
Unix	Virt_ OracleSolarisHostCPUUtilMonitor	CPUload	Monitors the CPU utilization on the host servers for Solaris zones.	Measurement Threshold Template
	Virt_ OracleSolarisHostMemoryUtilMonitor	MemoryUsageLevel	Monitors the physical memory utilization on Oracle Solaris zones.	
	Virt_ OracleSolarisFmdProcessMonitor		This policy template monitors the fault manager daemon (fmd) running on Solaris zones.	

CI Type	Policy Template	Indicator	Policy Description	Policy Type
	Virt_ OracleSolarisRcapdProcessMonitor		This policy template monitors the resource capping daemon (rcapd) running on Solaris zones.	
	Virt_PerfAgentProcessMonitor		This policy template monitors the performance agent processes running on the nodes.	

VMware Cluster Performance

The VMware Cluster Performance Aspect monitors the CPU and memory utilization for VMware clusters. This Aspect consists of the following policy templates:

CI Type	Policy Template	Indicator	Policy Description	Policy Type
VMware VirtualCenter	Virt_ VMwareVCCLusterCPUPerformanceMonitor	CPUUsageLevel	Monitors the CPU Utilization at the VMware cluster level. CPU utilization of cluster can be high if: a) The CPU	Measurement Threshold Template

CI Type	Policy Template	Indicator	Policy Description	Policy Type
			utilization of the hosts in a cluster is constantly high. b) The cluster cannot perform vMotion to maximize the hardware utilization when the cluster hosts are in a saturated state.	
	Virt_VMwareVCClusterMemoryPerformance Monitor	MemoryUsageLevel	Monitors the memory utilization at the VMware cluster level. Memory utilization of cluster can be high if: a) The Memory Utilization of the hosts in a cluster is constantly high.	

CI Type	Policy Template	Indicator	Policy Description	Policy Type
			b) The cluster cannot perform vMotion to maximize the hardware utilization if the cluster hosts are in a saturated state.	

VMware Datastore Performance

The VMware Datastore Performance Aspect monitors the utilization of datastore in a VMware vSphere environment. This Aspect consists of the following policy template:

CI Type	Policy Template	Indicator	Policy Description	Policy Type
VMware VirtualCenter	Virt_VMwareVCDatastoreSpaceUtilizationMonitor	Datastore Utilization	<p>Monitors the space utilization of each VMware datastore. Space utilization of datastore can be high due to one of the following reasons.</p> <ul style="list-style-type: none"> • Snapshots: Snapshot files store information about virtual machine snapshots. 	Measurement Threshold Template

CI Type	Policy Template	Indicator	Policy Description	Policy Type
			<ul style="list-style-type: none"> <li data-bbox="1036 338 1218 772">• Other VM files: Additional files used by all other files associated with a virtual machine, such as the .vmx configuration file and log files. <li data-bbox="1036 810 1218 1209">• Other: All other non-managed files placed on the datastore, such as documentation, backups, and ISO or Floppy images. <li data-bbox="1036 1247 1218 1541">• Virtual Disks: Virtual disk files store the contents of the virtual machines hard disk drive. 	

VMware Host Health

The VMware Host Health Aspect monitors the host resource utilization in a virtualized VMware environment. This Aspect consists of the following policy templates:

CI Type	Policy Template	Indicator	Policy Description	Policy Type
VMware ESX server	Virt_VMwareVCHostCPUSaturationMonitor	CPUload	Monitors the consumption of host CPUs by virtual machines. This policy also monitors the increased CPU time of VMs within a host.	Measurement Threshold Template
	Virt_VMwareVCHostCPUUtilMonitor	CPUload	Monitors the CPU utilization for ESX or ESX/i host.	
	Virt_VMwareVCHostMemUtilMonitor	MemoryLoad	Monitors the host memory pressure on Esx/i host in a VMware environment. The factors affecting the host machines memory are memory over commitment, high memory reservations, high swap outs and ballooning in the VMs, and number of virtual machines running on the host machine.	

VMware Resource Pool Monitor

The VMware Resource Pool Monitor Aspect monitors CPU utilization levels for VMware resource pools. This Aspect consists of the following policy template:

CI Type	Policy Template	Indicator	Policy Description	Policy Type
VMware VirtualCenter	Virt_ VMwareVCRespoolCPUUtilMonitor	CPUload	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.	Measurement Threshold Template

VMware Guest Health

The VMware Guest Health Aspect monitors the guest availability and resources in a virtualized VMware environment. This Aspect consists of the following policy templates:

CI Type	Policy Template	Indicator	Policy Description	Policy Type
Computer	Virt_VMWareVCGuestStateMonitor	NodeStatus	Monitors the state of VMware logical system. It raises an alert if the VM is in On, Off, Suspended, or Unknown state.	Measurement Threshold Template

CI Type	Policy Template	Indicator	Policy Description	Policy Type
	Virt_ VMwareVCGuestCPUPerformanceMonitor	CPULoad	Monitors the CPU utilization of the guest systems and sends an alert message in case the performance level goes below the set threshold.	
	Virt_VMwareVCGuestLatencyMonitor	NA	Monitors the read or write latency of a guest leading to reduced performance of a virtual machine. An alert is raised if the read or write latency is greater than the warning threshold.	

CI Type	Policy Template	Indicator	Policy Description	Policy Type
	Virt_VMwareVCGuestMemoryPerformanceMonitor	MemoryLoad	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.	

VMware vSphere Events

The VMware vSphere Events Aspect notifies when critical events are raised from VMware vSphere environment. This Aspect consists of the following policy templates:

CI Type	Policy Template	Indicator	Policy Description	Policy Type
VMware VirtualCenter	Virt_VMwareVCEventMonitor	VMRemoval	Monitors the events from ESX vCenter server.	Measurement Threshold Template
	Virt_VMwareVCEventTypes	NA	Monitors specific events of interest by adding or removing the event types.	Config File Template

Virtual Infrastructure Discovery

The Virtual Infrastructure Discovery Aspect discovers the virtual components like hypervisor host, guest, and resource pool in a virtualization environment. This Aspect consists of the following policy template:

CI Type	Policy Template	Indicator	Policy Description	Policy Type
Computer	Virt_Discovery	NA	Discovers the virtual infrastructure components like hypervisor host, guest, and resource pool in a virtualization environment.	Service Auto-Discovery Template

Xen Guest Health

The XEN Guest Health Aspect monitors the guest availability and resources in a virtualized XEN environment. This Aspect consists of the following policy templates:

CI Type	Policy Template	Indicator	Policy Description	Policy Type
Computer (Virtualization Layer Software)	Virt_LinuxHV_GuestCPUUtilMonitor	CPULoad	Monitors the CPU utilization of VMs within a host. The CPU utilization of each VM is checked against the threshold limits. In case of any violation, alerts are raised with the list of VMs on that host.	Measurement Threshold Template
	Virt_LinuxHV_StateMonitor	NodeStatus	Monitors and evaluates the KVM and Xen logical system which has any one of the states such as nostate, running, run/idle, paused, shutdown, crashed, or shut off. An alert is raised only if the VM is in the same transient state for more than 30 minutes.	

Xen Guest Performance

The XEN Guest Performance Aspect monitors the guest performance in a virtualized XEN environment. This Aspect consists of the following policy templates:

CI Type	Policy Template	Indicator	Policy Description	Policy Type
Computer (Virtualization Layer Software)	Virt_LinuxHV_DiskPhysByteRateBaseline-AT	InterfaceUtilization	Uses an instance baseline for monitoring the average number of bytes transferred per second from and to the physical disk for KVM or XEN.	Measurement Threshold Template
	Virt_LinuxHV_GuestCPUTotalUtilMonitor-AT	CPULoad	Uses the multi-instance baseline for monitoring the total CPU utilization of the guest machines for KVM or XEN.	
	Virt_LinuxHV_NetByteRateBaseline-AT	InterfaceUtilization	Uses an instance baseline for monitoring the net byte rate for KVM or XEN.	

Xen Host Health

The XEN Host Health Aspect monitors the host resource utilization in a virtualized XEN environment. This Aspect consists of the following policy templates:

CI Type	Policy Template	Indicator	Policy Description	Policy Type
Computer	Virt_LinuxHV_HostCPUUtilMonitor	CPUload	Monitors the host CPU utilization for KVM and Xen systems in a virtualized environment. The CPU bottleneck symptom is indicated by high CPU utilization rate in the host system.	Measurement Threshold Template
	Virt_LinuxHV_HostMemoryUtilMonitor	MemoryUsageLevel	Monitors the physical memory utilization of hosts in Linux virtualization environment. The memory bottleneck symptom is indicated by high memory utilization rate along with low available memory.	

Cluster Infrastructure Aspects

Cluster Infrastructure Aspects discovers the high availability components such as cluster nodes and resource pool availability in a clustered environment. It is used to monitor the single point of failure (SPOF), quorum conditions, and node strength in a clustered environment. Cluster Infrastructure Aspects monitor the FailoverCluster CI types.

User Interface Reference

General	Provides an overview of the general attributes of the Cluster Infrastructure Aspects.
CI Type	The type of CIs that can be assigned to the Aspect. This is the type of CI which is assigned to the Management Template. The Cluster Infrastructure Aspects contain the FailoverCluster CI types.
Instrumentation	Provides an overview of the programs deployed to the CI types which contains the Aspect.

Aspects	Provides an overview of any Aspects that contain the Cluster Infrastructure Aspects. You can expand each item in the list to see more details about the nested Aspect.
Policy Templates	Provides an overview of the policy templates that contain the Cluster Infrastructure Aspects. You can expand each item in the list to see more details about the policy template.

The Cluster Infrastructure Aspects consists of the following:

Cluster Infrastructure Discovery

This Aspect discovers the high availability components such as cluster nodes and resource pool availability in a clustered environment. This Aspect consists of the following policy template:

CI Type	Policy Template	Indicator	Policy Description	Policy Type
Computer	Clus_ ClusterDiscovery	NA	Discovers the high availability infrastructure components such as cluster nodes and resource groups in a clustered environment.	Service Auto-Discovery Template

Cluster Strength and Status

This Aspect monitors the single point of failure (SPOF), quorum conditions, and node strength in a clustered environment. This Aspect consists of the following policy templates:

CI Type	Policy Template	Indicator	Policy Description	Policy Type
FailoverCluster	Clus_ ClusterDataCollector	NA	Collects the availability or state data of a cluster and logs into embedded performance component (CODA). This policy template is scheduled	Scheduled Task Template

CI Type	Policy Template	Indicator	Policy Description	Policy Type
			to run every 5 minutes.	
	Clus_ClusterMonitor	ClusterStrength	<p>Monitors the single point of failure (SPOF), quorum conditions, and node strength in a clustered environment. A single point of failure alert is raised when a single node is active and all other nodes are inactive in a cluster. This is a risk in a high availability environment. If the number of inactive nodes is greater than the number of defined nodes in a cluster, the quorum value is not met and an alert is raised.</p>	Measurement Threshold Template

CI Type	Policy Template	Indicator	Policy Description	Policy Type
	Clus_ ClusterNodeMonitor	NodeStatus	Monitors the status of a node in a clustered environment. An alert is raised when a failure is detected on the node in a cluster.	
	Clus_ ClusterResGroupMonitor	ClusterResourceGroupStatus	Monitors the state and availability of resource groups in a cluster. An alert is raised when a failure is detected on the resource group in a cluster environment. The resource group cannot provide its services unless it is resumed back again.	

Parameters

Parameters are variables that are integral components of Infrastructure Management Templates, Infrastructure Aspects, and Policy Templates. Each parameter corresponds to a variable. Parameters


contain default values that are used for monitoring the different components of Infrastructure systems. You can modify the values of the variables to suit your monitoring requirements.

Types of Parameters

OMi MP for Infrastructure parameters are grouped as follows:

- **Simple Parameter:** A simple parameter has a name and a value.
- **Instance Parameter:** An instance parameter has a name and a list of instance values.

Parameter Flags

- **Mandatory:** It is required during the assignment of a template to a CI.
- **ReadOnly:** The parameter cannot be modified while combining or assigning parameters.
- **Hidden:** This parameter will not be visible during the assignment or combining of parameters.
- **Expert:** By default, expert parameters are not shown during assignment. This must be explicitly enabled by clicking  **Show Expert Parameters**.

Infrastructure Parameters

The following table contains the list of parameters:

Parameter	Parameter Type	Description	Default Values
Avg Bytes Transferred Per Sec from this interface	Mandatory	Set the threshold value for the average bytes transferred per second at which you want to receive a <i>Major</i> severity message.	5000
		Set the threshold value for the average bytes transferred per second at which you want to receive a <i>Minor</i> severity message.	4500
		Set the threshold value for the average bytes transferred per second at which you want to receive a <i>Warning</i> severity message.	4000

Parameter	Parameter Type	Description	Default Values
Outbound Queue Length	Mandatory	Indicates the number of packets waiting in the outbound queue length for all network interfaces.	5
		Set the threshold value for outbound queue length at which you want to receive a <i>Major</i> severity message.	
		Set the threshold value for outbound queue length at which you want to receive a <i>Warning</i> severity message.	1
		Set the threshold value for outbound queue length at which you want to receive a <i>Minor</i> severity message.	3
Bandwidth Used (%)	Mandatory	Indicates the percentage of bandwidth used with respect to the total available bandwidth.	85
		Set the threshold value for bandwidth utilization at which you want to receive a <i>Major</i> severity message.	
		Set the threshold value for bandwidth utilization at which you want to receive a <i>Warning</i> severity message.	50
		Set the threshold value for bandwidth utilization at which you want to receive a <i>Minor</i> severity message.	70
Memory Utilization (%)	Mandatory	Indicates the Memory utilization for the IBM LPAR Frame virtual infrastructure.	65525
		Set the threshold value at which you want to receive a <i>Critical</i> severity message.	
		Set the threshold value at which you want to receive a <i>Major</i> severity message.	96
		Set the threshold value at which you want to receive a <i>Minor</i> severity message.	76
		Set the threshold value at which you want to receive a <i>Warning</i> severity message.	60

Parameter	Parameter Type	Description	Default Values
CPU Utilization (%)	Mandatory	Indicates the CPU utilization for IBM LPAR Frame virtual infrastructure. Set the threshold value at which you want to receive a <i>Critical</i> severity message.	65525
		Set the threshold value at which you want to receive a <i>Major</i> severity message.	92
		Set the threshold value at which you want to receive a <i>Minor</i> severity message.	80
		Set the threshold value at which you want to receive a <i>Warning</i> severity message.	70
Memory Utilization (%)	Mandatory	Indicates the physical memory utilization for Oracle Solaris zones. Set the threshold value at which you want to receive a <i>Critical</i> severity message.	65525
		Set the threshold value at which you want to receive a <i>Major</i> severity message.	90
		Set the threshold value at which you want to receive a <i>Minor</i> severity message.	80
		Set the threshold value at which you want to receive a <i>Warning</i> severity message.	70
CPU Utilization (%)	Mandatory	Indicates the CPU utilization for Oracle Solaris zones. Set the threshold value at which you want to receive a <i>Critical</i> severity message.	65525
		Set the threshold value at which you want to receive a <i>Major</i> severity message.	90
		Set the threshold value at which you want to receive a <i>Minor</i> severity message.	80
		Set the threshold value at which you want to receive a <i>Warning</i> severity message.	70
Free memory available (MB)	Mandatory	Indicates the available memory for Oracle Solaris zones. Set the threshold value at which you want to receive a <i>Critical</i> severity message.	65525

Parameter	Parameter Type	Description	Default Values
		Set the threshold value at which you want to receive a <i>Major</i> severity message.	90
		Set the threshold value at which you want to receive a <i>Minor</i> severity message.	80
		Set the threshold value at which you want to receive a <i>Warning</i> severity message.	70
Message Group	Mandatory + Expert Setting	Indicates the Message group for outgoing messages.	OS or Virtualization or HA Cluster
CPU Utilization Level (%)	Mandatory	Set the threshold value for global CPU utilization level at which you want to receive a <i>Critical</i> severity message.	65535
		Set the threshold value for global CPU utilization level at which you want to receive a <i>Major</i> severity message.	95
		Set the threshold value for global CPU utilization level at which you want to receive a <i>Warning</i> severity message.	90
		Set the threshold value for global CPU utilization level at which you want to receive a <i>Minor</i> severity message.	85
CPU Utilization Level (%)	Mandatory	Indicates the CPU utilization during a CPU Spike. Set the threshold value at which you want to receive a <i>Critical</i> severity message.	65535
		Set the threshold value at which you want to receive a <i>Major</i> severity message.	95
		Set the threshold value at which you want to receive a <i>Minor</i> severity message.	90
		Set the threshold value at which you want to receive a <i>Warning</i> severity message.	85
CPU Utilization Level In User Mode (%)	Mandatory	Set the threshold value for CPU utilization level in user mode at which you want to receive a <i>Critical</i> severity message.	65535

