Operations Smart Plug-in for Cluster Infrastructure

Software Version: 12.06
Operations Manager for Windows®, HP-UX, Linux, and Solaris

User Guide

Document Release Date: May 2018
Software Release Date: May 2018

Legal Notices

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus 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. Except as specifically indicated, valid license from Micro Focus required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of the Microsoft group of companies.

UNIX® is a registered trademark of The Open Group.

Documentation Updates

To check for recent updates or to verify that you are using the most recent edition of a document, go to: https://softwaresupport.softwaregrp.com/.

This site requires that you register for an Passport and to sign in. To register for an Passport ID, click **Register** on the Software Support site or click **Create an Account** on the Passport login page.

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

Support

Visit the Software Support site at: https://softwaresupport.softwaregrp.com/.

Most of the support areas require that you register as an Passport user and to sign in. Many also require a support contract. To register for an Passport ID, click **Register** on the Support site or click **Create an Account** on the Passport login page.

Contents

Chapter 1: Conventions Used in this Document

The following conventions are used in this document.

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

Chapter 2: Introduction

The Smart Plug-in for Cluster Infrastructure (CI SPI) helps you monitor high availability (HA) cluster infrastructure on the network. The HA clusters are created to ensure the service availability specially for business critical applications and services. The HA clusters have redundant nodes. This redundancy provides high availability of services by eliminating single points of failure. The CI SPI helps to monitor and analyze the availability and state of cluster components such as cluster nodes and cluster resource groups, along with the process and services running on them.

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

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

The CI SPI integrates with other software products such as the Operations Manager (OM), Reporter, and Embedded Performance Component (EPC) of Operations Agent. The integration provides policies, tools, and the additional perspective of Service Views.

The current version of CI SPI monitors clusters on Windows, Linux, Solaris, AIX, and HP-UX operating systems. For information about the versions of operating system and clusters supported by the Cluster Infrastructure SPI, see the *Operations Smart Plug-in for Cluster Infrastructure Release Notes.*

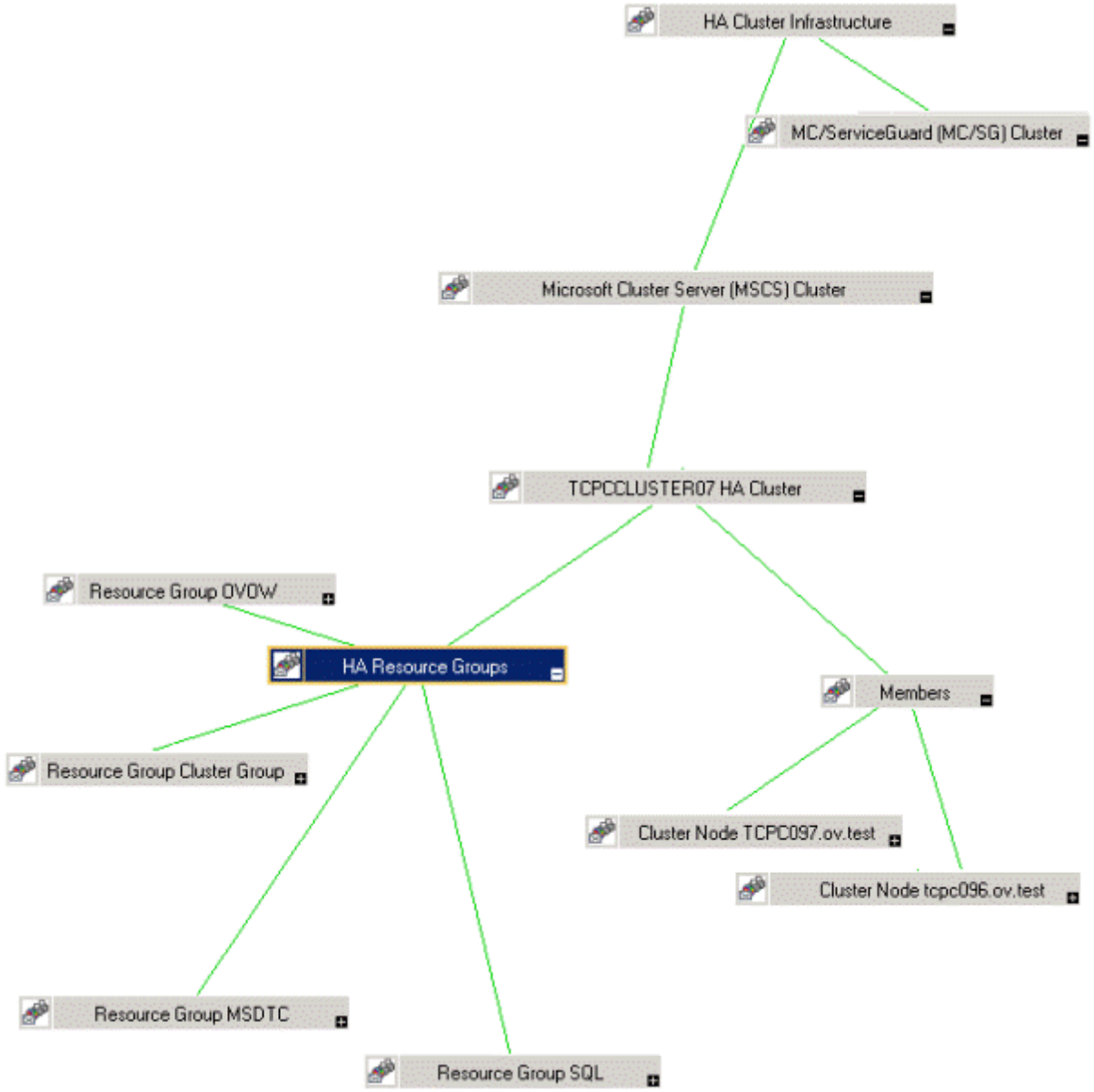
Chapter 3: Cluster Infrastructure SPI Components

The Cluster Infrastructure SPI (CI SPI) components include policies that enable you to configure and receive data in the form of service problem alerts, messages, and metric reports. CI SPI service map alerts are shown in the OM service map, while CI SPI messages and automatic action reports are available through the OM message browser. You can double-click an alert message in the message browser to see message details.

The CI SPI integrates with Reporter to produce web-based reports to display metric data on cluster performance levels and server availability. CI SPI reports provide information about clusters on specific cluster managed nodes, the reports provide an overview of cluster infrastructure that is helpful in determining needs for the long term.

Map View on Operations Manager for Windows

The map view displays the real-time status of your cluster infrastructure environment. To see, select **Services,** and click **Cluster Infrastructure**. The map view graphically represents the structural view of your entire service or node hierarchy in the cluster infrastructure environment including any resource group or cluster node.



