Operations Bridge Manager 2018.05

Evolution Guide

Table of Contents

Transfer functions from OM to OBM

Learn how to transfer functions from OM to OBM (that is, the evolution process) through phases.

Start off by reviewing the Related Topics, which provide an overview of the evolution process, describes the evolution strategy, and also lists the additional resources that can be useful when for transferring functions from OM to OBM. Each of the following sections describes the corresponding evolution phase:

- Plan the evolution
- Introducing OBM
- Establish an effective operator workflow
- Manage Operations Agents from OBM
- Configure SiteScope from OBM
- Establish reporting by using OBR
- Switch off OM and Reporter
- Add value on top

Related Topics

- Evolution from OM to OBM
- Evolution strategy
- Additional resources

Introduction

See the following topics for an introduction to the evolution process:

- Evolution from OM to OBM
- Evolution strategy
- Additional resources

Evolution OM to OBM

Operations Bridge Manager (OBM) 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 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 Operations Manager.

With the introduction of the Monitoring Automation feature in OBM 9.20, OBM was already able to take over the Operations Agent configuration and management part that by then had to be done in 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 OBM 10, the first OBM version with the intention to replace OM has been released. With this many gaps are closed and although there is no need to move to OBM immediately, it can be considered as the successor of OM.

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

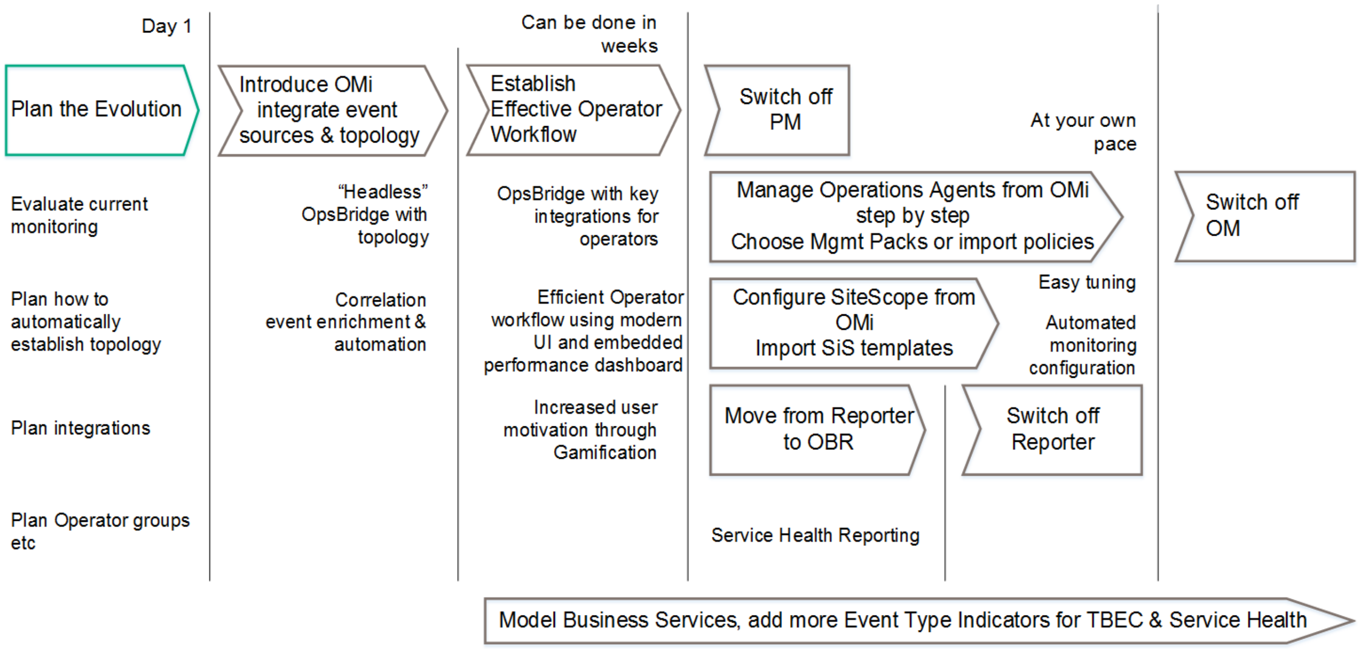
This and the following topics are for OBM implementers who want to replace an existing OM installation with OBM version 10.00 or later. It provides step-by-step evolution information on how existing OM configurations can be transferred and used with OBM and offers a comprehensive comparison of key OM features and their equivalent in OBM. It also explains how OBM and Operations Bridge Reporter (OBR) can be used to replace functions that are offered by Operations Manager (OM) for UNIX or Windows and HPE Reporter while providing additional features and a modern web-based user interface.

With version 10.x, Service Health Reporter (SHR) is renamed to Operations Bridge Reporter (OBR). In the following topics and sections, Operations Bridge Reporter (OBR) refers to both Operations Bridge Reporter 10.x as well as Service Health Reporter 9.4x.

Evolution strategy

We recommend that you transfer functions from OM to OBM in phases. The following topics explain each step in detail. The Operations Bridge Evolution Overview video in the Video Library provides an overview as well.

This is not a strict sequence that has to be followed in all cases. For example, instead of adding correlation rules in the first OBM 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 Operations Bridge efficiency.


Day 1
Plan the Evolution
Evaluate current monitoring
Plan how to automatically establish topology
Plan integrations
Plan Operator groups etc
Introduce OMi integrate event sources & topology
"Headless" OpsBridge with topology
Correlation event enrichment & automation
Can be done in weeks
Establish Effective Operator Workflow
OpsBridge with key integrations for operators
Efficient Operator workflow using modern UI and embedded performance dashboard
Increased user motivation through Gamification
Switch off PM
At your own pace
Manage Operations Agents from OMi step by step
Choose Mgmt Packs or import policies
Easy tuning
Configure SiteScope from OMi
Import SiS templates
Automated monitoring configuration
Move from Reporter to OBR
Switch off Reporter
Service Health Reporting
Switch off OM
Model Business Services, add more Event Type Indicators for TBEC & Service Health

Evolution phases

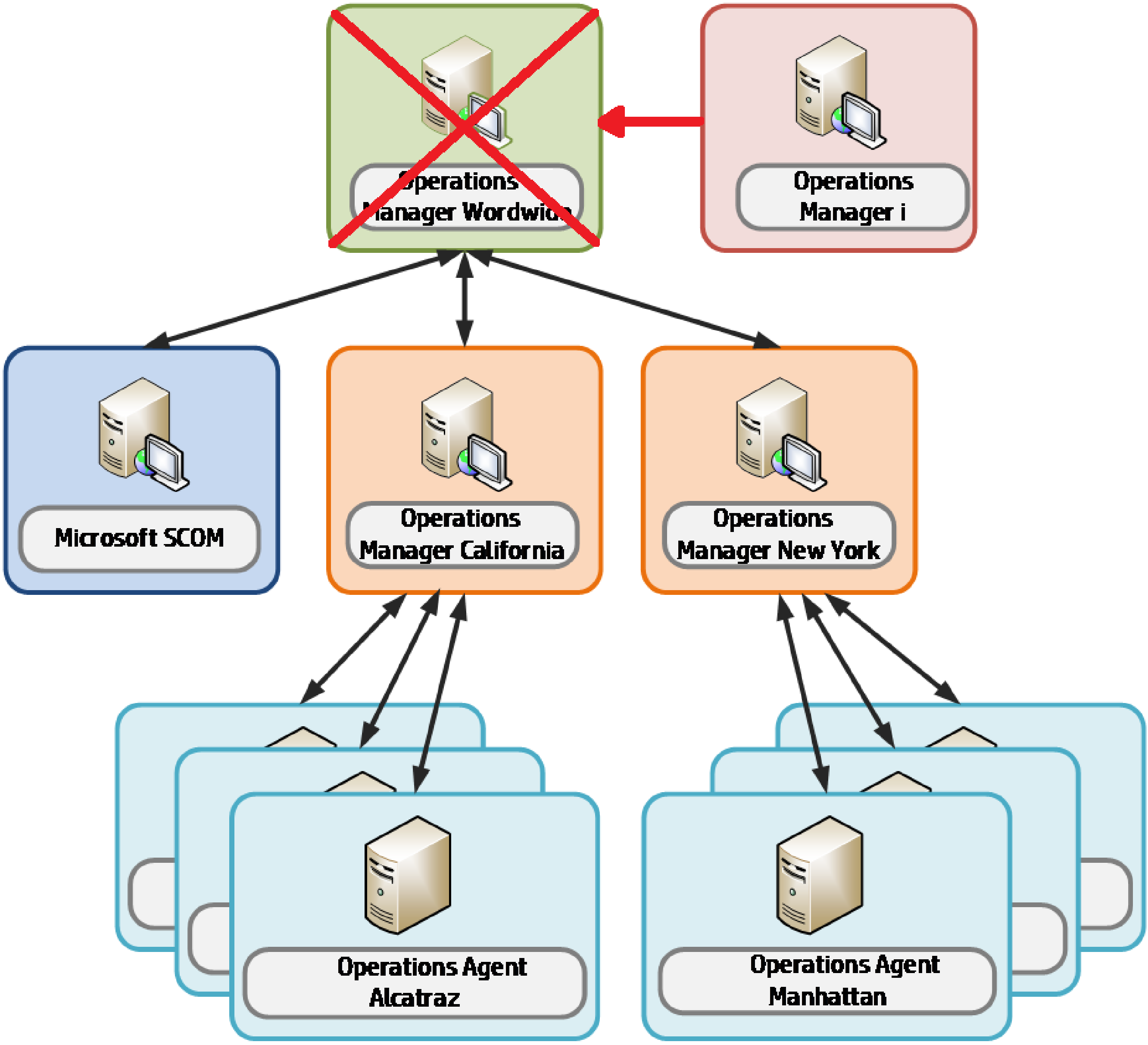
Evolution phases are the following:

1. Plan the evolutionTo avoid unnecessary effort, any implementation of OBM should be planned and developed upfront, before the actual software installation and configuration is done. OBM allows a lot of automation that can greatly simplify ongoing monitoring, however this automation requires thoughtful planning and clear understanding of how you want to monitor your IT environment.Moving from OM to OBM can be considered as an opportunity to revise your current monitoring configuration and operator setup. You will benefit the most from OBM capabilities not by trying to reestablish the configuration offered by OM, but by taking advantage of the new concepts and possibilities that OBM offers.With any OBM implementation there are certain deployment options (with or without external UCMDB, single- or multi-server deployment, load balancer, and so forth) that depend on your sizing, security, and integration requirements or preferences. For an overview of what should be considered when planning the solution deployment, see the *Moving to Service Centric Management with OBM Technical White Paper*.
2. Introduce OBMThe next phase introduces OBM and focuses on the integration of the various event sources and topology. Once this is established you can benefit from the OBM correlation, event enrichment and automation features. Some customers stop with this step and use OBM in a “headless” fashion, which means that all events are forwarded to another system (such as Service Manager) and processed there. All other customers perform this as a necessary first implementation step before they move on to the next step.
3. Establish effective operator workflowIn this phase, operators are moved from OM to OBM. This includes setting up operators and operator groups, defining work roles and responsibilities, and establishing key integrations for operators such as 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 OBM UI and efficient operator workflow as well as from the advanced

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

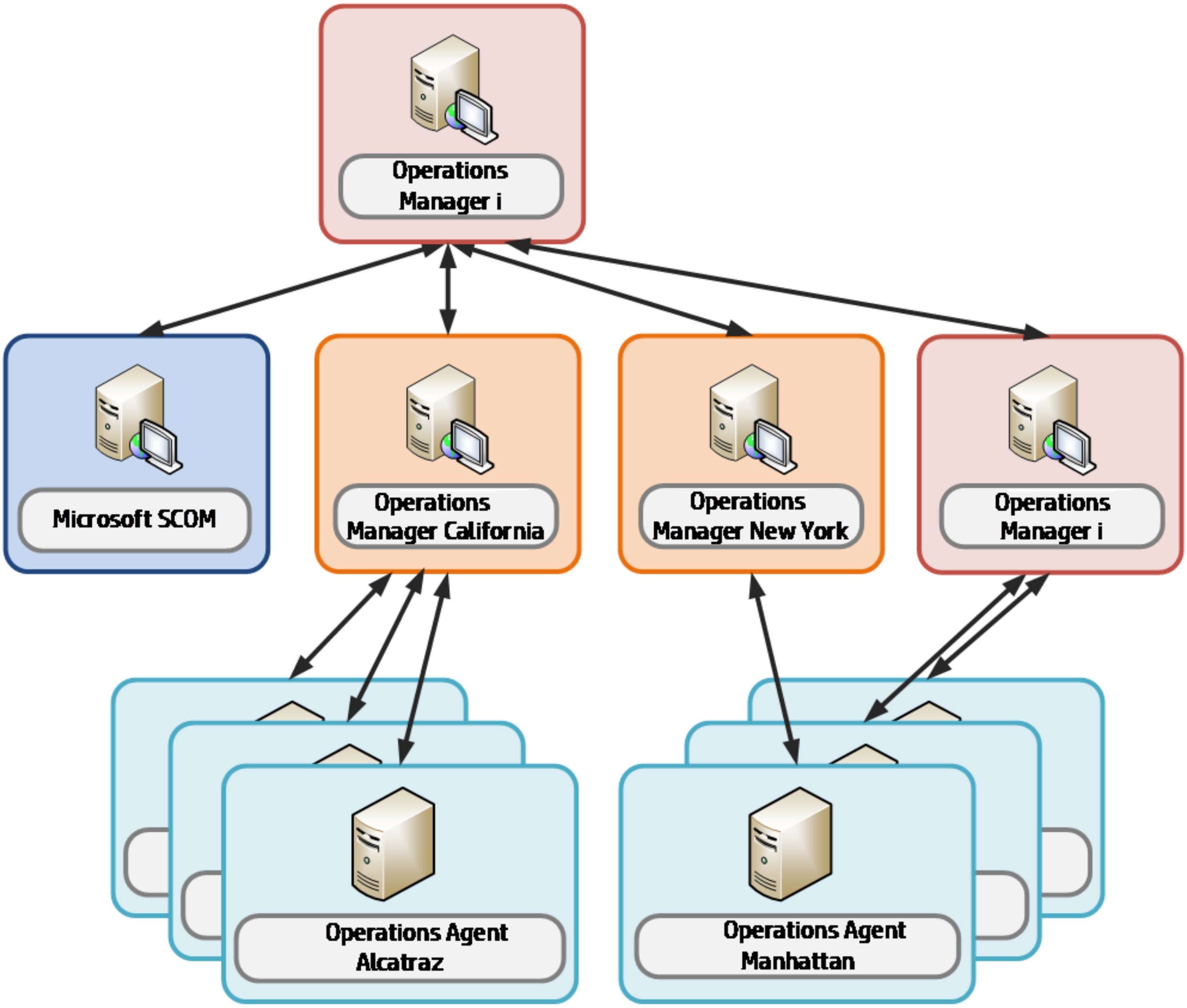
- Linkage to the RTSM
- Modern, web-based user interface
- Extended event automation capabilities including automatically assigning events to users and time-based automatic triggering event updates and actions
- Multidimensional approach to calculating service health
- Integration capabilities by using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

4. With these functions, OBM can replace an OM system in an Operations Bridge or Manager-of-Managers role.Example of replacing OM Manager-of-Managers acting as Operations Bridge with OBMOperators log in to OBM 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 (in OBM 10.10 and later, these are referred to as performance dashboards).Key integrations with other HPE products also exist in OBM, such as the integrations with SiteScope, UCMDB, Service Manager, Operations Orchestration, Network Node Manager i, Operations Bridge Reporter, and notification systems.

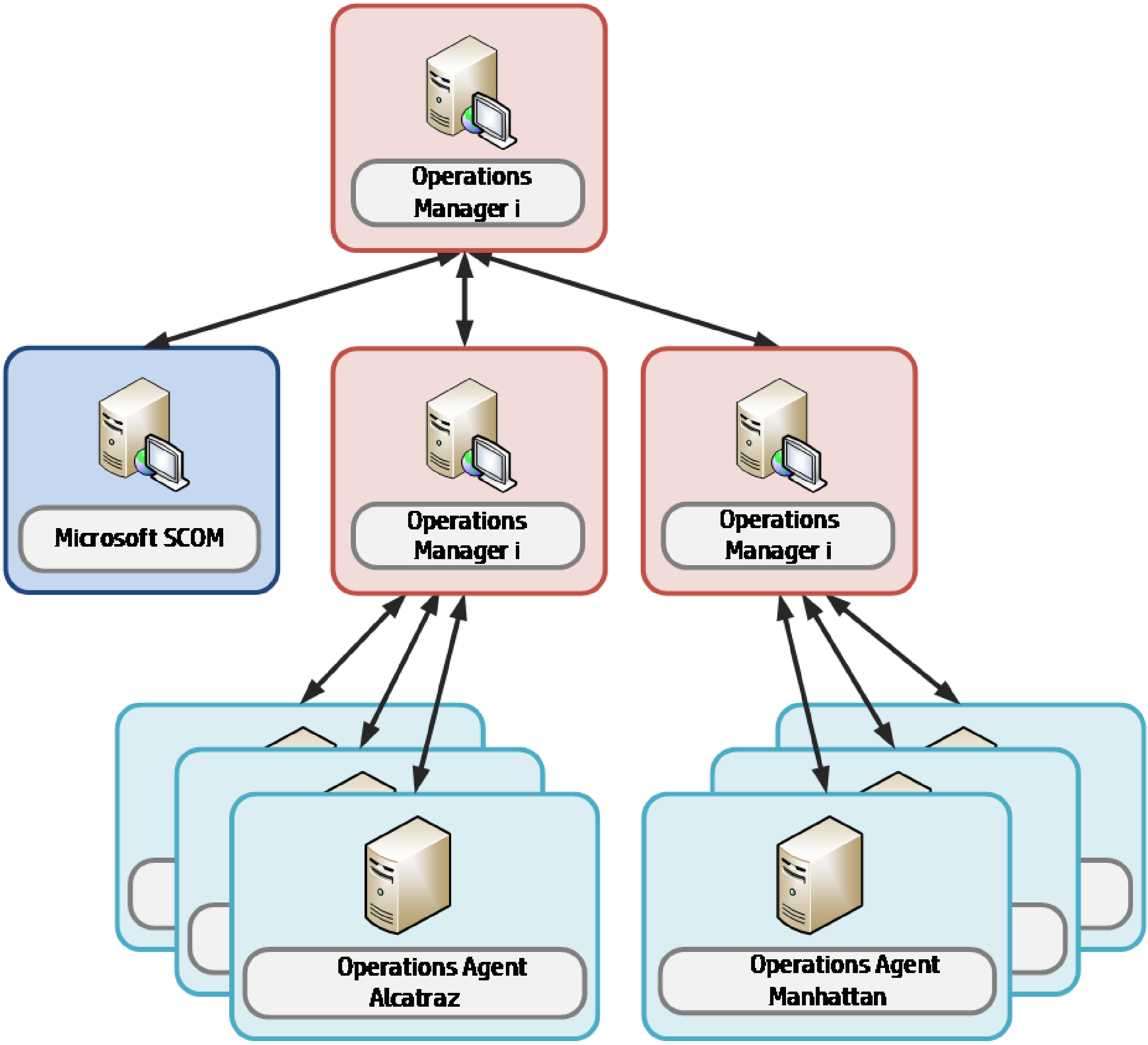


In the following steps, you can add monitoring configuration for SiteScope and OM agents.

5. Manage Operations Agents from OBMIn this phase OBM Monitoring Automation provides an automated, topology-based monitoring configuration.You can use OBM Management Packs or build your own management packs for your custom applications to benefit from OBM's monitoring configuration concepts, such as aspects and parameterized policies.For an up-to-date list of OBM Management Packs, go to Marketplace.Example of OBM taking over policy management for some nodes


Operations Manager i
Microsoft SCOM
Operations Manager California
Operations Manager New York
Operations Manager i
Operations Agent Alcatraz
Operations Agent Manhattan

This can be accomplished step by step by having OBM and OM in parallel, until all Operations Agents are configured from OBM.Note When you exchange your OM license for an OBM license as part of the license exchange program, you will continue to get support for your exchanged OM licenses.Example of OBM being used as Operations Bridge and for system management



6. Manage SiteScope from OBMIn this phase you use OBM Monitoring Automation to configure SiteScope systems.
7. Move from Reporter to OBRIn this phase you establish business service-centric reporting that uses Operations Bridge Reporter, which replaces the Reporter.
8. Switch off Performance Manager, Reporter, and OMAt the end of the evolution, when OBR and OBM have taken over all functions and when the older products are no longer required, the older products can be switched off.
9. Add value on topAt this point in the evolution process, you already gained a lot of benefits by using OBM 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. OBM comes with a number of content packs that provide many features free of charge for particular application areas (such as Microsoft Active Directory, Oracle Databases, and so on).However, there are situations where you must 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.These tasks can be regarded as optional, depending on your specific business needs.

Related Topics

Video Library

Plan the evolution

Introducing OBM

Establish an effective operator workflow

SPI to MP Evolution Tool

Manage Operations Agents from OBM

Configure SiteScope from OBM

Establish reporting by using OBR

Switch off OM and Reporter

Add value on top

Additional resources

When performing the evolution from OM to OBM, the following additional resources could be useful:

- *OBM Management Packs Evolution*. This help 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 OBM Management Packs.
- ITOM Marketplace. This is intended for practitioners and users of OBM and of the Operations Bridge Suite, and contain many useful links to forums, blog articles, videos, trainings, help centers, tools, and so on.
- == Related Topics == Video LibraryMoving to Service Centric Management with HP Technical White PaperManagement Packs EvolutionITOM Marketplace

Plan the evolution

See the following sections for information on how to plan the evolution:

- Plan how to establish infrastructure topology
- Plan operator groups
- Plan integrations
- Plan monitoring configuration
- Plan license migration

Plan how to establish infrastructure topology

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 OBM 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 OBM.

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 with 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.
- 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 OBM topology-based event correlation feature to correlate events
- The topology can be used by OBM topology-based management template feature to automate the selection of the monitoring configurations for setup or removal

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

Although node groups exist in OBM, they do not play a special role.

OBM users 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, if these CIs and relationships are 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 OBM 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. Automatic discovery features of OBM play a central role in these mechanisms. Although OBM allows you to start with a 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 such as Oracle can be created by using the discovery policies that are present in the OBM Management Pack for Oracle.

All management packs contain such discovery policies so that you do not need to think about populating the RTSM by 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 OBM. Every agent sends basic information about itself to its primary manager, and this information is used by OBM to create node, IP address, interface, and Operations Agent CIs with corresponding relationships.

In case there are no management packs, there are several options to populate the RTSM with CIs and CI relationships:

- Use a separate UCMDB and Universal Discovery (known previously as Dependency Mapping and Automation (DDMA)) to discover CIs (additional licenses required) and use UCMDB-BSM Synchronization to synchronize them within the RTSM. For details, see the *RTSM Best Practices* document.
- Use the UCMDB integration features available on the OBM or RTSM system. The available licensing levels are as follows:
    - UCMDB Foundation License (included in the OBM license). This license grants the right to use UCMDB as the backbone component of selected 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 Universal CMDB Web Service API and the Universal CMDB API (Java).
    - UCMDB Integration Only License (not included in the OBM license). This license grants the right to integrate third-party products with UCMDB by using various types of integrations.
    - DDM Advanced Edition License (not included in the OBM license). This license grants the rights to:
        - Integrate BTO and third-party products with UCMDB by using any type of integration
        - Use all Discovery and Dependency Mapping (DDM) capabilities to populate UCMDB

If other domain managers such as NNMi, Microsoft SCOM, or Nagios are integrated into OBM, these integrations add also the topology from those domain managers. Check the corresponding integration documentation for details on the connectors that create node and infrastructure CIs.

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

A similar approach can be used for OBM by using the RTSM Enrichment rules: Enrichment rules can look for the particular node names and then create Running Software CIs. Monitoring Automation could then deploy monitoring aspects to the newly “discovered” CIs automatically.

Related Topics

[Task: How to create CIs by 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 other way around.

In OBM responsibilities can be defined in a very similar way by using user roles that grant permissions to certain views, tool categories, and event categories. Additionally, the Workspace pages can provide OBM 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, because different operator groups might require different information to perform their tasks. Operators that focus on business applications might have other requirements in comparison to operators that focus on the problems on the OS-level. In case one or more operators are part of multiple groups, you could also create a special My Workspace page for them.

Therefore in this planning phase you should determine the number of My Workspace pages and the data they should show, the number of operator roles with different responsibilities and permissions, and the types of events that should be automatically assigned to particular operator groups.

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

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

Related Topics

Create users, user roles, and user groups

Plan integrations

OM integrates with various applications from HPE and other vendors by using a variety of different technologies and interfaces. Many of the HPE product integrations are provided for OBM as well.

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.

Integrations for event enrichment, correlation or automationOM enables 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, OBM offers server-side Stream-Based Event Correlation (SBEC), Topology-Based Event Correlation (TBEC), and the Event Processing Interface (EPI) that 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 replacements in OBM.

OM Composer	OBM
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

- Event integrationsSeveral Operations Connectors exist to integrate 3rd-party domain managers in OBM. Additionally all integrations that are using standard operations agent policies (opcmsg, opcmon, SNMP, Logfile, and so on) can be reused because OBM supports the same policy types. OBM provides the opportunity to leverage new policy types that are not available in OM, such as XML (in Monitoring Automation and Operations Connector), structured log file, Database, REST Web Service Listener (all in Operations Connector).
- Integrations for operatorsImplementation of efficient operator workflow integrations into trouble-ticket or notification systems might be as important as integrations into help systems or knowledge-bases and systems used for the remediation of problems.OBM contains a built-in notification system and a flexible forwarding interface for trouble-ticket or notification system integrations. Out-of-the-box integrations for Service Manager are available. Other incident management systems can be integrated by using the forwarding interface or partner solutions.For details about the event forwarding and notification interfaces, see Administer. For details about integrating external event processes, see Develop. For details about the out-of-the-box integration with Service Manager, see Integrate.OBM integrates with Operations Orchestration, and operators can launch books from their console. Run books can be even executed automatically when events arrive. For more information, seeIntegrate.Like OM, OBM offers an external instruction text interface, which enables you to retrieve instructions from external databases, web pages or other sources. For details about external instructions, see Administer.
- Composer imposes fixed order of execution for each correlation. OBM SBEC rules are executed in the order chosen by the user.Composer has the capability to perform look-ups and extract substrings from message attributes. With OBM, EPI Groovy scripting can perform this function before feeding the events to SBEC.To enable step by step transition from OM Composer Perl scripts to Groovy, you can call Perl scripts from Groovy. 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. With SBEC rules the handling of such events is simplified by identifying either the events that can be withheld or removed, or the need of generating a new event and displaying it to the operators. SBEC can be used as an 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 details about the Event Processing Interface, see Develop.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. All C/Java/COM-based MSI implementations must be replaced by Groovy-based EPI implementations if they cannot be achieved by one of the following OBM features.
    - Topology-Based Event Correlation (TBEC) The Topology-Based Event Correlation license is required for the topology-based event correlation functionality. For details about topology-based event correlation, see Administer.
    - Time-Based Event Automation (TBEA) Time-Based Event Automation rules enable administrators to configure actions to be executed on events that match a user-defined set of criteria after a specified time. For details about time-based event automation, see Administer.
    - Suppression rules Events that match a user-defined filter can be suppressed. For details about event suppression, see Administer.
    - Event Web Service interface OBM offers the Event Web Service interface, which is similar to OM's Incident Web Service interface. It enables you to receive, modify, and create events. If an OM MSI application is taking a feed for external purposes, you could consider implementing it in OBM by using the Event Web Service interface or forwarding it to external event processing. For details, see Develop.
- Integrations for Onboarding and Automation of Configuration OM enables automation of various configuration tasks, such as: node setup, node to node group assignments, policy deployment, policy creation and modification, operator setup, automatic granting of certificates, and 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 OBM, nodes are replaced by Configuration Items and are either discovered or can be created by using RTSM interfaces, or by using the opr-node command. For automatic configuration deployment, OBM users can use Monitoring Automation automatic assignment rules. If a CI is modified or newly discovered, Monitoring Automation automatically evaluates all 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 OBM based on IP ranges or by using a Groovy script. For configuration exchanges between OBM servers, OBM offers the content pack concept. This enables semi-automated configuration exchange. After manually creating or updating a content pack on the source system, you can export and import the content pack on another system by using the Content Manager command-line interface. By using content packs you can exchange various configuration data, such as policy templates and instrumentation files, indicator definitions, user roles, filters, and so on. Similarly, CI Types, views, and other RTSM artifacts can be exchanged by using the RTSM package manager. You can synchronize topology data by using RTSM-RTSM synchronization.

However, OBM currently does not support synchronizing users, user groups, My Workspace pages, or infrastructure settings.

Related Topics Available integrations and integration technologies

Plan monitoring configuration

If you do not plan to use OBM Monitoring Automation, you can skip this step.

OBM Monitoring Automation provides the biggest value when you automate the configuration of Operations Agents or SiteScope. Although OM provides some automation features as well, such as 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 later, we recommend that you evaluate your current monitoring configuration and think about the specific standards you want to establish.

Consider the type of systems and applications (represented in the RTSM as Configuration Items) that should always be monitored in the same way, and the variations necessary for a larger or smaller group of configuration items. Decide which systems should and can be monitored automatically and which systems must always be configured manually.

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. Nevertheless 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, you can start the monitoring of those systems automatically by 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, however, all of 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 newly configured database user and password.

Evaluate your current monitoring configuration

In this planning phase evaluate what your current monitoring looks like: how you are monitoring Oracle databases today, which policies are used, which metrics are collected, and where are the same policies used, but with slightly different thresholds.

You can answer some of these questions by using simple OM database scripts. You can download a policy statistic script, which informs you about the used policies, from the ITOM Marketplace.

As a next step you should determine if your monitoring needs can be addressed by the Infrastructure Management Pack, which comes without charge with OBM, or by other management packs.

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

In case you created policy versions or copies of policies to change thresholds or parameters, such as message groups or custom attributes, it is not required to import all these policies. You can import one base policy and then use the OBM parameterization feature to implement all variations.

Related Topics

ITOM Marketplace

Plan license migration

When planning license migration, consider the following:

- Optional Operations Bridge License Exchange Program The Operations Bridge License Exchange Program 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 OBM Management Pack licenses. This license exchange allows customers to continue to concurrently use their existing software (such as OM and SPIs), which then enables customers to move to OBM, Operations Bridge Reporter, and Operations Bridge Management Packs at their own pace. For more information, contact your HPE account team or HPE partner.
- TBEC license The Operations Bridge License Exchange Program does not include the OBM 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 is not expired. It is activated when OBM is installed. If OBM is already in use, request a new temporary evaluation license from the Software License Center.

Introducing OBM

See the following sections for information about OBM's infrastructure topology, event consolidation, and event control:

- Establish infrastructure topology
- Consolidate events from various sources
- Control events

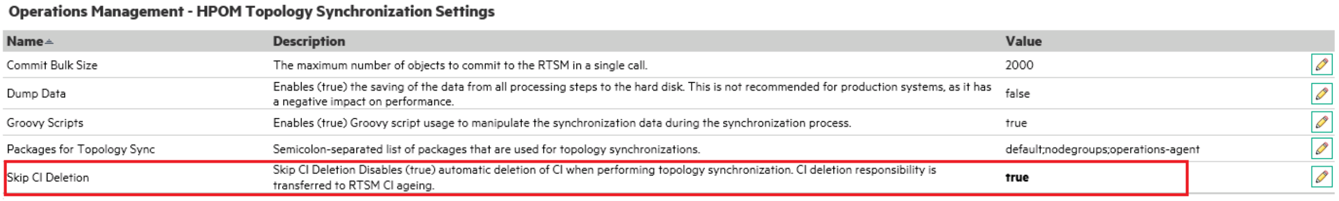
Establish infrastructure topology

As described in the planning phase, OBM offers various advantages when the monitored IT objects 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.

Establishing infrastructure topology involves creating the following:

- Node and infrastructure CIs (by using topology-synchronization of OM node and service data) As an OM user, the easiest way to populate the RTSM is by using the data that is already available in OM. OBM topology synchronization enables you to create CIs based on the OM nodes, node groups, layout groups and SPI service models. You can specify the SPI service models that 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), and SAP. See the following information in the Integrate section:
  - Establishing a trust relationship between OBM and OM
  - Setting up the OM server as a connected server
  - Synchronizing the topology
- Node CIs Node CIs (and corresponding IP address and Operations Agent CIs) are either created by using topology synchronization or automatically for all nodes that run an Operations Agent when an agent is installed and connected to OBM. Every agent sends basic information about itself to its primary manager and this information is used by OBM to create node, IP address, interface and Operations Agent CIs with corresponding relationships. However, if you perform a lot of proxy monitoring where one agent acts as proxy and creates events for various other nodes (for example, by using SNMP policies), these nodes must 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.
- Node CIs manually (proxied) The easiest way to create node CIs manually is by using **Administration > Setup and Maintenance > Monitored Nodes**. For details, see the Administer section.
- Infrastructure CIs Infrastructure CIs can be created by 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 OBM, when SPIs are no longer used, it is necessary to replace the SPI discovery with corresponding OBM Management Pack discovery aspects (if available). Removing a SPI discovery policy from a node triggers the deletion of services in OM and of CIs in the OBM RTSM. To prevent this from happening, set the Skip CI Deletion infrastructure setting (**Applications > Operations Management > HPOM Topology Synchronization Settings**) to true. This disables 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. For details on how to deploy the discovery aspects, see the corresponding Management Pack Online Help section. If no Management Pack exists, there are several ways to populate the RTSM with CIs and CI relationships. If Operations Connector is used to integrate other domain managers, it can also integrate topology from those domain managers. Details about Operations Connector installation and topology policies are provided in the Operations Connector installation instructions. The documentation of the specific Operations Connectors is available on the ITOM Marketplace and in the Operations Connector Help.

Task: How to create CIs by 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, RHFINTST for Red Hat, Finance application, Test system), then enrichment rules can look for particular nodes and create RunningSoftware CIs.

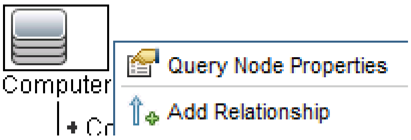
This is possible as long as there is only one RunningSoftware CI per node and if the RunningSoftware CI creation does not require additional identification attributes or key attributes. Enrichment rules are not a suitable solution for creating Oracle database CIs, because multiple Oracle instances can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

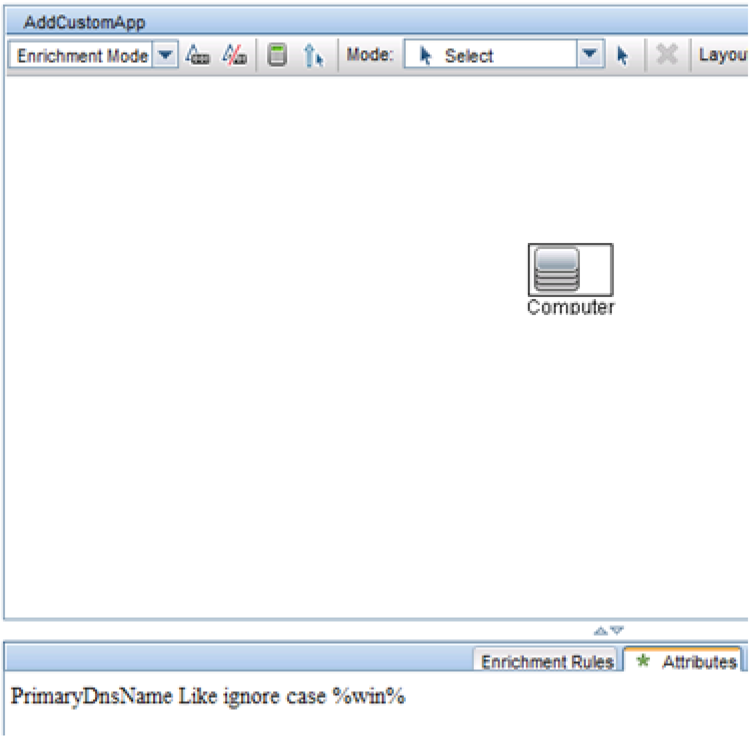
For information on creating enrichment rules by using the enrichment manager, go to **Administration > RTSM Administration > Modeling > Enrichment manager**. For details, see the OMi Help.

The following example shows the most important settings. It assumes that a new Custom Application CI type is created as a subtype of the RunningSoftware CI, inheriting all settings, such as attributes and the identification rule.

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

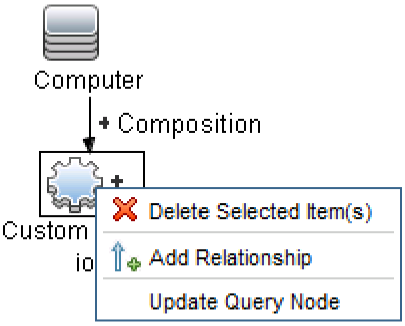
1. Create a new enrichment rule.
   Add the computer CI type and use Query Node Properties to filter the nodes: about node queries. For details about Query Node Properties, see the OMi Help. The example rule looks for all nodes that contain “win” in the PrimaryDnsName, as shown in the Attributes tab of the Computer CIT:

   PrimaryDnsName Like ignore case %win%

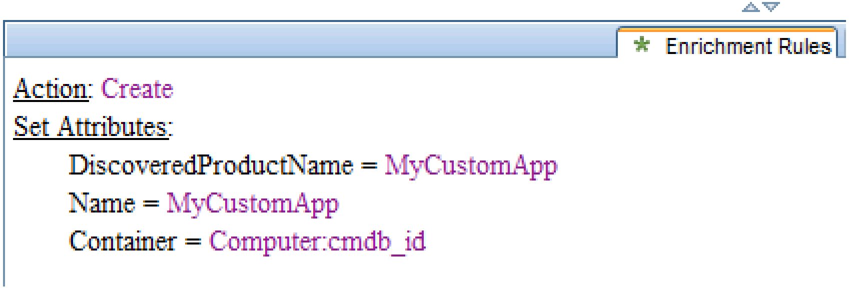
2. Switch to enrichment mode, add the custom application CI type, and then create the composition relationship between CI



Delete Selected Item(s)
Add Relationship
Update Query Node

type and the node. Use Update Query Node:

3. Provide a Name and DiscoveredProductName, because these attributes are required for identifying a RunningSoftware CI. The enrichment rule summary is shown on the Enrichment Rules tab:



Enrichment Rules

Action: Create

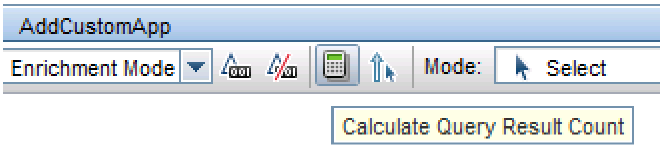
Set Attributes:

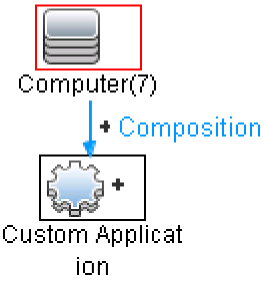
DiscoveredProductName = MyCustomApp

Name = MyCustomApp

Container = Computer:cmdb_id

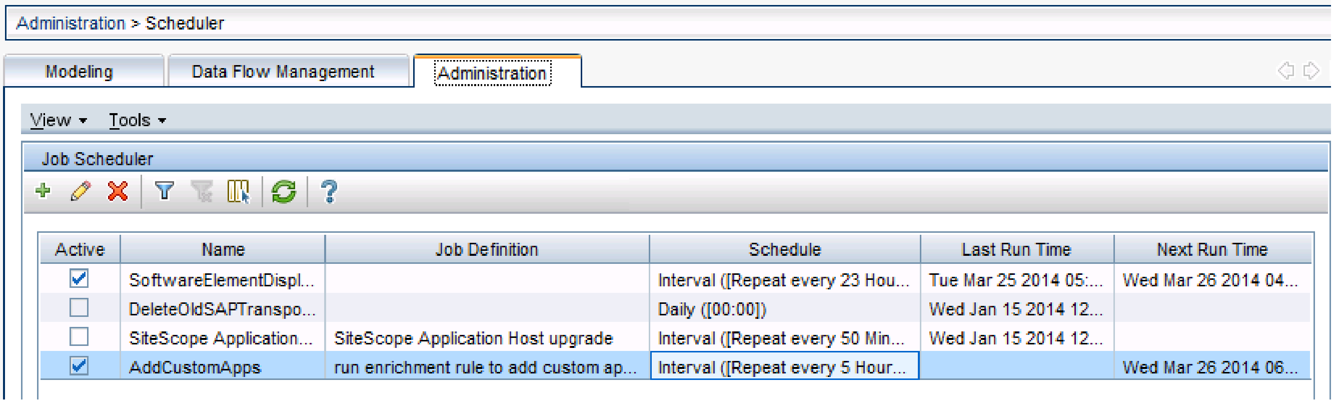
You can use the Calculate Query Result Count button to check how many Computers currently match the query. In this example there are seven matching



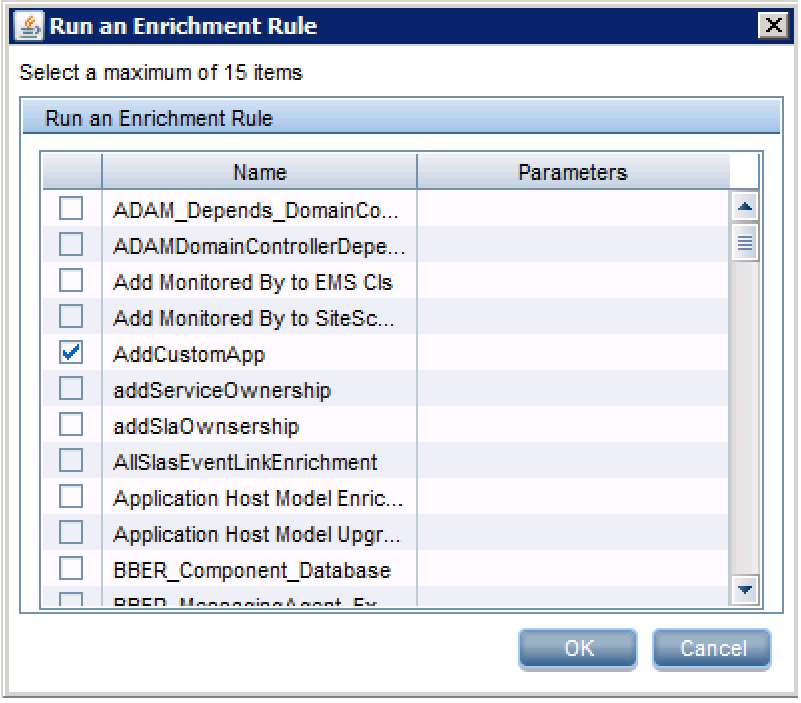


Computers.

4. 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 that you created and define a schedule, for example, once per day.



Active	Name	Job Definition	Schedule	Last Run Time	Next Run Time
☑	SoftwareElementDispl...		Interval ([Repeat every 23 Hou...	Tue Mar 25 2014 05:...	Wed Mar 26 2014 04...
□	DeleteOldSAPTranspo...		Daily ([00:00])	Wed Jan 15 2014 12...	
□	SiteScope Application...	SiteScope Application Host upgrade	Interval ([Repeat every 50 Min...	Wed Jan 15 2014 12...	
☑	AddCustomApps	run enrichment rule to add custom ap...	Interval ([Repeat every 5 Hour...		Wed Mar 26 2014 06...



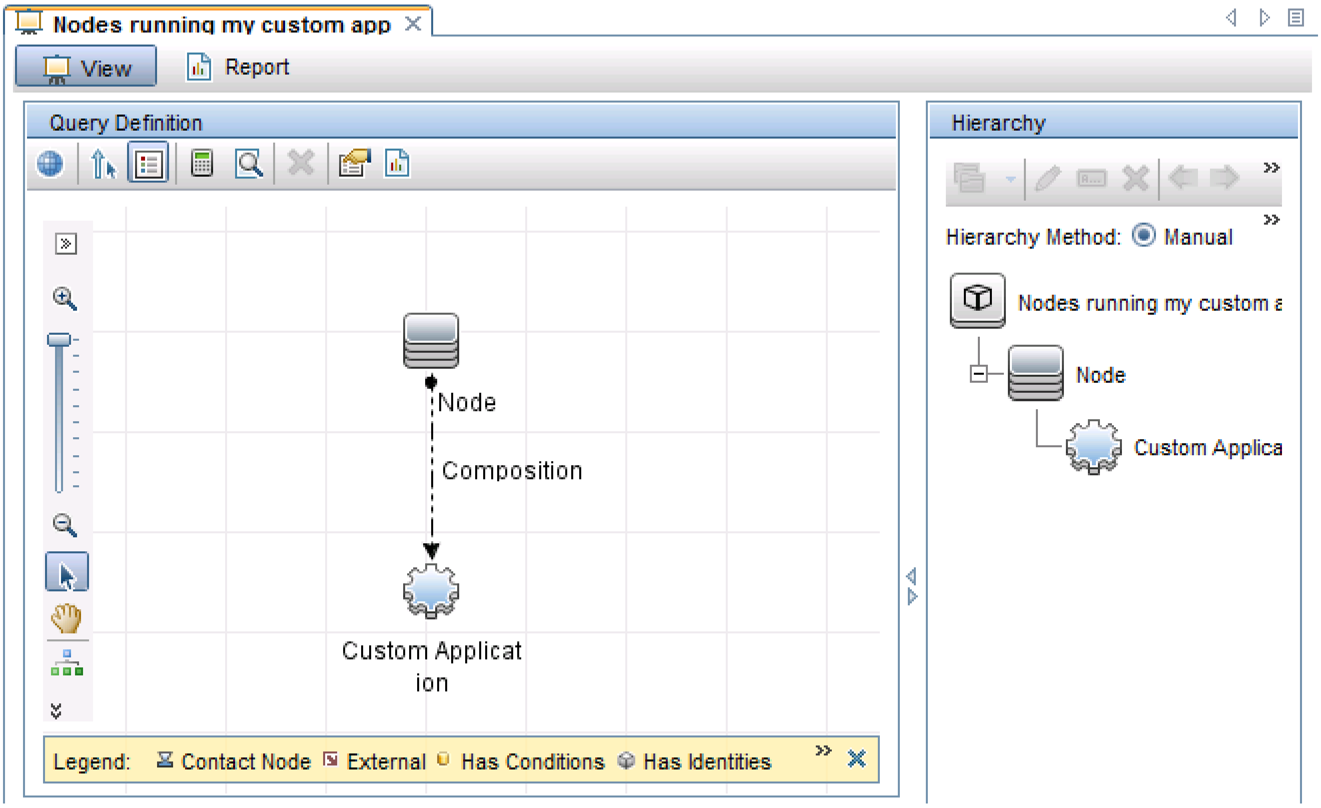
Run an Enrichment Rule

Select a maximum of 15 items

Run an Enrichment Rule

	Name	Parameters
□	ADAM_Depends_DomainCo...	
□	ADAMDomainControllerDepe...	
□	Add Monitored By to EMS CIs	
□	Add Monitored By to SiteSc...	
☑	AddCustomApp	
□	addServiceOwnership	
□	addSlaOwnsership	
□	AllSlasEventLinkEnrichment	
□	Application Host Model Enric...	
□	Application Host Model Upgr...	
□	BBER_Component_Database	
□	BBER_ManagingAgent_Ex	

If needed, you can use the Modeling Studio to create a view that shows all nodes with the Custom Application software running, for example, by using a simple pattern view:



Hierarchy Method: ● Manual

Related Topics Technologies for Establishing Infrastructure Topology ITOM Marketplace

Consolidate events from various sources

After establishing the infrastructure topology it is required to integrate events. Because the necessary CI topology already exists, OBM CI resolver can relate events to the correct CIs, which enables view-based filtering and other CI-type specific functions.

Consolidating events involves connecting the following:

- OM to OBM For the information on forwarding events from OM to OBM, see the following procedures in Integrate:
  - Configuring the OM forwarding policy
  - Validating event synchronization **Note**: Other steps are completed when integrating the topology of OM.
- SiteScope to OBM For the information on forwarding events from SiteScope, see the SiteScope Manual Integration with Operations Manager Products.
- Other domain managers to OBM by using Operations Connectors For the information on forwarding events from other event managers, see the documentation of the specific Operations Connectors that is available on the ITOM Marketplace and the Operations Connector Help.

Related Topics

ITOM Marketplace

Control events

When events are integrated, you can use OBM correlation, enrichment, and automation features to control events. Controlling events is described in the following sections:

Contents

Event correlation

If you plan to use event correlation, get familiar with the following:

- Duplicate suppression The duplicate suppression concepts are similar in OBM and OM. However, OBM can detect duplicates based on ETI values, which is not possible in OM. If required, you can change the default duplicate suppression settings in **Administration > Setup and Maintenance > Infrastructure Settings**. Select **Applications**, set the administration context to **Operations Management**, and then navigate to **Operations Management - Duplicate Events Suppression Settings**.
- Closing related events Like OM, OBM can close related events based on message keys and key-matching patterns. OBM also can detect related events based on HI values. If required, you can change the default settings in **Administration > Setup and Maintenance > Infrastructure Settings**. Select **Applications**, set the administration context to **Operations Management**, and then navigate to **Operations Management - Change State of Related Events Settings**.

Stream-Based Event Correlation (SBEC)

Stream-Based Event Correlation (SBEC) uses rules and filters to identify commonly occurring events or combinations of events. With SBEC rules the handling of such events is simplified by identifying either the events that can be withheld or removed, or the need of generating a new event and displaying it to the operators. SBEC can be used as an OM ECS replacement.

The following types of SBEC rules can be configured:

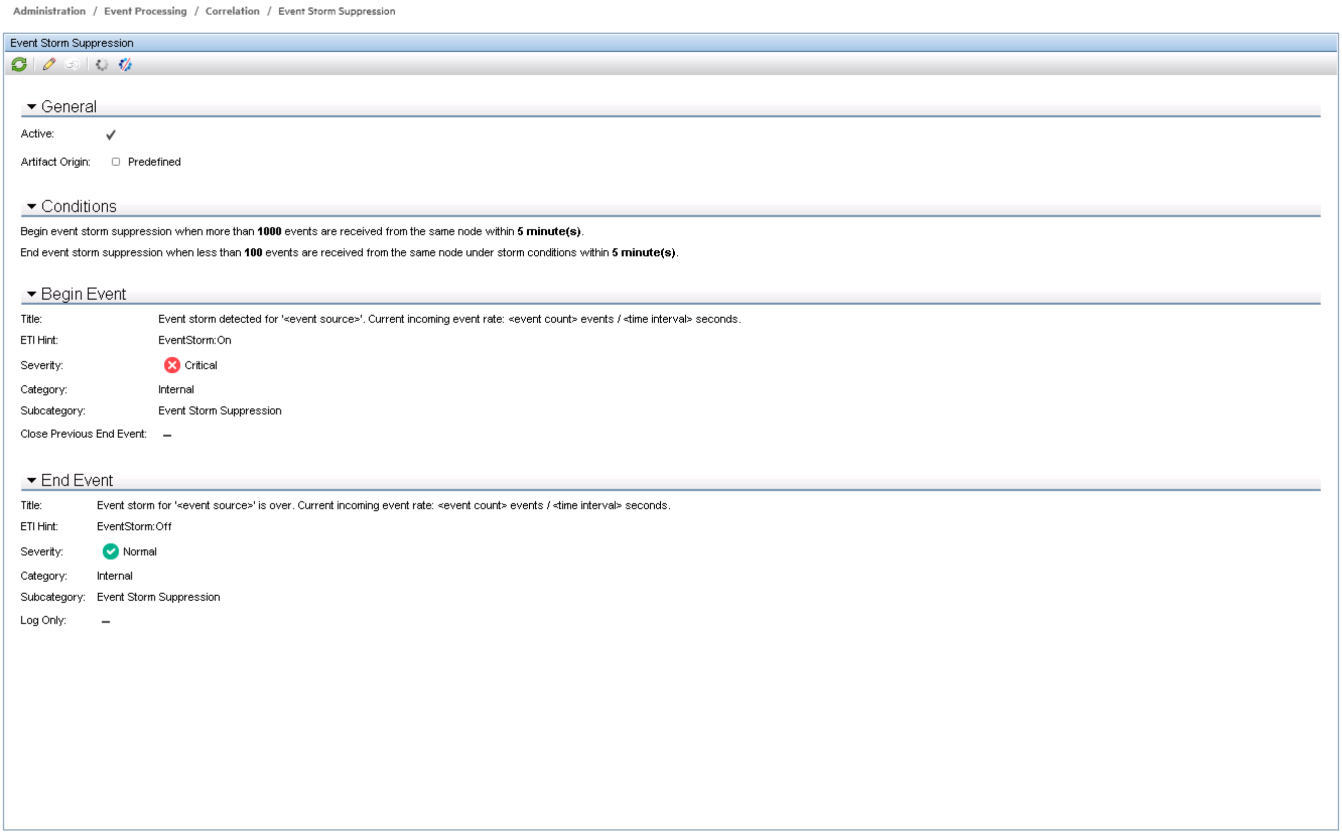
- Repetition Rules: Frequent repetitions of the same event may indicate a problem that requires attention.
- Combination Rules: A combination of different events occurring together or in a particular order indicates an issue, and requires special treatment.
- Missing Recurrence Rules: A regularly recurring event is missing, for example, a regular heartbeat event 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.

For details about SBEC go to **Administration > Event Processing > Correlation > Stream-Based Event Correlation** and see the corresponding OMi Help topics and the SBEC tutorials.

Consider also the following:

- Topology-Based Event Correlation (TBEC) The Topology-Based Event Correlation license is required for the topology-based event correlation (TBEC) functionality. For details about topology-based event correlation, see the Administer section. If you are using OM SPIs, you can benefit from TBEC, because these 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, TBEC cannot correlate them. We recommend that you add Event Type Indicators to your custom policies later.
- Event storm suppression Like OM, OBM 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.



Administration / Event Processing / Correlation / Event Storm Suppression

Event Storm Suppression

General

Active: ✓

Artifact Origin: □ Predefined

Conditions

Begin event storm suppression when more than **1000** events are received from the same node within **5 minute(s)**.

End event storm suppression when less than **100** events are received from the same node under storm conditions within **5 minute(s)**.

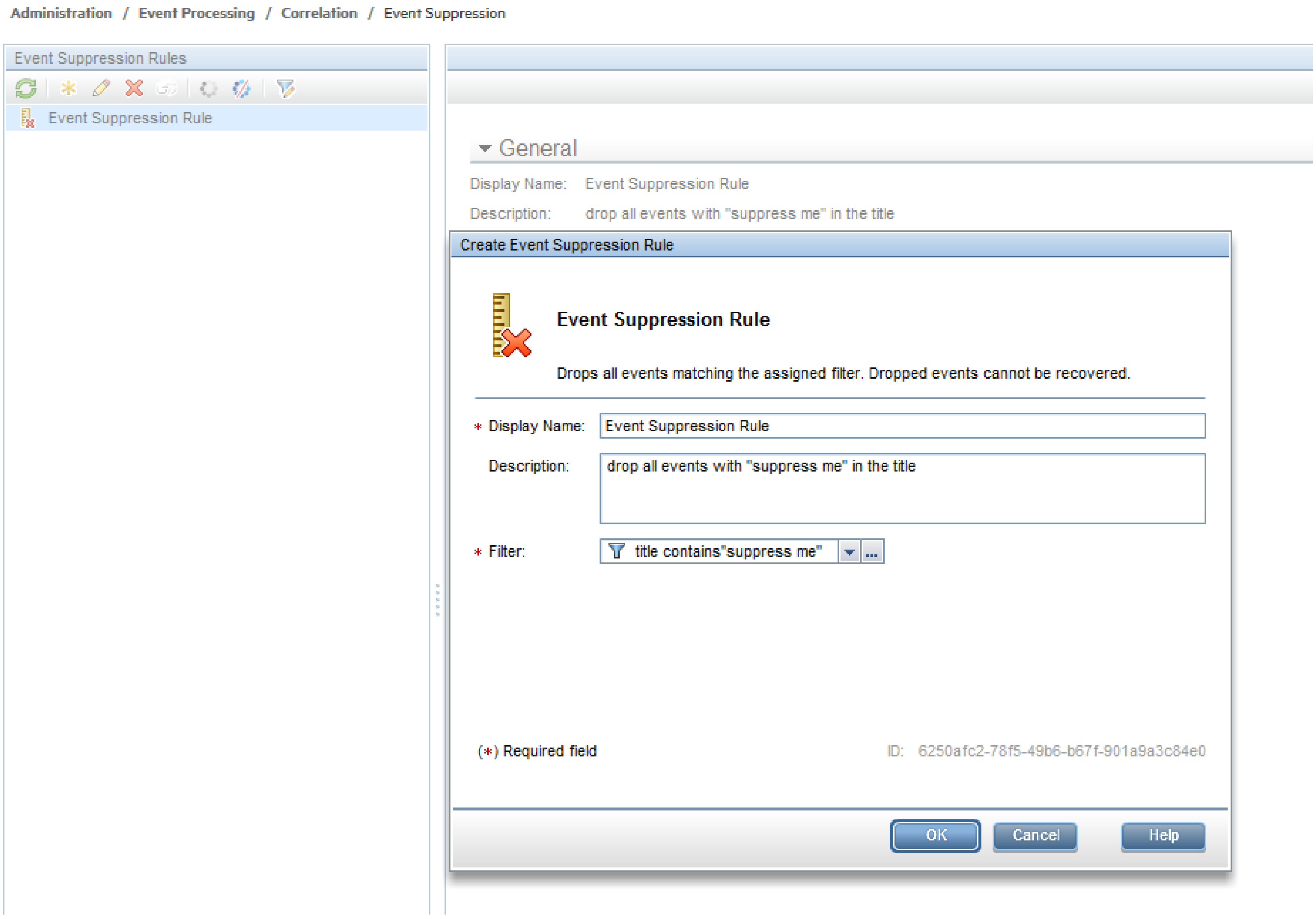
Begin Event

Title:	Event storm detected for '<event source>'. Current incoming event rate: <event count> events / <time interval> seconds.
ETI Hint:	EventStorm:On
Severity:	☒ Critical
Category:	Internal
Subcategory:	Event Storm Suppression
Close Previous End Event:	–

End Event

Title:	Event storm for '<event source>' is over. Current incoming event rate: <event count> events / <time interval> seconds.
ETI Hint:	EventStorm:Off
Severity:	✓ Normal
Category:	Internal
Subcategory:	Event Storm Suppression
Log Only:	–

- Event suppression OBM can suppress events on the server by 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. For more details, go to **Administration > Event Processing > Correlation > Event Suppression** and see the corresponding OMi Help topics.



Administration / Event Processing / Correlation / Event Suppression

Event Suppression Rules

Event Suppression Rule

General

Display Name: Event Suppression Rule

Description: drop all events with "suppress me" in the title

Create Event Suppression Rule

Event Suppression Rule

Drops all events matching the assigned filter. Dropped events cannot be recovered.

* Display Name: Event Suppression Rule

Description: drop all events with "suppress me" in the title

* Filter: title contains"suppress me"

(*) Required field

ID: 6250afc2-78f5-49b6-b67f-901a9a3c84e0

Event enrichment and custom processing through EPIs

Event processing customization enables you to implement custom script-based event processing directly on events. You can do this during 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 must be supplied as a Groovy script. A number of sample scripts are available in the following directory:

```
<OMi_HOME>/opr/examples/epi_scripts
```

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

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

For more details, go to **Administration > Event Processing > Automation > Event Processing Customizations** and see the corresponding OMi Help topics.

EPI Script Development Kit

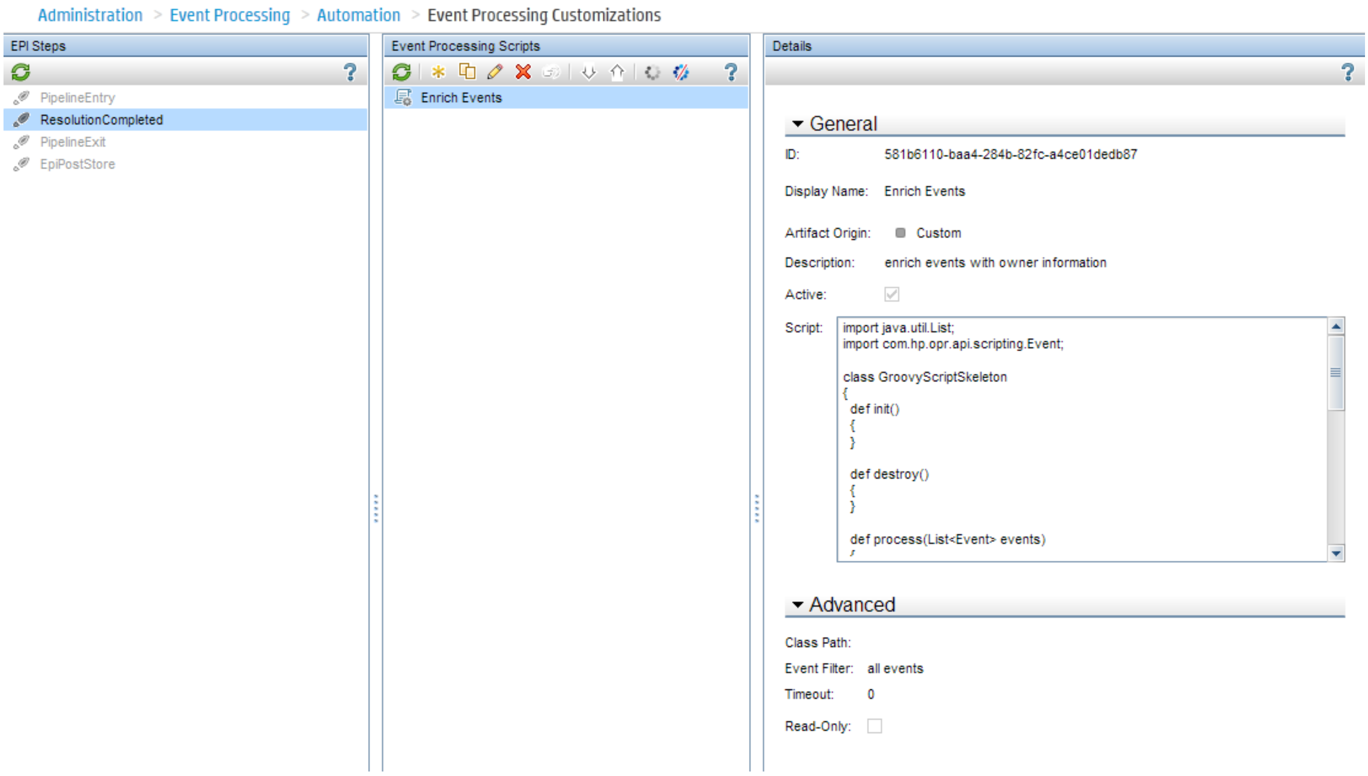
The OBM Script Development Kit available under `<HPBSM>\opr\support\script-devkit` helps script developers to edit, validate, test, and debug their HPE OBM Groovy scripts within Eclipse, outside of an HPE OBM installation. The benefits of using the OBM Script Development Kit in Eclipse include:

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

Example of an EPI script used 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.setHint("My Hint");
    hints.setIpAddress("0.0.0.0");
    return hints;
    hints.setDnsName("mydqdn.com");
  }


  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:



ID: 581b6110-baa4-284b-82fc-a4ce01dedb87

Display Name: Enrich Events

Artifact Origin: Custom

Description: enrich events with owner information

Active: ☑

Script:

```
import java.util.List;
import com.hp.opr.api.scripting.Event;

class GroovyScriptSkeleton
{
 def init()
 {
 }

 def destroy()
 {
 }

 def process(List<Event> events)
```

Class Path:

Event Filter: all events

Timeout: 0

Read-Only: □

Event automation

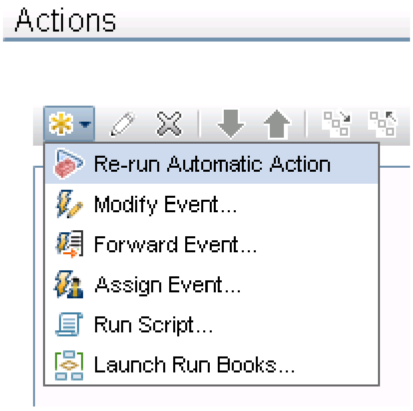
Some of the automation features described in the following section refer to operators or operator groups that are created in a later phase. Therefore, the implementation of these operator-focused automations might have to be completed later. If the operator groups are already defined, you can refer to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

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.

