HPE Operations Manager i

Software Version: 10.10

OMi Evolution Guide

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise 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. HPE 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 HPE 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

Citrix® and XenDesktop® are registered trademarks of Citrix Systems, Inc. and/or one more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries.

Java is a registered trademark of Oracle and/or its affiliates.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Microsoft®, Windows®, Lync®, Windows NT®, Windows® XP, and Windows Vista® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates.

Red Hat® is a registered trademark of Red Hat, Inc. in the United States and other countries.

SAP® is the trademark or registered trademark of SAP SE in Germany and in several other countries.

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 HPE Software Support website at: https://softwaresupport.hp.com

This website provides contact information and details about the products, services, and support that HPE Software offers.

HPE 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 website to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HPE 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

HPE Software Solutions & Integrations and Best Practices

Visit HPE Software Solutions Now at https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01702710 to explore how the products in the HPE Software catalog work together, exchange information, and solve business needs.

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

Contents

Chapter 1: Introduction

Overview

HPE Operations Manager i (OMi) with its modern user interface, advanced Topology-Based and Stream-Based Event Correlation (TBEC and SBEC), and Monitoring Automation for infrastructure and composite applications, offers features that are not available with HP Operations Manager for Windows, HP-UX, Solaris or Linux.

Therefore, many customers are using it today as their Operations Bridge where topology and event data come together from various data sources, including HP Operations Manager.

With the introduction of the Monitoring Automation feature in OMi 9.20, OMi was already able to take over the OM agent configuration and management part that so far had to be done in HP Operations Manager, however, several features present in OM were still missing, such as agent health checks, an external instruction text interface, and others.

With the introduction of OMi 10, HPE has released the first OMi version meant to replace OM. It closes many gaps and although there is no need to move to OMi immediately, it can be considered the successor of OM.

This raises the question of how to evolve an HP Operations Manager deployment so that OM agents and operators, as well as all kinds of integrations, are shifted from OM to OMi.

This guide explains how to transition to OMi in phases while adding value to the overall solution in each phase, and compares OM functionality with OMi functionality. It also explains how OMi and HPE Operations Bridge Reporter (OBR) can be used to replace functions that are handled by HP Operations Manager (OM) for UNIX or Windows and HPE Reporter today while providing additional features and a modern web-based user interface.

> **Note:** With version 10.x, HP Service Health Reporter (SHR) is renamed to HPE Operations Bridge Reporter (OBR). In this guide, HPE Operations Bridge Reporter (OBR) refers to both Operations Bridge Reporter 10.x as well as HP Service Health Reporter 9.4x.

It provides step-by-step evolution information that adds value after each step and presents an overview of how existing OM configurations can be transferred and used with HPE OMi. It also contains a comprehensive comparison of key OM features and their equivalent in HPE OMi.

It also describes the sequence of typical steps required when shifting responsibilities from an OM server to OMi.

This guide is for HPE OMi implementers who want to replace an existing OM installation with HPE OMi version 10.00 or later.

OM Evolution in Phases

HPE recommends that you transition functions from OM to OMi in phases. Each phase will add value to the overall solution. The following chapters explain each step in detail.

Note: This is not a strict sequence that has to be followed in all cases. For example, instead of adding correlation rules in the first OMi implementation step, they could be added at a later date. However, it makes sense to add correlation rules before operators start to work on events, as it increases overall OpsBridge efficiency.

Day 1 / Can be done in weeks / At your own pace

Plan the Evolution → Introduce OMi integrate event sources & topology → Establish Effective Operator Workflow → Switch off PM → Switch off OM

Evaluate current monitoring / "Headless" OpsBridge with topology / OpsBridge with key integrations for operators / Manage Operations Agents from OMi step by step Choose Mgmt Packs or import policies

Plan how to automatically establish topology / Correlation event enrichment & automation / Efficient Operator workflow using modern UI and embedded performance grapher / Configure SiteScope from OMi Import SiS templates / Easy tuning / Automated monitoring configuration

Plan integrations / Increased user motivation through Gamification / Move from Reporter to SHR / Switch off Reporter

Plan Operator groups etc / Service Health Reporting

Model Business Services, add more Event Type Indicators for TBEC & Service Health

Evolution Phases

Plan the Evolution

In the first phase you plan the move and evaluate your current monitoring and operator workflow in OM.

Introduce OMi

The next phase will introduce OMi and focus on the integration of the various event sources and topology. Once this is established you can benefit from OMi correlation, event enrichment and automation features. Some customers even stop here and use OMi in a "headless" fashion, which means all events are forwarded to another system, like HPE Service Manager, and processed there. All other customers can see this step as a necessary first implementation step - before they move to the next step.

Establish Effective Operator Workflow

In this step, operators are moved from OM to OMi. This includes setting up operators and operator groups, defining work roles and responsibilities, and establishing key integrations for operators like the integrations of trouble-ticket or notification systems, as well as tools and run book automation. Once this is established, operators can benefit from the modern OMi UI and efficient operator workflow as well as from advanced features like OMi User Engagement.

Since its release in 2009, the classical use case of OMi has been to cover Operations Bridge functions, receiving events from various event sources. In this use case, multiple domain or regional managers forward events to a central OMi server on which the events are processed and handled by operators. It is here that OMi can provide additional value:

- Linkage to the RTSM
- Modern, web-based user interface
- Extended event automation capabilities including automatically assigning events to users and time-based automatic triggering event updates and actions
- Multidimensional approach to calculating service health
- Integration capabilities via the BSM Connectors or
- Advanced topology-based event automation

When these functions are achieved, OMi can replace an OM system in an Operations Bridge or Manager-of-Managers role.

Example of OMi Replacing OM Manager-of-Managers Acting as Operations Bridge

Operators log in to OMi instead of OM and use the flexible Workspaces pages, for example the Event Perspective, Health Perspective or custom user-created pages to process events. They can use features similar to those found in OM to analyze, fix or escalate problems such as instruction text, tools, event-related actions or performance graphs. Key integrations with other HPE products also exist in OMi, such as the integrations with HPE SiteScope, HPE UCMDB, HPE Service Manager, HPE Operations Orchestration, HPE Network Node Manager i, HPE Operations Bridge Reporter, and notification systems.
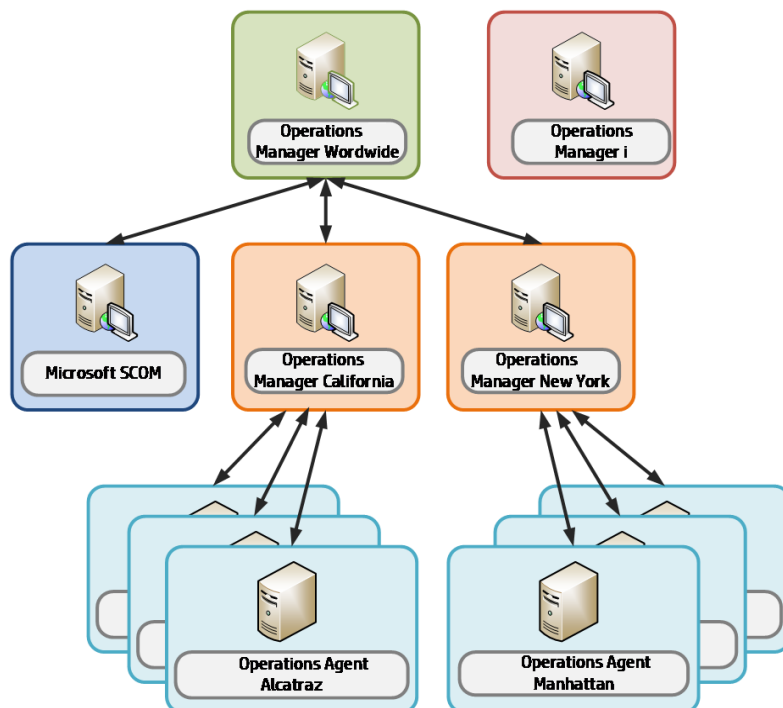
The next steps add monitoring configuration for SiteScope and OM agents.

Manage Operations Agents from OMi

This is the phase where OMi Monitoring Automation provides an automated, topology-based monitoring configuration. You can use OMi management packs or build your own management packs for your custom applications in order to benefit from OMi advanced monitoring configuration concepts, such as aspects and parameterized policies.

For an up-to-date list of OMi management packs, go to https://hpln.hpe.com/group/operations-manager-i.

Example of OMi taking over Policy Management for Certain Nodes
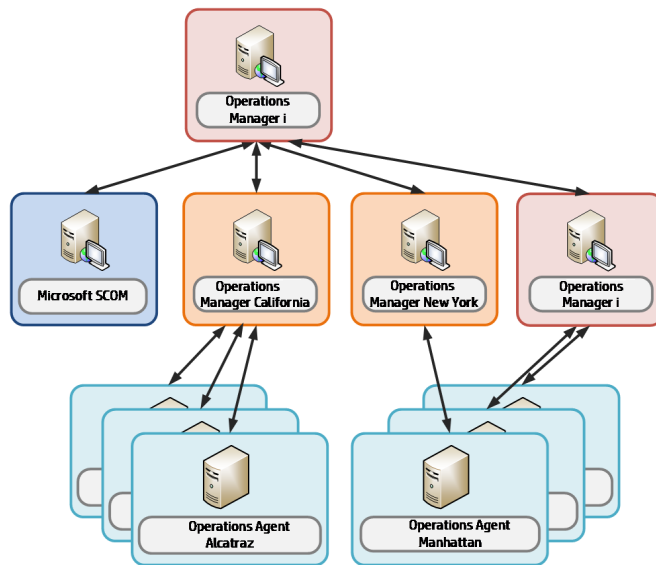
This can be accomplished step by step by having OMi and OM in parallel, until all OM agents are configured from OMi.

Note: When you exchange your OM license for an OMi license as part of the HPE license exchange program, you will continue to get support for your exchanged OM licenses.

OMi used as Operations Bridge and for System Management
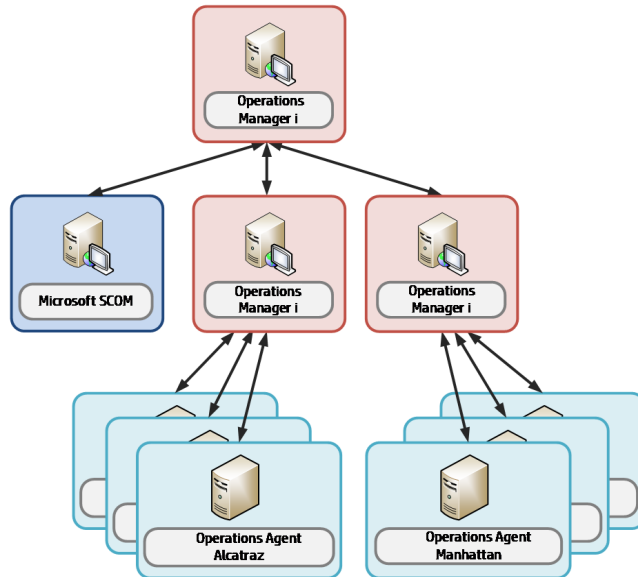
Manage SiteScope from OMi

In this step you use OMi Monitoring Automation to configure SiteScope systems.

Move from Reporter to OBR

In this step, business service-centric reporting using Operations Bridge Reporter is established and replaces HPE Reporter.

Switch Off Performance Manager, Reporter, and OM

At the end of the evolution, when OBR and OMi have taken over all functions and when the older products are no longer required, the older products can be switched off.

Add Value on Top

Modeling Business Services and defining additional indicators for OMi Topology-based Event Correlation (TBEC) and Service Health features are optional tasks that can be completed at various phases, if needed.

The following chapters guide you through each of the evolution phases by describing necessary and optional steps in detail.

Further Resources

- OMi guides and OMi Help

  The Operations Bridge Evolution Guide does not duplicate information that is already available in the OMi Help, but refers to chapters that are important for the evolution. In the planning phase, when OMi is not yet installed, the PDF format of the guides can be used. Once OMi is installed, HPE recommends to use the OMi Help, as it combines the information contained in the PDF guides into a single, integrated, and easy to access resource.

  For the latest version of the following guides, see the https://softwaresupport.hp.com/group/softwaresupport webpage:

    ○ OMi Administration Guide

    ○ OMi Extensibility Guide

    ○ OMi Integration Guide

  For an overview of OMi, search for the OMi Concepts Guide.

- Moving to Service Centric Management with HP OMi Technical White Paper available at https://softwaresupport.hp.com/group/softwaresupport/search-result?keyword=. This white paper is useful for consultants and architects planning the implementation of an HPE OMi-based solution. Although it does not focus on evolution aspects, it provides a good overview of the implementation steps that are necessary in any OMi implementation, regardless of whether OM is replaced or not.

- OMi Management Packs Evolution Guide available at https://softwaresupport.hp.com/group/softwaresupport/search-result?keyword=. This guide explains the differences between SPIs and Management Packs and how to retain customizations. It is intended for OM Smart Plug-In (SPI) users who want to switch to the corresponding OMi management packs.

- Operations Bridge Solution community: https://hpln.hpe.com/group/operations-bridge.

- Operations Manager i Product community: https://hpln.hpe.com/group/operations-manager-i.

  Both communities are meant for practitioners and users of OMi and of the Operations Bridge solution, and contain many useful links to forums, blog articles, videos, trainings, guides, tools, and so on.
  This guide refers to several how-to tutorials that are mentioned on the HPE Live Network Content Marketplace at https://hpln.hpe.com/page/omi-tutorials.

Chapter 2: Planning the Evolution

To avoid misplaced effort, any implementation of OMi should be planned and developed upfront, before the actual software installation and configuration is done. OMi allows a lot of automation that can greatly simplify ongoing monitoring, but this automation requires thoughtful planning and a clear understanding of how you want to monitor your IT environment.

Moving from OM to OMi can be considered an opportunity to revisit your current monitoring configuration and operator setup. You will benefit the most from OMi capabilities not if you are trying to reestablish everything as on OM, but by taking advantage of the new concepts and possibilities that OMi offers.

Plan Operations Bridge Solution Deployment

With any OMi implementation there are certain deployment options (with or without external UCMDB, single- or multi-server deployment, with or without a load balancer, and so forth) that depend on your sizing, security, and integration requirements or preferences. See the Moving to Service Centric Management with HP OMi Technical White Paper for an overview of what should be considered when planning the solution deployment.

Plan How to Establish Infrastructure Topology

Move from a Node-Centric to a CI and Topology-Centric Approach

System and Application Infrastructure Management in OM is based on a node-centric approach. Many tasks such as tool launches or policy deployments refer to nodes, a list of nodes, or node groups. Node groups are also referenced when defining responsibilities for operators.

The approach in OMi is different, as it is Configuration Item-centric, which can also be called a topology-centric approach. Operators typically work with views that show CIs of various CI types (such as business applications, running software, databases, web servers, and so on) and the relationships between them. These views typically return a subset of all the CIs that exist in the RTSM – the Run-time Service Model of OMi.

Having such a model of CIs and relationships in the RTSM provides the following benefits:

- Operators can see relationships between IT components and business services, which helps them in prioritizing, filtering, troubleshooting, and isolating problems
- Topology information can be used to provide CI-type specific guidance to operators (CI-specific context menus, tools, run books, graphs, and so on).

  For example: selecting an Oracle database event shows all available Oracle tools and run books. Launching the neighborhood graphs for an Oracle database CI shows important DB metrics and important system metrics from the node that runs the DB.

- The relationships between CIs can be used to propagate health status providing an at-a-glance 360 degree view of service health

- The topology can be used by OMi topology-based event correlation feature to correlate events

- The topology can be used by OMi topology-based management template feature to automate what monitoring configuration is applied or removed

The node that hosts applications like databases or middleware is not as important as in OM, as operators can launch tools or deploy monitoring to CIs directly, without knowing which nodes are affected. Mass policy deployment to nodes via node groups in OM is replaced by deployment of aspects to views or automatic deployment of aspects based on RTSM changes in OMi.

Though node groups exist in OMi, they do not play a special role, requiring OM users to think differently.

OMi users will use views in various places inside the product: when filtering events, when setting up assignment rules, when creating topology-based event correlation rules, and even when defining responsibilities for operators. These views would typically show all sorts of CI types and relationships, provided that these CIs and relationships have been added to the RTSM. The following sections show you how you can populate the RTSM with CIs and Relationships.

Technologies for Establishing Infrastructure Topology

Topology (node, node group, and services data) that exists in OM can be forwarded to OMi and converted into a corresponding RTSM topology. HPE recommends that this topology synchronization is used as a starting point in every OM evolution project. This will ensure that all OM nodes and OM SPI service models are reflected in the RTSM, and that OM events can be related to corresponding CIs.

However, as OM will be switched off at some point, the topology has to be created and maintained through other mechanisms.

Here the automatic discovery features of OMi play a central role. Although OMi allows you to start with a rather simple topology that represents just the nodes in your IT environment, it is recommended to populate the RTSM with additional CIs.

For example, as in the OM SPI discovery, all the necessary CIs and relationships for an application area like Oracle can be created using the discovery policies that are contained in the OMi Management Pack for Oracle.

All Management Packs contain such discovery policies so that you don't have to worry about populating the RTSM yourself.

Even the nodes, which are represented as Configuration Items of type Node in the RTSM, are created automatically when an agent is installed and connected to OMi. Every agent sends basic information about itself to its primary manager, and this information is used by OMi to create node, IP address, interface, and Operations Agent CIs with corresponding relationships.

Where no Management Pack exists, there are several option to populate the RTSM with CIs and CI Relationships:

- Use a separate HPE UCMDB and HPE Universal Discovery (previous product name: Dependency Mapping and Automation - DDMA) to discover CIs (additional licenses required) and use UCMDB-BSM Synchronization to synchronize them into the RTSM (see the RTSM Best Practice document for more details)

- Use the UCMDB integration features available on the OMi/RTSM system itself. Note the licensing levels:

○ UCMDB Foundation License (included in the OMi license). This license grants the right to use UCMDB as the backbone component of select BTO products and includes the right to use Custom data exchange integrations (that is, the Generic DB Adapter, the Generic Push Adapter and customer-developed Java adapters), as well as the HPE Universal CMDB Web Service API and the HPE Universal CMDB API (Java)

○ UCMDB Integration Only License (not included in the OMi license)
This license grants the right to integrate third-party (non-HPE) products with UCMDB using various types of integrations

○ DDM Advanced Edition License (not included in the OMi license). This license grants the rights to:

  ■ Integrate BTO and third-party (non-HPE) products with UCMDB, using any type of integration

  ■ Use all Discovery and Dependency Mapping (DDM) capabilities to populate UCMDB

If other domain managers like NNMi, Microsoft SCOM, or Nagios are integrated into OMi, then these integrations typically also add topology from those domain managers. Check the corresponding integration documentation for details on which connectors creates node or infrastructure CIs.

Some OM customers use node names that include the purpose of the node and the software running on it, like W28HRPROD – Windows 2008, HR application, Production system, or RHFINTST – Red Hat, Finance application, Test system. By parsing these node names they are able to automatically group nodes into corresponding node groups (to which they assign corresponding policies).

A similar approach can be used on OMi using the RTSM Enrichment rules: Enrichment rules can look for nodes with certain node names and can then create Running Software CIs. Monitoring Automation is then able to automatically deploy monitoring aspects to those newly "discovered" CIs. For details, see How to create CIs Using Enrichment Rules.

Plan Operator Groups

In larger environments with more than a few operators processing events, operators are often organized into groups with dedicated responsibilities and permissions.

For example, in OM responsibilities can be defined in such a way that database operators are allowed to see and close database events, but not storage events and vice versa.

In OMi responsibilities can be defined in a very similar way using user roles that grant permissions to certain views, tool categories and event categories. Additionally, the customizable Workspace pages can provide OMi operators with overview dashboards and contextual information from business impact information to detailed performance graphs. You can customize these pages to provide the exact information that is needed to resolve issues quickly, as different operator groups might require different information to do their jobs. Operators focusing on business applications might have other needs compared to operators focusing on OS-level problems. In case one or more operators are part of multiple groups, you could also create a special My Workspace page for them.

So in this planning phase you should determine the number of My Workspace pages and what information they should show, as well as the number of operator roles with different responsibilities and permissions, and which types of events should be automatically assigned to which operator groups.

In an early implementation phase you might use an event-state driven event dashboard in My Workspace pages. In later phases, when you have implemented KPIs and His, you can add to that with Service Health components.

You can also create user groups and user roles for OMi administrators and delegate administrative permissions to different users.

For more details, see "Create Users, User Roles, and User Groups" on page 73.

Plan Integrations

OM integrates with various applications from HPE and other vendors using a variety of different technologies and interfaces. Many of the HPE product integrations are provided for OMi as well. See Appendix - Available Integrations & Integration Technologies for a list of all available integrations.

Different use cases require different integrations. Depending on your needs, determine which integrations need to be reestablished and whether out-of-the-box integrations exist and can be used.

Event Integrations

Several BSM Connectors exist to integrate 3rd-party domain managers in OMi. Additionally all integrations using standard operations agent policies (opcmsg, opcmon, SNMP, logfile, and so on) can be reused as OMi supports the same policy types. OMi provides the opportunity to leverage new policy types that are not available in OM, such as XML (in Monitoring Automation and BSM Connector), structured log file, Database, REST Web Service Listener (all in BSM Connector).

For an up-to-date list of available BSM Connectors, check the HPE Live Network Content Marketplace: https://hpln.hpe.com/node/122/contentfiles.

Integrations for Operators

To implement an efficient operator workflow integrations into trouble-ticket or notification systems might be important as well as integrations into help systems or knowledge-bases and systems used for the remediation of problems.

OMi contains a built-in notification system and a flexible forwarding interface for trouble-ticket or notification system integrations. Out-of-the-box integrations for HPE Service Manager are available from HPE. Other incident management systems can be integrated using the forwarding interface or partner solutions.

For more details about the forwarding interface, see the **Extensibility Guide > Integrating External Event Processes and Administration Guide > Event Processing > Event Forwarding**.

For details regarding the out-of-the-box integration with Service Manager, see the OMi Integration Guide.

For more details about the Notification interface, see the **Administration Guide > Event Processing > Notifications**.

OMi integrates with Operations Orchestration, and operators can launch run books from their console. Run books can even be executed automatically when events arrive. For more information, see the OMi Integration Guide.

Like OM, OMi offers an external instruction text interface, which allows you to retrieve instructions from external databases, web pages or other sources. See the **Administration Guide > Operations Console > External Instructions** for more details.

Integrations for Event Enrichment, Correlation or Automation

OM allows event enrichment and automation through its Message Stream interface (MSI) implemented in C, Java, or COM or via WMI APIs, the OM Incident Web service interfaces, ECS and Composer.

Instead of ECS and Composer, OMi offers server-side Stream-Based Event Correlation (SBEC), Topology-Based Event Correlation (TBEC), and the Event Processing Interface (EPI) which uses Groovy scripting. Groovy is an agile and dynamic scripting language that builds upon the strengths of Java but has additional power features inspired by languages like Python, Ruby and Smalltalk. It makes modern programming features available to Java developers with an almost-zero learning curve and interoperates with other Java code and libraries.

You can use these technologies to replace ECS and Composer. The following table lists the main OM Composer use cases and their replacement in OMi.

OM Composer		OMi
Enhance (Perl)		EPI (Groovy)
Multi Source		SBEC Combination Rule
Rate		EPI (Groovy) or SBEC Repetition Rule
Repeated		SBEC Repetition Rule
Suppress		SBEC Combination Rule or Event Suppression Rule
Transient		SBEC Combination Rule

Note: Composer imposes a fixed order of execution for each correlation. OMi SBEC rules are executed in the order chosen by the user.

Composer has the capability to perform Lookups and extract substrings from message attributes. With OMi, EPI Groovy scripting can perform this function prior to feeding the events to SBEC.

To allow a step by step transition from OM Composer perl scripts to groovy, it is possible to call perl scripts from groovy. See Running External Programs (such as Perl Scripts) from Groovy for more details. For best performance translate your perl script into Groovy code.

Stream-Based Event Correlation (SBEC)

Stream-based event correlation uses rules and filters to identify commonly occurring events or combinations of events and helps simplify the handling of such events by identifying events that can be withheld, removed or need a new event to be generated and displayed to the operators. This can be used as OM ECS replacement.

The following types of SBEC rules can be configured:

- Repetition Rules: Frequent repetitions of the same event may indicate a problem that requires attention.
- Combination Rules: A combination of different events occurring together or in a particular order indicates an issue, and requires special treatment.
- Missing Recurrence Rules: A regularly recurring event is missing, for example, a regular heartbeat event does not arrive when expected.

Event Processing Interface (EPI)

The EPI enables you to run user-defined Groovy scripts for events that match a user-defined event filter during event processing. With these scripts, you can modify and enhance events. For information, see the **Extensibility Guide > Event Processing Interface**.

You can find the corresponding Groovy and Java API Documentation at the following location:

<OMi_HOME>/opr/api/doc/opr-external-api-javadoc.zip

The EPI interface is also the replacement of OM MSI interfaces. Any C/Java/COM-based MSI implementations have to be replaced by Groovy-based EPI implementations if they cannot be achieved by one of the following OMi features.

Topology-Based Event Correlation (TBEC)

The Topology-Based Event Correlation license is required for the topology-based event correlation functionality. For details, see the **Administration Guide > Event Processing > Topology-Based Event Correlation**.

Time-Based Event Automation (TBEA)

Time-Based Event Automation rules enable administrators to configure actions to be executed on events matching a user-defined set of criteria after a specified time.

For information, see the **Administration Guide > Event Processing > Time-Based Event Automation**.

Suppression Rules

Events that match a user-defined filter can be suppressed. For information, see the **Administration Guide > Event Processing > Event Suppression**.

Event Web Service Interface

OMi offers the Event Web Service interface, which is similar to OM's Incident Web Service interface. It allows you to receive, modify, and create events. If an OM MSI application is taking a feed for external purposes, then you could consider implementing it in OMi using the Event Web Service interface or forward it to external event processing.

For details, see the **Extensibility Guide > Automating Operator Functions and Event Change Detection > Automating Operator Functions using the Event Web Service Interface**.

Integrations for Onboarding and Automation of Configuration

OM allows to automate various configuration tasks, such as:

- Node setup
- Node to node group assignments
- Policy deployment
- Policy creation and modification
- Operator setup
- Automatic granting of certificates
- Configuration exchange between OM servers

These tasks can be automated through the WMI interfaces (OM for Windows), COM interfaces (OM for Windows), C and Java APIs (OM for UNIX), and server command line interfaces like ovpmutil (OM for Windows) or opcnode (OM for UNIX).

In OMi, nodes are replaced by Configuration Items and are either discovered or can be created using RTSM interfaces as outlined above, or using the opr-node CLI.

For automatic configuration deployment, OMi users can use Monitoring Automation automatic assignment rules. If a CI is modified or newly discovered, Monitoring Automation automatically evaluates any auto-assignment rules defined for its CI type. If an automatic assignment rule evaluates to true, Monitoring Automation automatically assigns the items specified in the rule to the modified or newly discovered CI, and starts the corresponding deployment jobs.

The automatic granting of certificates is possible in OMi based on IP ranges or using a Groovy script.

For configuration exchanges between OMi servers, OMi offers the content pack concept. This allows a semi-automated configuration exchange. After manually creating or updating a content pack on the source system, it's possible to export and import the Content Pack on another system using the Content Manager CLI. Using content packs you can exchange many configuration data, including policy templates and instrumentation files, indicator definitions, user roles, filters, … Similarly, CI Types, views, and other RTSM artifacts can be exchanged using the RTSM package manager. Topology data can be synchronized using RTSM-RTSM synchronization.
However, OMi currently does not allow synchronizing users, user groups, My Workspace pages, or infrastructure settings.

Plan Monitoring Configuration

Note: If you do not plan to use OMi Monitoring Automation, you can skip this step.

OMi Monitoring Automation provides the biggest value when you automate the configuration of Operations Agents or SiteScope. Although OM offers some automation features as well, like automatic deployment of policy groups based on node groups or discovered services, you might not have used these extensively, or policy groups or even single policies might have been assigned and deployed manually.

To avoid unnecessary effort during a later step, we recommend that you evaluate your current monitoring configuration and specifically think about the standards you want to establish.

Consider what type of systems and applications (represented in the RTSM as Configuration Items) should always be monitored in the same way, and where are variations necessary for a larger or smaller group of configuration items. Which systems should and can be monitored automatically? Which systems always need to be configured manually?

Although Monitoring Automation allows to easily tune parameters, it is still a good idea to try to standardize the monitoring using meaningful defaults, and to try to automate assignments.

For example, you might want to monitor some key Oracle metrics and log files for most of your Oracle databases, and additional metrics for a smaller group of business-critical databases for which you also want to be alerted sooner. You can achieve this by using the Oracle Essential Management template for the first group and a customized Oracle Extensive Management template for the second. But you should also plan the automatic or manual assignment of those templates.

If you have a standard mechanism to roll out Oracle databases and standard database users and passwords for Oracle management, then you can start the monitoring of those systems automatically using an automatic assignment rule. You can specify the database user and password either in the automatic assignment rule or in your management template.

If instead all your business-critical databases will have varying passwords that are not known in advance, you must provide the passwords when assigning the Extensive management template manually. Another option is to assign and deploy the Extensive management template automatically with a wrong password – knowing that this will produce some error events – and to change the password parameter on the database CI afterward.

A third option is to use the Monitoring Automation Web Service interface to automatically assign the Extensive Management template after setting up a business-critical database, with the database user and password that were just configured.

Evaluate Your Current Monitoring Configuration

In this planning phase it is a good idea to evaluate what your current monitoring looks like: how you are monitoring Oracle databases today, What policies are used, What metrics are collected, Where should the same and where should different thresholds, and therefore different policies, be used.

Some of these questions can be answered using simple OM database scripts. You can download a policy statistic script that tells you what policies are in use from the HPE Live Network Content Marketplace at https://hpln.hpe.com/node/14127/contentfiles/?dir=18240.

As a next step you should determine if your monitoring needs can be addressed by the Infrastructure Management Pack, which comes for free with OMi, or by other Management Packs.

If there is no Management Pack available and if you want to reuse existing OM policies in OMi, you need to estimate how many policies need to be imported into OMi. You should only import policies that are in use or that you plan to use and not the complete policy inventory.

> **Note:** In case you created policy versions or copies of policies to change thresholds or parameters, such as message groups or custom attributes, then you will not have to import all these variations. You will instead import one base policy and then use the OMi parameterization feature to implement those variations.

Plan License Migration

Optional Operations Bridge License Exchange Program

HPE offers an Operations Bridge License Exchange Program. It provides Operations Manager customers with an easy, standard way to exchange their OM Management Server, OM Basic Suite, Operations Agent/Operations OS Instance, Operations SPI and Reporter licenses to Operations Bridge Premium and OMi Management Pack licenses.

> **Note:** This license exchange will allow customers to continue to concurrently use their existing software (like OM and SPIs), which allows customers to move to OMi, Operations Bridge Reporter, and Operations Bridge Management Packs at their own pace.

Contact your HPE account team or HPE partner for details.

TBEC License

> **Note:** The Operations Bridge License Exchange Program does not include the OMi add-on product TBEC (Topology-based event correlation).

If you want to evaluate this feature during an evolution project, make sure the temporary Instant-on license has not expired. It is activated when OMi is installed. If OMi was already in use, request a new temporary evaluation license from the HPE Software License Center.

Chapter 3: Establishing Topology, Consolidating, and Controlling Events

Establish Infrastructure Topology

As described in the planning phase, OMi offers various advantages when the IT objects being monitored are represented in the RTSM as Configuration Items of specific CI types.

You should create these CIs as part of a first step, before integrating events, so that you can benefit from these advantages from the start.

Creating Node and Infrastructure CIs Using Topology-Synchronization of OM Node and Service Data

As an OM user, the easiest way to populate the RTSM is using the data that is already available in OM. OMi topology synchronization allows you to create CIs based on the OM nodes, node groups, layout groups and SPI service models. You can specify which SPI service models should be synchronized.

Infrastructure CIs can be created from the discovered services of the following SPIs:

- Microsoft Active Directory
- Exchange
- Lync
- SQL Server
- IIS
- Oracle Database
- WebLogic
- WebSphere
- Blackberry Enterprise Server
- Infrastructure (including System, Cluster and Virtualization Infrastructure)
- SAP

See the following information in the OMi Integration Guide:

- Establishing a trust relationship between OMi and OM
- Setting up the OM server as a connected server
- Synchronizing the topology

Creating Node CIs

Node CIs (and corresponding IP address and Operations Agent CIs) are either created via topology synchronization or created automatically for all nodes that run an Operations Agent when an agent is installed and connected to OMi. Every agent sends basic information about itself to its primary manager and this information is used by OMi to create node, IP address, interface and Operations Agent CIs with corresponding relationships.

However, if you do a lot of proxy monitoring where one agent acts as proxy and creates events for various other nodes (for example using SNMP policies), then these nodes have to be created either manually or by using other mechanisms. If you are using topology synchronization, those proxied nodes are created based on OM external nodes or message allowed nodes.

Creating (Proxied) Node CIs Manually

The easiest way to create node CIs manually is using **Administration > Setup and Maintenance > Monitored Nodes**. For details, see the **Administration Guide > Setup and Maintenance > Monitored Nodes**.

Creating Infrastructure CIs

Infrastructure CIs can be created using topology synchronization based on OM SPI discovery data for the following areas: Microsoft Active Directory, Exchange, Lync, SQL Server, IIS, Oracle Database, WebLogic, WebSphere, Blackberry Enterprise Server, Infrastructure (including System, Cluster and Virtualization Infrastructure) and SAP.

After moving to OMi, when SPIs are no longer used, it is necessary to replace the SPI discovery with corresponding OMi Management Pack discovery aspects (where available). See the OMi Management Packs Evolution Guide for details.

Note: Removing a SPI discovery policy from a node triggers the deletion of services in OM and of CIs in the OMi RTSM. To prevent this from happening, set the **Skip CI Deletion** infrastructure setting (Infrastructure Settings for Operations Management > HPOM Topology Synchronization Settings) to **true**. This will disable the automatic deletion of CIs when performing topology synchronization.

Operations Management - HPOM Topology Synchronization Settings		
Name ▲	**Description**	**Value**
Commit Bulk Size	The maximum number of objects to commit to the RTSM in a single call.	2000
Dump Data	Enables (true) the saving of the data from all processing steps to the hard disk. This is not recommended for production systems, as it has a negative impact on performance.	false
Groovy Scripts	Enables (true) Groovy script usage to manipulate the synchronization data during the synchronization process.	true
Packages for Topology Sync	Semicolon-separated list of packages that are used for topology synchronizations.	default;nodegroups;operations-agent
Skip CI Deletion	Skip CI Deletion Disables (true) automatic deletion of CI when performing topology synchronization. CI deletion responsibility is transferred to RTSM CI ageing.	**true**

Discovery aspects are often assigned to Computer or node CIs. See the corresponding Management Pack Online Help section for details about how to deploy the discovery aspects.

If no Management Pack exists, there are several ways to populate the RTSM with CIs and CI Relationships. For more details, see Technologies for Establishing Infrastructure Topology in the Plan the Evolution chapter.

If a BSM Connector is used to integrate other domain managers, it can also integrate topology from those domain managers. Details about BSM Connector installation and topology policies are described in the BSM

Connector installation and Upgrade Guide (interactive document), the documentation of the specific BSM connectors available on the HPE Live Network Content Marketplace (for example, see https://hpln.hpe.com/contentoffering/bsm-connector-microsoft-scom), and in the BSM Connector Help under **Integrating Data With BSM Connector > Topology Policies**.

How to Create CIs Using Enrichment Rules

If the purpose of the node and the software running on it can be determined from node attributes like the node name, for example W28HRPROD for Windows 2008, HR application, Production system, or RHFINTST for Red Hat, Finance application, Test system), then Enrichment rules can look for nodes with certain node names and can create Running Software CIs.

This is possible as long as there is only one such running software CI per node and if the Running Software CI creation does not require additional identification attributes or key attributes. Enrichment rules are not a suitable solution for creating Oracle database CIs, as multiple such Oracle instances can run on one node, and the oracle SID must be known to create the CIs.

For information on creating enrichment rules using the enrichment manager, go to **Administration > RTSM Administration > Modeling > Enrichment Manager**. See the corresponding OMi Help topics for details.

The following example shows the most important settings. It assumes that a new "Custom Application" CI type has been created as a sub-type of the Running Software CIT, inheriting all settings, such as attributes and identification rule.

The example enrichment rule creates a running Software CI of type "Custom Application" and the composition relationship to the node.

Create a new enrichment rule. Add the computer CI type and use Query Node Properties to filter the nodes:about node queries.

The example rule looks for all nodes containing "win" in the PrimaryDnsName, as you can see in the Attributes tab of the Computer CIT:
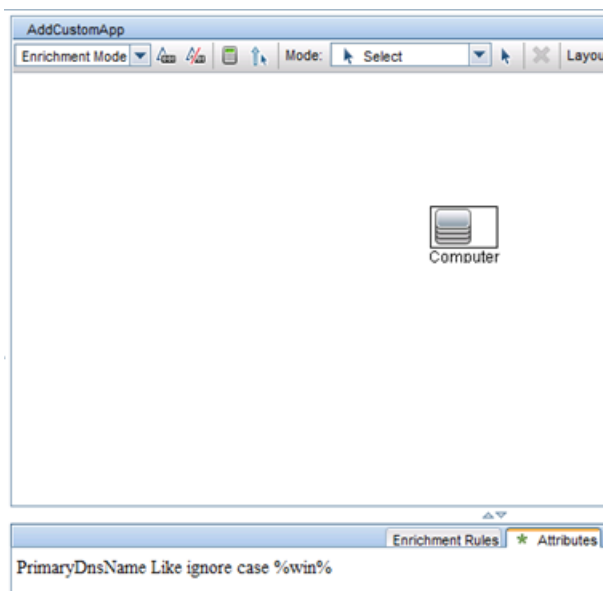
Switch to enrichment mode and add the custom application CI type. Create the composition relationship between both. Use Update Query Node:
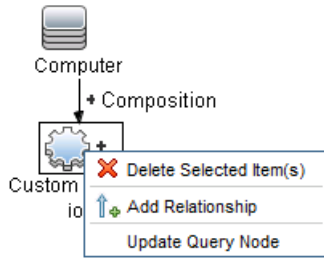
Provide a Name and DiscoveredProductName, as these attributes are required for identifying a Running Software CI.

The enrichment rule summary can be seen on the **Enrichment Rules** tab:
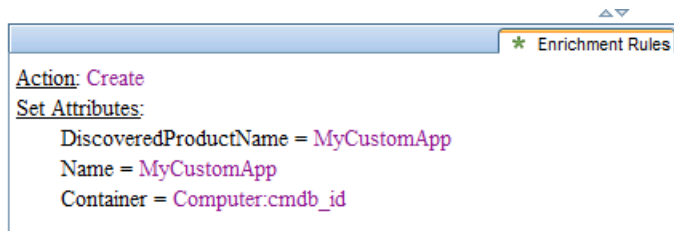
You can use the Calculate Query Result Count button to check how many Computers currently match the query. In the example there are seven matching Computers.
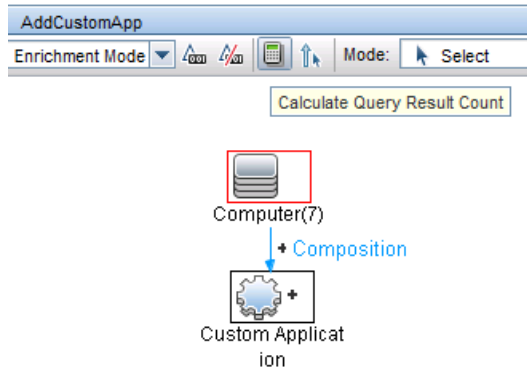
Next, you have to activate the rule (in the rule properties) and create a schedule job to run it:

Go to **Administration > RTSM Administration > Administration > Scheduler** and create a new job that executes an enrichment rule. Pick the enrichment rule you created and define a schedule, for example, once per day.
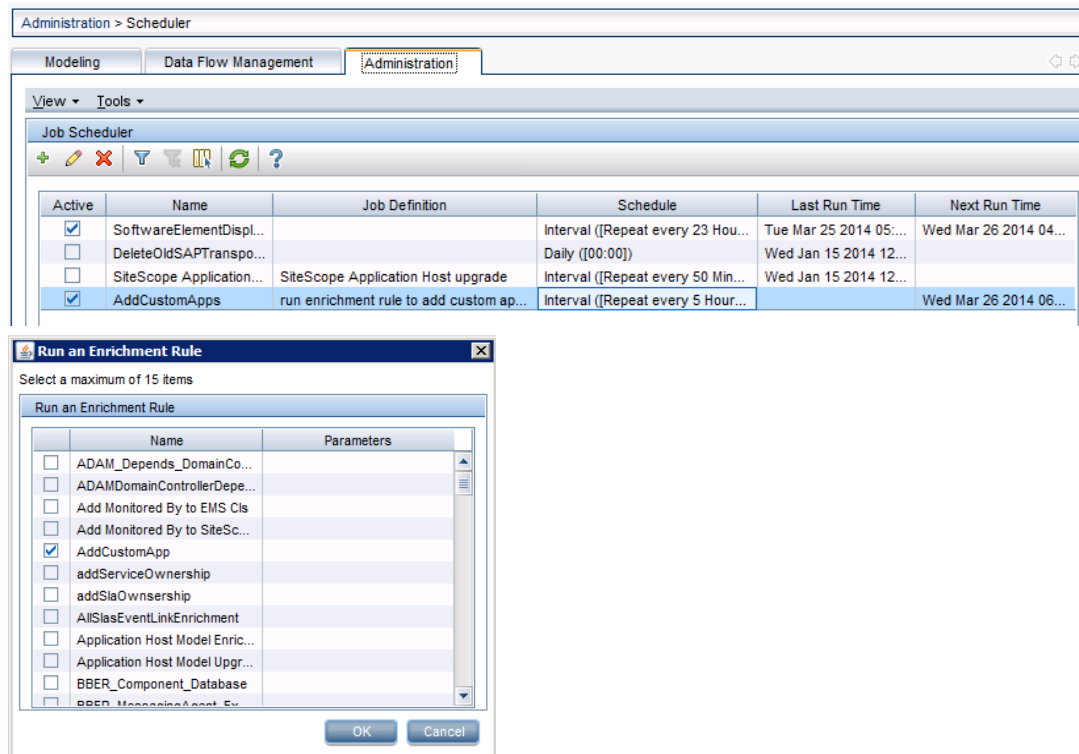
If needed, you can use the Modeling Studio to create a view that shows all nodes with the "Custom Application" SW running, for example, using a simple pattern view:
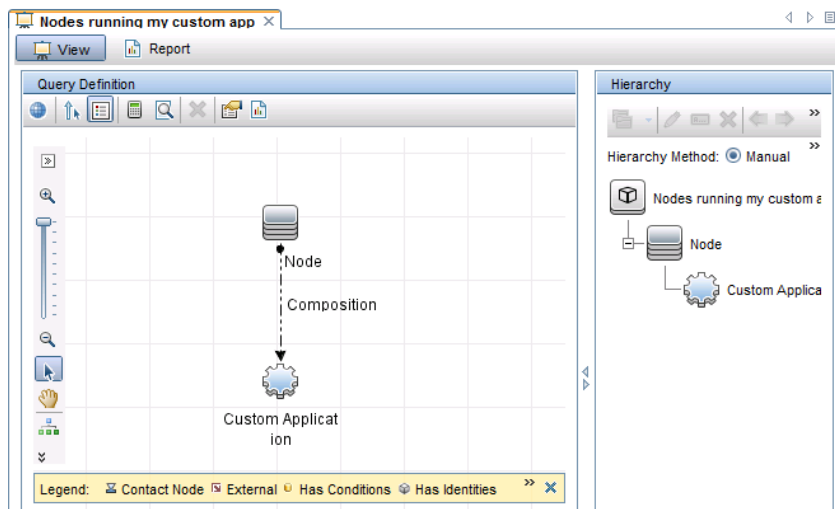
Consolidate Events from Various Sources

After establishing the infrastructure topology it's time to integrate events. As the necessary CI topology already exists, OMi CI resolver can relate events to the correct CIs, which allows view-based filtering and other CI-type specific functions.

Connect OM to OMi

To forward events from OM to OMi, see the following information in the OMi Integration Guide:

- Configuring the OM forwarding policy
- Validating event synchronization

> **Note:** Other steps were completed when integrating the topology of OM.

Connect SiteScope to OMi

To forward events from SiteScope, see the SiteScope manual Integration with HP Operations Manager Products.

Connect Other Domain Managers to OMi Using BSM Connectors

To forward events from other event managers, see the documentation of the specific BSM Connectors available on the HPE Live Network Content Marketplace (for example, see https://hpln.hpe.com/contentoffering/bsm-connector-microsoft-scom) and the BSM Connector Help.

Control Events

Once events are integrated, you can use OMi correlation, enrichment, and automation features to control events.

A high-level overview of the available features has been provided in the Planning the Evolution chapter of this guide.

Event Correlation

Duplicate Suppression

The duplicate suppression concepts are almost the same between OMi and OM. Unlike OM, however, OMi is also able to detect duplicates based on ETI values.

If required, you can change the default duplicate suppression settings in **Administration > Setup and Maintenance > Infrastructure Settings**.

Select **Applications** and use the list to set the administration context to **Operations Management**. Scroll to **Operations Management - Duplicate Events Suppression Settings**.

Closing Related Events

Like OM, OMi is able to close related events based on message keys and key-matching patterns. OMi is also able to detect related events based on HI values. If required, you can change the default settings in **Administration > Setup and Maintenance > Infrastructure Settings**.

Select **Applications** and use the list to set the administration context to **Operations Management**. Scroll to **Operations Management - Change State of Related Events Settings**.

Stream-Based Event Correlation (SBEC)

Go to **Administration > Event Processing > Correlation > Stream-Based Event Correlation**, and see the corresponding OMi Help topics for details.

Stream-Based Event Correlation (SBEC) uses rules and filters to identify commonly occurring events or combinations of events, and helps simplify the handling of such events by automatically identifying events that can be withheld, removed, or require a new event to be generated and displayed to the operators. This can be useful when replacing OM ECS.

The following types of SBEC rules can be configured:

- Repetition Rules: Frequent repetitions of the same event may indicate a problem that requires attention.
- Combination Rules: A combination of different events occurring together or in a particular order indicates an issue, and requires special treatment.
- Missing Recurrence Rules: A regularly recurring event is missing, for example, a regular heartbeat event do not arrive when expected.

SBEC Rules are processed in the order defined in the rules list. Modifications are executed as soon as the rule is matched, and subsequent rules see modifications done by earlier rules.