The map view indicates severity levels for problems in the cluster infrastructure organization with the help of colors (red, yellow, blue, and green). Use the map view to drill down to the level in your node or service hierarchy where a problem is occurring.

The graphical representation of discovered elements in the service views enables speedy diagnosis of problems.

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

Map View on Operations Manager for UNIX

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

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

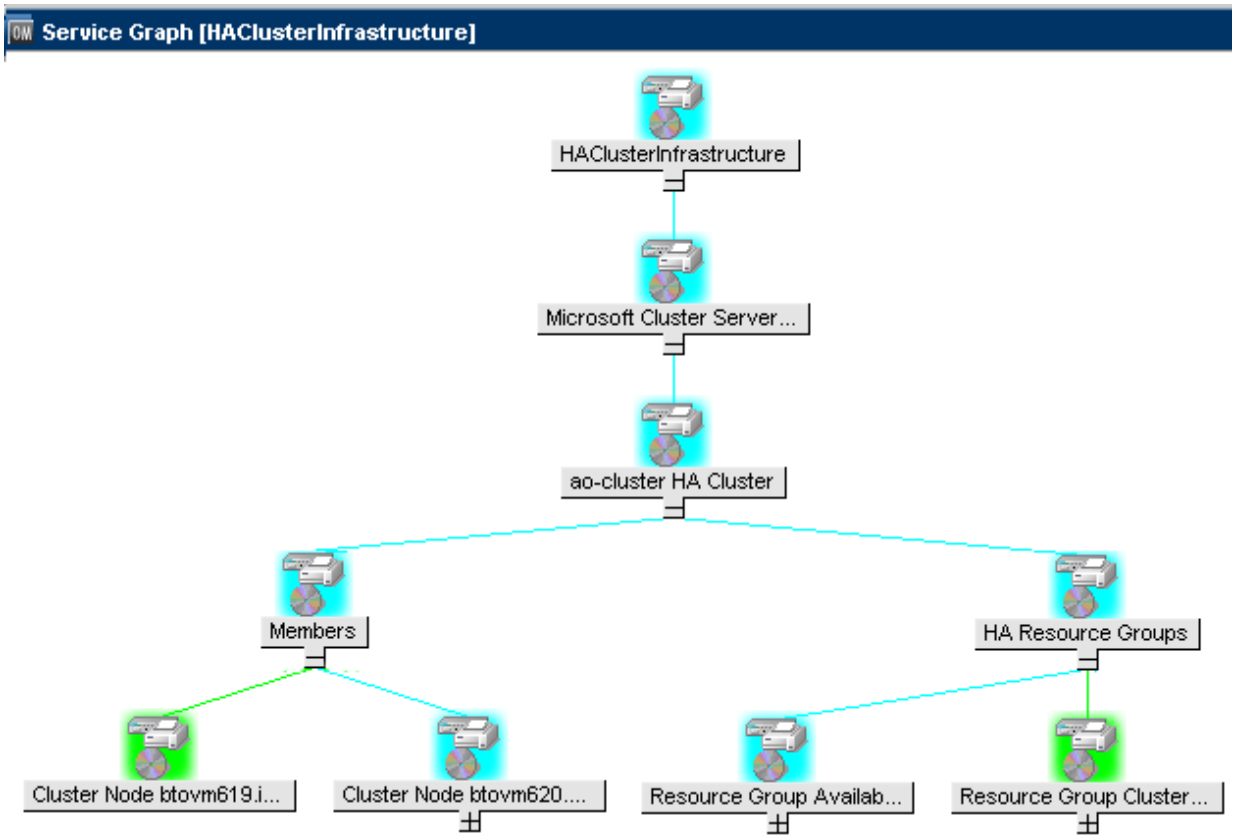
where operator name is the operator (for example, opc_adm or opc_op) to which you want to assign the service.

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

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

To see the map view, follow these steps:

1. Launch the OM Java console.
2. Log on using your user name and password.
3. Select **Services** → **Cluster Infrastructure** → **Show Graph**, to see the map view



The map view graphically represents the structural view of your entire service or node hierarchy in the cluster infrastructure environment including any subsystems or subservices.

Policies

You can use the Policy Groups folder to find a cluster specific policy. The CI SPI policy types are as follows:

- **Logfile Entry policies** (all begin with CI) capture status or error messages generated by the cluster nodes and resource groups application.
- **Measurement Threshold policies** (all begin with CI) define conditions for each metric so that the collected metric values can be interpreted and alerts or messages can be displayed in the message browser.

  The CI SPI measurement threshold policies are based on specific metrics. Each policy uses one or more metrics for data collection and compares the actual metric value against the specified

threshold. A mismatch between the threshold and the actual metric value generates message and instruction text that help you resolve a problem.

- **Scheduled Task policies** (all begin with CI) determine when and what metric values to collect and define the collection interval. Collection intervals can be 5 minutes, 15 minutes, one hour, or one day. The collection interval indicates how often data is collected for a specific group. The scheduled task policy has two functions: to run the collector or analyzer at each collection interval on a node and to collect data for all metrics listed within the polices' Command text box.
- **Service Discovery policy** - Discovers cluster nodes and resource group instances and builds a service map for all CI SPI discovered instances.

For more information about the policies provided by CI SPI, see "Getting Started" on page 12.

Reports

You can integrate the CI SPI with Reporter to generate web-based reports on metric data.

If Reporter is installed on the Operations Manager Management Server for Windows, you can see reports from the console. To see a report, expand **Reports** in the console tree, and then double-click individual reports.

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

For information about the reports provided by Cluster Infrastructure SPI, see "Cluster Infrastructure SPI Reports" on page 31.

Chapter 4: Getting Started

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

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

Deployment Checklist

Complete (Y/N)	Tasks
	Verify that you have installed OM 9.10 on the management server. In addition, verify that Operations Agent version 11.00 or above is installed. Make sure that you have installed all the available patches and hotfixes for OM and Operations agent.
	Verify that you have Reporter installed to generate reports.
	Make sure that you give sufficient time to Operations agent to collect the metrics before you start deploying the monitoring policies.

On OM for Windows

Follow the steps to getting started on OM for Windows.

Starting the CI SPI

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

Prerequisites for Deploying CI SPI Policies

Before deploying the CI SPI policies, ensure the following:

1. Install the latest OM patches. Make sure to check if you have installed OMW_000120 or higher patches.
2. On the cluster node, run the command to update the instance deletion threshold value:

```
ovconfchg -ns agtrep -set

INSTANCE_DELETION_THRESHOLD 3

ovconfchg -ns agtrep -set

RESEND_RELATIONSHIP_INSTANCES TRUE
```

By default, the threshold value is set to 5.