Parameter	Parameter Type	Description	Default Values
CPU Utilization Level In System Mode (%)	Mandatory	Set the threshold value for CPU utilization level in system mode at which you want to receive a <i>Critical</i> severity message.	65535
		Set the threshold value for CPU utilization level in system mode at which you want to receive a <i>Major</i> severity message.	35
		Set the threshold value for CPU utilization level in system mode at which you want to receive a <i>Minor</i> severity message.	30
		Set the threshold value for CPU utilization level in system mode at which you want to receive a <i>Warning</i> severity message.	25
Rate of Interrupts (%)	Mandatory	Set the threshold value for the CPU interrupt rate at which you want to receive a <i>Major</i> , <i>Warning</i> or <i>Minor</i> severity message. The threshold is expressed as the average number of device interrupts per second for the CPU during the sampling interval.	200, 180, 160
Number of free page table entries available on the system	Mandatory	Set the threshold value for the number of free page table entries available on the system at which you want to receive a <i>Critical</i> severity message. The <i>Number of free page table entries available on the system</i> parameter is applicable only to Windows OS.	-1
		Set the threshold value at which you want to receive a <i>Major</i> severity message.	5000
		Set the threshold value at which you want to receive a <i>Minor</i> severity message.	6000
		Set the threshold value at which you want to receive a <i>Warning</i> severity message.	10000
Memory Utilization (%)	Mandatory	Set the threshold value for the memory utilization at which you want to receive a <i>Critical</i> severity message.	65535
		Set the threshold value for the memory utilization at which you want to receive a <i>Major</i> severity message.	98

Parameter	Parameter Type	Description	Default Values
		Set the threshold value for the memory utilization at which you want to receive a <i>Minor</i> severity message.	96
		Set the threshold value for the memory utilization at which you want to receive a <i>Warning</i> severity message.	90
Free Memory Available (MB)	Mandatory	Set the threshold value for minimum memory available on the node at which you want to receive a <i>Major</i> , <i>Warning</i> , or <i>Minor</i> severity message. This parameter is applicable only to Windows OS.	4, 10, 1064
Memory Utilization (%)	Mandatory	Set the threshold value for minimum memory utilized on the node at which you want to receive a <i>Critical</i> severity message.	65535
		Set the threshold value for minimum memory utilized on the node at which you want to receive a <i>Major</i> severity message.	98
		Set the threshold value for minimum memory utilized on the node at which you want to receive a <i>Warning</i> severity message.	96
		Set the threshold value for minimum memory utilized on the node at which you want to receive a <i>Minor</i> severity message.	90
Swap Space Utilization (%)	Mandatory	Set the threshold value for the swap space utilized on the node at which you want to receive a <i>Critical</i> severity message.	65535
		Set the threshold value for the swap space utilized on the node at which you want to receive a <i>Major</i> severity message.	75
		Set the threshold value for the swap space utilized on the node at which you want to receive a <i>Minor</i> severity message.	70
		Set the threshold value for the swap space utilized on the node at which you want to receive a <i>Warning</i> severity message.	65

Parameter	Parameter Type	Description	Default Values
NFS space utilization	Mandatory	Monitors the disk utilization on remote filesystems (NFS). Set the threshold value for the NFS space utilized on remote filesystems at which you want to receive a <i>Critical</i> severity message.	65535
		Set the threshold value for the NFS space utilized on remote filesystems at which you want to receive a <i>Major</i> severity message.	95
		Set the threshold value for the NFS space utilized on remote filesystems at which you want to receive a <i>Minor</i> severity message.	90
		Set the threshold value for the NFS space utilized on remote filesystems at which you want to receive a <i>Warning</i> severity message.	85
CIFS space utilization	Mandatory	Monitors disk utilization on remote filesystems (CIFS). Set the threshold value for the CIFS disk utilized on remote filesystems at which you want to receive a <i>Critical</i> severity message.	65535
		Set the threshold value for the CIFS disk utilized on remote filesystems at which you want to receive a <i>Major</i> severity message.	
		Set the threshold value for the CIFS disk utilized on remote filesystems at which you want to receive a <i>Minor</i> severity message.	
		Set the threshold value for the CIFS disk utilized on remote filesystems at which you want to receive a <i>Warning</i> severity message.	
Free Swap Space Available (in Mbs)	Mandatory	Set the threshold value for free swap space available on the disk/filesystem at which you want to receive a <i>Critical</i> severity message.	32
		Set the threshold value for free swap space available on the disk/filesystem at which you want to receive a <i>Major</i> severity message.	48

Parameter	Parameter Type	Description	Default Values
		Set the threshold value for free swap space available on the disk/filesystem at which you want to receive a <i>Minor</i> severity message.	64
		Set the threshold value for free swap space available on the disk/filesystem at which you want to receive a <i>Warning</i> severity message.	96
CIFS Space Utilization (%)	Mandatory	Indicates the percentage (0 to 100%) of space utilization on the monitored remote filesystem. Set the threshold value for minimum free space on the filesystem at which you want to receive a <i>Critical</i> severity message.	65535
		Set the threshold value for minimum free space on the filesystem at which you want to receive a <i>Major</i> severity message.	95
		Set the threshold value for minimum free space on the filesystem at which you want to receive a <i>Minor</i> severity message.	90
		Set the threshold value for minimum free space on the filesystem at which you want to receive a <i>Warning</i> severity message.	85
CIFS FileSystem Type	Mandatory	Indicates the filesystem type that you would like to monitor for space utilization level. For example, if you specify <i>cifs</i> , the policy will monitor all CIFS remote filesystems for space utilization level.	cifs
NFS FileSystem Type	Mandatory + Expert Setting	Indicates the filesystem type that you would like to monitor for space utilization level. For example, if you specify <i>nfs</i> , the policy will monitor all NFS remote filesystems for space utilization level.	nfs

Parameter	Parameter Type	Description	Default Values
NFS Space Utilization (%)	Mandatory	The threshold is expressed as the percentage (0 to 100%) of space utilization on the monitored remote filesystem. Set the threshold value for minimum free space on the filesystem at which you want to receive a <i>Critical</i> severity message.	65535
		Set the threshold value for minimum free space on the filesystem at which you want to receive a <i>Major</i> severity message.	95
		Set the threshold value for minimum free space on the filesystem at which you want to receive a <i>Minor</i> severity message.	90
		Set the threshold value for minimum free space on the filesystem at which you want to receive a <i>Warning</i> severity message.	85
Summarized CPU Utilization (%)	Mandatory	Monitors the global CPU utilization level in a CPU Bottleneck situation. Set the threshold value at which you want to receive a <i>Critical</i> severity message.	65535
		Set the threshold value at which you want to receive a <i>Major</i> severity message.	95
		Set the threshold value at which you want to receive a <i>Minor</i> severity message.	90
		Set the threshold value at which you want to receive a <i>Warning</i> severity message.	85
Logical drive/fs Space Utilization	Mandatory	Indicates the space utilization for the logical drive or filesystem. Set the threshold value at which you want to receive a <i>Critical</i> severity message.	65535
		Set the threshold value at which you want to receive a <i>Major</i> severity message.	95
		Set the threshold value at which you want to receive a <i>Minor</i> severity message.	90
		Set the threshold value at which you want to receive a <i>Warning</i> severity message.	85

Parameter	Parameter Type	Description	Default Values
Space Utilization for Busiest Disk/FS (%)	Mandatory	Set the threshold value for the utilization of the busiest disk or filesystem at which you want to receive a <i>Major</i> , <i>Warning</i> , or <i>Minor</i> severity message.	95, 90, 85
Free Memory Available (MB)	Mandatory	Set the threshold value for free physical memory (in MBs) available on the disk or filesystem at which you want to receive a <i>Major</i> , <i>Warning</i> , or <i>Minor</i> severity message.	4,10,1064
Memory Page Out Rate (Pages Swapped Out/sec)	Mandatory	Set the threshold value for total number of pages swapped out from the physical memory to the disk per second at which you want to receive a <i>Major</i> , <i>Warning</i> , or <i>Minor</i> severity message.	400, 40, 0
Average number of page-ins from disk per second	Mandatory	A page-in refers to an event when pages (memory) are written to the disk. This parameter monitors the total number of page-ins from disk per second. Set the threshold value at which you want to receive a <i>Critical</i> alert.	65535
		Set the threshold value at which you want to receive a <i>Major</i> alert.	10000
		Set the threshold value at which you want to receive a <i>Minor</i> alert.	1000
		Set the threshold value at which you want to receive a <i>Warning</i> alert.	100
Memory Page Request Rate (Pages Requested/sec)	Mandatory	Set the threshold value for the number of page requests from disk per second.	100
Memory Cache Flush Rate (Data Flushes/sec)	Mandatory	Set the threshold value for the rate at which the file system cache flushes its contents to disk.	100
Disk Instance	Mandatory	Set the threshold value for space utilization at which you want to receive the <i>Critical</i> severity message.	65535
		Set the threshold value for space utilization at which you want to receive the <i>Major</i> severity message.	95

Parameter	Parameter Type	Description	Default Values
		Set the threshold value for space utilization at which you want to receive the <i>Warning</i> severity message.	90
		Set the threshold value for space utilization at which you want to receive the <i>Minor</i> severity message.	85
DiskPeakUtil	Mandatory	Monitors utilization level of fullest disk on system. Set the threshold value for space utilization at which you want to receive the <i>Critical</i> severity message.	65535
		Set the threshold value for space utilization at which you want to receive the <i>Major</i> severity message.	95
		Set the threshold value for space utilization at which you want to receive the <i>Warning</i> severity message.	90
		Set the threshold value for space utilization at which you want to receive the <i>Minor</i> severity message.	85
Ratio of collision packets to total packets transmitted out of this NIC	Mandatory	Monitors the ratio of collision packets to total packets transmitted out of NIC. Set the threshold value for collision packets that are transmitted out of NIC at which you want to receive the <i>Major</i> severity message.	5
		Set the threshold value for collision packets that are transmitted out of NIC at which you want to receive the <i>Minor</i> severity message.	3
		Set the threshold value for collision packets that are transmitted out of NIC at which you want to receive the <i>Warning</i> severity message.	2

Parameter	Parameter Type	Description	Default Values
Ratio of error packets to total packets transmitted in and out of this NIC	Mandatory	Monitors the ratio of error packets that are transmitted to and from an NIC. Set the threshold value for collision packets that are transmitted out of NIC at which you want to receive the <i>Major</i> severity message.	5
		Set the threshold value for collision packets that are transmitted out of NIC at which you want to receive the <i>Minor</i> severity message.	3
		Set the threshold value for collision packets that are transmitted out of NIC at which you want to receive the <i>Warning</i> severity message.	2
Free Space (MB) on device/filesystem	Mandatory	Indicates the free space available (in MBs) on the disk or filesystem. Set the threshold value at which you want to receive a <i>Critical</i> severity message.	-1
		Set the threshold value at which you want to receive a <i>Major</i> severity message.	64
		Set the threshold value at which you want to receive a <i>Minor</i> severity message.	96
		Set the threshold value at which you want to receive a <i>Warning</i> severity message.	128
Space Utilization (%)	Mandatory	Set the threshold value for the space utilized on the disk or filesystem at which you want to receive a <i>Major</i> , <i>Warning</i> , or <i>Minor</i> severity message.	95, 90, 85
VM CPU Utilization (%)	Mandatory	Set the threshold value for the CPU Utilization of a virtual machine at which you want to receive a <i>Major</i> , <i>Warning</i> , or <i>Minor</i> severity message.	95, 90, 85
Alert On Planned Outage	Mandatory + Expert Setting	Set the value to <code>True</code> or <code>hh:mm:ss-hh:mm:ss</code> format, if you want to receive alerts for time-bound alerting. By default, the value is set to <code>False</code> .	False

Parameter	Parameter Type	Description	Default Values
Host CPU Utilization (%)	Mandatory	Set the threshold value for the CPU utilization of a host at which you want to receive a <i>Major</i> , <i>Warning</i> , or <i>Minor</i> severity message.	95, 90, 85
Host Memory Utilization (%)	Mandatory	Set the threshold value for the memory utilization of a host at which you want to receive a <i>Major</i> , <i>Warning</i> , or <i>Minor</i> severity message.	95, 90, 85
Host Free Memory Available Thresholds (MB)	Mandatory	Set the threshold value for the free memory available of a host at which you want to receive a <i>Major</i> , <i>Warning</i> , or <i>Minor</i> severity message.	50, 200, 1024
Enable Trend Based monitoring	Mandatory	Set <i>TrendingCheckFlag</i> to On, if you want to enable trend based monitoring else set to Off state.	off
Cluster CPU Utilization Thresholds	Mandatory	Set the threshold value for the CPU utilization of a cluster at which you want to receive a <i>Major</i> , <i>Warning</i> , or <i>Minor</i> severity message.	90, 80, 70
Cluster Memory Utilization Thresholds	Mandatory	Set the threshold value for the memory utilization of a cluster at which you want to receive a <i>Major</i> , <i>Warning</i> , or <i>Minor</i> severity message.	90, 80, 70
Data Store Utilization (%)	Mandatory	Set the threshold value for the datastore (disk space) utilization at which you want to receive a <i>Major</i> , <i>Warning</i> , or <i>Minor</i> severity message.	90, 85, 80
VM CPU Utilization Thresholds	Mandatory	Set the threshold value for the logical ready utilization of a virtual machine at which you want to receive a <i>Major</i> , <i>Warning</i> , or <i>Minor</i> severity message.	90, 80, 70
Disk Read Latency for a Guest	Mandatory	Set the threshold value for the disk read latency of a guest at which you want to receive a <i>Major</i> , <i>Warning</i> , or <i>Minor</i> severity message.	50, 25, 15
Disk Write Latency for a Guest	Mandatory	Set the threshold value for the disk write latency of a guest at which you want to receive a <i>Major</i> , <i>Warning</i> , or <i>Minor</i> severity message.	50, 25, 15

Parameter	Parameter Type	Description	Default Values
VM Memory Utilization Thresholds	Mandatory	Set the threshold value for the memory utilization of a virtual machine at which you want to receive a <i>Major</i> , <i>Warning</i> , or <i>Minor</i> severity message.	90, 80, 70
Respool CPU Utilization (%)	Mandatory	Set threshold value for the CPU utilization of a resource pool at which you want to receive a <i>Major</i> , <i>Warning</i> , or <i>Minor</i> severity message.	95, 90, 85

Tuning of Parameters



You can edit the parameters of the Management Templates that are deployed to the CIs.

To edit the parameters:

1. Open the Assignments & Tuning pane:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Assignments & Tuning**.

On OMi 10.x, click **Administration > Monitoring > Assignments & Tuning**.

2. In the **Browse Views** tab, select the view that contains the CI for which you want to tune parameters. Alternatively, you can use the **Search** tab to find a CI.
3. In the list of CIs, select a CI. The Assignments pane shows details of any existing assignments for the CI.
4. Click the assignment for which you want to tune parameters. The Details of Assignment pane shows the current parameter values.
5. In the Details of Assignment pane, change the parameters:
 - a. (*Optional*). By default, the list shows only mandatory parameters. To see all parameters, click .
 - b. Select a parameter in the list, and then click .
 - o For standard parameters, the Edit Parameter dialog box opens.
Click **Value**, specify the value, and then click **OK**.
 - o For instance parameters, the Edit Instance Parameter dialog box opens.

Change the instance values if necessary, and then for each instance value, change dependent parameter values. After you change the instances and dependent parameter values, click **OK**.

6. In the Details of Assignment pane, click **Save Changes**. Operations Management deploys the new parameter values to the relevant HP Operations agent.

