MICRO FOCUS® | **Documentation**

Operations Bridge Manager
10.64

Get started

Operations Bridge Manager (OBM) is the core component of the Operations Bridge Suite and the only product that dynamically and automatically discovers and correlates data, event topology, and metrics. As part of the Operations Bridge, it consolidates all IT infrastructure monitoring in a central event console, and relates the events to the IT services that depend on that infrastructure.

OBM combines events from Application Management components with events from System and Network products, such as OM and Network Node Manager i. This enables you to keep track of all the events that occur in your monitored environment.

Watch the video below for a general introduction about how OBM, as part of the Operations Bridge, can help you to see through the flare of all your data via a single pane of glass:

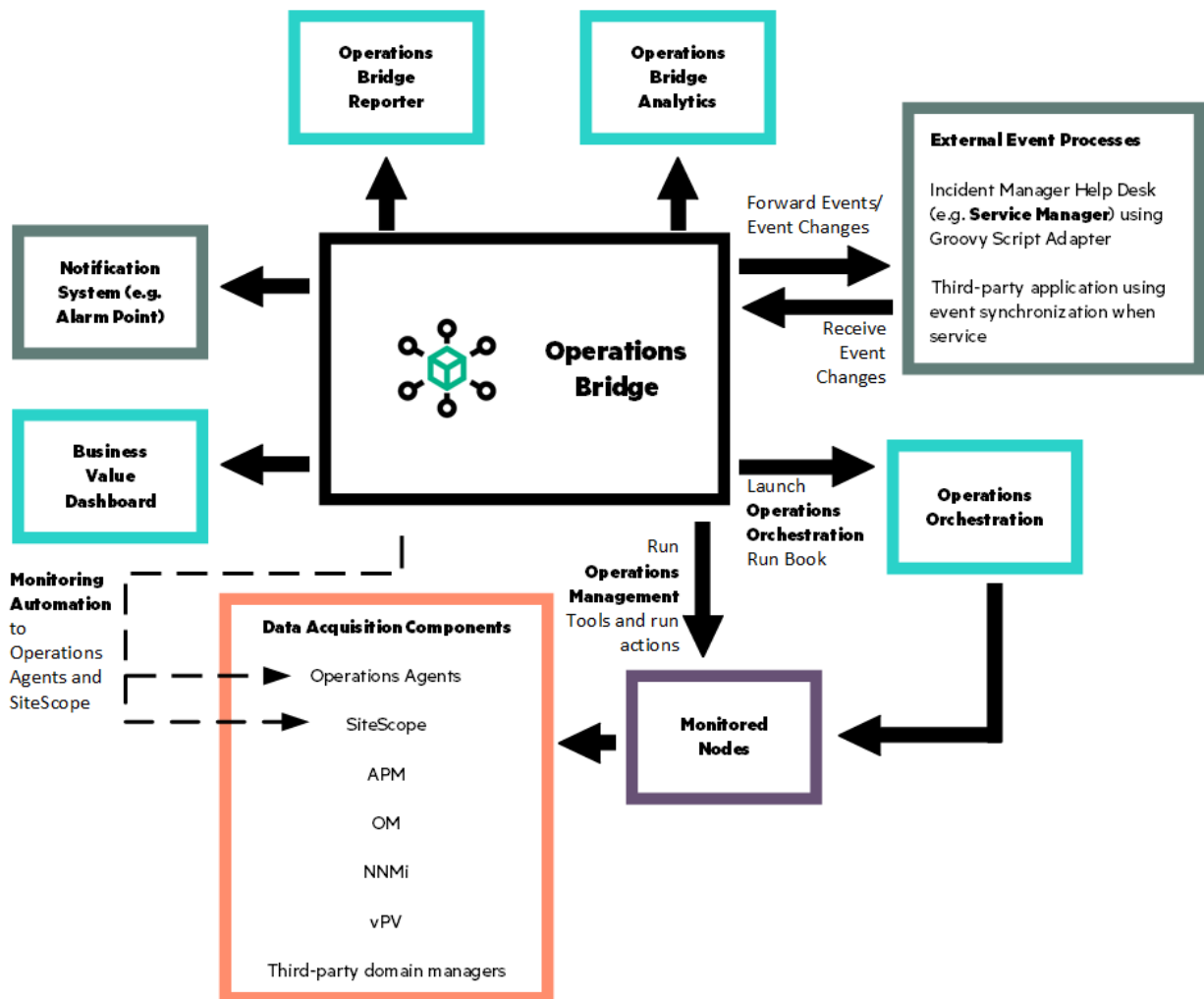https://youtu.be/P5bg3k1F7A4

Related Topics

Key concepts
Additional resources

Key concepts

OBM as the operations bridge provides a single center of control for your IT operations.

All event and performance management data originating from servers, networks, applications, storage, and other IT silos in your infrastructure is consolidated into a single event stream in an advanced, central event console. The console displays monitoring alerts to the appropriate team of operators.

You can quickly identify, monitor, troubleshoot, report on, and resolve problems in your distributed IT environment. These abilities make it possible for you to improve the performance and availability of the infrastructure and services in your monitored environment, adding to the efficiency and productivity of your business. OBM helps you locate and solve event-related issues before business service quality degrades. It offers the tools that help operators solve problems without involving a subject matter expert. This frees subject matter

experts to focus on strategic activities.

Key concepts

The following key concepts are important to understand before you start working with OBM:

- Consolidated Event and Performance Management
- Structured Problem Solving
- Performance Dashboard and Performance Engine
- Management Packs
- Scalable Architecture with Multiple Servers
- Monitoring Automation

Data Acquisition from Multiple Sources

The events, regardless of where they originate, are processed and managed in a unified manner. Examples of event sources include:

- Operations Agents configured by OBM
- Operations Manager for UNIX
- Operations Manager for Windows
- Network Node Manager i
- SiteScope
- Systems Insight Manager
- Third-party management software, normally used to monitor specific environments or special needs not monitored by other solution components, such as Microsoft Systems Center Operations Manager or Oracle Enterprise Manager. Connectors to integrate third-party management software, such as Microsoft SCOM, Nagios, and IBM Tivoli into OBM are available from Marketplace.

Related Topics

Structured Problem Solving
Performance Dashboard and Performance Engine
Management Packs
Scalable Architecture with Multiple Servers
Monitoring Automation
Marketplace

<comments voting="Plus" />

Consolidated Event and Performance Management

In OBM, events from multiple sources are consolidated into a centralized console. 'Perspectives' provide operators with different levels of information about the events they are responsible for. For example, general event handling is done in the Event Perspective, while the Health Perspective provides additional service health-related information about the events. These perspectives are centered around the Event Browser.

Event information

Events report important occurrences in the managed IT environment. They are generated by domain managers, forwarded to OBM, and then mapped to related configuration items (CIs) in the RTSM. These events are assigned to operators for resolution. In the Event Browser, operators can see a complete overview of all active events that need to be worked on. They can see such things as the event severity, the type and category of event, the source of the event, the time and location of the event, and the affected configuration item.

Events pass through a "lifecycle," which is an informative way to display and monitor the status of an event. An operator's workflow is based around the lifecycle of an event. The lifecycle state of an event represents the progress of the investigation into the problem that caused the event. An operator assigned to an event opens an investigation and works on finding a solution to the event's underlying problem. Experts can then assess the proposed solution, verify that it solves the problem that caused the event, and close the event, which completes the lifecycle.

Operators can configure the Event Browser to suit the requirements of their typical workflows. The contents of the Event Browser are filtered according to the selected view or configuration item. Operators can configure new filters or modify existing filters, according to their needs, to change the information displayed. Filtering the Event Browser content helps operators focus on the most useful information, for example, to identify the highest priority events and to determine which of these events should be worked on first to minimize their impact on business services. You can also configure users and groups so that they can see only the events filtered by views associated with that user or group.

