



HPE Operations Bridge Reporter

Software Version: 10.21

Windows® and Linux operating systems

Administration Guide

Document Release Date: August 2017
Software Release Date: August 2017



Hewlett Packard
Enterprise

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

© 2015 - 2017 Hewlett Packard Enterprise Development LP

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

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

Documentation Updates

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

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

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

Support

Visit the HPE Software Support site at: <https://softwaresupport.hpe.com/>.

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

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

HPE Software Solutions Now accesses the HPSW Solution and Integration Portal website. This site enables you to explore HPE Product Solutions to meet your business needs, includes a full list of Integrations between HPE Products, as well as a listing of ITIL Processes. The URL for this website is <https://softwaresupport.hpe.com/km/KM01702731>.

About this PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format. Because this content was originally created to be viewed as online help in a web browser, some topics may not be formatted properly. Some interactive topics may not be present in this PDF version. Those topics can be successfully printed from within the online help.

Contents

Part I: Introduction	12
Chapter 1: Role of the Administrator	13
Chapter 2: Accessing the Administration Console	14
Part II: Getting Started	16
Chapter 2: Configuration Wizard	17
Time Zone Selection	17
Vertica Database Creation	18
Management Database Creation	18
Collector Configuration	18
Chapter 3: Post-install Data Source Selection	19
Data Source Selection	19
Configure Topology Source	20
Content Type Selection	20
OMi Management Packs/OM SPIs Selection	21
Content Pack Deployment	21
Data Source Configuration	21
Chapter 4: Dashboard	22
Task pane	23
License details	23
User	23
Logout	23
Online Help	23
View pane	24
Chapter 5: Data Source Selection	27
Managing Data Source Configuration	27
Chapter 6: Managing Content Packs	30
Managing Content Packs	30
Chapter 7: Managing Topology Source and data collection	32
Managing the enterprise topology	36
Managing the OM data collection	37
Managing the SiteScope data collection	38

Managing collection from generic databases	39
Managing the VMware vCenter data collection	40
Managing the Operations Agent data source data collection	41
Managing the Management, Profile, and Operations Database data collection	42
Chapter 8: Additional Configurations	44
Managing Vertica Database	45
Managing Management Database	45
Configuring Collector	45
Managing data processes	45
Managing security	46
Managing time shifts	48
Managing data aging	49
Managing licenses	50
Managing user accounts	51
Managing Pending Configuration	52
Chapter 9: Monitoring OBR	53
Monitoring the OBR content	53
Monitoring Data Collection Status	54
Monitoring the data processes	54
Understanding the job stream status	56
Scenario 1	56
Scenario 2	57
Scenario 3	57
Scenario 4	58
Back up and restore OBR PostgreSQL management database	58
Monitoring the application platform	59
Chapter 10: Help	60
Online Help	60
About OBR	61
Part III: Administration Console Screens	62
Chapter 11: Configuration Wizard	63
Chapter 12: Data Source Selection Wizard	66
Chapter 13: Dashboard	70
Using the Home page	73

View OBR status	73
View details of the Orchestration Alerts	75
Chapter 14: Data Source Selection Wizard	77
OM Deployment scenario	79
BSM/OMi Deployment scenario	80
VMware vCenter only Deployment scenario	81
Others Deployment scenario	82
Chapter 15: Content Pack Deployment	84
Content Pack Deployment	85
Content Pack Component Status History	86
Install a Content Pack	98
Upgrade a Content Pack	99
Remove an Installed Content Pack	99
Chapter 16: Topology Source	101
Topology Source	101
Connection Parameters: RTSM	102
Connection Parameters: OM	103
Connection Parameters: VMware vCenter	104
Create a Topology Source connection	104
Modify a Topology Source connection	108
Enable or disable a Topology Source data collection	111
Schedule a Topology Source collection	112
Test the Topology Source connection	113
View Topology Source connection status	114
View Topology Source data collection status	114
Chapter 17: Operations Manager	115
Connection Parameters	116
Create an OM data source connection	118
Modify an OM data source connection	120
Enable or disable an OM data collection	122
Schedule an OM data collection	123
Test the OM data source connection	123
View the OM data source connection status	123
View the OM data collection status	124
Delete an OM data source connection	124

Chapter 18: SiteScope	125
Connection Parameters	126
Create a SiteScope data source connection	127
Modify a SiteScope data source connection	129
Enable or disable SiteScope data collection	131
Test the SiteScope data source connection	131
View the SiteScope data source connection status	132
View the SiteScope data collection status	132
Delete a SiteScope data source connection	133
Chapter 19: Generic Database	134
Connection Parameters	135
Create a generic database connection	136
Modify a generic database connection	138
Enable or disable a generic database data collection	139
Schedule a generic database data collection	140
Test the generic database connection	140
View the generic database connection status	140
View the generic database collection status	141
Delete a generic database connection	141
Chapter 20: VMware vCenter	142
Connection Parameters	143
Create VMware vCenter data source connection	143
Modify a VMware vCenter data source connection	144
Enable or disable a VMware vCenter data collection	144
Schedule a VMware vCenter data collection	145
Test the VMware vCenter data source connection	145
View the VMware vCenter data source connection status	145
Chapter 21: Operations Agent (OA)	146
View the Operations Agent data source details	148
Enable or disable a Operations Agent data source data collection	150
Schedule a Operations Agent data source data synchronization	151
Blacklisting of Nodes	152
Test the Operations Agent data source connection	152
Assign View/Node Group based Rules for Data Collection	153
Assign Pattern based Rules for Data Collection	153

Chapter 22: BSM/APM/OMi	155
Management Database	156
Management Database: Create New: Connection Parameters	157
Profile Database	159
Profile Database: Create New: Connection Parameters	160
OMi	163
OMi: Create New: Connection Parameters	164
Create a new Management, Profile, and Operations Database connection	166
Create a new Management Database	166
Create a new Profile Database	170
Create a new Operations Database	174
Modify a new Management, Profile, and Operations Database connection	176
Enable or disable Profile Database data collection	179
Schedule Profile Database synchronization	179
Test the Management Database and Profile Database connection	179
View the Management Database and Profile Database connection status	180
View the Management Database and Profile Database collection status	180
Delete a Management Database connection	181
Create an OMi data source connection	182
Modify an OMi data source connection	183
Enable or disable an OMi data collection	184
Schedule an OMi data collection	185
Test the OMi data source connection	185
View the OMi data source connection status	185
View the OMi data collection status	185
Delete an OMi data source connection	186
Chapter 23: Vertica Database & Time Zone	187
View Vertica database and time zone configurations	188
Change the OBR database password	188
Enable TLS for Vertica	189
Disable TLS for Vertica	190

Chapter 24: Management Database	191
View Management database configurations	192
Change the OBR management database password	192
Chapter 25: Collectors	193
Configuring a Collector Installed on a Remote System	194
Disabling a Collector Installed on a Remote System	195
Testing a Collector Installed on a Remote System	195
Chapter 26: Data Processing	196
Stream Details	196
Stream Resource Control	196
Configure a maximum number of retries and the maximum execution time	197
Configure the stream resource details	198
Chapter 27: Security	200
Configure LW-SSO authentication	201
Configure SAP BusinessObjects Trusted Authentication	202
Configure Logon Banner	203
Chapter 28: Shifts	205
Shift Management	205
Create New Shift	205
Edit Shift	206
View shift information	206
Create a new time shift	207
Modify the time shift	207
Expire a time shift	208
Chapter 29: Aging	209
Aging	209
Configure Retention	209
Configure active retention period	210
Chapter 30: Licensing	211
View license information	212
Obtain a Permanent license key	212
Install the Permanent license key	213
Reactivate SAP BOBJ license and Re-enable the SAP BOBJ Servers	214
Chapter 31: Reporting Platform	216

Access SAP BusinessObjects Central Management Console	216
Access SAP BusinessObjects BI Launch pad	217
Create a password for the Administrator account	218
Troubleshooting BusinessObjects Services	218
Chapter 32: Pending Configuration	219
Chapter 33: Platform Summary	220
View the application server details	221
Chapter 34: Data Collection Status	225
View the data collection status	226
Chapter 35: Data Process Status	227
View the job stream details	229
View the historical stream overview	231
View the historical trend of the streams	232
Chapter 36: Content Health Status	234
Fact Tables Content Pack Component name: <Content Pack Component name>	235
View the installed Content Pack component	236
View the fact table details	237
Chapter 37: Online Help	239
About OBR	239
	240
Part IV: Appendix	241
Additional Administration Details	246
Configuring custom groups	247
Creating custom group	248
Managing dimensions	251
Managing inactive dimensions	252
List inactive dimensions	252
Delete inactive dimensions	252
Managing duplicate dimensions	253
List duplicate dimensions	253
Delete duplicate dimensions	254
Managing dimensions using business key	254
Managing dimensions using natural key	256
Managing inactive or duplicate dimensions in data source	257

List inactive dimensions in data source	257
List duplicate dimensions in data source	257
Configuring downtime in reports	259
Create the downtime XML file	260
Syntax for downtime schedule with one occurrence	261
Syntax for weekly downtime schedule	263
Syntax for monthly downtime schedule	267
Configuring downtime in the past	270
Configuring customer in reports	273
Creating Customer XML	273
Customer XML Example	276
Configuring location in reports	278
Creating Location XML	278
Location XML Example	281
OBR Reports	282
Integrating with Data Sources for Operations Smart Plug-ins	284
Working of the Integration	284
Prerequisites for Generating OBR Reports from the Operations SPIs Data	285
Integrating with Data Sources for Operations Manager i Management Packs	286
Working of the Integration	286
Prerequisites for Generating OBR Reports from the Operations Manager i Management Packs Data	288
OML Policies to Monitor OBR	289
Prerequisites	289
OBR Services Monitored by OML	290
Importing and Deploying OML Policy Templates for OBR	291
Importing Policy Templates to OML System	291
Deploying Policy Templates	292
OMi Policies to Monitor OBR	300
Prerequisites	300
OBR Services Monitored by OMi	302
OMi Policies for OBR	303
Measurement Threshold Policies	303

Service/Process Monitoring Policies	304
Importing and Deploying Policies	304
Importing Policies to OMi System	304
Deploying Linux Policy Templates	308
Deploying Windows Policy Templates	310
OBR Log File Inventory	313
OBR service log files	324
Log file message format	325
Changing Default Passwords	326
Administration Console Log on Password	326
Vertica Database Password	327
Management Database Password	328
SAP BusinessObjects Database Password	329
Send documentation feedback	334

Part I: Introduction

Operations Bridge Reporter (OBR) is a cross-domain historical IT infrastructure performance reporting software. It displays top-down and bottoms-up reports on resource, event and response time across server, network and application environments. It consolidates resource metrics, event metrics, response time data and business service topology data to show how the underlying infrastructure health, performance, and availability affect the performance of the existing IT infrastructure as well as the dynamic IT infrastructure.

For more information about OBR features, functionality and architecture, see the *Operations Bridge Reporter Concepts Guide*.

OBR provides extensive administrative functions that can help you monitor and configure your applications. You can perform these administrative tasks by using the Administration Console, which is the web-based user interface (UI) of OBR.

This guide provides an overview of the Administration Console and guides you through the step-by-step tasks that you have to perform using the Administration Console.

Chapter 1: Role of the Administrator

As an administrator, you must perform the following tasks after you install the OBR software. Here is the priority listing of the required tasks:

- **Configuration tasks**—These tasks are performed immediately after installing the OBR. You must perform these tasks to ensure that OBR is up and running and data collection operations take place according to your requirements. Configuration tasks include:
 - Performing various post-install configuration tasks.
 - Selecting and installing the required Content Packs¹.
 - Configuring your data sources to provide topology information² to OBR for data collection.
 - Configuring the different data collectors to collect fact data based on the collection policies defined in the Content Packs.
- **Monitoring tasks**—These tasks help you monitor the performance of OBR and identify and troubleshoot any problems with the application and the database. Monitoring tasks include:
 - Monitoring the data that is loaded in the OBR database for each installed Content Pack.
 - Monitoring and troubleshooting the data processes.
 - Monitoring the performance and availability of the OBR database and the host platform.
 - Tracking the errors reported by OBR.
 - Monitoring the OBR, SAP BOBJ, and database services.
- **Administrative tasks**—These tasks help you ensure that the OBR's data and database are useful, usable, available, and accurate at all times. Administrative tasks include:
 - Setting up database access and security.
 - Managing the product license.
 - Controlling the execution of data processes.
 - Defining data retention policies for each Content Pack.

¹OBR provides out-of-the-box business intelligent solutions called Content Packs that define the data collection and data warehousing policies. The Content Packs also contain the required information to display reports.

²The relationship between Configuration Items (CIs), such as applications, servers, and system resources in your IT environment.

Chapter 2: Accessing the Administration Console

Log on to the Administration Console

1. Access the Administration Console by typing the OBR host system address in a web browser. The default address is **http://<OBR_Server_FQDN>:21411/OBRApp** where *server name* refers to the name of the host system on which you have installed OBR. In addition, you can use this URL to remotely access the Administration Console from any other system.

For information about the web browser requirements to access the Administration Console, see the *Operations Bridge Reporter Support Matrix*.

2. Type:

Field	Description
Login Name	Name of the OBR administrator. Note: For first-time access, use the default log on name and password. The default log on name is <code>administrator</code> . The default user, <code>administrator</code> , has complete administrative privileges.
Password	Password of the OBR administrator. The default password is <code>1ShrAdmin</code> . Ensure to change the default password before you start using OBR.

3. Click **Log In**.

The Administration Console appears.

If you have logged on to Administrator Console for the first time as `administrator` you can change the default password. Follow these steps:

1. Launch the Administration Console in a web browser using the following URL:

`http://<OBR_Server_FQDN>:21411/OBRApp`

where, `<OBR_Server_FQDN>` is the fully qualified domain name of the system where *OBR* is installed.

The Log on page appears.

2. Enter user name as administrator in **User Name** and 1ShrAdmin as password in **Password**. Click **Log in**. The change password page is displayed.
3. To change the password, click **Change Password** and follow these steps:
 - a. Enter default password in **Old Password**.
 - b. Enter new password in **New Password**.

Note: The new password should have uppercase, lowercase alphabetical characters and numbers with a minimum of six characters in length.

- c. Retype the new password in **Confirm Password**. Click **Change Password**.

The web browser closes after few seconds. Log on to the Administrator Console with your new password for the Administrator user.

Tip: You can update the password policy in the Central Management Console (CMC). Follow these steps:

- a. Log on to the Administration Console using the new password.
- b. Go to **Additional Configurations > Reporting Platform**.
- c. Click **Launch CMC**. The Central Management Console log on page appears. Log on to CMC. OR

You can also log on to the CMC from the URL: `http://<System_FQDN>:8080/CMC`

where, `<System_FQDN>` is the fully qualified domain name of the system where SAP BusinessObjects is installed.

For steps to update the password policy settings, see the *Central Management Console Help*.

Logging out of the Administration Console

To prevent unauthorized access, log out of the Administration Console after use.

From the Administration Console, click **Logout** to log out of the Administration Console. The You are successfully logged out message appears.

Part II: Getting Started

After you install the OBR application, you must perform the configuration tasks to ensure that OBR is operational and can start collecting data from the various data sources. These tasks help you set up the OBR database user account details and define the database schema.

Perform post-install tasks by sequentially configuring the OBR database, creating the configuring the management database and configuring collectors.	A guided configuration wizard to configure the topology and data source immediately after completing the database and time zone configuration.	An overall view of the status of HPE OBR, its associated services, the database, and the host platform.
Configuration Wizard	Data Source Selection Wizard	Dashboard

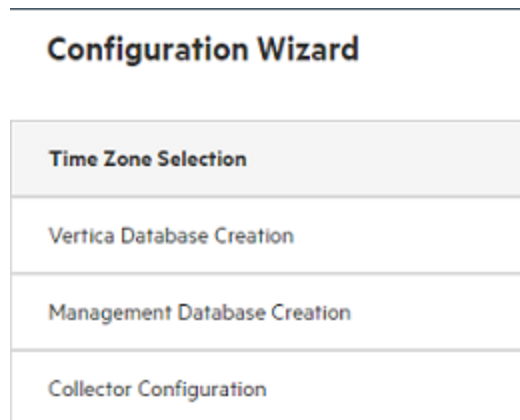
After completing the initial configuration task, you can move ahead with the following modules in the Administration Console:

A guided configuration which helps you to select the required data sources based on the deployment scenario.	Configure the topology and the data sources for OBR data collectors to collect fact data for the various installed Content Pack components.	A single, easy-to-use interface for installing and uninstalling Content packs based on the topology source.
Data Source Selection Wizard	Data Source Configuration	Content Pack Deployment
Perform additional administrative tasks that improve the accessibility, usability, and operability of OBR.	Perform the monitoring of status, data processes, OBR database and the application service platform.	See more information about the HPE OBR Administration Console.
Additional Configurations	Internal Monitoring	Help

Chapter 2: Configuration Wizard

In Configuration Wizard, perform the mandatory OBR post-installation configuration tasks. The wizard sequentially takes you through the steps for configuring the OBR database, creating the database and configuring the management database.

Mouse over the image and click on the sections for more information.



The Configuration Wizard appears when you launch the OBRAdministration Console for the first time. You can access the Administration Console only after you successfully complete the OBR post-installation configuration tasks.

Using the Configuration Wizard, you can perform the following configuration tasks:

- Configure the time zone for OBR.
- Create the database for OBR and configure an administrator user account to access the database.
- Manage the user account for the management database, which is a repository used by OBR to store run-time data such as data processing¹ stream status, changed table status, and node information.
- Configure the collectors for the data collection.

For the step-by-step procedure to perform these tasks, see the *Operations Bridge Reporter Configuration Guide*.

Time Zone Selection

On the Time Zone Selection page, select **GMT** or **Local** time zone, under which you want OBR to operate.

Note: The time zone that you select here applies to the OBR system and reports. However, the run-time information for processes like collection and work flow streams is always based on local time zone irrespective of selection.

For more information, see [Configuration Wizard](#).

¹Data processing refers to a set of best practices in the context of data storage. They have been developed by HPE to improve the quality and control during the loading of data into data stores.

Vertica Database Creation

On the Vertica Database Creation page, you will be able to create the database for Vertica and configure an administrator user account to access the database.

For more information, see [Configuration Wizard](#).

Management Database Creation

The OBR management database (PostgreSQL) refers to the online transaction processing (OLTP) store used by OBR to store its run-time data such as job stream status, changed tables status, and node information. On the Management Database Creation page, you can change the password of the administrator and user account for accessing the management database.

For more information, see [Configuration Wizard](#).

Collector Configuration

In OBR, data collection involves collecting domain-specific data from the various product center repositories such as Operations Manager i (OMi), Business Service Management Profile database, NNMi and Operations agent. The collected data is stored in the OBR database, which is then used for long-term, cross-domain performance analysis and reporting.

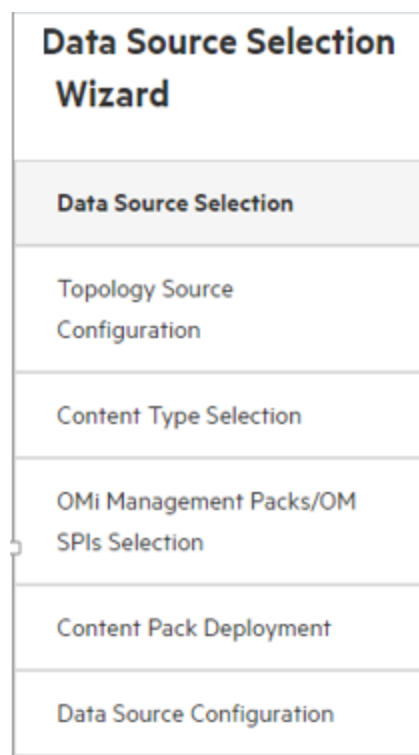
You can use the Collection Configuration page to create and configure a collector that is installed on a remote system (and not on the OBR system).

For more information, see [Configuration Wizard](#) and [Collectors](#).

Chapter 3: Post-install Data Source Selection

The Post-install Data Source Selection Wizard is a web-based user interface (UI) to perform the OBR post-installation configuration tasks. The wizard sequentially takes you through the steps for configuring the data sources, topology source selection and selecting the type of content. Based on the data sources you may use the Data Source Selection Wizard to select the OMi Management Packs or OM SPIs.

Mouse over the image and click on the sections for more information.



The Post-install Data Source Selection Wizard appears after you successfully complete the OBR post-installation configuration tasks.

Using the Post-Install Data Source Selection Wizard, you can perform the following configuration tasks:

- Select the data sources based on the deployment scenario.
- Configure the topology source for the data collection.
- Configure the data source for data collection.
- Select the OMi Management Packs or OM SPIs.
- Install the content packs.

For the step-by-step procedure to perform these tasks, see the *Operations Bridge Reporter Configuration Guide*.

Data Source Selection

On the Data Source Selection page, select the data sources from which the data is collected based on the deployment scenario.

The following table describes the data sources applicable for different deployment scenarios:

Deployment Scenario	Data Source Type
OM	<ul style="list-style-type: none"> • Operations Manager (OM) • Operations Agent • VMware vCenter <i>(optional)</i> • Network Node Manager i (NNMi) <i>(optional)</i>
BSM/OMi	<ul style="list-style-type: none"> • Business Service Manager (BSM) • Operations Manager i (OMi) 10.x <p>Tip: If you have only BSM deployed in your environment, select Business Service Manager (BSM). If you have only OMi 10.x deployed in your environment, select Operations Manager i (OMi) 10.x. If you have both BSM and OMi 10.x deployed in your environment and BSM and OMi 10 systems are integrated, select both Business Service Manager (BSM) and Operations Manager i (OMi) 10.x.</p> <ul style="list-style-type: none"> • SiteScope <i>(optional)</i> • Operations Agent <i>(optional)</i> • VMware vCenter <i>(optional)</i>
VMware vCenter	<ul style="list-style-type: none"> • VMware vCenter • Network Node Manager i (NNMi) <i>(optional)</i>
Other	Network Node Manager i (NNMi)

Note: Customized content is not included in this page.

For more information, see [Data Source Selection Wizard](#).

Configure Topology Source

You can configure the topology source on the Configure Topology Source page.

For information, see [Data Source Selection Wizard](#) and [Topology Source](#).

Content Type Selection

On the Content Type Selection page, select the Content Type that is displayed according to the data source selected.

For more information, see [Data Source Selection Wizard](#).

OMi Management Packs/OM SPIs Selection

On the OMi Management Packs/OM SPIs Selection page, select the OMi Management Packs/OM SPIs Selection that is displayed according to the data source selected.

For more information, see [Data Source Selection Wizard](#).

Content Pack Deployment

This page displays the list of Content Packs that can be installed according to the selected data sources.

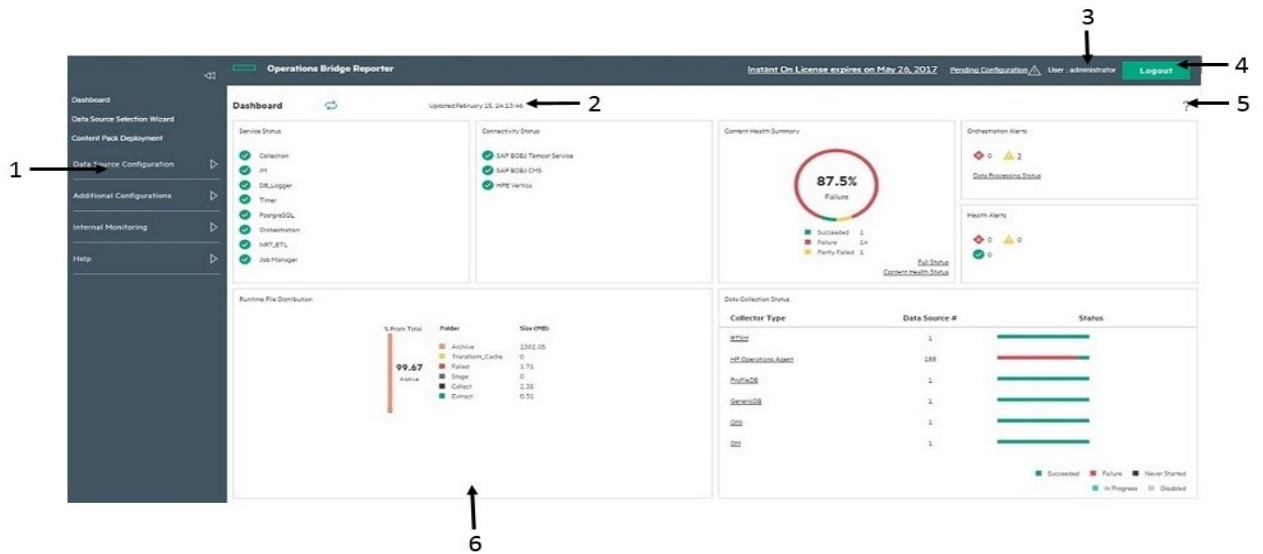
For more information, see [Data Source Selection Wizard](#) and [Content Pack Deployment](#).

Data Source Configuration

The data sources selected in the Data Source Selection Wizard is displayed in the left tab. The data sources can be configured using this page.

For more information, see [Data Source Configuration](#).

Chapter 4: Dashboard



Legend description:

1	Task pane
2	Updated
3	User
4	Logout
5	Help
6	View pane

Task pane

OBR collection configuration, administration, and monitoring options:

- [Dashboard](#)
- [Data Source Selection Wizard](#)
- [Content Pack Deployment](#)
- [Data Source Configuration](#)
- [Additional Configurations](#)
- [Internal Monitoring](#)
- [Help](#)

License details

Summary of the OBR license information.

User

Name of the current OBR user.

Logout










Click to log out of the Administration Console.











Online Help





Use this page to view the *Online Help for Administrators*.

View pane

View the administration, configuration, and monitoring options and attributes.

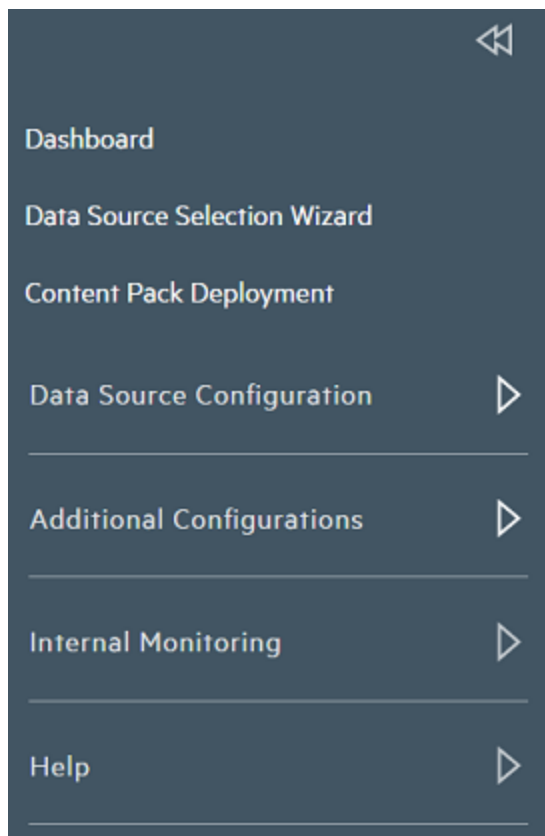
Group	Field	Description
Status Summary	Services Status	<p>Displays the status of the OBR database and SAP BOBJ Enterprise services.</p> <p>Status of the service:</p> <ul style="list-style-type: none">  indicates that all the services are running successfully.  indicates that one or all of the services are not running. <p>The data displayed in this table is refreshed periodically. Click  to update the table with the latest data.</p>
	Connectivity Status	<p>Displays the status of OBR's connectivity to the following components:</p> <ul style="list-style-type: none"> Tomcat service (SAP BOBJ Tomcat Service) SAP BusinessObjects Central Management Service (SAP BOBJ CMS) HPE Vertica (Vertica database service)
	Runtime File Distribution	<p>Displays the data distribution of the OBR file system according to the size of the files in the following folders:</p> <p>Folder</p> <ul style="list-style-type: none">  Archive  Transform_Cache  Failed  Stage  Collect  Extract <p>Before the data collected from the data sources are loaded into the appropriate Vertica database tables, it is held in the OBR system for processing. Also, the data that failed to pass the data processing streams (<code>lstage\failed_to_*</code> folder). are also stored on the OBR file system. Runtime file distribution shows the disk space used by these files.</p>
	Data Collection	Displays the number of data sources that are configured for each

Group	Field	Description
	Status	<p>data collector. The status is represented in the following ways:</p> <p>  Succeeded  Failure  Never Started  In Progress  Disabled </p> <ul style="list-style-type: none"> • Succeeded: When data collection from the data sources occurs without issues. • Failure: When data collection from the data sources has failed. • Never Started: When data collection from the data source has never occurred. • In Progress: When data collection from the data sources is in progress. • Disabled: When data collection from the data sources is disabled. <p>The data displayed in this table is refreshed periodically. Click  to update the table with the latest data.</p>
	Content Health Summary	<p>Displays the graphical representation of the health of data flow from data source into the fact tables associated with the dimensions of installed content packs. The status is represented in the following ways:</p> <p>  Succeeded 1  In Progress 15 </p> <ul style="list-style-type: none"> • Succeeded: When data flow occurs without issues. • In Progress: When data flow is in progress. <p>Click the adjoining link Full Status to view the graphical details or Content Health Status to go to Content Health Status page.</p> <p>The data displayed in this table is refreshed periodically. Click  to update the table with the latest data.</p>
Alerts	Orchestration Alerts	<p>Displays the number of data processing job streams that have failed to complete or with warnings. For more information, see View details of the Orchestration Alerts. The following icons are used to identify the types of alerts:</p> <ul style="list-style-type: none"> •  indicates an error alert. Click the adjoining link to view the details.

Group	Field	Description
		<ul style="list-style-type: none">•  indicates a warning alert. Click the adjoining link to view the details.
	Health Alerts	<p>This table displays the severity, message, and date of the all error, warning, and information alerts generated by OBR. The following icons are used to identify the types of alerts:</p> <ul style="list-style-type: none">•  indicates an information alert. No action is required for this type of alert.•  indicates an error alert. These are critical alerts and immediate action is required to resolve these issues.•  indicates a warning alert. You might need to resolve these types of alerts to ensure functions properly. However, immediate action might not be required.

Chapter 5: Data Source Selection

Mouse over the image and click on the sections for more information.



This is a guided configuration page that helps to select the data sources based on the deployment scenario.

Using the Data Source Selection Wizard, you can perform the following configuration tasks:

- configure the data source for data collection.
- select the content type for the data source.
- select the OMi Management Packs or OM SPIs.

This wizard can be used to select the data sources, content type and OMi Management Packs or OM SPIs if they are not selected during the post-installation. Also, the selections made can be viewed or modified using this page.

For the step-by-step procedure to perform these tasks, see the *Operations Bridge Reporter Configuration Guide*.

Managing Data Source Configuration

Use this wizard to configure the data sources and content types if it is not performed or completed during post-install. You may also view the data sources, content pack type and the OMi Management Packs/OM SPIs Selection made during post-install using this wizard.

The following table provides areas that can be reported on each deployment scenario:

Deployment Scenario	Areas of Monitoring
OM	<ul style="list-style-type: none">• System Performance

Deployment Scenario	Areas of Monitoring
	<ul style="list-style-type: none"> ◦ Operations Agent • Virtual Environment Performance <ul style="list-style-type: none"> ◦ Operations Agent ◦ VMware vCenter • Network Performance • Operations Events <ul style="list-style-type: none"> ◦ OM Events • Enterprise Application Performance <ul style="list-style-type: none"> ◦ Microsoft SQL Server ◦ Microsoft Exchange Server ◦ Microsoft Active Directory ◦ Oracle ◦ Oracle Weblogic Server ◦ IBM Webshpere Application Server
BSM/OMi	<ul style="list-style-type: none"> • System Performance <ul style="list-style-type: none"> ◦ Operations Agent ◦ SiteScope • Virtual Environment Performance <ul style="list-style-type: none"> ◦ Operations Agent ◦ SiteScope ◦ VMware vCenter • Network Performance • Operations Events and KPI <ul style="list-style-type: none"> ◦ OM Events ◦ OMi Events ◦ Service Health • End User Monitoring <ul style="list-style-type: none"> ◦ Real User Monitor ◦ Business Process Monitor • Enterprise Application Performance <ul style="list-style-type: none"> ◦ Microsoft SQL Server ◦ Microsoft Exchange Server ◦ Microsoft Active Directory ◦ Oracle ◦ Oracle Weblogic Server ◦ IBM Webshpere Application Server

Deployment Scenario	Areas of Monitoring
VMware vCenter only	<ul style="list-style-type: none">• Virtual Environment Performance• Network Performance
Others	<ul style="list-style-type: none">• Network Performance

For more information, see the *Operations Bridge Reporter Configuration Guide*.

Data Source Selection

On the Data Source Selection page, select the data sources from which the data is collected.

Note: Customized content is not included in this page.

Content Type Selection

On the Content Type Selection page, select the Content Type that is displayed according to the data source selected.

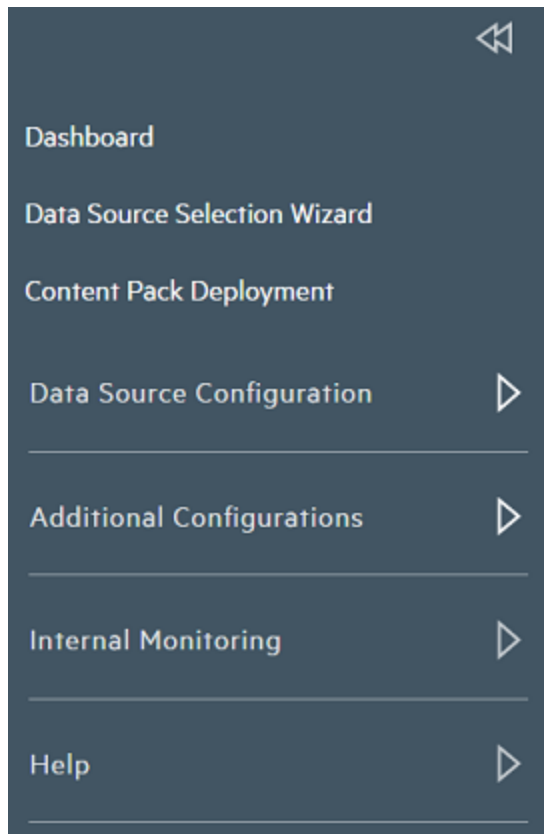
OMi Management Packs/OM SPIs Selection

The OMi Management Packs/OM SPIs Selection tab displays the selection options only when Enterprise application performance is selected in Content Type Selection tab.

For more information, see [Data Source Selection Wizard](#).

Chapter 6: Managing Content Packs

Mouse over the image and click on the sections for more information.



The Content Pack Deployment page simplifies the selection of the Content Packs by filtering them based on the topology source that you defined in the post-install configuration phase. From the filtered list, you can then select the Content Packs or specific Content Pack components that you want to install.

Managing Content Packs

OBR enables you to install and manage Content Packs with the help of the Content Pack Deployment page, a web-based interface that is a part of the Administration Console.

The Content Pack Deployment page provides the following benefits:

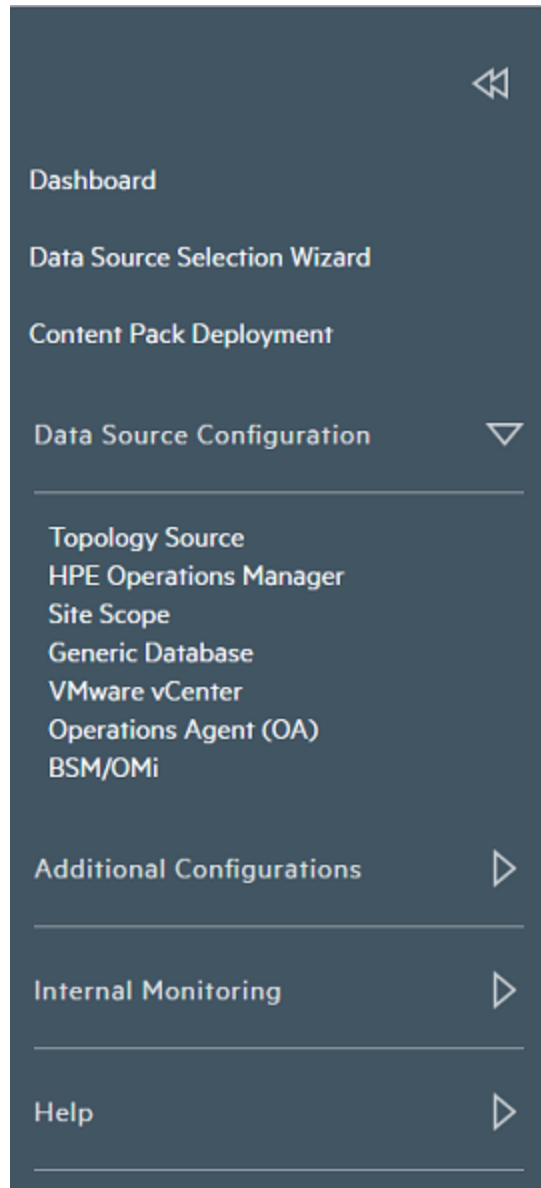
- Gives you more control over how you want to install a Content Pack; whether it is the entire Content Pack or individual components.
- Displays the data source dependencies for each Content Pack

- Supports the installation of custom Content Pack and custom Content Pack components
- Provides a single, easy-to-use interface for installing and uninstalling Content Packs.

For more information, see [Content Pack Deployment](#).

Chapter 7: Managing Topology Source and data collection

Mouse over the image and click on the sections for more information.



Enterprise topology source

Before OBR can start collecting domain-specific data, such as fact data related to applications, databases, and system resources, from the nodes or Configuration Items (CIs), it must first identify and collect the topology information¹ about the managed environment, your business services, and the underlying IT components. Using this information, OBR can align and reconcile the collected fact data for long-term storage, analytics, and cross-domain reporting.

The enterprise topology includes IT components such as applications, servers, databases, and system resources, which are monitored by HPE business service-oriented product, such as Runtime Service Model (RTSM) or OM. These monitored components are called Configuration Items (CIs). Identifying the enterprise topology helps you understand how each of your business services is linked to the underlying CIs. It provides a map of the dependencies of the business services to the IT infrastructure. It helps you track configuration changes.

OBR supports the collection of topology-related data from the following data sources:

- RTSM—is the central repository for the configuration information, which stores and handles the topology and configuration data that is collected and updated through data

¹The relationship between Configuration Items (CIs), such as applications, servers, databases, and system resources in your IT environment.

	<p>Discovery¹ process. The information concerning the discovered CIs and their relationships are used to generate a topology model of all the components that constitute your IT environment on which your business functions.</p> <ul style="list-style-type: none"> • OM—is a distributed, client-server software solution designed to help system administrators detect, solve, and prevent problems that occur in networks, systems, and applications in any enterprise. OM collects data that enable you to maximize IT system performance, reduce downtime, delegate tasks to operators, and reduce costs. OM constantly monitors thousands of events¹ that occur on all your managed nodes¹ and presents just the information you want to know just when you need it. OM uses a component called Service Navigator (SN) to create the topology service tree for the managed nodes and builds the relationship between the nodes and the applications in your environment. • VMware vCenter - is a distributed server-client software solution. It centrally monitors performance and events, and provides an enhanced level of visibility of the virtual environment, thus helping IT administrators to control the environment with ease. <p>The collection of the topology data from these data sources depends on the type of scenario in which OBR is deployed. OBR currently supports three types of deployment scenarios:</p> <ul style="list-style-type: none"> • BSM Operations Bridge • Application Performance Management (APM) • OM <p>If OBR is deployed within the BSM Operations</p>
--	---

¹The mechanism that enables you to collect data about your system by discovering the IT infrastructure resources and their interdependencies. Discovery can discover such resources as applications, databases, network devices, different types of servers, and so on. Each discovered IT resource is stored in the RTSM, where it is represented as a managed CI.

¹A particular fault or incident within the computing environment that occurs on an object.

¹Managed nodes are computers that are controlled and monitored by OM.

Bridge or the APM environment, you must configure the data collector to collect topology data from RTSM. If OBR is deployed in the OM environment, the OM database becomes the source of the topology information for OBR.

For more information about deployment scenarios, see the *Operations Bridge Reporter Configuration Guide*.

Data Collection

In OBR, data collection involves collecting domain-specific data from the various product center repositories such as Operations Manager i (OMi), Business Service Management Profile database, and Operations Agent. The collected data is stored in the OBR database, which is then used for long-term, cross-domain performance analysis and reporting.

OBR provides an open and flexible data collection framework that can be used to collect data from heterogeneous data sources. OBR uses various data collectors to collect the required data:

- Operations Agent collector—Collects system performance metrics for the System Management Content Pack and application metrics for domain-specific applications. The data is collected from the Operations Agents installed on the host systems.
- Database collector—Collects events, messages, availability, and performance Key Performance Indicators (KPIs) from the databases of the data source such as Profile database, Management database, OM database, OMi database, and Network Performance Server (NPS). The database collector can also collect data from generic databases that use Sybase, Oracle, Vertica or SQL Server as the database system. This collector uses the database collector technology to collect the data.

These data collectors work internally within the OBR infrastructure to collect the data. Therefore, you cannot directly interface with these collectors. Instead, you can specify the data sources from

	<p>where the collectors can collect the data through the Administration Console.</p> <p>The Administration Console supports the configuration of these types of data source connections:</p> <ul style="list-style-type: none">• Operations Agent• OM• Generic databases• VMware vCenter• SiteScope• Server/Network Automation• Management and Profile databases and OMi• NNMi/NPS <p>The deployed Content Packs determine the fact data that are to be collected from the various data sources, and the interval at which the data is collected. Configuration of the data source connections for the installed Content Packs depends on the type of deployment scenario used. For more information about the data collection process and what Content Packs are supported for each deployment scenario, see the <i>Operations Bridge Reporter Configuration Guide</i>.</p> <p>For more information on prerequisites and details of each Content Pack, see the respective <i>Operations Bridge Reporter Content Reference Guide</i>.</p>
--	--

Managing the enterprise topology

OBR uses various out-of-the-box collectors to collect topology data:

- RTSM collector — Collects topology information and data about the various CI types in your environment from the RTSM database. The data to be collected is defined by the RTSM view provided with each Content Pack.
- OM collector — Collects topology information and data about the various CI types in your environment from the OM database. The information collected by the OM collector is limited to node list and node groups.

These data collectors collect the required data from the topology sources, which you must configure in OBR. You can create and configure the topology source connections on the Topology Source page of the Administration Console. In addition, you can schedule OBR to collect data from the data repositories at specific intervals. You can also add new data source connections or modify the existing connections.

For more information, see [Topology Source](#).

Managing the OM data collection

OM is a distributed server-client software solution that provides service-driven event and performance management of business-critical enterprise systems, applications, and services. OM centrally monitors performance and events by using agents that are installed on the managed nodes. An agent is a deployment package that helps you manage nodes by collecting data, discovering services, monitoring events, and running actions and commands that control the nodes.

OBR collects event statistics, severity statistics for each of those events, as well as operator statistics, such as how many events were handled by each operator, from the OM database.

For more information, see [Operations Manager](#).

Managing the SiteScope data collection

You can use the SiteScope page to configure a SiteScope data source, which collects data from several SiteScope monitors in your environment. Using this page, you can enable or disable data collection and add or delete the SiteScope application programming interface (API) collector according to your requirement.

For more information, see [SiteScope](#).

Managing collection from generic databases

OBR enables you to configure data collection from any generic database source. Using the Generic Database page, you can configure OBR to connect to and collect data from any generic data source that use Sybase, Oracle, Vertica or Microsoft SQL Server as the database system.

This page is typically used to configure and collect network-related data from the Network Performance Server (NPS) for the Network reports in OBR. The Network Performance Server (NPS) provides the infrastructure that is used in conjunction with Network Node Manager i Software (NNMi) to monitor the operational performance of the network infrastructure. With the performance data collected by different NNMi Software Smart Plug-ins (iSPIs), the NPS builds data tables, runs queries in response to user selections, and displays query results in web-based reports that help you diagnose and troubleshoot problems in your network environment. The NPS enables you to effectively store, access, and track performance data.

Out-of-the-box, OBR supports configuration to generic data sources that use the above-mentioned database types. However, using this page, you can configure OBR to connect to and collect data from other generic database types as well such as MySQL, PostgreSQL, Sybase, and so on. For a particular database type, you can specify the domain for which you want OBR to collect data such as system data, network data, and so on. For more information on how to configure such data sources, contact HPE Support.

For more information, see [Generic Database](#).

Managing the VMware vCenter data collection

VMware vCenter is a distributed server-client software solution that provides a central and a flexible platform for managing the virtual infrastructure in business-critical enterprise systems. VMware vCenter centrally monitors performance and events, and provides an enhanced level of visibility of the virtual environment, thus helping IT administrators to control the environment with ease.

OBR collects event statistics, severity statistics for each of those events, as well as operator statistics, such as how many events were handled by each operator, from the VMware vCenter database.

Note: It is recommended to set the VMware stats logging level to 2. If the logging level is set to 1, then some of the metrics of logging level 2 may not be available in OBR reports. For information on logging levels and their corresponding metrics, use the URL:

<https://communities.vmware.com/docs/DOC-5600>

For more information, see [VMware vCenter](#).

Managing the Operations Agent data source data collection

OBR reports on various facts collected from the Operations Agent managed nodes. The Operations Agent collects, summarizes, timestamp¹, and detects alarm conditions on current and historical resource data across your system. These agents provide performance, resource, and end-to-end transaction response time measurements, and support network and database measurement information.

Operations Agent data sources

OBR integrates with Operations Agent to collect historical system and application-performance data. Depending on the deployment scenario, RTSM or OM discovers the hosts on which the agent is installed and running. OBR uses an Operations Agent data collector to collect the fact data from the hosts. The list of metrics to be collected from each Operations Agent host is identified by the Content Packs.

For more information about Operations Agent, see the Operations Agent documentation.

Managing the data collection

You can use the Operations Agent configuration page of the Administration Console to manage the Operations Agent data collection. You do not need to create new agent data source connections because, by default, OBR discovers all the nodes on which Operations Agents are installed during the topology data collection phase. These discovered agent data sources or nodes are listed in the Operations Agent Data Source page.

For more information, see [Operations Agent](#).

¹The process of recording timestamps that is the time at which an event occurred in the system. Timestamps are typically used for logging events.

Managing the Management, Profile, and Operations Database data collection

You can configure OBR to collect data from the following Business Service Management data repositories:

- **Management database:** The Management database stores system-wide and management-related metadata for the Business Service Management environment.
- **Profile database:** The Profile database stores raw and aggregated measurement data obtained from the Business Service Management data collectors. The Profile database also stores measurements collected through OMi, BPM, RUM, and Service Health.
- **Operations database:** The Operations database stores event, KPI and HI data obtained from OMi 10 data source.

OBR supports the configuration of and data collection from multiple Profile databases. You might have set up multiple Profile database in your Business Service Management environment for scaling purposes—one database might not be enough to store all the data—or for data separating—all critical data in one Profile database and all non-critical data in another. The information about the various Profile databases deployed in your environment is stored in the Management database.

For more information about the Management and Profile databases, see the *Business Service Management Database Guide*.

You can use the BSM/APM/OMi page of the Administration Console to configure the data source connections. To configure the multiple Profile database connections, you only need to configure the Management database on the BSM/APM/OMi page. After the Management database data source connection is configured, OBR discovers all the deployed Profile databases and lists them on the BSM/OMi page.

Managing the OMi data collection

OMi combines business-service management and infrastructure management so that you can monitor and manage a wide variety of problems that occur in your IT environment from different but complimentary perspectives at the same time. OMi generates Health Indicators (HIs) for the CI types in your environment, which provide a detailed status of a CI type. These HIs are mapped with the events that are generated by other domain manager products in your environment such as Network Node Manager (NNM), SiteScope, and OM. The HIs are used to calculate the KPIs of a CI type, which

displays the aggregated state of a CI type. The KPIs represent the high-level health of the CI types to the operator and shows the health and event summary of your business.

OMi data

OBR collects the historical HI and KPI values against RTSM instances from the Business Service Management Profile database over a period of time and displays the trend of these values through reports and dashboards. OBR uses the database collector to collect the historical HI and KPI values from the Profile database. The KPI names, HI dimension details, and value details are collected from the BSM Management database.

For more information about OMi, see the OMi documentation.

Prerequisite for Management Packs

To view reports for the following OBR content packs that gather data from the OMi10 data source, the corresponding Management Packs must be installed:

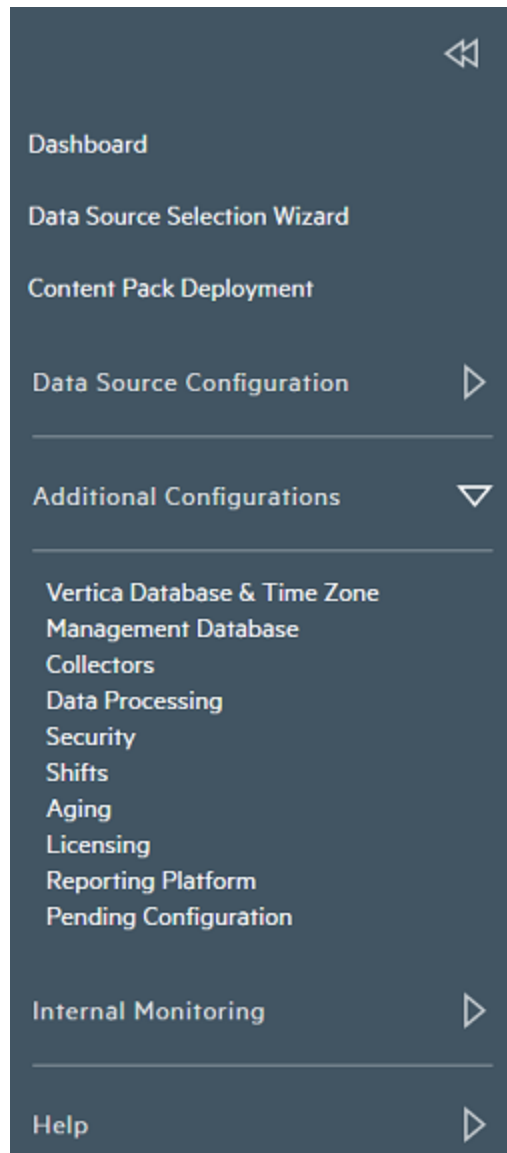
- Microsoft Active Directory
- Microsoft Exchange
- Microsoft SQL Server
- Oracle
- Oracle WebLogic
- IBM WebSphere

Installing these management packs is also mandatory to view OBR reports for Service Health and OMi.

For more information, see [BSM/APM/OMi](#).

Chapter 8: Additional Configurations

Mouse over the image and click on the sections for more information.



Using the Administration Console, you can perform additional administrative tasks that improve the accessibility, usability, and operability of OBR.

You can use the Administration Console to perform the following administrative tasks:

- View the database credentials.
- View the licensing details.
- Configuring secure authentication.
- Control the execution of the work-flow job streams.
- Manage user accounts.
- Configure the data retention period.
- Manage the OBR services.
- Configure the time shifts.
- Installing and managing Content Packs.
- Configuring Collector installed on a remote system.
- Manage Pending Configuration.

Managing Vertica Database

Vertica database and Time zone involves managing the centralized OBR database and the time zone configuration of OBR. The OBR database stores fact and topology information collected from different data sources based on the policies that are defined in the Content Packs. The database is configured when you perform the post-install configuration steps after installing the OBR application.