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

Running the Discovery Policies

If you add a cluster node on OM for Windows, the SI SPI automatically adds the cluster nodes and resource groups in the node bank. The cluster nodes are regrouped in the console tree under the following Node folders:

- **Nodes→ HA Clusters → Clustered Nodes**
- **Nodes→ HA Clusters →** *<cluster name>* **→ Nodes**

The resource groups are regrouped in the console tree under the following Node folder:

Nodes→ HA Clusters → *<cluster name>* **→ Resource Groups**

> **Note:** All the resource groups configured in a cluster should have a resolvable Virtual_IP. All the elements of a cluster such as cluster nodes and resource groups should have an entry in the `/etc/host`.

After adding the nodes in console tree Nodes folder, the SI SPI initiates CI SPI discovery policy.

The CI SPI discovery policy adds the discovered elements to the OM service map. Select **Services→ HA Cluster Infrastructure**, to view the CI SPI service map that graphically represents the discovered cluster infrastructure.

Deploying Quick Start Policies from OM for Windows

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

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

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

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

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

On OM for UNIX

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

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

List of the Patches

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

Starting the CI SPI

To get started with discovering cluster infrastructure, the first step is to run the SI SPI discovery policy (SI-SystemDiscovery policy).

Prerequisites for Deploying CI SPI Policies

Before deploying the CI SPI policies, ensure the following:

1. Install the latest OM patches. Make sure to check if you have installed OMW_000120 or higher patches.
2. On the cluster node, run the command to update the instance deletion threshold value:

```
ovconfchg -ns agtrep -set

INSTANCE_DELETION_THRESHOLD 3

ovconfchg -ns agtrep -set

RESEND_RELATIONSHIP_INSTANCES TRUE
```

By default, the threshold value is set to 5.

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

Running the Discovery Policies on the Cluster Infrastructure

The SI SPI discovery adds the cluster nodes to the relevant cluster node groups.

For example if the node is MCSG cluster on HP-UX, the cluster nodes get added to **SISPI-HPUX** and **CISPI-MCSG** HPUX node groups. In case of resource group, it will add it to **CI-Resource Group** node group.

After the cluster nodes get added to the respective node groups, deploy the auto-assigned policies to the cluster nodes. Deploy the CI SPI discovery policy (CI- Discovery) and other quick start policies to the cluster nodes.

> **Note:** All the resource groups configured in a cluster should have a resolvable Virtual_IP. All the elements of a cluster like cluster nodes and resource groups should have an entry in the `/etc/host`.

The CI SPI discovery policy adds the discovered elements to OM service map. You can view the CI SPI service map that graphically represents the discovered cluster infrastructure.

Deploying Quick Start Policies from OM for UNIX

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

By default, QuickStart policies are assigned to these node groups. When a node is added to the node group, these QuickStart policies get assigned to the node automatically. You must then deploy these

policies manually on the node by selecting **Deploy Configuration** from the **Actions** menu in the Admin GUI.

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

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

Viewing Reports and Graphs

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

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

Updating Reports after Upgrading the SPI

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

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

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

Data Collection for Reports

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

Reports	Policies	Managed Node Platform	SPI
Cluster Configuration	CI-ClusterDataCollector	Solaris Cluster, VCS Clusters, Service Guard, RHEL Cluster	Cluster Infrastructure
Cluster Uptime	CI-ClusterDataCollector	Solaris Cluster, VCS Clusters, Service Guard, RHEL Cluster	Cluster Infrastructure
Cluster System Availability	CI-ClusterDataCollector	Solaris Cluster, VCS Clusters, Service Guard, RHEL Cluster	Cluster Infrastructure

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

Chapter 5: Cluster Infrastructure SPI Policies

The Cluster Infrastructure SPI (CI SPI) provides a wide range of policies to help manage your clusters. These policies enable you to monitor the operations and performance of the services that run on the cluster managed nodes. The CI SPI policies help you monitor cluster on OM for Windows, HP-UX, Linux, and Solaris environments.

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

To access the policies on OM for Windows, select the following:

Policy management→Policy groups→Infrastructure Management→*language*→Cluster Infrastructure

To access the policies on console or Administration interface for OM for UNIX/Linux/Solaris, select the following:

Policy Bank→Infrastructure Management→*language*→Cluster Infrastructure

After you install the CI SPI on the OM for Windows management server and add nodes, the discovery policy is automatically deployed to the managed nodes (if policy autodeployment is enabled). Autodeployment of policies is enabled by default. You can choose to turn off automatic deployment of policies when services are discovered. In addition, you can modify and save preconfigured policies with new names to create custom policies for your own specialized purposes. For information about how to deploy policies on OM for Windows, see "Deploying CI SPI Policies from OM for Windows Management Server".

On OM for UNIX/Linux/Solaris, the discovery policy does not automatically deploy policies to the nodes. You can manually deploy them. For information about how to deploy policies on OM for UNIX, see "Deploying CI SPI Policies from OM for UNIX Management Server".

CI SPI policy groupings are based on monitored aspects and operating systems. The monitored aspects based grouping helps you to access and deploy policies to monitor performance, availability, capacity, logs, and security aspects across multiple operating systems. For example, to monitor the availability of resource group on your cluster infrastructure, expand the following to access CI-ClusterResGroupMonitor policy:

Policy management→Policy groups→Infrastructure Management→*language*→Cluster Infrastructure→Availability →Monitors

The operating system based grouping (Policies grouped by Vendor) helps you to quickly access the policies relevant to your operating system at one location. For example, to monitor cluster node status of the MSCS cluster, expand the following to access CI-ClusterMonitor policy:

Policy management→Policy groups→Infrastructure Management→*language*→Cluster Infrastructure→Policies grouped by Vendor→ MSCS - Advanced Policies.

> **Note:** There are no new policies to monitor the Power HA (HACMP) cluster. The default Advanced and QuickStart policies monitor the HACMP cluster. They are listed under:

Policy management→Policy groups→ Infrastructure Management→*language*→Cluster Infrastructure→Policies grouped by Vendor→HACMP - Advanced Policies.

Policy management→Policy groups→Infrastructure Management→*language*→Cluster Infrastructure→Policies grouped by Vendor→HACMP - QuickStart Policies.

Discovery Policy

The CI-ClusterDiscovery policy collects the following information from the managed nodes:

- Cluster name
- Cluster type
- Nodes
- Resource Groups
- State of nodes (offline or online)
- State of Resource Group (offline or online)
- Details of resource group’s virtual IP

The CI-ClusterDiscovery policy initiates ovclusterinfo tool to collect the details about the cluster. These details are framed in a service xml file and sent to the server.

After the discovery process is completed successfully, the service view is updated with the cluster infrastructure elements. The service elements for each cluster's components are represented as child elements below the respective cluster name.

Availability Policies

The availability of clustered nodes can be affected due to downtime. Downtime may be planned due to maintenance or routine operations such as upgrade, space management or system reconfiguration or unplanned due to power outage, human error, data corruption, and software or hardware errors. The availability policies monitor and check for the state and availability of cluster nodes, resource groups, network interfaces, and cluster services.