Topology-Based Event Correlation (TBEC)

The Topology-Based Event Correlation license is required for the topology-based event correlation (TBEC) functionality. This builds on the Event Management Foundation license.

For details, see the OMi Help section **Administration > Event Processing > Correlation > Topology-Based Event Correlation**.

At this stage you can begin to benefit from TBEC if you are using OM SPIs, as those SPIs send events that match the out-of-the-box TBEC rules. These rules are enabled per default, and no additional configuration is necessary.

If you use custom policies without Event Type Indicators, then TBEC will not be able correlate them. We recommend that you add Event Type Indicators to your custom policies at a later stage, see chapter Add value on Top.

Event Storm Suppression

Like OM, OMi can detect an event storm on a system and discard events (if not matched by an exception rule), until the rate of incoming events drops below the event storm end threshold.

To change the default settings, go to **Administration > Event Processing > Correlation > Event Storm Suppression** and see the corresponding OMi Help topics.
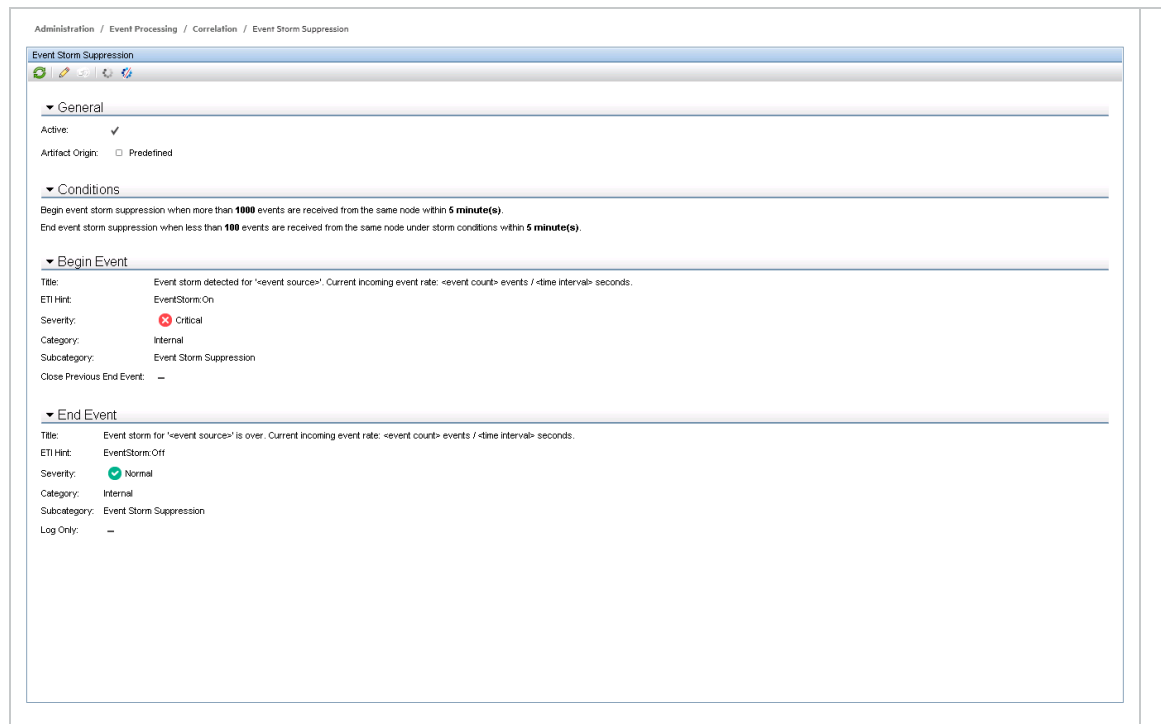
Event Suppression

OMi can suppress events on the server using event filters. This is useful if the event generation is not under control of the Operations Bridge and cannot be disabled at the source. Go to **Administration > Event Processing > Correlation > Event Suppression** and see the corresponding OMi Help topics.
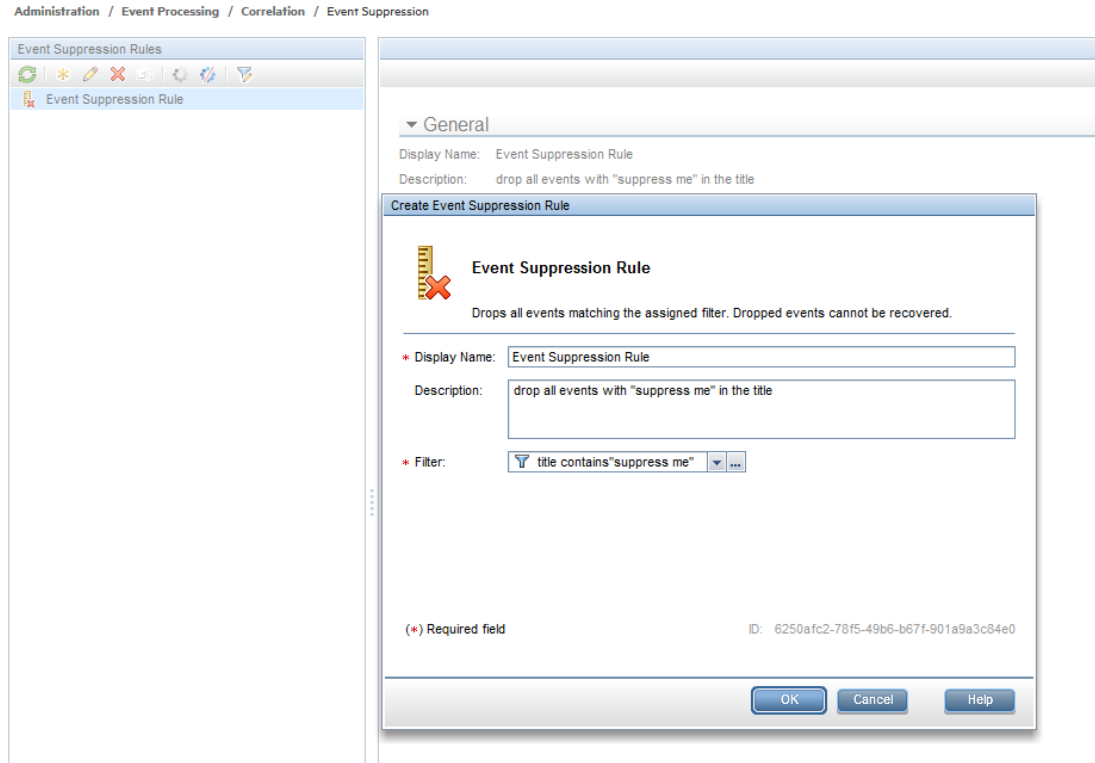
Event Enrichment

Event Enrichment and Custom Processing Through EPIs

Event processing customization enables you to implement custom script-based event processing directly on events. This is possible at four different processing stages: before CI/ETI resolution, after CI/ETI resolution, before storing the event in the database and after storing the event.

The range of events fed into the custom event processing can be controlled by specifying event filters. Different scripts can be enabled or disabled during runtime.

The script-based event processing logic has to be supplied as a groovy script. A number of sample scripts are available in the following directory:

<OMi_HOME>`/opr/examples/epi_scripts`

Go to **Administration > Event Processing > Automation > Event Processing Customizations** and see the corresponding OMi Help topics for details.

You can find the Groovy/Java API Documentation at the following location:

<OMi_HOME>`/opr/api/doc/opr-external-api-javadoc.zip`

EPI Script Development Kit

The OMi Script Development Kit available from the HPE Live Network Content Marketplace (https://hpln.hpe.com/node/14127/contentfiles) helps script developers edit, validate, test, and debug their

HPE OMi groovy scripts within Eclipse, outside of an HPE OMi installation. The benefits of using the OMi Script Development Kit in Eclipse include:

- Automatic completion and online documentation for HPE OMi Event Processing Interface (EPI) APIs.
- Create and feed test events into an EPI scripts and get the resulting modifications Visual debugging support to step through EPI script execution.
- Import sample events from a running HPE OMi system.
- Configurable access to a running HPE OMi Run-time Service Model (RTSM) instance for topology queries.
- back for verification.

Example of an EPI Script to Modify Event Attributes

```
import java.util.Date;

import java.util.List;


import com.hp.opr.api.scripting.Action;

import com.hp.opr.api.scripting.Event;

import com.hp.opr.api.scripting.EventActionFlag;

import com.hp.opr.api.scripting.LifecycleState;

import com.hp.opr.api.scripting.MatchInfo;

import com.hp.opr.api.scripting.NodeInfo;

import com.hp.opr.api.scripting.PolicyType;

import com.hp.opr.api.scripting.Priority;

import com.hp.opr.api.scripting.ResolutionHints;

import com.hp.opr.api.scripting.Severity;


/*
 * This example set all possible event attribute to some example values.
 */


class SimpleExample
{
  def init()
  {

  }


  def destroy()
  {

  }


  def process(List<Event> events)
  {
      events.each {
      event -> modifyEvent(event);
```

```
  }

 }


        def modifyEvent(Event event)

        {

   String application = event.getApplication();

   event.setApplication("Modified by EPI: " + application);


   long groupId = event.getAssignedGroupId();

   event.setAssignedGroupId(groupId);


   int assignedUserId = event.getAssignedUserId();

   event.setAssignedUserId(assignedUserId);


   Action autoAction = createSampleAction();

   event.setAutoAction(autoAction);



   ResolutionHints hints = createSampleResolutionHints();


   event.setNodeHints(hints);

   String ciInfo = event.getRelatedCiHint();

   event.setRelatedCiHint("Modified by EPI: " + ciInfo);


        }


 def ResolutionHints createSampleResolutionHints()

 {

   ResolutionHints hints = new ResolutionHints(false);


   hints.setCoreId("CoreId");

   hints.setDnsName("mydqdn.com");

   hints.setHint("My Hint");

   hints.setIpAddress("0.0.0.0");
```

```
    return hints;

  }



  def Action createSampleAction()

  {

    NodeInfo actionNodeInfo = new NodeInfo(false);

    Action action = new Action(false);


    actionNodeInfo.setCoreId("CoreId");

    actionNodeInfo.setDnsName("myfqdn.com");

    actionNodeInfo.setIpAddress("0.0.0.0");


    action.setCall("Call");

    action.setNode(actionNodeInfo);

    action.setStatus(EventActionFlag.AVAILABLE);

    return action;

  }

}
```

The following figure shows the configuration dialog where EPI scripts are specified:
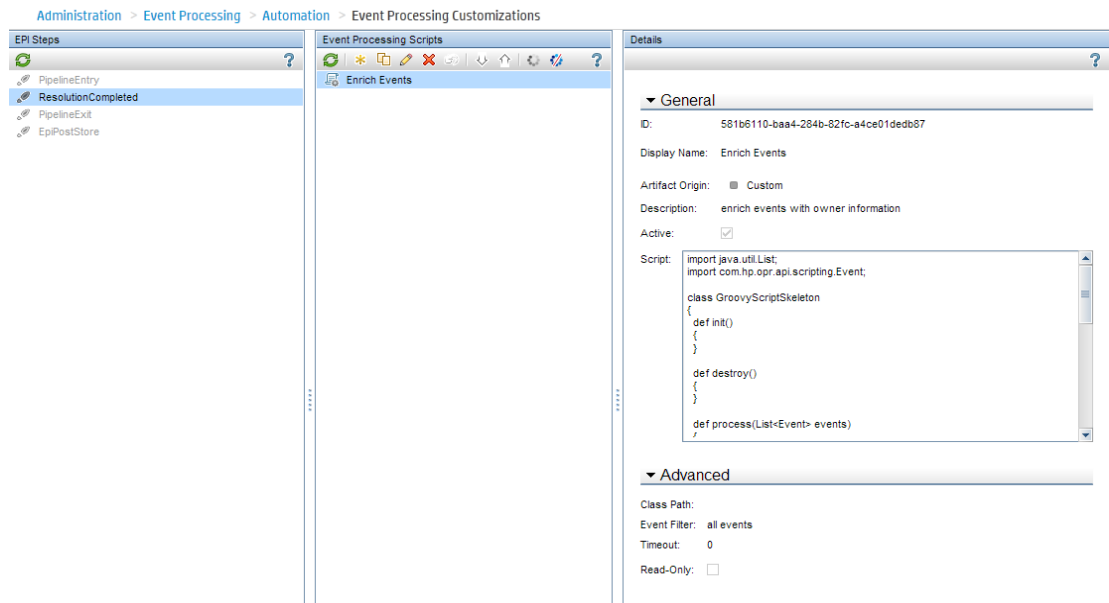
Event Automation

Some of the automation features described in the following section refer to operators or operator groups that are created in a later phase. Therefore, the implementation of these operator-focused automations might have to be completed at later point. If the operator groups are already defined, you can already refer to them in automation rules (even if the permissions for each group are not yet defined). Otherwise, set up the rules when the operators and groups are set up.

Time-Based Event Automation (TBEA)

Time-Based Event Automation rules enable administrators to configure actions to be executed on events matching a user-defined set of criteria after a specified time.

- If an automatic action for a message fails, you can configure a restart of the automatic action after a short delay. If it repeatedly fails, after a predefined number of retries, further retries are stopped and the event is escalated.

- If an event is not being worked on after a predefined period in time, you can configure a change to give it higher priority, for example by increasing its severity, or by assigning it to the next support level.

- You can configure the closing of an event that is older than a predefined period of time.

- You can configure transferring control of events based on event age. For example, escalate if an event remains in the browser for more than 2 days, close if the message remains for longer than 7 days (despite the escalation after 2 days).

The following figure shows available actions for Time-Based Event Automation rules:
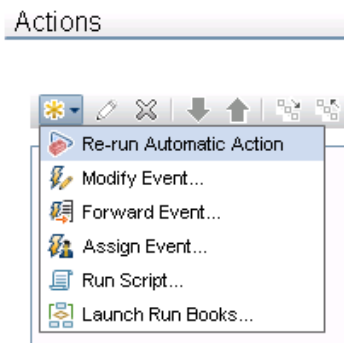
Go to **Administration > Event Processing > Automation > Time-Based Event Automation**, and see the corresponding OMi Help topics for more details.

The following example shows a time-based event automation scenario, which increases the severity of an open event after 1 hour:
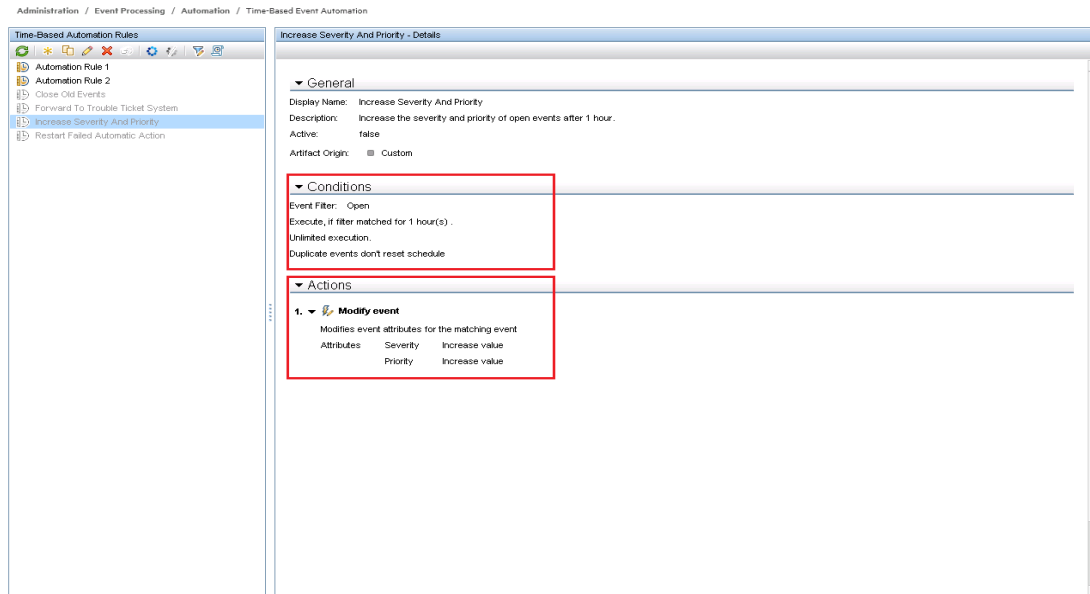
Automatic Run Book Execution

HPE Operations Orchestration (OO) run books that do not require any user input can be started automatically when an event matching a certain filter is received. The start and the result of the run book execution will be added as annotations to the event.

To achieve this, you first have to integrate OO into OMi and map OO run books to CI Types. See the OMi Integration Guide for more information. This integration will then also allow operators to launch run books manually. You can then use those run books in automatic run book execution rules by going to **Administration > Event Processing > Automation > Automatic Run Book Execution**.

Create a new rule and specify an event filter for which the run book should be executed, then select the run book.

> **Note:** You will only be able to select run books after completing the OO integration.

The following figure shows an example automatic run book execution rule:
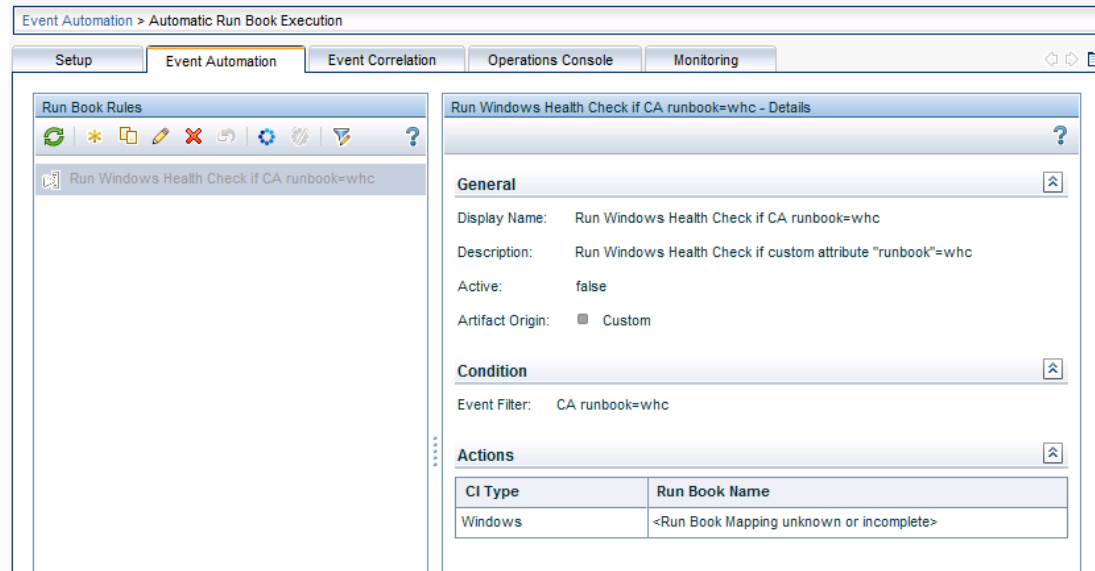
Automatic User Group Assignments

OMi can automatically assign events to user groups. The events to be assigned are defined by an event filter or view filter. Automatic user assignment is initiated as soon as events arrive in HPE OMi.

To configure user group assignment rules, go to **Administration > Event Processing > Automation > User Group Assignments**.

> **Note:** This requires operator groups to have already been defined, which might not be the case at this stage of the evolution.

Forwarding to Incident Management Systems

Incoming events can be automatically forwarded to Incident Management Systems like HPE Service Manager and others.

OMi provides an enhanced out-of-the-box integration for HPE Service Manager that includes:

- Relating incidents, when the corresponding events are related
- Displaying current incident attributes (lifecycle, assigned group, severity, priority) in the event
- Light-weight single sign on cross launch in context from the event to the incident
- Visibility of recent changes and incidents for the related CI
- Downtime handling

Events can be forwarded using two techniques: using a Groovy script that accesses specific APIs of the external server, or through an event web service interface that has to be implemented by the external server.

See the **Extensibility Guide > Integrating External Event Processes and Administration Guide > Event Processing > Event Forwarding** for more details about the forwarding interface. See the OMi Integration Guide for details regarding the out-of-the-box integration with Service Manager.

To set up an external event processing server, go to **Administration > Setup and Maintenance > Connected Servers** and create a new server of type external event processing server.

Once the external server is ready, you can set up a forwarding rule. Go to **Administration > Event Processing > Automation > Event Forwarding**.

OMi provides a default forwarding rule called "Automatically Forward to Trouble Ticket Systems", which is disabled per default. It forwards all events for which the trouble ticket flag is set. The flag is internally translated into a corresponding custom attribute ForwardToTroubleTicket, which can be used in the forwarding event filter. You only have to specify the server it should use.
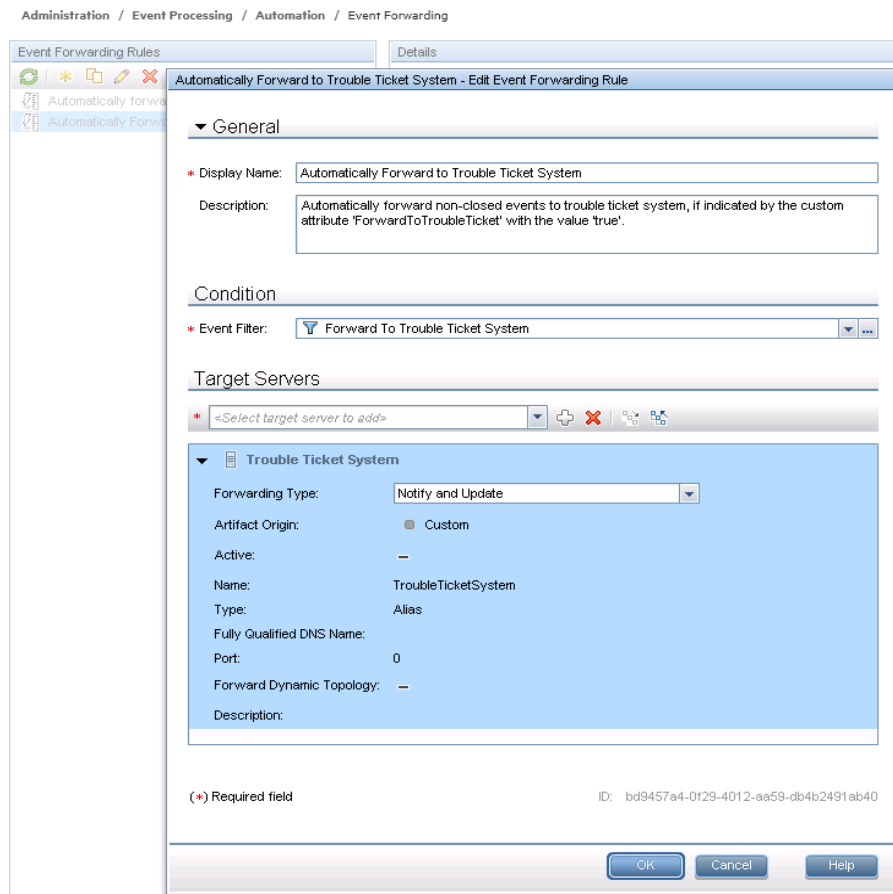
By default, the forwarding type "Notify and Update" is used, but other forwarding types are possible, depending on your requirements.

- Notify and Update: target server receives original events and all further updates (event will be closed in OMi).

- Synchronize: target server receives original events and all further updates and sends back all updates (event might be closed by OMi or target server using event sync web service).

- Synchronize and Transfer Control: target server receives original events and updates and sends back all updates. Ownership of the event is transferred to the other server. (event will be closed by target server using event sync web service).

Event Integrations via Web Services and CLI

OMi offers the Event Web Service for integrating events into other applications, and automating operator functions. This is a REST-based web service that allows you to do everything that an operator can do in the console while working on events. It also provides subscription support through Atom feed functionality. You

can read an Atom feed in your browser, where you can see a list of events, and you can also create and update events using the Atom service.

Create, read, update, and delete operations can also be performed from the command line using the REST Web Service command-line utility.

For more details and examples, see the **Extensibility Guide > Automating Operator Functions and Event Change Detection**.

OM provides its own Incident Web Services as well as CLIs and APIs to manage events externally. OM Incident Web Services comply with the DMTF WS Management standard, enabling these operations on one or multiple events:

- Get, create, and update events
- Close, reopen, own, disown events
- Get, add, update and delete Annotations
- Add, update and delete Custom Message Attributes
- Start or stop automatic or operator-initiated actions
- Get instruction text for an event
- Get notification for changes on events (including filtering support)

All CLI functionality described below, except for deleting events and downloading and uploading events, can be achieved with OM Incident Web Services and with the OMi REST-based Event Web Service.

OM and OMi CLI Functionality Comparison

The following table compares auditing functionality in OM and OMi.

Functionality	OM for UNIX	OM for Windows	OMi
Close events	opcmack (agent) opcack opcackmsg opcackmsgs	opcmack (agent) ovowmsgutil* Create a VB script using WMI methods	through Incident web service / RestWsUtil CLI or opr-close-events[.bat|.sh] – close all events or close events selectively based on by date received range, severity, related CI, node CI. This is designed to be run 'offline' since it does not update running UIs
Reopen closed events	opcunack	ovowmsgutil* Create a VB script using WMI methods	Through Incident web service / RestWsUtil CLI

Set, unset, and change ownership	opcownmsg	ovowmsgutil* Create a VB script using WMI methods	Through Incident web service / RestWsUtil CLI
Add, modify, remove, and list custom attributes	opccmachg	Create a VB script using WMI methods	Through Incident web service / RestWsUtil CLI
Add and list annotations	opcannoadd opcannoget	Create a VB script using WMI methods	Through Incident web service / RestWsUtil CLI
Change severity and text	opcmsgchg	ovowmsgutil* can change severity (not message text) Create a VB script using WMI methods	Through Incident web service / RestWsUtil CLI
Read events	opcgetmsgdet opcmsgsrpt	Create a VB script using WMI methods	Through Incident web service / RestWsUtil CLI
Delete events	opcdelmsg	No	No
Delete queued events	opcdelmsgs	No	No

Download or upload events	opcactdwn, opcactupl opchistdwn, opchistupl	ovowmsgutil*	opr-archive-events[.bat|.sh] – Download closed events, based on date range, severity, and node from the DB. Uploading archived events is not supported.
			opr-export-events[.bat|.sh] and opr-import-events [.bat|.sh] support exporting and importing all or selected events in any lifecycle state

* ovowmsgutil runs bulk operations on messages. It makes changes directly to the database, stopping some OM for Windows services while it executes.

Running External Programs (such as Perl scripts) from Groovy

There is currently no tool to export and import OM Composer elements into OMi. However, it is possible to reuse Perl scripts, which were used in OM Composer to enrich events, inside OMi EPI scripts. This is possible because Groovy allows running external programs, and can run a Perl interpreter and Perl script. With Groovy you can also use the execution function to start an external program.

For example, you could launch your OM-based Perl script using the following code:

```
def start_exec( List<String> cmd)
{

    def sout = new StringBuffer(), serr = new StringBuffer()
    def proc = cmd.execute()

    sleep(50);
    proc.consumeProcessOutput(sout, serr)
    proc.waitForOrKill(2000000)

    if (serr.length()>0){
        println "error $serr";
    }

    return sout
}
```

You can use the above function with below code:

```
ret=start_exec( ["perl.exe", "your_perl_code.pl", "parmeter2"]);
```

The package jerlWrapper.perlVM is available from https://code.google.com/p/jerl/, which might perform faster when loaded into the EPI script init area.

Downtime Handling

OMi downtime is scheduled to occur once or on a recurring basis. It is based on selected CIs and their relationships in the RTSM, dynamically listening to topology changes. For example, if a node CI is put into downtime, all impacted CIs are put into downtime as well: if at the time there are two Oracle instances on the node, they are put into downtime.

Each downtime is associated with a selected downtime category which defines how events are processed for the CIs in downtime. For example, you could have a downtime category that sets the event to closed, execute EPI scripts and automatic run books.

Other actions during downtime can be to suppress notifications, set KPIs to downtime status and disable SiteScope monitors. For further details, see the **Administration Guide > Service Health > Downtime Management**.

> **Note:** While a downtime is active, you cannot modify it. You can delete it from the JMX console. For details, go to https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM1155257).

OM and OMi Downtime Functionality Comparison

The following table compares downtime functionality in OM and OMi.

Functionality	OM for UNIX	OM for Windows	OMi
Define scheduled outage	Yes.	Yes.	Yes.
Define unplanned or ad hoc outage	Yes.	Yes.	No.
Put node or node group in outage	Yes.	Yes.	Yes. For CiCollection (node group equivalent)
Other outage criteria	Services and other message attributes (severity, application, object, type, text, CMA).	Services and service hierarchies.	Additional default CI Types include running software, business application, Infrastructure service, business service. Can add or change CI Types to include. Impacted CIs are also put into downtime.
Event state set during outage	Log only or delete.	Log only or delete.	Closed (log only), resolved or no change.

Event attribute to indicate received during outage	No.	Yes, custom message attribute.	Yes, 'Received in downtime' flag.
Disable heartbeat polling	No.	Yes.	Not applicable.
Automation	Yes, through outage file editing and opccfgout CLI.	Yes, through ovownodeutil and ovowserviceutil CLI.	Yes, via Downtime REST API.
User permission	Create tool(s) that execute opccfgout to set unplanned outage. Create tool(s) that assign node to node group in "maintenance". Grant user access to the tool(s).	Permission to set unplanned outage on nodes/services in user's responsibilities. Permission to specific policies (for example, for scheduled outage).	Permission to view or to have full control of scheduled downtimes to set downtime for CIs in views to which the user has access.

Chapter 4: Establishing Effective Operator Workflow

Overview

OMi allows building one or more customized operator My Workspace pages for each operator group, or even individual operator, with its My Workspace framework and UI components such as the event browser, view explorer, event dashboards, watch list, health views, action panel, or business impact view.

Within a My Workspace page operators can use different views to monitor the health of the CIs they are responsible for, or the events that occurred in their IT environment.

Operators can review the instruction text for an event and run tools, run books, event-related actions, and performance graphs in the context of a specific event or Configuration Item from the context menu or action panel.
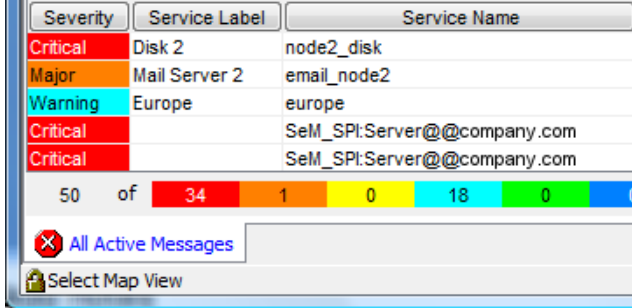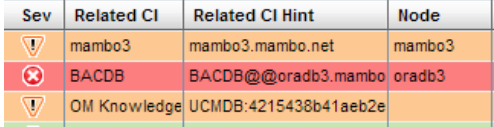
The following figure shows an example of a customized My Workspace page:
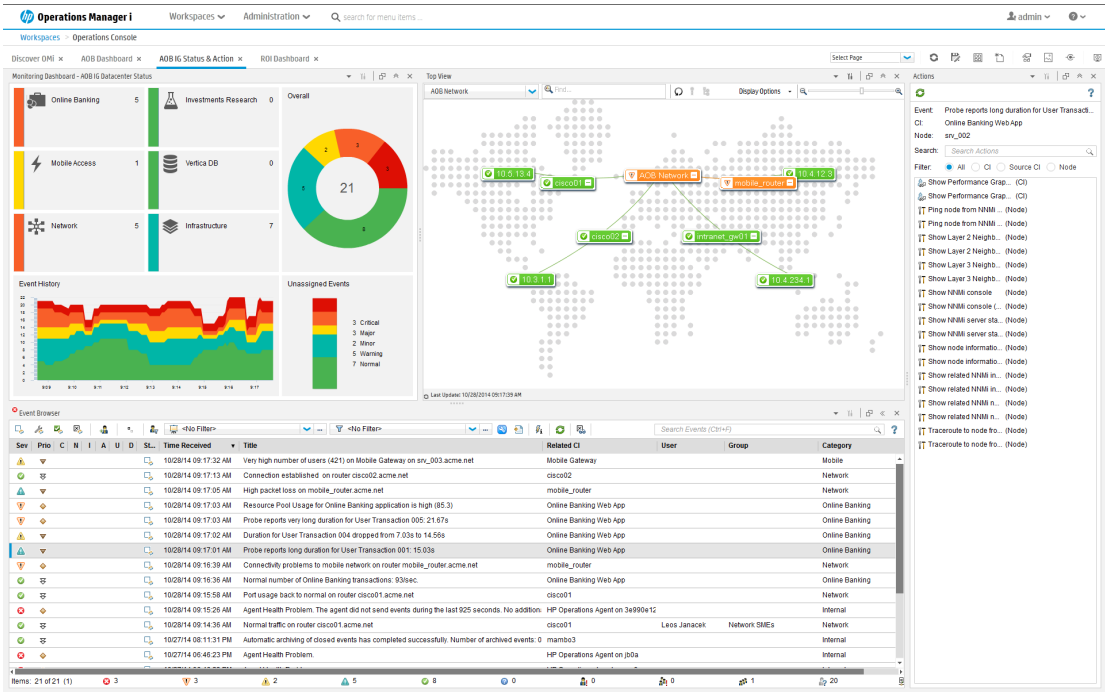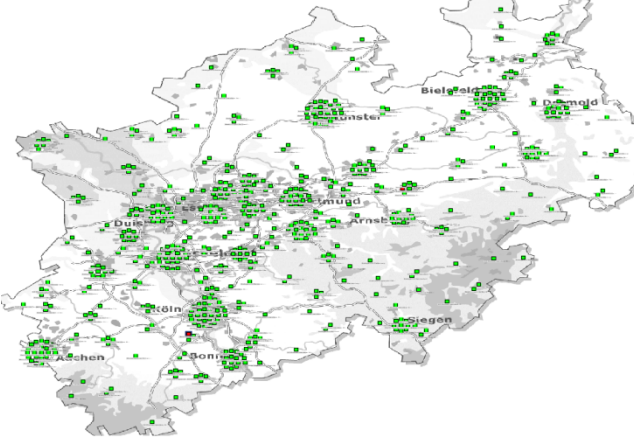
The following table shows the comparison between OM and OMi operator features:

OM operator functionality	Equivalent in OMi
Review instructions.	Yes.
Launch tools on messages, nodes, services.	Yes, launch tools on events and CIs.

(Re-)Launch event actions.	Yes.
Launch graphs on messages, nodes, services.	Yes, launch graphs on events and CIs.
Launch reports on messages, nodes, services (OM for Windows).	OBR reports, can be integrated in My Workspace which allows launch in context of a CI.
Event lifecycle (own, disown, acknowledge, assign (OM for Windows)).	Enhanced event workflow (assign to/work on/ /resolve/close).
Modify Event attributes: text, severity, CMAs, annotations.	Yes: title, severity, CAs, annotations, as well as description and solution.
Hyperlinks (http/s, ftp) embedded in text (OM for UNIX and OM for Windows), application, object, CMAs, annotations (OM for UNIX).	Yes, title, CAs, annotations, original text, description, solution.
Set unplanned outage (OM for Windows).	Currently only possible by defining a scheduled CI Downtime which starts immediately.
Broadcast to all or selected operators (OM for UNIX).	Not supported.
$OPC_NODES replacement in tools (allows to launch a tool which gets selected nodes as input parameter). Start tool on many nodes (multi select nodes).	Currently not possible in OMi.
Instruction text interface to retrieve instructions from external system.	OMi offers an external instruction text interface, which allows you to retrieve instructions from external databases, web pages or other sources. See the Administration Guide > Operations Console > External Instructions for more details.
First time received event column (OM for Windows), time received and time last received event column (OM for UNIX).	OMi has Time First Received and Time Received columns (duplicate overrides time received).
Browser Filters.	Supported (also public and private filters).
History filters.	Yes. OMi allows to use event and date filters for the Closed Events Browser.
Message colors.	Supported (browser options).
Reorder columns.	Supported (browser options).

Column choices.	Supports most columns available in OM. Does not have first time received attribute, unmatched, time unbuffered. Has these attributes, but cannot select as columns: message key, origin, policy, policy type CAs can be selected in columns, but it requires the admin to predefine the list of CAs the operator can choose. Many new columns available, for example, event age, correlation, priority, received in downtime, …
Play sound.	Supported (browser options, default sound).
Run local application or trigger popup based on event severity (OM for UNIX).	Not supported.
System tray icon / popup (OM for Windows).	Not supported.
Custom UI layout.	Conceptual (My Workspace).
Service maps/views.	Yes, several widgets. For example, Top View, Health Top View, Watch List.
Service Label and Service ID in message browser. 	Related CI, Related CI hint (equivalent to service ID) and Node in event browser.
Contextual link to OM policy from message	Yes.
Restrict operator permissions: globally set limited for messages owned by others, per user/profile can allow perform actions, modify message, own, (un-)ack (OM for Windows) or view, (dis-)own, (un-)ack, perform actions, modify message on a per message group basis (OM for Windows).	More granular control.
OM for UNIX Java feature.	
Font size (Edit -> Preferences -> General).	Not supported.

Browser advanced filters – event filters and very flexible message view filters.	Supported (same on concept base). OMi has an extensive list of attributes and patterns that can be combined together with AND, OR, and NOT operators. **Note:** OMi does not have an equivalent node event attribute (the closest is related CI hint).
Dynamic Label in event browser.	Not supported.
Custom or Sub Service Maps can be created with moving icons or externally calculated icon positions.	Use "Geographic Map" using "Location" Ci in RTSM. Otherwise use "Custom Maps" to position CIs using drag and drop.
Property files customization.	Not supported.
secure https mode.	Supported (see OMi hardening information).
Broadcast tool.	Not supported (tool has to be created in OMi).
Custom message icons.	Not supported.
List connected UIs.	Not supported.
Dashboard – event history, pie chart, bar chart, cockpit view.	Event Dashboard, but the dashboard choices are be pre-created by the administrator in the Dashboard Designer, rather than the operator creating their own.
Detach window.	Yes, URL for access to Event Browser only.

Pending browser supporting service hours.	Not supported.
Operational Service View showing unowned service status.	In OMi you can use multiple KPIs to propagate more than one state. Unassigned Events KPI is equivalent to Unowned status.
GUI failover to backup OM server.	Load balancer in front of Gateway servers of a single OMi instance.
Disable user logins.	Limited: Infrastructure Setting (Foundation=Security) can prevent login if BSM_ODB or DASHBOARD service is down.
opcuistartupmsg	Not supported.
Integration: Java GUI can be launched context sensitive from other applications opening a specific service view including related message browser filter.	OMi standalone event browser can be launched with context.

Recommended Operator Workflow and My Workspace Page Setup

We recommend that you provide operators or operator groups a customized My Workspace pages that fits their needs. It should contain a dashboard component that shows the event status in each area the operator or group is responsible for. For example, if the group is responsible for three major areas, like Databases, Linux Servers, and WebLogic in EMEA, then they should see the high-level status of each area represented through dashboard widgets, which will also allow them to quickly filter the event browser. Using such dashboard widgets, they will be able to quickly switch between areas and corresponding views. If required, the dashboard could also contain a widget that shows all unassigned events, so that operators are informed about new issues that are not yet assigned to anyone.

For a short overview of how to create an event dashboard and My Workspace page, see the **HP OMi: How to create an Event Dashboard** tutorial at https://hpln.hpe.com/page/omi-tutorials.

The following figure shows a Dashboard example for operators:
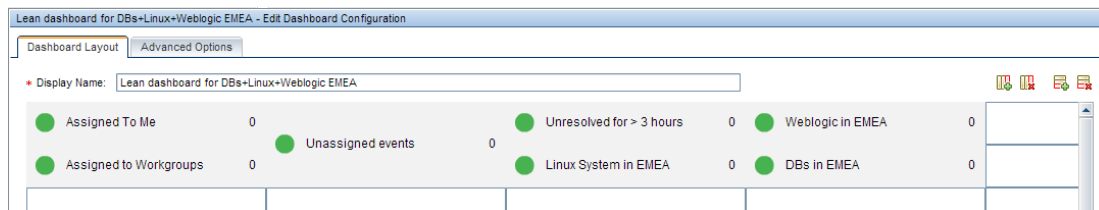
By using the **Show events assigned to Me** button in the event browser, operators can see all events assigned to the user or the user's group independent of the view. Events not related to a view are also shown if an operator is allowed to see them based on the event category.

The following figure shows the Show events assigned to Me option in the Event Browser:
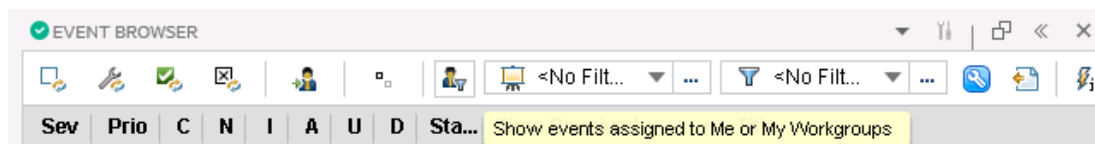
The My Workspace page should also contain other components that are typically needed by the operators to solve problems, like components that show the business impact, KPI Over Time dashboard, health indicators, performance metrics or available actions.

The following figure shows an example of a customized My Workspace page with various components:

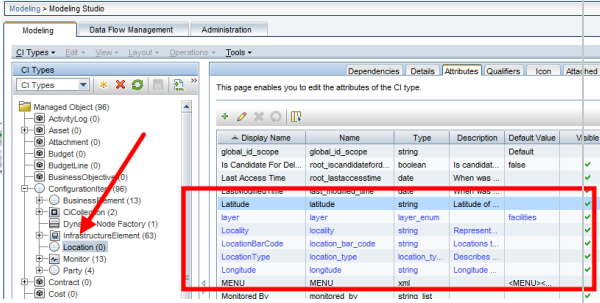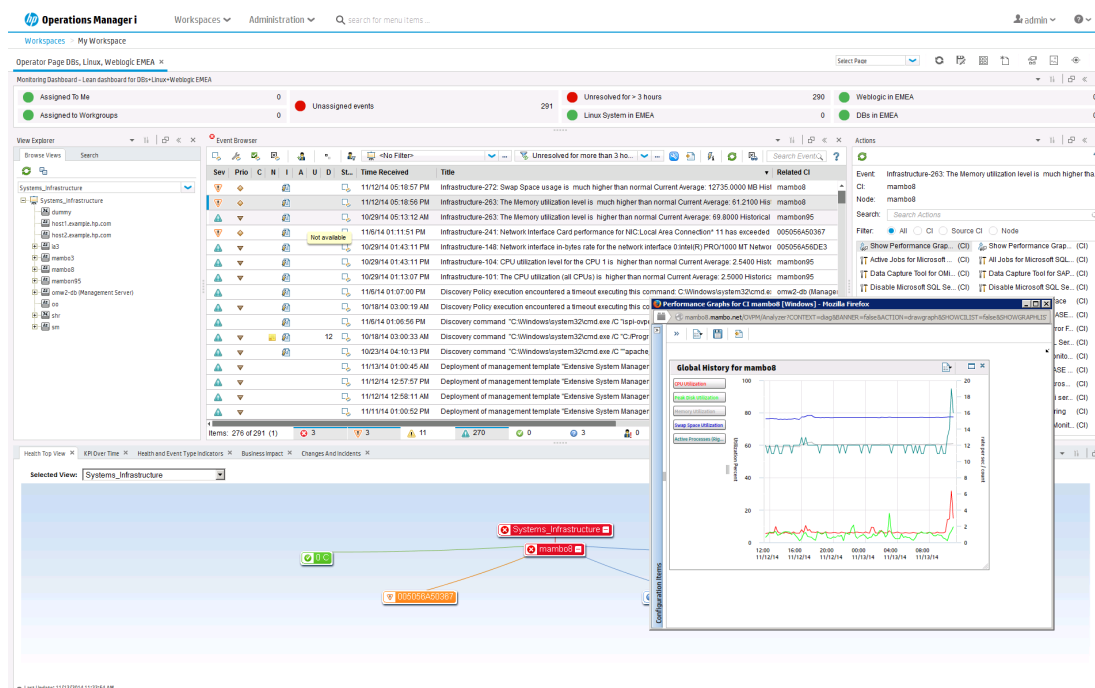# Implement Integrations for Operators

To support Operations operators, several integrations might be necessary. This chapter provides details about the integrations that support the operator workflow.

Operations Orchestration Integration

Operations Orchestration run books can be defined for certain CI Types and can be launched in the context of a CI or event. See [365] Event to remediation (OMi - OO) 1.1 and [673] CI to remediation (BSM-OO) 1.0 for details.

Documentation for this integration can be found in the OMi Integrations Guide.

Knowledge Base Integrations

Knowledge Base systems that provide useful information for operators can be integrated using OMi external instruction text interface. It is able to call a script or executable, query databases, web pages or other external sources to retrieve instruction text for a certain event. For details, see the **Administration Guide > Operations Console > External Instructions**.

It is also possible to integrate web pages directly into My Workspace pages using a dynamic URL. For details, see the **User Guide > My Workspace > How to Set Up My Workspace > How to Create an External Component**.

Cross-Launches into Other Applications

Context-specific cross-launches into other web-based applications are possible through context menus with dynamic URLs or tools.

For more information on context menus with dynamic URLs, see the **Administration Guide > Service Health > Repositories Overview > How to Create a Dynamic URL – Use-Case Scenario**.

Forwarding to Incident Management Systems

Documentation about the generic forwarding interface can be found in the **Extensibility Guide > Integrating External Event Processes. Forwarding rules can be setup by going to Administration > Event Processing > Automation > Event Forwarding**.

Documentation for the specific HPE Service Manager integration can be found in the OMi Integration Guide.

Forwarding to User Notification Systems

Events can be forwarded to external notification systems using the generic forwarding interface. For information, see the **Extensibility Guide > Integrating External Event Processes**.

Users can also be notified using the OMi own notification interface, which can send e-mail, sms, or pager notifications. Go to **Administration > Event Processing > Automation > Notifications** and see the corresponding OMi Help topics for details.

Re-Create Custom Tools

Tools

In OM, administrators can define tools that open a specific URL, or run certain executables or scripts on nodes with Operations Agents. The same is possible in OMi.

Operators in OM can start tools in the context of one or more nodes or node groups, and can then run those tools on multiple systems. OMi can currently run tools on single CIs only, but allows launching tools on nodes

as well as on various types of CIs. This also enables context-specific tools, where only the tools that apply to a specific CI are shown to operators.

In OM, some tools are provided out-of-the-box and some are supplied with OM SPIs.
Tools are supplied with OMi content packs and management packs. If a content pack exists in OMi, it usually provides comparable tools to the corresponding OM SPI.