For more information, see [Vertica Database and Time Zone](#).

Managing Management Database

Management Database involves managing the OBR management database. The database is configured when you perform the post-install configuration steps after installing the OBR application.

For more information, see [Management Database](#).

Configuring Collector

You can use the Collectors page to create and configure a collector that is installed on a remote system (and not on the OBR system).

For more information, see [Collectors](#).

Managing data processes

Using the Data Processing page of the Administration Console, you can view the number and status of the job streams corresponding to each installed Content Pack. You can also configure the job streams and specify a maximum number of retries for the batches in the event of its failure during execution as well as a maximum execution time per step. When the number of retries for a job step exceeds the maximum number allowed, the workflow framework blocks the job stream and generates an error event.

The maximum execution time and maximum retries are two configuration parameters that directly impact the stream execution functionality. In the case of the maximum execution time, setting a very high value can result in delay in identifying hanged processes. Setting a low value can result in the step being marked as Error too often. In addition, the maximum retries option should be set to a positive

value only if a retry could result in successful execution. This option is most commonly used to overcome resource unavailability issues.

However, the best way to arrive at the value for the configuration parameters is to understand the use case, test, and arrive at an optimum value.

The number of job steps that are run simultaneously in the workflow framework is proportional to the number of job streams under execution. However, if the number of streams deployed on a system is high, it can result in a very high load on the system, which can lead to system failure. In such a situation, the resource control feature of data processing helps mitigate problems caused by the high load by providing the ability to limit resource usage to configured limits.

By managing the job stream resources, you can:

- Provide exclusive access to resources and help resolve locking issues with critical resources. If the pool count is zero, then the access to the resource becomes exclusive.
- Control the number of processes that are launched. For example, if you set a pool count of “5” for a resource named “Summary” and attach the resource to all the data aggregation jobs, then only a maximum of five instances of five aggregations can run at any point of time. This way, you can control the number of processes that are running.

You can also specify the resource definition details and set limits for the number of streams that can access the resource types concurrently. By default, all resource types are configured with the unlimited count, which means that there is no control based on the resource type.

For more information, see [Data Processing](#).

Managing security

OBR provides seamless access to integrated HPE and SAP BusinessObjects applications through Lightweight Single Sign-On (LW-SSO) and SAP BusinessObjects Trusted Authentication.

LW-SSO

Single Sign-On allows you to log on once to OBR and gain access to multiple integrated HPE products or software systems without being prompted to log on again. The products within the configured group of products trust the authentication, and there is no need for further authentication when moving from one application to another. All requests to integrated applications are channeled through the LW-SSO authentication.

LW-SSO is embedded in OBR and does not require an external machine for authentication. You need only to specify the shared key (Init String¹), which is used for encryption and decryption of the LW-SSO session token². You must ensure that the other applications in the Single Sign-On environment have LW-SSO enabled and are working with the same Init String.

OBR supports LW-SSO authentication with the following HPE products:

- Business Service Management
- OM
- OMi

Note: In OBR, all applications participating in an LW-SSO integration must use the same GMT time.

SAP BusinessObjects Trusted Authentication

SAP BusinessObjects Trusted Authentication facilitates single sign-on between OBR and SAP BusinessObjects applications. Applications that have established trust with the SAP BusinessObjects Central Management Server (CMS)³ can use Trusted Authentication to allow users to log on without providing their passwords.

To use single sign-on, you must specify the SAP BusinessObjects shared key (Shared Secret), which is used for encryption and decryption of the Trusted Authentication session token. You must ensure that all the other applications in the Trusted Authentication environment have Trusted Authentication enabled and are working with the same shared key.

OBR supports Trusted Authentication with the following SAP BusinessObjects applications:

- SAP BusinessObjects Central Management Console (CMC)
- SAP BusinessObjects Launch pad

For more information, see the *SAP BusinessObjects Enterprise Administrator's Guide*. For the latest documents, see <http://help.sap.com/bobip41?current=bobip41>.

¹Init String is a connection string that contains the initialization information. This information is passed as a parameter from the data provider to the data source while attempting to open a connection with the data source.

²A session token is a unique identifier—8-byte binary value—that is generated and sent from a server to a client to identify the connection between the server and the client.

³The CMS is a key component of the SAP BusinessObjects Enterprise XI that is bundled with HPE OBR. It is responsible for handling security and managing services. The CMS maintains a database which contains information that helps you manage the SAP BusinessObjects Enterprise infrastructure.

Logon Banner

After completing the post installation configuration, using the Logon Banner you can configure the text that you prefer to be displayed when you log on to the Administration Console and SAP BusinessObjects in Operations Bridge Reporter. This text appears as the first screen and warns the user against unauthorized entry.

For more information, see [Security](#).

Managing time shifts

Using OBR, you can configure the shift timings and enable shift-based availability reporting for the monitored system resources in your environment. Out-of-the-box, OBR defines a default shift period, which ranges from 0 to 23 hours.

Using the Shift Management page of the Administration Console, you can define the shift timings. Once configured, the shifts are applied globally across all relevant reports.

When configuring the shifts, you must consider the following points:

- Shift-based data is available to a maximum of the initial history (by default, this is set to 15 days) prior to the current date when the shift is created.
- You can modify the start and end times of the shifts.
- A shift must have a time range defined.
- The value must be in the 24-hour format.
- You can define multiple shifts.
- A single shift can have multiple time ranges.
- Shifts can have overlapping time ranges.
- You can delete a time range from the shift.
- If you delete a shift, all the time ranges within that shift are also deleted.
- You cannot create a shift that has the same name of an existing shift.
- Time ranges that do not correspond to any shift is referred to as off-shift.
- Node or group-level shift configuration is not supported.

For more information, see [Shift Management](#).

Managing data aging

OBR collects data from different data sources at periodic intervals based on the collection policies predefined in the Content Packs. The collected data is stored in the database in various types of fact tables. If the data is collected as polled events from the data source, it is called raw data and stored in "As-polled" tables. Data can also be collected as a 5-minute summarized data. This type of data is called rate data and stored in "5-minute" tables.

The OBR database performs aggregation routines on the raw or rate data through the workflow process. The aggregation routines convert the data into hourly and daily data. This data is then stored in the following physical data tables:

- Hourly—This table contains the raw or rate data that is aggregated at an hourly level.
- Daily—This table contains the hourly data that is aggregated at the daily level.
- Monthly—This table contains the daily data that is aggregated at the monthly level. (not available in OOTB content packs)
- Yearly—This table contains the monthly data that is aggregated at the yearly level. (not available in OOTB content packs)

When reports are generated for a month or year, the data from daily tables is aggregated online to display in the OBR reports. Monthly table and yearly table are not physical tables in the database for any out-of-the-box (OOTB) content packs.

The data tables vary based on the content pack. For a given content pack, the available data tables is based on the model defined for that content pack.

Active retention

To prevent the accumulation of excessive data in the tables, OBR ages the data. Aging involves the concept of retention time, which is the number of days the data is stored in the table. The aging process deletes the data when it has been in the table longer than the specified retention time for that table.

Each table has a default retention time:

- As-polled table: 90 days
- 5-minute table: 90 days
- Hourly table: 365 days
- Daily table: 1825 days
- Monthly table: 1825 days (not available in OOTB content packs)
- Yearly table: 1825 days (not available in OOTB content packs)

Note: Dimension data such as CI types and nodes that is collected by OBR remains in the database tables. OBR does not delete this data.

For more information, see [Aging](#).

Managing licenses

By default, OBR includes a temporary, instant-on license, which is valid for 60 days. To continue using OBR after 60 days, you must install a permanent license.

The OBR license includes:

- **Operations Bridge Reporter Software:** This license includes the data collection framework, the SAP BusinessObjects Enterprise, a high-performance Performance Management Database for storing and processing the collected metrics, and the out-of-the-box Content Packs. Also included is an entitlement to collect and report on the metrics for up to 50 nodes.
- **Additional scalability packs of 50 nodes:** Additional data collection and reporting entitlements can be added to grow the solution to fit your environment.

OBR is integrated with the HPE License Manager licensing package for its licensing needs. The HPE License Manager provides the OBR license framework and the functionality of installing a temporary or permanent license.

Basic license information is displayed on the Licensing page of the Administration Console. To obtain a permanent license, you can either use the HPE License Manager or directly retrieve the license from the HPE Licensing Center by using the HPE Webware web site.

Note: If you uninstall Content Pack, run the Dimension Life cycle (DLC) to get the correct license usage count in the **Administration > Licensing** page of Administration Console.

For more information on licensing, see *Licensing Requirement for OBR* section in the *Operations Bridge Reporter Configuration Guide*.

For more information, see [Licensing](#).

For steps to activate the license using CLI, see *Activate License from Command Line Interface* in the *Operations Bridge Reporter Configuration Guide*.

Managing user accounts

In OBR, user accounts are managed by using the SAP BusinessObjects Central Management Console (CMC). By default, OBR includes an Administrator account, which is created during the post-install configuration stage. The Administrator account is a privileged account for managing and configuring OBR. Only accounts with administrative privileges can log onto the Administration Console. You can create additional accounts with administrative privileges by using the SAP BusinessObjects CMC.

SAP BusinessObjects CMC

You create and manage user accounts by using the SAP BusinessObjects CMC, which is integrated with OBR. After you create user accounts and groups, you can specify access rights to them.

Using the SAP BusinessObjects CMC, you can perform the following user management tasks:

- Manage enterprise and general accounts
- Add users to groups
- Manage passwords
- Manage aliases

For more information, see the Central Management Console documentation. This guide is located in the installation directory of SAP BOBJ at:

Windows: <drive>\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Help\en

Linux: \$PMDB_
HOME/BOWebServer/webapps/BOE/WEBINF/eclipse/plugins/webpath.CmcAppBranding_lang.en/web/help/en

For the latest help documents, see http://help.sap.com/businessobject/product_guides/.

SAP BusinessObjects BI Launch pad

SAP BusinessObjects BI Launch pad is the central web-based GUI in OBR that allows you to view and interface with reports and dashboards. You can use the integrated search facility or the folder navigation tree to locate specific reports. In addition, BI Launch pad allows you to personalize your experience by customizing the Start page to display reports that you want to view when you log on, change your password, choose your preferred language, and the level of interaction for different information.

For additional information and the latest help documents about SAP BOBJ Launch pad, see <http://scn.sap.com/docs/DOC-19231>.

For more information, see [Reporting Platform](#).

Managing Pending Configuration

This page helps you to verify if the OBR configuration is complete.

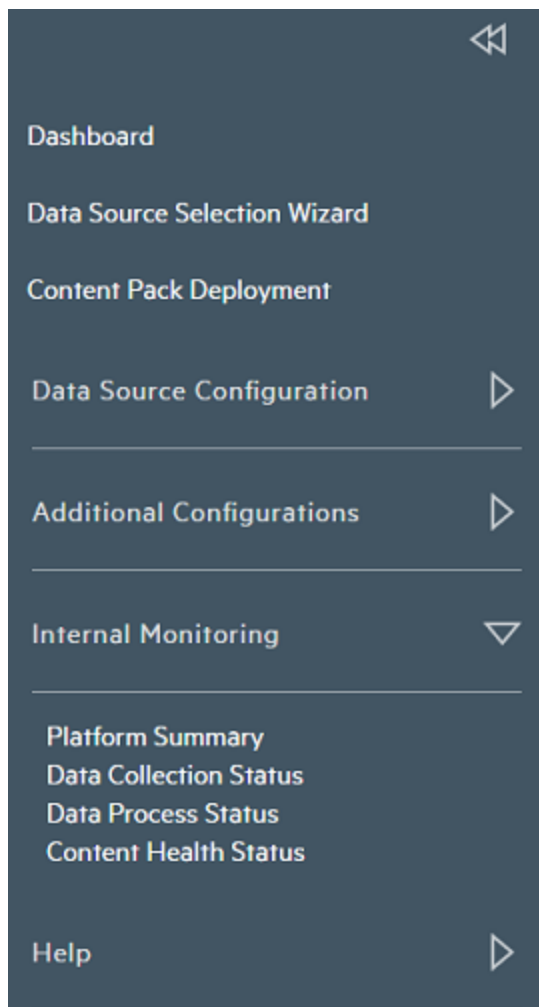
After completing the post-installation configuration and selecting the topology, you can configure or install remaining package using the Pending Configuration page. You can also see the configurations that are not completed and configure them through this page.

If any of the configurations are listed in this page that are pending, click on the subsequent links to complete the configuration.

For more information, see [Pending Configuration](#).

Chapter 9: Monitoring OBR

Mouse over the image and click on the highlighted sections for more information.



After you perform the initial tasks to get OBR up and running, your next task is to monitor the OBR to ensure that it functions properly.

You can use the Administration Console to perform the following monitoring tasks:

- View the status of OBR.
- Monitor the OBR content.
- Monitor the data processes.
- Monitor the OBR database.
- Monitor the application server platform.

Internal monitoring not only helps you identify the problematic processes or utilities that take a long time to run but also identify specific nodes where the data is stuck. If something goes wrong at the collection, reconciliation, or aggregation level, this feature helps you precisely identify the nodes where the problem occurred. You can also view the trend of usage of the database and the application server platform and a trend of the different data processes.

Monitoring the OBR content

In OBR, a fact table consists of the measurements or facts of a business process. It is often located at the center of a star schema or a snowflake schema, surrounded by dimension tables. The dimension tables contain attributes (or fields) used to constrain and group data when performing data processing queries. Fact tables are often defined by their grain. The grain of a fact table represents the smallest

level by which the facts may be defined. For example, the grain of a CPU fact table might be stated as CPU utilization every five minute or CPU utilization every day. In the OBR database, the raw data or rate data that is collected is stored as unique records in fact tables called "As-pollled" table or "5-minute" table. The workflow process then performs summary routines on these tables and converts it into hourly, daily, monthly, and yearly data. The converted data is stored in hourly, weekly, monthly, or yearly fact tables.

Note: Monthly table and yearly table are not physical tables in the database for any out-of-the-box (OOTB) content packs.

OBR allows you to monitor the data throughput, that is, the volume of data that is stored in the database, for specific Content Pack component. Using the OBR Content page, you can monitor the growth of the fact tables for a specific Content Pack component.

For more information, see [Content Health Status](#).

Monitoring Data Collection Status

You can use the Data Collection Status page to view a summary for the time of the last data collected by Operations Agent data source. This page displays the time stamp of when the last data was pulled from the Operations Agent Content Pack Component. You can also view information about the data source, the class, and the last data time performed by the Operations Agent Content Pack Component.

The Data Collection Status page of the Administration Console provides a detailed status of last polled data of the Operations Agents content pack component that is installed.

Note: This page will not display any details if the Operations Agents content pack component is not installed

For more information, see [Data Collection Status](#).

Monitoring the data processes

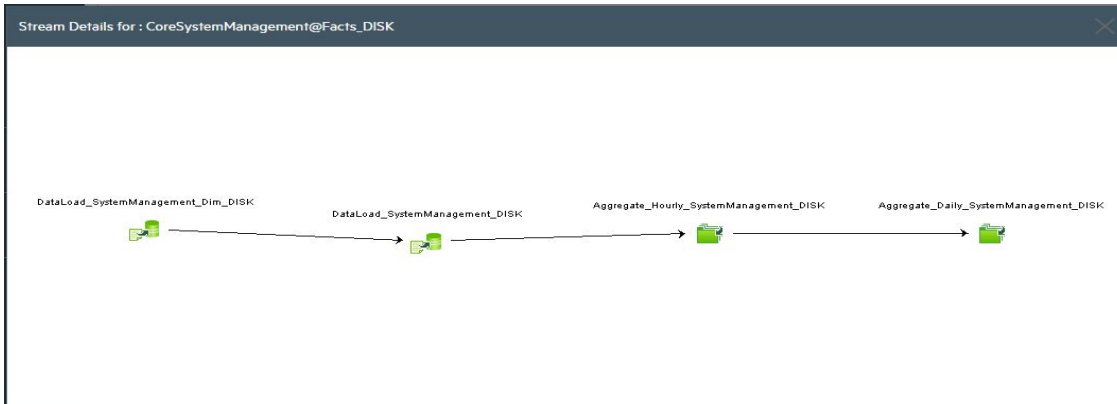
OBR provides a workflow framework that handles the tasks of taking raw data, running reconciliation and aggregation routines on it, and then loading the data into the data store. The Content Packs contains the predefined workflow job streams¹ that are loaded into the framework during the

¹A set of workflow execution tasks related through parent-child relationships. A child task can have zero, one, two, three, or more parent tasks.

installation of the Content Pack. A job stream is made up of multiple job steps, which are processed in batches¹ by the workflow framework.

The workflow framework centrally organizes and manages the flow and the execution of the steps that each job stream based on metadata defined in the Content Packs.

The following figure illustrates the execution flow of a sample OBR job stream.



In this example, the job stream starts from data collection and ends with facts aggregation. All steps are dependent on the preceding steps; therefore, in the event of a failure on one of the steps, the workflow framework prevents the job stream from completing successfully. The workflow framework loads the next job stream for execution only after the current stream completes successfully.

Using the workflow framework, you can:

- Monitor the status of the execution of the workflow.
- Control the processes that move data into the data store.

Knowing how the workflow job streams perform becomes the most important task in monitoring the status of the OBR database operations.

Monitoring job stream details

OBR provides you with a way of monitoring the execution of the job streams of each installed Content Pack. The Data Process Status page of the Administration Console displays stream information under the following three tabs:

- Stream Details—This tab displays information about the status of active streams that are currently running. You can also view the step-wise execution flow of the job stream.

¹A run-time instance of a job stream is called a batch.

- **Historical Stream Overview**—This tab displays number and status of the job streams that completed with errors or with warnings. Job streams that were aborted by the user because of it warning or error state, also appear on this tab.
- **Historical Streams Details**—This tab displays a graphical trend of the number of error and warning states encountered by a job stream during its execution over a period of time.

Using the Data Process Status page, you can monitor the execution of the active job streams and troubleshoot any issues if the execution fails. In addition, you can perform a trend analysis for the stream over a period of time to identify the cause of the failure.

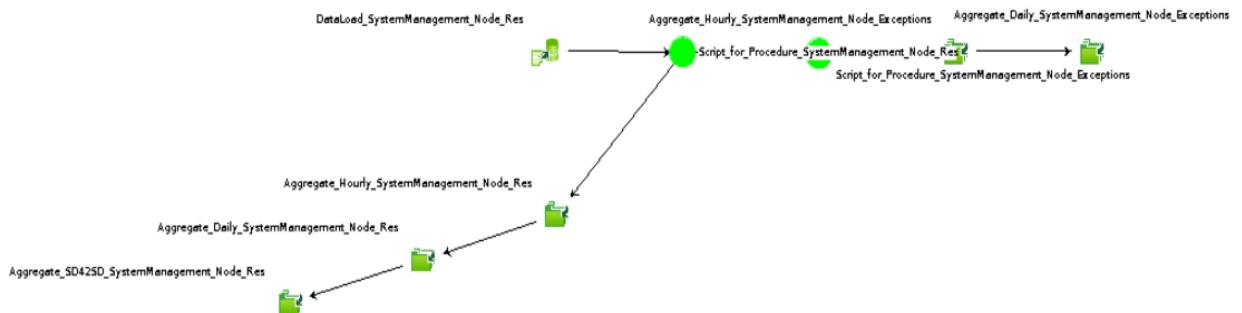
For more information, see [Data Process Status](#).


Understanding the job stream status

To help you understand the information displayed on the Data Process Status page and the relationship between the states and statuses of the job streams, sample possible job stream scenarios are provided.

Scenario 1

Consider the following sample job stream.




This job stream contains eight job steps. All of the job steps completed successfully, as indicated by the green color. In the **Completed/Total** column, the value for this stream will be 8/8 because there were eight steps and all the steps completed execution. The **Step Status** column displays the  indicator because all the job steps completed successfully. Therefore, the job stream status is OK. Now, let's look at another scenario

Scenario 2

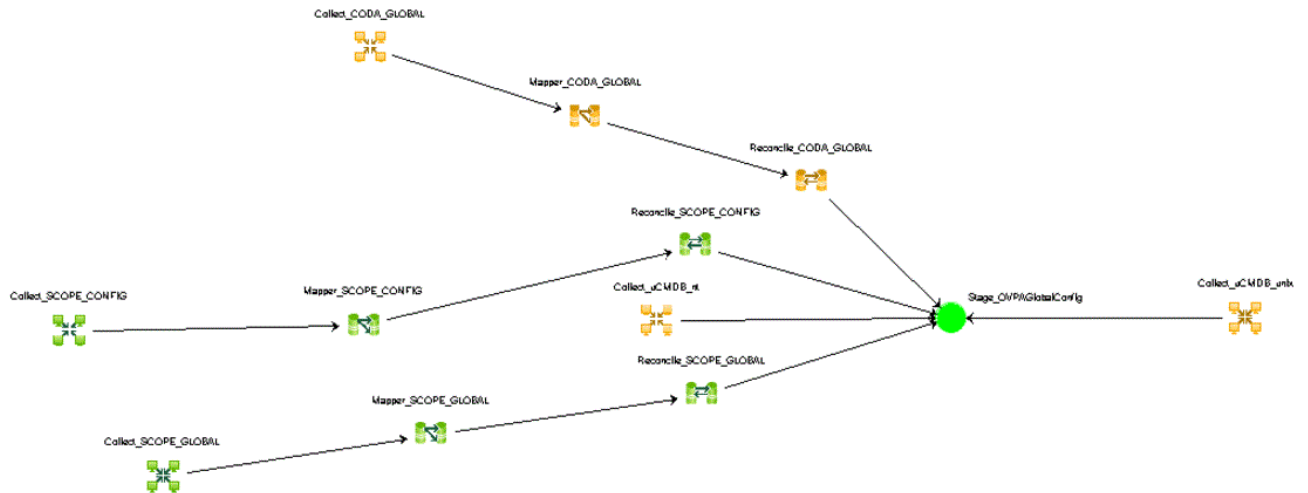
Consider the following sample job stream.




This job stream contains 3 job steps. In the **Completed/Total** column, the value for this stream will be 1/3 because only one step is complete. The second step, **Aggregate_Hourly**, is currently running, as indicated by the blue color. However, the **Step Status** column displays the  indicator. This is because the first job step **DataLoad** completed successfully.

Scenario 3

Consider the following sample job stream.

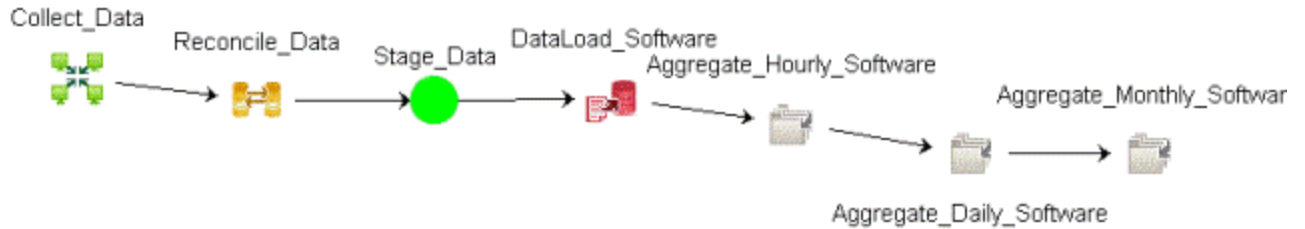



This job stream contains twelve job steps. In the **Completed/Total** column, the value for this stream will be 12/12. However, the **Step Status** column displays the  indicator because few job steps

completed with few warnings. However, this does not block the job stream and, as you can see, the Stage_OVPAGlobalConfig job step completed successfully.

Scenario 4

Consider the following sample job stream.



This job stream contains seven job steps. In the **Completed/Total** column, the value for this stream will be 4/7. However, the **Step Status** column displays the  indicator because the DataLoad_Software job step failed to complete. A failed job step continues to block the execution of the remaining steps until it is resolved. Therefore, only four job steps are complete in this stream.

Back up and restore OBR PostgreSQL management database

The OBR PostgreSQL management database stores three types of information:

- Data processing stream information
- Internal tables that control the deletion of stage tables (stage_control)
- Collection audit information (Data Audit)

Backing up the database

You might want to back up the management database for data recovery purposes. To back up the database, follow these steps:

1. Stop the PMDB Platform Timer service.
2. Stop the PMDB Platform Collection service.
3. Wait for all the loaded data processing stream processes to stop running.

4. Check the status of the streams on the Data Processing page of the Administration Console. You can also check the status by typing the following command:

```
abcMonitor -stream ID=ALL, state=active
```
5. Back up the database using a PostgreSQL database backup utility.

Restoring the database

You might want to restore the management database to get the historical step execution status details. To restore the database, follow these steps:

1. Stop the PMDB Platform Timer service.
2. Stop the PMDB Platform Collection service.
3. Wait for all the loaded data processing stream processes to stop running.
4. Check the status of the streams on the Data Processing page of the Administration Console. You can also check the status by typing the following command:

```
abcMonitor -stream ID=ALL, state=active
```
5. Restore the Management database using a PostgreSQL restore utility.
6. Restart the PMDB Platform Collection Service and the PMDB Platform Timer service after the restore operation is complete.

After the services are started, the data processing framework automatically starts executing the restored steps from where it stopped, handling the Step status automatically. Restoration of the old database also results in old data for the stage_control and data audit tables. However, these tables are automatically updated by the framework within a couple of hours.

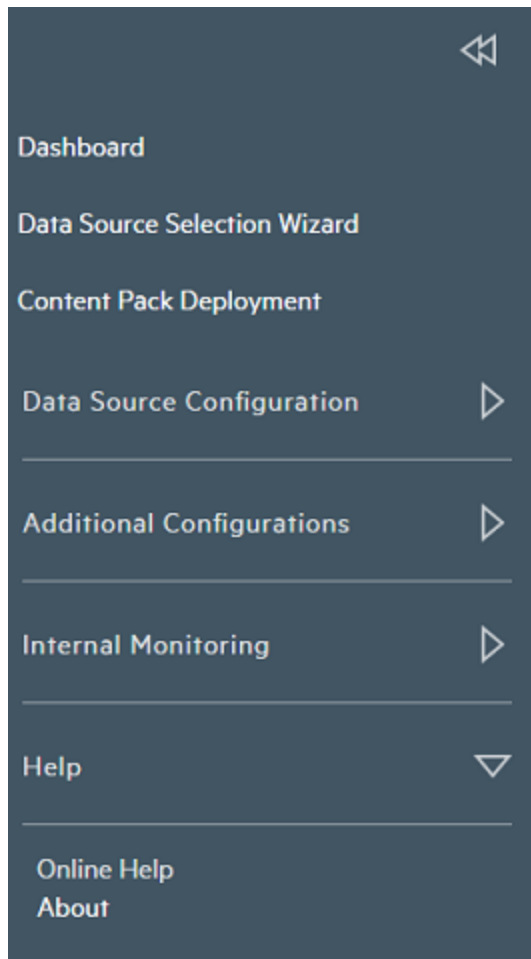
Monitoring the application platform

The Platform Summary page of the Administration Console enables you to monitor the Administration Console's application server. Monitoring the application server platform provides data to diagnose the cause of poor application performance.

For more information, see [Platform Summary](#).

Chapter 10: Help

Mouse over the image and click on the sections for more information.



You can see the following information from the Help page of the Administration Console:

- About the version of OBR
- Online Help for Administrators

Online Help

Use this page to view the *Online Help for Administrators*.

About OBR


This page displays the details about the PMDB Platform.

The About page includes:

Field	Description
Version	The version number of the product.
Patch Level	The patch level for the version number of the product.
Build Number	The build number of the product.

Part III: Administration Console Screens

This section lists the context-sensitive Help pages for the different Administration Console screens. These Help pages provide an overview of the screens that are present in the Administration Console.

You can directly launch these Help pages for a particular screen by clicking the  icon on the top-right corner of the screen.

Chapter 11: Configuration Wizard

The Configuration Wizard appears when you log on to the Administration Console for the first time or if the post-install configuration is not complete in the previous session. Using Configuration Wizard, you can complete the post-install configuration of your OBR system.

The Configuration Wizard includes:

Time Zone Selection:

Field	Description
<ul style="list-style-type: none">• GMT• Local	Select Time Zone from the given options

Vertica Database Creation

Field	Description
Remote Database	Select the check box only if the Vertica database is installed in a separate server or if Vertica is not is the same server as OBR server.
Host name	The host name of the system where the Vertica database is installed.
Port	The port number of the system where the Vertica database is installed. Default port is 5433.
Database File Location	The location where the database files will be stored. Note: This field will be disabled if the Remote Database check box is selected.
Catalog File Location	The location where the database meta data information will be stored. Note: This field will be disabled if the Remote Database check box is selected.
Database Name	Name of the Vertica database. By default, it is PMDB. You can edit the Vertica database name.
DBA User Name	Vertica database user name with DBA privilege to log on to Vertica database. If you have already created the Vertica user, enter the user name and password in the respective fields. Otherwise, enter the username and

	password details for the Vertica user to be created. Note: This field does not appear if the Remote Database check box is selected.
Password	Vertica database password to log on to the Vertica database. Note: This field does not appear if the Remote Database check box is selected.
Confirm Password	Retype the password for confirmation. Note: This field does not appear if the Remote Database check box is selected.
User name	Type the Vertica database user name.
Password	Type the Vertica database user name password.
Confirm Password	Retype the password for confirmation.

A confirmation dialog box is displayed. Click **Yes** to create the Vertica Database schema.

For more information on different scenarios to Create Vertica Database, see *Creating the Vertica Database Schema* section in *Operations Bridge Reporter Configuration Guide*.

Management Database Creation

Management Database User (DBA privilege) and password:

Field	Description
User name	Name of the PostgreSQL database administrator (DBA Privilege). The default value is postgres .
New DBA Password	Password of the PostgreSQL database administrator.
Confirm New DBA Password	Retype the password for confirmation purpose.

Management Database User Information:

Field	Description
User name	Name of the OBR management database user. This field is disabled and the default value is pmdb_admin .
New Password	Password of the OBR management database user.
Confirm New Password	Retype the password for confirmation purpose.

A confirmation dialog box is displayed. Click **Yes** to create the management database user account.

Collectors Configuration

Field	Description
Name	Display name of the collector. (Note: it cannot be changed once configured)
Host Name	Collector host name.
Enable	To enable or disable the collector that is installed on the remote system. If a data source has already been assigned to any the collector for data collection, then the application will not allow you to disable the collector.
Connection	To test the connection between OBRsystem and the remote system where the collector is installed.
Install	It indicates whether the collector is installed.
Policy	It indicates whether all necessary collection policies are installed on the collector system. If necessary policies are not present for a remote collector, click the  icon to synchronize the policy.
Data Source	It indicates whether any data sources are configured with the collector. Click the  icon to synchronize the data sources for a remote collector.
Test Connection	Test a Collector connection.
Create New	Create a new remote collector connection by entering the configurations parameters.
Edit	Edit the collectors configured.
Delete	Delete a remote collector configured for data collection.
Save	Save the changes made to the collectors.

For more information, see [Collectors](#).

You can proceed with the Data Source Selection Wizard to configure the data sources or go to Dashboard and configure data sources later.

Chapter 12: Data Source Selection Wizard

The Post-install Data Source Selection Wizard appears when you select to configure the data sources immediately after completing the Configuration Wizard. Using the Data Source Selection Wizard, you can complete the post-install configuration of your data sources, topology source selection and selecting the type of content. Based on the data sources you may use the Data Source Selection Wizard to select the OMi Management Packs or OM SPIs.

Note: If you refresh the browser while performing selections in the Data Source Selection Wizard, the Dashboard page appears. You can continue to perform the data source selections using the Data Source Selection Wizard available in the Administration Console.

Use the Data Source Selection Wizard to configure the following data sources based on the deployment scenario:

- [OM Deployment scenario](#)
- [BSM/APM/OMi Deployment scenario](#)
- [VMware vCenter only Deployment scenario](#)
- [Others Deployment scenario](#)







For more information, see the *Operations Bridge Reporter Configuration Guide*.

The Data Source Selection Wizard includes:

Data Source Selection

Operations Manager i (OMi 10.x)	Option to select OMi 10.0x or 10.10 and later versions as data source.
Business Service Manager (BSM/APM)	Option to select BSM as data source.
Operations Manager (OM)	Option to select OM as data source.
Network Node Manager i (NNMi)	Option to select NNMi as data source.
SiteScope	Option to select SiteScope as data source.
Operations Agent	Option to select Operations Agent as data source.
VMware Vcenter	Option to select VMware Vcenter as data source.

Topology Source Configuration

Field	Description
Collection Frequency (hrs)	Time (in hours) to collect data from the data sources.
Host name	IP address or fully-qualified name (FQDN) of the service definition host system.
Enable Collection	Enable or disable the service definition data collection.
Connection Status	Status of the service definition source connection. <ul style="list-style-type: none">  indicates that the host system is connected to the data source.  indicates that the host system is not connected to the data source.
Collection Status	Status of the collection with the date and time of the latest collection attempt and the current status: <ul style="list-style-type: none">  indicates that the data collection is in progress.  indicates that the data collection completed successfully in the previous attempt.  indicates that the data collection failed in the previous attempt.  indicates that the data collection was never started.
Create New	Create a new service definition source connection.
Test Connection	Test a service definition source connection.
Edit	Modify an existing service definition source connection.
Save	Save a specific service definition source configuration attribute.

For information on how to configure a topology source connection, see [Topology Source](#).

Content Type Selection

This page displays the Content Types according to the selected data sources in the Data Source Selection tab. Select the required Content Type and click Next.

Data Source Type	Content Type
Operations Manager i (OMi) 10.x	<ul style="list-style-type: none"> Service health (KPI's and health indicators)

	<ul style="list-style-type: none"> Enterprise application performance OMi events
Business Service Manager (BSM/APM)	<ul style="list-style-type: none"> Service health (KPI's and health indicators) Real user monitoring Synthetic transaction monitoring OMi events Enterprise application performance
Operations Manager (OM)	<ul style="list-style-type: none"> OM events Enterprise application performance
Network Node Manager i (NNMi)	<ul style="list-style-type: none"> Network Performance <p>Direct NNM integration (NRT): Select Yes or No.</p>
SiteScope	<p>Metric Channel: Direct API</p> <ul style="list-style-type: none"> System Performance Virtual environment performance
Operations Agent	<ul style="list-style-type: none"> System Performance Virtual environment performance <p>Technology</p> <ol style="list-style-type: none"> VMware IBM LPAR Microsoft Hyper-V Solaris Zones
VMware vCenter	<ul style="list-style-type: none"> Virtual environment performance

Tip: You may click **Next** continuously to go to the end of the Data Source Selection Wizard. The Content Type selection can be done from the Administration Console > Data Source Selection Wizard.

OMi Management Packs/OM SPIs Selection

The OMi Management Packs/OM SPIs Selection tab displays the selection options only when Enterprise application performance is selected in Content Type Selection tab. Select the required OMi Management Packs/OM SPIs Selection and click Next.

Tip: You may click **Next** continuously to go to the end of the Data Source Selection Wizard. The

OMi Management Packs/OM SPIs selection can be done from the Administration Console > Data Source Selection Wizard.

Content Pack Deployment

This page displays the list of Content Packs that can be installed according to the selected data sources in the Data Source Selection tab.

For more information, see [Content Pack Deployment](#).

Tip: You may click **Next** continuously to go to the end of the Data Source Selection Wizard. The Content pack installation can be done from the Administration Console > Content Pack Deployment page.

Data Source Configuration

Select the Data Sources that are displayed according to the data sources selected in the Data Source Selection tab and configure the data sources.

For more information, see [Data Source Configuration](#).

Tip: You may click **Next** continuously to go to the end of the Data Source Selection Wizard. The data source can be configured from the Administration Console > Data Source Configuration tab.




Chapter 13: Dashboard


The Dashboard is the main page of the Administration Console. This page gives you an overall view of the status of OBR, its associated services, the database, and the host platform. You can also view the status of the data collection, check the performance of the Content Packs, and view a list of Orchestration and Health alerts generated by OBR.









Use the Home page to:

- [View the OBR status](#)
- [View details of the Orchestration alerts](#)

The Dashboard includes:

Group	Field	Description
Status Summary	Services Status	<p>Displays the status of the OBR database and SAP BOBJ Enterprise services.</p> <p>Status of the service:</p> <ul style="list-style-type: none">•  indicates that all the services are running successfully.•  indicates that one or all of the services are not running. <p>The data displayed in this table is refreshed periodically. Click  to update the table with the latest data.</p>
	Connectivity Status	<p>Displays the status of OBR's connectivity to the following components:</p> <ul style="list-style-type: none">• Tomcat service (SAP BOBJ Tomcat Service)• SAP BusinessObjects Central Management Service (SAP BOBJ CMS)• HPE Vertica (Vertica database service)
	Runtime File Distribution	<p>Displays the data distribution of the OBR file system according to the size of the files in the following folders:</p>

Group	Field	Description
		<p>Folder</p> <ul style="list-style-type: none"> ■ Archive ■ Transform_Cache ■ Failed ■ Stage ■ Collect ■ Extract <p>Before the data collected from the data sources are loaded into the appropriate Vertica database tables, it is held in the OBR system for processing. Also, the data that failed to pass the data processing streams (<code>!stage!failed_to_*</code> folder). are also stored on the OBR file system. Runtime file distribution shows the disk space used by these files.</p>
	Data Collection Status	<p>Displays the number of data sources that are configured for each data collector. The status is represented in the following ways:</p> <ul style="list-style-type: none"> ■ Succeeded ■ Failure ■ Never Started ■ In Progress ■ Disabled <ul style="list-style-type: none"> • Succeeded: When data collection from the data sources occurs without issues. • Failure: When data collection from the data sources has failed. • Never Started: When data collection from the data source has never occurred. • In Progress: When data collection from the data sources is in progress. • Disabled: When data collection from the data sources is disabled. <p>The data displayed in this table is refreshed periodically. Click  to update the table with the latest data.</p>
	Content Health Summary	<p>Displays the graphical representation of the health of data flow from data source into the fact tables associated with the dimensions of installed content packs. The status is represented in the following ways:</p>

Group	Field	Description
		<p>  Succeeded 1  In Progress 15 </p> <ul style="list-style-type: none"> • Succeeded: When data flow occurs without issues. • In Progress: When data flow is in progress. <p>Click the adjoining link Full Status to view the graphical details or Content Health Status to go to Content Health Status page.</p> <p>The data displayed in this table is refreshed periodically. Click  to update the table with the latest data.</p>
Alerts	Orchestration Alerts	<p>Displays the number of data processing job streams that have failed to complete or with warnings. For more information, see View details of the Orchestration Alerts. The following icons are used to identify the types of alerts:</p> <ul style="list-style-type: none"> •  indicates an error alert. Click the adjoining link to view the details. •  indicates a warning alert. Click the adjoining link to view the details.
	Health Alerts	<p>This table displays the severity, message, and date of the all error, warning, and information alerts generated by OBR. The following icons are used to identify the types of alerts:</p> <ul style="list-style-type: none"> •  indicates an information alert. No action is required for this type of alert. •  indicates an error alert. These are critical alerts and immediate action is required to resolve these issues. •  indicates a warning alert. You might need to resolve these types of alerts to ensure functions properly. However, immediate action might not be required.




Using the Home page


OBR performs various self-monitoring tasks where it monitors the database system, its key services, the data collection, and the database loading operations. This information is displayed on the Home page of the Administration Console. The Home page gives you an overall status of the OBR components. You can directly troubleshoot performance issues with OBR by using this information. For additional information, you can drill down from this page by using the hyperlinks or open the relevant pages from the Task pane.









View OBR status

The Home page displays information such as the status of the OBR services, the host system, and the database. You can view the number and status of active streams for the installed Content Pack components and the status of the data collection. You can also view the list of ABC and database alerts reported by OBR.

The Home page includes the following tables:

Group	Field	Description
Status Summary	Services Status	<p>Displays the status of the OBR database and SAP BOBJ Enterprise services.</p> <p>Status of the service:</p> <ul style="list-style-type: none"> indicates that all the services are running successfully. indicates that one or all of the services are not running. <p>The data displayed in this table is refreshed periodically. Click  to update the table with the latest data.</p>
	Connectivity Status	<p>Displays the status of OBR's connectivity to the following components:</p> <ul style="list-style-type: none">Tomcat service (SAP BOBJ Tomcat Service)SAP BusinessObjects Central Management Service (SAP BOBJ CMS)HPE Vertica (Vertica database service)
	Runtime File	Displays the data distribution of the OBR file system according to

Group	Field	Description
	Distribution	<p>the size of the files in the following folders:</p> <p>Folder</p> <ul style="list-style-type: none"> ■ Archive ■ Transform_Cache ■ Failed ■ Stage ■ Collect ■ Extract <p>Before the data collected from the data sources are loaded into the appropriate Vertica database tables, it is held in the OBR system for processing. Also, the data that failed to pass the data processing streams (<code>\stage\failed_to_*</code> folder). are also stored on the OBR file system. Runtime file distribution shows the disk space used by these files.</p>
	Data Collection Status	<p>Displays the number of data sources that are configured for each data collector. The status is represented in the following ways:</p> <ul style="list-style-type: none"> ■ Succeeded ■ Failure ■ Never Started ■ In Progress ■ Disabled <ul style="list-style-type: none"> • Succeeded: When data collection from the data sources occurs without issues. • Failure: When data collection from the data sources has failed. • Never Started: When data collection from the data source has never occurred. • In Progress: When data collection from the data sources is in progress. • Disabled: When data collection from the data sources is disabled. <p>The data displayed in this table is refreshed periodically. Click  to update the table with the latest data.</p>
	Content Health Summary	<p>Displays the graphical representation of the health of data flow from data source into the fact tables associated with the dimensions of installed content packs. The status is represented in the following ways:</p>

Group	Field	Description
		<p>  Succeeded 1  In Progress 15 </p> <ul style="list-style-type: none"> • Succeeded: When data flow occurs without issues. • In Progress: When data flow is in progress. <p>Click the adjoining link Full Status to view the graphical details or Content Health Status to go to Content Health Status page.</p> <p>The data displayed in this table is refreshed periodically. Click  to update the table with the latest data.</p>
Alerts	Orchestration Alerts	<p>Displays the number of data processing job streams that have failed to complete or with warnings. For more information, see View details of the Orchestration Alerts. The following icons are used to identify the types of alerts:</p> <ul style="list-style-type: none"> •  indicates an error alert. Click the adjoining link to view the details. •  indicates a warning alert. Click the adjoining link to view the details.
	Health Alerts	<p>This table displays the severity, message, and date of the all error, warning, and information alerts generated by OBR. The following icons are used to identify the types of alerts:</p> <ul style="list-style-type: none"> •  indicates an information alert. No action is required for this type of alert. •  indicates an error alert. These are critical alerts and immediate action is required to resolve these issues. •  indicates a warning alert. You might need to resolve these types of alerts to ensure functions properly. However, immediate action might not be required.


View details of the Orchestration Alerts

The OBR workflow framework creates an execution log file that stores the information of all the job steps. The Orchestration Alerts tab picks up and displays a list of the 10 latest active data processes

that failed to complete successfully. You can use the information displayed on the **Orchestration Alerts** tab to troubleshoot data processing-related issues.

To view more information about the error:

1. In **Orchestration Alerts**, click a numbered hyperlink.
The **Orchestration Alerts** dialog box appears.
2. View:

Field	Description
Status	Type of alert, which can be of two types: <ul style="list-style-type: none"> ○ Error—This status indicates that the job step failed to complete the execution process because of a serious error. The execution of the job stream cannot continue. ○ Warning—This status indicates that the job step failed to complete the execution process within the defined time frame.
Stream	The stream name.
Step	The step where the job stopped execution.
Message	Displays the error message that lead to the job to stop executing.
Time	Time when the job stopped execution.
	Displays the execution log of the job step with detailed information on how the error was generated during the execution of the job step.
Stream Name	The stream name.
Log File	The location of the log file.
Command	The command that was used to run the job stream when the error was generated. This field only appears for job steps with error states.

Chapter 14: Data Source Selection Wizard

This wizard is a guided configuration which helps you to select the required data sources based on the deployment scenario.

Use the Data Source Selection Wizard to configure the following data sources based on the deployment scenario:

Deployment Scenario	Data Source Type
OM	<ul style="list-style-type: none">• Operations Manager (OM)• Operations Agent• VMware vCenter <i>(optional)</i>• Network Node Manager i (NNMi) <i>(optional)</i>
BSM/APM/OMi	<ul style="list-style-type: none">• Business Service Manager (BSM)• Operations Manager i (OMi) 10.x <p>Tip: If you have only BSM deployed in your environment, select Business Service Manager (BSM). If you have only OMi 10.x deployed in your environment, select Operations Manager i (OMi) 10.x. If you have both BSM and OMi 10.x deployed in your environment and BSM and OMi 10 systems are integrated, select both Business Service Manager (BSM) and Operations Manager i (OMi) 10.x.</p> <ul style="list-style-type: none">• SiteScope <i>(optional)</i>• Operations Agent <i>(optional)</i>• VMware vCenter <i>(optional)</i>
VMware vCenter	<ul style="list-style-type: none">• VMware vCenter• Network Node Manager i (NNMi) <i>(optional)</i>
Other	Network Node Manager i (NNMi)

- [OM Deployment scenario](#)
- [BSM/APM/OMi Deployment scenario](#)
- [VMware vCenter only Deployment scenario](#)
- [Others Deployment scenario](#)

The Data Source Selection Wizard page includes:

Data Source Selection

Operations Manager i (OMi 10.x)	Option to select OMi 10.0x or 10.10 and later versions as data source.
Business Service Manager (BSM/APM)	Option to select BSM as data source.
Operations Manager (OM)	Option to select OM as data source.
Network Node Manager i (NNMi)	Option to select NNMi as data source.
SiteScope	Option to select SiteScope as data source.
Operations Agent	Option to select Operations Agent as data source.
VMware Vcenter only	Option to select VMware Vcenter as data source.

Content Type Selection

This page displays the Content Types according to the selected data sources in the Data Source Selection tab. Select the required Content Type and click Next.

Data Source Type	Content Type
Operations Manager i (OMi) 10.x	<ul style="list-style-type: none"> Service health (KPI's and health indicators) Enterprise application performance OMi events
Business Service Manager (BSM/APM)	<ul style="list-style-type: none"> Service health (KPI's and health indicators) Real user monitoring Synthetic transaction monitoring OMi events Enterprise application performance
Operations Manager (OM)	<ul style="list-style-type: none"> OM events Enterprise application performance
Network Node Manager i (NNMi)	<ul style="list-style-type: none"> Network Performance Direct NNM integration (NRT): Select Yes or No.
SiteScope	Metric Channel: Direct API <ul style="list-style-type: none"> System Performance

	<ul style="list-style-type: none"> • Virtual environment performance
Operations Agent	<ul style="list-style-type: none"> • System Performance • Virtual environment performance Technology <ul style="list-style-type: none"> a. VMware b. IBM LPAR c. Microsoft Hyper-V d. Solaris Zones
VMware vCenter	<ul style="list-style-type: none"> • Virtual environment performance

OMi Management Packs/OM SPIs Selection

The OMi Management Packs/OM SPIs Selection tab displays the selection options only when Enterprise application performance is selected in Content Type Selection tab.

Note: To view the previous selections, click the tabs **Data Source Selection**, **Content Type Selection** and **OMi Management Packs/OM SPIs Selection**.

To modify the selections made in each of the tabs, select the required options and click **Next**. Click **Finish** to save the updates made.

OM Deployment scenario

Data Source Selection

1. In the **Data Source Selection**, select **Operations Manager (OM)** and **Operations Agent**.
2. *(Optional)*. Select **VMware vCenter**, **Network Node Manager i (NNMi)** if data source for virtual environment and NNMi and the NNMi SPI Performance is available in your environment.
3. Click **Next**.

Content Type Selection

1. In **Content Type Selection > Operations Manager (OM)**, select **OM Events** for events. You can select the additional Content Type as required.
2. Click **Next**.

OMi Management Packs/OM SPIs Selection

The OMi Management Packs/OM SPIs Selection tab displays the selection options only when Enterprise application performance is selected in Content Type Selection tab.

1. In **OMi Management Packs/OM SPIs Selection** select **Management Pack** and/or **Smart Plug-In(SPi)**.

Note: You must ensure that necessary Management Pack and/or Smart Plug-In (SPi) policies are installed.

2. Click **Finish**.

BSM/OMi Deployment scenario

Data Source Selection

1. In **Data Source Selection**, select **Business Service Manager (BSM/APM)** and **Operations Manager i (OMi) 10.x**.
2. In **Operations Manager i (OMi) 10.x**, select the version of the application deployed in your environment.

If you have only BSM deployed in your environment, select **Business Service Manager (BSM/APM)**. If you have only OMi 10.x deployed in your environment, select **Operations Manager i (OMi) 10.x**. If you have both BSM and OMi 10.x deployed in your environment and BSM and OMi 10 systems are integrated, select both **Business Service Manager (BSM/APM)** and **Operations Manager i (OMi) 10.x**.

3. *(Optional)*. You may select **SiteScope** for system performance, **Operations Agent** and **VMware vCenter** data source for the virtual environment
4. Click **Next**

Content Type Selection

1. In **Content Type Selection > Business Service Manager (BSM/APM)**, select the required Content Type.
2. In **Content Type Selection > Operations Manager i (OMi) 10.x**, select the required Content Type.
3. *(Optional)*.
 - a. If you select **SiteScope** for system performance, then **SiteScope Metric Channel** section appears.

- b. You must select either **Profile DB** or **Direct API** as the metric channel for SiteScope.

In the **Content Pack Deployment** page, components for Direct API are selected automatically if the option is selected in the Configuration Wizard.

Note: If SiteScope is used to monitor system or virtual environment performance in OMi 10.x, the metric channel for SiteScope is through Direct API.

4. (Optional). If **Operations Agent** and **VMware vCenter** data source are selected for the virtual environment, select the required content type and the technology.

Data Source	Select Technology
Operations Agent	<ul style="list-style-type: none"> o VMware o IBM LPAR o Microsoft Hyper-V o Solaris Zones

5. Click **Next**.

OMi Management Packs/OM SPIs Selection

The OMi Management Packs/OM SPIs Selection tab displays the selection options only when Enterprise application performance is selected in Content Type Selection tab.

1. In **OMi Management Packs/OM SPIs Selection** select **Management Pack** and/or **Smart Plug-In(SPi)**.

Note: You must ensure that necessary Management Pack and/or Smart Plug-In (SPi) policies are installed.

2. Click **Finish**.

VMware vCenter only Deployment scenario

Data Source Selection

1. In **Data Source Selection**, select **VMware vCenter**.
2. (Optional). Select **Network Node Manager i (NNMi)** if NNMi and the NNMi iSPI Performance is available in your environment.
3. Click **Next**.

Content Type Selection

1. In **Content Type Selection > VMware vCenter**, select **Virtual environment performance**. You can select the additional Content Type as required.
2. Click **Next**.

OMi Management Packs/OM SPIs Selection

The OMi Management Packs/OM SPIs Selection tab displays the selection options only when Enterprise application performance is selected in Content Type Selection tab.

1. In **OMi Management Packs/OM SPIs Selection** select **Management Pack** and/or **Smart Plug-In(SPi)**.

Note: You must ensure that necessary Management Pack and/or Smart Plug-In (SPi) policies are installed.