Configuration Items and Configuration Item Types

Configuration Item (CI) is a component that needs to be managed to deliver an IT Service. Infrastructure CIs includes IT Services, hardware, software and so on. A Configuration Item Type (CIT) describes the type of CI and its attributes. Infrastructure CIT includes Computer, VMware VirtualCenter, Unix, FailoverCluster and so on. For a list of CITs used in OMi MP for Infrastructure, see the section [CI Types Mapped in OMi](#).

CI Types Mapped in OMi

The following table lists the CITs from HP Operations Manager (HPOM) that are mapped to the RTSM database in OMi using the OMi MP for Infrastructure.

Package	CI Type
HPOprVir	Node
	Computer
	UNIX
	Windows
	VMware ESX server
	VMware Cluster
	VMware Resource Pool
	VMware Virtual Center
	VMware Datastore
	Datacenter
	Hypervisor
	IBM Frame
	IBM HMC

Package	CI Type
HPOprSys	FileSystem
	Disk Devices
HPOprClu	Cluster Software
	Failover Cluster
	Clustered Resource Group
	mscluster
	serviceguardcluster
	veritascluster

Run Time Service Model (RTSM) Views

A View enables you to visualize the context of an event. A typical View shows a subset of Infrastructure CIs and their relationships with other neighboring CIs. Using the Views, you can visualize the topology of an Infrastructure environment. In addition, Views can be used to do the following:

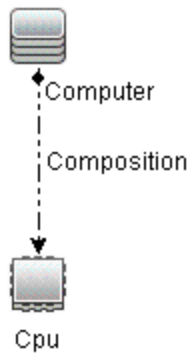
- Manage the Event Perspective of Infrastructure CIs
- Manage the Health Perspective of Infrastructure CIs
- Assign and Tune the Management Templates, Aspects, and Policy Templates

How to Access the RTSM Views

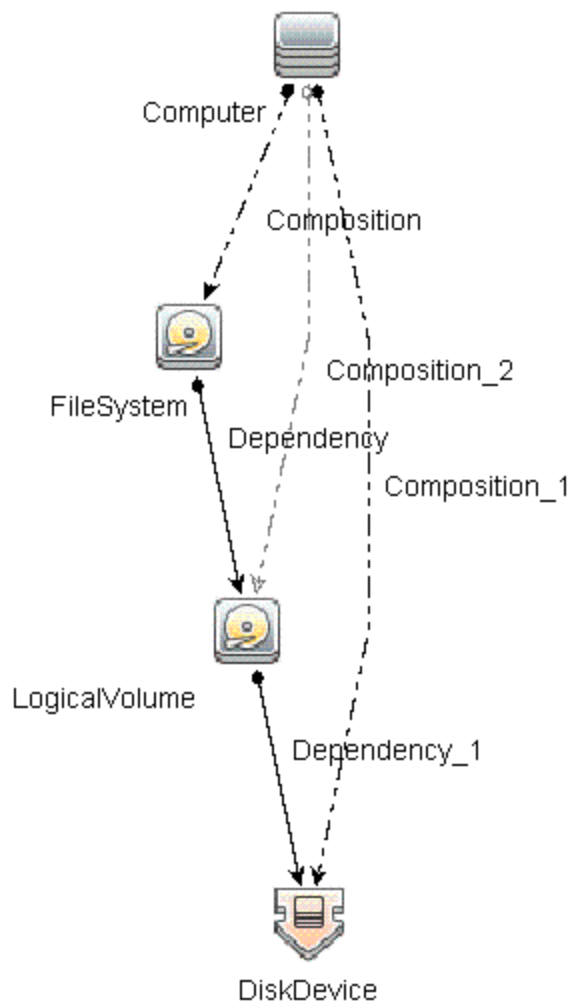
1. Open the Modeling Studio pane:
On BSM 9.2x, click **Admin > RTSM Administration > Modeling > Modeling Studio**.
On OMi 10.x, click **Administration > RTSM Administration > Modeling > Modeling Studio**.
2. Go to the **Resources** tab. Select **Views** in the **Resource Type** drop down.
3. Select **Operations Management > Infrastructure**.

The OMi MP for Infrastructure contains the following views:

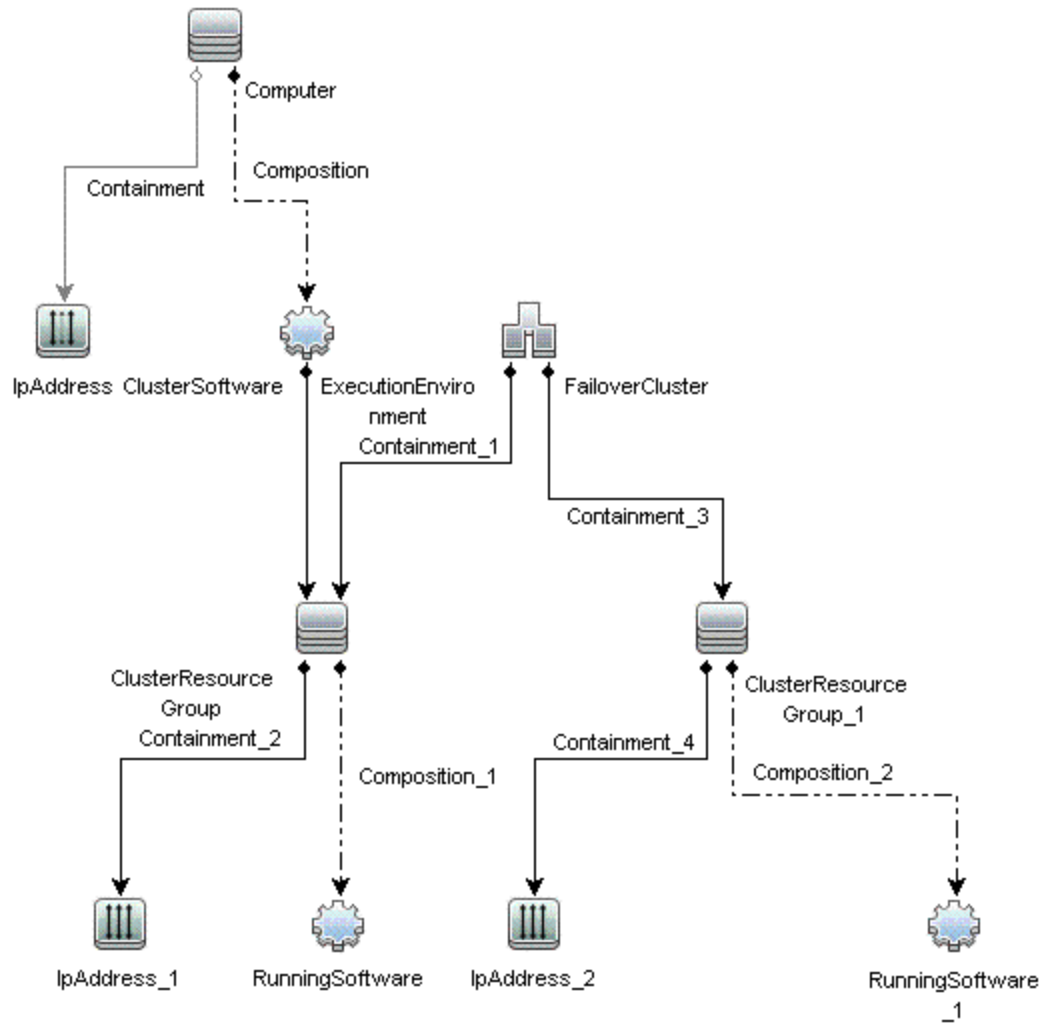
- **CPU_Infrastructure:** This view shows the CPU and Computer CI types in a pictorial format.



- **Filesystem_Infrastructure:** This view shows the File System and Computer CI types in a pictorial format.

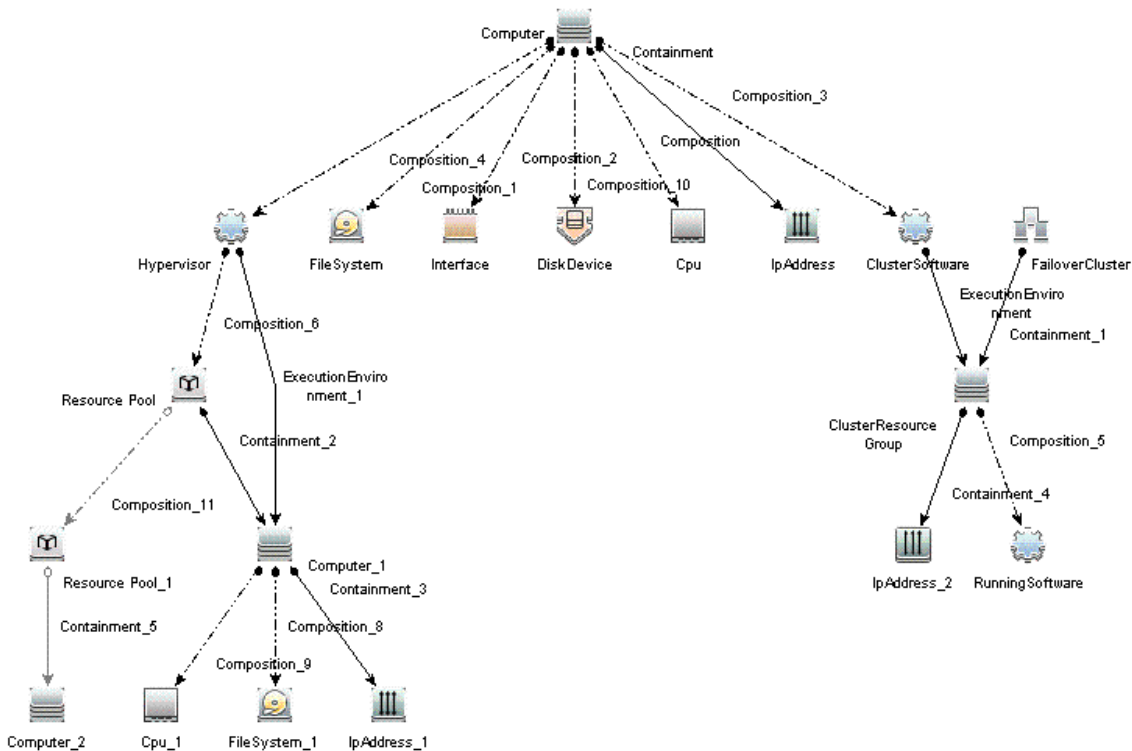


- **HACluster_Infrastructure:** This view shows the Computer (Windows or UNIX), Cluster Software, Clustered Server, Failover Cluster, Software Element, and IP Address CI types in a pictorial format.

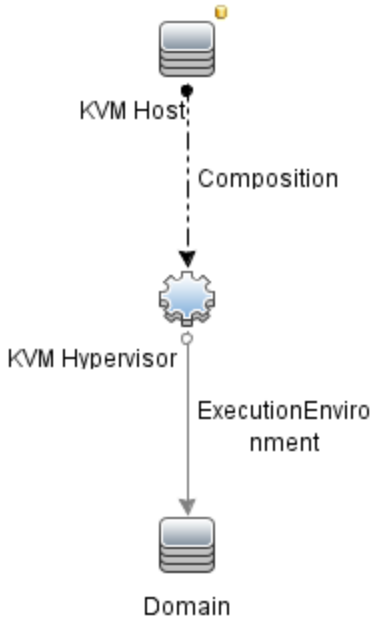


- **Infrastructure_Common:** This view represents a combined view for the HACluster_Infrastructure, Systems_Infrastructure, and Virtualization_Infrastructure views.

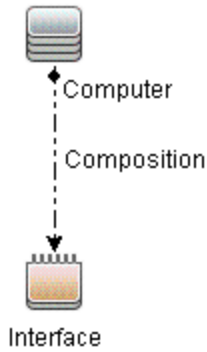
Note: CPUs and disk devices are shown only for virtualization servers.



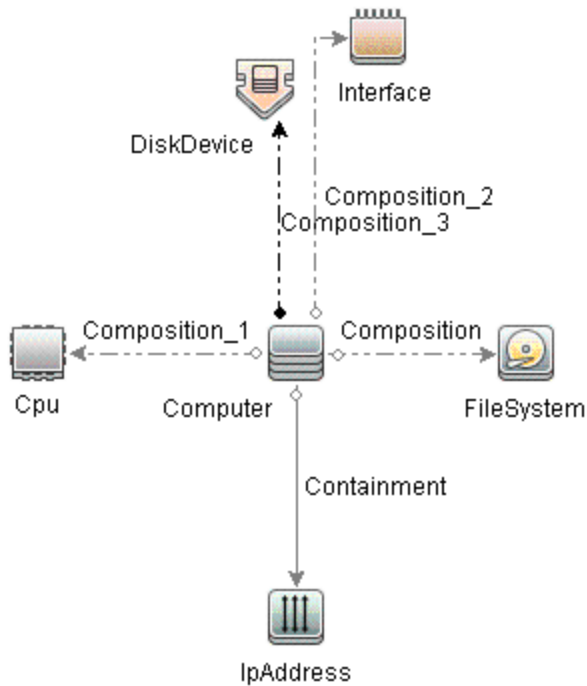
- **KVM_Infrastructure:** This view shows the KVM host, hypervisor, and domains in a pictorial format.



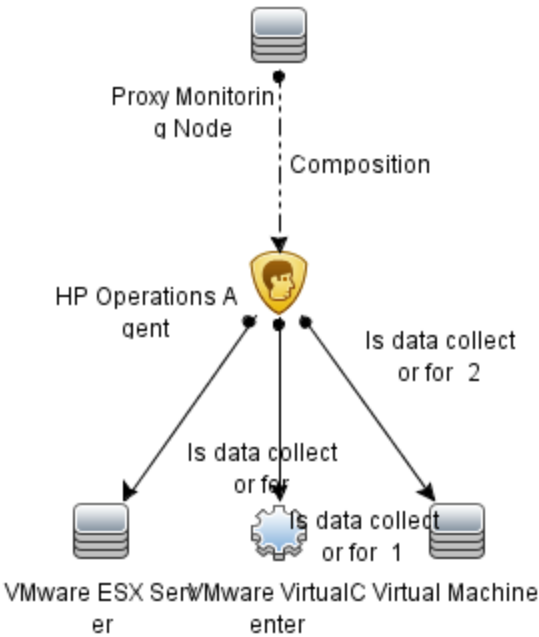
- **NetworkInterface_Infrastructure:** This view shows the Network Interface and Computer CI types in a pictorial format.