If a content pack does not yet exist, or if a custom tool was developed on OM, then a corresponding tool can be re-created manually in OMi in **Administration > Operations Console > Tools**.

> **Note:** There is currently no method to automatically exchange tools between OM and OMi.

There are some differences in the variables that can be used when defining tools – the most important difference is that OMi does not support $OPC_NODES, which allows launching tools on several nodes or with several nodes as the input parameter. For a complete list of variable differences, see the following sections.

Tools in OMi

Using a Configuration Item-centric approach, tools in OMi are linked to Configuration Items. Tools are assigned a category and operators are given execute permissions by administrators to tool categories that are appropriate to their roles.

A Tool contains a command, script or URL, and can contain the following parameters:

- CI attributes
- Event attributes
- Infrastructure settings
- Runtime parameters
- Monitoring host name
- Management server name
- Hosted on host name (where the CI is hosted)

Tools are created to help users perform common tasks on CIs and are associated with a CI type, which can be run from the centralized console. For example, you can run a tool to check the status of an Oracle database instance. The tool is assigned to the Configuration Item type Oracle.

For more details, go to **Administration > Operations Console > Tools** and see the corresponding OMi Help information.

OM and OMi Feature Comparison

OM Tool Features	OMi Equivalent
Command types	
Executable	Yes
VBscript (OM for Windows)	Yes

Jscript (OM for Windows)	Yes
Windows scripting host (OM for Windows)	Yes
Perl (OM for Windows)	Yes
URL	Yes
Allow operator to change parameters flag.	Use ${option} to prompt operator for missing parameters. Cannot change parameters but can add missing parameters.
Allow operator to change logon flag.	Not available, but tool can prompt operator for logon credentials (operator is prompted every time the tool is started).
Possible parameter variables	
Message properties	Event properties.
Node properties	CI properties/Monitoring Host/Hosted on host.
Service properties	CI properties.
Environment variables Used to retrieve environment variables from the console that launched the action	Not available (typical tools do not need access to environment variables on console systems).
Server configuration variables	Infrastructure Settings.

Node group properties / $OPC_ NODEGROUP_ ID $OPC_ NODEGROUP	Not available (OMi is CI/view centric).
$OPC_MSG_ IDS	Not available/launch from single event only, event ID of selected event is accessible.
$OPC_MSG_ NODES $OPC_ NODEID	Not available/launch from single node only, monitoring host of selected event/CI is available.
$OPC_MGMTSV	Available in the UI. Execution is done on the Gateway Server.
$OPC_USER (OMU)	Executing OMi user variable.
Execute on possibilities	
Management server	Yes. Requires that an operations agent is installed on all gateway servers. (currently uses node of infrastructure setting Default Virtual Gateway Server for Application Users URL as target for agents connected to an OMi server). **Note:** A managed_by relationship to an OM server takes precedence. To make sure that tools are executed on the OMi server, remove any relationships to OM servers or remove the OM server CI.
Selected node	Selected CI / related CI of selected event.
Node list	Not possible, tool can be launched on single CI/node only.
Node list (predefined)	Not possible, tool can be launched on single CI/node only.
Console	OMi does not allow executables or scripts to start on a console system. This is because the OMi console is web-based and runs inside a browser that does not allow the launching of executables—for security reasons. However, running an executable on the client system is not the primary use case of OM tools and a user on the client system can run the executable manually. Such a useful tool including parameters could also be mentioned in the instructions for the event.
URL in local web browser	Yes.

Broadcast Execute a command specified by the operator on all nodes (OM for UNIX)	Not available.
Presentation output options: OM for UNIX: Window (output only), No Window, Window (input/output) OM for Windows: Windows, No Window	Tool execution always displays a Window.
Tool can launch X-applications (OM for UNIX)	Not available.

How to Re-Create Custom OM Tools in OMi

To create a tool in OMi, go to **Administration > Operations Console > Tools**.

Navigate through the CI Types tree, for example to **InfrastructureElement > Node > Computer > Windows**.

Click **Windows** and the **New Item** icon in the Windows – Tools pane. The Create New Tool window appears.

Copy the tool command and other settings from the OM tool definition to the OMi tool definition.

To test the tool, open the Event Perspective or another My Workspace page that shows CIs, and select a suitable CI (of the CI Type for which you defined the tool), and select **Launch Tool** from the CI context menu.

Note: If the Tool contains event attributes it can be triggered from an event only.

Import Performance Dashboards

Performance Dashboards

OMi includes an embedded Performance Dashboard component that does not require an additional license. The OMi Performance Dashboard enables you to create customized performance dashboards for the CI types you are monitoring. You can also compare multiple instances of a resource or an application of a Configuration Item (CI).

For details on how to launch a performance dashboard, see the **User Guide > Operations Console > Performance Perspective > Managing Performance Dashboard > Launching a Performance Dashboard**.

Predefined Performance Dashboards

OMi content packs and OMi Management Packs add many predefined performance dashboards that are comparable to the graph templates provided by Performance Manager.

How to Design a Performance Dashboard

Designing a performance dashboard includes the tasks of creating a performance dashboard, configuring a performance dashboard, visualizing events in the performance dashboard, and managing different multiple instances across systems using instance parameterization.

For details, see the **User Guide > Operations Console > Performance Perspective > Designing Performance Dashboard**.

Import Custom Performance Manager Graphs

Performance Manager Graphs

OM for UNIX and OM for Windows do not offer an integrated dashboard component like the OMi Performance Dashboard but integrate with Performance Manager and are able to cross-launch into Performance Manager.

OM, PM, and OMi Performance Dashboard Feature Comparison

OM policies can include operator-initiated actions that refer to a specific performance dashboard. The performance dashboard-related operator-initiated actions are filtered out by OMi and are not shown to operators.

The following tables compare OM and OMi functionalities, as well as Performance Manager and OMi Performance Dashboard functionalities.

OM functionality	OMi functionality
Performance Manager integration	OMi Performance Dashboard embedded
Separately manage user permissions	Single configuration and authorization model
Separately manage nodes and node groups (integration with Reporter or OM for Windows)	

Performance Manager functionality	OMi Performance Dashboard functionality
Design custom graphs	Design custom performance dashboards
User-defined and global graph templates	Out-of-the-box performance dashboards
Export and import graph templates	Yes (by using content packs and management packs)
Export graphs: TSV, CSV, Excel, XML, PDF	CSV only
URL based launch capability in PM for embedding in their own portal	Yes
RESTful web services for retrieving data	Yes
Command line utility to generate graphs	No
Reporter reports integration	*Recommendation*: use OBR. OBR reports can be viewed in My Workspace, but no contextual cross-launch.
Data sources: Operations Agent, SiteScope, Reporter	Data sources: Operations Agent, vPV, SiteScope, BSM Connector, APM
RTM data source support	Real time graphing support added for Operations Agent and SiteScope
Proxied Log Files	No
Flat file data source	Use BSM Connector to process metrics from file into OMi
Add node temporarily on-the-fly	No
Active Directory authentication	Any authentication supported by OMi
Add to Favorites (loaded when PM home page is launched)	Yes
Create graph templates containing multiple metrics on multiple nodes	CI centric approach means each performance dashboard corresponds to metrics from a single CI
Diagnostic View: Load and Save State	Yes (Favorites in OMi)
Diagnostic View: Drill down to Process, tables of each metric class	No

System Information page	No

How to Import Custom Performance Manager Graphs into OMi

If you have created custom graphs in HPE Performance Manager, you can import those into OMi as performance dashboards and map them to CI types using the following procedure:

1. Copy all graph templates you want to import from the HPE Performance Manager system:

    ○ PM on Windows: copy from `%OvShareDir%/server/conf/perf` directory

    ○ PM on Linux: copy from `/var/opt/OV/shared/server/conf/perf`) to `<OMi_HOME>`/opr/newconfig/OVPM on an OMi GW server.

    Create the OVPM directory if it does not exist.

2. Follow these steps:

    a. Log on to OMi.

    b. On a separate browser tab, open `<OMiGWServer>`/OVPM/Options.jsp.

    c. Click **Import Dashboard**.

    This uploads all graph templates from the above file location to the OMi database. This is a one-time import. If you modify graph templates in HPE Performance Manager afterward, use the same procedure again to upload the modified graph templates.

3. Associate these graph templates (performance dashboards in OMi) to the respective CI Types. Go to **Administration > Operations Console > Performance Dashboard Mappings**, and select the CI Type to which you want to link the graph.

Note:

- If the graph template contains specific node names, the graph can be imported into OMi, but the specific node names are ignored when the graph is launched. The graph will be launched in the context of the selected CI.

- If a graph template with a SiteScope data source is imported from PM into OMi, the graph will retrieve metrics directly from a corresponding SiteScope server. This assumes that the monitor in SiteScope is configured to report metrics to the HPE Operations agent.

- PM graph templates that refer to a Reporter data source will not work in OMi.

Prepare Operator Console

User Management in OMi: Users and User Groups

User roles, user groups, and user profiles help simplify authorization in OM.

Similar functionality is available in OMi using user roles and user groups. You can define roles and permissions and create users and groups to provide access to the features for specialist operators, for

example, email application experts. In order to reduce the effort and complexity involved in configuring roles for individual users in OMi, permissions are granted only through roles. You can specify roles either by assigning them to a group (so that all members of the group have access to the same roles) or by assigning them to a user directly.

> **Note:** OMi does not distinguish between administrators and operators – there are just users.

There is also no strict separation between administrative permissions and non-administrative permissions. You can grant any permission to any user. To simplify the granting of all permissions, an OMi user can be flagged as Super-Admin.

The following figure shows user groups in OMi:
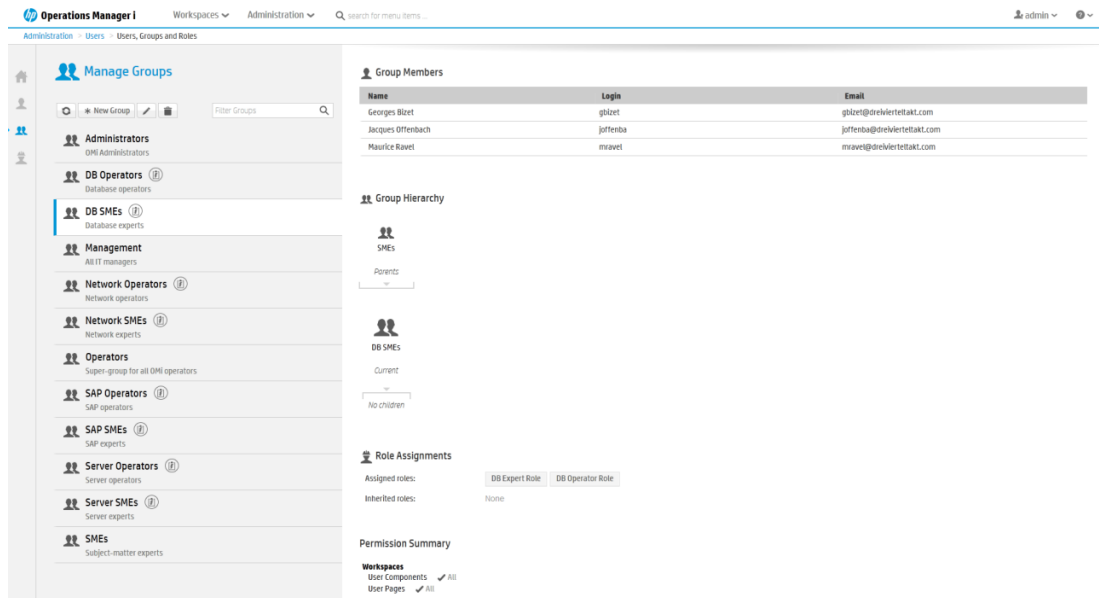
The following figures show user profiles in OM for UNIX and user roles in OM for Windows:
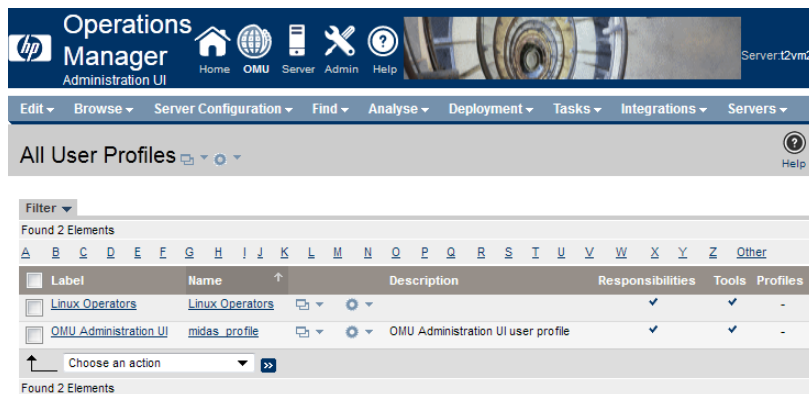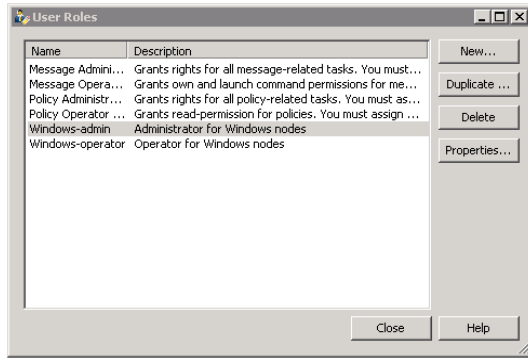
User Roles

OMi enables you to fine-tune permissions management by applying permissions within roles. Permissions enable you to restrict the scope of a role.
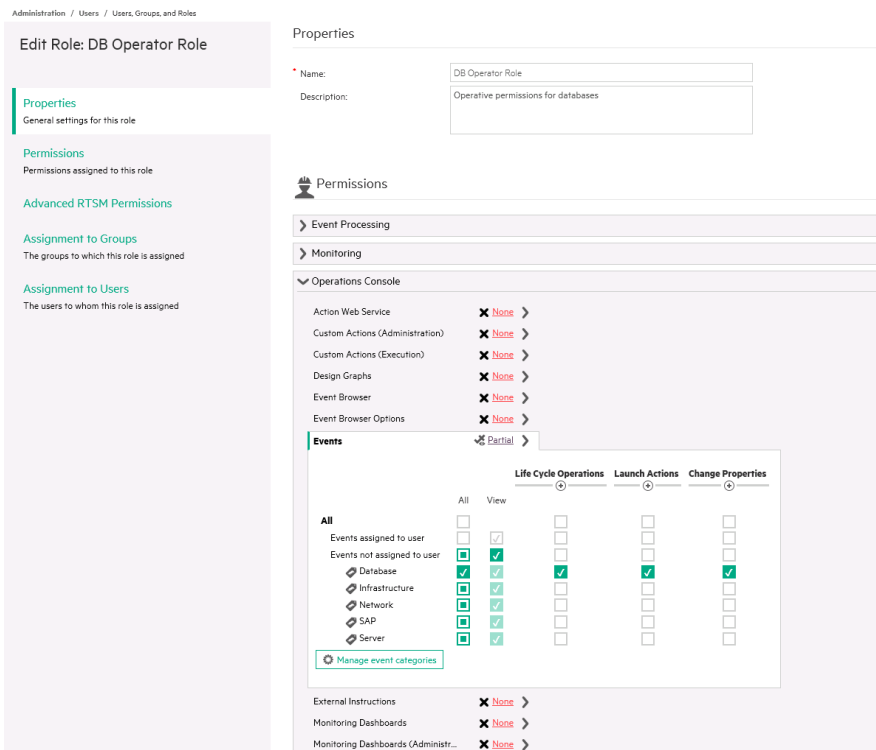
For more details, see the **Administration Guide > Users > Users, Groups, and Roles**.

Responsibilities for Nodes and CIs

OMi focuses on CI and CI type-centric or view-based monitoring, instead of node and node group-centric monitoring. Therefore, node groups are not used for authorization in OMi. Corresponding user responsibilities can be defined in OMi using views, which is a more flexible concept.

A view typically contains a subset of the CIs that exist in the RTSM and can contain all types of CIs, including node groups, which in OMi are represented by CI collections. Therefore, it is theoretically possible to continue with node-group based management by creating views that contain only certain node groups or CI

collections. However, with OMi it is recommended to use all possibilities that views provide, and to define the areas that operators are responsible for by using views that contain all the CIs of interest.

The following figures show views and view permissions in OMi:
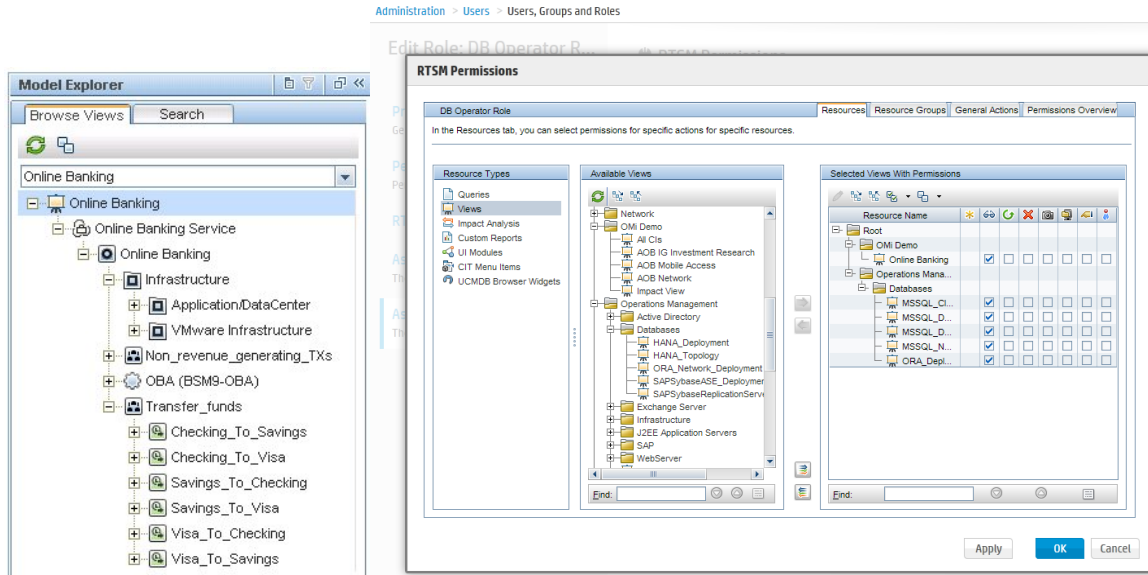
In OMi, user responsibilities can be restricted by granting view rights to certain views only.

Responsibilities for Events

In addition to the node group-based restrictions, OM uses message groups to restrict access to events. In OMi, message groups are called event categories and can also be used to restrict access.

OMi additionally allows different permissions to be defined, based on whether an event is assigned to a user or not. Typically, operators are granted permissions to work on and close all assigned events, but with limited permissions on events not assigned to them.

In OMi events can be automatically assigned to user groups by auto-assignment rules and can also be assigned automatically to individual operators by time-based event automation rules or EPI Groovy scripts.

However, the OM message group (OMi event category)-based authorization is still available and should be used for unassigned events.

The following figure shows event categories in OMi:
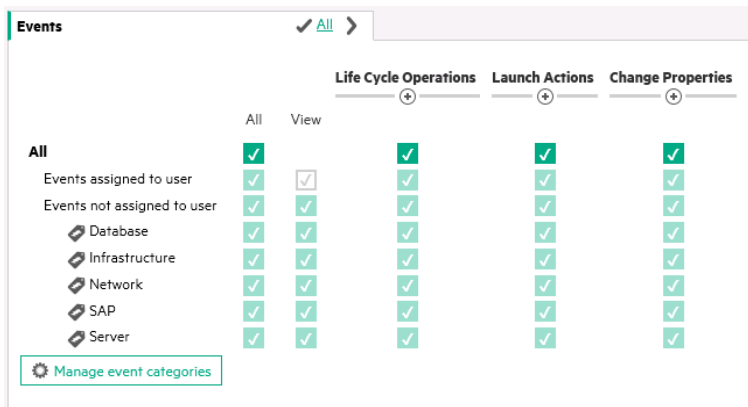
OM for UNIX and OM for Windows can restrict which messages an operator will be able to see by restricting which nodes groups and message groups an operator has access to.

The following figures show event responsibilities in OM:

Event Permissions

In OM for Windows, granular permissions can be set regarding message modifications per message group.

For OM for UNIX, some global permissions per operator can be set.

In OMi, you can set the same detailed permissions as in OM for Windows and additional permissions, for example regarding the assignment or transfer control features of OMi.

The following figure shows fine-grained event permissions in OMi:

The following figure shows message permissions in OM for Windows:
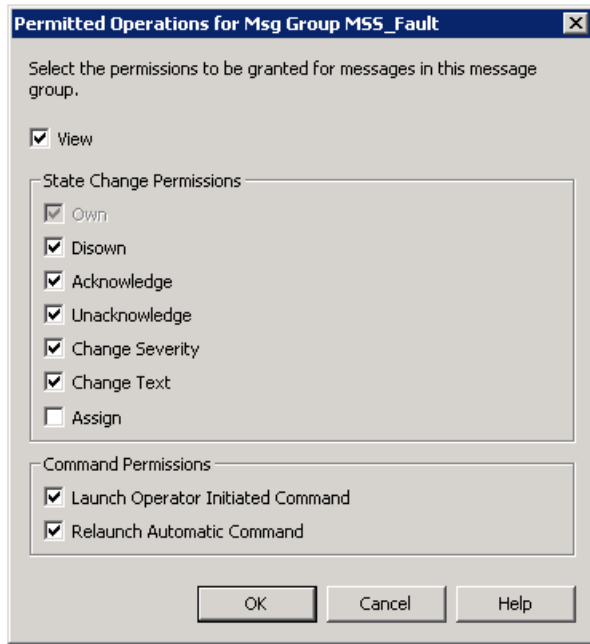
The following figure shows operator message permissions in OM for UNIX:
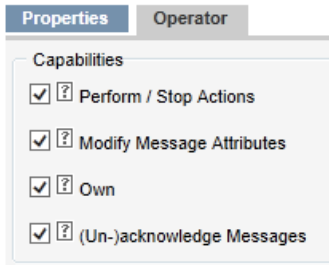
Restrict Access to Tools

OM can restrict access to tools based on tool groups, and OM for UNIX can restrict access on an individual tool level.

In OMi, tools are defined for a certain CI type, and access to tools can be restricted using tool categories.

The following figure shows the configuration of Execute Permissions for tool categories in OMi:

The following figures show the tool permissions in OM for Windows and OM for UNIX:
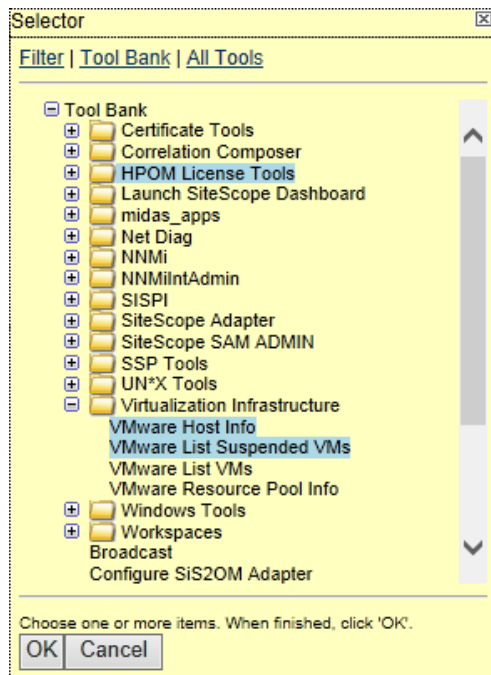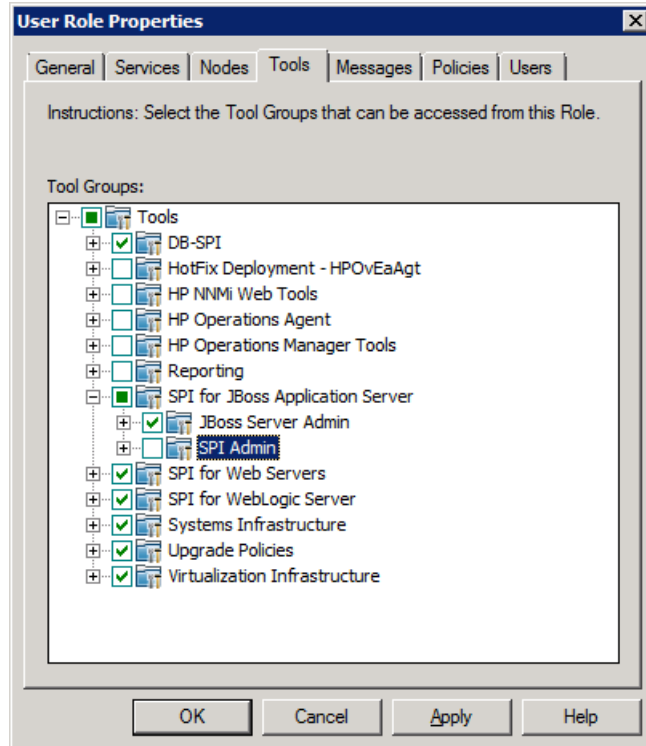
Administrative Permissions

Access to administrative tasks such as creating new tools, setting up new nodes, or deploying policies can be given in OMi by granting Full Control permission to the corresponding Administration UI.

Permissions for viewing, editing and assigning policy templates, aspects or management templates can be granted per policy template group respectively per configuration folder.

The following figure shows an example of administrative permissions in OMi:
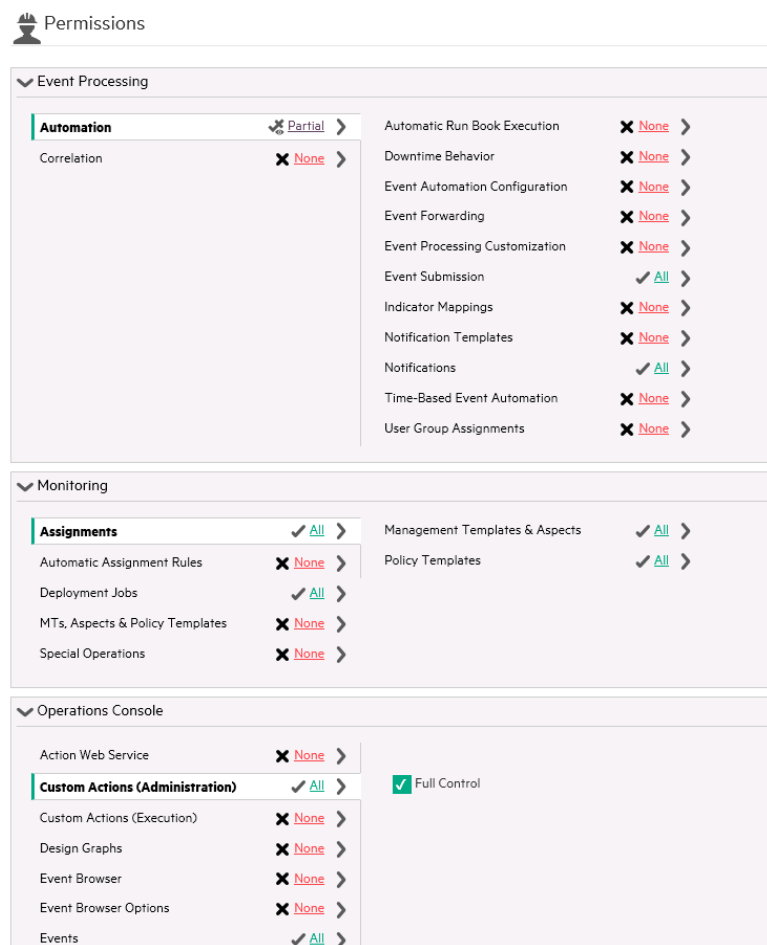
Fine-grained Administrative Permissions per Policy Category or Pattern

The policy management area of OM for Windows allows separation of administrative tasks. In this area, the read, edit, deploy, and delete permissions can be defined for each policy category.

In OM for UNIX, different administrative permissions can be selectively granted for certain object groups using patterns. It is also possible to grant read-only access.
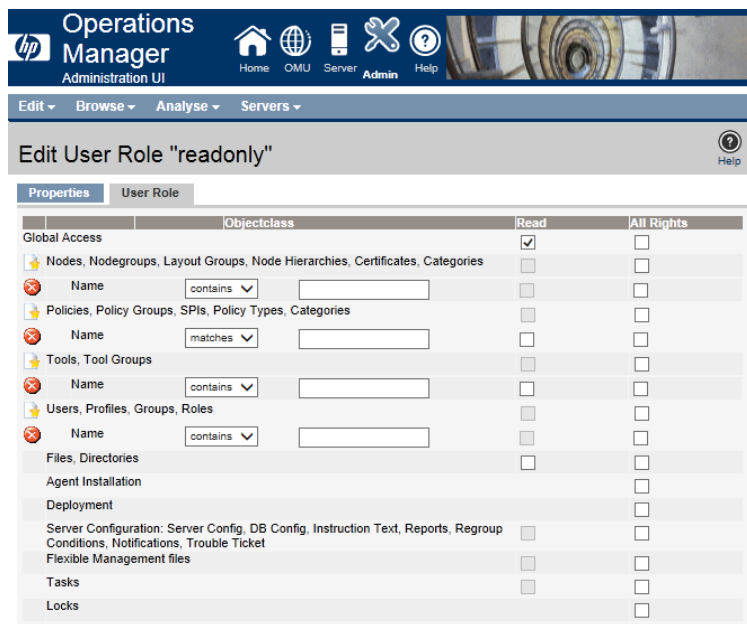
In OMi 10.01 and earlier versions, you can grant access to an Administration UI, and this grants access to all objects that can be edited in that UI (for example, to all policy templates or all tools).

In OMi 10.10 and later, permissions for viewing, editing and assigning policy templates, aspects or management templates can be granted per policy template group respectively per configuration folder.
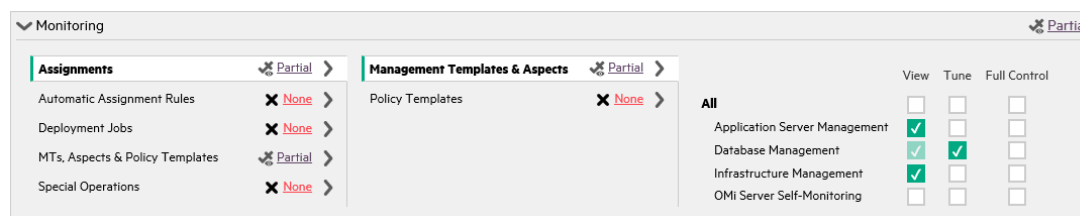
User Authentication

Users and user groups can be managed inside or outside OMi using an LDAP server. Authentication can be performed internally, or by using an LDAP server. The default single sign-on authentication strategy for OMi is LW-SSO. LW-SSO is embedded in OMi and does not require an external machine for authentication. OMi also supports Smart Card Authentication and Identity Management Single Sign-On (IDM-SSO).

As Windows Active Directory implements an LDAP server, users and user groups that have been set up for OM for Windows can be set up in OMi as well.

The Pluggable Authentication Module (PAM) that is offered with OM for UNIX is not available with OMi.

LDAP Authentication

LDAP can be configured with OMi as an authentication mechanism for users logging into OMi and to map groups and synchronize OMi users with users configured on the external LDAP server. For OMi administrators, this simplifies the process of managing users. You can use internal users, LDAP authentication or both.

You enable and disable LDAP using the LDAP Authentication Management Wizard:
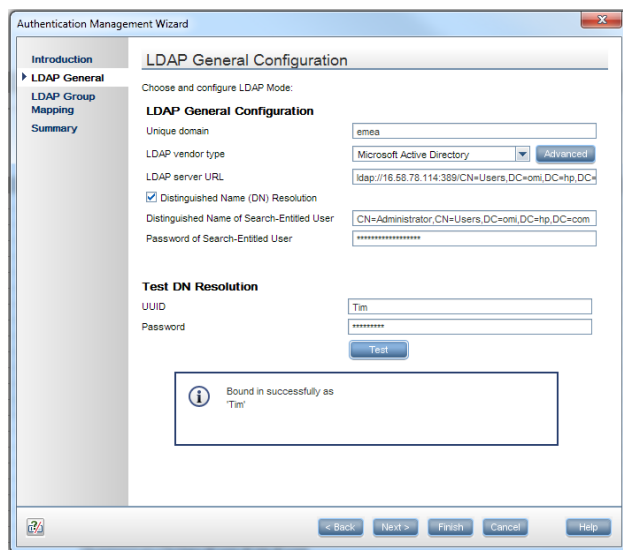
API and Command-Line Interfaces for User Management

OMi currently does not offer any APIs or command-line interfaces to add, modify, export, or import users, user groups, LDAP or SSO settings, however, user roles, including permissions can be exported and imported using content packs.

OM and OMi User Management Feature Comparison

OM functionality	Equivalent in OMi
User groups and user profiles (OM for UNIX). User roles (OM for Windows).	User groups and user roles.

Restrict responsibilities using message groups and node groups.	Same concept, using views and event categories (message groups).
Fine-grained event permissions (OM for Windows).	Yes.
Restrict access to tools based on tool groups.	Same concept: restrict access to tools based on tool categories.
Grant permissions on both operator features and administrative features.	Yes.
Restrict access to policies using policy categories.	Yes.
Fine-grained administrative permissions (OM for Windows)	Yes.
Fine-grained administrative permissions per object category or pattern (OM for UNIX).	Yes, per policy template category / configuration folder.
Read-only administrative permissions (OM for UNIX).	Yes (view permission).
User Authentication via Windows Active Directory (OM for Windows).	Yes, through LDAP authentication.
User Authentication internally (OM for UNIX)	Yes.
Pluggable Authentication Module (PAM) authentication (OM for UNIX).	No, LDAP authentication or integrated authentication only.
API to configure users and permissions. opccfguser (OM for UNIX)	Yes, User Management Web Services and opr-user CLI.
CLI to export and import user roles and permissions. opccfgdwn/upl (OM for UNIX) ovpmutil (OM for Windows)	Content Manager CLI and Content Packs UI to export and import user roles and permissions.

Create Users, User Roles, and User Groups

There is currently no tool to automatically import OM users and permissions to OMi.

Create users and define permissions manually in **Administration > Users > Users, Groups, and Roles**. If you have more than a few operators and want to separate their responsibilities and permissions, then you should create multiple user roles and groups.

Before you start, you should map out the required roles and their relevant permissions, as well as the users and groups you intend to assign the roles to.

Start by creating the necessary user roles and permissions, then create the necessary groups and assign roles to them.

> **Note:** Users can be members of multiple groups, and groups can be nested and inherit permissions from parent groups.

As the last step create the necessary users. If you use LDAP, users can be created automatically at their first login, and OMi user group memberships can be created based on LDAP group memberships. For more details, see the **Administration Guide > Users > Authentication Management > LDAP Authentication and Mapping**.

Create Views for Different Operator Responsibilities

In OMi you can define responsibility boundaries by granting access, or not granting access, to views. Views are also used by operators to filter the RTSM content and events. Therefore, it is necessary to choose or create RTSM views.

For example, for a database operators group that should only have access to event and health information for all databases in EMEA, you should create a custom view that shows only the database systems in EMEA.

For other operator groups choose out-of-the-box views or create other suitable views. You can define more than one view per operator group.

It is recommended to use pattern views as much as possible, as these will be updated automatically when new CIs appear in the RTSM. Instance-based views that are maintained manually are often not ideal in dynamic environments.

> **Note:** Ensure the view contains ALL CIs for which you might expect to see events. For example, if an event is mapped to an Interface CI and the view contains the computer CI but not the underlying interface CI, then that event will not be visible with that view filter.

Create User Group Assignment Rules

Once you have defined the different operator groups and the views they will have access to, it is recommended to define User Group Assignment rules that automatically assign incoming events to one of the operator groups. A manual alternative is to define a special dispatcher role in your organization and to let the dispatcher assign events to operator groups manually.

As a result of an assignment, every operator of the group will get advanced permissions on the event, and will be able to modify and close events.

To define auto-assignment rules, go to **Administration > Event Processing > Automation > User Group Assignments**.

> **Note:** You can reuse the views created in the previous step in the assignment rules. Events that are related to a CI in such a view are then automatically assigned to the specified user group.

The following figure shows Event Automation - User Group Assignments using different view and event filters:

Create Event Dashboards and My Workspace Pages

As described in the planning chapter, you typically want to provide an operator group with a customized My Workspace page. My Workspace pages can provide OMi operators with overview dashboards and contextual information, from business impact information to detailed performance graphs. You can customize pages to provide exactly the information that is needed to resolve issues quickly, as different operator groups might require different information to perform their jobs. Operators focusing on business applications might have other interests compared to operators focusing on OS-level problems, and might therefore also require different event dashboard layouts.

As a first step, create all the required event dashboard layouts.

Create Event Dashboards

Go to **Administration > Operations Console > Monitoring Dashboards**.

Create an event dashboard layout for each combination of operator groups you require. You can use the **Example: Lean Status** as a starting point.

For example, if you have individual operators that are part of three operator groups "DBs EMEA operators", "Linux EMEA operators" and "WebLogic EMEA operators", it is recommended to create an event dashboard layout similar to the following, with one dashboard widget per view. This assumes that you have one view for each group. If one operator group has access to multiple views with different CIs, add multiple corresponding widgets.

The following figure shows a dashboard example for operators:
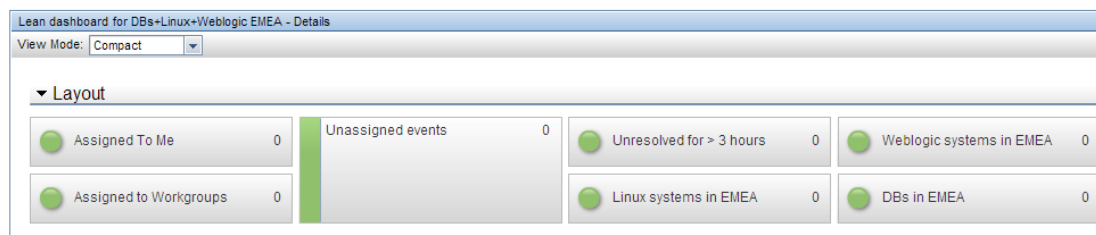
When integrated into a My Workspace page called, for example, "DB, Linux, WebLogic EMEA perspective", this dashboard will allow operators to quickly see the event status in each area and to quickly filter the event browser by clicking a widget. The event dashboard will provide an overview of the event status for all events a user is responsible for, so that they are not forced to switch between views or My Workspace pages.

Create My Workspace Pages

Before creating My Workspace pages, it is recommended to sketch out the page and the components it should consist of. A typical operator page could for example consist of the corresponding lean event dashboard component, a watch list component to keep track of the status of the most important CIs, the event browser in the middle, additional components that provide useful information to operators, like event details, health indicator, business impact, and the action panel to provide fast access to remediation tools. Explore the available My Workspace components and discuss with the operator groups what they need on their My Workspace page for an effective operator workflow.

The following figures show two examples of customized My Workspace pages with various components:
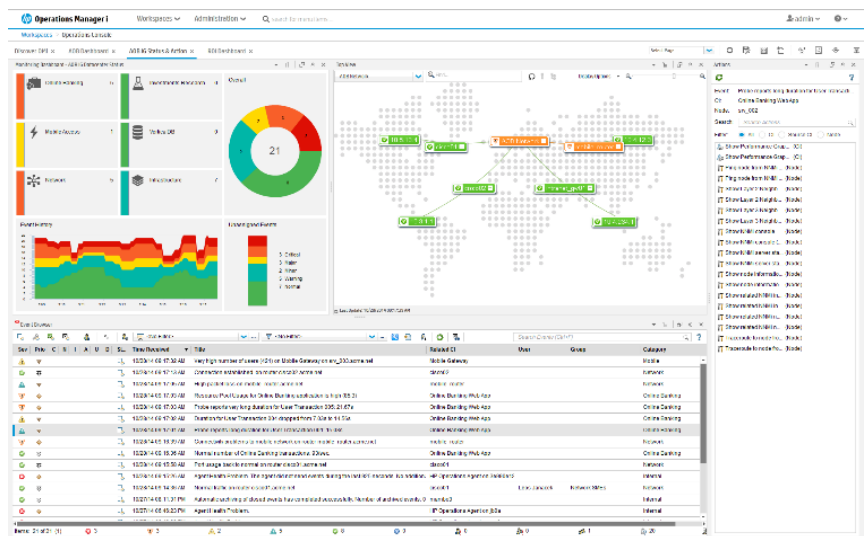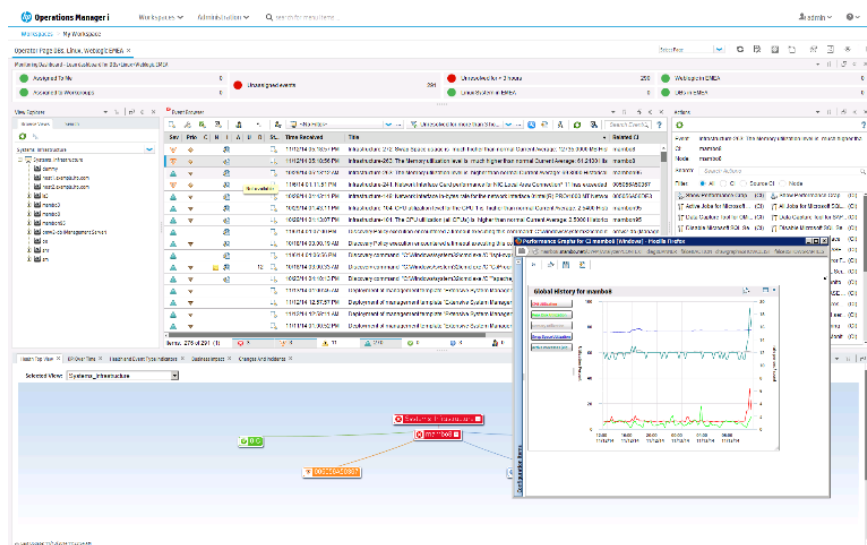
Grant Permissions

As a last step, grant the corresponding permissions on the views, pages, and components you created, and grant general event and administrative permissions. Permissions are assigned through user roles. Go to

Administration > Users > Users, Groups, and Roles and edit the corresponding role.

What (CIs) Views an Operator Should Have Access to

Grant view permissions for the corresponding views in the RTSM permissions section of a user role.
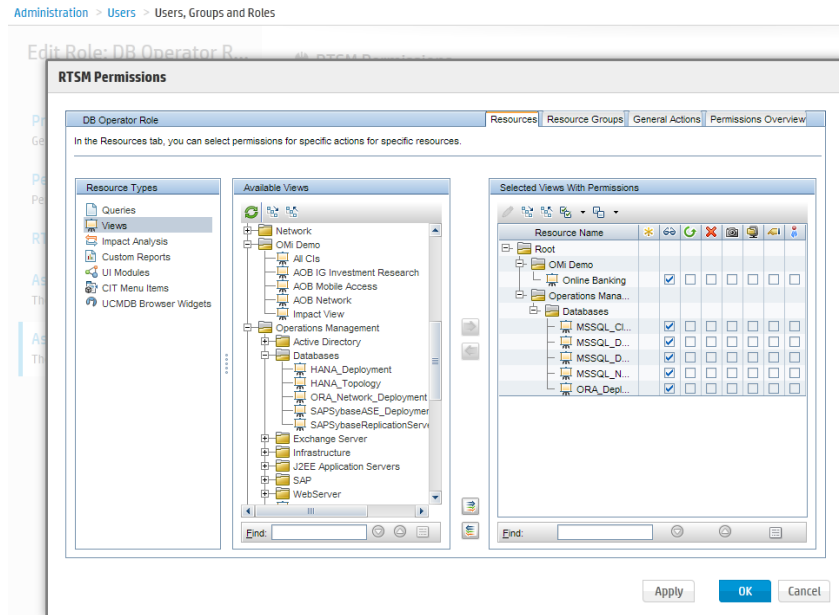
What My Workspace Pages Should Operators Have Access to

Event operators must have access to at least one My Workspace page that includes the event browser component.

The following figure shows how to grant permissions to My Workspace pages:
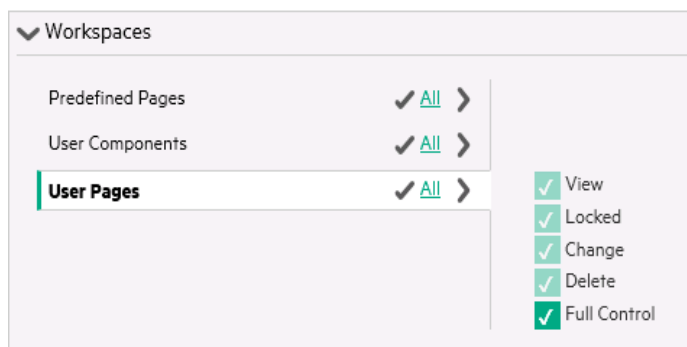
What Events Should be Visible to the Operator, and what Permissions Should an Operator Have

Note: To ensure that operators can see only events for CIs and Views they have access to, make sure that operators do not have the right to clear the view filter.

The following figure shows how to clear view filter permission:
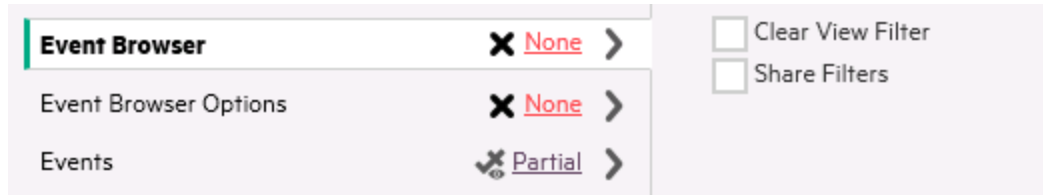
Otherwise, operators would be allowed to clear the view filter in the event browser by selecting <No Filter> from the view drop-down list. This would result in all events being shown independently of the view and would typically show all events.
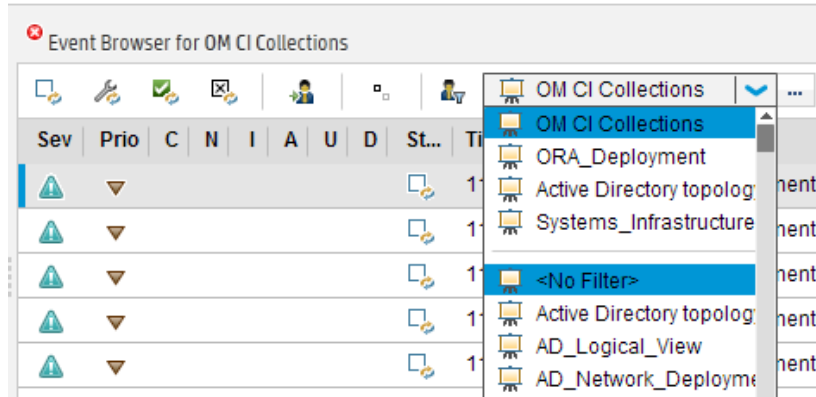
Specify which permissions an operator should have for assigned events and unassigned events per event category.