2. Click **Finish**.

Others Deployment scenario

Data Source Selection

1. In **Data Source Selection**, select **Network Node Manager i (NNMi)**.
2. Click **Next**.

Content Type Selection

1. In **Content Type Selection > Network Node Manager i (NNMi)**, select **Network Performance**.
2. Select **Yes** or **No** for the **Direct NNM integration (NRT)**

The **NNMi with Direct Integration** collects network performance data directly from NNMi. The data collection gives you detailed real time view of component or interface health in your network. You have to install Network Component_Health/Network Interface_Health Content Packs. You can view detailed health or utilization reports. You have to revisit the hardware requirements, if you choose to install these Content Packs.

3. (*Optional*). Select the **NNM integrated with BSM/APM/OMi** check box.

The **NNMi integrated with NPS DB** collects network performance data from NPS. The data collection is based on hourly, daily and aggregate summary. You have to install Network Performance Content Pack. You can view executive summary reports.

4. Click **Next**.

OMi Management Packs/OM SPIs Selection

The OMi Management Packs/OM SPIs Selection tab displays the selection options only when Enterprise application performance is selected in Content Type Selection tab.

1. In **OMi Management Packs/OM SPIs Selection** select **Management Pack** and/or **Smart Plug-In(SPi)**.

Note: You must ensure that necessary Management Pack and/or Smart Plug-In (SPi) policies are installed.

2. Click **Finish**

Chapter 15: Content Pack Deployment

You can use the Content Pack Deployment page to install and remove Content Pack components.

Note: You must make sure to complete the Data Source Selection before installing the content packs from the Content Pack Deployment page.

Use the Content Pack Deployment page to:

- [Install a Content Pack or upgrade a Content](#)
- [Remove an Installed Content Pack](#)

In OBR, the Content Packs are structured into the following layers or components:

Domain Content Pack component

The Domain or Core Domain component defines the data model for a particular Content Pack. It contains the rules for generating the relational schema. It also contains the data processing rules, including a set of standard pre-aggregation rules, for processing data into the database. The Domain component can include the commonly-used dimensions and cubes, which can be leveraged by one or more Report Content Pack components. The Domain Content Pack component does not depend on the configured topology source or the data source from where you want to collect data.

ETL Content Pack component

The ETL Content Pack component defines the collection policies and the transformation, reconciliation, and staging rules. It also provides the data processing rules that define the order of execution of the data processing steps. The ETL Content Pack component is data source dependent. Therefore, for a particular domain, each data source application has a separate ETL Content Pack component. For example, if you want to collect system performance data from the Performance Agent and SiteScope data source applications, you must install the **SysPerf_ETL_PerformanceAgent** and **ETL_SystemManagement_SiS** ETL components respectively. A single data source application can have multiple ETL components. For example, you can have one ETL component for each virtualization technology supported in Operations agent such as Oracle Solaris Zones, VMware, IBM LPAR, and Microsoft HyperV. The ETL component can be dependent on one or more Domain components. In addition, you can have multiple ETL components feeding data into the same Domain component.

Report Content Pack component

The Application Content Pack component defines the application-specific aggregation rules, business views, SAP BOBJ universes, and the reports for a particular domain. Application components can be dependent on one or more Domain components. It also provides the flexibility to extend the data model



that is defined in one or more Domain components.

The Content Pack Deployment page simplifies the selection of the Content Pack components by displaying filtered list of content packs based on the selections made in the Data Source Selection tab. From the filtered list, you can then select the Content or specific Content Pack components that you want to install. The Content Pack Deployment page performs a silent installation or uninstallation of the Content Pack components while displaying the updated status on the page.

The Content Pack Deployment page includes:

Content Pack Deployment

Field	Description
Content	The type of content or domain for which data is collected by OBR. The list of Content displayed is filtered based on the topology source that is defined, that is, RTSM or OM.
Data Source Application	The data sources from where OBR will collect data for the Content.
Content Pack Component Name	<p>Name of the Content Pack component. A Content Pack is typically comprised of three components—domain, ETL, and report. For more information about these Content Pack types, see the <i>Operations Bridge Reporter Concepts Guide</i>.</p> <p>The name of the Content Pack component is based on the following syntax:</p> <p>AcronymofContentPack_Component_<Technology>_<DatasourceVersion></p> <p>For example, SysPerf_Domain, VirtualEnvPerf_ETL_HyperV_PerformanceAgent, RealUsrTrans_Reports</p> <p>The technology, data source, and version of the data source are optional. The data source and its version will be appended only in the case of the ETL component where the component is data-source dependent.</p>
Installed Version	Version of the Content Pack component.
Status	Displays the status of the installation or uninstallation process. During the installation or uninstallation process, the Content Pack Deployment page automatically refreshes and displays the updated status of the process.

Field	Description
	Displays the Content Pack Component Status History.
	Removes an installed Content Pack component.
Install	Install the selected Content Pack components.

Content Pack Component Status History

Field	Description
Content Pack Component Name	Name of the Content Pack component.
Status	Displays the status of the installation or uninstallation process. During the installation or uninstallation process, the Deployment Manager page automatically refreshes and displays the updated status of the process.
Install Date	The data and time when the selected Content Pack component was installed or uninstalled.
Version	Version of the Content Pack component.
Message	Description of the installation or uninstallation status.

The list of all ready-to-use Content Packs available on the Content Pack Deployment page:

Core Content Pack

You must install this content pack before or while installing any other content pack. Following are the components:

- Core_Domain
- Core_Domain_AppServer
- Core_Domain_EUM

Cross-Domain Operations Events

OMi: If you are installing this content pack to generate reports on data from OMi 10, select the following and click Install:

- Operations Manager i
 - CrossOprEvent_ETL_OMi10
 - CrossOprEvent_ETL_OMi (if topology is RTSM)
 - CrossOprEvent_Domain_Reports

OMi Extended: The OMi Extended content pack includes an extended set of attributes from OMi as follows:

- Event Annotations
- Event Property Changes
- Event Forwarding Details
- Custom Message Attributes (CMAs)

If you are installing the OMi Extended content pack to generate reports on data from OMi, select the following and click Install:

- Operations Manager i
 - CrossOprEvent_ETL_OMi_Extended (if topology is RTSM)
 - CrossOprEvent_Domain_Reports_Extended
 - CrossOprEvent_ETL_OMi10x_Extended

Note: You must upgrade CrossOprEvent_Domain_Reports_Extended to the latest version to use CrossOprEvent_ETL_OMi10x_Extended.

Tip: Install the following dependent content packs (and their components) along with this content pack for it to function:

- Core
 - Core_Domain

Health and Key Performance Indicators (Service Health)

BSM: If you are installing this content pack to generate reports on data from BSM, select the following and click Install:

- BSM Service Health
 - HIKPI_ETL_ServiceHealth

- HIKPI_Domain
- HIKPI_Reports_ServiceHealth

OMi: If you are installing this content pack to generate reports on data from OMi 10, select the following and click Install:

- BSM Service Health
 - HIKPI_ETL_ServiceHealth_OMi10
 - HIKPI_Domain
 - HIKPI_Reports_ServiceHealth

Tip: Install the following dependent content packs (and their components) along with this content pack for it to function:

- Core
 - Core_Domain

Server Automation

Server Automation: If you are installing this content pack to generate reports on data from Server Automation, select the following and click Install:

- SA_Core_Domain
- SA_CoreETL-Base

IBM WebSphere Application Server

OM: If you are installing this content pack to generate reports on data from OM, select the following and click Install/Upgrade:

- Operations Smart Plug-in for WebSphere Application Server
 - IBMWebSphere_ETL_WebSphereSPI
 - IBMWebSphere_Domain
 - IBMWebSphere_Reports

Also, review the [Prerequisite Policies for IBM WebSphere Reports \(SPI\)](#).

BSM/OMi: If you are installing this content pack to generate reports on data from BSM/OMi, select the following and click Install:

- OMi Management Pack for IBM WebSphere Application Server
 - IBMWebSphere_ETL_WebSphereMP
 - IBMWebSphere_Domain
 - IBMWebSphere_Reports

Also, review the [Prerequisite Policies for IBM WebSphere Reports \(SPI\)](#). If you have an underlying OM environment that collects data through SPIs and feeds it to OMi, review these [Prerequisite Policies for IBM WebSphere Reports \(MP\)](#).

Tip: Install the following dependent content packs (and their components) along with this content pack for it to function:

- Core
 - Core_Domain
 - Core_Domain_AppServer
- Operations Manager
 - OprEvent_Domain_Reports
- System Performance
 - SysPerf_Domain

Microsoft Active Directory

OM and BSM/OMi: If you are installing this content pack to generate reports on data from OM, BSM, or OMi, select the following and click Install:

- Operations Smart Plug-in for Microsoft Active Directory, OMi Management Pack for Microsoft Active Directory
 - MicrosoftActiveDirectory_ETL_ADSPi
 - MicrosoftActiveDirectory_Domain
 - MicrosoftActiveDirectory_Reports

Also, review the [Prerequisite Policies for Microsoft Active Directory Reports \(SPI\)](#) and [Prerequisite Policies for Microsoft Active Directory Reports \(MP\)](#).

Tip: Install the following dependent content packs (and their components) along with this content pack for it to function:

- Core
 - Core_Domain
 - MSAppCore

Microsoft Exchange Server

OM and BSM/OMi: If you are installing this content pack to generate reports on data from OM, BSM, or OMi, select the following and click Install:

For Microsoft Exchange 2007

- Operations Smart Plug-in for Microsoft Exchange 2007
 - MicrosoftExchange_ETL_ExchangeSPI2007
 - MicrosoftExchange_Domain
 - MicrosoftExchange_Reports

For Microsoft Exchange 2010

- Operations Smart Plug-in for Microsoft Exchange 2010, OMi Management Pack for Microsoft Exchange Server
 - MicrosoftExchange_ETL_ExchangeSPI2010
 - MicrosoftExchange_Domain
 - MicrosoftExchange_Reports

For Microsoft Exchange 2013

- Operations Smart Plug-in for Microsoft Exchange 2013, OMi Management Pack for Microsoft Exchange Server
 - MicrosoftExchange_ETL_ExchangeSPI2013
 - MicrosoftExchange_Domain
 - MicrosoftExchange_Reports

Also, review the [Prerequisite Policies for Microsoft Exchange Server Reports \(SPI\)](#).

Tip: Install the following dependent content packs (and their components) along with this content pack for it to function:

- Core
 - Core_Domain
 - MSAppCore
- System Performance
 - SysPerf_Domain
 - SysPerf_Reports

Microsoft SQL Server

OM and BSM/OMi: If you are installing this content pack to generate reports on data from OM, BSM, or OMi, select the following and click Install:

- Operations Smart Plug-in for Microsoft SQL Server, OMi Management Pack for Microsoft SQL Server
 - MicrosoftSQLServer_ETL_DBSPI
 - MicrosoftSQLServer_Domain
 - MicrosoftSQLServer_Reports

Also, review the [Prerequisite Policies for Microsoft SQL Server Reports \(SPI\)](#) and [Prerequisite Policies for Microsoft SQL Server Reports \(MP\)](#).

Tip: Install the following dependent content packs (and their components) along with this content pack for it to function:

- Core
 - Core_Domain
- System Performance
 - SysPerf_Domain

Network Component Health

Network Component Health: If you are installing this content pack to generate reports on network component health where Network Mode Manager i (NNMi) is integrated with BSM, select the following and click Install:

NNM iSPI for Performance:

- ComponentHealth_Reports
- Core_ComponentHealth

Network Interface Health

Network Interface_Health: If you are installing this content pack to generate reports on network interface health where Network Mode Manager i (NNMi) is integrated with BSM, select the following and click Install:

NNM iSPI for Performance:

- Core_InterfaceHealth
- InterfaceHealth_Reports

Network Performance

RTSM: If you are installing this content pack to generate reports on network data where Network Mode Manager i (NNMi) is integrated with BSM, select the following and click Install:

- NNM iSPI for Performance
 - NetworkPerf_ETL_PerfiSPI_RTSM
 - NetworkPerf_Domain
 - NetworkPerf_Reports

Non-RTSM: If you are installing this content pack to generate reports on network data where Network Mode Manager i (NNMi) is not integrated with BSM, select the following and click Install:

- NNM iSPI for Performance
 - NetworkPerf_ETL_PerfiSPI_NonRTSM
 - NetworkPerf_Domain
 - NetworkPerf_Reports

Tip: Install the following dependent content packs (and their components) along with this content pack for it to function:

- Core
 - Core_Domain
- System Performance
 - SysPerf_Reports

Operations Events

OM: If you are installing this content pack to generate reports on events logged into OM, select the following and click Install:

- Operations Manager
 - OprEvent_ETL_OM
 - OprEvent_Domain_Reports

Tip: Install the following dependent content packs (and their components) along with this content pack for it to function:

- Core
 - Core_Domain

Oracle

OM and BSM/OMi: If you are installing this content pack to generate reports on data from OM, BSM, or OMi, select the following and click Install:

- Operations Smart Plug-in for Oracle, OMi Management Pack for Oracle
 - Oracle_ETL_DBSPI
 - Oracle_Domain
 - Oracle_Reports

Also, review the [Prerequisite Policies for Oracle Database Reports \(SPI\)](#) and [Prerequisite Policies for Oracle Database Reports \(MP\)](#).

Tip: Install the following dependent content packs (and their components) along with this content pack for it to function:

- Core
 - Core_Domain
- Operations Manager
 - OprEvent_Domain_Reports
- System Performance
 - SysPerf_Domain

Oracle WebLogic Server

OM: If you are installing this content pack to generate reports on data from OM, select the following and click Install:

- Operations Smart Plug-in for Oracle WebLogic Server
 - OracleWebLogic_ETL_WebLogicSPI
 - OracleWebLogic_Domain
 - OracleWebLogic_Reports

Also, review the [Prerequisite Policies for Oracle WebLogic Reports \(SPI\)](#).

BSM/OMi: If you are installing this content pack to generate reports on data from BSM/OMi, select the following and click Install:

- OMi Management Pack for Oracle WebLogic Server
 - OracleWebLogic_ETL_WebLogicMP
 - OracleWebLogic_Domain
 - OracleWebLogic_Reports

Also, review the [Prerequisite Policies for Oracle WebLogic Reports \(MP\)](#). If you have an underlying OM environment that collects data through SPIs and feeds it to OMi, review these [Prerequisite Policies for Oracle WebLogic Reports \(SPI\)](#).

Tip: Install the following dependent content packs (and their components) along with this content pack for it to function:

- Core
 - Core_Domain
 - Core_Domain_AppServer
- Operations Manager
 - OprEvent_Domain_Reports
- System Performance
 - SysPerf_Domain

Real User Transaction Monitoring (RUM)

OM: If you are installing this content pack to generate reports on data from OM, select the following and click Install:

- Real User Monitor
 - RealUsrTrans_ETL_RUM
 - RealUsrTrans_Domain_Reports

BSM/OMi: If you are installing this content pack to generate reports on data from BSM/OMi, select the following and click Install:

- Real User Monitor
 - RealUsrTrans_ETL_RUM_OMi
 - RealUsrTrans_Domain_Reports

Tip: Install the following dependent content packs (and their components) along with this content pack for it to function:

- Core
 - Core_Domain
 - Core_Domain_EUM
- Operations Manager
 - OprEvent_Domain_Reports
- System Performance
 - SysPerf_Domain
 - SysPerf_Reports
- Virtualization Performance
 - VirtualEnvPerf_Domain
- Operation Events (Operations Manager)
 - ServiceHealth

Synthetic Transaction Monitoring (BPM)

OM: If you are installing this content pack to generate reports on data from OM, select the following and click Install:

- Business Process Monitor
 - SynTrans_ETL_BPM
 - SynTrans_Domain_Reports

BSM/OMi: If you are installing this content pack to generate reports on data from BSM/OMi, select the following and click Install:

- Business Process Monitor
 - SynTrans_ETL_BPM_OMi
 - SynTrans_Domain_Reports

Tip: Install the following dependent content packs (and their components) along with this content pack for it to function:

- Core
 - Core_Domain
 - Core_Domain_EUM

System Performance

Operations Agent: If you are installing this content pack to generate reports on data from Operations Agent, select the following and click Install:

- Performance Agent, Operations agent
 - SysPerf_ETL_PerformanceAgent
 - SysPerf_Domain
 - SysPerf_Reports

SiteScope: If you are installing this content pack to generate reports on data from SiteScope, select the following and click Install:

- SiteScope
 - SysPerf_ETL_SiS_API or SysPerf_ETL_SiS_DB (SysPerf_ETL_SiS is deprecated)
 - SysPerf_Domain
 - SysPerf_Reports

For more information on Sitescope ETL, see *Appendix C: Listing of ETLs in Operations Bridge Reporter Configuration Guide*.

The SysPerf_SiS_ETL Content Pack component is deprecated. Instead of SysPerf_SiS_ETL, use SysPerf_SiS_DB or SysPerf_SiS_API.

If you have upgraded from an older version of OBR, follow these steps to move from SysPerf_SiS_ETL to SysPerf_SiS_DB or SysPerf_SiS_API:

1. Log on to the OBR Administration Console.
2. Go to the Administration tab.
3. Click **Data Source Selection**.
4. Make appropriate data source selection, and then, under every SiteScope check box, select **Direct API** or **ProfileDB**.

Note: These options appear only after you select the SiteScope check box.

5. Click **Save**.
6. Click **Content Pack Deployment**.
7. Select `SysPerf_SiS_API` if you select Direct API or `SysPerf_SiS_DB` if you selected ProfileDB, and then click **Install**.

Tip: Install the following dependent content packs (and their components) along with this content pack for it to function:

- Core
 - Core_Domain

Virtual Environment Performance

Operations Agent: If you are installing this content pack to generate reports on data from Operations Agent, select the following and click Install:

Note: For Operations Agent version 11.x or earlier, use the `VirtualEnvPerf_ETL_VMWare_PerformanceAgent` and `VirtualEnvPerf_ETL_HyperV_PerformanceAgent` ETLs. For Operations Agent version 12 use Cloud Optimizer (earlier known as Virtualization Performance Viewer (vPV)) content.

- Performance Agent
 - `VirtualEnvPerf_ETL_HyperV_PerformanceAgent`
 - `VirtualEnvPerf_ETL_IBMLPAR_PerformanceAgent`
 - `VirtualEnvPerf_ETL_SolarisZones_PerformanceAgent`
 - `VirtualEnvPerf_ETL_VMWare_PerformanceAgent`
 - `VirtualEnvPerf_Domain`
 - `VirtualEnvPerf_Reports`

SiteScope: If you are installing this content pack to generate reports on data from SiteScope, select the following and click Install:

- SiteScope
 - VirtualEnvPerf_ETL_VMware_SiS_API
 - VirtualEnvPerf_ETL_VMware_SiteScope
 - VirtualEnvPerf_Domain_VMWare
 - VirtualEnvPerf_Reports_VMWare

VMware vCenter: If you are installing this content pack to generate reports on data from VMware vCenter, select the following and click Install:

- VMware vCenter
 - VirtualEnvPerf_ETL_VMWare_vCenter
 - VirtualEnvPerf_Domain_VMWare
 - VirtualEnvPerf_Reports_VMWare

Tip: Install the following dependent content packs (and their components) along with this content pack for it to function:

- Core
 - Core_Domain
- System Performance
 - SysPerf_Domain

Install a Content Pack


1. In the Administration Console, click **Content Pack Deployment**.
The Content Pack Deployment page appears. By default, all the Content Pack components that have not been installed are selected for installation.
2. To modify the selection of the Content Pack components, in the **Content Pack Component Name** column, clear the components of the selected Content Pack that you do not want to install.

Note: While you clear the components of the selected Content Pack that you do not want to

install, make sure that you clear the dependent components of the Content Pack.

3. Click **Install / Upgrade** to install the Content Packs.

An `Installation Started` status appears in the **Status** column for each Content Pack. The Content Pack Deployment page automatically refreshes itself to display the updated status. Once the installation completes, an `Installation Successful` status appears. If the installation fails, an `Installation Failed` status appears.

4. Click the  icon in the **Status** column for more information about the installation process. The Content Pack Component Status History window opens. It displays the details of the current and historical status of that Content Pack component's installation.

Note: During the installation process, you cannot remove a Content Pack component that is already installed. Instead, you must wait till installation of the all the Content Pack components is complete before you can perform any other operations on the Content Pack Deployment page.

Upgrade a Content Pack

1. In the Administration Console, click **Content Pack Deployment**.

The Content Pack Deployment page appears. By default, all the Content Pack components that have not been installed are selected for installation.

2. Click the  icon in the Installed Version column to upgrade the Content Packs.

Note: If the upgrade fails, do not uninstall the content pack; attempt upgrade again.

Remove an Installed Content Pack

1. In the Administration Console, click **Content Pack Deployment**.

The Content Pack Deployment page appears.


2. In the column for each Content Pack component, click the  icon to uninstall the component.

The Content Pack Components Removal Summary dialog box appears. This dialog box lists the selected component and all the dependent components that will be uninstalled.

3. Click **OK** to confirm the removal of the selected Content Pack component.

An `Uninstallation Started` status appears in the **Status** column for each Content

Pack. The Content Pack Deployment page automatically refreshes itself to display the updated status of the uninstallation. Once the uninstallation completes, an `Uninstallation Successful` or an `Uninstallation Successful with Warnings` status appears in the **Status** column. If the uninstallation fails, an `Uninstallation Failed` status appears.

4. Click the  icon in the **Status** column for more information about the uninstallation process. The Content Pack Component Status History window appears. It displays the details of the current and historical status of that Content Pack component's uninstallation.

Note: If the Status column displays either the `Uninstallation Successful with Warnings` or `Uninstallation Failed` status, you must uninstall the Content Pack component again for it to succeed.

Chapter 16: Topology Source

You can use the Topology Source page to create and configure RTSM and OM data source connections to provide topology-related data of your enterprise. On this page, you can schedule OBR to collect data from the data repositories at specific intervals. In addition, you can view the status of the connection and data collection.



You can configure the Topology Source only when the data sources are selected according to the required topology in the Data Source Selection Wizard.





Use the Data Source Configuration page to:

- [Create a Topology Source connection](#)
- [Modify a Topology Source connection](#)
- [Enable or disable a Topology Source data collection](#)
- [Schedule a Topology Source collection](#)
- [Test the Topology Source connection](#)
- [View a Topology Source connection status](#)
- [View a Topology Source data collection status](#)

The Topology Source page includes:

Topology Source

Field	Description
Collection Frequency (hrs)	Time (in hours) to collect data from the data sources.
Host name	IP address or fully-qualified name (FQDN) of the service definition host system.
Enable Collection	Enable or disable the service definition data collection.
Connection Status	Status of the service definition source connection. <ul style="list-style-type: none">•  indicates that the host system is connected to the data source.•  indicates that the host system is not connected to the data

Field	Description
	source.
Collection Status	<p>Status of the collection with the date and time of the latest collection attempt and the current status:</p> <ul style="list-style-type: none">  indicates that the data collection is in progress.  indicates that the data collection completed successfully in the previous attempt.  indicates that the data collection failed in the previous attempt.  indicates that the data collection was never started.
Create New	Create a new service definition source connection.
Test Connection	Test a service definition source connection.
Edit	Modify an existing service definition source connection.
Save	Save a specific service definition source configuration attribute.

To configure data collection when HTTPS is enabled for the Topology source, see *Configuring the Topology Source* section in *Operations Bridge Reporter Configuration Guide*.

Connection Parameters: RTSM

Field	Description
Host name	IP address or FQDN of the Business Service Management server. If your Business Service Management deployment is distributed, type the name of the gateway server in this field.
Port	Port number to query the RTSM web service. The default port is 80.
User name	Name of the RTSM web service user.
Password	Password of the RTSM web service user.
Collection station	This option is used for a collector installed on a remote system.

Connection Parameters: OM

Field	Description
Database in Oracle RAC	Option to enable OM database on Oracle RAC. This option is not displayed when OM for Windows is selected.
Enable TLS	Enable JDBC connection over TLS. This option is displayed when Database type selected is ORACLE .
Truststore Path	Full path to the truststore path. This option is displayed when Enable TLS is selected.
Truststore Password	The password to access the truststore. This option is displayed when Enable TLS is selected.
Datasource Type	Select the type of OM that is configured in your environment. The options include: <ul style="list-style-type: none"> • OM for Windows • OM for UNIX • OM for LINUX • OM for Solaris
Database Type	Depending on the data source type that you select, the database type is automatically selected for you. For the OM for Windows data source type, the database type is MSSQL. For the OM for UNIX, OM for LINUX, or OM for Solaris, the database type is Oracle.
Service Name	Specify the name by which OBR connects to the Oracle instance. This option appears only if Database in Oracle RAC is selected.
File Name	The *.ora configuration file that defines database addresses for establishing connections. Manually copy this file from the data source system to the {PMDb_HOME}/config folder in the OBR system. This option appears only if OM on Oracle RAC is selected.
Host name	IP address or fully-qualified domain name (FQDN) of the OM database server. If the OM database is configured on a remote system, the machine name of the remote system must be provided here. Host name is not displayed when the database type is Oracle and Management DB on Oracle RAC is selected.
Database instance	System identifier (SID) of the database instance. The default database instance is OVOPS. Database instance is not displayed when the database type is Oracle and Management DB on Oracle RAC is selected.
Database name	Name of the OM database. This field only appears if OM for Windows is selected as the data source type. The name of the database is openview.

Connection Parameters: VMware vCenter

Field	Description
Host name	IP address or FQDN of the VMware vCenter server.
User name	Name of the VMware vCenter user.
Password	Password of the VMware vCenter user.
Collection station	This option is used for a collector installed on a remote system.

Create a Topology Source connection

To create an RTSM topology source connection:

1. In the Administration Console, click **Data Source Configuration > Topology Source**.
The Topology Source page appears.
2. Ensure that the required topology source is selected under **Topology Source**.
3. Click **Create New**.
The Connection Parameters dialog box appears.
4. In the **Connection Parameters** dialog box, type the following values:

Field	Description
Host name	IP address or FQDN of the Business Service Management (BSM) server. If your BSM deployment is distributed, type the name of the gateway server in this field. Note: In a distributed BSM deployment with multiple gateway servers and load balancer configured, type the virtual IP address of the load balancer in this field.
Port	Port number to query the RTSM web service. The port number is 80.
User name	Name of the RTSM web service user.
Password	Password of the RTSM web service user.
Collection Station	This option is used for a collector installed on a remote system.

5. Click **OK**.
6. Click **Save**.
7. In the message box, click **Yes**.
A Saved Successfully message appears in the Information message panel.

Note: You can create a single RTSM data source connection. The Create New button is disabled by default at the data source connection is created.

To create an OM topology source connection:

1. In the Administration Console, click **Data Source Configuration > Topology Source**.
The Topology Source page appears.
2. Ensure that the required topology source is selected under **Topology Source**.
3. Click **Create New**.
The **Connection Parameters** dialog box appears.

Note: If you are using the database method of authentication to connect to the OM database server, you must provide the user details that have the select and connect permissions for the “openview” database here.

4. Type:

Field	Description
Database in Oracle RAC	Option to enable OM database on Oracle RAC. This option is not displayed when OM for Windows is selected.
Enable TLS	Enable JDBC connection over TLS. This option is displayed when Database type selected is ORACLE .
Truststore Path	Full path to the truststore path. This option is displayed when Enable TLS is selected.
Truststore Password	The password to access the truststore. This option is displayed when Enable TLS is selected.
Datasource Type	Select the type of OM that is configured in your environment. The options include: <ul style="list-style-type: none">○ OM for Windows○ OM for UNIX○ OM for LINUX○ OM for Solaris

Field	Description
Database Type	Depending on the data source type that you select, the database type is automatically selected for you. For the OM for Windows data source type, the database type is MSSQL. For the OM for UNIX, OM for LINUX, or OM for Solaris, the database type is Oracle.
Service Name	Specify the name by which OBR connects to the Oracle instance. This option appears only if Database in Oracle RAC is selected.
File Name	The *.ora configuration file that defines database addresses for establishing connections. Manually copy this file from the data source system to the {PMDb_HOME}/config folder in the OBR system. This option appears only if OM on Oracle RAC is selected.
Host name	IP address or fully-qualified domain name (FQDN) of the OM database server. If the OM database is configured on a remote system, the machine name of the remote system must be provided here. Host name is not displayed when the database type is Oracle and Management DB on Oracle RAC is selected.
Database instance	System identifier (SID) of the database instance. The default database instance is OVOPS. Database instance is not displayed when the database type is Oracle and Management DB on Oracle RAC is selected.
Database name	Name of the OM database. This field only appears if OM for Windows is selected as the data source type. The name of the database is openview.
Port	<p>Port number to query the OM database server. Port number is not displayed when the database type is Oracle and Management DB on Oracle RAC is selected.</p> <p>To find the port number, see <i>Checking for the OM Server Port Number</i> section in <i>Operations Bridge Reporter Configuration Guide</i>.</p>
Windows Authentication	<p>Option to enable Windows authentication for accessing the OM database. The user can use the same credentials to access OM as that of the Windows system hosting the database.</p> <p>This option only appears if OM for Windows is selected as the data source type.</p>

Field	Description
User name	Name of the OM database user. Note: For the OM for Windows data source type, if the Windows Authentication option is selected, this field is disabled.
Password	Password of the OM database user. Note: For the OM for Windows data source type, if the Windows Authentication option is selected, this field is disabled.
Collection Station	This option is used for a collector installed on a remote system.

5. Click **OK**.
6. Click **Save**.
7. In the message box, click **Yes**.
A Saved Successfully message appears in the Information message panel.

Note: The default SQL Server Express that is installed with OM for Windows does not accept remote connections.

Data collection for the newly created service definition data source is enabled by default. In addition, the collection frequency is scheduled for every 24 hours.

Note: When you create a data source connection for OM on the Service Definition page, the same data source connection appears on the Operations Manager page as well. However, updating the data source connection on the Service Definition page does not update the connection details on the Operations Manager page.

To create a VMware vCenter topology source connection:

1. In the Administration Console, click **Data Source Configuration > Topology Source**.
The Topology Source page appears.
2. Ensure that the required topology source is selected under **Topology Source**.
3. Click **Create New**.
The **Connection Parameters** dialog box appears.
4. Type:

Field	Description
Host name	IP address or FQDN of the VMware vCenter server.
User name	Name of the VMware vCenter user.
Password	Password of the VMware vCenter user.
Collection Station	This option is used for a collector installed on a remote system.

5. Click **OK**.
6. Click **Save**.
7. In the message box, click **Yes**.
A Saved Successfully message appears in the Information message panel.

Modify a Topology Source connection

To modify an RTSM topology source connection:

1. In the Administration Console, click **Data Source Configuration > Topology Source**.
The Topology Source page appears.
2. For a specific host, click **Edit**.
The Connection Parameters dialog box appears.
3. In the **Connection Parameters** dialog box, type the following connection parameters:

Field	Description
Host name	IP address or FQDN of the Business Service Management server. You cannot modify the host name after it has been specified during the creation process. This field is disabled by default.
Port	Port number to query the RTSM web service. The default port is 80.
User name	Name of the RTSM web service user. The default user name is admin.
Password	Password of the RTSM web service user.
Collection Station	This option is used for a collector installed on a remote system.

4. Click **OK**.

5. Click **Save**.

A Saved Successfully message appears in the Information message panel.

To modify an OM topology source connection:

1. From the Administration Console, select **Data Source Configuration > Topology Source**.
The Topology Source page appears.
2. For a specific host, click **Edit**.
The Connection Parameters dialog box appears.

Note: If you are using the database method of authentication to connect to the OM database server, you must provide the user details that have the select and connect permissions for the “openview” database here.

3. In the **Connection Parameters** dialog box, type the following connection parameters:

Field	Description
Database in Oracle RAC	Option to enable OM database on Oracle RAC. This option is not displayed when OM for Windows is selected.
Enable TLS	Enable JDBC connection over TLS. This option is displayed when Database type selected is ORACLE .
Truststore Path	Full path to the truststore path. This option is displayed when Enable TLS is selected.
Truststore Password	The password to access the truststore. This option is displayed when Enable TLS is selected.
Datasource Type	Select the type of OM that is configured in your environment. The options include: <ul style="list-style-type: none">○ OM for Windows○ OM for UNIX○ OM for LINUX○ OM for Solaris
Database Type	Depending on the data source type that you select, the database type is automatically selected for you. For the OM for Windows data source type, the database type is MSSQL. For the OM for UNIX, OM for LINUX, or OM for Solaris, the database type is Oracle.
Service Name	Specify the name by which OBR connects to the Oracle instance. This option appears only if Database in Oracle

Field	Description
	RAC is selected.
File Name	The *.ora configuration file that defines database addresses for establishing connections. Manually copy this file from the data source system to the {PMDB_HOME}/config folder in the OBR system. This option appears only if OM on Oracle RAC is selected.
Host name	IP address or fully-qualified domain name (FQDN) of the OM database server. If the OM database is configured on a remote system, the machine name of the remote system must be provided here. Host name is not displayed when the database type is Oracle and Management DB on Oracle RAC is selected.
Database instance	System identifier (SID) of the database instance. The default database instance is OVOPS. Database instance is not displayed when the database type is Oracle and Management DB on Oracle RAC is selected.
Database name	Name of the OM database. This field only appears if OM for Windows is selected as the data source type. The name of the database is openview.
Port	<p>Port number to query the OM database server. Port number is not displayed when the database type is Oracle and Management DB on Oracle RAC is selected.</p> <p>To find the port number, see <i>Checking for the OM Server Port Number</i> section in <i>Operations Bridge Reporter Configuration Guide</i>.</p>
Windows Authentication	<p>Option to enable Windows authentication for accessing the OM database. The user can use the same credentials to access OM as that of the Windows system hosting the database.</p> <p>This option only appears if OM for Windows is selected as the data source type.</p>
User name	<p>Name of the OM database user.</p> <p>Note: For the OM for Windows data source type, if the Windows Authentication option is selected, this field is disabled.</p>
Password	Password of the OM database user.

Field	Description
	Note: For the OM for Windows data source type, if the Windows Authentication option is selected, this field is disabled.
Collection Station	This option is used for a collector installed on a remote system.

4. Click **OK**.
5. Click **Save**.
 A Saved Successfully message appears in the Information message panel.

To modify a VMware vCenter topology source connection:

1. In the Administration Console, click **Data Source Configuration > Topology Source**.
 The Topology Source page appears.
2. For a specific host, click **Edit**.
 The Connection Parameters dialog box appears.
3. In the **Connection Parameters** dialog box, type the following connection parameters:

Field	Description
Host name	IP address or FQDN of the VMware vCenter server.
User name	Name of the VMware vCenter user.
Password	Password of the VMware vCenter user.
Collection Station	This option is used for a collector installed on a remote system.

4. Click **OK**.
5. Click **Save**.
6. In the message box, click **Yes**.
 A Saved Successfully message appears in the Information message panel.

Enable or disable a Topology Source data collection

1. In the Administration Console, click **Data Source Configuration > Topology Source**.
 The Topology Source page appears.

2. For a specific host, perform any one of the followings steps:
 - Select the check box in the **Enable Collection** column to enable data collection.
 - Clear the check box in the **Enable Collection** column to disable data collection.
3. Click **Save**.

A Saved Successfully message appears in the Information message panel.

Schedule a Topology Source collection

To schedule an RTSM topology source collection:

1. In the Administration Console, click **Data Source Configuration > Topology Source**.

The Topology Source page appears.
2. For one or more hosts, specify a synchronization time between 1 and 24 hours in the **Hrs** box in the **Collection Frequency (Hrs)** column.
3. Click **Save**.

A Saved Successfully message appears in the Information message panel.

To schedule an OM topology source collection:

1. In the Administration Console, click **Data Source Configuration > Topology Source**.

The Topology Source page appears.
2. For one or more hosts, specify a synchronization time between 1 and 24 hours in the **Hrs** box under **Collection Frequency (Hrs)**, and then click **Apply**.
3. Click **Save**.

A Saved Successfully message appears in the Information message panel.

To schedule a VMware vCenter topology source collection:

1. In the Administration Console, click **Data Source Configuration > Topology Source**.

The Topology Source page appears.
2. For one or more hosts, specify a synchronization time between 1 and 24 hours in the **Mins** box under **Collection Frequency (Hrs)**, and then click **Apply**.
3. Click **Save**.

A Saved Successfully message appears in the Information message panel.

Test the Topology Source connection

To test the RTSM topology source connection:

1. In the Administration Console, click **Data Source Configuration > Topology Source**.
The Topology Source page appears.
2. Select the required host and click **Test Connection**.
A `Test Connection Successful` message appears in the Information message panel if the connection exists.

Note: The test connection to RTSM topology source will be successful only if Oracle view exist in the RTSM.

To test the OM topology source connection:

1. In the Administration Console, click **Data Source Configuration > Topology Source**.
The Topology Source page appears.
2. Select the required host and click **Test Connection**.

Note: You cannot test more than one OM connection at a time.

A `Test Connection Successful` message appears in the Information message panel if the connection exists.



To test the VMware Vcenter topology source connection:

1. In the Administration Console, click **Data Source Configuration > Topology Source**.
The Topology Source page appears.
2. Select the required host and click **Test Connection**.





Note: You cannot test more than one VMware vCenter connection at a time.

A `Test Connection Successful` message appears in the Information message panel if the connection exists.

View Topology Source connection status

1. In the Administration Console, click **Data Source Configuration > Topology Source**.
The Topology Source page appears.
2. Check the connection status indicator in the **Connection Status** column:
 -  indicates that the host system is connected to the data source.
 -  indicates that the host system is not connected to the data source.

View Topology Source data collection status

1. In the Administration Console, click **Data Source Configuration > Topology Source**.
The Topology Source page appears.
2. Check the collection status indicator in the **Collection Status** column:
Status of the collection with the date and time of the latest collection attempt and the current status:
 -  indicates that the data collection is in progress.
 -  indicates that the data collection completed successfully in the previous attempt.
 -  indicates that the data collection failed in the previous attempt.
 -  indicates that the data collection was never started.

Collection Status column is not displayed when VMware vCenter is the topology source.



Chapter 17: Operations Manager





You can use the Operations Manager page to view a list of OM data sources, which collect performance and event-related data of business-critical enterprise systems, applications, and services. Using this page, you can schedule the data collection frequency, enable, or disable data collection, and also add or delete data collection connections based on your requirements.

Use the Operations Manager page to:

- [Create an OM data source connection](#)
- [Modify an OM data source connection](#)
- [Enable an OM data collection](#)
- [Schedule an OM data collection](#)
- [Test the OM data source connection](#)
- [View the OM data source connection status](#)
- [View the OM data collection status](#)
- [Delete an OM data source connection](#)

The Operations Manager page includes:

Field	Description
Host name/Service Name	IP address or FQDN of the OM database server.
Enable Collection	Enable or disable a OM data collection.
Schedule Frequency	Time (in hours) to synchronize the OBR database with the OM data source.
Status	Status of an OM connection and data collection.
Connection	Status of the OM connection. <ul style="list-style-type: none">•  indicates that the host system is connected to the data source.•  indicates that the host system is not connected to the data source.
Collection	Status of the collection with the date and time of the latest collection attempt and the current status:

Field	Description
	<ul style="list-style-type: none">  indicates that the data collection is in progress.  indicates that the data collection completed successfully in the previous attempt.  indicates that the data collection failed in the previous attempt.  indicates that the data collection was never started.
Test Connection	Test an OM data source connection.
Delete	Delete an OM data source connection.
Create New	Create a new OM data source connection.
Edit	Modify an existing OM data source connection.
Save	Save a specific OM configuration attributes.

Connection Parameters

Field	Description
Database in Oracle RAC	Option to enable OM database on Oracle RAC.
Enable TLS	Enable JDBC connection over TLS.
Host name	IP address or FQDN of the OM database server. If the OM database is configured on a remote system, the machine name of the remote system must be typed here.
Port	Port number to query the OM database server. The default port is 1433 if SQL Server is the database type and 1521 if Oracle is the database type.
Database Instance	System Identifier (SID) of the database instance. The default database instance is OVOPS. Note: For information about the database host name, port number, and SID, contact your OM database administrator.
Database type	The type of database engine that is used to create the OM database. It can either be Oracle or MSSQL.
Windows	If you have selected MSSQL as the database type, you have the option to

Field	Description
Authentication	<p>enable Windows authentication for MSSQL, that is, the user can use the same credentials to access SQL Server as that of the Windows system hosting the database.</p> <p>Note: If you are using the database method of authentication to connect to the OM database server, you must provide the user details that have the select and connect permissions for the “openview” database here.</p>
User name	Name of the OM database user.
Password	Password of the OM database user.
Collection Station	This option is used for a collector installed on a remote system.
Database in Oracle RAC selected:	
Service Name	Specify the name by which OBR connects to the Oracle instance. This option appears only if OM on Oracle RAC is selected.
ORA file name	The *.ora configuration file that defines database addresses for establishing connections. Manually copy this file from the data source system to the {PMDB_HOME}/config folder in the OBR system. This option appears only if OM on Oracle RAC is selected.
Database type	The type of database engine that is used to create the OM database.
User name	Name of the database user.
Password	Password of the database user.
Collection Station	This option is used for a collector installed on a remote system.
Enable TLS selected:	
Truststore Path	Full path to the truststore path. This option is displayed when Enable TLS is selected.
Truststore Password	The password to access the truststore. This option is displayed when Enable TLS is selected.
Service Name	Specify the name by which OBR connects to the Oracle instance. This option appears only if OM on Oracle RAC is selected.
ORA file name	The *.ora configuration file that defines database addresses for establishing connections. Manually copy this file from the data source system to the {PMDB_HOME}/config folder in the OBR system. This option appears only if OM on Oracle RAC is selected.
Database type	The type of database engine that is used to create the OM database.

Field	Description
User name	Name of the database user.
Password	Password of the database user.
Collection Station	This option is used for a collector installed on a remote system.

Create an OM data source connection

Note: When you create a data source connection for OM on the Topology Source page, the same data source connection appears on the Operation Manager page as well. However, updating the data source connection on the Topology Source page does not update the connection details on the Operation Manager page.

1. In the Administration Console, click **Data Source Configuration > Operations Manager**.
The Operations Manager page appears.
2. Click **Create New**.
The Connection Parameters dialog box appears.

Note: If you are using the database method of authentication to connect to the OM database server, you must provide the user details that have the select and connect permissions for the “openview” database here.

3. In the **Connection Parameters** dialog box, type the following values:

Field	Description
Database in Oracle RAC	Option to enable OM database on Oracle RAC.
Enable TLS	Enable JDBC connection over TLS.
Host name	IP address or FQDN of the OM database server. If the OM database is configured on a remote system, the machine name of the remote system must be typed here.
Port	Port number to query the OM database server. The default port is 1433 if SQL Server is the database type and 1521 if Oracle is the database type.
Database Instance	System Identifier (SID) of the database instance. The default database instance is OVOPS.

Field	Description
	<p>Note: For information about the database host name, port number, and SID, contact your OM database administrator.</p>
Database type	The type of database engine that is used to create the OM database. It can either be Oracle or MSSQL.
Windows Authentication	<p>If you have selected MSSQL as the database type, you have the option to enable Windows authentication for MSSQL, that is, the user can use the same credentials to access SQL Server as that of the Windows system hosting the database.</p> <p>Note: If you are using the database method of authentication to connect to the OM database server, you must provide the user details that have the select and connect permissions for the “openview” database here.</p>
User name	Name of the OM database user.
Password	Password of the OM database user.
Collection Station	This option is used for a collector installed on a remote system.
Database in Oracle RAC selected:	
Service Name	Specify the name by which OBR connects to the Oracle instance. This option appears only if OM on Oracle RAC is selected.
ORA file name	The *.ora configuration file that defines database addresses for establishing connections. Manually copy this file from the data source system to the {PMDB_HOME}/config folder in the OBR system. This option appears only if OM on Oracle RAC is selected.
Database type	The type of database engine that is used to create the OM database.
User name	Name of the database user.
Password	Password of the database user.
Collection Station	This option is used for a collector installed on a remote system.
Enable TLS selected:	
Truststore Path	Full path to the truststore path. This option is displayed when Enable TLS is selected.
Truststore Password	The password to access the truststore. This option is displayed when Enable TLS is selected.

Field	Description
Service Name	Specify the name by which OBR connects to the Oracle instance. This option appears only if OM on Oracle RAC is selected.
ORA file name	The *.ora configuration file that defines database addresses for establishing connections. Manually copy this file from the data source system to the {PMDB_HOME}/config folder in the OBR system. This option appears only if OM on Oracle RAC is selected.
Database type	The type of database engine that is used to create the OM database.
User name	Name of the database user.
Password	Password of the database user.
Collection Station	This option is used for a collector installed on a remote system.

4. Click **Save**.

A Saved Successfully message appears in the Information message panel.

Data collection for the newly created OM data source is enabled by default. In addition, the collection frequency is scheduled for every one hour.

Modify an OM data source connection

1. In the Administration Console, click **Data Source Configuration > Operations Manager**. The Operations Manager page appears.
2. Select the column for a specific host that has to be modified and click **Edit**. The Connection Parameters dialog box appears.

Note: If you are using the database method of authentication to connect to the OM database server, you must provide the user details that have the select and connect permissions for the “openview” database here.

3. In the **Connection Parameters** dialog box, type the following values:

Field	Description
Database in Oracle RAC	Option to enable OM database on Oracle RAC.
Enable TLS	Enable JDBC connection over TLS.

Field	Description
Host name	IP address or FQDN of the OM database server. If the OM database is configured on a remote system, the machine name of the remote system must be typed here.
Port	Port number to query the OM database server. The default port is 1433 if SQL Server is the database type and 1521 if Oracle is the database type.
Database Instance	System Identifier (SID) of the database instance. The default database instance is OVOPS. Note: For information about the database host name, port number, and SID, contact your OM database administrator.
Database type	The type of database engine that is used to create the OM database. It can either be Oracle or MSSQL.
Windows Authentication	If you have selected MSSQL as the database type, you have the option to enable Windows authentication for MSSQL, that is, the user can use the same credentials to access SQL Server as that of the Windows system hosting the database. Note: If you are using the database method of authentication to connect to the OM database server, you must provide the user details that have the select and connect permissions for the "openview" database here.
User name	Name of the OM database user.
Password	Password of the OM database user.
Collection Station	This option is used for a collector installed on a remote system.
Database in Oracle RAC selected:	
Service Name	Specify the name by which OBR connects to the Oracle instance. This option appears only if OM on Oracle RAC is selected.
ORA file name	The *.ora configuration file that defines database addresses for establishing connections. Manually copy this file from the data source system to the {PMDb_HOME}/config folder in the OBR system. This option appears only if OM on Oracle RAC is selected.
Database type	The type of database engine that is used to create the OM database.
User name	Name of the database user.

Field	Description
Password	Password of the database user.
Collection Station	This option is used for a collector installed on a remote system.
Enable TLS selected:	
Truststore Path	Full path to the <code>truststore</code> path. This option is displayed when Enable TLS is selected.
Truststore Password	The password to access the truststore. This option is displayed when Enable TLS is selected.
Service Name	Specify the name by which OBR connects to the Oracle instance. This option appears only if OM on Oracle RAC is selected.
ORA file name	The <code>*.ora</code> configuration file that defines database addresses for establishing connections. Manually copy this file from the data source system to the <code>{PMDB_HOME}/config</code> folder in the OBR system. This option appears only if OM on Oracle RAC is selected.
Database type	The type of database engine that is used to create the OM database.
User name	Name of the database user.
Password	Password of the database user.
Collection Station	This option is used for a collector installed on a remote system.

4. Click **Save**.

A `Saved Successfully` message appears in the Information message panel.

Enable or disable an OM data collection

1. In the Administration Console, click **Data Source Configuration > Operations Manager**.
The Operations Manager page appears.
2. For one or more hosts, perform any one of the following steps:
 - Select the check box in the **Enable Collection** column to enable data collection.
 - Clear the check box in the **Enable Collection** column to disable data collection.
3. Click **Save**.

A `Saved Successfully` message appears in the Information message panel.



Schedule an OM data collection

1. In the Administration Console, click **Data Source Configuration > Operations Manager**.
The Operations Manager page appears.
2. For one or more hosts, specify a collection time between 1 and 24 hours in the **Hrs** box in the **Schedule Frequency** column.
3. Click **Save**.
A `Saved Successfully` message appears in the Information message panel.

Test the OM data source connection

1. In the Administration Console, click **Data Source Configuration > Operations Manager**.
The Operations Manager page appears.
2. Select the specific host to test the connection.
Note: You cannot test more than one OM connection at a time.
3. Click **Test Connection**.
A `Test Connection Successful` message appears in the Information message panel if connection exists.





View the OM data source connection status

1. In the Administration Console, click **Data Source Configuration > Operations Manager**.
The Operations Manager page appears.
2. For one or more hosts, check the connection status indicator in the **Connection Status** column:
 -  indicates that the host system is connected to the data source.
 -  indicates that the host system is not connected to the data source.

View the OM data collection status

1. In the Administration Console, click **Data Source Configuration > Operations Manager**.
The Operations Manager page appears.
2. For one or more hosts, check the connection status indicator in the **Collection Status** column:

Status of the collection with the date and time of the latest collection attempt and the current status:

-  indicates that the data collection is in progress.
-  indicates that the data collection completed successfully in the previous attempt.
-  indicates that the data collection failed in the previous attempt.
-  indicates that the data collection was never started.

Delete an OM data source connection

1. In the Administration Console, click **Data Source Configuration > Operations Manager**.
The Operations Manager page appears.
2. Select the column to delete one or more OM data source connections.
3. Click **Delete**.
A Deleted Successfully message appears in the Information message panel.
4. Click **Save**.
A Saved Successfully message appears in the Information message panel.






Chapter 18: SiteScope

You can use the SiteScope page to configure a SiteScope data source, which collects data from several SiteScope monitors in your environment. Using this page, you can enable or disable data collection and add or delete the data collection connection according to your requirements.

Use the SiteScope page to:

- [Create a SiteScope data source connection](#)
- [Modify a SiteScope data source connection](#)
- [Enable or disable SiteScope data collection](#)
- [Test the SiteScope data source connection](#)
- [View the SiteScope data source connection status](#)
- [View the SiteScope data collection status](#)
- [Delete a SiteScope data source connection](#)

The SiteScope page includes:

Field	Description
Host name	IP address or FQDN of the SiteScope server.
Enable Collection	Enable or disable data collection.
Connection Status	Status of SiteScope connection. <ul style="list-style-type: none">•  indicates that the host system is connected to the data source.•  indicates that the host system is not connected to the data source.
Collection Status	Status of the collection with the date and time of the latest collection attempt and the current status: <ul style="list-style-type: none">•  indicates that the data collection is in progress.•  indicates that the data collection completed successfully in the previous attempt.•  indicates that the data collection failed in the previous attempt.

Field	Description
	<ul style="list-style-type: none"> □□ indicates that the data collection was never started.
Test Connection	Test a SiteScope data source connection.
Discover Data Source	If you have configured the RTSM topology source, this button discovers all the associated SiteScope servers. Also, you must have deployed the SiS_Profile view.
Create New	<p>Create a new SiteScope data source connection.</p> <p>Note: The Create New option is disabled after you create a new connection or if an SiteScope connection already exists.</p>
Edit	Modify an existing SiteScope data source connection.
Delete	Delete a SiteScope data source connection.
Save	Save the changes made on this page.

Connection Parameters

You must fill out the following fields to create a new SiteScope data source.