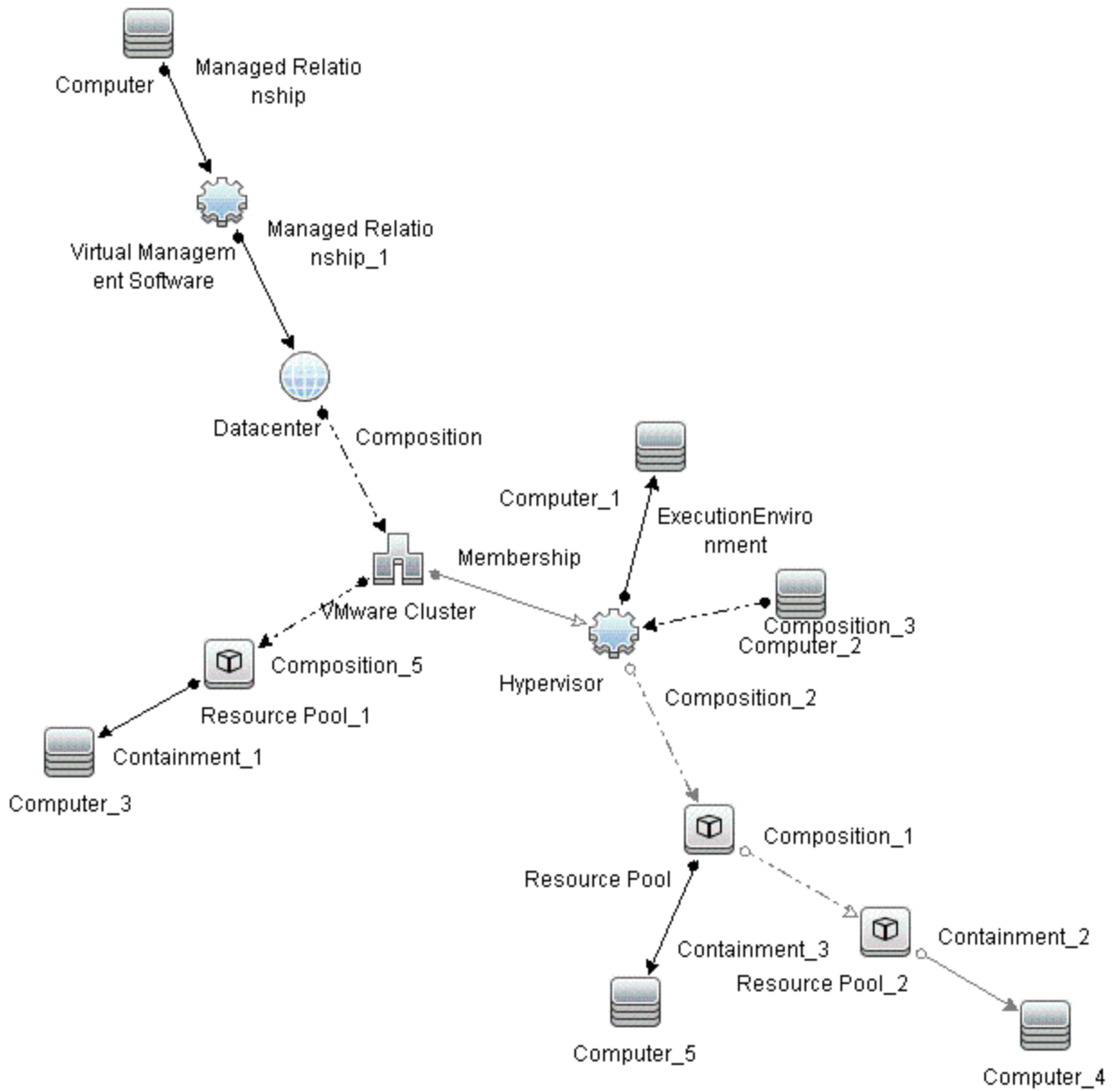
- **Systems_Infrastructure:** This view shows the relationship between the Computer (Windows or UNIX), CPU, File System, Network Interface, and IP Address CI types in a pictorial format.



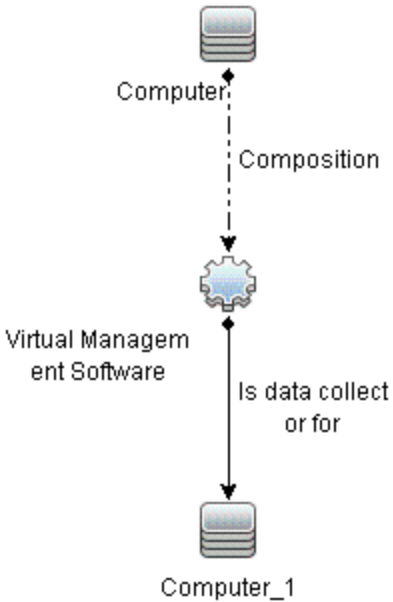
- **VA_Infrastructure:** This view shows the Proxy Node, Operations Agent and relation between Proxy Node to VMware VirtualCenter, ESX servers, and Virtual machines in a pictorial format.



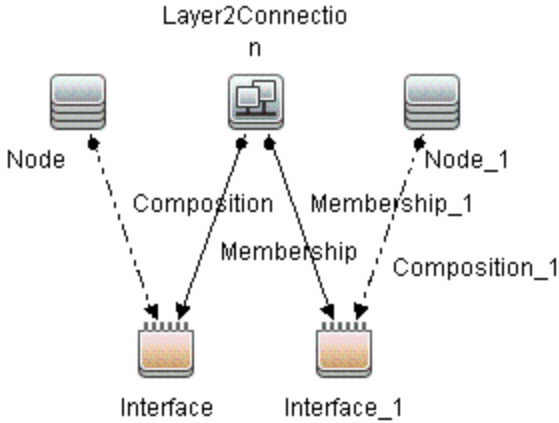
- **Virtualization_Infrastructure:** This view displays the Computer and Hypervisor CI types. The following image shows the relationship between the CI types in a pictorial format.



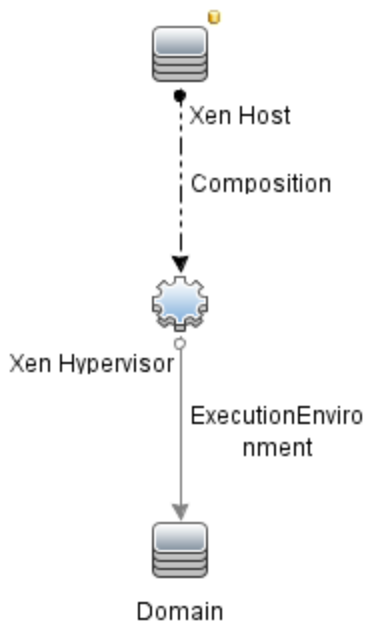
- **vMA_Infrastructure:** This view displays the vMA, virtual management software and relation between vMA and virtual machines. vMA collects the data for hosts and virtual machines in a pictorial format.



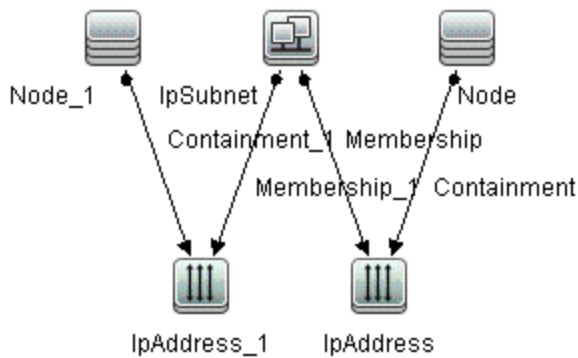
- **NNMi_Layer2**: This view displays layer 2 connectivity between servers and the switches or routers to which they are connected. The view also shows connectivity between the network switches and routers.



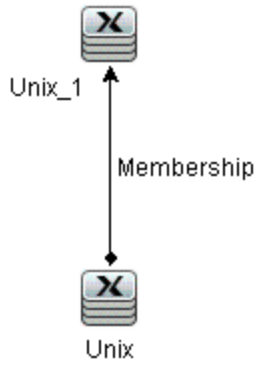
- **Xen_Infrastructure**: This view displays the Xen host, hypervisor, and domains in a pictorial format.



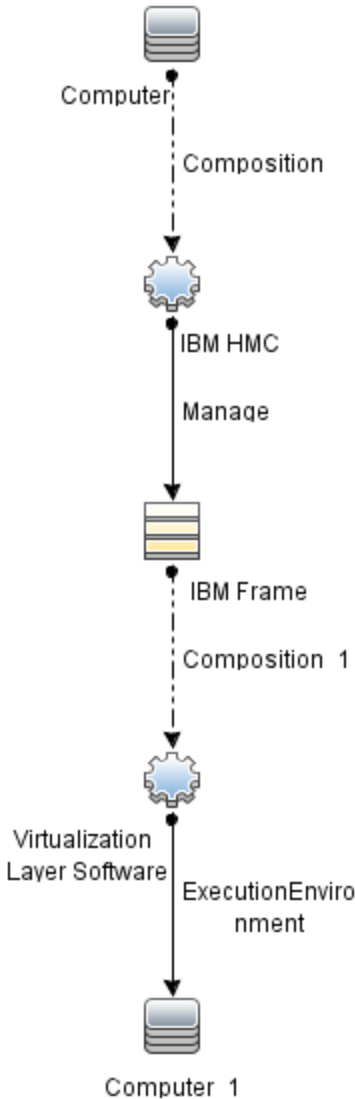
- **NNMi_Layer3:** This view displays layer 3 (IP Subnet) connectivity between servers and the switches or routers in the same subnet as the servers. The view also shows layer 3 (IP Subnet) connectivity between the network switches and routers.



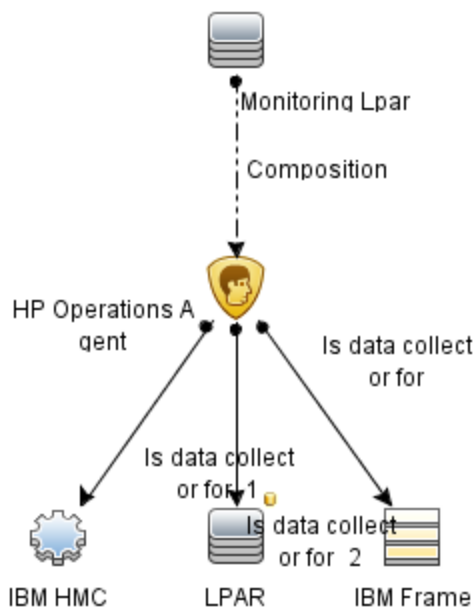
- **Sol_Zones_Infrastructure:** This view shows the relationship between the Solaris global and non-global zones in a pictorial format.



- **IBMHMC_Infrastructure:** This view displays the IBM HMC, IBM Frame, and LPARs CI types. The following image shows the relationship between the CI Types.



- **IBMHMC_Deployment:** This view shows the Monitoring LPAR and Operations Agent and relationship between Monitoring LPAR to IBM HMC, LPAR, and IBM Frame in a pictorial format.



Event Type Indicators

Event Type Indicators (ETIs) are categorization of events based on the type of occurrence.

How to Access the Event Type Indicators (ETIs)

1. Open the Indicators pane:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Indicators**.

On OMi 10.x, click **Administration > Service Health > CI Status Calculation > Health- and Event Type Indicators**.

2. In the **CI Types** tab, select **Infrastructure Element**.

The ETIs are mentioned under **Node**, **Node Element**, and **Running Software** categories.

The OMi MP for Infrastructure includes the following ETIs to monitor Infrastructure-related events. The CI Type is Computer.

ETI	Description	Value
Batch Jobs	Indicates when one or more scheduled tasks or cron jobs fail on the system.	Failed
VMCreation	Indicates when a VM is created.	Occurred
VMMigration	Indicates when a VM is migrated.	Occurred
VMRemoval	Indicates when a VM is removed.	Occurred
VMRename	Indicates when a VM is renamed.	Occurred
BatchJobService	Indicates availability of the Batch Job Service (UNIX or Linux Cron, Windows Schedule Task Services).	Available, Unavailable
DHCPService	Indicates status of the DHCP Server Service on the DHCP server system. This can be a very crucial service for many mobile users.	Available, Unavailable
DNSService	Indicates status of the DNS (Domain Nameserver) service. Multiple network dependent services could potentially fail if this service undergoes unplanned downtime.	Available, Unavailable
EventLoggingService	Indicates availability of the Event Logging service (UNIX or Linux syslog and Windows Event Logger services).	Available, Unavailable
SecureLoginService	Indicates availability of the SSH (Secure Shell) service on the host.	Available, Unavailable
WebServerService	Indicates status of the Web Server service on the system. Associated services are IIS on Windows and Apache on UNIX or Linux.	Available, Unavailable

Health Indicators

Health Indicators (HIs) analyze the events that occur in Infrastructure CIs and report the health of the Infrastructure CIs.

How to Access Health Indicators (HIs)

1. Open the Indicators pane:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Indicators**.

On OMi 10.x, click **Administration > Service Health > CI Status Calculation > Health- and Event Type Indicators**.

2. In the **CI Types** tab, click **Infrastructure Element**.

The HIs are mentioned under **Node**, **Node Element**, and **Running Software** categories.

The OMi MP for Infrastructure includes the following HIs to monitor Infrastructure-related events:

CI Type	HI	Description	Value
Layer2 Connection	L2Connection Status	Indicates that both (or all) ends of a connection are not responding to SNMP queries.	Unavailable, Available (default)
VMware Cluster	DRSStatus	Monitors the status of Distributed Resource Scheduler (DRS).	Enabled (default), Disabled
VMware Cluster	Cluster Strength	Indicates the cluster up or down status based on node strength.	Normal, Major, Critical
VMware Cluster	CPU usage level	Indicates CPU usage level.	Normal (default), Warning, Critical
VMware Cluster	Legacy System		Normal (default), Warning, Minor, Major, Critical, Unknown
VMware Cluster	Memory Usage Level	Indicates memory usage level.	Normal (default), Warning, Critical
VMware Cluster	Performance Analytics		Normal (default), Warning, Minor, Major, Critical, Informational
Node	Ping Availability	Indicates the Processing System is reachable through ping.	Available (default), Unavailable
Node	NodeStatus	Indicates the current state of the computer system. The states Unknown, Hang, and Suspended apply only to virtual machines.	Up (default), Down, Hang, Maintenance, Suspended, Unknown
Computer	CPU Entitlement UsageLevel	Indicates the percentage of entitlement (CPU cycles allotted) used by a virtual machine. May exceed 100%.	Much Lower Than Normal, Higher Than Normal, Normal (default), Lower Than Normal, Much Higher Than Normal

CI Type	HI	Description	Value
Computer	CPUload	Indicates if the system is undergoing heavy processing load.	Normal (default), Bottlenecked, Overloaded, Busy, Constrained, Critical, Warning
Computer	CPUQueue	Indicates the load on the processor job queue.	Normal (default), Overloaded, Much Lower Than Normal, Higher Than Normal, Lower Than Normal, Much Higher Than Normal
Computer	HostDisk Utilization	Indicates the utilization level for disks.	Normal (default), Much Lower Than Normal, Higher Than Normal, Lower Than Normal, Much Higher Than Normal, Critical, Warning
Computer	InterfaceError Rate	Indicates the input error rate based on the reported change in the number of input packets and the packet error count on the interface.	High, Normal (default)
Computer	Interface Utilization	Indicates the network utilization based on interface speed, and the change in number of output bytes on the interface. The queried MIB (Management Information Bases) values can vary depending on the speed of the interface and whether the system supports high speed counters for the interface.	Normal (default), Higher Than Normal, Much Higher Than Normal, Much Lower Than Normal, Lower Than Normal, High, Low, Critical, Warning, none
Computer	Interface DiscardRate	Indicates the output discard rate based on the change in the number of output packets on the interface and the discarded packet count. Packets may be discarded due to issues like buffer overflows, congestion, or system specific issues.	Normal (default), High

CI Type	HI	Description	Value
Computer	Memory Entitlement Usage Level	Indicates the memory entitlement utilization for the virtual machine. May exceed 100%.	Normal (default), Higher Than Normal, Lower Than Normal, Much Higher Than Normal, Much Lower Than Normal
Computer	MemoryLoad	Indicates the memory pressure on a computer - high memory utilization and pressure to obtain more memory through paging. If left unattended the system may reach point of excessive paging and an unstable state.	Normal (default), Paging, Starving for Memory, Bottleneck, Critical, Warning
Computer	MemoryUsage Level	Indicates the memory usage level for the system.	Normal (default), Much Lower Than Normal, Much Higher Than Normal, Lower Than Normal, Higher Than Normal, Near Capacity, Low, Critical, Warning
Computer	NetworkFile ShareUsage Level	Indicates the usage level for network file shares - Microsoft Windows Network Drives (mounts) and NFS, CIFS mounts.	Normal (default), Near Capacity
Computer	PageFile_UsageWIN	Indicates how much of the paging file capacity is used on a Window.	Normal (default), High, Near Capacity
Computer	Virtualization Overhead	Indicates the additional memory used by the VMware ESX or ESXi server to store the runtime information for virtual machines. Typically there is little variation in the value. The variation depends on size of the memory and the operating system running on the virtual machine.	Normal (default), Much Lower Than Normal, Much Higher Than Normal, Lower Than Normal, Higher Than Normal
Computer	ResourceUsage	Indicates the system resource (CPU and memory) used by the processes and services running on the system.	Normal (default), High

CI Type	HI	Description	Value
Computer	Root_disk_Usage_level	Indicates the disk usage on primary (root) disk on system. This would refer to space utilization on root (/) filesystem on UNIX and Linux systems. This would refer to C: or whatever is defined using SystemDrive setting on Windows systems.	Normal (default), High
Computer	SwapUsage Level	Indicates the swap space usage level on the system.	Normal (default), Near Capacity, Much Higher Than Normal, Much Lower Than Normal, Higher Than Normal, Lower Than Normal
Computer	KernelHandles Usage	Indicates capacity utilization by the kernel handles such as file handles, process handles, semaphores, and message queues.	Normal (default), NearCapacity
Computer	BatchJobService	Indicates the availability of the batch job services on the system such as Schedule Task Service on Microsoft Windows, and Cron services on UNIX or Linux.	Available (default), Unavailable
Computer	EventLogging Service	Indicates the availability of event logging services on the system such as event log service on Microsoft Windows and syslog services on UNIX or Linux.	Available (default), Unavailable
Computer	PrintService	Indicates the status of print services on the system such as the print spooler service on Microsoft Windows, print server role services on Windows 2008, lp, and cupsd services on UNIX or Linux.	Available (default), Unavailable
Computer	FileServer Service	Indicates the status of the file server services on the system such as FileServer role services on Microsoft Windows and NFS server and CIFS server services on UNIX or Linux.	Available (default), Unavailable