Typically, operators are set up with permissions to work on and close all assigned events (grant all operations), but with limited permissions on events not assigned to them.

For example, you could grant database operators full permissions for the DBSPI category, View permissions for the Infrastructure category, and no permissions in other categories.
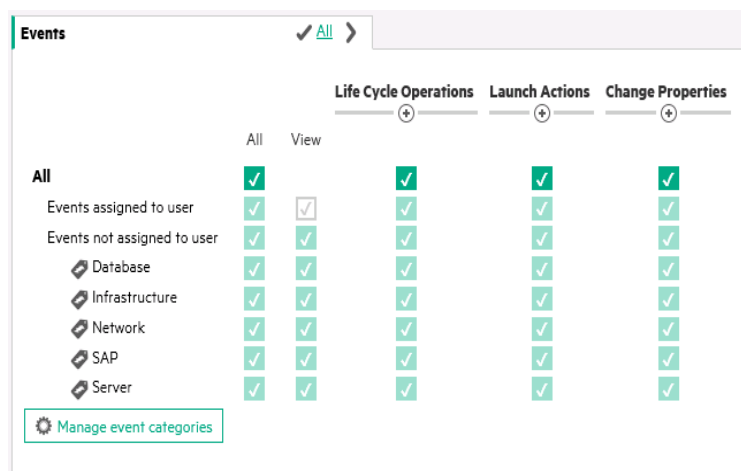
There are three permissions that are new to OM customers:

- **Event Relations.** Allows an operator to create cause-symptom relationships manually, or to break those relationships. Typically granted to all operators.
- **Transfer Control.** Allows an operator to forward an event to an incident management system (via event context menu).

- **Close Transferred.** Allows an operator to close forwarded events. It should not be granted if the event should be under control of the incident management system after forwarding.

Which Tool Categories Should be Made Available to Operators

Specify which tools an operator should have access to. For example, database operators should get access to the database-related categories and default tools.

The following figure shows authorization for different tool categories:

> **Note:** OMi displays all categories used in existing tools. The tool category can be set in the tool definition.

What Administrative Tasks the User Should be Able to Perform

Access to administrative tasks such as creating new tools, setting up new nodes, or deploying policies, can be given in OMi by granting Full Control permission to the corresponding Administration UI.

The following figures show an example of administrative permissions in OMi:

Permissions

> Event Processing

> Monitoring

> Operations Console

> RTSM

> Service Health

> Setup and Maintenance

> Users

> Workspaces

Permissions

Event Processing

Automation	Partial >	Automatic Run Book Execution	✗ None >	
Correlation	✗ None >	Downtime Behavior	✗ None >	
		Event Automation Configuration	✗ None >	
		Event Forwarding	✗ None >	
		Event Processing Customization	✗ None >	
		Event Submission	✓ All >	
		Indicator Mappings	✗ None >	
		Notification Templates	✗ None >	
		Notifications	✓ All >	
		Time-Based Event Automation	✗ None >	
		User Group Assignments	✗ None >	

Monitoring

Assignments	✓ All >	Management Templates & Aspects	✓ All >
Automatic Assignment Rules	✗ None >	Policy Templates	✓ All >
Deployment Jobs	✓ All >		
MTs, Aspects & Policy Templates	✗ None >		
Special Operations	✗ None >		

Operations Console

Action Web Service	✗ None >		
Custom Actions (Administration)	✓ All >	☑ Full Control	
Custom Actions (Execution)	✗ None >		
Design Graphs	✗ None >		
Event Browser	✗ None >		
Event Browser Options	✗ None >		
Events	✓ All >		

Chapter 5: Managing Operations Agents from OMi Step by Step

Overview: How to Move Operations Agents to OMi Step by Step

Note: OM allows installing agents remotely using technologies such as Rexec, SSH/SCP, Windows DCOM, Windows shares.

OMi does not offer remote agent deployment (sometimes called bootstrapping or initial agent deployment) today, but is able to deploy agent patches and hotfixes once the agent is installed. Agents can be installed manually (also remotely using technologies such as SSH/SCP) or using other software deployment tools such as HPE CDA. For more details, see https://hpln.hpe.com/blog/hp-operations-agent-can-be-deployed-cda-and-csa, and HPE Server Automation or Microsoft Systems Center 2012 Configuration Manager (see the HP Operations Agent and HP Operations Smart Plug-ins for Infrastructure Installation Guide).

Another option is to keep an existing OM server for agent deployment.

This is the recommended sequence of steps for managing Operations Agents from OMi. These steps are explained in detail in the following sections.

1. Allow management from both servers using a flexible management template.
2. Choose a group or type of nodes to move over, for example: all my Oracle Database systems.
   a. Test policy and aspect deployment and tool execution from OMi on a representative node of that type. This might include importing OM policies and creating OMi aspects and management templates.
   b. After a successful test, roll out the configuration to the remaining nodes of that type, either manually or by using automatic assignment rules.
   c. Switch the primary manager and target server to OMi. Doing so still allows configuration from both OMi and OM servers.
3. Repeat steps 2-5 until all nodes are managed by OMi.
4. Before switching off the OM server, switch the agents to OMi completely, and clean up old OM policies if necessary.

Configure the OMi Server as Secondary Manager

To allow step-by-step agent moves, we recommend that you configure the OMi server as secondary manager.

First, verify that the OM and OMi server certificates have been set up correctly, as described in the **Administration Guide > Setup and Maintenance > Connected Servers > How to Verify the Trusted Relationship**, and that the OMi server is part of the trusted server list of all nodes.

On the OMi server, list the server certificate using `ovcert -list`.

The **(OVRG: server)** part of the output lists the server certificate alias, shown in red.

Example ovcert –list output on OMi server:

```
+------------------------------------------------------------+
| Keystore Content (OVRG: server)                            |
+------------------------------------------------------------+
| Certificates:                                              |
|     a2b49ad2-5134-755f-0178-8d3940bf71cf  (*)              |
+------------------------------------------------------------+
| Trusted Certificates:                                      |
|     CA_a2b49ad2-5134-755f-0178-8d3940bf71cf  (*)           |
|     CA_a2b49ad2-5134-755f-0178-8d3940bf71cf_2048           |
|     CA_e1abcac2-aced-7549-05f7-bfec2ef15250                |
|     CA_e1abcac2-aced-7549-05f7-bfec2ef15250_2048           |
+------------------------------------------------------------+
```

On a node, `ovcert -list` should show the alias as trusted certificate:

```
+------------------------------------------------------------+
| Keystore Content                                           |
+------------------------------------------------------------+
| Certificates:                                              |
|     4636e042-5475-7559-0b81-aa37955f88c2  (*)              |
+------------------------------------------------------------+
| Trusted Certificates:                                      |
|     CA_a2b49ad2-5134-755f-0178-8d3940bf71cf                |
|     CA_a2b49ad2-5134-755f-0178-8d3940bf71cf_2048           |
|     CA_e1abcac2-aced-7549-05f7-bfec2ef15250                |
|     CA_e1abcac2-aced-7549-05f7-bfec2ef15250_2048           |
+------------------------------------------------------------+
```

If necessary, update the trusted server list of all nodes by running `ovcert -updatetrusted` on all nodes. On OM for Windows you can use the HP Operations Manager Tools – Certificate Management – Update trusted certificates tool to do this.

Set up OMi as **secondary** and **action allow** manager for the agents using an agent-based flexible management policy. Create this policy on the OM server. You can use the ManagementResponsibilitySwitch example as a starting point:

```
#
# Configuration file
# defines management responsibility switching
#
TIMETEMPLATES
#none
RESPMGRCONFIGS
    RESPMGRCONFIG
        DESCRIPTION "OM and OMi as responsible mgrs"
        SECONDARYMANAGERS
            SECONDARYMANAGER
                NODE IP 0.0.0.0 "omi.example.net"
                DESCRIPTION "OMi"
```

```
              SECONDARYMANAGER
                    NODE IP 0.0.0.0 "om.example.net"
                    DESCRIPTION "OM"
          ACTIONALLOWMANAGERS
              ACTIONALLOWMANAGER
                    NODE IP 0.0.0.0 "om.example.net"
                    DESCRIPTION "OM"
              ACTIONALLOWMANAGER
                    NODE IP 0.0.0.0 "omi.example.net"
                    DESCRIPTION "OMi"
              ACTIONALLOWMANAGER
                    NODE IP 0.0.0.0 "$OPC_PRIMARY_MGR"
                    DESCRIPTION "current primary manager"
      MSGTARGETRULES
        MSGTARGETRULE
              DESCRIPTION "always send all messages to current primary manager"
              MSGTARGETRULECONDS
              MSGTARGETMANAGERS
                  MSGTARGETMANAGER
                        TIMETEMPLATE "$OPC_ALWAYS"
                        OPCMGR IP 0.0.0.0 "$OPC_PRIMARY_MGR"
```

Note: OM will automatically add the `ovcoreid` for each manager to the policy. It retrieves the ID from the corresponding node in the OM database. Make sure that the `ovcoreid` stored there is the OMi server core id (the ID returned when calling `ovcoreid -ovrg server` on the OMi server).

On OM for Windows, you can check and change the `ovcoreid` in the node properties:
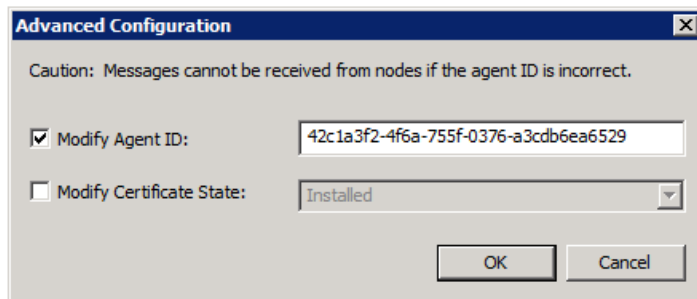
On OM for UNIX and Linux, you can check the ovcoreid of a node using `/opt/OV/bin/OpC/utils/opcnode –list_id node_name=<omi GW/LB/server node>` and change it using the `-chg_id` option.

Deploy the policy from the OM server to all nodes.

To verify if the configuration is correct, you can check a single node from the OMi gateway server using `ovpolicy -list -host <node.example.net> -ovrg server`.

Note: When running command line utilities like `ovpolicy` or `ovrc` from an OMi server, you always have to specify the `-ovrg server` option (unlike OM where this option is only needed in cluster environments). Otherwise the command will fail with a "not authorized" error.

Move Configuration to OMi

Overview

It is recommended to move the configuration of nodes to OMi step-by-step to reduce risk and to allow you to become familiar with new features in OMi.

To familiarize yourself with the new OMi Monitoring Automation features, examine and test the Infrastructure Management Pack. It is free and does not require a separate license.

During the evaluation period you can also install, test, and examine other available Management Packs.

Once you have explored the Monitoring Automation features, you can begin to move the configuration of nodes from OM to OMi Monitoring Automation.

We recommend that you do not configure a node partially from OMi and partially from OM. Instead, identify those nodes or node groups that can be configured completely from OMi.

For example, systems running the Oracle 11 database can be easily managed using the Oracle Management pack and Infrastructure Management Pack. They are good candidates to be moved over first. For other systems, you might want to wait until a corresponding Management Pack is available. If you do not plan to use HPE or Partner Management Packs, then you can import your custom OM policies into OMi.

We recommend you select an OM node group to start with. Determine how it is monitored today and decide how it should be monitored in the future, using an available Management Pack, custom policies, or both. Depending on your decision, adjust the management template or import customs policies. For details, see cases 1-3 below.

Once all monitoring artifacts have been brought to the OMi server, pick a representative node and test the configuration from OMi by assigning management templates or aspects manually. You might have to assign some aspects to the node CI and others to application CIs running on the node. Compare the old configuration with the new configuration and check if all policies have been redeployed.

After the test phase, you can roll out the configuration to all nodes of that node group. Depending on your preferences or needs, you can either do this manually or automate it using automatic assignment rules.

Choose the next OM node group and repeat the steps.

Case 1: Manage Nodes Using an Available Management Pack

If you want to replace the existing OM configuration with a Management Pack, see the corresponding Management pack installation guide and the OMi Help for details.

Moving From an Existing SPI to a Management Pack

When you are currently using a SPI on OM, you have two options when moving to the new Management Pack:

1. Deploy the new Management Pack as it is, and check if it fits your needs. Adjust aspect parameters, such as thresholds, if needed, on assignment or individual CI level. This option might be appropriate for customers who have modified the OM SPI slightly, or who want to establish new standards for monitoring.

2. Analyze the SPI customizations that have been performed on the OM side to determine which of these are still needed with the new parameterized aspects. See the OMi Management Packs Evolution Guide for details.

Case 2: Import and Reuse Custom Policies from OM

To reuse custom OM policies, you export and then import policies, parameterize them if needed, and group them into aspects and management templates.

It is recommended to do this step-by-step, policy group by policy group.

For example, if you want to move over the configuration for all your SAP nodes, which you have organized on the OM side using a SAP node group. A single SAP node might not only receive SAP policies, but OS and System infrastructure policies as well, based on the Linux node group the system is part of. To move over the configuration for the node group, several policy groups need to be moved.

To avoid unnecessary effort, you should only export and import policies that will be used on the OMi side. Do not just export all policies stored on the OM server.

Identify or Create Policy Groups with Policies to Export

Larger OM customers typically have all their active policies in certain policy groups that are often also used for automatic deployment. If this is your case, you can use those policy groups for the export.

If policies were assigned manually and from various source policy groups, then it is recommended to first create a dedicated new policy group that contains all active policies that represent how a node is managed today. You don't have to copy policies that are anyhow not supported by OMi, like ECS, but as OMi simply skips those during the import, you don't have to worry about supported and unsupported types when doing the export. You then export all these policies using the policy group name.

For extensive information, see the **Administration Guide > Monitoring > Migrating Configuration Data > Importing Configuration Data from HP Operations Manager**.

The following sections list the most important commands.

Export Policies from OM for Windows

```
ovpmutil cfg pol dnl <folder> /p <identifier> [/instrum]
```

The switch `/instrum` also exports all instrumentation related to the policies inside the group, for example:

```
ovpmutil cfg pol dnl c:\test /p \Samples /instrum
```

Note: ovpmad service needs to have access/write permissions to the export directory.

Export Policies from OM for UNIX and Linux

Use `opcpolicy` to download policy groups together with instrumentation:

```
# /opt/OV/bin/OpC/utils/opcpolicy -download pol_group=<groupNameWithPath>
dir=<downloadDir>
```

Copy Data

After the export, copy the downloaded files to an OMi gateway server system.

Import Policies on OMi

Syntax Check

It is recommended to run a syntax check for all policies which should be uploaded to OMi.

```
c:\HPBSM\opr\bin\ConfigExchange.bat -username <username> -password <password> -check
-policyfile c:\temp\OML_Test -logfile c:\temp\omlpolicies.txt
```

The specified user must be a BSM user with permission to create policy templates.

Review the logfile for warnings and an overview.

OM for Linux Config Data Upload

Specify the copied folder as input directory:

```
c:\HPBSM\opr\bin\ConfigExchange.bat -username <username> -password <password> -uploadOM
-i c:\temp\OMLExport\
```

OM for Windows Config Data Upload

Specify the copied folder as input directory:

```
c:\HPBSM\opr\bin\ConfigExchange.bat -username <username> -password <password> -uploadOM
-i c:\tmp\OMWPolicies
```

Using this import mechanism, the policy group structure is imported as well and will show up as template groups under **Administration > Monitoring > Policy Templates**.

The following figure shows an example of a group structure that was created as part of a policy import:
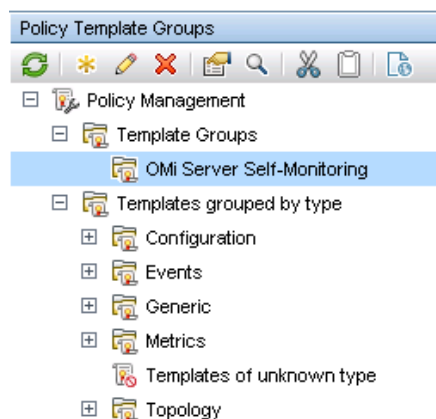
Adjust Policies if Necessary

If the import returned warnings, edit the imported policies in **Administration > Monitoring > Policy Template**. This might be necessary if the policies refer to OM server variables like $OPC_MGMTSV, or use features that are not available in OMi, such as server-based MSI.

For information, see the **Administration Guide > Monitoring > Policy Templates**, which also contains information on how to search policy templates.

Group Policy Templates into Aspects

After importing policies, grouped them into meaningful aspects. An aspect is defined for a specific CI type and should contain all policies that are required to monitor a certain aspect of the CI, like its performance or availability.

video 1: See the OMi tutorial "How to create an aspect containing a group of policy templates" at https://hpln.hpe.com/page/omi-tutorials.

Go to **Administration > Monitoring > Management Templates & Aspects**. Create a suitable configuration folder and add aspects there. When creating an aspect you have to give it a meaningful name, specify the CI Type it is for, and select the corresponding policies.
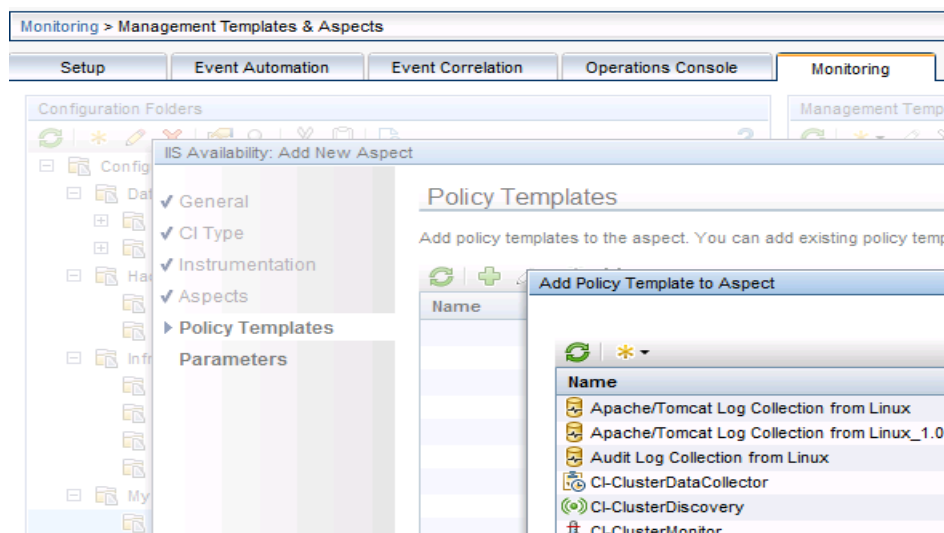
In this step you can create various aspects for various different CI types.

Optional, but Recommended: Create Management Templates to Group Aspects

Creating management templates is not necessary, but advisable. Management templates can simplify the assignment of many aspects, and also allows starting the monitoring of composite applications with a single assignment. You can group aspects using nested aspects as well, but this is limited to a single CI Type. You cannot include an aspect for CI Type A into another aspect for CI Type B. If you want to assign several aspects for different CI Types in one assignment, you need Management templates.

To use management templates, the Monitoring Automation for Composite Applications license is required.

To simplify the assignment of multiple aspects, it is recommended to create one or several management templates after all aspects have been created. For example, you can create several management templates with different aspects, representing for example Essential and Extensive monitoring levels.

Go to **Administration > Monitoring > Management Templates & Aspects**. Create a configuration folder to add management templates into. When creating a management template, you have to give it a meaningful name, specify a view and root CI Type it is for, and select the corresponding aspects. If you use the management template just for the grouping of aspects that belong to one CI Type, you can select any view that contains this CI Type as starting point. You don't have to create a sophisticated view for that. The view is just used as the starting point for the management template definition.

If you want to start the monitoring of multiple related CIs of various CI types using a single assignment, then you have to create a management template for that. In this use case you have to select (and might have to first create) a view that shows all the CI Types and their relations as a starting point for the management template.

> **Note:** Each Management Pack typically ships application views that can be used as a starting point.

For more information, see the **Administration Guide > Monitoring > Management Templates & Aspects > Configuring Management Templates**.

Case 3: Reuse Configuration for Other Node Groups

You might have created multiple policy groups on the OM side to monitor different node groups slightly differently, for example, because you wanted to use different thresholds or different message groups. This was necessary because OM has limited built-in parameterization.

If you created copies or versions of policies in OM and only changed parameters without changing the policy logic, then you should not import those copies into OMi. Reuse and parameterize an existing policy instead.

The parameter values are then changed either when assigning the aspect or management template or when defining multiple aspects or management templates.
Additionally, the tuning of these values can be performed afterward without changing the policy data.

Parameterize Policy Templates

Go to **Administration > Monitoring > Policy Templates** and search for the existing policy that contains the same logic.

Edit the policy and identify the parameters that differ between policies in OM.

For each such parameter, create a parameter in the OMi policy.

video 2: See the OMi tutorial "How to add a parameter to a policy template" on
https://hpln.hpe.com/page/omi-tutorials.

Here you can see an example of a simple measurement threshold policy with four rules. The thresholds used in each rule have been parameterized. Other message attributes, for example, severity, can also be parameterized:
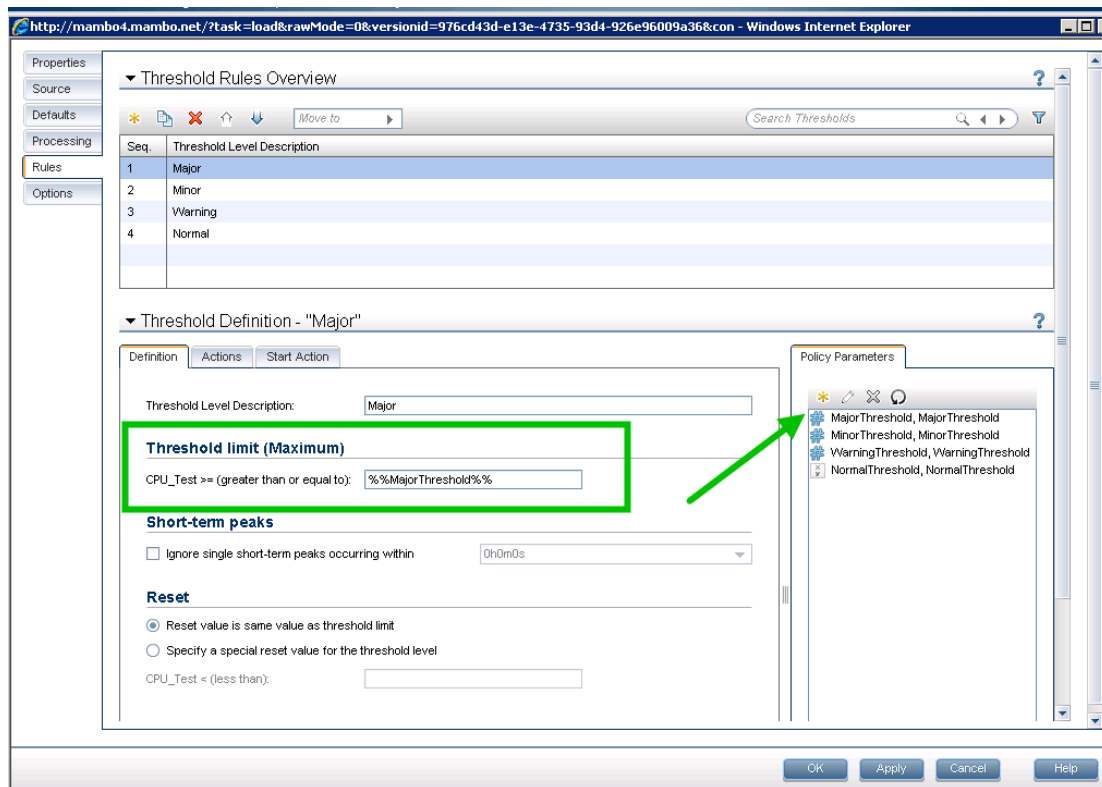
Instance Parameters

Sometimes it is necessary to monitor different instances of a monitored object on the same node differently. OM allowed this using instance conditions in measurement threshold policies. Such instance conditions should be replaced by an instance parameter in OMi, which makes it easier to add or remove instances using parameter tuning without changing the policy.

An instance parameter enables you to create policy templates that monitor multiple instances of the same type of object, for example, multiple database instances or multiple hard disks.

Each policy template can have only one instance parameter. When you add an instance parameter to a policy template, all other parameters become dependent on it. The user can specify separate values for the dependent parameters of each instance.

For example, if you have a policy template that monitors the percentage of disk space in use, you could create an instance parameter called 'DiskDrive', and dependent parameters called 'Minor disk usage threshold', 'Major disk usage threshold', and 'Critical disk usage threshold'. A user of this policy template can specify multiple disk instances using the 'DiskDrive' parameter, for example, by adding the instance values C:, D:, and E:. For each disk instance, the user can then set different values for the dependent parameters, for example, the value of 'Critical disk usage threshold' could be 85% for disk C:, 90% for disk D:, and 95% for disk E:.

Replace both the instance filters and thresholds with a parameter:
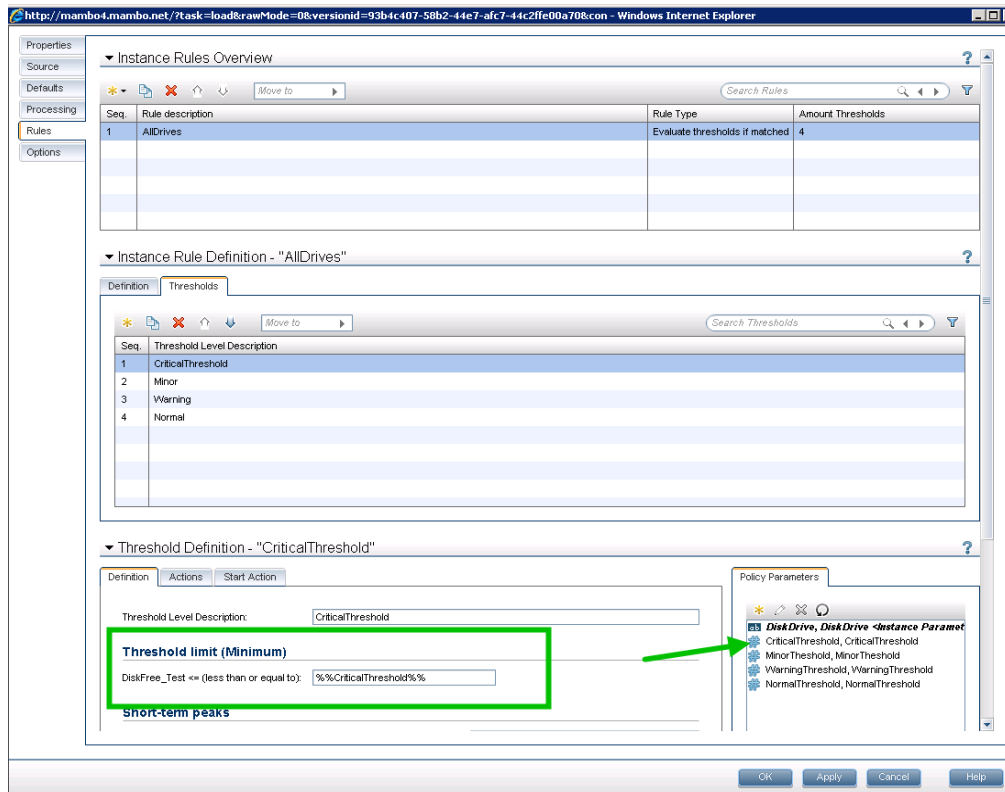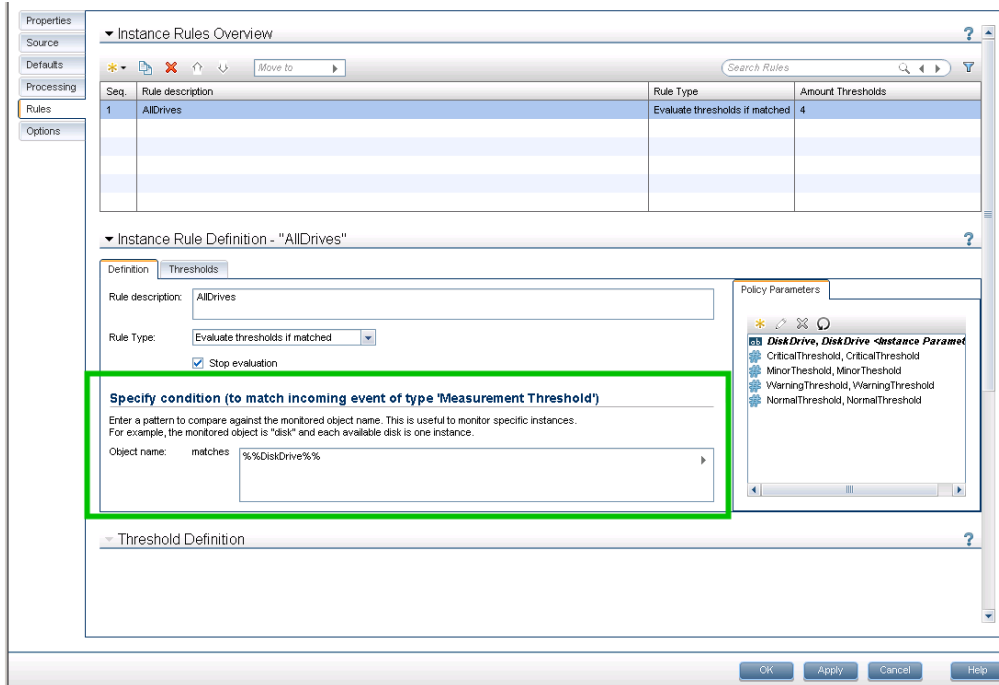
Moving from Instance Conditions to Instance Parameters

The following example demonstrates how to change a measurement threshold policy from using static instance filters and thresholds to using instance parameters. This example policy monitors the percentage of
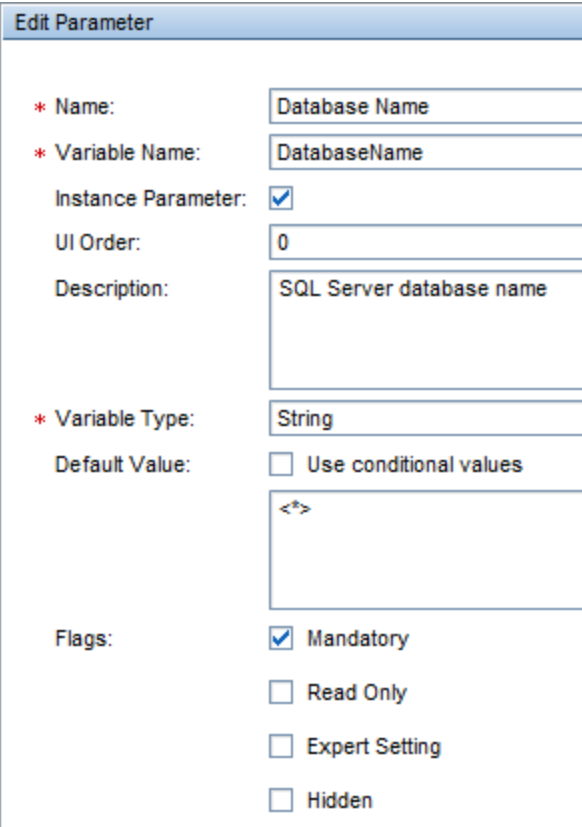
space used in the log of the databases configured in Microsoft SQL Server. Different thresholds are set based on the database name. The database name is the instance that will be parameterized.

MSSQL Databases Percent Log Used [1.0] (Measurement Threshold)

File View Help

Save and Close   Save   Help

Source | Rules | Options

Short name*   DBPctUsed

Description

Source type   Real Time Performance Measurement

Windows NT performance monitor parameters

Object*   SQLServer:Databases

Counter*   Percent Log Used

Instance

Browse on node...

☐ Store in Embedded Performance Component

Data Source*

Object*

Metric

Polling interval   0 h 5 m 0 s   Add source...

MSSQL Databases Percent Log Used [1.0] (Measurement Threshold)

File View Help

Save and Close   Save   Help

Source | Rules | Options

Maximum

Seq.	Description	Rule Type	
1	AdventureWorksDW	If matched, do actions and stop	New...
2	tempdb	If matched, do actions and stop	Modify...
3	ReportServer	If matched, do actions and stop	Delete
4	ReportServerTempDB	If matched, do actions and stop	Copy
5	other	If matched, do actions and stop	

Rule summary   Move up

IF Condition (Object name: AdventureWorksDW)   Move down
of this rule is true THEN:
   Evaluate threshold levels: Move to:
     {Major (Threshold limit >= 90; Severity: Major)}
     {Minor (Threshold limit >= 85; Severity: Minor)}   Defaults...
     {Warning (Threshold limit >= 80; Severity: Warning)}
   Stop evaluation   Test...
ELSE evaluate next rule

Once you have imported the policy into OMi, it can be assigned and used as is. However, to allow setting parameters that can be defined during assignment rather than being hard-coded in the policy, edit the policy template and make these changes:

1. In the Policy Parameters tab, click ☀ to create a new policy parameter. Mark it as an Instance Parameter. Set the default value to the pattern <*> so that all instances are monitored by default if the

user doesn't override the settings during assignment.

Edit Parameter	
* Name:	Database Name
* Variable Name:	DatabaseName
Instance Parameter:	✔
UI Order:	0
Description:	SQL Server database name
* Variable Type:	String
Default Value:	☐ Use conditional values
	<*>
Flags:	✔ Mandatory
	☐ Read Only
	☐ Expert Setting
	☐ Hidden

2. Modify the first rule and give it a generic description. Remove all the other rules that enumerate the instances.

3. Drag and drop the instance parameter into the Object Name field. Because the object is a pattern, you might want to anchor it with ^$ to ensure an exact match. For example, ^%%DatabaseName%%$.
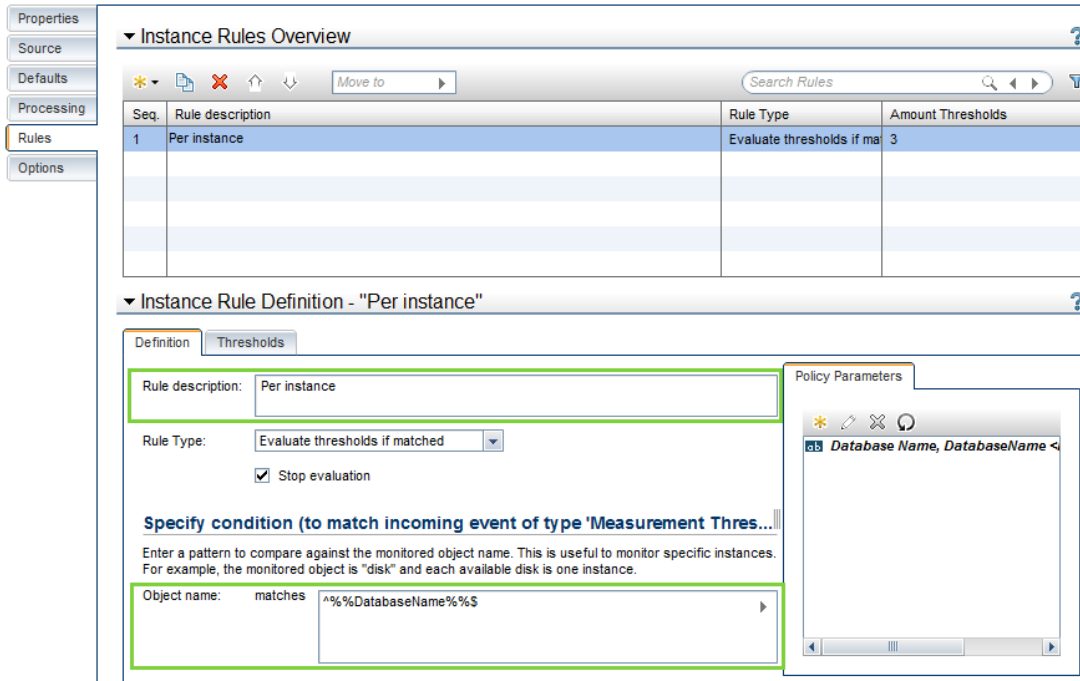
4. To enable different thresholds to be set for each database instance, you also need to parameterize the threshold settings. This policy has threshold rules for Major, Minor, and Warning thresholds.

    In the Policy Parameters tab, click to create a new policy parameter for MajorThreshold. Specify if it is numeric, and provide a valid range and a default value.

5. Drag and drop the MajorThreshold policy parameter into the **Threshold** field of the Major rule.

6. Create additional policy parameters for each of the other thresholds (Minor and Warning), and drag and drop them into the Threshold field of the Minor and Warning rules respectively.

7. Save the policy template.

While you can assign the policy template to a CI, it is best to create or modify an aspect to include the policy template. When it is assigned, you can specify the database instance(s) to be monitored and override the thresholds for each instance.

Note: The order in which you list the instances is important, because it dictates the order of the rules within the policy when it is deployed to the managed node. Therefore, place the more specific instance names at the top of the list.
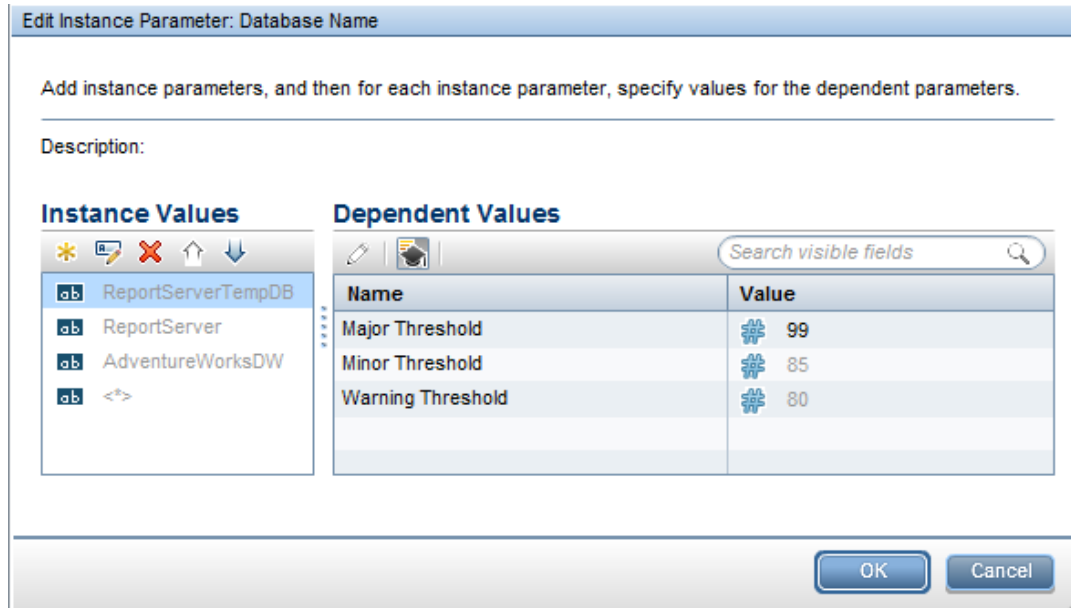
You could specify whether the aspect is associated with the Microsoft SQL Database CI Type and then modify the instance parameter to use the CI attribute containing the name of the database, instead of manually entering the names. All database instances will get the same threshold settings, but you can override the thresholds for each instance in the Assignments and Tuning screen.
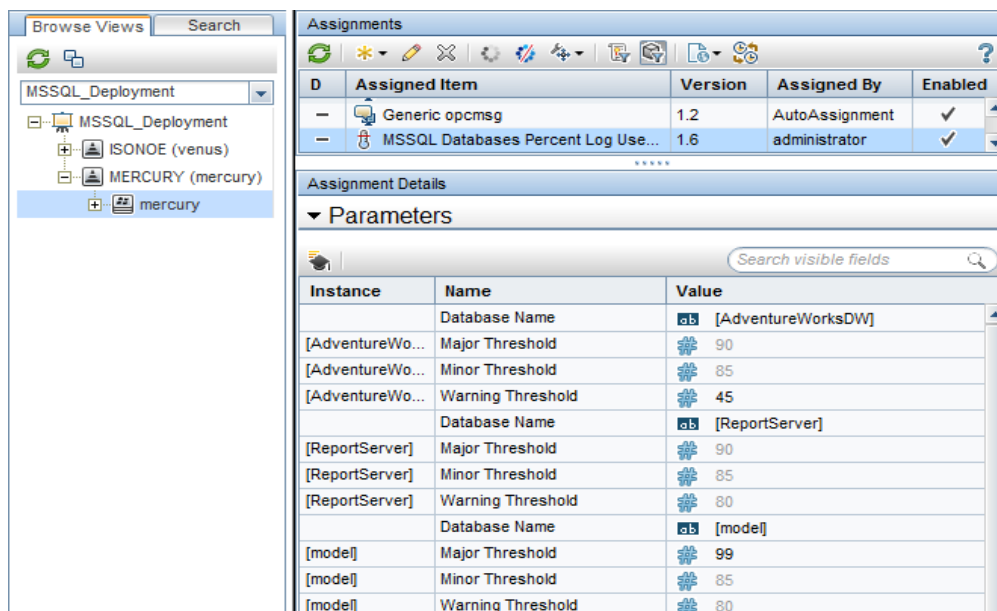
Test Configuration

Once you have chosen or created the aspects and Management Templates you want to use, you should use manual assignments to test and verify the configuration.

You can assign Management Templates and aspects using the aspect or Management Template as a starting point. Go to **Administration > Monitoring > Management Templates & Aspects**. Select the aspect or Management Template you want to deploy and choose Assign and Deploy Item:
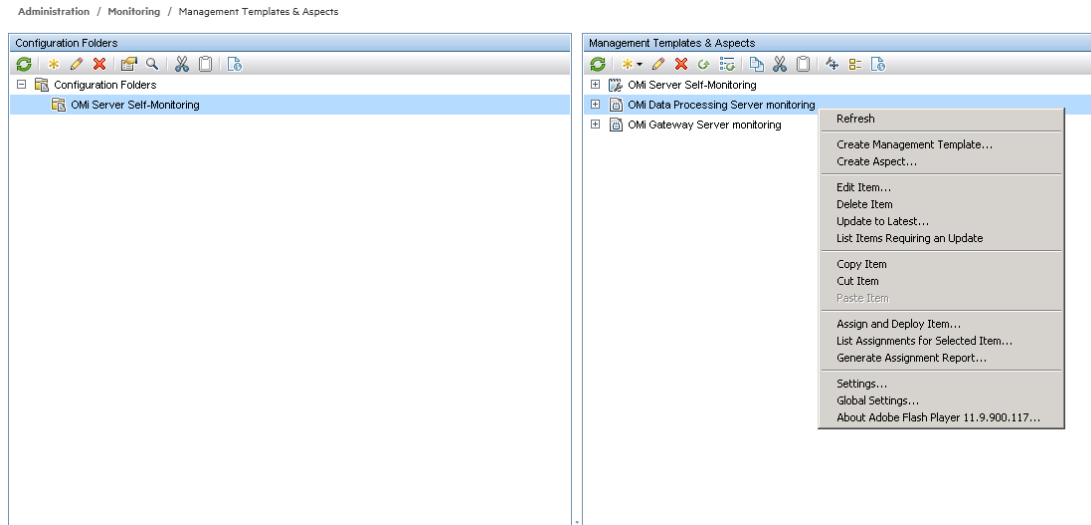
Alternatively, you can use the CI as a starting point: Go to **Administration > Monitoring > Assignments & Tuning**. Select a view that contains the CI and choose **Assign …** from the drop-down list.

The assignment will by default initiate an immediate deployment of all included policy templates to the corresponding nodes.

On the representative node, you can then verify whether all policies have been redeployed:

```
ovpolicy -list -host <hostname> -level 2 –ovrg server
```

This will list all policies and the management server that installed the policy. It might list old policies deployed from OM that have not yet been replaced by OMi.

You can also use the Synchronize Policy Template Assignments feature of OMi to see the policies deployed from OM: Go to **Administration > Setup and Maintenance > Monitored Nodes**. Select a node and choose Synchronize Policy Template Assignments from the context menu. Then check the assignments on **Administration > Monitoring > Assignments & Tuning**. Make sure to show policy assignments as well, as OM can only assign policies and does not know aspects or management templates.

> **Note:** Only one policy with the same name can exist on a node. If multiple assignments on the OMi side

assign policy templates with different versions, then the policy template with the highest version number (and its parameter values) will be deployed by OMi.

What happens if a policy was deployed by OM, got imported into OMi, and redeployed as part of an aspect or a management template?

The policy will be deployed again from OMi and will replace the existing policy with the same version. Afterward, the policy owner will be the OMi server.

What happens if a policy was deployed by OM, got imported into OMi, adjusted (new version created), and redeployed?

The policy will be deployed again from OMi and will replace the existing policy with a lower version. Afterward, the policy owner will be the OMi server.

What happens if a policy was deployed by OM, got imported into OMi, renamed, and redeployed as part of an aspect or Management Template?

The renamed policy will be deployed from OMi, in addition to the already existing policy. The OM policy should be removed manually.

What happens when someone tries to delete a policy or policy assignment on OM after policies were deployed from OMi?

OM checks the policy owner before deleting policies. If the policy owner is OMi, then OM will not delete the policy (unless you specifically ignore the owner or choose force update).

How and when should I remove old OM policies?

If policies were not renamed and if all used policies were imported into OMi and redeployed from OMi through corresponding aspect or management template assignments, then there is no need to delete old OM policies as these no longer exist. They were deleted and replaced by corresponding OMi policies.