You can configure data collectors from HPE or third-party companies to forward events to OBM. Events are synchronized between servers. For example, OBM and OM synchronize the state of events and messages. If an OBM operator closes an event, a notification is automatically sent to OM. Similarly, OM notifies OBM about the acknowledgment of messages, and OBM automatically updates the lifecycle state of the corresponding events to "closed."

Operators can enrich events with additional information, for example, by adding annotations to the event to either aid further problem resolution or to document what action has already been taken.

Closed events are automatically moved to the Closed Events Browser. Operators can access this list of closed events, and can use these events as a reference for solving similar problems.

Monitoring Dashboards

Monitoring Dashboards provide you an at-a-glance overview of the events from your monitored environment. They enable you to quickly assess the health of the environment and to identify areas that require your attention.

Monitoring Dashboards help you to:

- Get an overview of your monitored environment
- Visualize a starting point for daily management operations
- Quickly apply event filters to the event browser
- Keep an eye on the monitored environment while working on an event

Monitoring Dashboards display status information by using widgets as building blocks (for example, stack and pie widgets). Each widget references an event filter, a view, or both, and only displays the status of those events that match the criteria of the filter and that are related to the configuration items included in the referenced view, making it easy to customize.

The following figure shows a Monitoring Dashboard screen:
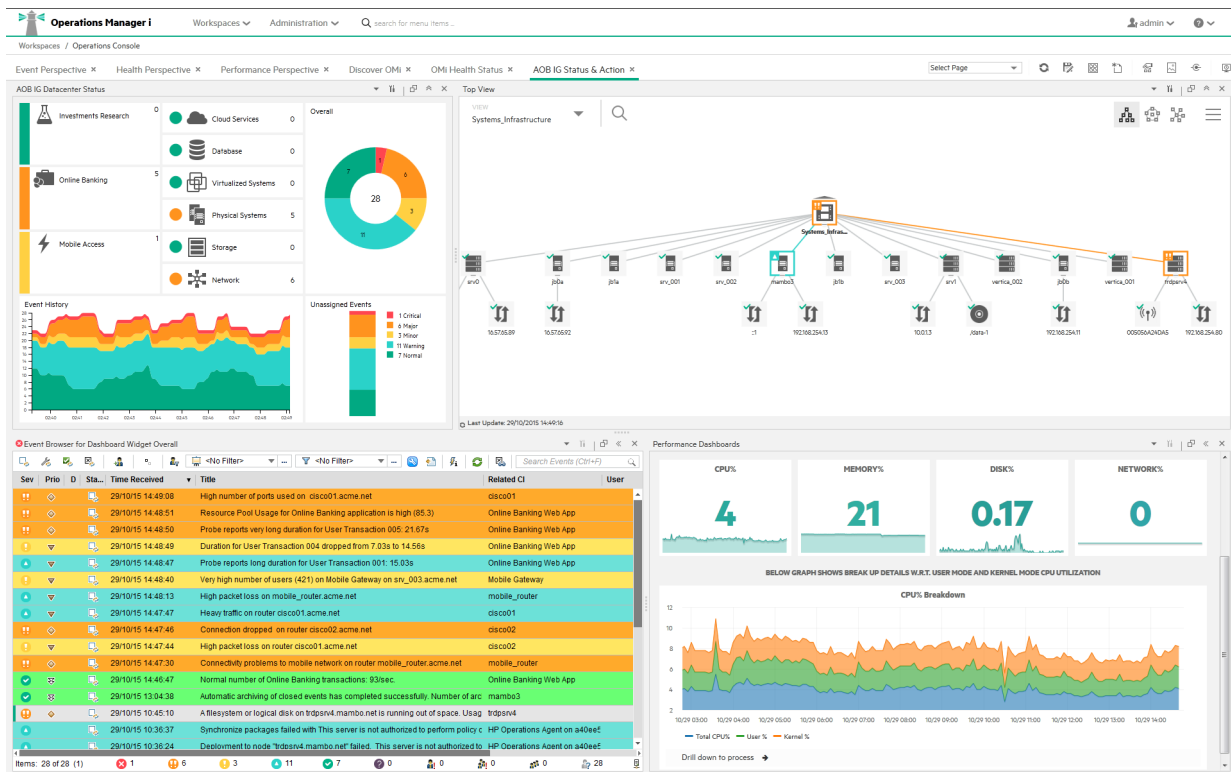

Health information

With event-based data, you can see in the Event Browser which related CI is affected by the event. Additionally, OBM health data, such as event type indicators (ETIs), health indicators (HIs), and key performance indicators (KPIs) are used to evaluate the health of related CIs in the context of the events.

For any device, such as a server, the severity of the problems directly associated with the server are collated and combined with information about devices associated with the server. The combined data is passed to calculation rules that evaluate and set the key performance indicators that indicate the overall health of the object.

The figure below shows a Health Perspective screen, with the Health Top View showing a hierarchical overview of the relationships among the objects associated with the event.
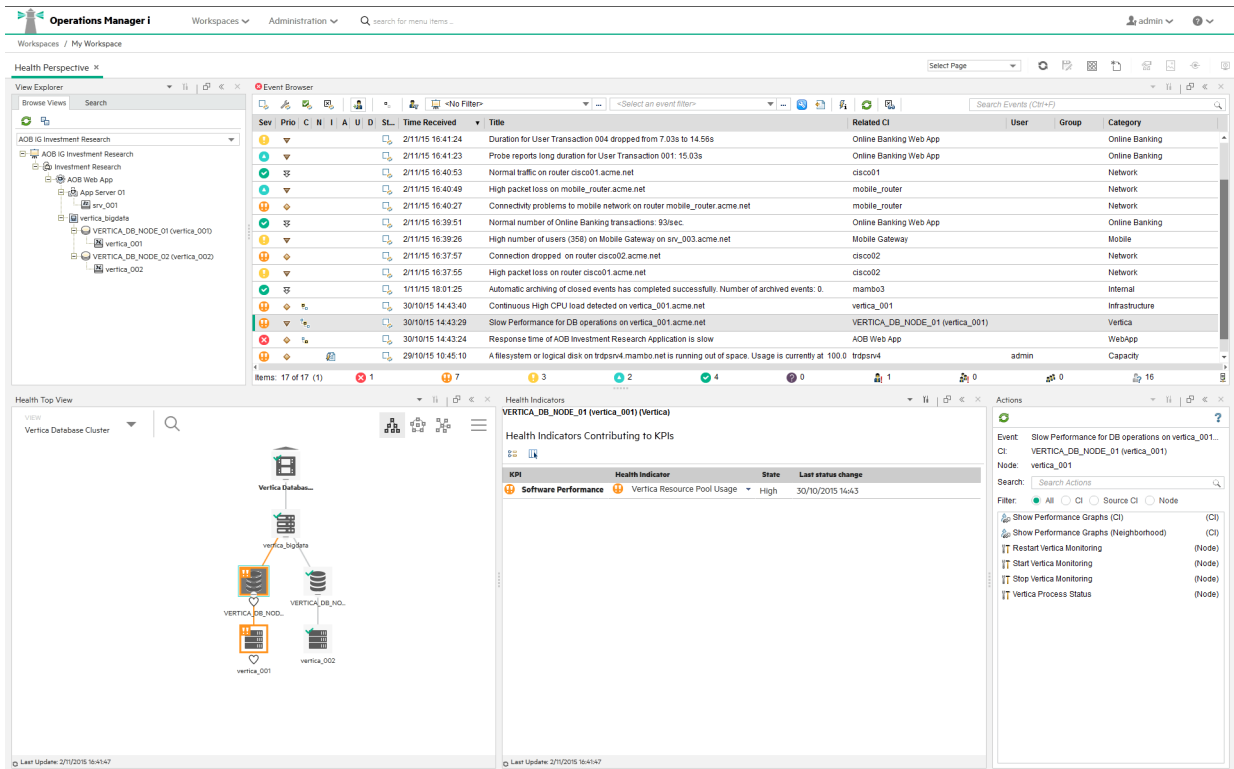
You can see the health status of an object, its KPIs, and Health Indicators, and see how the health status of the selected object affects the health of related objects. For example, you can navigate to check the health of neighboring CIs. This information helps you analyze which events to focus on, and prioritize event handling to maximize availability and minimize negative impact on business services. Users can also select views to show only the events and CIs they are responsible for.