Field	Description
Connection Settings	
Host name	IP address or FQDN of the SiteScope server.
Port	Port number to query the SiteScope server.
Use SSL	Optional; if selected, you must enable the SiteScope server too to support communication over Secure Sockets Layer (SSL).
User name	Name of the SiteScope user.
Password	Password of the SiteScope user.
Collection Station	This option is used for a collector installed on a remote system.
<p>General Data Integration Settings: These settings create a generic data integration between the SiteScope server and the OBR server. After the connection is successful, SiteScope servers push data to the OBR server.</p> <p>Also, you must create a tag in OBR that you must manually apply to the SiteScope monitors that you want to report on. For more information on applying the tag, see documentation for SiteScope.</p>	

Field	Description
Create Integration	Check box to create integration between the SiteScope server and the OBR server.
Integration name	Enter the name of the integration. Note: You cannot change it later.
Encoding	The encoding type for communication between OBR and SiteScope.
Init String	Shared key used to establish a connection to SiteScope server.
Use SSL	Optional; if selected, you must enable the SiteScope server too to support communication over Secure Sockets Layer (SSL).
Reporting interval (seconds)	User configurable; frequency at which SiteScope pushes data to OBR.
Request timeout (seconds)	User configurable; the time to wait before the connection times out. Value of zero (0) gives you infinite timeout period.
Connection timeout (seconds)	User configurable; timeout until connection is reestablished. Value of zero (0) means timeout is not used.
Number of retries	Number of retries that SiteScope server attempts during connection error with OBR.
Authentication when requested	Optional; if selected, authentication is performed using the Web server user name and password.
Authentication user name	If OBR is configured to use basic authentication, specify the user name to access the server.
Authentication password	If OBR is configured to use basic authentication, specify the password to access the server.
Proxy address	If proxy is enabled on SiteScope, enter the proxy address.
Proxy user name	Enter user name of the proxy server.
Proxy password	Enter password of the proxy server.
Create tag	Select it to create a tag for the SiteScope monitors that you must manually apply from the SiteScope server.
Tag name	User defined name of the tag.

Create a SiteScope data source connection

To create a new SiteScope data source connection:

1. In the Administration Console, click **Data Source Configuration > SiteScope**.
The SiteScope page appears.
2. Click **Create New**.
The Connection Parameters dialog box appears.
3. In the **Connection Parameters** dialog box, type the following values:

Field	Description
Connection Settings	
Host name	IP address or FQDN of the SiteScope server.
Port	Port number to query the SiteScope server.
Use SSL	Optional; if selected, you must enable the SiteScope server too to support communication over Secure Sockets Layer (SSL).
User name	Name of the SiteScope user.
Password	Password of the SiteScope user.
Collection Station	This option is used for a collector installed on a remote system.
<p>General Data Integration Settings: These settings create a generic data integration between the SiteScope server and the OBR server. After the connection is successful, SiteScope servers push data to the OBR server.</p> <p>Also, you must create a tag in OBR that you must manually apply to the SiteScope monitors that you want to report on. For more information on applying the tag, see documentation for SiteScope.</p>	
Create Integration	Check box to create integration between the SiteScope server and the OBR server.
Integration name	Enter the name of the integration. Note: You cannot change it later.
Encoding	The encoding type for communication between OBR and SiteScope.
Init String	Shared key used to establish a connection to SiteScope server.
Use SSL	Optional; if selected, you must enable the SiteScope server too to support communication over Secure Sockets Layer (SSL).
Reporting interval (seconds)	User configurable; frequency at which SiteScope pushes data to OBR.
Request timeout	User configurable; the time to wait before the connection times out.

Field	Description
(seconds)	Value of zero (0) gives you infinite timeout period.
Connection timeout (seconds)	User configurable; timeout until connection is reestablished. Value of zero (0) means timeout is not used.
Number of retries	Number of retries that SiteScope server attempts during connection error with OBR.
Authentication when requested	Optional; if selected, authentication is performed using the Web server user name and password.
Authentication user name	If OBR is configured to use basic authentication, specify the user name to access the server.
Authentication password	If OBR is configured to use basic authentication, specify the password to access the server.
Proxy address	If proxy is enabled on SiteScope, enter the proxy address.
Proxy user name	Enter user name of the proxy server.
Proxy password	Enter password of the proxy server.
Create tag	Select it to create a tag for the SiteScope monitors that you must manually apply from the SiteScope server.
Tag name	User defined name of the tag.

4. Click **Save**.

A *Saved Successfully* message appears in the Information message panel.

Data collection for the newly created SiteScope data source connection is enabled by default. In addition, the collection frequency is scheduled for every 15 minutes.

Modify a SiteScope data source connection

1. In the Administration Console, click **Data Source Configuration > SiteScope**.
The SiteScope page appears.
2. Select the column for a specific host that has to be modified and click **Edit**.
The Connection Parameters dialog box appears.
3. In the **Connection Parameters** dialog box, type the following values:

Field	Description
Connection Settings	
Host name	IP address or FQDN of the SiteScope server.
Port	Port number to query the SiteScope server.
Use SSL	Optional; if selected, you must enable the SiteScope server too to support communication over Secure Sockets Layer (SSL).
User name	Name of the SiteScope user.
Password	Password of the SiteScope user.
Collection Station	This option is used for a collector installed on a remote system.
<p>General Data Integration Settings: These settings create a generic data integration between the SiteScope server and the OBR server. After the connection is successful, SiteScope servers push data to the OBR server.</p> <p>Also, you must create a tag in OBR that you must manually apply to the SiteScope monitors that you want to report on. For more information on applying the tag, see documentation for SiteScope.</p>	
Create Integration	Check box to create integration between the SiteScope server and the OBR server.
Integration name	Enter the name of the integration. Note: You cannot change it later.
Encoding	The encoding type for communication between OBR and SiteScope.
Init String	Shared key used to establish a connection to SiteScope server.
Use SSL	Optional; if selected, you must enable the SiteScope server too to support communication over Secure Sockets Layer (SSL).
Reporting interval (seconds)	User configurable; frequency at which SiteScope pushes data to OBR.
Request timeout (seconds)	User configurable; the time to wait before the connection times out. Value of zero (0) gives you infinite timeout period.
Connection timeout (seconds)	User configurable; timeout until connection is reestablished. Value of zero (0) means timeout is not used.
Number of retries	Number of retries that SiteScope server attempts during connection error with OBR.
Authentication when	Optional; if selected, authentication is performed using the Web

Field	Description
requested	server user name and password.
Authentication user name	If OBR is configured to use basic authentication, specify the user name to access the server.
Authentication password	If OBR is configured to use basic authentication, specify the password to access the server.
Proxy address	If proxy is enabled on SiteScope, enter the proxy address.
Proxy user name	Enter user name of the proxy server.
Proxy password	Enter password of the proxy server.
Create tag	Select it to create a tag for the SiteScope monitors that you must manually apply from the SiteScope server.
Tag name	User defined name of the tag.

4. Click **Save**.

A Saved Successfully message appears in the Information message panel.

Enable or disable SiteScope data collection

1. In the Administration Console, click **Data Source Configuration > SiteScope**.
The SiteScope page appears.
2. Perform any one of the following steps:
 - o Select the check box in the **Enable Collection** column to enable data collection.
 - o Clear the check box in the **Enable Collection** column to disable data collection.
3. Click **Save**.



A Saved Successfully message appears in the Information message panel.

Test the SiteScope data source connection





1. In the Administration Console, click **Data Source Configuration > SiteScope**.
The SiteScope page appears.

2. Select a specific host to be tested and click **Test Connection**.
A `Test Connection Successful` message appears in the Information message panel if connection exists.

View the SiteScope data source connection status

1. In the Administration Console, click **Data Source Configuration > SiteScope**.
The SiteScope page appears.
2. Check the connection status indicator in the **Connection Status** column:
 -  indicates that the host system is connected to the data source.
 -  indicates that the host system is not connected to the data source.

View the SiteScope data collection status

1. In the Administration Console, click **Data Source Configuration > SiteScope**.
The SiteScope page appears.
2. Check the collection status indicator in the **Collection Status** column:
Status of the collection with the date and time of the latest collection attempt and the current status:
 -  indicates that the data collection is in progress.
 -  indicates that the data collection completed successfully in the previous attempt.
 -  indicates that the data collection failed in the previous attempt.
 -  indicates that the data collection was never started.

Delete a SiteScope data source connection

1. In the Administration Console, click **Data Source Configuration > SiteScope**.
The SiteScope page appears.
2. Click **Delete**.
A Deleted Successfully message appears in the Information message panel.
3. Click **Save**.
A Saved Successfully message appears in the Information message panel.

Chapter 19: Generic Database


You can use the Generic Database page to configure generic databases from where you want to collect any type of data. This page is typically used to configure the Network Performance Server (NPS) to collect performance data from Network Node Manager i (NNMi). Using this page, you can schedule the data collection frequency, enable, or disable data collection, and also add or delete data collection connections based on your requirements.






Out-of-the-box, OBR supports configuration to generic data sources that use Oracle, Sybase, or Microsoft SQL Server database types. However, using this page, you can also configure OBR to connect to and collect data from other generic database types as well, such as MySQL, PostgreSQL, and so on. For a particular database type, you can specify the domain for which you want OBR to collect data such as system data, network data, and so on. For more information on how to configure such data sources, contact HPE Support.

Use the Operations Manager page to:

- [Create a generic database connection](#)
- [Modify a generic database connection](#)
- [Enable or disable a generic database data collection](#)
- [Schedule a generic database data collection](#)
- [Test the generic database connection](#)
- [View the generic database connection status](#)
- [View the generic database collection status](#)
- [Delete a generic database connection](#)

The Generic Database page includes:

Field	Description
Host name	IP address or FQDN of the generic database server.
Enable Collection	Enable or disable data collection from a generic database.
Schedule Frequency	Time (in hours) to synchronize the OBR database with the generic database.
Connection Status	Status of generic database connection. <ul style="list-style-type: none">•  indicates that the host system is connected to the data source.

Field	Description
	<ul style="list-style-type: none">  indicates that the host system is not connected to the data source.
Collection Status	<p>Status of the collection with the date and time of the latest collection attempt and the current status:</p> <ul style="list-style-type: none">  indicates that the data collection is in progress.  indicates that the data collection completed successfully in the previous attempt.  indicates that the data collection failed in the previous attempt.  indicates that the data collection was never started.
Configuration	Modify an existing generic database connection.
Test Connection	Test a generic database connection.
Delete	Delete a generic database connection.
Create New	Create a new generic database connection.
Save	Save specific generic database attributes.

Connection Parameters

Field	Description
Host name	IP address or FQDN of the generic database server.
Port	Port number to query the database server.
Time zone	<p>The time zone in which the database instance is configured.</p> <p>Note: You must select the same time zone for the database as the time zone of the data collected from data sources. They cannot be in different time zones.</p>
Database type	The type of database engine that is used to create the database. It can be Sybase IQ, Sybase ASE, Oracle, PostgreSQL, Vertica or MSSQL.
Domain	Select the domain (s) for which you want OBR to collect data from the selected database type.

Field	Description
URL	<p>The URL of the database instance. The syntax for the URL for each of the database types is:</p> <ul style="list-style-type: none"> • Oracle: <code>jdbc:hp:oracle://<server>:<port>;SID=<sid></code> <p>In an Oracle Real Application Cluster (RAC), copy the TNS ORA file to the OBR system and provide the absolute path in the following URL syntax:</p> <pre>jdbc:hp:oracle:TNSNamesFile=<absolute path of TNS ORA file>;TNSServerName=<Service name></pre> <ul style="list-style-type: none"> • MSSQL: <code>jdbc:jtds:sqlserver://<server><port>/<database>;instance=<dbInstance></code> • Sybase IQ: <code>jdbc:sybase:Tds:<server>:<port>/<database></code> • Sybase ASE: <code>jdbc:sybase:Tds:<server>:<port>?ServiceName=<dbInstance></code> • PostgreSQL: <code>jdbc:postgresql://<server>:<port>/<database></code> • Vertica: <code>jdbc:vertica://<server>:<port>/<database></code> <p>where <code><server></code>, <code><port></code>, <code><sid></code>, <code><database></code>, and <code><dbInstance></code> are replaceable variables that you must enter.</p>
User name	Name of the generic database user.
Password	Password of the generic database user.
Collection Station	This option is used for a collector installed on a remote system.

Create a generic database connection

1. In the Administration Console, click **Data Source Configuration > Generic Database**.
The Generic Database page appears.
2. Click **Create New**.
The Connection Parameters dialog box appears.
3. In the **Connection Parameters** dialog box, type the following values:

Field	Description
Host name	IP address or FQDN of the generic database server.
Port	Port number to query the database server.
Time zone	The time zone in which the data is stored into the source database.
Database type	The type of database engine that is used to create the database. It can be Sybase IQ, Sybase ASE, Oracle, MSSQL, PostgreSQL or Vertica.
Domain	Select the domain(s) for which you want OBR to collect data from the selected database type.
URL	<p>The URL of the database instance. The syntax for the URL for each of the database types is:</p> <ul style="list-style-type: none"> ◦ Oracle: <code>jdbc:hp:oracle://<server>:<port>;SID=<sid></code> <p>In an Oracle Real Application Cluster (RAC), copy the TNS ORA file to the OBR system and provide the absolute path in the following URL syntax:</p> <pre>jdbc:hp:oracle:TNSNamesFile=<absolute path of TNS ORA file>;TNSServerName=<Service name></pre> <ul style="list-style-type: none"> ◦ MSSQL: <code>jdbc:jtds:sqlserver://<server>:<port>/<database>;instance=<dbInstance></code> ◦ Sybase IQ: <code>jdbc:sybase:Tds:<server>:<port>/<database></code> ◦ Sybase ASE: <code>jdbc:sybase:Tds:<server>:<port>?ServiceName=<dbInstance></code> ◦ PostgreSQL: <code>jdbc:postgresql://<server>:<port>/<database></code> ◦ Vertica: <code>jdbc:vertica://<server>:<port>/<database></code> <p>where <server>, <port>, <sid>, <database>, and <dbInstance> are replaceable variables that you must enter.</p>
User name	Name of the generic database user.
Password	Password of the generic database user.
Collection Station	The name of the system where the collector is installed.

4. Click **Save**.

A Saved Successfully message appears in the Information message panel.

Data collection for the newly created data source is enabled by default. In addition, the collection frequency is scheduled for every one hour.

Note: Sybase IQ as Data Source

If you have configured Sybase IQ as your data source and collection is not happening when network data source is configured, follow these steps:

1. Copy the `jconn4.jar` from Sybase IQ server to `$PMDB_HOME/lib` directory.
2. Restart the collection service.

Note: If the Generic DB is configured to collect from Remote Collector, you have to manually copy the `jconn4.jar` file to the Collector system and then continue with the generic database configuration.

To copy the `jconn4.jar` file, follow these steps:

1. Copy the `jconn4.jar` from Generic DB server to `$PMDB_HOME/lib` directory on Collector system.
2. Restart the collection service.

Modify a generic database connection

1. In the Administration Console, click **Data Source Configuration > Generic Database**. The Generic Database page appears.
2. Select the column for a specific host that has to be modified and click **Edit**. The Connection Parameters dialog box appears.
3. In the **Connection Parameters** dialog box, type the following values:

Field	Description
Host name	Address (IP or name) of the generic database server.
Port	Port number to query the database server.
Time zone	The time zone under which the database instance is configured.
Database type	The type of database engine that is used to create the generic database. It can be Sybase IQ, Sybase ASE, Oracle, PostgreSQL, Vertica or MSSQL.

Field	Description
Domain	Select the domain(s) for which you want OBR to collect data from the selected database type.
URL	<p>The URL of the database instance. The syntax for the URL for each of the database types is:</p> <ul style="list-style-type: none"> ◦ Oracle: <code>jdbc:hp:oracle://<server>:<port>;SID=<sid></code> <p>In an Oracle Real Application Cluster (RAC), copy the TNS ORA file to the OBR system and provide the absolute path in the following URL syntax:</p> <pre>jdbc:hp:oracle:TNSNamesFile=<absolute path of TNS ORA file>;TNSServerName=<Service name></pre> <ul style="list-style-type: none"> ◦ MSSQL: <code>jdbc:jtds:sqlserver://<server>:<port>/<database>;instance=<dbInstance></code> ◦ Sybase IQ: <code>jdbc:sybase:Tds:<server>:<port>/<database></code> ◦ Sybase ASE: <code>jdbc:sybase:Tds:<server>:<port>?ServiceName=<dbInstance></code> ◦ PostgreSQL: <code>jdbc:postgresql://<server>:<port>/<database></code> ◦ Vertica: <code>jdbc:vertica://<server>:<port>/<database></code> <p>where <i><server></i>, <i><port></i>, <i><sid></i>, <i><database></i>, and <i><dbInstance></i> are replaceable variables that you must enter.</p>
User name	Name of the generic database user.
Password	Password of the generic database user.
Collection Station	The name of the system where the collector is installed.

4. Click **Save**.

A Saved Successfully message appears in the Information message panel.

Enable or disable a generic database data collection

1. In the Administration Console, click **Data Source Configuration > Generic Database**.
 The Generic Database page appears.

2. For one or more hosts, perform any one of the following steps:
 - Select the check box in the **Enable Collection** column to enable data collection.
 - Clear the check box in the **Enable Collection** column to disable data collection.
3. Click **Save**.

A `Saved Successfully` message appears in the Information message panel.

Schedule a generic database data collection

1. In the Administration Console, click **Data Source Configuration > Generic Database**.

The Generic Database page appears.
2. For one or more hosts, specify a collection time between 1 and 24 hours in the **Hrs** box in the **Schedule Frequency** column.
3. Click **Save**.

A `Saved Successfully` message appears in the Information message panel.

Test the generic database connection

1. In the Administration Console, click **Data Source Configuration > Generic Database**.

The Generic Database page appears.
2. Select the column for a specific database connection.



Note: You cannot test more than one connection at a time.
3. Click **Test Connection**.

A `Test Connection Successful` message appears in the Information message panel if connection exists.

View the generic database connection status





1. In the Administration Console, click **Data Source Configuration > Generic Database**.

The Generic Database page appears.
2. For one or more hosts, check the connection status indicator in the **Connection Status** column:

-  indicates that the host system is connected to the data source.
-  indicates that the host system is not connected to the data source.

View the generic database collection status

1. In the Administration Console, click **Data Source Configuration > Generic Database**.
The Generic Database page appears.
2. For one or more hosts, check the connection status indicator in the **Collection Status** column:
Status of the collection with the date and time of the latest collection attempt and the current status:

-  indicates that the data collection is in progress.
-  indicates that the data collection completed successfully in the previous attempt.
-  indicates that the data collection failed in the previous attempt.
-  indicates that the data collection was never started.

Delete a generic database connection

1. In the Administration Console, click **Data Source Configuration > Generic Database**.
The Generic Database page appears.
2. Select the column to delete one or more database connections.
3. Click **Delete**.
A Deleted Successfully message appears in the Information message panel.
4. Click **Save**.
A Saved Successfully message appears in the Information message panel.



Chapter 20: VMware vCenter

You can use the VMware vCenter Data Source page to view a list of VMware vCenter data sources, which collect performance and event-related data of business-critical VMware installed in your environment. Using this page, you can schedule the data collection frequency, enable, or disable data collection, and also add or delete data collection connections based on your requirements.

Use the VMware vCenter page to:

- [Create VMware vCenter data source connection](#)
- [Modify a VMware vCenter data source connection](#)
- [Enable a VMware vCenter data collection](#)
- [Schedule a VMware vCenter data collection](#)
- [Test the VMware vCenter data source connection](#)
- [View the VMware vCenter data source connection status](#)

The VMware vCenter Data Source page includes:

Field	Description
Host name	IP address or FQDN of the VMware vCenter database server.
Enable Collection	Enable or disable a VMware vCenter data source data collection.
Schedule Frequency	Time (in minutes) to synchronize the OBR database with the VMware vCenter data source.
Connection Status	Status of VMware vCenter connection. <ul style="list-style-type: none">•  indicates that the host system is connected to the data source.•  indicates that the host system is not connected to the data source.
Edit	Modify an existing VMware vCenter data source connection.
Test Connection	Test a VMware vCenter data source connection.
Create New	Create a new VMware vCenter data source connection.
Save	Save a specific VMware vCenter configuration attributes.

Connection Parameters

Field	Description
Host name	IP address or FQDN of the VMware vCenter database server. If the VMware vCenter database is configured on a remote system, the machine name of the remote system must be typed here.
User name	Name of the VMware vCenter database user.
Password	Password of the VMware vCenter database user.
Collection Station	This option is used for a collector installed on a remote system.

Note: If you have configured VMware vCenter as the topology source, data collection parameters are automatically configured.

Create VMware vCenter data source connection

Note: When you create a data source connection for VMware vCenter on the Topology Source page, the same data source connection appears on the VMware vCenter data collection page as well. You can create additional data sources from the VMware vCenter collection configuration page.

1. In the Administration Console, click **Data Source Configuration > VMware vCenter**.
The VMware vCenter page appears.
2. Click **Create New**.
The Connection Parameters dialog box appears.
3. In the **Connection Parameters** dialog box, type the following values:

Field	Description
Host name	IP address or FQDN of the VMware vCenter database server.
User name	Name of the VMware vCenter database user.
Password	Password of the VMware vCenter database user.
Collection Station	The name of the system where the collector is installed.

4. Click **Save**.
A **Saved Successfully** message appears in the Information message panel.

Data collection for the newly created VMware vCenter data source is enabled by default. In addition, the collection frequency is scheduled for every one hour.

Modify a VMware vCenter data source connection

1. In the Administration Console, click **Data Source Configuration > VMware vCenter**.
The VMware vCenter page appears.
2. Select the column for a specific host that has to be modified and click **Edit**.
The Connection Parameters dialog box appears.
3. In the **Connection Parameters** dialog box, type the following values:

Field	Description
Host name	IP address or FQDN of the VMware vCenter database server.
User name	Name of the VMware vCenter database user.
Password	Password of the VMware vCenter database user.
Collection Station	The name of the system where the collector is installed.

4. Click **Save**.
A **Saved Successfully** message appears in the Information message panel.

Enable or disable a VMware vCenter data collection

1. In the Administration Console, click **Data Source Configuration > VMware vCenter**.
The VMware vCenter page appears.
2. For one or more hosts, perform any one of the following steps:
 - Select the check box in the **Enable Collection** column to enable data collection.
 - Clear the check box in the **Enable Collection** column to disable data collection.
3. Click **Save**.
A **Saved Successfully** message appears in the Information message panel.



Schedule a VMware vCenter data collection

1. In the Administration Console, click **Data Source Configuration > VMware vCenter**.
The VMware vCenter page appears.
2. For one or more hosts, specify a collection time between 5 and 60 minutes in the **Mins** box in the **Schedule Frequency** column.
3. Click **Save**.
A `Saved Successfully` message appears in the Information message panel.

Test the VMware vCenter data source connection

1. In the Administration Console, click **Data Source Configuration > VMware vCenter**.
The VMware vCenter page appears.
2. Select a specific VMware vCenter connection host.
Note: You cannot test more than one VMware vCenter connection at a time.
3. Click **Test Connection**.
A `Test Connection Successful` message appears in the Information message panel if connection exists.

View the VMware vCenter data source connection status

1. In the Administration Console, click **Data Source Configuration > VMware vCenter**.
The VMware vCenter page appears.
2. For one or more hosts, check the connection status indicator in the **Connection Status** column:
 -  indicates that the host system is connected to the data source.
 -  indicates that the host system is not connected to the data source.

For more information on VMware vCenter data source configuration, see *Configuring the VMware vCenter Data Source* section in the *Operations Bridge Reporter Configuration Guide*.

Chapter 21: Operations Agent (OA)

You can use the Operations Agent (OA) page to manage the Operations Agent data collection. You do not need to create new Operations Agent data source connections because, by default, all the nodes on which the Operations Agent is installed are automatically discovered when the topology data is collected. These data sources or nodes are listed on the Operations Agent page. Using this page, you can schedule the Operations Agent data collection, enable or disable the data collection, and delete Operations Agent connections.

Use the Operations Agent page to:

- [View the Operations Agent data source details](#)
- [Enable an Operations Agent data source data collection](#)
- [Schedule an Operations Agent data source synchronization](#)
- [Test the Operations Agent data source connection](#)
- [Assign View/Node Group based Rules for Data Collection](#)
- [Assign Pattern based Rules for Data Collection](#)

The Operations Agent Data Source page includes:

Hosts tab: Host collection status summary

Field	Description
ETL Content pack component name	A list of topology views for the installed Content Packs. These topology views contain the specific CI attributes that the Operations Agent collector uses to collect the relevant data. <i>All</i> indicates all the views. <i>Unassigned</i> indicates the Operations Agent data sources that do not have any topology views assigned to it.
Hosts	The number of Operations Agent data sources for that particular view.
Passed	The number of distinct Operations Agent data sources from where the raw data was successfully collected.
Failed	The number of distinct Operations Agent data sources from where data collection failed.
Never Collected	The number of distinct Operations Agent data sources from where data was never collected.
Enabled	The number of distinct Operations Agent data sources that are enabled

Field	Description
	for data collection.
Disabled	The number of distinct Operations Agent data sources that are disabled for data collection.

Hosts tab: Hosts : <ETL Content pack component name>

OBR shows all the managed nodes discovered from the OM topology where the Operations Agent is installed. In an OM for Windows environment, the table lists the message allowed nodes too. However, the message allowed nodes do not contribute to the licensing computation.

Field	Description
Host name	Name of the Operations Agent data source.
Enabled	Option to select the Operations Agent data source data collection.
Collection Frequency	Time (in hours) to synchronize the OBR database with the Operations Agent data source. The minutes can be set in multiples of 15 minutes.
Assigned Collector	List of remote collectors enabled for data collection configured in OBR.
Collector assignment mode	List of rules you can apply on the remote collector. User: Select it when you want to overwrite any pre-assigned rule or when you want to manually assign a remote collector to a host. System: If the remote collector assignment is based on the rules mentioned by the user from the Assignment tab. Unassigned: Indicates that no rules are defined for the host. You must manually assign a remote collector to the host using the rule type "User" or add/modify the rule from the Assignment tab to assign a remote collector to the host.
Connection	Status of the Operations Agent data source connection.
Collection	Status of the data collection showing the date and local time of the latest collection attempt and the current status.
Test Connection	Test an Operations Agent data source connection.
Edit Group	Edit the listed nodes to change enable/disable status, Assigned collector and Collection frequency. Click Save to save the changes.
Save	Save the changes made to an Operations Agent data source connection.

Host Assignments tab: Hosts assignment

Field	Description
Collector name	Hostname of the remote collector.
Assigned patterns	Shows the rules or node/view groups assigned to the collector.
Assigned host groups	Shows the hosts assigned to the collector.
Total hosts assigned	Shows the total hosts assigned to the collector.
Update	Update the details of the collector.

Update Host Assignment

Field	Description
Collector name	Remote collectors configured in the OBR system.
Assignment based on: Host Group	Select it for writing a regular expression to assign a remote collector to Operations Agents.
Assignment based on: Host Pattern (Regular Expression)	Select it to assign a remote collector to a view or node group of the installed content packs.
Add new pattern	Define a new pattern. Appears only when Assignment based on Host Pattern(Regular Expression) is selected.
Available Groups	If the Assignment based on is "Host Group", it lists rules defined by the user.
Assigned Groups	If the Assignment based on "Host Pattern (Regular Expression)", it lists view or node groups of the installed content packs.

View the Operations Agent data source details

1. In the Administration Console, click **Data Source Configuration > Operations Agent**.
 The Operations Agent page appears.
2. In the Hosts tab: Host collection status summary, view:

Field	Description
ETL Content pack component name	A list of topology views for the installed Content Packs. These topology views contain the specific CI attributes that the Operations Agent collector uses to collect the relevant data.

Field	Description
	<i>All</i> indicates all the views. <i>Unassigned</i> indicates the Operations Agent data sources that do not have any topology views assigned to it.
Hosts	The number of Operations Agent data sources for that particular view.
Passed	The number of distinct Operations Agent data sources from where the raw data was successfully collected.
Failed	The number of distinct Operations Agent data sources from where data collection failed.
Never Collected	The number of distinct Operations Agent data sources from where data was never collected.
Enabled	The number of distinct Operations Agent data sources that are enabled for data collection.
Disabled	The number of distinct Operations Agent data sources that are disabled for data collection.

3. To view detailed information about the Operations Agent data sources, click the view name or the number in the Operations Agent Data Source Summary table. You can:
- Click the number in the Hosts column to list details of all the Operations Agent data sources.
 - Click the number in the Passed column to view the details of the Operations Agent data sources from where data collection was successful.
 - Click the number in the Failed column to view the details of the Operations Agent data sources from where data collection failed.
 - Click the number in the Never Collection column to view the details of the Operations Agent data sources from where data was never collected.
 - Click the number in the Enabled/Disabled column to view the details of the Operations Agent data sources were enabled or disabled for data collection.

The Operations Agent Data Source Application Details <view name> table appears as follows:


Field	Description
Host name	Name of the Operations Agent data source.
Enabled	Option to select the Operations Agent data source data collection.
Collection Frequency	Time (in hours) to synchronize the OBR database with the

Field	Description
	Operations Agent data source. The minutes can be set in multiples of 15 minutes.
Assigned Collector	List of remote collectors enabled for data collection configured in OBR.
Collector assignment mode	List of rules you can apply on the remote collector. User: Select it when you want to overwrite any pre-assigned rule or when you want to manually assign a remote collector to a host. System: If the remote collector assignment is based on the rules mentioned by the user from the Assignment tab. Unassigned: Indicates that no rules are defined for the host. You must manually assign a remote collector to the host using the rule type "User" or add/modify the rule from the Assignment tab to assign a remote collector to the host.
Connection Status	Option to select and view the status of the Operations Agent data source connection.
Collection Status	Option to select and view the status of the data collection showing the date and local time of the latest collection attempt and the current status.
Test Connection	Test an Operations Agent data source connection.
Edit Group	Edit the listed nodes to change enable/disable status, Assigned collector and Collection frequency. Click Save to save the changes.
Save	Save the changes made to an Operations Agent data source connection.

Enable or disable a Operations Agent data source data collection

1. In the Administration Console, click **Data Source Configuration > Operations Agent**.
The Operations Agent page appears.
2. In the Host collection status summary table, click the number in the column to list the Operations Agent data sources for which you want to enable or disable data collection. The Operations Agent Data Source Application Details table appears.

3. Type the host name in the **Host name** box and click **Search**, if you want to filter the list of Operations Agent data sources.
4. You can enable or disable a Operations Agent data source data collection in the following ways:
 - For one or more hosts, select the check box in the **Enable Collection** column.
 - To disable data collection, clear the **Enable Collection** check box.
 - For one or more hosts, select host(s) and click **Edit Group**, select or clear the **Enabled** check box to enable/disable collection. Click **Save**.

Tip: Use the  icon to filter the list of nodes and easily enable or disable the data collection on such nodes.

5. Click **Save**.

A Saved Successfully message appears in the Information message panel.

Note: The collection for the Operations Agent data source connections are enabled by default.

Administration Console allows filtering of Operations Agent managed nodes by set of attributes and setting enable or disable for the filtered group.

Schedule a Operations Agent data source data synchronization

By default, the data collection from the various Operations Agent data sources is scheduled for every one hour. However, you can modify this according to your requirements.

To schedule a Operations Agent data source polling frequency:

1. In the Administration Console, click **Data Source Configuration > Operations Agent (OA)**. The Operations Agent (OA) page appears.
2. In the Host collection status summary table, click the number in the column to list the Operations Agent data sources for which you want to enable or disable data collection. The Operations Agent Data Source Application Details table appears.
3. For a specific host, specify a polling time between 1 and 24 hours in the **Collection frequency** column.

For one or more hosts, select host(s) and click **Edit Group**, specify a polling time between 1 and 24 hours in the **Collection frequency** column. Click **Save**.

Note: Type the host name in the **Host name** box and click **Search**, if you want to filter the list of Operations Agent data sources.

4. Click **Save**.

A Saved Successfully message appears in the Information message panel.

Blacklisting of Nodes

Data collection from a host will not occur when the connection to the Operations Agent is lost. If the node is unreachable for three consecutive data collection runs, the node is noted in the blacklisted category. Once a node is blacklisted, the interval of the data collection run is doubled with every three retries until the data collection interval reaches 24 hours. If the connection to the node is resumed, it is no longer considered a blacklisted node and the data collection interval resumes to the original value.

You can view the blacklisted hosts from the **Java Monitoring & Management Console**. Access this console from an OBR system through `<BO install dir>\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin\jconsole.exe` and log on with the `<host name>;<port>` credentials, where the port is 21409 for OBR.

To disable the blacklisting of nodes:

1. Browse to the `{PMDB.HOME}/config/collection.properties` file.
2. Locate the property `pa.collector.blacklist.mode` parameter
3. Set the value to `FALSE`. The default value is `TRUE`.

Test the Operations Agent data source connection

1. In the Administration Console, click **Data Source Configuration > Operations Agent (OA)**. The Operations Agent (OA) page appears.
2. In the Host collection status summary table, click the number in the column to list the Operations Agent data sources for which you want to enable or disable data collection. The Operations Agent Data Source Application Details table appears.

3. Select a specific Operations Agent data source connection.

Note: Type the host name in the **Host name** box and click **Search**, if you want to filter the list of Operations Agent data sources. You cannot test more than one Operations Agent data source connection at a time.

4. Click **Test Connection**.

A `Test Connection Successful` message appears in the Information message panel if the connection exists.

Assign View/Node Group based Rules for Data Collection

You can collect data from the Operations Agent data source by grouping the views or nodes together.

1. In the Administration Console, click **Data Source Configuration > Operations Agent (OA)**.
2. Click the **Hosts Assignments** tab.
3. Select a **Collector name** based on your environment. Click **Edit**.
4. For **Assignment based on**, select **Host Group**.
5. In the **Available Groups** field, select a pattern for host names based on your choice and click



to add the rule. The selected rule moves to **Assigned Groups**.

Tip: click  to add all the rules.

6. Click **Save**.

Assign Pattern based Rules for Data Collection

You can collect data from the Operations Agent data source by grouping the nodes together.

1. In the Administration Console, click **Data Source Configuration > Operations Agent (OA)**.
2. Click the **Hosts Assignments** tab.
3. Select a **Collector name** based on your environment. Click **Edit**.

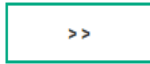
4. For **Assignment based on**, select **Host Pattern(Regular Expression)**.
5. In the **Available Groups** field, select a pattern for host names based on your choice and click



to add the rule. The selected rule moves to **Assigned Groups**.



Tip: click



to add all the rules.

6. Click **Save**.

Chapter 22: BSM/APM/OMi

You can use the BSM/APM/OMi page to create and configure the Management Database, Profile Database, and OMi as a data source.

Management Database and Profile Database connections collect performance-related data of your enterprise for various BSM applications such as Business Process Monitor (BPM), Real User Monitor (RUM), and so on. You can schedule OBR to collect data from the data repositories at specific intervals. In addition, you can view the status of the connection and data collection.

You can use the OMi page to view an OMi data source, which collect events and health indicators from managed entities in your environment. Using this page, you can schedule the OMi data collection times, enable or disable data collection, and delete the data collection connection according to your requirements.

Before you create a new OMi data source connection, make sure that a data source connection for the BSM Management Database exists. This data connection is a prerequisite for the OMi connection because OBR collects the KPI metadata for OMi from the Management Database.







If you have one or more OMi setups in your environment, you must configure the OMi data source belonging to the BSM RTSM that was configured as the topology source.

Use BSM/APM/OMi page to:

Manage the data collection for Profile/Operations database and Management database	Manage the data collection for OMi
<ul style="list-style-type: none">• Create a new Management Database and Profile Database connection• Modify a new Management Database and Profile Database connection• Enable or disable Profile Database data collection• Schedule Profile Database synchronization• Test the Management Database and Profile Database connection• View the Management Database and Profile Database connection status• View the Management Database and Profile Database collection status• Delete a Management Database connection	<ul style="list-style-type: none">• Create an OMi data source connection• Modify an OMi data source connection• Enable or disable an OMi data collection• Schedule an OMi data collection• Test the OMi data source connection• View the OMi data source connection status• View the OMi data collection status• Delete an OMi data source connection

The BSM/APM/OMi page includes three tabs (Management Database, Profile Database, and OMi) that have the following options:

Management Database

Field	Description
Host name	IP address or FQDN of the Management Database host system.
Data source	Name of the data source configured for the Management Database.
Connection Status	<p>Status of the Management Database connection.</p> <ul style="list-style-type: none">  indicates that the host system is connected to the data source.  indicates that the host system is not connected to the data source.
Collection Status	<p>Status of the collection with the date and time of the latest collection attempt and the current status:</p> <ul style="list-style-type: none">  indicates that the data collection is in progress.  indicates that the data collection completed successfully in the previous attempt.  indicates that the data collection failed in the previous attempt.  indicates that the data collection was never started.
Test Connection	Test the Management Database connection.
Create New	Create a new Management Database connection.
Edit	Modify the existing Management Database connection.
Delete	Delete the Management Database connection.
Discover Database	Discovers the Profile Database if it exists in the same Management Database host system.







Management Database: Create New: Connection Parameters

Field	Description
<ul style="list-style-type: none">• BSM• OMi	Select the data source from the options
Database in Oracle RAC	Enable this option to select the Database in Oracle RAC.
Enable TLS	Enable JDBC connection over TLS. This option is displayed when Database type selected is ORACLE .
Host name	IP address or FQDN of the Management Database server. Not displayed when Database in Oracle RAC is selected.
Port	Port number to query the Management Database server. Not displayed when Database in Oracle RAC is selected.
Database instance	System Identifier (SID) of the Management Database instance. Not displayed when Database in Oracle RAC is selected. Note: For information about the database host name, port number, and SID, contact your <i>Business Service Management</i> administrator.
Database type	The type of database engine that is used to create the Management Database. It can either be Oracle or MSSQL.
Windows Authentication	If you have selected MSSQL as the database type, you have the option to enable Windows authentication for MSSQL, that is, the user can use the same credentials to access SQL Server as that of the Windows system hosting the database.
Database name	Name of the database. This field appears only if MSSQL is selected as the database type.
User name	Name of the Management Database user, which was specified in the BSM Configuration Wizard when setting up the Management Database. Note: If the Windows Authentication option is selected, this field is disabled.
Password	Password of the Management Database user.

Field	Description
	Note: If the Windows Authentication option is selected, this field is disabled.
Collection Station	This option is used for a collector installed on a remote system.
Database in Oracle RAC selected:	
Service name	Name of the service. This option appears only if Database in Oracle RAC is selected.
ORA file name	The ORA file that contains connection information to the Oracle Real Application Cluster. This option appears only if Database in Oracle RAC is selected.
Database type	The type of database engine that is used to create the Management Database.
User name	Name of the Management Database user, which was specified in the BSM Configuration Wizard when setting up the Management Database.
Password	Password of the Management Database user.
Collection Station	This option is used for a collector installed on a remote system.
Enable TLS selected	
Truststore Path	Full path to the truststore path. This option is displayed when Enable TLS is selected.
Truststore Password	The password to access the truststore. This option is displayed when Enable TLS is selected.
Service name	Name of the service. This option appears only if Database in Oracle RAC is selected.
ORA file name	The ORA file that contains connection information to the Oracle Real Application Cluster. This option appears only if Database in Oracle RAC is selected.
Database type	The type of database engine that is used to create the Management Database.
User name	Name of the Management Database user, which was specified in the BSM Configuration Wizard when setting up the Management Database.
Password	Password of the Management Database user.
Collection Station	If you installed collectors on remote systems, you can choose either the local collector or a remote collector.

Field	Description
	<p>To configure a remote collector with this topology source, select one of the available remote systems in the drop down list.</p> <p>To use the collector that was installed by default on the OBR system, select local.</p>

Profile Database

Field	Description
Host name	IP address or FQDN of the Profile Database host system.
Enable Collection	Option to enable or disable data collection.
Schedule Frequency	Time (in hours) to synchronize the OBR database with the Profile Database.
Connection Status	<p>Status of the Profile Database connection.</p> <ul style="list-style-type: none">  indicates that the host system is connected to the data source.  indicates that the host system is not connected to the data source.
Collection Status	<p>Status of the collection with the date and time of the latest collection attempt and the current status:</p> <ul style="list-style-type: none">  indicates that the data collection is in progress.  indicates that the data collection completed successfully in the previous attempt.  indicates that the data collection failed in the previous attempt.  indicates that the data collection was never started.
Test Connection	Test the Profile Database source connection.
Create New	Create a new Profile Database connection.
Edit	Modify the existing Profile Database connection.
Delete	Delete the Profile Database connection.
Save	Save the changes made to the Profile Database connection parameters.







Profile Database: Create New: Connection Parameters

Field	Description
Database in Oracle RAC	Enable this option to select the Database in Oracle RAC.
Enable TLS	Enable JDBC connection over TLS.
Host name	IP address or FQDN of the Profile Database server. Not displayed when Database in Oracle RAC is selected.
Port	Port number to query the Profile Database server. Not displayed when Database in Oracle RAC is selected.
Database instance	System Identifier (SID) of the Profile Database instance. Not displayed when Database in Oracle RAC is selected. Note: For information about the database host name, port number, and SID, contact your <i>Business Service Management</i> administrator.
Database type	The type of database engine that is used to create the Profile Database. It can either be Oracle, MSSQL, or PostgreSQL.
Management Database	Links Profile Database to the Management Database. If you collect data from only SiteScope, no Management Database needs to be selected.
Domains	Select the domains for which you want to enable data collection. Note: You must select the domains from which you want to enable data collection. If you have skipped topology configuration during post-install configuration and installed the content packs, you must return here to select from among the following domains to enable data collection. <ul style="list-style-type: none">• Operations Manager• OMi• RUM• BPM• Service Health
Windows Authentication	If you have selected MSSQL as the database type, you have the option to enable Windows authentication for MSSQL, that is, the user can use the

Field	Description
	same credentials to access SQL Server as that of the Windows system hosting the database.
Database name	Name of the database. This field appears only if MSSQL is selected as the database type.
User name	<p>Name of the Profile Database user, which was specified in the BSM Configuration Wizard when setting up the Profile Database.</p> <p>Note: If the Windows Authentication option is selected, this field is disabled.</p>
Password	<p>Password of the Profile Database user, which was specified in the BSM Configuration Wizard when setting up the Profile Database.</p> <p>Note: If the Windows Authentication option is selected, this field is disabled.</p>
Collection Station	This option is used for a collector installed on a remote system.
Database in Oracle RAC selected:	
Service name	Name of the service. This option appears only if Database in Oracle RAC is selected.
ORA file name	The ORA file that contains connection information to the Oracle Real Application Cluster. This option appears only if Database in Oracle RAC is selected.
Database type	The type of database engine that is used to create the Profile Database.
Management Database	Links Profile Database to the Management Database. If you collect data from only SiteScope, no Management Database needs to be selected.
Domains	<p>Select the domains for which you want to enable data collection.</p> <p>Note: You must select the domains from which you want to enable data collection. If you have skipped topology configuration during post-install configuration and installed the content packs, you must return here to select from among the following domains to enable data collection.</p> <ul style="list-style-type: none"> • Operations Manager • OMi • RUM • BPM • Service Health

Field	Description
User name	Name of the Profile Database user, which was specified in the BSM Configuration Wizard when setting up the Profile Database.
Password	Password of the Profile Database user, which was specified in the BSM Configuration Wizard when setting up the Profile Database.
Collection Station	This option is used for a collector installed on a remote system.
Enable TLS selected:	
Truststore Path	Full path to the truststore path. This option is displayed when Enable TLS is selected.
Truststore Password	The password to access the truststore. This option is displayed when Enable TLS is selected.
Service name	Name of the service. This option appears only if Database in Oracle RAC is selected.
ORA file name	The ORA file that contains connection information to the Oracle Real Application Cluster. This option appears only if Database in Oracle RAC is selected.
Database type	The type of database engine that is used to create the Profile Database.
Management Database	Links Profile Database to the Management Database. If you collect data from only SiteScope, no Management Database needs to be selected.
Domains	<p>Select the domains for which you want to enable data collection.</p> <p>Note: You must select the domains from which you want to enable data collection. If you have skipped topology configuration during post-install configuration and installed the content packs, you must return here to select from among the following domains to enable data collection.</p> <ul style="list-style-type: none"> • Operations Manager • OMi • RUM • BPM • Service Health
User name	Name of the Profile Database user, which was specified in the BSM Configuration Wizard when setting up the Profile Database.
Password	Password of the Profile Database user, which was specified in the BSM Configuration Wizard when setting up the Profile Database.
Collection Station	This option is used for a collector installed on a remote system.

OMi

Field	Description
Host name	IP address or FQDN of the OMi database server.
Enable Collection	Option to enable or disable data collection.
Schedule Frequency	Time (in hours) to synchronize the OBR database with the OMi database.
Data source	Name of the data source configured for the OMi database.
Connection Status	<p>Status of OMi connection.</p> <ul style="list-style-type: none">  indicates that the host system is connected to the data source.  indicates that the host system is not connected to the data source.
Collection Status	<p>Status of the collection with the date and time of the latest collection attempt and the current status:</p> <ul style="list-style-type: none">  indicates that the data collection is in progress.  indicates that the data collection completed successfully in the previous attempt.  indicates that the data collection failed in the previous attempt.  indicates that the data collection was never started.
Test Connection	Test an OMi database connection.
Create New	<p>Create a new OMi database connection.</p> <p>Note: The Create New option is disabled after you create a new connection or if an OMi connection already exists.</p>
Edit	Modify an existing OMi database connection.
Delete	Delete an OMi database connection.
Save	Save the changes made on this page.

OMi: Create New: Connection Parameters

Field	Description
Event Operations	Select your data source.
Database in Oracle RAC	Enable this option to select the Database in Oracle RAC.
Enable TLS	Enable JDBC connection over TLS. This option is displayed when Database type selected is ORACLE .
Host name	IP address or FQDN of the Management Database server. Not displayed when Database in Oracle RAC is selected.
Port	Port number to query the Management Database server. Not displayed when Database in Oracle RAC is selected.
Database instance	System Identifier (SID) of the Management Database instance. Not displayed when Database in Oracle RAC is selected. Note: For information about the database host name, port number, and SID, contact your <i>Business Service Management</i> administrator.
Database type	The type of database engine that is used to create the Management Database. It can either be Oracle or MSSQL.
Management Database	Links Profile Database to the Management Database. If you collect data from only SiteScope, no Management Database needs to be selected.
Windows Authentication	If you have selected MSSQL as the database type, you have the option to enable Windows authentication for MSSQL, that is, the user can use the same credentials to access SQL Server as that of the Windows system hosting the database.
Database name	Name of the database. This field appears only if MSSQL is selected as the database type.
User name	Name of the OMi Database user, which was specified in the BSM Configuration Wizard when setting up the Profile Database. Note: If the Windows Authentication option is selected, this field is disabled.
Password	Password of the OMi Database user, which was specified in the BSM Configuration Wizard when setting up the Profile Database.

Field	Description
	Note: If the Windows Authentication option is selected, this field is disabled.
Collection Station	This option is used for a collector installed on a remote system.
Database in Oracle RAC selected:	
Service name	Name of the service. This option appears only if Database in Oracle RAC is selected.
ORA file name	The ORA file that contains connection information to the Oracle Real Application Cluster. This option appears only if Database in Oracle RAC is selected.
Database type	The type of database engine that is used to create the Database.
Management Database	Links Profile Database to the Management Database.
User name	Name of the OMi Database user, which was specified in the BSM Configuration Wizard.
Password	Password of the OMi Database user, which was specified in the BSM Configuration Wizard.
Collection Station	This option is used for a collector installed on a remote system.
Enable TLS selected:	
Truststore Path	Full path to the truststore path. This option is displayed when Enable TLS is selected.
Truststore Password	The password to access the truststore. This option is displayed when Enable TLS is selected.
Service name	Name of the service. This option appears only if Database in Oracle RAC is selected.
ORA file name	The ORA file that contains connection information to the Oracle Real Application Cluster. This option appears only if Database in Oracle RAC is selected.
Database type	The type of database engine that is used to create the Database.
Management Database	Links Profile Database to the Management Database.
User name	Name of the OMi Database user, which was specified in the BSM Configuration Wizard.
Password	Password of the OMi Database user, which was specified in the BSM Configuration Wizard.
Collection Station	This option is used for a collector installed on a remote system.

Create a new Management, Profile, and Operations Database connection

Create a new Management Database

1. In the Administration Console, click **Data Source Configuration > BSM/APM/OMi > Management Database**.
2. Under **Management Database**, click **Create New**.
The Connection Parameters dialog box appears.
3. In the **Connection Parameters** dialog box, specify or type the connection parameters:

Field	Description
<ul style="list-style-type: none">◦ BSM◦ OMi	Select the data source from the options
Database in Oracle RAC	Enable this option to select the Database in Oracle RAC.
Enable TLS	Enable JDBC connection over TLS. This option is displayed when Database type selected is ORACLE .
Host name	IP address or FQDN of the Management Database server. Not displayed when Database in Oracle RAC is selected.
Port	Port number to query the Management Database server. Not displayed when Database in Oracle RAC is selected.
Database instance	System Identifier (SID) of the Management Database instance. Not displayed when Database in Oracle RAC is selected. Note: For information about the database host name, port number, and SID, contact your <i>Business Service Management</i> administrator.
Database type	The type of database engine that is used to create the Management Database. It can either be Oracle or MSSQL.
Windows Authentication	If you have selected MSSQL as the database type, you have the option to enable Windows authentication for MSSQL, that is, the user can use the same credentials to access SQL Server as that of

Field	Description
	the Windows system hosting the database.
Database name	Name of the database. This field appears only if MSSQL is selected as the database type.
User name	Name of the Management Database user, which was specified in the BSM Configuration Wizard when setting up the Management Database. Note: If the Windows Authentication option is selected, this field is disabled.
Password	Password of the Management Database user. Note: If the Windows Authentication option is selected, this field is disabled.
Collection Station	This option is used for a collector installed on a remote system.
Database in Oracle RAC selected:	
Service name	Name of the service. This option appears only if Database in Oracle RAC is selected.
ORA file name	The ORA file that contains connection information to the Oracle Real Application Cluster. This option appears only if Database in Oracle RAC is selected.
Database type	The type of database engine that is used to create the Management Database.
User name	Name of the Management Database user, which was specified in the BSM Configuration Wizard when setting up the Management Database.
Password	Password of the Management Database user.
Collection Station	This option is used for a collector installed on a remote system.
Enable TLS selected	
Truststore Path	Full path to the truststore path. This option is displayed when Enable TLS is selected.
Truststore Password	The password to access the truststore. This option is displayed when Enable TLS is selected.
Service name	Name of the service. This option appears only if Database in Oracle RAC is selected.

Field	Description
ORA file name	The ORA file that contains connection information to the Oracle Real Application Cluster. This option appears only if Database in Oracle RAC is selected.
Database type	The type of database engine that is used to create the Management Database.
User name	Name of the Management Database user, which was specified in the BSM Configuration Wizard when setting up the Management Database.
Password	Password of the Management Database user.
Collection Station	This option is used for a collector installed on a remote system.

4. Click **Save**.
5. Click **Test Connection** to test the connection.
6. Click **Discover Database** to automatically discover corresponding Profile database(s).

Note: If management database and profile database are on the same system as the BSM system (local database), clicking **Discover Database** will automatically discover the corresponding Profile database. If the databases are on different systems (remote database), you have to manually configure the Profile database using the Profile Database tab.

Note: After you configure management database with **Database in Oracle RAC** option selected and the Test Connection is successful, clicking **Discovery Database** does not automatically discover the corresponding Profile database(s). You have to manually configure the profile database using the **Profile Database** tab.