The CI SPI provides two types of availability policies:

- "Data Collector Policy" below: This policy collects data about state and availability of the cluster elements from the managed cluster nodes and logs the individual instances into Embedded Performance Component.
- "Monitor Policies" on the next page: These policies monitor the availability and state of cluster elements along with the process and services running on them.

Data Collector Policy

CI-ClusterDataCollector policy

This policy is a scheduled task policy that checks for the state and availability of resource groups, network interfaces, and cluster services. It collects data from the managed cluster nodes and logs the individual instances into the Embedded Performance Component in defined time intervals. By default, the time interval is 5 minutes. The recorded information stored in the Embedded Performance Component is used by the following policies to monitor, compare, and alert:

- Cluster Monitor Policy
- Cluster Node Monitor Policy
- Cluster Resource Group Monitor Policy

The policy collects all information and metrics of a cluster using the ovclusterinfo tool provided by cluster awareness of the Operations Agent, and records the data in the Embedded Performance Component.

The default policy group for the policy is:

Infrastructure Management→*language*→Cluster Infrastructure→Availability→Data Collector

Monitor Policies

The Cluster Infrastructure SPI provides a wide range of monitor policies to help you manage your cluster environment. These policies enable you to monitor the nodes, cluster, and resource groups. The default policy group for monitor policies is:

Infrastructure Management→*language*→Cluster Infrastructure→Availability→Monitors

Cluster Monitor Policy

CI-ClusterMonitor

Before deploying this policy, make sure you have deployed the CI-ClusterDataCollector policy for cluster data collection.

The CI-ClusterMonitor policy monitors the availability and strength of a cluster group. This is helpful to ensure high availability of services running on the cluster servers. The policy monitors following conditions:

- The cluster is down and the cluster status is offline.
- There are no redundant nodes active in the cluster group. Only a single node is active. If the single active node becomes inactive, it will bring the cluster down. This is referred to as a Single Point of Failure (SPOF) condition.
- Majority of nodes are offline. This is determined by comparing the number of active nodes against the cluster quorum. If (<number of cluster nodes>*/2 + 1*) cluster nodes are not active in a cluster, the cluster quorum is not met and the policy will send out an alert message.
- Any resource group in the cluster is offline.

Metrics Used	CLUSTER_NAME CLUSTER_TYPE CLUSTER_STATUS CLUSTER_TOTAL_NODES CLUSTER_TOTAL_ACTIVE_NODES
Supported Clusters	Veritas Cluster Server MC Service Guard Microsoft Cluster Server

	RHA Server Cluster Solaris Cluster
Script-Parameter	**Description**
MessageGroup	Message group for outgoing messages.
Debug	Set the value as 0 to disable trace messages, as 1 to receive trace messages on the console, and as 2 to log the messages in the trace file on the managed node.
Trace	Set a non-zero value to enable tracing.

> **Note:** To get quicker alerts about resource groups and cluster nodes going offline, the collector and the monitor policies can be set to run every minute. If this is done, it is important to set the summarization interval as well. Data queried from EPC is normally summarized (averaged) over a 5-minute interval before EPC gives this data to the monitor agent. This can cause an issue when data collection is done more than once in a 5-minute interval. So the summarization interval must appropriately be lowered.

To set the summarization interval to 1-minute, run the following command on the cluster nodes where data collection and monitoring is happening:

```
ovconfchg -ns eaagt -set OPC_SET_CODA_SI 1m
```

Cluster Node Monitor Policy

CI-ClusterNodeMonitor

The CI-ClusterNodeMonitor policy monitors the cluster node status. Before deploying this policy, make sure you have deployed the CI-ClusterDataCollector policy for cluster data collection.

Metrics Used	CLUSTER_NAME CLUSTER_TYPE NODE_NAME NODE_STATUS
Supported Clusters	Veritas Cluster Server MC Service Guard Microsoft Cluster Server RHA Server Cluster

	Solaris Cluster
Script-Parameter	**Description**
MessageGroup	Message group for outgoing messages.
Debug	Set the value as `0` to disable trace messages, as `1` to receive trace messages on the console, and as `2` to log the messages in the trace file on the managed node.
Trace	Set a non-zero value to enable tracing.

Cluster Resource Group Monitor Policy

CI-ClusterResGroupMonitor

The CI-ClusterResGroupMonitor policy monitors the state and availability of resource groups in a cluster. Before deploying this policy, make sure you have deployed the CI-ClusterDataCollector policy for cluster data collection.

Metrics Used	CLUSTER_NAME CLUSTER_TYPE RESGROUP_NAME RESGROUP_NODE_LIST RESGROUP_STATUS RESGROUP_LOCAL_STATE RESGROUP_ACTIVE_NODE RESGROUP_VIRTUAL_IP_ADDR
Supported Clusters	Veritas Cluster Server MC Service Guard Microsoft Cluster Server RHA Server Cluster
Script-Parameter	**Description**
MessageGroup	Message group for outgoing messages.
Debug	Set the value as `0` to disable trace messages, as `1` to receive trace messages on the console, and as `2` to log the messages in the trace file on the

	managed node.
Trace	Set a non-zero value to enable tracing.

Note: CI-ClusterResGroupMonitor policy sends an alert only when the resource group is *globally offline* on all the cluster nodes configured in a cluster.

Microsoft Windows Cluster Service Monitor Policy

CI-MSWindowsClusterServiceMonitor policy

The CI-MSWindowsClusterServiceMonitor policy is a Service/Process Monitoring type policy that checks for the state and availability of Microsoft Windows services. It monitors the Microsoft Windows services on the managed cluster nodes and sends out an alert in case the service is unavailable or stopped.

The CI-MSWindowsClusterServiceMonitor policy is only supported on Microsoft Windows platform. The default policy group for the policy is:

Infrastructure Management→*language*→Cluster Infrastructure→Availability→Monitors→MS Cluster Server

MC/ServiceGuard Cluster Process Monitor Policy

CI-MCSGClusterProcessMonitor policy

The CI-MCSGClusterProcessMonitor policy is a Service/Process Monitoring type policy that monitors the state and availability of MC/ServiceGuard Cluster process on Linux, for RHEL and SLES systems. It monitors the process *cmcld* and sends out an alert in case the process is not running on the managed node. The *cmcld* process runs on every cluster node and helps to initialize and monitor the health of the cluster.

The CI-MCSGClusterProcessMonitor policy is only supported on RHEL and SLES platforms. The default policy group for this policy is:

Infrastructure Management→*language*→Cluster Infrastructure→Availability→Monitors→MCSG Cluster Server

Red Hat Cluster Process Monitor Policies

CI-RHClusterCCSDProcessMonitor policy

The CI-RHClusterCCSDProcessMonitor policy is a Service/Process Monitoring type policy that monitors the state and availability of the Red Hat Cluster process on Linux, for RHEL systems. It monitors the process *ccsd* (Cluster Configuration System Daemon) and sends out an alert in case the process is not running on the managed node.