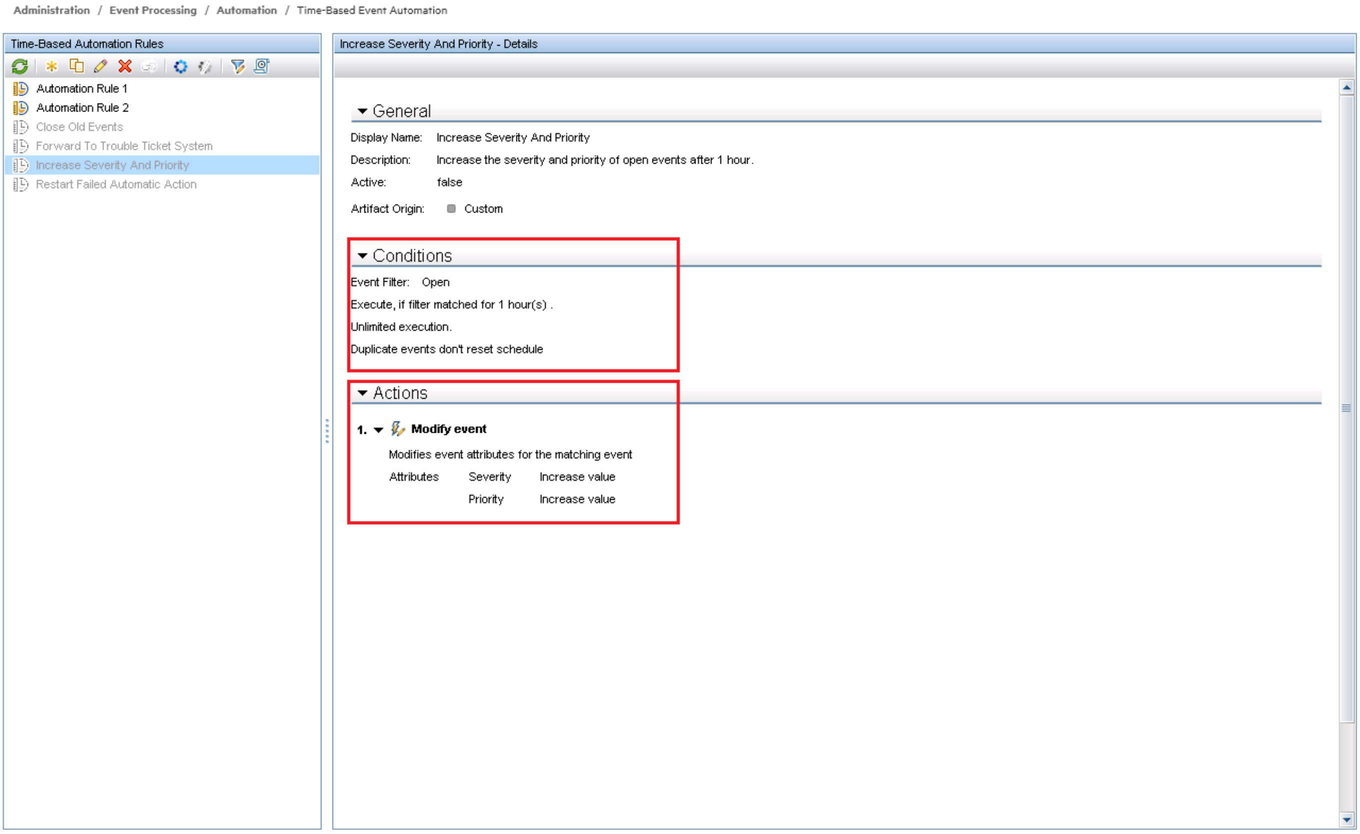
- If an automatic action for a message fails, you can configure a restart of the automatic action after a short delay. If it repeatedly fails, after a predefined number of retries further retries are stopped and the event is escalated.
- If an event is not being addressed for a predefined period in time, 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, to escalate if an event remains in the browser for more than two days, and to close if the message remains for longer than seven days (despite the escalation after two days).

The following figure shows available actions for Time-Based Event Automation rules:



For more details, go to **Administration > Event Processing > Automation > Time-Based Event Automation** and see the corresponding OMi Help topics.

The following example shows a time-based event automation scenario, which increases the severity of an open event after one hour:


Administration / Event Processing / Automation / Time-Based Event Automation
Time-Based Automation Rules
Automation Rule 1
Automation Rule 2
Close Old Events
Forward To Trouble Ticket System
Increase Severity And Priority
Restart Failed Automatic Action
Increase Severity And Priority - Details

General

Display Name: Increase Severity And Priority

Description: Increase the severity and priority of open events after 1 hour.

Active: false

Artifact Origin: Custom

Conditions

Event Filter: Open

Execute, if filter matched for 1 hour(s) .

Unlimited execution.

Duplicate events don't reset schedule

Actions

1. Modify event

Modifies event attributes for the matching event

Attributes	Severity	Increase value
	Priority	Increase value

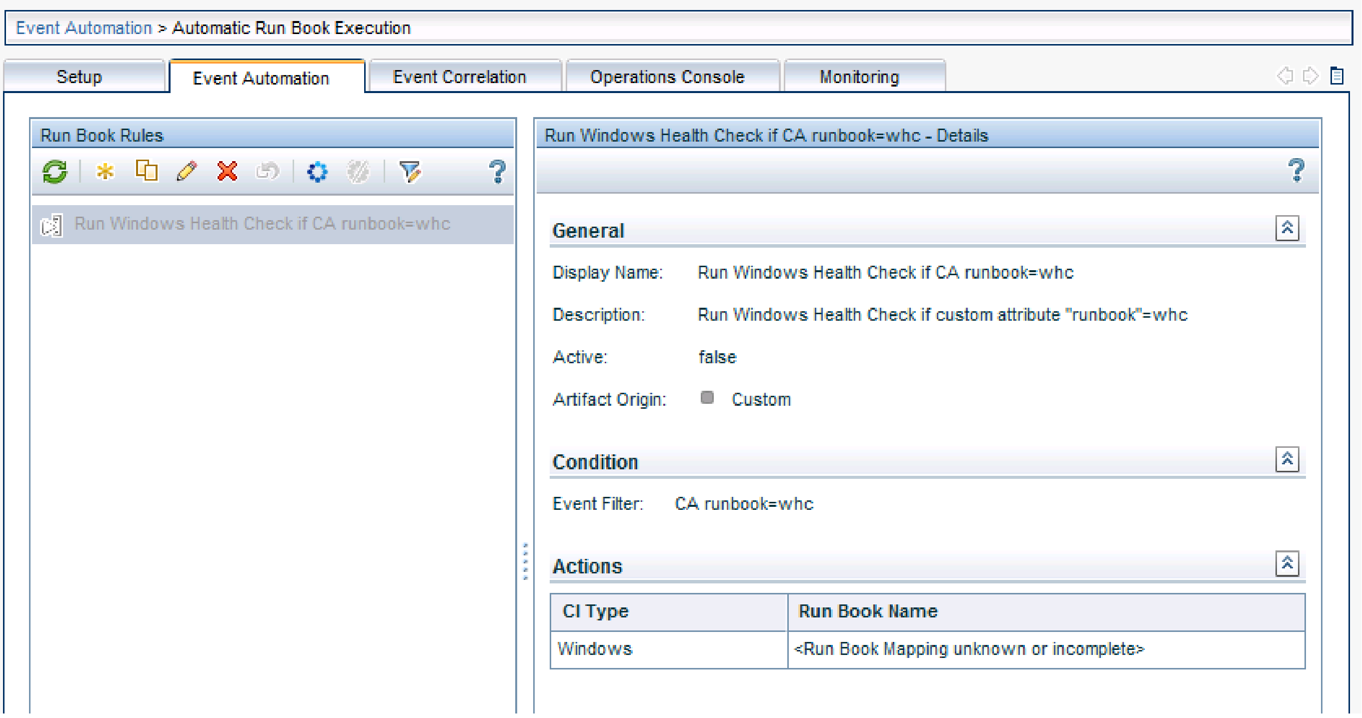
Automatic run book execution

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

To achieve this, you first have to integrate OO into OBM and map OO run books to CI Types. For more details, see the Integrate section. This integration also enables operators to launch run books manually. You can use these run books in automatic run book execution rules as follows:

1. Go to **Administration > Event Processing > Automation > Automatic Run Book Execution**.
2. Create a new rule and specify an event filter for which the run book should be executed, and then select the run book.You will be able to select run books only after completing the OO integration.

Example of the automatic run book execution rule:



Event Automation > Automatic Run Book Execution
Setup
Event Automation
Event Correlation
Operations Console
Monitoring
Run Book Rules
Run Windows Health Check if CA runbook=whc
Run Windows Health Check if CA runbook=whc - Details
General
Condition
Actions

Display Name: Run Windows Health Check if CA runbook=whc

Description: Run Windows Health Check if custom attribute "runbook"=whc

Active: false

Artifact Origin: ■ Custom

Event Filter: CA runbook=whc

CI Type	Run Book Name
Windows	<Run Book Mapping unknown or incomplete>

Automatic user group assignments

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

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

This requires operator groups to be already 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 such as Service Manager.

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

- Incidents where the corresponding events are related
- Displaying current incident attributes (lifecycle, assigned group, severity, priority) in the event
- Lightweight 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

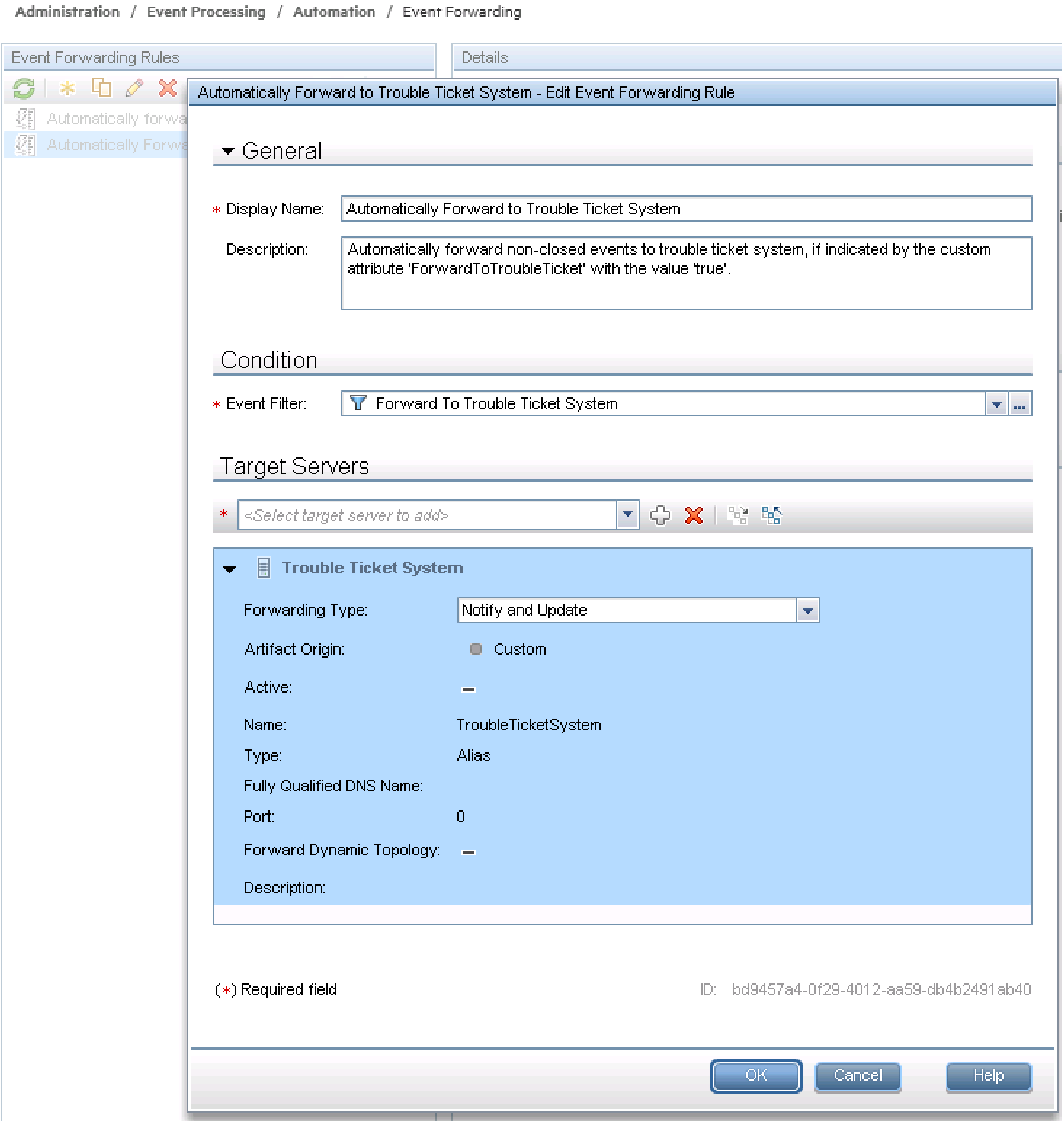
You can forward events either by using a Groovy script that accesses specific APIs of the external server or through an event web service interface that must be implemented by the external server.

For details about integrating external event processes, see the Develop section. For details about the Event Forwarding manager, see the Administer section. For details about the out-of-the-box integration with Service Manager, see the Integrate section.

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.

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

OBM provides a default forwarding rule named 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 must only specify the server to be used.



Administration / Event Processing / Automation / Event Forwarding

Automatically Forward to Trouble Ticket System - Edit Event Forwarding Rule

General

* Display Name: Automatically Forward to Trouble Ticket System

Description: Automatically forward non-closed events to trouble ticket system, if indicated by the custom attribute 'ForwardToTroubleTicket' with the value 'true'.

Condition

* Event Filter: Forward To Trouble Ticket System

Target Servers

* <Select target server to add>

Trouble Ticket System

Forwarding Type: Notify and Update

Artifact Origin: Custom

Active: —

Name: TroubleTicketSystem

Type: Alias

Fully Qualified DNS Name:

Port: 0

Forward Dynamic Topology: —

Description:

(*) Required field

ID: bd9457a4-0f29-4012-aa59-db4b2491ab40

By default, the Notify and Update forwarding type is used. However, depending on your requirements, you can use also other forwarding types. The following forwarding types are available:

- Notify and Update: target server receives original events and all further updates (event is closed in OBM).
- Synchronize: target server receives original events and all further updates, and sends back all updates (event can be closed by OBM or by the target server through the 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 is closed by the target server through the event sync web service).

Event integrations through web services and CLI

OBM offers Event Web Service for integrating events into other applications and for automating operator functions. This is a REST-based web service that enables you to perform all operator tasks available in the UI 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 by using the Atom service.

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

For details about automating operator functions and event change detection, see the Develop section.

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 the following operations on one or multiple events:

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

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

OM and OBM CLI functionality comparison

The following table compares auditing functionality in OM and OBM.

Functionality	OM for UNIX	OM for Windows	OBM

Close events	`opcmack` (agent)
	`opcack`
	`opcackmsg`
	`opcackmsgs`
		`opcmack` (agent)
		`ovowmsgutil*`
		Create a VB script by using WMI methods
			Through Incident web service / RestWsUtil CLI or by using `opr-close-events[.bat|.sh]`:
			• Closes all events or the ones that are based on one of the following: date range for the received events, severity, related CI, node CI, title
			• Designed to be run when the UI is not running because it does not update running UIs

Reopen closed events	`opcunack`	`ovowmsgutil*` Create a VB script by using WMI methods	Through Incident web service / RestWsUtil CLI
Set, unset, and change ownership	`opcownmsg`	`ovowmsgutil*` Create a VB script by using WMI methods	Through Incident web service / RestWsUtil CLI
Add, modify, remove, and list custom attributes	`opccmachg`	Create a VB script by using WMI methods	Through Incident web service / RestWsUtil CLI
Add and list annotations	`opcannoadd` `opcannoget`	Create a VB script by 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 by using WMI methods	Through Incident web service / RestWsUtil CLI
Read events	`opcgetmsgdet` `opcmsgsrpt`	Create a VB script by 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]`:
			• Downloads closed events based on the date range, severity, category, and node from the database
			• Uploading archived events is not supported
			`opr-export-events[.bat|.sh]` and `opr-import-events[.bat|.sh]`:
			Support exporting and importing of all or selected events in any part of the lifecycle

- `ovowmsgutil` runs bulk operations on messages. It makes changes directly to the database, stopping some OM for Windows services during the execution.

Running external programs from Groovy

There is currently no tool available for exporting and importing OM Composer elements into OBM. However, you can reuse Perl scripts that were used in OM Composer to enrich events, inside OBM EPI scripts. This is possible because Groovy allows running external programs, and therefore can run a Perl interpreter and a Perl script. With Groovy you can also use the execution function to start an external program.

Example of launching an OM-based Perl script

```
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 described function with the following code:

```
ret=start_exec( ["perl.exe", "your_perl_code.pl", “parameter2”]);
```

The package jerlWrapper.perlVM is available from Google, which might perform faster when loaded into the EPI script init area.

Downtime handling

OBM downtime is scheduled to occur either once or on a recurring basis. It is based on selected CIs and their relationships in the RTSM, and it dynamically listens to topology changes. For example, if a node CI is put into downtime, all impacted CIs are put into downtime as well: if there are two Oracle instances on the node at the time, they are both 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, and execute EPI scripts and automatic run books.

Other actions during downtime can be suppression of notifications, setting KPIs to downtime status, and disabling SiteScope monitors. For details about downtime management, see the Administer section.

While a downtime is active, you cannot modify it. You can delete it from the JMX console.

OM and OBM downtime functionality comparison

The following table compares downtime functionality in OM and OBM.

Functionality	OM for UNIX	OM for Windows	OBM
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, and business service • Included CI Types can be added or changed • 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	No
Automation	Yes, through outage file editing and opccfgout CLI	Yes, through ovownodeutil and ovowserviceutil CLI	Yes, through Downtime REST API and `opr-downtime` CLI
User permission	• Create tools that execute opccfgout to set unplanned outage • Create tools that assign node to node group in “maintenance” • Grant user access to the tools	• Permission to set unplanned outage on nodes or services in user’s responsibilities • Permission for specific policies (for example, for scheduled outage)	Permission to: • View or to have full control of scheduled downtimes • Set downtime for CIs in views to which the user has access

Related Topics

Plan the evolution

SBEC Tutorials

Add value on top

jerlWrapper.perlVM

BSM 9.0x: How to stop a Downtime

Establish an effective operator workflow

See the following sections for information on how to establish an effective operator workflow:

- Move operators from OM to OBM
- Implement integrations for operators
- Recreate custom tools
- Performance dashboards
- Prepare operator console

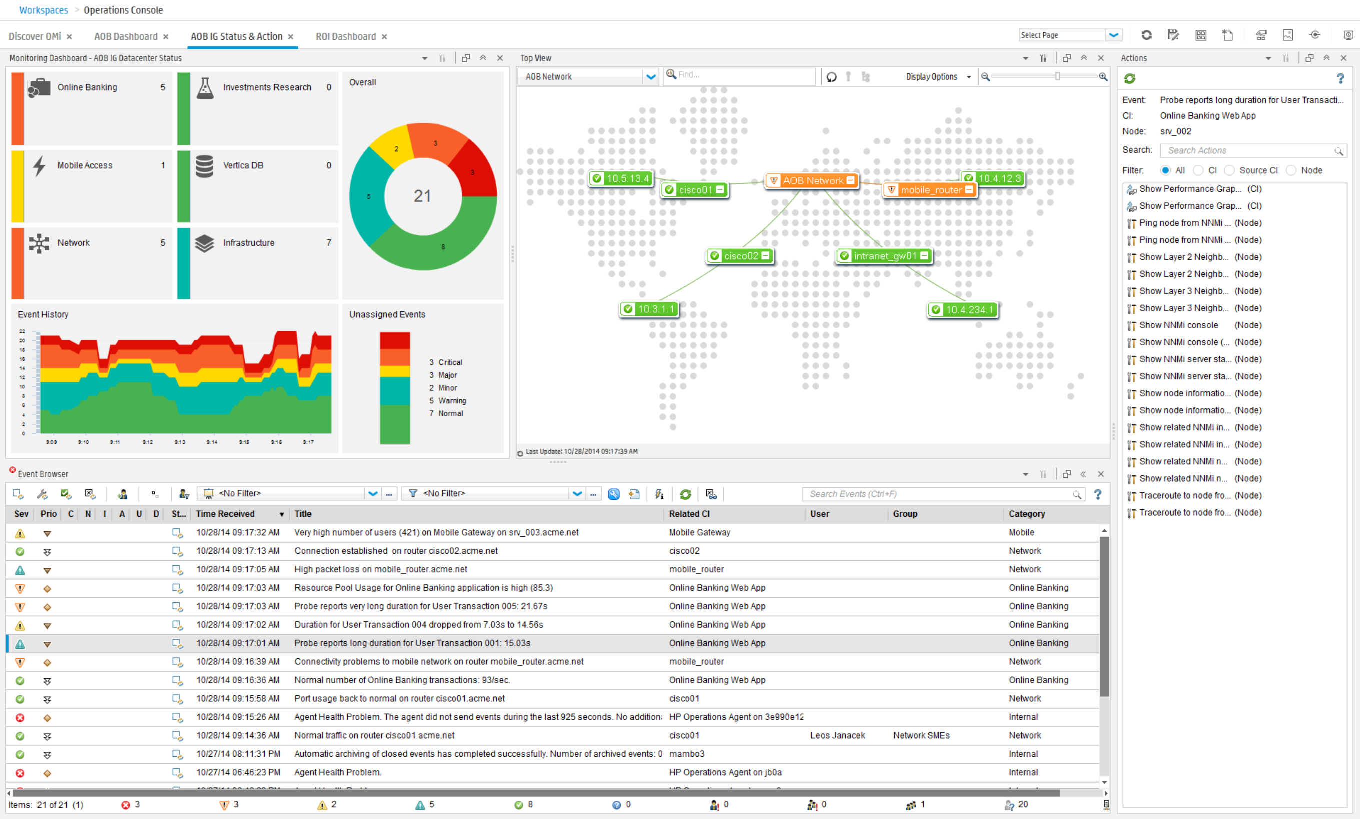
Move operators from OM to OBM

OBM enables building one or more customized operator My Workspace pages for each operator group or an individual operator with its My Workspace framework and UI components such as Event Browser, View Explorer, Monitoring Dashboard, Watch List, Top View, Actions, or Business Impact.

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 the action panel.

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



Sev	Prio	Time Received	Title	Related CI	User	Group	Category
⚠	▼	10/28/14 09:17:32 AM	Very high number of users (421) on Mobile Gateway on srv_003.acme.net	Mobile Gateway			Mobile
✓	≚	10/28/14 09:17:13 AM	Connection established on router cisco02.acme.net	cisco02			Network
⚠	▼	10/28/14 09:17:05 AM	High packet loss on mobile_router.acme.net	mobile_router			Network
!	◇	10/28/14 09:17:03 AM	Resource Pool Usage for Online Banking application is high (85.3)	Online Banking Web App			Online Banking
!	◇	10/28/14 09:17:03 AM	Probe reports very long duration for User Transaction 005: 21.67s	Online Banking Web App			Online Banking
⚠	▼	10/28/14 09:17:02 AM	Duration for User Transaction 004 dropped from 7.03s to 14.56s	Online Banking Web App			Online Banking
⚠	▼	10/28/14 09:17:01 AM	Probe reports long duration for User Transaction 001: 15.03s	Online Banking Web App			Online Banking
!	◇	10/28/14 09:16:39 AM	Connectivity problems to mobile network on router mobile_router.acme.net	mobile_router			Network
✓	≚	10/28/14 09:16:36 AM	Normal number of Online Banking transactions: 93/sec.	Online Banking Web App			Online Banking
✓	≚	10/28/14 09:15:58 AM	Port usage back to normal on router cisco01.acme.net	cisco01			Network
✗	◇	10/28/14 09:15:26 AM	Agent Health Problem. The agent did not send events during the last 925 seconds. No addition:	HP Operations Agent on 3e990e12			Internal
✓	≚	10/28/14 09:14:36 AM	Normal traffic on router cisco01.acme.net	cisco01	Leos Janacek	Network SMEs	Network
✓	≚	10/27/14 08:11:31 PM	Automatic archiving of closed events has completed successfully. Number of archived events: 0	mambo3			Internal
✗	◇	10/27/14 06:46:23 PM	Agent Health Problem.	HP Operations Agent on jb0a			Internal

Items: 21 of 21 (1) ✗ 3 ! 3 ⚠ 2 ⚠ 5 ✓ 8 ? 0 0 0 1 20

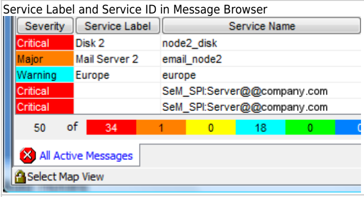
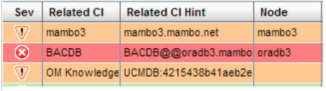
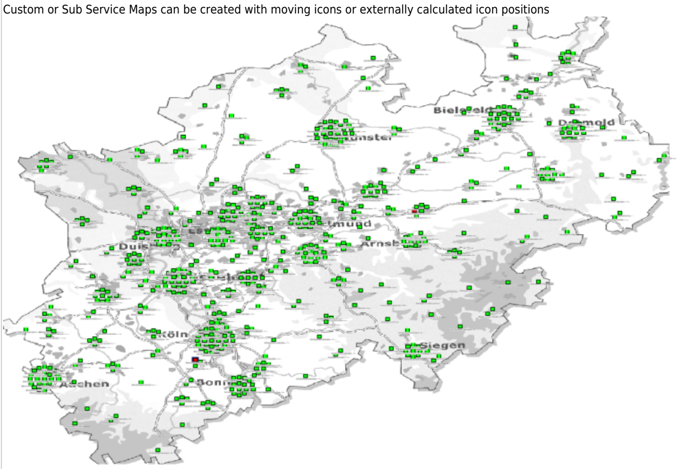
Actions

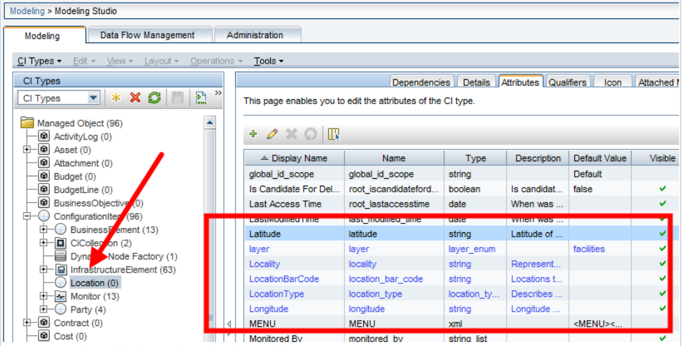
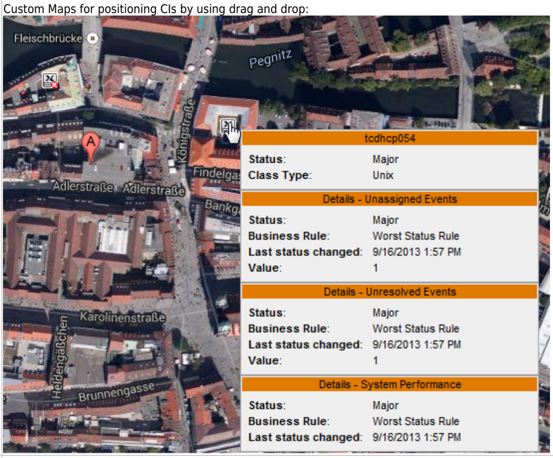
Event: Probe reports long duration for User Transacti...
CI: Online Banking Web App
Node: srv_002
Search: Search Actions
Filter: ● All ○ CI ○ Source CI ○ Node

- Show Performance Grap... (CI)
- Show Performance Grap... (CI)
- Ping node from NNMi ... (Node)
- Ping node from NNMi ... (Node)
- Show Layer 2 Neighb... (Node)
- Show Layer 2 Neighb... (Node)
- Show Layer 3 Neighb... (Node)
- Show Layer 3 Neighb... (Node)
- Show NNMi console (Node)
- Show NNMi console (... (Node)
- Show NNMi server sta... (Node)
- Show NNMi server sta... (Node)
- Show node informatio... (Node)
- Show node informatio... (Node)
- Show related NNMi in... (Node)
- Show related NNMi in... (Node)
- Show related NNMi n... (Node)
- Show related NNMi n... (Node)
- Traceroute to node fro... (Node)
- Traceroute to node fro... (Node)

The following table shows the comparison between OM and OBM operator features:

OM operator functionality	Equivalent in OBM
Review instructions	Yes
Launch tools on messages, nodes, services	Yes, launch tools on events and CIs
Launch (also repeatedly)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 that can be integrated in My Workspace, which enables 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 possible only by defining a scheduled CI downtime that starts immediately
Broadcast to all or selected operators (OM for UNIX)	Not supported
$OPC_NODES replacement in tools (enables to launch a tool that gets selected nodes as input parameter) Start tools on many nodes (multi-select nodes)	Currently not possible in OBM
Instruction text interface to retrieve instructions from an external system	OBM offers an external instruction text interface that enables you to retrieve instructions from external databases, web pages, or other sources.
First time received event column (OM for Windows), time received and time last received event column (OM for UNIX)	Time First Received and Time Received columns (duplicate overrides time received)
Browser filters	Supported (also public and private filters)
History filters	Yes, enables you to use event and date filters for the Closed Events Browser
Message colors	Supported (browser options)
Reorder columns	Supported (browser options)

<table>
<tr><td>Column choices</td><td>• Supports most columns available in OM
• Not available attributes: unmatched, and time unbuffered
• Available attributes, but cannot be selected as columns: message key, origin, policy, and policy type
• CAs can be selected in columns, but it is required that the admin predefines the list of CAs that the operator can choose
• Various new columns available, for example: event age, correlation, priority, received in downtime, and so on</td></tr>
<tr><td>Play sound</td><td>Supported (browser options, default sound)</td></tr>
<tr><td>Run local application or trigger a popup based on event severity (OM for UNIX)</td><td>Not supported</td></tr>
<tr><td>System tray icon / popup (OM for Windows)</td><td>Not supported</td></tr>
<tr><td>Custom UI layout</td><td>Conceptual (My Workspace)</td></tr>
<tr><td>Service maps/views</td><td>Yes, several widgets (for example, Top View, Health Top View, and Watch List)</td></tr>
<tr><td>Service Label and Service ID in Message Browser

<table>
<tr><th>Severity</th><th>Service Label</th><th>Service Name</th></tr>
<tr><td>Critical</td><td>Disk 2</td><td>node2_disk</td></tr>
<tr><td>Major</td><td>Mail Server 2</td><td>email_node2</td></tr>
<tr><td>Warning</td><td>Europe</td><td>europe</td></tr>
<tr><td>Critical</td><td></td><td>SeM_SPI:Server@@company.com</td></tr>
<tr><td>Critical</td><td></td><td>SeM_SPI:Server@@company.com</td></tr>
</table>
50 of 34 1 0 18 0
All Active Messages
Select Map View</td>
<td>Related CI, Related CI hint (equivalent to service ID), and Node in Event Browser

<table>
<tr><th>Sev</th><th>Related CI</th><th>Related CI Hint</th><th>Node</th></tr>
<tr><td>!</td><td>mambo3</td><td>mambo3.mambo.net</td><td>mambo3</td></tr>
<tr><td>☒</td><td>BACDB</td><td>BACDB@@oradb3.mambo</td><td>oradb3</td></tr>
<tr><td>!</td><td>OM Knowledge</td><td>UCMDB:4215438b41aeb2e</td><td></td></tr>
</table></td></tr>
<tr><td>Contextual link to OM policy from message</td><td>Yes</td></tr>
<tr><td>Restrict operator permissions: globally set limited for messages owned by others, allow perform actions per user/profile, modify message, own, (un)acknowledge (OM for Windows) or view, (dis)own, (un)acknowledge, perform actions, modify message on a per message group basis (OM for Windows).</td><td>More granular control</td></tr>
<tr><td>OM for UNIX Java feature</td><td></td></tr>
<tr><td>Font size (Edit -> Preferences -> General)</td><td>Event browser has two font sizes to choose from (default and compact view)</td></tr>
<tr><td>Browser advanced filters: event filters and very flexible message view filters</td><td>• Supported (same on concept base)
• Extensive list of attributes and patterns that can be combined together with AND, OR, and NOT operators
• Does not have an equivalent node event attribute (the closest is related CI hint)</td></tr>
<tr><td>Dynamic Label in event browser</td><td>Not supported</td></tr>
<tr><td>Custom or Sub Service Maps can be created with moving icons or externally calculated icon positions

Bielefeld
Münster
Detmold
Dortmund
Arnsberg
Duisburg
Köln
Siegen
Aachen
Bonn

</td>
<td>Geographic Map functionality available by using Location CI in the RTSM:

Modeling &gt; Modeling Studio
Modeling
Data Flow Management
Administration
CI Types
Edit
View
Layout
Operations
Tools
CI Types
CI Types
Managed Object (96)
ActivityLog (0)
Asset (0)
Attachment (0)
Budget (0)
BudgetLine (0)
BusinessObjective (0)
ConfigurationItem (96)
BusinessElement (13)
CiCollection (2)
Dynamic Node Factory (1)
InfrastructureElement (63)
Location (0)
Monitor (13)
Party (4)
Contract (0)
Cost (0)
Dependencies
Details
Attributes
Qualifiers
Icon
Attached
This page enables you to edit the attributes of the CI type.
<table>
<tr><th>Display Name</th><th>Name</th><th>Type</th><th>Description</th><th>Default Value</th><th>Visible</th></tr>
<tr><td>global_id_scope</td><td>global_id_scope</td><td>string</td><td></td><td>Default</td><td></td></tr>
<tr><td>Is Candidate For Del...</td><td>root_iscandidateford...</td><td>boolean</td><td>Is candidat...</td><td>false</td><td>✓</td></tr>
<tr><td>Last Access Time</td><td>root_lastaccesstime</td><td>date</td><td>When was ...</td><td></td><td>✓</td></tr>
<tr><td>LastModifiedTime</td><td>last_modified_time</td><td>date</td><td>When was ...</td><td></td><td>✓</td></tr>
<tr><td>Latitude</td><td>latitude</td><td>string</td><td>Latitude of ...</td><td></td><td>✓</td></tr>
<tr><td>layer</td><td>layer</td><td>layer_enum</td><td></td><td>facilities</td><td>✓</td></tr>
<tr><td>Locality</td><td>locality</td><td>string</td><td>Represent...</td><td></td><td>✓</td></tr>
<tr><td>LocationBarCode</td><td>location_bar_code</td><td>string</td><td>Locations t...</td><td></td><td>✓</td></tr>
<tr><td>LocationType</td><td>location_type</td><td>location_ty...</td><td>Describes ...</td><td></td><td>✓</td></tr>
<tr><td>Longitude</td><td>longitude</td><td>string</td><td>Longitude ...</td><td></td><td>✓</td></tr>
<tr><td>MENU</td><td>MENU</td><td>xml</td><td></td><td>&lt;MENU&gt;&lt;...</td><td></td></tr>
<tr><td>Monitored By</td><td>monitored_by</td><td>string_list</td><td></td><td></td><td>✓</td></tr>
</table>
Custom Maps for positioning CIs by using drag and drop:

Fleischbrücke
Pegnitz
Königstraße
Adlerstraße
Findelgasse
Bankgasse
Karolinenstraße
Heldengäßchen
Brunnengasse
tcdhcp054
Status: Major
Class Type: Unix
Details - Unassigned Events
Status: Major
Business Rule: Worst Status Rule
Last status changed: 9/16/2013 1:57 PM
Value: 1
Details - Unresolved Events
Status: Major
Business Rule: Worst Status Rule
Last status changed: 9/16/2013 1:57 PM
Value: 1
Details - System Performance
Status: Major
Business Rule: Worst Status Rule
Last status changed: 9/16/2013 1:57 PM</td></tr>
<tr><td>Property files customization</td><td>Not supported</td></tr>
<tr><td>Secure https mode</td><td>Supported (see OBM hardening information)</td></tr>
<tr><td>Broadcast tool</td><td>Not supported (tool must be created in OBM)</td></tr>
<tr><td>Custom message icons</td><td>Not supported</td></tr>
<tr><td>List connected UIs</td><td>Not supported</td></tr>
<tr><td>Dashboard: event history, pie chart, bar chart, and cockpit view</td><td>Event Dashboard (the dashboard choices are preferably predefined by the administrator in the Dashboard Designer, rather than the operator creating their own)</td></tr>
<tr><td>Detach window</td><td>Yes, URL for access to Event Browser only</td></tr>
<tr><td>Pending browser supporting service hours</td><td>Not supported</td></tr>
<tr><td>Operational Service View showing unowned service status</td><td>• Multiple KPIs to propagate more than one state
• Unassigned Events KPI is equivalent to Unowned status</td></tr>
<tr><td>GUI failover to backup OM server</td><td>Load balancer in front of Gateway servers of a single OBM instance</td></tr>
<tr><td>Disable user logins</td><td>Limited: Infrastructure Setting (Foundation=Security) can prevent login if BSM_ODB or DASHBOARD services are down</td></tr>
<tr><td>opcuistartupmsg</td><td>Not supported</td></tr>
<tr><td>Integration: Java GUI can be launched in a context sensitive manner from other applications by opening a specific service view that includes related message browser filter</td><td>OBM standalone event browser can be launched with context</td></tr>
</table>

Implement integrations for operators

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

- Operations Orchestration integrationOperations Orchestration run books can be defined for particular CI Types and can be launched in the context of a CI or an event.For more information, see Integrate.
- Knowledge Base integrationsKnowledge Base systems that provide useful information for operators can be integrated by using the OBM external instruction text interface. It can call a script or executable, query databases, web pages, or other external sources to retrieve instruction text for a certain event. For details about external instructions, see Administer.You can also integrate web pages directly into My Workspace pages by using a dynamic URL. For details, see *Use*.
- Cross-launches into other applicationsContext-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 Administer.
- Forwarding to Incident Management SystemsFor documentation about the generic forwarding interface, see Develop. Forwarding rules can be set up by using **Administration > Event Processing > Automation > Event Forwarding**.For documentation on the specific Service Manager integration, see Integrate.
- Forwarding to user notification systemsEvents can be forwarded to external notification systems by using the generic forwarding interface. For details, see Develop.Users can also be notified by using the OBM own notification interface, which can send e-mail, sms, or pager notifications. For more details, go to **Administration > Event Processing > Automation > Notifications** and see the corresponding OMi Help topics.

Recreate custom 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 OBM.

Operators in OM can start tools in the context of one or more nodes or node groups, and run those tools on multiple systems. OBM 10.10 and later can run tools on multiple CIs, which can be of the node type or of another CI type. This also enables context-specific tools, which means that 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 OBM content packs and management packs. If a content pack exists in OBM, it usually provides comparable tools to the corresponding OM SPI.

If a content pack does not yet exist, or if a custom tool is developed in OM, then a corresponding tool can be recreated manually in OBM in **Administration > Operations Console > Tools**.

Currently no method is available to automatically exchange tools between OM and OBM.

There are some differences in the variables that can be used when defining tools – the most important difference is that OBM does not support $OPC_NODES that 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 OBM

Tools in OBM are linked to Configuration Items by using a Configuration-Item-centric approach. 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, a script or a URL, and can also contain the following parameters:

- CI attributes
- Event attributes
- Infrastructure settings
- Runtime parameters
- Monitoring host name
- Management server name
- Host name of a system that hosts the CI

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

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

OM and OBM feature comparison

The following table lists features in OM and their equivalents in OBM.

OM Tool Features	OBM 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 `${option}` to prompt operator for missing parameters Cannot change parameters but can add missing parameters
Allow operator to change log-on flag	Not available, however the tool can prompt an operator for log-on credentials (the operator is prompted every time the tool is started)
Possible parameter variables	
Message properties	Event properties
Node properties	CI properties/Monitoring Host/Hosted on host
Service properties	CI properties
Environment variables Used to retrieve environment variables from the console that launched the action	Not available (typical tools do not require access to environment variables on console systems)
Server configuration variables	Infrastructure Settings
Node group properties / `$OPC_NODEGROUP_ID` `$OPC_NODEGROUP`	Not available (OBM is CI/view centric)
`$OPC_MSG_IDS`	Not available, an event ID of the selected event is accessible
`$OPC_MSG_NODES` `$OPC_NODEID`	Not available, a monitoring host of the selected event/CI is available
`$OPC_MGMTSV`	Available in the UI Execution is done on the Gateway Server
`$OPC_USER (OMU)`	Executing OBM user variable
Execute on possibilities	
Management server	Yes, requires that an Operations Agent is installed on all gateway servers Currently uses node of the infrastructure setting Default Virtual Gateway Server for Application Users URL as a target for agents connected to an OBM server. A managed_by relationship to an OM server takes precedence. To make sure that tools are executed on the OBM server, remove any relationships to OM servers or remove the OM server CI.
Selected node	Selected CI / related CI of the selected event
Node list	To start a tool on multiple nodes, select the corresponding node CIs and choose Launch tool from the context menu
Node list (predefined)	A predefined node list is not possible
Console	OBM does not allow executables or scripts to be started on a console system. This is because the OBM 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; a user on the client system can run the executable manually. Such a useful tool, as well as its 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

Task: How to recreate custom OM tools in OBM

To create a tool in OBM, follow these steps:

1. Go to **Administration > Operations Console > Tools**.
2. Navigate through the CI Types tree, for example to **InfrastructureElement > Node > Computer > Windows**.
3. Click **Windows** and the **New Item** icon in the Windows – Tools pane. The Create New Tool window appears.
4. Copy the tool command and other settings from the OM tool definition to the OBM tool definition.To test the tool, open the Event Perspective or another My Workspace page that shows CIs, select a suitable CI (of the CI Type for which you defined the tool), and then select **Launch Tool** from the CI context menu.If the tool contains event attributes it can be triggered from an event only.

Performance dashboards

OBM includes an embedded Performance Dashboard component that does not require an additional license. The OBM 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 Configuration Items (CI).

OM for UNIX and OM for Windows do not offer an integrated dashboard component such as the OBM Performance Dashboard, however OM integrate with Performance Manager and can cross-launch into Performance Manager.

For details on how to launch a performance dashboard, see Use.

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

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

For details about designing performance dashboards, see Use.

OM, PM, and OBM performance dashboard feature comparison

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

The following tables compare OM and OBM functionality, as well as Performance Manager and OBM Performance Dashboard functionality.

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

Performance Manager functionality	OBM 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 and PDF only
URL-based launch capability in PM for embedding in their own portal	Yes
REST web services for retrieving data	No
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, Cloud Optimizer, SiteScope, Operations Connector, OpsBridge Store
RTM data source support	Real time graphing support added for Operations Agent and SiteScope OBM 10.11 and later provides metric streaming also for application and custom metrics
Proxied Log Files	No
Flat file data source	Use Operations Connector to process metrics from file into OBM
Add node temporarily on-the-fly	No
Active Directory authentication	Any authentication supported by OBM
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 OMi 10.11 and later: Metric comparison dashboards enable comparison of metrics from multiple CIs or nodes
Diagnostic View: Load and Save State	Yes (Favorites in OBM)
Diagnostic View: Drill down to Process, tables of each metric class	OBM 10.11 or later: Yes
System Information page	No

Task: How to import custom Performance Manager graphs into OBM

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

1. Copy all graph templates that you want to import from the 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 OBM GW server.

   Create the OVPM directory if it does not exist.
2. Follow these steps:
   1. Log on to OBM.
   2. On a separate browser tab, open `<OMiGWServer>/OVPM/Options.jsp`.
   3. Click **Import Dashboard**.

   This uploads all graph templates from the above file location to the OBM database. This is a one-time import. If you modify graph templates in Performance Manager afterward, use the same procedure again to upload the modified graph templates.
3. Associate these graph templates (performance dashboards in OBM) 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.

- If the graph template contains specific node names, the graph can be imported into OBM, but the specific node names are ignored when the graph is launched. The graph is launched in the context of the selected CI.
- If a graph template with a SiteScope data source is imported from PM into OBM, the graph retrieves metrics directly from a corresponding SiteScope server. This assumes that the monitor in SiteScope is configured to report metrics to the Operations Agent.
- PM graph templates that refer to a Reporter data source do not work in OBM.

Prepare operator console

The following sections describe how to prepare an operator console:

Contents

Manage users and user groups in OBM

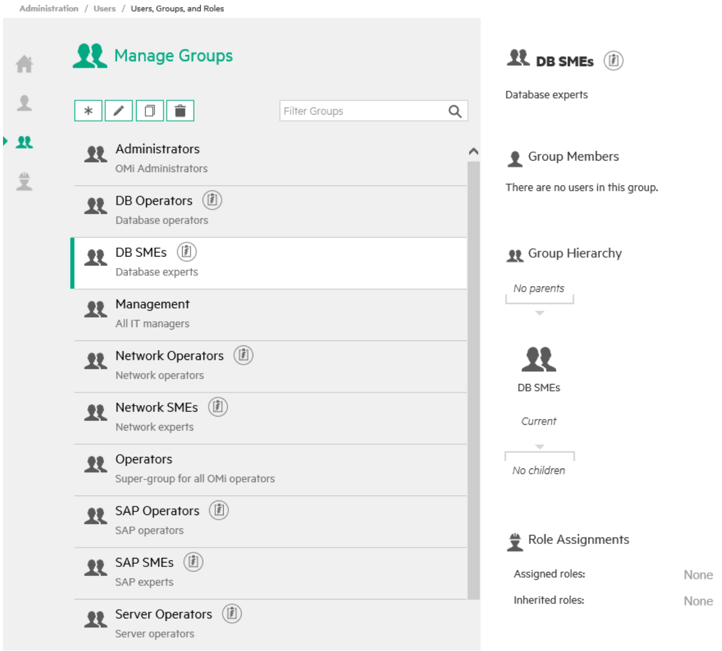
User roles, user groups, and user profiles help simplify authorization in OM.

Similar functionality is available in OBM: 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. To reduce the effort and complexity involved in configuring roles for individual users in OBM, 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.

OBM does not distinguish between administrators and operators – there are just users.

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

The following figure shows user groups in OBM:



Administration / Users / Users, Groups, and Roles

Manage Groups

Filter Groups

- Administrators — OMi Administrators
- DB Operators — Database operators
- DB SMEs — Database experts
- Management — All IT managers
- Network Operators — Network operators
- Network SMEs — Network experts
- Operators — Super-group for all OMi operators
- SAP Operators — SAP operators
- SAP SMEs — SAP experts
- Server Operators — Server operators

DB SMEs

Database experts

Group Members

There are no users in this group.

Group Hierarchy

No parents

DB SMEs

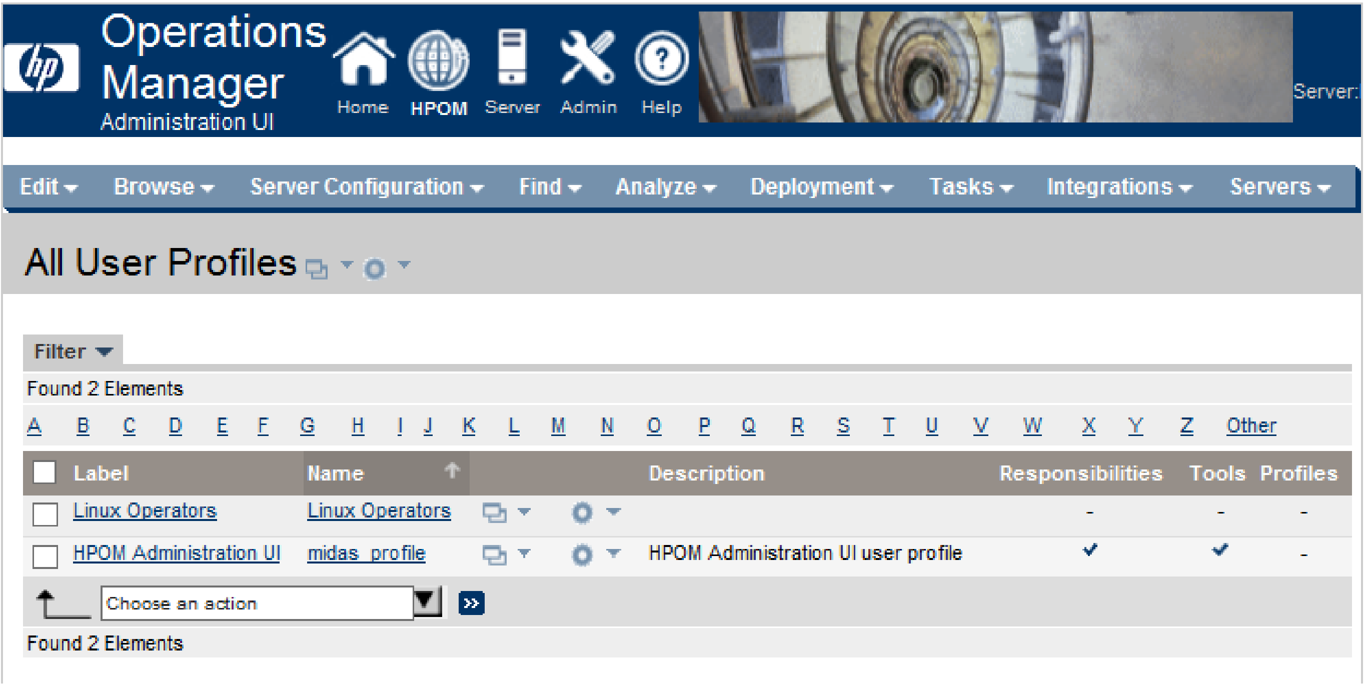
Current

No children

Role Assignments

Assigned roles:	None
Inherited roles:	None

The following figures show user profiles in OM for UNIX and user roles in OM for Windows:



All User Profiles

Filter

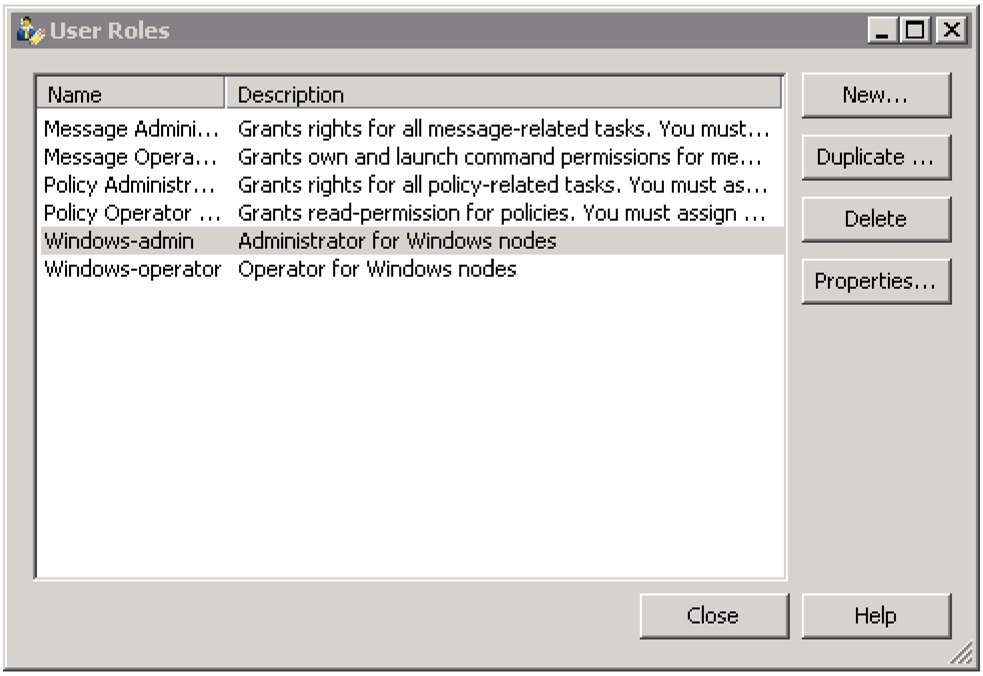
Found 2 Elements

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z Other

☐ Label	Name			Description	Responsibilities	Tools	Profiles
☐ Linux Operators	Linux Operators				-	-	-
☐ HPOM Administration UI	midas_profile			HPOM Administration UI user profile	✓	✓	-

Choose an action

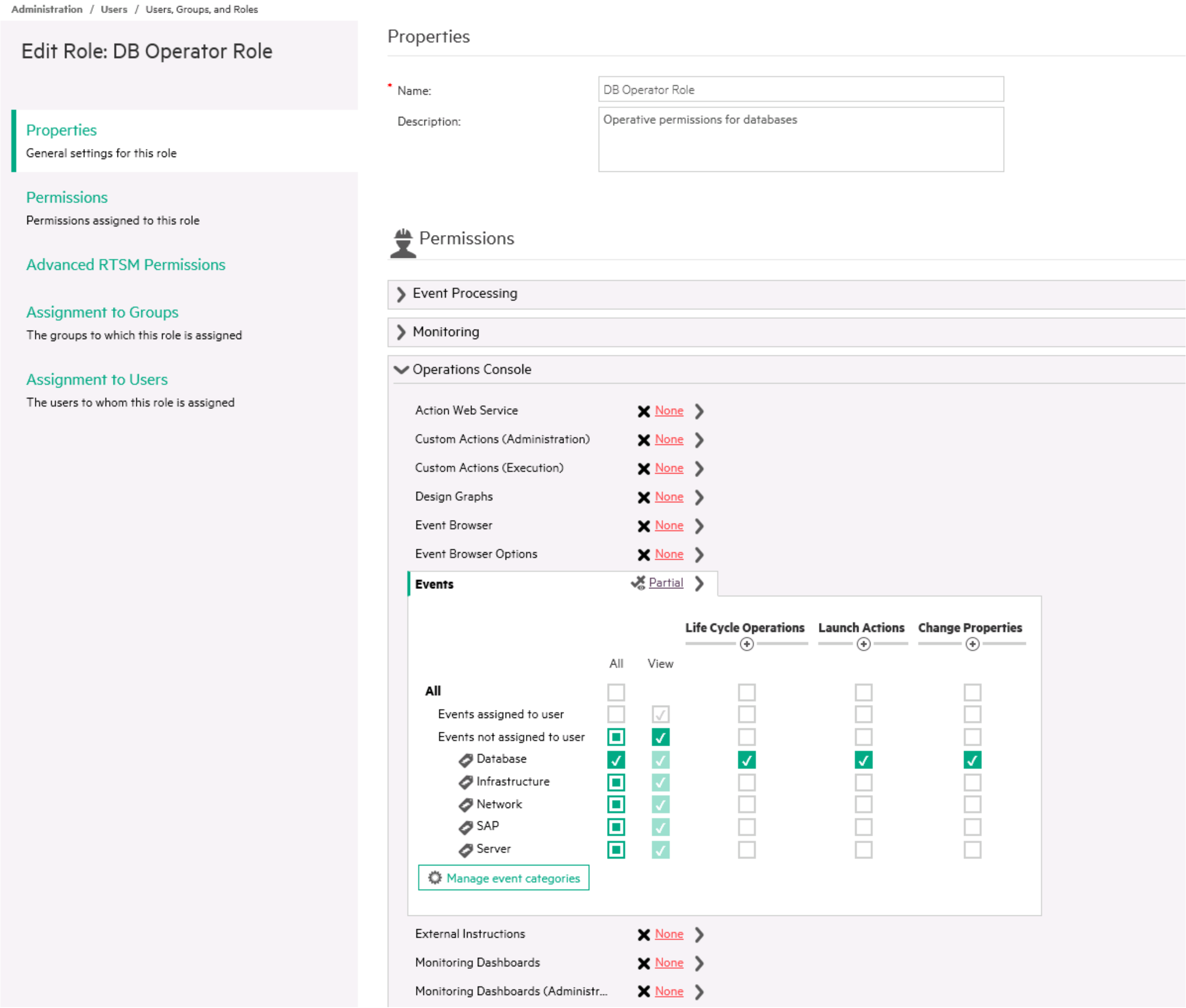
Found 2 Elements



Name	Description
Message Admini...	Grants rights for all message-related tasks. You must...
Message Opera...	Grants own and launch command permissions for me...
Policy Administr...	Grants rights for all policy-related tasks. You must as...
Policy Operator ...	Grants read-permission for policies. You must assign ...
Windows-admin	Administrator for Windows nodes
Windows-operator	Operator for Windows nodes

User roles

OBM enables you to fine-tune permissions management by applying permissions within roles. Permissions enable you to restrict the scope of a role.



Administration / Users / Users, Groups, and Roles

Edit Role: DB Operator Role

Properties
General settings for this role

Permissions
Permissions assigned to this role

Advanced RTSM Permissions

Assignment to Groups
The groups to which this role is assigned

Assignment to Users
The users to whom this role is assigned

Properties

* Name:	DB Operator Role
Description:	Operative permissions for databases

Permissions

Action Web Service	✗ None
Custom Actions (Administration)	✗ None
Custom Actions (Execution)	✗ None
Design Graphs	✗ None
Event Browser	✗ None
Event Browser Options	✗ None
Events	Partial

	All	View	Life Cycle Operations	Launch Actions	Change Properties
All	□		□	□	□
Events assigned to user	□	✓	□	□	□
Events not assigned to user	■	✓	□	□	□
Database	✓	✓	✓	✓	✓
Infrastructure	■	✓	□	□	□
Network	■	✓	□	□	□
SAP	■	✓	□	□	□
Server	■	✓	□	□	□

External Instructions	✗ None
Monitoring Dashboards	✗ None
Monitoring Dashboards (Administr...	✗ None

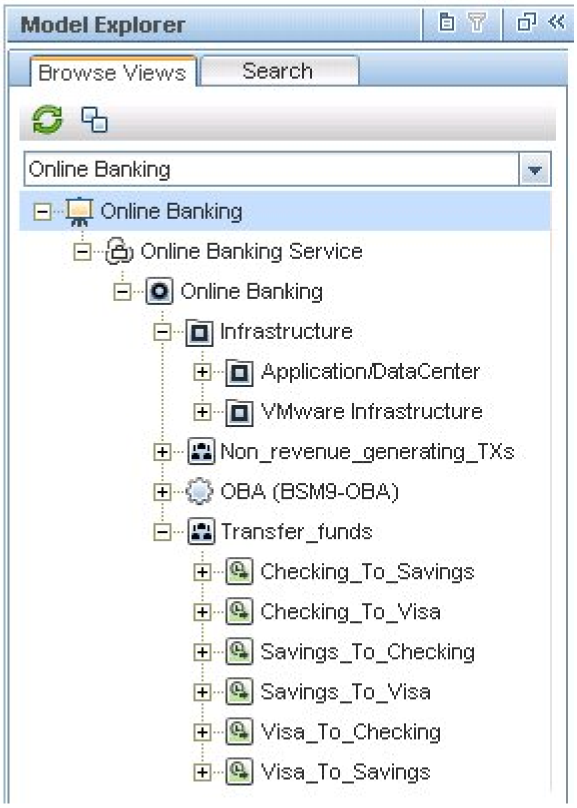
For details about users, groups, and roles, see Administer.

Responsibilities for nodes and CIs

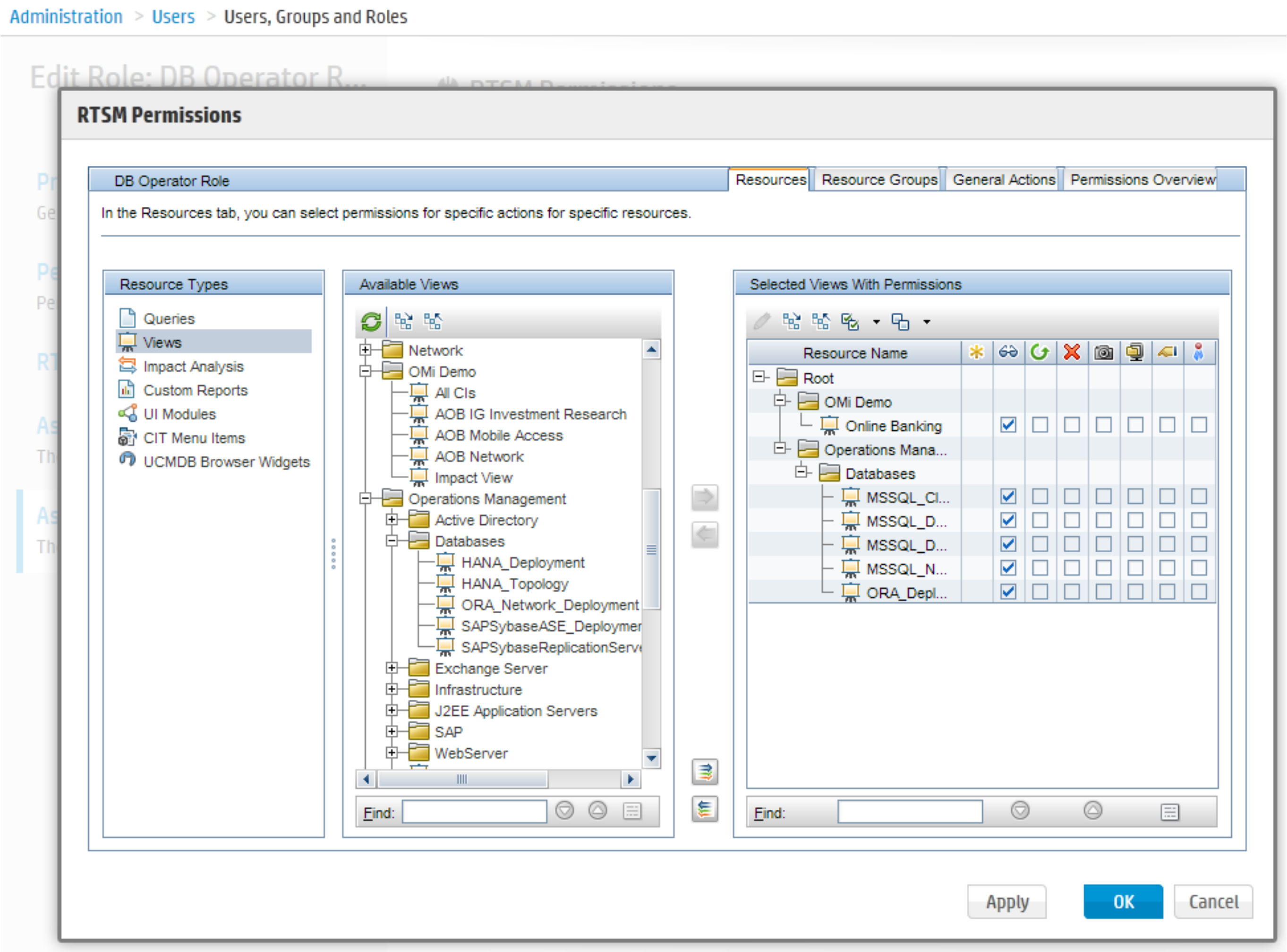
OBM focuses on CI and CI-type-centric or view-based monitoring, instead of node and node-group-centric monitoring. Therefore, node groups are not used for authorization in OBM. Corresponding user responsibilities can be defined in OBM by using views, which is a more flexible concept.

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 are represented in OBM 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 OBM 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 OBM:



```
⊟ Online Banking
   ⊟ Online Banking Service
      ⊟ Online Banking
         ⊟ Infrastructure
            ⊞ Application/DataCenter
            ⊞ VMware Infrastructure
         ⊞ Non_revenue_generating_TXs
         ⊞ OBA (BSM9-OBA)
         ⊟ Transfer_funds
            ⊞ Checking_To_Savings
            ⊞ Checking_To_Visa
            ⊞ Savings_To_Checking
            ⊞ Savings_To_Visa
            ⊞ Visa_To_Checking
            ⊞ Visa_To_Savings
```



In the Resources tab, you can select permissions for specific actions for specific resources.

Resource Name							
Root							
OMi Demo							
Online Banking	☑	☐	☐	☐	☐	☐	☐
Operations Mana...							
Databases							
MSSQL_Cl...	☑	☐	☐	☐	☐	☐	☐
MSSQL_D...	☑	☐	☐	☐	☐	☐	☐
MSSQL_D...	☑	☐	☐	☐	☐	☐	☐
MSSQL_N...	☑	☐	☐	☐	☐	☐	☐
ORA_Depl...	☑	☐	☐	☐	☐	☐	☐

In OBM, user responsibilities can be restricted by granting view rights to only particular views.

Responsibilities for events

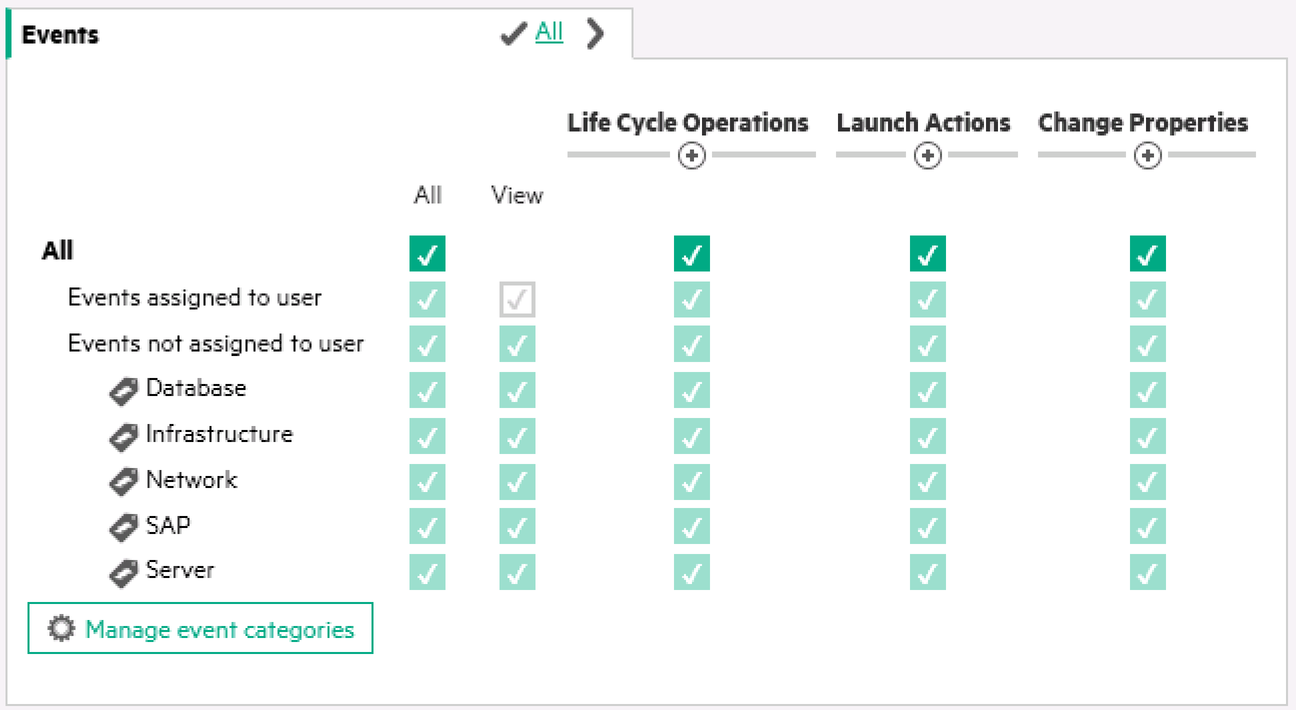
In addition to the node-group-based restrictions, OM uses message groups to restrict access to events. In OBM, message groups are called event categories and can also be used to restrict access.

OBM 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 that are not assigned to them.

In OBM 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 authorization based on the OM message groups (OBM event categories) is still available and should be used for unassigned events.

The following figure shows event categories in OBM:

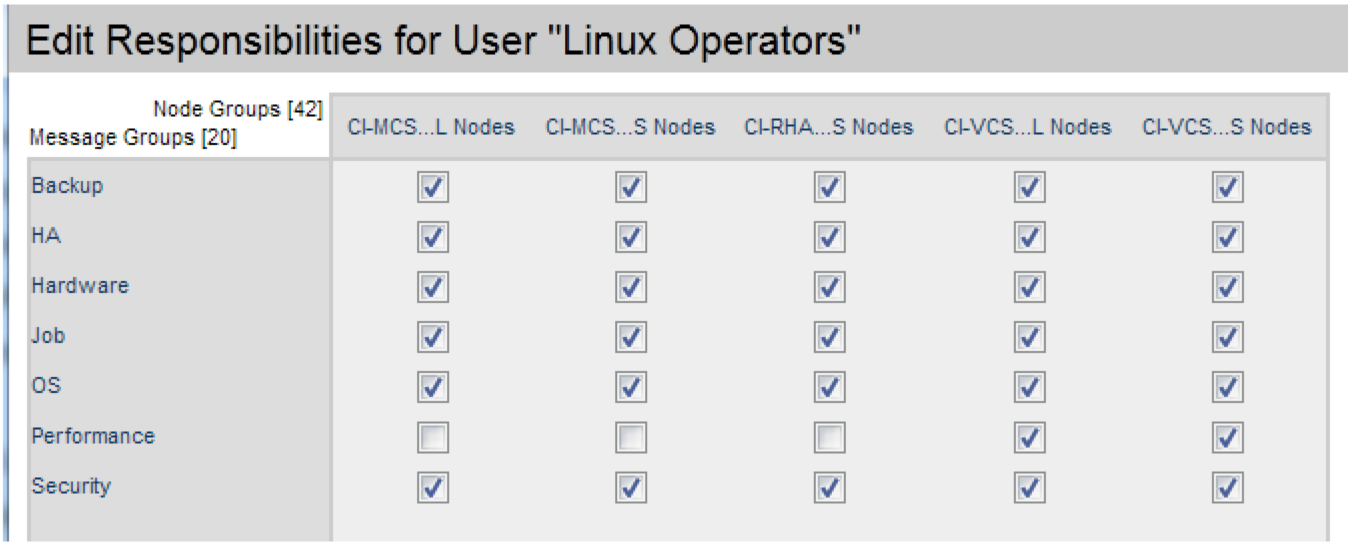


Events ✓ All >

	All	View	Life Cycle Operations	Launch Actions	Change Properties
All	☑		☑	☑	☑
Events assigned to user	☑	☐	☑	☑	☑
Events not assigned to user	☑	☑	☑	☑	☑
Database	☑	☑	☑	☑	☑
Infrastructure	☑	☑	☑	☑	☑
Network	☑	☑	☑	☑	☑
SAP	☑	☑	☑	☑	☑
Server	☑	☑	☑	☑	☑

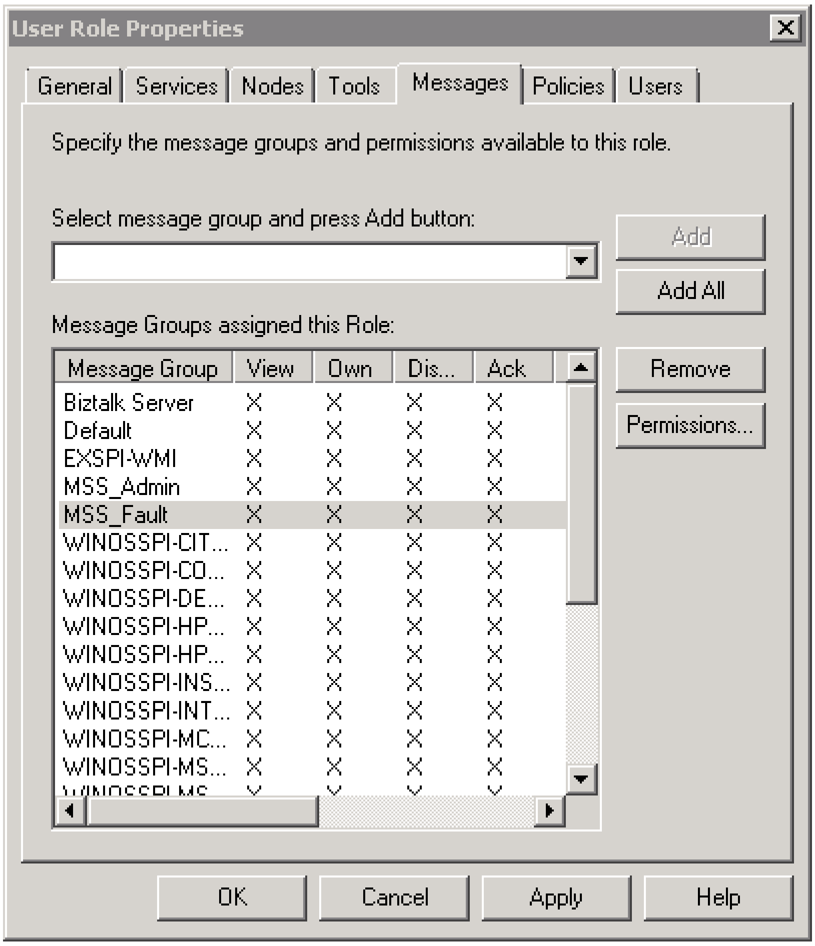
OM for UNIX and OM for Windows can restrict the messages that an operator can see by restricting the node groups and message groups this operator has access to.

The following figures show event responsibilities in OM:



Edit Responsibilities for User "Linux Operators"

Node Groups [42] Message Groups [20]	CI-MCS...L Nodes	CI-MCS...S Nodes	CI-RHA...S Nodes	CI-VCS...L Nodes	CI-VCS...S Nodes
Backup	☑	☑	☑	☑	☑
HA	☑	☑	☑	☑	☑
Hardware	☑	☑	☑	☑	☑
Job	☑	☑	☑	☑	☑
OS	☑	☑	☑	☑	☑
Performance	☐	☐	☐	☑	☑
Security	☑	☑	☑	☑	☑



User Role Properties

Specify the message groups and permissions available to this role.

Select message group and press Add button:

Message Groups assigned this Role:

Message Group	View	Own	Dis...	Ack
Biztalk Server	X	X	X	X
Default	X	X	X	X
EXSPI-WMI	X	X	X	X
MSS_Admin	X	X	X	X
MSS_Fault	X	X	X	X
WINOSSPI-CIT...	X	X	X	X
WINOSSPI-CO...	X	X	X	X
WINOSSPI-DE...	X	X	X	X
WINOSSPI-HP...	X	X	X	X
WINOSSPI-HP...	X	X	X	X
WINOSSPI-INS...	X	X	X	X
WINOSSPI-INT...	X	X	X	X
WINOSSPI-MC...	X	X	X	X
WINOSSPI-MS...	X	X	X	X
WINOSSPI-MS	X	X	X	X

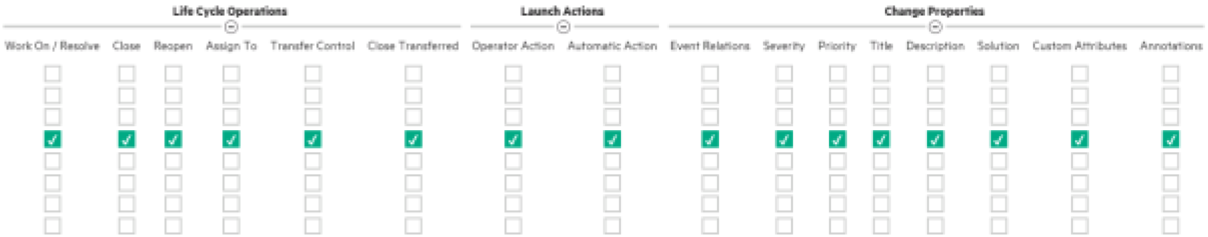
Event permissions

In OM for Windows, granular permissions can be set with regards to message modifications per message group.

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

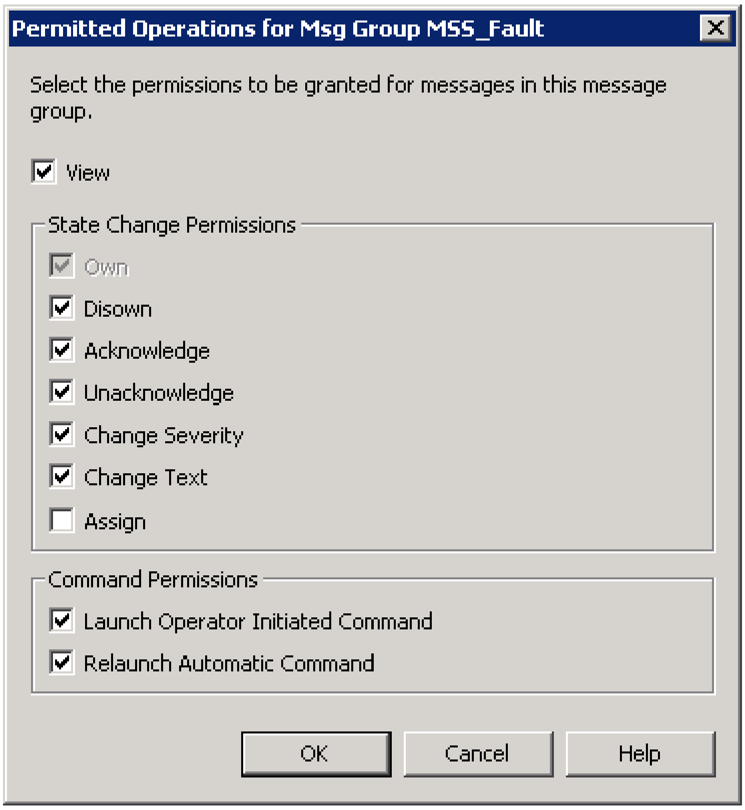
In OBM, you can set the same detailed permissions as in OM for Windows and also the additional permissions, for example, for the assignment or transfer control features of OBM.

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



Life Cycle Operations						Launch Actions		Change Properties							
Work On / Resolve	Close	Reopen	Assign To	Transfer Control	Close Transferred	Operator Action	Automatic Action	Event Relations	Severity	Priority	Title	Description	Solution	Custom Attributes	Annotations
□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

The following figure shows message permissions in OM for Windows:



Permitted Operations for Msg Group MSS_Fault

Select the permissions to be granted for messages in this message group.

☑ View

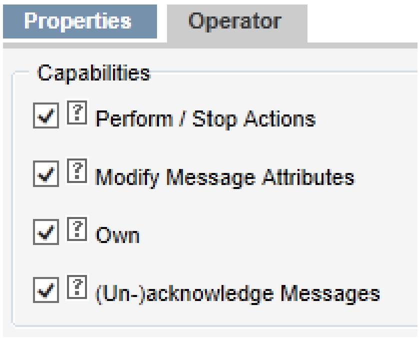
State Change Permissions

☑ Own
☑ Disown
☑ Acknowledge
☑ Unacknowledge
☑ Change Severity
☑ Change Text
□ Assign

Command Permissions

☑ Launch Operator Initiated Command
☑ Relaunch Automatic Command

The following figure shows operator message permissions in OM for UNIX:



Capabilities

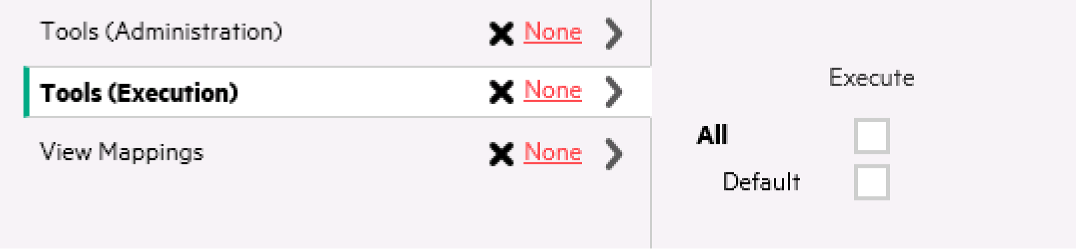
☑ Perform / Stop Actions
☑ Modify Message Attributes
☑ Own
☑ (Un-)acknowledge Messages

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 OBM, tools are defined for a particular CI type, and access to tools can be restricted by using tool categories.

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



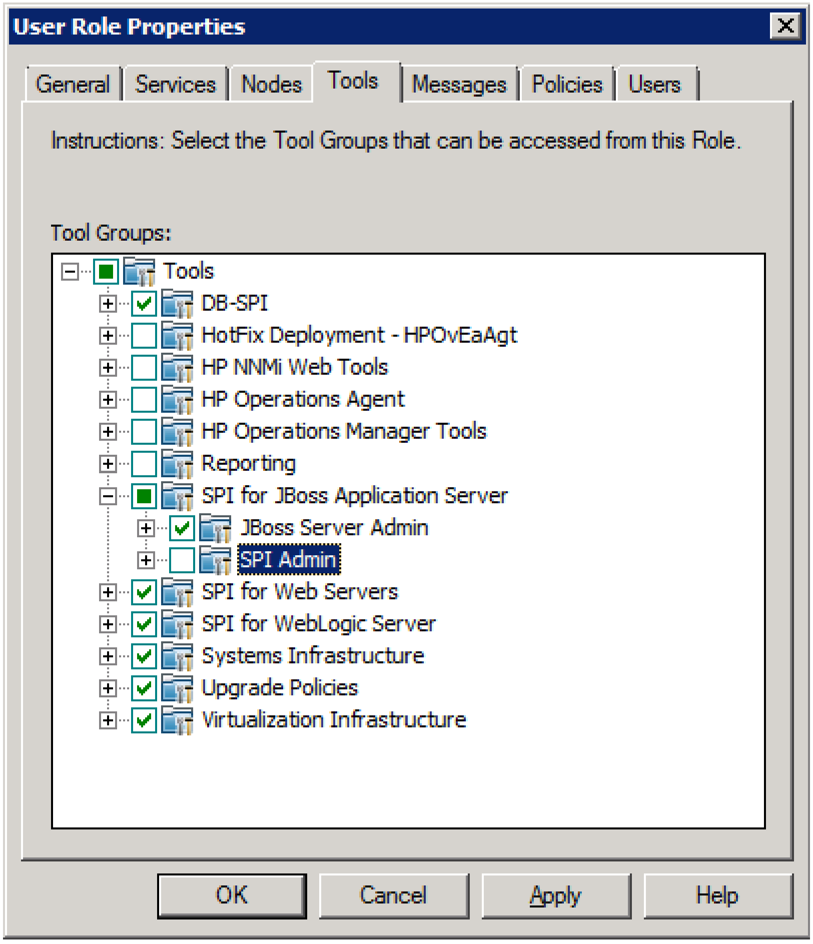
Tools (Administration) ✗ None

Tools (Execution) ✗ None

View Mappings ✗ None

	Execute
All	□
Default	□

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

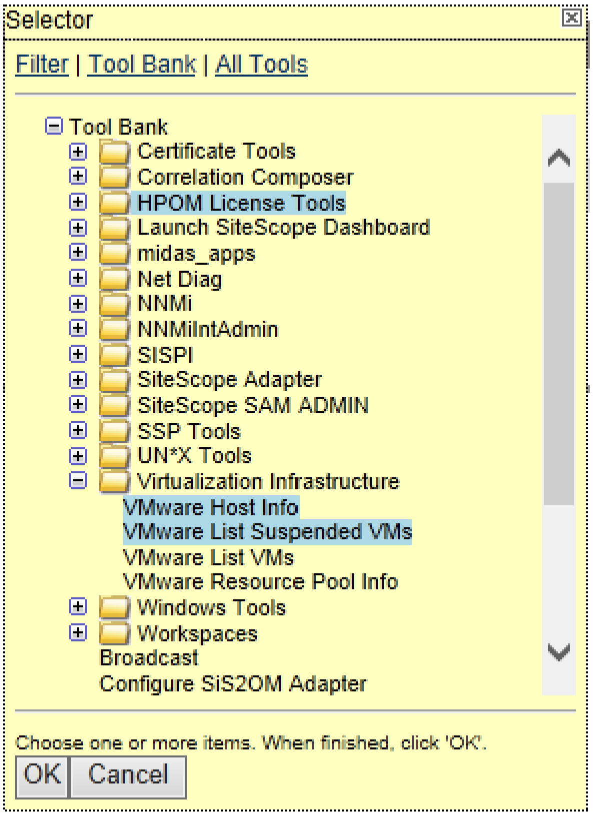


User Role Properties

Instructions: Select the Tool Groups that can be accessed from this Role.

Tool Groups:

```
⊟ ■ Tools
    ⊞ ☑ DB-SPI
    ⊞ □ HotFix Deployment - HPOvEaAgt
    ⊞ □ HP NNMi Web Tools
    ⊞ □ HP Operations Agent
    ⊞ □ HP Operations Manager Tools
    ⊞ □ Reporting
    ⊟ ■ SPI for JBoss Application Server
        ⊞ ☑ JBoss Server Admin
        ⊞ □ SPI Admin
    ⊞ ☑ SPI for Web Servers
    ⊞ ☑ SPI for WebLogic Server
    ⊞ ☑ Systems Infrastructure
    ⊞ ☑ Upgrade Policies
    ⊞ ☑ Virtualization Infrastructure
```

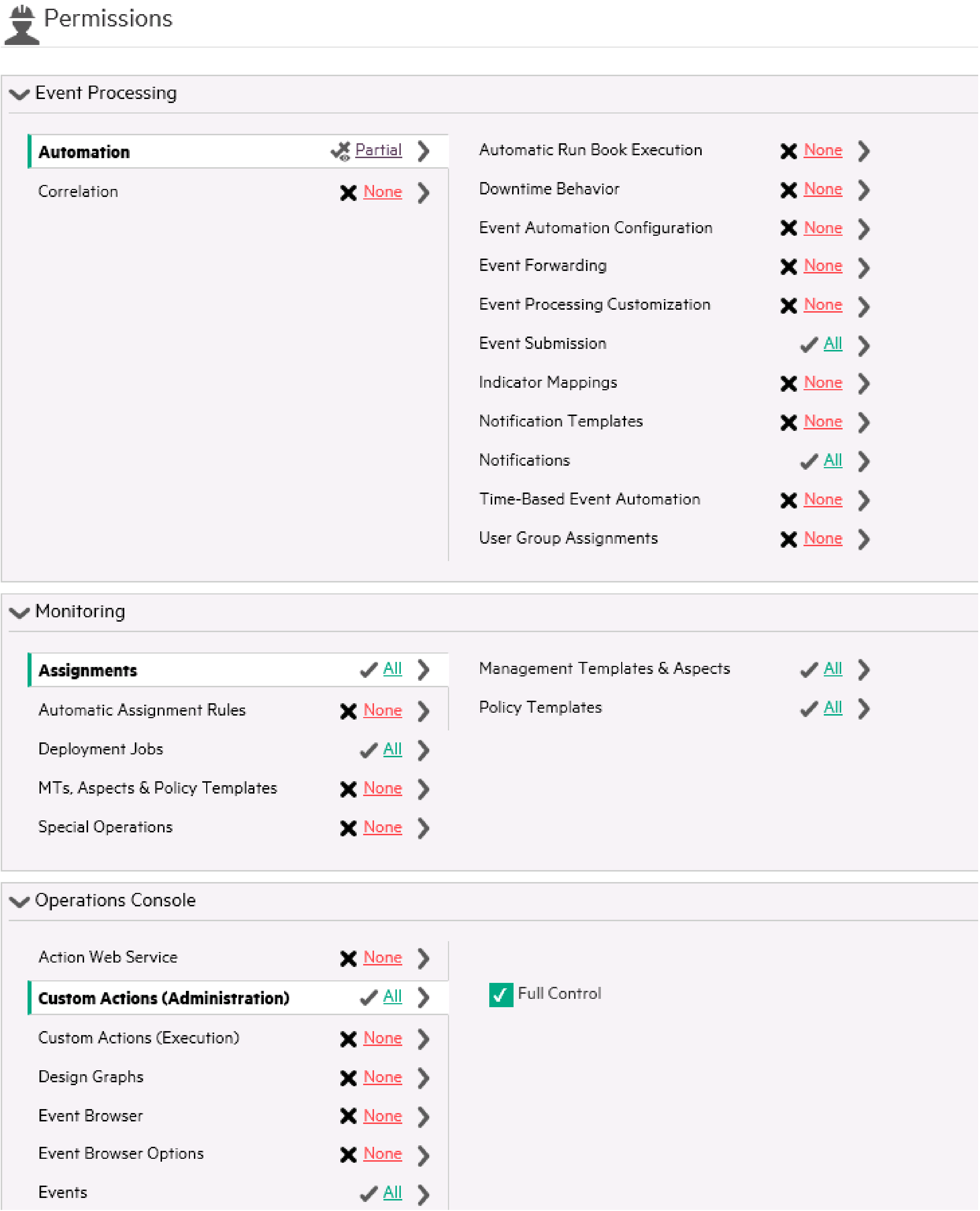


Administrative permissions

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

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

The following figure shows an example of administrative permissions in OBM:



Permissions

Event Processing

Automation	Partial
Correlation	✗ None

Automatic Run Book Execution	✗ 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
Automatic Assignment Rules	✗ None
Deployment Jobs	✓ All
MTs, Aspects & Policy Templates	✗ None
Special Operations	✗ None

Management Templates & Aspects	✓ All
Policy Templates	✓ All

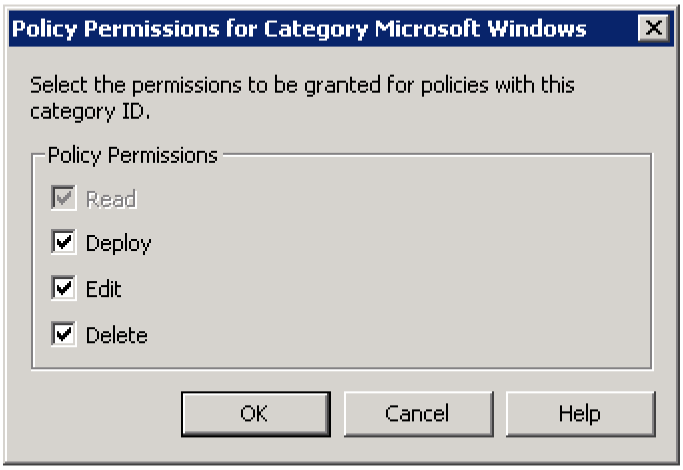
Operations Console

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

☑ Full Control

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.



Policy Permissions for Category Microsoft Windows

Select the permissions to be granted for policies with this category ID.

Policy Permissions

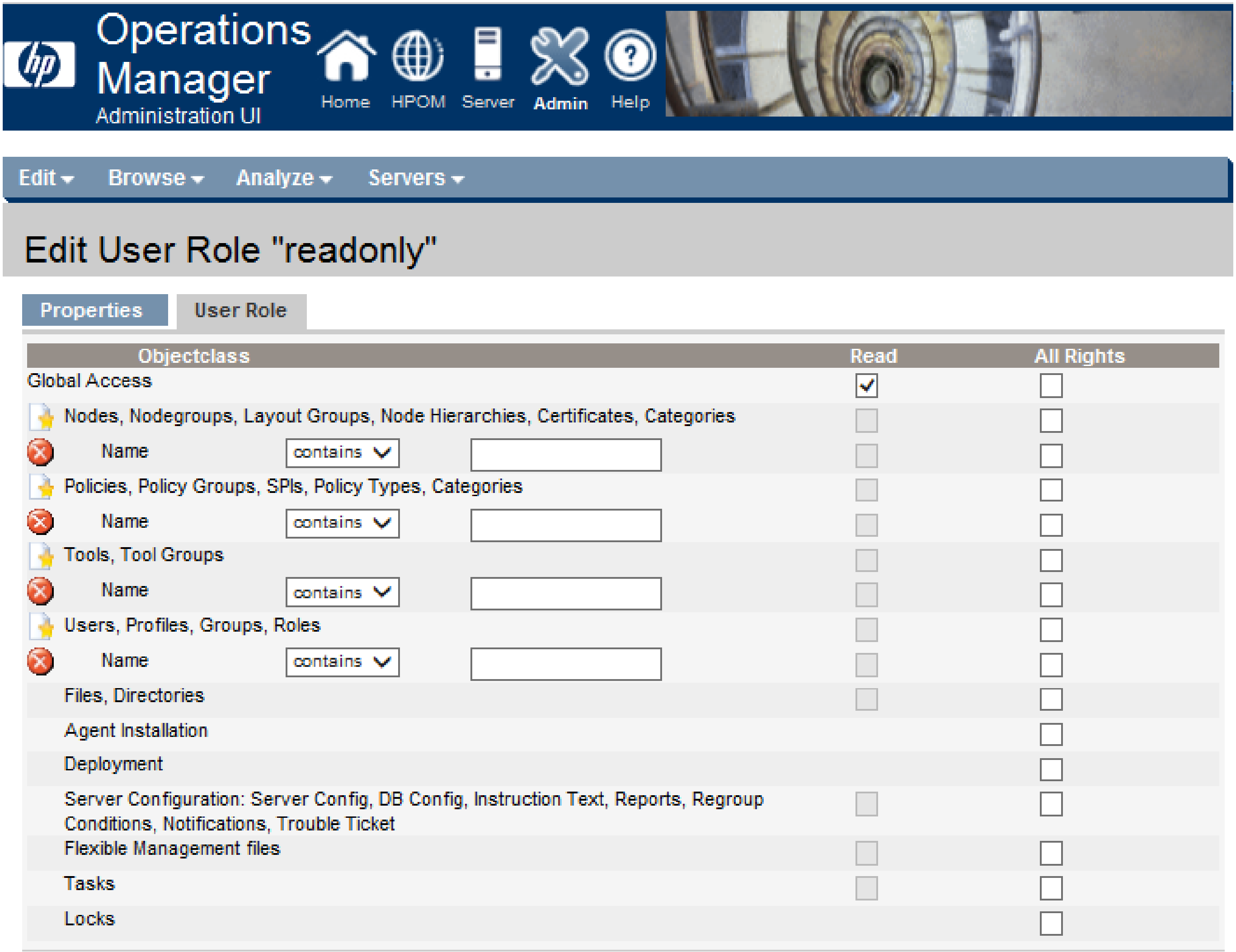
☑ Read

☑ Deploy

☑ Edit

☑ Delete

In OM for UNIX, different administrative permissions can be selectively granted for particular object groups by using patterns. It is also possible to grant read-only access.

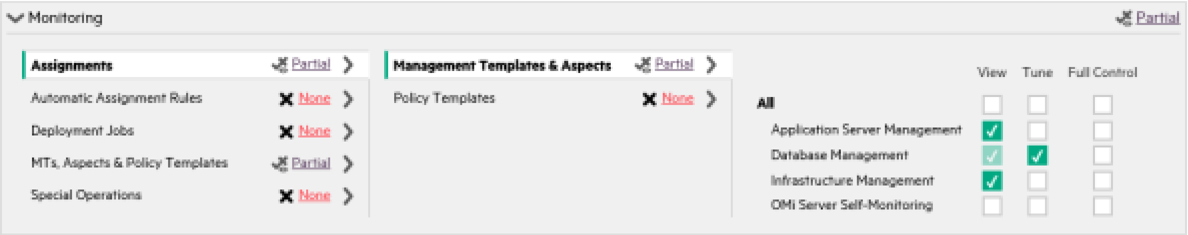


Edit User Role "readonly"

Objectclass			Read	All Rights
Global Access			☑	□
Nodes, Nodegroups, Layout Groups, Node Hierarchies, Certificates, Categories			□	□
Name	contains		□	□
Policies, Policy Groups, SPIs, Policy Types, Categories			□	□
Name	contains		□	□
Tools, Tool Groups			□	□
Name	contains		□	□
Users, Profiles, Groups, Roles			□	□
Name	contains		□	□
Files, Directories			□	□
Agent Installation				□
Deployment				□
Server Configuration: Server Config, DB Config, Instruction Text, Reports, Regroup Conditions, Notifications, Trouble Ticket			□	□
Flexible Management files			□	□
Tasks			□	□
Locks				□

In OBM 10.01 and earlier versions, you can grant access to an Administration UI, and with this also access to all objects that can be edited in that UI (for example, to all policy templates or all tools).

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


Monitoring Partial

Assignments	Partial
Automatic Assignment Rules	✗ None
Deployment Jobs	✗ None
MTs, Aspects & Policy Templates	Partial
Special Operations	✗ None

Management Templates & Aspects	Partial
Policy Templates	✗ None

	View	Tune	Full Control
All	□	□	□
Application Server Management	☑	□	□
Database Management	☑	☑	□
Infrastructure Management	☑	□	□
OMi Server Self-Monitoring	□	□	□

User authentication

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

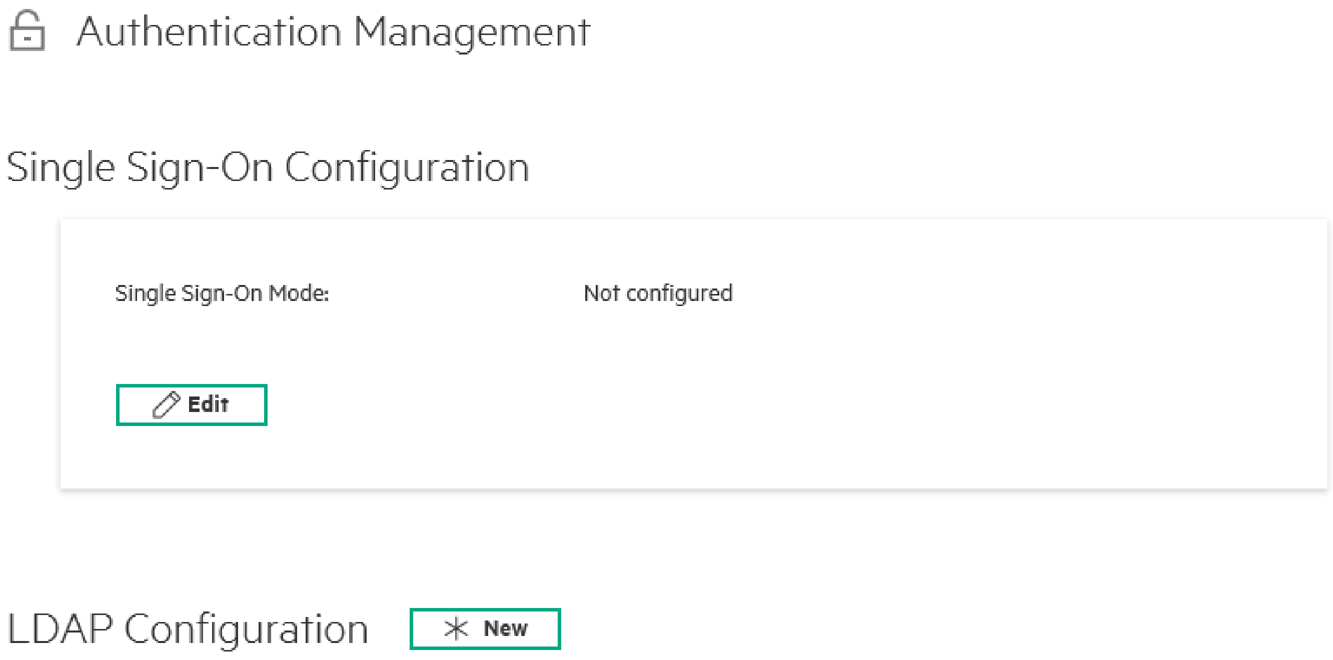
Because Windows Active Directory implements an LDAP server, users and user groups that are set up for OM for Windows can also be set up in OBM.

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

LDAP authentication

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

You can configure LDAP by using the LDAP configuration editor:

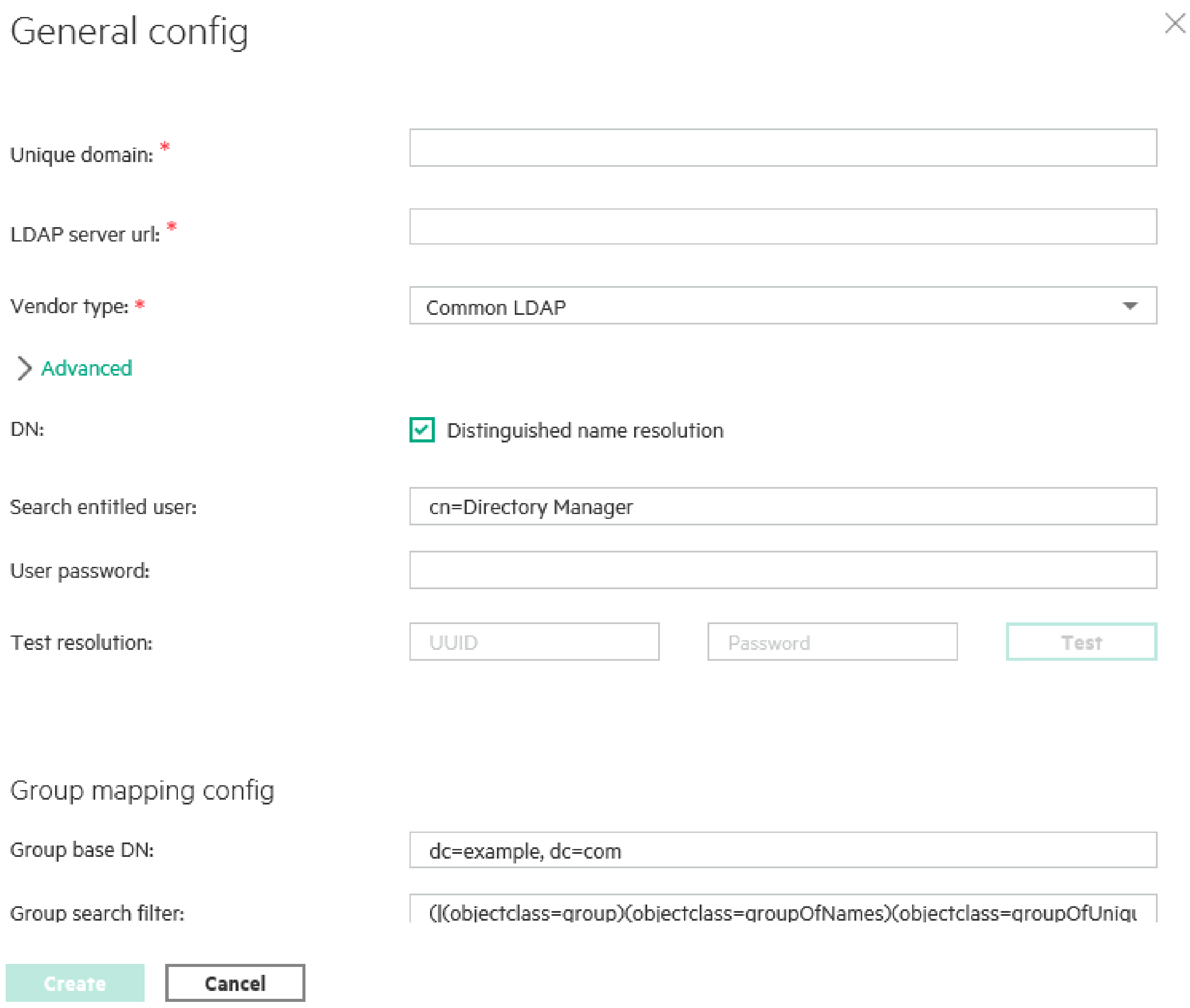


Authentication Management

Single Sign-On Configuration

Single Sign-On Mode: Not configured

LDAP Configuration



General config

Unique domain: *	
LDAP server url: *	
Vendor type: *	Common LDAP

DN:	☑ Distinguished name resolution
Search entitled user:	cn=Directory Manager
User password:	
Test resolution:	UUID Password Test

Group mapping config

Group base DN:	dc=example, dc=com
Group search filter:	(|(objectclass=group)(objectclass=groupOfNames)(objectclass=groupOfUniqu

API and command-line interfaces for user management

You can use the `opr-user` command-line interface (CLI) to manage users, groups, and roles manually. User roles including their permissions can also be exported and imported by using content packs.

OM and OBM user management feature comparison

OM functionality	Equivalent in OBM
User groups and user profiles (OM for UNIX) User roles (OM for Windows)	User groups and user roles
Restrict responsibilities by using message groups and node groups	Restrict responsibilities by using views and event categories (message groups)

Fine-grained event permissions (OM for Windows)	Yes
Restrict access to tools based on tool groups	Restrict access to tools based on tool categories
Grant permissions on both operator features and administrative features	Yes
Restrict access to policies by 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 or configuration folder
Read-only administrative permissions (OM for UNIX)	Yes (view permission)
User Authentication through 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 OBM.

Create users and define permissions manually in **Administration > Users > Users, Groups, and Roles**:

1. Map out the required roles and their relevant permissions, as well as the users and groups that you intend to assign the roles to.
2. Create the necessary user roles and permissions, and then create the necessary groups and assign roles to them.Users can be members of multiple groups, and groups can be nested and inherit permissions from parent groups.
3. Create the necessary users. If you use LDAP, users can be created automatically at their first login, and OBM user group memberships can be created based on LDAP group memberships. For details about LDAP authentication and mapping, see Administer.

If you have more than a few operators and want to separate their responsibilities and permissions, create multiple user roles and groups.

Create views for different operator responsibilities

In OBM 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 have access only to event and health information for all databases in EMEA, you must 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, because they are updated automatically when new CIs appear in the RTSM. In dynamic environments, it is not recommended to use instance-based views that are maintained manually.

Make sure the view contains **all** CIs for which you want to see events. For example, if an event is mapped to an Interface CI and the view contains the computer CI but not also the underlying interface CI, the event will not be visible with this view filter.

Create user group assignment rules

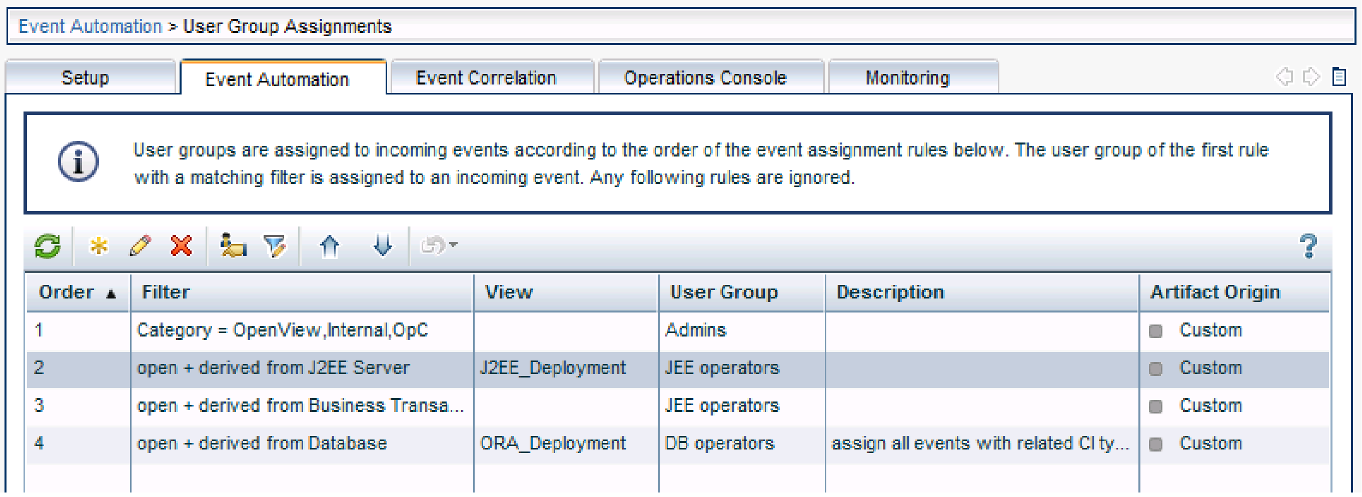
When you have defined various operator groups and the views they will have access to, it is recommended to define User Group Assignment rules that automatically assign incoming events to one of the operator groups. An alternative is to define a special dispatcher role in your organization and to let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

As a result of an assignment, every operator of the group gets advanced permissions for the event, and can modify and close events.

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

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 by using different view and event filters:



Event Automation > User Group Assignments

User groups are assigned to incoming events according to the order of the event assignment rules below. The user group of the first rule with a matching filter is assigned to an incoming event. Any following rules are ignored.

Order ▲	Filter	View	User Group	Description	Artifact Origin
1	Category = OpenView,Internal,OpC		Admins		Custom
2	open + derived from J2EE Server	J2EE_Deployment	JEE operators		Custom
3	open + derived from Business Transa...		JEE operators		Custom
4	open + derived from Database	ORA_Deployment	DB operators	assign all events with related CI ty...	Custom

Create monitoring dashboards and My Workspace pages

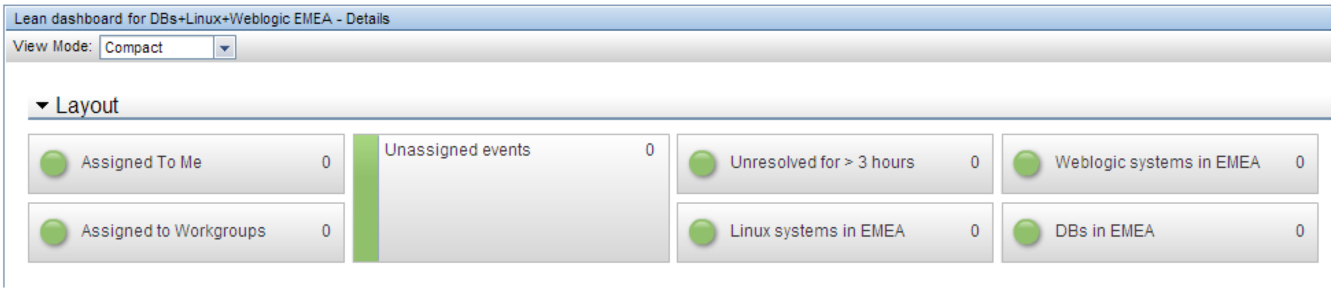
An operator group is typically provided with a customized My Workspace page. My Workspace pages can provide OBM operators with overview dashboards and contextual information, from business impact information to detailed performance graphs. You can customize pages to provide exactly the information that is required to resolve issues quickly, because different operator groups 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 therefore also require different monitoring dashboard layouts.

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

Create Monitoring Dashboards

To create a monitoring dashboard, follow these steps:

1. Go to **Administration > Operations Console > Monitoring Dashboards**.
2. Create an monitoring 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 operator groups DBs EMEA, Linux EMEA, and WebLogic EMEA, it is recommended to create an monitoring 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:



Lean dashboard for DBs+Linux+Weblogic EMEA - Details

View Mode: Compact

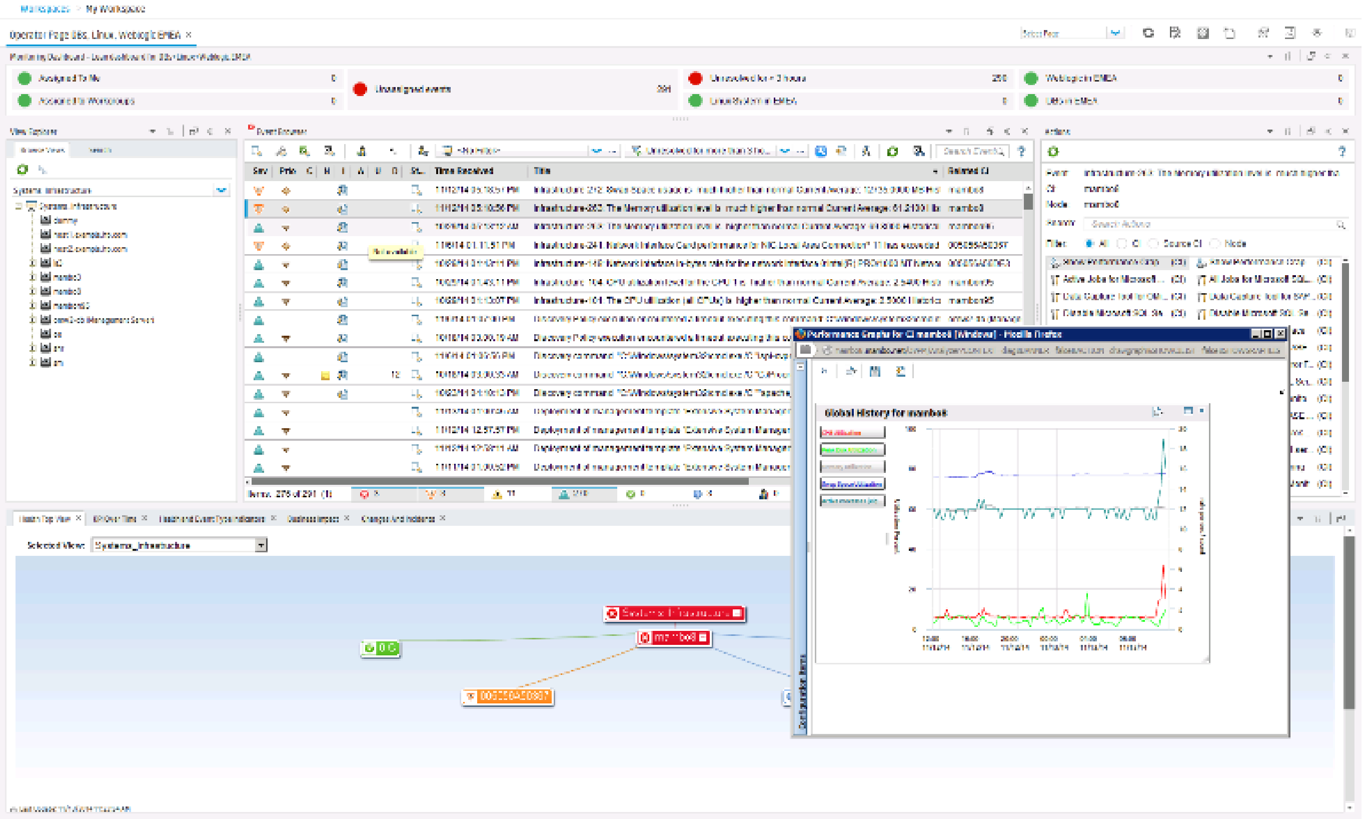
When integrated into a My Workspace page named, for example, DB, Linux, WebLogic EMEA perspective, this dashboard enables operators to quickly see the event status in each area and to quickly filter the event browser by clicking a widget. The monitoring dashboard provides an overview of the event status for all events users are responsible for, so that they are not forced to switch between views or My Workspace pages.

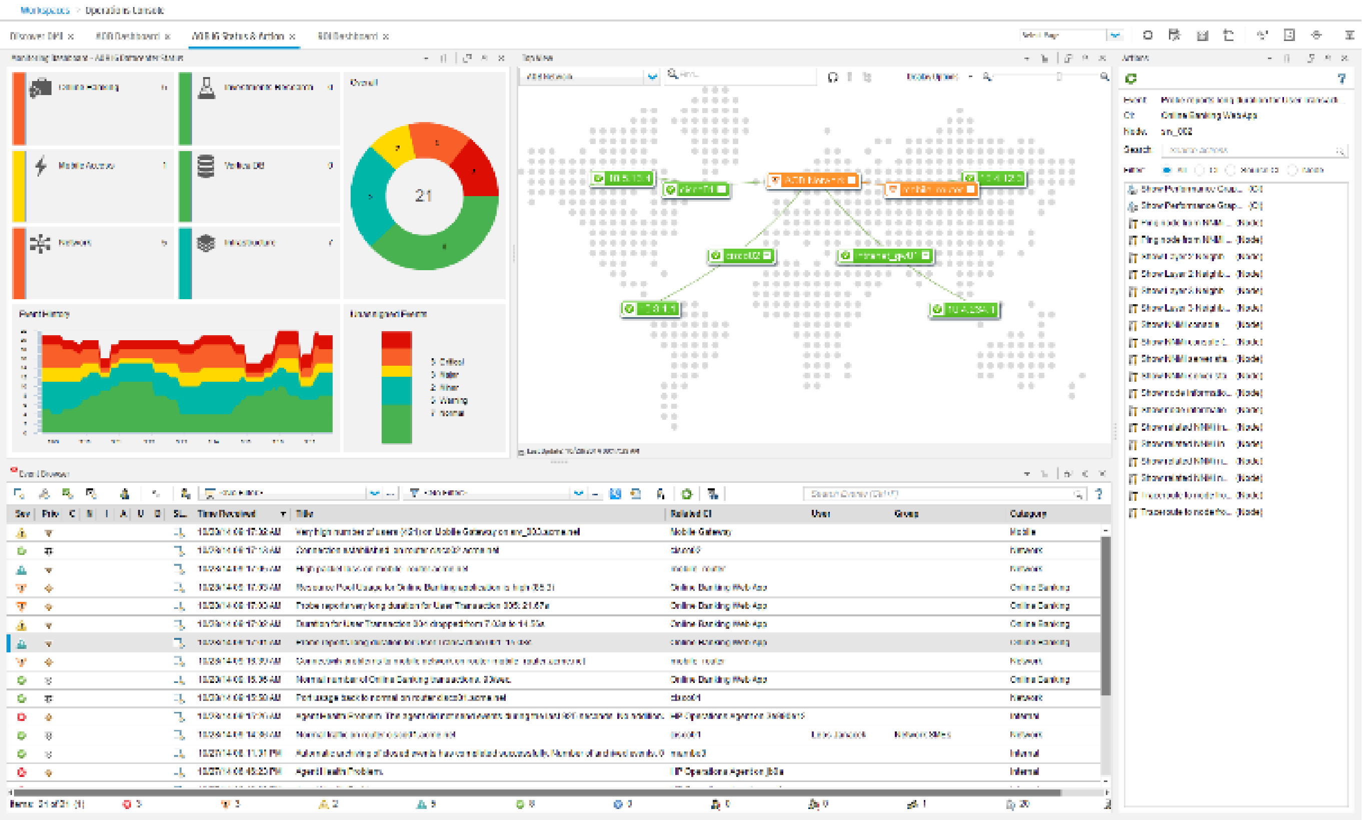
See also the video How to create a Monitoring Dashboard in Video Library.

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 monitoring 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, such as 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:


Workspaces > My Workspace
Operator Page DB, Linux, WebLogic EMEA
Unassigned events
View Explorer
Event Browser
Actions
Systems_Infrastructure
Performance Graphs for CI mambo8 [Windows] - Mozilla Firefox
Global History for mambo8
Selected View: Systems_Infrastructure
Systems_Infrastructure
mambo8



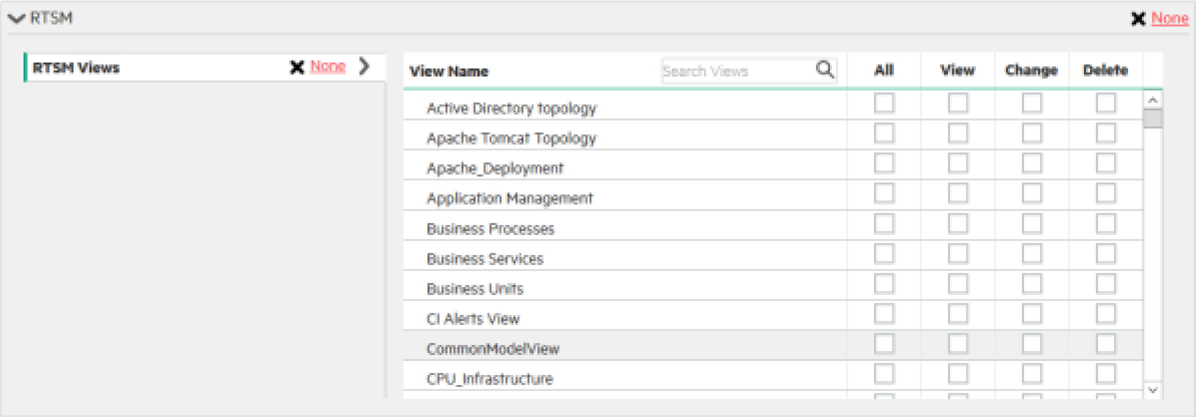
Time Received	Title	Related CI	User	Group	Category
10/28/14 08:17:32 AM	Very high number of users (121) on Mobile Gateway on srv_002.acme.net	Mobile Gateway			Mobile
10/28/14 08:17:13 AM	Connection established on router cisco02.acme.net	cisco02			Network
[illegible]	High packet loss on mobile_router.acme.net	mobile_router			Network
10/28/14 08:17:03 AM	Resource Pool Usage for Online Banking application is high (85.3)	Online Banking Web App			Online Banking
10/28/14 08:17:03 AM	Probe reports very long duration for User Transaction 306: 21.67s	Online Banking Web App			Online Banking
10/28/14 08:17:02 AM	Duration for User Transaction 304 dropped from 7.03s to 14.53s	Online Banking Web App			Online Banking
[illegible]	Probe reports long duration for User Transaction [illegible]	Online Banking Web App			Online Banking
10/28/14 08:16:30 AM	Connectivity problems to mobile network on router mobile_router.acme.net	mobile_router			Network
10/28/14 08:15:36 AM	Normal number of Online Banking transactions: 30/sec.	Online Banking Web App			Online Banking
10/28/14 08:15:30 AM	Port usage back to normal on router cisco01.acme.net	cisco01			Network
[illegible]	Agent Health Problem. The agent did not send events during the last 300 seconds. In addition,	HP Operations Agent on [illegible]			Internal
10/28/14 08:14:58 AM	Normal traffic on router cisco01.acme.net	cisco01	[illegible]	Network Sites	Network
10/27/14 08:11:31 PM	Automatic archiving of closed events has completed successfully. Number of archived events: 0	mambo3			Internal
10/27/14 08:45:23 PM	Agent Health Problem.	HP Operations Agent on jb3a			Internal

Grant permissions

Finally, grant the corresponding permissions on the views, pages, and components that 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.

Views for operators

Grant view permissions for the corresponding views in the RTSM permissions section of a user role.

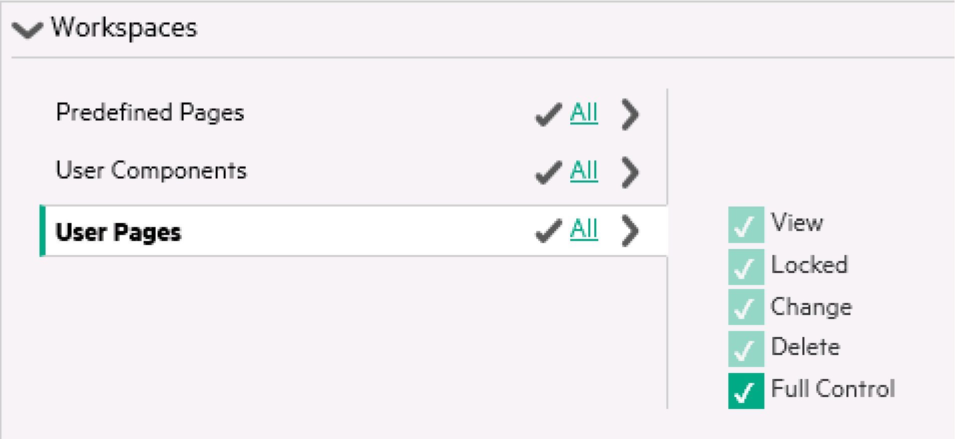


View Name	All	View	Change	Delete
Active Directory topology	□	□	□	□
Apache Tomcat Topology	□	□	□	□
Apache_Deployment	□	□	□	□
Application Management	□	□	□	□
Business Processes	□	□	□	□
Business Services	□	□	□	□
Business Units	□	□	□	□
CI Alerts View	□	□	□	□
CommonModelView	□	□	□	□
CPU_Infrastructure	□	□	□	□

My Workspace pages for operators

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:



Workspaces

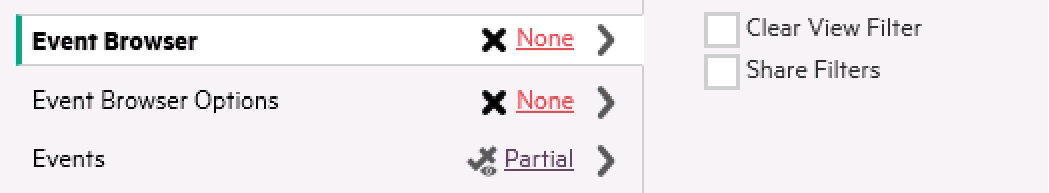
Predefined Pages	✓ All
User Components	✓ All
User Pages	✓ All

☑ View
☑ Locked
☑ Change
☑ Delete
☑ Full Control

Events and permissions for operators

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.

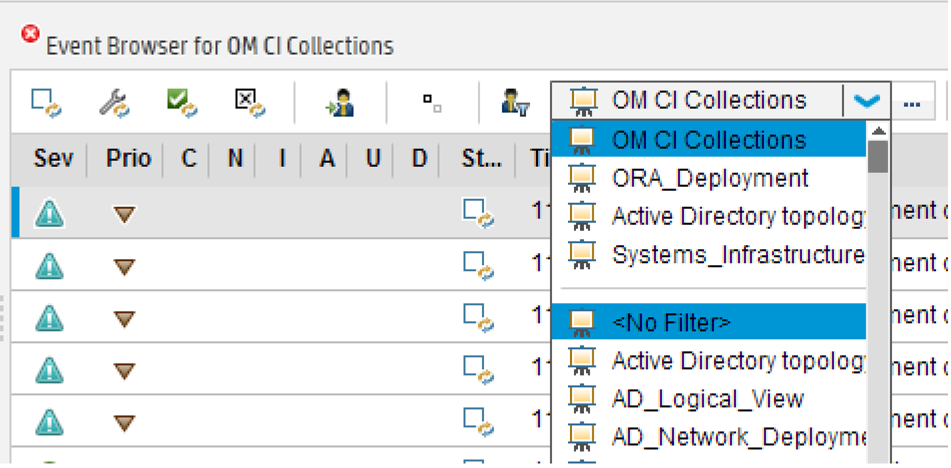
The following figure shows how to clear view filter permission:



Event Browser	✗ None
Event Browser Options	✗ None
Events	Partial

□ Clear View Filter
□ Share Filters

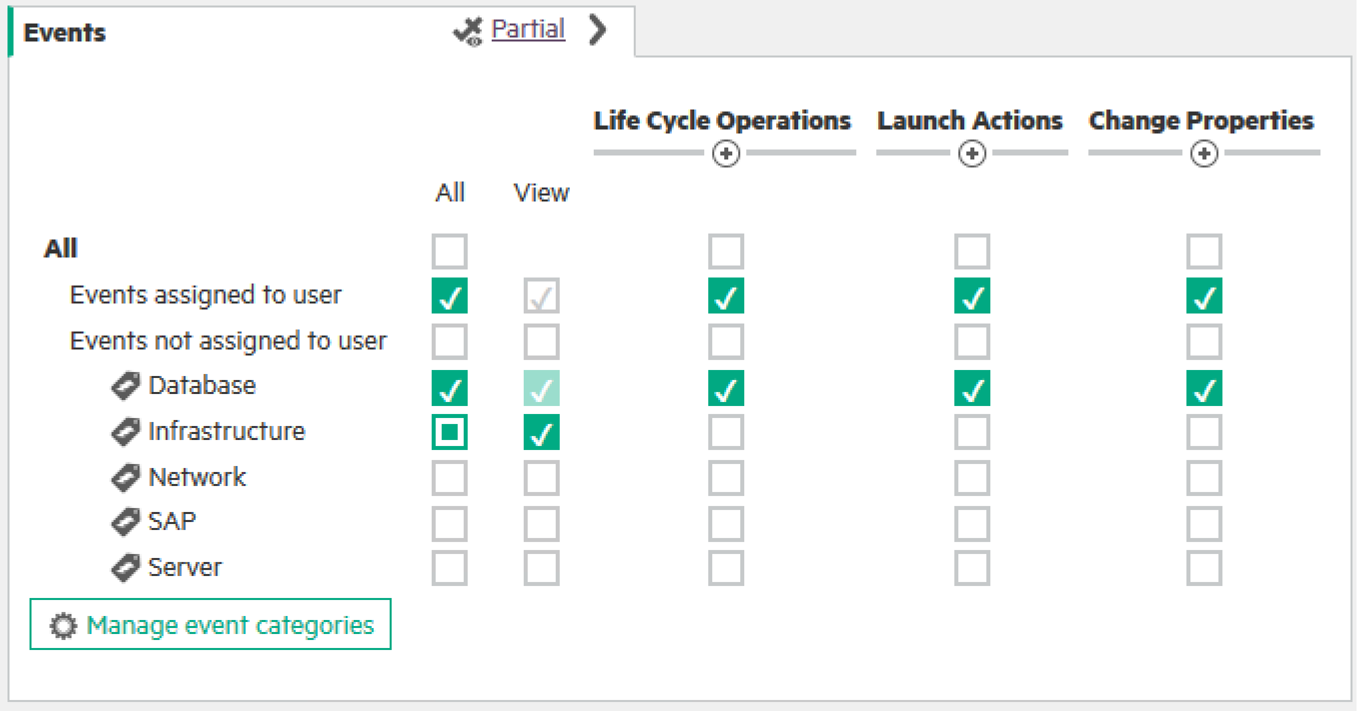
Otherwise, operators would be allowed to clear the view filter in the event browser by selecting <*No Filter*> from the view drop-down list. This would result in all events being shown independently of the view.



Specify the permissions that 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), however with limited permissions for events that are 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.



	All	View	Life Cycle Operations ⊕	Launch Actions ⊕	Change Properties ⊕
All	□		□	□	□
Events assigned to user	☑	☑	☑	☑	☑
Events not assigned to user	□	□	□	□	□
Database	☑	☑	☑	☑	☑
Infrastructure	▣	☑	□	□	□
Network	□	□	□	□	□
SAP	□	□	□	□	□
Server	□	□	□	□	□

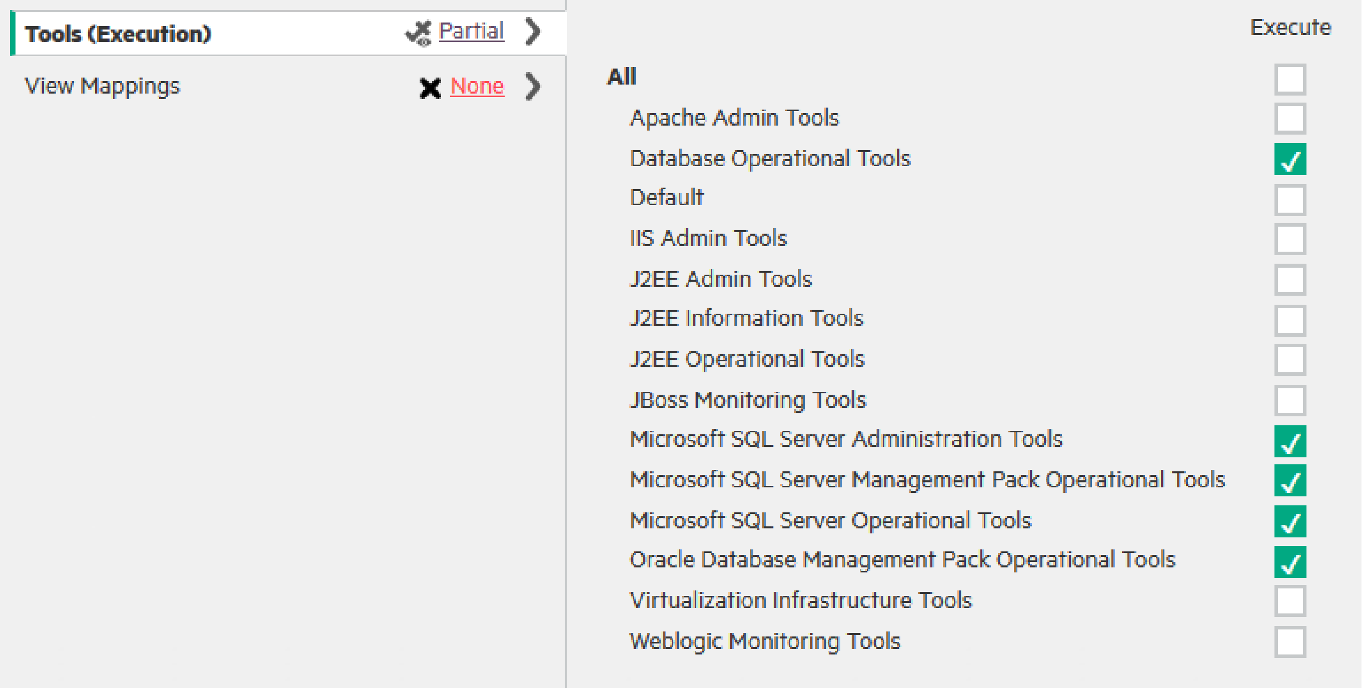
The following permissions are new to OM customers:

- **Event Relations.** Allows an operator to create cause-symptom relationships manually, or to break these relationships. Typically granted to all operators.
- **Transfer Control.** Allows an operator to forward an event to an incident management system (by using the event context menu).
- **Close Transferred.** Allows an operator to close forwarded events. It may not be granted if the event must be under control of the incident management system after forwarding.

Tool categories for operators

Specify the 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:

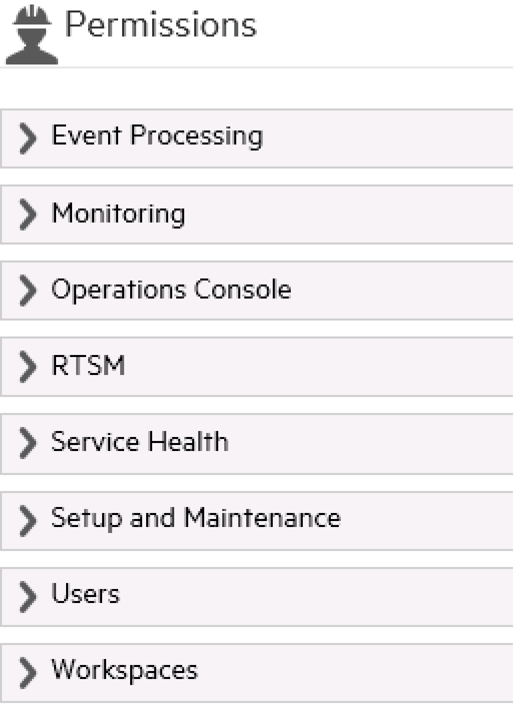


		Execute
Tools (Execution) Partial	All	□
View Mappings ✗ None	Apache Admin Tools	□
	Database Operational Tools	☑
	Default	□
	IIS Admin Tools	□
	J2EE Admin Tools	□
	J2EE Information Tools	□
	J2EE Operational Tools	□
	JBoss Monitoring Tools	□
	Microsoft SQL Server Administration Tools	☑
	Microsoft SQL Server Management Pack Operational Tools	☑
	Microsoft SQL Server Operational Tools	☑
	Oracle Database Management Pack Operational Tools	☑
	Virtualization Infrastructure Tools	□
	Weblogic Monitoring Tools	□

Note OBM displays all categories used in existing tools. The tool category can be set in the tool definition.

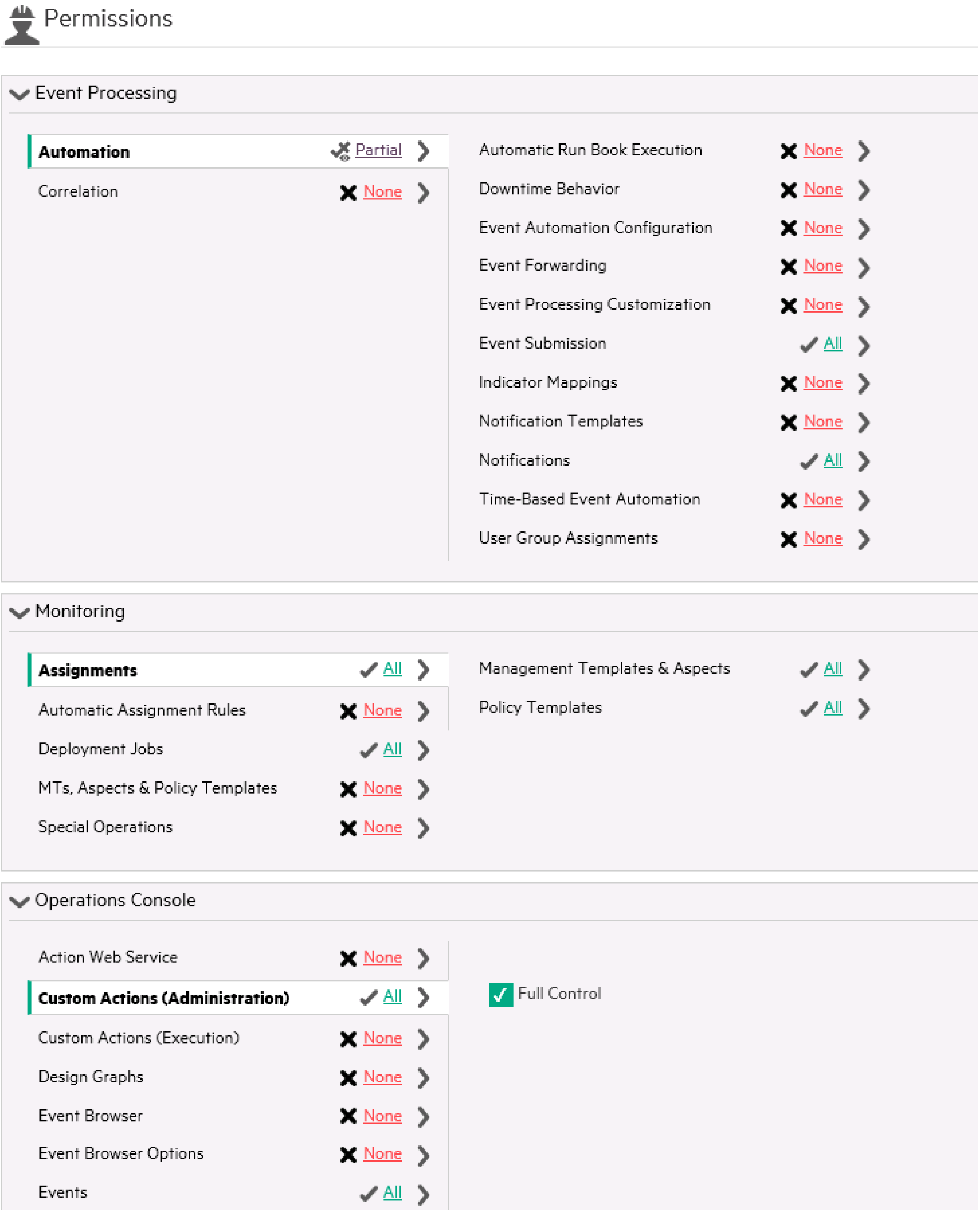
Administrative tasks for users

Access to administrative tasks, such as creating new tools or setting up new nodes, can be given in OBM by granting Full Control permission for the corresponding Administration UI. In OBM 10.10 and later, permissions for viewing, editing and assigning policy templates, aspects, or management templates can be granted for policy template groups respectively per configuration folder. The following figures show an example of administrative permissions in OBM:



Permissions

- Event Processing
- Monitoring
- Operations Console
- RTSM
- Service Health
- Setup and Maintenance
- Users
- Workspaces



Permissions

Event Processing

Automation	Partial
Correlation	✗ None

Automatic Run Book Execution	✗ 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

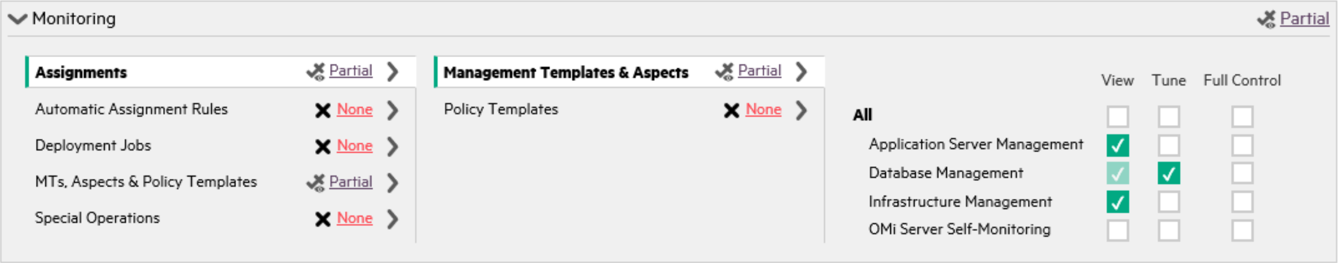
Assignments	✓ All
Automatic Assignment Rules	✗ None
Deployment Jobs	✓ All
MTs, Aspects & Policy Templates	✗ None
Special Operations	✗ None

Management Templates & Aspects	✓ All
Policy Templates	✓ All

Operations Console

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

☑ Full Control



Monitoring — Partial

Assignments	Partial
Automatic Assignment Rules	✗ None
Deployment Jobs	✗ None
MTs, Aspects & Policy Templates	Partial
Special Operations	✗ None

Management Templates & Aspects	Partial
Policy Templates	✗ None

	View	Tune	Full Control
All	□	□	□
Application Server Management	☑	□	□
Database Management	☑	☑	□
Infrastructure Management	☑	□	□
OMi Server Self-Monitoring	□	□	□

Related Topics

Video Library

Manage Operations Agents from OBM

For information on how to manage Operations Agents from OBM, see the following sections:

- Move Operations Agents and their configuration to OBM
- Additional considerations

Move Operations Agents and their configuration to OBM

The following sections describe how to move Operations Agents as well as their configuration to OBM.

Contents

Move Operations Agents to OBM

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

OBM does not offer remote agent deployment (that is, bootstrapping or initial agent deployment) yet, but can deploy agent patches and hotfixes when the agent is installed.
Agents can be installed manually (also remotely by using technologies such as SSH/SCP) or by using other software deployment tools, such as CDA, Server Automation, Microsoft Systems Center 2012 Configuration Manager, puppet, or yum. For details, see the *Operations Agent Help*.

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

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

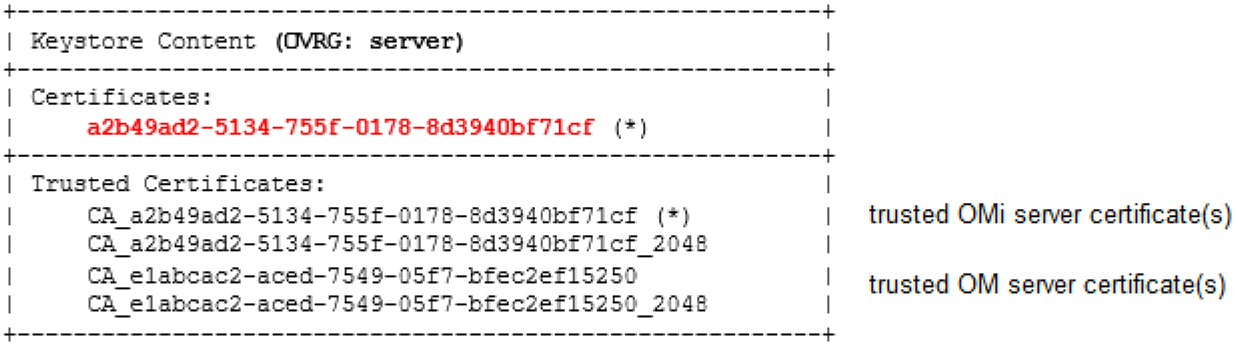
1. Allow the Operations Agent management from both servers by using a flexible management template.
2. Choose a group or type of nodes to move over, for example: all my Oracle Database systems.
   1. Test policy and aspect deployment as well as tool execution from OBM on a representative node of that type. This might include importing OM policies and creating OBM aspects and management templates.
   2. After a successful test, roll out the configuration to the remaining nodes of that type, either manually or by using automatic assignment rules.
   3. Switch the primary manager and target server to OBM. This still allows configuration from both OBM and OM servers.
3. Repeat step 2 until all nodes are managed by OBM.

4. Before switching off the OM server, switch the agents to OBM completely, and clean up old OM policies if necessary.

Configure the OBM server as a secondary manager

To allow step-by-step agent moves, we recommend that you configure the OBM server as a secondary manager:

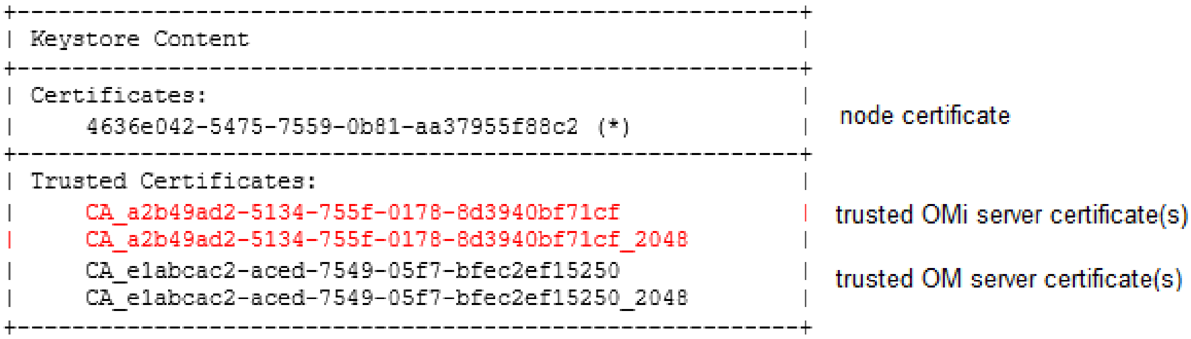
1. Verify that the OM and OBM server certificates are set up correctly (that is, verify the trusted relationship), as described in the Administer section, and that the OBM server is part of the trusted server list of all nodes.On the OBM server, list the server certificate by using `ovcert –list`.The **(OVRG: server)** part of the output lists the server certificate alias, shown in red.Example of an `ovcert –list` output on an OBM 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        |
+---------------------------------------------------------+
```