For more information about KPIs, HIs, ETIs, and how Service Health in OBM is calculated, see the *Service Health Concepts* topic.

Correlating events

In a large environment, one of the biggest challenges is how to manage the large number of events that originate from a variety of sources. Within this sea of data, the aim is to identify the events that have a significant impact on business services. So while it is essential to minimize the number of events that appear in the Event Browser, it is even more important to highlight the events that, if not managed properly, could cause a breach in service level agreements (SLAs) and generate incidents in your help desk system.

OBM correlates events automatically using the following forms of event correlation:

- Suppressing duplicate events
- Closing related events automatically
- Stream-based event correlation
- Topology-based event correlation

Suppressing duplicate events

A new event may be a duplicate of an existing event. As a simple example, due to network stability problems, the same event is sent twice by the source domain manager because it did not receive an acknowledgment quickly enough for the first instance of the event. As new events are received, they are checked against existing events. If duplicates are found, new information, such as a change in severity, is used to update the existing

event, and the new event is ignored. If duplicate event suppression is enabled, new events that are duplicates of an existing event are not retained and the original event is updated.

The advantage of correlating events using duplicate event suppression is that it reduces the number of events displayed in the console, but without losing any important information.

Suppressing duplicate events can result in additional correlations of the original event (both as cause or as symptom). When a duplicate is identified, the timestamp for the original event is updated to the time when the duplicate was received. The event is then correlated again and may now be related to other events which were not available for correlation when the original event was received.

Closing related events automatically

A new event can automatically close one or more existing events. When a new event arrives, a search is made for existing related events. Some specific information contained in the new event is used to match the new event to any existing events, and the new event closes the existing event. This type of event correlation is similar to the "good/bad message correlation" provided by Operations Manager.

For example, an existing event may be a notification of a problem or abnormal condition (a bad event) for a particular device. The bad event could be "SQL Query Performance SLOW". Consider a new event matching this existing related event which notifies that the abnormal condition no longer exists (a good event). The good event could be "SQL Query Performance OK". The new (good) event closes the existing (bad) related event.

You can track related events that were closed automatically in the event history.

Stream-based event correlation

Stream-based event correlation (SBEC) uses rules and filters to identify commonly occurring events or combinations of events and helps simplify the handling of such events by automatically identifying the events that can be withheld, removed, or need a new event to be generated and displayed to the operators.

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.

Topology-based event correlation

The event management process is simplified not only by consolidating events from all sources in a central console, but also by categorizing events using topology-based event correlation (TBEC). Dependencies between events are analyzed to determine whether some events can be explained by other events. For example, consider a database server (DB Server) running on a server (Server1). If the Server1 CPU usage becomes persistently overloaded, the resulting event **"SLA for DB Server breached"** can be explained by the causal event **"Server1: CPU persistently overloaded (100% for more than 10 minutes)"**.

The key is to pinpoint the underlying causal events that are responsible for other symptom events, so that you can prioritize the resolution of these causal events based on the impact to your business.

If two events occur concurrently (within a configurable time span), TBEC correlation rules identify one event as the cause and the other event to be the symptom. Rule-based event management enables you to manage large

numbers of similar (related) symptom events in a large network.

When any combination of cause and symptom event occurs in the monitored environment, the correlated events are flagged in the Event Browser. You can configure the Event Browser to display the root-cause event and a separate overview of all the symptom events, thus enabling you to drill down into the correlation process and browse through the hierarchy of correlated events.

Events can also be correlated across technical domains, such as databases, hardware, networks, and web applications. This comprehensive scope enables you to correlate events that, at first sight, might not seem to have any connection. The cross-domain functionality also increases productivity by reducing the amount of overlap between operators responsible for monitoring different technical areas. For example, by correlating events relating to database problems, network problems, and storage problems, you can avoid the scenario of operators from the different technical areas all separately investigating different events that are the symptoms of one root cause event.

TBEC offers a number of benefits related to resolving complex events:

- Reduces the number of events displayed in the console, but without ignoring or losing important data that enables users to drill down through the hierarchy of related events.
- Supports event correlation across multiple domains to simplify root-cause analysis of events that generate symptom events.
- Changes to topological data do not require changes to correlation rules.

Event storm suppression

If a problem is experienced on a managed system that results in the generation of an abnormally high number of events within a relatively short period of time, this phenomenon is known as an event storm. It is very probable that the root cause is already known and is being addressed. However, related events are also being generated. These events do not provide any useful information but may result in significantly increased loads on the servers. To avoid this situation, OBM can be configured to look for event storms from managed systems and discard all subsequent events until the event storm condition for a particular system is over.

An event storm is detected when the number of events received within the detection time period, as a result of a problem on a system, exceeds the configured threshold required to enter an event storm condition.

When an event storm is detected on a system, events from this system are discarded until the rate of incoming events drops below the event storm end threshold. You can configure exception rules to select events from a system under event storm conditions that match a filter and either display these events in the Event Browser or close them (available in the Event Browser under Closed Event). The event storm end event automatically closes the associated event storm begin event.

Related Topics

Service Health Concepts

<comments voting="Plus" />

Structured Problem Solving

OBM streamlines the whole event management process. With centralized, consolidated information, you can create consistent, reusable, and optimized processes for event response.

You can deal with the majority of the events in your environment in a highly structured way. To help you manage events more efficiently and more effectively, you can use the following:

- ToolsYou can create tools to help users perform common tasks on CIs. When you create a tool, it is associated with a CI type, and you can run the tool from the centralized console. For example, you can run a command tool to check the status of an Oracle Database instance. The tool is assigned to the configuration item type Oracle Database. If you are managing multiple versions of Oracle Databases, where the tool requires different parameters and options to check the status of the Oracle Database processes, you can create copies of the most appropriate tool and customize them for the various Oracle versions using the duplicate feature. Each tool is then dedicated to a specific version of Oracle.
- Custom ActionsYou can automate your event management by creating actions to run on events to help solve problems and improve operator efficiency and productivity. Administrators can define a variety of custom actions for the operator to use when resolving certain types of events. Context-sensitive actions and context-specific tools can also be defined for specific circumstances. For example, you might create a set of database diagnostic tools that are designed to be used to help solve database problems.For guidance about script definition and creation, including sample scripts provided with the product, see the *Develop* section.
- Operations Agent ActionsThe events received in the Event Browser from Operations Agent or OM may contain event-related actions configured corresponding policy templates in OBM or in OM policies. If event-related actions exist, you can run these actions from the OBM console. Those actions can be either operator-initiated or can run automatically when an event occurs.
- Operations Orchestration Run BooksIf you are already using Operations Orchestration (OO) to automate operator tasks for analyzing or fixing problems, these OO Run Books can be mapped to CI types within OBM. You can launch OO Run Books in an event context from the OBM console.In addition to manually launching Run Books, it is also possible to configure rules to automatically run a Run Book or a series of Run Books in the context of an event.
- DashboardsDashboards and charts provide additional data to help you visualize and analyze performance-related problems and trends affecting the CI impacted by an event, or any neighboring CIs. OBM performance dashboards can display metrics from Operations Agent, SiteScope, HPvPV, Operations Connectors, and Application Management systems.