CI Type	HI	Description	Value
Computer	EmailService	Indicates the status of E-Mail service on the system such as SMTP service on Microsoft Windows and sendmail delivermail services on UNIX or Linux.	Available (default), Unavailable
Computer	WebServer Service	Indicates the status of web server services on system such as IIS services on Windows and Apache service on UNIX or Linux.	Available (default), Unavailable
Computer	RPCService	Indicates the availability of the RPC service on the system.	Available (default), Unavailable
Computer	FirewallService	Indicates the status of firewall service on the system such as Windows Firewall service on Microsoft Windows and iptables service on Linux.	Available (default), Unavailable
Computer	DNSService	Indicates the status of DNS (Domain Nameserver) service on the system.	Available (default), Unavailable
Computer	FTPService	Indicates the state of FTP services on the system. FTP protocol is used for transferring files between systems.	Available (default), Unavailable
Computer	DHCP Server Service	Indicates the status of DHCP Server Service on the DHCP server system.	Available (default), Unavailable
Computer	SecureLogin Service	Indicates the availability of SSH (Secure Shell) service on the system.	Available (default), Unavailable
UNIX	Filesystem Usage	Indicates the file system usage on the UNIX system.	Normal (default), High
UNIX	SwapSpace Available	Indicates the swap space available on the system.	Normal (default), Depleted, Near Capacity
Windows	LogicalDisk FreeSpaceWIN	Indicates the degree of logical free disk space on the system.	Normal (default), Near Capacity
Windows	TerminalServer Service	Indicates the status of services for Windows Terminal Server on the Windows system.	Available (default), Unavailable
Cluster Resource Group	Cluster Resource Group Status	Indicates the status of the resource group in a failover cluster.	Online (default) Failed, Offline, Reached SPOF condition

CI Type	HI	Description	Value
CPU	CPUUsage Level	Indicates the CPU usage level.	Normal (default), Idle, Busy, Spike, Much Higher Than Normal, Much Lower Than Normal, Higher Than Normal, Lower Than Normal, High
File System	DiskUsage Level	Indicates the disk usage level.	Normal (default), NearCapacity, Low
File System	Peak Disk Usage Level	Indicates utilization of fullest filesystem or logical desk	Normal (default), Major
Disk Device	DiskUtilization	Indicates the disk utilization level.	Normal (default), Much Higher Than Normal, Much Lower Than Normal, Higher Than Normal, Lower Than Normal
Disk Device	DiskService Time	Indicates the average of disk I/O service time.	Normal (default), Much Higher Than Normal, Much Lower Than Normal, Higher Than Normal, Lower Than Normal
Interface	InterfaceError Rate	Indicates the input error rate based on the change in the number of input packets on the interface and the packet error count.	Normal (default), High
Interface	Interface Utilization	Indicates the network utilization based on the interface speed, and the change in the number of output bytes on the interface. The queried MIB (Management Information Base) values vary based on the speed of the interface and whether the system supports high speed counters for interface.	Normal (default), Lower Than Normal, Much Lower Than Normal, High, Higher Than Normal, Much Higher Than Normal, Low, None

CI Type	HI	Description	Value
Interface	Interface DiscardRate	Indicates the output discard rate based on the change in the number of output packets on the interface and the discarded packet count. Packets may be discarded due to reasons such as receive buffer overflows, congestion, or system specific issues.	Normal (default), High
Interface	Interface Communication Status	Indicates the availability status of the interface.	Available (default), Unavailable
IpAddress	AddressStatus	Indicates the availability status of the IP Address.	Available (default), Unavailable
Cluster Software	Cluster Software Service	Indicates the availability status of the Cluster Service.	Available (default), Unavailable
Failover Cluster	Cluster Strength	Indicates the cluster availability status based on node strength.	QuorumMet (default), NotAllNodesDown, RedundantOkay, QuorumNotMet, SPOF, AllNodesDown
VMware Datastore	Datastore Utilization	Indicates high utilization on datastore	Normal (default), High
VMware Datastore	Legacy System		Normal (default), Warning, Major, Minor, Critical, Unknown
VMware Datastore	Performance Analytics		Normal (default), Warning, Major, Minor, Critical, Informational
Marge ESX Server	VMFSUsage Level	Indicates the usage level of the VMFS (Virtual Machine File System). VMFS is a clustered file system that is used by the VMware host systems to store virtual machines and virtual disk files.	Normal (default), NearCapacity
VMware ESX Server	VMwareHost NetworkUsage	Data on all network interfaces, received at or dispatched from the VMware ESX/ESXi Host (in MBs).	Normal (default), Much Higher Than Normal, Much Lower Than Normal, Higher Than Normal, Lower Than Normal

CI Type	HI	Description	Value
Hypervisor	Virtualization Service	Indicates the status of virtualization service running on Host such as Hyper-V service running on Microsoft Windows 2008 Server. The service is essential for running of virtual machines.	Available (default), Unavailable
Computer	CPU Wait	Total CPU time spent in wait state.	Low (Normal) (default), Medium (Minor), High (Critical)
Computer	Memory Compression	Amount of compressed and decompressed memory per second.	Low (Normal) (default), Medium (Minor), High (Critical)
Computer	Host Disk Load	Load on the Host storage device	Low (Normal) (default), Medium (Minor), High (Critical)
Computer	Memory Utilization	Memory usage on ESX by VM.	Low (Normal) (default), Medium (Minor), High (Critical)
Node	Ping Quality	Indicates percentage of packets reached the monitoring system.	Good (Normal) (default), Medium (Minor), Bad (Critical)
VMware ESX	CPU Ready Time	Percentage of time that the virtual machine was ready, but could not get scheduled to run on the physical CPU. CPU ready time is dependent on the number of virtual machines on the host and their CPU loads.	Low (Normal) (default), Medium (Minor), High (Critical)
Computer	CPU Usage Level	CPU Usage Level	Normal (default), Idle, Busy, Spike, Much Higher Than Normal, Much Lower Than Normal, Higher Than Normal, Lower Than Normal, High
Computer	DiskIO	Indicates the average Disk Input or Output rate on the machine.	Normal, Major
Computer	KernelLatency	Indicates the Kernel latency on the host.	Normal, Major

Topology Based Event Correlation (TBEC) Rules

In event correlation, rules are applied to identify commonly occurring events or combinations of events and helps handling of such events by automatically identifying events that can be withheld, removed or need a new event to be generated and displayed to the operators.

For more information on how the correlation rules work, see the *Operations Manager i Concepts Guide*.

How to Access the Correlation Rules

Open the Correlation Rules pane:

On BSM 9.2x, click **Admin > Operations Management > Event Correlation > Topology-Based Event Correlation**.

On OMi 10.x, click **Administration > Event Processing > Correlation > Topology-Based Event Correlation**.

The OMi MP for Infrastructure includes the following rules to correlate Infrastructure- related events.

System::Computer:CPU Load >> CPU Usage Level

Description: CPU usage of one or more CPUs on the system is high as the system is in a CPU bottleneck.		
Cause		
CIT: Computer	ETI: CPU Load	Value: Bottlenecked
Symptom		
CIT: CPU	ETI: CPU Usage Level	Value: High/ Much Higher Than Normal/ Spike

System::Computer:Memory Load >> CPU Load

Description: CPU bottleneck caused by paging		
Cause		
CIT: Computer	ETI: Memory Load	Value: Paging
Symptom		
CIT: Computer	ETI: CPU Load	Value: Bottlenecked

System::Computer:Memory Load >> Memory Usage Level

Description: Memory usage on system is high as the system is in a memory bottleneck		
Cause		
CIT: Computer	ETI: Memory Load	Value: Paging
Symptom		
CIT: Computer	ETI: Memory Usage Level	Value: Much Higher Than Normal/ Near Capacity

System::Computer:Memory Usage Level >> Swap Usage Level

Description: High memory usage results in swapping		
Cause		
CIT: Computer	ETI: Memory Usage Level	Value: Near Capacity
Symptom		
CI: Computer	ETI: Swap Usage Level	Value: Much Higher Than Normal/ Near Capacity

System Down >> System Applications Down

Description: Services or applications are unavailable as the system is down		
Cause		
CIT: Computer	ETI: Node Status	Value: Down, Suspended, Unknown
Symptom		
CIT: Computer	ETI:	Value:
	Batch Jobs	Job Failed
	E-Mail Service	Unavailable
	Event Logging Service	Unavailable
	Firewall Service	Unavailable
	WebServer Service	Unavailable
	Print Service	Unavailable
	RPC Service	Unavailable

System::Computer:Resource Usage >> CPU Usage Level

Description: Process using high amount of cpu on system causing system cpu usage high		
Cause		
CIT: Computer	ETI: Resource Usage	Value: High
Symptom		
CIT: CPU	ETI: CPU Usage Level	Value: High/ Much Higher Than Normal/ Spike

System::Computer:Resource Usage >> Memory Usage Level

Description: Process using high amount of memory on system causing system memory usage high		
Cause		
CIT: Computer	ETI: Resource Usage	Value: High
Symptom		
CIT: Computer	ETI: Memory Usage Level	Value: Higher Than Normal/ Much Higher Than Normal/ Near Capacity

System::File System:Disk Usage Level >> Swap Usage Level

Description: Swap usage caused by system drive full		
Cause		
CIT: FileSystem	ETI: Disk Usage Level	Value: Near Capacity
Symptom		
CIT: Computer	ETI: Swap Usage Level	Value: Higher Than Normal/ Much Higher Than Normal/ Near Capacity

System::Node:PingAvailability >> NodeStatus

Description: Ping availability of node failed because node is down		
Cause		
CIT: Node	ETI: Node Status	Value: Suspended, Down, Unknown
Symptom		
CIT: Node	ETI: Ping Availability	Value: Unavailable

System::File System:PingAvailability >> InterfaceCommunicationStatus

Description: Node cannot be pinged because interface communication status is unavailable		
Cause		
CIT: Interface	ETI: Interface Communication Status	Value: Unavailable
Symptom		
CIT: Interface	ETI: Ping Availability	Value: Unavailable

Virtual::Computer:Memory Usage Level >> Hypervisor Memory Usage Level

Description: Hypervisor is constrained by high memory usage done by VM		
Cause		
CIT: Computer	ETI: Memory Usage Level	Value: Much Higher Than Normal
Symptom		
CIT: Computer	ETI: Memory Usage Level	Value: Much Higher Than Normal/ Near Capacity

Virtual::Computer::CPU Usage >> Hypervisor System CPU Load

Description: A VM using high amount of physical CPU cycles on the hypervisor can cause bottleneck in Hypervisor.		
Cause		
CIT: Computer	ETI: CPU Load	Value: Bottlenecked/ Busy/ Overloaded
Symptom		
CIT: Computer	ETI: CPU Load	Value: Bottlenecked/ Busy/ Overloaded

Virtual::Computer::CPU Load>> CPU Entitlement Usage Level

Description: A VM using high amount of CPU entitled can cause CPU load to become high on server.		
Cause		
CIT: Computer	ETI: CPU Entitlement Usage Level	Value: Higher Than Normal/ Much Higher Than Normal
Symptom		

Description: A VM using high amount of CPU entitled can cause CPU load to become high on server.		
CIT: Computer	ETI: CPU Load	Value: Bottlenecked/ Busy/ Overloaded/ Constrained

Virtual::Computer::Memory Usage Level>> Memory Entitlement and Swap Usage Level

Description: Memory Entitlement and Swap Usage Level becoming high on VMs can cause High Memory Usage levels on Server.		
Cause		
CIT: Computer	ETI: Swap Usage Level	Value: Near Capacity/ Higher Than Normal/ Much Higher Than Normal
	ETI: Memory Entitlement Usage Level	Value: Higher Than Normal/ Much Higher Than Normal
Symptom		
CIT: Computer	ETI: Memory Usage Level	Value: Near Capacity/ Higher Than Normal/ Much Higher Than Normal

Hypervisor::Ping Availability >> VM::Ping Availability

Description: VMs are unavailable as the hypervisor host running the VMs is down.		
Cause		
CIT: Computer	ETI: Ping Availability	Value: Unavailable
Symptom		
CIT: Computer	ETI: Ping Availability	Value: Unavailable

Cluster Software Service Unavailable >> Clustered Server Offline

Description: Cluster software Services on cluster systems failing to run causes clustered servers (resource groups) to be inactive.		
Cause		
CIT: ClusterSoftware	ETI: Cluster Software Service	Value: Unavailable
Symptom		
CIT: ClusterResourceGroup	ETI: Cluster Resource Group Status	Value: Offline

Cluster Nodes Down >> Cluster Resource Group Impacted

Description: When 1 or more cluster nodes are down, clustered servers (resource groups) running in failover mode on these nodes are impacted		
Cause		
CIT: Computer	ETI: Node Status	Value: Down/ Hang/ Suspended/ Unknown
Symptom		
CIT: ClusterResourceGroup	ETI: Cluster Resource Group Status	Value: Offline

Cluster Members Down >> FailoverCluster Impacted (many symptoms)

Description: When a few cluster members are unavailable, the cluster is down.		
Cause		
CIT: Computer	ETI: Node Status	Value: Down/ Hang/ Suspended/ Unknown
Symptom		
CIT: FailoverCluster	ETI: Cluster Strength	Value: All Nodes Down/ Quorum Not met/ SPOF

Cluster Member Down >> Cluster Software Service Down

Description: When the cluster member is down, the cluster software service on the node is down.		
Cause		
CIT: Computer	ETI: Node Status	Value: Down/ Suspended
Symptom		
CIT: ClusterSoftware	ETI: Cluster Software Service	Value: Unavailable

Mapping Rules

The OMi MP for Infrastructure contains the following mapping rules:

CI Type: ClusterSoftware				
Name	Description	Event Filter	Indicator	Map to Indicator Value
hadUnAvailability	VCS cluster process monitor	HADMajor	Cluster Software Service	Based on Severity
hadAvailability	VCS cluster process availability	HADNormal	Cluster Software Service	Based on Severity
hashadow Unavailability	VCS cluster process unavailability	Hashadow Major	Cluster Software Service	Based on Severity
hashadow Availability	VCS cluster process availability	Hashadow Normal	Cluster Software Service	Based on Severity
HadUnavailability Windows	VCS cluster Windows Had process unavailability	HadWindows Unavailable Filter	Cluster Software Service	Based on Severity
HadAvailability WindowsFilter	VCS windows cluster service Had availability	HadWindows AvailableFilter	Cluster Software Service	Based on Severity
VCSComm UnAvailability	VCS cluster process VCSComm unavailability	VCSComm Unavailable Filter	Cluster Software Service	Based on Severity
VCSCommAvailable	VCS Cluster Windows process availability	VCSComm AvailableFilter	Cluster Software Service	Based on Severity
CmdServer UnAvailable	VCS Windows Cluster service CmdServer unavailable	CmdServer UnAvailable Filter	Cluster Software Service	Based on Severity
CmdServerAvailable	VCS Windows cluster service CmdServer availability	CmdServer Availability Filter	Cluster Software Service	Based on Severity

CI Type: ClusterSoftware				
Name	Description	Event Filter	Indicator	Map to Indicator Value
clusterUnavailability	Sun cluster process unavailability	Cluster Unavailable Filter	Cluster Software Service	Based on Severity
clusterAvailability	Sun cluster process availability	Cluster Available Filter	Cluster Software Service	Based on Severity
clurgmgrd Unavailability	Red Hat cluster process clurgmgrd unavailability	clurgmgrd Unavailable Filter	Cluster Software Service	Based on Severity
clurgmgrd Availability	Red Hat cluster process clurgmgrd availability	clurgmgrd AvailableFilter	Cluster Software Service	Based on Severity
ccsdUnavailability	Red Hat cluster process /sbin/ccsd process unavailability	ccsd Unavailable Filter	Cluster Software Service	Based on Severity
ccsdAvailable	Red Hat cluster process /sbin/ccsd process availability	ccsdAvailable Filter	Cluster Software Service	Based on Severity
ClusSvcUnavailability	Microsoft cluster service ClusSvc unavailability	ClusSvc Unavailable Filter	Cluster Software Service	Based on Severity
ClusSvcAvailability	Microsoft cluster service ClusSvc availability	ClusSvc Available Filter	Cluster Software Service	Based on Severity
cmclDUnavailability	MCSG cluster process cmclD unavailability	cmclD Unavailable Filter	Cluster Software Service	Based on Severity
cmclDAvailability	MCSH cluster process cmclD availability	cmclDAvailable Filter	Cluster Software Service	Based on Severity

CI Type: Node				
Name	Description	Event Filter	Indicator	Map to Indicator Value

CI Type: Node				
Ping Unavailability	Indicates failure to contact node using ping	Ping UnAvailability Filter	Ping Availability	Based on Severity
PingAvailability	Indicates node can be contacted using ping.	Ping UnAvailability Filter	Ping Availability	Based on Severity

Operations Orchestration (OO) Flows

When creating the mapping for the Operations Orchestration (OO) flows, you can set default values for the attributes listed in the following table. You need not specify these values each time you run the flows.