7. Click **Save**.
A Saved Successfully message appears in the Information message panel.







After you save the newly created Management database connection, OBR retrieves the Profile database information from the Management database data source and lists all the available Profile database data sources under the Profile Database section.

To view details of the Profile database data source connection:

1. Click **Discover Database**.
The message to save the changes appears. Click **Save**. A Saved Successfully message

appears in the Information message panel.

2. View the Profile Database details:

Field	Description
Host name	IP address or FQDN of the Profile Database host system.
Enable Collection	Option to enable or disable data collection.
Schedule Frequency	Time (in hours) to synchronize the OBR database with the Profile Database.
Connection Status	<p>Status of the Profile Database connection.</p> <ul style="list-style-type: none"> ○  indicates that the host system is connected to the data source. ○  indicates that the host system is not connected to the data source.
Collection Status	<p>Status of the collection with the date and time of the latest collection attempt and the current status:</p> <ul style="list-style-type: none"> ○  indicates that the data collection is in progress. ○  indicates that the data collection completed successfully in the previous attempt. ○  indicates that the data collection failed in the previous attempt. ○  indicates that the data collection was never started.
Test Connection	Test the Profile Database source connection.
Create New	Create a new Profile Database connection.
Edit	Modify the existing Profile Database connection.
Delete	Delete the Profile Database connection.
Save	Save the changes made to the Profile Database connection parameters.

Set up parameters for the profile management database, only if Profile DB on Oracle RAC is selected, or when both Management DB on Oracle RAC and Profile DB on Oracle RAC are selected. In such an instance, the Create New option under Profile Database is displayed.

Data collection for the Profile database data source is enabled by default. In addition, the collection frequency is scheduled for every one hour.

Copy the `seed.properties` and `encryption.properties` files from the `%topaz_home%\Conf` folder on HPE BSM Gateway Server to the `%PMDB_HOME%\config` folder on the OBR system to discover Profile Database. In case of Oracle RAC, copy the `bsm-tnsnames.ora` file to the `%PMDB_HOME%\config` folder.

If you have configured multiple management databases (both BSM and OMi topology), create multiple folders at `%PMDB_HOME%\config` (such as `%PMDB_HOME%\config\Mgmt_DB_hostname`) and copy the `seed.properties` and `encryption.properties` files into each folder. In case of Oracle RAC, copy the `bsm-tnsnames.ora` files to the `%PMDB_HOME%\config` folder and rename them to ensure they are unique.

The file name of the `bsm-tnsnames.ora` file must be specified when entering the database connection details for BSM in an Oracle RAC.

Create a new Profile Database

1. In the Administration Console, click **Collection Configuration > BSM/APM/OMi > Profile Database**.
2. Under **Profile Database**, click **Create New**.
The Connection Parameters dialog box appears.
3. In the **Connection Parameters** dialog box, specify or type the connection parameters:

Field	Description
Database in Oracle RAC	Enable this option to select the Database in Oracle RAC.
Enable TLS	Enable JDBC connection over TLS.
Host name	IP address or FQDN of the Profile Database server. Not displayed when Database in Oracle RAC is selected.
Port	Port number to query the Profile Database server. Not displayed when Database in Oracle RAC is selected.
Database instance	System Identifier (SID) of the Profile Database instance. Not displayed when Database in Oracle RAC is selected.

Field	Description
	<p>Note: For information about the database host name, port number, and SID, contact your <i>Business Service Management</i> administrator.</p>
Database type	The type of database engine that is used to create the Profile Database. It can either be Oracle, MSSQL, or PostgreSQL.
Management Database	<p>Links Profile Database to the Management Database. If you collect data from only SiteScope, no Management Database needs to be selected.</p> <p>Select the Management Database host from the drop down to see the list of Domains.</p>
Domains	<p>Select the domains for which you want to enable data collection.</p> <p>Note: You must select the domains from which you want to enable data collection. If you have skipped topology configuration during post-install configuration and installed the content packs, you must return here to select from among the following domains to enable data collection.</p> <ul style="list-style-type: none"> ○ Operations Manager ○ OMi ○ RUM ○ BPM ○ Service Health
Windows Authentication	If you have selected MSSQL as the database type, you have the option to enable Windows authentication for MSSQL, that is, the user can use the same credentials to access SQL Server as that of the Windows system hosting the database.
Database name	Name of the database. This field appears only if MSSQL is selected as the database type.
User name	<p>Name of the Profile Database user, which was specified in the BSM Configuration Wizard when setting up the Profile Database.</p> <p>Note: If the Windows Authentication option is selected, this field is disabled.</p>
Password	Password of the Profile Database user, which was specified in the BSM Configuration Wizard when setting up the Profile Database.

Field	Description
	<p>Note: If the Windows Authentication option is selected, this field is disabled.</p>
Collection Station	This option is used for a collector installed on a remote system.
Database in Oracle RAC selected:	
Service name	Name of the service. This option appears only if Database in Oracle RAC is selected.
ORA file name	The ORA file that contains connection information to the Oracle Real Application Cluster. This option appears only if Database in Oracle RAC is selected.
Database type	The type of database engine that is used to create the Profile Database.
Management Database	<p>Links Profile Database to the Management Database. If you collect data from only SiteScope, no Management Database needs to be selected.</p> <p>Select the Management Database host from the drop down to see the list of Domains.</p>
Domains	<p>Select the domains for which you want to enable data collection.</p> <p>Note: You must select the domains from which you want to enable data collection. If you have skipped topology configuration during post-install configuration and installed the content packs, you must return here to select from among the following domains to enable data collection.</p> <ul style="list-style-type: none"> ○ Operations Manager ○ OMi ○ RUM ○ BPM ○ Service Health
User name	Name of the Profile Database user, which was specified in the BSM Configuration Wizard when setting up the Profile Database.
Password	Password of the Profile Database user, which was specified in the BSM Configuration Wizard when setting up the Profile Database.
Collection Station	This option is used for a collector installed on a remote system.

Field	Description
Enable TLS selected:	
Truststore Path	Full path to the truststore path. This option is displayed when Enable TLS is selected.
Truststore Password	The password to access the truststore. This option is displayed when Enable TLS is selected.
Service name	Name of the service. This option appears only if Database in Oracle RAC is selected.
ORA file name	The ORA file that contains connection information to the Oracle Real Application Cluster. This option appears only if Database in Oracle RAC is selected.
Database type	The type of database engine that is used to create the Profile Database.
Management Database	<p>Links Profile Database to the Management Database. If you collect data from only SiteScope, no Management Database needs to be selected.</p> <p>Select the Management Database host from the drop down to see the list of Domains.</p>
Domains	<p>Select the domains for which you want to enable data collection.</p> <p>Note: You must select the domains from which you want to enable data collection. If you have skipped topology configuration during post-install configuration and installed the content packs, you must return here to select from among the following domains to enable data collection.</p> <ul style="list-style-type: none"> ○ Operations Manager ○ OMi ○ RUM ○ BPM ○ Service Health
User name	Name of the Profile Database user, which was specified in the BSM Configuration Wizard when setting up the Profile Database.
Password	Password of the Profile Database user, which was specified in the BSM Configuration Wizard when setting up the Profile Database.
Collection Station	This option is used for a collector installed on a remote system.

5. Click **Save**.

A Saved Successfully message appears in the Information message panel.

Create a new Operations Database

1. In the Administration Console, click **Data Source Configuration > BSM/APM/OM > OMi**.
2. Under **OMi**, click **Create New**.
The Connection Parameters dialog box appears.
3. In the **Connection Parameters** dialog box, specify or type the connection parameters:

Field	Description
Event Operations	Select your data source.
Database in Oracle RAC	Enable this option to select the Database in Oracle RAC.
Enable TLS	Enable JDBC connection over TLS. This option is displayed when Database type selected is ORACLE .
Host name	IP address or FQDN of the Management Database server. Not displayed when Database in Oracle RAC is selected.
Port	Port number to query the Management Database server. Not displayed when Database in Oracle RAC is selected.
Database instance	System Identifier (SID) of the Management Database instance. Not displayed when Database in Oracle RAC is selected. Note: For information about the database host name, port number, and SID, contact your <i>Business Service Management</i> administrator.
Database type	The type of database engine that is used to create the Management Database. It can either be Oracle or MSSQL.
Management Database	Links Profile Database to the Management Database. If you collect data from only SiteScope, no Management Database needs to be selected.

Field	Description
Windows Authentication	If you have selected MSSQL as the database type, you have the option to enable Windows authentication for MSSQL, that is, the user can use the same credentials to access SQL Server as that of the Windows system hosting the database.
Database name	Name of the database. This field appears only if MSSQL is selected as the database type.
User name	Name of the OMi Database user, which was specified in the BSM Configuration Wizard when setting up the Profile Database. Note: If the Windows Authentication option is selected, this field is disabled.
Password	Password of the OMi Database user, which was specified in the BSM Configuration Wizard when setting up the Profile Database. Note: If the Windows Authentication option is selected, this field is disabled.
Collection Station	This option is used for a collector installed on a remote system.
Database in Oracle RAC selected:	
Service name	Name of the service. This option appears only if Database in Oracle RAC is selected.
ORA file name	The ORA file that contains connection information to the Oracle Real Application Cluster. This option appears only if Database in Oracle RAC is selected.
Database type	The type of database engine that is used to create the Database.
Management Database	Links Profile Database to the Management Database.
User name	Name of the OMi Database user, which was specified in the BSM Configuration Wizard.
Password	Password of the OMi Database user, which was specified in the BSM Configuration Wizard.
Collection Station	This option is used for a collector installed on a remote system.
Enable TLS selected:	
Truststore Path	Full path to the truststore path. This option is displayed when Enable TLS is selected.

Field	Description
Truststore Password	The password to access the truststore. This option is displayed when Enable TLS is selected.
Service name	Name of the service. This option appears only if Database in Oracle RAC is selected.
ORA file name	The ORA file that contains connection information to the Oracle Real Application Cluster. This option appears only if Database in Oracle RAC is selected.
Database type	The type of database engine that is used to create the Database.
Management Database	Links Profile Database to the Management Database.
User name	Name of the OMi Database user, which was specified in the BSM Configuration Wizard.
Password	Password of the OMi Database user, which was specified in the BSM Configuration Wizard.
Collection Station	This option is used for a collector installed on a remote system.

4. Click **Save**.

A `Saved Successfully` message appears in the Information message panel.

Modify a new Management, Profile, and Operations Database connection

You can only modify the Management database data source connection, not the Profile database data source connections.

To modify a Management database data source connection:

1. In the Administration Console, click **Data Source Configuration > BSM/APM/OMi > Management Database**.
2. Under **Management Database**, click **Configure**.
The Connection Parameters dialog box appears.
3. In the **Connection Parameters** dialog box, specify or type the connection parameters:

Field	Description
Data source	Select your data source: BSM or OMi.
Database in Oracle RAC	This option appears only if you have selected Oracle as the database type.
Enable TLS	Enable JDBC connection over TLS. This option is displayed when Database type selected is ORACLE .
Truststore Path	Full path to the truststore path. This option is displayed when Enable TLS is selected.
Truststore Password	The password to access the truststore. This option is displayed when Enable TLS is selected.
Host name	IP address or FQDN of the Management Database server. Not displayed when Database in Oracle RAC is selected.
Port	Port number to query the Management Database server. Not displayed when Database in Oracle RAC is selected.
Database type	The type of database engine that is used to create the Management Database. It can either be Oracle, MSSQL, or PostgreSQL.
Windows Authentication	If you have selected MSSQL as the database type, you have the option to enable Windows authentication for MSSQL, that is, the user can use the same credentials to access SQL Server as that of the Windows system hosting the database.
Database instance	System Identifier (SID) of the Management Database instance. Not displayed when Database in Oracle RAC is selected. Note: For information about the database host name, port number, and SID, contact your <i>Business Service Management</i> administrator.
Database name	Name of the database. This field appears only if MSSQL is selected as the database type.
Service name	Name of the service. This option appears only if Database in Oracle RAC is selected.
ORA file name	The ORA file that contains connection information to the Oracle Real Application Cluster. This option appears only if Database in Oracle RAC is selected.
User name	Name of the Management Database user, which was specified in

Field	Description
	the BSM Configuration Wizard when setting up the Management Database. Note: If the Windows Authentication option is selected, this field is disabled.
Password	Password of the Management Database user, which was specified in the BSM Configuration Wizard when setting up the Management Database. Note: If the Windows Authentication option is selected, this field is disabled.

4. Click **OK**.
5. Click **Save**.

A Saved Successfully message appears in the Information message panel.

Although you cannot configure the individual Profile database data source connections, you can retrieve the updated list of Profile database connections from the Management database. You can use the **Refresh** button to synchronize the databases and get the updated list of Profile database changes. Changes can include:

- New Profile database discovered from Management database.
- Existing Profile database deleted from Management database.
- Changes in configuration data for existing database.

To update the list of Profile database connections:

1. In the Administration Console, click **Data Source Configuration > BSM/APM/OMi**.
The BSM/API/OMi page appears.
2. Under **Profile Database**, click **Refresh**.
3. Click **Save**.

A Saved Successfully message appears in the Information message panel.

To update the list of Operations database connections:

1. In the Administration Console, click **Data Source Configuration > BSM/APM/OMi**.
The BSM/API/OMi page appears.
2. Under **OMi**, click **Refresh**.

3. Click **Save**.

A `Saved Successfully` message appears in the Information message panel.

Enable or disable Profile Database data collection

1. In the Administration Console, click **Data Source Configuration > BSM/APM/OMi**.
2. For one or more hosts, under **Profile Database**, perform any one of the following steps:
 - Select the **Enable Collection** check box to enable data collection.
 - Clear the **Enable Collection** check box to disable data collection.
3. Click **Save**.

A `Saved Successfully` message appears in the Information message panel.

Schedule Profile Database synchronization

1. In the Administration Console, click **Data Source Configuration > BSM/APM/OMi**.
2. Under **Profile Database**, specify a synchronization time between 1 and 24 hours in the **Schedule Frequency (Hrs.)** box.
3. Click **Save**.

A `Saved Successfully` message appears in the Information message panel.

Test the Management Database and Profile Database connection

To test the Management database data source connection:



1. In the Administration Console, click **Data Source Configuration > BSM/APM/OMi > Management Database**.
2. Click **Test Connection** for a specific Management database data source connection.
A `Test Connection Successful` message appears in the Information message panel if connection exists.

To test the Profile database data source connections:



1. In the Administration Console, click **Data Source Configuration > BSM/APM/OMi > Profile Database**.
2. Click **Test Connection** for a specific Profile database data source connection.
A `Test Connection Successful` message appears in the Information message panel if connection exists.

View the Management Database and Profile Database connection status

To view the connection status of a Management database data source:

1. In the Administration Console, click **Data Source Configuration > BSM/APM/OMi**.
2. Under **Management Database**, check the connection status indicator in the **Connection Status** column:
 -  indicates that the host system is connected to the data source.
 -  indicates that the host system is not connected to the data source.

To view the connection status of a Profile database data source:





1. In the Administration Console, click **Data Source Configuration > BSM/APM/OMi**.
2. Under **Profile Database**, for one or more Profile databases, check the connection status indicator in the **Connection Status** column:
 -  indicates that the host system is connected to the data source.
 -  indicates that the host system is not connected to the data source.

View the Management Database and Profile Database collection status

To view the collection status of a Management database data source:

1. In the Administration Console, click **Data Source Configuration > BSM/APM/OMi**.
2. Under **Management Database**, check the collection status indicator in the **Collection Status** column:





Status of the collection with the date and time of the latest collection attempt and the current status:

-  indicates that the data collection is in progress.
-  indicates that the data collection completed successfully in the previous attempt.
-  indicates that the data collection failed in the previous attempt.
-  indicates that the data collection was never started.

To view the collection status of Profile database data sources:

1. In the Administration Console, click **Data Source Configuration > BSM/APM/OMi**.
2. Under **Profile Database**, for one or more Profile databases, check the collection status indicator in the **Collection Status** column:

Status of the collection with the date and time of the latest collection attempt and the current status:

-  indicates that the data collection is in progress.
-  indicates that the data collection completed successfully in the previous attempt.
-  indicates that the data collection failed in the previous attempt.
-  indicates that the data collection was never started.

Delete a Management Database connection

1. In the Administration Console, click **Data Source Configuration > BSM/APM/OMi**.
2. Under **Management Database**, select the specific host and click **Delete**.
3. In the message box, click **Yes**.

A Deleted Successfully message appears in the Information message panel.

4. Click **Save**.

A `Saved Successfully` message appears in the Information message panel.

Although you cannot delete individual Profile database data source connections, deleting the Management database data source connection automatically removes all the Profile database data source connections. However, deleting a Management database connection does not delete the collected data from the OBR database.

Create an OMi data source connection

Before you create a new OMi data source connection, make sure that a data source connection for the BSM Management database exists on the BSM/APM/OMi page. This data connection is a prerequisite for the OMi connection because OBR collects the KPI metadata for OMi from the Management Database.

If you have one or more OMi setups in your environment, you must configure the OMi data source that belongs to the Business Service Management RTSM that was configured as the topology source.

To create a new OMi data source connection:

1. In the Administration Console, click **Data Source Configuration > BSM/APM/OMi > OMi**.
2. Click **Create New**.
The Connection Parameters dialog box appears.
3. In the **Connection Parameters** dialog box, select the **Data Source** and type the following values:

Field	Description
Data Source	Select your data source: Event or Operations.
Database in Oracle RAC	Enable this option to select the Database in Oracle RAC.
Enable TLS	Enable JDBC connection over TLS. This option is displayed when Database type selected is ORACLE .
Truststore Path	Full path to the truststore path. This option is displayed when Enable TLS is selected.
Truststore Password	The password to access the truststore. This option is displayed when Enable TLS is selected.
Host name	IP address or FQDN of the Management Database server.

Field	Description
	Not displayed when Database in Oracle RAC is selected.
Port	Port number to query the Management Database server. Not displayed when Database in Oracle RAC is selected.
Database type	The type of database engine that is used to create the Management Database. It can either be Oracle, MSSQL, or PostgreSQL.

4. Click **OK**.

5. Click **Save**.

A *Saved Successfully* message appears in the Information message panel.

You can only create a single OMi data source connection. The Create New button is disabled after you create a new OMi data source connection or if a connection already exists.

Data collection for the newly created OMi data source connection is enabled by default. In addition, the collection frequency is scheduled for every one hour.

Modify an OMi data source connection

1. In the Administration Console, click **Data Source Configuration > BSM/APM/OMi > OMi**.

2. For a specific host, click **Configure**.

The Connection Parameters dialog box appears.

3. In the **Connection Parameters** dialog box, type the following values:

Field	Description
Data Source	Select your data source: Event or Operations.
Database in Oracle RAC	Enable this option to select the Database in Oracle RAC.
Enable TLS	Enable JDBC connection over TLS. This option is displayed when Database type selected is ORACLE .
Truststore Path	Full path to the truststore path. This option is displayed when Enable TLS is selected.
Truststore Password	The password to access the truststore. This option is displayed when Enable TLS is selected.

Field	Description
Host name	IP address or FQDN of the Management Database server. Not displayed when Database in Oracle RAC is selected.
Port	Port number to query the Management Database server. Not displayed when Database in Oracle RAC is selected.
Database type	The type of database engine that is used to create the Management Database. It can either be Oracle, MSSQL, or PostgreSQL.
Management Database	Links Profile Database to the Management Database. If you collect data from only SiteScope, no Management Database needs to be selected.
Database instance	System Identifier (SID) of the Management Database instance. Not displayed when Database in Oracle RAC is selected. Note: For information about the database host name, port number, and SID, contact your <i>Business Service Management</i> administrator.
Windows Authentication	If you have selected MSSQL as the database type, you have the option to enable Windows authentication for MSSQL, that is, the user can use the same credentials to access SQL Server as that of the Windows system hosting the database.
Database name	Name of the database. This field appears only if MSSQL is selected as the database type.

4. Click **OK**.

5. Click **Save**.

A *Saved Successfully* message appears in the Information message panel.

Enable or disable an OMi data collection

1. In the Administration Console, click **Data Source Configuration > BSM/APM/OMi > OMi**.

2. Perform any one of the following steps:

- Select the check box in the **Enable Collection** column to enable data collection.
- Clear the check box in the **Enable Collection** column to disable data collection.

3. Click **Save**.

A *Saved Successfully* message appears in the Information message panel.



Schedule an OMi data collection

1. In the Administration Console, click **Data Source Configuration > BSM/APM/OMi > OMi**.
2. Specify a collection time between 1 and 24 hours in the **Hrs** box in the **Schedule Frequency** column.
3. Click **Save**.
A **Saved Successfully** message appears in the Information message panel.

Test the OMi data source connection





1. In the Administration Console, click **Data Source Configuration > BSM/APM/OMi > OMi**.
2. Click **Test Connection**.
A **Test Connection Successful** message appears in the Information message panel if connection exists.

View the OMi data source connection status

1. In the Administration Console, click **Data Source Configuration > BSM/APM/OMi > OMi**.
2. Check the connection status indicator in the **Connection Status** column:
 -  indicates that the host system is connected to the data source.
 -  indicates that the host system is not connected to the data source.

View the OMi data collection status

1. In the Administration Console, click **Data Source Configuration > BSM/APM/OMi > OMi**.
2. Check the collection status indicator in the **Collection Status** column:
Status of the collection with the date and time of the latest collection attempt and the current status:

-  indicates that the data collection is in progress.
-  indicates that the data collection completed successfully in the previous attempt.
-  indicates that the data collection failed in the previous attempt.
-  indicates that the data collection was never started.

For information to enable the CI attributes for Content pack to collect additional information relevant to your business needs, see *Enabling CI Attributes for a Content Pack* section in *Operations Bridge ReporterConfiguration Guide*.

Delete an OMi data source connection

1. In the Administration Console, click **Data Source Configuration > BSM/APM/OMi > OMi**.
2. Click **Delete**.
A Deleted Successfully message appears in the Information message panel.
3. Click **Save**.
A Saved Successfully message appears in the Information message panel.

Chapter 23: Vertica Database & Time Zone

You can use the Vertica Database & Time Zone page to manage the centralized OBR database and the time zone. You can view the details of the OBR database and change the database administrator password on this page.

Use the Vertica Database & Time Zone page to:

- [View database configuration details](#)
- [Change the OBR database password](#)
- [Enable and Disable TLS for Vertica](#)

The Vertica Database & Time Zone page includes:

Time Zone

Field	Description
Time Zone	The time zone type selected during the Initial setup.

Vertica Database

Field	Description
Database Type	Type of the database engine that is used for the OBR database.
Host name	FQDN or IP address of the host system on which the OBR database is running.
Port	Port number to query the database. The default port is 21424.
User name	Name of the OBR database user account. This account is created during the post-installation stage.
TLS	Enable or disable TLS for Vertica database.

Change Password

Field	Description
Old Password	Type the existing Vertica database password.
New Password	Enter a new password. The password should be an alphanumeric value.

Field	Description
Confirm New Password	Retype the new password for confirmation purposes.

Enable TLS

Field	Description
TrustStore File	Enter the trust store path.
TrustStore Password	Enter the trust store password.
TrustStore Confirm Password	Retype the new password for confirmation.

View Vertica database and time zone configurations

1. In the Administration Console, click **Additional Configurations > Vertica Database & Time Zone**.

The Vertica Database & Time Zone page appears.

Field	Description
Time Zone	The time zone type selected during the Initial setup.
Database Type	Type of the database engine that is used for the OBR database.
Host name	Name or IP address of the host system on which the OBR database is running.
Port	Port number to query the database.
User name	Name of the OBR database user account. This account is created during the post-installation stage.
TLS	Enable or disable TLS for Vertica database.

Change the OBR database password

1. In the Administration Console, click **Additional Configurations > Vertica Database & Time Zone**.

The Vertica Database & Time Zone page appears.

2. Click **Change Password**.

The Change Password dialog box appears.

3. In the **Change Password** dialog box, type the database password details:

Field	Description
Old Password	Enter the existing database administrator password.
New Password	Enter a new password.
Confirm New Password	Retype the new password for confirmation purposes.

4. Click **Save**.

A Password Successfully Changed message appears in the Information message panel indicating that the password has been successfully changed.

After changing the OBR database password, the **HPE_PMDB_Platform_Administrator** service must be restarted. Perform the following steps:

On Windows

1. From the Start, type **Run** in **Search**. The Run dialog box appears.
2. Type **services.msc** in the open field, and then press **ENTER**.
3. Right-click on **HPE_PMDB_Platform_Administrator** and click **Restart**.

On Linux:

Run the following command on the command line interface to restart the service:

```
service HPE_PMDB_Platform_Administrator restart
```

Enable TLS for Vertica

To enable TLS for Vertica, follow these steps:

1. In the Administration Console, click **Additional Configurations > Vertica Database & Time Zone**.
The Vertica Database & Time Zone page appears.
2. In **TLS** options, select **Enabled**. A confirmation dialog box appears.
3. Click **Yes**. The **Enable TLS** dialog box appears.

4. In the **Enable TLS** dialog box, type the database password details:

Field	Description
TrustStore File	Enter the trust store path.
TrustStore Password	Enter the trust store password.
TrustStore Confirm Password	Retype the new password for confirmation.

5. Click **OK**. The confirmation message appears.

For more steps, see *Operations Bridge Reporter Configuration Guide*.

Disable TLS for Vertica

To disable TLS for Vertica, follow these steps:

1. In the Administration Console, click **Additional Configurations > Vertica Database & Time Zone**.
The Vertica Database & Time Zone page appears.
2. In **TLS** options, select **Disabled**.
3. Click **Save**.

Chapter 24: Management Database

You can use the Management Database page to manage the OBR management database. You can view the details of the OBR management database and change the management database password on this page.

Use the Management Database page to:

- [View management database configuration details](#)
- [Change the OBR management database password](#)

The Management Database page includes:

Management Database

Field	Description
Database Type	Type of the database engine that is used for the OBR management database.
Database name	Name of the OBR management database instance.
Host name	Name or IP address of the host system on which the OBR management database is running.
Port	Port number to query the management database. The default port is 21425.
User name	Name of the OBR management database user account. This account is created during the post-installation stage.

Change Password

Field	Description
Old Password	Enter the existing database administrator password.
New Password	Enter a new password. The password should be an alphanumeric value.
Confirm New Password	Retype the new password for confirmation purposes.

View Management database configurations

1. In the Administration Console, click **Additional Configurations > Management Database**. The Management Database page appears.

Field	Description
Database Type	
Database name	
Host name	Name or IP address of the host system on which the OBR management database is running.
Port	
User name	Name of the OBR management database user account. This account is created during the post-installation stage.

Change the OBR management database password

1. In the Administration Console, click **Additional Configurations > Management Database**. The Management Database page appears.
2. Click **Change Password**.
The Change Password dialog box appears.
3. In the **Change Password** dialog box, type the database password details:

Field	Description
Old Password	Enter the existing management database administrator password.
New Password	Enter a new password. The password should be an alphanumeric value.
Confirm New Password	Retype the new password for confirmation purposes.

4. Click **OK**.
A **Password Successfully Changed** message appears in the Information message panel indicating that the password has been successfully changed.




Chapter 25: Collectors


You can use the Collectors page to create and configure a collector that is installed on a remote system (and not on the OBR system).

Use the Collectors page to perform the following tasks:

- [Configuring a Collector Installed on a Remote System](#)
- [Disabling a Collector Installed on a Remote System](#)
- [Testing a Collector Installed on a Remote System](#)

Collector Summary

Field	Description
Name	Display name of the collector. Use the  icon to sort the names in alphabetical order. Note: Cannot be changed once configured.
Host Name	Collector host name. Use the  icon to sort the names in alphabetical order.
Enable	To enable or disable the collector that is installed on the remote system. If a data source has already been assigned to any the collector for data collection, then the application will not allow you to disable the collector.
Connection	To test the connection between OBR system and the remote system where the collector is installed.
Install	It indicates whether the collector is installed.
Policy	It indicates whether all necessary collection policies are installed on the collector system. Click  icon to synchronize the policy for a newly created remote collector.
Data Source	It indicates whether any data sources are configured with the collector.

Field	Description
	Click  icon to synchronize the data sources for a newly created remote collector.
Test Connection	Test a Collector connection.
Create New	Create a new remote collector connection by entering the configurations parameters.
Edit	Modify configuration parameters of a remote collector. Important: Make sure that you edit the parameters of one collector at a time and the save the changes.
Delete	Delete a remote collector configured for data collection.
Save	Save the changes made to the collectors.



Configuration Parameters

Field	Description
Name	Display name of the collector that is installed on a remote system. The name must not contain spaces or special characters. Note: Cannot be changed once configured.
Host Name	Collector host name.

Configuring a Collector Installed on a Remote System

To configure a collector that is installed on a remote system (and not on the OBR system), do the following:

1. In the Administration Console, click **Additional Configurations >Collectors**. The Collector Configuration page appears.
2. Click **Create New**, the **Configuration Parameters** section appears.
3. In the **Name** field type a name for the collector.

4. In the **Host name** field type the host name of the collector.
5. Click **Save** to complete the configuration.
6. In the Collector Configuration page, click  icon in **Policy** to synchronize the policy for a newly created remote collector.
7. Click  icon in **Data Source** to synchronize the policy for a newly created remote collector.

Disabling a Collector Installed on a Remote System

To disable a collector that is installed on a remote system (and not on the OBR system), do the following:

1. In the Administration Console, click **Additional Configurations >Collectors**. The Collector Configuration page appears.
2. Uncheck the **Enable** field in the Collector Summary section.
3. Click **Save**.

Note: If a source is assigned to the collector, you will not be able to clear the **Enable** check box; it is required to ensure that no data source is assigned to the collector.

Testing a Collector Installed on a Remote System

To test a collector that is installed on a remote system (and not on the OBR system), do the following:

1. In the Administration Console, click **Additional Configurations >Collectors**. The Collector Configuration page appears.
2. Select the Collector that you want to test, and then click **Test Connection**.
A `Test Connection Successful` message appears in the information message panel if the connection exists.

Chapter 26: Data Processing

The Data Processing page enables you to control the workflow job stream. Information on this page is divided between the following two tabs:

Stream Details

This tab allows you to configure the job streams and specify a maximum number of retries for the streams as well as a maximum execution time per step. You can specify the number of retries and the execution time across all Content Packs, for a particular Content Pack component, for a job stream, or for a particular job step in a stream.

Stream Resource Control

This tab displays the job stream resource details and helps you to manage the resources attached to a particular step in a job stream and set limits for the number of jobs that can access the resource types.

Use the Data Processing page to:

- [Configure the maximum number of retries and the maximum execution time](#)
- [Configure the stream resource details](#)

The Stream Details tab includes:

Field	Description
Level	Select the level at which you want to configure the maximum number of retries and the maximum execution time. The options include: <ul style="list-style-type: none">• All content packs• Content pack• Stream• Step
Content Pack Component name	Name of the Content Pack Component. This drop-down list appears only when you select Content pack , Stream , or Step in the Level list.

Field	Description
Stream Name	Name of the job stream present in the selected Content Pack. This drop-down list appears only when you select Stream or Step in the Level list.
Step ID	Unique identifier for the job step. This column appears only when you select Step in the Level list.
Business Name	An alias name for the stream. This column appears only when you select Step in the Level list.
Maximum Number of Retries	Maximum number of retries for the job step in the event of its failure. The maximum value that you can set for this field is 8640.
Maximum Execution Time (Mins)	Maximum amount of time, in minutes, for a job step to complete running. The maximum value that you can set for this field is 180 minutes.
Save	Save the changes made.

The Stream Resource Control tab includes:



Field	Description
Resource Type	Type of resource that is used for data processes.
Unlimited Resources	Option to provide access to unlimited resources. Selecting this option disables the Resource Count field.
Resource Count	Maximum number of streams that can access the resource concurrently. The maximum value that you can set for this field is 20,000.
Save	Save the changes made.

Configure a maximum number of retries and the maximum execution time



You can configure the maximum number of retries and the maximum execution time across all installed Content Packs, for a particular Content Pack, for a particular job stream in the Content Pack, or for a particular job step in the job stream. Perform the following steps:

1. In the Administration Console, click **Additional Configurations > Data Processing**.
The Data Processing page appears.

2. On the **Stream Details** tab, perform any one of the following steps:
 - To configure the maximum number of retries and maximum execution time for all Content Packs, in the **Level** list, select **All Content Pack Components**.
 - To configure the maximum number of retries and maximum execution time for a particular Content Pack, in the **Level** list, select **Content Pack Component**, and then in the **Content Pack Component name** list, select the Content Pack component.
 - To configure the maximum number of retries and maximum execution time for a particular job stream, in the **Level** list, select **Stream**, in the **Content Pack Component name** list, select the Content Pack component, and then in the **Stream Name** list, select the job stream.
 - To configure the maximum number of retries and maximum execution time for a particular job step, in the **Level** list, select **Step**, in the **Content Pack Component name** list, select the Content Pack, and then in the **Stream Name** list, select the job stream.

3. In the **Maximum Number of Retries** column, and type a value. You may click the  or  icons to increase or decrease the values.

Note: The maximum value that you can set for this field is 8640.



4. In the **Maximum Execution Time (Mins)** column, and then type a value. You may click the  or  icons to increase or decrease the values.

Note: The maximum value that you can set for this field is 180 minutes.

5. Click **Save**.
A `Successfully saved the JOB details` message appears in the Information message panel.

Configure the stream resource details

1. In the Administration Console, click **Additional Configurations > Data Processing**.
The Data Processing page appears.
2. Click the **Stream Resource Control** tab to view the resource details.
3. Perform any one of the following steps:
 - For a specific resource type, if you want to provide the job streams with unlimited access resources, select the check box under the **Unlimited Resources** column.
 - To specify the number of streams that can access the resource type, under the **Resource**

Count column, type a value in the box. You may click the  or  icons to increase or decrease the values.

Note: The maximum value that you can set for this field is 20,000.

4. Click **Save**.

A Saved Successfully message appears in the Information message panel.

Chapter 27: Security

You can use the Security page to configure the security authentication protocols that are used by OBR—Lightweight Single Sign-On (LW-SSO) and SAP BusinessObjects Trusted Authentication.

Use the Security page to:

- [Configure LW-SSO authentication](#)
- [Configure SAP BusinessObjects Trusted Authentication](#)
- [Configure Logon Banner](#)

Note: This page is only visible if OBR is installed on the system.

The Security page includes:

LW-SSO tab

Field	Description
LW-SSO	Option to enable or disable LW-SSO.
Domain	Domain for which LW-SSO is valid; by default, the OBR host system's domain is enabled.
Expiration Period	Period for which the LW-SSO session is valid; The default value is 60 minutes. Note: The LW-SSO expiration period should be at least the same value as that of the application session expiration value. The recommended value is 60 minutes. For applications that do not require high levels of security, you can configure higher values, such as 300 minutes. All applications participating in an LW-SSO integration must use the same GMT time.
Init String	Shared key used for encryption and decryption of a LW-SSO session token. Note: For LW-SSO, ensure that the other applications in the Single Sign-On environment have LW-SSO enabled and are working with the same Init String.
Protected Domains	Domains for which LW-SSO is protected; by default, the OBR host system's domain is protected.

BO Trusted Authentication tab

Field	Description
Enabled	Option to enable or disable SAP BusinessObjects Trusted Authentication.
Shared Secret	Shared key used for encryption and decryption of a Trusted Authentication session token.

Logon Banner tab

Field	Description
Display banner	Check box to enable or disable the display message for the Log on banner.
Banner Message	The text to be displayed on the OBR log on.

Configure LW-SSO authentication

1. In the Administration Console, click **Additional Configurations > Security**.
The Security page appears.
2. Under **LW-SSO Configuration**, specify or type the authentication details:

Field	Description
LW-SSO	Option to enable or disable LW-SSO.
Domain	Domain for which LW-SSO is valid; by default, the OBR host system's domain is enabled.
Expiration Period	Period for which the LW-SSO session is valid; The default value is 60 minutes. Note: The LW-SSO expiration period should be at least the same value as that of the application session expiration value. The recommended value is 60 minutes. For applications that do not require high levels of security, you can configure higher values, such as 300 minutes. All applications participating in an LW-SSO integration must use the same GMT time.

Field	Description
Init String	Shared key used for encryption and decryption of a LW-SSO session token. Note: For LW-SSO, ensure that the other applications in the Single Sign-On environment have LW-SSO enabled and are working with the same Init String.
Protected Domains	Domains for which LW-SSO is protected; by default, the OBR host system's domain is protected.

3. Click **Save**.

A Saved Successfully message appears in the Information message panel.

Note: This page is only visible if OBR is installed on the system.

Configure SAP BusinessObjects Trusted Authentication

1. In the Administration Console, click **Additional Configurations > Security**.
The Security page appears.
2. Click the **BO Trusted Authentication** tab.
3. Under **BO Trusted Authentication Configuration**, specify or type the authentication details:

Field	Description
Enabled	Option to enable or disable SAP BusinessObjects Trusted Authentication.
Shared Secret	Shared key used for encryption and decryption of a Trusted Authentication session token.

4. Click **Save**.

A Saved Successfully message appears in the Information message panel. On successful save, the Shared key value gets automatically configured to CMC.

Note: This page is only visible if OBR is installed on the system.

Configure Logon Banner

1. In the Administration Console, click **Additional Configurations > Security**.
The Security page appears.
2. Click the **Logon Banner** tab.
3. Under **Logon Banner Configuration**, specify or type the following details:

Field	Description
Display banner	Check box to enable or disable the display message for the Log on banner.
Banner Message	The text to be displayed on the OBR log on.

4. Click **Save**.

After configuring the Logon Banner, if you launch SAP BusinessObjects or CMC from the Administration Console, the Logon Banner warning message is displayed.

In typical scenario, after you enable the logon banner in Administration Console and launch the SAP BusinessObjects Launch Pad or CMC from the Administration Console, the logon banner warning message is displayed. Click **OK** and respective SAP BusinessObjects or CMC log on screen is displayed. Enter the user credentials to log on and proceed with the tasks.

In custom or distributed scenario where SAP BusinessObjects is installed on a remote server, after you enable the Logon Banner in Administration Console, perform these steps:

1. In OBR system, go to the location `{PMDB_HOME}/data/`.
2. Copy the `config.prp` file manually to `{PMDB_HOME}/data/config.prp` in remote SAP BusinessObjects system.
3. Launch the SAP BusinessObjects or CMC from the web browser, the Logon Banner warning message is displayed.
4. Click **OK** and respective SAP BusinessObjects or CMC log on screen is displayed.
5. Enter the user credentials to log on and proceed with the tasks.

Launch the SAP BusinessObjects Launch Pad or CMC from the Administration Console, the logon banner warning message is displayed. Click **OK** and respective SAP BusinessObjects or CMC log on screen is displayed. Enter the user credentials to log on and proceed with the tasks.

To launch the SAP BusinessObjects Launch Pad or CMC directly from the web browser use the following URLs:

`https://<System_FQDN>:8443/BI/`

`https://<System_FQDN>:8443/CMC/`

where, `<System_FQDN>` is the fully qualified domain name of the system where SAP BusinessObjects is installed.

Note: By default HTTPs is enabled for OBR. If you have disabled HTTPs, you can also launch SAP BusinessObjects Launch Pad or CMC using the following URLs:

`http://<System_FQDN>:8080/CMC`

`http://<System_FQDN>:8080/CMC`

where, `<System_FQDN>` is the fully qualified domain name of the system where SAP BusinessObjects is installed.

Disabling the Logon Banner

1. In the Administration Console, click **Additional Configurations > Security**.
The Security page appears.
2. Click the **Logon Banner** tab.
3. Under **Logon Banner Configuration**, clear the **Display banner** check box.
4. Click **Save**.

Chapter 28: Shifts

You can use the Shift Management page to create new time shifts, modify the shift, and expire shifts that are no longer required.

Use the Shift Management page to:

- [View time shifts](#)
- [Create a new time shift](#)
- [Modify the time shift](#)
- [Expire the time shift](#)

The Shift Management page includes:

Shift Management

Field	Description
Shift Name	Name of the shift.
Effective From	The date from which shift-based data is collected by OBR.
Expires On	The date when the shift will expire. If a shift is configured to not expire, "Do Not Expire" is displayed.
Expire Shift	Expire the shift if it no longer required.
Create New	Create a new shift.
Edit	Edit a selected shift.

Create New Shift

Field	Description
Shift Name	Name of the shift that you want to create such as prime, swing, or graveyard.

Field	Description
Effective From	The date from when you want the shift to be implemented.
Expires On	The date when the shift should expire.
Cancel	Cancel the changes.
Save	Save the changes.

Edit Shift

Field	Description
New Shift Day	Click to start editing the shift.
Shift Day	The day that you want to include in your shift period.
Start Time	The starting time of the shift. The value must in 24-hour format. The range of the start time is 0 to 23 hours.
End Time	The ending time of the shift. The value must in 24-hour format. The range of the end time is 1 to 24 hours.
Delete Shift Day	Delete a row.
Shift Name	Name of the shift. This field is disabled by default.
Effective From	The date from when you want the shift to be implemented. This field is disabled by default.
Expires On	The date when the shift should expire. This field is disabled if the Do Not Expire check box is selected.
Cancel	Cancel the changes.
Save	Save the changes.

View shift information

1. In the Administration Console, click **Additional Configurations > Shifts**.
The Shift Management page appears.
2. View:

Field	Description
Shift Name	Name of the shift.
Effective From	The date from which shift-based data is collected by OBR.
Expires On	The date when the shift will expire. If a shift is configured to not expire, "Do Not Expire" is displayed.
Expire Shift	Expire the shift if it no longer required.

Create a new time shift

1. In the Administration Console, click **Additional Configurations > Shifts**.
The Shift Management page appears.
2. To create a new shift, click **Create New**.
The Create New box appears.
3. Type:

Field	Description
Shift Name	Name of the shift that you want to create such as prime, swing, or graveyard.
Effective From	The date from when you want the shift to be implemented.
Expires On	The date when the shift should expire.
Cancel	Cancel the changes.
Save	Save the changes.

4. Click **Save**.
The newly created shift appears in the Shift Management table.

Modify the time shift

A shift includes all the time ranges that you defined for that shift. To modify the shift, you need to modify the time ranges in that shift or you can add new time ranges to that shift.

To modify the shift:

1. In the Administration Console, click **Additional Configurations > Shifts**.
The Shift Management page appears.
2. In the **Shift Name** column, click the shift that you want to modify.
3. Click **Edit**. The Edit Shift box appears.
4. To edit a shift, click **New Shift Day**:
 - Change the day in the Shift Day column.
 - Change the start and end times of the shift.
 - Click the **Delete Shift Day** to remove a shift day.

Note: You cannot change the shift name or the Effective from date. These fields are disabled by default. If the shift is modified, data that is already collected by OBR will not be reprocessed.

5. Click **Save** to save the changes.

Expire a time shift

Once a time shift is created, OBR does not allow you to delete it. This is because the data collected and aggregated based on that shift period can be used for data analysis purposes. This data remains in the OBR database. However, if you no longer require the time shift, you can disable it by expiring it. Once expired, OBR does not store any data for that shift period.

To expire a shift:

1. In the Administration Console, click **Additional Configurations > Shifts**.
The Shift Management page appears.
2. In the **Shift Name** column, click the shift that you want to expire.
3. Click **Expire Shift** to expire the shift.
4. In the confirmation message box, click **Yes**.

Note: If the shift is modified, data that is already collected by OBR will not be reprocessed.

Chapter 29: Aging

You can use the Aging page to manage the retention time of the data stored in the OBR database tables. You can specify the period for which OBR retains the data in the tables, after which it is purged.

Use the Aging page to [configure active retention period](#).

The Aging page includes:

Aging

Field	Description
Content Pack Component Name	Name of the Content Pack component for which to view aging and archiving details.
Installation Date	Date and time of the Content Pack component installation.
Version	Version number of the Content Pack component.
Configure Retention	Options to configure retention policies.

Configure Retention

Field	Description
Time Type	<p>The type of data table used for storing the collected or summarized data. The types are:</p> <ul style="list-style-type: none">• 5-minute—This table contains the summary data collected every five minutes.• As-polled—This table contains the as polled or raw data.• Hourly—This table contains the raw or rate data that is aggregated at an hourly level.• Daily—This table contains the hourly data that is aggregated at the daily level.• Yearly—This table contains the monthly data that is aggregated at the yearly level.

Field	Description
	<p>Note: Monthly table and yearly table are not physical tables in the database for any out-of-the-box (OOTB) content packs.</p>
Active Retention	<p>Period for which OBR retains data. The default values are:</p> <ul style="list-style-type: none"> • Rate or 5-minute data: 90 days • Raw or as polled data: 90 days. • Daily data: 1825 days • Hourly data: 365 days • Yearly data: 1825 days

Configure active retention period

1. In the Administration Console, click **Additional Configurations > Aging**.

The Aging page appears.

2. For a specific Content Pack component, click **Configure Retention**.

The Content Pack retention configuration details appears.

You may type the Content Pack Component Name or select the Content Pack Component Name from the table.

3. For a specific type of periodic data, type the number of days for which the data is to be retained.
4. Click **Save**.

A Saved Successfully message appears in the Information message panel.

Important Considerations:

- You cannot modify the active retention policies of the Core Content Pack components.
- You cannot modify the active retention policies of the ETL and App components for all content packs (modification is allowed only on the Domain component of all content packs).

Caution: For the Service Health and OMi Content Pack components, you should not change the retention period of the "As-polled" table. The data in this table is a snapshot data and the status might not change within a short period of time. However, you can change the retention periods of the hourly and daily data.

Chapter 30: Licensing

The Licensing page displays the OBR license details. You can change the license type by accessing the HPE Password Center through the hyperlink provided on the page.

Use the Licensing page to:

- [View license information](#)
- [Obtain a Permanent license key](#)
- [Install the Permanent license key](#)
- [SAP BOBJ license reactivation](#)

The Licensing page includes:

Filed	Description
License Feature	Displays the feature which is licensed - Operations Bridge Reporter Server
Active License Type	Type of existing license; license types include: <ul style="list-style-type: none">• Instant On (IO): 60-day evaluation license (default)• Permanent (PERM): Permanent license
Days to License Expiry	Number of days remaining for the license to expire.
License Entitlement	The maximum number of nodes that are supported under the current license.
License Usage	The number of nodes being used under the current license.
Nodes Remaining	The remaining number of nodes that can be added under the current license or the number of nodes that exceed the current license usage.
Vertica Entitlement	The maximum number of nodes that are supported under the current Vertica license.
Vertica Usage	The number of nodes being used under the current Vertica license.
Launch HPE Password Center	Link to access the HPE Licensing Center web site to obtain a permanent license key.

View license information

1. In the Administration Console, click **Additional Configurations > Licensing**.
The Licensing page appears.
2. Under **OBR License Details**, view:

Field	Description
License Feature	Displays the feature which is licensed - Operations Bridge Reporter Server
Active License Type	Type of existing license; license types include: <ul style="list-style-type: none">o Instant On (IO)o Permanent (PERM)
Days to License Expiry	Number of days remaining for the license to expire.
License Entitlement	The maximum number of nodes that are supported under the current license.
License Usage	The number of nodes being used under the current license.
Nodes Remaining	The remaining number of nodes that can be added under the current license or the number of nodes that exceed the current license usage.
Vertica Entitlement	The maximum number of nodes that are supported under the current Vertica license.
Vertica Usage	The number of nodes being used under the current Vertica license.

Obtain a Permanent license key

1. In the Administration Console, click **Additional Configurations > Licensing**.
The Licensing page appears.
2. Log on to HPE Passport with your user ID and password. If you do not have an account, you must create one before you can proceed.
3. Follow the instructions provided on the website to obtain license keys.

OR

1. Go to the [HPE Software Licensing website](#).
2. Log on to HPE Passport with your user ID and password. If you do not have an account, you must create one before you can proceed.
3. Follow the instructions provided on the website to obtain license keys.

Install the Permanent license key

You must install the permanent license key by using HPE License Manager.

To install the license:

1. Log on to the OBR system with the same user name used during the installation of OBR.
2. Open the command prompt and run the following command:

```
SHRLicenseManager -install <License file path>
```

where, *<License file path>* is the path to save the license file.

3. To list the installed licenses, run the following command in the command prompt:

```
SHRLicenseManager -list
```

The following display is an example of the list of installed licenses:

```
PID:1502
```

```
(1) License Feature :HPE Operations Bridge Reporter B0 Pack
```

```
License Feature Id :1004
```

```
Active License Type :Instant On
```

```
Days to License Expiry :60
```

```
License Entitlement :50
```

```
(2) License Feature :HPE Operations Bridge Reporter Server
```

```
License Feature Id :1002
```

```
Active License Type :Instant On
```

```
Days to License Expiry :60
```

```
License Entitlement :50
```

```
(3) License Feature :HPE Operations Bridge Reporter Collector
```

```
License Feature Id :1006
```

Active License Type :Instant On

Days to License Expiry :60

License Entitlement :50

4. You must restart the administrator service to apply the installed license. To restart the HPE_PMDB_Platform_Administrator service on the HPE OBR system, follow these steps:

On Windows:

- a. Click **Start > Run**. The Run dialog box is displayed.
- b. Enter service.msc in Open. The Services windows is displayed.
- c. On the right pane, right-click on the **HPE_PMDB_Platform_Administrator** service and then click **Restart**.
- d. Close the Services window.

On Linux:

Type the following command at the command prompt:

```
service HPE_PMDB_Platform_Administrator restart
```

Reactivate SAP BOBJ license and Re-enable the SAP BOBJ Servers

The SAP BOBJ license depends on the validity of the OBR license. If the OBR license expires, it deactivates the SAP BOBJ license key and disables all the SAP BOBJ servers.

To reactivate the SAP BOBJ license

1. Obtain a new OBRlicense key, see ["Obtain a Permanent license key" on page 212](#)
2. Install a new OBR license key, see ["Install the Permanent license key" on the previous page](#)

Note: After you install the Permanent license key , wait for at least five minutes before accessing the Administration Console to reactivate the SAP BOBJ license.

3. Access the OBR Administration Console.

After you reactivate the OBR license and access the Administration Console, OBR automatically reactivates the SAP BOBJ license key. However, the SAP BOBJ servers remain in the disabled state. To ensure that SAP BOBJ works, you must manually enable the servers.

To enable the SAP BOBJ servers:

On Windows:

1. Log on to the OBR system as administrator.
2. Click **Start > Programs > BusinessObjects XI 4.x > SAP Business Intelligence > Central Configuration Manager**. The Central Configuration Manager window appears.
3. In the Display Name column, select **Server Intelligence Agent (OBR)**.
4. On the main tool bar, click the **Manage Servers** icon. The Log On dialog box appears.
5. In the System list, select the system on which SAP BusinessObjects is installed.
6. In the User name and Password field, type the user credentials of the SAP BusinessObjects server.

The default user name is *Administrator* and the default password is *<Administration Console Password>*.

7. Click **Connect**. The Manage Servers window appears.
8. Click the **Refresh** icon to refresh the server list.
9. Click **Select All** to select all the listed servers, and then click the **Enable** icon to restart the servers.
10. Click **Close** to close the window.
11. Close all open windows.

On Linux:

1. Log on to the Central Management Console by launching the following URL:

`http://<OBR_System_FQDN>:8080/CMC`

In this instance, *<OBR_System_FQDN>* is the fully qualified domain name of the OBR system.

2. Log on as **Administrator** with password *<Administration Console Password>*.
3. Click **Servers** and select the Servers list in the left menu.

Hold down the Shift or Ctrl key and click on server to select multiple servers.
4. Right-click on the selected group of servers and then click **Enable Server**.