Structured event management processes are deployed to:

- Assign incoming events automatically to users in specific user groups. Automatic event assignment significantly increases the efficiency of event management and decreases the amount of time elapsed before a response to the event is possible. Administrators can configure OBM to automatically assign incoming events immediately to available operator groups who are responsible for resolving those events.
- Start actions on events that match a specified set of criteria after a specified time. Time-based event automation rules consist of three main elements:

- Filter defining the events to which time-based event automation rules are to be applied.
- Time period defining the duration an event has to continuously match the rule filter to start the rule actions on that event.
- List of actions to be started on matching events. Available actions are re-running automatic actions on events, modifying event attributes, forwarding events to external servers, assigning events to users and groups, running scripts, and running Run Books.
- Display and monitor the status of events using lifecycle management concepts. You can also see who is currently working on resolving the event, along with all other users who have already played a part in the solution.
- Document how an event is handled and solved. You can annotate the event to describe the problem resolution process, or capture domain expertise by tagging events with tips and hints that improve understanding and explain the event underlying problem.

<comments voting="Plus" />

Performance Dashboard and Performance Engine

The **Performance Dashboard** in OBM enables you to visualize system metrics and custom application metrics in the form of performance dashboards. You can use out-of-the-box dashboards, as well as create custom performance dashboards for the Configuration Items (CIs) that you are monitoring. Performance Dashboard works with the following data sources to visualize performance metrics as dashboards:

- Operations Agent
- SiteScope
- Operations Connector
- OpsBridge Store (provided by Performance Engine)
- Application Performance Management (APM)
- Cloud Optimizer

The **Performance Engine** is an add-on component of Operations Bridge Manager that provides streaming of custom metrics and system metrics in a large scale environment. Performance Engine aggregates streamed data from Operations Agent or Operations Connector which receive data using the RTCM-REST Web Service interface. OBM Management Packs also use the Operations Agent REST WebService interface to submit metrics data for metric streaming. You can visualize the metric data in the Performance Dashboard by using the OpsBridgeStore data source. Performance Engine stores 720 points of data for a metric. If the collection and forwarding interval is configured for 5 seconds, the cache will hold 1 hour of data. The metric data is stored for one hour and can be displayed as real-time data in the Performance Dashboard. If a Vertica database is installed and configured, you can also store metrics for longer than an hour and display them in the Performance Dashboard.

Performance Dashboard and Performance Engine provide the following capabilities for users:

- Visualize, investigate, and review the performance of specific system infrastructure metrics as well as custom application metrics in real-time.
- Aggregate and stream custom metric data and system metric data for more than 25000 datapoints/sec from managed nodes.
- Performance Engine can be installed separately on an additional server to support additional real-time data sources and thus provides a scalable environment.
- Share existing Vertica database available with OpsBridge Reporter for additional data retention for more than one hour.

<comments voting="Plus" />

Management Packs

Management Packs

Management packs provide add-on content on top of OBM. They deliver automatic and end-to-end monitoring solutions of infrastructure and applications. Management packs enable users to monitor, detect, troubleshoot, and remediate issues in the IT domain. They increase the productivity of the user by optimizing and automating various tasks and reduce the mean time to resolve (MTTR) incidents.

Management packs discover application domains and proactively monitor the domains for availability and performance issues. They include, for example, management templates, aspects, policy templates, performances graphs, troubleshooting tools, auto remediation flows, Health Indicator and KPI definitions, as well as topology-based event correlation (TBEC) rules.

The following figure shows an overview of the content that can be included in a set of management packs.
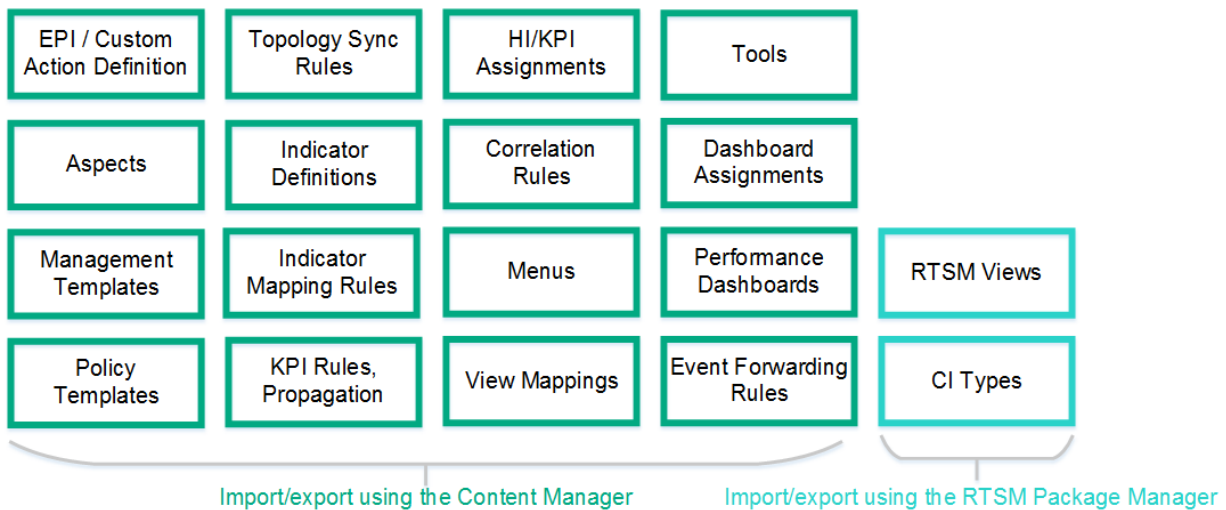
Note: A management pack provided by HPE typically consists of an RTSM package, a content pack, manuals, and the online help. All this content is automatically uploaded during the management pack installation. To use a management pack, a separate license may be required.

Content management tools

OBM has a set of tools to help you manage your own content. These tools are the RTSM Package Manager and the Content Packs Manager. You can use them to package your own content and to exchange the content between systems. For example, you can prepare content in a test environment and then transfer the tested content to a production environment when the tests confirm that the content works as expected.

Export and import tools also enable you to exchange content between systems so that you can keep snapshots or backup images of the content you developed. In addition, they make sure that different instances remain synchronized and up to date.

<comments voting="Plus" />

Scalable Architecture with Multiple Servers

Scalable Architecture with Multiple Servers

OBM enables you to manage widely distributed systems from a central location. In a distributed deployment, you can configure your environment hierarchically. You can then spread management responsibility across multiple management levels, according to criteria such as operator expertise, geographical location, and the time of day. This flexible management enables operators to focus on their specialized tasks, with the benefit of round-the-clock technical support available automatically and on demand.

The scalable architecture enables one or more OBM instances to be combined into a single, powerful management solution arranged to meet the requirements of your organizational structure. So you can configure servers to forward events to other servers in your environment.

In a distributed environment, servers hosting OBM can be configured to work not only with other like servers, but also with multiple OM for Windows and OM for UNIX management servers, other OBM servers, and third-party domain managers.

In such an hierarchical, distributed environment, you can configure OBM to:

- Be the central event consolidator, or a manager-of-managers (MoM), for the whole environment at the top of the hierarchy.
- Work with other HPE products, such as NNMi and SiteScope.
- Work with third-party domain managers, such as Microsoft Systems Center Operations Manager.

You can configure servers hosting OBM to:

- Forward events to other servers hosting OBM and keep those events synchronized among the servers.
- Receive messages forwarded from multiple OM for Windows and OM for UNIX management servers and keep those messages synchronized between servers hosting OBM and OM management servers.
- Receive events forwarded from a BSM 9.x server receiving alerts from APM applications, such as Business Process Monitor (BPM).