The CI-RHClusterCCSDProcessMonitor policy is only supported on the RHEL platform. The default policy group for the policy is:

Infrastructure Management→*language*→Cluster Infrastructure→Availability→Monitors→RH Cluster Server

CI-RHClusterRGManagerProcessMonitor policy

The CI-RHClusterRGManagerProcessMonitor policy is a Service/Process Monitoring type policy that monitors the state and availability of the Red Hat Cluster process on Linux, for RHEL systems. It monitors the process *clurgmgrd* (Cluster Resource Group Manager) and sends out an alert in case the process is not running on the managed node.

The CI-RHClusterRGManagerProcessMonitor policy is only supported on the RHEL platform. The default policy group for the policy is:

Infrastructure Management→*language*→Cluster Infrastructure→Availability→Monitors→RH Cluster Server

Veritas Cluster Server Process Monitor Policies

The Cluster Infrastructure SPI monitors the Veritas cluster processes and services on the Windows, HP-UX, Linux, AIX, and Solaris operating systems.

CI-VCSWindowsProcessMonitor policy

The policy is a Service/Process Monitoring type policy that monitors the state and availability of the Veritas cluster server process or service on Microsoft Windows systems and sends out an alert in case the monitored process or service is not running on the managed node. The policy monitors the following:

- High Availability Daemon (HAD). The daemon tracks all changes within the cluster configuration and resource status by communicating with the Global Atomic Broadcast (GAB).
- VCSComm service. The service is responsible for configuring the GAB and Low Latency Transport (LLT) in a VERITAS cluster.
- The Veritas Cluster Server Helper or HADHelper. The service is used by Veritas Cluster Server to perform operations that require administrator permissions.

The default group for the policy is:

Infrastructure Management→*language*→Cluster Infrastructure→Availability→Monitors→VERITAS Cluster Server →Windows

CI-VCSUnixProcessMonitor policy

The policy is a Service/Process Monitoring type policy that monitors the state and availability of the Veritas cluster server process on HP-UX, Linux (for RHEL and SUSE), AIX, and Solaris operating systems and sends out an alert in case the process is not running on the managed node. The policy monitors the following:

- High Availability Daemon (HAD). The daemon tracks all changes within the cluster configuration and resource status by communicating with the global atomic broadcast (GAB).
- Hashadow daemon. The daemon monitors HAD and if HAD fails hashadow attempts to restart it.

The default group for the policy is:

Infrastructure Management→*language*→Cluster Infrastructure→Availability→Monitors→VERITAS Cluster Server →Unix

Solaris Cluster Process Monitor Policy

The Cluster Infrastructure SPI monitors the Solaris cluster processes and services on the Solaris operating system.

CI-SunClusterProcessMonitor policy

The policy is a Service/Process Monitoring type policy that monitors the state and availability of the Solaris cluster daemon on the Solaris operating systems and sends out an alert in case the monitored process or service is not running on the managed node. The default group for the policy is:

Infrastructure Management→ *language*→ Cluster Infrastructure→ Availability→ Monitors→ Solaris Cluster Server

Log Policies

Cluster Infrastructure SPI provides logfile policies to monitor crucial logs for the managed nodes. The default policy group for these policies is:

Infrastructure Management→*language*→Cluster Infrastructure→Logs

MS Cluster Server Policies

The default group for Microsoft Windows Event Log Monitor policies is:

Infrastructure Management→*language*→Cluster Infrastructure→Logs→MS Cluster Server

- **CI-MSWindowsClusterServer_NetworkWarnError policy:** This policy forwards all warning and error event log entries related to cluster IP address resources, initialization of the cluster and network driver, and creation of NetBIOS interface to the OM console.
- **CI-MSWindowsClusterServer_NodeWarnError policy:** This policy forwards all warning and error event log entries related to cluster node to the OM console.
- **CI-MSWindowsClusterServer_StorageWarnError policy:** This policy forwards all warning and error event log entries related to cluster disks and quorum resource to the OM console.
- **CI-MSWindowsClusterServer_AvailabilityWarnError policy:** This policy forwards all warning and error event log entries related to failover cluster server availability to the OM console.

Solaris Cluster Server Policies

- **CI-SunClusterResourceLogMonitor:** This policy forwards all warning and error event log entries related to cluster resources to the OM console.
- **CI-SunClusterNetworkLogMonitor:**This policy forwards all warning and error event log entries related to cluster network to the OM console.
- **CI-SunClusterNodeLogMonitor:** This policy forwards all warning and error event log entries related to cluster nodes to the OM console.

Veritas Cluster Server Policies for UNIX

- **CI-VCSUnixNetworkLogMonitor:** This policy forwards all warning and error event log entries related to cluster network to the OM console.
- **CI-VCSUnixNodeLogMonitor:** This policy forwards all warning and error event log entries related to cluster node to the OM console.
- **CI-VCSUnixResourceLogMonitor:**This policy forwards all warning and error event log entries related to cluster resources to the OM console.