If Business Object services do not get activated even after installing new license, see [Troubleshooting Business Object Services](#)

Chapter 31: Reporting Platform

You can use the Reporting Platform page to create and manage user accounts by using the SAP BusinessObjects CMC, which is integrated with OBR. SAP BusinessObjects InfoView allows you to personalize user experience when viewing the OBR reports by providing interactivity and customization options.

Use the Reporting Platform page to:

- [Access SAP BusinessObjects Central Management Console](#)
- [Access SAP BusinessObjects Launch pad](#)
- [Create a password for the Administrator account](#)
- [Troubleshooting BusinessObjects Services](#)

Note: This page is only visible if OBR is installed on the system.

The Reporting Platform page includes:

Field	Description
Business Objects CMC	Launch the SAP BusinessObjects CMC.
Business Objects Launch Pad	Launch the SAP BusinessObjects BI Launch pad.

Access SAP BusinessObjects Central Management Console

1. In the Administration Console, click **Additional Configurations > Reporting Platform**.
The Reporting Platform page appears.
2. Click **Launch CMC**.
The SAP BusinessObjects CMC Log On page appears.
3. Type

Field	Description
System	The name of the SAP BusinessObjects installed system that is displayed by default.
User Name	Name of the SAP BusinessObjects CMC user.
Password	Password of the SAP BusinessObjects CMC user.
Authentication	The authentication type to log on to CMC. The default type is Enterprise.

4. Click **Log On**.
The SAP BusinessObjects CMC opens.

Note: This page is only visible if OBR is installed on the system.

Access SAP BusinessObjects BI Launch pad

1. In the Administration Console, click **Additional Configurations > Reporting Platform**.
The Reporting Platform page appears.
2. Click **Launch BI launch pad**.
The SAP BusinessObjects BI launch pad Log On page appears.
3. Type

Field	Description
System	The name of the SAP BusinessObjects installed system that is displayed by default.
User Name	Name of the SAP BusinessObjects BI launch pad user.
Password	Password of the SAP BusinessObjects BI launch pad user.

4. Click **Log On**.
The SAP BusinessObjects BI launch pad portal opens.

Note: This page is only visible if OBR is installed on the system.

Create a password for the Administrator account

If you want to create a password for the default Administrator user name, perform the following steps:

1. Access the SAP BusinessObjects CMC.
2. On the Central Management Console log on screen, in the **User Name** field, type Administrator.
3. Click **Log On**. The CMC Home screen appears.
4. Click **Users and Groups**. The Users and Groups screen appears.
5. On the right pane, double-click **Administrators**.
6. Right-click **Administrator** and then click **Properties**. The Properties:Administrator dialog box appears.
7. Under **Enterprise Password Settings**, in the **Password** field, type a new password.
8. In the **Confirm** field, retype the password to confirm it. You can change the Administrator user name, if required, and specify other necessary details on this screen.
9. Click **Save & Close** to accept the changes.
10. Click **Log Out** to exit the Central Management Console.

Note: This task is valid only if OBR is installed on the system.

Troubleshooting BusinessObjects Services

1. Log in to **CMC** Application from the link http://<OBR_System_FQDN>:8443/CMC.
2. Click on **License Key** and verify if license exist. If no license exists then you have to obtain the license see [SAP BOBJ License Reactivation](#).
3. If license exist, click **Servers**, a page appears where you can check if the servers are enabled.
4. If not, select all servers and click on the **Enable** button to enable all the servers.
5. Go to the next page.
6. Enable the items in the **Server** section.

Chapter 32: Pending Configuration

You can check the status of Content Pack Component Installation, and Data Source Configuration in this page. Based on the status displayed in this page you can decide to install the remaining Content Pack or configure the data sources.

The Pending Configuration page includes:

Field	Description
Content Pack Component Installation	Displays if the Content Pack components based on the Data Source selected is installed or not. If the required Content Pack components are yet to be installed click on the subsequent link to install.
Data Source Configuration	Displays if the connection of the Content Pack components to the Data Source selected is configured or not. If the required connection is not completed click on the subsequent link to completed the connection.

Chapter 33: Platform Summary

The Platform Summary page provides a detailed status of the health and availability of the Administration Console's application server.



Use the Platform Summary page to [view the application server details](#).

The Platform Summary page includes:



Application Server Information

Field	Description
Host Name	Name of the Administration Console application server.
Port	Port number to query the Administration Console application server.
Host OS	Operating system installed on the application server.
Server Type	Type of application server.
Virtual Machine Name	Name of the application server host virtual machine.
Virtual Machine Version	Version number of the application server host virtual machine.
Virtual Machine Vendor	Provider of the host virtual machine.



Application Server Availability

Field	Description
Application Server Availability	<p>Graphical representation of the time the application server was available in the:</p> <ul style="list-style-type: none">• Last 7 days• Last 1 day <p>Legend description:</p> <p> Available indicates the percentage the server was available.</p> <p> Not Available indicates the percentage the server was not available.</p>

Memory Usage

Field	Description
Memory type	Option for the Memory type used - Heap Memory or Non-Heap Memory.
Latest Memory Usage (%)	Graphical representation of the percentage of heap memory usage. Legend description:  Good indicates that the heap memory usage is within the critical limits.  Critical indicates that the heap memory usage is outside the critical limits.
Memory Usage Over Time	Interactive graphical representation of the memory usage over time in the: <ul style="list-style-type: none"> • Last 1 Day • Last 7 Days

CPU Utilization

Field	Description
Latest CPU Utilization (%)	Graphical representation of the percentage of CPU utilization. Legend description:  Good indicates that the CPU utilization is within the critical limits.  Critical indicates that the CPU utilization usage is outside the critical limits.
CPU Utilization Over Time (%)	Interactive graphical representation of the percentage of CPU used by the application server in the: <ul style="list-style-type: none"> • Last 1 Day • Last 7 Days

View the application server details



To view information about the application server, its availability, CPU, and memory usage:

1. In the Administration Console, click **Internal Monitoring > Platform Summary**.
 The Platform Summary page appears.

2. Under **Application Server Information**, view:

Field	Description
Host Name	Name of the Administration Console application server.
Port	Port number to query the Administration Console application server.
Host OS	Operating system installed on the application server.
Server Type	Type of application server.
Virtual Machine Name	Name of the application server host virtual machine.
Virtual Machine Version	Version number of the application server host virtual machine.
Virtual Machine Vendor	Provider of the host virtual machine.



3. Under **Application Server Availability (%)**, view the availability of the application server:

Field	Description
Application Server Availability	<p>Graphical representation of the time the application server was available in the:</p> <ul style="list-style-type: none"> ○ Last 7 days ○ Last 1 day <p>Legend description:</p> <p> Available indicates the time, in hours, the server was available.</p> <p> Not Available indicates the time, in hours, the server was not available.</p>



4. Under **Memory Usage**, select **Heap Memory** in the **Memory type** list to view the heap¹ memory usage.
5. Under **Memory Usage Over Time**, view:

Field	Description
Latest Memory Usage (%)	Graphical representation of the percentage of heap memory usage.


¹Dynamic memory allocation or heap-based memory allocation is the allocation of memory storage for use in a computer program during the runtime of that program.


Field	Description
	<p>Legend description:</p> <p> Available indicates that the heap memory usage is within the critical limits.</p> <p> Not Available indicates that the heap memory usage is outside the critical limits.</p>
Memory Usage Over Time	<p>Interactive graphical representation of the memory usage over time in the:</p> <ul style="list-style-type: none"> ○ Last 1 Day ○ Last 7 Days

6. Under **Memory Usage**, select **Non-Heap Memory** in the **Memory type** list to view the non-heap memory usage.
7. Under **Memory Usage Over Time**, view:

Field	Description
Latest Memory Usage (%)	<p>Graphical representation of the percentage of heap memory usage.</p> <p>Legend description:</p> <p> Available indicates that the heap memory usage is within the critical limits.</p> <p> Not Available indicates that the heap memory usage is outside the critical limits.</p>
Memory Usage Over Time	<p>Interactive graphical representation of the memory usage over time in the:</p> <ul style="list-style-type: none"> ○ Last 1 Day ○ Last 7 Days

8. Under **CPU Utilization**, view the current CPU utilization of the application server:

Field	Description
Latest CPU Utilization (%)	<p>Graphical representation of the percentage of CPU utilization.</p> <p>Legend description:</p> <p> Good indicates that the CPU utilization is within the critical limits.</p>

Field	Description
	 Critical indicates that the CPU utilization usage is outside the critical limits.
CPU Utilization Over Time (%)	Interactive graphical representation of the percentage of CPU used by the application server in the: <ul style="list-style-type: none">○ Last 1 Day○ Last 7 Days

Chapter 34: Data Collection Status

You can use the Data Collection Status page to view a summary for the time of the last data collected by Operations Agent data source. This page displays the time stamp of when the last data was pulled from the Operations Agent Content Pack Component. You can also view information about the data source, the class, and the last data time performed by the Operations Agent Content Pack Component

Use the Data Collection Status page to [View the data collection status](#).

Operations Agent Audit

Type the values for the following fields to set the filter:

Field	Description
Domain name	The content pack component name or the domain name as in the Operations Agent page.
Host name	Name of the Operations Agent data source.
Delay(#days)	Type the number of the delay in days.

Operations Agent Audit Summary

Field	Description
Domain name	Name of the installed Content component for the domain.
Host name	Name of the Operations Agent data source.
Last Data Time	Time since the last data polling has occurred.

View Data Sources

Field	Description
Domain name	Domain name of the data source for the selected host.
Host name	Host name of the data source for the selected host.
Data Source	Name of the data source for the selected host.
Class	Name of the class for the selected host.
Last Data Time	Time since the last data polling has occurred.

View the data collection status

1. In the Administration Console, click **Internal Monitoring > Data Collection Status**.
The Data Collection Status page appears.
2. Type the values for the following fields to set the filter and press **Enter**:

Field	Description
Domain name	The content pack component name or the domain name as in the Operations Agent page.
Host name	Name of the Operations Agent data source.
Delay(#days)	Type the number of the delay in days

3. View **Operations Agent Audit Summary**

Field	Description
Domain name	Name of the installed Content component for the domain.
Host name	Name of the Operations Agent data source.
Last Data Time	Time since the last data polling has occurred.

4. To view the summary for a particular host click the desired Host name in **Operations Agent Audit Summary** table or click **View Data Sources**.

Field	Description
Domain name	Domain name of the data source for the selected host.
Host name	Host name of the data source for the selected host.
Data Source	Name of the data source for the selected host.
Class	Name of the class for the selected host.
Last Data Time	Time since the last data polling has occurred.

Chapter 35: Data Process Status

You can use the Data Process Status page to monitor the workflow processes that move data to the data store. You can monitor the status of the job streams of each installed Content Pack component. You can also use this page to view historical execution trends and variations of workload or focus on operational data about the job streams.

Use the Data Processing page to:

- [View the number of active data streams](#)
- [View the historical stream details](#)
- [View the historical trend of the streams](#)





The Data Process Status page includes:


Latest Stream Overview tab

The Latest Stream Overview tab includes:

Field	Description
Content Pack Component name	Name of the Content Pack component.
Number of Streams	Total number of job streams. This value indicates the number of streams that are currently running, or the number of streams that are loaded for execution, or the number of streams that completed in the last run.
OK	The number of job streams that completed successfully.
Warning	The number of job streams that completed with warnings. These warnings do not hinder the execution of the remaining job steps in the stream.
Error	The number of job streams that failed to complete. This stops the entire job stream from running until the error is resolved.
Total	The total number of streams that are running.

Streams Content Pack Component: <Content Pack Component Name>

Field	Description
Stream Name	Name of the job stream.
Completed/Total	Status of the job stem in the stream. Completed indicates the number of steps in the job stream that have completed irrespective of whether it was successful or generated a warning or error. Total indicates the total number of job steps in the stream.
Step Status	Status of the job step execution:  indicates that the job stream has not started running but has been loaded for execution.  indicates that all job steps in the stream completed successfully.  indicates that some job steps completed with warnings.  indicates that a job step in the stream failed to complete and generated an error.
Start Time	Local time when the execution of the job step started.

To view a diagrammatic representation of the job stream, click  icon for specific Stream Name. The **Stream Details** diagram opens which displays the execution flow and status of the job steps.

Historical Stream Overview tab

The Historical Stream Overview tab includes:

Field	Description
Content Pack Component name	Name of the Content Pack component.
Number of Streams	Total number of job streams that ran during the specified period of time.
OK	The number of job streams that completed successfully
Warning	The number of job streams that completed with warnings. These warnings do not hinder the execution of the remaining job steps in the stream.
Error	The number of job streams that failed to complete. This stops the entire job stream from running until the error is

Field	Description
	resolved.
Total	The total number of streams that are running.

Streams Content Pack Component: <Content Pack Component Name>

Field	Description
Content Pack Component name	Name of the Content Pack component.
OK	The number of job streams that completed successfully
Warning	The number of job streams that completed with warnings. These warnings do not hinder the execution of the remaining job steps in the stream.
Error	The number of job streams that failed to complete. This stops the entire job stream from running until the error is resolved.
Total	The total number of streams that are running.

View the job stream details

To view the number of job streams for a Content Pack component:





1. In the Administration Console, click **Internal Monitoring > Data Process Status**.
 The Data Process Status page appears.
2. On the **Latest Stream Overview** tab, view:


Field	Description
Content Pack Component name	Name of the Content Pack component.
Number of Streams	Total number of job streams. This value indicates the number of streams that are currently running, or the number of streams that are loaded for execution, or the number of streams that completed in the last run.
OK	The number of job streams that completed successfully.
Warning	The number of job streams that completed with warnings. These

Field	Description
	warnings do not hinder the execution of the remaining job steps in the stream.
Error	The number of job streams that failed to complete. This stops the entire job stream from running until the error is resolved.
Total	The total number of streams that are running.

To view the details of the streams:

1. Click a specific Content Pack Component name in the **Latest Stream Overview** table. The **Streams Content Pack Component: <Content Pack Component Name>** table appears.
2. In the **Streams Content Pack Component: <Content Pack Component Name>** view:

Field	Description
Stream Name	Name of the job stream.
Completed/Total	Status of the job stem in the stream. Completed indicates the number of steps in the job stream that have completed irrespective of whether it was successful or generated a warning or error. Total indicates the total number of job steps in the stream.
Step Status	Status of the job step execution:  indicates that the job stream has not started running but has been loaded for execution.  indicates that all job steps in the stream completed successfully.  indicates that some job steps completed with warnings.  indicates that a job step in the stream failed to complete and generated an error.
Start Time	Local time when the execution of the job step started.

3. To view a diagrammatic representation of the job stream, click  icon for specific Stream Name. The **Stream Details** diagram opens which displays the execution flow and status of the job steps.

To understand the information displayed in the job stream diagram and relate it to the information in the tables, see [Understanding the job stream status](#). To troubleshoot the stream alerts, see the *Operations Bridge Reporter Troubleshooting Guide*.

View the historical stream overview

To view the number of historical job streams for a Content Pack component:

1. In the Administration Console, click **Internal Monitoring > Data Process Status**.
The Data Process Status page appears.
2. Click **Historical Stream Overview**, select one of the following **Stream Details** options:
 - Last 1 day
 - Last 7 days

Note: The workflow framework stores information about job steps in run-time tables for a maximum period of 7 days, after which the data is automatically purged by the PMDB_Platform_IM_Service.

3. In the table, view:

Field	Description
Content Pack Component name	Name of the Content Pack component.
Number of Streams	Total number of job streams that ran during the specified period of time.
OK	The number of job streams that completed successfully
Warning	The number of job streams that completed with warnings. These warnings do not hinder the execution of the remaining job steps in the stream.
Error	The number of job streams that failed to complete. This stops the entire job stream from running until the error is resolved.
Total	The total number of streams that are running.

To view the details of the job stream:

1. Click a specific Content Pack Component name in the **Historical Stream Overview** table. The **Streams Content Pack Component: <Content Pack Component Name>** table appears.

Field	Description
Content Pack Component name	Name of the Content Pack component.
OK	The number of job streams that completed successfully
Warning	The number of job streams that completed with warnings. These warnings do not hinder the execution of the remaining job steps in the stream.
Error	The number of job streams that failed to complete. This stops the entire job stream from running until the error is resolved.
Total	The total number of streams that are running.

View the historical trend of the streams


1. In the Administration Console, click **Internal Monitoring > Data Process Status**.
The Data Processing page appears.
2. On the **Historical Stream Details** tab, under **Select Filter**, select a Content Pack component in the **CP** list.
3. In the **Stream** list, select a stream.
4. In the **Severity** list, select the appropriate severity option that you want to generate the graph for.
The option include:
 - WARNING—displays the number of warning states encountered by the job stream during its execution.
 - ERROR—displays the number of error states encountered by the job stream during its execution.
5. In the **State** list, select the required state of the job stream. The options include:
 - ALL—all states of the job stream.
 - FINISHED—state where the job stream completed successfully irrespective of the warning or error encountered during its execution.
 - ABORTED—state where the execution of the job stream was aborted by the user.

6. Click **Find**.

The graph for the selected stream is displayed. This graph displays the number of times a job stream generated a warning or error over a specific period of time.

Chapter 36: Content Health Status

The Content page allows you to monitor the status of the data in OBR fact tables for each installed content pack. You can verify the health of data flow from data source into the fact tables associated with the dimensions of each content pack.




When a caution status () is indicated in the row labeled "Health", you can drill down to the reports, fact tables, and dimensions or CIs that are impacted by gaps in data.

If the CIs have not logged data, verify if they have been decommissioned. If yes, you can delete those dimensions and their fact tables from OBR.

Use the Content Health Status page to:


- [View the installed Content Pack component](#)
- [View the fact table details](#)

The Content Health Status page includes:

Field	Description
Content Pack Component Name	Name of the content pack.
Total	Indicates the total number of fact tables impacted by data gaps in the corresponding content pack.
Facts Affected	Indicates the number of fact tables impacted by data gaps in the corresponding content pack.
Health	<p>Indicates the health of data for the content pack based on the fact tables in the Vertica database.</p> <p>Legend description:</p> <ul style="list-style-type: none"> indicates that the data tables have no issues. indicates that the data tables need attention. <p>If a fact table encounters any of the following conditions, its health is marked :</p> <ul style="list-style-type: none">• Data is not available for >10% of the dimensions.• Data is not available in hourly tables for the last 6 hours.


Field	Description
	<ul style="list-style-type: none"> Data is not available in daily table for the last 1 day. The table holds data for more than the configured period. <p>You can configure these threshold values from <code>{PMDB_HOME}/adminServer/webapps/AdminService/threshold.prp</code> file.</p> <p>To exclude tables due to non-availability of data at the source, modify the <code>{PMDB_HOME}adminServer/webapps/AdminService/tableExclusion.prp</code> file.</p>
Reports Impacted	Indicates the number of reports impacted by data gaps in the corresponding content pack.
View Affected Reports	Displays a list of Affected Reports.

Fact Tables Content Pack Component name: <Content Pack Component name>

Field	Description
Fact	Displays a list of affected hourly and daily fact tables.
Status	<p>Displays the status of fact collection.</p> <p>By default, the caution status () is indicated if:</p> <ul style="list-style-type: none"> Hourly tables have not been updated for 12 hours. Daily tables have not been updated for 24 hours.
Row Count	Total number of rows currently in the fact table.
Last Updated	<p>The time stamp when data was last loaded to the fact table.</p> <p>You can configure the default period by changing the values in the <code>latency.prp</code> file located at <code>{PMDB_HOME}adminServer/webapps/AdminService</code>.</p>
Fact	Ratio of the number of dimensions that have fact data against the total number of dimensions in tables.
Dimension	The number of dimensions that have fact data against the total number of dimensions in tables.
Primary Dimension	The primary dimension associated with the fact table.




Field	Description
Reports Impacted	<p>Indicates the number of reports impacted by data gaps in the corresponding content pack.</p> <p>You can click to view the names of the reports impacted from the Affected Reports and launch them.</p>

For more information on troubleshooting data gaps in OBR reports, see section, "*Troubleshooting Reporting Issues*" in the *Operations Bridge Reporter Troubleshooting Guide*.

To view Missing Dimensions(CI's) of a specific Fact, click  icon for specific Fact. The **Missing Dimensions(CI's)** table opens.

View the installed Content Pack component


1. In the Administration Console, click **Internal Monitoring > Content Health Status**.
 The Content Health Status page appears.
2. View:


Field	Description
Content Pack Component Name	Name of the content pack.
Total	Indicates the total number of fact tables impacted by data gaps in the corresponding content pack.
Facts Affected	Indicates the number of fact tables impacted by data gaps in the corresponding content pack.
Health	<p>Indicates the health of data for the content pack based on the fact tables in the Vertica database.</p> <p>Legend description:</p> <p> indicates that the data tables have no issues.</p> <p> indicates that the data tables need attention.</p> <p>If a fact table encounters any of the following conditions, its health is marked :</p> <ul style="list-style-type: none"> o Data is not available for >10% of the dimensions.


Field	Description
	<ul style="list-style-type: none"> Data is not available in hourly tables for the last 6 hours. Data is not available in daily table for the last 1 day. The table holds data for more than the configured period. <p>You can configure these threshold values from <code>{PMDB_HOME}/adminServer/webapps/AdminService/threshold.prp</code> file.</p> <p>To exclude tables due to non-availability of data at the source, modify the <code>{PMDB_HOME}/adminServer/webapps/AdminService/tableExclusion.prp</code> file.</p>
Reports Impacted	Indicates the number of reports impacted by data gaps in the corresponding content pack.
View Affected Reports	Displays a list of Affected Reports.

View the fact table details

- In the Administration Console, click **Internal Monitoring > Content Health Status**.
The Content Health Status page appears.
- For a specific Content Pack component, click the **Content Pack Component Name**.
The Fact Tables tab opens.
- On the **Fact Tables** tab, view:

Field	Description
Fact	Displays a list of affected hourly and daily fact tables.
Status	<p>Displays the status of fact collection.</p> <p>By default, the caution status () is indicated if:</p> <ul style="list-style-type: none"> Hourly tables have not been updated for 12 hours. Daily tables have not been updated for 24 hours.
Row Count	Total number of rows currently in the fact table.
Last Updated	<p>The time stamp when data was last loaded to the fact table.</p> <p>You can configure the default period by changing the values in the <code>latency.prp</code> file located at <code>{PMDB_HOME}/adminServer/webapps/AdminService</code>.</p>

Field	Description
Fact	<p>Ratio of the number of dimensions that have fact data against the total number of dimensions in tables.</p> <p>You can click and launch a new pane to view the dimensions or CIs that have not logged data.</p> <p>This ratio is assigned a default threshold value of 90%. So, when more than 10% dimensions do not have fact data, the caution status () is displayed. You can configure the threshold values in the <code>threshold.prp</code> file located at <code>{PMDB_HOME}/adminServer/webapps/AdminService</code>.</p>
Dimension	The number of dimensions that have fact data against the total number of dimensions in tables.
Primary Dimension	The primary dimension associated with the fact table.
Reports Impacted	<p>Indicates the number of reports impacted by data gaps in the corresponding content pack.</p> <p>You can click to view the names of the reports impacted from the Affected Reports and launch them.</p>

To view Missing Dimensions(CI's) of a specific Fact, click  icon for specific Fact. The **Missing Dimensions(CI's)** table opens.

Note: The fact table information displayed on this page is stored in the database for seven days, after which it is purged.

Chapter 37: Online Help

Use this page to view the *Online Help for Administrators*.

About OBR

This page displays the details about the PMDB Platform.

The About page includes:

Field	Description
Version	The version number of the product.
Patch Level	The patch level for the version number of the product.
Build Number	The build number of the product.

Part IV: Appendix

Parameters in the Config.prp file

The following table lists the config.prp parameters.

Parameters	Parameter Details
#Fully qualified hostname of the system that is running the SAP BO component for OBR	bo.cms = bohost
#Port number where the SAP BO is listening for connections	bo.cms.port = 6400
#Port number where the SAP BO InfoViewApp web application is running	bo.infoview.port = 8080
#Authentication type for logging in to BO and subsequently OBR Administration console as well Note: Supported options – Enterprise and Group based	bo.authType = secEnterprise
#Parameters that enable trusted authentication in SAP BO Note: These get updated when setting up CAC	bo.trusted.auth.enable = false bo.trusted.auth.shared.secret =
#SAP BO install location	bo.install.path=C:/Program Files (x86)/Business Objects/
#Host and port details where Java messaging service is to be run Note: Deprecated in OBR 9.40	jms.host=localhost jms.port=21401
#Port where JMX beans from OBR are accessible via HTTP	jmx.port=21422
# Abc_ DataServicesWSMaxTimeToLaunch=60	BSMR_ABC_Version=0.16.5
#Port details where Tomcat Mbeans are exposed	tomcat.jmx.port=21416

Parameters	Parameter Details
#Default logger class for OBR modules	logger.classname=com.hp.bto.bsmr.util.logger.BsmrLoggerFactory
#default Image source for OBR Administration console	DefaultImageSource=svcgen.32.gif
#Image size	GeneratedImageWidth=1035 GeneratedImageHeight=400
#Is BSM installed - Deprecated	bsm.install=false
# Indicate OBR installation. Value=Enterprise – OBRInstallation ,Value=headless OBRInstallation	SHR.install=Enterprise
#OS architecture for OBR	pmdb.os.platform=64
#Name of DWH DB JDBC driver	database.driver.name=SQL Anywhere 12 SQL Anywhere 12 is the SAP BusinessObjects database.
#connection details for ABC - deprecated	abc.db.host=localhost abc.db.instance=dwabc abc.db.port=3699 abc.db.pmdb.user=dwabc abc.db.pmdb.user.pwd=dwabc
#DWH DB connection details (Vertica)	database.type=vertica database.port=5433 database.sybase.engine=databaseEngine database.host=databaseHost database.dsn=BSMR
#start/stop script by bsm, relative to PMDB home	bsm.start.script=bin/hp_bsm_pmdb_start bsm.stop.script=bin/hp_bsm_pmdb_stop
#Management DB connection details (PostgreSQL)	management.db.type=postgres management.db.driver=org.postgresql.Driver management.db.hostname = localhost management.db.port=21425 management.db.dialect=org.hibernate.dialect.PostgreSQLDialect
#property to specify distributed collection – deprecated	collection.distributed.mode = false

Parameters	Parameter Details
#Log level for loader.log	loader.debug.level=INFO
#Log level for aggregate.log	aggregate.debug.level=INFO aggregate.daily.interval=6
#Log level for runProc command	runProc.debug.level=INFO
#Name of the 64 bit DSN created to connect to Vertica database from SHR	database.dsn64=SHRDB
# ADDED FOR SIS GROUP NAME	SISGroupName=SIS
# ADDED FOR COLLECTION MAX HISTORY AND INITIAL HISTORY SUPPORT	collector.maxHistory=360 collector.initHistory=360
# ADDED FOR DBCOLLECTOR MAX HISTORY AND INITIAL HISTORY SUPPORT	dbcollector.maxHistory=360 dbcollector.initHistory=360
#Host and port details where Collection MBeans are enabled	collection.host = localhost collection.jmx.port = 21409
#default frequency in minutes with which a newly discovered HPE Operations Agent source will be configured for collection	pa.frequency=60
#Number of hours of data a file is kept since its arrival in {PMDB.HOME} /stage/archive folder Note: Any file older than this period will be deleted	stage.archive.retention.period=48
#character encoding system for OBR	charset=UTF8
#IM Threshold for Diskspace Note: Deprecated for SHR 9.40	im.disk.space.errorLimit=5 im.disk.space.warnLimit=15
#view name that is used for querying during test connection to RTSM configured	default.cmdb.view = Oracle
#ADDED FOR DEFAULT AGGREATE.BATCHSIZE	aggregate.batchsize=20000000

Parameters	Parameter Details
#default stage batch size	stage.batchsize=10000000
#default loader batch size	loader.batchsize=10000000
# min and max value used by Internal monitoring to generate database alert.	dbspace.min.percentage=70 dbspace.max.percentage=85 stage.backup.failedRows=false
#Added for enabling SSL	bo.protocol=http bo.ssl.enabled.port=8443 shr.admin.ui.port=21412
#Added for downtimeutility	downtimedays=7
#Added for chain of authentication, you have to update this property by appending comma separated value	shr.auth.classes=com.hp.bto.bsmr.security.auth.BOAuthenticator
#property to indicate whether any remote collectors are configured or not Note: Will change to true automatically on configuring the first remote collector	remote.poller.is.enabled=false
#Added for CAC authentication, needs to have a value certbased for CAC authentication and default otherwise	shr.loginMethod=default
#URL for the web service that is to be queried in case of RTSM collection	ucmdbservice.url=/axis2/services/UcmdbService
#Maximum number of retries attempted to acquire a connection to OBR management DB (PostgreSQL) before exiting with error	management.db.connection.retry=3
#Number of milliseconds to check that connection to OBR management DB held in the pool is not stale and in case it is, refresh the same	management.db.connection.check.interval=30000
#User group on BO used OBR	shr.user.groups=administrators

Parameters	Parameter Details
authentication	
#Minimum CPU and Memory requirements for various deployment configurations (low, medium and high)	low_volume_cpu_number=4 low_volume_ram_size=8 medium_volume_cpu_number=8 medium_volume_ram_size=16 high_volume_cpu_number=32 high_volume_ram_size=64
#Parameter to indicate whether this is a remote BO setup or not Note: Updated by OBR installer based on the features selected for installation on the system	isRemoteBO=false

The `aggregate.daily.interval` runs every 6 hours by default. To reduce the delay between daily aggregation runs, user may add the parameter `aggregate.daily.delay` with the value in hours in `config.prp` file.

Additional Administration Details

This section guides you to perform the following:

- [Configuring custom groups](#)
- [Managing dimensions](#)
- [Configuring downtime in reports](#)
- [Configuring customer in reports](#)
- [Configuring location in reports](#)

Configuring custom groups

Custom groups in OBR help to retrieve information pertaining to the set of nodes that comprise a specific dimension. Custom groups in OBR can be created for conformed dimensions only. For instance, if you wish to view the nodes that are linked to a specific network, you can create a custom group that displays information pertaining only to the nodes that are a part of the specific network. Custom groups are created as an XML and imported to OBR through the platform stream.

To create a Custom Group:

1. Create an XML for the Custom Group. For syntax on creating the Custom Group XML, see [Creating Custom Groups](#).
2. After creating the XML, save it in the following folder:

Windows: %PMDB_HOME%\config

Linux: \$PMDB_HOME/config

After you create the Custom Group:

- The Custom Group is processed by the PMDB Platform stream **PMDB_Platform@CustomGroup**.
- To confirm whether the Custom Group is imported to OBR, check whether the PMDB_Platform@CustomGroup stream is loaded successfully.
- You must wait for the OBR dimension stream to populate the OBR data tables with the Custom Group information.

Note: The stream **PMDB_Platform@CustomGroup** runs 3 times per day and gets populated with the custom group information at an interval of 8 hours.

OBR enables you to:

- Create multiple custom groups for an operating system in a single XML file, by changing the values of the syntax.
- Select the desired custom group from the **Prompts** section of the reports.

Creating custom group

To create a Custom Group, copy the following syntax in an XML file:

Note: You can enter a file name of your choice for the XML file, but follow the **<name>customgroup.xml** restriction; where, *<name>* is any file string supported by the operating system.

For example, shr_customgroup.xml or SHR9XXcustomgroup.xml and so on.

```
<groups>
<group name=" " type=" ">
<instances type=" ">
<instance>
<attribute name=" " value=" " operator=" " relation=" " />
</instance>
</instances>
</group>
</groups>
```

Note: Copy the attribute tag for each entity type that you want to define for the Custom Group.

The following table provides a description of the tags used in the above example:

Field	Description
group name	New Custom Group name.
type	The Group type.
instances type	Dimension table conformed to the K_CI table. The dimensions are extracted from this table.
attribute name	Name of the string column (not numeric column) in the dimension table defined in the <i><instance type></i> tag.
value	The column value in the dimension table must match this value.
operator	Operator for searching the node name value.

Field	Description
	<p>To perform an exact match of values, use the EQUALS operator. For example, "abcvalue1"</p> <p>To perform a pattern based match of values, use the LIKE operator. You can specify the value as "abcvalue1%" or "%abcvalue1%" and so on.</p> <p>For other operators such as IN, NOT IN, NOT LIKE, EXISTS, "=", or "!=" , you must specify the values enclosed within double quotes. For example, the IN operator must have the values as "'abcvalue1', 'abcvalue2', 'abcvalue3' ".</p> <p>Note: All the value comparisons in the XML against the OBR database is case insensitive.</p>
relation	<p>Determines the relation between the attribute name and value. The relation value can either be AND or OR.</p> <p>Note: If you do not define a relation value, OBR considers the default value as AND.</p>

For examples of Custom Group syntax, see:

Custom Groups in Windows® and Linux operating systems

```
<groups>
<group name="Windows" type="CUSTOMGROUP">
<instances type="K_CI_System">
<instance>
<attribute name="OS" value="NT" operator="LIKE" relation="OR" />
<attribute name="OS" value="Windows" operator="LIKE" relation="OR" />
<attribute name="OS" value="windows" operator="LIKE" relation="OR" />
<attribute name="OS" value="Win" operator="LIKE" relation="OR" />
<attribute name="OS" value="win" />
</instance>
</instances>
</group>
</groups>
```

Custom Groups in UNIX Operating System

```
<groups>  
  
<group name="Unix" type="CUSTOMGROUP">  
  
<instances type="K_CI_System">  
  
<instance>  
  
<attribute name="OS" value="%ux%" operator="LIKE" relation="OR" />  
<attribute name="OS" value="%UX%" operator="LIKE" relation="OR" />  
<attribute name="OS" value="AIX" operator="LIKE" relation="OR" />  
<attribute name="OS" value="Sun%" operator="LIKE" />  
  
</instance>  
  
</instances>  
  
</group>  
  
</groups>
```

Managing dimensions

When a data source is configured in OBR, it collects dimension and fact data from the nodes (host, network device, application, and so on) for generating reports. Dimension data is collected from the topology source. But, when you remove a node or CI from your environment, it is not removed from the OBR database. This is meant to enable you to generate historical reports on deleted dimensions.

Inactive dimension: When a node is deleted from your environment and you continue to have an inactive dimension in the OBR database.

Duplicate dimension: When a new node is added to the environment with the name of an older node, you have a duplicate dimension in the OBR database.

When you have retired nodes or CIs permanently from your environment and no longer generate reports on them, you can delete the inactive dimensions. You can do it for both local and conformed dimensions from the OBR system using the Command Line Interface (CLI).

If you have added new nodes and they have taken up the names of older nodes, you can rename the duplicate dimensions. You can do it for only conformed dimensions from the OBR system using the Command Line Interface (CLI).

Note: When you delete a dimension, the dimension and its fact data is deleted permanently. Take a backup of the OBR database before you perform this operation.

For more information, refer *Database Back up and Recovery* section in *Operations Bridge Reporter Configuration Guide*.

For more information on fact, dimension, and types of dimensions, see the section, "*Architecture*" in the *Operations Bridge Reporter Concepts Guide*.

Note: Dimension Manager lists nodes based on the CI UID and not according to the DNS names. If there are changes in the long name or short names of the nodes it will not be listed by the Dimension Manager.

To view the CLI Help that lists the commands you can use, run the following command:

```
dimensionmanager --help
```

Before running the commands in this section, stop the `HPE_PMDB_Platform_Orchestration` service.

Managing inactive dimensions

You can identify the dimensions that have remained inactive for a certain period in the OBR database and delete them.

List inactive dimensions

To generate a list of inactive dimensions, run the following command:

```
dimensionmanager -inactive_dim_list -caption <caption name> -inactive <number of days inactive> -output_dir <directory location>
```

For details on the command parameters, see ["Inactive Dimension Parameters" below](#)

Delete inactive dimensions

To delete inactive dimensions, run the following command:

```
dimensionmanager -inactive_dim_delete -caption <caption name> -file <input file> -mode <test/commit>
```

For details on the command parameters, see ["Inactive Dimension Parameters" below](#)

Caution: When you execute this command in the commit mode, the dimension and its fact data will be deleted permanently. Take a backup of the OBR database before you perform this operation.

For more information, refer *Database Back up and Recovery* section in *Operations Bridge Reporter Configuration Guide*.

The following table provides a description of the parameters used in the preceding commands:

Inactive Dimension Parameters

Parameter	Description
inactive_dim_list	Operation for listing the inactive dimensions.
inactive_dim_delete	Operation for deleting inactive dimensions.
caption	Caption name or table name for a dimension. Obtain it from the model interface document available with each content pack in their respective

Inactive Dimension Parameters, continued

Parameter	Description
	<i>/doc</i> folder. Example: "K_CI_System" or "System".
file	Absolute path of the input CSV file that lists the inactive dimensions to be deleted.
inactive	Number of days for which data does not exist for the dimension. Example: 180
output_dir	Directory location of the output CSV file that lists inactive dimensions. Example: Directory location: {PMDB_HOME}\DLC CSV file: <dimension_table_name>_0_*.csv
mode	Mode of the operation [test/commit]. Use the test (default) mode to review the data that will be modified or deleted. Execute the commit mode to permanently apply the changes to the OBR database. You should use the test mode and review the affected files before you perform the commit operation.

Managing duplicate dimensions

When a new node is added to the environment with the name of an older node, you have a duplicate dimension in the OBR database. You can list out duplicate entries and delete them or rename them. The Configuration Item (CI) with the latest time-stamp is considered the original dimension and the earlier entries are considered duplicate dimensions. This feature is supported only on conformed dimensions.

List duplicate dimensions

To generate a list of duplicate dimensions, run the following command:

```
dimensionmanager -duplicate_dim_list -caption <caption name> -output_dir <output directory>
```

For details on the command parameters, see ["Duplicate Dimension Parameters" on the next page](#).

Delete duplicate dimensions

To delete duplicate dimensions, run the following command:

```
dimensionmanager -duplicate_dim_delete -caption <caption name> -file <input file> -  
mode <test/commit>
```

For details on the command parameters, see ["Duplicate Dimension Parameters" below](#).

Note: Dimension Manager deletes duplicate data only from conformed dimensions and respective fact tables. It will not delete duplicate data from local dimensions.

Caution: When you execute this command in the commit mode, the dimension and its fact data will be deleted permanently. Take a backup of the OBR database before you perform this operation.

For more information, refer *Database Back up and Recovery* section in *Operations Bridge Reporter Configuration Guide*.

The following table provides a description of the parameters used in the preceding commands:

Duplicate Dimension Parameters

Parameter	Description
duplicate_dim_list	Operation for listing duplicate dimensions.
duplicate_dim_delete	Operation for deleting duplicate dimensions.
caption	Caption name or table name for a dimension. Obtain it from the model interface document available with each content pack. Example: "K_CI_System" or "System".
file	Delete or remove duplicate dimension: Absolute path of the input CSV file that lists the duplicate dimensions to be deleted or renamed.
mode	Mode of the operation [test/commit]. Use the test (default) mode to review changes to your reports. Execute the commit mode to permanently apply the changes to the OBR database. You should use the test mode and review the affected files before you perform the commit operation.

Managing dimensions using business key

To list the business keys (CI_UID) of a conformed dimension, run the following command:

```
dimensionmanager -dim_list -business_keys all -caption <caption name> -output_dir
<directory location>
```

To delete business keys (CI_UID) based on your requirement, run the following command:

```
dimensionmanager -dim_delete -caption <caption name> -file <input file> -mode
<test/commit>
```

To modify the business key (CI_UID) of the duplicate or older dimensions, perform the following steps:

1. In the generated .csv, change column header to OLD_CIID, DSI_KEY_ID, NEW_CIID.
2. In the NEW_CIID column, manually copy the values from the OLD_CIID column to the NEW_CIID column.
3. Run the following command:

```
dimensionmanager -rename_key -caption <caption name> -file <input file>
```

The format of the input file for rename option is caption_name_0_timestamp.csv.

Dimension Parameters

Parameter	Description
dim_list	Operation for listing dimensions.
dim_delete	Operation for deleting dimensions.
business_keys	Comma separated values/patterns (only '*' wildcard is supported) for listing business keys. Use '-business_keys all' to list all the business keys (CI_UID).
rename_key	Operation for renaming the old value of business key (CI_UID) with new value.
caption	Caption name or table name for a dimension. Obtain it from the model interface document available with each content pack. Example: "K_CI_System" or "System".
file	Absolute path of the input CSV file that lists the business keys to be deleted or renamed.
output_dir	Directory location of the output CSV file. Example: C:\DLC
mode	Mode of the operation [test/commit]. Use the test (default) mode to review changes to your reports. Execute the commit mode to permanently apply the changes to the OBR database.

Managing dimensions using natural key

To list the natural keys of a conformed dimension, run the following command:

```
dimensionmanager -dim_list -natural_keys all -caption <caption name> -output_dir  
<directory location>
```

To delete natural keys based on your requirement, run the following command:

```
dimensionmanager -dim_delete -caption <caption name> -file <input file> -mode  
<test/commit>
```

To modify the natural key of the duplicate or older dimensions, perform the following steps:

1. In the generated .csv, change column header to OLD_NK_CI_UID, NEW_NK_CI_UID.
2. Delete the column dsi_key_id from the .csv.
3. In the NEW_NK_CI_UID column, manually copy the values from the OLD_NK_CI_UID column to the NEW_NK_CI_UID column.
4. Run the following command:

```
dimensionmanager -rename -caption <caption name> -file <input file>
```

The format of the input file for rename option is caption_name_0_timestamp.csv.

The following table provides a description of the parameters used in the preceding commands:

Dimension Parameters

Parameter	Description
dim_list	Operation for listing dimensions.
dim_delete	Operation for deleting dimensions.
natural_keys	Comma separated values/patterns (only '*' wildcard is supported) for listing natural keys. Use '-natural_keys all' to list all the natural keys.
rename	Operation for renaming the old value of natural key with new value.
caption	Caption name or table name for a dimension. Obtain it from the model interface document available with each content pack. Example: "K_CI_System" or "System".
file	Absolute path of the input CSV file that lists the natural keys to be deleted or renamed.
output_dir	Directory location of the output CSV file. Example: C:\DLC

Dimension Parameters, continued

Parameter	Description
mode	Mode of the operation [test/commit]. Use the test (default) mode to review changes to your reports. Execute the commit mode to permanently apply the changes to the OBR database.

Managing inactive or duplicate dimensions in data source

You can list and delete the dimensions that have remained inactive for a certain period in the Run-time Service Model (RTSM) data source from which OBR gathers data.

List inactive dimensions in data source

To generate a list of inactive dimensions in the RTSM data source, run the following command:

```
dimensionmanager -check_datasource -list_inactive -output_dir <directory location>
```

For details on the command parameters, see ["Check data source dimension parameters" below](#)

List duplicate dimensions in data source

To generate a list of duplicate dimensions in the RTSM data source, run the following command:

```
dimensionmanager -check_datasource -list_duplicate -output_dir <directory location>
```

For details on the command parameters, see ["Check data source dimension parameters" below](#)

The following table provides a description of the parameters used in the preceding commands:

Check data source dimension parameters

Parameter	Description
list_inactive	Operation for listing the inactive dimensions in data source.
list_duplicate	Operation for listing duplicate dimensions in data source.
check_datasource	Operation for verifying dimensions in the RTSM data source.
output_dir	Directory location of the output CSV file that lists inactive dimensions. Example:

Check data source dimension parameters, continued

Parameter	Description
	Directory location: {PMDB_HOME}\DLC CSV file: <dimension_table_name>_0_*.csv

Configuring downtime in reports

Downtime refers to periods when a system, network, or application is not available to the user because of known or unknown reasons. Downtime is important for calculating the availability of a system, application, or network, which is typically expressed as the percentage of uptime in a given period. When using OBR to generate service-level agreement (SLA)-based reports, there is a need to exclude the predefined downtime to provide accurate availability information. This is because downtime can skew the CI data in the reports.

Note: OBR computes Availability metrics based on initial samples received from NNMi/NPS. Updates to the metric values after the initial samples are received from NNMi/NPS is not supported.

In OBR, there are two types of downtime:

- **Planned downtime:** This refers to the scheduled periods of time where the system or network is brought down to run maintenance job such as running a backup, or patching software, or performing a system reboot. Planned downtime is a result of logical, management-initiated event.
- **Excused downtime:** This refers to the unscheduled periods of time when the system is not available because of some physical event, such as hardware or software failure or a power outage.

Downtime is configured based on associated CIs. For example, you might want to exclude a recurring maintenance event or a holiday for a specific host CI whose physical host you know will be down for that period of time.

OBR enables you to:

- Configure the downtime to occur once or to recur weekly or monthly.
- Select multiple CIs to be affected by the downtime.

The downtime information is defined for each CI in an XML file, where you must manually specify the downtime period, the duration, and the specific instances of the CIs. OBR uses this XML file to update the collected fact data with the downtime information before loading the data into the database.

The downtime period is marked on the "As-pollled" data or "5-minute" data only. When this data is summarized for the hourly table and upwards, the downtime period is excluded from it. OBR OOTB Availability reports display the overall uptime and downtime of the node in your environment over a period of time.

The following table provides information if the downtime is applicable for each Content packs:

Content Pack	Downtime Applicable
Real User Monitor	No
Business Process Monitor	No
Service Health	No
IBM WebSphere Application Server	Yes
Microsoft Active Directory	Yes
Microsoft Exchange	Yes
Microsoft SQL Server	Yes
Oracle	Yes
Oracle WebLogic Server	Yes
Network	No
Operations Manager	No
OMi	No
System Management	Yes
Virtualization	Yes

Create the downtime XML file

You can provide the downtime information at any time after installing the Content Packs. To provide downtime information to OBR, following these steps:

1. Depending on the deployment scenario, identify the CIs or managed nodes that are going to be affected by downtime.
2. Get the CI details from the Model Automation XML file. For more information, see the Operations Bridge Reporter *Content Development Guide*.
3. Decide whether the downtime will occur once or recur at a weekly or monthly basis.
4. Based on the recurrence, create a downtime schedule XML file using any one of the following examples:
 - [Downtime schedule with one occurrence](#)
 - [Weekly downtime schedule](#)
 - [Monthly downtime schedule](#)

5. After creating the XML file, place the file in the C : \HP-SHR\PMDB\data\downtime folder.

After the files are placed in the downtime folder, the data processing in OBR handles the downtime enrichment on the collected data. The enriched data is aggregated and stored in the database for reporting purposes. You can monitor the downtime enrichment on the **Internal Monitoring > Data Process Status** page, which displays the downtime stream details for a particular Content Pack.

Syntax for downtime schedule with one occurrence

To create a downtime schedule that occurs only once, you can use one of the following XML syntax:

Syntax 1

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<downtime>
  <name>Sample1</name>
  <category>Other</category>
  <schedule >
    <type>ONCE</type>
    <startDate>2012-02-07 10:00:00</startDate>
    <endDate>2012-02-07 22:00:00</endDate>
  </schedule>
  <instances type="System">
    <instance>
      <attribute name="CI_UID"
        value="c2fa6553dd16af591b128e19feec3d49"/>
    </instance>
  </instances>
</downtime>
```

Syntax 2

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
```

```
<downtime>
  <name>Sample1</name>
  <category>Application maintenance</category>
  <schedule >
    <type>ONCE</type>
    <startDate>2012-02-07 10:00:00</startDate>
    <endDate>2012-02-07 22:00:00</endDate>
  </schedule>
  <selectedCIs>
    <ci>
      <id>ciid_bizsvc1</id>
    </ci>
    <ci>
      <id>ciid_bizsvc2</id>
    </ci>
  </selectedCIs>
</downtime>
```

The following table provides a description of the tags used in the above sample.

Tag	Description
<name>	Provide a name for the downtime in the tag.
<category>	The category assigned to the downtime. Options include: <ul style="list-style-type: none">• Application installation• Application maintenance• Hardware installation• Hardware maintenance• Network maintenance• Operating system reconfiguration

Tag	Description
	<ul style="list-style-type: none"> • Other • Security issue
<schedule>	Define the downtime schedule in this section of the XML.
<type>	Define the type of downtime schedule that you want to create. The values can be ONCE, WEEKLY, or MONTHLY.
<startDate>	Specify the starting date and time of the scheduled downtime for the monitored component or CI. The date format is yyyy-mm-dd hh:mm:ss. You can change this value at any time. However, data that is enriched with downtime information will not be reprocessed.
<endDate>	Specify the ending date and time of the scheduled downtime for the CI. The date format is yyyy-mm-dd hh:mm:ss. You can change this value at any time. However, data that is enriched with downtime information will not be reprocessed.
<instances type>	In this section, you define the CI type that will be affected by downtime such as node, CPU, Disk, Web server, application, event, and so on. The downtime XML that you create is applicable for one CI type only. For additional CIs, you must create additional XML files.
<instance>	Each instance of the CI type must be defined in a separate <instance> tag. The attribute name refers to the instance metric and the value refers to the value of that metric. If a particular CI instance is defined by more than one metric, additional instances must also be defined by the same number and type of metrics. For the CI parameters, see the Model Automation XSD.
<selectedCIs>	In this section, you can directly define multiple CIs that will be affected by downtime. You can refer to these CIs by using their unique IDs. This section is applicable if OBR is deployed in the SaOB and APM deployment scenarios where RTSM is the topology source.

Syntax for weekly downtime schedule

To create a downtime schedule that occurs on a weekly basis, you can use one of the following XML syntax:

Syntax 1

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<downtime>
  <name>Sample2</name>
  <category>Other</category>
  <schedule >
    <type>WEEKLY</type>
    <days>
      <selectedDays>SUNDAY</selectedDays>
      <selectedDays>MONDAY</selectedDays>
      <selectedDays>TUESDAY</selectedDays>
      <selectedDays>WEDNESDAY</selectedDays>
    </days>
    <startTimeInSecs> 57600</startTimeInSecs>
    <durationInSecs> 10800</durationInSecs>
    <validFrom>2012-02-02 12:00:00</validFrom>
    <validTo>2012-03-10 12:00:00</validTo>
  </schedule>
  <instances type="CPU">
    <instance>
      <attribute name="CI_UID"
        value="c2fa6553dd16af591b128e19feec3d49"/>
    </instance>
    <instance>
      <attribute name="CI_UID"
        value="b1ta83456aa13rf352h908e19teec3d49"/>
    </instance>
  </instances>
</downtime>
```



```
</instances>
```

```
</downtime>
```

Syntax 2

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
```

```
<downtime>
```

```
  <name>Sample2</name>
```

```
  <category>Other</category>
```

```
  <schedule >
```

```
    <type>WEEKLY</type>
```

```
    <days>
```

```
      <selectedDays>SUNDAY</selectedDays>
```

```
    </days>
```

```
    <startTimeInSecs> 57600</startTimeInSecs>
```

```
    <durationInSecs> 10800</durationInSecs>
```

```
    <validFrom>2012-02-02 12:00:00</validFrom>
```

```
    <validTo>2012-03-10 12:00:00</validTo>
```

```
  </schedule>
```

```
  <selectedCIs>
```

```
    <ci>
```

```
      <id>ciid_bizsvc1</id>
```

```
    </ci>
```

```
    <ci>
```

```
      <id>ciid_bizsvc2</id>
```

```
    </ci>
```

```
</selectedCIs>
```

```
</downtime>
```

The following table provides a description of the tags used in the above sample.