Manager-of-Managers

The following figure shows an example of an hierarchical, distributed environment, with a central server hosting OBM managing other regional servers hosting OBM:
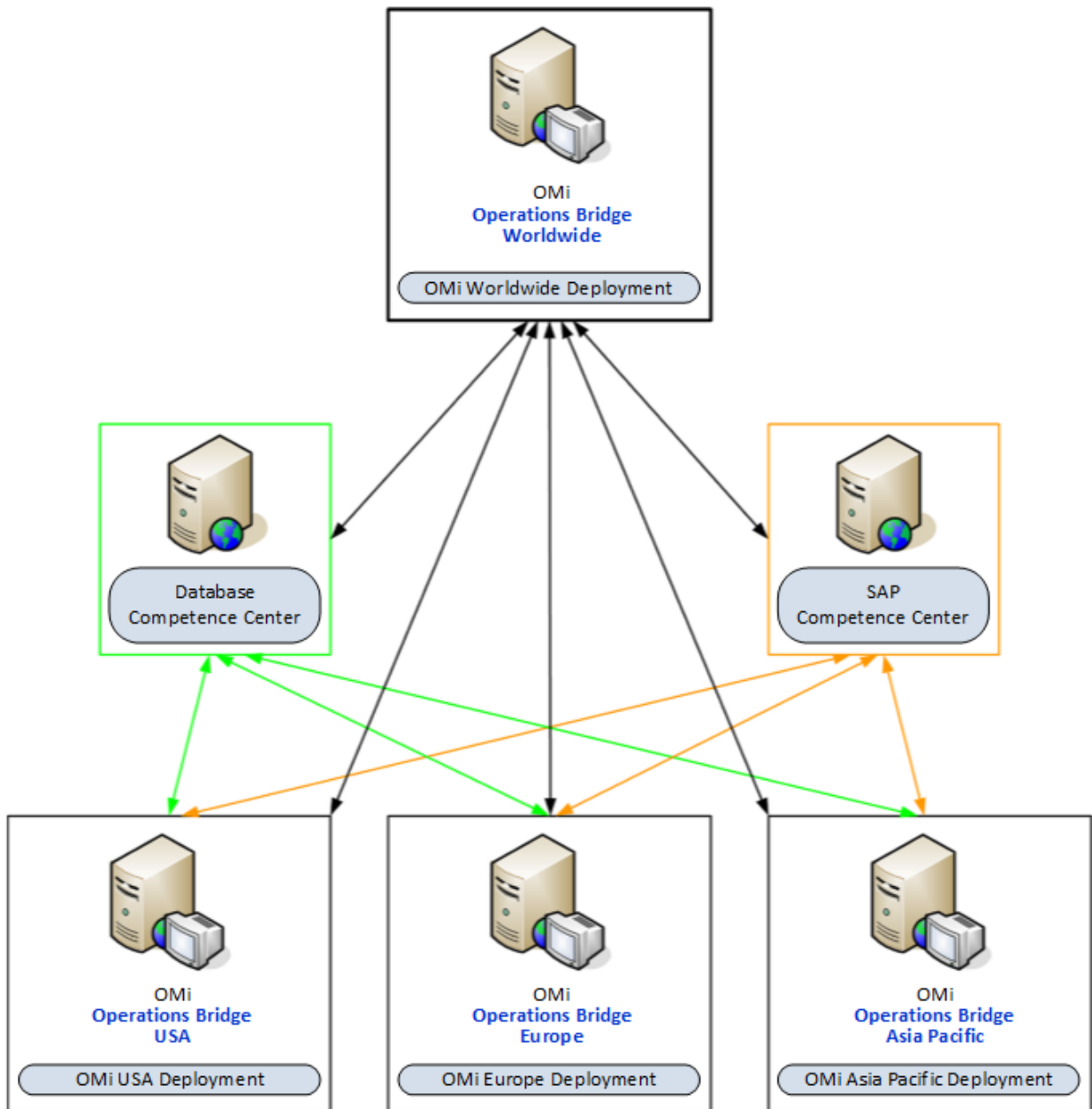
In this example, OBM Europe, OBM USA, and OBM Asia Pacific regional server deployments are managing different geographies. OBM hosted on the OBM Worldwide server deployment is at the top of the hierarchy, and is managing regional servers. It is acting as the central event consolidator, or MoM, for the complete environment. It is a worldwide operations bridge. Regional servers can also act as managers in their own geographies for subordinate systems to create a regionally monitored environment. It is possible to cascade the management of monitored environments in a hierarchical design.

If you operate in a large enterprise with multiple management servers distributed over a wide area, specialist knowledge relating to a specific subject is not always available locally. For example, your organization might have a competence center responsible for SAP. In addition, another center of expertise may be responsible for databases.

A competence center hierarchy distributes responsibility for configuration items in the monitored environment. Regional servers are not solely responsible for configuration items.

Instead, events about specific subjects go to a competence center server, where expertise exists to solve

problems for similar types of configuration items in the monitored environment.

In a distributed environment, the system administrator can configure regional servers to forward certain messages to other servers in the network. The same administrator can configure regional servers to forward events to any server anywhere in the network, based on event attributes.

In the example scenario, all regional servers (OBM Europe, OBM USA, and OBM Asia Pacific) forward all database-related events to the database competence center server, and all SAP-related events to the SAP competence center server.

In this type of scenario, the operations bridge synchronizes event actions (for example resolve, assign, severity change) among the regional servers and the competence centers. This ensures the event states are always synchronized across the enterprise environment.

<comments voting="Plus" />

Monitoring Automation

Monitoring Automation

Monitoring Automation automates the configuration of monitoring for infrastructure and composite applications. Whether the monitoring tool used is agent-based or agentless, Monitoring Automation deploys the appropriate monitoring configuration to the target instances. It offers easy-to-tune monitoring and reporting, detecting new instances of components and mapping them to management templates and aspects that model the desired configuration and resource type.

Monitoring is the generation of events if a CI behaves in an unexpected manner. Typical events are:

- A monitored value exceeds a certain threshold. Example: Used disk space on a database exceeds a predefined limit of 90%.
- A node is removed from the network. Example: A power cut causes a server to shut down so it can no longer be reached.

Monitoring Automation provides a complete management solution for an application or service, enabling you to create a management solution for the entire set of configuration items (CIs) comprising the application. The solution can be made to respond dynamically to changes in the topology, making the monitoring solution independent of the hardware and platform running the application.

The key to understanding Monitoring Automation is to familiarize yourself with the underlying terminology and architecture. Consider the stack shown in the following figure:
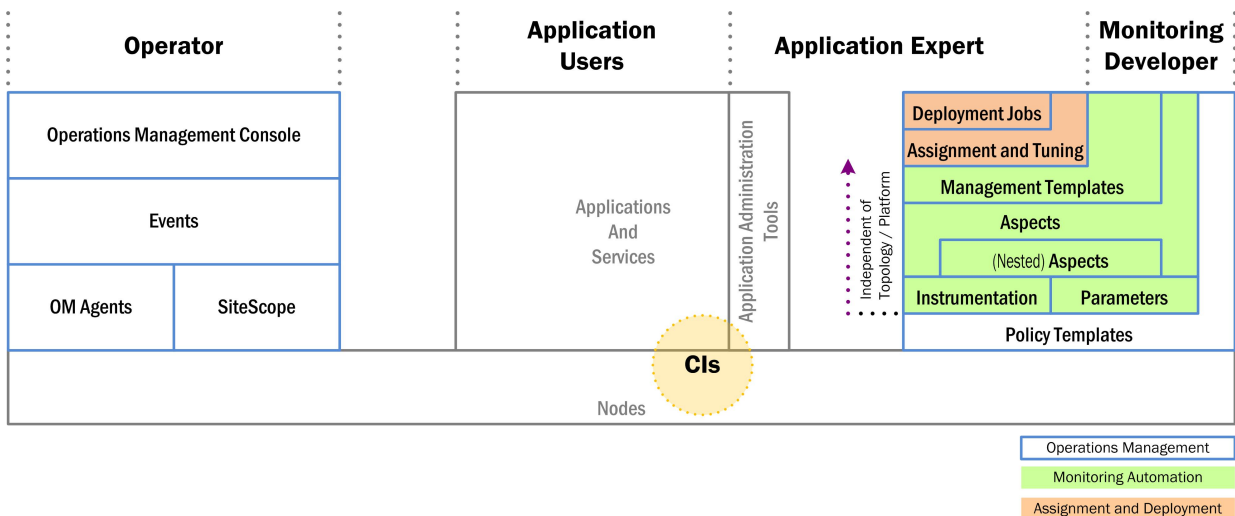
The base of the stack represents the CIs to be monitored. CIs can be network elements such as computers, as well as applications or sets of applications providing a service. CIs are accessed in the following ways:

- Users interact with the CIs independent of any monitoring, as suggested in the central section of the figure.
- OBM monitors the CIs using the familiar monitoring structure shown in the left-hand section of the figure.
- A monitoring developer configures monitoring solutions as shown in the right-hand section of the figure.
- An application expert starts the monitoring process after tuning the configuration made by the monitoring developer, and acts on events passed by the operator by inspecting deployment jobs and using application-specific administration tools.