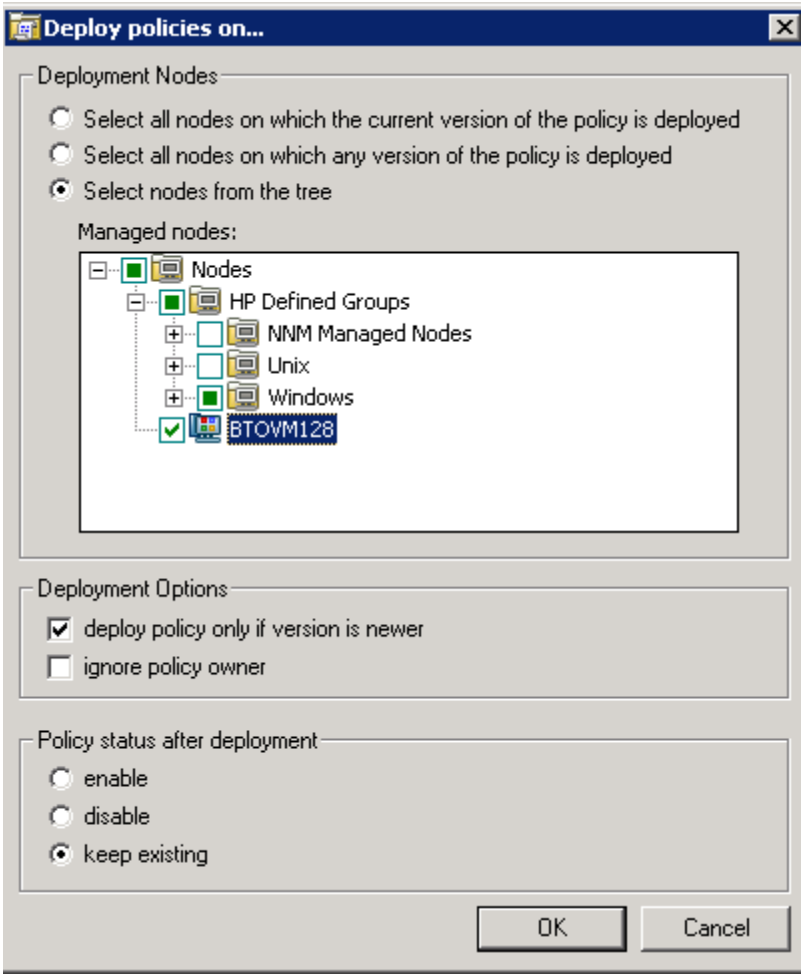
Policies for Windows

- **CI-VCSWindowsResourceLogMonitor:** This policy forwards all warning and error event log entries related to cluster resources to the OM console.
- **CI-VCSWindowsNodeLogMonitor:** This policy forwards all warning and error event log entries related to cluster node to the OM console.
- **CI-VCSWindowsNetworkLogMonitor:** This policy forwards all warning and error event log entries related to cluster network to the OM console.

Deploying CI SPI Policies from Operations Manager for Windows Management Server

To manually deploy policies from the management server, follow these steps:

1. Right-click the policy you want to deploy.
2. From the menu, select **All Tasks**.
3. Select **Deploy on**. The Deploy policies on dialog box opens.



4. Select the option **Select nodes from the tree**. From the list of managed nodes, select the nodes where you want to deploy the policy.
5. Click **OK**.

Deploying CI SPI Policies from Operations Manager for UNIX Management Server

Before you deploy policies, make sure that the nodes have been added to the management server and have Operations Agent software installed. For more information about how to add nodes to the management server, refer to the Operations Manager for UNIX Online Help.

You can manually deploy the policies to the nodes or enable auto deployment of policies.

To enable auto deployment of policies, follow these steps:

1. To enable auto deployment on the server, run the following command:

   /opt/OV/contrib/OpC/autogranting/enableAutoGranting.sh

2. To enable auto deployment for Infra SPI using XPL config change, run the following command:

   ovconfchg -ns infraspi -set AUTODEPLOYMENT true

3. To activate the node, run the following command on the management server:

   opcactivate -srv <HPOM Server> -cert_srv <HPOM Server> -f

4. Grant the certificates.
5. Add the node to the SI-Deployment node group.
6. Deploy configuration.
7. Check whether the node is added to the appropriate node group.
8. Verify auto deployment of policies to the node.

To manually deploy policies from the management server for OM for UNIX (HP-UX, Linux, or Solaris) follow these steps:

Task1: Assign Policy or Policy group

1. Log on to OM as the administrator. The OM Administration interface appears.
2. Click **Policy Bank** under the Objects Bank category. The Policy Bank window opens.
3. In the Policy Bank window, select the policy or policy groups you want to assign to a node or a node group.
4. Select **Assign to Node** or **Node group** from the **Choose an Action** drop-down box and click submit. The Select window opens.
5. Select the node or the node groups and click **OK**. The selected policies are assigned to the nodes.

Task2: Deploy Policies

1. From the OM Administration interface, click **Node Bank** under the Objects Bank category. The Node Bank window opens.
2. In the Node Bank window, select the nodes or node groups on which you want to deploy policies.
3. Select **Deploy Configuration** from the **Choose an Action** drop-down box and click **Submit**. The Select window opens.
4. Select the **Distribute Policies** check box and click **OK**. The policies are deployed on the selected nodes.

Chapter 6: Cluster Infrastructure SPI Reports

The Reporter captures and formats data collected at nodes and generates web-based reports. These reports help you understand an overall picture of cluster resources. To generate and see reports from data collected by the Cluster Infrastructure SPI (CI SPI), you must use Reporter in conjunction with OM.

After you install Reporter in your environment, you can access the CI SPI reports from the OM for Windows console. Those reports are available under **Reports** section in the OM console tree and offer helpful information for analyzing trends for cluster infrastructure availability and performance. To install Reporter package, see the *Infrastructure SPI Installation Guide*. To see reports, expand **Reports→HA Cluster Infrastructure** in the console tree.

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

The Reports folder is not created until data is collected on nodes and the Service Reporter consolidation process has run, which is usually 24 hours after a node becomes managed.

The Cluster Infrastructure SPI provides the following reports:

Cluster Configuration Report

This report displays the configuration information for all nodes that are members of the cluster. It provides information about the active nodes and resource group in the cluster. You can use this report to see the cluster configuration details for a cluster. The following is an example report for Cluster Configuration report:

Operations - Smart Plug-ins for Infrastructure

Cluster Configuration
for Group HA Cluster Infrastructure

This report was prepared: 8/11/2009, 2:59:12 AM

This report shows the configuration information of all the clusters nodes

cluster1

Active Nodes	2
Number of nodes configured	2
Number of failover resource groups configured	1
Cluster Type	MC/ServiceGuard (MC/SG)
Cluster SPI Collector Node	tcivmi07.ov.test

Resource Groups Configuration

Resource Group Name	Node List	Active Node
test-oval	tcivmi07 tcivmi08	tcivmi07.ov.test