If you decided to no longer use certain policies, these need to be removed from the corresponding nodes. One way to do this is to use the OM console:

In OM for UNIX delete the corresponding assignment to a policy group, node group or node and deploy policies. Make sure that Force Update is not selected.
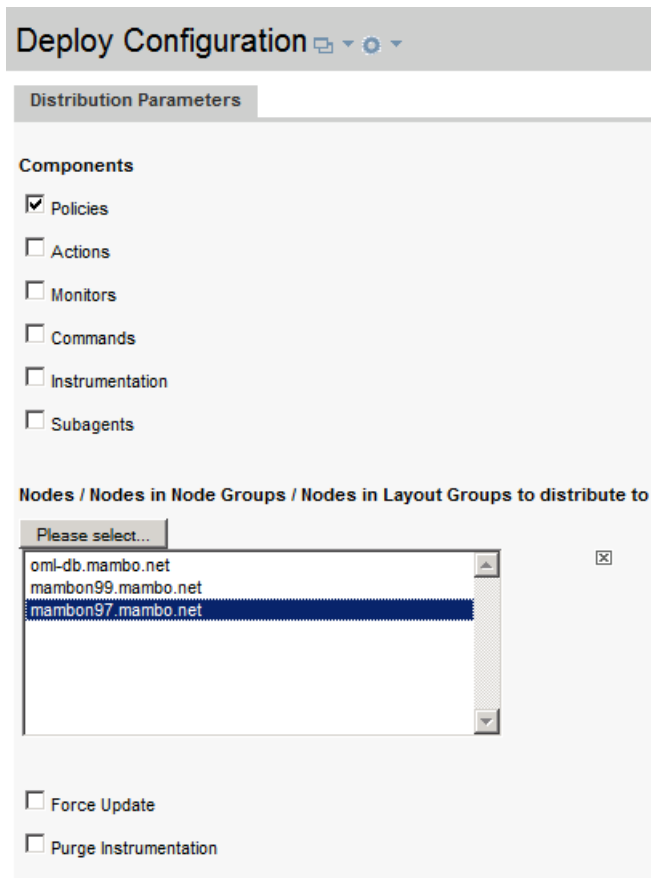
In OM for Windows, choose the policy version and choose **Uninstall from…** from the context menu.
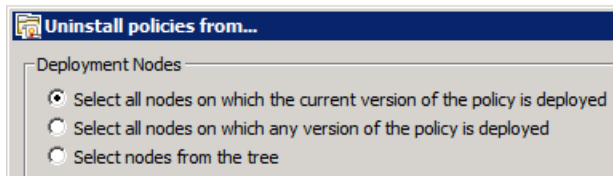
Make sure that **Ignore policy owner** is not selected:
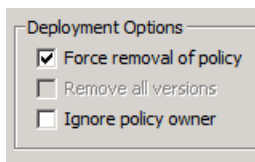
It is also possible to remove old OM policies using the `-deploy -clean` option of the `opr-agt` tool. For example, by using:

```
opr-agt -deploy –clean -node_list "node1.example.com,node2.example.com"
```

For more details, see the **Administration Guide > Monitoring > Command-Line Interfaces > The opr-agt Command-Line Interface** and **opr-agt –help**.

What happens when I delete a node from OM?

Caution: We do not recommend deleting nodes from OM during the evolution, because if the topology synchronization between OM and OMi is still active, this will delete the node CI from the RTSM as well. To prevent this from happening, set the **Skip CI Deletion** infrastructure setting (Infrastructure Settings for Operations Management > OM Topology Synchronization Settings) to True. This will disable the automatic deletion of CIs when performing topology synchronization.

Roll Out Configuration

Once the configuration is validated using a test node, you can roll out the configuration to the rest of the nodes. You can do this either manually, if there is only limited change in the environment, or automatically using web services or automatic assignment rules.

Manual Roll Out

To manually assign configuration to multiple CIs, use **Administration > Monitoring > Management Templates & Aspects** with the aspect/Management Template as a starting point. Select all corresponding CIs manually.

Automation Using Web Services

Automation can be achieved using the Monitoring Automation web services interface. For example, a Management Template can be assigned programmatically to a CI when a new server is provisioned. For details, see the **Extensibility Guide > Web Service Interfaces > Monitoring Automation Web Service Interface > Examples of Monitoring Automation Web Service Applications**.

Automatic Assignment Rules

Automation can also be achieved using automatic assignment rules.

Automatic assignment rules are defined for certain views. Aspects and policies get assigned and deployed to all matching CIs in the view. Make sure that you do not assign configuration to CIs that you do not yet want to configure from OMi. For example, if you create an automatic assignment rule for a System Infrastructure aspect and choose the Systems_Infrastructure view, this would trigger an assignment and deployment to all nodes in the RTSM (because the out-of-box Systems_Infrastructure view includes all nodes). If you have used topology synchronization from OM as recommended, a deployment to all OM nodes will be triggered. To avoid this, choose another view which only contains those CIs that you want to configure from OMi. See How to avoid policy assignment to nodes that are not yet managed by OMi below.

Example 1: How to assign Gold, Silver, and Bronze monitoring levels to different "nodes".

On the OM side you might have deployed different policy groups representing Gold, Silver, and Bronze monitoring levels to different node groups. To automate this in OMi, you use three Management Templates (or summary aspects with nested aspects), and three views that contain the corresponding CIs.

Note: Management templates and aspects are defined for certain CI Types, like Oracle or computer.

> When you want to assign these, you need views that contain CIs of those CI types.

To separate CI groups, you can use pattern views with queries that return only those CIs of a CI type that matches a certain query. For example, if you have certain Oracle databases that should be monitored using a Gold Management template, and if you can determine those databases based on CI attributes or relationships to other CIs, then you can define a pattern view that only contains those CIs.

If the CI attributes do not yet contain enough information, then you should try to add the information in an automated way, for example, by using enrichment rules or RTSM APIs, as manually adding and maintaining CI collections is often not suitable when you want to automate monitoring.

Example 2: How to assign multiple Management Templates or aspects to the same "nodes".

On the OM side you might have deployed different policy groups, for example for Linux, Oracle or other application management areas, to a single node. To automate this in OMi, you use multiple automatic assignment rules with corresponding Management Templates, or summary aspects with nested aspects, and views.

> **Note:** You should avoid assigning the same policy templates multiple times through multiple assignments. This could happen if you assign one Management Template to a view that contains many CIs, for example all Linux nodes, and another Management Template to a subset of these CIs, for example all Linux systems that run Oracle databases. If both Management templates contain the same policy templates with varying parameter values, the system applies one of the two values and you cannot tell which one. To avoid this, either make sure that the views used in auto-assignment rules do not contain the same CIs (disjoint views) or that the Management Templates and aspects that are assigned to a single node do not contain the same policy templates (non-overlapping Management Templates and aspects).

Go to **Administration > Monitoring > Automatic Assignments Rules** and see the corresponding OMi Help topics for more details.

How to avoid policy assignment to nodes that are not yet managed by OMi

When the OMi server is specified as the primary manager of an agent, the Operations Agent will send information about its node name and IP address to the OMi server. When this data is received, OMi also creates a relationship between the OA CI and the OMi server CI in the RTSM, which means that the agent is now managed by OMi. This relationship can also be created manually by using the node editor "managed by OMi" icon.

This relationship can be employed in views used in automatic assignment rules so that the only CIs shown in the view are those that are hosted on nodes managed by OMi. Add the Operations agent and OMi server CI types to your view with corresponding relationships to nodes. Nodes and related CIs that are not managed by OMi should not appear in the view result.

Use such a view in automatic assignment rules. Whenever another agent is switched to OMi and sends its node name/IP address data to OMi, it will appear in the view and will automatically get the corresponding assignments.

Alternatively, you could assign aspects to all nodes, but deploy the flexible management policy that grants OMi the right to deploy policies only to those nodes you want to switch. In this case, deployment jobs for nodes that don't allow policy deployment from OMi will fail, but these jobs can be deleted manually and the deployment can then be triggered again when the node is switched. However, this option does not transparently show which nodes have already been switched.

OM and OMi Policy Assignment and Deployment Functionality Comparison

The following table compares policy assignment and deployment functionality in OM and OMi.

Functionality	OM for UNIX	OM for Windows	OMi
Assignment and deployment process.	Assignment and deployment are separate tasks.	Assignment and deployment are combined.	Assignment and deployment are combined. Can prevent automatic deployment globally via "Create suspended deployment jobs" in Infrastructure Settings.
Deployed policy state.	Deployed policies are enabled.	Can choose whether deployed policies are enabled, disabled or unchanged.	Can choose whether deployed policies are enabled or disabled.
Version assignment to configuration object or CI.	Can assign fixed, latest or minor to latest version to policy group, node group or node.	Can assign fixed or latest policy version to policy group. Fixed policy version is assigned/deployed to node or node group.	Relationships between management templates, aspects and policy templates are based on fixed versions. Fixed versions are assigned/deployed to CIs.
Update version assignment to configuration object or CI.	Yes.	Can update to the latest version for selected policies in a policy group. Can update to the latest version for all policies assigned to a node. Can manually assign a different version.	Can update to latest version of the objects within a management template or aspect. Can manually assign a different version.
Delete assigned policy.	Policy is deleted, including assignments.	Policy is deleted, including assignments.	Need to delete assignments before being permitted to delete policy.

Change Primary Manager and Target Server of Agents

During the move to OMi you can continue to use your existing OM server as (primary) manager, receiving the events from the agents, until you switch off OM, and as long as OM forwards all events to OMi.

However, to verify that all server-based correlation features of OMi are working as expected, including duplicate suppression and event storm suppression, it is recommended to change the target server for events to OMi gradually. For example, when you have moved the configuration of the corresponding nodes to OMi

then you could also switch the target server to OMi. In case you still would like to receive all events in OM as well, you can use an OMi forwarding rule that forwards all events received on OMi to OM. Instruction retrieval might also fail if the OM server does not have the policy that was deployed from OMi in its policy inventory.

With the earlier mentioned flexible management policy, you can switch the target server by switching the primary manager of a node, because the flexible management policy contains
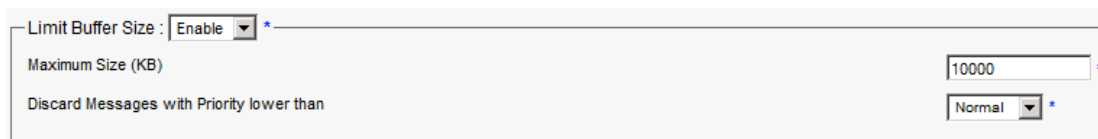
```
MSGTARGETMANAGER
            TIMETEMPLATE "$OPC_ALWAYS"
            OPCMGR IP 0.0.0.0 "$OPC_PRIMARY_MGR"
```

as message target rule. If you used another message target rule, change it accordingly and redeploy the policy to those nodes you want to switch.

You can switch the primary manager from OMi using, for example:

```
opr-ragt -username admin -primmgr <node selection>
```

> **Note:** OM allows setting certain agent configuration variables in the OM UI, like agent buffering and DHCP settings.

OMi does not allow changing these via the UI, but these settings can be changed using ovconfpar.

To configure these from OMi, use the `opr-agt -set_config_var` option: For example, use:

```
opr-agt -set_config_var eaagt:OPC_BUFLIMIT_SEVERITY=major –node_list node1,node2
```

```
opr-agt -set_config_var eaagt:OPC_BUFLIMIT_SIZE=10000 –node_list node1,node2
```

Consequences of a Primary Manager Switch

A switch of the primary manager affects the license counting and heartbeat monitoring. The agent will now report to the OMi server and increase the number of Operations Agents shown on the OMi Server license report.

A switch to the OMi server as primary manager also causes the agent to report its IP address and node name to the OMi server, which will create corresponding CIs and relationships in the RTSM and start agent health checking from OMi. It might also trigger the deployment of policy templates if you have defined corresponding automatic assignment rules.

Consequences on the OM side:

The OM server might report that the agent is no longer running as it is no longer receiving heartbeat messages. Switch off the health check on the OM server side.

> **Note:** After a primary manager switch it is still possible to manage and configure an agent from the OM Server. It is therefore still possible to deploy or remove policies from OM.

Complete Switch of an Agent

To be able to switch off the OM server, the agents need to be reconfigured so that they use the OMi server as their server, even when the flexible management template is removed.

This can be done using the opr-agt `-switch_manager` option. It changes the following settings on the agent:

```
sec.cm.client CERTIFICATE_SERVER
sec.core.auth MANAGER
sec.core.auth MANAGER_ID
eaagt.lic.mgrs GENERAL_LICMGR
```

opr-agt allows a mass update using a TQL, node group, or node list. For example, from OMi use:

```
opr-agt -switch_manager —query_name All_agents_mgd_by_OMi* -username admin
```

or

```
opr-agt -switch_manager —node_list node1fqdn,node2fqdn,node3fqdn
```

> **Note:** Make sure that this TQL only contains those nodes you want to switch. Especially make sure that the OM server node is not part of that TQL. As an alternative use the –nodelist option.

To clean up old OM policies that might still be installed on the node, run:

```
opr-agt —deploy -clean <node selection> -username <user>
```

This deletes all existing policies on the node, including the flexible management template that grants rights to both OMi and OM servers, and then deploys all policies that are assigned to the node in OMi.

The result of both calls is that the agent is completely managed by OMi.

Summary and Command Overview: How to Move Operations Agents to OMi Step by Step

This section contains the most important steps and command line calls used in moving operations agents and their configuration to OMi.

1. Allow management from both servers using a flexible management template.

2. Choose a group or type of nodes to move over, for example, all Oracle Database systems.

   a. Test policy and aspect deployment and tool execution from OMi on a representative node of that type. This might include importing OM policies
      ```
      ConfigExchange.bat -username <user> -check -policyfile c:\tmp\OMPolicies -logfile
      c:\tmp\ompolicies.txt
      ConfigExchange.bat|.sh -username <user> -uploadOM -i c:\tmp\OMPolicies
      ```
      and creating OMi aspects and management templates.

   b. After a successful test, roll out configuration to the remaining nodes of that type manually or by using automatic assignment rules.

    c. Switch the primary manager and target server to OMi. This still allows configuration from both OMi and OM servers

       `opr-agt -primmgr <node selection> -username <user>`

3. Repeat steps 2-5 until all nodes are managed by OMi.

4. Before switching off the OM server, switch the agents to OMi completely

   `opr-agt —switch_manager <node selection> -username <user>`

   and clean up old OM policies if necessary

   `opr-agt —deploy -clean <node selection> -username <user>`

Additional Information

Deployment of Policy Groups to Node Groups

OM customers deploy policies or policy groups to node groups. In a node-centric model, this is an easy way to structure and control the deployment of policies. In OMi, as explained above, this model is replaced by a CI-centric deployment in order to benefit from all CI-type related features (such as using CI attributes for setting monitoring parameters and so on).

If you do not use these features, you can continue deploying policy groups (in the form of management templates) to node groups (which are represented as CI collections in OMi) as explained below.

How to Create and Maintain Node Groups/CI Collections

Node groups or layout groups that exist in OM are forwarded to OMi as part of the OM topology synchronization. Those node groups are converted into CI Collection CIs. See How to Move Node Topology to OMi/Topology Synchronization for more information.

> **Note:** When OM will be discontinued, node group hierarchy will need to be maintained through other mechanisms.

The easiest way to maintain node groups manually is by using the Monitored Nodes Admin UI. You can create node collections (CI Collection CIs). You can add and remove nodes to/from these node collections.
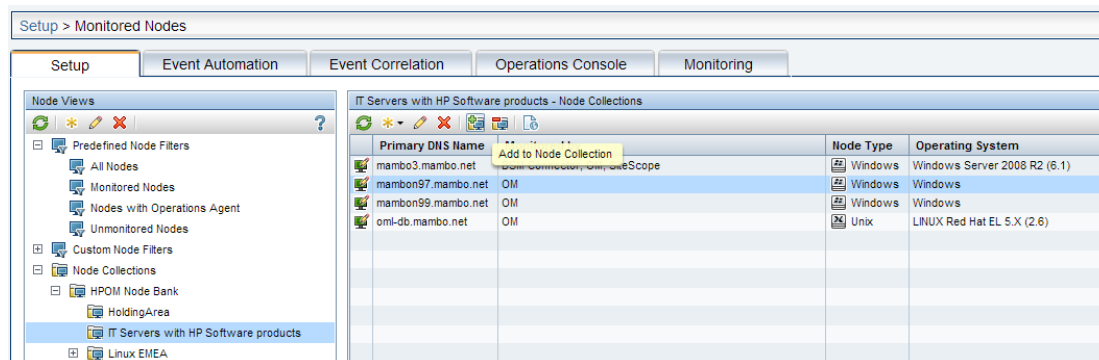
CI collection > node membership relationships can also be created using the RTSM Admin UI or RTSM APIs, but these require deeper knowledge of the RTSM.

You can also automatically create CI collection -> node membership relationships using enrichment rules. See the RTSM documentation for more details.

How to Create Management Templates for Policy Group/Node Group-Centric Deployment

You can assign an aspect to a CI collection CI, but it gets assigned to that CI only, and not to all related node CIs. However, you can use the management template mechanism as described below to achieve the required behavior.

Create a new management template. For the topology view, select the view that contains the CI Collection CI Type and the membership relationship to Node or Computer CIs. If all your aspects are defined for the Node CI type or are marked as 'node compatible', you can use the OM CI Collection view. If you plan to deploy aspects of the infrastructure management pack, create a similar pattern view using the Computer CI type, as the infrastructure aspects are defined for that CI type.

Make sure that CICollection is the CI type to which the management template will be assigned. Then assign the aspects to the Node CI type or Computer CI type as required.

The following figure shows how to create a management template representing a policy group:
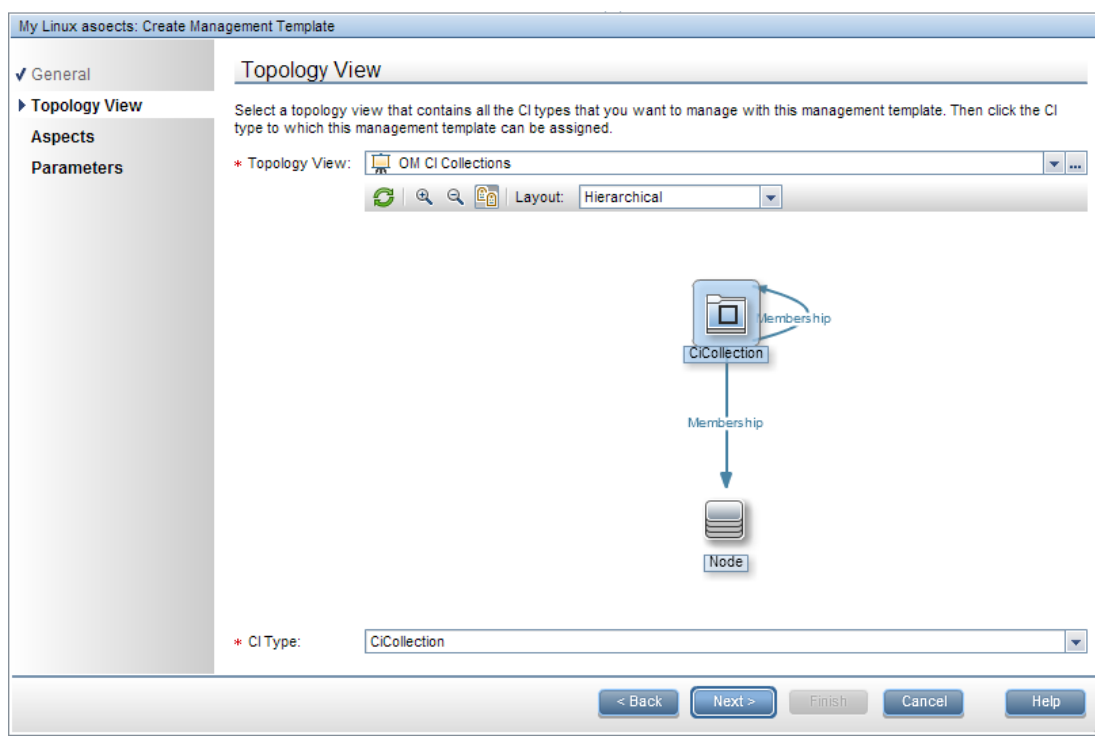
For example, by using this method, you can create a "Linux management template" that contains all aspects (policy templates) you want to deploy to the Linux node group. Create other management templates (policy groups) for other node groups.

How to Deploy to a Node Group/CI Collection

Once node groups and management templates are created, assign management templates as required using the Management Templates & Aspects UI or the Automatic Assignment Rules UI.

Manual Deployment

Select the management template (policy group) you want to deploy and choose **Assign and Deploy Item** from the context menu.

Then select one or more node groups (CI collections) to which you want to deploy:
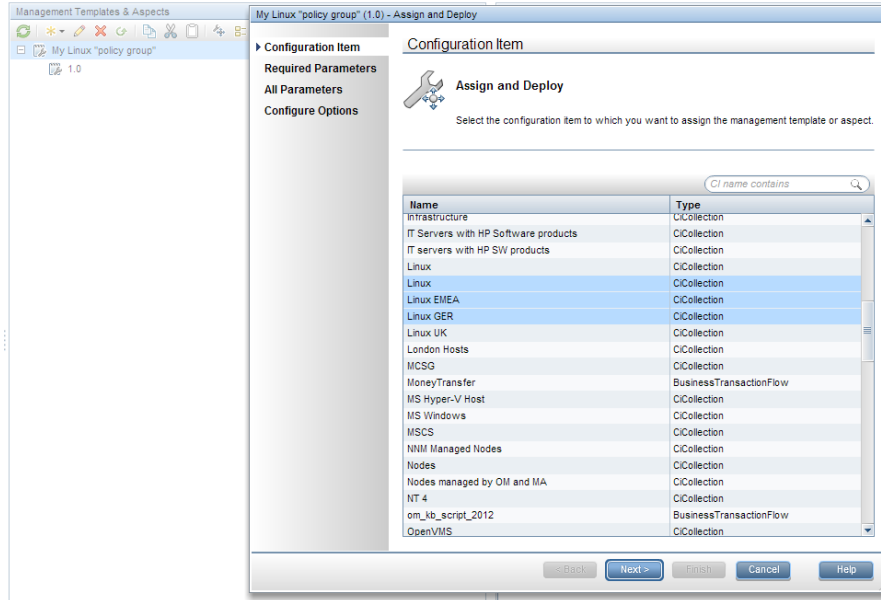
Assignment Summary lists the resulting assignment to each node CI:
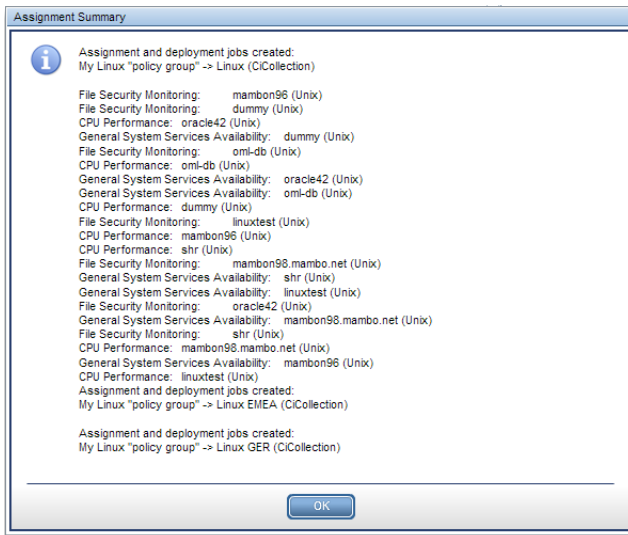
The Assignment and CI configuration reports show the management template/policy group assignment:

Automatic Deployment

Using a corresponding "Linux node groups" view, you can also automatically assign such management templates using automatic assignment rules. Create a pattern view with the CI Collection CI type and membership relationship and query node properties that select one or more specific node groups:
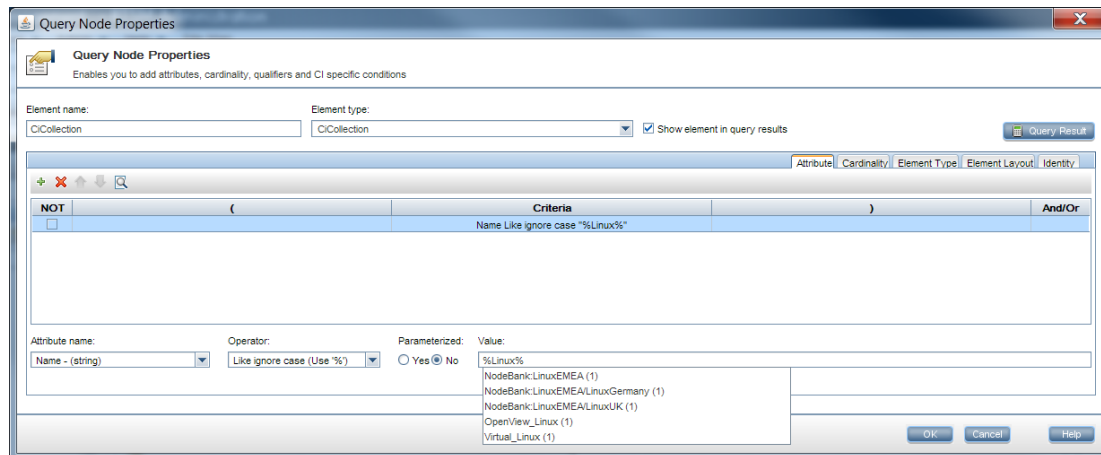
The resulting view contains only Linux node groups and nodes. This view can then be used in automatic assignment rules to deploy the Linux management template to Linux node groups.

Scheduled Deployment

By default, manual and automatic assignments trigger an immediate deployment of the corresponding policies. If you plan the deployment at a later time (for example, during non-office hours), you can achieve this by setting the **Create suspended deployment jobs** infrastructure setting and using the opr-jobs tool to start the deployment jobs. See the **Administration Guide > Monitoring > Command-Line Interfaces > The opr-jobs Command-Line Interface** and the **Administration Guide > Monitoring > Deployment Jobs** for more details.

OMi Policy Limitations and Corresponding Workarounds

Limitations compared to OM for Windows:

- WMI policy editor: no WMI browser available.
  Workaround: Use WMI browsing tools available from Microsoft. For more information, see
  http://technet.microsoft.com/en-us/library/cc181099.aspx.

- Measurement Threshold Policy editor: no data source browsing of WMI metrics, Windows Performance Counters, or metrics of the embedded performance component (coda).
  Workaround: Use WMI tools as mentioned above for WMI and the built-in Performance Monitor of Windows (perfmon.exe) to connect to performance counters of another computer. To browse the metrics of the embedded performance component, use the OMi Performance Perspective.

- Measurement Threshold policy does not support the "Show only newest message in message browser" feature.
  Workaround: If needed, set MsgKey and MsgKeyRelation manually using the following pattern:

```
MsgKey: <$NAME>:<$MSG_NODE_NAME>:<$MSG_OBJECT>:START<$THRESHOLD>
MsgKeyRelation: <$NAME>:<$MSG_NODE_NAME>:<$MSG_OBJECT>:<*>
```

Limitations compared to OM for UNIX and Linux:

- Search/edit/replace/undo options are not available in the RAW Mode Policy Editor.
  Workaround: Copy a complete policy to the external editor that supports these operations.

Limitations compared to OM for UNIX and Linux and OM for Windows:

- When using patterns for event correlation (inside the **Close Events with Key** field of a policy template), there is a difference between the patterns that can be used in OM and OMi. Currently, OMi does not support using range patterns (using -lt, -gt, and so on) and always performs a case-sensitive comparison. If OM policies use range patterns or a case-insensitive check, syntax check used before uploading the policies reports a warning.

- Test Pattern functionality (and opcpat(1) CLI) is not available in Logfile Entry and Windows Event Log Templates.

- Event Browser: Select Message -> Edit condition/policy is not supported in OMi.

Event-Related Actions

In OM, administrators can define automatic and operator-initiated actions inside a policy. Those actions, when executed on nodes with an HPE Operations Agent, can be used by operators to collect more information about the specific problem or even solve it. These event-related actions exist in OMi as well.

However, there are four types of event-related actions that cannot be launched from an OMi console:

- Actions using $GRAPH

- Actions launched on $OPC_MGMTSV

- Actions launched on $OPC_GUI_CLIENT

- Actions launched on $OPC_GUI_CLIENT_WEB
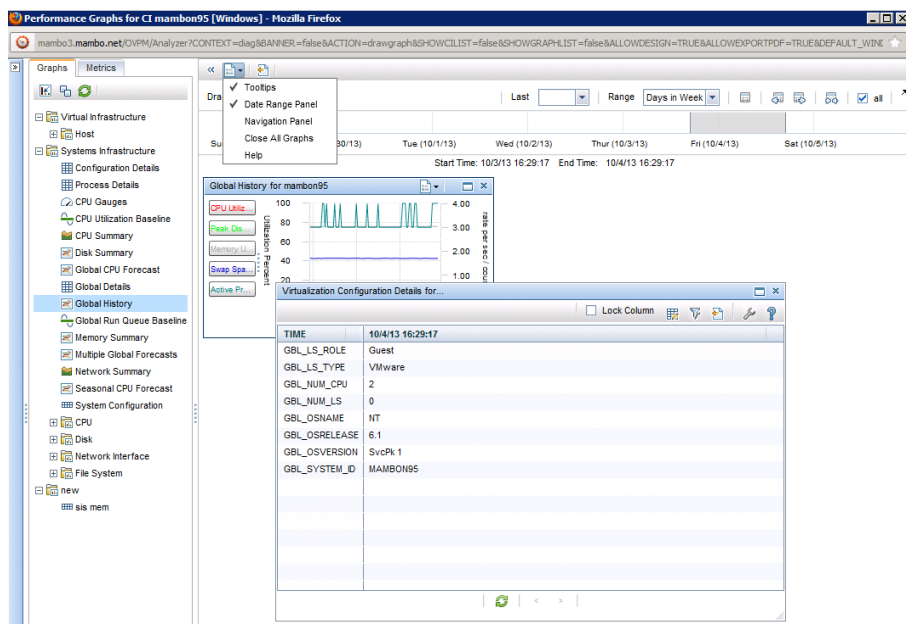
The actions that use these variables are filtered out by OMi and not displayed. It is also not possible to define those actions in OMi policy template editors.

OMi Solutions for $OPC_MGMTSV Actions

Instead of executing an action on the management server using the HPE Operations Agent, you can execute an action on the management server using an EPI script when a certain event arrives. EPI groovy scripts are executed on the OMi gateway server that receives the event. EPI scripts have full access to all event properties and can be used for different purposes. Consider this option for actions relevant for many events (for example to log certain events, to enrich events, and so on).

If the action call is very event-specific (every policy condition defines another action) and uses varying parameters extracted from the event source, you may consider to continue using event related actions. This is less error-prone because everything is configured in one location, namely the policy, and not across multiple UIs. In this case, we recommend that you introduce an "OMi server" policy parameter instead of using the $OPC_MGMTSV variable. This parameter can then be set to the OMi data processing server name (or the OMi load balancer name, depending on your requirements where the tool needs to be executed) inside a management template.

OMi Solution for $GRAPH Actions

Actions using $GRAPH launch predefined performance graphs and can even pre-define the displayed time range so that the time when the problem occurred is shown. In OMi, graphs can be launched using the event context menu (show Performance Graphs (CI)) which automatically shows all default graphs for the selected CI. From there, you can easily select additional graphs and use the Date Range Panel to navigate to the time when the problem occurred.

OMi Solution for $OPC_GUI_CLIENT_WEB Actions

Instead of specifying the URL in the action, you can specify it in the instructions of the event.

OMi Solution for $OPC_GUI_CLIENT Actions

The OMi web-based user interface runs within a web browser that does not allow calling external programs due to security reasons. As an alternative, such actions (including the parameters) can be mentioned in the instructions. The user can copy and paste the command line into a command prompt on the client OS.

Policy Types

OMi supports the following policy template types:

- ArcSight Logger
- ConfigFile
- Flexible Management (agent-based)
- Logfile Entry
- Measurement Threshold

> **Note:** Script parameters are automatically converted into MA parameters.

- Node Info

- Open Message Interface
- Scheduled Task
- Service Auto-Discovery
- Service/Process Monitoring
- SiteScope Templates
- SNMP Interceptor
- Windows Event Log
- Windows Management Interface
- XML File

Not supported are:

- OM for UNIX v.8x templates
- SiteScope policy type exported from OM -> import directly from SiteScope
- ECS (Event correlation, event composer) -> TBEC, SBEC, EPI
- RAS (Remote action security)
- Server-based MSI -> EPI
- Server-based Flexible Management -> Connected servers and forwarding rules
- Custom policy types (OM for UNIX and Linux)

Conversion of Trouble-Ticket and Notification Flags

Policies that set the **Forward to trouble ticket** or **Forward to notification server** flag can be imported and reused without modification.

The flags are kept in the policy data and can be edited in RAW mode. When an event with those flags arrives in OMi, those flags are automatically converted into custom attributes **ForwardToTroubleTicket = true** and **NotifyUser = true**.

These custom attributes can then be checked in the event filters of OMi forwarding or notification rules (**Administration > Event Processing > Automation > Forwarding and Administration > Event processing > Automation > Notifications**) to forward events automatically as on OM.

How to Deploy Custom Instrumentation (OM for UNIX and Linux)

OM for UNIX and Linux v.9x introduces instrumentation categories and allows to group instrumentation files into such categories. When a policy is imported into OMi, the referenced instrumentation category is automatically imported as well and is automatically deployed when the policy template is deployed.

Additional instrumentation files stored under `/var/opt/OV/share/databases/OpC/mgd_node/customer` are imported automatically as well, but stored under a new category `OMU_customer_data`. Add this instrumentation category to policy templates or aspects that need the instrumentation. To save time, you can add the instrumentation category on the aspect level.

> **Note:** If you deploy individual policies for testing purposes, this will not trigger instrumentation

deployment.

How to Edit Already Uploaded Instrumentation Files

During the policy export and import, all assigned instrumentation categories are exported and imported on the OMi side. When a second policy import refers to the same instrumentation categories, the instrumentation is not uploaded again.

To update the instrumentation files on the OMi side, either during the migration because the instrumentation files have changed on the OM side in the meantime, or after the migration, proceed as follows:

Download the current instrumentation (including all patches and hotfixes) available in OMi.

For example, to download the category Database, use:

```
/opt/HP/BSM/opr/bin/ConfigExchange.sh -user <username> -password <password> -merge
-output /tmp/Database -instrumname Database
```

1. Make the necessary changes to the instrumentation files in the downloaded directory `/tmp/Database`.

2. Upload the instrumentation files using the `-force` option:

   ```
   /opt/HP/BSM/opr/bin/ConfigExchange.sh -user <username> -password <password> -upload
   -input /tmp/Database -instrumname Database -force
   ```

Chapter 6: Configuring SiteScope from OMi

Overview

 SiteScope is an agentless monitoring solution that enables you to remotely monitor the availability and performance of your IT infrastructure (for example, servers, operating systems, network devices, network services, applications, and application components). OMi allows you to combine agent-based monitoring with Operations Agents and agentless monitoring with SiteScope.

You can use templates in SiteScope to create sets of monitors that you want to deploy together. When you add a monitor to a template, you can specify fixed values for the monitor settings. In addition, you can add variables to a template so that you can set the values of some settings when you deploy the template.

For example, you have a template that contains the monitors called CPU and Memory. You can configure fixed settings that you always want to use for those monitors, but add variables called Remote Host and Monitoring Interval, for the settings that you want to modify each time you deploy the template.

Those SiteScope templates can now be imported into OMi, be grouped into aspects, included in management templates and assigned manually or automatically by OMi. As with agent-based monitoring, this allows you to standardize and automate the monitoring configuration and automatically respond to changes in your IT environment.

The parameters in OMi offer the additional benefit that you can use CI attributes to set SiteScope Template parameters. You can also pre-define certain parameter sets in different management templates, which are then assigned to different CIs.

The most important advantage, however, is that you hide the underlying monitoring technology in the aspects and management templates: assigning an aspect does not require in-depth know-how of SiteScope. You can also combine SiteScope policy templates with other agent-based policy templates.

SiteScope Deployment from OM and OMi: Functionality Comparison

Functionality	OMi	OM for UNIX
Deploy monitors, groups, and remote servers	Yes.	Yes.
Automated deployment	Yes.	Can be scripted using OM for UNIX CLIs.
Automated lifecycle monitoring	Yes. If the CI is no longer part of the view (for example, the monitored business application), then monitoring is automatically removed.	Can be scripted using OM for UNIX CLIs.

Deployment workflow	Assign and deploy configuration starting from a CI or a policy template, aspect, or management template.	Assign and deploy SiteScope policy.
Undeployment workflow	Can delete an assignment that removes the monitor(s).	Unassign and undeploy the SiteScope policy.
Deployment flexibility across multiple SiteScope servers	Default behavior is to deploy monitors to the SiteScope server with most free points. Alternatively, you can configure OMi to decide according to other criteria, such as the IP address or domain name of the monitored target via Groovy script.	Deploy SiteScope policy to a selected SiteScope server. Can also assign policy to a virtual node (target system) where SiteScope is the physical node.
Agent-based and agentless monitoring configuration	Yes.	Yes.
SiteScope template handling	Create/modify templates in SiteScope. Import templates to OMi manually.	Create/modify templates in SiteScope. Import templates to OM for UNIX manually.
Parameterization	Pre-populate parameters with CI attribute values or manually enter values	Edit the policy to set or change parameters. Supports special variables: `HOST`, `NODEGROUP`, and `FILE`
Template versioning	OMi stores multiple template versions, allowing one chosen version to be deployed at a time.	OM for UNIX stores multiple template versions, allowing one chosen version to be deployed at a time.
Assignment management	SiteScope templates are the lowest granularity of monitoring elements. They can be grouped with other policy templates into aspects or management templates to manage assignments at a macro level, which is important for large-scale deployments. You can combine parameters that are the same across templates so that you are prompted for each value only once.	Assign SiteScope policies or policy groups to the SiteScope node.
CI-centric deployment	Yes.	Node-centric.
CIs must be in the RTSM before use	Yes.	SiteScope server must be a managed node. Target nodes do not have to be in the Node Bank but an external node is required to allow events through.

Leverage RTSM node credentials	No. Can create templates that use SiteScope Credential Preferences.	N/A. Can create templates that use SiteScope Credential Preferences.
Validate points required and available prior to deployment	No.	No.
Control SiteScope monitor group structure	Parent monitor group is hard-coded to "Deployed from Operations Manager" with subgroup named as `gwserver.fqdn`.	Parent monitor group is hard-coded to "`Deployed from Operations Manager`" with subgroup named as `OVO:omserver.fqdn`.
Deployment status	The Deployment Jobs screen shows pending and failed deployments, where you can view the error and restart the deployment job. Review `<OvDataDir>/log/system.0.en_US` on the SiteScope server to see what happens on the SiteScope side.	OM for UNIX generates a message on success and on failure to deploy policies. Review `<OvDataDir>/log/system.0.en_US` on SiteScope server to view what happens on the SiteScope side.
Assignment report	From **Setup > Connected Servers**, select a SiteScope server and click **Launch SiteScope Report**. This generates a report of the CIs monitored by SiteScope via OMi, along with the list of templates for each CI.	The OM for UNIX server shows the SiteScope policies assigned to the SiteScope server.

Moving SiteScope Monitor Deployment from OM for UNIX to OMi

If you currently use OM for UNIX to deploy SiteScope monitors, there are two possible approaches to moving the configuration to OMi:

- Import SiteScope templates directly from SiteScope to OMi using the `ConfigExchangeSIS[.bat|.sh]` command.

- Import OM for UNIX SiteScope policies to OMi using the `ConfigExchange[.bat|.sh]` command.

The best option is to perform an import directly from SiteScope. The reason is that OM for UNIX supports special variable values that are not used in OMi. Since you cannot edit the policy within OMi, you cannot make use of those imported policies. OM for UNIX allows the use of %%HOST%%, %%NODEGROUP:*<nodegroup_name>*%%, %%FILE:*<file>*%% and %%FILE:*<file>*.$SISHOST%%.

Configuring Multiple SiteScope Servers

OMi can configure multiple SiteScope servers. Prepare all SiteScope servers as described below.

By default, OMi instantiates monitors on the SiteScope server that has the most available license points. It is also possible to choose a SiteScope server using other attributes, such as the hostname or IP addresses of the monitor target. See the **Administration Guide > Setup and Maintenance > Connected Servers > How to Create a Connection to a SiteScope Server** for more details.

Example proxy deployment scripts are available under `<OMi_HOME>/opr/examples/deployment-server-selection`.

Steps for Configuring SiteScope

Preparing SiteScope

Before you can configure the monitoring with SiteScope, you must complete the following steps:

1. Install and configure the agent on the SiteScope system.

2. Set up the SiteScope system as a connected server.

See the **Administration Guide > Monitoring > Policy Templates > Importing SiteScope Templates** for more details.

Adjusting Templates in SiteScope

SiteScope templates contain information about the remote servers or applications that they monitor. This information is usually stored in a variable that is replaced by the list of remote servers or application instances when the template is deployed.

When importing a SiteScope template, the import tool must be able to identify the variable that contains the instance information in order to create a corresponding instance parameter in the resulting policy template. The import tool chooses one the following SiteScope variables, in the order described below, to create the instance parameter:

- The variable with the display order number 0 in the SiteScope template.

- The variable named "host" in the SiteScope template.

> **Note:** If the variable "host" exists in a SiteScope template but does not have a value, the value will be set to %%HOST%% during the template import.

- The variable with the value %%HOST%% in the SiteScope template.

If none of the above variables exist or if the wrong variable would be used as instance parameter, adjust the SiteScope template in SiteScope. In most cases, the easiest way to do this is to change the display order number in the SiteScope template.

> **Note:** System variables starting with $$ (such as $$SERVER_DISPLAY_NAME$$) are not converted and need to be replaced with %%HOST%% before importing the template.

Linux Host
  Linux monitors for $$SERVER_DISPLAY_NAME$$
      CPU Utilization on $$SERVER_DISPLAY_NAME$$
      Filesystem Status on $$SERVER_DISPLAY_NAME$$
      Linux Resource monitor on $$SERVER_DISPLAY_NAME$$
      Memory Utilization on $$SERVER_DISPLAY_NAME$$
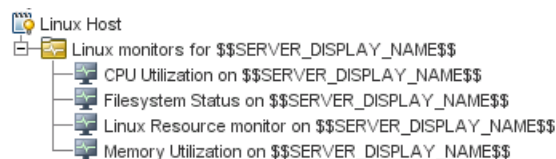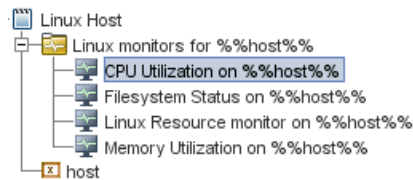
To simplify the import, copy all templates that need to be imported into one template group.

Importing SiteScope Templates into OMi

On the OMi server, open a command prompt and run the ConfigExchangeSIS command-line interface to import templates from a SiteScope server.

For example, the following command loads the templates that are in the template container called "Template Examples" from sitescope1.example.com:

```
c:\HPBSM\opr\bin\ConfigExchangeSIS.bat -sis_group_container "Template Examples"
-sis_hostname sitescope1.example.com -sis_user integrationViewer -sis_passwd
password -bsm_hostname bsm1.example.com -bsm_user admin -bsm_passwd password
-bsm_port 80
```

For more information on importing SiteScope templates, see the **Administration Guide > Monitoring > Command-Line Interfaces > ConfigExchangeSIS Command-Line Interface**.

Grouping Policy Templates into Aspects

After templates are imported, they need to be grouped into meaningful aspects. An aspect is defined for a specific CI Type and contains all policies required to monitor a certain aspect of the CI, for example its performance or availability.

Go to **Administration > Monitoring > Management Templates & Aspects**. Create a suitable configuration folder and add aspects there. When creating an aspect, enter its name, specify the CI Type and select the corresponding policy templates.
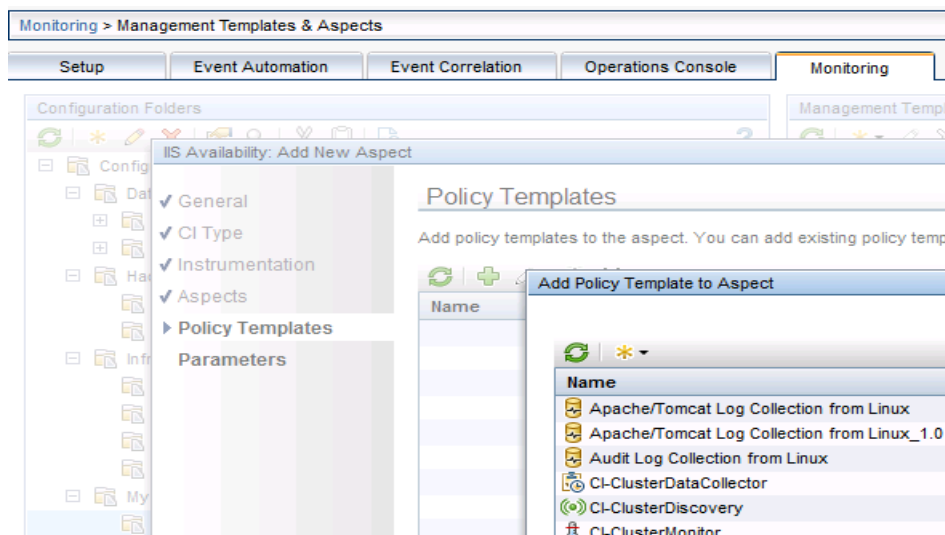
Set Parameter Values Using CI Attributes

In this step, make sure that the instance parameter value is either %%HOST%% (which will be automatically replaced by the corresponding host node name) or that the value is set using a CI attribute that represents the instance. For example, if the SiteScope template is targeted to monitor Oracle instances, the instance parameter will be the Oracle Instance Name. The corresponding Oracle aspect will be defined for the Oracle CI Type and a single Oracle CI will represent an Oracle instance. When defining the aspect, you can use the available information in the RTSM, which already contains the instance name, to set the instance parameter value as shown in the following figure:

General	CI Type	Instrumentation	Aspects	Policy Templates	Parameters

Combine or edit parameters. You can combine similar parameters, and set or override default parameter values.

I	C	UI ...	Name	Default Value
✓	—	0	Oracle Instance Name	CI Attribute: name
—	—	1	Oracle Database Host Name	
—	—	2	Oracle Instance User Name	
—	—	3	Oracle Instance Password	****
—	—	4	Oracle Instance Port Number	CI Attribute: application_port
—	—	5	Oracle Database Availability Frequency	300

You can use other CI attributes, such as application_port, to set other parameters, but you need to make sure that these attributes are filled by your discovery process.

Optional (Recommended): Create Management Templates to Group Aspects

Creating management templates is optional but recommended. Management templates simplify the assignment of many aspects thus allowing to monitor composite applications with a single assignment. To use management templates, the Monitoring Automation for Composite Applications license is required.

To simplify the assignment of multiple aspects, it is recommended to create one or several management templates after all aspects are created. For example, you can create several management templates with different aspects, representing, for example, Essential and Extensive monitoring levels.