Tag	Description
<name>	Provide a name for the downtime in the tag.
<category>	<p>The category assigned to the downtime. Options include:</p> <ul style="list-style-type: none"> • Application installation • Application maintenance • Hardware installation • Hardware maintenance • Network maintenance • Operating system reconfiguration • Other • Security issue
<schedule>	Define the downtime schedule in this section of the XML.
<type>	Define the type of downtime schedule that you want to create. The values can be ONCE, WEEKLY, or MONTHLY.
<days>	Specify the days of the week when downtime for the CI type is planned for in this section.
<startTimeInSecs>	Specify the starting time of the scheduled downtime in seconds. For example, 57600 seconds equals to 16:00, which means that the downtime is scheduled to start at 4 P.M. on each day that is defined in the <days> tag.
<durationInSecs>	Specify the duration of the downtime in seconds. For example, 10800 seconds equals to 3 hours, which means that the downtime period lasts for 3 hours from 4 P.M. to 7 P.M.
<validFrom>	Specify the starting date and time when OBR must start collecting the downtime information for data enrichment. The date format is yyyy-mm-dd hh:mm:ss.
<validTo>	Specify the ending date and time when OBR must stop collecting the downtime information for data enrichment. The date format is yyyy-mm-dd hh:mm:ss.
<instances type>	In this section, you define the CI type that will be affected by downtime such as node, CPU, Disk, Web server, application, event, and so on. The downtime XML that you create is applicable for one CI type only. For additional CIs, you must create additional XML files.

Tag	Description
<instance>	Each instance of the CI type must be defined in a separate <instance> tag. The attribute name refers to the instance metric and the value refers to the value of that metric. If a particular CI instance is defined by more than one metric, additional instances must also be defined by the same number and type of metrics. For the CI parameters, see the Model Automation XSD.
<selectedCIs>	In this section, you can directly define multiple CIs that will be affected by downtime. You can refer to these CIs by using their unique IDs. This section is applicable if OBR is deployed in the SaOB and APM deployment scenarios where RTSM is the topology source.

Syntax for monthly downtime schedule

To create a downtime schedule that occurs on a monthly basis, you can use one of the following XML syntax:

Syntax 1

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<downtime>
  <name>Sample3</name>
  <category>Other</category>
  <schedule >
    <type>MONTHLY</type>
    <days>
      <selectedDays>4</selectedDays>
      <selectedDays>8</selectedDays>
    </days>
    <startTimeInSecs>57600</startTimeInSecs>
    <durationInSecs>10800</durationInSecs>
    <validFrom>2012-02-02 12:00:00</validFrom>
```

```
<validTo>2012-03-10 12:00:00</validTo>
</schedule>
<instances type="CPU">
  <instance>
    <attribute name="CI_UID"
      value="c2fa6553dd16af591b128e19feec3d49"/>
  </instance>
</instances>
</downtime>
```

Syntax 2

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<downtime>
  <name>Sample3</name>
  <category>Other</category>
  <schedule >
    <type>MONTHLY</type>
    <days>
      <selectedDays>4</selectedDays>
      <selectedDays>8</selectedDays>
    </days>
    <startTimeInSecs>57600</startTimeInSecs>
    <durationInSecs>10800</durationInSecs>
    <validFrom>2012-02-02 12:00:00</validFrom>
    <validTo>2012-03-10 12:00:00</validTo>
  </schedule>
  <selectedCIs>
```

```

    <ci>
      <id>ciid_bizsvc1</id>
    </ci>
    <ci>
      <id>ciid_bizsvc2</id>
    </ci>
  </selectedCIs>
</downtime>

```

The following table provides a description of the tags used in the above sample.

Tag	Description
<name>	Provide a name for the downtime in the tag.
<category>	The category assigned to the downtime. Options include: <ul style="list-style-type: none"> • Application installation • Application maintenance • Hardware installation • Hardware maintenance • Network maintenance • Operating system reconfiguration • Other • Security issue
<schedule>	Define the downtime schedule in this section of the XML.
<type>	Define the type of downtime schedule that you want to create. The values can be ONCE, WEEKLY, or MONTHLY.
<days>	Specify the days of the month when downtime for the CI type is planned for in this section. For example, 4 and 8 refers to the 4th and 8th day of the month when the downtime for the particular CI is planned.
<startTimeInSecs>	Specify the starting of the scheduled downtime in seconds. For example, 57600 seconds equals to 16:00, which means that the downtime is scheduled to start at 4 P.M. each day that is defined in the <days> tag.

Tag	Description
<durationInSecs>	Specify the duration of the downtime in seconds. For example, 10800 seconds equals to 3 hours, which means that the downtime period lasts for 3 hours from 4 P.M. to 7 P.M.
<validFrom>	Specify the starting date and time when OBR must start collecting the downtime information for data enrichment. The date format is yyyy-mm-dd hh:mm:ss.
<validTo>	Specify the ending date and time when OBR must stop collecting the downtime information for data enrichment. The date format is yyyy-mm-dd hh:mm:ss.
<instances type>	In this section, you define the CI type that will be affected by downtime such as node, CPU, Disk, Web server, application, event, and so on. The downtime XML that you create is applicable for one CI type only. For additional CIs, you must create additional XML files.
<instance>	Each instance of the CI type must be defined in a separate <instance> tag. The attribute name refers to the instance metric and the value refers to the value of that metric. If a particular CI instance is defined by more than one metric, additional instances must also be defined by the same number and type of metrics. For the CI parameters, see the Model Automation XSD.
<selectedCIs>	In this section, you can directly define multiple CIs that will be affected by downtime. You can refer to these CIs by using their unique IDs. This section is applicable if OBR is deployed in the SaOB and APM deployment scenarios where RTSM is the topology source.

Configuring downtime in the past

Past downtime in OBR can be configured by performing the following steps:

1. Log on to the system as an administrator.
2. Configure downtime under the following folder:

Windows: %pmdb_home%\datadowntime

Linux: \$pmdb_home/data/downtime

To configure the downtime, see ["Configuring downtime in reports" on page 259](#)

3. Click **Start > Run >** type **cmd**. The command prompt window appears.
4. Type **downtime** to populate the CIs that are associated with the downtime streams.

Past downtime for all the streams in OBR can be processed as follows:

1. Click **Start > Run >** type **cmd**. The command prompt window appears.
2. Type **downtimeutility** to process all the downtime streams as shown in the following image:

```
G:\Users\Administrator>downtimeutility
PID:28108
Started processing all the streams...
Processing downtime streams, please wait for some time...
in executer
Waiting for all running streams to complete there job
Aborting all ABC streams...
Aborted all ABC streams...
Running ABCBatch load (loading all streams)..
Finished loading streams..
Running streams..
Starting limer service..
in executer
Successfully processed all the streams...
```

Processing past downtime for all the streams is time consuming. If you wish to process past downtime for a single stream perform the following steps:

1. Log on to the Administration Console.
2. Go to **Home Page**, click **PMDB Platform** under the **Content Pack Component Name** for the list of streams that are configured in OBR.
3. Select the Stream ID of the specific stream for which you wish to process past downtime.
4. Click **Start > Run >** type **cmd**. The command prompt window appears.
5. Type **downtimeutility -streamid <stream ID>**.
6. This processes the past downtime only for the specific stream and the associated CI.

Note: Processing past downtime stops the **HPE_PMDB_Platform_Orchestration** service. Reprocessing of the streams is started after processing the streams that are currently running. The service is automatically restarted after reprocessing the streams.

Past Downtime is automatically configured for a period of 7 days. To change this value, perform the following steps:

1. Open the file **config.prp** file resented in the following folder:

Windows: %pmdb_home%\data

Linux: \$pmdb_home/data

2. Change the value assigned to the field **downtimedays**. The default number of days is 7.

Configuring customer in reports

If you are a Managed Service Provider (MSP) using OBR, you can generate reports per customer or aggregate data per customer by:

1. Provisioning customers and customer-dimension associations in an XML file.
2. Creating custom reports using the Customer Name object in the SAP BusinessObjects Universe.

You can associate only conformed dimensions [Configuration Items (CIs)] to customers. You can configure multiple customers in a single XML file which is processed periodically. Newer dimensions that meet the conditions defined in the XML file are automatically associated to the customer.

To provision customers and associate them with dimensions in OBR:

1. Create an XML file with the name of the customer and associate it with the appropriate dimensions. For the syntax of this XML file, see [Creating customer XML](#).
2. Save the XML file in the **PMDB_HOME/config** folder.
3. Wait for a few minutes and verify if the **PMDB_Platform@CustomerDefinition** stream has run successfully. This stream processes the XML and creates CSV files that OBR consumes for generating reports.

To generate reports grouped by customers you configured, use the Customer Name object from the SAP BusinessObjects Universe. You can enhance out-of-the-box (OOTB) reports or create new reports.

Note: You must make a copy of the OOTB reports when you modify them.

Creating Customer XML

To provision customers, copy the following syntax in an XML file:

Note: You can enter a file name of your choice for the XML file, but follow the **<name>customerenrich.xml** restriction; where, **<name>** is any file string supported by the operating system.

For example, shr_customerenrich.xml or SHR9XXcustomerenrich.xml and so on.

<customers>

```
<customer name="">  
  
<Address1></Address1>  
  
<Address2></Address2>  
  
<City></City>  
  
<State></State>  
  
<Zipcode></Zipcode>  
  
<Phonenumber></Phonenumber>  
  
<Description></Description>  
  
<instances type="">  
  
<instance>  
  
<attribute name="" value="" operator="" relation=""/>  
  
<attribute name="" value="" operator=""/>  
  
</instance>  
  
</instances>  
  
</customer>  
  
</customers>
```

The following table provides a description of the attribute tags used in the above syntax.

Field	Description
<customer name>	Enter name of a customer. Entering a value in this field is mandatory.
<address1>	Enter address here. (Optional)
<address2>	Enter address here. (Optional)
<city>	Enter the name of a city here. (Optional)
<state>	Enter the name of a state here. (Optional)
<zipcode>	Enter the zipcode here; only numbers are allowed. (Optional)
<phonenumber>	Enter the phone number here; only numbers are allowed. (Optional)
<description>	Enter a description of your choice. (Optional)
<instances type>	Dimension table name conformed to the K_CI table. See the model interface document available with each content pack in their respective <i>/doc</i> folder to

Field	Description
	fetch the list of dimensions. The dimensions are extracted from this table.
<attribute name>	Name of the string column (not numeric column) in the dimension table defined in the <instance type> tag.
<value>	The column value in the dimension table must match this value.
<operator>	<p>Operator for searching the node name value.</p> <p>To perform an exact match of values, use the EQUALS operator. For example, "abcvalue1"</p> <p>To perform a pattern based match of values, use the LIKE operator. You can specify the value as "abcvalue1%" or "%abcvalue1%" and so on.</p> <p>For other operators such as IN, NOT IN, NOT LIKE, EXISTS, "=", or "!=", you must specify the values enclosed within double quotes. For example, the IN operator must have the values as "'abcvalue1', 'abcvalue2', 'abcvalue3'".</p> <p>Note: All the value comparisons in the XML against the OBR database is case insensitive.</p>
<relation>	<p>Determines if the AND or OR operation must be performed when multiple attribute-value pairs are specified.</p> <p>If you do not define a relation value, OBR considers the default value as AND.</p>

Applicable Content Packs

You can associate customers to conformed dimensions in the following content packs:

- Cross-Domain Operations Events
- IBM WebSphere Application Server
- Microsoft Active Directory
- Microsoft Exchange Server
- Microsoft SQL Server
- Network Performance
- Oracle
- Oracle WebLogic Server

- System Performance
- Virtualization Infrastructure Management

The customer information is available from the data source for the following content packs:

- Real User Transaction Monitoring
- Health and Key Performance Indicators
- Synthetic Transaction Monitoring

The customer information is not available in the Operations Events content pack.

Customer XML Example

```
<customers>
<customer name="Hewlett-Packard Company">
<Address1>3000 Hanover Street</Address1>
<Address2></Address2>
<City>Palo Alto</City>
<State>California</State>
<ZipCode>94304</ZipCode>
<PhoneNumber>16508571501</PhoneNumber>
<Description></Description>
<instances type="K_CI_Oracle">
<instance>
<attribute name="CI_UID" value="8c5e2d0fd63a0b0bd66d6e" operator="EQUALS"
relation="OR" />
<attribute name="CI_UID" value="3f5a2d0fd64a0b0wg66d6e" operator="EQUALS"
relation="OR" />
<attribute name="CI_UID" value="98cd49a3e850a455788286" operator="EQUALS" />
</instance>
</instances>
```

</customer>

</customers>

Configuring location in reports

You can use OBR to generate reports on infrastructure and applications based on their geographical location.

To generate reports grouped by location, you must associate dimensions with location information as follows:

1. Create an XML file, enter location details, and associate dimensions to the location. For the syntax of this XML file, see [Creating location XML](#).
2. Save the XML file in the **PMDB_HOME/config** folder.
3. Wait for a few minutes and verify if the **PMDB_Platform@platform_poller_registry_build** stream has run successfully. This stream processes the XML and creates CSV files that OBR consumes for generating reports.

You can associate only conformed dimensions [Configuration Items (CIs)] to locations. Newer dimensions that meet the conditions defined in the XML file are automatically associated to the location.

Creating Location XML

To create a location record, copy the following syntax in an XML file:

Note: You can enter a file name of your choice for the XML file, but follow the **<name>locationenrich.xml** restriction; where, *<name>* is any file string supported by the operating system.

For example, shr_locationenrich.xml or SHR9XXlocationenrich.xml and so on.

```
<locations>
<location name="">
<Country></Country>
<State ></State>
<City></City>
<Region></Region>
```

```

<Address></Address>

<Building></Building>

<Floor></Floor>

<instances type=" ">

<instance>

<attribute name="" value="" operator="" relation=""/>

<attribute name="" value="" operator="" />

</instance>

</instances>

</location>

</locations>
  
```

The following table provides a description of the tags used in the above example:

Note: Ensure that you do not use comma (,) in the values entered.

Field	Description
<location name>	Enter name of the location. Entering a value in this field is mandatory.
<country>	Enter the name of a country here. (Optional)
<state>	Enter the name of a state here. (Optional)
<city>	Enter the name of a city here. (Optional)
<region>	Enter the name of a region here. Entering a value in this field is mandatory.
<address>	Enter address here. (Optional)
<building>	Enter the name of a building here. (Optional)
<floor>	Enter the floor here. (Optional)
<instances type>	Dimension table name conformed to the K_CI table. See the model interface document available with each content pack in their respective /doc folder to fetch the list of dimensions. The dimensions are extracted from this table.
<attribute name>	Name of the string column (not numeric column) in the dimension table defined in the <instance type> tag.
<value>	Value of the column in the dimension table for which you create the location, such as values in the column "node_name" of the "K_CI_Oracle" dimension

Field	Description
	table. Or, values in the column "dns_name" of the "K_CI_System" dimension table, and so on.
< operator>	<p>Operator for searching the node name value.</p> <p>To perform an exact match of values, use the EQUALS operator. For example, "abcvalue1"</p> <p>To perform a pattern based match of values, use the LIKE operator. You can specify the value as "abcvalue1%" or "%abcvalue1%" and so on.</p> <p>For other operators such as IN, NOT IN, NOT LIKE, EXISTS, "=", or "!=" , you must specify the values enclosed within double quotes. For example, the IN operator must have the values as "'abcvalue1', 'abcvalue2', 'abcvalue3'".</p> <p>Note: All the value comparisons in the XML against the OBR database is case insensitive.</p>
<relation>	<p>Determines if the AND or OR operation must be performed when multiple attribute-value pairs are specified.</p> <p>If you do not define a relation value, OBR considers the default value as AND.</p>

Applicable Content Packs

You can associate location to conformed dimensions in the following content packs:

- IBM WebSphere Application Server
- Microsoft Active Directory
- Microsoft Exchange Server
- Microsoft SQL Server
- Oracle
- Oracle WebLogic Server
- System Performance
- Virtualization Infrastructure Management

The location information is available from the data source in the following content packs:

- Network Performance
- Real User Transaction Monitoring

- Synthetic Transaction Monitoring

The location information is not available in the following content packs:

- Operations Events
- Cross-Domain Operations Events
- Health and Key Performance Indicators

Location XML Example

```
<locations>
<location name="Santa Clara County">
<Country>USA</Country>
<State>California</State>
<City>Palo Alto</City>
<Region>San Francisco Bay Area</Region>
<Building>239</Building>
<Floor>5th floor A block</Floor>
<instances type="K_CI_System">
<instance>
<attribute name="dns_name" value="abc%" operator="LIKE" relation="OR" />
<attribute name="dns_name" value="xyz1" operator="EQUALS" relation="OR" />
<attribute name="dns_name" value="pqr2%" operator="LIKE" />
</instance>
</instances>
</location>
</locations>
```

OBR Reports

The reports in OBR are grouped as follows:

- Operations Bridge Reporter
 - Business Service Management
 - End User Management
 - Real User Monitor
 - Synthetic Transaction Monitoring (BPM)
 - Service Health
 - Infrastructure Management
 - Service and Operations Bridge (OMi)
 - Enterprise Application Management
 - Microsoft Active Directory
 - Microsoft Exchange
 - Microsoft SQL Server
 - Oracle
 - IBM WebSphere
 - Oracle WebLogic
 - Operations (OM)
 - Network
 - Component Health
 - Executive Summary
 - Interface Health
 - System Management
 - Virtualized Environment Management

For more information on procedures to configure OBR to collect data from the data sources, prerequisite policies to be deployed and installing the Content Packs, refer the individual guides mentioned in the following table:

Content Pack	Reference Guide name
Real User Monitor (RUM)	<i>Operations Bridge Reporter Real User Transaction Monitoring Content Pack Reference</i>
Synthetic Transaction Monitoring (BPM)	<i>Operations Bridge Reporter Synthetic Transaction Monitoring Content Pack Reference</i>
Service Health	<i>Operations Bridge Reporter Health and Key Performance Indicators Content Pack Reference</i>
Microsoft Active Directory	<i>Operations Bridge Reporter Microsoft Active Directory Content Pack Reference</i>
Microsoft Exchange	<i>Operations Bridge Reporter Microsoft Exchange Server Content Pack Reference</i>
Microsoft SQL Server	<i>Operations Bridge Reporter Microsoft SQL Server Content Pack Reference</i>
Oracle	<i>Operations Bridge Reporter Oracle Content Pack Reference</i>
Oracle WebLogic	<i>Operations Bridge Reporter Oracle WebLogic Server Content Pack Reference</i>
IBM WebSphere	<i>Operations Bridge Reporter IBM WebSphere Application Server Content Pack Reference</i>
Operations (OM)	<i>Operations Bridge Reporter Operations Events Content Pack Reference</i>
Network Component Health	<i>Operations Bridge Reporter Network Component Health Content Pack Reference</i>
Network Executive Summary	<i>Operations Bridge Reporter Network Performance Content Pack Reference</i>
Network Interface Health	<i>Operations Bridge Reporter Network Interface Health Content Pack Reference</i>
System Management	<i>Operations Bridge Reporter System Performance Content Pack Reference</i>
Virtualized Environment Management	<i>Operations Bridge Reporter Virtual Environment Performance Content Pack Reference</i>
Cross-Domain Operations Events	<i>Operations Bridge Reporter Cross-Domain Operations Events Content Pack Reference</i>

For more information on procedures to configure OBR to collect data from the SPI data sources, see [Operations SPIs](#) and from OMi MP, see [Operations Manager i Management packs](#).

Integrating with Data Sources for Operations Smart Plug-ins

To show reports on the data collected from different enterprise applications, OBR relies on the metrics collected by collectors of Operations Smart Plug-ins (SPIs). SPI collectors store the data into the data store provided by the Operations Agent. OBR's integration with SPI data sources facilitate transfer of data from Operations Agent's data store to OBR's database.

This integration is established when you deploy OBR in the OM deployment scenario.

OBR provides performance reports for the following enterprise applications:

- Microsoft Active Directory
- Microsoft Exchange
- Microsoft SQL Server
- Oracle Database
- Oracle WebLogic Server
- IBM WebSphere Application Server

Working of the Integration

1. Installation and configuration of a SPI ensures that necessary instrumentation, scripts, programs, and policies are transferred to a node where the application is running and the Operations Agent is already installed.

Tip: For successful installation and configuration of SPIs, follow the SPI documentation.

2. SPI collectors start collecting data on the node based on rules and specifications available with the policies deployed on the node.
3. SPI stores the collected data into Operations Agent's data store. Each SPI creates at least one *data source* in agent's data store.
4. After configuring OBR to collect data from a data source and installing Content Packs, OBR starts collecting historical data from agent's data store.

Tip: Procedures to configure OBR to collect data from the SPI data sources and installing Content Packs are available in the *Operations Bridge Reporter Configuration Guide*.

Prerequisites for Generating OBR Reports from the Operations SPIs Data

Ensure the following prerequisites are met before integrating OBR with Operations SPIs. Otherwise, blank OBR reports will be generated:

- **Ensure data is logging into the Operations SPIs data store.**
 - a. Ensure Operations SPIs is installed and configured. For further information on deploying and configuring Operations SPIs, see the reference documents mentioned for each Operations SPIs in individual chapters of this book.
 - b. Ensure all necessary Operations SPIs policies are deployed correctly.
 - c. Ensure Operations SPIs collector is logging metrics into Operations Agent database. For details on verifying that Operations SPIs is logging metrics into database, see the *Operations Bridge Reporter Troubleshooting Guide*.

Note: If any of the preconditions are not fulfilled by the Operations SPIs, OBR cannot gather the necessary information from the data source and reports will not generate.

- **Ensure OBR is configured for Operations SPIs data store.**
 - a. Ensure the topology source (OM or RTSM) is configured to collect fact metrics from the data store of Operations SPIs. Verify this from the OBR Administration Console > Topology Configuration > Test Connection (which should be successful). For more information, see "*Configuring OBR*" in the *Operations Bridge Reporter Configuration Guide*.
 - b. Ensure the OBR Content Packs relevant to the Operations SPIs are installed. Verify this from the OBR Administration Console > Content Pack Deployment ; you will see a column that indicates the deployment status of the content pack.

Note: If the Operations SPIs data store is not configured for OBR, it cannot gather the necessary information from the data source and reports will not generate.

Each OBR report uses a specific set of Operations SPIs metrics available in HPE Operations Agent's data store. Collection of metric data is governed by the Operations SPIs policies deployed on the node. In other words, to be able to view reports of your interest successfully, you must deploy all the prerequisite policies.

Integrating with Data Sources for Operations Manager i Management Packs

To show reports on the data collected from different enterprise applications, OBR relies on the metrics collected by Operations Manager i Management Pack (OMi MP). OMi MP collectors store the data into the data store provided by the Operations Agent. OBR's integration with OMi MP data sources facilitates transfer of data from Operations Agent's data store to OBR's database.

This integration is established when you deploy OBR views in the RTSM deployment scenario.

OBR provides performance reports for the following enterprise applications:

- OMi MP for Microsoft Active Directory
- OMi MP for Microsoft SQL Server
- OMi MP for Microsoft Exchange
- OMi MP for Oracle Database
- OMi MP for Oracle WebLogic
- OMi MP for IBM WebSphere

Working of the Integration

1. Installation and configuration of an OMi MP ensures that necessary instrumentation, scripts, programs, and policies are transferred to a node where the application is running and the Operations Agent is already installed.

Tip: For successful installation and configuration of OMi MPs, follow the *OMi MP* documentation.

2. OMi MP collectors start collecting data on the node based on rules and specifications available with the policies deployed on the node.
3. OMi MP stores the collected data into Operations agent's data store. Each OMi MP creates at least one *data source* in agent's data store.
4. After configuring OBR to collect data from a data source and installing Content Packs, OBR starts collecting historical data from agent's data store.

Tip: Procedures to configure OBR to collect data from the OMi MP data sources and installing Content Packs are available in the *Operations Bridge Reporter Configuration Guide*.

Prerequisites for Generating OBR Reports from the Operations Manager i Management Packs Data

Ensure the following prerequisites are met before integrating OBR with OMi MP. Otherwise, blank OBR reports will be generated:

- **Ensure data is logging into the Operations Agent data store.**
 - a. Ensure OMi MP is installed and configured. For further information on deploying and configuring OMi MPs, see the reference documents mentioned for each OMi MP in individual chapters of this book.
 - b. Ensure all necessary OMi MP policies are deployed correctly.
 - c. Ensure OMi MP collector is logging metrics into Operations Agent database. For details on verifying that OMi MP is logging metrics into database, see the *Operations Bridge Reporter Troubleshooting Guide*.

Note: If any of the preconditions are not fulfilled by the OMi MP, OBR cannot gather the necessary information from the data source and blank reports will be generated.

- **Ensure OBR is configured to connect to the Business Service Management (BSM) system where OMi MP is configured.**
 - a. Ensure the topology source (RTSM) is configured to collect fact metrics from the data store of OMi MP. Verify this from the OBR Administration Console > Data Source Configuration > Topology Source > Test Connection (which should be successful). For more information, see "Configuring OBR" in the *Operations Bridge Reporter Configuration Guide*.
 - b. Ensure the OBR Content Packs relevant to the OMi MP are installed. Verify this from the OBR Administration Console > Content Pack Deployment; you will see a column that indicates the deployment status of the content pack.

Note: If the OMi MP data store is not configured in BSM for OBR's use, it cannot gather the necessary information from the data source and blank reports will be generated.

Each OBR report uses a specific set of OMi MP metrics available in Operations Agent's data store. Collection of metric data is governed by the OMi MP policies deployed on the node. In other words, to be able to view OBR reports of your interest successfully, you must deploy all the prerequisite policies.

OML Policies to Monitor OBR

An OBR policy template for Operations Manager for Linux (OML) is a set of configuration data for OBR to integrate into OML. These policy templates define the details of specific configuration and monitoring tasks. Through these policies, OML monitors all the OBR services on Windows and Linux.

The `OBR_OML_Monitoring_policies.zip` file contains OML policy templates to monitor OBR Linux and Windows services.

The OML policy templates are available at the following location in OBRsystem:

```
$PMDB_HOME/scripts/OMLPolicies/OBR_OML_Monitoring_policies.zip
```

This document lists the OML policies for OBR Linux and Windows services, and provides step-by-step instructions to import the policies to an OML system and deploy these policies on nodes or node groups.

Prerequisites

Note: The OML policy templates are supported on OBR 10.01 or later versions only.

Before importing OBR policies to OML, ensure that the following prerequisites are met:

- Ensure that Agent is installed on OBR system.
- Performed the steps required for OBR-Agent coexistence, and request the certificate and apply it.

For more information about coexistence set up and certificate, see *Operations Bridge Reporter Interactive Installation Guide*.

- Add the OBR-Agent node to the OML server.

For more information, see *Operations Bridge Reporter Configuration Guide*.

OBR Services Monitored by OML

OML monitors the following OBR Linux services using the OBR-OML policies:

OBRLinux Services

- HPE_PMDB_Platform_Administrator
- HPE_PMDB_Platform_Collection
- HPE_PMDB_Platform_DB_Logger
- HPE_PMDB_Platform_IA
- HPE_PMDB_Platform_IM
- HPE_PMDB_Platform_JobManager
- HPE_PMDB_Platform_NRT_ETL
- HPE_PMDB_Platform_Orchestration
- HPE_PMDB_Platform_PostgreSQL
- HPE_PMDB_Platform_TaskManager
- HPE_PMDB_Platform_Vertica
- TrendTimer

The policy template Zip file contains one policy template for each of the OBRLinux services.

Following are the policies to monitor OBR services on a Linux system:

- OBR_LinuxAdministrationService
- OBR_LinuxCollectionService
- OBR_LinuxDBLoggerService
- OBR_LinuxIAService
- OBR_LinuxIMService
- OBR_LinuxJobManagerService
- OBR_LinuxNRT_ETLService
- OBR_LinuxOrchestrationService
- OBR_LinuxTaskManagerService

- OBR_LinuxTimerService
- OBR_LinuxPostgreSQLService
- OBR_LinuxVerticaService

OBRWindows Services

The policy rules for all the following Windows services are under a single policy:

- HPE_PMDB_Platform_Administrator
- HPE_PMDB_Platform_Collection
- HPE_PMDB_Platform_DBLogger
- HPE_PMDB_Platform_IA
- HPE_PMDB_Platform_IM
- HPE_PMDB_Platform_JobManager
- HPE_PMDB_Platform_NRT_ETL
- HPE_PMDB_Platform_NRT_ETL_UTILITY
- HPE_PMDB_Platform_Orchestration
- HPE_PMDB_Platform_PostgreSQL
- HPE_PMDB_Platform_TaskManager
- HPE_PMDB_Platform_Timer

All the OBRservices are handled using the following policy template:

- OBR_Windows_Services

Importing and Deploying OML Policy Templates for OBR

Importing Policy Templates to OML System

1. Open the command prompt and connect to OML system using the appropriate credentials.
2. Download or transfer the OML policy Zip from OBR system to OML system.

The OML policy templates are available at the following location in OBR system:

```
$PMDB_HOME/scripts/OMLPolicies/OBR_OML_Monitoring_policies.zip
```

The OBR_OML_Monitoring_policies.zip file contains OML policy templates to monitor OBR Linux and Windows services.

3. Unzip the file using the `unzip <file_name>` command.
4. Upload the policies onto the OML system using the following command:

```
opctempl -upload dir=<zip file extracted path with the directory name>
```

5. On receiving the success message for 13 policies, verify the upload by executing the following command:

```
opctempl -list
```

Check the service names for Linux and Windows.

Deploying Policy Templates

1. In a web browser, enter the following :

```
http://<server_name>.<domain_name>:9662
```

where

<server_name> and <domain_name> represent the Fully Qualified Domain Name (FQDN) of the OML server.

HP Operations Manager

User Name: *

Password: *

Display:

Language: English ▼

HP Operations Manager Administration UI 09.21.110
(c)Copyright 2015 Hewlett-Packard Development Company, L.P.

2. Log on to OML Administration console with appropriate credentials.
3. Click **HPOM** and then click **Policy Bank** as show below.

The screenshot shows the HPOM Administration UI. The top navigation bar includes the HPOM icon, which is highlighted with a red box. Below the navigation bar, the 'Object Banks' section is displayed, with 'Policy Bank' highlighted in red in a list of object hierarchies.

Under Policy bank, you can see OBR Policies.

<input type="checkbox"/>		Infrastructure Management			2 / 0
<input type="checkbox"/>		Management Server			0 / 3
<input type="checkbox"/>		midas			2 / 0
<input type="checkbox"/>		OBR Policies			1 / 0
<input type="checkbox"/>		SiteScope Integration			3 / 0
<input type="checkbox"/>		SNMP			0 / 3

4. Select **OBR Policies** and click the policy template version **1.0**.

Linux and Windows options are displayed.

The screenshot shows the 'Elements in Policy Group "OBR Policies/1.0"' view. The table displays two elements: 'Linux' and 'Windows'.

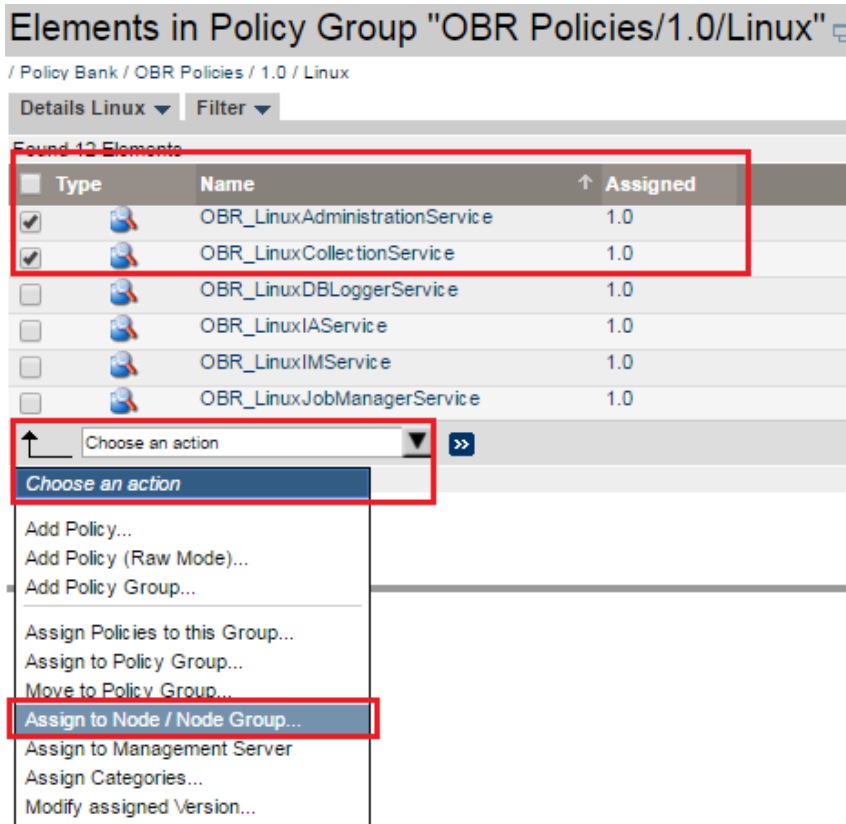
Type	Name	Assigned	Mode
<input type="checkbox"/>	Linux		
<input type="checkbox"/>	Windows		

5. Choose appropriate operating system type depending on the operating system on which OBR is

installed.

For Linux:

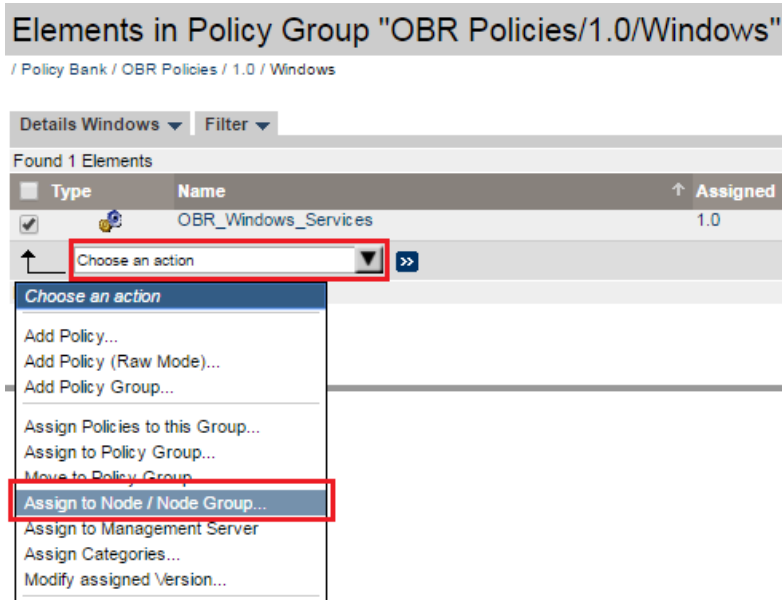
- a. Click **Linux**, and select the policy templates by clicking the check boxes listed.



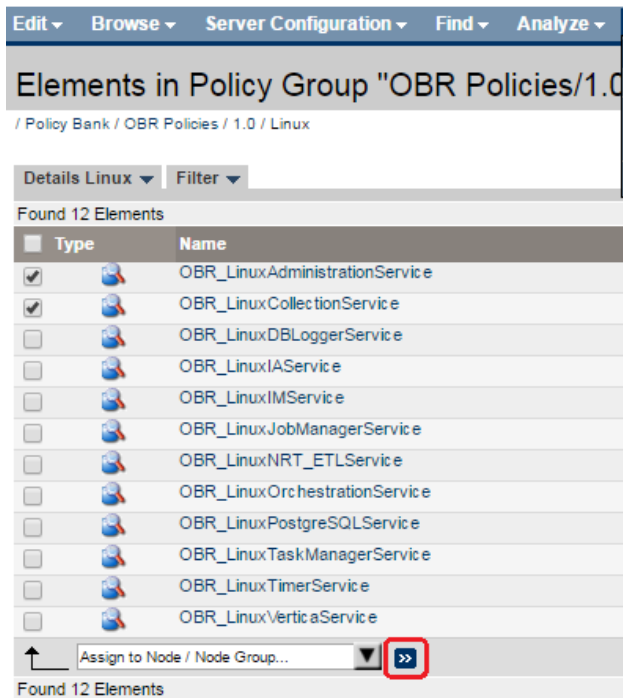
- b. Click **Choose an action** and select **Assign to Node/Node Group**.

For Windows:

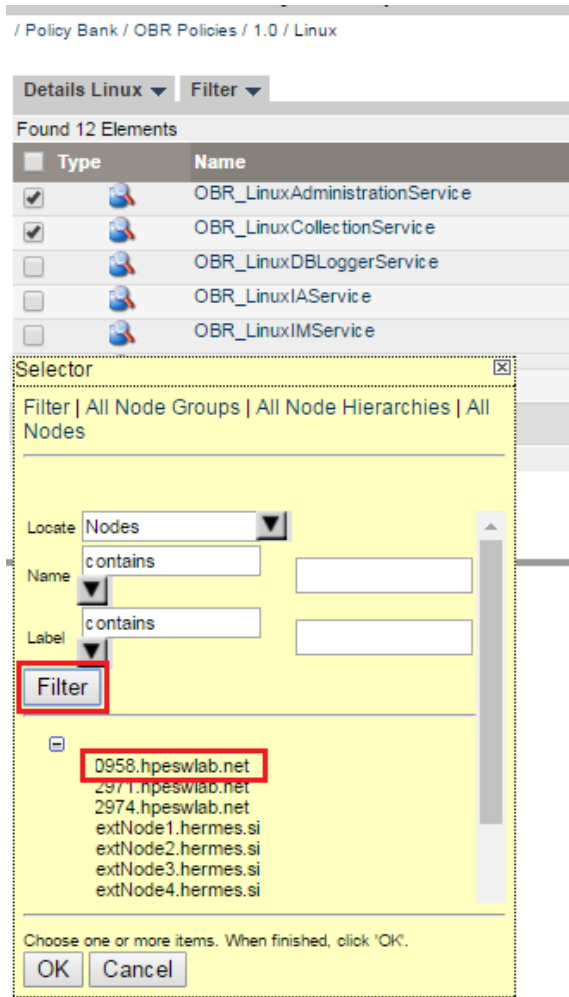
- a. Click **Windows** and then click **OBR_Windows_Services**.
- b. Click **Choose an action** and select **Assign to Node/Node Group**.



6. After selecting the *Assign to Node/Node Group...* action, select the policy templates and click the >> icon.

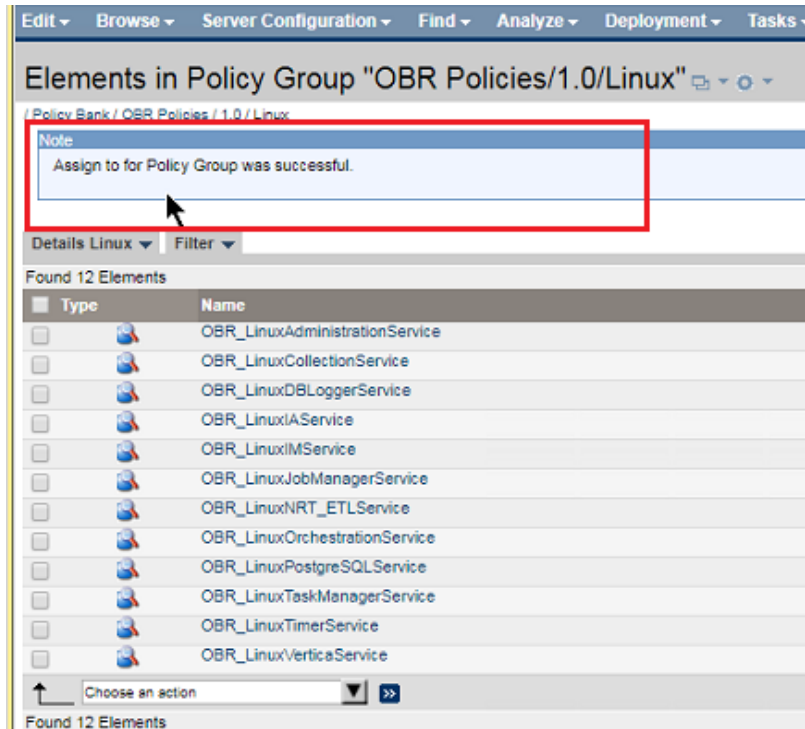


The Selector pop-up appears with a list of nodes.

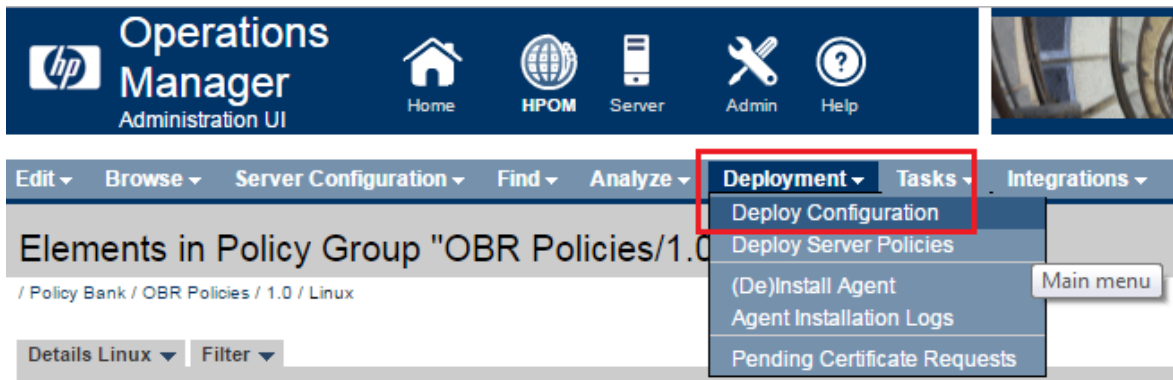


7. Click **Filter**, click and select the nodes, and then click **OK**.

The selected policies are assigned to the node groups and the following message is displayed:

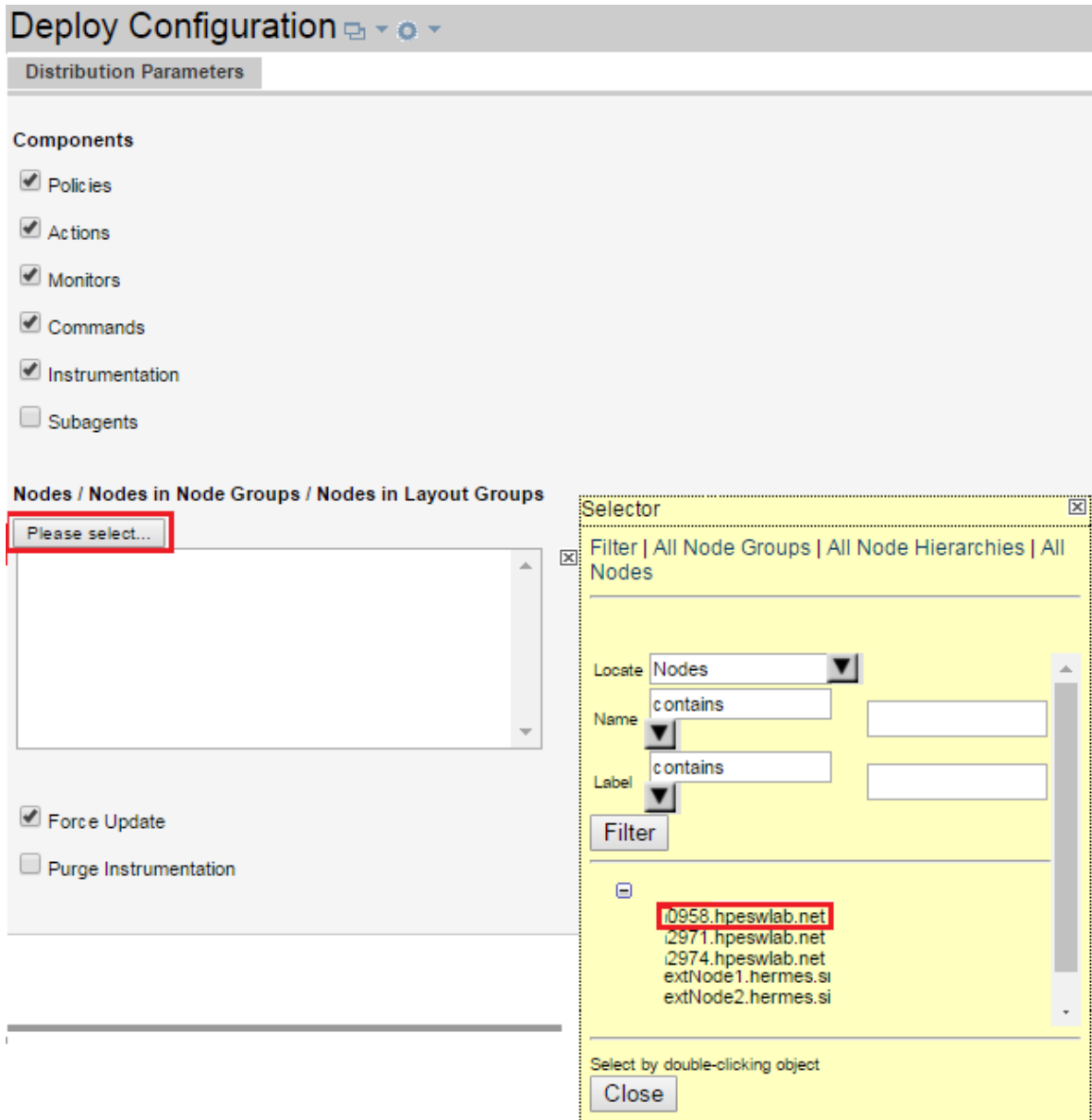


- Click **Deployment > Deploy Configuration**.

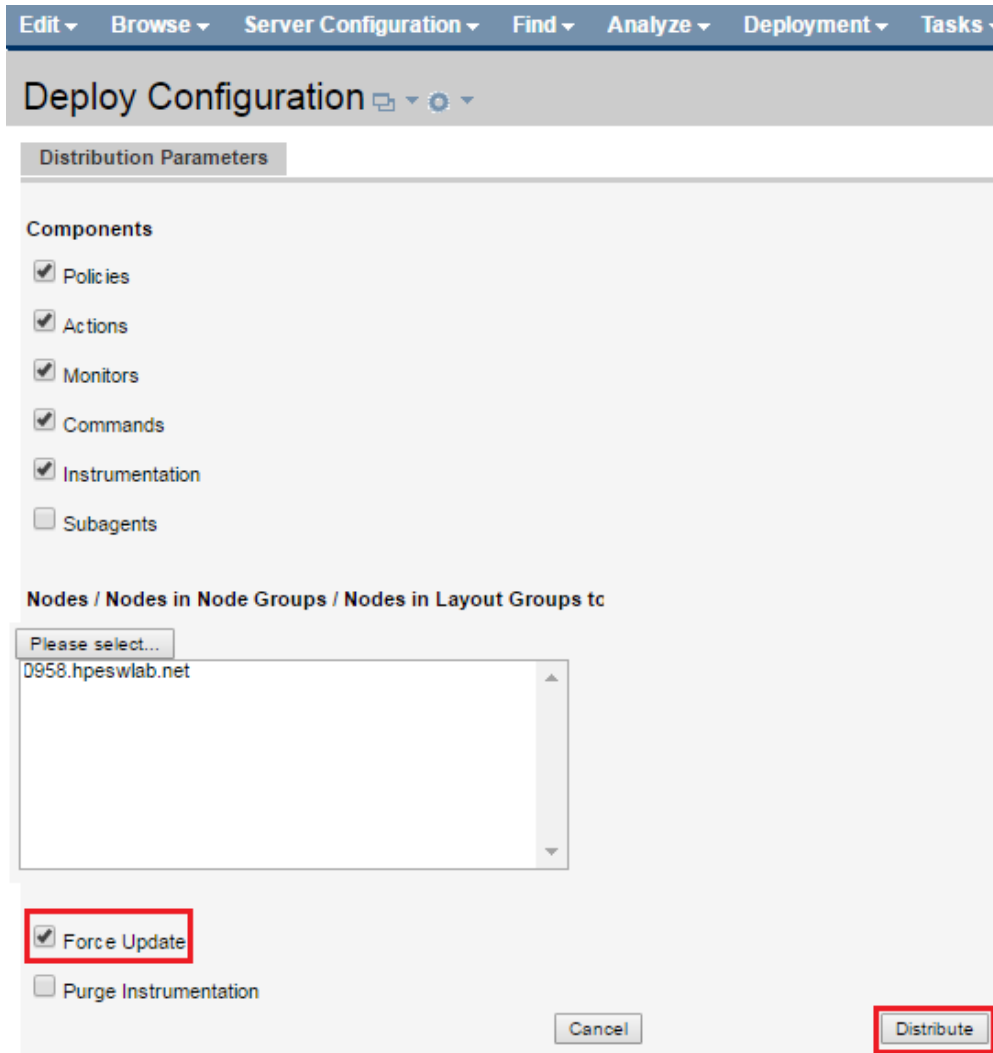


- On the Deploy Configuration page, click **Please select**.

The Selector pop-up window appears.

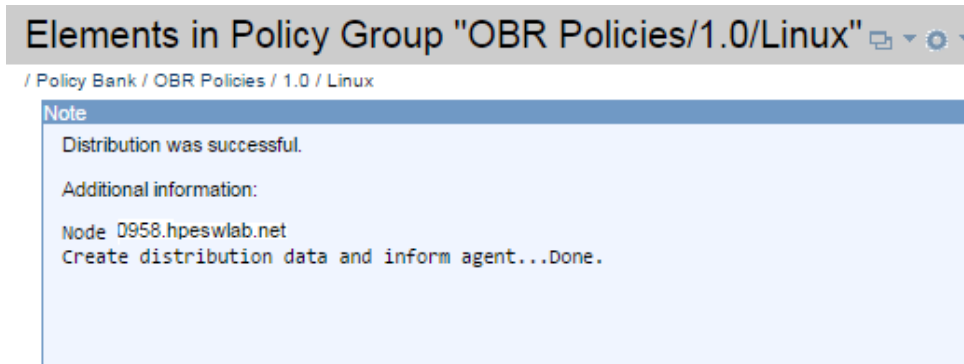


10. On the Selector pop-up, double-click the node/nodes to which you want to deploy the policies.
The selected nodes are listed in a box.
11. Select the **Force Update** check box and click **Distribute**.



Note: Select the **Force Update** to overwrite an existing policy template of any earlier version, on the selected node/nodes.

12. On successful deployment of policy templates, the following message is displayed:



The selected policy templates are successfully deployed on the selected nodes.

OMi Policies to Monitor OBR

An OBR policy template for Operations Manager i (OMi) is a set of configuration data for OBR to integrate into OMi. These policy templates define the details of specific configuration and monitoring tasks. Through these policies, OMi monitors all the OBR services on Windows and Linux, including the Vertica service on Linux.

OMi policies for OBR are available in the OBR installation directory in the following location:

```
$PMDB_HOME/scripts/OMiPolicies/OBR_OMi_Monitoring_policies.zip
```

The `OBR_OMi_Monitoring_policies.zip` file contains OBR policy templates for Linux and Windows.

This document lists the OBR-OMi policies for Linux and Windows, and provides step-by-step instructions to import and deploy these policies.

Prerequisites

Note: The OMi policy templates are supported on OBR 10.01 or later versions only.

Before importing OBR policies to OMi, ensure that the following prerequisites are met:

- Ensure that Agent is installed on OBR.
- Performed the steps required for OBR-Agent coexistence, and request the certificate and apply it.

For more information about coexistence set up and certificate, see *Operations Bridge Reporter Interactive Installation Guide*.

- Add the OBR-Agent node to the OMi server.

For more information, see *Operations Bridge Reporter Configuration Guide*.

