



Operations Bridge Reporter

Software Version: 10.22
Windows® and Linux operating systems

Configuration Guide

Document Release Date: December 2017
Software Release Date: December 2017


Hewlett Packard
Enterprise

Legal Notices

Warranty

The only warranties for Seattle SpinCo, Inc and its subsidiaries ("Seattle") 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. Seattle shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Except as specifically indicated, valid license from Seattle 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 EntIT Software LLC, a Micro Focus company

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.

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 HPE SW 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>.

Contents

Part I: OBR Overview and Planning	9
Revision History	9
Chapter 1: Configuration Planning	12
Know your Deployment Scenarios	12
Business Service Management/Application Performance Management/Operations Manager i	12
Operations Manager (OM)	15
VMware vCenter	16
Other Deployments	17
Know the Data Sources	18
Determine the Readiness	19
Licensing Requirement for OBR	20
Licenses to Use (LTUs)	21
Obtaining a Permanent License Key	23
Installing the Permanent License Key	24
SAP BusinessObjects License Reactivation	26
Part II: Configuring OBR	28
Chapter 2: Post-Install Configuration	29
Configuration Wizard	31
Task 1: Launching the Administration Console	32
Task 2: Creating the Vertica Database Schema	34
Creating Database Schema for Co-located Vertica	35
Creating Database Schema for Remote Vertica	39
Task 3: Creating the Management Database User Account	51
Task 4: Configuring the Remote Collectors	53
Data Source Selection Wizard	55
Task 1: Data Source Selection	57
Data Sources for the OM Deployment Scenario	59
Data Sources for the BSM/APM or OMi Deployment Scenario	59
OMi10 Topology Source with Integrated BSM/APM	60
OMi10 Topology Source after BSM Upgrade	61

Data Source for the VMware vCenter Deployment Scenario	63
Data Sources for Other Database Deployment Scenario	64
Task 2: Configuring the Topology Source	64
Configuring OM Topology Source	64
Supported Data Source Selections	67
Configuring RTSM Topology Source	67
Supported Data Source Selections	71
Configuring VMware vCenter Topology Source	71
Supported Data Source Selections	73
Task 3: Content Type Selection	73
Task 4: OMi Management Packs/OM SPIs Selection	75
Task 5: Content Pack Deployment	75
Task 6: Data Source Configuration	76
Logon Banner	76
Chapter 3: Configure OBR for BSM/APM/OMi Deployment Scenario	77
Configuring RTSM Topology Source for OBR	77
List of Content Pack and Topology Views to Deploy	78
BSM Server	84
OMi 10 Server	86
Enabling CI Attributes for a Content Pack	88
Chapter 4: Configure OBR for OM Deployment Scenario	93
Authentication for OBR connection with OM	93
OBR connection with OM using NT authentication	94
OBR connection with OM using database authentication	95
Checking for the OM Server Port Number	102
Chapter 5: Install and Uninstall the Content Packs	103
Before You Begin	103
Check Availability and Integrity of Data Sources	103
Selecting the Content Pack Components	106
Installing the Content Pack Components	108
Uninstalling the Content Pack Components	112
Disabling Memory Analysis and APS Service Monitoring	113
Upgrading Content Packs	116
Chapter 6: Data Source Configuration	117
Topology Source	118

Configuring the Operations Manager Data Source	119
Configuring the SiteScope Data Source	122
Configuring the Generic Data Source	127
Configuring the VMware vCenter Data Source	130
Configuring the Operations Agent Data Source	131
Configuring the Management and Profile Database Data Source	132
Configuring the OMi Data Source	140
Chapter 7: Pending Configuration	144
Part III: Additional Configuration and Administration	145
Chapter 8: Configuring the Operations Agent for Data Collection in Secure Mode	146
Chapter 9: Configuring the Report Drill Feature Settings	151
Chapter 10: Configuring the Internal Alerting Service	154
Chapter 11: Certificates for OBR	158
Use Secure Sockets Layer (SSL) Certificate	158
Client Authentication Certificate for OBR	159
Authentication and Authorization	159
Prerequisites of Certificate Based Authentication	159
Configuring Username Extraction Method	163
Configuring OBR Administration Console	163
Configuring SAP BusinessObjects BI Launch Pad	168
Chapter 12: Configuring OBR with Network Node Manager i (NNMi)	173
Chapter 13: Configuring DSN on Windows for Vertica Database Connection	178
Chapter 14: Discover Profile or Operations Database	182
Chapter 15: Configuring OBR to Setup Vertica Cluster	185
Prerequisites for the nodes of Cluster	186
Set up Vertica Cluster and Scale Out	186
Chapter 16: Configuring OBR for External Vertica	187
For New OBR Installation	188
Scenario 1: OBR is the Only Product	188
Scenario 2: OBR is Installed Before Other Product	189
Scenario 3: OBR is Installed After Other Products	190
Scenario 4: OBR is installed after the other product installation and then again other product is installed	191