Flow input	Description
port	Port number of the HPOM Tool WS. This attribute is optional.
username	The user name for the HPOM Server that will use used in the HPOM Tool WS.
password	The password for the HPOM Server that will use used in the HPOM Tool WS.

For more information about creating the mapping and Run Book automation rules, see the topics *How to Create a Run Book Automation Rule* and *Run Books Configuration Page* in the *OMi help*.

The following section lists the OO flows:

Host Health

You can use the Host Health flow to check the health of a VmWare ESX Server.

Note: You can run this flow only on an HPOM node.

This flow analyzes the following:

- CPU Utilization
- Memory Utilization

You must map this flow to the CIT **vmware_esx_server**.

The following table lists the user input items when executing this OO flow.

Flow input	Description
hpomNode	FQDN of the ESX Server. This must be a managed node for the HPOM Server and must be specified each time you run the OO flow.

Flow input	Description
host	FQDN of the HPOM Server. You can map this input to the Event attribute Originating Server .
ESX Server Name	Name of the ESX Server. You can map this input to the CI attribute name of CI Type vmware_esx_server .

Sanity check for VISPI

You can use this flow to check the sanity of VISPI utilization.

This flow checks the following:

- Performance Agent Version
- Operations Agent Version
- Firewall Settings

You must map this flow to the CIT **UNIX** or **nt**.

Note: You can run this flow only on a node, which is monitored by HPOM Smart Plug-in for Virtualization Infrastructure.

The following table lists the user input items when executing this OO flow.

Flow input	Description
hpomNode	FQDN of the node. This must be a managed node for the HPOM Server and must be specified each time you run the OO flow.
host	FQDN of the HPOM Server. You can map this input to the Event attribute Originating Server .

VM Health

You can use this flow to check the health of a VM.

Note: You can run this flow only on an HPOM node.

This flow analyses the following:

- CPU Utilization
- Memory Utilization

You must map this flow to the CIT **host_node**.

The following table lists the user input items when executing this OO flow.

Flow input	Description
hpomNode	FQDN of the VM. This must be a managed node for the HPOM Server.
host	FQDN of the HPOM Server. You can map this input to the Event attribute Originating Server .
VM Name	Name of the VM. You can map this input to the CI attribute name of CI Type host_node .

Tools

The OMi MP for Infrastructure is packaged with tools which enable administering, monitoring, and troubleshooting the Infrastructure CIs.

How to Access Tools

- Open the Tools pane:
 - On BSM 9.2x, click **Admin > Operations Console > Tools**.
 - On OMi 10.x, click **Administration > Operations Console > Tools**.
- In the CI Types pane, click **ConfigurationItem > InfrastructureElement <CI Type>**.

The OMi MP for Infrastructure contains the following tools of CI Type Unix:

CI Type	Tool Name	Tool Description
Node	Ping node from Network Node Manager i (NNMi) server	Shows the output of a ping from the NNMi server to a selected node in a web browser. This tool requires that the NNMi server name and port are correctly configured in the HP NNMi adapter section of the general server configuration GUI.
	Ping node from NNMi server (https)	Shows the output of a ping from the NNMi server to a selected node in a web browser, using https connection. This tool requires that the NNMi server name and port are correctly configured in the HP NNMi adapter section of the general server configuration GUI.

CI Type	Tool Name	Tool Description
	Show Layer 2 Neighbors to related NNMi node	<p>Shows the Layer 2 Neighbors of the node from which the corresponding NNMi incident originated.</p> <p>This tool requires that it is started in the context of a forwarded NNMi incident, so that the message contains custom message attributes about the NNMi incident UUID, NNMi server name and the NNMi server port.</p>
	Show Layer 2 Neighbors to related NNMi node (https)	<p>Shows the Layer 2 Neighbors of the node from which the corresponding NNMi incident originated, using https connection.</p> <p>This tool requires that it is started in the context of a forwarded NNMi incident, so that the message contains custom message attributes about the NNMi incident UUID, NNMi server name and the NNMi server port.</p>
	Show Layer 3 Neighbors to related NNMi node	<p>Shows the Layer 3 Neighbors of the node from which the corresponding NNMi incident originated.</p> <p>This tool requires that it is started in the context of a forwarded NNMi incident, so that the message contains custom message attributes about the NNMi incident UUID, NNMi server name and the NNMi server port.</p>
	Show Layer 3 Neighbors to related NNMi node (https)	<p>Shows the Layer 3 Neighbors of the node from which the corresponding NNMi incident originated, using https connection.</p> <p>This tool requires that it is started in the context of a forwarded NNMi incident, so that the message contains custom message attributes about the NNMi incident UUID, NNMi server name and the NNMi server port.</p>
	Show NNMi console	<p>Shows the main console of the NNMi server in a web browser.</p> <p>This tool requires that the NNMi server name and port are correctly configured in the HP NNMi adapter section of the general server configuration GUI.</p>

CI Type	Tool Name	Tool Description
	Show NNMi console (https)	Shows the main console of the NNMi server in a web browser, using https connection. This tool requires that the NNMi server name and port are correctly configured in the HP NNMi adapter section of the general server configuration GUI.
	Show NNMi server status	Shows the status of the NNMi server processes and services in a web browser. This tool requires that the NNMi server name and port are correctly configured in the HP NNMi adapter section of the general server configuration GUI.
	Show NNMi server status (https)	Shows the status of the NNMi server processes and services in a web browser, using https connection. This tool requires that the NNMi server name and port are correctly configured in the HP NNMi adapter section of the general server configuration GUI.
	Show node information in NNMi	Shows the setup information of a selected node in a web browser. This tool requires that the NNMi server name and port are correctly configured in the HP NNMi adapter section of the general server configuration GUI.
	Show node information in NNMi (https)	Shows the setup information of a selected node in a web browser, using https connection. This tool requires that the NNMi server name and port are correctly configured in the HP NNMi adapter section of the general server configuration GUI.
	Show related NNMi incident	Shows the corresponding NNMi incident to a selected message in a web browser. This tool requires that it is started in the context of a forwarded NNMi incident, so that the message contains custom message attributes about the NNMi incident UUID, NNMi server name and the NNMi server port.

CI Type	Tool Name	Tool Description
	Show related NNMi incident (https)	Shows the corresponding NNMi incident to a selected message in a web browser, using https connection. This tool requires that it is started in the context of a forwarded NNMi incident, so that the message contains custom message attributes about the NNMi incident UUID, NNMi server name and the NNMi server port.
	Show related NNMi node	Shows the NNMi setup information for the node from which the corresponding NNMi incident originated. This tool requires that it is started in the context of a forwarded NNMi incident, so that the message contains custom message attributes about the NNMi incident UUID, NNMi server name and the NNMi server port.
	Show related NNMi node (https)	Shows the NNMi setup information for the node from which the corresponding NNMi incident originated, using https connection. This tool requires that it is started in the context of a forwarded NNMi incident, so that the message contains custom message attributes about the NNMi incident UUID, NNMi server name and the NNMi server port.
	Traceroute to node from NNMi server	Shows the output of a traceroute from the NNMi server to a selected node in a web browser. This tool requires that the NNMi server name and port are correctly configured in the HP NNMi adapter section of the general server configuration GUI.
	Traceroute to node from NNMi server (https)	Shows the output of a traceroute from the NNMi server to a selected node in a web browser, using https connection. This tool requires that the NNMi server name and port are correctly configured in the HP NNMi adapter section of the general server configuration GUI.
UNIX	VMware List VMs	Lists the Virtual Machines configured on ESX/ESXi servers managed by vMA.
	VMware Host Info	Lists information of the ESX and ESXi servers managed by vMA.
	VMware Resource Pool Info	Lists information of the Resource Pools associated with ESX/ESXi servers managed by vMA.
	VMware List Suspended VMs	Lists suspended and powered off Virtual Machines of ESX/ESXi servers managed by vMA.

Chapter 4: Customizing OMi MP for Infrastructure

OMi MP for Infrastructure can be customized to suit your monitoring requirements. You can edit the existing Infrastructure Management Templates or create new Infrastructure Management Templates to monitor the systems in your environment.

The following section provides information about the customization scenarios for OMi MP for Infrastructure.

- [Creating Infrastructure Management Templates](#)
- [Editing Infrastructure Management Templates](#)

Creating Infrastructure Management Templates


1. Open the Management Templates & Aspects pane:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Management Templates & Aspects**.


On OMi 10.x, click **Administration > Monitoring > Management Templates & Aspects**.

2. In the Configuration Folders pane:



Configuration Folders > Infrastructure Management > Infrastructure Management Templates

3. If you need to create a new configuration folder, click . The Create Configuration Folder opens.
4. Type the name of the new configuration folder and the description. For example, you can type the new configuration folder name as Test.
5. Click **OK**. The new configuration folder is created.

Configuration Folders > Infrastructure Management > Test

6. Select the new configuration folder. In the Management Templates & Aspects pane, click . The Create Management Template wizard opens.
7. In the **General** tab, type a **Name** for the new Management Template. Click **Next**.
8. Select a **Topology View** that shows the CI type that you want to manage, and all the related CI types. Click an item in the topology map to select the **CI Type** of the CIs that this Management Template enables you to manage. You can assign the type of CI to a Management Template. For

example, you can select Systems_Infrastructure as the topology view and Computer as the CI Type. Click **Next**.

9. In the **Aspects** tab, click , and then click  to add existing Aspects to the new Management Template. The Add Existing Aspect dialog box opens. Select the Aspects that you want to add, and then click **OK**.


If suitable Aspects do not exist, click , and then click  to create an Aspect.

10. For each Aspect that you add, you must specify at least one **Target CI**.

Click an Aspect in the list, and then in the topology map, click the CI types you want the Aspect to monitor when this Management Template is assigned. (Press **CTRL** to select several CI types.) Each CI type that you select here must correspond to one of the CI types assigned within the Aspect itself (or a child of one of those CI types). For example, you can select CI from the topology map.

11. In the **Parameters** tab, the list of all the parameters added to this Aspect from the policy templates is displayed.


To combine the parameters:

- a. Press **CTRL** and click the parameters that you want to combine.
- b. Click . The Edit/Combine Parameters dialog box opens.
- c. Type a **Name** for the combined parameters.
- d. (*Optional*). Specify a **Description**, **Default Value**, and whether the combined parameter is **Read Only**, an **Expert Setting**, or **Hidden**.

You can specify either a specific default value, or you can click **From CI Attribute** and then browse for a CI attribute. When you specify a CI attribute, Operations Management sets the parameter value automatically during the deployment of the underlying policy templates, using the actual value of this attribute from the CI. You can also change values of conditional parameters. (The conditions are read-only and cannot be changed at Management Template level.)

Note: Read Only prevents changes to the parameter value when the Aspect is assigned to a configuration item. Hidden also prevents changes, but additionally makes the parameter invisible. Users can choose whether to show expert settings when they make an assignment.

- e. Click **OK**.

You can also edit the parameters without combining them, to override the defaults in the Aspects or policy templates. Click one parameter, and then click . The Edit/Combine Parameters dialog box opens.

12. In the Create Management Template wizard, click **Finish** to save the Management Template and close the wizard. The new Management Template appears in the Management Templates & Aspects pane.

Editing Infrastructure Management Templates

You can edit the Management Templates to change the following artifacts:

- [Editing Parameters - Changing the default values](#)
- [Editing Aspects - Deleting an Aspect](#)

Editing Parameters - Changing the Default Values

Use Case: You are using Essential System Management Template to monitor the health of every single system in the datacenter. You are monitoring the availability and utilization of the system resources in your environment. You want to modify the parameters corresponding to the resources of the system like hardware and software to closely monitor the health of the system.

To edit the parameters:



1. Open the Management Templates & Aspects pane:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Management Templates & Aspects**.

On OMi 10.x, click **Administration > Monitoring > Management Templates & Aspects**.

2. In the Configuration Folders pane:

Configuration Folders > Infrastructure Management > Infrastructure Management Templates > Essential System Management

3. In the Management Templates & Aspects pane, select **Essential System Management** from the list, and then click . The Edit Management Template dialog box opens.
4. Click the **Parameters** tab. The list of parameters appear.
5. Double-click the desired parameter. The Edit/Combine Parameters window appears.
6. You can change the default value by clicking .

7. Specify the value and click **OK**. The Edit Management Template dialog box opens.
8. Click **OK**. The version of the Management Template is incremented.

Note: The version number of the Management Template is incremented when any customization is made to the Management Template.

Editing Aspects - Deleting an Aspect



Use Case: You are using Extensive System Management Template to monitor the performance of systems in a datacenter. You are monitoring the performance of all system resources like CPU, memory, disk, filesystem, network interface, system process and services, security, system logging and so on. You do not want to use some Aspects which are part of the Extensive System Management Template.

To edit the Aspects:

1. Open the Management Templates & Aspects pane:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Management Templates & Aspects**.

On OMi 10.x, click **Administration > Monitoring > Management Templates & Aspects**.
2. In the Configuration Folders pane:

Configuration Folders > Infrastructure Management > Infrastructure Management Templates
3. In the Management Templates & Aspects pane, select **Extensive System Management** from the list, and then click . The Edit Management Template dialog box opens.
4. Click the **Aspects** tab. The list of Aspects appear.
5. Select the Aspect that you want to delete from the list.
6. Click  to delete the selected Aspect.
7. Click **OK**. The version of the Management Template is incremented.

Chapter 5: Troubleshooting

The following section provides information about troubleshooting scenarios:

Problem: Management Templates or Aspects are not deployed on the managed nodes.

Solution: To resolve the problem, check for the following:

1. Check for assignment of Management Template or Aspect under:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Assignments & Tuning**.

On OMi 10.x, click **Administration > Monitoring > Assignments & Tuning**.

2. Check for deployment of Management Template or Aspect under:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Deployment Jobs**.

On OMi 10.x, click **Administration > Monitoring > Deployment Jobs**.

3. Check the following OMi log files:

Windows:

`%topaz_home%\log\EJBContainer\opr-webapp.log`

`%topaz_home%\log\EJBContainer\opr-configserver.log`

Linux:

`/opt/HP/BSM/log/EJBContainer/opr-webapp.log`

`/opt/HP/BSM/log/EJBContainer/opr-configserver.log`

Note: To debug a policy you must edit the policy and enable the `debug` parameter.

Problem: WPAR is not discovered in RTSM since BYLS_LS_PARENT_UUID is na

Solution: To discover WPAR, Parent UUID should not be na.

Appendix: Graph Templates

Graphs represent pictorial representation of metrics. The OMi MP for Infrastructure includes the Systems Infrastructure and Virtualization Infrastructure graph family, which is mapped to the Computer CI type. For information about creating and viewing graphs, see the *Performance Graphing* documents available in the OMi documentation. The data source used for logging data is SCOPE.

How to Access the Graphs

1. Open the Performance Graph Mapping pane:
 - On BSM 9.2x, click **Admin > Operations Console > Performance Graph Mappings**.
 - On OMi 10.x, click **Administration > Operations Console > Performance Graph Mappings**.
2. In the **CI Types** tab, click **Infrastructure Element**.