Go to **Administration > Monitoring > Management Templates & Aspects**. Create a configuration folder and add there management templates. Enter the management template name, specify a view and root CI Type, and select the corresponding aspects. If you use the management template for grouping aspects belonging to one CI Type, you can select any view that contains this CI Type. The view is used as a starting point for the management template definition. As an alternative, you can also use nested aspects (group several aspects into a new aspect).

To start monitoring multiple related CIs of various CI types using one single assignment, you need to create a management template. As this is not possible using nested aspects, you need to create/select the view that shows all CI Types and their relations as a starting point for the management template. See the **Administration Guide > Monitoring > Management Templates & Aspects > Configuring Management Templates** for more details.

Testing Configuration

Once you created the aspects and management templates, use the manual assignments to test and verify configuration.

You can assign management templates and aspects from **Administration > Monitoring > Management Templates & Aspects** (with the aspect/management template as a starting point) or **Administration > Monitoring > Assignments & Tuning** (with the CI as a starting point).

The assignment will by default initiate an immediate deployment of all included policy templates to the corresponding nodes.

You can verify on the SiteScope Server whether the corresponding monitors have been deployed.

Roll Out Configuration

Once the configuration is validated, you can rollout the configuration to more systems, either manually (if there is only limited change in the environment) or automatically using web-services or automatic assignment rules.

See Roll Out Configuration in the Manage Operations Agents from OMi Step by Step chapter for more details.

Chapter 7: Establishing Reporting Using OBR

Overview

Operations Bridge Reporter (OBR) is a cross-domain performance reporting product. It collects end-user performance metrics from Application Management and infrastructure utilization details from System Management products to provide integrated reports on service and application performance. In order to do this, OBR leverages service topology definitions from the OMi RTSM.

OBR is designed to support pluggable content. Content packs are delivered as modules that can be deployed to an existing OBR instance thus allowing users to tailor their OBR instances to meet their reporting needs. Based on the content deployed, an OBR instance may be used for specific domain reporting needs, such as providing System Management reports.

A Content Development Environment (CDE) enables customers and partners to develop the content for OBR. The development process involves creating metadata artifacts that generate the content. OBR bundles Business Objects for all its enterprise reporting needs.

HPE Reporter and OBR Reports Comparison

Check the Operations Bridge Reporter Content Catalog available on the HPE Live Network Content Marketplace (https://hpln.hpe.com/node/8902/contentfiles) for up-to-date information about available OBR content packs.

The following table shows the comparison of HPE Reporter and OBR Standard Edition reports:

Domain	Report Pack in HPE Reporter	Available in OBR SE (as of August 2014)
System	System	Yes
	Virtualization	Yes
OM SPIs	Oracle, MSSQL	Yes
	Sybase, Informix	Content in BO Universe*
	WLS, WBS	Yes
	SAP	No
	Exchange/AD	Yes
	Lync, SP, BizTalk	No
	Tibco	No
Event	OM	Yes

| Partner SPIs | NICE: Blackberry, PeopleSoft, DB2 | No |
| | Comtrade: CITRIX, Siebel, EMC Documentum | No |

*no out-of-the-box reports available, but data is collected in BO Universe

In addition to the report packs mentioned above, OBR contains additional reports packs (called content packs for OBR) for OMi events, His, and KPIs and collects metric data for OAS and JBOSS.

HPE Reporter and OBR Feature Comparison

Reporter Functionality	Equivalent in OBR
Report scheduling	Yes
Data summarization	Yes
Report customization via Crystal Designer	Yes, using Business Objects
Custom Groups	CMDB Views + Node Groups + user-defined
Time Shift support	Yes
Scalability, 2000 nodes per instance	20.000 nodes per instance
Support external DB (Oracle, MSSQL)	No - OBR embeds Sybase IQ
PA collector	Yes
Data Access Layer (DAL) – SQL	DAL – SQL, BO SDK
Custom extension	CDE
OOTB Process and Logical Volume reports	No
Viewing Reports from the OM for Windows console	OBR reports can be integrated into My Workspace, which allows automatic display of report in context of a CI. It is also possible to set up an OMi URL tool that launches an OBR report in context of a CI on demand.
Collection from multiple OM servers	Yes
High Availability (Microsoft Cluster support)	Veritas HA Cluster
AutoGrouping based on PA configuration metrics	Auto-grouping based on OM node groups and/or RTSM views.
UI for configuring collections (a collection can be configured per group of nodes or single nodes, that is more metrics from group of critical server (s) and fewer metrics from less-critical servers).	All collections are at 5-minute granularity with hourly frequency. Nodes collection can be enabled/disabled.
Agent metrics collected at 1-hour granularity with daily frequency.	Agent metrics collected at 5-minute granularity with hourly frequency.

Report output formats: html, PDF, Excel, Word	Web intelligence (web page), PDF, Excel, CSV Can also send to email, FTP site, and folder.
Operations Agent nodes populated by discovery in user-defined Windows Domain, by manually adding systems, or by OM discovery.	Topology source is either OM or the RTSM. (Special standalone cases exist for VMware-only and for NPS-only scenarios.)
Login security: by default, none. Can implement your own web server security.	Uses Business Objects login security and authorization mechanism

How to Establish Reporting Using OBR

Install OBR

OBR can be installed in multiple deployment modes based on the target environment. See the OBR Installation Guide to determine the deployment architecture suitable for your environment (https://softwaresupport.hp.com/group/softwaresupport/search-result?keyword=).

Install Available Content Packs

OBR ships with a rich set of content packs. In addition, partners and other HPE product teams may create content. These content packs are available for download from the HPE Live Network Content Marketplace site. HPE Live Network Content Marketplace is also the vehicle for releasing off-product cycle content and content upgrades. Depending on your license, you may be entitled to download and deploy these content packs to an existing OBR instance. Visit https://hpln.hpe.com/group/service-health-reporter for more information.

Configure Collections

OBR supports the notion of Remote Collectors. These collectors enable collection of performance metrics from OM agents and other sources from behind a firewall (providing a secure and distributed collection). For more details, see the OBR Installation and Administration guides (https://softwaresupport.hp.com/group/softwaresupport/search-result?keyword=).

Re-Define Custom Shifts

OBR allows users to create time shifts. These shifts are used to summarize and create shift-specific reports. Shifts are defined via the OBR Administration GUI. See the OMi Help topics of the Administration GUI for more details.

Re-Define Custom Groups

OBR interprets RTSM views as groups that may be used in reports. These views serve to group Configuration Items in reports. Similarly, node groups are supported in OM deployments. OBR also enables users to create their own custom groups. These groups are on part with RTSM views or node groups. See the OMi Help topics of the Administration GUI for more details

Use ootb Reports

OBR ships more than 120 out-of-box reports. See the Handbook of Reports for details (https://softwaresupport.hp.com/group/softwaresupport/search-result?keyword=).

Additional Tasks

How to Re-Create Custom Reports Using BO

OBR bundles Business Objects 3.1 (BO) for all its BI requirements. BO provides a browser-based editor to create and edit reports. The data collected, cleansed and aggregated by OBR is stored in Sybase IQ Column DB and is exposed via BO Universe. Each content pack ships with a Universe, which can be used to create reports. To learn more on BO and its usage in OBR, see the following blogs/video at http://community.hpe.com/t5/Business-Service-Management/Jumpstart-report-customizations-using-report-templates-in-HP/ba-p/6308707.

How to Integrate Custom Metrics into OBR Reports

OBR ships with a Content toolkit (CDE) used to build content for OBR. This toolkit accepts metadata input and generates various content pack artifacts, such as collection policies, DB schema, aggregate procedures, and BO Universe. The CDE may also be used to enhance the existing content. See the CDE Guide for details (https://softwaresupport.hp.com/group/softwaresupport/search-result?keyword=).

How to Use Reporter as Gatherer

To simplify the move to OBR, it is possible to continue to use HPE Reporter as data gatherer for some time. OBR can retrieve data from HPE Reporter and combine it with the data from OMi. The OBR generic Database Collector is used to connect to the HPE Reporter DB and gather collected metrics. This can be used to start the Reporter migration projects. However, it is advisable to migrate to the more efficient and extensible OBR collection framework. See the migration toolkit for more details.

Move Agent Collection to OBR

To switch off Reporter, move the agent data collection to the OBR collection framework. A prerequisite for that is to have all agents managed by OMi and discovered and modeled in the OMi RTSM instance. Once all

agents are available as CIs in the RTSM, OBR connects to the RTSM, builds a list of available agents, and schedules periodic collection. The agents in the RTSM have a new CIID, which is now used to identify them. To link the older agent-based IDs in OBR to the new RTSM CIIDs, you can use Data Warehouse Lifecycle tools. See the migration toolkit for more details.

How to Switch the Topology Source from OM to OMi

If you are already using OBR with OM as a topology source, you need to switch to OMi as a topology source. OBR uses agent-based IDs in the OM deployment. These IDs are distinct from OMi RTSM-based CIIDs. To successfully migrate OBR from the OM deployment to the OMi deployment, you need to map older agent-based IDs to their corresponding OMi-based CIIDs. See https://hpln.hpe.com/blog/shr-om-bsm-migration-tool-taking-shr-deployment-om-bsm-topology-scenario-%E2%80%A6 for more details.

Chapter 8: Switching Off OM and Reporter

Preparing to Switch Off OM

Switching All Operations Agents to OMi

If not already done, switch all Operations Agents to OMi. See Complete Switch of an Agent for details.

Removing the Flexible Management Template from Nodes

On the OM server from which you deployed the flexible management template, undeploy the template from all nodes.

If the OM server is no longer available, you can delete the flexible management template from OMi using the `opr-agt -deploy -clean` option. This deletes all old OM policies.

Switching Off Topology and Event Forwarding / Shutting Down OM

You can shut down OM completely. If you want to keep OM running but disconnected from your OMi environment, execute the following steps:

1. On the OM server, undeploy the server-based forwarding policy (which was created when you connected OM to OMi).
2. Remove the OMi server from the topology server configuration.

   - **OM for Windows:**
     i. In the console tree, right-click **Operations Manager**, and then click **Configure > Server**. The Server Configuration dialog box opens.
     ii. Click **Namespaces**, and then click **Discovery Server**. A list of values appears.
     iii. Remove the hostname of the OMi server from the list of target servers.

   - **OM for UNIX and Linux:** Run `/opt/OV/contrib/OpC/enableToposync.sh –stop` to stop all topology forwarding.

Switching Agent Licenses to OMi

To reuse the OS instance licenses previously used on OM, you can import the same license keys in OMi. You can do this for the following licenses:

BB165ZAE, BB165ZA, TB672AAE, TB672AA, TB673AAE, TB673AA, TB674AAE, TB674AA, BB196ZAE, BB196ZA, TA124AAE, TA124AA, TB056AAE, TB056AA, TB969AAE, TB969AA, TB058AAE, TB058AA, TB975AAE, TB975AA, TB057AAE, TB057AA, TB973AAE, TB973AA, TD768AAE, TD769AAE, TD770AAE, TD771AAE, TD772AAE, TD779AAE, TD780AAE, TD781AAE, TD782AAE, TD783AAE, TD773AAE, TD774AAE, TD775AAE, TD776AAE, TD778AAE, TD136AAE, TD136AAE, TD138AAE, TD138AAE, TD137AAE, TD137AAE, TB917AAE, TB918AAE, TB919AAE, TB920AAE, TB921AAE, TB932AAE, TB934AAE, TB935AAE, TB936AAE, TB937AAE, TB938AAE, TB939AAE, TB945AAE, TB966AAE, TB971AAE, TJ721AAE, TJ722AAE, TJ723AAE, TJ724AAE, TJ738AAE, TJ739AAE, TJ740AAE, TJ741AAE.

Other licenses need to be migrated into new licenses. Contact your HPE account team or partner to request the license migration.

Disabling/Deleting Connected Server in OMi

In OMi, go to **Administration > Setup and Maintenance > Connected Servers** and disable or delete the connected server for your OM system.

Event Synchronization / Tool Execution after the Switch Off

Shortly after the switch off, you might still have active events in the OMi Event Browser that have the original OM server as the originating server. When changing events, OMi will still try to synchronize changes to the originating server and the synchronization details will be shown on the Forwarding tab of Event Details. Synchronization problems can be safely ignored. After a few hours, OMi will stop synchronization attempts automatically.

As soon as the OM connected server is disabled or deleted, OMi will no longer route tool executions via the OM server, but execute the tool by contacting the agent directly.

Destroying OM Certificate Authority Private Key

To make sure that agent certificates using the old OM certificate authority (which is still trusted by OMi) can no longer be issued, delete the CA certificate from the OM server that is no longer in use and make sure that all CA certificate copies including the private key (previously exported via `ovcm -exportcacert`) are destroyed.

Switching Off Reporter

Before decommissioning HPE Reporter, verify that HPE Operations Bridge Reporter has taken over the following tasks of HPE Reporter:

- Collecting the required metrics from the HPE Operations Agents and any OM server(s) that are not being decommissioned
- Producing the required reports
- Email integration is configured, if required

If any HPE Reporter web pages are linked into another application, for example a custom portal, update the application to remove references to HPE Reporter.

If HPE Reporter is integrated to an OM for Windows server that is not being decommissioned, remove the integration from the OM for Windows server. The integration is configured under **Configure > Server > HP Reporter Integration**.

If HPE Reporter is integrated to an HPE Performance Manager server that is not being decommissioned, remove the integration from the PM server. Before doing so, be aware that the HPE Reporter integration to PM provides PM with:

- Node and node group list automatically populated from the HPE Reporter database.

- Data source for generating graphs from the HPE Operations Agent metrics in the HPE Reporter database.

After the HPE Reporter integration is removed from PM, any nodes and node groups provided by HPE Reporter are automatically removed from PM. Node and node group management will be done using the PM CLI or GUI. For details, see the HP Performance Manager Administrator Guide available at https://softwaresupport.hp.com/group/softwaresupport/search-result?keyword=.

Verify that PM users are not using any graphs that source data from HPE Reporter.

To remove HPE Reporter integration from PM:

1. Edit *<PM_data_dir>*`/shared/server/conf/perf/OVPMconfig.ini`.

2. In the `[REPORTER]` section, remove or comment out the entries related to the HPE Reporter instance being decommissioned.

3. Restart Performance Manager for the change to take effect (by using `ovpm stop` and `ovpm start`).

Chapter 9: Adding Value on Top

At this point in the evolution process, you already gain a lot of benefits by using of OMi advanced event consolidation, correlation, and automation features. Operators can benefit from the modern UI, the flexible My Workspace pages, and the context-specific actions and graphs. OMi comes with a number of content packs that provide many features free of charge for certain application areas (like Microsoft Active Directory, Oracle Databases, and other).

However, there are situations where you need to correlate more events or show more application-related health indicators or KPIs (in addition to already provided event-related KPIs) or you want to model your logical business services on top of your discovered IT services and applications and use that information to specify the priority of events. In such cases, see the below sections that explain additional tasks.

> **Note:** These tasks can be regarded as optional, depending on your specific business needs.

These additional tasks are explained in the following sections. They should be regarded as optional tasks that you might or might not do, depending on your specific needs.

Modeling Business Services

Modeling your logical business services includes creating business services, business applications, and/or business transaction CIs, as well as linking those logical CIs to the IT services and applications they use.

The following figure shows a logical business service structure and monitored service contributors:
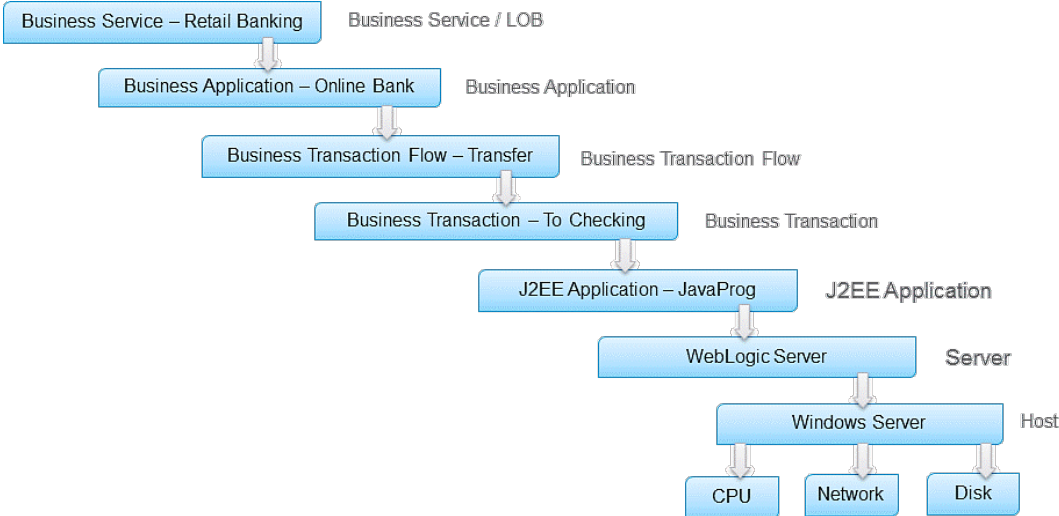
This relates the event information to business services allowing the operational staff to identify and understand the impact of the events on business services and enable them to focus on the most important ones.

To support service-centric management, the RTSM must be extended by defining a model of business services and applications. Such a model must contain a relationship to all relevant CI instances contributing to the business service.

Unlike CI-centric monitoring (where CI instances and relationships are maintained through discovery, integrations, and automatic processes), the modeling of business services and their relations is a manual procedure. It requires a profound understanding of the service and its dependencies to the contributing service elements. Additionally, the structure of the service presentation is service-specific and needs to consider the views on the business service model as required by the user.

For more information on this topic, see the following:

- See the following sections in the **RTSM Guides > Modeling > Modeling Guide > Modeling > Modeling Studio: Building a Business View, Business CI Model, Build a Business CI Model – Scenario**.

- End-to-End Service Monitoring in IT Environment Best Practice. It provides information on how to deploy and implement end-to-end service monitoring solutions to ensure adherence to the level agreed upon between the service provider and the service consumer.

- Moving to Service Centric Management with HP OMi. This technical white paper contains an example Business Service Model and shows how to create corresponding CIs and views in OMi.

> **Note:** When business services are defined and linked to infrastructure services, you can change the following Infrastructure Setting to enable business service/business app CIs to show up as part of events:
>
>
>
> | Resolve Impacted CIs | Resolve impacted CIs in EventPriority Resolution. If set to true, impacted Business Applications & Services will be added as custom attributes to the event. | false | |

Event Priority

Once events and their related CIs impact business services, OMi instantly calculates an additional event attribute allowing to classify events depending on their impact on a business service. The event attribute, Event Priority, can be used to identify the events to work on.

The calculation of event priority is based on the event severity and the business service impact, as shown in the following table:

Business Service Impact	Event Severity					
	Unknown	Normal	Warning	Minor	Major	Critical
No Impact	Lowest	Lowest	Low	Low	Medium	Medium
Low	Lowest	Lowest	Low	Low	Medium	Medium
MediumLow	Low	Low	Low	Medium	Medium	High
Medium	Medium	Low	Medium	Medium	High	High
MediumHigh	High	Medium	Medium	High	High	Highest
High	Highest	Medium	High	High	Highest	Highest

The following figure shows an example business impact of a CI (low):
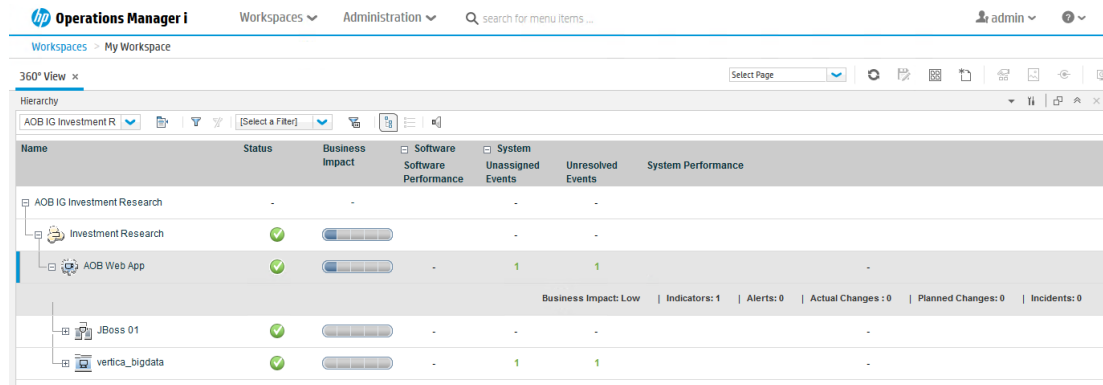
> **Note:** To display the Business Impact information in Service Health 360° View, the business impact bar needs to be enabled in the Service Health infrastructure settings. See How to Configure the Business Impact Component for further information.

The following figure shows an example of the resulting event priority in Event Browser:
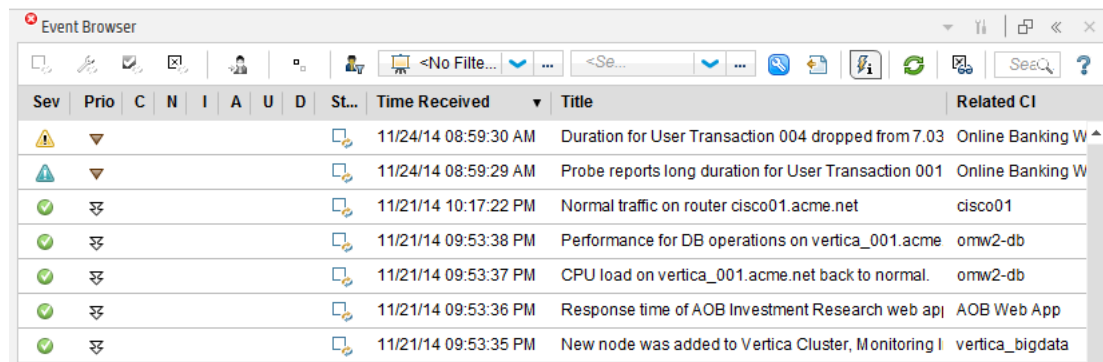
Adding Custom TBEC Rules

TBEC is built on top of Event Type Indicators, as well as on the topology information between the CI instances. This allows TBEC to relate, for example, a "CPU Load high" event related to a node with a "SQL response time slow" event from a database that is running on that same node.

If you want to relate two events with TBEC, you first need to make sure that each event is related to a CI and that both CIs are connected in the RTSM. The relationships between CIs are typically created by discovery. See Establish Infrastructure Topology for more information. Linking events to CIs is achieved through CI hints or using the node, application, and object fields. See the **Administration Guide > Event Processing > Automation > Event Processing Customizations > CI Resolution** for more details.

Additionally, TBEC needs to know the semantics of the event (since you do not want to correlate any event from CI A with any event from CI B). The semantic "CPU Load high" must be represented by an Event Type Indicator (ETI), such as **System restart:Occurred** or **CPU Load:High**. If the events you want to correlate do not contain an ETI, add this information as described in the below section.

Once these preparation steps are done (the two events are related to (connected) CIs and contain ETIs), you can create a new TBEC rule. One possibility is to select the two events in the Event Browser and choose Create Correlation Rule from the context menu.

If you currently do not have two such events available, you can also define the same rule using the TBEC Administration UI: **Administration > Event Processing > Correlation > Topology-Based Event Correlation**.

See the **Administration Guide > Event Processing > Topology-Based Event Correlation > How to Configure Topology-based Event Correlation Rules** for more details.

Adding Event Type Indicators

Add Event Type Indicators that represent the semantics of an event for the following use cases:

- As input for TBEC
- As input for Service Health if the ETI represents a Health Indicator (HI)

Such ETIs/HIs must first be defined in OMi and can then be set at the source of the event or by using an ETI mapping rule on the OMi server. HIs can also be set by metric samples (see below sections for more information).

To define a new ETI, go to **Administration > Monitoring > Indicators** and see the corresponding OMi Help topics.

To set ETIs, set the ETI Event Attribute in the corresponding OMi policy template:

If still used, you can also set the custom message attribute **EventTypeIndicator** (or **ETIhint**) inside an OM policy:
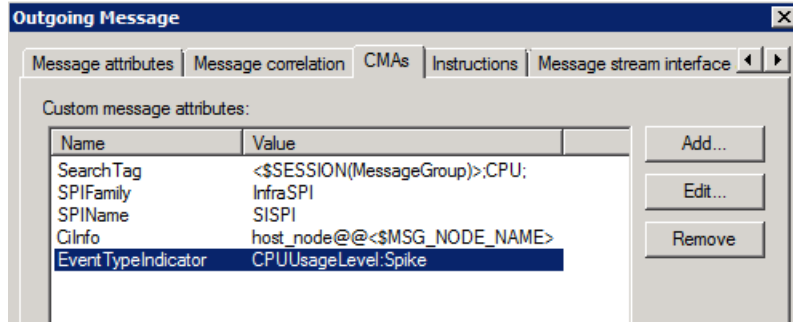
As an alternative, ETIs can also be set on the OMi server when the event arrives using an ETI mapping rule. Go to **Administration > Monitoring > Indicators**. Select the CI type for which the ETI was defined. In the ETI details, select **Go to Indicator Mapping Rules**:
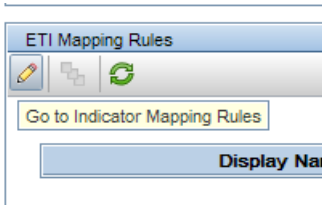
The following figure shows Indicator Mapping Rules Manager:
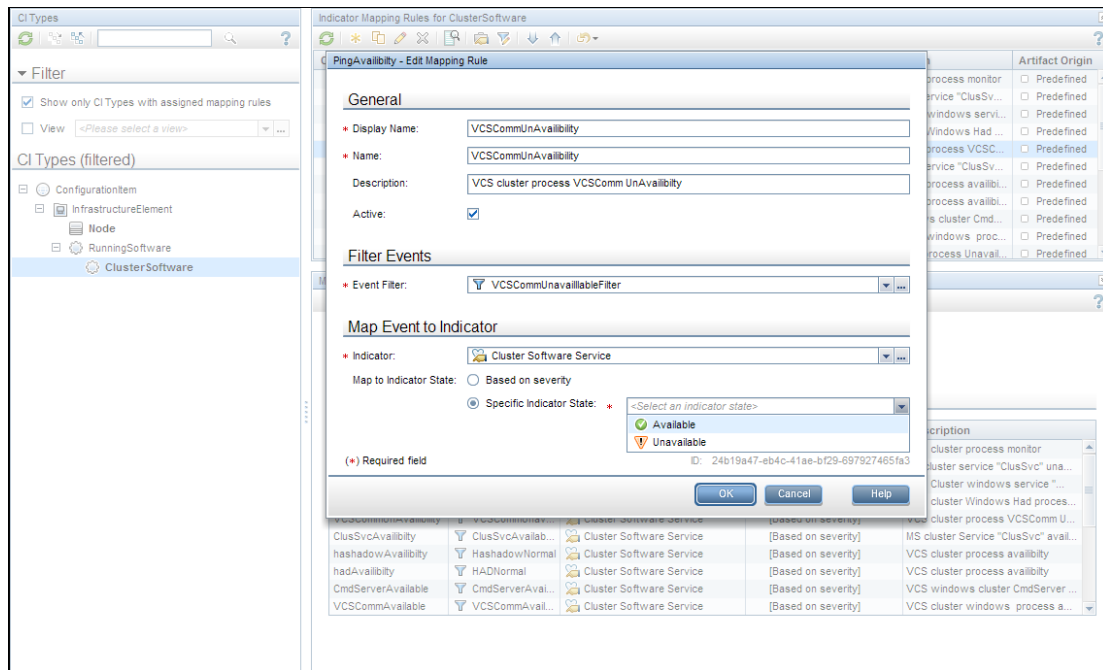
See the **Administration Guide > Event Automation > Indicator Mappings** for more details.

Adjusting Service Health

Service Health Overview

Service Health provides similar features as OM Service Navigator, as it enables you to monitor the availability and performance of the applications and services in your organization.

Applications and services are represented as CIs in the RTSM and Service Health can show the hierarchy of CIs using predefined views. A view acts like a filter and retrieves only certain CIs from the RTSM for display.

Service Health shows the hierarchy of the CIs and the CI status. Each CI has a CI status and can have one or multiple Key Performance Indicators (KPIs) representing the high-level CI status, such as its performance or availability. Each KPI can be fed by one or multiple Health Indicators (HIs), representing the fine-grained measurements on the CI.

Unlike OM Service Navigator that only knows one service status, Service Health calculates multiple HIs and KPIs representing the status.

A KPI status is propagated from a child to a parent CI according to the propagation definition, when the parent and child CIs are linked by either Impacted By (Directly) or Impacted By (Potentially) calculated relationship.

KPI status propagation is defined in KPI propagation rules, also known as group rules. These group rules determine the KPI status based on the data received from other KPIs or HIs. The received data can come from the KPIs of child CIs or from other KPIs or HIs associated with the same CI. See the **Administration Guide > Service Health > Customizing KPI Propagation** for more details.

The following figure shows KPIs and HIs displayed in the Health Indicator component:
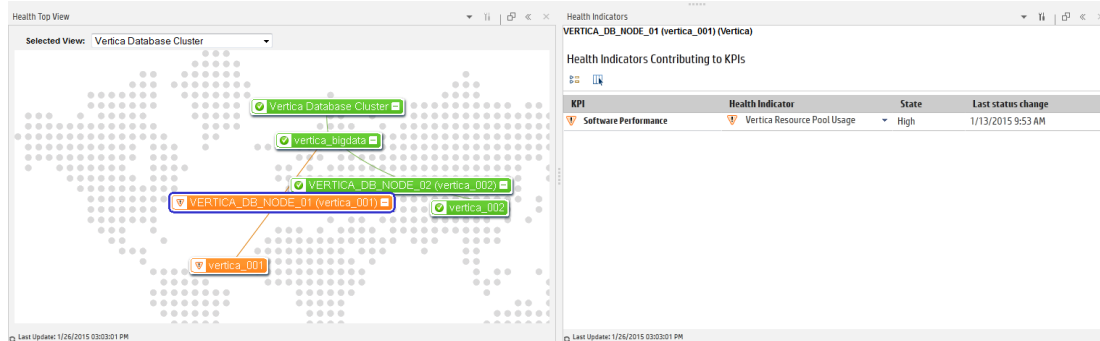
The following figure shows the CI status and KPIs displayed in the Watchlist component:
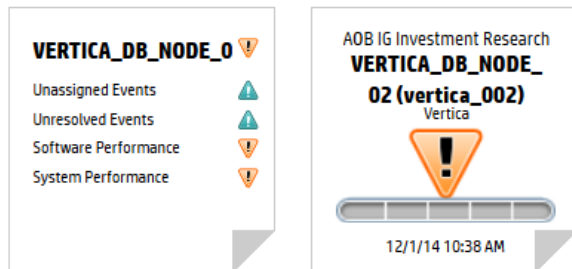
KPI calculation rules can be changed and extended. See the **Administration Guide > Service Health > Customizing KPI and HI Calculation Rules** for more details.

Out-of-the-box content packs contain many HI and KPI definitions and many KPI calculation rules that can be used as a starting point.

Health Indicators

Health indicators (HIs) provide fine-grained measurements on the CIs that represent your monitored applications and business services. Some HIs provide business metrics, such as backlog and volume, while other monitor various aspects of performance and availability, such as CPU load or disk space.

The following figure shows a Health indicator definition with possible HI states:
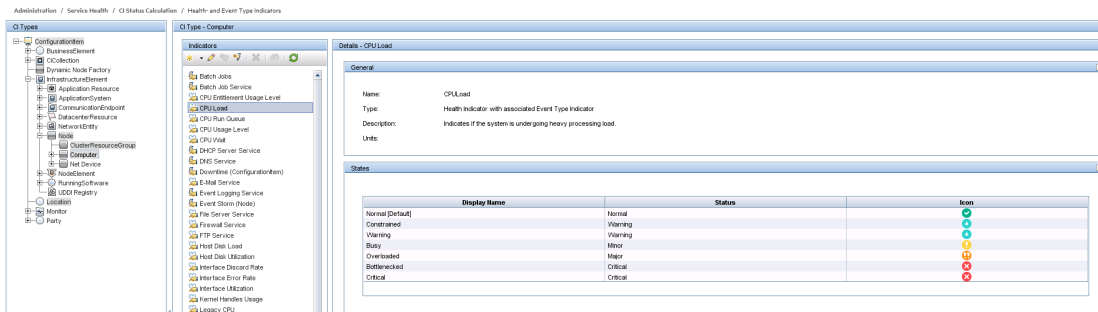
In OMi, HIs can be set via events. When an event is sent to Service Health inside OMi, it is sent with an ETI (Event Type Indicator). The ETI includes a name, a state and an optional metric value, for example **CPULoad:exceeded** or **CPULoad:exceeded:98**. Using HI definitions in the indicator repository, Service Health translates the ETI state into one of the standard Service Health statuses (Critical, Major, Minor, and so on).

> **Note:**
>
> - An HI maintains its state until another event arrives that sets the same HI with a different state.
>
> - To reset the HI manually to its default value, close the corresponding OMi event with **Close and Reset Health Indicator**. In normal production environments, OMi expects a good event that resets the HI.

Key Performance Indicators

Key Performance Indicators (KPIs) are high-level indicators of CI performance and availability, which apply calculation rules to the data provided by HIs to determine CI status. KPIs can be calculated using statuses of HIs, KPIs, or a combination of these. For example, you can specify a rule that sets the severity of the KPI to the worst severity status of any assigned HI, or to the average severity status of all child KPIs.

The following figure shows a KPI assignment displaying HIs contributing to the KPI status:
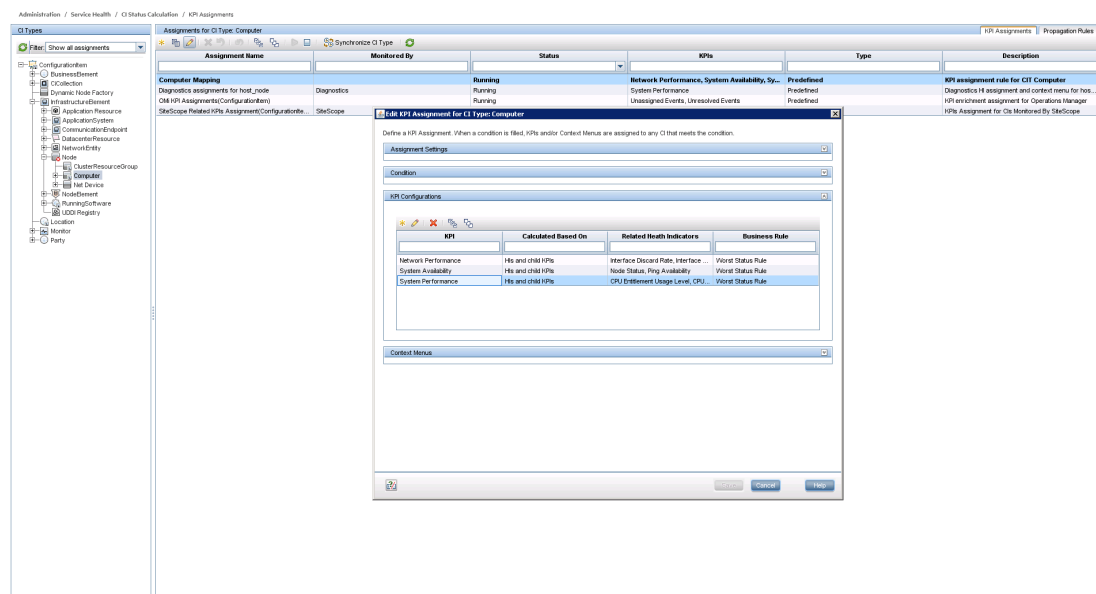
The value that results from the calculation is used to set a severity level for the KPI based on the KPI definitions; KPI severity can be normal, warning, minor, major, or critical. The resulting measurement for the KPI is translated into a color-coded status indicator displayed in Service Health, where the color represents a more desirable or less desirable condition for the KPI.

You can define a KPI to use only specific HIs that are of interest to you. For example, the System Availability KPI has two HIs: Node Status and Ping Availability. If you are only interested in the local status, you can set the KPI to include the Node Status HI only in its calculation.

Note: An HI is created when the first event with a corresponding ETI arrives. Therefore, it can happen that many of your CIs do not show any HIs or KPIs as long as no problems are reported.

Unresolved and Unassigned Events KPIs

An Unresolved Events KPI shows the most critical severity of related events and the event count (an Unassigned Events KPI shows the same for the unassigned events).

Therefore, the Unresolved Events KPI can be seen as the equivalent of the service status in OM. It changes its status when new events with higher severity arrive or when events are closed. No configuration is required, as these KPIs are automatically created for all CIs that receive events.

However, unlike in OM, these event-related KPIs are not propagated by default. This is the intended behavior, as it is often not desired that a single event of unknown semantics for a low-level CI impacts the CI status of a higher-level business service CI. Therefore, OMi by default does not propagate the event-related KPIs, but propagates all other health-related KPIs instead.

To propagate event-related KPIs, see follow the instructions described in the **User Guide > Introduction > Health > HI-Based KPI Calculations > How to Propagate and Sum Up the Events Along the CI Impact Hierarchy**.

You can also count active events (unresolved and unassigned) for a specific event subcategory. For example, an Unresolved Security Events KPI can be configured to display the number of unassigned or unresolved security events. For details, see the **Administration Guide > Additional Configuration > Active Event Count in KPIs**.

CI Status

The CI status can be configured per view and is the worst status of all selected KPIs. To configure which KPI contributes to the CI status, go to **Administration > Service Health > KPIs in Views**. Select the view and then select the KPIs.

The following figure shows KPIs included in the CI status:

See the corresponding OMi Help topics for more details.

Appendix A: Agent Management

Deploying Agents

OM allows installing agents remotely using various technologies, such as telnet, SSH/SCP, Windows DCOM, Windows shares.

OMi does not offer remote deployment. Agents can be installed manually (and also remotely using such technologies as SSH/SCP) or using other software deployment tools, such as HPE CDA (see https://hpln.hpe.com/blog/hp-operations-agent-can-be-deployed-cda-and-csa for more information) and HPE Server Automation or Microsoft Systems Center 2012 Configuration Manager (see HP Operations Agent and HP Operations Smart Plug-ins for Infrastructure Installation Guide for more information).

Once the agents are installed using one of the above methods, they can be updated with hotfixes and patches from OMi.

Patch and Hotfix Deployment

OM can deploy agent patches and hotfixes remotely. OMi can deploy patches and hotfixes remotely and can deploy new agent versions if the agent is already installed.
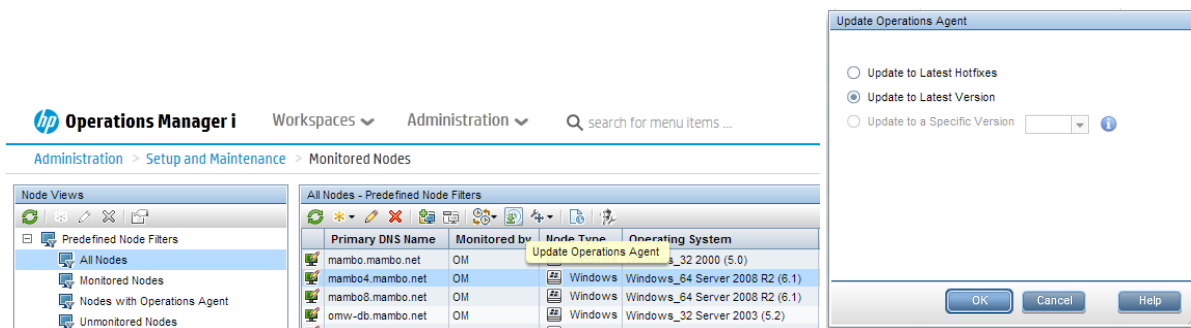
For details, see the **OMi Administration Guide > Setup and Maintenance > Monitored Nodes > Connecting HPE Operations Agents to OMi > Updating HPE Operations Agent Installations**.

Certificates Handling

Certificate requests from agents can be granted in the OMi UI (**Administration > Setup and Maintenance > Certificate Requests**) or using the command-line interface ovcm as on OM systems.

OMi supports granting certificates automatically based on IP ranges, node names, or using other attributes via groovy scripts.

Maintaining Agents

Many CLIs that exist in OM, such as `ovpolicy` or `ovconfpar`, are provided in OMi as well. You can use them to perform operations on a single node. To perform mass operations on multiple nodes, use the `opr-agt` command-line interface. See the **Administration Guide > Monitoring > Command-Line Interfaces > The opr-agt Command-Line Interface** for details.

Starting and Stopping Agents

Use the following OMi CLI to check the agent status or to start/stop the agent:

`ovrc with options –start|-stop|-status|-restart|-notify`

`opr-agt with options -status|-start|-restart|-stop`

Examples:

`ovrc -ovrg server -host mynode.example.com -status`

`opr-agt -status –view_name "Hosts with HPE Operations Agents" -username admin`
`opr-agt -status –node_list node1.example.com,node2.example.com`

Agent Configuration Changes

Use OMi CLIs `ovconfget`, `ovconfpar` and `opr-agt` to list and change the agent configuration.

Examples:

`ovconfpar -change -host mynode.example.com -src-ovrg server -ns eaagt -set OPC_BUFLIMIT_SIZE 10000`

`opr-agt -set_config_var eaagt:OPC_BUFLIMIT_SIZE=10000 –node_list node1,node2`

Policy Management

Use the `ovpolicy` CLI to list and change installed policies. Use `opr-agt` to list installed policies.

Examples:

`ovpolicy –list –host mynode.example.com –ovrg server`

`opr-agt –list_policies –view_name "Hosts with HPE Operations Agents" –username admin`

Installed Agent Packages

Use the `ovdeploy` CLI to list installed agent packages.

Example:

`ovdeploy -inv -host mynode.example.com -ovrg server`

Monitoring Agent Health

OM servers are able to ping agents regularly and report when the agents no longer respond. OMi provides the capability to check and report agent health as well. Default health check settings check the health every 30 minutes, the interval can be changed per node.

Additionally, self-monitoring policies on OM ensure that problems with the agent own core components do not compromise its ability to monitor managed nodes. Using the self-monitoring feature, you can easily identify if the OVO agent is working correctly by configuring the agent to poll its own core components and generate an alert if problems are detected.

These self-monitoring policies are not shipped out of the box with OMi, but can be imported and deployed if required. See the sections below for details.

Besides that, the `ovc` process on any agent automatically restarts aborted or killed agent processes and sends corresponding events to its management server.

Using Operations Agent Self-Monitoring Policies

Using the OM self-monitoring feature, you can establish if the OVO agent is working properly by configuring the agent to poll its own core components and generate an alert if it detects any problems. Although OMi does not ship these self-monitoring policies, you can import and use them in OMi.

Some policies use `$OPC_MGMTSV` as an operator-action target and run `ovrc` on the OM server to restart certain agent processes. These actions must be changed to run `ovc -restart` locally on the node itself (which works as long as the action agent is working properly).

In OMi, create a wrapper around imported policies by creating a self-monitoring aspect for the HPE Operations Agent CI Type and assign it to the HPE Operations Agent CIs. This will deploy all included self-monitoring policies with a single assignment.

Supported Agents

OMi can receive events from all Operations Agents v.11.0x and later (Operations Agents v.8.6x were previously supported by OMi but reached the end of support phase).

To use OMi Monitoring Automation features, Operations Agents version 11.12 or later is required.

OM and OMi Feature Comparison

OM Functionality	Equivalent in OMi
Start, stop, status, version, switch a primary manager, set variables on agents using `opcragt`.	Yes, using `ovrc`, `ovconfpar`, `opr-agt`.

OM Functionality	Equivalent in OMi
Mass operations (start, stop, status, version, switch a primary manager, set variables) on agents using `opcragt -all -nodegroup`.	Yes, mass operations (start, stop, status, version, switch a primary manager, set variables) on agents using `-query`, `-view`, or `-nodegroup` options of `opr-agt`.
Deployment of agents.	No, use HPE CDA or other Software distribution tool.
Deployment of patches.	Yes, integrated into OMi. Latest patches can be deployed using the Update Operations Agent function.
Deployment of hotfixes (only possible using a hotfix deployment tool).	Yes, integrated into OMi. Latest hotfixes can be deployed using the Update Operations Agent function.
Supports download of policies and instrumentation files (`opctmpldwn` and `opcinstrumdwn`), which can be included in the base agent package.	No, but aspects and management templates (including policies and instrumentation files) can be automatically deployed as soon as the agent is connected to the OMi server.
Query detailed installed agent packages.	Yes, using `ovdeploy`. The HPE Operations Agent version is also displayed in the Monitored Nodes UI.
Supports OA 11.0x and later.	Yes.

How to Manage Agents from OM and OMi

Using agent-based flexible management policy templates, OMi and OM systems can be configured as action-allowed and secondary managers, which allows configuration and management of agents from both OM and OMi servers. However, HPE recommends that you avoid deploying policies from two servers to the same node as this may complicate the move of agents. Instead, use the flexible management template to prepare the switch to OMi.

See the **Administration Guide > Setup and Maintenance > Monitored Nodes > Connecting HPE Operations Agents to OMi** for more details.

How to Switch Agents from OM to OMi

Recommended: Switch Agents Using a Flexible Management Template (Using Existing Certificates)

Switch the agents to OMi using a flexible management template as described in Manage Operations Agents from OMi Step by Step. Using this approach, you can continue monitoring business-critical applications on the node and replace its configuration while the agent is running.

Below is the summary of recommended steps:

1. Allow management from both servers using a flexible management template.
2. Choose a group or type of nodes to move over (for example, all my Oracle Database systems).

a. Test policy and aspect deployment and tool execution on a representative node.

b. After a successful test, rollout configuration to the remaining nodes of the same type.

c. Switch the primary manager and target server to OMi. This still allows configuration from both OMi and OM servers.

```
opr-agt -primmgr <node selection> -username <user>
```

3. Repeat steps 2-5 until all nodes are managed by OMi.

4. Before switching off the OM server, switch the agents to OMi completely:

```
opr-agt –switch_manager <node selection> -username <user>
```

and clean up old OM policies if necessary:

```
opr-agt –deploy -clean <node selection> -username <user>
```

Caution: At this point, the node still has a certificate issued by the old OM server and is configured to trust both OMi and OM server certificates. However, as the primary manager was changed and the flexible management template removed, the old OM server no longer has rights to make changes on the agent. Therefore, there is no need to re-issue or replace agent certificates. The OM certificate authority can be completely shut down and the private key can be destroyed.

However, you can also request new agent certificates. See the below section for more information.