trusted OMi server certificate(s)
trusted OM server certificate(s)

On a node, `ovcert –list` shows 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        |
+---------------------------------------------------------+
```

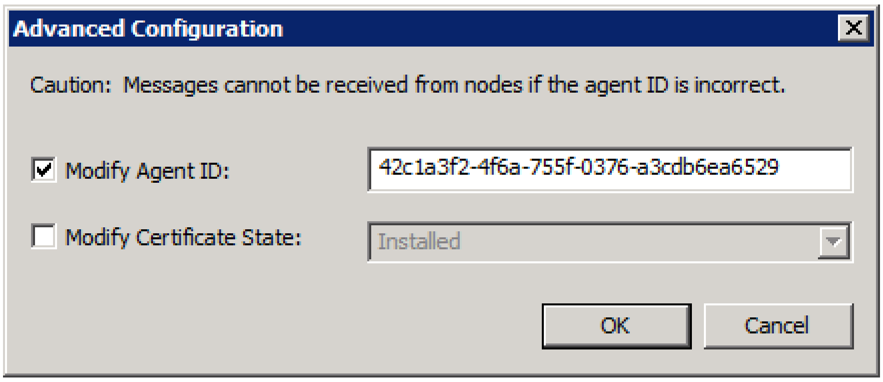
node certificate
trusted OMi server certificate(s)
trusted OM server certificate(s)

   If necessary, update the trusted server list of all nodes by running `ovcert –updatetrusted` on all nodes. To do this in OM for Windows you can use the HP Operations Manager Tools – Certificate Management – Update trusted certificates tool.
2. Set up OBM as **secondary** and **action allow** manager for the agents by using an agent-based flexible management policy. Create this policy on the OM server. You can use the following example as a starting point.The

```
ManagementResponsibilitySwitch example#
# Configuration file
# defines management responsibility switching
#
TIMETEMPLATES
#none
RESPMGRCONFIGS
  RESPMGRCONFIG
    DESCRIPTION "OM and OBM 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"
```

OM automatically adds the `ovcoreid` for each manager to the policy. It retrieves the ID from the corresponding node in the OM database. Make sure that this is the OBM server core id (the ID returned when calling `ovcoreid –ovrg server` on the OBM server). In OM for Windows, you can check and change `ovcoreid` in the node properties:



Advanced Configuration

Caution: Messages cannot be received from nodes if the agent ID is incorrect.

☑ Modify Agent ID: 42c1a3f2-4f6a-755f-0376-a3cdb6ea6529

□ Modify Certificate State: Installed

In OM for UNIX and Linux, you can check `ovcoreid` of a node by using `/opt/OV/bin/OpC/utils/opcnode –list_id node_name=<omi GW/LB/server node>` and change it by using the same command with the `-chg_id` option.

3. Deploy the policy from the OM server to all nodes.

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

When running command-line utilities, such as `ovpolicy` or `ovrc` from an OBM server, you must always specify the `-ovrg server` option (which is not the case with OM, where this option is required only in cluster environments). If you fail to do so, the command fails returning a “not authorized” error.

Move configuration to OBM

We recommend that you move the configuration of nodes to OBM step-by-step to reduce risk and to enable you to become familiar with new features in OBM. Follow these steps:

1. To familiarize yourself with the new OBM 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.

2. Move the configuration of nodes from OM to OBM Monitoring Automation. We recommend that you do not configure a node partially from OBM and partially from OM. Instead, identify those nodes or node groups that can be configured completely from OBM. For example, systems running the Oracle 11 database can be easily managed by 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, you can import your custom OM policies into OBM.
3. When all monitoring artifacts are brought to the OBM server, pick a representative node and test the configuration from OBM 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 are redeployed.
4. 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 you can automate it by using automatic assignment rules.
5. Choose the next OM node group and repeat the steps.

We recommend that you select an OM node group to start with. Determine how it is monitored now and decide how it should be monitored in the future, by using an available Management Pack, custom policies, or both. Depending on your decision, adjust the management template or import customs policies. For details, see the following scenarios:

Scenario 1: Manage nodes by using an available management pack

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

Move from an existing SPI to a management pack

If you are currently using an SPI in OM, you have the following options when moving to the new Management Pack:

1. Deploy the new Management Pack as it is, and check if it fits your needs. If needed, adjust aspect parameters (such as thresholds) on assignment or individual CI level. This option is appropriate for customers who modified the OM SPI slightly, or who want to establish new standards for monitoring.
2. Analyze the SPI customizations that are performed on the OM side to determine which of them are still needed with the new parameterized aspects. For details, use the SPI to MP Evolution Tool to analyze how these customizations are performed.

Scenario 2: Import and reuse custom policies from OM

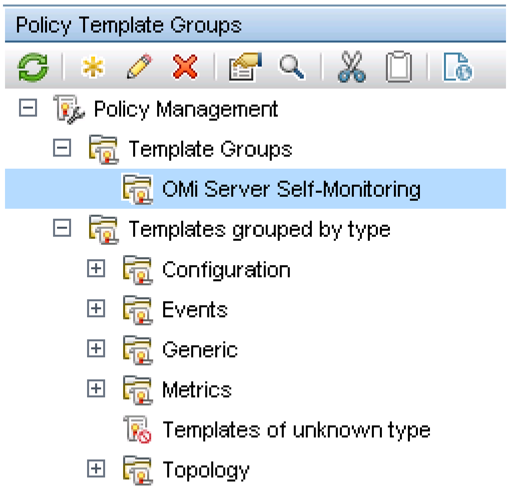
To reuse custom OM policies, you must export and then import policies, parameterize them if needed, and then group them into aspects and management templates.

We recommend that you do this step-by-step, policy group by policy group.

For example, you want to move over the configuration for all your SAP nodes that you organized on the OM side by using a SAP node group. A single SAP node might not receive only 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 must be moved.

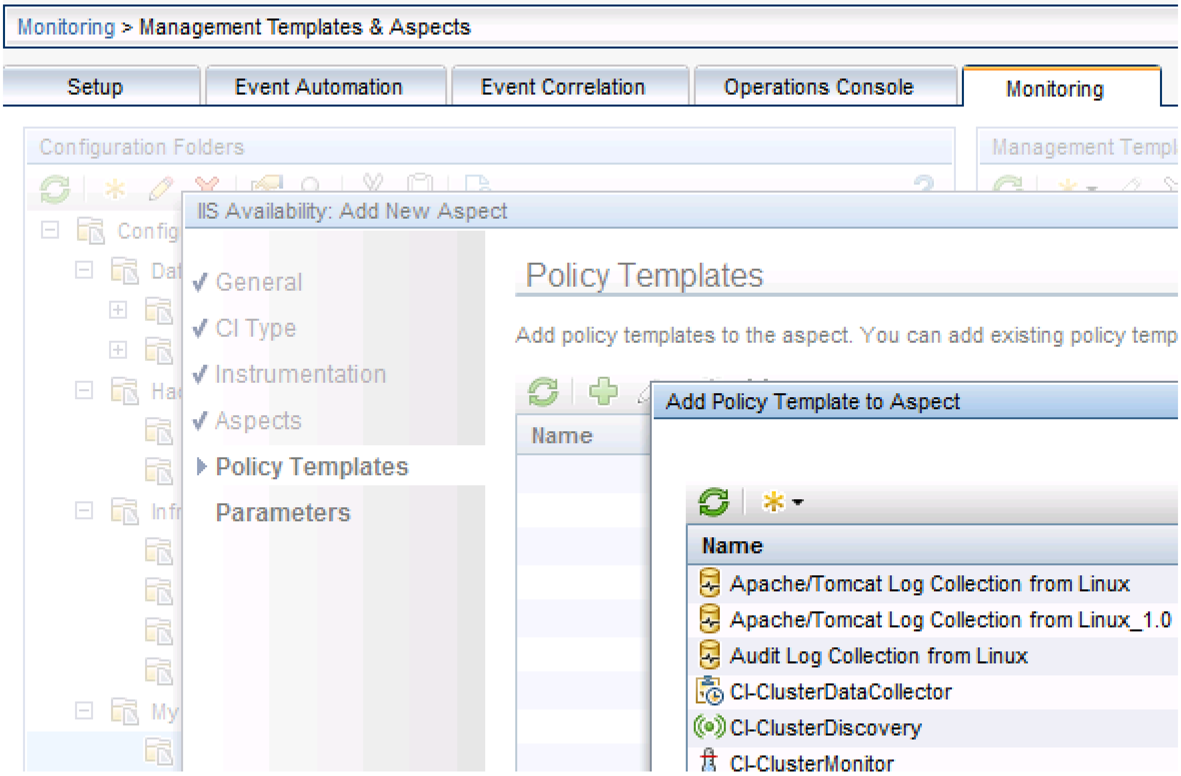
To avoid unnecessary effort, export and import only policies that will be used on the OBM side. Do not export all policies stored on the OM server. Consider the following steps:

1. Identify or create policy groups with policies to export Larger OM customers typically have all their active policies in particular policy groups that are often used also for automatic deployment. If this is your case, you can use these policy groups for the export. If policies are assigned manually from various source policy groups, we recommend that you first create a dedicated new policy group that contains all active policies, the way a node is managed today. Policies that are not supported by OBM, such as ECS, are not copied. Because OBM skips such policies during the import, you do not have to think about supported and unsupported types, just export all the policies by using the policy group name. For details about importing configuration data from Operations Manager, see the Administer section.
2. Export and import policies from OM to OBM The following are 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 `ovpmad` service must have the access or write permissions to the export directory. After the export, copy the downloaded files to an OBM gateway server system.
   - 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> After the export, copy the downloaded files to an OBM gateway server system.
   - Import policies to OBM Consider the following when importing policies to OBM:
     - Syntax check We recommend that you run a syntax check for all policies that are uploaded to OBM. 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 log file for warnings and for an overview. See also the related blog article "Evolve to OBM: Implementing instruction text lookup and addressing other policy import “warnings” at Micro Focus Software Community. OM allows policies with the same name if the policy type is different. However, OBM does not allow policy templates with the same name. Therefore uploading a policy will fail if a policy with the same name already exists. In such cases, first rename the policy in OM and export it again.
     - OM for Linux configuration 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 configuration data upload Specify the copied folder as input directory: c:\HPBSM\opr\bin\ConfigExchange.bat -username <username> -password <password> -uploadOM -i c:\tmp\OMWPolicies By using this import mechanism, the policy group structure is imported as well and shows up as template groups in **Administration > Monitoring > Policy Templates**. The following figure shows an example of



a group structure created as part of a policy import:

3. Adjust policies if necessary If the import returned warnings, edit the imported policies in **Administration > Monitoring > Policy Templates**. This might be necessary if the policies refer to OM server variables such as `$OPC_GUI_CLIENT`, or use features that are not available in OBM, such as server-based MSI. For details about policy templates, see the Administer section.
4. Group policy templates into aspects After importing policies, group them into meaningful aspects. An aspect is defined for a specific CI type and contains all policies that are required to monitor a particular aspect of the CI, such as its performance or availability. For more information, see the OBM tutorial "How to create an aspect containing a group of policy templates" in Video Library. Go to **Administration > Monitoring > Management Templates & Aspects** to create a configuration folder for the aspects. When creating an aspect you must give it a meaningful name, specify its CI Type, and then select the corresponding policies.


Monitoring > Management Templates & Aspects
Setup
Event Automation
Event Correlation
Operations Console
Monitoring
Configuration Folders
Management Templ
Config
Dat
Ha
Infr
My
IIS Availability: Add New Aspect
✓ General
✓ CI Type
✓ Instrumentation
✓ Aspects
Policy Templates
Parameters
Policy Templates
Add policy templates to the aspect. You can add existing policy temp
Name
Add Policy Template to Aspect
Name
Apache/Tomcat Log Collection from Linux
Apache/Tomcat Log Collection from Linux_1.0
Audit Log Collection from Linux
CI-ClusterDataCollector
CI-ClusterDiscovery
CI-ClusterMonitor

In such a way you can create various aspects for various different CI types.

5. Create management templates to group aspects Creating management templates is not necessary, however it is advisable. Management templates can simplify the assignment of many aspects, and also enable you to start monitoring of composite applications with a single assignment. You can group aspects by 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 must use Management templates. To simplify the

assignment of multiple aspects, we recommend that you create one or several management templates after all aspects are created. For example, you can create several management templates with different aspects that represent, for example, Essential and Extensive monitoring levels. Go to **Administration > Monitoring > Management Templates & Aspects** to create a configuration folder for the management templates. When creating a management template, you must give it a meaningful name, specify its view and the root CI Type, and then select the corresponding aspects. If you use the management template for grouping of aspects that belong to a CI Type, you can select any view that contains this CI Type. You do not have to create a sophisticated view for this purpose, because this view is used just as a starting point for the management template definition. If you want to start the monitoring of multiple related CIs of various CI types by using a single assignment, you must create a management template for this purpose. In such a case, you must select (and might have to first create) a view that shows all the CI types and their relations, and use it as a starting point for the management template. Each Management Pack typically ships application views that can be used as a starting point. For details about configuring management templates, see the Administer section.

Scenario 3: Reuse configuration for other node groups

You might have created multiple policy groups on the OM side to monitor various node groups 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 changed only parameters without changing the policy logic, do not import these copies into OBM. Reuse and parameterize an existing policy instead.

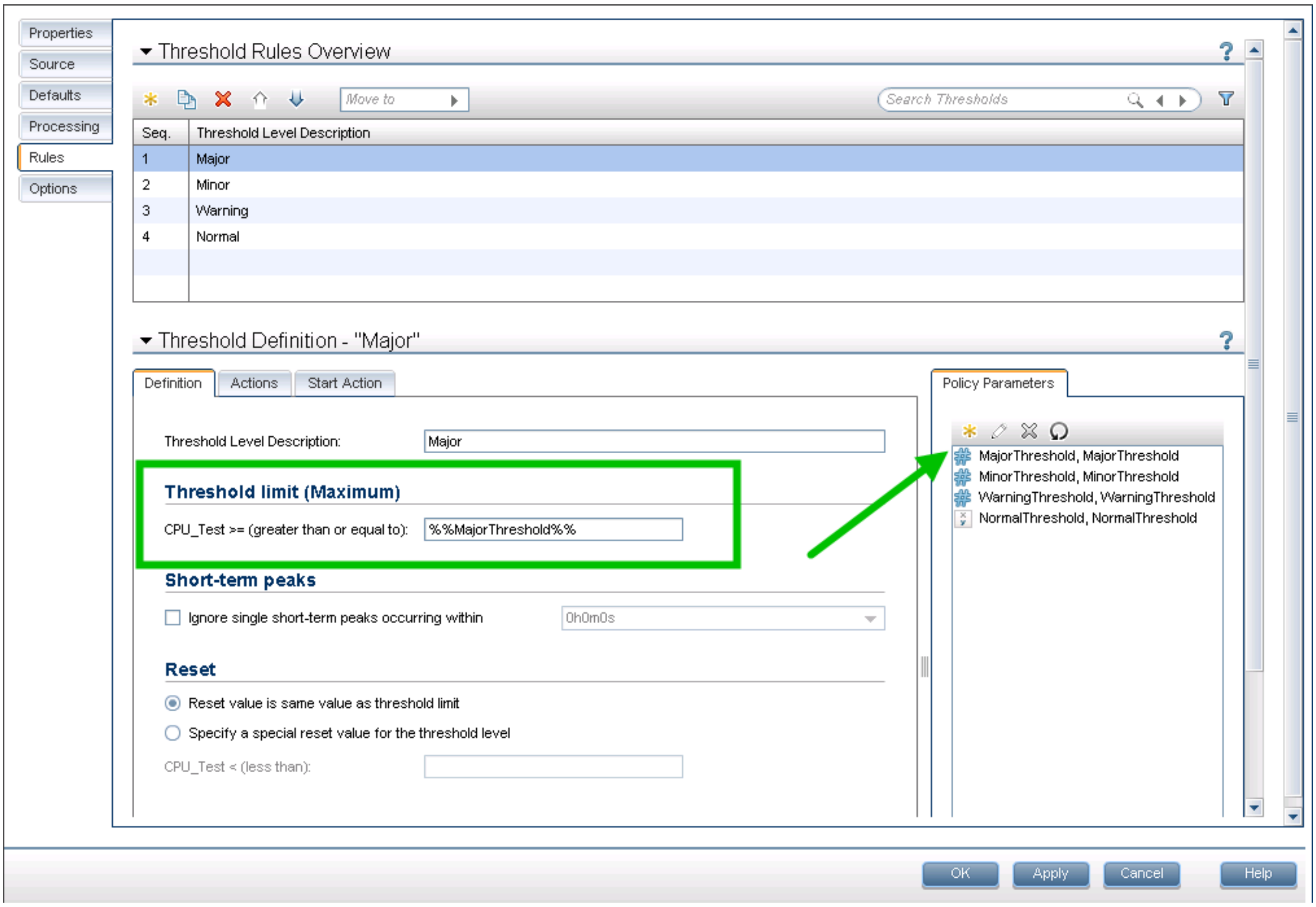
The parameter values are then changed either when assigning an aspect or a management template or when defining multiple aspects or management templates.
Additionally, the tuning of these values can be performed afterward without changing the policy data.

Parameterize policy templates

To parameterize policy templates, follow these steps:

1. Go to **Administration > Monitoring > Policy Templates** and find the existing policy that contains the policy logic that you search for.
2. Edit the policy and identify the parameters that differ among policies in OM. For each such parameter, create a parameter in the OBM policy. For more information, see the OBM tutorial “How to add a parameter to a policy template“ in Video Library.

The following is an example of a simple measurement threshold policy with four rules. The thresholds used in each rule are parameterized. Other message attributes, for example, severity, can also be parameterized:



Threshold Rules Overview

Seq.	Threshold Level Description
1	Major
2	Minor
3	Warning
4	Normal

Threshold Definition - "Major"

Threshold Level Description: Major

Threshold limit (Maximum)

CPU_Test >= (greater than or equal to): %%MajorThreshold%%

Short-term peaks

□ Ignore single short-term peaks occurring within 0h0m0s

Reset

● Reset value is same value as threshold limit

○ Specify a special reset value for the threshold level

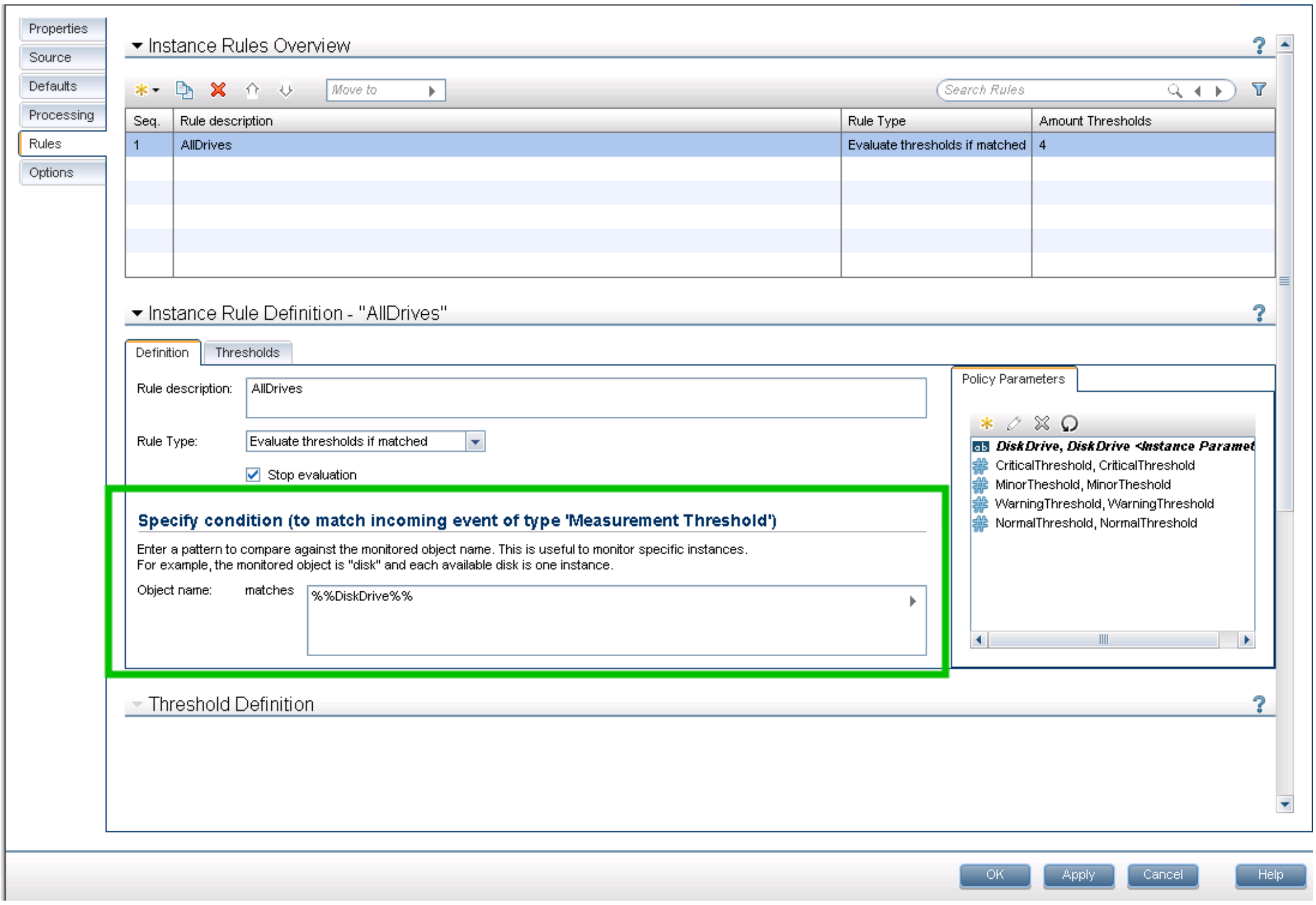
CPU_Test < (less than):

Policy Parameters:

- MajorThreshold, MajorThreshold
- MinorThreshold, MinorThreshold
- WarningThreshold, WarningThreshold
- NormalThreshold, NormalThreshold

Consider the following:

- Instance parameters Sometimes it is necessary to monitor different instances of a monitored object on the same node differently. In OM this is achieved by using instance conditions in measurement threshold policies. Such instance conditions must be replaced by an instance parameter in OBM, which makes it easier to add or remove instances by 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 named **DiskDrive**, and dependent parameters named **Minor disk usage threshold**, **Major disk usage threshold**, and **Critical disk usage threshold**. A user of this policy template can specify multiple disk instances by using the **DiskDrive** parameter, for example, by adding the instance values C:, D:, and E:. For each disk instance, the user can 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:



Seq.	Rule description	Rule Type	Amount Thresholds
1	AllDrives	Evaluate thresholds if matched	4

Rule description: AllDrives

Rule Type: Evaluate thresholds if matched

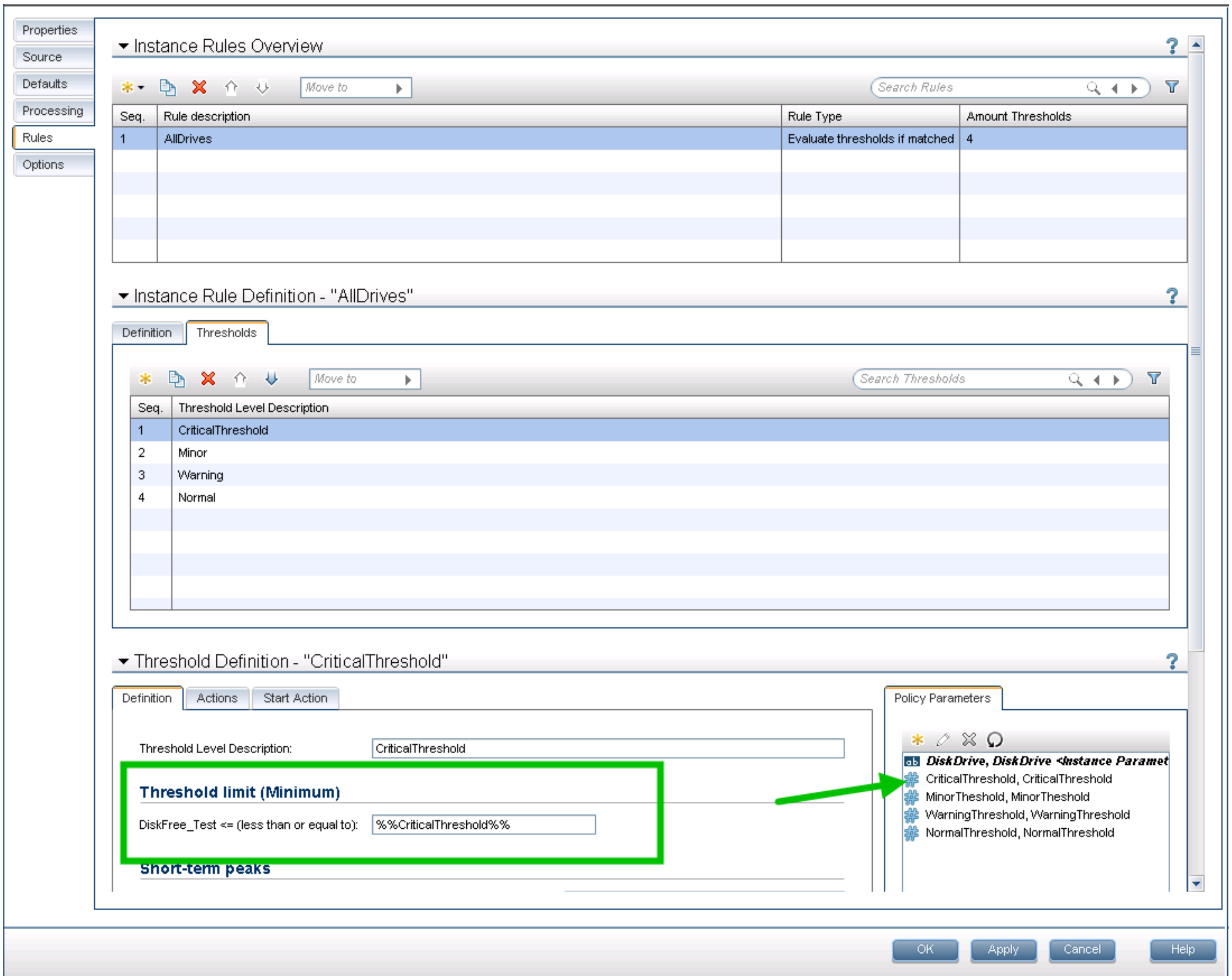
☑ Stop evaluation

Specify condition (to match incoming event of type 'Measurement Threshold')

Enter a pattern to compare against the monitored object name. This is useful to monitor specific instances.
For example, the monitored object is "disk" and each available disk is one instance.

Object name: matches %%DiskDrive%%

- DiskDrive, DiskDrive <Instance Paramet
- CriticalThreshold, CriticalThreshold
- MinorTheshold, MinorTheshold
- WarningThreshold, WarningThreshold
- NormalThreshold, NormalThreshold



Instance Rules Overview

Seq.	Rule description	Rule Type	Amount Thresholds
1	AllDrives	Evaluate thresholds if matched	4

Instance Rule Definition - "AllDrives"

Seq.	Threshold Level Description
1	CriticalThreshold
2	Minor
3	Warning
4	Normal

Threshold Definition - "CriticalThreshold"

Threshold Level Description: CriticalThreshold

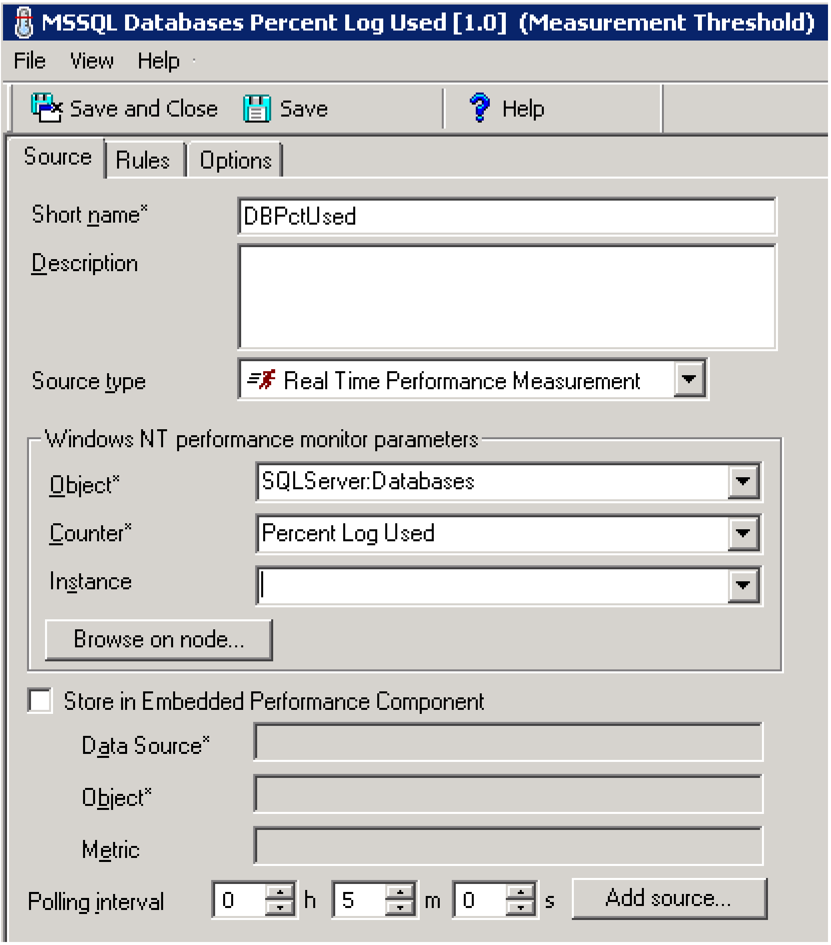
Threshold limit (Minimum)

DiskFree_Test <= (less than or equal to): %%CriticalThreshold%%

Short-term peaks

DiskDrive, DiskDrive <Instance Paramet
CriticalThreshold, CriticalThreshold
MinorTheshold, MinorTheshold
WarningThreshold, WarningThreshold
NormalThreshold, NormalThreshold

- 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, which are configured in Microsoft SQL Server. Different thresholds are set based on the database name. The database name is the instance that is parameterized.



Short name* DBPctUsed

Description

Source type Real Time Performance Measurement

Windows NT performance monitor parameters

Object* SQLServer:Databases

Counter* Percent Log Used

Instance

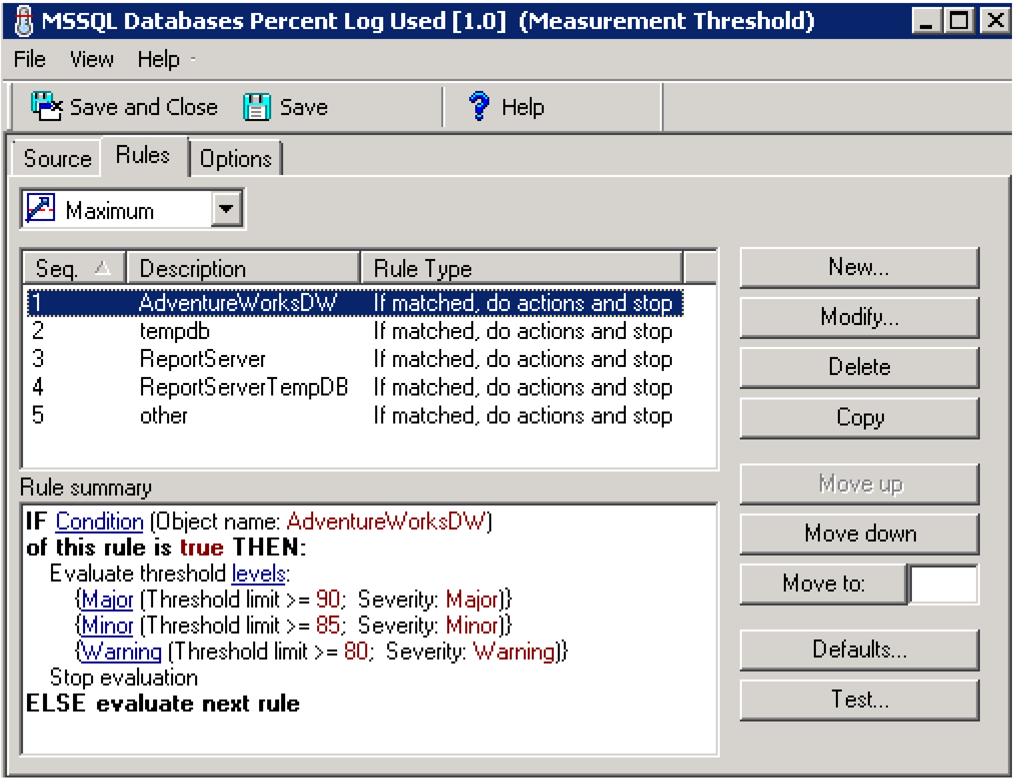
☐ Store in Embedded Performance Component

Data Source*

Object*

Metric

Polling interval 0 h 5 m 0 s



Maximum

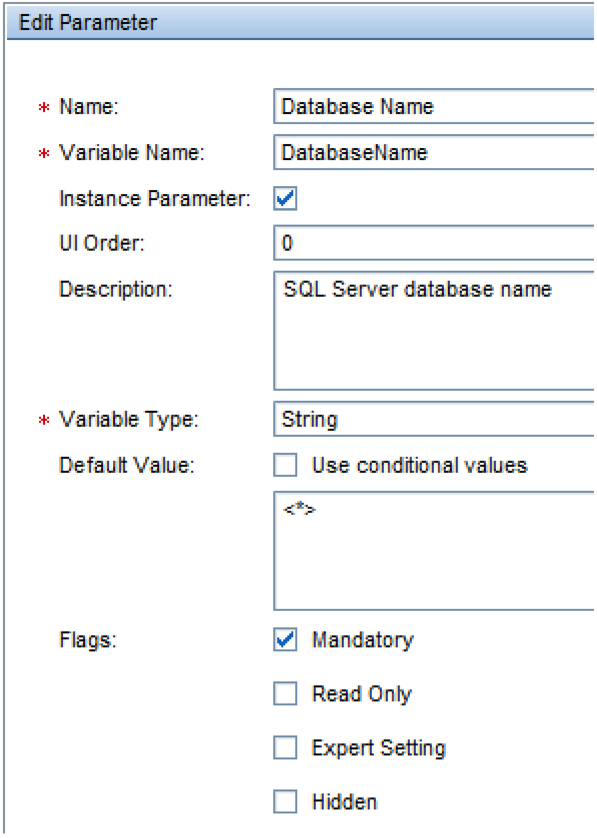
Seq.	Description	Rule Type
1	AdventureWorksDW	If matched, do actions and stop
2	tempdb	If matched, do actions and stop
3	ReportServer	If matched, do actions and stop
4	ReportServerTempDB	If matched, do actions and stop
5	other	If matched, do actions and stop

Rule summary

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

When you have imported the policy into OBM, it can be assigned and used as it is. However, instead of being hard-coded in the policy, the parameters can be defined during the assignment. To enable this, edit the policy template and make the following changes:

1. On 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 does not override the settings during the 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

<*>

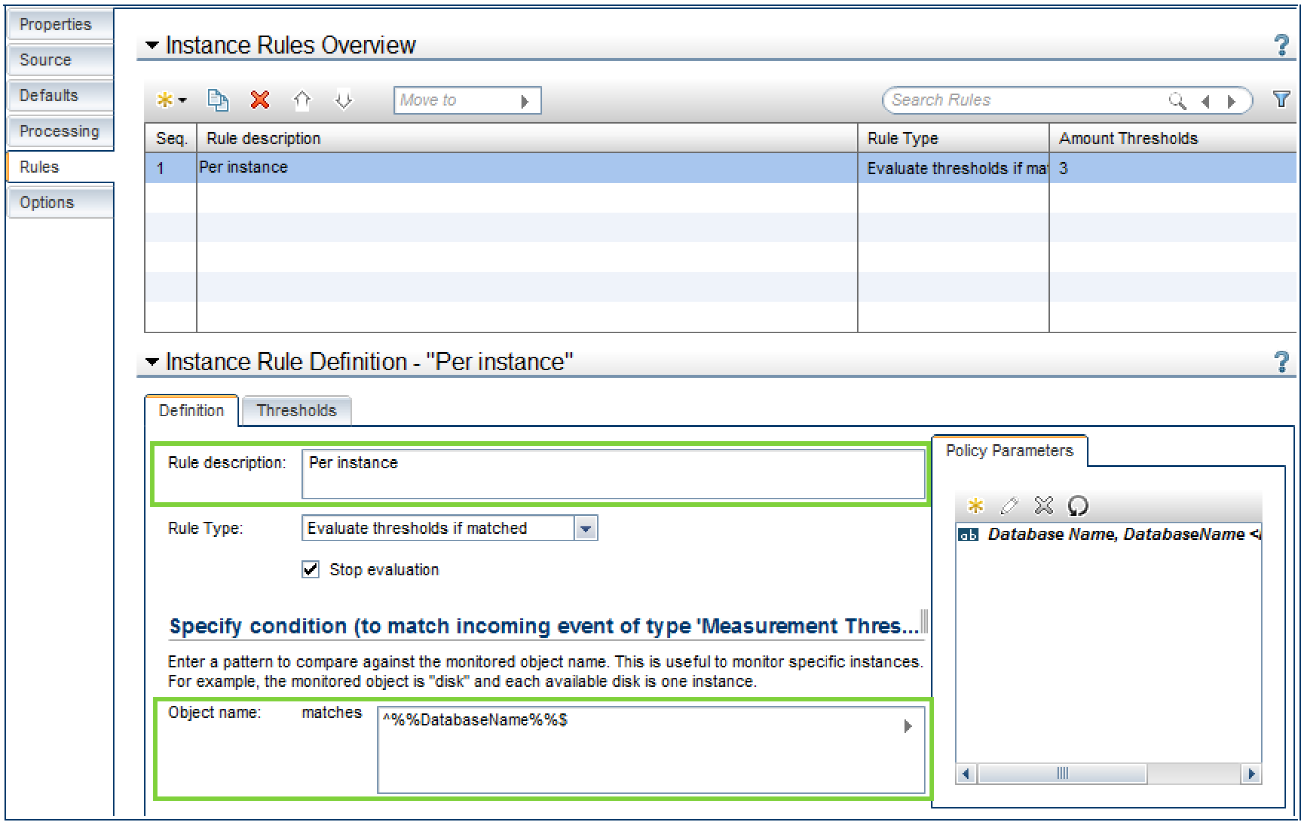
Flags: ☑ Mandatory

□ 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 `^$` to ensure an exact match. For example, `^%%DatabaseName%%$`.



Instance Rules Overview

Seq.	Rule description	Rule Type	Amount Thresholds
1	Per instance	Evaluate thresholds if mat	3

Instance Rule Definition - "Per instance"

Rule description: Per instance

Rule Type: Evaluate thresholds if matched

☑ Stop evaluation

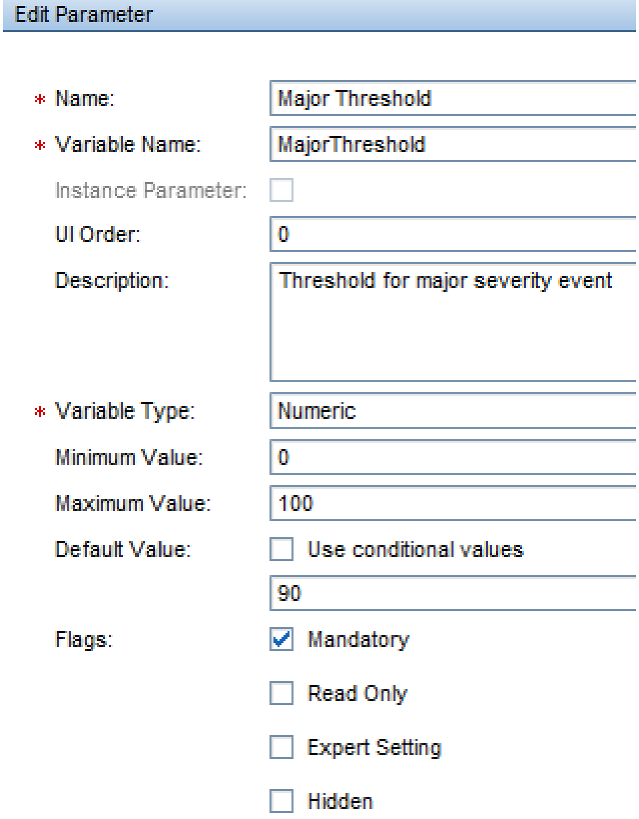
Specify condition (to match incoming event of type 'Measurement Thres...

Enter a pattern to compare against the monitored object name. This is useful to monitor specific instances. For example, the monitored object is "disk" and each available disk is one instance.

Object name: matches ^%%DatabaseName%%$

Policy Parameters: Database Name, DatabaseName <

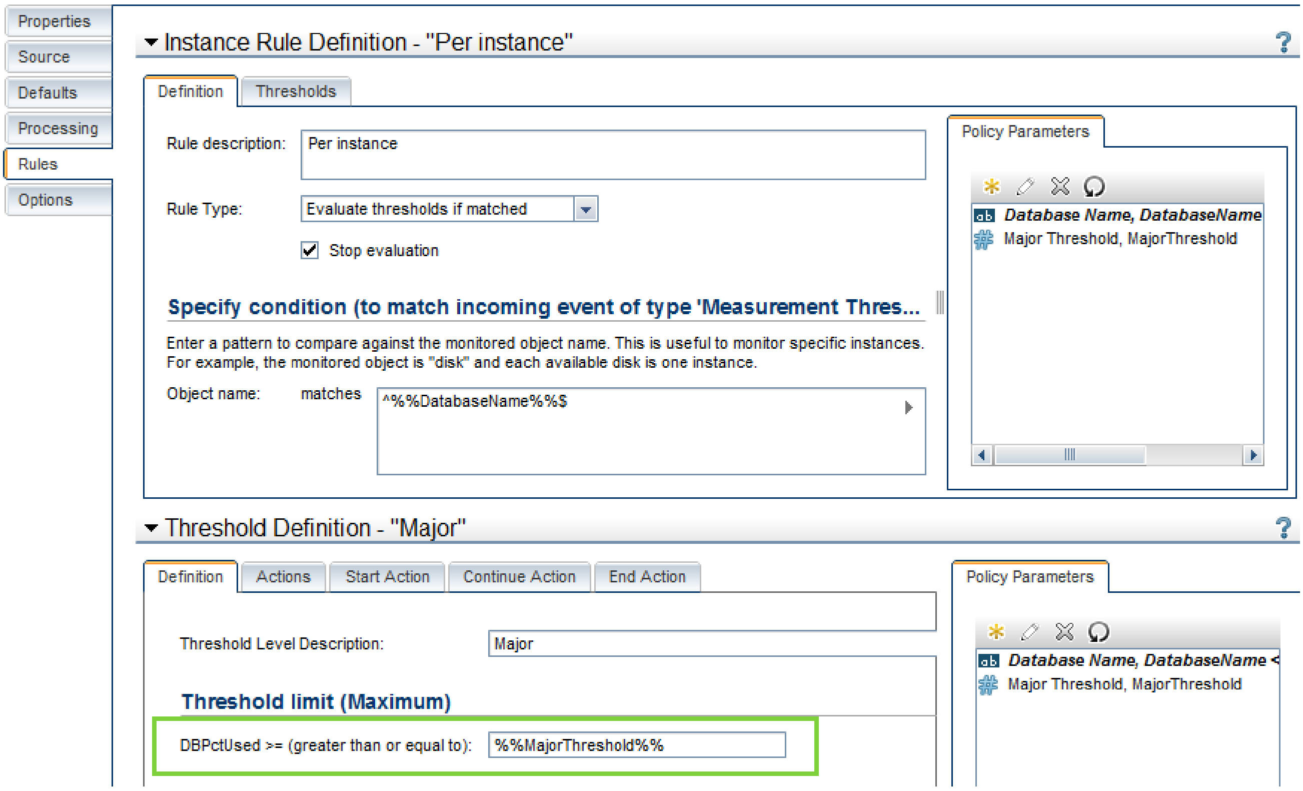
4. To enable setting different thresholds for each database instance, you must also parameterize the threshold settings. This policy has threshold rules for Major, Minor, and Warning thresholds. In the Policy Parameters tab, click to create a new policy parameter for MajorThreshold. Specify if it is numeric, and provide a valid range and a default value.



Edit Parameter

* Name:	Major Threshold
* Variable Name:	MajorThreshold
Instance Parameter:	□
UI Order:	0
Description:	Threshold for major severity event
* Variable Type:	Numeric
Minimum Value:	0
Maximum Value:	100
Default Value:	□ Use conditional values 90
Flags:	☑ Mandatory □ Read Only □ Expert Setting □ Hidden

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



Instance Rule Definition - "Per instance"

Rule description: Per instance

Rule Type: Evaluate thresholds if matched

☑ Stop evaluation

Specify condition (to match incoming event of type 'Measurement Thres...

Enter a pattern to compare against the monitored object name. This is useful to monitor specific instances. For example, the monitored object is "disk" and each available disk is one instance.

Object name: matches ^%%DatabaseName%%$

Policy Parameters: Database Name, DatabaseName; Major Threshold, MajorThreshold

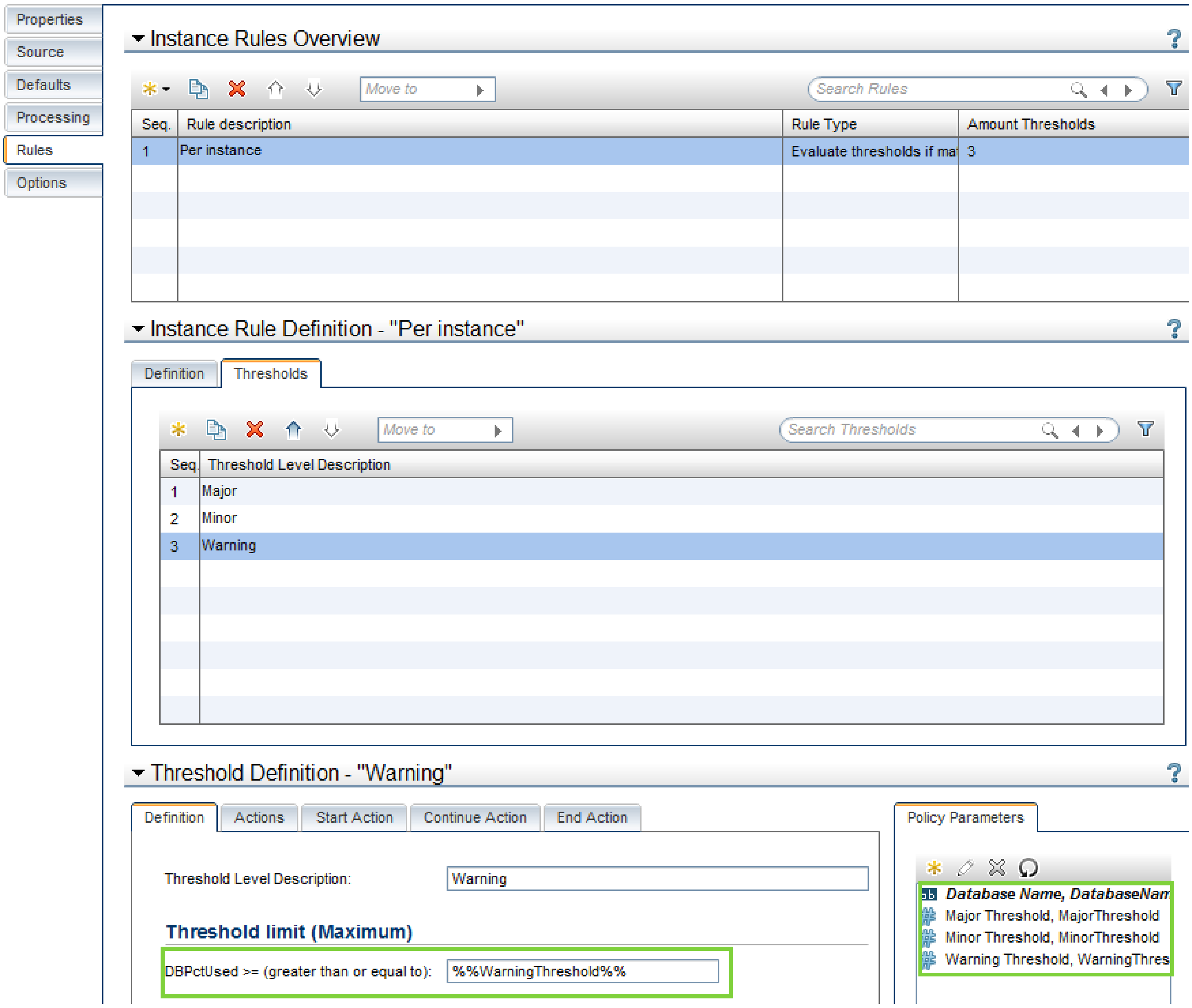
Threshold Definition - "Major"

Threshold Level Description: Major

Threshold limit (Maximum)

DBPctUsed >= (greater than or equal to): %%MajorThreshold%%

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.



Seq.	Rule description	Rule Type	Amount Thresholds
1	Per instance	Evaluate thresholds if mat	3

Seq.	Threshold Level Description
1	Major
2	Minor
3	Warning

Threshold Level Description: Warning

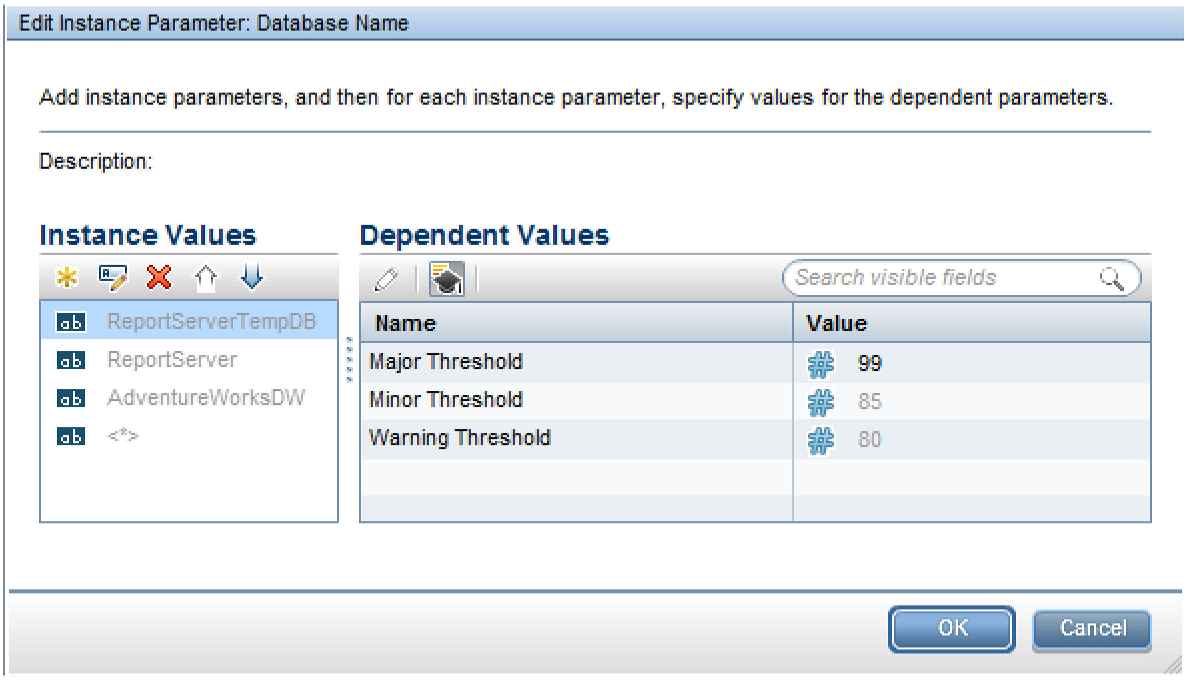
Threshold limit (Maximum)

DBPctUsed >= (greater than or equal to): %%WarningThreshold%%

Database Name, DatabaseNam
Major Threshold, MajorThreshold
Minor Threshold, MinorThreshold
Warning Threshold, WarningThres

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 instances to be monitored and override the thresholds for each instance. 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.



Edit Instance Parameter: Database Name

Add instance parameters, and then for each instance parameter, specify values for the dependent parameters.

Description:

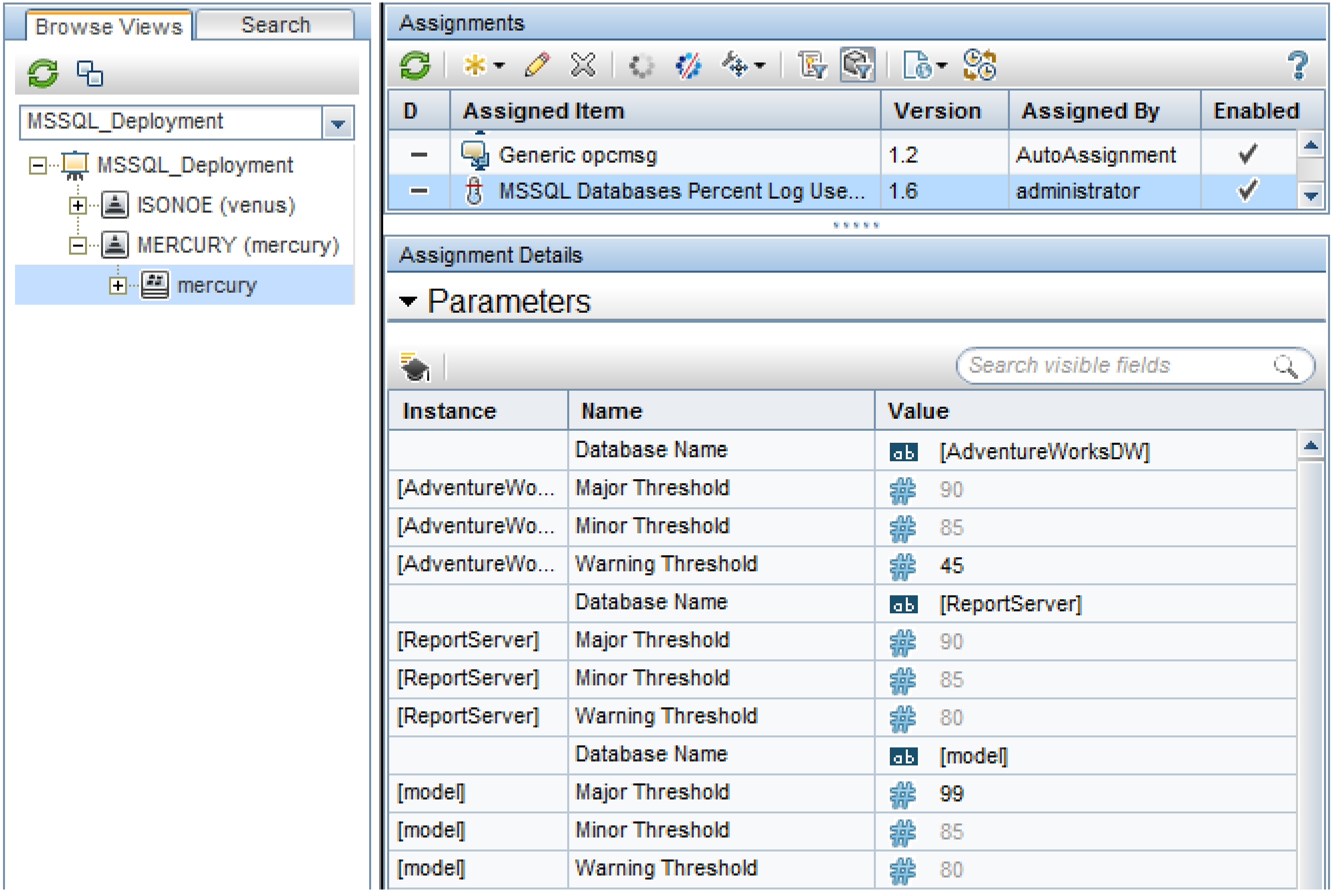
Instance Values

ReportServerTempDB
ReportServer
AdventureWorksDW
<*>

Dependent Values

Name	Value
Major Threshold	99
Minor Threshold	85
Warning Threshold	80

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 get the same threshold settings, but you can override the thresholds for each instance in the Assignments and Tuning screen.



Assignments

D	Assigned Item	Version	Assigned By	Enabled
–	Generic opcmsg	1.2	AutoAssignment	✓
–	MSSQL Databases Percent Log Use...	1.6	administrator	✓

Assignment Details

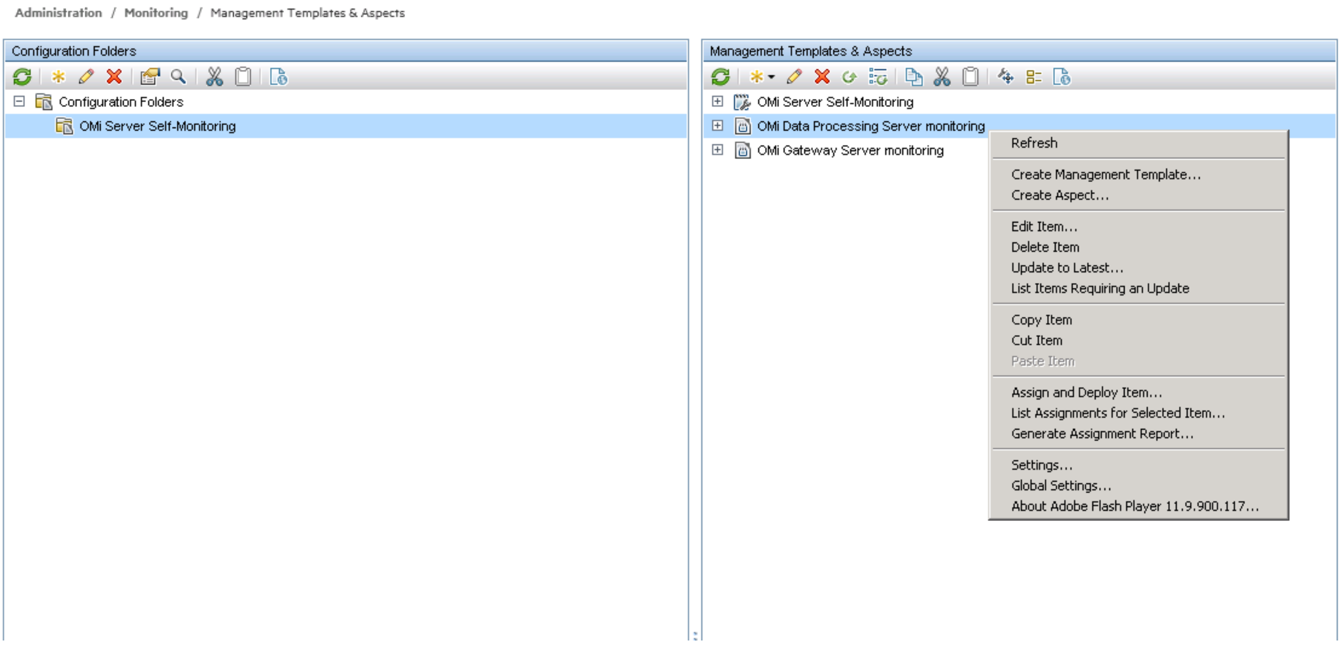
Parameters

Instance	Name	Value
	Database Name	[AdventureWorksDW]
[AdventureWo...	Major Threshold	90
[AdventureWo...	Minor Threshold	85
[AdventureWo...	Warning Threshold	45
	Database Name	[ReportServer]
[ReportServer]	Major Threshold	90
[ReportServer]	Minor Threshold	85
[ReportServer]	Warning Threshold	80
	Database Name	[model]
[model]	Major Threshold	99
[model]	Minor Threshold	85
[model]	Warning Threshold	80

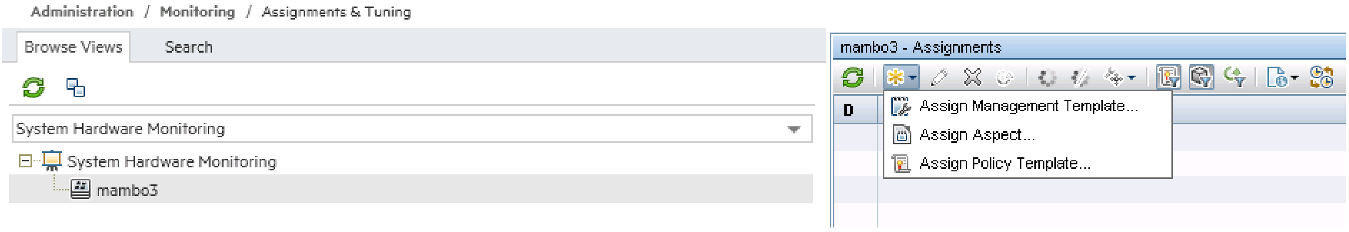
Test configuration

When you choose or create the aspects and Management Templates you want to use, use manual assignments to test and verify the configuration:

- You can assign Management Templates and aspects by using the aspect or Management Template as a starting point: Go to **Administration > Monitoring > Management Templates & Aspects**, select the aspect or Management Template that you want to deploy, and then choose Assign and Deploy Item:


Administration / Monitoring / Management Templates & Aspects
Configuration Folders
Configuration Folders
OMi Server Self-Monitoring
Management Templates & Aspects
OMi Server Self-Monitoring
OMi Data Processing Server monitoring
OMi Gateway Server monitoring
Refresh
Create Management Template...
Create Aspect...
Edit Item...
Delete Item
Update to Latest...
List Items Requiring an Update
Copy Item
Cut Item
Paste Item
Assign and Deploy Item...
List Assignments for Selected Item...
Generate Assignment Report...
Settings...
Global Settings...
About Adobe Flash Player 11.9.900.117...

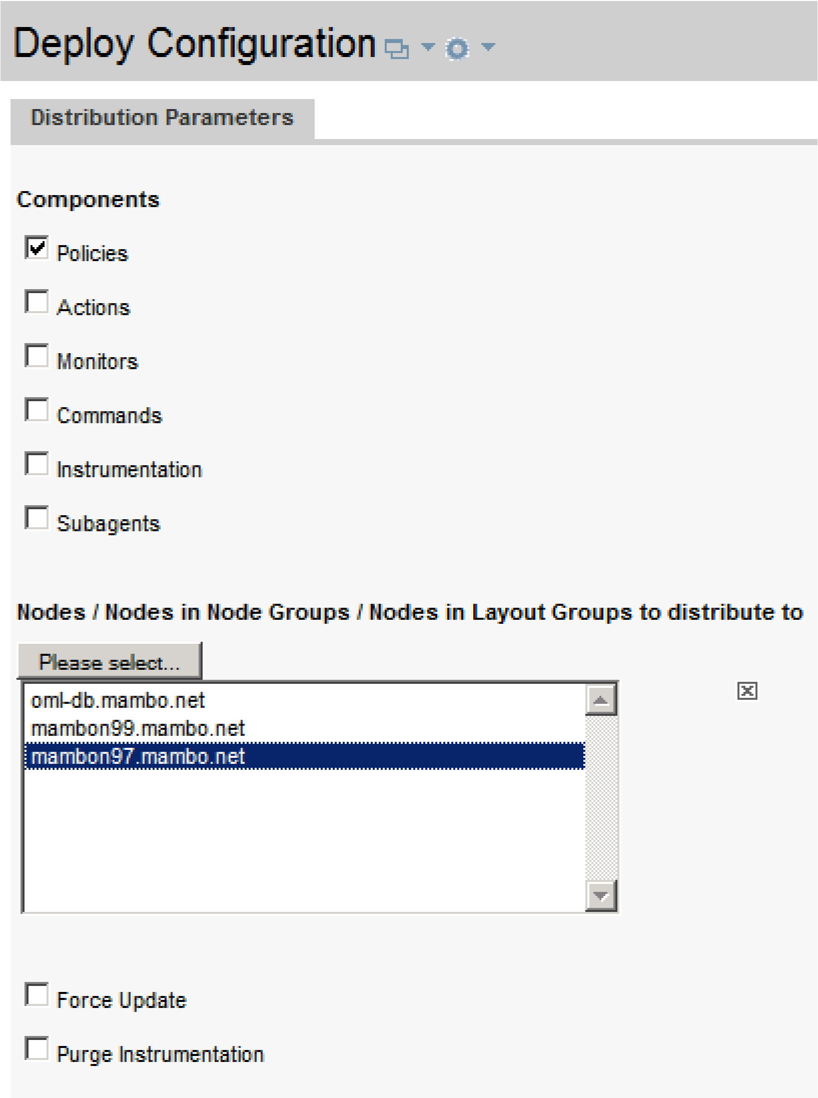
- Alternatively, you can use the CI as a starting point: Go to **Administration > Monitoring > Assignments & Tuning**, select a view that contains the CI, and then choose **Assign ...** from the drop-down list:


Administration / Monitoring / Assignments & Tuning
Browse Views
Search
System Hardware Monitoring
System Hardware Monitoring
mambo3
mambo3 - Assignments
D
Assign Management Template...
Assign Aspect...
Assign Policy Template...

  The assignment by default initiates an immediate deployment of all included policy templates to the corresponding nodes. You can then verify whether all policies are redeployed on the representative node: ovpolicy -list -host <hostname> -level 2 –ovrg server This lists all policies and the management server where the policy is installed. It might list old policies deployed from OM that are not replaced by OBM.
- You can also use the Synchronize Policy Template Assignments feature of OBM to see the policies deployed from OM:
  1. Go to **Administration > Setup and Maintenance > Monitored Nodes** and select a node.
  2. Choose Synchronize Policy Template Assignments from the context menu, and then check the assignments on **Administration > Monitoring > Assignments & Tuning**. Make sure to show policy assignments as well, because OM can assign only policies and does not operate with aspects or management templates. Policies on a node cannot have the identical name. If multiple assignments on the OBM side assign policy templates with different versions, the policy template with the highest version number (and its parameter values) is deployed by OBM.

Make sure you understand what happens in the following scenarios:

- A policy is deployed by OM, got imported into OBM, and redeployed as part of an aspect or a management template The policy is deployed again from OBM and replaces the existing policy with the same version. Afterward, the policy owner becomes the OBM server.
- A policy is deployed by OM, got imported into OBM, adjusted (new version created), and redeployed The policy is deployed again from OBM and replaces the existing policy with a lower version. Afterward, the policy owner becomes the OBM server.
- A policy is deployed by OM, got imported into OBM, renamed, and redeployed as part of an aspect or Management Template The renamed policy is deployed from OBM, in addition to the already existing policy. The OM policy must be removed manually.
- Someone tries to delete a policy or policy assignment on OM after policies are deployed from OBM OM checks the policy owner before deleting policies. If the policy owner is OBM, then OM does not delete the policy (unless you specifically ignore the owner or choose force update).
- Removal of the old OM policies If policies are not renamed and if all used policies are imported into OBM and redeployed from OBM through corresponding aspect or management template assignments, there is no need to delete old OM policies because they no longer exist. They are deleted and replaced by corresponding OBM policies. If you decided to no longer use certain policies, they must be removed from the corresponding nodes. One way to do this is by using the OM console:
    - In OM for UNIX, delete the corresponding assignment to a policy group, a node group or a node and deploy policies.



Deploy Configuration

Distribution Parameters

Components

☑ Policies

☐ Actions

☐ Monitors

☐ Commands

☐ Instrumentation

☐ Subagents

Nodes / Nodes in Node Groups / Nodes in Layout Groups to distribute to

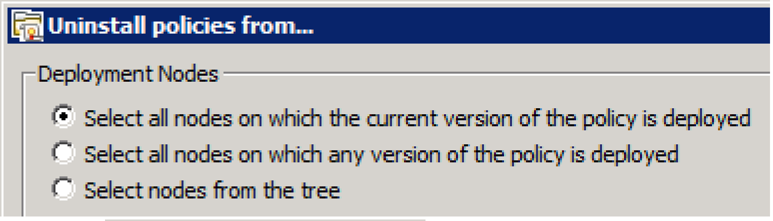
Please select...

oml-db.mambo.net
mambon99.mambo.net
mambon97.mambo.net

☐ Force Update

☐ Purge Instrumentation

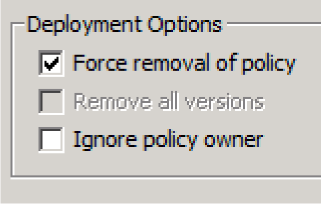
    Make sure that Force Update is not selected.
    - In OM for Windows, choose the policy version and choose **Uninstall from...** from the context menu.



Uninstall policies from...

Deployment Nodes

● Select all nodes on which the current version of the policy is deployed
○ Select all nodes on which any version of the policy is deployed
○ Select nodes from the tree



Deployment Options

☑ Force removal of policy
□ Remove all versions
□ Ignore policy owner

Make sure that **Ignore policy owner** is not selected: You can also remove old OM policies by using the `-deploy -clean` option of the `opr-agt` tool. For example: opr-agt -deploy –clean -node_list "node1.example.com,node2.example.com" For details about the `opr-agt` command-line interface, see the Develop section.

- A node is deleted from OM We do not recommend deleting nodes from OM during the evolution, because if the topology synchronization between OM and OBM is still active, the node CI is deleted from the RTSM as well. To prevent this from happening, set the **Skip CI Deletion** infrastructure setting (**Application > Operations Management > OM Topology Synchronization Settings**) to True. This disables the automatic deletion of CIs when performing topology synchronization.

Roll out configuration

When the configuration is validated by 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, by using web services or automatic assignment rules, as follows:

- Manual Roll Out To assign configuration to multiple CIs manually, use **Administration > Monitoring > Management Templates & Aspects** with an aspect or a management template as a starting point. Select all corresponding CIs manually.
- Automation Through Web Services You can achieve automation by using the Monitoring Automation Web Service Interface. For example, a management template can be assigned programmatically to a CI when a new server is provisioned. For more information on use cases for the Monitoring Automation (MA) Web Service Interface, see the Develop section.
- Automatic Assignment Rules You can also achieve automation by using automatic assignment rules, as described in the following section.

Use automatic assignment rules

Automatic assignment rules are defined for particular 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 want yet to configure from OBM. 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 is triggered. To avoid this, choose another view that contains only those CIs that you want to configure from OBM.

The following are examples of using automatic assignment rules:

- Example of assigning Gold, Silver, and Bronze monitoring levels to different nodes On the OM side you deployed different policy groups representing Gold, Silver, and Bronze monitoring levels to different node groups. To automate this in OBM, you use three Management Templates (or summary aspects with nested aspects), and three views that contain the corresponding CIs. Management templates and aspects are defined for particular CI Types, such as Oracle or computer. When you want to assign them, you require 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 particular query. For example, if you have Oracle databases to be monitored by using a Gold Management template, and if you can determine these databases based on CI attributes or relationships to other CIs, then you can define a pattern view that contains only those CIs. If the CI attributes do not yet contain enough information, then try to add the information in an automated way, for example, by using enrichment rules or RTSM APIs, because adding and maintaining CI collections manually is often not suitable when you want to automate monitoring.
- Example of assigning multiple management templates or aspects to the same nodes On the OM side you deployed different policy groups, for example, for Linux, Oracle, or other application management areas, to a single node. To automate this in OBM, you use multiple automatic assignment rules with corresponding management templates or summary aspects with nested aspects, and views. 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 it cannot be determined which one is applied. 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). For more details, go to **Administration > Monitoring > Automatic Assignment Rules** and see the corresponding OMi Help topics.

Avoid policy assignment to nodes that are not yet managed by OBM

When the OBM server is specified as the primary manager of an agent, the Operations Agent sends information about its node name and IP address to the OBM server. When this data is received, OBM creates a relationship between the OA CI and the OBM server CI in the RTSM, which means that the agent is now managed by OBM. This relationship can also be created manually by using the node editor “managed by OBM” 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 OBM. Add the Operations Agent and OBM server CI types to your view with corresponding relationships to nodes. Nodes and related CIs that are not managed by OBM may not appear in the view result.

Use such a view in automatic assignment rules. Whenever another agent is switched to OBM and sends its node name or IP address data to OBM, it appears in the view and automatically gets the corresponding assignments.

Alternatively, you could assign aspects to all nodes, but deploy the flexible management policy that grants OBM the right to deploy policies only to the nodes that you want to switch. In this case, deployment jobs for nodes that do not allow policy deployment from OBM fail, but they can be deleted manually and the deployment can be triggered again when the node is switched. However, this option does not show which nodes are already switched.

OM and OBM policy assignment and deployment functionality comparison

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

Functionality	OM for UNIX	OM for Windows	OBM
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 through "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 a configuration object or a CI	Can assign fixed, latest, or minor to latest version to a policy group, a node group or a node	Can assign fixed or latest policy version to a policy group Fixed policy version is assigned or deployed to a node or a node group	Relationships among management templates, aspects, and policy templates are based on fixed versions Fixed versions are assigned or deployed to CIs
Update version assignment to a configuration object or a 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 assign a different version manually	Can update to the latest version of the objects within a management template or an aspect Can assign a different version manually
Delete assigned policy	Policy is deleted, including assignments	Policy is deleted, including assignments	Must delete assignments before being permitted to delete policy

Change primary manager and target server of agents

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

However, to verify that all server-based correlation features of OBM are working as expected, including duplicate suppression and event storm suppression, we recommend that you change the target server for events to OBM gradually. For example, when you move the configuration of the corresponding nodes to OBM, you could also switch the target server to OBM. If you still would like to receive all events in OM as well, you can use an OBM forwarding rule that forwards all events received in OBM to OM. Instruction retrieval might also fail if the OM server does not have the policy that is deployed from OBM in its policy inventory.

With the before mentioned flexible management policy, you can switch the target server by switching the primary manager of a node, because the flexible management policy contains the following text as a message target rule:

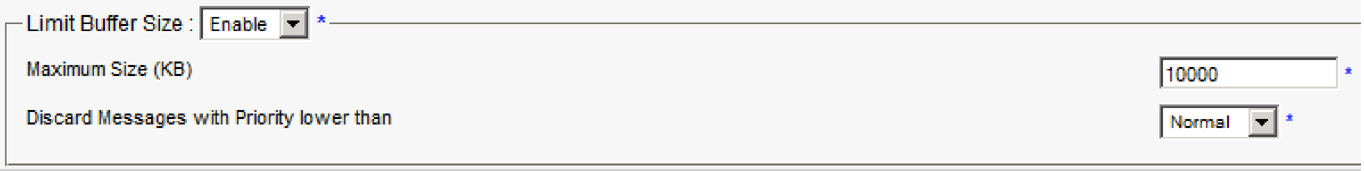
```
MSGTARGETMANAGER
             TIMETEMPLATE "$OPC_ALWAYS"
             OPCMGR IP 0.0.0.0 "$OPC_PRIMARY_MGR"
```

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

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

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

OM allows setting some agent configuration variables in the OM UI, such as agent buffering and DHCP settings.



Limit Buffer Size : Enable *

Maximum Size (KB) 10000 *

Discard Messages with Priority lower than Normal *

OBM does not allow changing agent configuration variables in the UI, however they can be changed by using `ovconfpar`.

To configure agent configuration variables from OBM, use the `opr-agt -set_config_var` option. For example:

```
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 now reports to the OBM server and increases the number of Operations Agents shown on the OBM server license report.

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

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

After a primary manager switch you can still manage and configure an agent from the OM server. Therefore, it is 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 must be reconfigured so that they use the OBM server as their server, even when the flexible management template is removed.

You can do this by using `opr-agt -switch_manager`. 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 by using a TQL, a node group, or a node list. For example, from OBM use:

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

or

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

Make sure that this TQL contains only the nodes the 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 are still 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 the OBM and OM servers, and then deploys all policies that are assigned to the node in OBM.

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

Summary and command overview

This section contains the most important steps and command-line calls used when moving Operations Agents and their configuration to OBM. They are the following:

1. Allow management from both servers by using a flexible management template.
2. Choose a group or a type of nodes to move over, for example, all Oracle Database systems. Follow these steps:
    1. Test policy and aspect deployment and tool execution from OBM 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`Additionally this might include creating OBM aspects and management templates.

   2. After a successful test, roll out configuration to the remaining nodes of that type manually or by using automatic assignment rules.
   3. Switch the primary manager and target server to OBM. This still allows configuration from both the OBM and OM servers:
      `opr-agt -primmgr <node selection> -username <user>`
3. Repeat Step 2 until all nodes are managed by OBM.
4. Before switching off the OM server, switch the agents to OBM completely:`opr-agt –switch_manager <node selection> -username <user>`
   If necessary, clean up old OM policies:
   `opr-agt –deploy -clean <node selection> -username <user>`

Related Topics

SPI to MP Evolution Tool

Micro Focus Software Community

Video Library

Additional considerations

This section contains the following topics:

Contents

Deployment of policy groups to node groups

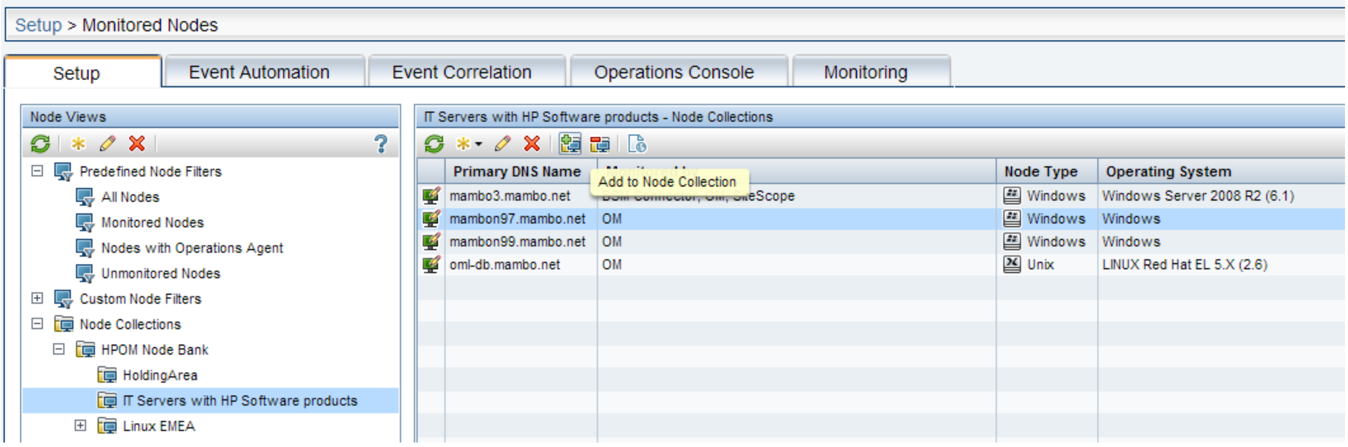
OM customers deploy policies or policy groups to node groups. In a node-centric model, this is an easy way to structure and control the deployment of policies. In OBM, this model is replaced by a CI-centric deployment to benefit from all CI-type related features (such as using CI attributes for setting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

If you do not use these features, you can continue with deploying policy groups (as aspects) to node groups that are represented as CI collections in OBM.

Deployment tasks

Consider the following tasks:

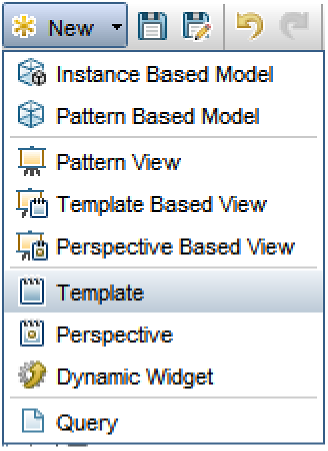
- How to create and maintain node groups or CI collectionsNode groups or layout groups that exist in OM are forwarded to OBM as part of the OM topology synchronization. These node groups are converted into CI Collection CIs.When you discontinue using OM, you must maintain node group hierarchy through 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) as well as add and remove nodes to or from these node collections.



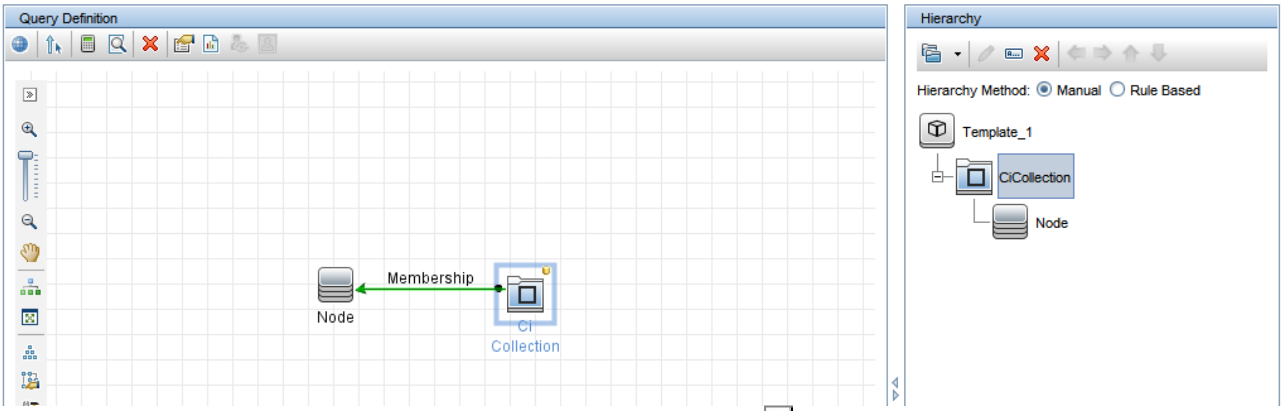
Primary DNS Name		Node Type	Operating System
mambo3.mambo.net	BSM Connector, OM, SiteScope	Windows	Windows Server 2008 R2 (6.1)
mambon97.mambo.net	OM	Windows	Windows
mambon99.mambo.net	OM	Windows	Windows
oml-db.mambo.net	OM	Unix	LINUX Red Hat EL 5.X (2.6)

You can also create relationships between CI collections and nodes by using the RTSM Admin UI or RTSM APIs, for which you require deeper knowledge of the RTSM. These relationships can be created also automatically by using enrichment rules. For more details, see the RTSM documentation.You can maintain node groups and node membership by using the `opr-node` command-line interface.

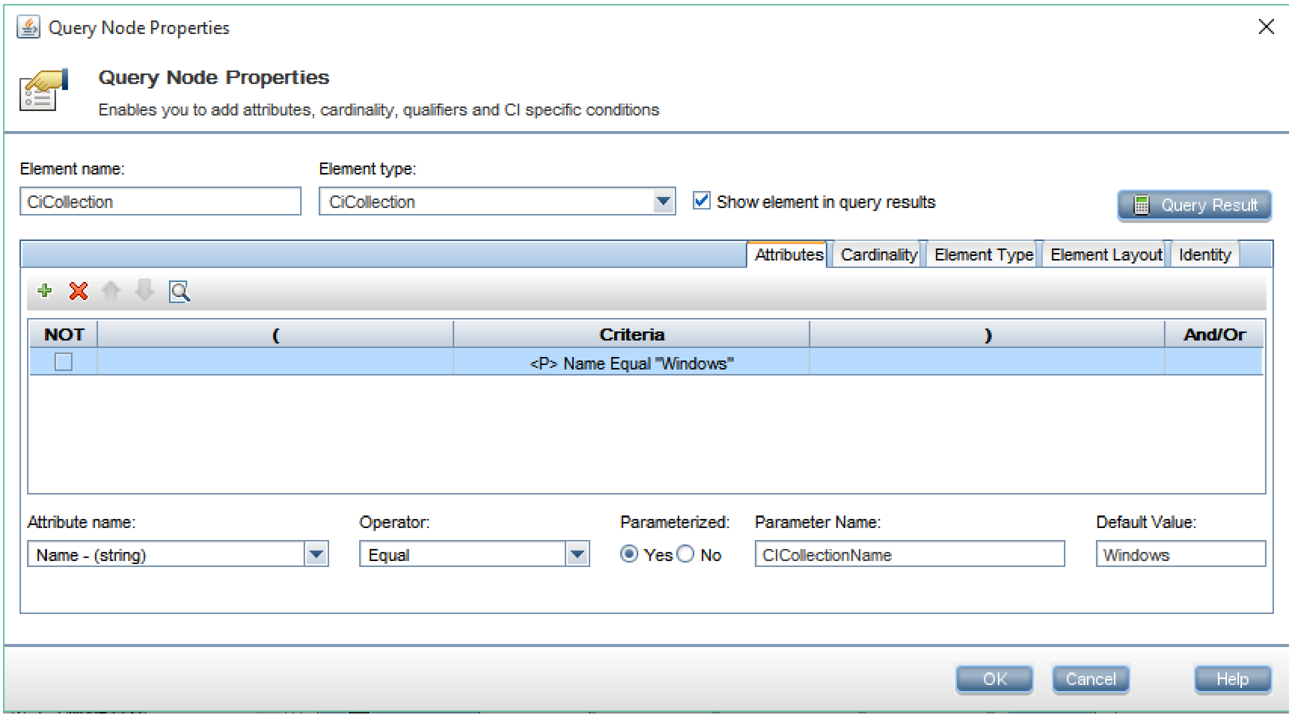
- How to create a view and aspect for policy group/node group-centric deploymentWhen you assign an aspect to a CI collection (node group), this aspect gets assigned to the CI collection CI only, but not to all node CIs that are part of the CI collection. However, to achieve such a behavior, you can use views and assignment rules.First, create a view for each node group or CI collection for which you want to assign aspects. If you need several views, you can create a template, as described below, from which you can then create all the views, as this is faster than creating each view separately.Second, create a policy group aspect. This is an aspect that acts as a policy group and contains all the policies that you want to deploy.Lastly, create an automatic assignment rule that assigns the aspect/policy group to the view/node group.
  1. In **Administration > RTSM Administration > Modeling > Modeling Studio**, create a template for CI collection/node group views.



  2. Add the following CI types:
     - CI collection
     - Node
  3. Add the membership relationship between the CiCollection and Node CI types, change the hierarchy method to Manual, and move the Node CI type below the CiCollection CI type.



4. Right-click the CiCollection CI type and click **Query node properties**.
5. Add an attribute with the following settings:
   - Attribute name: **Name - (string)**
   - Operator: **Equal**
   - Parameterized: **Yes**
   - Parameter Name: **CiCollectionName** (or similar)
6. Specify a default value so that you can test the template using the Preview option.Note If you have node groups with the same name, use the **CI Collection ID** instead as attribute name.



Query Node Properties

Query Node Properties

Enables you to add attributes, cardinality, qualifiers and CI specific conditions

Element name: CiCollection

Element type: CiCollection

☑ Show element in query results

NOT	(	Criteria	)	And/Or
□		<P> Name Equal "Windows"		

Attribute name: Name - (string)

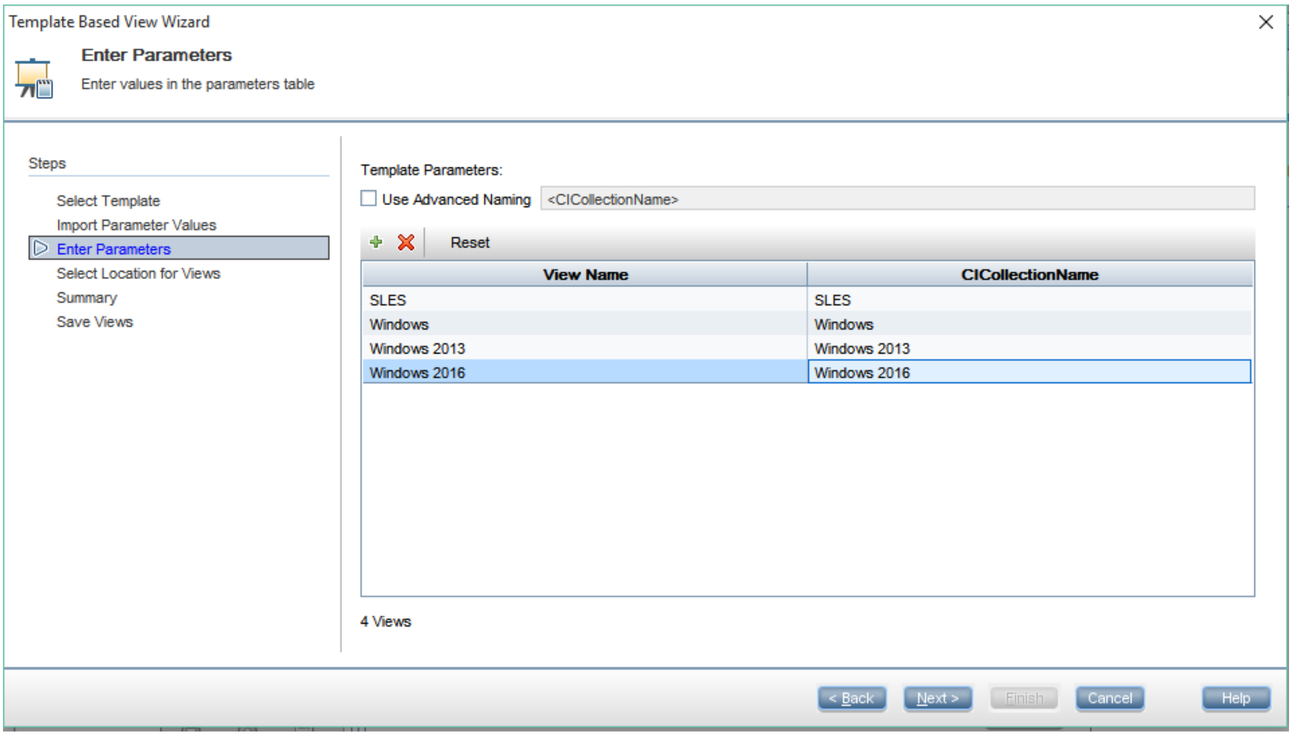
Operator: Equal

Parameterized: ● Yes ○ No

Parameter Name: CICollectionName

Default Value: Windows

7. Verify that the preview shows the correct nodes and save the template.
8. *Optional*. You can use this template to create views. Create a template based view and provide all the CI collection names for which an individual view should be created. The following configuration creates four views for four different CI collections:



Template Based View Wizard

Enter Parameters

Enter values in the parameters table

Template Parameters:

□ Use Advanced Naming <CICollectionName>

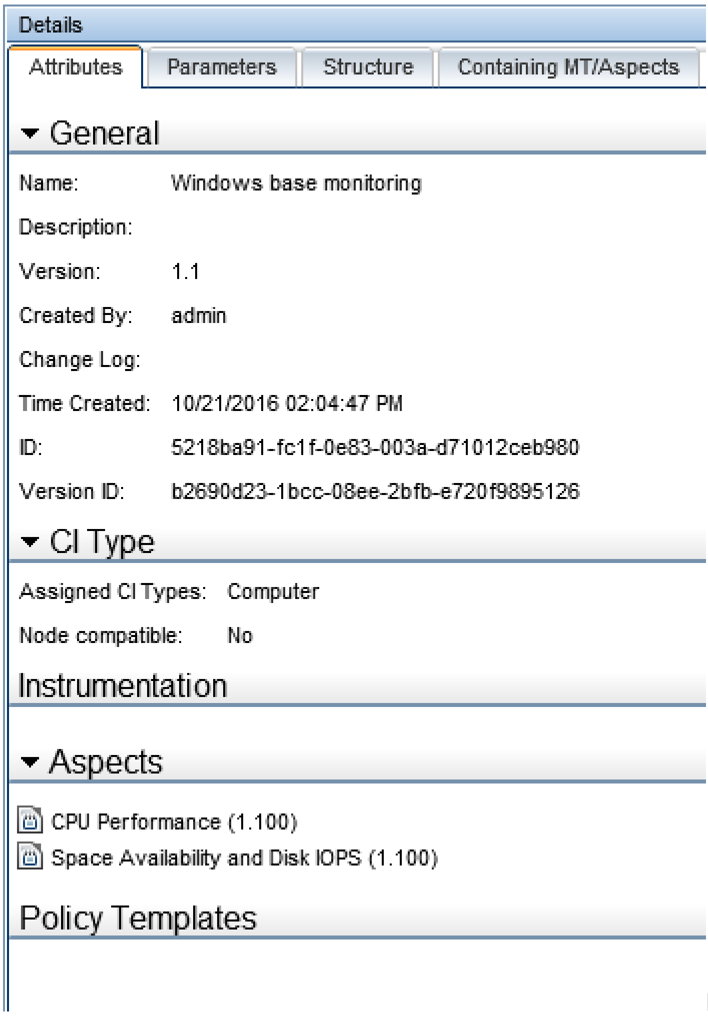
View Name	CICollectionName
SLES	SLES
Windows	Windows
Windows 2013	Windows 2013
Windows 2016	Windows 2016

4 Views

When creating multiple views this way, the view properties are not copied correctly from the template: the priority in the View Definition properties is incorrectly set to **Not Active**. Make sure that you manually set the priority to **Medium** (or Low/High) for each view.

A view with priority **Not Active** will not trigger any assignments when used in assignment rules.

9. Create aspects that represent your policy groups.For example, create an aspect called "Windows base monitoring" for the CI type Computer and add relevant aspects or policy templates to the aspect, for example CPU and disk



General

Name: Windows base monitoring

Description:

Version: 1.1

Created By: admin

Change Log:

Time Created: 10/21/2016 02:04:47 PM

ID: 5218ba91-fc1f-0e83-003a-d71012ceb980

Version ID: b2690d23-1bcc-08ee-2bfb-e720f9895126

CI Type

Assigned CI Types: Computer

Node compatible: No

Instrumentation

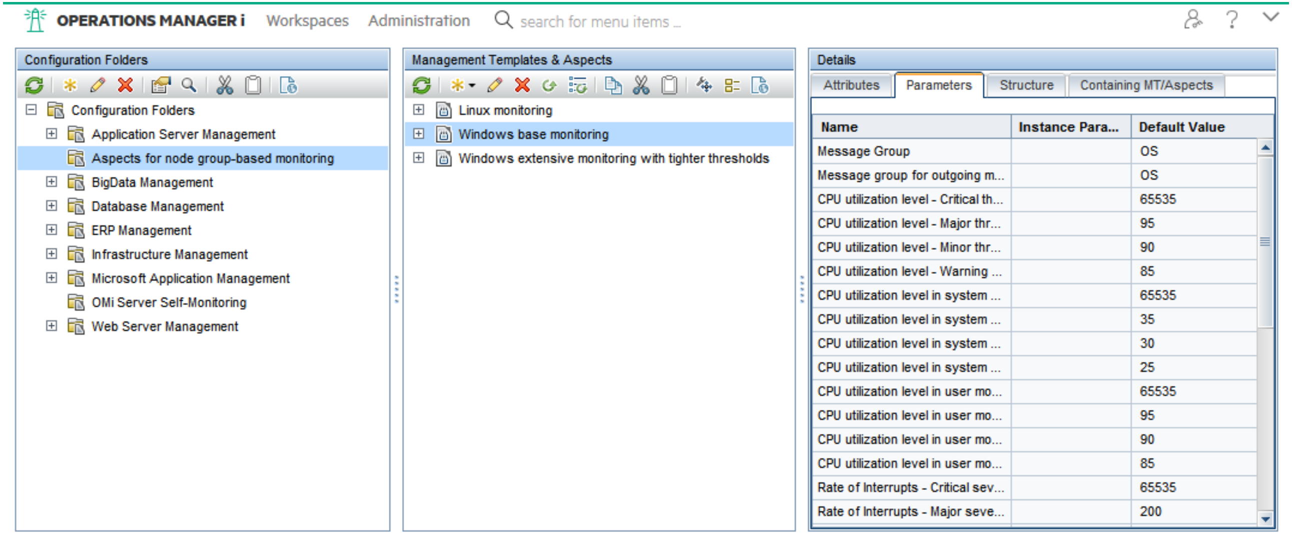
Aspects

CPU Performance (1.100)

Space Availability and Disk IOPS (1.100)

Policy Templates

monitoring. If you select the CI type Node for your new aspect, then you will not be able to add nested aspects defined for more specific CI types, like Computer.By overwriting the default parameters, you can create various aspects (policy groups) with various parameter sets for different needs. For example, "Windows base monitoring", "Windows extensive monitoring with tighter thresholds", "Linux process monitoring", and so on.



Configuration Folders
- Application Server Management
- Aspects for node group-based monitoring
- BigData Management
- Database Management
- ERP Management
- Infrastructure Management
- Microsoft Application Management
- OMi Server Self-Monitoring
- Web Server Management

Linux monitoring

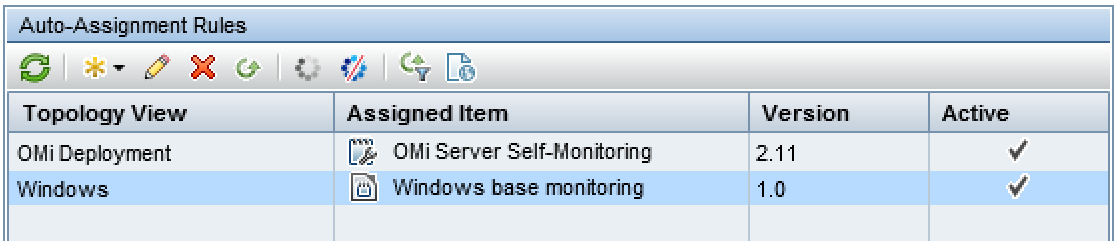
Windows base monitoring

Windows extensive monitoring with tighter thresholds

Name	Instance Para...	Default Value
Message Group		OS
Message group for outgoing m...		OS
CPU utilization level - Critical th...		65535
CPU utilization level - Major thr...		95
CPU utilization level - Minor thr...		90
CPU utilization level - Warning ...		85
CPU utilization level in system ...		65535
CPU utilization level in system ...		35
CPU utilization level in system ...		30
CPU utilization level in system ...		25
CPU utilization level in user mo...		65535
CPU utilization level in user mo...		95
CPU utilization level in user mo...		90
CPU utilization level in user mo...		85
Rate of Interrupts - Critical sev...		65535
Rate of Interrupts - Major seve...		200

10. *Recommended*. Deploy aspects (policy groups) using automatic assignment rules.Create an automatic assignment rule and specify the CI collection view, for example the "Windows" view and the corresponding aspect, for example "Windows base monitoring". This will deploy all policies that are part of the "Windows base monitoring"

aspect (policy group) to all nodes that are part of the "Windows" CI collection (node group).

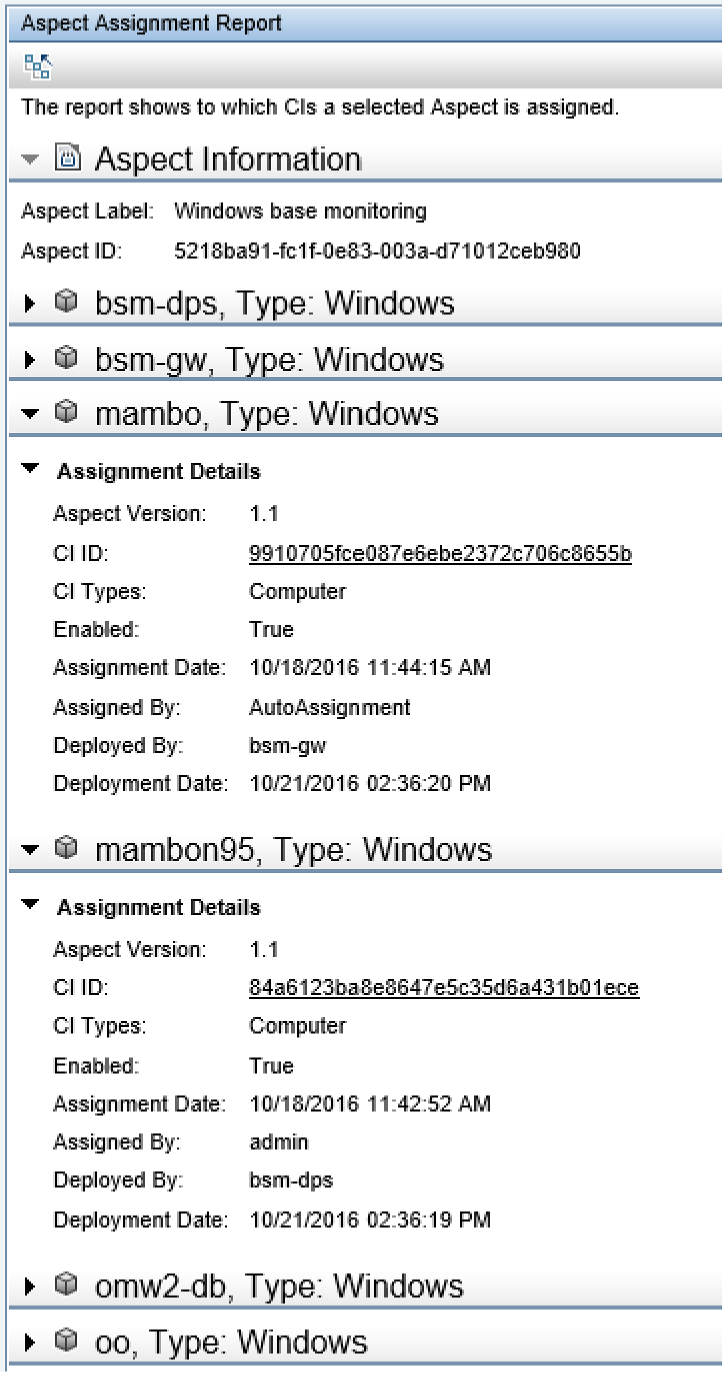


Topology View	Assigned Item	Version	Active
OMi Deployment	OMi Server Self-Monitoring	2.11	✓
Windows	Windows base monitoring	1.0	✓

Manual deploymentPolicy group aspects that are defined for the Node or Computer CI type cannot be deployed manually to the CI Collections CIs, but you can deploy these aspects to the nodes of a CI collection. In **Administration > Monitoring > Management Templates & Aspects**, select the aspect (policy group) that you want to deploy and click **Assign and Deploy Item** in the context menu.

Select the nodes that belong to the CI collection. This method has the disadvantage that you cannot see or select the node group to which a node belongs. Due to this, it is only suitable for assignments to a single or a small number of nodes. Also note that this is a one-time assignment to nodes. If a node is added or removed from the CI collection, this does not change any assignments.**Assignment reports**

The **Aspect Assignment** report and the **CI Configuration Report for All CIs in View** show the aspect (policy group) assignment.



Aspect Assignment Report

The report shows to which CIs a selected Aspect is assigned.

Aspect Information

Aspect Label: Windows base monitoring

Aspect ID: 5218ba91-fc1f-0e83-003a-d71012ceb980

bsm-dps, Type: Windows

bsm-gw, Type: Windows

mambo, Type: Windows

Assignment Details

Aspect Version:	1.1
CI ID:	9910705fce087e6ebe2372c706c8655b
CI Types:	Computer
Enabled:	True
Assignment Date:	10/18/2016 11:44:15 AM
Assigned By:	AutoAssignment
Deployed By:	bsm-gw
Deployment Date:	10/21/2016 02:36:20 PM

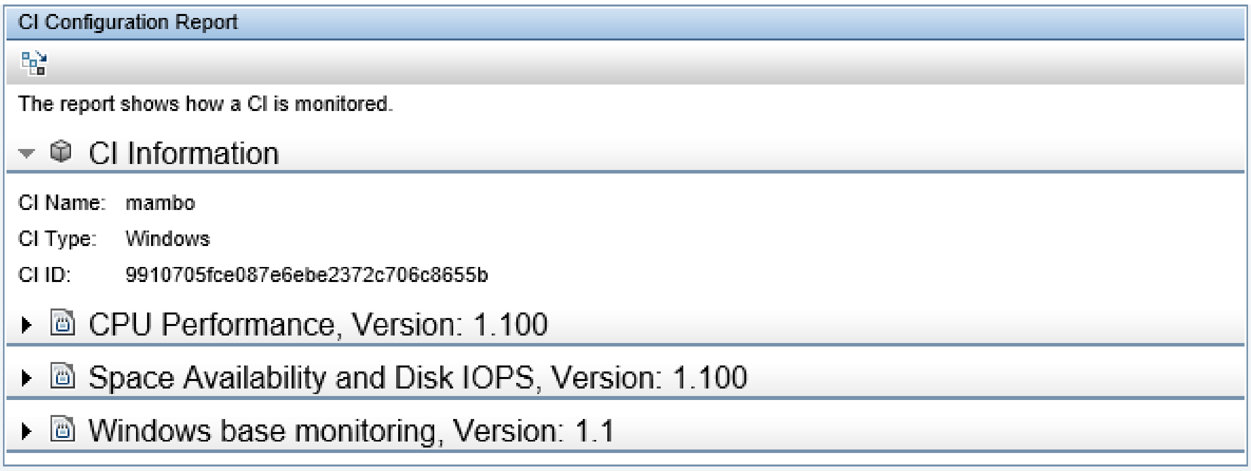
mambon95, Type: Windows

Assignment Details

Aspect Version:	1.1
CI ID:	84a6123ba8e8647e5c35d6a431b01ece
CI Types:	Computer
Enabled:	True
Assignment Date:	10/18/2016 11:42:52 AM
Assigned By:	admin
Deployed By:	bsm-dps
Deployment Date:	10/21/2016 02:36:19 PM

omw2-db, Type: Windows

oo, Type: Windows



CI Configuration Report

The report shows how a CI is monitored.

CI Information

CI Name: mambo

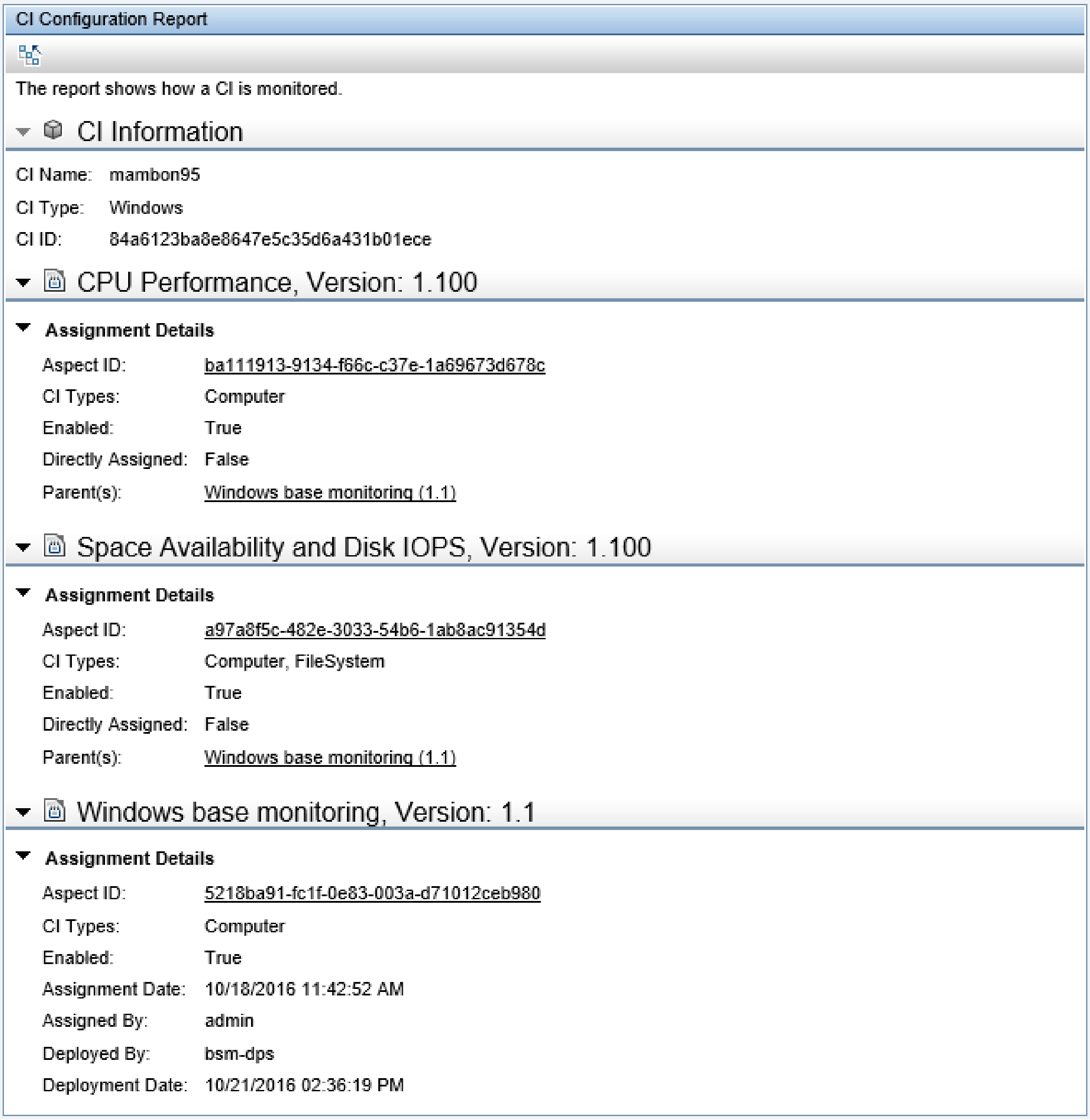
CI Type: Windows

CI ID: 9910705fce087e6ebe2372c706c8655b

CPU Performance, Version: 1.100

Space Availability and Disk IOPS, Version: 1.100

Windows base monitoring, Version: 1.1



CI Configuration Report

The report shows how a CI is monitored.

CI Information

CI Name: mambon95

CI Type: Windows

CI ID: 84a6123ba8e8647e5c35d6a431b01ece

CPU Performance, Version: 1.100

Assignment Details

Aspect ID: ba111913-9134-f66c-c37e-1a69673d678c

CI Types: Computer

Enabled: True

Directly Assigned: False

Parent(s): Windows base monitoring (1.1)

Space Availability and Disk IOPS, Version: 1.100

Assignment Details

Aspect ID: a97a8f5c-482e-3033-54b6-1ab8ac91354d

CI Types: Computer, FileSystem

Enabled: True

Directly Assigned: False

Parent(s): Windows base monitoring (1.1)

Windows base monitoring, Version: 1.1

Assignment Details

Aspect ID: 5218ba91-fc1f-0e83-003a-d71012ceb980

CI Types: Computer

Enabled: True

Assignment Date: 10/18/2016 11:42:52 AM

Assigned By: admin

Deployed By: bsm-dps

Deployment Date: 10/21/2016 02:36:19 PM

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 by using the `opr-jobs` tool to start the deployment jobs. For details about the `opr-jobs` command-line interface and deployment jobs, see the *Administer* section.