Note: The Virtualization Infrastructure graph family is visible for all nodes under the CI type Computer, however you can launch graphs only for virtual machines.

Systems Infrastructure Graph Templates

The following table lists the graph templates for System Infrastructure.

Configuration Details

The following table lists the Metric names corresponding to the Configuration Details graph template.

Metric Names	Metric Description
GBL_SYSTEM_ID	The network node hostname of the system.
GBL_OSNAME	A string representing the name of the operating system.
GBL_OSRELEASE	The current release of the operating system.
GBL_MACHINE_MODEL	CPU model
GBL_COLLECTOR	ASCII field containing collector name and version.
GBL_NUM_CPU	Number of physical CPUs on the system. This includes all CPUs, either online or offline.

Metric Names	Metric Description
GBL_NUM_DISK	Number of disks on the system. Only local disk devices are counted in this metric.
GBL_NUM_NETWORK	Number of network interfaces on the system. This includes the loopback interface.
GBL_MEM_PHYS	Amount of physical memory in the system (in MBs unless otherwise specified).
GBL_SWAP_SPACE_AVAIL_KB	Total amount of potential swap space, in KB.
TBL_PROC_TABLE_AVAIL	The configured maximum number of the proc table entries used by the kernel to manage processes. This number includes both free and used entries.
GBL_LOGGING_TYPES	A 13-byte field indicating the types of data logged by the collector. This is controlled by the LOG statement in the parm file.
GBL_THRESHOLD_CPU	The percentage of CPU that a process must use to become interesting during an interval.
GBL_THRESHOLD_PROCMEM	The virtual memory in MB that a process must use to become interesting during an interval.
GBL_THRESHOLD_DISK	The rate of physical disk IOs that a process must generate to become interesting during an interval.
GBL_LOGFILE_VERSION	Three byte ASCII field containing the log file version number.
GBL_MACHINE	An ASCII string representing the Processor Architecture.
GBL_OSKERNELTYPE_INT	This indicates the word size of the current kernel on the system.
GBL_MEM_AVAIL	The amount of physical available memory in the system (in MBs unless otherwise specified).
TBL_BUFFER_CACHE_AVAIL	The size (in KBs unless otherwise specified) of the file system buffer cache on the system
GBL_OSVERSION	A string representing the version of the operating system.
MEMORY_MEMFREE	

Metric Names	Metric Description
MEMORY_AVAILABLE_MBYTES	
MEMORY_MEMTOTAL	
MEMORY_SWAP_AVAIL	
MEMORY_SWAP_FREE	
Free swap space available	

Process Details

The following table lists the Metric names corresponding to the Process Details graph template.

Metric Names	Metric Description
PROC_PROC_NAME	The process (or kernel thread) program name.
PROC_PROC_CMD	The full command line with which the process was initiated.
PROC_PROC_ID	The process ID number (PID) of this process (associated process for kernel threads) that is used by the kernel to uniquely identify the process.
PROC_CPU_TOTAL_UTIL	The total CPU time consumed by a process (kernel thread) as a percentage of the total CPU time available during the interval.
PROC_DISK_PHYS_IO_RATE	The average number of physical disk IOs per second made by the process or kernel thread during the interval.
PROC_INTEREST	A field of flags indicating why the process was considered interesting enough to be logged.
PROC_STOP_REASON	A text string describing what caused the process (kernel thread) to stop executing.
PROC_APP_ID	The ID number of the application to which the process (kernel thread) belonged during the interval.

Metric Names	Metric Description
PROC_PRI	The dispatch or current base priority of a process (kernel thread) at the end of the interval.
PROC_MEM_RES	The size (in KB) of resident memory allocated for the process.
PROC_MEM_VIRT	The size (in KB) of virtual memory allocated for the process.
PROC_CPU_USER_UTIL	
PROC_CPU_SYS_MODE_UTIL	The percentage of time that the CPU was in system mode in the context of the process during the interval.
PROC_PARENT_PROC_ID	The parent process PID number.
PROC_USER_NAME	This is real user name of a process or the login account (from /etc/passwd) of a process.
PROC_RUN_TIME	The elapsed time since a process started, in seconds.
PROC_INTERVAL_ALIVE	The number of seconds that the process was alive during the interval.
PROCESS_PID	
PROCESS	
PROCESS_CPU0D37	
PROCESS_MEMSIZE	
PROCESS_USER	
PROCESS_PPID	
PROCESS_0D37_PROCESSOR_TIME	
PROCESS_IO_DATA_OPERATIONS_SEC	
PROCESS_PRIORITY_BASE	
PROCESS_PRIVATE_BYTES	
PROCESS_VIRTUAL_BYTES	
PROCESS_0D37_USER_TIME	
PROCESS_CREATING_PROCESS_ID	
PROCESS_ELAPSED_TIME	

CPU Gauges

The Metric name corresponding to the CPU Gauges graph template is GBL_CPU_TOTAL_UTIL. It is the percentage of time the CPU was not idle during the interval.

CPU Utilization Baseline

The Metric name corresponding to the CPU Utilization Baseline graph template is GBL_CPU_TOTAL_UTIL. It is the percentage of time the CPU was not idle during the interval.

CPU Summary

The following table lists the Metric names corresponding to the CPU Summary graph template.

Metric Names	Metric Definition
GBL_CPU_INTERRUPT_UTIL	The percentage of time that the CPU spent processing interrupts during the interval.
GBL_CPU_SYS_MODE_UTIL	Percentage of time the CPU was in system mode during the interval.
GBL_CPU_USER_MODE_UTIL	The percentage of time the CPU was in user mode during the interval.
CPU_UTILIZATION_0D37SYS	
CPU_UTILIZATION_0D37USER	
PROCESSOR_0D37_INTERRUPT_TIME	

Disk Summary

The following table lists the Metric names corresponding to the Disk Summary graph template.

Metric Names	Metric Definition
GBL_DISK_UTIL_PEAK	The utilization of the busiest disk during the interval.
GBL_FS_SPACE_UTIL_PEAK	The percentage of occupied disk space to total disk space for the fullest file system found during the interval.
GBL_DISK_PHYS_BYTE_RATE	The average number of KBs per second at which data was transferred to and from disks during the interval.
GBL_DISK_PHYS_IO_RATE	The number of physical IOs per second during the interval.
GBL_DISK_LOGL_READ_RATE	The average number of logical reads per second made during the interval.
BLOCK_DEVICE_ACTIVITY_R0D43W_S	

Metric Names	Metric Definition
PHYSICALDISK_DISK_BYTES_SEC	
LOGICALDISK_READS_SEC	

Global CPU Forecast

The Metric name corresponding to the Global CPU Forecast graph template is GBL_CPU_TOTAL_UTIL. It is the percentage of time the CPU was not idle during the interval.

Global Details

The following table lists the Metric names corresponding to the Disk Summary graph template.

Metric Names	Metric Description
GBL_CPU_TOTAL_UTIL	Percentage of time the CPU was not idle during the interval.
GBL_ACTIVE_PROC	It is the sum of the alive-process- time/interval-time ratios of every process that is active (uses any CPU time) during an interval.
GBL_PRI_QUEUE	The average number of processes or kernel threads blocked on PRI (waiting for their priority to become high enough to get the CPU) during the interval.
GBL_RUN_QUEUE	The average number of threads waiting in the runqueue over the interval.
GBL_DISK_UTIL_PEAK	The utilization of the busiest disk during the interval.
GBL_DISK_PHYS_IO_RATE	The number of physical IOs per second during the interval.
GBL_DISK_PHYS_BYTE_RATE	The average number of KBs per second at which data was transferred to and from disks during the interval.
GBL_DISK_LOGL_IO_RATE	The number of logical IOs per second during the interval.
GBL_MEM_CACHE_HIT_PCT	The percentage of buffer cache reads resolved from the buffer cache (rather than going to disk) during the interval.
GBL_MEM_PAGEOUT_RATE	The total number of page outs to the disk per second during the interval.
GBL_MEM_SWAPOUT_RATE	The number of swap outs per second during the interval.
GBL_MEM_UTIL	The percentage of physical memory in use during the interval. This includes system memory (occupied by the kernel), buffer cache and user memory.

Metric Names	Metric Description
GBL_MEM_USER_UTIL	The percent of physical memory allocated to user code and data at the end of the interval.
GBL_MEM_SYS_AND_CACHE_UTIL	The percentage of physical memory used by the system (kernel) and the buffer cache at the end of the interval.
GBL_SWAP_SPACE_UTIL	The percent of available swap space that was being used by running processes in the interval.
GBL_FS_SPACE_UTIL_PEAK	The percentage of occupied disk space to total disk space for the fullest file system found during the interval.
GBL_NET_PACKET_RATE	The number of successful packets per second (both inbound and outbound) for all network interfaces during the interval.
GBL_NET_IN_PACKET_RATE	The number of successful packets per second received through all network interfaces during the interval.
GBL_NET_OUT_PACKET_RATE	The number of successful packets per second sent through the network interfaces during the interval.
GBL_NFS_CALL_RATE	The number of NFS calls per second the system made as either a NFS client or NFS server during the interval.
GBL_NET_COLLISION_1_MIN_RATE	The number of collisions per minute on all network interfaces during the interval.
GBL_NET_ERROR_1_MIN_RATE	The number of errors per minute on all network interfaces during the interval.
GBL_SYSCALL_RATE	The average number of system calls per second during the interval.
GBL_CPU_SYS_MODE_UTIL	Percentage of time the CPU was in system mode during the interval.
GBL_CPU_USER_MODE_UTIL	Percentage of time the CPU was in user mode during the interval.
GBL_NUM_USER	The number of users logged in at the time of the interval sample.
GBL_ALIVE_PROC	It is the sum of the alive-process-time/interval-time ratios for every process.
GBL_STARTED_PROC_RATE	The number of processes that started per second during the interval.
CPU_UTILIZATION_0D37USR	

Metric Names	Metric Description
CPU_UTILIZATION_0D37SYS	
SYSTEM_SWAPPING_AND_SWITCHING_ACTIVITY_SWPOT_S	
SYSTEM_SWAPPING_AND_SWITCHING_ACTIVITY_SWPIN_S	
PAGING_ACTIVITY_PGIN_S	
PAGE0D45OUT_AND_MEMORY_FREEING_ACTIVITIES_PGOUT_S	
5MINAVG	
MEMORY_FREEMEM	
MEMORY_PERCENT_USED	
BLOCK_DEVICE_ACTIVITY_R0D43W_S	
CACHE_COPY_READ_HITS_0D37	
SYSTEM_SYSTEM_CALLS_SEC	
SYSTEM_PROCESSOR_QUEUE_LENGTH	

Global History

The following table lists the Metric names corresponding to the Global History graph template.

Metric Names	Metric Description
GBL_CPU_TOTAL_UTIL	Percentage of time the CPU was not idle during the interval.
GBL_DISK_UTIL_PEAK	The utilization of the busiest disk during the interval.
GBL_SWAP_SPACE_UTIL	The percent of available swap space that was being used by running processes in the interval.

Metric Names	Metric Description
GBL_MEM_UTIL	The percentage of physical memory in use during the interval. This includes system memory (occupied by the kernel), buffer cache and user memory.
GBL_ACTIVE_PROC	It is the sum of the alive-process- time/interval-time ratios of every process that is active (uses any CPU time) during an interval

Global Run Queue Baseline

The following table lists the Metric names corresponding to the Global Run Queue Baseline graph template.

Metric Names	Metric Description
GBL_RUN_QUEUE	The average number of threads waiting in the run queue over the interval.
SCALLS_S	
5MINAVG	
SYSTEM_PROCESSOR_QUEUE_LENGTH	

Memory Summary

The following table lists the Metric names corresponding to the Memory Summary graph template.

Metric Names	Metric Description
GBL_MEM_UTIL	The percentage of physical memory in use during the interval. This includes system memory (occupied by the kernel), buffer cache and user memory.
GBL_MEM_USER_UTIL	The percentage of physical memory allocated to user code and data at the end of the interval.
GBL_MEM_SYS_AND_CACHE_UTIL	The percentage of physical memory used by the system (kernel) and the buffer cache at the end of the interval.
GBL_MEM_CACHE_HIT_PCT	The percentage of buffer cache reads resolved from the buffer cache (rather than going to disk) during the interval.
GBL_MEM_QUEUE	The average number of processes or kernel threads blocked on memory (waiting for virtual memory disk accesses to complete) during the interval.
GBL_MEM_SWAPOUT_RATE	The number of swap outs per second during the interval.

Metric Names	Metric Description
GBL_MEM_PAGEOUT_RATE	The total number of page outs to the disk per second during the interval.
GBL_MEM_PG_SCAN_RATE	The number of pages scanned per second by the pageout daemon during the interval.
MEMORY_SWAP_FREE	
MEMORY_MEMFREE	
MEMORY_PERCENT_USED	
SYSTEM_SWAPPING_AND_SWITCHING_ACTIVITY_SWPOT_S	
CACHE_COPY_READ_HITS_0D37	

Multiple Global Forecasts

The following table lists the Metric names corresponding to the Multiple Global Forecasts graph template.

Metric Names	Metric Description
GBL_CPU_TOTAL_UTIL	Percentage of time the CPU was not idle during the interval.
GBL_DISK_UTIL_PEAK	The utilization of the busiest disk during the interval.
GBL_SWAP_SPACE_UTIL	The percentage of available swap space that was being used by running processes in the interval.
GBL_RUN_QUEUE	This is the average number of threads waiting in the runqueue over the interval.
GBL_MEM_PAGEOUT_RATE	The total number of page outs to the disk per second during the interval.
GBL_NET_IN_PACKET_RATE	The number of successful packets per second received through all network interfaces during the interval.
GBL_NET_OUT_PACKET_RATE	The number of successful packets per second sent through the network interfaces during the interval.
GBL_ACTIVE_PROC	The sum of the alive-process- time/interval-time ratios of every process that is active (uses any CPU time) during an interval.
5MINAVG	

Metric Names	Metric Description
SYSTEM_PROCESSOR_QUEUE_LENGTH	

Network Summary

The following table lists the Metric names corresponding to the Network Summary graph template.

Metric Names	Metric Description
GBL_NET_OUT_PACKET_RATE	The number of successful packets per second sent through the network interfaces during the interval.
GBL_NET_IN_PACKET_RATE	The number of successful packets per second received through all network interfaces during the interval.
GBL_NET_ERROR_RATE	The number of errors per second on all network interfaces during the interval.

Seasonal CPU Forecast

The Metric name corresponding to the Seasonal CPU Forecast graph template is GBL_CPU_TOTAL_UTIL. It is the percentage of time the CPU was not idle during the interval.

System Configuration

The following table lists the Metric names corresponding to the System Configuration graph template.

Metric Names	Metric Description
GBL_SYSTEM_ID	The network node hostname of the system.
GBL_MACHINE	An ASCII string representing the Processor Architecture.
GBL_MACHINE_MODEL	The CPU model.
GBL_CPU_CLOCK	The clock speed of the CPUs in MHz if all of the processors have the same clock speed.
GBL_OSNAME	A string representing the name of the operating system.
GBL_OSVERSION	A string representing the version of the operating system.
GBL_OSRELEASE	The current release of the operating system.
GBL_MEM_PHYS	The amount of physical memory in the system (in MBs unless otherwise specified).
GBL_ACTIVE_CPU	The number of CPUs online on the system.

Metric Names	Metric Description
GBL_NUM_CPU	The number of physical CPUs on the system. This includes all CPUs, either online or offline.
GBL_NUM_DISK	The number of disks on the system. Only local disk devices are counted in this metric.
GBL_NUM_NETWORK	The number of network interfaces on the system.
GBL_COLLECTOR	ASCII field containing collector name and version.
GBL_SWAP_SPACE_AVAIL	The total amount of potential swap space, in MB.
GBL_LOGGING_TYPES	A 13-byte field indicating the types of data logged by the collector.
GBL_THRESHOLD_CPU	The percentage of CPU that a process must use to become interesting during an interval.
GBL_GMTOFFSET	The difference, in minutes, between local time and GMT.
MEMORY_SWAP_FREE	
MEMORY_MENTOTAL	

CPU Comparison

The Metric name corresponding to the Seasonal CPU Forecast graph template is GBL_CPU_TOTAL_UTIL. It is the percentage of time the CPU was not idle during the interval.