Monitoring Automation offers a number of features for creating flexible monitoring solutions. The following section explains each configuration element in turn. The explanation follows the order of the layers comprising the configuration stack from bottom to top.

Node

A node is a physical element you can access on the network.

CI

A CI is a node or an application or services running on a node. CIs are what is actually monitored by OBM. Events always relate back to CIs.

Policy Templates

Policy templates define what is monitored and how the monitoring is done. Note that policy templates are platform-dependent.

Before Monitoring Automation, all configurations were done through Policies and Policy Templates, meaning that for each change in a CI with respect to the platform, the topology, or the monitoring policy, the values in the CI's policy templates against which the CI is monitored had to be modified.

Parameters and Instrumentation

Monitoring Automation introduces parameters. Each parameter corresponds to a monitoring setting for a single CI attribute in the policy template. Changing the parameter value changes the monitoring behavior, removing the need to manually change hard-coded values in a policy template. The concept of cascading default values is central to Monitoring Automation. The idea is that the monitoring developer or application expert uses as many default values as possible on a certain level, creating a baseline for monitoring. On the next level up, a subset of these values can and may need to be overridden for the specific monitoring task at hand, but every value already covered by the baseline setting can be taken over without having to redefine it.

The following features of parameters allow additional flexibility:

- Conditional parameter values enable using the same parameter with several policy templates, allowing hardware- and platform-independent monitoring solutions.
- Parameters with the same value can be combined into a single parameter. This removes the need to enter the same value multiple times.

Instrumentation includes scripts and programs executed by the Operations Agent as defined in policies for managed nodes that have the agent installed on them.

Aspects

Policy templates and instrumentation representing a certain expected behavior of the application or service to be monitored are grouped together in aspects. At aspect level, developers streamline the configuration as

follows:

- They combine parameters with the same function into single parameters.
- They can nest aspects to combine aspects representing the same behavior, but defined in different policy templates, into a single aspect. Each nested aspect can be coupled with a deployment condition telling OBM which nested aspect is to be used in which environment. This allows any CI of the target CI type to use the same aspect, independent of the platform.
- They set default values at aspect level in line with the company monitoring policies.

Management Template

A management template combines all aspects needed to monitor a composite application or service. The management template configuration includes the topology of the composite application and the aspects to be monitored. In addition, the developer overrides any company-wide default values at management template level if the application to be monitored requires this.

The developer hands the finished management template over to the application expert, who uses it to start monitoring the target application.

Tuning, Assignment, and Deployment

Before starting the monitoring process, the application expert may want to override certain default values configured by the monitoring developer to take situation-specific monitoring requirements into account. This is called tuning.

The monitoring configuration represented by an aspect is defined in terms of a CI type. To start monitoring, this CI type has to be matched to an actual CI instance that has been discovered by the topology discovery process. This matching process is called assignment and can be done in the following ways:

- Manual assignment of a management template. The application expert links the management template to a CI instance of the management template's root CI.
- Manual assignment of an aspect. The application expert links the aspect to a CI instance of the aspect's target CI type.
- Auto-assignment. If the application expert defines auto-assignments for a management template or aspect, OBM dynamically assigns aspects to the relevant CI instances as and when they are discovered.

After assignment is completed, the monitoring solution is deployed in the same step. While the monitoring is running, the application expert can keep an eye on any deployment jobs to make sure the monitoring process proceeds as expected, or to acquire information related to events reported by an operator.

<comments voting="Plus" />

Additional resources

This section lists additional resources that should help you understand how to make the most out of the Operations Bridge Suite capabilities.

Operations Bridge Evolution

Video Library

Blog Posts

Downloads, Support, and Training

<comments voting="Plus" />

Operations Bridge Evolution

Free License Exchange

Many customers have experienced years of success with Operations Manager, but the surging complexity of IT operations inspired us to create Operations Bridge, our next-generation, analytics-driven operations solution. We recommend that all OM customers evolve to Operations Bridge (Premium Edition) with a free license exchange.

Why evolve?

Operations Bridge is a holistic product suite designed to help shift IT from a cost function to a strategic business partner. With OBM incorporated directly into Operations Bridge, it delivers all the capabilities of Operations Manager and much more:

- True single pane of glass with expansive technology coverage
- Business Value Dashboard
- Adaptive event management and event reduction
- Automated discovery and monitoring
- Cross-domain reporting

To get started today, download the Operations Bridge Evolution Starter Pack and browse the resources below for more information and technical guidance. Also see **Develop > Transfer functions from OM to OMi** for more information on the evolution process.

Presentations

Presentation	Link
Customer deck. **OM to Ops Bridge Evolution Program**: How to successfully evolve to a greater value (July 2017)	go
Technical customer deck. **OM to Ops Bridge Evolution Program**: How to successfully evolve to a greater value (July 2017)	go

Webcasts

Webcast	Link
What is an IT Operations Bridge and who benefits from it? High-level Operations Bridge overview including a short product demonstration. (December 2013)	go
Darwinian Evolution of Operations Manager. OM to Operations Bridge evolution overview and case study of how Fidelity started their evolution and their return on the investment. (January 2015)	go
Operations Bridge Evolution Overview. See how to move from Operations Manager to OMi, including adding OBM on top of OM, reusing the exiting investment in agents and policies, and switching off OM.	go

OBM 10 Best Practices. Our partner Whitlock has developed a custom deployment kit that walks you through a value-based planning process and guides you on best practices for deployment and integrations. It also provides basic event process design, as well as initial integrations to existing processes, and facilitates knowledge transfer with a transition support plan to allow you to come up to speed on the new interface and features of OMi 10. (September 2015)

go

Case Studies

Case Study	Link
Canada's biggest credit union leverages software from HPE for visibility, proactive control	go
Single view makes monitoring easier for GE Money Bank	go

White Papers

White Paper	Link
Moving to Service Centric Management with OMi. Recommended implementation steps when moving to Service Centric Management with OMi. Technical White Paper developed for new OMi customers, which can also be helpful for OM to OMi evolution customers, in order to learn more about the OMi deployment best practices.	go

Blog Posts

Blog Post	Link
Grow your IT monitoring by evolving to the OpsBridge Suite	go
OM users - Here is why and how to move to OBM	go
Darwinian evolution of OMi Management Pack	go
OM-to-OpsBridge Evolution: Evolve to OMi Management Pack with "SPI to MP Evolution Tool"	go
Evolve to OMi: How to keep your OM policy investment and when to use OMi Management Packs	go
Evolve to OMi: How to smoothly move hundreds of Operations Agents to OMi	go
Evolve OM Unix to OMi: Simple command Line tools admins need to know	go
Evolve to OMi: How to set up user permissions similar to those in OM	go
Evolve to OMi: Implementing instruction text lookup and addressing other policy import warnings	go
Operations Manager i: Unlock the value of stream-based event correlation	go