OBM policy limitations and workarounds

The following are OBM limitations in comparison to OM for Windows:

- WMI policy editor: No WMI browser available.*Workaround*: Use WMI browsing tools available from Microsoft.
- 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 stated in the previous list item 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 OBM Performance Perspective.
- Measurement Threshold policy does not support the “Show only newest message in message browser” feature.*Workaround*: Set MsgKey and MsgKeyRelation manually by using the following pattern:MsgKey: <$NAME>:<$MSG_NODE_NAME>:<$MSG_OBJECT>:START<$THRESHOLD>
  MsgKeyRelation: <$NAME>:<$MSG_NODE_NAME>:<$MSG_OBJECT>:<*>

The following OBM limitation exist in comparison to OM for UNIX and Linux:

- In the RAW Mode Policy Editor, the following options are not available: search, edit, replace, and undo. *Workaround*: Copy a complete policy to the external editor that supports these operations.

The following are OBM limitations in comparison 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 OBM. Currently, OBM does not support using range patterns (`-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. OM allows policies with the same name if the policy type is different. However, OBM does not allow policy templates with the same name. Therefore uploading a policy will fail if a policy with the same name already exists. In such cases, first rename the policy in OM and export it again.

Limitations and workarounds for event-related actions

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

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

- Actions using `$GRAPH`
- Actions launched on `$OPC_GUI_CLIENT`
- Actions launched on `$OPC_GUI_CLIENT_WEB`

The actions that use these variables are filtered out by OBM and they are not displayed. It is also not possible to define these actions in OBM policy template editors.

These are the OBM workarounds for the following actions:

- $OPC_MGMTSV Instead of using the Operations Agent to execute an action on the management server, you use an EPI script when an event arrives. EPI groovy scripts are executed on the OBM gateway server that receives the event. EPI scripts have full access to all event properties and can be used for different purposes. Consider this option for actions relevant for many events (for example, to log or enrich events, and so on). If you want to continue with using `$OPC_MGMTSV` as target for an event-related action, consider that the command will be executed on one of the OBM Gateway servers and not on the OMi Data processing server.
- $GRAPH Actions using $GRAPH launch predefined performance graphs and can also preset the displayed time range so that the time when the problem occurred is shown. In OBM, graphs can be launched by using the event context menu (show Performance Graphs (CI)) which automatically shows all default graphs for the selected CI. From this menu, you can easily select additional graphs and use the Date Range Panel to navigate to the time when the problem occurred.
- $OPC_GUI_CLIENT_WEB Instead of specifying the URL in the action, you can specify it in the instructions of the event.
- $OPC_GUI_CLIENT The OBM 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–support facts

OBM supports the following OM template types:

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

OBM does not support the following:

- OM for UNIX v.8x templates
- Importing SiteScope policy that is exported from OM 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 these flags arrives in OBM, the flags are automatically converted into custom attributes **ForwardToTroubleTicket = true** and **NotifyUser = true**.

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

Deployment of custom instrumentation (OM for UNIX and Linux)

OM for UNIX and Linux v.9x introduces instrumentation categories and enables to group instrumentation files into such categories. When a policy is imported into OBM, 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 require the instrumentation. To save time, you can add the instrumentation category on the aspect level.

If you deploy individual policies for testing purposes, this does not trigger instrumentation deployment.

Editing already uploaded instrumentation files

During the policy export and import, all assigned instrumentation categories are exported and imported on the OBM 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 OBM side, either during the migration because the instrumentation files changed on the OM side in the meantime, or after the migration, download the current instrumentation (including all patches and hotfixes) available in OBM.

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
```

Perform the following steps:

1. Make the necessary changes to the instrumentation files in the downloaded directory `/tmp/Database`.
2. Upload the instrumentation files by using the `-force` option:
   /opt/HP/BSM/opr/bin/ConfigExchange.sh -user <username> -password <password> -upload -input /tmp/Database -instrumname Database -force

Related Topics

Node management

WMI Browsing Tools

Configure SiteScope from OBM

You can configure SiteScope templates to be imported into OBM. For details, see the following sections:

- Configuration details
- Configure SiteScope

Configuration details

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). OBM 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 these monitors, but add variables named Remote Host and Monitoring Interval, for the settings that you want to modify each time you deploy the template.

The SiteScope templates can now be imported into OBM, be grouped into aspects, included in management templates and assigned manually or automatically by OBM. 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 OBM offer the additional benefit that involves using CI attributes to set SiteScope Template parameters. You can also predefine particular 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, therefore 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 OBM: functionality comparison

Functionality	OM for UNIX	OBM
Deploy monitors, groups, and remote servers	Yes	Yes
Automated deployment	Can be scripted by using OM for UNIX CLIs	Yes
Automated lifecycle monitoring	Can be scripted by using OM for UNIX CLIs	Yes If the CI is no longer part of the view (for example, the monitored business application), then monitoring is automatically removed
Deployment workflow	Assign and deploy SiteScope policy	Assign and deploy configuration starting from a CI or a policy template, an aspect, or a management template
Undeployment workflow	Unassign and undeploy the SiteScope policy	Can delete an assignment that removes the monitors
Deployment flexibility across multiple SiteScope servers	Deploy SiteScope policy to a selected SiteScope server Can also assign policy to a virtual node (target system) where SiteScope is the physical node	Default behavior is to deploy monitors to the SiteScope server with most free points Alternatively, you can configure OBM to decide according to other criteria (such as the IP address or domain name of the monitored target by using Groovy script)

Agent-based and agentless monitoring configuration	Yes	Yes
SiteScope template handling	Create or modify templates in SiteScope Import templates to OM for UNIX manually	Create or modify templates in SiteScope Import templates to OBM manually
Parameterization	Edit the policy to set or change parameters Supports special variables: `HOST`, `NODEGROUP`, and `FILE`	Prepopulate parameters with CI attribute values or enter values manually
Template versioning	OM for UNIX stores multiple template versions, allowing one chosen version to be deployed at a time	OBM stores multiple template versions, allowing one chosen version to be deployed at a time
Assignment management	Assign SiteScope policies or policy groups to the SiteScope node	SiteScope templates: the lowest granularity of monitoring elements that 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) Possible to combine parameters that are the same across templates so that you are prompted for each value only once
CI-centric deployment	Node-centric	Yes
CIs must be in the RTSM before use	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	Yes
Leverage RTSM node credentials	N/A Can create templates that use SiteScope Credential Preferences	No Can create templates that use SiteScope Credential Preferences
Validate points required and available before deployment	No	No
Control SiteScope monitor group structure	Parent monitor group is hard-coded to “`Deployed from Operations Manager`” with subgroup named `OVO:omserver.fqdn`	Parent monitor group is hard-coded to “Deployed from Operations Manager” with subgroup named `gwserver.fqdn`
Deployment status	OM for UNIX generates a message upon success and upon failure to deploy policies Review `<OvDataDir>/log/system.0.en_US` on SiteScope server to check details on the SiteScope side	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 check details on the SiteScope side
Assignment report	The OM for UNIX server shows the SiteScope policies assigned to the SiteScope server	From **Administration > Setup and Maintenance > Connected Servers**, select a SiteScope server and click **Launch report** to generate a report of the CIs monitored by SiteScope through OBM, along with the list of templates for each CI

Additional considerations

Consider also the following configuration details:

- Moving SiteScope monitor deployment from OM for UNIX to OBM If you currently use OM for UNIX to deploy SiteScope monitors, there are two possible approaches for moving the configuration to OBM:
  - Importing SiteScope templates directly from SiteScope to OBM by using the `ConfigExchangeSIS[.bat|.sh]` command.
  - Importing OM for UNIX SiteScope policies to OBM by using the `ConfigExchange[.bat|.sh]` command.

  We recommend that you perform an import directly from SiteScope. This is because OM for UNIX supports special variable values that are not used in OBM. Because you cannot edit the policy within OBM, you cannot make use of the imported policies. OM for UNIX allows the use of `%%HOST%%`, `%%NODEGROUP:<nodegroup_name>%%`, `%%FILE:<file>%%` and `%%FILE:<file>.$SISHOST%%`.
- Configuring multiple SiteScope servers OBM can configure multiple SiteScope servers. Prepare all SiteScope servers as described below. By default, OBM instantiates monitors on the SiteScope server that has the most available license points. You can also choose a SiteScope server by using other attributes, such as the host name or IP addresses of the monitor target. For details on how to create a connection to a SiteScope server, see the *Administer* section. Example proxy deployment scripts are available at `<OMi_HOME>/opr/examples/deployment-server-selection`.

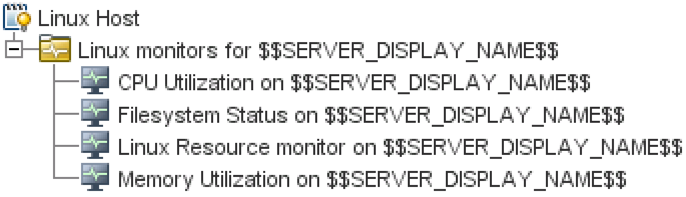
Configure SiteScope

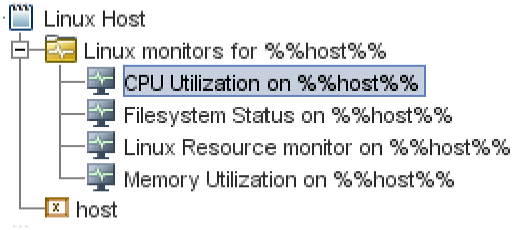
The following are steps that must be performed to configure SiteScope from OBM:

1. Prepare SiteScope To be able to configure 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.

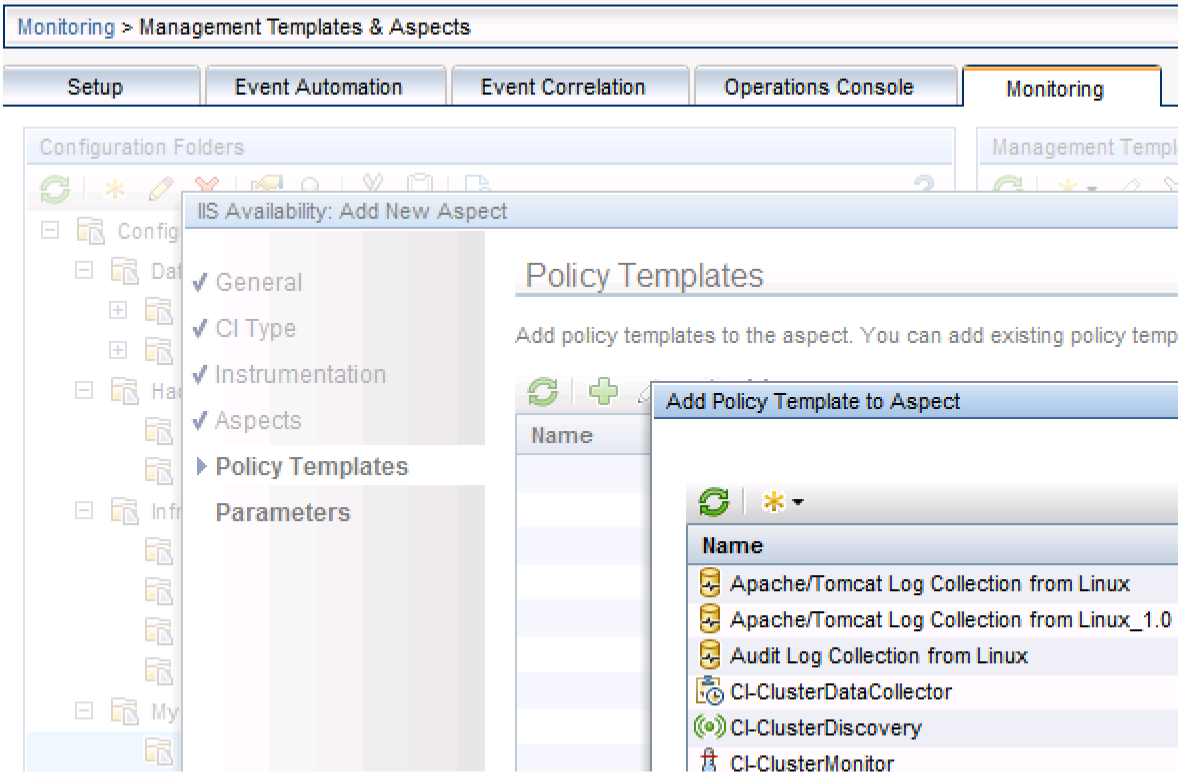
   For details about importing SiteScope templates, see Administer.
2. Adjust templates in SiteScope SiteScope templates contain information about the remote servers or applications that they monitor. This information is usually stored in a variable that is replaced by the list of remote servers or application 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 to create a corresponding instance parameter in the resulting policy template. The import tool chooses one the following SiteScope variables, in the order presented 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. If the variable "host" exists in a SiteScope template but does not have a value, the value is 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 you use the wrong variable as an 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. System variables starting with `$$` (such as `$$SERVER_DISPLAY_NAME$$`) are not converted and must 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 $$SERVER_DISPLAY_NAME$$

   
   Linux Host
   Linux monitors for %%host%%
   CPU Utilization on %%host%%
   Filesystem Status on %%host%%
   Linux Resource monitor on %%host%%
   Memory Utilization on %%host%%
   host

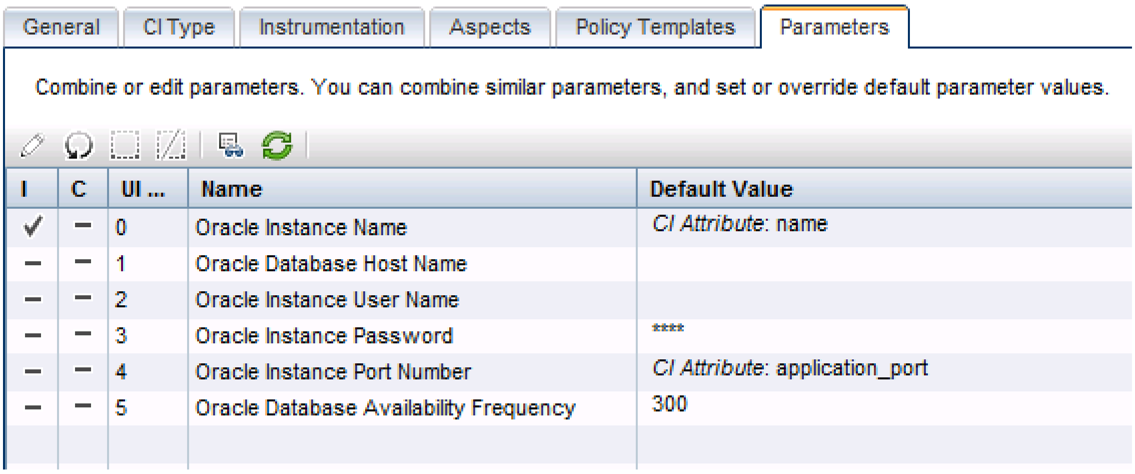
   To simplify the import, copy all the templates that must be imported into one template group.
3. Import SiteScope templates into OBM On the OBM server, open a command prompt and run the `ConfigExchangeSIS` command-line interface to import templates from a SiteScope server. For example, the following command loads the templates that are in the template container named "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 details about the `ConfigExchangeSIS` command-line interface, see the *Administer* section.
4. Group policy templates into aspects After templates are imported, they must be grouped into meaningful aspects. An aspect is defined for a specific CI Type and contains all policies required to monitor a particular aspect of the CI, for example, its performance or availability. Follow these steps:
   1. Go to **Administration > Monitoring > Management Templates & Aspects**.
   2. Create a suitable configuration folder and add aspects in it. When creating an aspect, enter its name, specify the CI Type, and then select the corresponding policy templates.



Add policy templates to the aspect. You can add existing policy temp

Name
Apache/Tomcat Log Collection from Linux
Apache/Tomcat Log Collection from Linux_1.0
Audit Log Collection from Linux
CI-ClusterDataCollector
CI-ClusterDiscovery
CI-ClusterMonitor

5. Set parameter values by using CI attributes In this step, make sure that the instance parameter value is either `%%HOST%%` (which is automatically replaced by the corresponding host node name) or that the value is set by using a CI attribute that represents the instance. For example, if the SiteScope template is targeted to monitor Oracle instances, the instance parameter is the `Oracle Instance Name`. The corresponding Oracle aspect is defined for the Oracle CI Type and a single Oracle CI represents 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:



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 must make sure that these attributes are filled by your discovery process.

6. Create management templates to group aspects Creating management templates is optional but recommended. Management templates simplify the assignment of many aspects and therefore enable monitoring 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 that represent, for example, Essential and Extensive monitoring levels. Follow these steps:
   1. Go to **Administration > Monitoring > Management Templates & Aspects**.
   2. Create a configuration folder and add management templates in it.

   3. Enter the management template name, specify a view and root CI Type, and then select the corresponding aspects.
   4. If you use the management template for grouping aspects that belong 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 by using one single assignment, you must create a management template. Because this cannot be done by using nested aspects, you must create or select the view that shows all CI Types and their relations as a starting point for the management template. For details, see Administer.

7. Test configuration When you create 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 or management template as a starting point) or **Administration > Monitoring > Assignments & Tuning** (with the CI as a starting point). The assignment by default initiates an immediate deployment of all included policy templates to the corresponding nodes. You can verify on the SiteScope Server whether the corresponding monitors are deployed.
8. Roll out the configuration When the configuration is validated, you can roll out the configuration to more systems, either manually (if there is only limited change in the environment) or automatically by using web services or automatic assignment rules.

Establish reporting by using OBR

See the following sections for information on how to establish reporting by using OBR:

- Reporting with OBR
- Establish reporting by using OBR
- Additional tasks

Reporting with OBR

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. To do this, OBR leverages service topology definitions from the OBM RTSM.

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

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.

Reporter and OBR reports comparison

Check the Operations Bridge Reporter Content Catalog available on the ITOM Marketplace 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) rowspan='2'|

System

System

Yes

Virtualization

Yes rowspan='7'|

OM SPIs

Oracle, MSSQL

Yes

Sybase, Informix

Content in BO Universe*

OBR has standard content for Sybase ASE released on ITOM Marketplace

WLS, WBS

Yes

SAP

Yes

OBR has standard content for SAP and SAP HANA released on ITOM Marketplace

Exchange/AD

Yes

Lync, SP, BizTalk

No

Tibco

No

Event

OM

Yes rowspan='2'|

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 OBM events, His, and KPIs. OBR has standard content for Hadoop and Vertica in addition to other Community content offerings.

Reporter and OBR feature comparison

The following table shows the comparison of Reporter and OBR features:

Reporter Functionality	Equivalent in OBR
Report scheduling	Yes
Data summarization	Yes
Report customization through Crystal Designer	Yes, by using Business Objects Web Intelligence (OBR does not ship Crystal Reports)
Custom Groups	CMDB Views, Node Groups, user-defined
Time Shift support	Yes
Scalability, 2000 nodes per instance	Supports scale out with Vertica (for more details, see the *OBR Help*)
Support external DB (Oracle, MSSQL)	No, OBR embeds Vertica
PA collector	Yes
Data Access Layer (DAL) – SQL	DAL – SQL, BO SDK, and Database views
Custom extension	CDE and Content Designer Studio(UI for building content)
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 You can also set up an OBM 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, which means more metrics from group of critical servers and fewer metrics from less-critical servers)	All collections are at five-minute granularity with hourly frequency Nodes collection can be enabled or disabled
Agent metrics collected at one-hour granularity with daily frequency	Agent metrics collected at five-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 adding systems manually, or by OM discovery	Topology source is either OM or the RTSM (Special standalone cases exist for VMware-only and for NPS-only scenarios, as well as for NNMi(direct), SOM, SA, and NA)
Log-in security: by default, none Can implement your own web server security	Uses Business Objects log-in security and authorization mechanism

Related Topics

Operations Bridge Reporter Content Catalog

OBR Community Content Offerings

Establish reporting by using OBR

To establish reporting by using OBR, follow these steps:

1. Install OBR You can install OBR in multiple deployment modes based on the target environment. To determine the deployment architecture suitable for your environment, see the *Install* section of the OBR Help.
2. 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.
3. Configure collections OBR supports the notion of Remote Collectors. These collectors enable collection of performance metrics from Operations Agents and other sources from behind a firewall (providing a secure and distributed collection). For more details, see the *Install* and *Administer* sections of the OBR Help.
4. Redefine custom shifts OBR allows users to create time shifts. These shifts are used to summarize and create shift-specific reports. Shifts are defined through the OBR Administration GUI. For details, see the OMi Help.
5. Redefine 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 part with RTSM views or node groups. For details, see the OMi Help.
6. Use ootb reports OBR ships more than 120 out-of-box reports. For details, see the *HPE Operations Bridge Reporter Handbook of Reports*.

Related Topics

OBR Content Packs

Additional tasks

The following are the additional tasks to be performed when establishing reporting by using OBR:

- Recreate custom reports by using BO OBR bundles Business Objects 4.1 (BO) for all its BI requirements. BO provides a browser-based editor to create and edit reports. The data that is collected, cleansed and aggregated by OBR is stored in Vertica Column DB and is exposed through 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, visit the OBR Documentation Library.
- 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. For details, see the *OBR Help*. More information on System Management content is available on OBR Community at Marketplace.
- Use reporter as gatherer To simplify the move to OBR, you can continue to use Reporter as data gatherer for some time. OBR can retrieve data from Reporter and combine it with the data from OBM. The OBR generic Database Collector is used to connect to the 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. To switch off Reporter, move the agent data collection to the OBR collection framework. As a prerequisite you must have all agents managed by OBM and discovered and modeled in the OBMRTSM instance. When 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 RTSM have a new CIID, which is now used for their identification. To link the older agent-based IDs in OBR to the new RTSM CIIDs, you can use Data Warehouse Lifecycle tools. For more details, see the migration toolkit.
- Switch the topology source from OM to OBM If you are already using OBR with OM as a topology source, you must switch to OBM as a topology source. OBR uses agent-based IDs in the OM deployment. These IDs are distinct from OBM RTSM-based CIIDs. To successfully migrate OBR from the OM deployment to the OBM deployment, you must map older agent-based IDs to their corresponding OBM-based CIIDs. For more details, see the video under Related Topics.

Related Topics

OBR Documentation Library

OBR Community at Marketplace

Video: SHR Migration Tool (OM to BSM deployment scenario)

Switch off Reporter

This section explains how to switch off OM and Reporter:

Switch off OM

To switch off OM, do the following:

1. If not already done, switch all Operations Agents to OBM.
2. 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 OBM by using the `opr-agt -deploy -clean` option. This deletes all old OM policies.
3. You can shut down OM completely. If you want to keep OM running but disconnected from your OBM environment, execute the following steps:
   1. On the OM server, undeploy the server-based forwarding policy (created when you connected OM to OBM).
   2. Remove the OBM server from the topology server configuration.
      - OM for Windows:
        1. In the console tree, right-click **Operations Manager**, and then click **Configure > Server**. The Server Configuration dialog box opens.
        2. Click **Namespaces**, and then click **Discovery Server**. A list of values appears.
        3. Remove the hostname of the OBM 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.
4. Switch agent licenses to OBM. To reuse the OS instance licenses that are previously used for OM, you can import the same license keys in OBM. 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 must be migrated into new licenses. Contact your HPE account team or partner to request the license migration.
5. In OBM, go to **Administration > Setup and Maintenance > Connected Servers** and disable or delete the connected server for your OM system. Shortly after the switch off, you might still have active events in the OBMEvent Browser that have the original OM server as the originating server. When changing events, OBM still tries to synchronize changes to the originating server and the synchronization details are shown on the Forwarding tab of Event Details. Synchronization problems can be safely ignored. After a few hours, OBM stops synchronization attempts automatically. As soon as the OBM connected server is disabled or deleted, OBM no longer routes tool executions through the OM server, but executes the tool by contacting the agent directly.
6. To make sure that agent certificates that use the old OM certificate authority (which is still trusted by OBM) 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 by using `ovcm -exportcacert`) are destroyed.

Switch off Reporter

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

- Collecting the required metrics from the Operations Agents and all OM servers that are not being decommissioned
- Producing the required reports
- Email integration is configured, if required

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

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

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

- Node and node group list automatically populated from the Reporter database.
- Data source for generating graphs from the Operations Agent metrics in the Reporter database.

After the Reporter integration is removed from PM, all nodes and node groups provided by Reporter are automatically removed from PM. Node and node group management is done by using the PM CLI or GUI. For details, see the *Performance Manager Help*.

Verify that PM users are not using any graph that sources data from Reporter.

To remove the 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 Reporter instance that is decommissioned.
3. Restart Performance Manager for the change to take effect (by using `ovpm stop` and `ovpm start`).

Related Topics

Summary and command overview

Add value on top

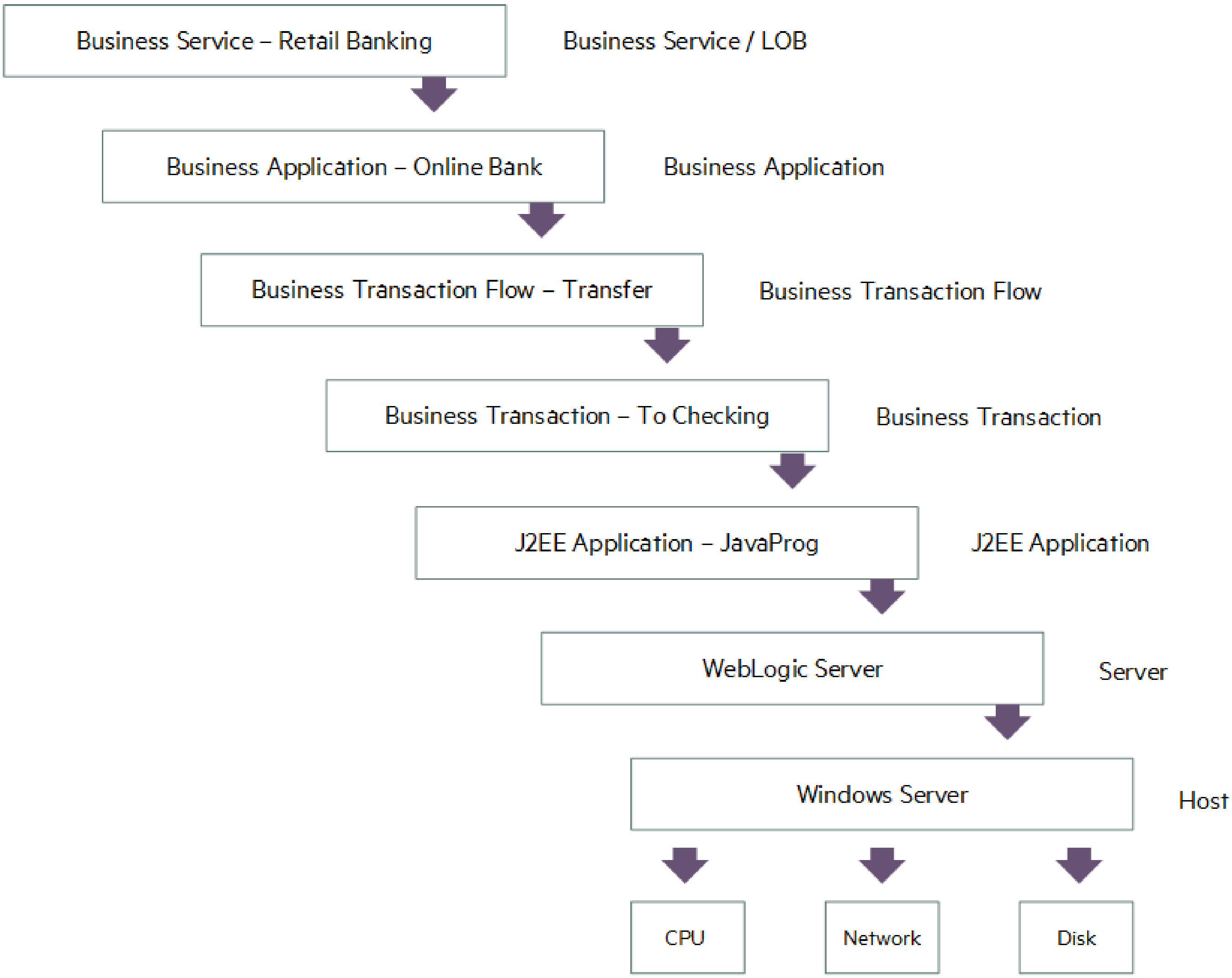
See the following sections for information on how you can add value on top of the OBM evolution:

- Model business services
- Add custom TBEC rules
- Add event type indicators
- Adjust Service Health

Model Business Services

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

The following figure shows a logical business service structure and monitored service contributors:


Business Service – Retail Banking
Business Service / LOB
Business Application – Online Bank
Business Application
Business Transaction Flow – Transfer
Business Transaction Flow
Business Transaction – To Checking
Business Transaction
J2EE Application – JavaProg
J2EE Application
WebLogic Server
Server
Windows Server
Host
CPU
Network
Disk

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.

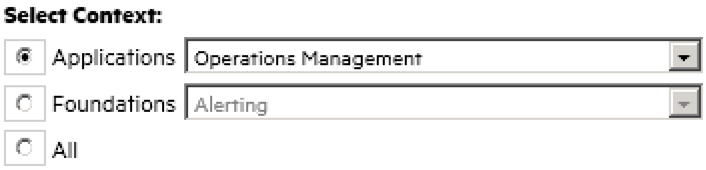
To support service-centric management, the RTSM must be extended by defining a model of business services and applications. Such a model must contain a relationship to all relevant CI instances that contribute to the business service.

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 requires considering the views on the business service model according to the specific user needs.

For more information on this topic, see the following:

- *Administer* > *RTSM* > *RTSM Modeling*. In this section, you can find the information about building a business view and a business CI model.
- *End-to-End Service Monitoring and Event Management Best Practices*. 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 OBM*. This technical white paper contains an example Business Service Model and shows how to create corresponding CIs and views in OBM.

When business services are defined and linked to infrastructure services, you can change the following Infrastructure Setting to enable business service or business application CIs to show up as part of events:

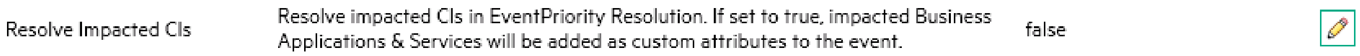


Select Context:

● Applications Operations Management

○ Foundations Alerting

○ All



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

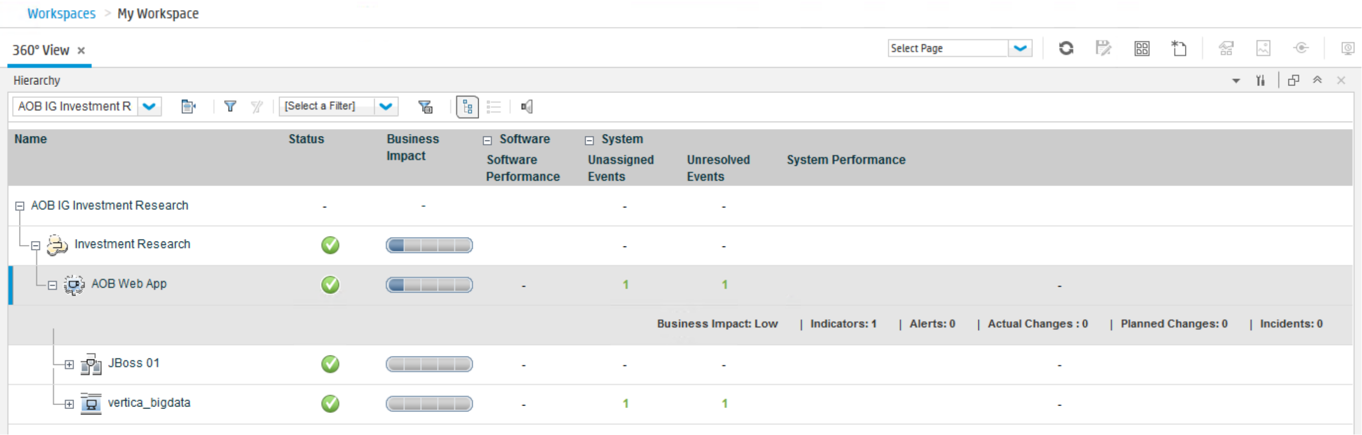
Event priority

When events and their related CIs impact business services, OBM instantly calculates an additional event attribute allowing the classification of the events depending on their impact on a business service. The event attribute, Event Priority, can be used to identify the events that require attention.

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

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

The following figure shows an example business impact of a CI (low):

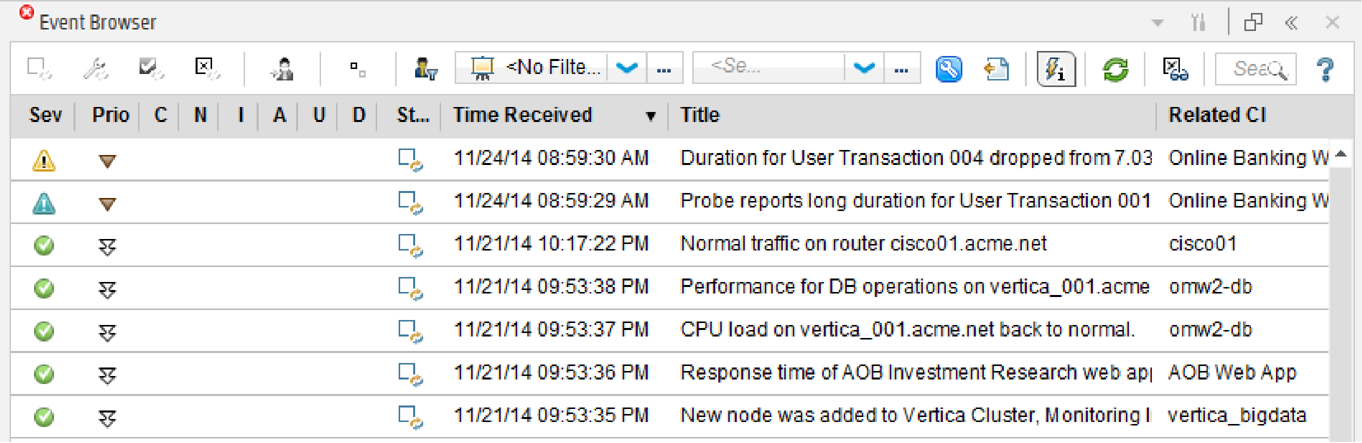


Name	Status	Business Impact	Software Software Performance	System Unassigned Events	Unresolved Events	System Performance
AOB IG Investment Research	-	-		-	-	
Investment Research	✓	▭		-	-	
AOB Web App	✓	▭	-	1	1	-
JBoss 01	✓	▭	-	-	-	-
vertica_bigdata	✓	▭	-	1	1	-

Business Impact: Low | Indicators: 1 | Alerts: 0 | Actual Changes : 0 | Planned Changes: 0 | Incidents: 0

To display the Business Impact information in Service Health 360° View, the business impact bar must be enabled in the Service Health infrastructure settings. For more information, see the *Administer* section.

The following figure shows an example of the resulting event priority in Event Browser:



Sev	Prio	C	N	I	A	U	D	St...	Time Received	Title	Related CI
⚠	▼								11/24/14 08:59:30 AM	Duration for User Transaction 004 dropped from 7.03	Online Banking W
⚠	▼								11/24/14 08:59:29 AM	Probe reports long duration for User Transaction 001	Online Banking W
✓	⇊								11/21/14 10:17:22 PM	Normal traffic on router cisco01.acme.net	cisco01
✓	⇊								11/21/14 09:53:38 PM	Performance for DB operations on vertica_001.acme	omw2-db
✓	⇊								11/21/14 09:53:37 PM	CPU load on vertica_001.acme.net back to normal.	omw2-db
✓	⇊								11/21/14 09:53:36 PM	Response time of AOB Investment Research web ap	AOB Web App
✓	⇊								11/21/14 09:53:35 PM	New node was added to Vertica Cluster, Monitoring I	vertica_bigdata

Add 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, first 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. Linking events to CIs is achieved through CI hints or by using the node, application, and object fields. For details about CI resolution, see Administer.

Additionally, TBEC must know the semantics of the event (because 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 that you want to correlate do not contain an ETI, add this information as described in the section below.

When these preparation steps are done (the two events are related to (connected) CIs and contain ETIs), you can create a new TBEC rule. You can 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 by using the TBEC Administration UI: **Administration > Event Processing > Correlation > Topology-Based Event Correlation**.

For details about configuring topology-based event correlation rules, see Administer.

Related Topics

Establish Infrastructure Topology

Add Event Type Indicators

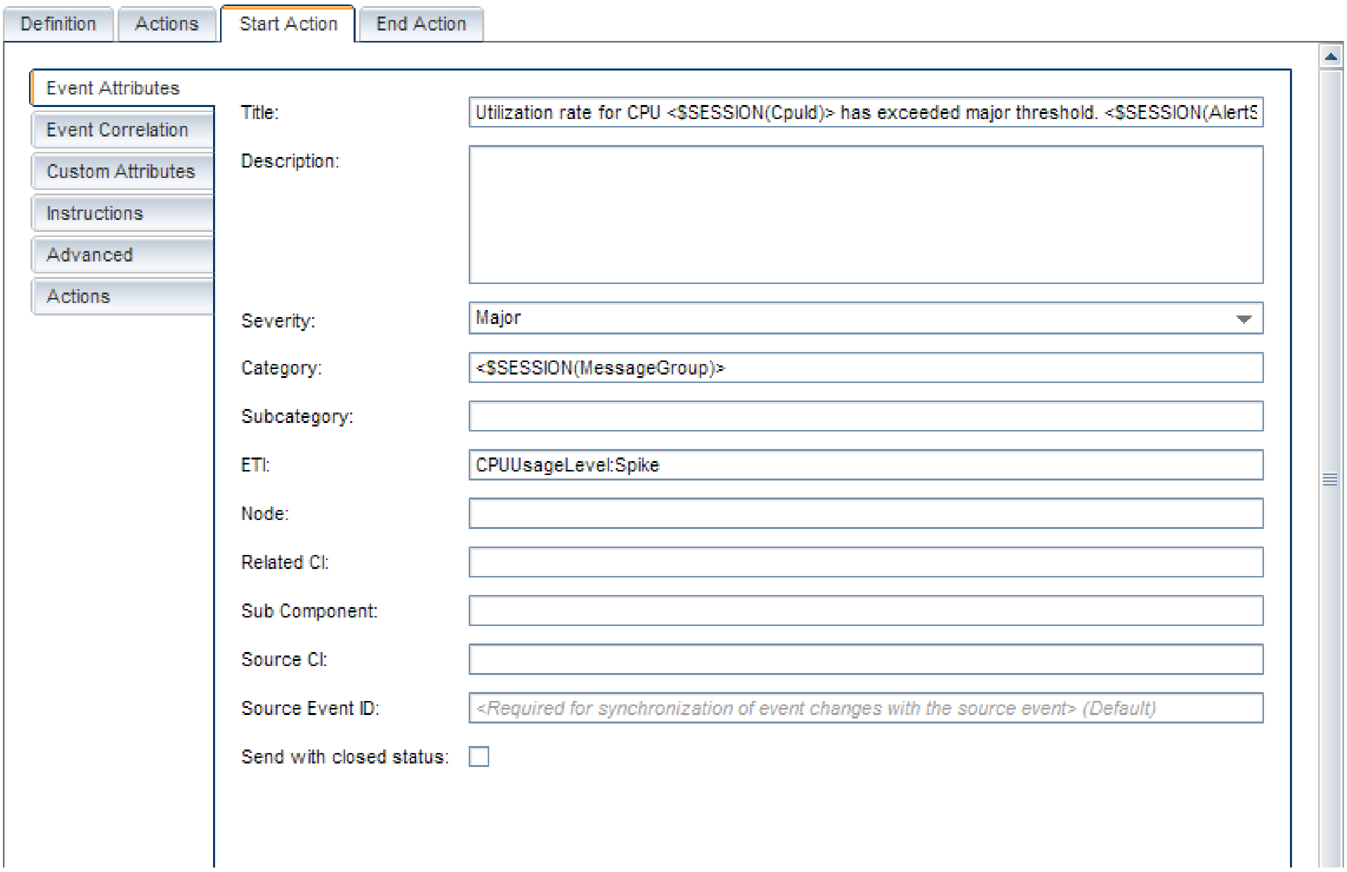
Add Event Type Indicators that represent the semantics of an event for the following use cases:

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

Such ETIs/HIs must first be defined in OBM and then can be set at the source of the event or by using an ETI mapping rule on the OBM server.

To define a new ETI, go to **Administration > Service Health > Indicator Definitions** and see the corresponding OMi Help topics.

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



Title: Utilization rate for CPU <$SESSION(CpuId)> has exceeded major threshold. <$SESSION(AlertS

Description:

Severity: Major

Category: <$SESSION(MessageGroup)>

Subcategory:

ETI: CPUUsageLevel:Spike

Node:

Related CI:

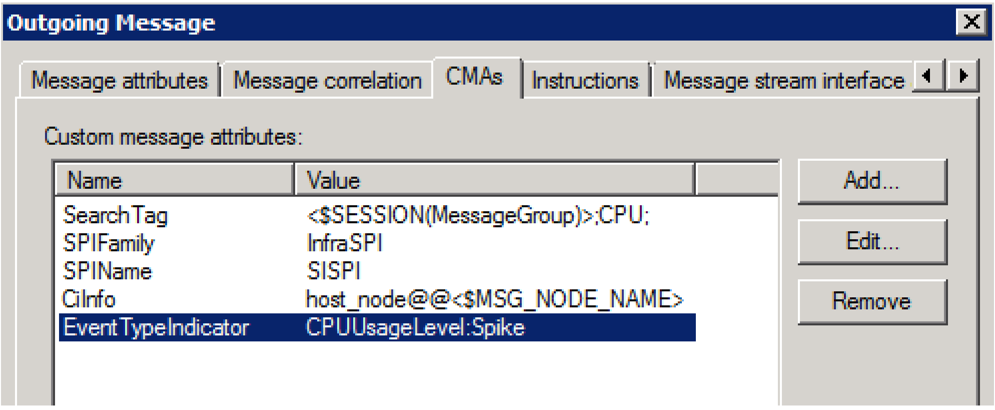
Sub Component:

Source CI:

Source Event ID: <Required for synchronization of event changes with the source event> (Default)

Send with closed status: □

If still used, you can also set the custom message attribute **EventTypeIndicator** (or **ETIhint**) inside an OM policy:



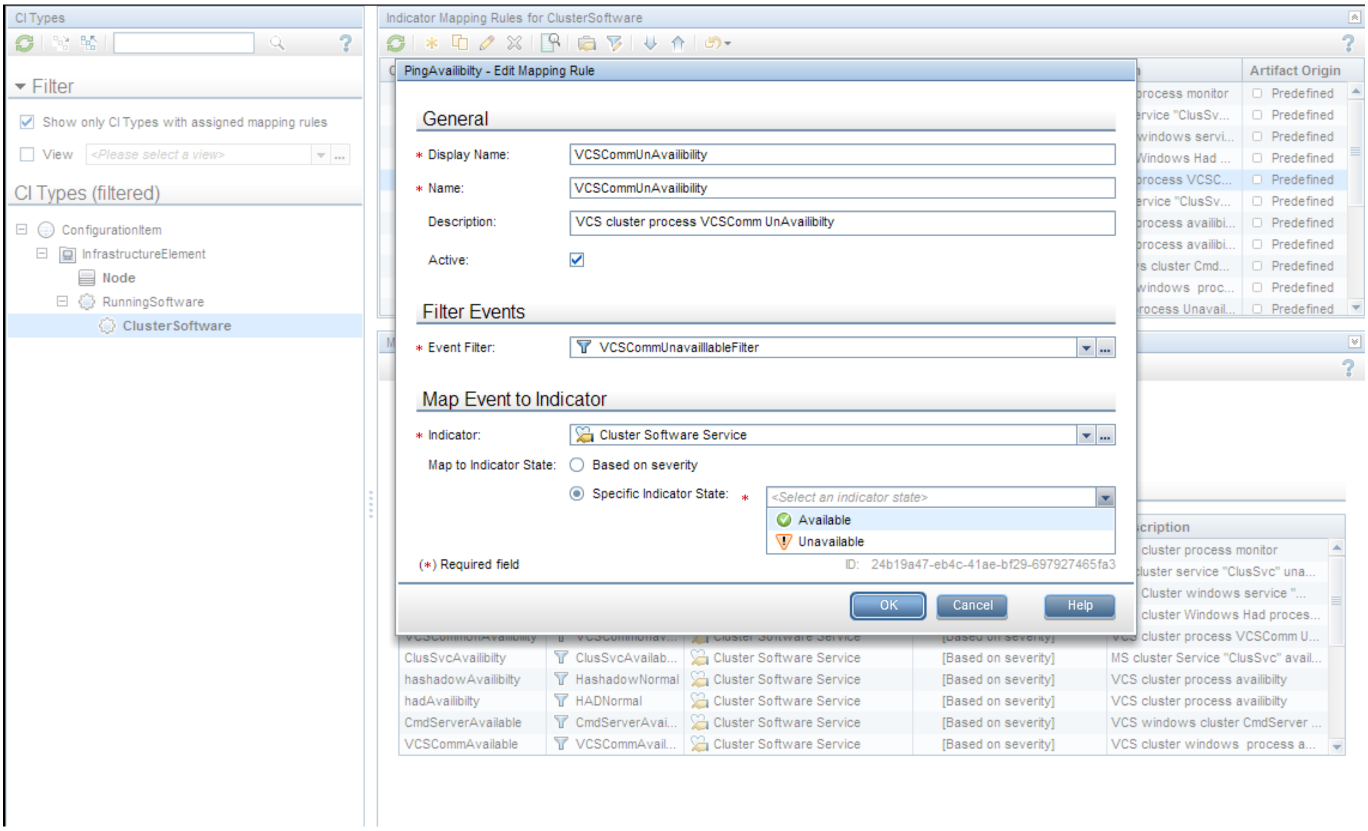
Custom message attributes:

Name	Value
SearchTag	<$SESSION(MessageGroup)>;CPU;
SPIFamily	InfraSPI
SPIName	SISPI
CiInfo	host_node@@<$MSG_NODE_NAME>
EventTypeIndicator	CPUUsageLevel:Spike

As an alternative, ETIs can also be set on the OBM server when the event arrives by using an ETI mapping rule:

1. Go to **Administration > Service Health > Indicator Definitions**.
2. Select the CI type for which the ETI is defined. In the ETI details, click **Edit Mapping Rules**.

The following figure shows Indicator Mapping Rules Manager:



☑ Show only CI Types with assigned mapping rules

□ View <Please select a view>

CI Types (filtered)

- ConfigurationItem
  - InfrastructureElement
    - Node
  - RunningSoftware
    - ClusterSoftware

PingAvailibilty - Edit Mapping Rule

General

* Display Name: VCSCommUnAvailibility

* Name: VCSCommUnAvailibility

Description: VCS cluster process VCSComm UnAvailibilty

Active: ☑

Filter Events

* Event Filter: VCSCommUnavailllableFilter

Map Event to Indicator

* Indicator: Cluster Software Service

Map to Indicator State: ○ Based on severity

● Specific Indicator State: * <Select an indicator state>

- Available
- Unavailable

(*) Required field

ID: 24b19a47-eb4c-41ae-bf29-697927465fa3

	Artifact Origin
process monitor	□ Predefined
ervice "ClusSv...	□ Predefined
windows servi...	□ Predefined
Windows Had ...	□ Predefined
process VCSC...	□ Predefined
ervice "ClusSv...	□ Predefined
process availibi...	□ Predefined
process availibi...	□ Predefined
s cluster Cmd...	□ Predefined
windows proc...	□ Predefined
rocess Unavail...	□ Predefined

				cription
				cluster process monitor
				luster service "ClusSvc" una...
				Cluster windows service "...
				cluster Windows Had proces...
				cluster process VCSComm U...
ClusSvcAvailibilty	ClusSvcAvailab...	Cluster Software Service	[Based on severity]	MS cluster Service "ClusSvc" avail...
hashadowAvailibilty	HashadowNormal	Cluster Software Service	[Based on severity]	VCS cluster process availibilty
hadAvailibilty	HADNormal	Cluster Software Service	[Based on severity]	VCS cluster process availibilty
CmdServerAvailable	CmdServerAvai...	Cluster Software Service	[Based on severity]	VCS windows cluster CmdServer ...
VCSCommAvailable	VCSCommAvail...	Cluster Software Service	[Based on severity]	VCS cluster windows process a...

Mapping rules allow you to set an ETI based on an event filter and a severity. For details about indicator mappings, see Administer.

Adjust Service Health

Service Health provides similar features as OM Service Navigator, because 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 by using predefined views. A view acts like a filter and retrieves only particular CIs from the RTSM for display.

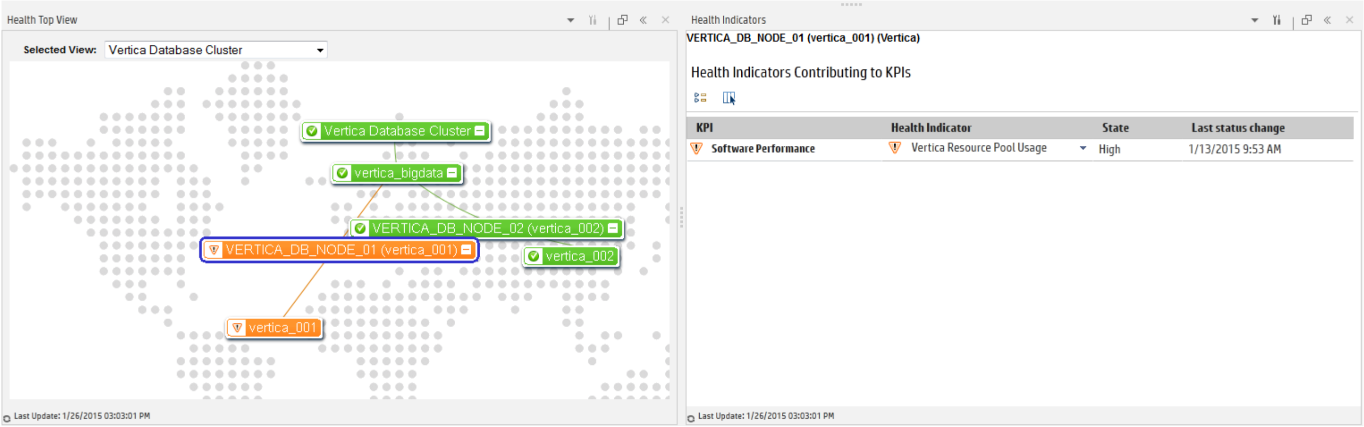
Service Health shows the hierarchy of the CIs and the CI status. Each CI has a CI status and can have one or multiple Key Performance Indicators (KPIs) that represent the high-level CI status, such as its performance or availability. Each KPI can be fed by one or multiple Health Indicators (HIs), representing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

Unlike OM Service Navigator that knows only one service status, Service Health calculates multiple HIs and KPIs that represent 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 that are associated with the same CI. For details about propagation rules, see the *Administer* section.

The following figure shows KPIs and HIs displayed in the Health Indicator component:



Selected View: Vertica Database Cluster

VERTICA_DB_NODE_01 (vertica_001) (Vertica)

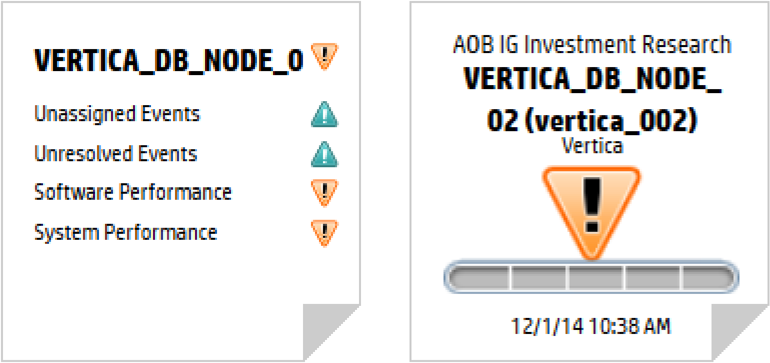
Health Indicators Contributing to KPIs

KPI	Health Indicator	State	Last status change
Software Performance	Vertica Resource Pool Usage	High	1/13/2015 9:53 AM

Last Update: 1/26/2015 03:03:01 PM

Last Update: 1/26/2015 03:03:01 PM

The following figure shows the CI status and KPIs displayed in the Watchlist component:



KPI calculation rules can be changed and extended. For details about business rules, see the *Administer* section.

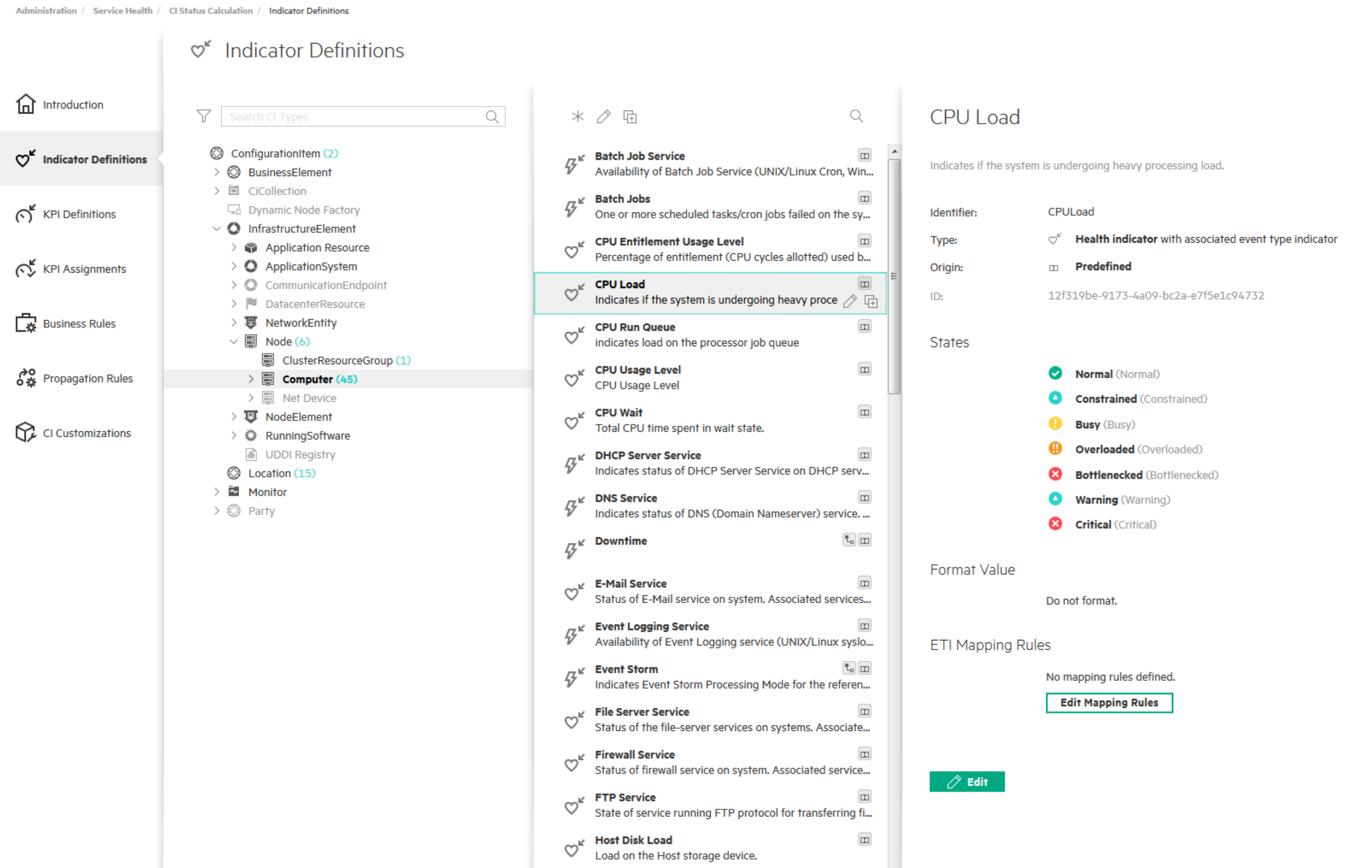
Out-of-the-box content packs contain many HI and KPI definitions and many KPI calculation rules that can be used as a starting point.

Contents

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 an HI definition with possible HI states:



Batch Job Service
Availability of Batch Job Service (UNIX/Linux Cron, Win...

Batch Jobs
One or more scheduled tasks/cron jobs failed on the sy...

CPU Entitlement Usage Level
Percentage of entitlement (CPU cycles allotted) used b...

CPU Load
Indicates if the system is undergoing heavy proce

CPU Run Queue
indicates load on the processor job queue

CPU Usage Level
CPU Usage Level

CPU Wait
Total CPU time spent in wait state.

DHCP Server Service
Indicates status of DHCP Server Service on DHCP serv...

DNS Service
Indicates status of DNS (Domain Nameserver) service. ...

Downtime

E-Mail Service
Status of E-Mail service on system. Associated services...

Event Logging Service
Availability of Event Logging service (UNIX/Linux syslo...

Event Storm
Indicates Event Storm Processing Mode for the referen...

File Server Service
Status of the file-server services on systems. Associate...

Firewall Service
Status of firewall service on system. Associated service...

FTP Service
State of service running FTP protocol for transferring fi...

Host Disk Load
Load on the Host storage device.

CPU Load

Indicates if the system is undergoing heavy processing load.

Identifier: CPULoad
Type: **Health indicator** with associated event type indicator
Origin: **Predefined**
ID: 12f319be-9173-4a09-bc2a-e7f5e1c94732

States

- ● **Normal** (Normal)
- ● **Constrained** (Constrained)
- ● **Busy** (Busy)
- ● **Overloaded** (Overloaded)
- ● **Bottlenecked** (Bottlenecked)
- ● **Warning** (Warning)
- ● **Critical** (Critical)

Format Value

Do not format.

ETI Mapping Rules

No mapping rules defined.

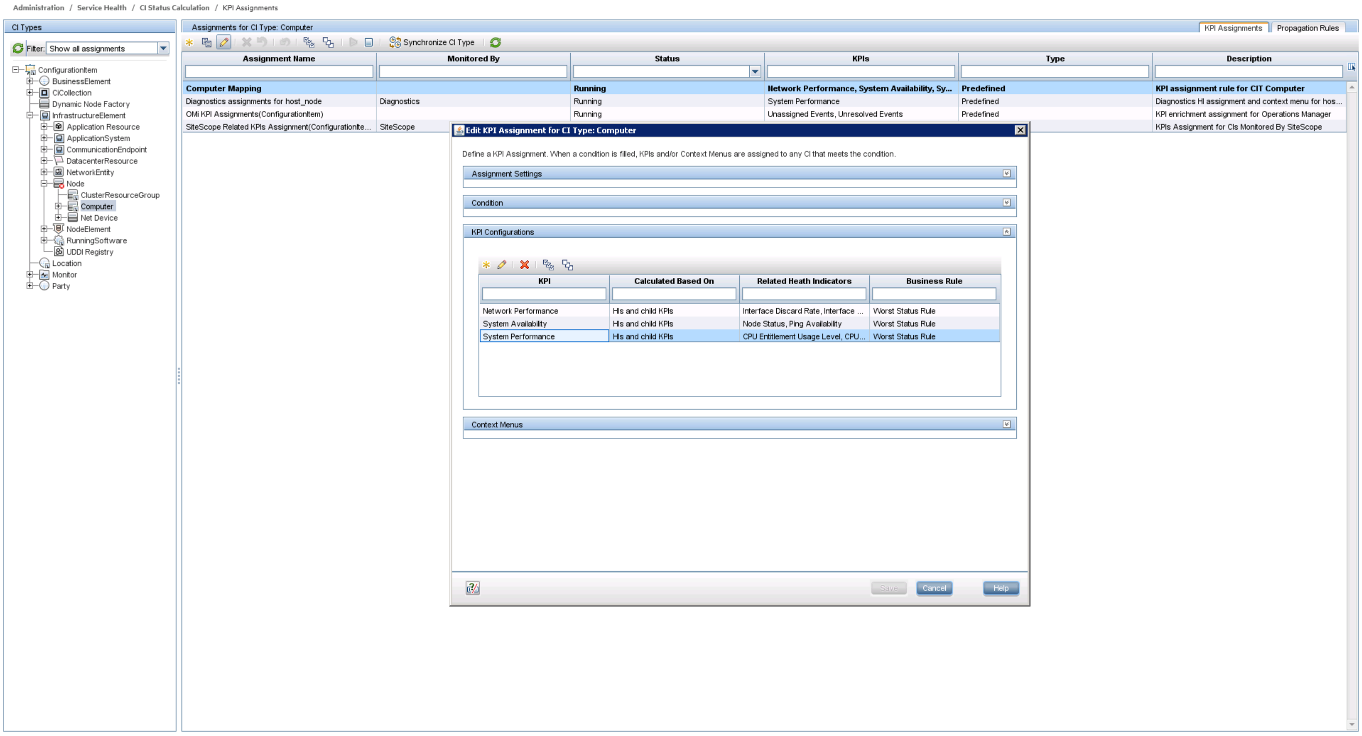
In OBM, HIs can be set through events. When an event is sent to OBM, it is sent with an ETI (Event Type Indicator). The ETI includes a name, a state and an optional metric value, for example, **CPULoad:exceeded** or **CPULoad:exceeded:98**. By using HI definitions in the indicator repository, OBM translates the ETI state into one of the standard OBM statuses (Critical, Major, Minor, and so on).

- An HI maintains its state until another event arrives that sets the same HI with a different state.
- To reset the HI to its default value manually, close the corresponding OBM event with **Close and Reset Health Indicator**. In normal production environments, OBM 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 by using statuses of HIs, KPIs, or their combination. 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 that displays HIs contributing to the KPI status:



Assignment Name	Monitored By	Status	KPIs	Type	Description
Computer Mapping		**Running**	**Network Performance, System Availability, Sy...**	**Predefined**	**KPI assignment rule for CIT Computer**
Diagnostics assignments for host_node	Diagnostics	Running	System Performance	Predefined	Diagnostics HI assignment and context menu for hos...
OMi KPI Assignments(ConfigurationItem)		Running	Unassigned Events, Unresolved Events	Predefined	KPI enrichment assignment for Operations Manager
SiteScope Related KPIs Assignment(ConfigurationIte...	SiteScope				KPIs Assignment for CIs Monitored By SiteScope

Define a KPI Assignment. When a condition is filled, KPIs and/or Context Menus are assigned to any CI that meets the condition.

KPI	Calculated Based On	Related Heath Indicators	Business Rule
Network Performance	HIs and child KPIs	Interface Discard Rate, Interface ...	Worst Status Rule
System Availability	HIs and child KPIs	Node Status, Ping Availability	Worst Status Rule
System Performance	HIs and child KPIs	CPU Entitlement Usage Level, CPU...	Worst Status Rule

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.

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

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, because 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, OBM by default does not propagate the event-related KPIs, but propagates all other health-related KPIs instead.

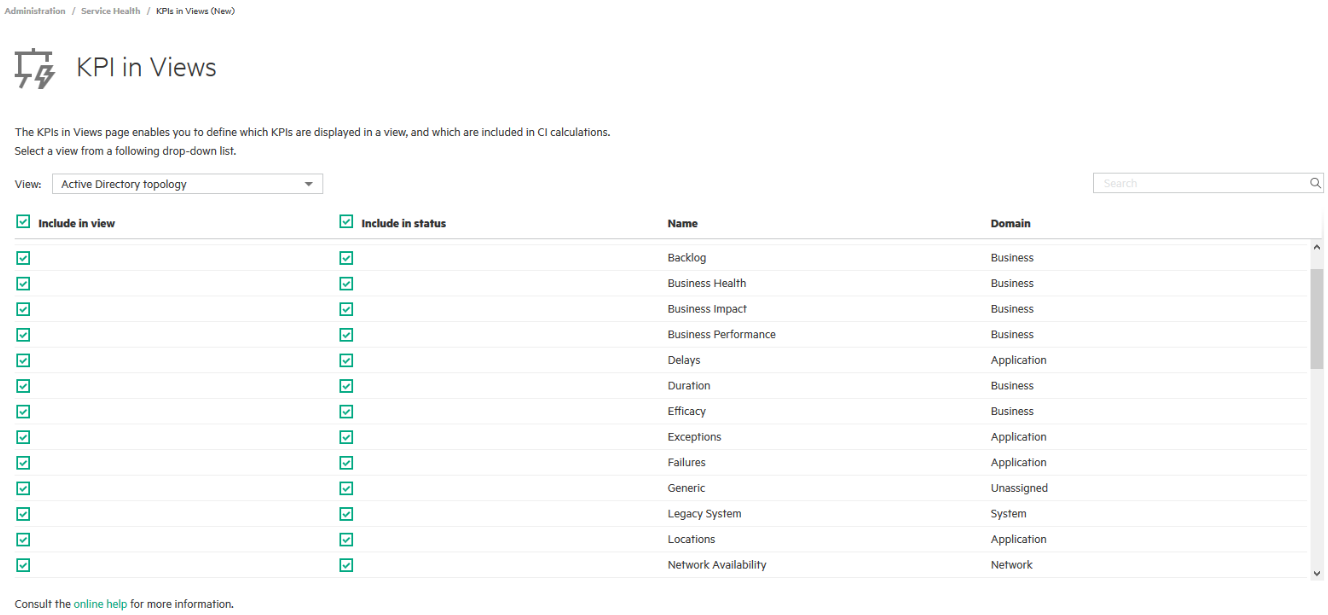
For details about how to propagate and sum up the events along the CI impact hierarchy, see Use.

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 about an active event count in KPIs, see Administer.

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:



Administration / Service Health / KPIs in Views (New)

KPI in Views

The KPIs in Views page enables you to define which KPIs are displayed in a view, and which are included in CI calculations.
Select a view from a following drop-down list.

View: Active Directory topology

☑ Include in view	☑ Include in status	Name	Domain
☑	☑	Backlog	Business
☑	☑	Business Health	Business
☑	☑	Business Impact	Business
☑	☑	Business Performance	Business
☑	☑	Delays	Application
☑	☑	Duration	Business
☑	☑	Efficacy	Business
☑	☑	Exceptions	Application
☑	☑	Failures	Application
☑	☑	Generic	Unassigned
☑	☑	Legacy System	System
☑	☑	Locations	Application
☑	☑	Network Availability	Network

Consult the online help for more information.

For details, see the corresponding OMi Help topics.

Review additional information

The following sections contain additional information that you might require for the evolution of OM to OBM:

- Agent management
- Node management
- Server configuration
- High availability and disaster recovery
- Available integrations and integration technologies
- Auditing and license reporting
- Preconfigured reports
- Command line, API, and web services reference
- Troubleshooting

Agent management

OBM can receive events from all Operations Agents version 11.0x and later (Operations Agents version 8.6x were previously supported by OBM but reached the end of the support phase).

To use OBM Monitoring Automation features, the Operations Agent version 11.12 or later is required.

For the successful agent management, get familiar with the following sections:

Contents

Deploy agents

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

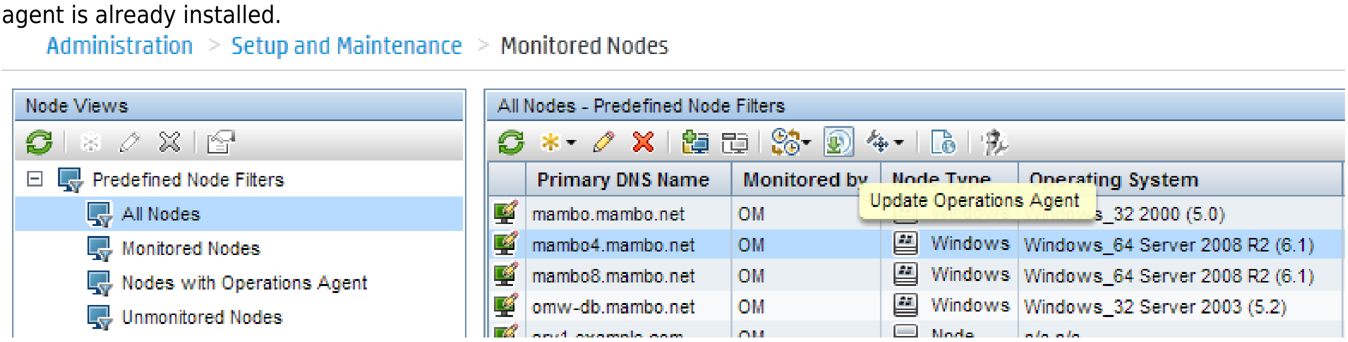
OBM does not offer remote agent deployment (that is, bootstrapping or initial agent deployment) yet, but can deploy agent patches and hotfixes when the agent is installed.
Agents can be installed manually (also remotely by using technologies such as SSH/SCP) or by using other software deployment tools, such as CDA, Server Automation, Microsoft Systems Center 2012 Configuration Manager, puppet, or yum. For details, see the Operations Agent Help.

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

After the agents are installed by using one of the above mentioned methods, they can be updated with hotfixes and patches from OBM.

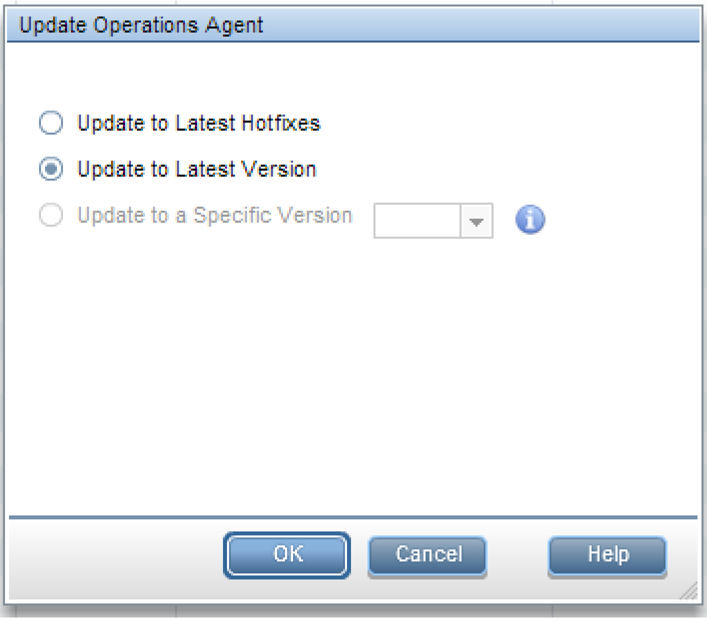
Consider the following:

- Patch and hotfix deployment OM can deploy agent patches and hotfixes remotely as well as the new agent versions if the agent is already installed.



Administration > Setup and Maintenance > Monitored Nodes
Node Views
Predefined Node Filters
All Nodes
Monitored Nodes
Nodes with Operations Agent
Unmonitored Nodes
All Nodes - Predefined Node Filters
Update Operations Agent

Primary DNS Name	Monitored by	Node Type	Operating System
mambo.mambo.net	OM		s_32 2000 (5.0)
mambo4.mambo.net	OM	Windows	Windows_64 Server 2008 R2 (6.1)
mambo8.mambo.net	OM	Windows	Windows_64 Server 2008 R2 (6.1)
omw-db.mambo.net	OM	Windows	Windows_32 Server 2003 (5.2)
[illegible]	OM	Node	n/a n/a



Update Operations Agent

○ Update to Latest Hotfixes

● Update to Latest Version

○ Update to a Specific Version

For details about updating Operations Agent installations, see the Administer section.

- Certificates handling Certificate requests from agents can be granted in the OBM UI (**Administration > Setup and Maintenance > Certificate Requests**) or by using the command-line interface `ovcm` as on OM systems. OBM supports granting certificates automatically based on IP ranges, node names, or by using other attributes through Groovy scripts.

Maintain agents

Many CLIs that exist in OM, such as `ovpolicy` or `ovconfpar`, are provided in OBM 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. For more information, see the Administer section.

Depending on the action that you want to perform, you can use the following CLIs:

- Start and stop agents Use the following OBM CLI to check the agent status, or to start or 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 Operations Agents" -username admin opr-agt -status –node_list node1.example.com,node2.example.com
- Agent configuration changes Use OBM 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 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

Monitor agent health

OM servers are able to ping agents regularly and report when the agents no longer respond. OBM 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 in OM ensure that problems with the agent own core components do not compromise its ability to monitor managed nodes. By using the self-monitoring feature, you can easily verify if the Operations 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 OBM, but they can be imported and deployed if required. Additionally, the `ovc` process on any agent automatically restarts aborted or killed agent processes and sends corresponding events to its management server.

By using the OM self-monitoring feature, you can establish if the Operations Agent is working properly by configuring the agent to poll its own core components and generate an alert if it detects any problems. Although OBM does not ship these self-monitoring policies, you can import and use them in OBM.

In OBM, create a wrapper around imported policies by creating a self-monitoring aspect for the Operations Agent CI Type and assign it to the Operations Agent CIs. This deploys all included self-monitoring policies with a single assignment.

OM and OBM feature comparison

OM Functionality	Equivalent in OBM
Start, stop, status, version, switch a primary manager, set variables on agents by using `opcragt`	Yes, by using `ovrc`, `ovconfpar`, `opr-agt`
Mass operations (start, stop, status, version, switch a primary manager, set variables) on agents by using `opcragt –all –nodegroup`	Yes, mass operations (start, stop, status, version, switch a primary manager, set variables) on agents by 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 OBM Latest patches can be deployed by using the Update Operations Agent function
Deployment of hotfixes (possible only by using a hotfix deployment tool)	Yes, integrated into OBM Latest hotfixes can be deployed by 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 OBM server
Query detailed installed agent packages	Yes, by using `ovdeploy` The Operations Agent version is also displayed in the Monitored Nodes UI
Supports OA 11.0x and later	Yes

Task: How to manage agents from OM and OBM

By using agent-based flexible management policy templates, OBM and OM systems can be configured as action-allowed and secondary managers, which allows configuration and management of agents from both OM and OBM 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 OBM.

For details about connecting Operations Agents to OBM, see the Administer section.

The following procedures are available for switching agents from OM to OBM:

- *Recommended*: switch agents using a flexible management template (using existing certificates) Switch the agents to OBM by using a flexible management template. By using this approach, you can continue monitoring business-critical applications on the node and replace its configuration while the agent is running. The following is the summary of recommended steps:
  1. Allow management from both servers by using a flexible management template.
  2. Choose a group or type of nodes to move over (for example, all my Oracle Database systems).
     1. Test policy and aspect deployment and tool execution on a representative node.
     2. After a successful test, roll out configuration to the remaining nodes of the same type.
     3. Switch the primary manager and target server to OBM: This still allows configuration from both OBM and OM servers. opr-agt -primmgr <node selection> -username <user>
  3. Repeat Step 2 until all nodes are managed by OBM.
  4. Before switching off the OM server, switch the agents to OBM completely: opr-agt –switch_manager <node selection> -username <user> Afterward, clean up old OM policies if necessary: opr-agt –deploy -clean <node selection> -username <user>
- At this point, the node still has a certificate issued by the old OM server and is configured to trust both OBM and OM server certificates. However, as the primary manager is 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 reissue or replace agent certificates. The OM certificate authority can be completely shut down and the private key can be destroyed. You can request new agent certificates.
- *Alternative*: Switch agents completely by using 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 OBM server by using the Admin UI or `ovcm`.
  7. Deploy aspects and management templates to start monitoring again.
- 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 must be reconfigured by OBM. Related Topics Manage Operations Agents from OBM

Node management

For the successful node management, get familiar with the following sections:

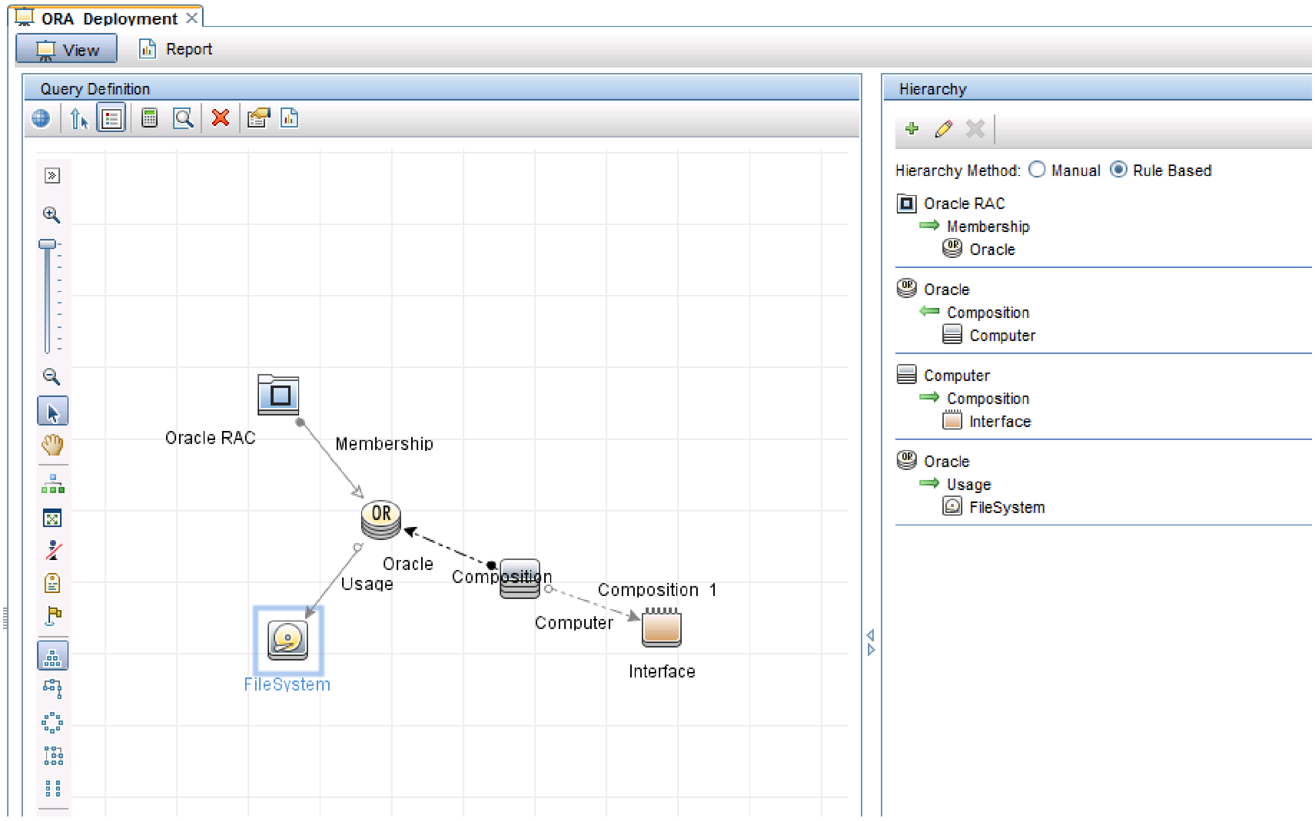
Contents

Management approach differences

Node management approaches in OM and OBM are not the same. These are the main differences:

- OM
  - Node-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.
  - 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 or IP address. Policies are enabled only on nodes that run a corresponding resource group. This functionality is currently not supported for cluster-based monitoring in OBM.
  - 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 may 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.
  - Node attributes Nodes in OM have attributes, such as machine type, control type, and so on (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` enables 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. The result is that all messages that match that pattern are assigned to that node.
  - Node group, node layout group, and node hierarchy In OM, you can group nodes into node groups, which can be used for mass policy deployment and mass tool execution, as well as for defining user responsibilities and filtering the events. You can mark node groups as hidden.
  - Structuring monitored objects by using node groups 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 used for grouping and structuring monitored objects or nodes to cope with the large amount of objects in the IT environment.



Hierarchy Method: ○ Manual ● Rule Based

- Oracle RAC
  - Membership
    - Oracle
- Oracle
  - Composition
    - Computer
- Computer
  - Composition
    - Interface
- Oracle
  - Usage
    - FileSystem

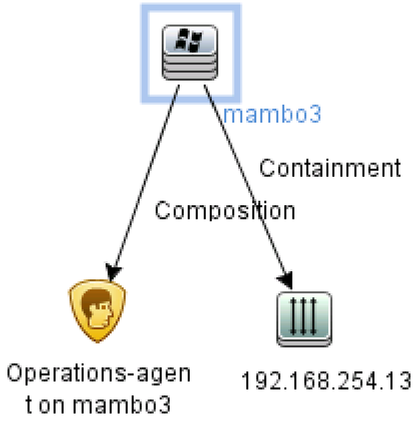
- OBM
  - CI-centric approach In OBM, the approach is CI-centric, or view-centric. Responsibilities are defined by using views and operators typically work with CIs of various CI types (such as business applications, running software, databases, web servers, and so on). The node that hosts the CIs is not as important as in OM, because operators can launch tools or deploy aspects to CIs directly, without knowing which nodes are affected. Mass deployment to nodes through node groups in OM is replaced in OBM 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 OBM (as CI collections), do not play a special role.
  - CI Collection In OBM, tool execution is done on CIs, mass policy deployment is replaced by manual or automatic RTSM-based aspect deployment, and user responsibilities are defined by using views. Therefore, the only use case where node groups can be beneficial is filtering the events.
  - Structuring monitored objects by using views In OBM, the structure of monitored objects (configuration items) is represented in the RTSM with relationships. RTSM views retrieve and display CIs and relationships. The displayed hierarchy is defined by the view definition. By 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. OBM 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.
  - Nodes as CIs Nodes in OBM are represented as CIs of type Node (or a subtype 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 Operations Agent CIs). A node with a Composition relationship to an 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 Operations Connector.
  - External nodes In OBM, 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 regardless of a view filter. Therefore, it is not necessary to set up an external node to view the events. To map particular events to specific, external nodes or 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 OBM server by 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.

Transition strategy

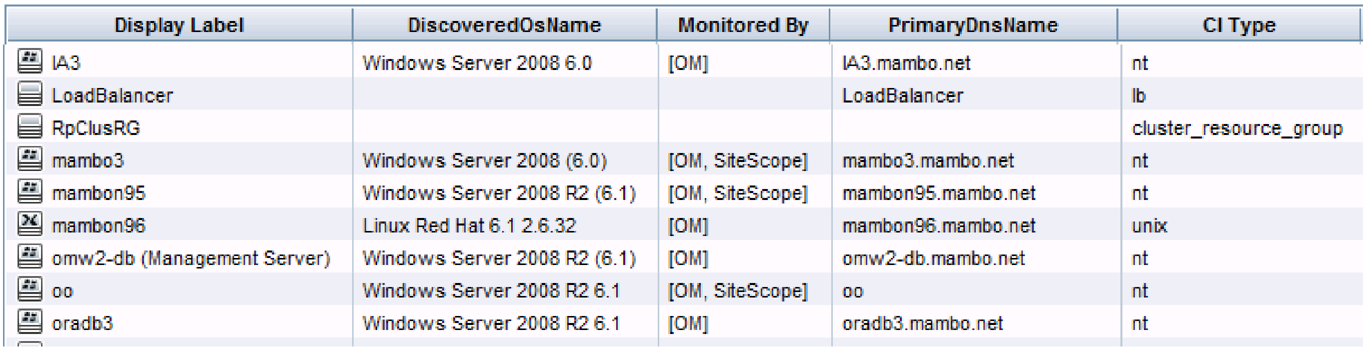
To simplify the move to OBM, OM operators can use the OM CI collection view to filter the events based on node groups. Node groups or CI collections can be created and updated automatically in OBM, if nodes are no longer managed by OM.

However, to benefit from all CI-centric features of OBM (CI-specific tools/run-books, CI-specific graphs, and so on), it is recommended that OBM operators switch from a node group-based approach to a view-based approach as soon as possible.

The following figure shows a typical node CI with related CIs in the RTSM:

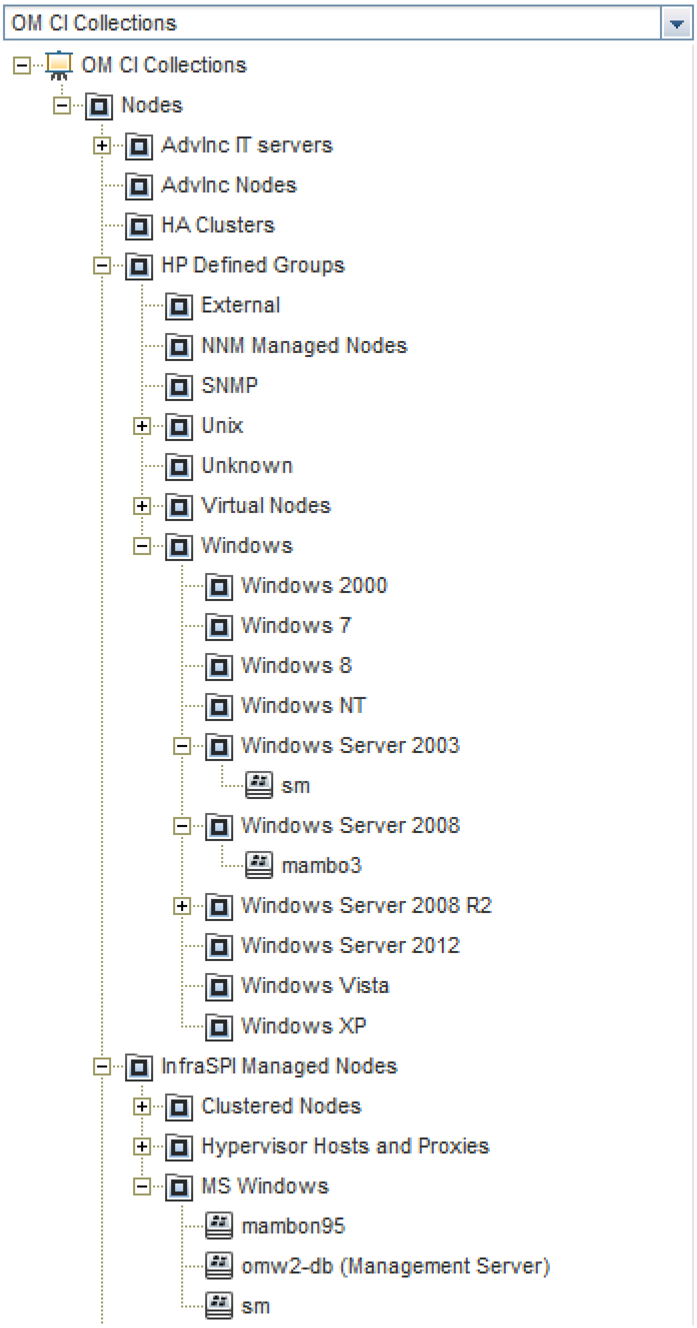


The following figure shows some attributes of nodes in the RTSM:



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

OBM automatically creates CI collections that represent the OM node group hierarchy. This hierarchy is created and updated by using topology synchronization from OM. This hierarchy can be displayed and used for filtering by using the out-of-the-box view **OM CI Collections**. This is very useful when OM and OBM are used side by side.



OM CI Collections

- OM CI Collections
  - Nodes
    - AdvInc IT servers
    - AdvInc Nodes
    - HA Clusters
    - HP Defined Groups
      - External
      - NNM Managed Nodes
      - SNMP
      - Unix
      - Unknown
      - Virtual Nodes
      - Windows
        - Windows 2000
        - Windows 7
        - Windows 8
        - Windows NT
        - Windows Server 2003
          - sm
        - Windows Server 2008
          - mambo3
        - Windows Server 2008 R2
        - Windows Server 2012
        - Windows Vista
        - Windows XP
    - InfraSPI Managed Nodes
      - Clustered Nodes
      - Hypervisor Hosts and Proxies
      - MS Windows
        - mambon95
        - omw2-db (Management Server)
        - sm

The underlying relationships in the RTSM (which CI/Node belongs to which CI Collection/node group) are updated by using toposync whenever changes occur on the OM side.

However, these group relationships are not created or updated automatically, because node groups do not play a special role in OBM.

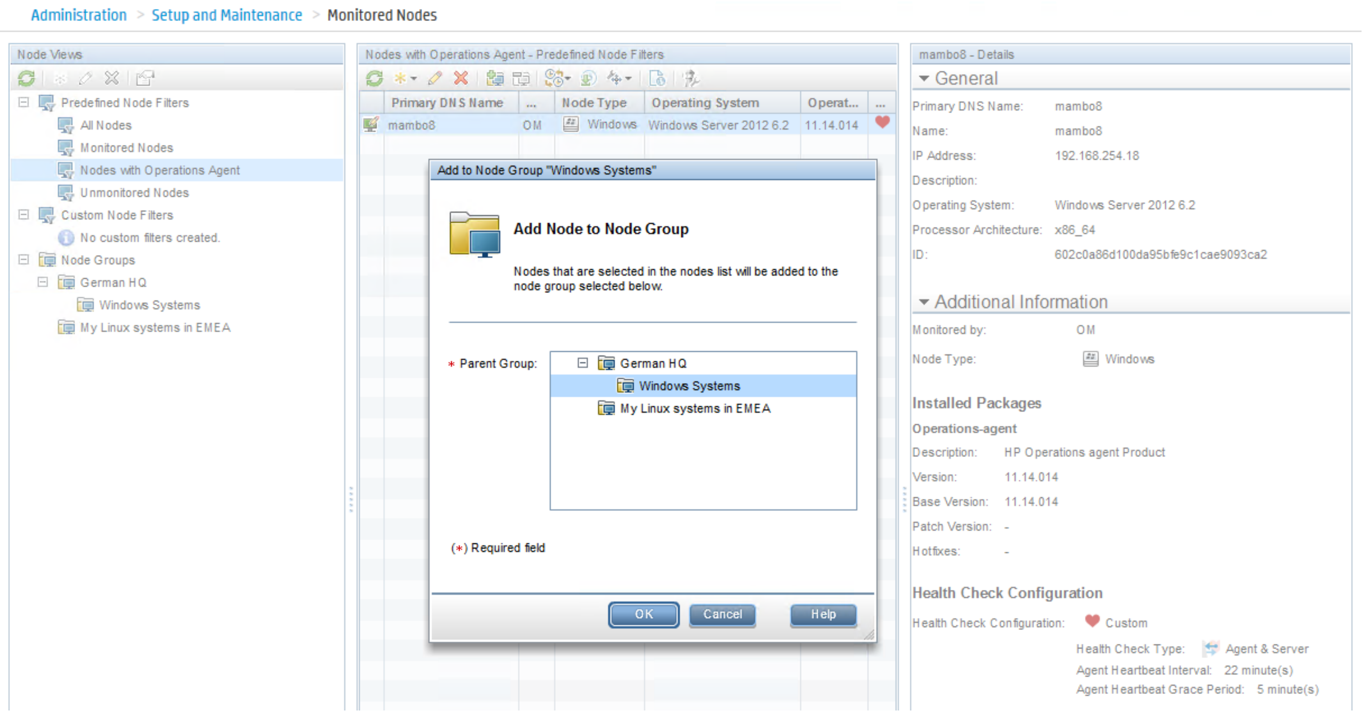
Tasks

The following sections contain some common tasks for node management in OBM.

How to set up nodes in OBM

In OBM, node CIs and related CIs are typically created automatically. Such CIs are created when the Operations Agent is installed for the first time and connected to the OBM server. Node CIs are also created by using topology synchronization from OM or by using various discovery technologies.

It is not required to set up nodes in advance as it is done in OM.



Add to Node Group "Windows Systems"

Add Node to Node Group

Nodes that are selected in the nodes list will be added to the node group selected below.

* Parent Group: German HQ / Windows Systems / My Linux systems in EMEA

(*) Required field

mambo8 - Details

General

Primary DNS Name: mambo8
Name: mambo8
IP Address: 192.168.254.18
Description:
Operating System: Windows Server 2012 6.2
Processor Architecture: x86_64
ID: 602c0a86d100da95bfe9c1cae9093ca2

Additional Information

Monitored by: OM
Node Type: Windows

Installed Packages

Operations-agent
Description: HP Operations agent Product
Version: 11.14.014
Base Version: 11.14.014
Patch Version: -
Hotfixes: -

Health Check Configuration

Health Check Configuration: Custom
Health Check Type: Agent & Server
Agent Heartbeat Interval: 22 minute(s)
Agent Heartbeat Grace Period: 5 minute(s)

If nodes are not created automatically, you can create CIs by using the Monitored Nodes UI. This UI is introduced to simplify viewing and maintaining node CIs and can also be used to add nodes to node collections (CI collections) manually. Starting with OBM 10, it also enables configuring health checks and updating agents. Nodes can also be created by using the `opr-node` command line tool.

How to change hostname or IP address of a managed node

When the node CI and its related CIs are already created, and you decide to change the hostname or the IP address of the node, it is highly recommended that you update the details in OBM manually before making changes on the node.

Otherwise, the node sends the updated IP address and hostname to OBM, which can result in a duplicate node CI. This is due to the CI reconciliation rules in the RTSM that require a 66% match of the IP addresses (this means, 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 the IP address:

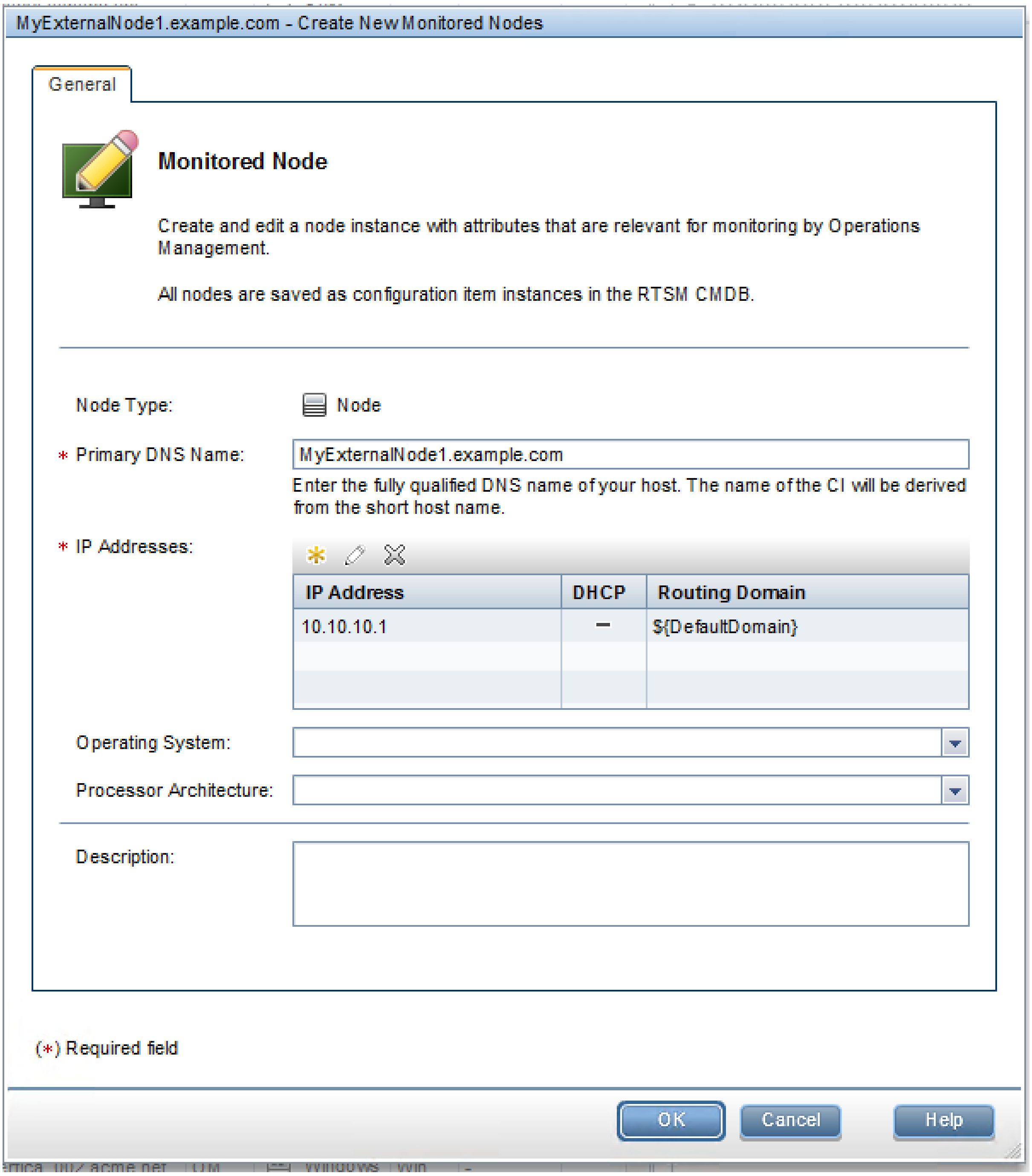
1. In OBM, go to **Administration > Setup and Maintenance > Monitored Nodes**.
2. Edit the node and change the hostname and/or the IP address. Click **OK**.
3. Change the hostname and/or the IP address on the managed node.

How to implement external nodes in OBM

This procedure is required if you want to map events from various nodes to one specific external node or CI, so that operators can get a list of these 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 by using **Administration > Setup and Maintenance > Monitored Nodes**. Other CIs can be created by using **Administration > RTSM Administration > Modeling > 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. Therefore, you can skip Step 1.



MyExternalNode1.example.com - Create New Monitored Nodes

Monitored Node

Create and edit a node instance with attributes that are relevant for monitoring by Operations Management.

All nodes are saved as configuration item instances in the RTSM CMDB.

Node Type: Node

* Primary DNS Name: MyExternalNode1.example.com

Enter the fully qualified DNS name of your host. The name of the CI will be derived from the short host name.

* IP Addresses:

IP Address	DHCP	Routing Domain
10.10.10.1	–	${DefaultDomain}

Operating System:

Processor Architecture:

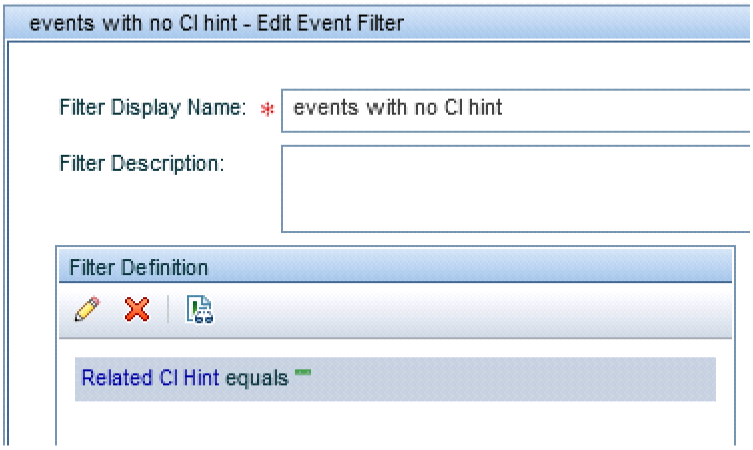
Description:

(*) Required field

Example:

1. Create a generic node (Node Type: Node) and provide a node name (for example, MyExternalNode1.example.com). Specify the IP address, because all nodes in the RTSM require an IP address. Use the IP address that is not used by any real node. Review the node properties and copy the node ID because you will use it in the next step.
2. Create an Event Processing Customization/ EPI script for the step Before CI/ETI resolution. Copy the below stated code into the Script tab and replace `<id of CI that acts as external node>` with the ID of the CI that you created. Change `NODE_SUFFIX` according to your needs. Example of a script that maps all events from nodes with that suffix to the external node CI You can implement more sophisticated checks by 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); } } } 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.



events with no CI hint - Edit Event Filter

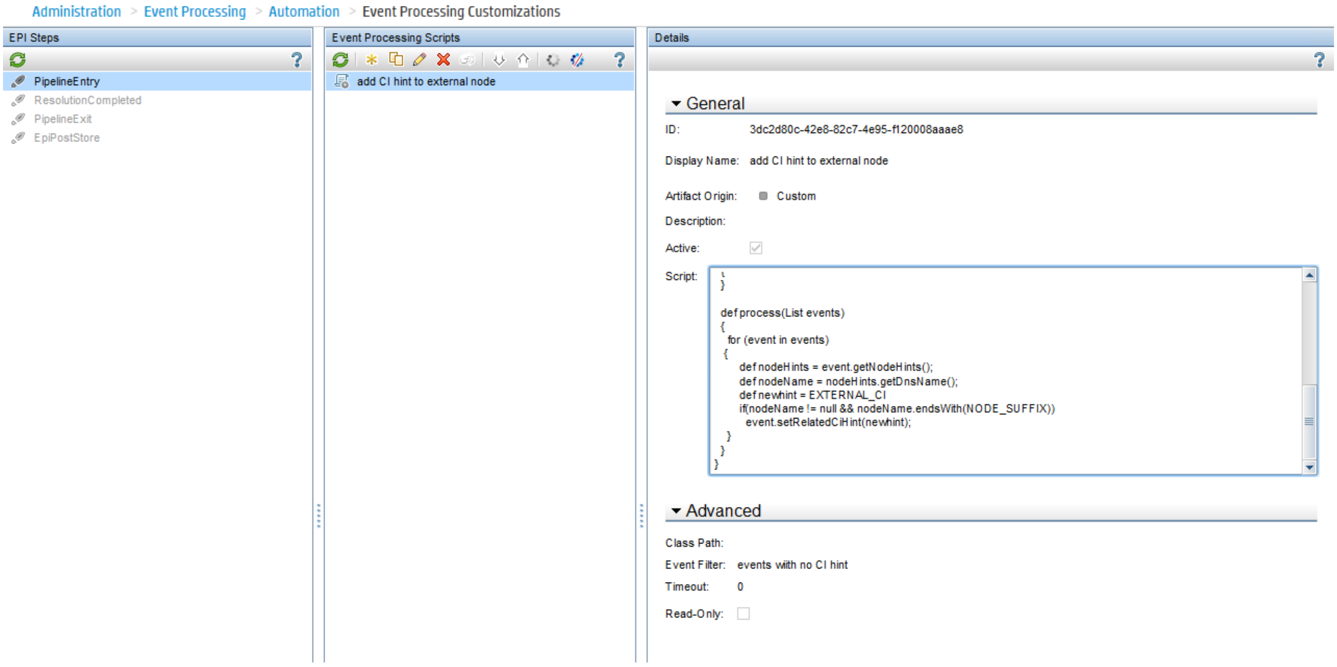
Filter Display Name: * events with no CI hint

Filter Description:

Filter Definition

Related CI Hint equals

Final EPI Script in **Administration > Event Processing > Automation > Event Processing Customizations**.



Administration > Event Processing > Automation > Event Processing Customizations

General

ID: 3dc2d80c-42e8-82c7-4e95-f120008aaae8

Display Name: add CI hint to external node

Artifact Origin: Custom

Description:

Active: ☑

Script:

```
 }

 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);
   }
 }
}
```

Advanced

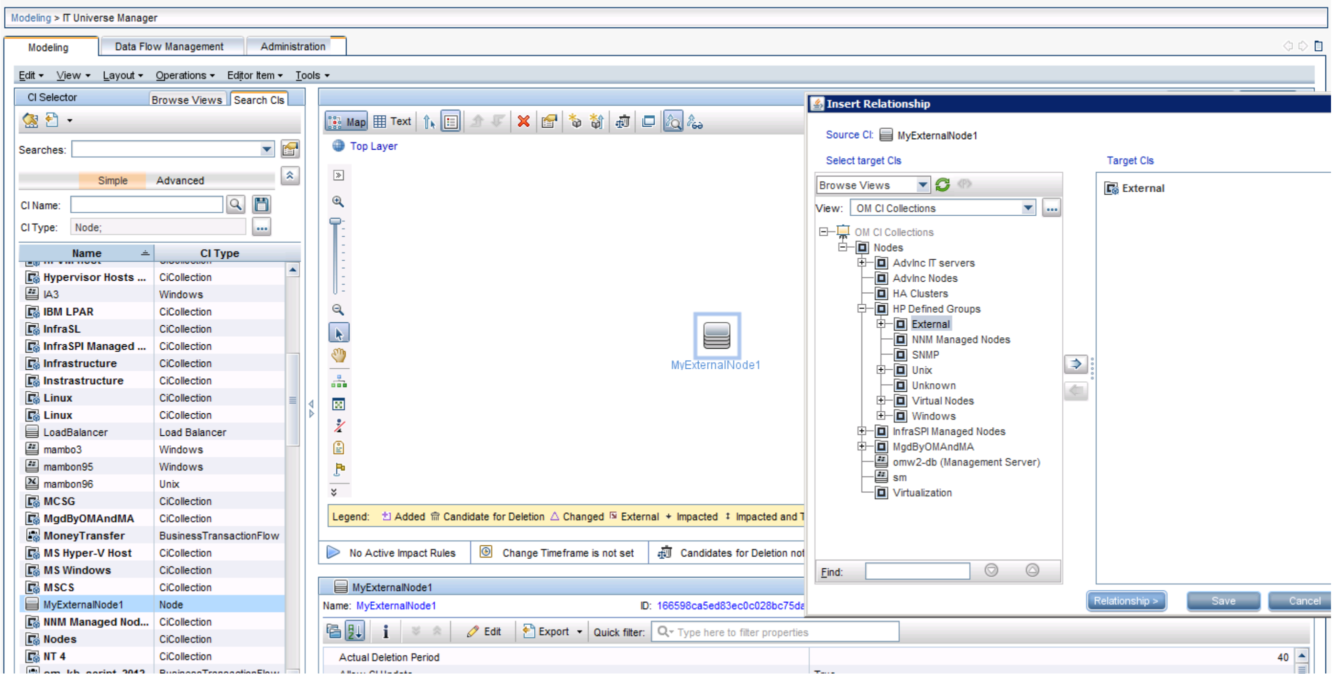
Class Path:

Event Filter: events with no CI hint

Timeout: 0

Read-Only: □

3. Add a 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:
   1. Create a relationship to the External node group by using the IT Universe Manager.
   2. Select the new CI and choose **Relate to CI** from the context menu.
   3. Search the “External” CI collection in the **OM CI Collections** view and create a membership relationship from the CI collection to the node.
4.

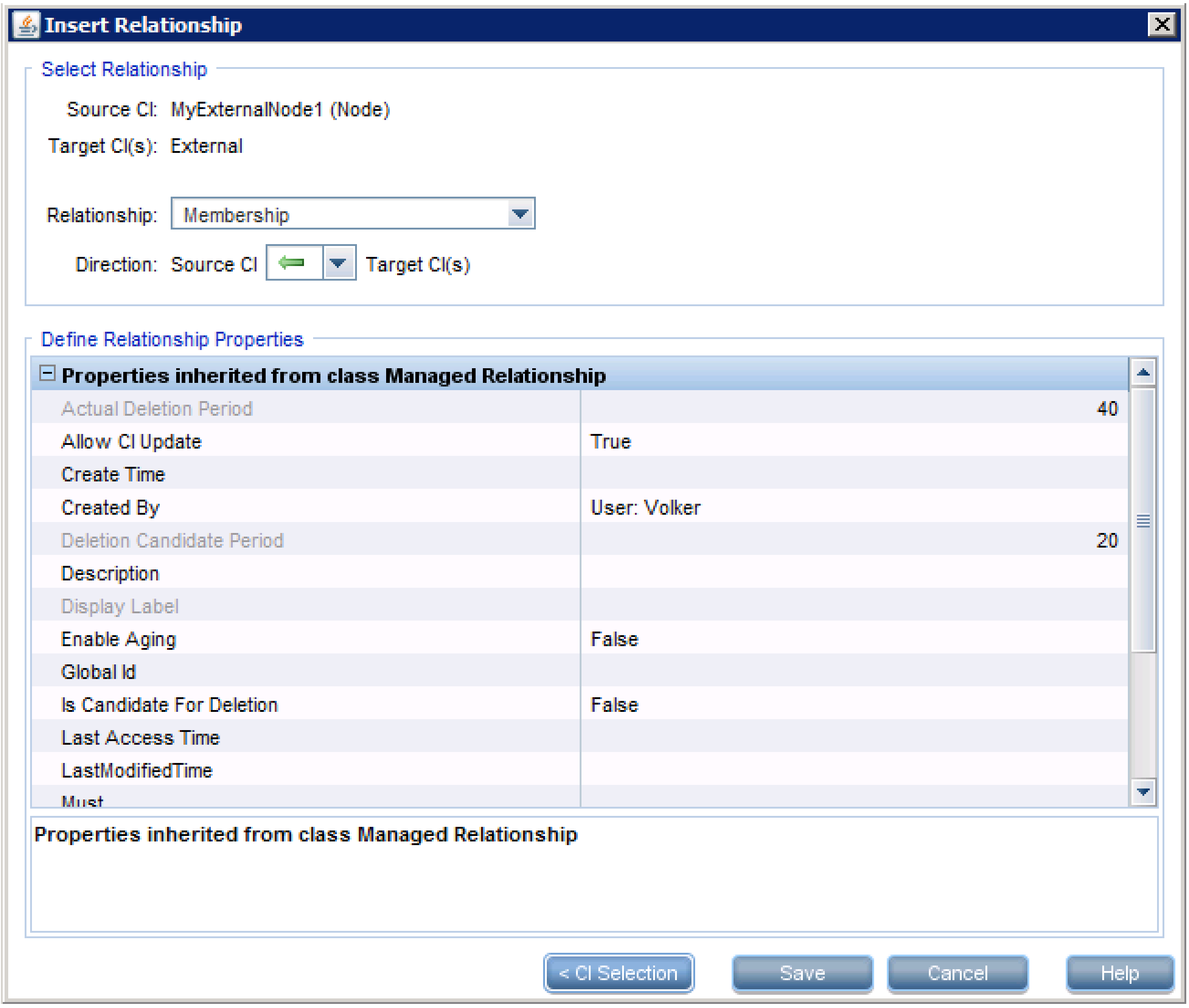


Name	CI Type
Hypervisor Hosts ...	CiCollection
IA3	Windows
IBM LPAR	CiCollection
InfraSL	CiCollection
InfraSPI Managed ...	CiCollection
Infrastructure	CiCollection
Instrastructure	CiCollection
Linux	CiCollection
Linux	CiCollection
LoadBalancer	Load Balancer
mambo3	Windows
mambon95	Windows
mambon96	Unix
MCSG	CiCollection
MgdByOMAndMA	CiCollection
MoneyTransfer	BusinessTransactionFlow
MS Hyper-V Host	CiCollection
MS Windows	CiCollection
MSCS	CiCollection
MyExternalNode1	Node
NNM Managed Nod...	CiCollection
Nodes	CiCollection
NT 4	CiCollection

OM CI Collections
- Nodes
  - Advlnc IT servers
  - Advlnc Nodes
  - HA Clusters
  - HP Defined Groups
    - External
    - NNM Managed Nodes
    - SNMP
    - Unix
    - Unknown
    - Virtual Nodes
    - Windows
  - InfraSPI Managed Nodes
  - MgdByOMAndMA
  - omw2-db (Management Server)
  - sm
  - Virtualization

MyExternalNode1
Name: MyExternalNode1 ID: 166598ca5ed83ec0c028bc75de

Actual Deletion Period	40



Select Relationship

Source CI: MyExternalNode1 (Node)

Target CI(s): External

Relationship: Membership

Direction: Source CI ← Target CI(s)

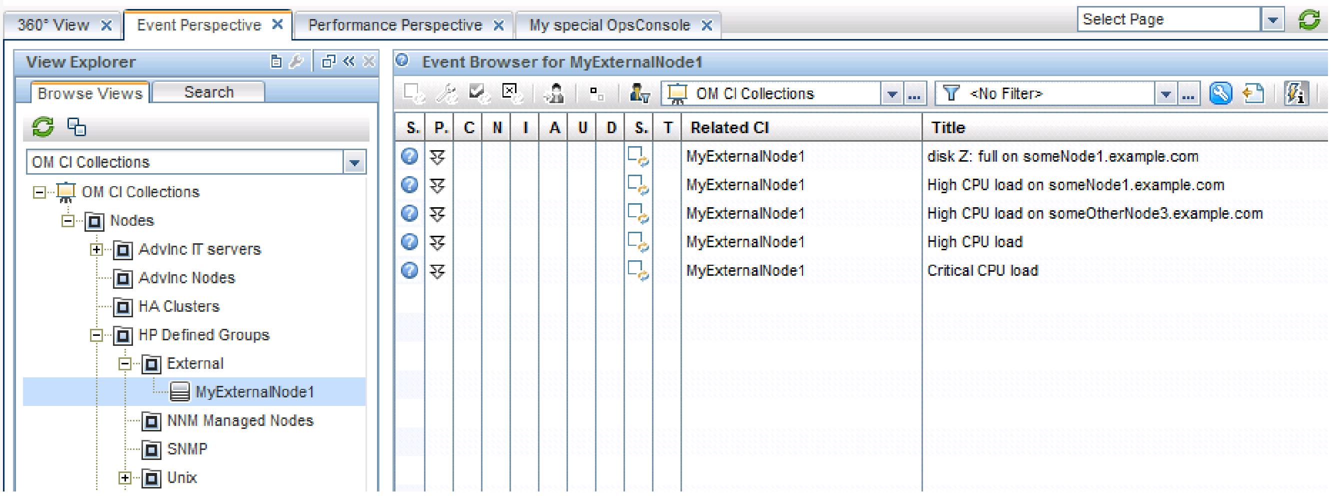
Define Relationship Properties

⊟ Properties inherited from class Managed Relationship

Actual Deletion Period	40
Allow CI Update	True
Create Time	
Created By	User: Volker
Deletion Candidate Period	20
Description	
Display Label	
Enable Aging	False
Global Id	
Is Candidate For Deletion	False
Last Access Time	
LastModifiedTime	
Must	

Properties inherited from class Managed Relationship

The operators can now select the external node CI in the **OM CI Collections** view and get the corresponding events as in OM:



S.	P.	C	N	I	A	U	D	S.	T	Related CI	Title
										MyExternalNode1	disk Z: full on someNode1.example.com
										MyExternalNode1	High CPU load on someNode1.example.com
										MyExternalNode1	High CPU load on someOtherNode3.example.com
										MyExternalNode1	High CPU load
										MyExternalNode1	Critical CPU load

How to move node topology to OBM/topology synchronization

Nodes and the node group hierarchy of OM are forwarded to OBM (as well as to RTSM) together with the services hierarchy by using topology synchronization. For details about topology synchronization, see the *Develop* section. Depending on the operating system that hosts OM, choose as follows:

- OM for Windows Use default configured toposync packages that include the nodegroups synchronization package.
- OM for UNIX Use toposync packages **layoutgroups** and **nodegroups**.

Configure the synchronization package as follows:

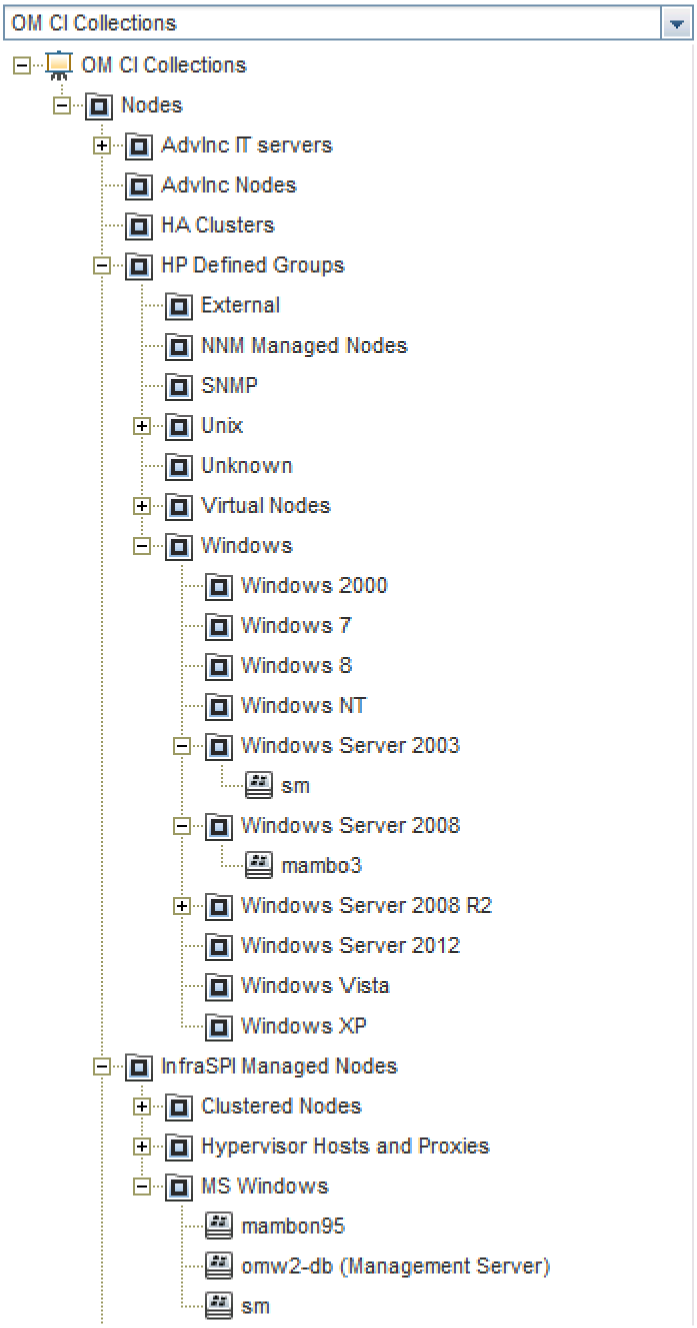
1. Go to **Administration > Setup and Maintenance > Infrastructure Settings**.
2. Select **Applications** and use the list to set the administration context to Operations Management.
3. Scroll to **Operations Management - HPOM Topology Synchronization Settings**.

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 types and Relationships in the RTSM

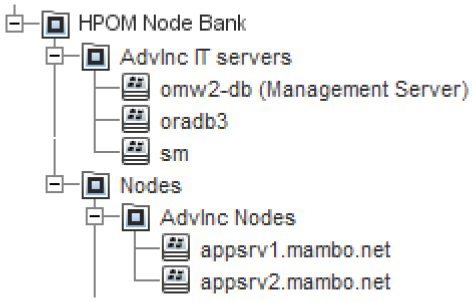
Node	OM for UNIX and Linux, OM for Windows	Node, Computer, Unix|Windows, other <*operating system*> Path in the CI Types tree: Managed Object -> ConfigurationItem -> InfrastructureElement -> Node -> Computer -> Unix | Windows | ... Mapping: External node -> Node Node with the operating system specification -> Computer or operating system-related CI type, for example, Unix, Windows, and so on Virtual node -> „virtualized_system“ added to the “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 the CI Types 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):



OM CI Collections

- OM CI Collections
  - Nodes
    - AdvInc IT servers
    - AdvInc Nodes
    - HA Clusters
    - HP Defined Groups
      - External
      - NNM Managed Nodes
      - SNMP
      - Unix
      - Unknown
      - Virtual Nodes
      - Windows
        - Windows 2000
        - Windows 7
        - Windows 8
        - Windows NT
        - Windows Server 2003
          - sm
        - Windows Server 2008
          - mambo3
        - Windows Server 2008 R2
        - Windows Server 2012
        - Windows Vista
        - Windows XP
    - InfraSPI Managed Nodes
      - Clustered Nodes
      - Hypervisor Hosts and Proxies
      - MS Windows
        - mambon95
        - omw2-db (Management Server)
        - sm