Alternative: Switch Agents Completely or Issue New Certificates

To request new certificates and switch the agent completely, execute the following commands on each node:

1. Log in to the node as root or administrator.

2. Stop the agent completely:

```
opcagt -kill
```

3. Delete the current certificate:

```
ovcert –list
```

```
ovcert –remove –alias <id of node certificate returned in previous step>
```

4. Go to the following location:

   ○ On Windows 64-bit nodes: *<ovinstalldir>*\bin\win64\OpC\install

   ○ On other Windows nodes: *<ovinstalldir>*\bin\OpC\install

   ○ On HP-UX, Linux, and Solaris: /opt/OV/bin/OpC/install

   ○ On AIX: /usr/lpp/OV/bin/OpC/install

5. Run the following command:

   ○ On Windows: cscript oainstall.vbs -a -configure -srv *<fqdn of omi server>* -cert_srv *<fqdn of omi server>*

   ○ On UNIX/Linux: ./oainstall.sh -a -configure -srv *<fqdn of omi server>* -cert_srv *<fqdn of omi server>*

6. Grant certificate requests on the OMi server using the Admin UI or ovcm.

7. Deploy aspects and management templates to start monitoring again.

Note: After executing the above-described procedure, all existing policies are deleted and the agent is shut down. To continue monitoring your business-critical applications, the agent needs to be reconfigured by OMi.

Appendix B: Node Management

Node-Centric and CI/View-Centric Approach

In OM, System and Application Management is based on a node-centric approach. Many tasks, such as tool launch or policy deployment, refer to the nodes, a list of nodes, or node groups. Node groups are also referenced when defining responsibilities for operators.

In OMi, the approach is CI-centric, or view-centric. Responsibilities are defined using views (see the **Administration Guide > Users** for more details) and operators typically work with CIs of various CI types (such as business applications, running software, databases, web servers, and so on). The node that hosts the CIs is not as important as in OM, as operators can launch tools or deploy aspects to CIs directly, without knowing what nodes are affected. Mass deployment to nodes through node groups in OM is replaced in OMi by deployment of aspects to views and automatic deployment of aspects based on the RTSM changes (such as new CIs, deleted CIs, and new relationships between CIs). Therefore, node groups, although they do exist in OMi (as CI collections), do not play a special role.

To simplify the move to OMi, OM operators can use the OM CI collection view to filter the events based on node groups. Node groups/CI collections can be created and updated automatically in OMi, if nodes are no longer managed by OM.

However, in order to benefit from all CI-centric features of OMi (CI-specific tools/run-books, CI-specific graphs, and so on), it is recommended that OMi operators switch from a node group-based approach to a view-based approach (rather sooner than later).

Nodes in OM have attributes, such as machine type, control type, and other, for example:
'machine type' = 'linux/x64/linux26' and 'control type' = 'controlled'.

Some node-related functionality is linked to the node attributes, for example:

- The attribute 'machine type' determines the agent packages to be installed.
- The attribute 'control type' (OM for UNIX) determines the level of management capabilities available for the node.
- The attribute 'virtual' allows deployment and tool execution to/on virtual nodes in an HA environment.
- A node can be set up as an external node with a pattern, resulting in all messages that match that pattern being assigned to that node.

Nodes in OMi are represented as CIs of type Node (or a sub-type such as `Computer`, `Windows`, and so on). Node CIs have attributes (for example, primaryDNSName or monitored_by) and relationships to other CIs in the RTSM (for example, an IP address CI or HPE Operations Agent CIs). A node with a Composition relationship to an HPE Operations Agent CI represents a node with an installed agent. For such nodes, the monitored_by attribute contains the value OM, but a node can also be monitored by other applications, such as SiteScope or BSM Connector.

OMi Evolution Guide
Appendix B: Node Management

The following figure shows a typical node CI with related CIs in the RTSM:
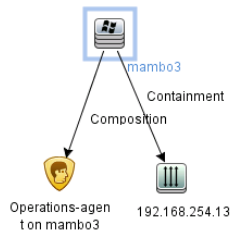
The following figure shows some attributes of nodes in the RTSM:

Display Label	DiscoveredOsName	Monitored By	PrimaryDnsName	CI Type
IA3	Windows Server 2008 6.0	[OM]	IA3.mambo.net	nt
LoadBalancer			LoadBalancer	lb
RpClusRG				cluster_resource_group
mambo3	Windows Server 2008 (6.0)	[OM, SiteScope]	mambo3.mambo.net	nt
mambon95	Windows Server 2008 R2 (6.1)	[OM, SiteScope]	mambon95.mambo.net	nt
mambon96	Linux Red Hat 6.1 2.6.32	[OM]	mambon96.mambo.net	unix
omw2-db (Management Server)	Windows Server 2008 R2 (6.1)	[OM]	omw2-db.mambo.net	nt
oo	Windows Server 2008 R2 6.1	[OM, SiteScope]	oo	nt
oradb3	Windows Server 2008 R2 6.1	[OM]	oradb3.mambo.net	nt

Node Setup

In OMi, node CIs and related CIs are typically created automatically. Such CIs are created when the HPE Operations Agent is first installed and connected to the OMi server. Node CIs are also created using topology synchronization from OM or using various discovery technologies.

Caution: There is no need to set up nodes in advance as in OM.
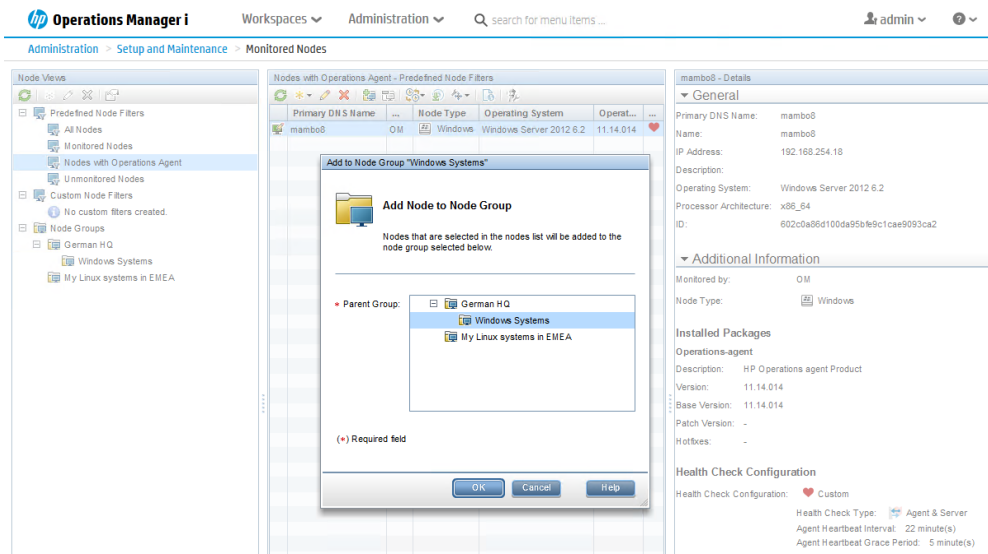
If nodes are not created automatically, you can create CIs using the Monitored Nodes UI. This UI was introduced to simplify viewing and maintaining node CIs and can also be used to add nodes to node

collections (CI collections) manually. Starting with OMi 10, it also allows configuring health checks and updating agents.

How to Change the Hostname or IP Address of a Managed Node

Once the node CI and its related CIs are created, if you later want to change the hostname or the IP address of the node, it is highly recommended that you manually update the details in OMi before making changes on the node. Otherwise, the node will send the updated IP address and hostname to OMi, which can result in a duplicate node CI, due to the CI reconciliation rules in the RTSM that require a 66% match of the IP addresses (if a node has only one IP address, there is a 0% match of IP addresses when this address changes).

To change the hostname or IP address:

1. In OMi, go to **Administration > Setup and Maintenance > Monitored Nodes**.

2. Edit the node and change the hostname and/or the IP address. Click **OK**.

3. Change the hostname and/or IP address on the managed node.

Virtual Nodes

OM uses virtual nodes in cluster-based, high-availability environments to simplify policy deployment. Policies can be deployed on a virtual node and are automatically deployed on all physical nodes related to that virtual node/IP address. Policies are enabled only on nodes that run a corresponding resource group.

> **Note:** This functionality is currently not supported for cluster-based monitoring.

External Nodes

OM uses external nodes to map incoming messages from various systems to one single node. This is required in the following scenarios:

1. When the node name is unknown.

2. When nodes must not be individually configured, for example, due to the number of nodes that must be set up.

Operators in OM can select an external node and see all events from corresponding nodes.

In OMi, events are received and can be shown to operators even if they are not related to a node in the RTSM. Such operators must be granted the right to view the events independent of a view filter. Therefore, it is not necessary to set up an external node to view the events.

To map certain events to specific, external nodes/CIs in order to allow operators to filter these CIs, create the CIs manually and use CI resolution hints to ensure that events are mapped to the right CIs.

CI resolution hints can be added on the OMi server using an EPI script that extracts the node information in the event, compares it against a string or pattern, and sets the CI hint accordingly (see How to Implement External Nodes in OMi below for details).

Node Group, Node Layout Group, Node Hierarchy, and CI Collection

In OM, you can group nodes into node groups, which can be used for mass policy deployment and mass tool execution, as well as to define user responsibilities and filter the events. You can mark node groups as hidden.

In OMi, tool execution is done on CIs, mass policy deployment is replaced by manual or automatic RTSM-based aspect deployment, and user responsibilities are defined using views. Therefore, the only use case where node groups can be beneficial is filtering the events.

Node Groups Versus Views as Means to Structure the IT Environment

In OM for Windows, node groups can be nested to build a hierarchy. In OM for UNIX, this is not possible, but it offers the concept of node layout groups and node hierarchy to organize the nodes into a logically structured view.

Conceptually, node groups and node layout groups in OM are a means to group and structure monitored objects/nodes to cope with the large amount of objects in the IT environment.
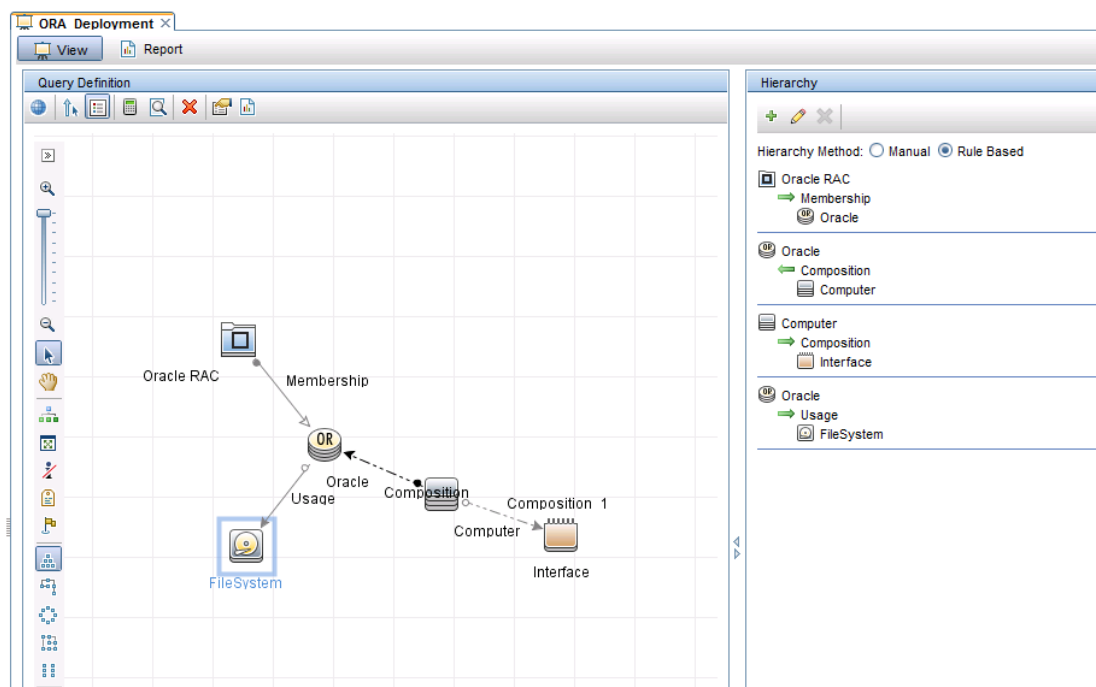
In OMi, the structure of monitored objects (configuration items) is represented in the RTSM using relationships. RTSM views retrieve and display CIs and relationships. The displayed hierarchy is defined by the view definition. Using different views, operators can have a more flexible view on their IT environment than with node groups where the structure is rather static and restricted.

OMi operators can switch between various views and use views and contained CIs as a filter. Therefore, it is not necessary to use node groups or layout groups as filters.

However, to simplify the transition, OMi automatically creates CI collections that represent the OM node group hierarchy. This hierarchy is created and updated using topology synchronization from OM. This hierarchy can be displayed and used for filtering using the out-of-the-box view **OM CI Collections**. This is very useful when OM and OMi are used side by side.
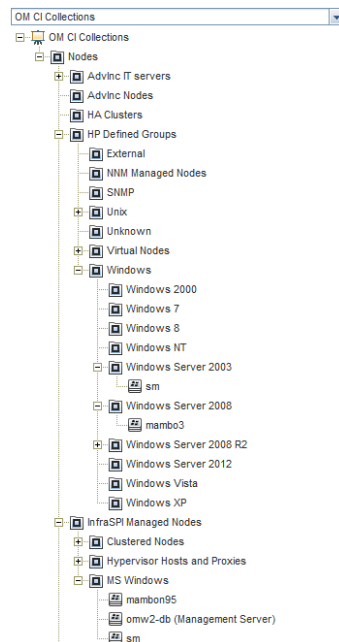
The underlying relationships in the RTSM (which CI/Node belongs to which CI Collection/node group) are updated using toposync whenever changes occur on the OM side.

However, those group relationships are not created or updated automatically, because node groups do not play a special role in OMi.

How to Move Node Topology to OMi/Topology Synchronization

Nodes and the node group hierarchy of OM are forwarded to OMi respectively RTSM together with the services hierarchy using topology synchronization. For details, see the **Extensibility Guide > Populating the Runtime Service Model > Topology Synchronization Overview**.

For OM for Windows, use default configured toposync packages that include the nodegroups synchronization package. For OM for UNIX, use toposync packages **layoutgroups** and **nodegroups**.

You can configure the synchronization package in **Administration > Setup and Maintenance > Infrastructure Settings**.

Select **Applications** and use the list to set the administration context to Operations Management. Scroll to **Operations Management - HPOM Topology Synchronization Settings**.

The following types of topology data related to node management can be transferred from OM to the RTSM:

OM topology data	Related OM Type	Resulting CI type(s) and Relationships in the RTSM
Node	OM for UNIX and Linux, OM for Windows	Node, Computer, Unix|Windows, other <operating system>. Path in CI type tree: Managed Object -> ConfigurationItem -> InfrastructureElement -> Node -> Computer -> Unix | Windows | … Mapping: External node -> Node Node with the operating system specification -> Computer or operating system-related CI type, for example Unix, Windows, and so on. Virtual node -> „virtualized_system" added to "node_role" attribute
Node group	OM for UNIX and Linux, OM for Windows	CI Collection and relationships between CI collections and node CIs Path in CI type tree: Managed Object -> ConfigurationItem -> CICollection
Node hierarchy	OM for UNIX and Linux	CICollection
Node layout group	OM for UNIX and Linux	CICollection

The following figures show synchronized node hierarchy examples from OM for Windows (Node Groups) and OM for UNIX (Node Layout Groups):
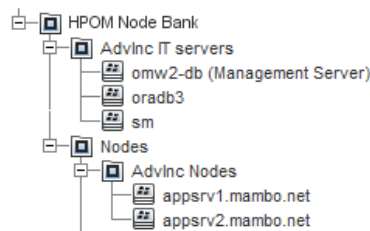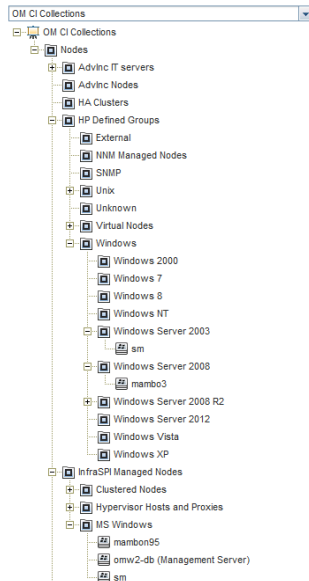
Note:

- Sub CI types of 'Node' are 'ClusterResourceGroup', 'Computer', and 'Net Device'.

  ○ External nodes are set up as 'Node'. This is also true for the following machine types: IP Network -> other -> other, non IP -> other -> other, as well as 'Node on external Events'.

  ○ OM (non-external) nodes are set up as CI Type Computer. When the operating system information of OM nodes is available, the corresponding CIs are assigned to CI Type subgroups of the CI Type Computer labeled with the operating system version. The other two sub CI Types have (at this point in time) no relevance for OM entities.

  ○ Although the 'Net Device' CI Type exists in the RTSM, toposync does not synchronize devices like routers, network printers, and so on.

- Not all attributes of nodes and node groups are transferred using toposync into the RTSM. The OM node attribute 'Control Type' is ignored by OMi.

- All node groups are transferred to CICollections, also if they are marked in the OM responsibility matrix as hidden.

How to Implement External Nodes in OMi

This step is required if you want to map events from various nodes to one specific external node/CI, so that operators can get a list of those external events by selecting the corresponding CI.

Create a CI (of any type) that acts as an external node. The following example uses a node CI, because it can be easily created using **Administration > Setup and Maintenance > Monitored Nodes**. Other CIs can be created using **Administration > RTSM Administration > IT Universe Manager**.

> **Note:** If you created an external node in OM and used topology synchronization, you already have an external node CI that you can use as a related CI, so you can skip Step 1.

Example:

- Step 1: Create a generic node (Node Type: Node) and provide a node name (for example, MyExternalNode1.example.com). Specify the IP address, since all nodes in the RTSM require an IP address. Use the IP address not used by any real node.

  Review the node properties and copy the node ID as it will be used in the next step.

- Step 2: Create an Event Processing Customization/ EPI script for the step Before CI/ETI resolution.

  Copy the below code into the Script tab and replace *<id of CI that acts as external node>* with the ID of the CI you have created. Change `NODE_SUFFIX` according to your needs. This example script maps all events from nodes with that suffix to the external node CI. You can implement more sophisticated checks using Java regular expressions.

  ```
  import java.util.List;
  ```

```
import com.hp.opr.api.scripting.Event;

import com.hp.opr.api.scripting.ResolutionHints;


class SetCIHintBasedOnNodeSuffix

{

  // This script can be used to replicate the external node functionality that exists
in HP Operations Manager for Windows/Unix.

  // It maps events from nodes of a certain domain to one specific CI that acts as
"external node".

  // More sophisticated checks can be implemented using Java regular expressions.

  // This is the generic CI to which all events will be related (related CI of event)

  static def EXTERNAL_CI = "UCMDB:<id of CI that acts as external node>"

  // this is the domain – all events from nodes with DNS name that matches
*.example.com will

  static def NODE_SUFFIX = ".example.com"

  def init()

  {

  }


  def destroy()

  {

  }


  def process(List events)

  {

    for (event in events)

   {

        def nodeHints = event.getNodeHints();

        def nodeName = nodeHints.getDnsName();

        def newhint = EXTERNAL_CI

        if(nodeName != null && nodeName.endsWith(NODE_SUFFIX))

          event.setRelatedCiHint(newhint);

    }

  }

}
```

> **Tip:** As an event filter, set up a filter that looks for events without CI hints. This way, the events that already have a CI hint are neither overwritten nor processed by the EPI script.
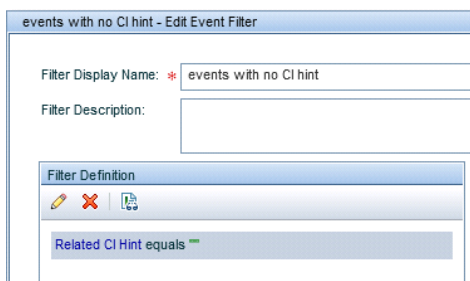
Final EPI Script in **Administration > Event Processing > Automation > Event Processing Customizations**.
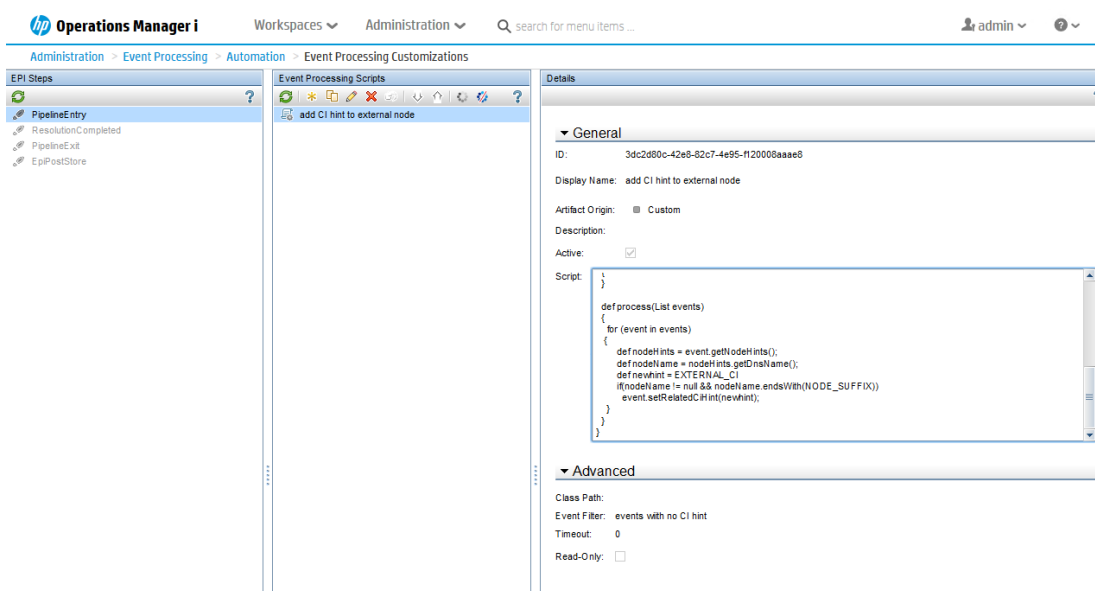
- Step 3: Add relationship to a CI collection

  The predefined view **OM CI Collections** does not automatically show all nodes, but only the nodes that belong to OM node groups. To see the newly created external node in the view, create a relationship to the External node group using the IT Universe Manager. Select the new CI and choose **Relate to CI** from the context menu. Search the CI collection "External" in the **OM CI Collections** view and create a membership relationship from the CI collection to the node.
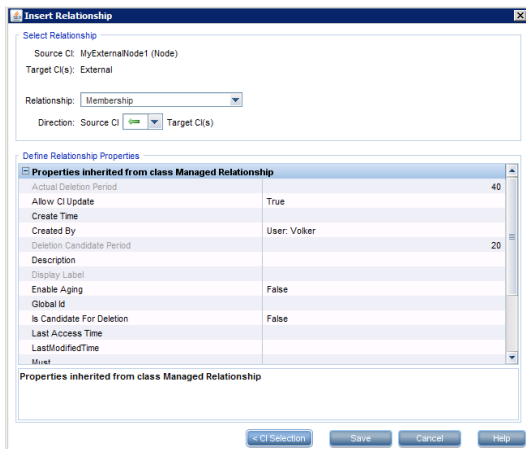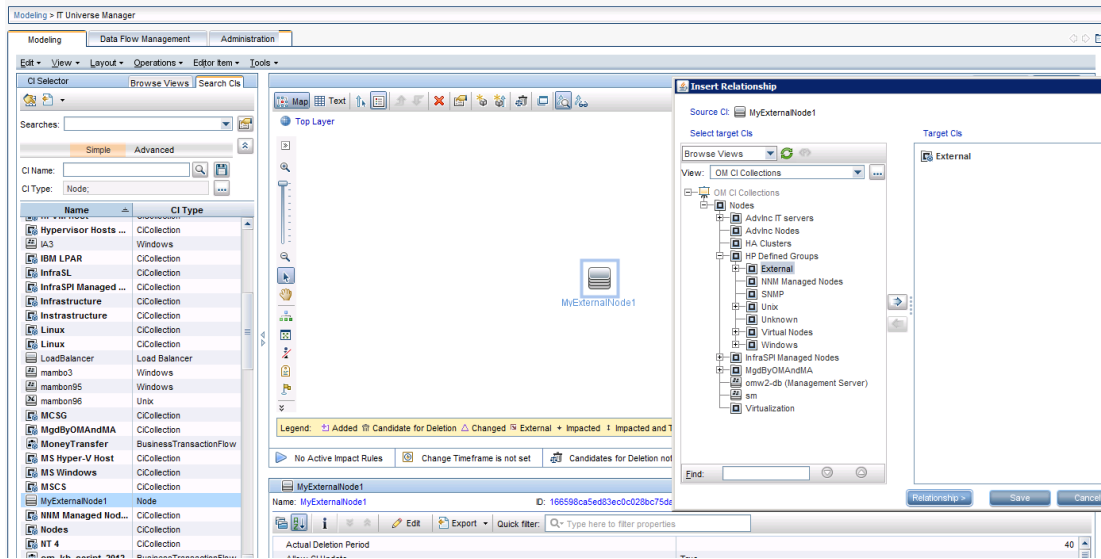
The operators can now select the external node CI in the **OM CI Collections** view and get the corresponding events as in OM:
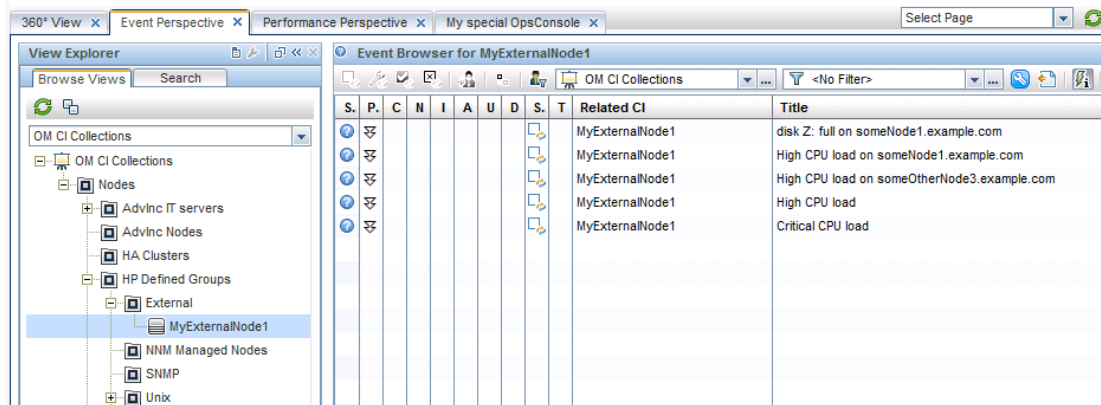
Appendix C: Command Line, API, and Web Services Reference

User Tasks

User tasks are outlined in the following table.

Event Handling and Tool Execution

Functionality	OM for UNIX	OM for Windows	OMi

External event manipulation	**CLI**
	
	`opcack, opcackmsg, opcackmsgs, opcmack` (agent CLI), `opcunack`
	
	`opcannoadd, opcannoget`
	
	`opccmachg, opcownmsg, opcmsgchg`
	
	`opcdelmsg`
	
	`opcgetmsgdet, opcmsgsrpt`
	
	API
	
	All operations on a message can be done with the OM Server Message API. OM for UNIX provides a C API.
		CLI
		
		`ovowmsgutil`
		
		`opcmack` (agent CLI)
		
		Create a VB script using WMI methods.
		
		API
		
		All operations on a message can be done with the OM Server Message API. OM for Windows provides a C API and COM API.
			CLI
			
			`RestWsUtil` CLI allows accessing all the Event Web Services functions from the command line.
			
			Web services
			
			REST-based Event Web Service allows all event modifications in the console. It also allows creating events (starting actions and retrieving instructions are not possible).

	Web services Get, create, and update events. Close, reopen, own, dis-own events. Get, add, update, and delete annotations. Add, update, and delete Custom Message Attributes. Start, stop automatic or operator-initiated actions. Get the instruction text for an event. Get notification for changes on events.		
Tool execution	**API** Application API to execute Tools.		
	Web services Launch a Tool within the operator's responsibility. Run arbitrary strings, run commands on an OM agent. Commands types: executable, Perl script, VBScript, JavaScript, or Windows Scripting Host script. Asynchronous requests/ result handling. WSMAN calls, payload in SOAP format. Trigger predefined tool calls. Use a "subscribe" call to wait on multiple requests. Call list for open requests.		**Web services** Action Web Service: Run arbitrary strings. Run commands on OM agent. Command types: executable (default), Perl script, VBScript, JavaScript, or Windows Scripting Host script. Asynchronous requests/ result handling. REST-based. Trigger a command on multiple hosts. Poll for requests with execution context ID. Requests can be routed to another server when needed. Requests can be canceled. **CLI** `opr-agt -cmd`

Administration Tasks

Administration tasks are outlined in the following tables.

Events

Functionality	OM for UNIX	OM for Windows	OMi
Export/Import events	**CLI** opcactdwn, opcactupl opchistdwn, opchistupl	**CLI** ovowmsgutil	**CLI** opr-archive-events[.bat|.sh] Downloads closed events, based on date range, severity, and node from the DB. Uploading archived events is not supported. opr-export-events[.bat|.sh] and opr-import-events[.bat|.sh] support exporting and importing all or selected events in any lifecycle state.
Delete queued event	**CLI** opcdelmsgs		

Agents

Functionality	OM for UNIX	OM for Windows	OMi
Agent prerequisite check		**CLI** ovowreqcheck **API** COM API methods to check node prerequisites.	**CLI** Not applicable.
Install agent software	**CLI** inst.sh		Not applicable.
Installed agent software setting	**CLI** opcsw		Not applicable.

| Remote agent commands | **CLI**

opcragt, ovrc

ovdeploy, opcdeploy

ovpolicy

ovcodautil

ovconfpar

API

Distribution API - distribute configuration (policies, actions, commands, monitors) to specific agents. | **CLI**

opcragt, ovrc

ovdeploy, opcdeploy

ovpolicy

ovcodautil

ovconfpar

API

COM API methods for administering agents remotely:

• get, set primary manager

• start, stop status of agent

• get agent version

• get, set config variable | **CLI**

ovrc,

opr-agt[.bat\|.sh]

Exceptions:

No -cleanstart. Use alternative remote command, such as ovdeploy, to perform opcagt – cleanstart.

ovdeploy

ovpolicy

java –jar jcodautil.jar

ovconfpar |

Users

Functionality	OM for UNIX	OM for Windows	OMi
User/Profile Management	**CLI** opccfguser **API** User configuration API - create, change, delete, list users, change user responsibilities, (de-)assign tools/tool groups User profile configuration API - create, change, delete, list profiles, (de-)assign tools, tool groups, responsibilities, profiles	API COM API methods	User Management Web Services and opr-user CLI

Manage user sessions	**CLI** listguis opcwall disable_java_gui, enable_java_gui opckilluiwww		

Configuration Objects

Functionality	OM for UNIX	OM for Windows	OMi
Tools/Tool groups	**CLI** opcappl **API** Application configuration API - create, change, delete, list, start tools and tool groups. Application group configuration API - create, change, delete, list tool groups, (de-)assign tools to tool groups.	**CLI** ovowtoolutil	**CLI** ContentManager [.bat|.sh] exports/imports content packs including tools. Content pack definition is done using the GUI.
Message groups	**CLI** opcmsggrp **API** Message group configuration API - create, change, delete, list message groups	**CLI** ovowmsggrouputil	

Services	**CLI**
	
	`opcservice`
	
	`opcsvcattr`
	
	`opcsvcdwn`, `opcsvcupl`
	
	API
	
	Service Navigator Interfaces and APIs:
	
	• XML Data Interface to write or get service configuration directly into or from the service engine via a file system socket.
	
	• C++ APIs of the service engine to register for service status changes
		CLI
		
		`ovowserviceutil`
			API
			
			UCMDB APIs (Java and Web Services)

Nodes/Node groups	**CLI**
	
	`opcnode`
	
	`opclaygrp`
	
	API
	
	Node configuration API - create, change, delete, list nodes and node groups, (de-)assign policies to nodes and node groups, change node type, (de-)assign nodes to node groups.
	
	Node hierarchy configuration API - create, change, delete, list node hierarchies and layout groups, get/move nodes and layout groups
		CLI
		
		`ovownodeutil`
			Other Automation
			
			`opr-node`
			
			Views and CiCollections– UCMDB API or enrichment rules to create relationships.
			
			UCMDB API to query/update CIs.
			
			OMi auto-assignment rules manage dynamic policy assignment/deployment.

Policies/Policy groups	**CLI**
	
	`opcpolicy`
	
	`opctempl`
	
	API
	
	Policy configuration API - get, set and change policies/policy groups, and (de-)assign to policy groups.
		API
		
		PMAD APIs - COM methods policies for handling:
		
		• Policy groups
		
		• Policy types
		
		• Packages
		
		• Nodes (including agent profile generation)
		
		• Deployment jobs
			CLI
			
			`ConfigWsTool`
			
			- (de-)assign and list management templates, list deployment jobs for management templates
			
			Web Services
			
			Monitoring Automation web services:
			
			• List management templates.
			
			• List deployment jobs created as a result of management template assignments.
			
			• Get status and parameter information for an assigned management template.
			
			• List, create, update, and delete management template assignments.
			
			Other automation
			
			OMi auto-assignment rules manage dynamic policy assignment/deployment.

Policy types	**CLI** `opcpoltype` **API** Policy type APIs - create, change, delete, list policy types.		
Change username and password for Measurement Threshold/Scheduled Task/WMI policies		**CLI** `ovpmpwutil`	

Message regrouping	**API** Message regroup condition configuration API - create, change, move, delete, list message regroup conditions	Not applicable.	**Other Automation** Not applicable. Can change message groups programmatically using EPI Groovy scripts, TBEA, SBEC, Event web service.
Instrumentation categories	**CLI** `opcpolicy` `opcinstrumcfg` **API** Category Configuration API - create, change, delete, list instrumentation categories, list and (de-)assign categories to nodes, policies, policy groups		

General Administration

Functionality	OM for UNIX	OM for Windows	OMi
Downtime handling	**CLI** `opccfgout`	**CLI** `ovownodeutil` `ovowserviceutil`	Web Services REST-based web service for downtime allows you to retrieve, update, create, and delete downtimes.
Node name/IP changes	**CLI** `opcchgaddr` `opc_node_ change.pl`		**API** UCMDB APIs (Java and Web Services) **Other Automation** Managed by agent sending ASSD information, which translates into updates in the RTSM.

Download/upload configuration and configuration exchange between servers	**CLI**
	
	`opcpolicy,`
	`opctempl`
	
	`opccfgdwn,`
	`opccfgupld`
	
	`opcinstrumdwn`
	
	`opctmpldwn`
	
	`opccfgsync`
	
	`opc_sis_`
	`template2pol`
		CLI
		
		`ovpmutil`
		
		`ovowconfigutil`
		
		`ovowconfigexchange`
		
		`ImportPolicies`
			CLI
			
			`ConfigExchange`
			`[.bat|.sh]`
			
			`ConfigExchangeSiS`
			`[.bat|.sh]`
			
			`ContentManager`
			`[.bat|.sh]`
			exports/imports content packs. Content pack definition is done using the GUI.
			
			Other Automation
			
			Use the OMi GUI to create a scheduled sync of CIs/relationships between the RTSM(s) and the UCMDB.

Server cloning	**CLI**
	
	`om_server_`
	`switch.sh`		

Server processes status, stop, start	**CLI** `opcsv, ovc`	**CLI** `vpstat, ovc`	**CLI** `run_hpbsm` (Linux), `SupervisorStop.bat` and `SupervisorStart.bat` (Windows), `opr-support-utils [.bat|.sh], ovc`

Self-monitoring: server and node	**CLI**
	
	`opchealth`
	
	`opchbp`
	
	`opchc.sh`
			Other Automation
			
			Use OMi Server Health page to view status

GUI start-up message	**CLI** `opcuistartupmsg`		
Server config settings	**CLI** `opcsrvconfig`		

Troubleticket / Notification	**CLI**
	
	`opctt`
	
	`opcnotischedule`
	
	`opcnotiservice`		

Flexible management	**CLI**
	
	`opcmomchk`
	
	`ovconfchg`
			Not applicable, since data is not created in files, so no explicit syntax check is required.

Certificate handling	**CLI**
	
	`opcsvcertbackup`
	
	`ovcm`
	
	`opccsa`
		CLI
		
		`ovcm`, `ovcert`
			CLI
			
			`ovcm`, `ovcert`

Licensing	**CLI**
	
	`omlicreporter`
	
	`ovolicense`
	
	`OVOLTTest`
	
	`opcremsyschk`
		CLI
		
		`omlicreporter`
		
		`ovolicense`	

Troubleshooting/Support	**CLI**
	
	`itochecker`
		CLI
		
		`ovsuptinfo`
			CLI
			
			LogGrabber (`saveLogs.sh` or `go.bat`)
			
			`opr-checker[.bat|.pl]`
			
			`sendEvent[.bat|.sh]`

(Re-) initialize database content	**CLI**
	
	`opcdbinst`
	
	`opcdbinit`		

Database password tool	**CLI** `opcdbpwd`		

Utilities	**CLI**
	
	`mib2policy`
	
	`opcpat`
	
	`BBCTrustServer.sh`
		CLI
		
		`mib2policy`
		
		`opcpat`
		
		`BBCTrustServer.bat`
			CLI
			
			`BBCTrustServer [.bat|.sh]`

Performance Manager

Functionality	OM for UNIX	OM for Windows	OMi
Start, Stop, License	**CLI** ovpm	**CLI** ovpm	Performance Dashboard is part of OMi so there is no need for separate user and node management.
Generate graphs	**CLI** ovpmbatch	**CLI** ovpmbatch	

Appendix D: Preconfigured Reports

Overview

OM provides preconfigured reports in addition to those provided in HPE Reporter and HPE Operations Bridge Reporter. These reports are mostly focused on OM configuration and are designed for use by an OM administrator. Similar reports are available in OMi Monitoring Automation.

OMi reports are HTML-based, with hyperlinks to quickly navigate from one report to another. OM for Windows reports are HTML-based. OM for UNIX reports are mostly ASCII-based. However, there are six HTML-based reports accessible in the Admin UI.

OM supports creating your own custom reports by directly querying the database tables (OM for UNIX and OM for Windows) or through WMI queries (OM for Windows). Although it is possible to query the OMi database, this is not supported in OMi, since the OMi database schema is not published and it may change in a future product version.

OM and OMi Preconfigured Reports Comparison

The reports in this table include preconfigured reports. Additional configuration information is available from command-line tools, such as `opcpolicy`, `opcnode`, `opclaygrp`, `opchbp`, `listguis`, `oainstall.sh`, `opcservice` (OM for UNIX) or `ovownodeutil`, `ovowmsggrouputil.vbs`, `ovdbstat` (OM for Windows).

> **Note:** License reports and audit reports are covered separately under their respective sections.

Report Area	OM for UNIX	OM for Windows	OMi
Nodes, Node Groups, CIs	Lists nodes, with node type and HBP settings. Lists nodes not in the Node Bank. Reports the status of security certificates assigned to all managed nodes. Detailed report for a selected node, includes type of node, HBP	Lists policies, agent package version, and component versions for each node.	Node Configuration report compares the monitoring configuration of a selected node to the actual state. It lists the aspects and policy templates assigned to the node and reports if the actual state on the node is different. CI Configuration report for a selected CI or all CIs in a view reports the assigned aspects (includes the aspect name/version, enabled/disabled, parent object, and other information). Comparison report compares the monitoring configuration of a selected CI with the

	settings, node group membership, policy, and policy group assignments.		monitoring configuration of all CIs of the same type in the current view. It lists the equal assignments, additional assignments, and missing assignments.
	List node groups and node membership.		User-defined view-based RTSM reports of selected CI attributes. Output to CSV, XLS, PDF, XML, Browser.
	Detailed report for a selected node group that lists the message group/operator assignments and policy/policy group assignments.		
	Lists nodes that are not a member of any node group.		
	Lists nodes that have no policies assigned to them.		
	Lists nodes that are not part of any user's responsibilities.		
	Lists node groups that have no policies assigned to them.		
	Lists node groups that are not part of any user's responsibilities.		

Events	Reports the number of active messages per message group.	Save selected events to a file (TXT, CSV).	Export selected events to a file (XLSX, XLS, CSV).
	Reports a list of active, history, or pending messages for an operator.		
	Exports selected messages to a text file or a drag and drop to another application, such as Excel.		
Users	Lists operators including a summary of permissions.	None	None
	Per-operator detailed report lists the permissions assigned directly and assigned using the profiles.		
User Profiles	Lists profiles.	None	None
	Lists permissions configured for a specific profile.		
Policies, Policy Groups	Lists all policy groups and policies.	Lists policies that are in use and the nodes they are installed on.	Inventory report lists all management templates, aspects, and policy templates.
			Aspect Assignment report shows the CIs assigned to a selected aspect.
			Management Template Assignment report shows the CIs assigned to a selected management template. This report also includes CI assignment details.

Agent Binaries	None	Lists agent package versions and the nodes they are installed on. Lists agent component versions and the nodes they are installed on.	N/A
Services	None	Lists services including their calculation and propagation rules.	None
Message Groups	Lists message groups that are not part of any user's responsibilities.	None	None

Appendix E: Auditing and License Reporting

Overview

OMi and OM provide auditing and license reporting.

Auditing

Both OMi and OM are capable of auditing configuration and event changes. Audit entries contain information indicating what kind of action took place, who performed it, when, and the audit area it concerns.

The primary source of OMi audit log data is displayed in **Administration > Setup and Maintenance > Audit Log**. It includes the following OMi-related audit contexts:

- **Operations Management.** Displays the actions related to Operations Management, such as creating and modifying content packs, event rules, and notifications.
- **User/Group Management.** Displays the actions related to adding, modifying, and deleting users and user groups.
- **Permissions Management.** Displays all actions related to assigning permissions, roles, and permission operations on resources for users and user groups.
- **Recipient Administration**. Displays the actions related to modifying information about the recipients of audit logs.
- **Downtime/Event Scheduling.** Displays the actions related to creating and modifying downtime and scheduled events.
- **Database Management.** Displays the actions related to creating, deleting, and modifying users and passwords for profile databases, as well as modifying the status of the Purging Manager.
- **Notification Template Administration.** Displays the actions related to modifying open-ticket information, ticket settings, closed tickets, ticket templates, and subscription information: notification types (locations or general messages), and recipients.
- **Service Health Administration.** Displays the actions related to configurations made in Service Health Administration.

For details on event changes and configuration changes that are written to the audit log, see the **Administration Guide > Setup and Maintenance > Audit Log**.

Some event audit data is available in the History tab of the event in the Event Browser. In addition to being a convenient event-centric view of changes, this can provide some additional information, such as the old and the new value for an attribute when an attribute value has changed.

CI change data is available in the RTSM. It provides a CI history, such as CI creation time, set or changed attributes, added or deleted relationships, as well as other information.

The following figure shows an example of CI configuration changes in the RTSM IT Universe Manager:
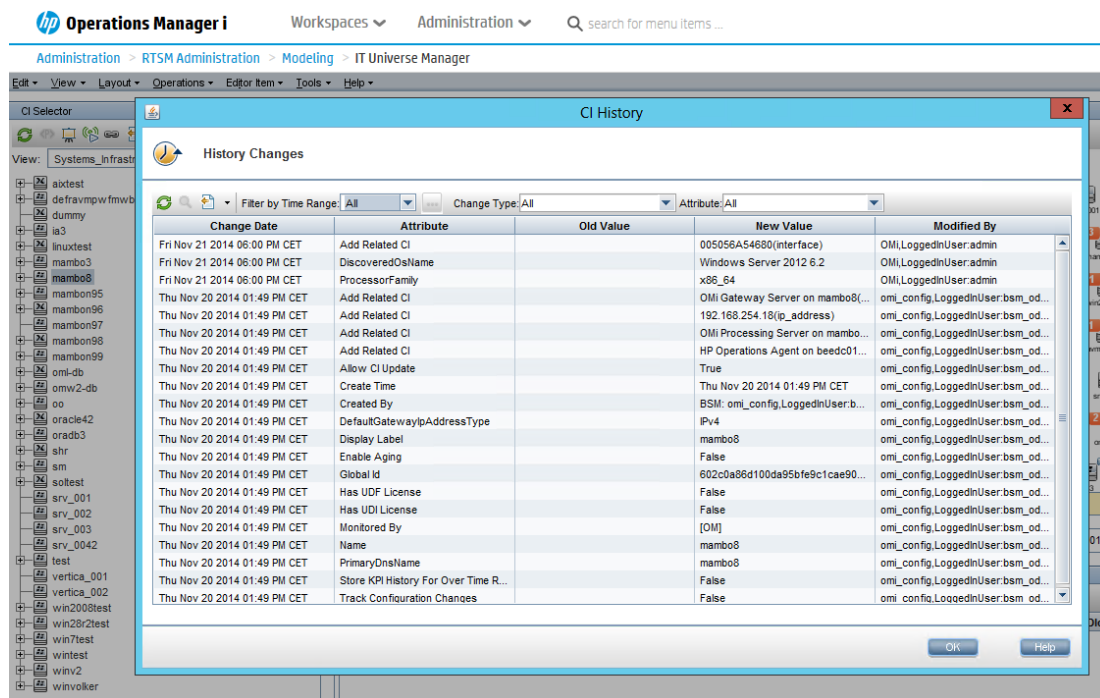
OM and OMi Auditing Functionality Comparison

The following table compares auditing functionality in OM and OMi.

Functionality	OM for UNIX	OM for Windows	OMi
Stored format	Text file, delimited	Windows Event Log	Text file, delimited
Visualization	OM for UNIX Admin UI displays Admin UI formatted audit log. View OM audit log with a text editor.	Windows Event Log	OMi GUI, with the ability to filter by context, user and time frame

Authorization required to change audit settings	Root user	OM for Windows administrator A Windows administrator must restart OM processes for changes to take effect.	OMi administrator An operating system administrator must change log4j settings.
Restrict access to audit data	File permissions	Standard Windows Event Log security	OMi user permissions
Configurable audit levels	Fine-grained audit levels on a per-operation type basis	Fine-grained audit levels on a per-operation type basis	Limited configurability. **Admin > Platform > Setup and Maintenance > Infrastructure Settings**, **Operations Management**, offers two settings for the OMi audit: Configuration or All (both configuration and event changes).

License Reporting

In OMi, you can view the current license details and usage in **Admin > Platform > Setup and Maintenance > License Management**. You can also query the installed capacity using the JMX console.