TCPCCLUSTER07

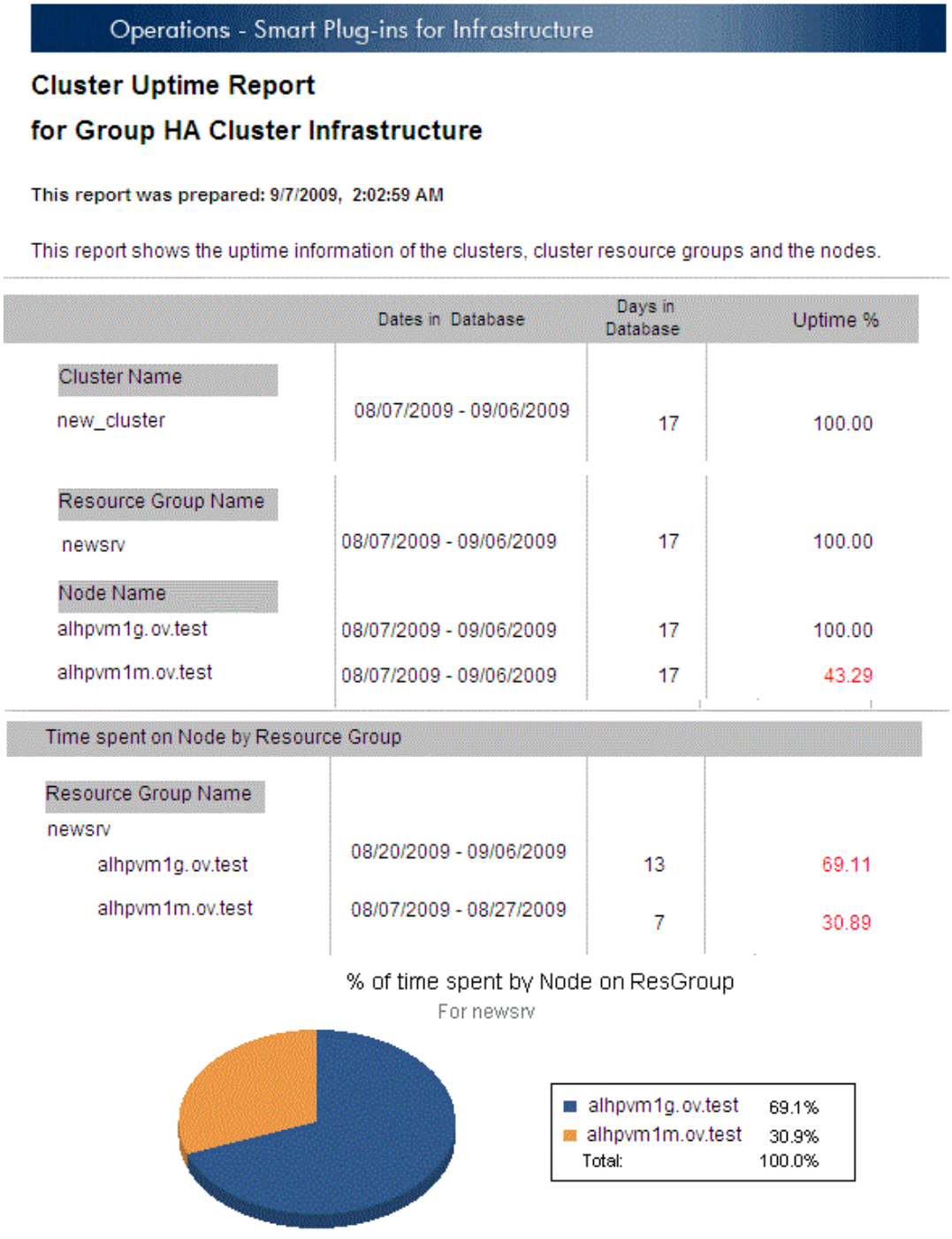
Active Nodes	2
Number of nodes configured	2
Number of failover resource groups configured	4
Cluster Type	Microsoft Cluster Server (MSCS)
Cluster SPI Collector Node	tcpc097.ov.test

Resource Groups Configuration

Resource Group Name	Node List	Active Node
Cluster Group	tcpc097 tcpc096	tcpc096.ov.test
MSDTC	tcpc096 tcpc097	TCPC096.ov.test
OVOW	tcpc097 tcpc096	tcpc096.ov.test
SQL	tcpc096 tcpc097	TCPC096.ov.test

Cluster Uptime Report

This report displays the uptime information of the cluster, cluster resource groups, and the member nodes. It also provides information about the time spent by the resource groups on each of the nodes it is configured to run on. You can use this report to see the cluster uptime details. The following is an example report for Cluster Uptime report:



Operations - Smart Plug-ins for Infrastructure

Cluster Uptime Report

for Group HA Cluster Infrastructure

This report was prepared: 9/7/2009, 2:02:59 AM

This report shows the uptime information of the clusters, cluster resource groups and the nodes.

	Dates in Database	Days in Database	Uptime %
Cluster Name			
new_cluster	08/07/2009 - 09/06/2009	17	100.00
Resource Group Name			
newsrv	08/07/2009 - 09/06/2009	17	100.00
Node Name			
alhpvm1g.ov.test	08/07/2009 - 09/06/2009	17	100.00
alhpvm1m.ov.test	08/07/2009 - 09/06/2009	17	43.29

Time spent on Node by Resource Group

Resource Group Name			
newsrv			
alhpvm1g.ov.test	08/20/2009 - 09/06/2009	13	69.11
alhpvm1m.ov.test	08/07/2009 - 08/27/2009	7	30.89

% of time spent by Node on ResGroup

For newsrv

alhpvm1g.ov.test 69.1%
alhpvm1m.ov.test 30.9%
Total: 100.0%

Cluster System Availability Report

This report displays the system availability information of cluster member nodes. The information is sorted by day and shift-time. The shifts are defined at the end of each report section. The following is an example report for Cluster System Availability report:

Operations - Smart Plug-ins for Infrastructure

System Availability

for Group HA Cluster Infrastructure

This report was prepared: 9/7/2009, 6:32:24 AM

System Up Time is calculated based on time when the system is rebooted.
The reboot time is logged by the performance agents. The named **Shift** is defined at the end of each report section. The **All Shifts** percent is based on all defined shifts for the range of dates in the database and does not cover time outside of shifts, weekends, or holidays. The %uptime is not showed for each shifts but this is available for **All Shifts** only.

System Name	Dates in Database	Days in Database	Downtime (minutes)	All Shifts Up Time %	Total no of Down
tcivmi07.ov.test	8/7/2009 - 8/28/2009	16	0.00	100.00	0
tcivmi08.ov.test	8/7/2009 - 8/28/2009	16	0.00	100.00	0
tcpc096.ov.test	8/7/2009 - 8/27/2009	15	0.00	100.00	0
tcpc097.ov.test	8/7/2009 - 8/28/2009	16	0.00	100.00	0
TCVM195	8/7/2009 - 8/28/2009	16	0.00	100.00	0

Graveyard

System Name	Dates in Database	Days in Database	Downtime (minutes)	All Shifts Up Time %
tcivmi07.ov.test	8/7/2009 - 8/28/2009	16	0.00	100.00
tcivmi08.ov.test	8/7/2009 - 8/28/2009	16	0.00	100.00
tcpc096.ov.test	8/7/2009 - 8/27/2009	15	0.00	100.00
tcpc097.ov.test	8/7/2009 - 8/28/2009	16	0.00	100.00
TCVM195	8/7/2009 - 8/28/2009	16	0.00	100.00

Graveyard Shift

	From	To	Hours:Minutes
Monday	12:00:00AM	8:00:00AM	8:00
Tuesday	12:00:00AM	8:00:00AM	8:00
Wednesday	12:00:00AM	8:00:00AM	8:00
Thursday	12:00:00AM	8:00:00AM	8:00
Friday	12:00:00AM	8:00:00AM	8:00
			40:00

Chapter 7: Troubleshooting

This chapter covers basic troubleshooting scenarios in CI SPI.

Problem	Advanced Monitoring policies modified in OM for UNIX Administrator interface fail to run after deployment to managed nodes.