Videos

Video	
How to integrate Operation Manager for UNIX/Linux (recorded with OMi 10.00)	go
How to integrate Operation Manager for Windows (recorded with OMi 10.00)	go
How to connect an Operations Agent (recorded with OMi 10.00)	go
How to deploy systems infrastructure monitoring to a monitored node (recorded with OMi 10.00)	go
How to filter events in the event browser (recorded with OMi 9.24)	go
How to create a monitoring dashboard (recorded with OMi 10.00)	go
How to create an aspect containing a group of policy templates (recorded with OMi 10.00)	go
How to add a parameter to a policy template (recorded with OMi 10.00)	go
How to combine and pre-set parameters in aspects or management templates (recorded with OMi 10.00)	go
How to create an SBEC repetition rule (recorded with OMi 10.11)	go
How to use stream-based event correlation (SBEC) to combine events (recorded with OMi 10.00)	go
How to use stream-based event correlation (SBEC) to correlate repeated events (recorded with OMi 10.00)	go

MICRO FOCUS | **Documentation**

Tools

Tool	
Policy Statistics Tool for Operations Manager	go
Policy Reporter for OMi	go
SPI to MP Evolution Tool	go

Related Topics

Operations Bridge Evolution Starter Pack

<comments voting="Plus" />

Video Library

The video library contains short how-to videos that help you to understand how to do certain things in OBM. Check out the following overview videos or see below to find videos organized by category:

- Focus Operations Through a Business Lens with Operations Bridge Suite. HPE partner Vivit walks you through how to get the most out of your Operations Bridge Suite.
- HPE Operations Bridge software demo. Learn more about the Operations Bridge, including performance and monitoring dashboards and Business Value Dashboard.

Business Value Dashboard

Video	Link
End to end business value dashboard creation. This video shows end to end how to create a dashboard in Microsoft Visio and how to use it in Business Value Dashboard (BVD). This includes sending data via HTTP-Post to BVD and connecting the data to BVD widgets (recorded with BVD 10.11).	go

Integrations

Video	Link
Operations Bridge: How to integrate Microsoft System Center Operations Manager. This video shows how to integrate Microsoft System Center Operations Manager into Operations Bridge / Operations Manager i, which provides a single pane of class to monitor your IT environment (recorded with SCOM 2012 and OMi/OpsCx 10.11).	go
Operations Bridge: How to integrate a SiteScope system into OMi. This video shows how to integrate SiteScope into Operations Bridge / Operations Manager i, which provides a single pane of class to monitor your IT environment (recorded with SiS 11.32 and OMi 10.11).	go
OMi: How to integrate Operation Manager for UNIX/Linux. In this video you will learn how to integrate Operations Manager for Linux so you can use OMi as a single pane of glass for monitoring across the IT enterprise (recorded with OMi 10).	go
OMi: How to integrate Operation Manager for Windows. In this video you will learn how to integrate Operations Manager for Windows so you can use OMi as a single pane of glass for monitoring across the IT enterprise (recorded with OMi 10).	go
Integrate Experience into Dashboards with Operations Bridge and AppPulse. HPE Partner Vivit shows how to integrate dashboards with Operations Bridge and AppPulse.	go

Operations Connector

Video	Link
Operations Bridge: How to install an Operations Connector. This video shows how to install an Operations Bridge Connector and how to connect it to an Operations Bridge / Operations Manager i system (recorded with Operations Connector 10.11 and OMi 10.11).	go

Event Processing

Video	Link
OMi: How to use stream-based event correlation (SBEC) to correlate repeated events. OMi provides several event reduction and event enrichment techniques. In this video you will learn how to use stream-based event correlation to correlate a set of repeated events to one event within a configured time window.	go
OMi: How to use stream-based event correlation (SBEC) to combine events. OMi provides several event reduction and event enrichment techniques. In this video you will learn how to use stream-based event correlation (SBEC) to combine two different events into a single enriched event (recorded with OMi 10.00).	go
OMi: How to filter events in the Event Browser. To fix problems faster, it is crucial to learn how to filter open and closed events in the OMi Event Browser. In this video you will learn how to limit the type of events that are displayed (recorded with OBM 9.24).	go

Evolution

Video	Link
Operations Bridge Evolution Overview. This video shows how to move from Operations Manager - for Windows, Unix or Linux - to Operations Manager i. The process involves adding OMi on top of OM, and re-using the existing investment in agents and policies, before switching off OM.	go

Monitoring Automation

Video	Link
OMi: How to connect an Operations Agent. In this video, you will learn how to connect an Operations Agent to OMi so you can monitor availability and performance and remediate issues on a monitored server (recorded with OMi 10.00).	go
OMi: How to deploy systems infrastructure monitoring to a monitored node. In this video, you will learn how to deploy monitoring systems infrastructure monitoring to a monitored node (recorded with OMi 10.00).	go
OMi: How to create an aspect containing a group of policy templates. Aspects play an important role in OMi's monitoring automation as they hide policy template complexity by only exposing parameters. Learn how to quickly create an aspect containing a group of policy templates (recorded with OMi 10.00).	go
OMi: How to add a parameter to a policy template. Parameterization inside OMi Monitoring Automation allows easy tuning of monitoring thresholds. This video shows how easy it is to add such a parameter to a monitoring policy and how to change a parameter value afterwards (recorded with OMi 10.00).	go
OMi: How to combine and pre-set parameters in aspects or management templates. In this video, you will learn how to combine parameters so that a user deploying an OMi management template is asked for the parameter only once. The tutorial also explains how to pre-set parameters using CI attributes (recorded with OMi 10.00).	go
OMi: How to create a Monitoring Dashboard. A Monitoring Dashboard provides an event-driven overview of the monitored environment. In this video, you will learn how to create a Monitoring Dashboard within an OMi 10.00 Workspace (recorded with OMi 10.00).	go

Operations Bridge Analytics

Video	Link
Operations Bridge: Log Streaming from the Operation Agent to Operations Bridge Analytics. This video shows how to stream Linux system log data from the Operations Agent to Operations Bridge Analytics (OBA) and then analyze that data in OBA (recorded with OMi 10.61, OBA 3.01, OA 12.03).	go

<comments voting="Plus" />

Blog Posts

Experts in the Operations Bridge community have created a wide variety of blog posts to help you get the most out of your Operations Bridge Suite. Check out these helpful blog posts to get started:

Next-Generation Operations Bridge

Blog Post	Link
What's new within the Operations Bridge 2017.04	go
Containers going wonky? Cloud service getting murky? Our monitoring brings visibility for solutions	go
New software deployment and delivery model: increasing innovation speed	go
Container Deployment Foundation delivers high capacity IT Ops Business Value Dashboards	go
Supercharge IT Operations using next generation Operations Bridge	go
Organic changes that transform – Operations Bridge evolution announced	go

Operations Bridge Dashboards

Blog Post	Link
Business Value Dashboard: Data integration (part 1)	go
Business Value Dashboard: Data integration (part 2)	go
Business Value Dashboard: Get started now!	go
Building your Business Value Dashboard using tags and dimensions	go
Using Business Value Dashboard with the Internet of Things	go
Power up Business Value Dashboard with Cloud Optimizer!	go
Speedy Cape2Cape globe trotting - connecting you to the driver experience	go
Visualize OMi event pipeline performance in the OMi Performance Dashboard	go
Making metrics sing with OMi Performance Analytics dashboards	go
Fasten your seat belts: Performance Engine to take off!	go
Real-time metric streaming of application and custom metrics	go

Operations Bridge Evolution

Blog Post	Link
Grow your IT monitoring by evolving to the OpsBridge Suite	go
Evolve to OMi: Implementing instruction text lookup and addressing other policy import "warnings"	go
Evolve to OMi: How to smoothly move hundreds of Operations Agents to OMi	go
Evolve OM Unix to OMi: Simple Command Line Tools admins need to know	go
Evolve to OMi: How to keep your OM policy investment + when to use OMi Management Packs	go
Evolve to OMi: How to Setup User Permissions similar to those in OM	go
Darwinian evolution of OMi Management Pack	go
OM-to-OpsBridge Evolution: Evolve to OMi Management Pack with "SPI to MP Evolution Tool"	go