The following figure shows an example of the OMi license usage:

Name	License Type	Days Left	Expiration Date	Capacity	Capacity Details
⊞ Service Health Analyzer					
⊞ RUM					
⊞ BPM					
⊟ Operations Management					
— Event Management Foundation	Time-based	287	04/05/2015	Not Applicable	Not Applicable
— Topology-Based Event Correlation	Time-based	287	04/05/2015	Not Applicable	Not Applicable
— Target Connector	Time-based	287	04/05/2015		Used 0 Connector(s) out of 10
— Operations Agent	Time-based	455	19/10/2015		Used 9 Agent(s) out of 10
— Monitoring Automation for Composite Applications	Time-based	287	04/05/2015	Not Applicable	Not Applicable
— Business Process Insight	Time-based	287	04/05/2015		Used 0 Business Process(es) out o...
— Management Pack	Time-based	455	19/10/2015		Used 5 OS Instance(s) out of 25

In OM, administrators can run a license report on demand. OM for Windows provides tools to generate and display reports in the HTML or ASCII format. OM for UNIX provides command-line access to generate reports.

OM and OMi License Reporting Comparison

The following table compares license reports in OM and OMi.

OM	OMi
The "OM Feature License Report" shows the license status of each OM license type (OM Server, Agents, Target Connectors, SPIs). It includes the number of installed licenses, the number of required licenses, and a license compliance status.	For the supported license types (OMi Server, Operations Agent, Target Connector, Management Pack), the equivalent information is reported.
The "OM License Password Report" lists all installed OM license passwords for each OM license type (OM Server, Agents, Target Connectors, SPIs). It also includes the number of licenses per license password.	Not available.
The "OM Node License Report" shows the license requirements of each managed node. This data is reported by the managed nodes and also includes node attributes, such as CPU count and operating system version details.	While the managed node reports this data to the OMi server and is stored in the OMi database, there are no out-of-the-box reports.

The OM server performs a license check at start-up time and every 24 hours thereafter. License violations are reported in the OM Message Browser. OM can be configured to email an ASCII license report if it exceeds a configured severity threshold that is checked on a daily basis.

OMi does not provide email notification of license compliance and does not generate an event for license violations.

Calculating License Consumption

OMi reports consumption levels of three types of licenses: Agent, Management Pack, and Target Connector.

The HPE Operations Agent reports its license requirements to the primary manager (OM or OMi) on a daily basis. This includes both agent license and if it is configured with a management pack. This data is stored in the OM or OMi database.

OM calculates Target Connector usage on a daily basis. OM for UNIX provides a command-line tool that you can run at any time to output the usage for the last 30 days, which you can average to determine the overall usage for license compliance purposes. HPE also provides a Target Connector license check utility that can be used with OM for UNIX and OM for Windows to list the nodes that may require a Target Connector license. For further details, see the HP Operations Manager "Licensing Best Practices and Reporting" available at https://softwaresupport.hp.com/group/softwaresupport/search-result?keyword=.

OMi calculates Target Connector usage in the same way on a daily basis. However, no such commands or utilities are available in OMi. The Agent, Management Pack, and Target Connector data is stored in the OMi database.

> **Note:** It is not always possible to programmatically determine if a Target Connector license is required. For example, if the node is already licensed through another HPE Software product, the Target Connector license may not be required. If the node is a single-purpose device, such as a switch, router, UPS, or printer, the Target Connector license is not required. In OM, you can exclude these nodes from the license check by setting appropriate variables in the tclfilter namespace. Such exclude functionality does not exist in OMi.

Appendix F: Available Integrations and Integration Technologies

Overview

OM integrates with various applications from HPE and other vendors using a variety of different technologies and interfaces. Many HPE product integrations are provided for OMi as well (see the detailed list below). Several BSM Connectors are provided to integrate third-party domain managers in OMi. Additionally, all integrations using standard operations agent policies (opcmsg, opcmon, SNMP, logfile, and other) can be technically reused as HPE OMi supports the same policy types.

HPE and HPE partners may provide additional integrations in the future.

"Southbound" Integrations Using Operations Agent Policies

OMi supports the following OM policy types:

- ConfigFile - not used for integrations
- Flexible Management - not used for integrations
- Logfile Entry
- Measurement Threshold
- Node Info - not used for integrations
- Open Message Interface
- Scheduled Task
- Service Auto-Discovery - not used for integrations
- Service/Process Monitoring - not used for integrations
- SiteScope - not used for integrations
- SNMP Interceptor
- Windows Event Log
- Windows Management Interface

Technically, all integrations using supported policy types can be reused in OMi. However, depending on the vendor and the license agreement, you may or may not be able to reuse the OM integration with OMi.

The following policy types can also be imported into a BSM Connector, which offers the additional possibility to integrate topology and metrics:

- Open Message Interface
- SNMP Interceptor

The following OM policy types are not supported (typically, they are not used for integrations):

- ECS (Event correlation, event composer)
- RAS (Remote action security)
- subagent (OM for Linux)
- Server-based MSI (OM for Windows)
- Server-based Flexible Management (OMi uses connected servers and forwarding rules)
- Server policies (OM for Linux)

Official HPE Integrations

For a list of integrations available for OM for UNIX , OM for Windows, and OMi, visit http://support.openview.hp.com/sc/solutions/index.jsp#tab=tab3.

In most cases, OMi offers identical or enhanced integrations. Check the Solution & Integration portal for up-to-date integration information, as new integrations might be added over time.

Existing Integrations into OM	Equivalent Integrations into OMi
Integrating with: ArcSight Logger	
[464] Event correlation and event pattern analysis (OMW - ArcSight Logger) V1.0 1.0 [618] Event correlation and event pattern analysis (OMU - ArcSight Logger) 1.0	For event analytics, see [704] Operations Analytics – Operations Manager i integration 2.0.
Integrating with: Operations Analytics	Identical.
[725] Operations Analytics – Operations Manager Data Collection integration 2.0	[704] Operations Analytics – Operations Manager i integration 2.0
Integrating with: Asset Manager	Identical. Using the UCMDB (RTSM) – Asset Manager integration.
[141] CI Inventory Replication via Connect-It (AM-OMW) 1.0	[616] UCMDB to AM Push Integration 2.0 [307] Asset to CI Replication (AM -> UCMDB) 1.1 [414] Business Service Reconciliation via Connect-It (AM <- UCMDB) 1.2 [420] Asset CI Federation for ITSM (AM -> UCMDB) 1.1
Integrating with: Network Node Manager i software	Enhanced.

[26] Incident Exchange (OMW - NNMi) 2.0 [657] Incident Exchange (OMU - NNMi) 2.0 [305] NNMi Integration with Operations Manager (NNMi - OMW) 2.5 [622] NNMi Integration with OMU/L (NNMi -> OMU) 3.0 [656] NNMi Integration with OMU/L (NNMi - OMU) 2.5 [347] NNMi Integration with OMW (NNMi -> OMW) 3	[344] Network to BSM operations management integration (OMi - NNMi) 1.0 [812] View NNMi UI components within OMi
Integrating with: OO / OO Content	Enhanced.
[35] OO to HP Operations Manager (Incident Web Service) (OO Content-OMW) 3.0 [615] OO to HP Operations Manager (Incident Web Service) (OO Content -OMU) 3.0	[811] CI to remediation (OMi-OO) 1.0 [365] Event to remediation (OMi - OO) 1.1

Integrating with: Performance Insight	Provided by the OBR integration.
[283] PI x-domain Reportpack Integration with OM (PI -> OMW) 1.0 [624] PI x-domain Reportpack Integration with OMU (PI -> OMU) 1.0	
Integrating with: Operations Bridge Reporter	Enhanced.
[410] OBR integration with HP Operations Manager for Windows (OM for Windows) 1.00 [620] OBR integration with HP Operations Manager on UNIX/Linux (OM on UNIX/Linux) 1.0	[299] OBR integration with BSM (Operations Management) events 1.00 [301] OBR integration with the Run-time Service Model (RTSM) of BSM 1.0
Integrating with: Service Manager	Enhanced.
[105] Systems and Incident Exchange via SCAuto (SM - OMW) 1.5 [104] Systems and Incident Exchange via SCAuto (SM - OMU) 1.5 [363] Node Bank and Outage integration (SM - OMU) 1.10 [142] CI Inventory Replication via Connect-It (SC/SM-OMW) 1.0	[337] Incident Exchange (OMi - SM) 1.0 [810] uCMDB to OMi Downtime Integration (OMi - UCMDB)

Integrating with: SiteScope	Enhanced
[39] View SiteScope Monitor Alerts and Events in OM (OMW - SiS) 2.0 [628] View SiteScope Monitor Alerts and Events in OM (OMU - SiS) 1.0 [405] System Availability Management: SAM Admin integration (OMW - SiS) 1.0 [621] System Availability Management: SAM Admin integration (OMU - SiS) 1.0	[412] Event forwarding from SiteScope to BSM OMi 1.0 System Availability Management: SAM Admin is part of BSM. [496] SiteScope Remote Configuration by Monitoring Automation 1.0
Integrating with: Storage Essentials	
[170] HP SPI for SE (SE -> OMW) 2.0 [625] HP SPI for SE (SE -> OMU) 2.0	[167] UCMDB - Storage Essentials 1.0
Integrating with: Systems Insight Manager	
[166] Integrate Hardware-Level Monitoring with System and Application Monitoring (OMW - SIM) 1.0 [626] Integrate Hardware-Level Monitoring with System and Application Monitoring (OMU - SIM) 1.0	[784] BSM Connector for HPE Systems Insight Manager 2.0
Integrating with: Continuous Delivery Automation	
[683] CDA & Operations Manager for UNIX Integration 1.00	https://hpln.hpe.com/blog/hp-operations-agent-can-be-deployed-cda-and-csa
Integrating with: Performance Manager	Enhanced.
[306] Performance Manager to SiteScope 1.0	Embedded Performance Dashboard gathering metrics from Operations Agents, SiteScope, BPM/RUM Profile database, and Diagnostics.

Integrating with: BLUE ELEPHANT SYSTEMS	MIDAS Supervisor supports OMi/BSM.
Core products:	
MIDAS Configurator	
MIDAS Administrator	
Add-ons:	
MIDAS Supervisor	
MIDAS Synchronizer	
MIDAS Outage Manager	
MIDAS Debugger	
MIDAS Analyzer: MIDAS Inventory	
MIDAS Operational Value Pack	
MIDAS Service Builder	
MIDAS Automator	

Appendix G: Server Configuration

Configuration Parameters

You can fine-tune OMi under **Administration > Setup and Maintenance > Infrastructure settings**. Fine-tuning replaces the OM configuration variables and the OM for Windows server configuration.

Where applicable, similar settings exist in OMi. The following figure shows OMi duplicate suppression settings:

See the **Administration Guide > Setup and Maintenance > Infrastructure Settings > Infrastructure Settings for Operations Management** for a complete list of settings.

Configuration Exchange Between Servers

OM for Windows and OM for UNIX offer command-line interfaces to export and import various configurations from a test system into production or backup systems.

OMi can export and import configuration using the RTSM package manager (deals with all RTSM-related artifacts, such as queries, views, CI-Types, and so on) and the Content Pack manager (indicators, correlation rules, tools, graphs, policies, and so on). However, infrastructure settings can currently not be exported and imported.

The following figure shows an example of configuration export using **Administration > RTSM Administration > Administration > Package Manager**:
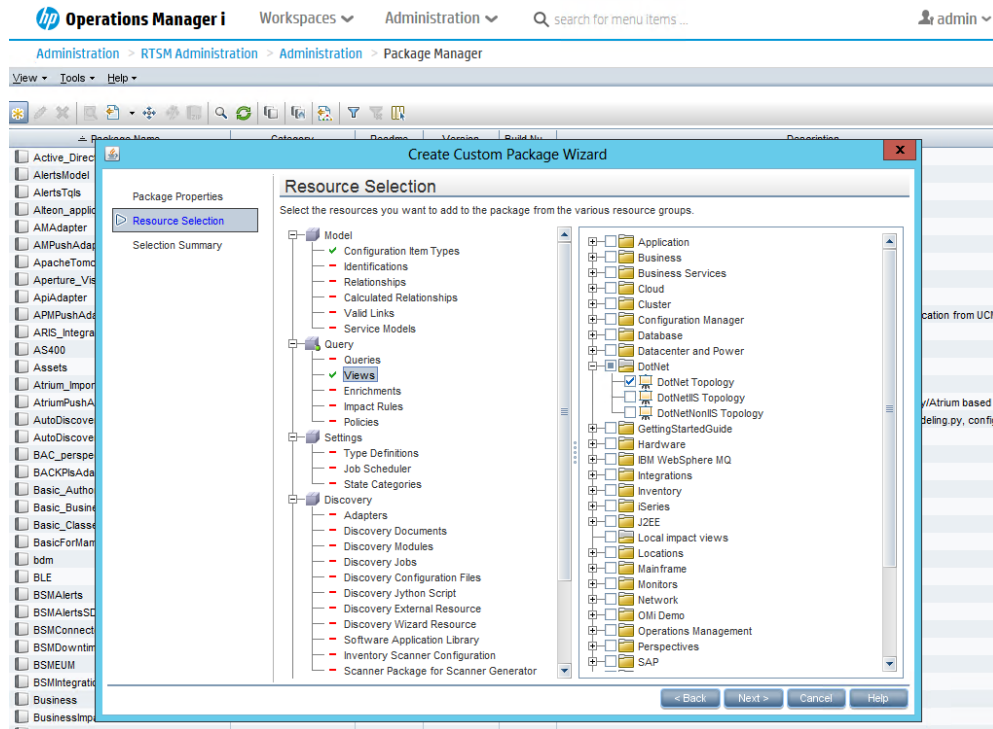
The following figure shows an example of configuration export using **Administration > Setup and Maintenance > Content Packs**:
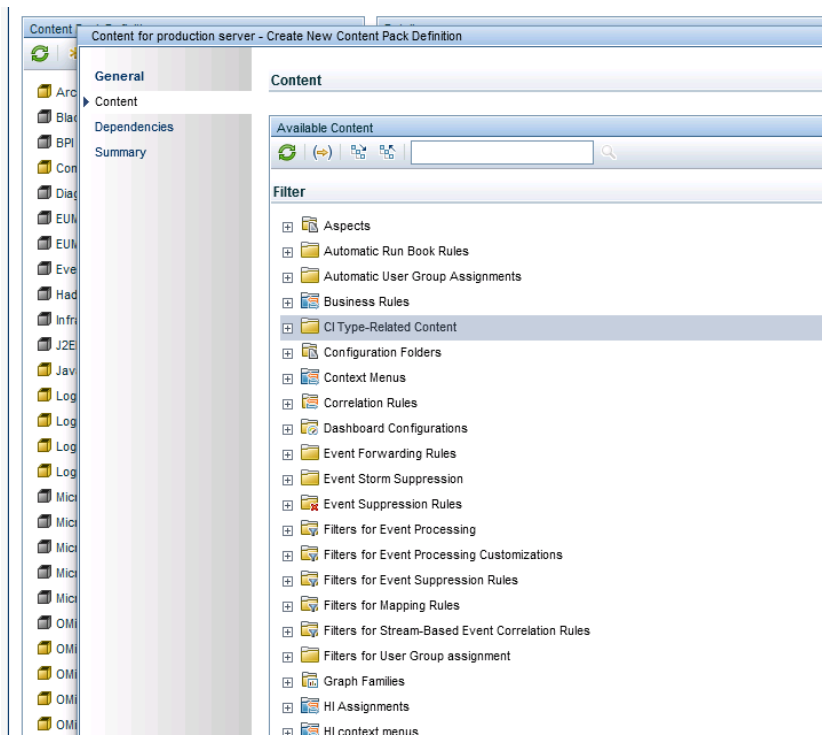
OM functionality	Equivalent in OMi

ovpmutil, opccfgupld/opccfgdwn CLI	RTSM package manager and Content Packs
	Content Manager CLI
Nodes and Services export/import	CI export/import using the RTSM Synchronization job (push or pull)
Tools	Using Content Packs
Policies	Export/import of policy templates, aspects, management templates using Content Packs
User roles	Using Content Packs
Instruction text	With policy export/import using Content Packs
Instrumentation (file copy)	Using Content Packs
Server configuration (ovowconfigutil -download)	Infrastructure settings: currently, there is no export/import.
CLI/APIs for configuration exchange	See Appendix - Command line, API and Web Services Reference for details.

How to Move Content from an OMi Server to Another OMi Server (Test/Production Use Case)

RTSM Content

Use the RTSM package manager to create a new package that includes RTSM artifacts you want to export, such as new CI types, views and queries, enrichment rules, and so on. Then, use "export package to local directory". See the **RTSM Guides > Administration > Package Manager > Create a Custom Package** for more information.

Connect to another OMi system and deploy the RTSM package.

OMi Content

Use the content manager to create a new content pack that includes OMi artifacts, such as tools, aspects, or management templates (included artifacts, such as instrumentation and policy templates, are automatically exported as well). See the **Administration Guide > Setup and Maintenance > Content Packs > Defining Content Packs** for more information.

Upload the exported content pack using the content manager.

Topology Synchronization Packages

You can edit topology synchronization packages in the file system and upload them to the OMi database using the `opr-sdtool` utility.

To exchange custom topology synchronization packages, copy the corresponding files from the file system and upload them using the `opr-sdtool` utility.

> **Note:** The following configuration cannot be exported/imported between OMi servers:
>
> - User groups and users
> - My Workspace pages
> - Auto-grant IP ranges and scripts (script code can be copied manually)
> - Infrastructure settings

Appendix H: High Availability and Disaster Recovery

High Availability

Implementing a high availability configuration means setting up your OMi servers so that the service is continuous despite power outages, machine downtime, and heavy load.

High availability for OMi is implemented in two layers:

- Hardware infrastructure. This layer includes redundant servers, networks, power supplies, and so forth.

- Application. This layer has two components:

  - Load balancing. Load balancing divides the work load among several computers. As a result, system performance and availability increases. External load balancing is a software and hardware unit supplied by an outside vendor. This unit must be installed and configured to work with OMi applications.

  - Failover. Work performed by the Data Processing Server is taken over by a backup server if the primary server or component fails or becomes temporarily unavailable.
    OMi provides its own failover mechanism and does not require separate cluster software.

Implementation of load balancing and failover is discussed in the OMi Administration Guide.

High-availability of the OMi database server (Oracle/MS SQL server) can be achieved through database vendor-specific HA solutions.

High availability concepts known from OM, such as HA using clusters, server pooling, or HA Manager (Linux) cannot be reused directly, but the HA concept outlined above offers almost the same benefits and features.
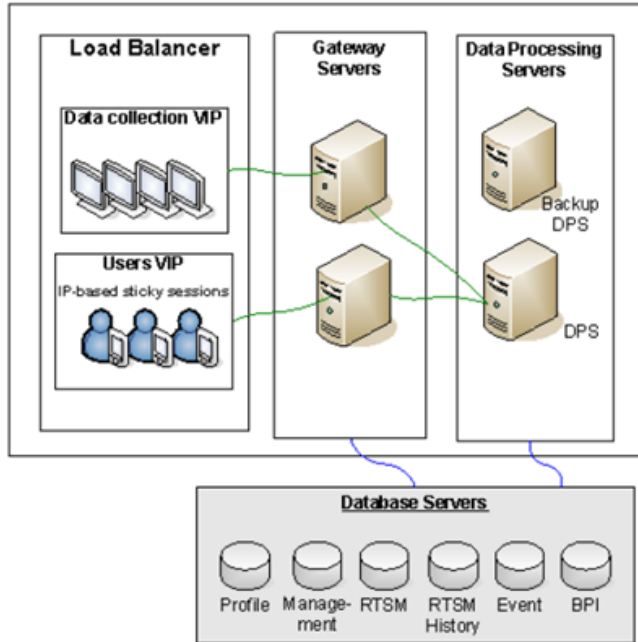
OMi supports MS SQL log file shipping (known from OM for Windows) as part of its disaster recovery process. See the section below for more information.

OM HA Feature	Equivalent in OMi
Use of virtual IP/hostname for server	Yes, using external Load balancer
Distribute load among several OM servers (server pooling)	Distribute load among several Gateway servers
HA concept allows installing patches on one server while other server is fully operational (server pooling)	Certain patches can be installed on a gateway or backup/non-active processing server while other gateway servers and the active processing server are running. However, patches updating the communication bus or other core services may require downtime. Patching the active DPS requires to move the services to the backup DPS (after the backup DPS has been patched), which involves some downtime as the services need to start on the backup DPS. OMi 10.10 and later uses a hot-standby backup server that reduces the downtime to less than a minute.

Disaster Recovery

OMi supports MS SQL log shipping, Oracle Data guard, and PostgreSQL hot standby as disaster recovery techniques for databases. Other configuration files have to be copied separately.
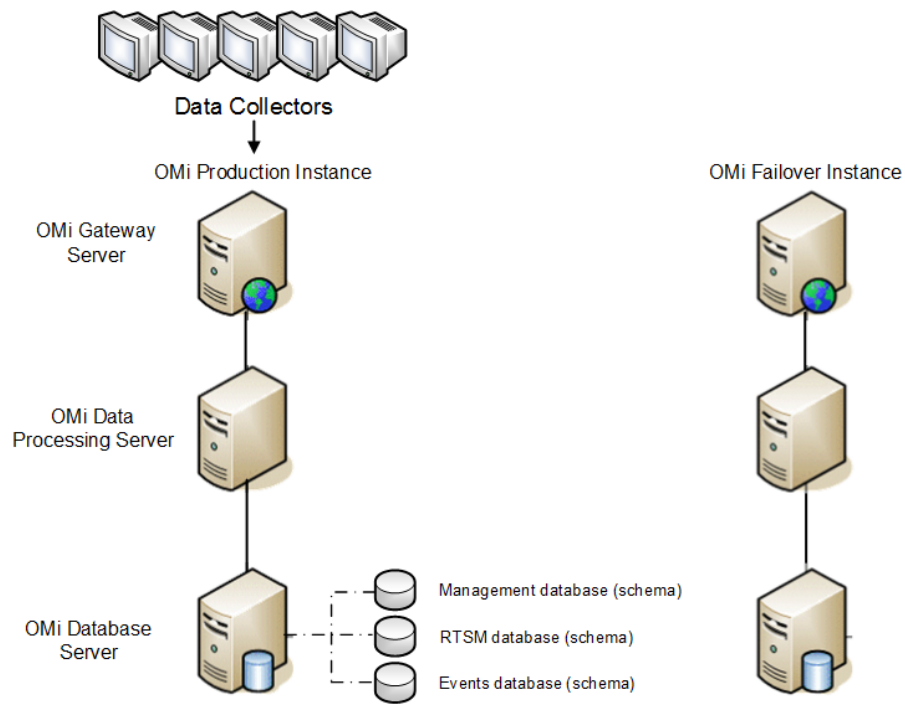
For details on disaster recovery, see the OMi Administration Guide.

Appendix I: Troubleshooting

Overview

Troubleshooting in OM and OMi depends on understanding:

- The product architecture
- How to check the status of the application processes
- Which log files to inspect
- How to enable tracing to collect more detailed information
- Tools to test configuration and connectivity

Self-Monitoring

Operations agents that are automatically installed on all OMi servers are used to detect OMi server problems. OMi server problems reported in OMi log files are detected and reported as events to OMi. The OMi Server Health page shows those OMi server events, as well as all the events related to operations agents health check and communication problems.

For certain problems that affect the event processing itself (and therefore also the display of these problems on the OMi Server health page), notifications can be send by the operations agents to a dedicated user. See the OMi Help for more details.

HPE Support

When problems occur and you log a case with HPE Support, HPE typically requests the output of itochecker (OM for UNIX) or ovsuptinfo (OM for Windows). For OMi, HPE Support typically requests:

- The zip file output of LogGrabber run on both GW and DPS (located in the `<OMi_HOME>/tools/LogGrabber` directory)

- The file output of `<OMi_HOME>/opr/support/opr-checker[.bat|.pl] –xml > tmpfile.xml`

Troubleshooting Information in the OMi Help

Your primary resource for troubleshooting is the OMi Help. Troubleshooting information is located within each section. Search for "troubleshooting" and filter by the area of interest.

Architecture

The OMi server is comprised of a Gateway Server and Data Processing Server which are predominantly Java-based, with a JMS bus to pass events between the servers. Client web browsers connect to the web server (IIS or Apache Tomcat) that is running on the Gateway Server. For high availability, OMi supports multiple Gateway Servers through a Load Balancer, and an additional Data Processing Server to fail over on the backend.

In contrast, OM server processes run on a single server. The client GUI for OM for Windows is either MMC or a web browser. The operator client GUI for OM for UNIX is Java-based (Java application, Java Web Start, or Java Applet), while the administrator GUI is a web browser. The OM server can run in a cluster to provide high availability.

HPE Operations Agents communicate with OM and OMi in the same way (HTTPS-based). Manager-to-manager event communication between and among OM and OMi servers is the same as well.

For southbound integrations, OMi can get events, metrics, and topology from BSM Connectors and from SiteScope.

For northbound integrations, OMi leverages web services and scripting. The details are available in the OMi Extensibility Guide.
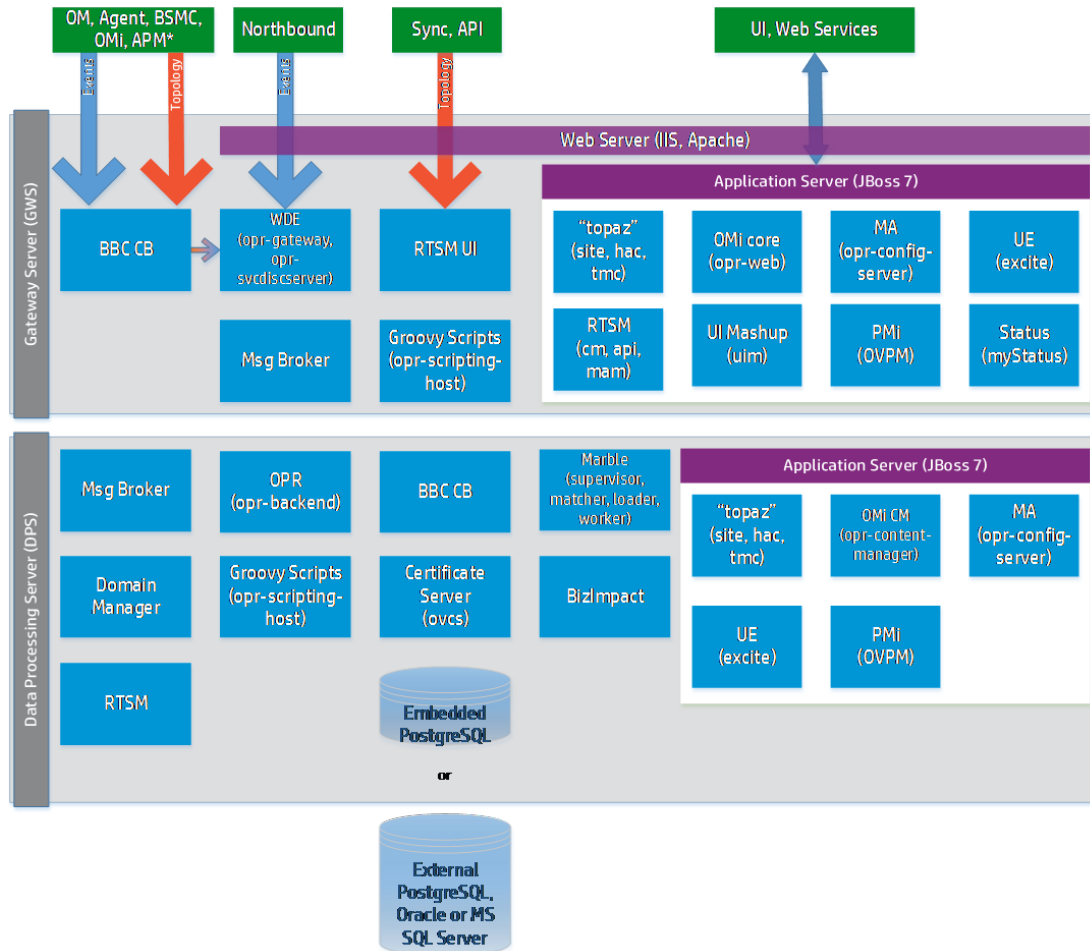
Status Check

In OMi, you can check the overall status of the server by selecting one of the following methods to run on the Gateway Server and Data Processing Server:

- Run *<OMi_HOME>*`/tools/bsmstatus/bsmstatus[.bat.sh]`.

  > **Note:** On Windows, this is the same as **Start > Programs > HPE Operations Manager i > Administration > Operations Manager i Status**.

- `https://OMiSERVER:8080/myStatus/myStatus.html` (JMX login credentials required)

If a non-graphical output is required, you can check the Nanny status of all processes by running:

<OMi_HOME>`/opr/support/opr-support-utils[.sh|.bat] -ls`

Logging and Tracing

OMi makes extensive use of log4j. The log4j properties files control logging characteristics. Log files are mostly located in the *<OMi_HOME>*`/log` directory. The most important log files are listed in the following

tables. For further details (including log file management and debugging), see the **Administration Guide > Troubleshooting > OMi Logs**.

Gateway Server

Location and Name	Server	Purpose	Debug
<OMi_HOME>\log\wde\opr-gateway.log	GW	OMi Gateway processing. Start here if you want to check whether a new or a changed event was received by OMi.	*<OMi_HOME>*\conf\core\Tools\log4j\wde\opr-gateway.properties
<OMi_HOME>\log\wde\opr-gateway-flowtrace.log	GW	Flowtrace log entries for events and event changes arriving at the Gateway	*<OMi_HOME>*\conf\core\Tools\log4j\wde\opr-gateway.properties You can log an individual event by specifying the custom attribute __TRACE__ in the event. You can capture flow tracing across both GW and DPS using the OMi GUI by navigating to **Administration > Setup and Maintenance > Infrastructure Settings**, selecting the **Operations Management** context and setting Event Flow Logging Mode to "mem". To access in-memory flow logging, go to the processing server and launch https://localhost:29922/. Click opr.backend:name=EventFlowTraceMBean and invoke the showAllEvents method.
<OMi_HOME>\log\opr-scripting-host\opr-scripting-host.log	GW	Custom Actions External event processing External instruction text lookup	*<OMi_HOME>*\conf\core\Tools\log4j\opr-scripting-host\opr-scripting-host.properties
<OMi_HOME>\log\jboss\opr-configserver.log	GW	Monitoring Automation	*<OMi_HOME>*\conf\core\Tools\log4j\jboss\opr-webapp.properties

`<OMi_HOME>\log\jboss\` `opr-event-ws.log`	GW	Event Web Services	`<OMi_HOME>\conf\core\Tools\log4j` `\jboss\opr-event-ws.properties`

`<OMi_HOME>\log\jboss\`
`opr-ws-response.log`
	GW	Event Web Services	`<OMi_`
			`HOME>\conf\core\Tools\log4j\jboss`
			`\opr-ws-response.properties`

`<OMi_HOME>\log\jboss\` `opr-policyeditors.log`	GW	Monitoring Automation	

`<OMi_HOME>\log\jboss\`
`opr-webapp.log`
	GW	Log file for OMi web UIs
		
		Monitoring Automation
		
		Content Pack import
		
		Tool execution
			`<OMi_`
			`HOME>\conf\core\Tools\log4j\jboss`
			`\opr-webapp.properties`

`<OMi_`
`HOME>\log\jboss\login.log`
	GW	LDAP, LWSSO	`<OMi_`
			`HOME>\conf\core\Tools\log4j\jboss`
			`\topaz.properties`

`<OMi_HOME>\log\jboss\`
`UserActions.servlets.log`
	GW	Login attempts	`<OMi_`
			`HOME>\conf\core\Tools\log4j\jboss`
			`\topaz.properties`

`<OMi_HOME>\log\wde\`
`opr-svcdiscserver.log`
	GW	Mapping/filtering part of OMi dynamic topology synchronization	`<OMi_`
			`HOME>\conf\core\Tools\log4j\wde`
			`\opr-svcdiscserver.properties`

`<OvDataDir>`
`\shared\server\log\`
`OvSvcDiscServer.log`
	GW	Receiving part of OMi dynamic topology synchronization	To set maximum logging:
			
			`<OvBinDir>\ovconfchg -ovrg server -`
			`ns`
			`om.svcdiscserver -set LOG_LEVEL 10`
			
			`<OMi_HOME>\opr\support`
			`\opr-support-utils.sh -restart wde`
			
			To return to the default logging:
			
			`<OvBinDir>\ovconfchg -ovrg server -`
			`ns`
			`om.svcdiscserver -clear LOG_LEVEL`
			
			`<OMi_HOME>\opr\support`
			`\opr-support-utils.sh -restart wde`

Location and Name	Server	Purpose	Debug

<OvDataDir>
`\shared\server\log\`
`ovpmtrace.0.txt`
	GW	Performance Dashboard trace file	Enable tracing in the OMi GUI by navigating to **Administration > Setup and Maintenance > Infrastructure Settings**, selecting the Performance Dashboard context and setting Trace Level to 2.

<OMi_HOME>`\log\jboss\` `content-manager.log`	GW	Content Manager functionality	*<OMi_ HOME>*`\conf\core\Tools\log4j\jboss` `\content-manager.log`
<OMi_HOME>`\log\jboss\` `kes.contentpack.log`	GW	Content Manager functionality	*<OMi_ HOME>*`\conf\core\Tools\log4j\jboss` `\kpi_enrichment.properties`

<OMi_HOME>`\log\jboss\`
`downtime.log`
	GW	Downtime	*<OMi_ HOME>*`\conf\core\Tools\log4j\jboss`
			`\downtime.properties`
			
			<OMi_ HOME>`\conf\core\Tools\log4j\jboss`
			`\downtime-client.properties`

<OMi_HOME>`\log\jboss\` `opr-ue.log`	GW	User Engagement	*<OMi_ HOME>*`\conf\core\Tools\log4j\jboss` `\opr-webapp.properties`

<OMi_HOME>`\log\opr-clis.log`	GW	opr-* Command-Line Interfaces	*<OMi_ HOME>*`\conf\core\Tools\log4j\opr-`
			`clis`
			`\cli-log4j.properties`

<OMi_HOME>`\log\wde\` `opr-heartbeat.log`	GW	Health Check	*<OMi_ HOME>*`\conf\core\Tools\log4j\wde` `\opr-heartbeat.properties`

Data Processing Server

Location and Name	Server	Purpose	Debug

<OMi_HOME>`\log\opr-backend\`
`opr-backend.log`
	DPS	OMi backend process.
		
		Start here if you want to check whether a new or changed event was
			<OMi_HOME>`\conf\core\Tools`
			`\log4j\opr-backend`
			`\opr-backend.properties`

		processed by OMi.	
<OMi_HOME>\log\opr-backend\ opr-flowtrace-backend.log	DPS	Flowtrace log entries for the events arriving from the OMi Gateway process	*<OMi_HOME>*\conf\core \Tools\log4j\opr-backend \opr-backend.properties You can log an individual event by specifying the custom attribute `__TRACE__` in the event. You can capture flow tracing across both GW and DPS using the OMi GUI by navigating to **Administration > Setup and Maintenance > Infrastructure Settings**, selecting the **Operations Management** context and setting Event Flow Logging Mode to "mem". To access in-memory flow logging, go to the processing server and launch https://localhost:29922/. Click `opr.backend:name=EventFlowTraceMBe an` and invoke the showAllEvents method.
<OMi_HOME>\log\opr-topologysync\ opr-topologysync.log	DPS	Log entries for the OMi topology synchronizati on application	*<OMi_HOME>*\conf\core\Tools\ log4j\opr-topologysync\ opr-topologysync.properties
<OMi_HOME>\log\opr-backend_ boot.log	DPS	Startup log entries for the OMi backend process	
<OMi_HOME>\log\ opr-backend_shutdown.log	DPS	Shutdown messages for the OMi backend process	
<OMi_HOME>\log\opr-backend\ opr-ciresolver.log	DPS	OMi backend process CI resolution	*<OMi_HOME>*\conf\core\Tools \log4j\opr-backend \opr-backend.properties
<OMi_HOME>\log\opr-scripting-host\ opr-scripting-host.log	DPS	EPI processing	*<OMi_HOME>*\conf\core\Tools \log4j\opr-scripting-host \opr-scripting-host.properties

<OMi_HOME>\log\opr-scripting-host\ scripts.log	DPS	EPI script errors	*<OMi_HOME>*\conf\core\Tools \log4j\opr-scripting-host \opr-scripting-host.properties
<OMi_HOME>\log\jboss\downtime.log	DPS	Downtime	*<OMi_HOME>*\conf\core\Tools \log4j\jboss\downtime.properties *<OMi_HOME>*\conf\core\Tools \log4j\jboss\downtime- client.properties
<OMi_HOME>\log\marble_worker_ 1\ downtime.log	DPS	Downtime	*<OMi_HOME>*\conf\core\Tools \log4j\marble_worker \dowtime-client.properties
<OMi_HOME>\log\jboss\opr- ue.log	DPS	User Engagement Runtime	*<OMi_HOME>*\conf\core\Tools \log4j\jboss\opr-webapp.properties
<OMi_HOME>\log\opr-backend\ opr-heartbeat.log	DPS	Health Check	*<OMi_HOME>*\conf\core\Tools \log4j\opr-backend \opr-heartbeat.properties

Gateway Server and Data Processing Server

Location and Name	Server	Purpose
<OMi_HOME>\log\supervisor\nanny_all.log	DPS/GW	Nanny Manager – startup/shutdown log
<OMi_HOME>\log\supervisor\wrapper.log	DPS/GW	Wrapper process – startup/shutdown log
<OMi_HOME>\log\configserver directory	DPS/GW	Configuration log files (for example, when patching or upgrading, running config wizard, running opr-mp-installer.bat/sh)
<OMi_HOME>\log\<ServiceName>_boot.log	DPS/GW	Boot log files for all OMi services
<OMi_HOME>\log\opr-scripting-host_boot.log	DPS/GW	EPI boot
<OMi_HOME>\log\opr-scripting-host_shutdown.log	DPS/GW	EPI shutdown
<OMi_HOME>\log\bus	DPS/GW	Bus logs
<OMi_HOME>\log\bus_shutdown.log	DPS/GW	Bus shutdown
<OMi_HOME>\log\opr-clis.log	DPS/GW	opr-* Command-line tools
<OMi_HOME>\log\jboss	GW	Jboss (MercuryAS) Application Server log files
<OMi_HOME>\log\jboss7_boot.log	GW	Jboss (MercuryAS) startup log file

<OMi_HOME>\log\wde	GW	Tomcat (wde) log files
<OvDataDir>\log\System.txt	DPS/GW	LCore and OM Agent log file

OM

Location and Name	Server	Purpose
<OvDataDir>\log\System.txt /var/opt/OV/log/System.txt	OM for Windows OM for UNIX	LCore and OM Agent log file
<OvShareDir>\server\log\om\incident-ws.trace.txt /var/opt/OV/log/om/incident_ws.0.en	OM for Windows OM for UNIX	Incident Web Service logging
<OvDataDir>\shared\server\log\OvSvcDiscServer.log /var/opt/OV/shared/server/log/OvSvcDiscServer.log	OM for Windows OM for UNIX	Service discovery
Windows Event Log	OM for Windows	Server-related events
/opt/OV/OMU/adminUI/logs	OM for UNIX	Admin UI log files

To debug problems with the flex-based user interface, you can enable logging in the GUI. For details, see the **Administration Guide > Troubleshooting > Tracing and Logging Operations Management User Interfaces > Logging Settings User Interface**.

OMi uses the same communications technology as OM to interact with the agent and other OM/OMi servers. This means you will find some of the same data logged to <OvDataDir>/log and <OvDataDir>/shared/server/log directories, as on OM. Tracing is configured in the same way as on OM, namely the OM-style (ovconfchg) and the newer HPE-style (ovtrccfg, ovtrcmon) in OM.

Tools – HPE Operations Agent Communication

The tools for troubleshooting communication with the HPE Operations Agent are similar between OMi and OM. Typically, configuration issues are related to connectivity (port, firewall settings) or certificates. The same bbcutil, ovcert, and ovdeploy commands can be used in OMi as in OM.

In OM, the oprcragt command is used to perform a range of tasks on one or multiple managed nodes. OMi provides ovrc, which, as oprcragt, can perform start, restart, stop, and status actions on remote managed nodes, for example:

```
ovrc -ovrg server -host pluto.hp.com -status

ovrc -ovrg server -host pluto.hp.com -start opcmsgi
```

Note: Each command operates on a single node. To perform the action on a group of nodes or all nodes,

use `opr-agt[.sh|.bat]`. For example, to query the status of all nodes in a view, run:

```
opr-agt.sh -status –view_name "Hosts with HPE Operations Agents" -username admin
```

Troubleshooting access to agent-based performance data in OMi is similar to Performance Manager but not identical. For example, the following Performance Manager commands:

`ovcodautil –ping –n mynode.fqdn`

`ovcodautil –obj –n mynode.fqdn`

`ovcodautil –dumpds SCOPE –n mynode.fqdn`

are implemented in OMi as:

`/opt/HP/BSM/JRE/bin/java -jar /opt/OV/java/jcodautil.jar -ping –n mynode.fqdn`

`/opt/HP/BSM/JRE/bin/java -jar /opt/OV/java/jcodautil.jar -obj –n mynode.fqdn`

`/opt/HP/BSM/JRE/bin/java -jar /opt/OV/java/jcodautil.jar –dumpds SCOPE –n mynode.fqdn`

Or:

`<OMi_HOME>\JRE\bin\java -jar "<OVInstallDir>\java\jcodautil.jar" -ping -n mynode.fqdn`

`<OMi_HOME>\JRE\bin\java -jar "<OVInstallDir>\java\jcodautil.jar" -obj –n mynode.fqdn`

`<OMi_HOME>\JRE\bin\java -jar "<OVInstallDir>\java\jcodautil.jar" –dumpds SCOPE –n mynode.fqdn`

Performance Manager provides a System Information web page that connects to the agent and reports a summary of data sources, classes, and the last time the data was logged. This functionality is not available in OMi.

Tools – Event Processing

In OMi, event processing is implemented differently than in OM, and so the troubleshooting is different. OM makes use of queue files that can be analyzed. It is possible that events are discarded if there is no matching node defined on the OM server. OMi uses a Bus to pass events through the Gateway to Data Processing server and into the database.

You can also use the JMX Console to query an extensive amount of configuration. Since you can make changes to configuration and data, it is important to take care when using the JMX Console. See the **Administration Guide > Additional Configuration > JMX Console** for an overview.

> **Note:** There is no separate documentation on the available methods.

You can run `<OMi_HOME>/opr/support/opr-jmsUtil[.sh|.bat]` to monitor the number of messages and the size of the bus queues and topics.

For troubleshooting purposes, in OMi, you can generate an event on demand. On the Gateway Server, run `<OMi_HOME>/opr/support/sendEvent[.sh|.bat]`. If you run the command without parameters, you will get the help syntax.

Tools – Connected Server Communication

In OMi, you can configure connected servers, such as OMi, APM, OM, SiteScope, BSM Connector, External Event Processing, and ArcSight Logger. With every connected server, you can test basic connectivity. In the case of OM, there are separate wizard pages to test the HTTPS-based datacomm to port 383 (default) and to test Incident Web Services connectivity (default port 8444 or 443).
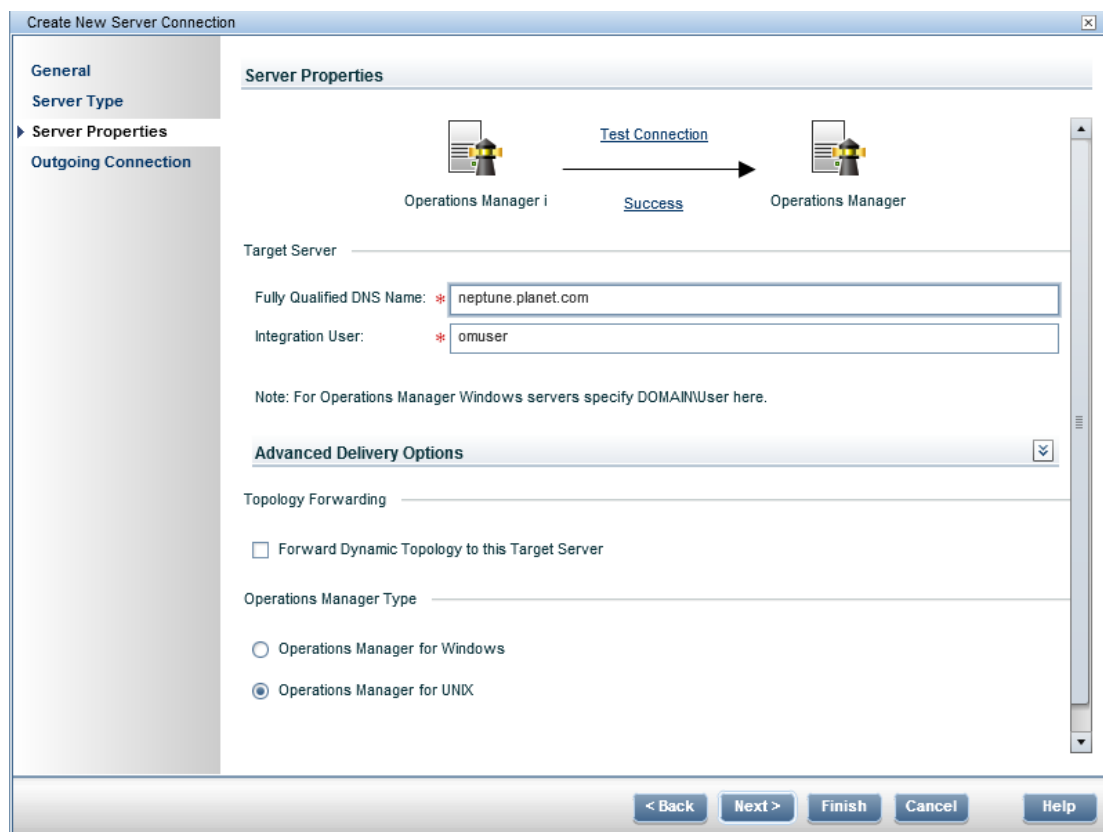
Tools – Topology Synchronization

To troubleshoot topology synchronization from OM to OMi, you can capture detailed data that the OMi server receives. In OMi, navigate to **Administration > Setup and Maintenance > Infrastructure Settings**, select the **Operations Management** context and set **Dump Data** to true.

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 OMi Evolution Guide (Operations Manager i 10.10)

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 ovdoc-asm@hpe.com.

We appreciate your feedback!

Go OMi!