For Existing OBR Installation	192
Configuring OBR for External Vertica after Post Installation	192
Chapter 17: Configuring Logon Banner for OBR	193
Enabling the Logon Banner	193
Disabling the Logon Banner	195
Chapter 18: Configuring FIPS for OBR	197
OBR in FIPS Mode	197
Considerations When Running OBR in FIPS Mode	198
Configure OBR for FIPS 140-2 Compliance	198
Prerequisites:	198
Chapter 19: Change the Vertica Data Storage Location	207
Chapter 20: Configuring TLS for Vertica	209
Configure TLS for Vertica in Typical Scenario	209
On Vertica:	209
On OBR:	213
On SAP BusinessObjects:	214
Configure TLS for Vertica in Distributed Scenario	216
On Vertica:	216
On OBR:	220
On SAP BusinessObjects:	224
On Remote Collector:	226
Part IV: Database Backup and Recovery	227
Chapter 21: Database Backup and Recovery	228
Terminologies used in this guide	229
Backup of OBR Components	229
Create Full Backup of OBR on Windows	230
Create Full Backup of OBR on Linux	234
Restore OBR Components	236
Restore Backup of OBR on Windows	236
For SAP BusinessObjects Database and File Store	236
For Management Database Table	249
Restore Backup of OBR on Linux	250
For SAP BusinessObjects Database and File Store	250
For Management Database Table	262
Back up and Restore Vertica Database	263

Part V: Appendix	264
Appendix A: Topology Source Migration (OM to OMi)	265
Prerequisites	265
Topology Migration Steps	266
1. Topology Migration Precheck	266
2. Generating the Mapping Files	267
3. Topology Invoke DLC	268
Points to Note	269
Limitations	269
PostgreSQL Management DB Backup and Restore	270
PostgreSQL Management DB backup	270
Restore PostgreSQL Management DB	271
Topology Source Migration FAQs	271
Appendix B: Topology Source Migration (BSM to OMi)	272
Prerequisites	272
Topology Migration Steps	273
1. Topology Migration Precheck	273
2. Generating the Mapping Files	274
3. Topology Invoke DLC	276
Points to Note	276
Limitations	277
PostgreSQL Management DB Backup and Restore	278
PostgreSQL Management DB backup	278
Restore PostgreSQL Management DB	278
Topology Source Migration FAQs	279
Appendix C: Status, Stopping and Starting OBR Services	280
On Linux	280
On Windows	283
Appendix D: SiteScope Monitors for OBR	287
Appendix E: Installing SAP BusinessObjects Dashboards (Earlier known as Xcelsius)	293
Hardware and Software Requirements	293
Installing SAP BusinessObjects Dashboards (Optional)	293
Appendix F: Listing of ETLs	294
Appendix G: System Management Reports with SiteScope data source ...	300

Appendix H: Disable TLS for Vertica	305
Appendix I: Drop Vertica Database	307
Send documentation feedback	308

Part I: OBR Overview and Planning

Operations Bridge Reporter (HPE OBR) is a cross-domain historical IT infrastructure performance reporting solution. It leverages the topology information to show how the underlying IT infrastructure's health, performance, and availability are affecting your business services and business applications in the long term. OBR manages the relationship of infrastructure elements to the business services at run-time by using the same topology services that are used by the products that collect the performance data from the managed nodes.