OBR Services Monitored by OMi

OMi monitors the following OBR Linux services using the OBR-OMi policies:

OBR Linux Services

- HPE_PMDB_Platform_Administrator
- HPE_PMDB_Platform_Collection
- HPE_PMDB_Platform_DB_Logger
- HPE_PMDB_Platform_IA
- HPE_PMDB_Platform_IM
- HPE_PMDB_Platform_JobManager
- HPE_PMDB_Platform_NRT_ETL
- HPE_PMDB_Platform_Orchestration
- HPE_PMDB_Platform_PostgreSQL
- HPE_PMDB_Platform_TaskManager
- HPE_PMDB_Platform_Vertica
- TrendTimer

OBR Windows Services

The policy rules for all the following Windows services are under a single policy:

- HPE_PMDB_Platform_Administrator
- HPE_PMDB_Platform_Collection
- HPE_PMDB_Platform_DBLogger
- HPE_PMDB_Platform_IA
- HPE_PMDB_Platform_IM
- HPE_PMDB_Platform_JobManager
- HPE_PMDB_Platform_NRT_ETL
- HPE_PMDB_Platform_NRT_ETL_UTILITY
- HPE_PMDB_Platform_Orchestration

- HPE_PMDB_Platform_PostgreSQL
- HPE_PMDB_Platform_TaskManager
- HPE_PMDB_Platform_Timer

OMi Policies for OBR

This section lists OMi policies that are used for monitoring OBR services on Linux and Windows systems.

Measurement Threshold Policies

Measurement threshold policies enable you to monitor performance metrics from various sources. You can configure policies to create events and launch commands whenever a performance metric crosses a threshold that you specify.

All the OBR Linux service monitoring policies are categorized under Measurement Threshold.

Following are the policies to monitor OBR services on a Linux system:

- OBR_LinuxAdministrationService
- OBR_LinuxCollectionService
- OBR_LinuxDBLoggerService
- OBR_LinuxIAService
- OBR_LinuxIMService
- OBR_LinuxJobManagerService
- OBR_LinuxNRT_ETLService
- OBR_LinuxOrchestrationService
- OBR_LinuxTaskManagerService
- OBR_LinuxTimerService
- OBR_LinuxPostgreSQLService
- OBR_LinuxVerticaService

Service/Process Monitoring Policies

Service/process monitoring policies enable you to monitor the status of services (on Windows) and processes (on any operating system that the Operations Agent supports). You can configure the policies to create events and launch commands when a change occurs in either the status of a service or the number of running processes. Policies for OBRWindows services are listed under Service/Process Monitoring in OMi.

- OBR_Windows_Services

For more information about OMi Measurement Threshold and Service/Process Monitoring policies, see *OMi Administration Guide*.

Importing and Deploying Policies

OMi policies for OBR are available in the OBR installation directory in the following location:

```
$PMDB_HOME/scripts/OMiPolicies/OBR_OMi_Monitoring_policies.zip
```

The `OBR_OMi_Monitoring_policies.zip` file contains OBR policy templates for Linux and Windows.

You can download or copy the policy template Zip file to your desktop and import it to OMi system.

Importing Policies to OMi System

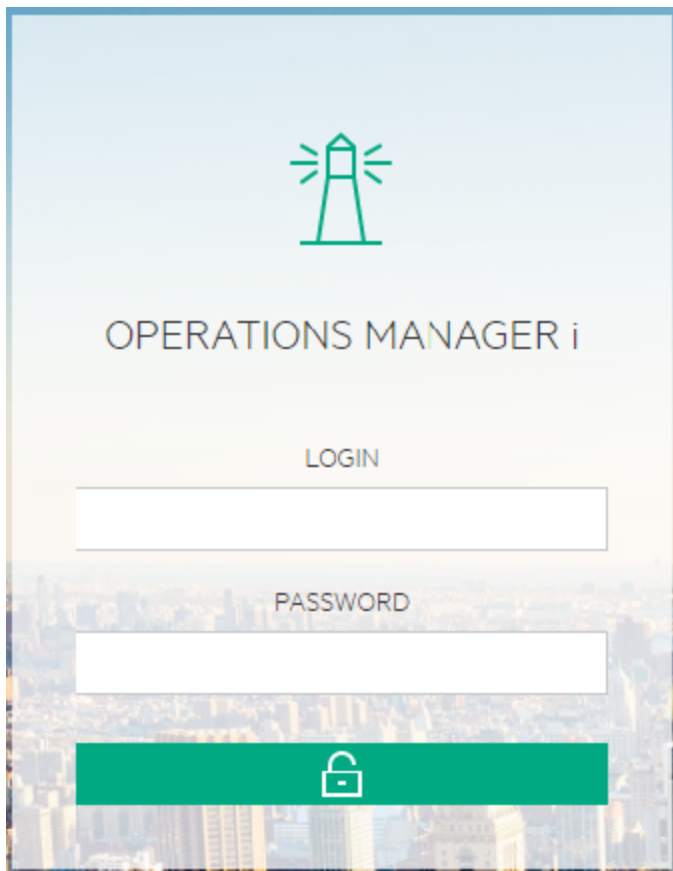
1. In a web browser, type the following URL:

```
https://<server_name>.<domain_name>/omi
```

where

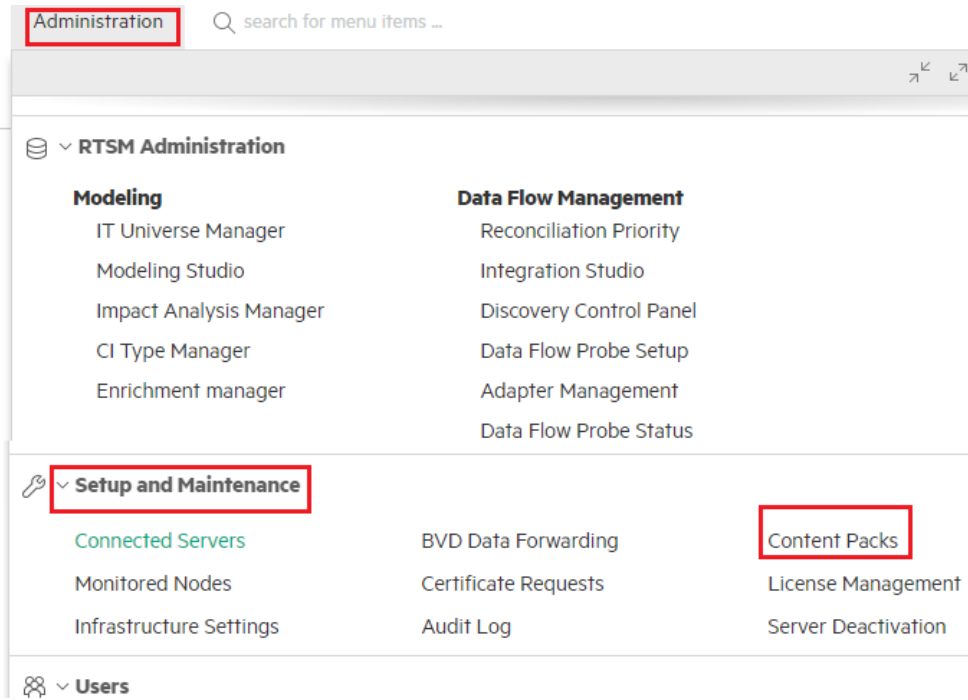
`<server_name>` and `<domain_name>` represent the Fully Qualified Domain Name (FQDN) of the OMi server.

2. Log on to OMi Administration Console with permission to deploy policy templates.

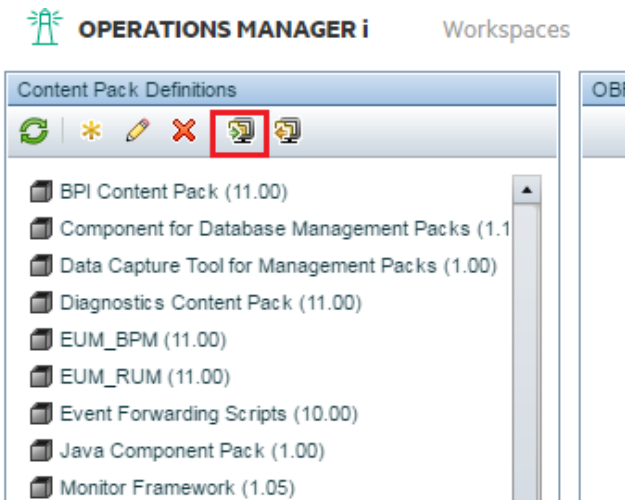


Note: All secondary managers of a node have permission to deploy policies to the node. For details about permissions, see the *OMi Administration Guide*.

3. On OMi system, go to **Administration > Setup and Maintenance > Content Packs**.

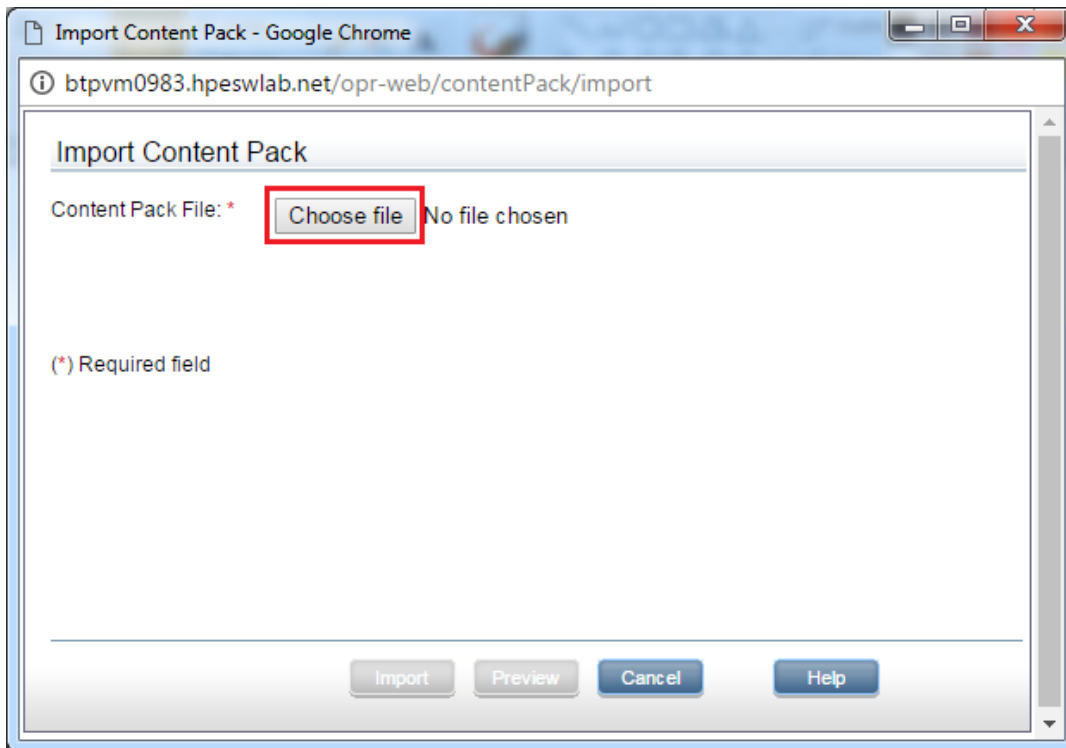


4. Click the **Import Content pack Definitions** icon.

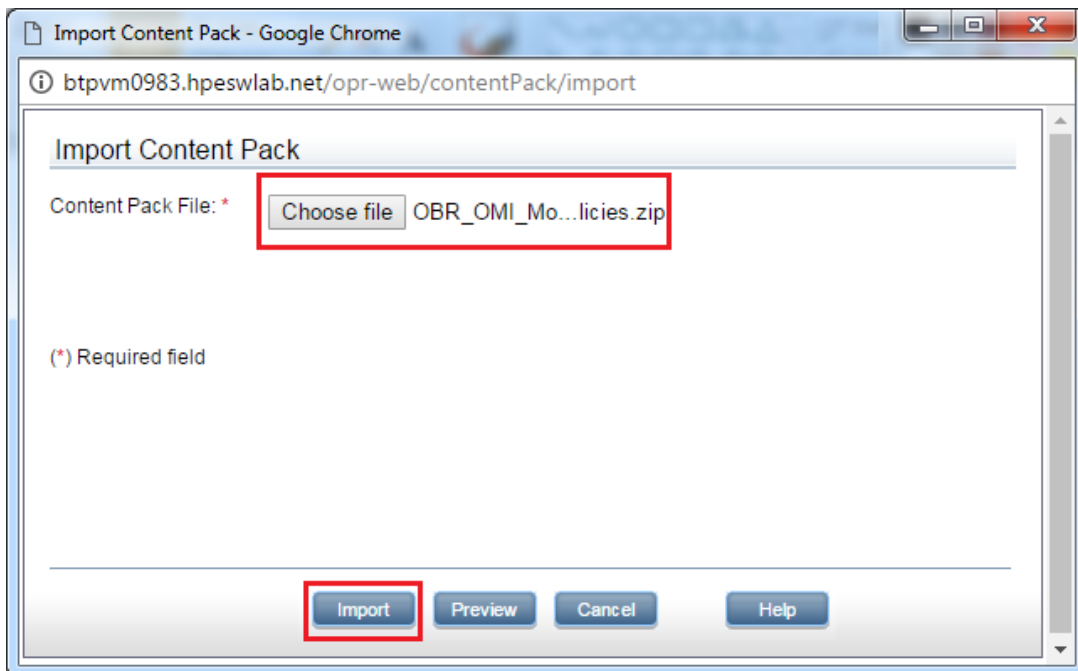


The *Import Content Pack* page appears.

5. Click **Choose file** Select the content pack Zip file from your system and click **Open**.



6. Click **Import** to import the policies to the OMi system.



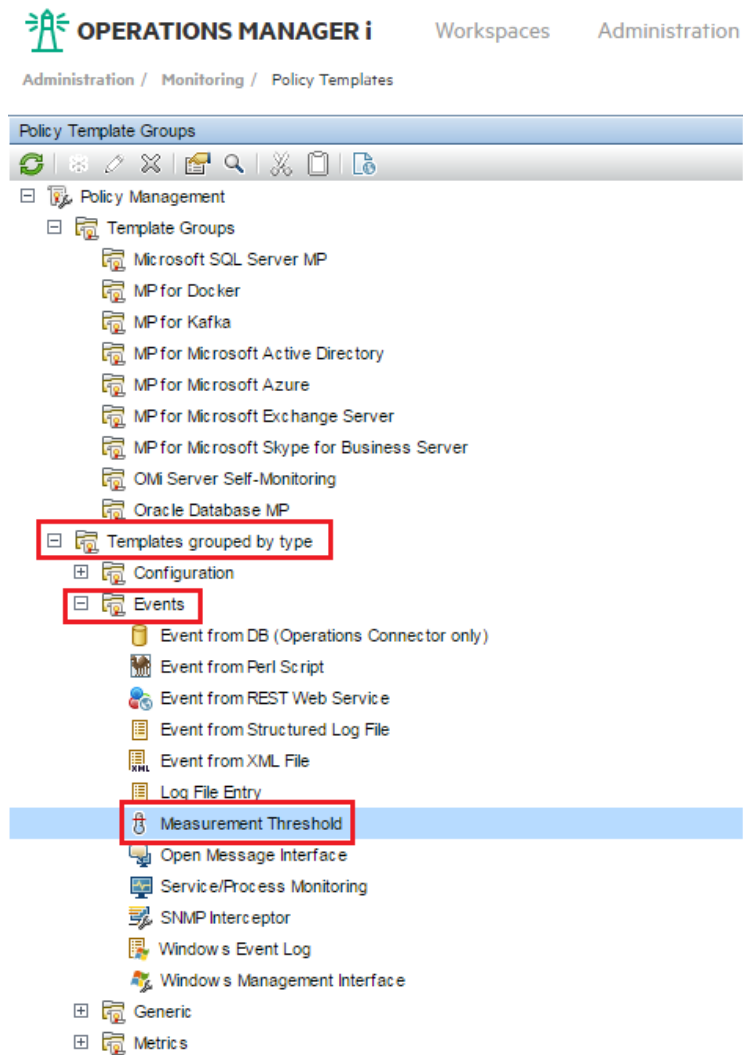
After importing the OBR-OMi policy content packs, you can view all the policies on the OMi Administration page under **Administration > Monitoring > Policy Template**.

On successful import to OMi system, OBR policies are organized under Policy Template Groups in OMi Administration console.

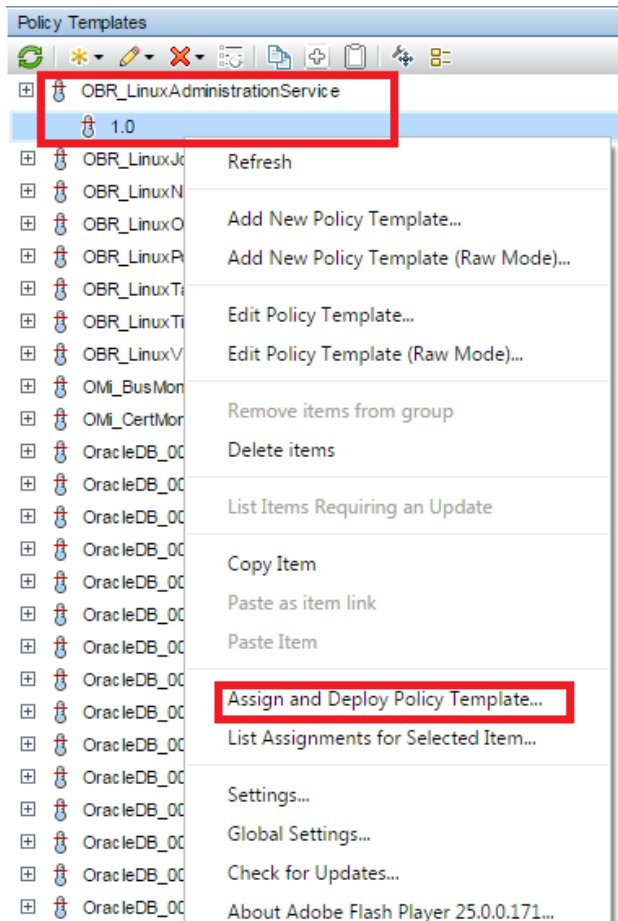
- The OBR service policies for Linux are available under **Measurement Threshold**
- The Windows services and database policies, and Linux database policies are organized under **Service/Process Monitoring**.

Deploying Linux Policy Templates

1. On OMi Administration console, go to **Administration > Monitoring > Policy Templates**.
2. Select the policy template group and policy type.

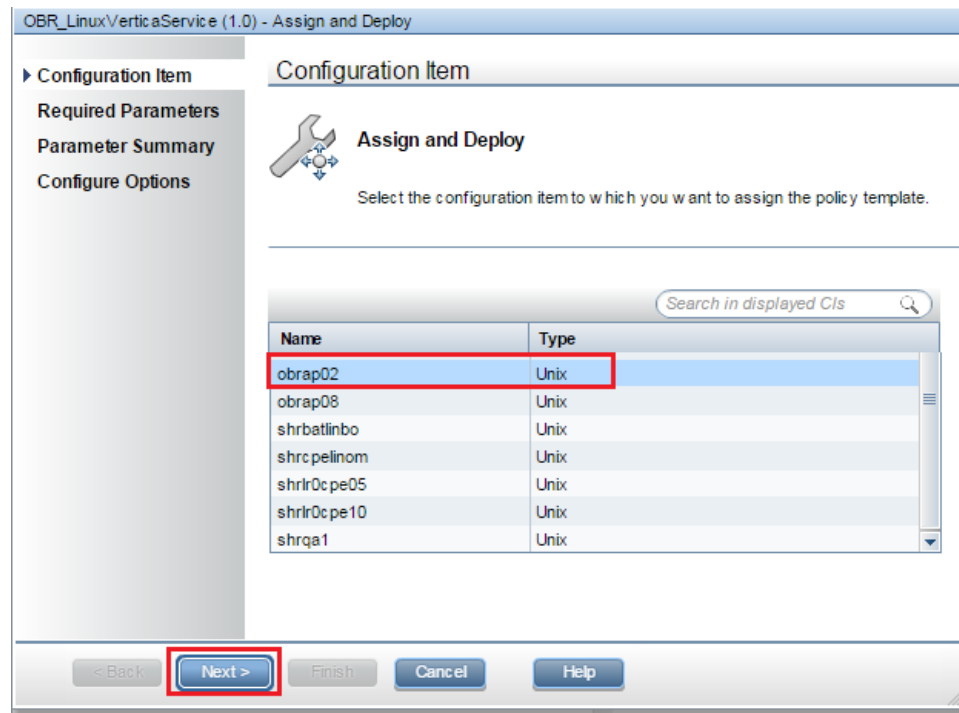


3. Select the policy and right-click on the version of the policy you want to deploy.



4. Select **Assign and Deploy the Policy Template**. The Assign and Deploy pop-up appears. Perform the following steps:

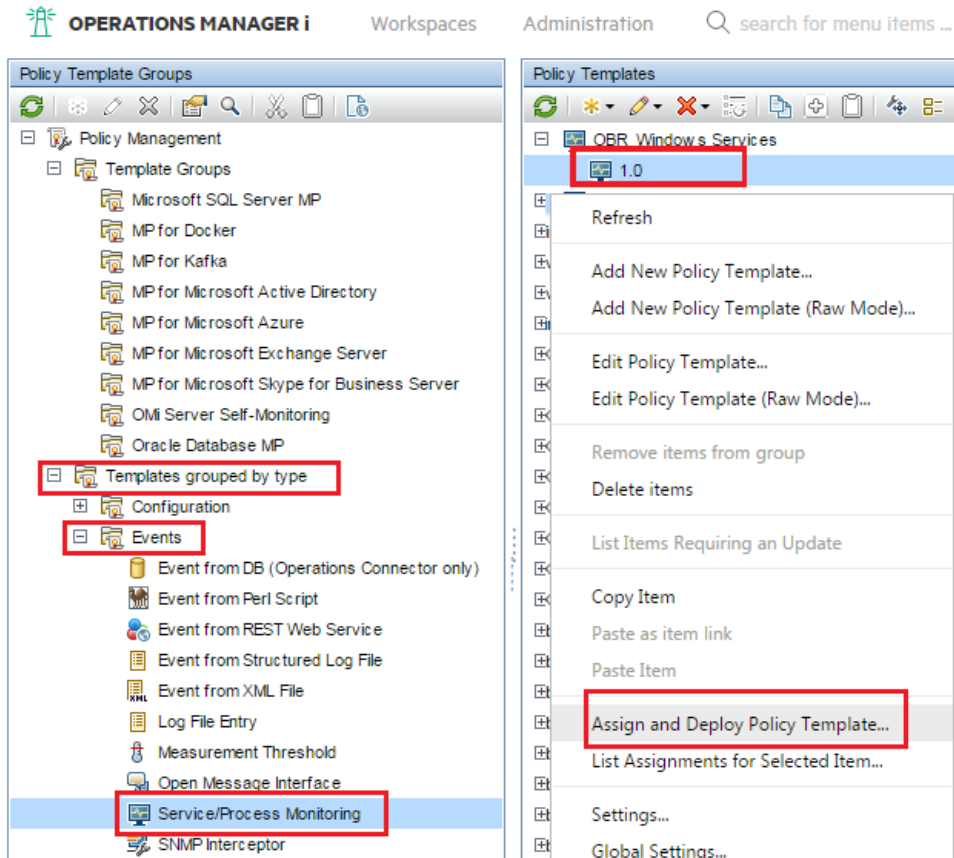
- a. i. Select the node where you want to deploy the policy template and click **Next**.



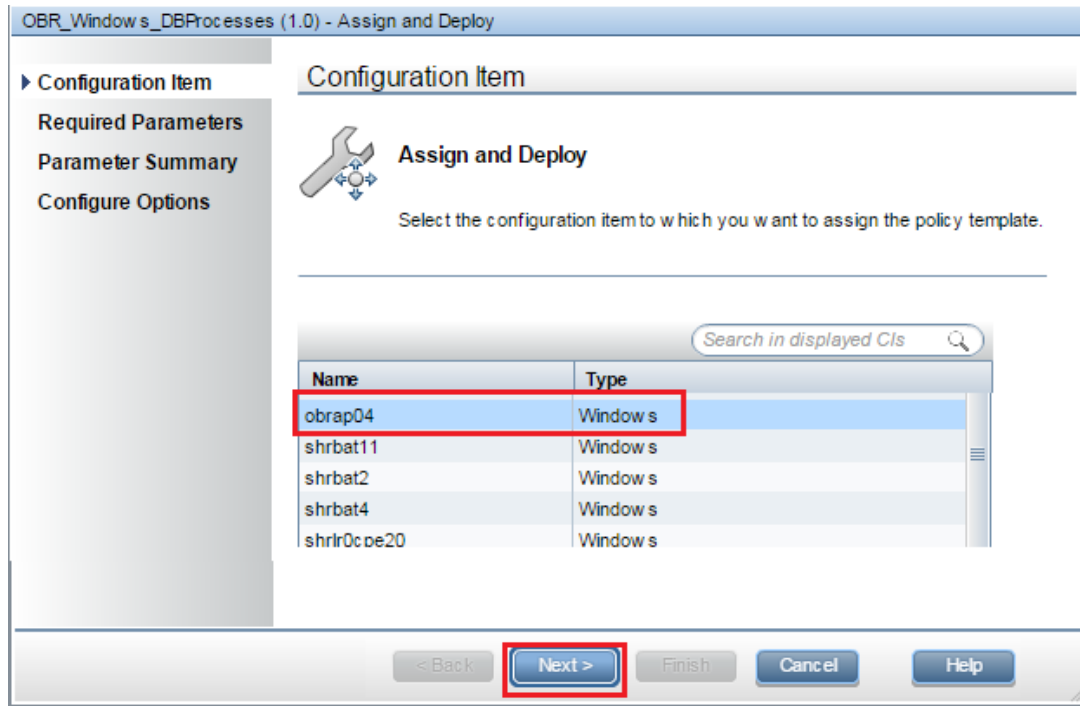
- ii. Select and edit the parameter values if required, and click **Next**.
- iii. Select the Configuration Options and click **Finish**.

Deploying Windows Policy Templates

1. On OMi Administration console, go to **Administration > Monitoring > Policy Templates**.
2. Select the policy template group and policy type.
3. Select the policy and right-click on the version of the policy you want to deploy.



4. Select **Assign and Deploy the Policy Template**.
5. Select the node where you want to deploy the policy template and click **Next**.



6. Select and edit the parameter values if required, and click **Next**.
7. Select the Configuration Options and click **Finish**.

The policy templates are deployed to the selected nodes.

OBR Log File Inventory

OBR uses the log4j API for most of its logging purposes. It maintains a log file for each of its modules, such as collector, loader, metadata repository, internal monitoring, Administration Console, package manager, and data processing. These log files are placed in the %PMDB_HOME%\log folder. OBR also maintains an application-wide log file that contains error messages from all the modules. These log files can be used for troubleshooting purposes.

The log files available in OBR are as follows:

Log File	Location on Disk	Module	Description
AdministratorService.log	Windows: %PMDB_HOME%\log\ Linux: \$PMDB_HOME/log/	Administrator Service	Contains log messages related to the service PMDB Platform Administrator.
aggregate.log	Windows: %PMDB_HOME%\log\ Linux: \$PMDB_HOME/log	Aggregate	Contains summarized log messages related to the data from the rate tables to the hourly, daily, and forecast tables, and from the hourly tables to the daily tables.
aggrgen.log	Windows:%PMDB_HOME%\log\ Linux:\$PMDB_HOME/log	Aggregate	Contains log messages related to aggregate script generation. Appender : aggrgenAppender
analyseStat.log	Windows:%PMDB_HOME%\log\ Linux:\$PMDB_HOME/log	Database	Contains log messages related to Vertica database maintenance.
audit.log	Windows: %PMDB_HOME%\log\ Linux: \$PMDB_HOME/log/	trendproc, trendtimer	Records the start time, end time, and duration of back-end processes. When a process

Log File	Location on Disk	Module	Description
			begins, the file assigns a Process Identification (PID) that also records when the process ends, showing that the PID for the process was terminated.
autopassJ.log	Windows: %PMDB_HOME%\log\ Linux: \$PMDB_HOME/log/	OBR Licensing	Contain messages for license-related tasks. Appender : AutopassAppender
backend.log	Windows: %PMDB_HOME%\log\ Linux: \$PMDB_HOME/log/	trendproc, trendtimer	Contains log information for all steps in the data processing job. Appender : backendLogAppender
BOEInstall_0.log BusinessObjects.12.7.log	Windows: <SAP BOBJ Install Directory>\Business Objects Enterprise 12.0\Logging\BOEInstall_0.log Linux: /opt/HP/BSM/BO/setup/logs	Business Objects	SAP BusinessObjects installation log files.
BSMRAbcservice.log	Windows: %PMDB_HOME%\log\ Linux: \$PMDB_HOME/log/	Orchestration	Contains log messages related to the service PMDB Platform Orchestration. Appender : abclogAppender
BSMRApp.log	Windows: %PMDB_HOME%\log\	NA	Application-wide log file that contains error

Log File	Location on Disk	Module	Description
	Linux: \$PMDB_ HOME/log/		messages from all the OBR modules except data processing. Appender : bsmrappender
BSMRCollectionService.log	Windows: %PMDB_ HOME%\log\ Linux: \$PMDB_ HOME/log/	Collector	Contains log messages related to the service PMDB Platform Collection.
BSMRDBLoggerService.log	Windows: %PMDB_ HOME%\log\ Linux: \$PMDB_ HOME/log/	Logger	Contains log messages related to the service PMDB Platform DB Logger.
bsmrfrontend.log	Windows: %PMDB_ HOME%\log\ Linux: \$PMDB_ HOME/log/	Administration Console	Contains log messages related to the Administration Console UI web application. Appender : BSMRFrontEndAppender
bsmrnim.log	Windows: %PMDB_ HOME%\log\ Linux: \$PMDB_ HOME/log/	Internal Monitoring	Contains log messages related to the internal monitoring of data processing job streams, Performance Management database (PMDB) platform, and Content Packs. Appender : BSMRIMAppender
BSMRIMService.log	Windows: %PMDB_ HOME%\log\ Linux: \$PMDB_ HOME/log/	Internal Monitoring	Contains log messages related to the service PMDB Platform IM.
catalina*.log	Windows: %PMDB_ HOME%\adminServer\1	Administrator Console	Contains log messages about the

Log File	Location on Disk	Module	Description
	ogs Linux: \$PMDB_ HOME/log/		Apache Tomcat server that is used by Administration Console and SAP BusinessObjects launch pad.
collections.log	Windows: %PMDB_ HOME%\log\ Linux: \$PMDB_ HOME/log/	Collector	Contains log messages related to the collection framework such as data sources configured collection, job scheduling, and maintenance. Appender: collectionAppender
collectStep.log	Windows: %PMDB_ HOME%\log\ Linux: \$PMDB_ HOME/log/	Collect	Contains log messages related to the collect step that moves data from the {PMDB_HOME} /collect directory to the {PMDB_HOME} /stage directory Appender: collectAppender
customer.log	Windows: %PMDB_ HOME%\log\ Linux: \$PMDB_ HOME/log/	Customer Enrichment	Contains log messages on customer enrichment. Appender: CustomerAppender
customgroup.log	Windows: %PMDB_ HOME%\log\ Linux: \$PMDB_ HOME/log/	Custom Group	Contains log messages related to importing of custom groups defined in an XML file. Appender: customgroupAppende r

Log File	Location on Disk	Module	Description
cpPatch.log	Windows: \${pmdb.home} /log/cppatch.log Linux: \$PMDB_ HOME/log/	Content Packs	Patch installation log file. Appender: cpPatchAppender
customgroup.log	Windows: %PMDB_ HOME%\log\ Linux: \$PMDB_ HOME/log/	Custom Group	Contains log messages related to importing of custom groups defined in an XML file. Appender: customgroupAppender
customscript.log	Windows: %PMDB_ HOME%\log\ Linux: \$PMDB_ HOME/log/	Custom Script	Contains log messages related to custom scripts defined for a data process in data warehouse. Appender: customscriptAppender
datetime.log	Windows: %PMDB_ HOME%\log\ Linux: \$PMDB_ HOME/log/	Date, Time management	Contains log messages related to date and time maintenance in data warehouse. Appender: datetimeAppender
dbcollector.log	Windows: %PMDB_ HOME%\log\ Linux: \$PMDB_ HOME/log/	Collector	Contains log messages related to database collection. Appender: dbCollectorAppender
dbdelete.log	Windows: %PMDB_ HOME%\log\ Linux: \$PMDB_ HOME/log/	Database	Contains log messages related to purging the data in the database as per

Log File	Location on Disk	Module	Description
	HOME/log/		retention rules. Appender : DbdeleteAppender
d1c.log	Windows: %PMDB_ HOME%\log\ Linux: \$PMDB_ HOME/log/	Dimension Life Cycle	Contains log messages related to management the Dimension Life Cycle. Appender : DLCAppender
downtime.log	Windows: %PMDB_ HOME%\log\ Linux: \$PMDB_ HOME/log/	Downtime	Contains log messages related to configuring downtime and enriching the performance data with configured downtime information. Appender : downtimeAppender
downtimeutility.1 og	Windows: %PMDB_ HOME%\log\ Linux: \$PMDB_ HOME/log/	Downtime	Contains log messages related to the reprocessing of downtime utility. Appender : downtimeutilityApp ender
DR.log	Windows: %PMDB_ HOME%\log\ Linux: \$PMDB_ HOME/log/	Disaster Recovery	Contains log messages related to Disaster Recovery.
dw_ abclauncher.log	Windows: %PMDB_ HOME%\log\ Linux: \$PMDB_ HOME/log/	Orchestration	Contains log messages related to job streams. Log messages specific to a process can be seen in the process-specific log file. For example, loader.log for the loader process.

Log File	Location on Disk	Module	Description
			Appender: ablauncher- RollingLogFileAppender
host-manager*.log	Windows: %PMDB_ HOME%\adminServer\logs Linux: \$PMDB_ HOME/log/	Administration Console	Contains log messages about the Apache Tomcat server that is used by Administration Console and SAP BusinessObjects launch pad.
enrich.log	Windows: %PMDB_ HOME%\log\ Linux: \$PMDB_ HOME/log/	Location Enrichment	Contains log messages on generic enrichments. Appender: enrichAppender
hpacollector.log	Windows: %PMDB_ HOME%\log\ Linux: \$PMDB_ HOME/log/	Collector	Contains log messages related to Performance Agent collection. Appender: hpaCollectorAppender
hpsacollector.log	Windows: %PMDB_ HOME%\log\ Linux: \$PMDB_ HOME/log/	Collector	Contains log messages related to Server Automation collection. Appender: hpsaAppender
IAEngine.log	Windows: %PMDB_ HOME%\log\ Linux: \$PMDB_ HOME/log/	Internal Alerting	Contains log messages related to Internal Alerts. Appender: iaEngineLogAppender
IAEvent.log	Windows: %PMDB_ HOME%\log\ Linux: \$PMDB_ HOME/log/	Internal Alerting	Contains log messages related to

Log File	Location on Disk	Module	Description
	Linux: \$PMDB_ HOME/log/		Internal Alerts. Appender: iaEventLogAppender
License.log	Windows: %PMDB_ HOME%\log\ Linux: \$PMDB_ HOME/log/	License	Contain messages for license-related tasks. Appender: licenseAppender
loader.log	Windows: %PMDB_ HOME%\log\ Linux: \$PMDB_ HOME/log/	Loader	Contains log messages related to data loading from the stage area to the data store.
localhost*.log	%PMDB_ HOME%\adminServer\logs	Administration Console	Contains log messages related to Administration Console and SAP BusinessObjects launch pad Server Access.
location.log	Windows: %PMDB_ HOME%\log\ Linux: \$PMDB_ HOME/log/	Location Enrichment	Contains log messages from location enrichment. Appender: LocationAppender
manager*.log	%PMDB_ HOME%\adminServer\logs	Administration Console	Contains log messages related to Administration Console and SAP BusinessObjects launch pad Server Access.
mapperStep.log	Windows: %PMDB_ HOME%\log\ Linux: \$PMDB_ HOME/log/	Mapper	Contains log messages related to transformation of collected data. Transformation includes pivot transform, rows

Log File	Location on Disk	Module	Description
			filtering, and so on. Appender : mapperAppender
metadata.log	Windows: %PMDB_ HOME%\log\ Linux: \$PMDB_ HOME/log/	Metadata Repository	Contains log messages related to metadata repository persistence, access, and modification. Appender : MetadataRepository Appender
mybsm.log	Windows: %PMDB_ HOME%\log\ Linux: \$PMDB_ HOME/log/	MyBSM Integ ration	Contains log messages related to launching of OBR reports from the MyBSM console.
nodefilter.log	Windows: %PMDB_ HOME%\log\ Linux: \$PMDB_ HOME/log/	Collection	Contains log messages related to the node filters.
OvInstallerLog.txt	%temp%\..\HPOvInsta ller\HP-SHR_ 9.30\HP-SHR_9.30_ <timestamp>_ HPOvInstallerLog.ht ml %temp%\..\HPOvInsta ller\HP-SHR_ 9.30\HP-SHR_9.30_ <timestamp>_ HPOvInstallerLog.txt.	Installer	Contains log messages related to OBR installer. This folder also stores log files for each component of OBR such as LCore components, OVPerl, and so on.
packagemanager.log	%PMDB_ HOME%\log\packagema nager.log	Package Manager	Contains log messages related to Content Pack deployment. Appender : pkgmgrAppender

Log File	Location on Disk	Module	Description
pollerDataProcessor.log	Windows :%PMDB_HOME%\log\ Linux :\$PMDB_HOME/log/	Collector	Contains logs related to data download from remote collectors to OBR server.
Postgresql-<date and time>.log	<Postgres_install_directory>/data/pg_log	PostgreSQL	PostgreSQL log file information.
postinstallconfig.log	Windows :%PMDB_HOME%\log\ Linux :\$PMDB_HOME/log/	Post Install	Contains log messages related to OBR post-install configuration. Details on database schema creation on Vertica, details on OBR Management database schema creation on Postgresql. Appender: postinstallAppender
reconcilStep.log	Windows :%PMDB_HOME%\log\ Linux :\$PMDB_HOME/log/	Reconciliation	Contains log messages related to reconciliation of collected data. Appender: reconcileAppender
remotepoller.log	Windows :%PMDB_HOME%\log\ Linux :\$PMDB_HOME/log/	Remote Collector	Contains log messages related to configuration and metadata synchronization and data transfer between OBR server and the different collectors configured. Appender: remotepollerAppender
reload.log	\${pmdb.home}	Reload	Log file for the contrib

Log File	Location on Disk	Module	Description
	/log/reload.log		utility (reload.exe) that handles reload of failed data. Appender: reloadAppender
shiftmaint.log	Windows: %PMDB_ HOME%\log\ Linux: \$PMDB_ HOME/log/	Shift Management	Contains log messages related to populating the shift fact tables based on shift configured in Administration Console. Appender: shiftMaintAppender
sis_aggregate.log	Windows: %PMDB_ HOME%\log\ Linux: \$PMDB_ HOME/log/	SiteScope Collector	Contains logs from the SiteScope aggregate process that runs as part of collection service Appender: sisAggrAppender
siscollector.log	Windows: %PMDB_ HOME%\log\ Linux: \$PMDB_ HOME/log/	SiteScope Collector	Contains logs from the SiteScope collector (for both GDI and DA) Appender: sisCollectorAppender
sqlexecutor.log	Windows: %PMDB_ HOME%\log\ Linux: \$PMDB_ HOME/log/	Sql Executor	Contains logs related to the custom SQL executions. Appender: sqlExecutorAppender
stage.log	Windows: %PMDB_ HOME%\log\ Linux: \$PMDB_ HOME/log/	Stage	Contains log messages related to data staging, and purging of staging area.

Log File	Location on Disk	Module	Description
			Appender: stageAppender
stderr*.log	%PMDB_ HOME%\adminServer\logs	Administrator Console	Contains messages logged to standard error by the Tomcat server.
stdout*.log	%PMDB_ HOME%\adminServer\logs	Administrator Console	Contains messages logged to standard output by the Tomcat server.
topologycollector.log	Windows: %PMDB_ HOME%\log\ Linux: \$PMDB_ HOME/log/	Collector	Contains log messages related to topology collection. Appender: topologyCollectorAppender
trend.log	Windows: %PMDB_ HOME%\log\ Linux: \$PMDB_ HOME/log/	Aggregate, trendproc, trendtimer	Contains messages for all back-end processes of OBR. Each message specifies the start and end time for the logged process.
TrendTimerService.log	Windows: %PMDB_ HOME%\log\ Linux: \$PMDB_ HOME/log/	Trend Timer	Contains log messages related to the OBR timer service.
VC_collector/collector.log	\${pmdb.home} /log/VC_collector/collector.log	VC Collector	VC Collector logfiles Appender: vcAppender

OBR service log files

All OBR services have a log file associated with it. These log files contain console error messages. These log files are not controlled through log4j API and are overwritten during service startup.

Log file	Service
BSMRService.log	Log file for the Performance Management Database (PMDB) ¹ Platform Administrator Service.
BSMRCollectionService.log	Log file for the PMDB Platform Collection Service.
BSMRDBLoggerService.log	Log file for the PMDB Platform DB Logger Service.
BSMRIMService.log	Log file for the PMDB Platform IM Service.
Trend.log	Log file for PMDB Platform Timer service
Postgresql-<date and time>.log	Log file for the OBR PostgreSQL service.

Log file message format

All entries in the log files have the following format

Format	Description
Timestamp	The timestamp field represents the time the log entry occurred. It uses a 24-hour clock with the YYYY-MM-DD hh:mm:ss,nnn format.
Severity	The severity field is the severity level for the log entry. The severity levels are DEBUG, INFO, WARN, ERROR, FATAL.
Class_name	The fully qualified class name of the caller issuing the logging request.
Method_name	The method name where the logging request was issued.
Message	The application-supplied message associated with the logging event.

¹A common repository of the health, performance, and availability data of the IT elements in your environment. The platform data store contains performance data that is processed, transformed, and aggregated in the data store, based on the metadata specifications in the content packs.

Changing Default Passwords

This section guides you to change the default passwords for the following:

[Administration Console log on password](#)

[Vertica database password](#)

[Management database password](#)

[SAP BusinessObjects database password](#)

Administration Console Log on Password

If you want to change the password for the default Administrator user name, perform the following steps:

1. In the Administrator Console, click **Additional Configurations > Reporting Platform**.
The Reporting Platform page is displayed.
2. Click **Launch CMC**. The Log On to the Central Management Console (CMC) page is displayed.
3. On the Central Management Console log on screen, in the **User Name** field, type *Administrator* and *<Administration Console Password>* in the **Password** field.
4. Click **Log On**. The CMC Home screen appears.
5. Click **Users and Groups**. The Users and Groups screen appears.
6. On the right pane, double-click **Administrators**.
7. Right-click **Administrator** and then click **Properties**. The Account Manager dialog box appears.
8. In the navigation panel, Click **Account Manager**.
9. Under **Enterprise Password Settings**, in the **Password** field, type a new password.
10. In the **Confirm** field, retype the password to confirm it. You can change the Administrator user name, if required, and specify other necessary details on this screen.
11. Click **Save & Close** to accept the changes.
12. Click **Log Out** to exit the Central Management Console.

Note: This task is valid only if OBR is installed on the system.

Vertica Database Password

If you want to change the password for the default Vertica database administrator user through Administration Console, perform the following steps:

1. In the Administration Console, click **Additional Configurations > Vertica Database & Time Zone**.

The Vertica Database & Time Zone page opens.

2. Click **Change Password**.

The Change Password dialog box opens.

3. In the **Change Password** dialog box, type the database password details:

Field	Description
Old Password	Enter the existing database administrator password.
New Password	Enter a new password. The password should be an alphanumeric value and less than 25 characters in length.
Confirm New Password	Retype the new password for confirmation purposes.

4. Click **OK**.

A `Password Successfully Changed` message appears in the Information message panel indicating that the password has been successfully changed.

5. From the command prompt, go to location `{PMDB_HOME}/bin`.

6. Open the `HPE_PMDB_Platform_Vertica` file.

7. In `SECURITY`, type the new password. Save and exit the file.

8. Check if the Vertica service is running, go to `etc/init.d` and run the command:

```
service HPE_PMDB_Platform_Vertica start
```

If the service is stopped, start the service by running the following command:

```
service HPE_PMDB_Platform_Vertica status
```

Management Database Password

To change default password for PostgreSQL database administrator - *postgres* user:

If you want to change the password for the default PostgreSQL database administrator user, perform the following steps:

On Windows:

1. Go to **Start > Administrative Tools > Computer Management**.

The Computer Management page appears.

2. Go to **System tools > Local Users and Groups > Users**.

3. Right-click **postgres** and click **Set Password**.

A warning message appears.

4. Click **Proceed**. The **Set Password for postgres** appears.

5. Type the new password in the **New Password**. Retype the password in **Confirm password** for confirmation purpose.

6. Click **OK**.

4. Open the services window.

5. Right-click on **HPE_PMDB_Platform_PostgreSQL** and select **Properties**.

The HPE_PMDB_Platform_PostgreSQL Properties page appears.

6. Click the **Log On** tab.

7. Provide the password provided in [step 5](#) and retype it to confirm the same.

8. Click **OK**.

On Linux:

1. Log on to the command line console.

2. Run the following command:

```
passwd postgres
```

3. Type the new password and press Enter.

To change default password for *Postgres - pmdb_admin* user:

If you want to change the password for the default Management database user, perform the following steps:

1. In the Administration Console, click **Additional Configurations > Management Database**.
The Management Database page appears.
2. Click **Change Password**.
The Change Password dialog box appears.
3. In the **Change Password** dialog box, type the database password details:

Field	Description
Old Password	Enter the existing management database administrator password.
New Password	Enter a new password. The password should be an alphanumeric value and less than 25 characters in length.
Confirm New Password	Retype the new password for confirmation purposes.

4. Click **OK**.
A **Password Successfully Changed** message appears in the Information message panel indicating that the password has been successfully changed.

SAP BusinessObjects Database Password

OBR is installed with a default SAP BusinessObjects database password. Perform this task to change the default SAP BusinessObjects database password.

After installing OBR, follow these steps to modify the default password of the database embedded with SAP BusinessObjects:

On Windows:

Task 1: Change the password using `updateSQLAnywhereDB` command

1. Log on to the system as administrator.
2. From the command line console go to the path `%PMDB_HOME%\lib`.
3. Run the command `perl updateSQLAnywhereDB.pl`

4. Type the new password and press Enter.

Note: Ensure that the first character of the password is not a number. The password should not have any space and special characters.

5. Retype the password to confirm.

Task 2: Update the Central Configuration Manager

1. From the Start, type **Central Configuration Manager** in **Search**. The Central Configuration Manager window appears.
2. Select the Server Intelligence Agent (SIA), right-click and select **Stop**. Wait for the SIA to stop.
3. Right-click and select **Properties** and then click the **Configuration** tab.
4. In the **Configuration** tab, you may see a error pop up click **OK** to proceed, and then click **Specify** of BOE120.
5. Click on the **Update Data Source Settings** .
6. Click **OK**.
7. Select **SQL Anywhere (ODBC)** and click **OK**.
8. The Select Data Source window appears. Select **Machine Data Source** tab.
9. Double-click **BI4_CMS_DSN** and provide the password that was changed using the updateSQLAnywhereDB.plcommand and click **OK**.
10. Enter Cluster Key as 1ShrAdmin.
11. Repeat from step 5 to 10 for BI4_Audit_DSN database by selecting the **BI4_Audit_DSN**.
12. In the Central Configuration Manager window, select the SIA, right-click and select **Start**.

Log on to the SAP BusinessObjects BI Launch pad and check if you are able to access the reports.

On Linux:

Task 1: Change the password using updateSQLAnywhereDB command

1. Log in to the system as root.
2. From the command line console go to the path \$PMDB_HOME/lib.
3. Run the command per1 updateSQLAnywhereDB.pl
4. Type the new password and press Enter.

Note: Ensure that the first character of the password is not a number. The password should not have any space and special characters.

5. Retype the password to confirm.

Log on to the SAP BusinessObjects BI Launch pad and check if you are able to access the reports.

Task 2: Synchronize database password with SAP BusinessObjects

Perform the following steps on your SAP BusinessObjects system:

1. Log on to SAP BusinessObjects system command prompt.
2. Switch to shrboadmin user using the following command:

```
su - shrboadmin
```

3. Run the following command to go to \$BOBJEDIR directory.

```
cd $BOBJEDIR
```

4. Run the following command:

```
.cmsdbsetup.sh
```

5. Type OBR as input when you are prompted to specify the node name.

The following message appears:

The node will be stopped. Do you want to continue?

6. Type 3 and press Enter to continue.

The following screen appears:

```
SAP BusinessObjects
Current CMS Data Source: BI4_CMS_DSN_1452664266

err: Error: Failed to get cluster name. (STU00165)
err: Error description: SAP BusinessObjects BI platform CMS: Unable to connect to the CMS system
ID or password

Current cluster key: [[8t2h5f7UfnlE2JbhkbRNUg]]

update (Update Data Source Settings)
reinitialize (Recreate the current data source)
copy (Copy data from another Data Source)
change cluster (Change current cluster name)
change cluster key (Change current cluster key)

[update(6)/reinitialize(5)/copy(4)/change cluster(3)/change cluster key(2)/back(1)/quit(0)]
-----
[update]6
```

7. Type 6 and press Enter to update.

The following message appears.

```
The destination data source must contain deployment information for this cluster.
Do not use this option for clustering with a different CMS cluster.
Refer to the administration guide for details on CMS clustering workflows.
Do you want to continue?
[yes (1) /no (0)] [no]1
```

8. Type 1 and press Enter to continue.
9. Type 2 to select SQLAnywhere as shown here:

```
-----
SAP BusinessObjects

Specify Source CMS database connection information.

Select the type of database connection from the following:
[SAPHANA (8) /Oracle (7) /DB2 (6) /Sybase (5) /MySQL (4) /MaxDB (3) /SQLAnywhere (2) /back (1) /quit (0)]
-----
[SAPHANA]2
```

10. Enter the ODBC data source name (DSN) from the following file:
\$BOBJEDIR/enterprise_xi40/odbc.ini

The DNS name starts with BI4_CMS_DSN_<number>; for example, BI4_CMS_DSN_1452664266 as shown in the following image:

```
[shrboadmin@vm06687 ~]$ cd /opt/HP/BSM/BOE4/sap_bobj/enterprise_xi40/
[shrboadmin@vm06687 enterprise_xi40]$ vi odbc.ini

[ODBC Data Sources]
BI4_CMS_DSN_1452664266=SQLAnywhere 12.0
BI4_Audit_DSN_1452664266=SQLAnywhere 12.0

[BI4_CMS_DSN_1452664266]
UID=dba
DatabaseName=BI4_CMS
ServerName=BI4_1452664266
Host=localhost:2638
Driver=/opt/HP/BSM/BOE4/sqlanywhere/lib64/libdbodbc12.so

[BI4_Audit_DSN_1452664266]
UID=dba
DatabaseName=BI4_Audit
ServerName=BI4_1452664266
Host=localhost:2638
Driver=/opt/HP/BSM/BOE4/sqlanywhere/lib64/libdbodbc12.so
```

11. Type dba as the user name when prompted.
12. Type the new password created in [Task 1: Change the password using updateSQLAnywhereDB command](#).

The new password is synced with SAP BusinessObjects.

Send documentation feedback

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

Feedback on Administration Guide (Operations Bridge Reporter 10.21)

Just add your feedback to the email and click send.

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

We appreciate your feedback!