Blog Post	Link
OM users - here is why and how to move to OMi	go
Successfully upgrade from Operations Manager to Operations Bridge: The myths, truths and expert tips	go
The perfect pass - The evolution of Operations Manager to OMi	go

Big Data

Blog Post	Link
New age monitoring solution for your Big Data technologies	go
A BIG brother for your BIG data environment	go

Cloud/Virtualization

Blog Post	Link
Operations Bridge and AWS: Automatic discovery and seamless Cloudwatch integration	go
OpsBridge monitors Docker on the fly	go
Your Private Cloud Operations through a Business Lens for more than 58,000 VMs and counting!	go
Monitor your x86-virtualized environment for free with vPV	go
Public Cloud Service Health Check - Simplified with Operations Bridge	go
Keys to deploying OMi 10 on Helion Public Cloud	go
Monitoring virtual environments - VM101	go
Now available! Public cloud monitoring: The end-to-end hybrid view with OMi and Helion	go

Operations Agent

Blog Post	Link
How to deploy hundreds of Operations Agents using Operations Orchestration	go
AIRVA: A new way to install the Operations Agent!	go
OMi: Metric Streaming with Operations Agent 12.01	go
HPE Discover 2016: Learn how Operations Agent improves the health of your monitoring infrastructure	go
Five questions to ask before you upgrade to the 64-bit Operations Agent 12.00 on HP-UX	go
Operations Agent 12.00—for the new style of IT management	go
Exploring the potential of Operations Agent version 12	go
Get agent health at a glance with the Health Dashboard for infrastructure monitoring	go

Operations Connector

Blog Post	Link
How to make sure that your critical Operations Bridge integrations are always up and running	go
Operations Connector SDK 2.0 – adding 3rd party systems into your OpsBridge just got a lot easier	go
Using OMi to manage policies for multiple Operations Connector systems	go
How to integrate Oracle Enterprise Manager (OEM) into OMi 10.60 and OpsCx 10.11	go

Operations Bridge Analytics

Blog Post	Link
Bridge to the Future: From Operations Analytics to the new Operations Bridge Analytics 3.0	go
Operations Bridge Analytics Log Streaming using Operations Agent	go

Correlation

Blog Post	Link
Operations Manager i: Unlock the value of stream-based event correlation	go

Bring your own code: How to simplify customizing event correlation software	go

Event Processing

Blog Post	Link
How to easily reduce events in OMi using Stream Based Event Correlation	go
OMi Subcomponent HIs: Granular HIs without creating CIs in RTSM	go
A closer look at the functionality of OMi Script Dev Kit	go
Easier event handling for Operations Manager i (send, export/import, archive events via CLI)	go
OMi: Looking Beyond Event Severity for Prioritization	go
OM-OMi: Dealing with Event Duplicates, effectively	go
Configuring OMi to propagate Event KPIs with the parent displaying the sum of events	go

Management Packs / Developing your own content

Blog Post	Link
"It really was working after just a few days of development" - OMi Management Pack Hackathon report	go
OMi Management Pack Development Kit - Overview	go
OMi Management Pack Development Kit - Topology	go
OMi Management Pack Development Kit - Events	go
Meet the OMi Management Pack DevKit	go
Meet the OMi Management Pack DevKit, Part 2	go

Monitoring Automation and out-of-the-box Management Packs

Blog Post	Link
What's new with the AWS and Azure Management Pack latest releases	go
What's new in the Operations Manager i Management Pack for Infrastructure 2.0	go
New in the Docker Store - Docker certified Software shows business impact of Docker containers	go
Step by Step: OMi Management Pack for Docker	go
Use Operations Bridge to Monitor Containerized Applications	go
Microsoft Azure Monitoring with OpsBridge Management Pack	go
Monitoring PostgreSQL with OMi Management Pack	go
Monitor Microsoft Active Directory with OMi Management Pack	go
Monitor Oracle Database with OMi Management Pack	go
Simplified SAP Monitoring using OMi Management Pack for SAP	go
Dock Your Docker with Operations Manager i (OMi Mgmt Pack for Docker)	go
Everything you want to know about OMi Management Pack for TIBCO	go
How to Configure and Monitor TIBCO using OMi Management Pack for TIBCO	go
Switching to Monitoring Automation: How to deploy monitoring configuration	go
OMi now includes Automation to simplify IT Monitoring	go
Visualize, monitor and remediate your Vertica environment with OMi Management Pack for Vertica	go
A new SQL to the IT Operations Management cockpit story	go
3 steps to new metric collection with OMi MP for Oracle Database	go
Monitor the job queue, ascertain system bottlenecks - best practice #1	go
Set threshold values correctly for good monitoring since not every day is Sunday - best practice #2	go
Gain the flexibility you need for Management Pack deployment with OMi 10.10	go
Troubleshoot Skype for Business server performance problems with OMi	go
Troubleshoot Microsoft SQL Server performance problems	go

MICRO FOCUS | **Documentation**

Reporting

Blog Post	Link
(Re)Introducing Operations Bridge Reporter	go
How to easily achieve "multi-tenant" reporting with Operations Bridge Reporter	go
Analyze your OMi events for an efficient IT Operations team	go

Service Health

Blog Post	Link
Configuring OMi to exclude event KPIs from impacting Service Health	go
OMi - Event Count based special KPIs (Unassigned Events and Unresolved Events KPIs)	go
From OMi Events to CI Status	go

Other topics

Blog Post	Link
Achieving your Operations Bridge migration in 5 steps	go
How to create your own custom topology using OMi policies	go
Hidden treasures in OMi 10.11 – useful CLI and web services enhancements you might not have noticed	go
OMi documentation – A new look, feel and simplified access to learn about Operations Bridge Suite	go
10 points on how to visualize and manage performance with OMi	go
Graphing Metrics Data in Hierarchical Operations Bridge Deployments	go
Operations Manager i: Event Browser unleashed! Your guide to IT event management	go
IT operations dashboards: OMi 10.01 new message browser features increases operator efficiency	go
How to use Roles, Groups and Users to efficiently manage access to OMi	go
Get to a working OMi in 35 minutes or less	go
Over the Business Rainbow - A new Business "Heads up Display"	go
Announcing Operations Bridge version 10 with 10 great reasons to adopt it	go
The Why, the What and the How of the new OMi Content Extension in Service Health Reporter	go
VMware tools and why it is important for monitoring and what-not	go
Transport Layer Security in OMi 10.10, Simplified Setup	go
OMi event console in a 3rd party ecosystem	go
Running a OMi proof-of-concept and other lessons from the road	go
Recorded Webinar: Gain visibility to the user experience in your Operations Management Dashboard	go
6 similarities between a deal aggregator and Operations Manager i (OMi)	go

<comments voting="Plus" />

Downloads, Support, and Training

Micro Focus provides lots of support and training resources to help you learn more about using the Operations Bridge Suite, and to remedy problems when the do occur. The following is a collection of links to Operations Bridge support, training, certification and download websites.

Downloads

Download	Link
Patch summary for Operations Bridge Manager	go
Free trial version of Operations Bridge Manager	go

Support

Resource	Link
Software support	go
Create a support case	go
Software support offerings	go
Support forum for Operations Bridge specific questions	go
Obsolete products: end of support dates	go

Community

Resource	Link
Operations Bridge Community Home	go
OBM Practitioners Forum	go
OBM Integrations Forum	go

Training

Training	Link
OBM training schedule	go
OMI01IT - Operations Manager i-Series 10 Interactive Training Created by ART	go
OMI120 - Operations Manager i Software 10 Essentials	go
OMI110 - Operations Manager i Software 10 for Operators	go
OMI200 - Operations Manager i Software 10 Advanced	go

Certification

Certification	Link
Software certification	go

<comments voting="Plus" />

MICRO FOCUS | **Documentation**