Operations Bridge Reporter collects data from different data sources, processes the data, and generates reports with the processed data. Operations Bridge Reporter uses Vertica database for storing performance data, SAP BusinessObjects for reporting and PostgreSQL database for storing management data. The collector component of OBR collects data from RTSM, Operations Manager (OM), BSM Profile database, BSM Management database, Application Performance Management (APM), Operations Manager i (OMi), SiteScope, Network Node Manager i (NNMi) as well as from the NNM iSPI Performance for Metrics, Operations Agent, and Cloud Optimizer.

All the components of Operations Bridge Reporter can be installed on a single system. If a single system is not capable of supporting all the components of Operations Bridge Reporter, the data collector, SAP BusinessObjects, and the Vertica components can be installed on separate systems. If the data sources are distributed over a large area, there is an option to deploy Operations Bridge Reporter collector on different systems. It reduces the network load and ensures connectivity to the data sources.

OBR supports both Windows and Linux. You can install OBR typical scenario only on Linux system. This is because you can install Vertica only on Linux. You can install the OBR custom scenario on a combination of both Windows and Linux operating systems. For more information on OBR installation and its preferences, see *Operations Bridge Reporter Interactive Installation Guide*.

A topology model or view, logically maps and relates your business services to your IT elements. OBR enables you to define a topology service and collect the infrastructure data from the nodes that are part of the topology. In this way any change in topology information gets automatically reflected in the reports at run-time.

Revision History

The following table lists the major changes for each new release of this document:

Document Release Date	Description of Major Changes
April 2017	Initial release.
June 2017	Enhanced the Post-installation steps in the guide.

Reference Documents

This section provides information on documents you can refer to for more information.

SAP BusinessObjects Documentation

- For documents on SAP BusinessObjects Business Intelligence Platform, see [SAP BusinessObjects Business Intelligence platform 4.x](#).
- For information on the following SAP BusinessObjects Official Product Tutorials, see:
 - [SAP BusinessObjects Dashboards 4.x](#)
 - [SAP BusinessObjects BI Launch Pad 4.x](#)
 - [SAP BusinessObjects Information Design Tool](#)
 - [Securing Business Objects Content – Folder Level, Top Level and Application Security](#)
- You can also refer to SAP BusinessObjects documents available at physical location on OBR server:
 - For information on Central Configuration Manager help, go to:
 - <Install_Drive>\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Help\en\Central Configuration Manager Help.chm **(On Windows)**
 - For information on Designer tool, go to:
 - <Install_Drive>\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Web Content\enterprise_xi40\help\en\designer_en.chm **(On Windows)**
 - For information on SDK samples and documents, go to:
 - <Install_Drive>\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\SL SDK **(On Windows)**
 - /opt/HP/BSM/BOE4/sap_bobj/enterprise_xi40/SL_SDK **(On Linux)**
 - For information on Central management console (Administration of Business objects), go to:

\$PMDB_HOME/BOWebServer/webapps/BOE/WEB-INF/eclipse/plugins/webpath.CmcAppBranding_lang.en/web/help/en **(On Linux)**

Tip: To view the help files, copy the en folder to your local system.

- For information on BI Launchpad (creation of reports, report functions and other admin tasks like scheduling), go to:

\$PMDB_HOME/BOWebServer/webapps/BOE/WEB-INF/eclipse/plugins/webpath.InfoView_lang.en/web/help/en **(On Linux)**

Tip: To view the help files, copy the en folder to your local system.

OMi Management Packs

- For information on OMi Management Packs and other contents, see [HPE Marketplace](#).

Vertica Documentation

- For information on Vertica documentation, see <https://my.vertica.com/docs/7.1.x/HTML/>

Chapter 1: Configuration Planning

This section provides information on planning tasks you need to perform before you start the post-install configuration. To plan the post-install configuration, you have to know the following:

1. ["Know your Deployment Scenarios"](#) following section
2. ["Know the Data Sources"](#) on page 18
3. ["Determine the Readiness"](#) on page 19
4. [" Licensing Requirement for OBR"](#) on page 20

Know your Deployment Scenarios

The following deployment scenarios are supported by OBR:

- [Deployment with BSM/APM/OMi](#)
- [Deployment with Operations Manager](#)
- [Deployment with VMware vCenter](#)
- [Other Deployments](#)

The deployment scenario that is chosen will dictate the choice of the topology source.