Cause	When advanced monitoring policies are edited in interface mode in OM for UNIX policy editor, syntax errors are induced into the Perl code module. This causes the policy to fail to run. Errors such as the following appear:
	`An error occurred in the processing of the policy 'SI-LinuxSshdProcessMonitor'. Please check the following errors and take corrective actions. (OpC30-797)`
	`Error during evaluation of threshold level "Processes - Fill Instance list" (OpC30-728)`
	`Execution of instance filter script failed. (OpC30-714)Perl Script execution failed: syntax error at PerlScript line 11, near "1`
	`#BEGIN_PROCESSES_LIST`
	`#ProcName=/usr/sbin/sshd`
	`#Params=`
	`#Params=`
	`#MonMode=>=`
	`#ProcNum=1`
	`#END_PROCESSES_LIST@ProcNames"`
	`Missing right curly or square bracket at PerlScript line 17, within string syntax error at PerlScript line 17, at EOF. (OpC30-750)`
	The un-edited advanced monitoring policies (Measurement Threshold type) work fine when deployed from OM for UNIX.

Solution	To edit the settings in the Measurement Threshold policy, use ‘Edit in Raw mode’ feature of the OM for UNIX Administrator interface to change the policy contents. This requires you to know the syntax of the policy data file.

Problem	Discovery and DNS resolution.
Solution	Ensure that cluster resource groups resolve their IP to a well-defined host name on both the server and the agent.

Problem	Discovery procedures and data collection gives error with non-English names.
Cause	HA Cluster configurations with non-English cluster names and resource group names are not supported by the Cluster Infrastructure SPI.
Solution	The Cluster Infrastructure SPI can be deployed successfully on a non-English OM. However, using non-English names for systems shows up as an error because non-English names are not recognized by the StoreCollection OvPerl APIs in Operations agent.

Problem	Alert Messages while Cluster Discovery automatically adds nodes.
Cause	While system discovery automatically adds nodes for cluster environments, it generates alert messages with normal severity. These messages take a while to get acknowledged because the auto-addition feature of the system discover policy takes time to populate the nodes bank.
Solution	Disable the Auto-addition feature by changing the following default values in the XPL configuration parameters:

Configuration Parameter	Default Value	Value to disable auto addition
AutoAdd_ClusterNode	true	false
AutoAdd_Cluster_RG_IP	true	false
AutoAdd_HypervisorNode	true	false
AutoAdd_Guests	false	true

Problem	The ovclusterinfo tool does not return valid data when a cluster is down for all cluster types.
Cause	The ovclusterinfo tool returns valid data when the cluster is down only in

	case of for MC/ServiceGuard cluster. For other cluster types the cluster data collector logs data for its members only when the cluster status is online.
Solution	If the clusters server goes down or loses connectivity with OM, it is considered as if the complete cluster is down and the NUM_ACTIVE_ NODES parameter shows zero. The value is set to zero because of absence of valid data from cluster. The value changes to non- zero when the cluster is up.

Problem	The following warning or error messages appear on the OM console: `An error occurred in the processing of the policy 'CI-ClusterNodeMonitor'. Please check the following errors and take corrective actions. (OpC30-797) Error during evaluation of threshold level "Node Offline" (OpC30-728) Execution of threshold script failed. (OpC30-712) Perl Script execution failed: (in cleanup) Value: Cannot get current instance at PerlScript line 40.(OpC30-750)`
Cause	The monitor policies may send out a warning message if they fail to retrieve any cluster information from CODA. This happens when the cluster collector has insufficient time to gather and record the cluster information.
Solution	To avoid such a scenario, first deploy the cluster collector to the node. The cluster collector is scheduled to run every 15 minutes by default. Allow at least two collection intervals before deploying the cluster monitor policies to the node. This ensures proper functioning of the collector and monitor policies.

Problem	If a fail-over occurs, the real-time status of your cluster infrastructure environment is not updated in the service map immediately.
Cause	The near real-time status of your cluster infrastructure environment is updated, when the CI-ClusterDiscovery policy runs, based on the following: • The next scheduled interval. • Value of the INSTANCE_DELETION_THRESHOLD in `agtrep` namespace.
Solution	To see the near real-time status of your cluster environment each time the CI-ClusterDiscovery runs, make the following changes on all the cluster nodes. 1. Type the command `Ovconfchg –edit` and search for `agtrep`

	namespace.
	The default value is:
	`[agtrep]`
	`INSTANCE_DELETION_THRESHOLD=5`
	2. Modify and add the following values under `agtrep namespace:`
	`[agtrep]`
	`INSTANCE_DELETION_THRESHOLD=1`
	`RESEND_RELATIONSHIP_INSTANCES=TRUE`
	3. Change the schedule interval of CI-ClusterDiscovery policy, as required.

Problem	Warning or error messages on the OM console: `Check the following errors and take corrective actions. (OpC30-797) Error during evaluation of threshold level "CPU Spikes level Critical" (OpC30-728) Execution of threshold script failed. (OpC30-712) Perl Script execution failed: Can't locate OvTrace.pm in @INC (@INC contains: /usr/lpp/OV\lbin\eaagt\perl /usr/lpp/OV/lbin/eaagt/perl /var/opt/OV/bin/instrumentation /usr/lpp/OV/nonOV/perl/a/lib/5.8.8/aix-thread-multi /usr/lpp/OV/nonOV/perl/a/lib/5.8.8 /usr/lpp/OV/nonOV/perl/a/lib/site_perl/5.8.8/aix-thread-multi /usr/lpp/OV/nonOV/perl/a/lib/site_perl/5.8.8 /usr/lpp/OV/nonOV/perl/a/lib/site_perl .) at PerlScript line 136.` `BEGIN failed--compilation aborted (in cleanup) Can't locate OvTrace.pm in @INC (@INC contains: /usr/lpp/OV\lbin\eaagt\perl /usr/lpp/OV/lbin/eaagt/perl /var/opt/OV/bin/instrumentation /usr/lpp/OV/nonOV/perl/a/lib/5.8.8/aix-thread-multi /usr/lpp/OV/nonOV/perl/a/lib/5.8.8 /usr/lpp/OV/nonOV/perl/a/lib/site_perl/5.8.8/aix-thread-multi /usr/lpp/OV/nonOV/perl/a/lib/site_perl/5.8.8 /usr/lpp/OV/nonOV/perl/a/lib/site_perl .) at PerlScript line 136.` `BEGIN failed--compilation aborted at PerlScript line 136. (OpC30-750)`
Cause	This error occurs on any policy and any *.pm file when the instrumentation is not deployed on the node correctly.
Solution	Forcefully deploy the instrumentation on the node.

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 (Operations Smart Plug-in for Cluster Infrastructure 12.06)

Just add your feedback to the email and click send.

We appreciate your feedback!