Disk Throughput

The following table lists the Metric names corresponding to the Disk Throughput graph template.

Metric Names	Metric Description
BYDSK_PHYS_BYTE_RATE	The average KBs per second transferred to or from this disk device during the interval.
LOGICALDISK_DISK_BYTES_SEC	

Individual Networks

The following table lists the Metric names corresponding to the Individual Networks graph template.

Metric Names	Metric Description
BYNETIF_IN_BYTE_RATE	Number of KBs per second received from the network via this interface during the interval. Only the bytes in packets that carry data are included in this rate.
BYNETIF_OUT_BYTE_RATE	Number of KBs per second sent to the network via this interface during the interval. Only the bytes in packets that carry data are included in this rate.
BYNETIF_IN_PACKET_RATE	Number of successful physical packets per second received through the network interface during the interval.
BYNETIF_OUT_PACKET_RATE	Number of successful physical packets per second sent through the network interface during the interval. Successful packets are those that have been processed without errors or collisions.
NETWORK_INTERFACE_IPKTS	
NETWORK_INTERFACE_OPKTS	

Individual CPUs

The Metric name corresponding to the Individual CPUs graph template is BYCPU_CPU_TOTAL_UTIL. It is the percentage of time that this CPU was not idle during the interval.

Disk Space

The Metric name corresponding to the Disk Space graph template is FS_SPACE_UTIL. It is the percentage of the file system space in use during the interval.

Disk Details

The following table lists the Metric names corresponding to the Disk Details graph template.

Metric Names	Metric Description
BYDSK_DEVNAME	Name of the disk device
BYDSK_PHYS_READ_BYTE_RATE	The average KBs per second transferred from this disk device during the interval.
BYDSK_PHYS_READ_RATE	The average number of physical reads per second for this disk device during the interval.

Metric Names	Metric Description
BYDSK_PHYS_WRITE_BYTE_RATE	The average KBs per second transferred to this disk device during the interval.
BYDSK_PHYS_WRITE_RATE	The average number of physical writes per second for this disk device during the interval.
BYDSK_UTIL	The percentage of the time during the interval that the disk device had IO in progress from the point of view of the Operating System.
BYDSK_REQUEST_QUEUE	The average number of IO requests that were in the wait queue for this disk device during the interval.
BYDSK_AVG_SERVICE_TIME	The average time, in milliseconds, that this disk device spent processing each disk request during the interval.
BYDSK_LOGL_READ_RATE	The number of logical reads per second for this disk device during the interval.
BYDSK_LOGL_WRITE_RATE	The number of logical writes per second for this disk device during the interval.
BYDSK_DIRNAME	The name of the file system directory mounted on the disk device.
BYDSK_ID	The ID of the current disk device.
PHYSICALDISK_DISK_READS_SEC	
PHYSICALDISK_DISK_WRITES_SEC	

FileSystem Details

The following table lists the Metric names corresponding to the FileSystem Details graph template.

Metric Names	Metric Description
FS_DIRNAME	The path name of the mount point of the file system.
FS_SPACE_UTIL	Percentage of the file system space in use during the interval.
FS_MAX_SIZE	Maximum number that the file system could obtain if full, in MB.
FS_SPACE_USED	The amount of file system space in MBs that is being used.
FS_SPACE_RESERVED	The amount of file system space in MBs reserved for superuser allocation.
FS_TYPE	A string indicating the file system type.
FS_DEVNAME	The path name string of the current device.

Metric Names	Metric Description
FS_DEVNO	The major and minor number of the file system.
FS_INODE_UTIL	Percentage of the file system inodes in use during the interval.
FS_MAX_INODES	Number of configured file system inodes
FS_BLOCK_SIZE	The maximum block size of the file system, in bytes.
FS_FRAG_SIZE	The fundamental file system block size, in bytes.
FILESYSTEMS_KBYTES	
FILESYSTEMS_10240D45BLOCKS	
FILESYSTEMS_USED	
FILESYSTEMS_AVAIL	
FILESYSTEMS_FILESYSTEM	

CPU Details

The following table lists the Metric names corresponding to the CPU Details graph template.

Metric Names	Metric Description
BYCPU_ID	ID number of the CPU.
BYCPU_CPU_SYS_MODE_UTIL	The percentage of time that the CPU was in system mode during the interval.
BYCPU_CPU_USER_MODE_UTIL	The percentage of time that the CPU was in user mode during the interval.
BYCPU_CSWITCH_RATE	The average number of context switches per second for this CPU during the interval.
BYCPU_INTERRUPT_RATE	The average number of device interrupts per second for this CPU during the interval.
BYCPU_STATE	A text string indicating the current state of a processor.
BYCPU_CPU_CLOCK	The clock speed of the CPU in the current slot. The clock speed is in MHz for the selected CPU.
BYCPU_CPU_TOTAL_UTIL	The percentage of time that this CPU was not idle during the interval.
PROCESSOR_SYSTEM	

Metric Names	Metric Description
PROCESSOR_USER	
PROCESSOR_SYSEXEC	
PROCESSOR_INFO_CPU_MHZ	
CPU_UTILIZATION_0D37SYS	
CPU_UTILIZATION_0D37USR	

Network Interface Details

The following table lists the Metric names corresponding to the Network Interface Details graph template.

Metric Names	Metric Description
BYNETIF_NAME	Name of the network interface
BYNETIF_IN_BYTE_RATE	The number of KBs per second received from the network via this interface during the interval. Only the bytes in packets that carry data are included in this rate.
BYNETIF_IN_PACKET_RATE	The number of successful physical packets per second received through the network interface during the interval. Successful packets are those that have been processed without errors or collisions.
BYNETIF_OUT_BYTE_RATE	The number of KBs per second sent to the network via this interface during the interval. Only the bytes in packets that carry data are included in this rate.
BYNETIF_OUT_PACKET_RATE	The number of successful physical packets per second sent through the network interface during the interval. Successful packets are those that have been processed without errors or collisions.
BYNETIF_QUEUE	The length of the outbound queue at the time of the last sample.
BYNETIF_COLLISION_RATE	The number of physical collisions per second on the network interface during the interval.
BYNETIF_ERROR_RATE	The number of physical errors per second on the network interface during the interval.
NETWORK_INTERFACE	

Metric Names	Metric Description
NETWORK_INTERFACE_RECEIVEBYTES	
NETWORK_INTERFACE_RBYTES	
NETWORK_INTERFACE_IPACKETS	
NETWORK_INTERFACE_PACKETS_RECEIVED_SEC	
NETWORK_INTERFACE_TRANSMITBYTES	
NETWORK_INTERFACE_OPACKETS	
NETWORK_INTERFACE_PACKETS_SENT_SEC	
NETWORK_INTERFACE_COLLIS	
NETWORK_INTERFACE_COLLISIONS	
NETWORK_INTERFACE_ERRS	
NETWORK_STATS	
NETWORK_STATS_IPKTS	
NETWORK_STATS_OPKTS	
NETWORK_STATS_	

Metric Names	Metric Description
COLL	

Virtualization Infrastructure Graph Templates

The following table lists the graph templates for Virtualization Infrastructure.

Graph Templates for Virtualization Infrastructure	Metric Name	Metric Description
Virtualization Configurations	GBL_SYSTEM_ID	The network node hostname of the system.
	GBL_OSNAME	A string representing the name of the operating system.
	GBL_OSVERSION	A string representing the version of the operating system.
	GBL_OSRELEASE	The current release of the operating system.
	GBL_LS_TYPE	The virtualization technology if applicable

Graph Templates for Virtualization Infrastructure	Metric Name	Metric Description
	GBL_LS_ROLE	Indicates whether Perf Agent is installed on logical system or host or standalone system. This metric will be either "GUEST", "HOST" or "STAND".
	GBL_NUM_LS	It indicates the number of LS hosted in a system.
	GBL_NUM_CPU	The number of physical CPUs on the system. This includes all CPUs, either online or offline.
	BYLS_LS_ID	An unique identifier of the logical system.
	BYLS_LS_NAME	Name of the computer.
	BYLS_NUM_CPU	The number of virtual CPUs configured for this logical system.

Graph Templates for Virtualization Infrastructure	Metric Name	Metric Description
	BYLS_NUM_NETIF	The number of network interfaces configured for this logical system.
	BYLS_NUM_DISK	The number of disks configured for this logical system. Only local disk devices and optical devices present on the system are counted in this metric.
	BYLS_LS_OSTYPE	The Guest OS the logical system is hosting
	BYLS_CPU_ENTL_MIN	The minimum CPU units configured for the logical system.
	BYLS_CPU_ENTL_MAX	The maximum CPU units configured for a logical system.

Graph Templates for Virtualization Infrastructure	Metric Name	Metric Description
	BYLS_MEM_ENTL_MIN	In a virtual environment, this metric indicates the minimum amount of memory configured for a logical system (in MB).
	BYLS_MEM_ENTL_MAX	In a virtual environment, this metric indicates the maximum amount of memory configured for a logical system (in MB).
CPU Entitlement by Logical Systems	BYLS_CPU_ENTL_MIN	The minimum CPU units configured for the logical system.
	BYLS_CPU_ENTL_MAX	The maximum CPU units configured for a logical system.
	VMWARE_GUARANTEED0D46SUMMATION0D910D93	

Graph Templates for Virtualization Infrastructure	Metric Name	Metric Description
Percentage Utilization of CPU Entitlement by Logical Systems	BYLS_CPU_ENTL_UTIL	Percentage of entitled processing units (guaranteed processing units allocated to this logical system) consumed by the logical system.
Percentage Utilization of Total Physical CPU by Logical Systems	BYLS_CPU_PHYS_TOTAL_UTIL	Percentage of total time the physical CPUs were utilized by this logical system during the interval.
	VMWARE_USAGE0D46AVERAGE0D910D93	
CPU Details of Logical System	GBL_CPU_ENTL_UTIL	Percentage of entitled processing units (guaranteed processing units allocated to this logical system) consumed by the logical system.

Graph Templates for Virtualization Infrastructure	Metric Name	Metric Description
	GBL_CPU_PHYS_USER_MODE_UTIL	The percentage of time the physical CPU was in user mode for the logical system during the interval.
	GBL_CPU_PHYS_SYS_MODE_UTIL	The percentage of time the physical CPU was in system mode (kernel mode) for the logical system during the interval.
	GBL_CPU_PHYS_TOTAL_UTIL	The percentage of time the available physical CPUs were not idle for this logical system during the interval.
	GBL_CPU_SHARES_PRIO	The weightage or priority assigned to a Uncapped logical system.
	CPU__UTILIZATION_0D37SYS	
	CPU__UTILIZATION_0D37USR	

Graph Templates for Virtualization Infrastructure	Metric Name	Metric Description
CPU Summary by Logical Systems	BYLS_LS_ID	An unique identifier of the logical system.
	BYLS_CPU_ENTL_UTIL	Percentage of entitled processing units (guaranteed processing units allocated to this logical system) consumed by the logical system.
	BYLS_CPU_USER_MODE_UTIL	On vMA, for a host and a logical system, this metric indicates the percentage of time the CPU was in user mode during the interval.
	BYLS_CPU_SYS_MODE_UTIL	On vMA, for a host and a logical system, this metric indicates the percentage of time the CPU was in system mode.

Graph Templates for Virtualization Infrastructure	Metric Name	Metric Description
	BYLS_CPU_PHYS_TOTAL_UTIL	Percentage of total time the physical CPUs were utilized by this logical system during the interval.
	BYLS_CPU_SHARES_PRIO	This metric indicates the weightage or priority assigned to a Uncapped logical system.
	VMWARE_USAGE0D46AVERAGE0D910D93	
	VMWARE_READY0D46SUMMATION0D910D93	
	VMWARE_EXTRA0D46SUMMATION0D910D93	
Percentage Utilization of Memory Entitlement by Logical Systems	BYLS_MEM_ENTL_UTIL	The percentage of entitled memory in use during the interval.
Memory Summary by Logical Systems	BYLS_LS_ID	An unique identifier of the logical system.

Graph Templates for Virtualization Infrastructure	Metric Name	Metric Description
	BYLS_MEM_ENTL_UTIL	The percentage of entitled memory in use during the interval. This includes system memory (occupied by the kernel), buffer cache and user memory.
	BYLS_MEM_PHYS_UTIL	On vMA, the metric indicates the percentage of physical memory used during the interval by a host, logical system.
	BYLS_MEM_SWAPPED	PLATFORMS: Linux On vMA, for a host, logical system and resource pool, this metrics indicates the amount of memory that has been transparently swapped to and from the disk.

Graph Templates for Virtualization Infrastructure	Metric Name	Metric Description
	BYLS_MEM_OVERHEAD	The amount of memory associated with a logical system, that is currently consumed on the host system, due to virtualization.
	BYLS_MEM_SHARES_PRIO	The weightage or priority for memory assigned to this logical system.
	VMWARE_ACTIVE0D46AVERAGE0D910D93	
	VMWARE_USAGE0D46AVERAGE0D910D93	
	VMWARE_SWAPPED0D46AVERAGE0D910D93	
	VMWARE_OVERHEAD0D46AVERAGE0D910D93	
CPU Entitlement Utilization Baseline	BYLS_CPU_ENTL_UTIL	Percentage of entitled processing units (guaranteed processing units allocated to this logical system) consumed by the logical system.

Graph Templates for Virtualization Infrastructure	Metric Name	Metric Description
VMware ESX/ESXi Host Memory Utilization	BYLS_MEM_PHYS_UTIL	The metric indicates the percentage of physical memory used during the interval by a host, logical system.
VMware ESX/ESXi Host Memory Utilization	VMWARE_USAGE0D46AVERAGE0D910D93	
VMware ESX/ESXi Host Memory Utilization Baseline	BYLS_MEM_PHYS_UTIL	The metric indicates the percentage of physical memory used during the interval by a host, logical system.
VMware ESX/ESXi Host Memory Utilization Baseline	VMWARE_USAGE0D46AVERAGE0D910D93	
VMware ESX/ESXi Host Disk Utilization	BYLS_DISK_UTIL	The average percentage of time during the interval (average utilization) that all the disks had IO in progress.
VMware ESX/ESXi Host Disk Utilization	VMWARE_USAGE0D46AVERAGE0D910D93	
VMware ESX/ESXi Host Disk Utilization	VMWARE_READ0D46AVERAGE0D910D93	
VMware ESX/ESXi Host Disk Utilization	VMWARE_WRITE0D46AVERAGE0D910D93	

Graph Templates for Virtualization Infrastructure	Metric Name	Metric Description
VMware ESX/ESXi Host - Network MB	BYLS_NET_IN_BYTE	Number of bytes, in MB, received during the interval.
VMware ESX/ESXi Host - Network MB	BYLS_NET_OUT_BYTE	Number of bytes, in MB, transmitted during the interval.
VMware ESX/ESXi Host - Network MB	VMWARE_USAGE0D46AVERAGE0D910D93	
VMware ESX/ESXi - CPU Utilization across Resource Pools	BYLS_CPU_PHYS_TOTAL_UTIL	Percentage of total time the physical CPUs were utilized by the logical system during the interval.
	VMWARE_USAGE0D46AVERAGE0D910D93	
IBM LPAR Frame level CPU Utilization	BYLS_CPU_TOTAL_UTIL	Percentage of total time the logical CPUs were not idle during this interval.
IBM LPAR - CPU Utilization across Frame and LPARs	BYLS_NUM_CPU	The number of virtual CPUs configured for the logical system.
IBM LPAR - CPU Utilization across Frame and LPARs	BYLS_CPU_PHYSC	This metric indicates the number of CPU units utilized by the logical system.

Graph Templates for Virtualization Infrastructure	Metric Name	Metric Description
IBM LPAR - CPU Utilization across Frame and LPARs	$(\text{BYLS_NUM_CPU} * (\text{BYLS_CPU_TOTAL_UTIL} / 100))$	Number of CPU units being used.
IBM LPAR - Memory Utilization across Frame and LPARs	BYLS_MEM_ENTL_UTIL	The percentage of entitled memory in use during the interval. This includes system memory (occupied by the kernel), buffer cache and user memory.

Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on User Guide (OMi Management Pack for Infrastructure 1.12)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to docfeedback@hp.com.

We appreciate your feedback!