```
HPOM Node Bank
  AdvInc IT servers
    omw2-db (Management Server)
    oradb3
    sm
  Nodes
    AdvInc Nodes
      appsrv1.mambo.net
      appsrv2.mambo.net
```

- 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 the CI Type subgroups of the CI Type Computer that is 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 such as routers, network printers, and so on.
- Not all attributes of nodes and node groups are transferred by using toposync into the RTSM. The OM node attribute ‘Control Type’ is ignored by OBM.
- All node groups are transferred to CICollections, also if they are marked in the OM responsibility matrix as hidden.

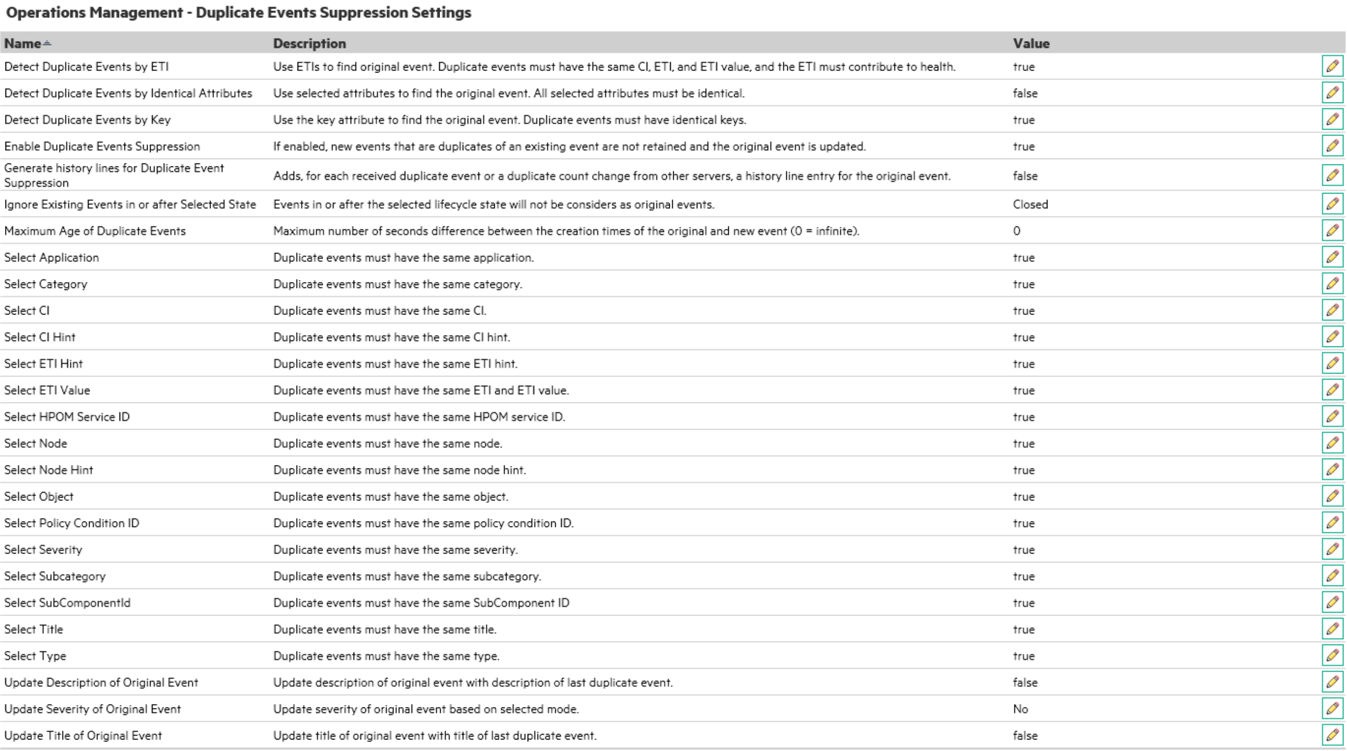
Server configuration

The following sections contain information that could be useful when configuring the server:

Configuration parameters

You can fine-tune OBM at **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 OBM. The following figure shows OBM duplicate suppression settings:



Operations Management - Duplicate Events Suppression Settings

Name▲	Description	Value	
Detect Duplicate Events by ETI	Use ETIs to find original event. Duplicate events must have the same CI, ETI, and ETI value, and the ETI must contribute to health.	true	✎
Detect Duplicate Events by Identical Attributes	Use selected attributes to find the original event. All selected attributes must be identical.	false	✎
Detect Duplicate Events by Key	Use the key attribute to find the original event. Duplicate events must have identical keys.	true	✎
Enable Duplicate Events Suppression	If enabled, new events that are duplicates of an existing event are not retained and the original event is updated.	true	✎
Generate history lines for Duplicate Event Suppression	Adds, for each received duplicate event or a duplicate count change from other servers, a history line entry for the original event.	false	✎
Ignore Existing Events in or after Selected State	Events in or after the selected lifecycle state will not be considers as original events.	Closed	✎
Maximum Age of Duplicate Events	Maximum number of seconds difference between the creation times of the original and new event (0 = infinite).	0	✎
Select Application	Duplicate events must have the same application.	true	✎
Select Category	Duplicate events must have the same category.	true	✎
Select CI	Duplicate events must have the same CI.	true	✎
Select CI Hint	Duplicate events must have the same CI hint.	true	✎
Select ETI Hint	Duplicate events must have the same ETI hint.	true	✎
Select ETI Value	Duplicate events must have the same ETI and ETI value.	true	✎
Select HPOM Service ID	Duplicate events must have the same HPOM service ID.	true	✎
Select Node	Duplicate events must have the same node.	true	✎
Select Node Hint	Duplicate events must have the same node hint.	true	✎
Select Object	Duplicate events must have the same object.	true	✎
Select Policy Condition ID	Duplicate events must have the same policy condition ID.	true	✎
Select Severity	Duplicate events must have the same severity.	true	✎
Select Subcategory	Duplicate events must have the same subcategory.	true	✎
Select SubComponentId	Duplicate events must have the same SubComponent ID	true	✎
Select Title	Duplicate events must have the same title.	true	✎
Select Type	Duplicate events must have the same type.	true	✎
Update Description of Original Event	Update description of original event with description of last duplicate event.	false	✎
Update Severity of Original Event	Update severity of original event based on selected mode.	No	✎
Update Title of Original Event	Update title of original event with title of last duplicate event.	false	✎

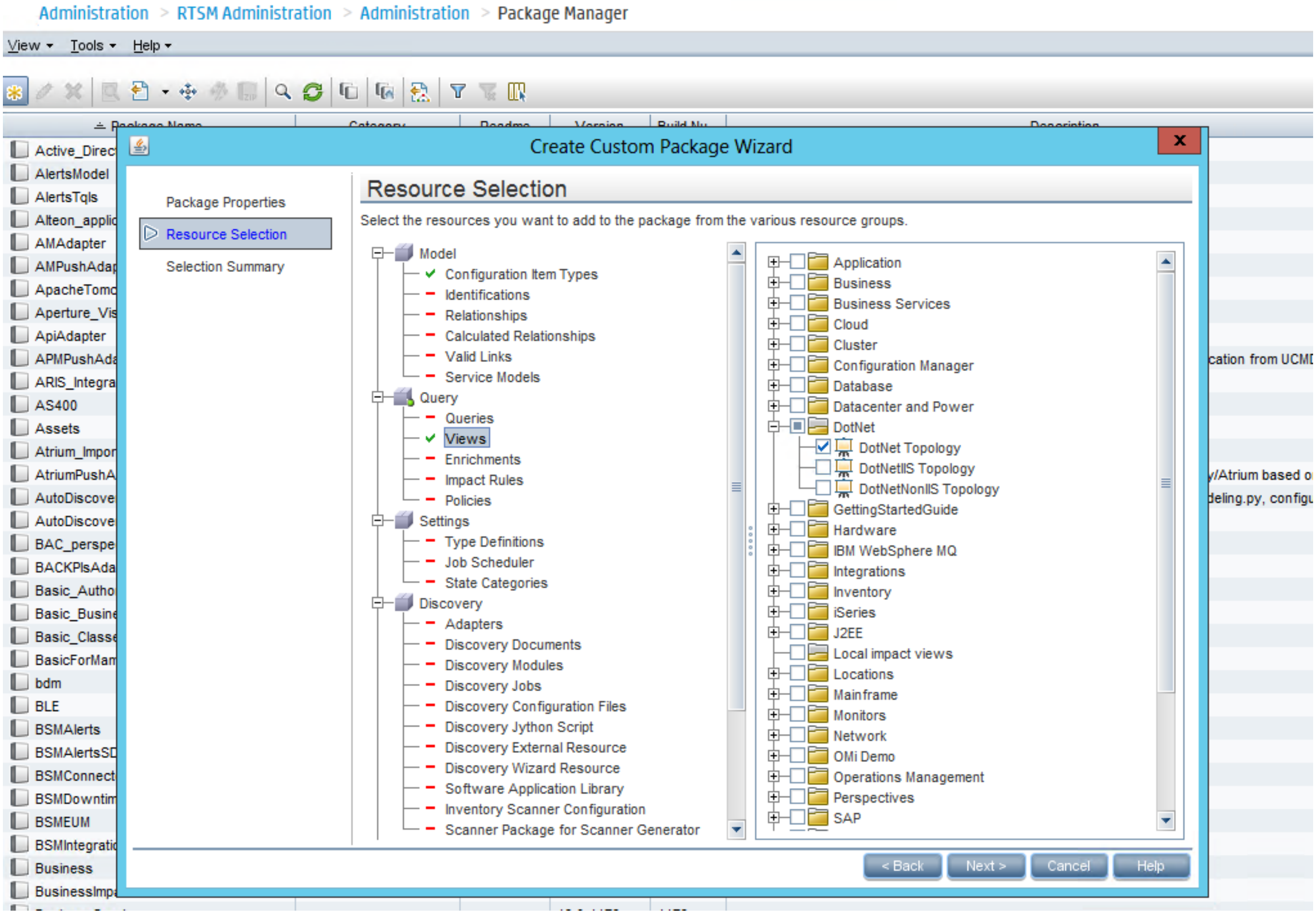
For a complete list of infrastructure settings for OBM, see the Administer section.

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.

OBM can export and import configuration by 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 cannot be currently exported and imported.

The following figure shows an example of configuration export by using **Administration > RTSM Administration > Administration > Package Manager**:



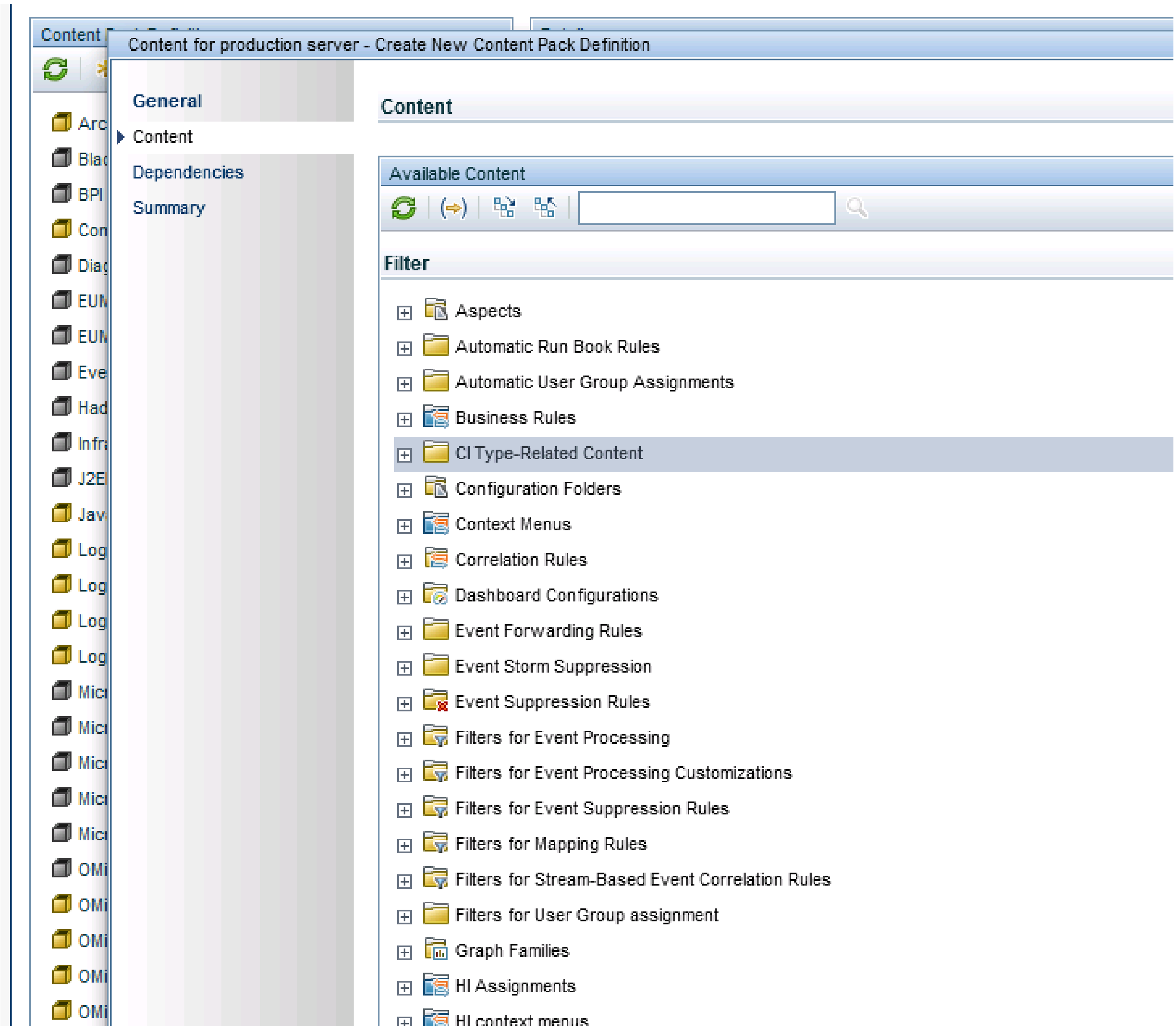
Resource Selection

Select the resources you want to add to the package from the various resource groups.

- Model
  - ✓ Configuration Item Types
  - Identifications
  - Relationships
  - Calculated Relationships
  - Valid Links
  - Service Models
- Query
  - Queries
  - ✓ Views
  - Enrichments
  - Impact Rules
  - Policies
- Settings
  - Type Definitions
  - Job Scheduler
  - State Categories
- Discovery
  - Adapters
  - Discovery Documents
  - Discovery Modules
  - Discovery Jobs
  - Discovery Configuration Files
  - Discovery Jython Script
  - Discovery External Resource
  - Discovery Wizard Resource
  - Software Application Library
  - Inventory Scanner Configuration
  - Scanner Package for Scanner Generator

- □ Application
- □ Business
- □ Business Services
- □ Cloud
- □ Cluster
- □ Configuration Manager
- □ Database
- □ Datacenter and Power
- ■ DotNet
  - ☑ DotNet Topology
  - □ DotNetIIS Topology
  - □ DotNetNonIIS Topology
- □ GettingStartedGuide
- □ Hardware
- □ IBM WebSphere MQ
- □ Integrations
- □ Inventory
- □ iSeries
- □ J2EE
- □ Local impact views
- □ Locations
- □ Mainframe
- □ Monitors
- □ Network
- □ OMi Demo
- □ Operations Management
- □ Perspectives
- □ SAP

The following figure shows an example of configuration export by using **Administration > Setup and Maintenance > Content Packs**:

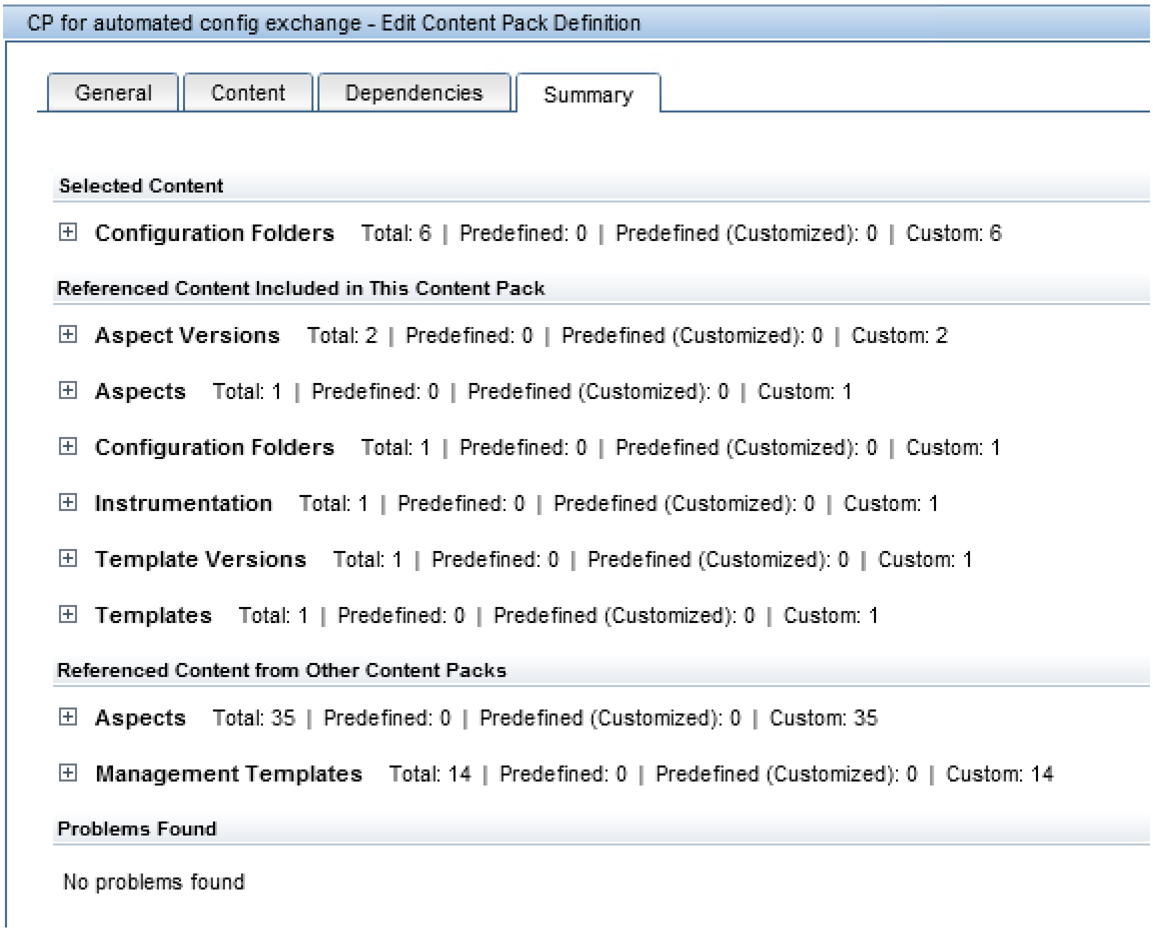


OM functionality	Equivalent in OBM
`ovpmutil`, `opccfgupld/opccfgdwn` CLI	RTSM package manager and Content Packs Content Manager CLI
Nodes and Services export or import	CI export or import by using the RTSM Synchronization job (push or pull)
Tools	Using Content Packs
Policies	Export or import of policy templates, aspects, management templates by using Content Packs
User roles	Using Content Packs
Instruction text	Policy export or import by using Content Packs
Instrumentation (file copy)	Using Content Packs
Server configuration (`ovowconfigutil -download`)	Currently it is not possible to export or import infrastructure settings
CLI or APIs for configuration exchange	For details, see Command line, API, and web services reference.

Task: How to move content from an OBM server to another OBM server

Depending on the content you want to export, use the corresponding guidelines:

- RTSM content Use the RTSM package manager to create a new package that includes RTSM artifacts that you want to export, such as new CI types, views and queries, enrichment rules, and so on. Afterward, use “export package to local directory”. For details about how to create a custom package, see *Administer* > *RTSM* > *RTSM Administer*. Connect to another OBM system and deploy the RTSM package.
- OBM content Use the content manager to create a new content pack that includes OBM artifacts, such as tools, aspects, or management templates (included artifacts, such as instrumentation and policy templates, are also automatically exported). For details about defining content packs, see the *Administer* section. Upload the exported content pack by using the content manager. To automate the exchange of management templates and aspects, including all underlying artifacts such as policy templates and instrumentation, you can do the following: For other artifacts that are not related to management templates or aspects an automated exchange is currently not possible. For these artifacts, new artifact versions created on the source system must be added to the content pack definition manually before the CP is exported.
  1. Create a new content pack.
  2. Add only configuration folders to the content pack definition. Include the configuration folders that you want to exchange.
  3. Do not change settings on the Dependencies tab. This is because the content that is already part of another content pack is not included directly, but is referenced.
  4. The content pack summary page should look similar to the following: Note Only Configuration Folders are shown under Selected Content.



CP for automated config exchange - Edit Content Pack Definition

Selected Content

⊞ Configuration Folders Total: 6 | Predefined: 0 | Predefined (Customized): 0 | Custom: 6

Referenced Content Included in This Content Pack

⊞ Aspect Versions Total: 2 | Predefined: 0 | Predefined (Customized): 0 | Custom: 2

⊞ Aspects Total: 1 | Predefined: 0 | Predefined (Customized): 0 | Custom: 1

⊞ Configuration Folders Total: 1 | Predefined: 0 | Predefined (Customized): 0 | Custom: 1

⊞ Instrumentation Total: 1 | Predefined: 0 | Predefined (Customized): 0 | Custom: 1

⊞ Template Versions Total: 1 | Predefined: 0 | Predefined (Customized): 0 | Custom: 1

⊞ Templates Total: 1 | Predefined: 0 | Predefined (Customized): 0 | Custom: 1

Referenced Content from Other Content Packs

⊞ Aspects Total: 35 | Predefined: 0 | Predefined (Customized): 0 | Custom: 35

⊞ Management Templates Total: 14 | Predefined: 0 | Predefined (Customized): 0 | Custom: 14

Problems Found

No problems found

Save the content pack.

5. Use the content-manager command-line interface to export the content pack and to import it on the target system. Content-manager CLI can connect to a remote OBM server, therefore both the export and import can be done by using the content-manager CLI of the same OBM system. This also enables scheduling of the configuration exchange with a scheduler in order to automate the configuration exchange.

- Topology synchronization packages You can edit topology synchronization packages in the file system and upload them to the OBM database by using the `opr-sdtool` utility. To exchange custom topology synchronization packages, copy the corresponding files from the file system and upload them by using the `opr-sdtool` utility. The following configuration cannot be exported or imported between OBM servers:
  - My Workspace pages
  - Auto-grant IP ranges and scripts (script code can be copied manually)
  - Infrastructure settings
- Users and user groups Unlike user roles, users and user groups cannot be exchanged by using content packs. However, it is possible to maintain users and user groups (and even user roles) by using the `opr-user` CLI. Therefore the `opr-user` CLI could be used to add users and user groups automatically on multiple OBM servers. However, it does not enable a complete export and reimport of users and user groups.

High availability and disaster recovery

The following sections contain information about the following:

High availability

Implementing a high availability configuration is setting up your OBM servers so that the service is continuous despite power outages, machine downtime, and heavy load.

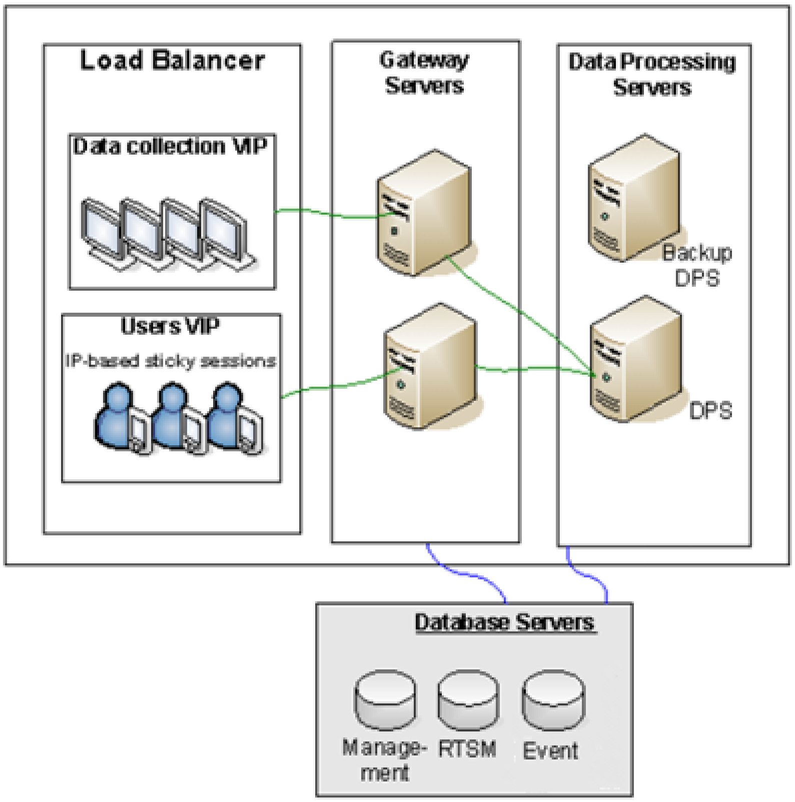
High availability for OBM is implemented in the following layers:

- Hardware infrastructure This layer includes redundant servers, networks, power supplies, and so on.
- Application This layer has the following components:
  - Load balancing This component 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 OBM 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.
    OBM provides its own failover mechanism and does not require separate cluster software.

Implementation of load balancing and failover is discussed in the *Administer* section.

High-availability of the OBM 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.

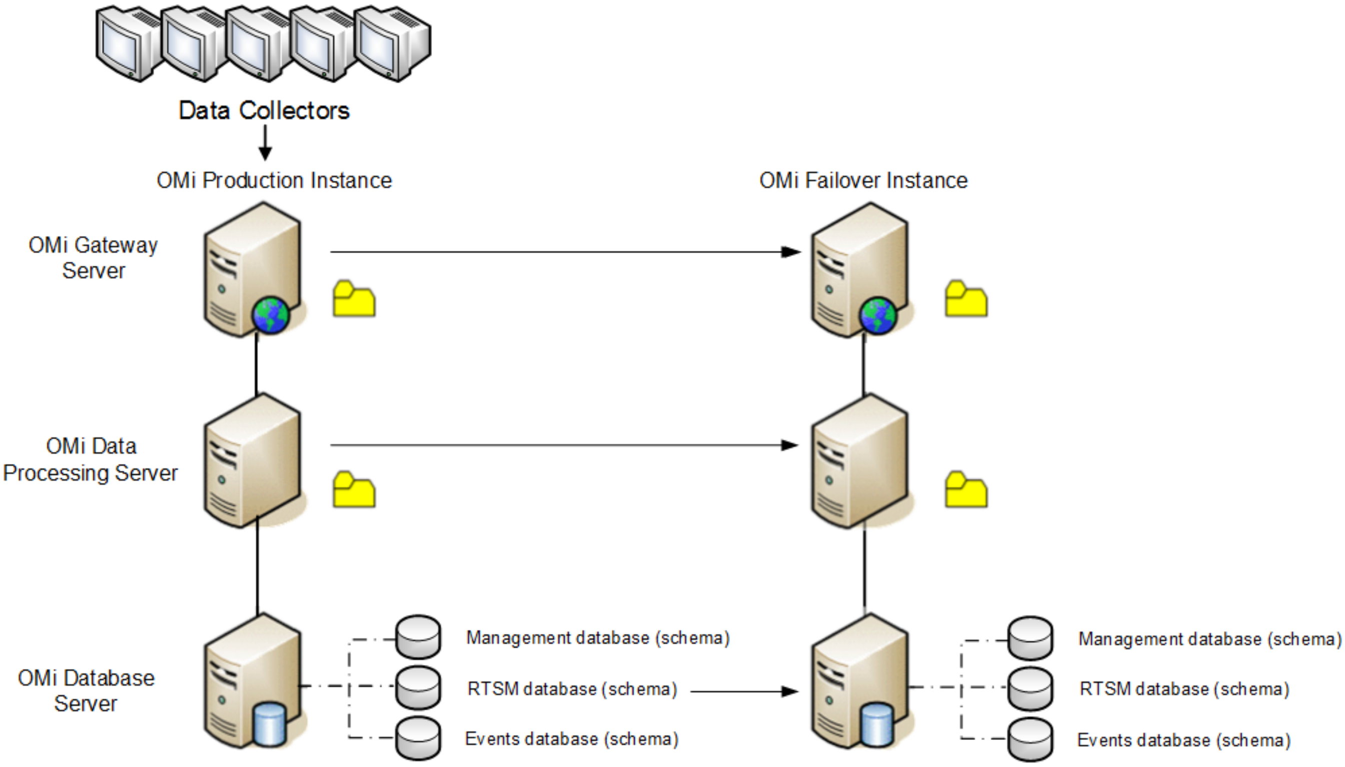


OBM supports MS SQL log file shipping (known from OM for Windows) as part of its disaster recovery process. For more information, see the section below.

OM HA Feature	Equivalent in OBM
Use of virtual IP or host name for server	Yes, by using external Load balancer
Distribute load among several OM servers (server pooling)	Distribute load among several Gateway servers
HA concept enables installing patches on one server while other server is fully operational (server pooling)	Certain patches can be installed on a gateway or a backup/non-active processing server while other gateway servers and the active processing server are running However, patches that update the communication bus or other core services may require downtime Patching the active DPS requires moving the services to the backup DPS (after patching the backup DPS), which involves some downtime because the services have to start on the backup DPS OBM 10.10 and later uses a hot-standby backup server that reduces the downtime to less than a minute

Disaster recovery

OBM supports MS SQL log shipping, Oracle Data guard, and PostgreSQL hot standby as disaster recovery techniques for databases. Other configuration files must be copied separately.



For details on disaster recovery, see Administer.

Available integrations and integration technologies

OM integrates with various applications from HPE and other vendors by using a variety of different technologies and interfaces. Several Operations Connectors are provided to integrate third-party domain managers in OBM. Additionally, all integrations that use standard operations agent policies (`opcmsg`, `opcmon`, SNMP, Logfile, and other) can be technically reused because OBM supports the same policy types.

HPE and HPE partners may provide additional integrations in the future.

“Southbound” integrations using Operations Agent policies

OBM 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 that use supported policy types can be reused in OBM. However, depending on the vendor and the license agreement, you may not be able to reuse the OM integration with OBM.

The following policy types can also be imported into Operations 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 (OBM 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 OBM, see the integration catalog.

In most cases, OBM offers identical or enhanced integrations in comparison to OM. 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 OBM
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 Bridge Analytics – Operations Bridge Manager integration 2.0
Integrating with Operations Bridge Analytics	Identical
[725] Operations Bridge Analytics – Operations Manager Data Collection integration 2.0	[704] Operations Bridge Analytics – Operations Bridge Manager 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 (OBM - NNMi) 1.0 [812] View NNMi UI components within OBM
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 (OBM-OO) 1.0 [365] Event to remediation (OBM - 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 (OBM - SM) 1.0 [810] uCMDB to OBM Downtime Integration (OBM - 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 OBM 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] Operations Connector for HPE Systems Insight Manager 2.0
Integrating with: Continuous Delivery Automation	
[683] CDA & Operations Manager for UNIX Integration 1.00	https://docs.software.hpe.com/OpsB/tutorials
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</span>

Related Topics

Integration Catalog

Auditing and license reporting

OBM and OM provide the following:

Contents

Auditing

Both OBM and OM are capable of auditing configuration and event changes. Audit entries contain information about the kind of action that took place, the user that performed this action, time when the action is performed, and the audit area related to this action.

The primary source of OBM audit log data is displayed in **Administration > Setup and Maintenance > Audit Log**. It includes the following OBM-related audit contexts:

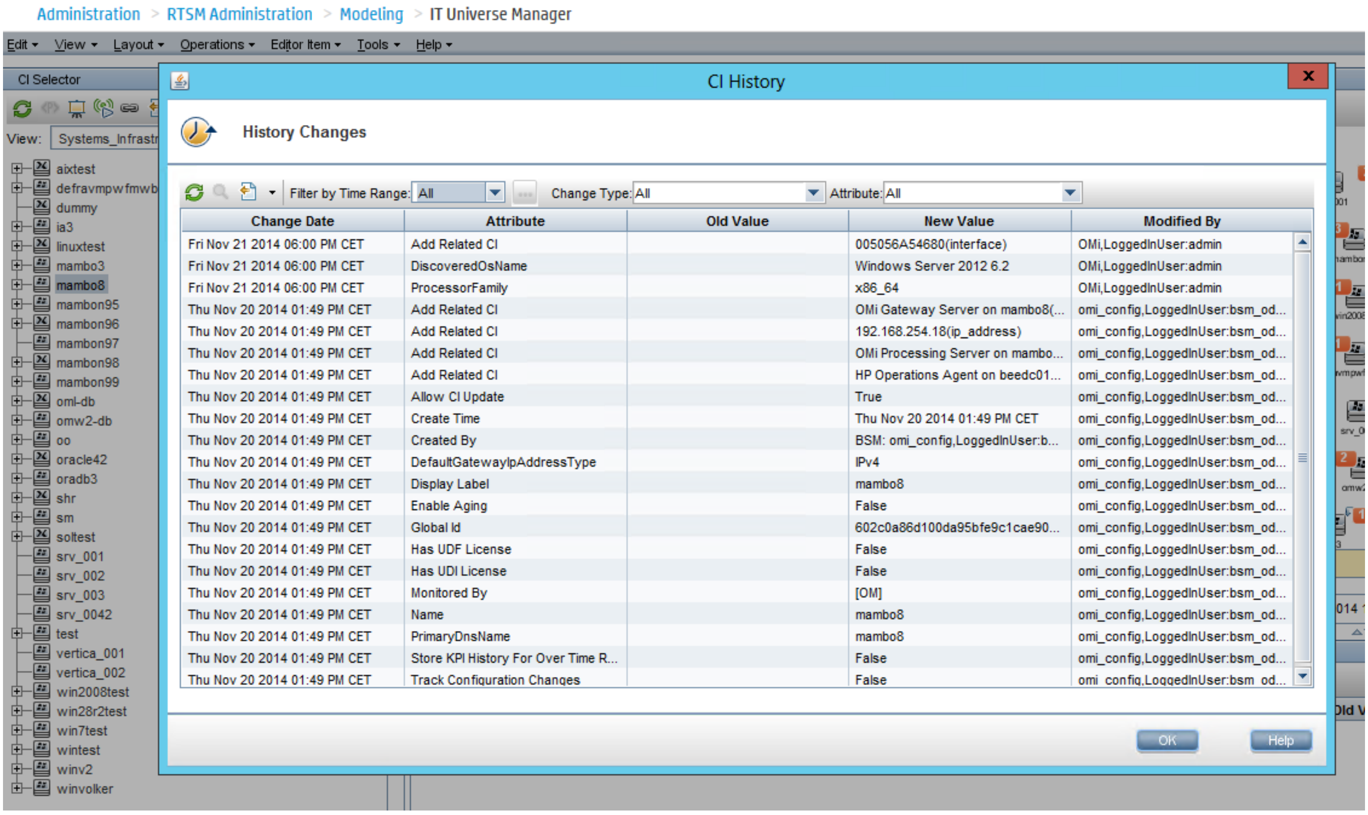
- **CI Status Alert Administration.** Displays actions related to creating alert schemes for a configuration item (CI) status alert.
- **Downtime/Event Scheduling.** Displays actions related to creating and modifying downtime and scheduled events.
- **Infrastructure Settings.** Displays actions related to modifying infrastructure settings. The result of each action is denoted as `SUCCESS` or `FAILURE`.
- **Login.** Displays actions related to users' logins and logouts. The result of each action is denoted as `SUCCESS` or `FAILURE`.
- **Notification Template Administration.** Displays actions related to modifying open ticket information, ticket settings, closed tickets, ticket templates, subscription information–notification types (locations or general messages), and recipients.
- **Operations Management.** Displays actions related to Operations Management, such as creating and modifying of content packs, event rules, and notifications.
- **Recipient Administration.** Displays actions related to modifying information about recipients of audit logs.
- **Service Health.** Displays actions related to the Service Health application.
- **Service Health Administration.** Displays the actions related to configurations made in Service Health Administration.
- **Startup/Shutdown.** Displays actions related to startups and shutdowns of OBM host systems.
- **User/Group Management.** Displays actions related to adding, modifying, and deleting users, user groups, and roles. Additionally, it displays the assignments of permissions to roles and the assignments of roles to users and user groups.
- **View Manager.** Displays actions related to KPIs, such as adding a KPI, editing a KPI, and deleting a KPI. Additionally, it displays actions related to changing the Save KPI data over time for this CI option.

For details on event changes and configuration changes that are written to the audit log, see *Administer*.

Some event audit data is available on 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 is changed.

CI change data is available in the RTSM. It provides history of a CI, such as CI creation time, set or changed attributes, added or deleted relationships, and so on.

The following figure shows an example of CI configuration changes in the RTSM IT Universe Manager:



Filter by Time Range: All   Change Type: All   Attribute: All

Change Date	Attribute	Old Value	New Value	Modified By
Fri Nov 21 2014 06:00 PM CET	Add Related CI		005056A54680(interface)	OMi,LoggedInUser:admin
Fri Nov 21 2014 06:00 PM CET	DiscoveredOsName		Windows Server 2012 6.2	OMi,LoggedInUser:admin
Fri Nov 21 2014 06:00 PM CET	ProcessorFamily		x86_64	OMi,LoggedInUser:admin
Thu Nov 20 2014 01:49 PM CET	Add Related CI		OMi Gateway Server on mambo8(...	omi_config,LoggedInUser:bsm_od...
Thu Nov 20 2014 01:49 PM CET	Add Related CI		192.168.254.18(ip_address)	omi_config,LoggedInUser:bsm_od...
Thu Nov 20 2014 01:49 PM CET	Add Related CI		OMi Processing Server on mambo...	omi_config,LoggedInUser:bsm_od...
Thu Nov 20 2014 01:49 PM CET	Add Related CI		HP Operations Agent on beedc01...	omi_config,LoggedInUser:bsm_od...
Thu Nov 20 2014 01:49 PM CET	Allow CI Update		True	omi_config,LoggedInUser:bsm_od...
Thu Nov 20 2014 01:49 PM CET	Create Time		Thu Nov 20 2014 01:49 PM CET	omi_config,LoggedInUser:bsm_od...
Thu Nov 20 2014 01:49 PM CET	Created By		BSM: omi_config,LoggedInUser:b...	omi_config,LoggedInUser:bsm_od...
Thu Nov 20 2014 01:49 PM CET	DefaultGatewayIpAddressType		IPv4	omi_config,LoggedInUser:bsm_od...
Thu Nov 20 2014 01:49 PM CET	Display Label		mambo8	omi_config,LoggedInUser:bsm_od...
Thu Nov 20 2014 01:49 PM CET	Enable Aging		False	omi_config,LoggedInUser:bsm_od...
Thu Nov 20 2014 01:49 PM CET	Global Id		602c0a86d100da95bfe9c1cae90...	omi_config,LoggedInUser:bsm_od...
Thu Nov 20 2014 01:49 PM CET	Has UDF License		False	omi_config,LoggedInUser:bsm_od...
Thu Nov 20 2014 01:49 PM CET	Has UDI License		False	omi_config,LoggedInUser:bsm_od...
Thu Nov 20 2014 01:49 PM CET	Monitored By		[OM]	omi_config,LoggedInUser:bsm_od...
Thu Nov 20 2014 01:49 PM CET	Name		mambo8	omi_config,LoggedInUser:bsm_od...
Thu Nov 20 2014 01:49 PM CET	PrimaryDnsName		mambo8	omi_config,LoggedInUser:bsm_od...
Thu Nov 20 2014 01:49 PM CET	Store KPI History For Over Time R...		False	omi_config,LoggedInUser:bsm_od...
Thu Nov 20 2014 01:49 PM CET	Track Configuration Changes		False	omi_config,LoggedInUser:bsm_od...

OM and OBM auditing functionality comparison

The following table compares event-related functionality in OM and OBM.

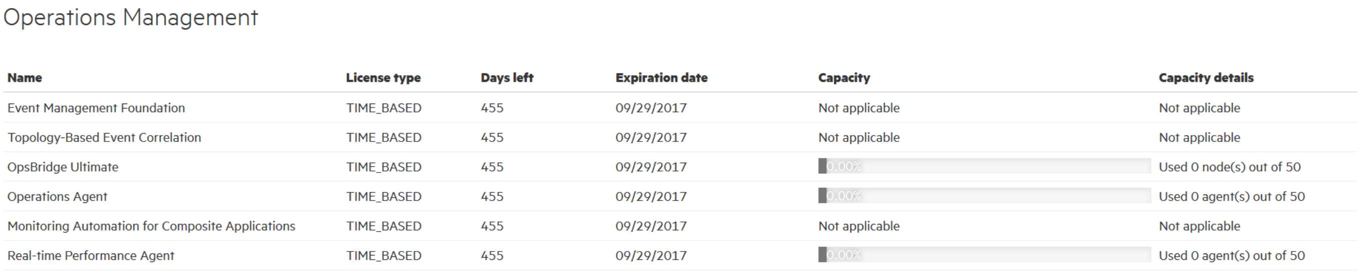
Functionality	OM for UNIX	OM for Windows	OBM
Stored format	Text file, delimited	Windows Event Log	Text file, delimited
Visualization	OM for UNIX Admin UI displays the Admin UI formatted audit log View OM audit log with a text editor	Windows Event Log	OBM GUI, with the ability to filter by context, user 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	OBM administrator An operating system administrator must change log4j settings
Restrict access to audit data	File permissions	Standard Windows Event Log security	OBM 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 **Administration > Setup and Maintenance > Infrastructure Settings**, **Operations Management** offers the following settings for the OBM audit: Configuration and All (both configuration and event changes)

License reporting

In OBM, you can view the current license details and usage in **Administration > Setup and Maintenance > License Management**. You can also query the installed capacity by using the JMX console.

The following figure shows an example of the OBM license usage:



Operations Management

Name	License type	Days left	Expiration date	Capacity	Capacity details
Event Management Foundation	TIME_BASED	455	09/29/2017	Not applicable	Not applicable
Topology-Based Event Correlation	TIME_BASED	455	09/29/2017	Not applicable	Not applicable
OpsBridge Ultimate	TIME_BASED	455	09/29/2017	0.00%	Used 0 node(s) out of 50
Operations Agent	TIME_BASED	455	09/29/2017	0.00%	Used 0 agent(s) out of 50
Monitoring Automation for Composite Applications	TIME_BASED	455	09/29/2017	Not applicable	Not applicable
Real-time Performance Agent	TIME_BASED	455	09/29/2017	0.00%	Used 0 agent(s) out of 50

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.

Calculate license consumption

The following are licensing models in OBM for calculating license consumption:

- Old licensing model OBM reports consumption levels of the following types of licenses: Agent, Management Pack, and Target Connector. The Operations Agent reports its license requirements to the primary manager (OM or OBM) on a daily basis. This includes both agent license and its configuration with a management pack. This data is stored in the OM or OBM 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 Technical White Paper*. OBM calculates Target Connector usage in the same way on a daily basis. However, no such commands or utilities are available in OBM. The Agent, Management Pack, and Target Connector data is stored in the OBM database. It is not always possible to programmatically determine whether 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, a router, a UPS, or a 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 functionality does not exist in OBM.
- New Operations Bridge licensing model OBM reports consumption levels of the following types of licenses: Operations Bridge nodes, Operations Agents (System Collector) and Management Packs. The Operations Agent reports its license requirements to the primary manager (OM or OBM) on a daily basis.
  This includes both agent license and its configuration with a management pack. This data is stored in the OM or OBM database.

OM and OBM license reporting comparison

The following table compares license reports in OM and OBM.

OM	OBM
The "OM Feature License Report" shows the license status of each OM license type (OM Server, Agents, Target Connectors, and SPIs) It includes the number of installed licenses, the number of required licenses, and a license compliance status	For the supported license types (Operations Bridge Express/Premium/Ultimate Nodes, OBM Server, Operations Agent, Target Connector, Management Pack, and so on) 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, and 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	The managed node reports this data to the OBM server and the data is stored in the OBM database, but 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 send an email ASCII license report if it exceeds a configured severity threshold that is checked on a daily basis.

OBM does not provide email notification of license compliance and does not generate an event for license violations.

Preconfigured reports

OM provides preconfigured reports in addition to those provided in Reporter and Operations Bridge Reporter. These reports are mostly focused on OM configuration and are designed to be used by an OM administrator. Similar reports are available in OBM Monitoring Automation.

OBM 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 that are 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 OBM database, this is not supported in OBM, since the OBM database schema is not published and it may change in a future product version.

The following section contain the comparison of OM and OBM preconfigured reports.

OM and OBM 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`, and `opcservice` for OM for UNIX, or `ovownodeutil`, `ovowmsggrouputil.vbs`, and `ovdbstat` for OM for Windows.

License reports and audit reports are described separately within their respective sections.

Report Area	OM for UNIX	OM for Windows	OBM

Nodes, Node Groups, and CIs	Lists nodes with node type and HBP settings Lists nodes that are 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 settings, node group membership, policy, and policy group assignments List node groups and node membership Detailed report for a selected node group that lists the message group/operator assignments and policy/policy group assignments Lists nodes that are not members of any node group Lists nodes that have no policies assigned to them Lists nodes that are not part of any user’s responsibility Lists node groups that have no policies assigned to them Lists node groups that are not part of any user’s responsibility	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 (including the aspect name or version, enabled or disabled, parent object, and other information) Comparison report compares the monitoring configuration of a selected CI with the monitoring configuration of all CIs of the same type in the current view It lists the equal assignments, additional assignments, and missing assignments User-defined view-based RTSM reports of selected CI attributes Output to CSV, XLS, PDF, XML, and Browser
Events	Reports the number of active messages per message group Reports a list of active, history, or pending messages for an operator Exports selected messages to a text file or a drag -and-drop of data to another application, such as Excel	Save selected events to a file (TXT, CSV)	Export selected events to a file (XLSX, XLS, CSV)
Users	Lists operators including a summary of permissions Per-operator detailed report lists the permissions assigned either directly or by using the profiles	None	None
User Profiles	Lists profiles Lists permissions configured for a specific profile	None	None

Policies, Policy Groups	Lists all policy groups and policies	Lists policies that are in use and the installed nodes	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 installed nodes Lists agent component versions and the installed nodes	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 responsibility	None	None

Related Topics

Auditing and license reporting

Command Line, API, and web Services reference

The following sections contain tables with various tasks and their command-line, API, and web sevices references in OM for UNIX, OM for Windows, and OBM:

User tasks

User tasks are outlined in the following table.

Event handling and tool execution

Functionality

OM for UNIX

OM for Windows

OBM rowspan='2'|

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 by 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 rowspan='2'|

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)

colspan='2'|

Web services

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

rowspan='2'|

Tool execution

API

Application API to execute Tools

rowspan='2'|

CLI

`opr-agt -cmd`

Tool Web Service:

- Launches a tool
- Requests a list of tools that can be applied to a specific CI, or which are applicable in the context of an event
- Cancels a tool execution

`opr-tool`

`opr-ci-list`

Retrieves a CI ID for use with `opr-tool`

Web services

Action Web Service:

- Runs arbitrary strings
- Runs commands on an Operations Agent
- Command types: executable (default), Perl script, VBScript, JavaScript, or Windows Scripting Host script
- Asynchronous requests or result handling
- REST-based
- Triggers a command on multiple hosts
- Polls for requests with execution context ID
- Requests can be routed to another server when required
- Requests can be canceled

colspan='2'|

Web services

- Launch a tool within the operator’s responsibility
- Run arbitrary strings and run commands on an Operations Agent
- Commands types: executable, Perl script, VBScript, JavaScript, or Windows Scripting Host script
- Asynchronous requests or result handling
- WSMAN calls and payload in the SOAP format
- Trigger predefined tool calls
- Use a "subscribe" call to wait on multiple requests
- Call list for open requests

Administration tasks

Administration tasks are outlined in the following tables.

Events

Functionality	OM for UNIX	OM for Windows	OBM

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 database
			Uploading of archived events is not supported
			
			`opr-export-events[.bat|.sh]` and `opr-import-events[.bat|.sh]` support exporting and importing of all or only selected events in any lifecycle state

Delete queued event	CLI `opcdelmsgs`		

Agents

Functionality	OM for UNIX	OM for Windows	OBM
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 of 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 and set primary manager
		• start and stop the status of agent
		• get agent version
		• get and set config variable
			CLI
			`ovrc`,
			`opr-agt[.bat|.sh]`
			Exceptions:
			No `-cleanstart`
			To perform `opcagt –cleanstart`, use an alternative remote command, such as `ovdeploy`
			`ovdeploy`
			`ovpolicy`
			`java –jar jcodautil.jar`
			`ovconfpar`

Users

Functionality	OM for UNIX	OM for Windows	OBM
User/Profile Management	CLI `opccfguser` API User configuration API - create, change, delete, list users, change user responsibilities and (de)assign tools/tool groups User profile configuration API - create, change, delete, list profiles, and (de)assign tools, tool groups, responsibilities, and 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	OBM
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, and (de)assign tools to tool groups	CLI `ovowtoolutil`	CLI `ContentManager[.bat|.sh]` exports/imports content packs including tools Content pack definition is done by using the GUI
Message groups	CLI `opcmsggrp` API Message group configuration API - create, change, delete, and 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 through 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, and (de)assign nodes to node groups
	
	Node hierarchy configuration API - create, change, delete, list node hierarchies and layout groups, get or move nodes and layout groups
		CLI
		`ovownodeutil`
			CLI
			`opr-node`
			Other Automation
			Views and CiCollections– UCMDB API or enrichment rules to create relationships
			UCMDB API to query or update CIs
			OBM auto-assignment rules manage dynamic policy assignment or deployment

Policies/Policy groups	CLI
	`opcpolicy`
	`opctempl`
	
	API
	Policy configuration API - get, set and change policies or 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
			`opr-config-ws-tool` (de)assigns and lists management templates and aspects, and lists deployment jobs for management templates and aspects
			`opr-ci-list` retrieves a CI ID for use with `opr-config-ws-tool`
			
			Web Services
			Monitoring Automation web services:
			• List management templates and aspects
			• List deployment jobs created as a result of management template or aspect assignments
			• Get status and parameter information for an assigned management template or an aspect
			• List, create, update, and delete management template or aspect assignments
			
			Other automation
			OBM auto-assignment rules manage dynamic policy assignment or deployment

Policy types	CLI `opcpoltype` API Policy type APIs - create, change, delete, and list policy types		
Change user name and password for Measurement Threshold/Scheduled Task/WMI policies		CLI `ovpmpwutil`	

Message regrouping	API Message regroup condition configuration API - create, change, move, delete, and list message regroup conditions	Not applicable	Other Automation Not applicable Can change message groups programmatically by using EPI Groovy scripts, TBEA, SBEC, and 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, and policy groups		

General administration

Functionality	OM for UNIX	OM for Windows	OBM
Downtime handling	CLI opccfgout	CLI ovownodeutil ovowserviceutil	Web Services REST-based web service for downtime enables you to retrieve, update, create, and delete downtimes CLI opr-downtime Enables you to retrieve, create, and delete downtimes
Node name or IP changes	CLI opcchgaddr opc_node_change.pl		API UCMDB APIs (Java and Web Services) Other Automation Managed by the agent that send ASSD information, which results with 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 or imports content packs Content pack definition is done by using the GUI Other Automation Use the OBM GUI to create a scheduled sync of CIs or relationships between the RTSM(s) and the UCMDB
Server cloning	CLI om_server_switch.sh		
Server processes: status, stop, and start	CLI opcsv, ovc	CLI vpstat, ovc	CLI run_hpbsm (Linux), SupervisorStop.bat and SupervisorStart.bat (Windows), opr-support-utils[.bat|.sh], and ovc
Self-monitoring: server and node	CLI opchealth opchbp opchc.sh		Other Automation Use OBM 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, because data is not created in files, therefore 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
			`mib2policy`
			`BBCTrustServer[.bat|.sh]`

Performance Manager

Functionality	OM for UNIX	OM for Windows	OBM
Start, Stop, License	CLI `ovpm`	CLI `ovpm`	Performance Dashboard is part of OBM, therefore separate user and node management is not required
Generate graphs	CLI `ovpmbatch`	CLI `ovpmbatch`	

Troubleshooting

Troubleshooting in OM and OBM depends on understanding the following:

- 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

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.

If you could not solve the problem this way and you log a case with HPE Support, HPE typically requests the output of `itochecker` (OM for UNIX) or `ovsuptinfo` (OM for Windows). For OBM, 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`

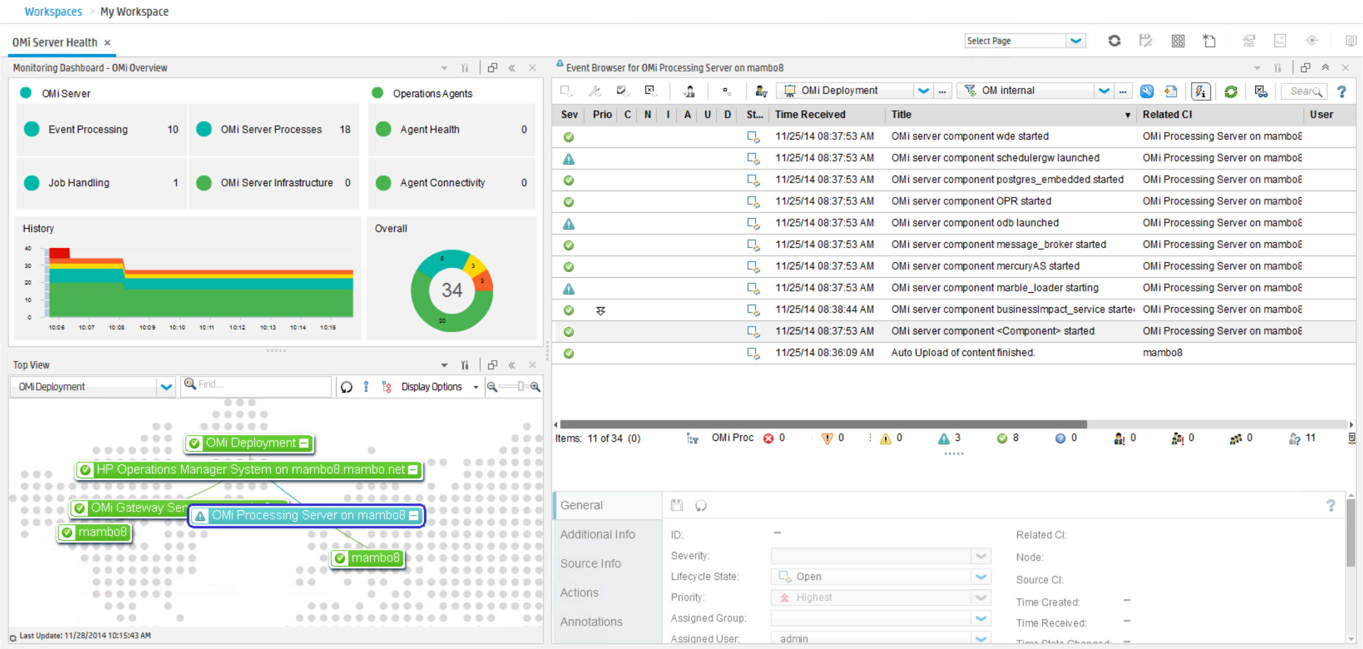
The following sections may be useful for troubleshooting purposes:

Contents

Self-monitoring

Operations Agents that are automatically installed on all OBM servers are used to detect OBM server problems. OBM server problems reported in OBM log files are detected and reported as events to OBM. The OBM Server Health page shows these OBM server events, as well as all the events related to Operations Agent health check and communication problems.

For some problems that affect the event processing (and therefore also the display of these problems on the OBM Server health page), notifications can be send by the Operations Agent to a dedicated user. For more details, see the OMi Help.



Workspaces > My Workspace

OMi Server Health

Monitoring Dashboard - OMi Overview

OMi Server		Operations Agents	
Event Processing	10	Agent Health	0
Job Handling	1	Agent Connectivity	0
OMi Server Processes	18		
OMi Server Infrastructure	0		

Last Update: 11/28/2014 10:15:43 AM

Select Page

Event Browser for OMi Processing Server on mambo8

OMi Deployment | OM internal

Sev	Prio	C	N	I	A	U	D	St...	Time Received	Title	Related CI	User
✓									11/25/14 08:37:53 AM	OMi server component wde started	OMi Processing Server on mambo8	
▲									11/25/14 08:37:53 AM	OMi server component schedulergw launched	OMi Processing Server on mambo8	
✓									11/25/14 08:37:53 AM	OMi server component postgres_embedded started	OMi Processing Server on mambo8	
✓									11/25/14 08:37:53 AM	OMi server component OPR started	OMi Processing Server on mambo8	
▲									11/25/14 08:37:53 AM	OMi server component odb launched	OMi Processing Server on mambo8	
✓									11/25/14 08:37:53 AM	OMi server component message_broker started	OMi Processing Server on mambo8	
✓									11/25/14 08:37:53 AM	OMi server component mercuryAS started	OMi Processing Server on mambo8	
▲									11/25/14 08:37:53 AM	OMi server component marble_loader starting	OMi Processing Server on mambo8	
✓	⇊								11/25/14 08:38:44 AM	OMi server component businessImpact_service starte	OMi Processing Server on mambo8	
✓									11/25/14 08:37:53 AM	OMi server component <Component> started	OMi Processing Server on mambo8	
✓									11/25/14 08:36:09 AM	Auto Upload of content finished.	mambo8	

Items: 11 of 34 (0) OMi Proc 0 0 0 3 8 0 0 0 0 11

General
Additional Info
Source Info
Actions
Annotations

ID: –
Severity:
Lifecycle State: Open
Priority: Highest
Assigned Group:
Assigned User: admin

Related CI:
Node:
Source CI:
Time Created: –
Time Received: –
Time State Changed: –

Architecture

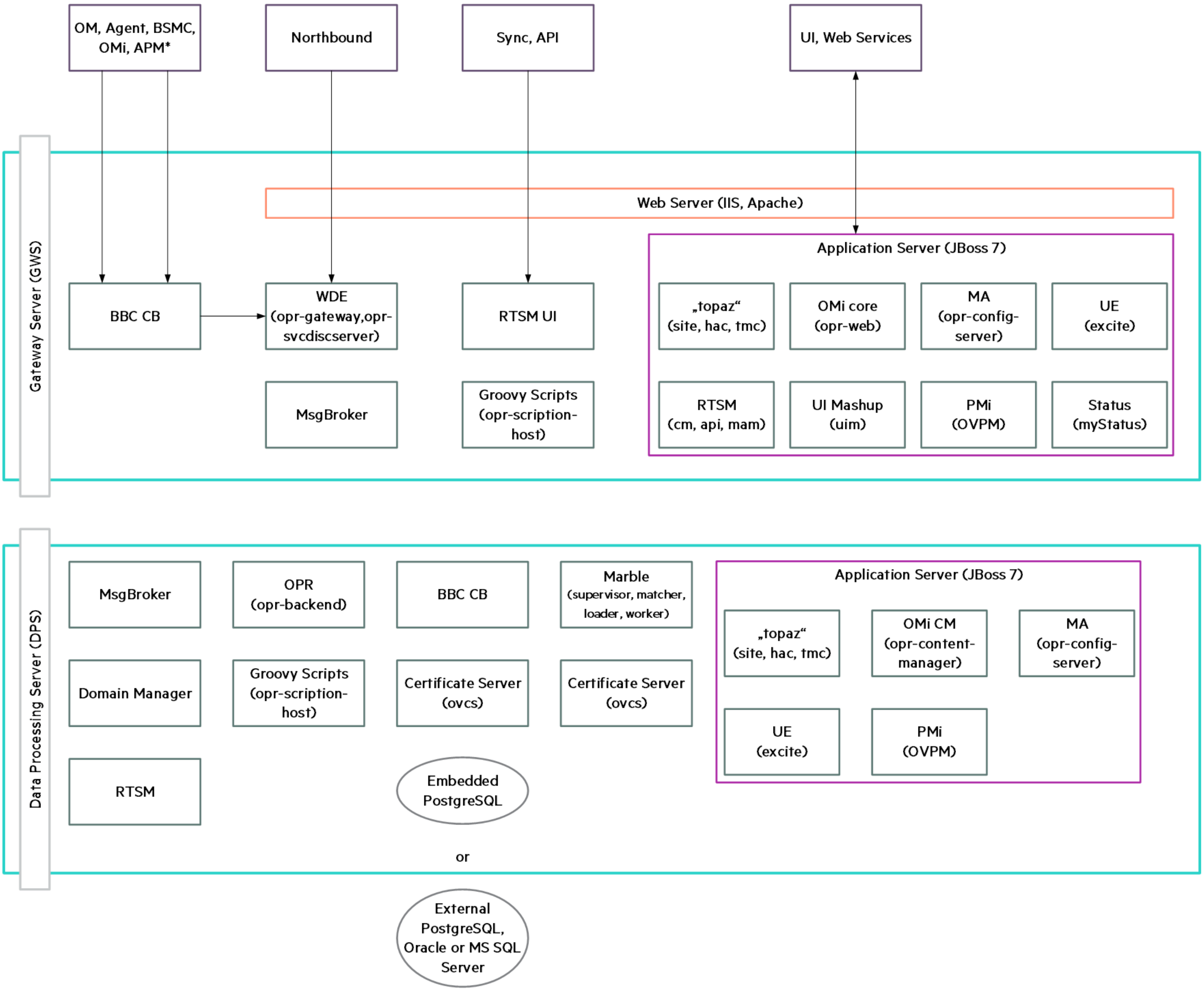
The OBM server is comprised of a Gateway Server and Data Processing Server which are predominantly Java-based, with a JMS bus to pass events between the servers. Client web browsers connect to the web server that is running on the Gateway Server. For high availability, OBM supports multiple Gateway Servers through a Load Balancer, and an additional Data Processing Server to fail over on the backend.

On the contrary, 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.

Operations Agents communicate with OM and OBM in the same way (HTTPS-based). Manager-to-manager event communication among OM and OBM servers is the same as well.

Depending on the integrations' type, OBM behaves as follows:

- For southbound integrations, OBM can get events, metrics, and topology from Operations Connectors and from SiteScope.
- For northbound integrations, OBM leverages web services and scripting. The details are available in Develop.


OM, Agent, BSMC, OMi, APM*
Northbound
Sync, API
UI, Web Services
Gateway Server (GWS)
Web Server (IIS, Apache)
Application Server (JBoss 7)
BBC CB
WDE (opr-gateway,opr-svcdiscserver)
RTSM UI
„topaz“ (site, hac, tmc)
OMi core (opr-web)
MA (opr-config-server)
UE (excite)
MsgBroker
Groovy Scripts (opr-scription-host)
RTSM (cm, api, mam)
UI Mashup (uim)
PMi (OVPM)
Status (myStatus)
Data Processing Server (DPS)
MsgBroker
OPR (opr-backend)
BBC CB
Marble (supervisor, matcher, loader, worker)
Application Server (JBoss 7)
„topaz“ (site, hac, tmc)
OMi CM (opr-content-manager)
MA (opr-config-server)
Domain Manager
Groovy Scripts (opr-scription-host)
Certificate Server (ovcs)
Certificate Server (ovcs)
UE (excite)
PMi (OVPM)
RTSM
Embedded PostgreSQL
or
External PostgreSQL, Oracle or MS SQL Server

Status check

In OBM, you can check the overall status of the server by running one of the following methods on the Gateway Server and Data Processing Server:

- `<OMi_HOME>/tools/bsmstatus/bsmstatus[.bat.sh]`. On Windows, this is the same as **Start > Programs > HPE Operations Manager i > Administration > Operations Manager i Status**.
- https://OMiSERVER:8080/myStatus/myStatus#$filename%7C (JMX log-in 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

OBM 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 more details (including log file management and debugging), see Administer.

Gateway Server

Location and Name	Server	Purpose	Debug
`<OMi_HOME>\log\wde\ opr-gateway.log`	GW	OBM Gateway processing To check whether a new or a changed event is received by OBM	`<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 that arrive 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 by using the OBM GUI at **Administration > Setup and Maintenance > Infrastructure Settings** (select the **Operations Management** context and set 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-webapp.log`	GW	Log file for OBM 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	Log-in attempts	`<OMi_HOME>\conf\core\Tools\ log4j\jboss\topaz.properties`
`<OMi_HOME>\log\wde\ opr-svcdiscserver.log`	GW	Mapping/filtering part of OBM dynamic topology synchronization	`<OMi_HOME>\conf\core\Tools\ log4j\wde\ opr-svcdiscserver.properties`

`<OvDataDir>\ shared\server\ log\OvSvcDiscServer.log`	GW	Receiving part of OBM 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`

`<OvDataDir>\ shared\server\ log\ovpmtrace.0.txt`	GW	Performance Dashboard trace file	Enable tracing in the OBM GUI by navigating to **Administration > Setup and Maintenance > Infrastructure Settings** (select the Performance Dashboard context and set 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	OBM backend process To check whether a new or changed event is processed by OBM	<OMi_HOME>\conf\core\Tools\ log4j\opr-backend\ opr-backend.properties
<OMi_HOME>\log\ opr-backend\ opr-flowtrace-backend.log	DPS	Flowtrace log entries for the events that arrive from the OBM 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 by using the OBM GUI at **Administration > Setup and Maintenance > Infrastructure Settings** (select the **Operations Management** context and set 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-topologysync\ opr-topologysync.log	DPS	Log entries for the OBM topology synchronization application	<OMi_HOME>\conf\core\Tools\ log4j\opr-topologysync\ opr-topologysync.properties
<OMi_HOME>\log\ opr-backend_boot.log	DPS	Start-up log entries for the OBM backend process	
<OMi_HOME>\log\ opr-backend_shutdown.log	DPS	Shutdown messages for the OBM backend process	
<OMi_HOME>\log\ opr-backend\ opr-ciresolver.log	DPS	OBM 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 configuration wizard, or running `opr-mp-installer.bat/sh`)
`<OMi_HOME>\log\ <ServiceName>_boot.log`	DPS/GW	Restart log files for all OBM services
`<OMi_HOME>\log\opr-scripting-host_boot.log`	DPS/GW	EPI restart
`<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) start-up log file
`<OMi_HOME>\log\wde`	GW	Tomcat (wde) log files
`<OvDataDir>\log\System.txt`	DPS/GW	LCore and Operations 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 Operations 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

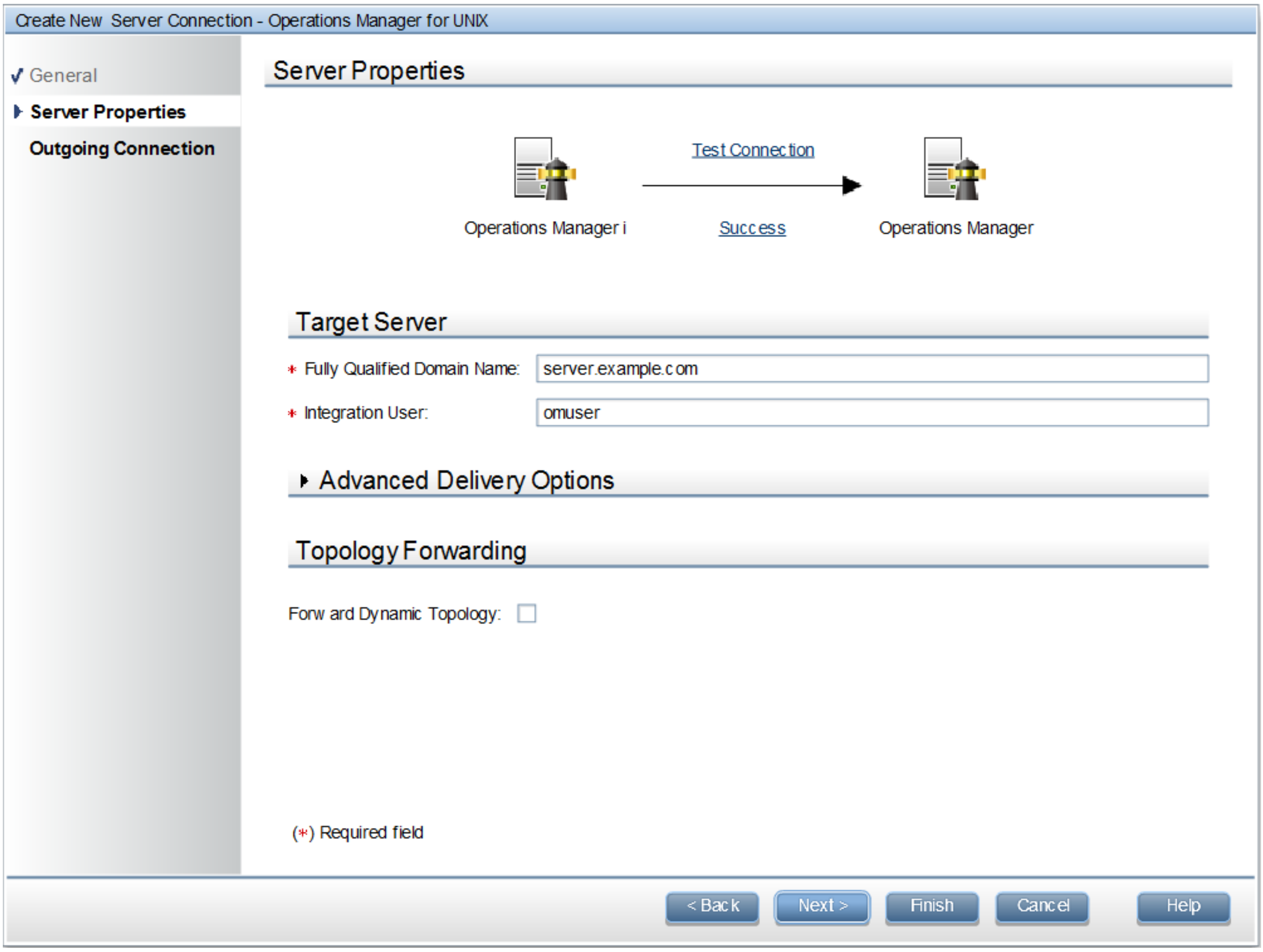
To debug problems with the flex-based user interface, you can enable logging in the GUI. For details about tracing and logging OBM user interfaces, see the *Administer* section.

OBM uses the same communication technology as OM to interact with the agent and other OM or OBM servers. Therefore some of the data is logged to `<OvDataDir>/log` and `<OvDataDir>/shared/server/log` directories, as it is in OM. Tracing is configured in the same way as in OM, that is, the OM-style (`ovconfchg`) and the newer HPE-style (`ovtrccfg`, `ovtrcmon`) in OM.

Tools

Depending of the problem that you have, use the corresponding guidelines:

- Operations Agent communicationThe tools for troubleshooting communication with the Operations Agent are similar in OBM 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 both OBM and OM.In OM, the `oprcragt` command is used to perform a range of tasks on one or multiple managed nodes. OBM provides `ovrc`, that can perform start, restart, stop, and status actions on remote managed nodes the same way as `oprcragt` does in OM. For example:ovrc -ovrg server -host server.example.com -status ovrc -ovrg server -host server.example.com -start opcmsgi 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 Operations Agents” -username admin Troubleshooting access to agent-based performance data in OBM 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 OBM 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 the following: <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 is logged. This functionality is not available in OBM.
- Event processing In OBM, event processing is implemented differently than in OM, and therefore 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. OBM 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. Because you can make changes to configuration and data, it is important to be careful when using the JMX console. For details about the JMX console, see the *Administer* section. 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, you can generate an event on demand in OBM. 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.
- Connected server communication In OBM, you can configure connected servers, such as OBM, APM, OM, SiteScope, Operations Connector, External Event Processing, and ArcSight Logger. With each connected server, you can test basic connectivity. In 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).



Create New Server Connection - Operations Manager for UNIX

Server Properties

Target Server

* Fully Qualified Domain Name: server.example.com

* Integration User: omuser

Advanced Delivery Options

Topology Forwarding

Forw ard Dynamic Topology: □

(*) Required field

- Topology synchronization To troubleshoot topology synchronization from OM to OBM, you can capture detailed data that the OBM server receives. In OBM, navigate to **Administration > Setup and Maintenance > Infrastructure Settings**, select the **Operations Management** context, and then set **Dump Data** to true.