Note: OBR connects only to one of the topology sources at a time.

The following sections describe the deployment scenarios and their source of topology information:

Business Service Management/Application Performance Management/Operations Manager i

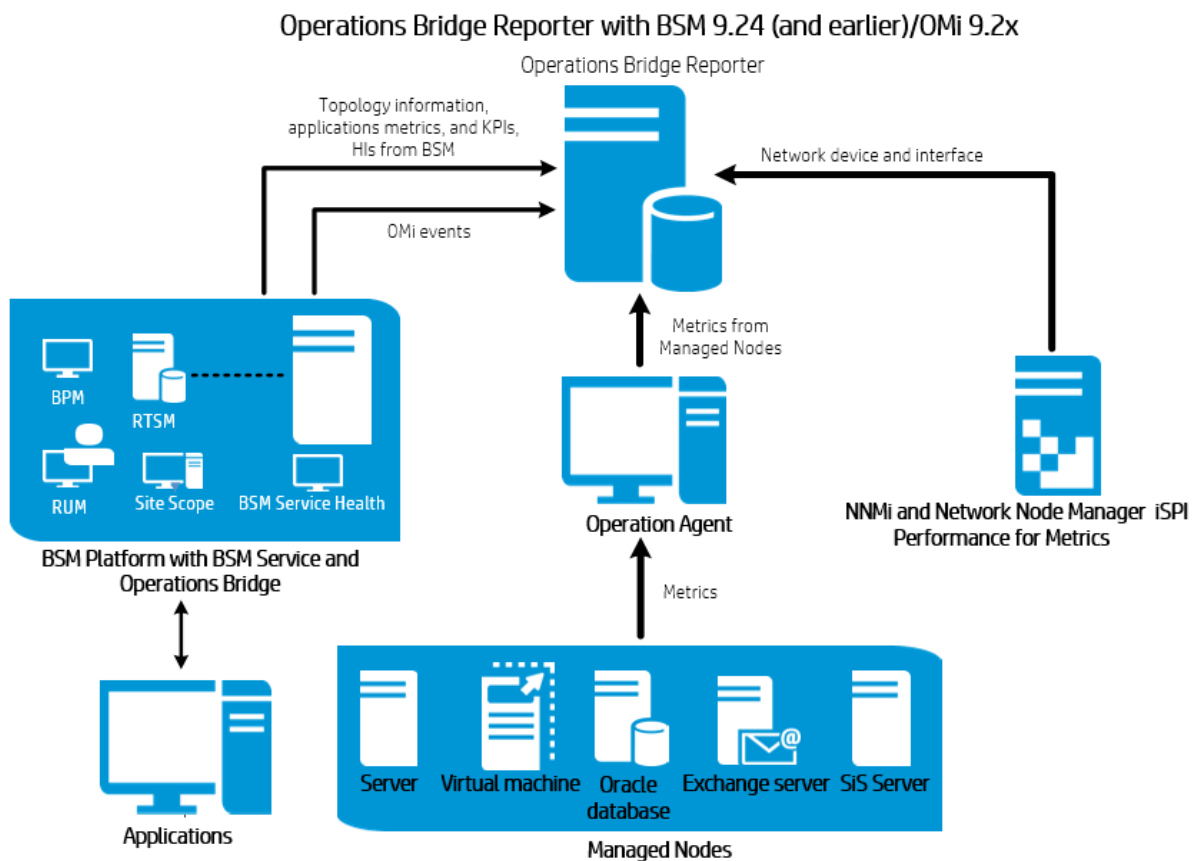
In this deployment, Run-time Service Model (RTSM) is the source of topology information. OBR discovers and synchronizes topology information from RTSM. In a BSM with RUM, BPM, SiteScope and OMi 9.2x scenario, this synchronization technique receives data from Operations Agent, NNMi, NNM iSPI Performance for Metrics, topology information from RTSM and event information from OMi. In a BSM and OMi 10 environment, the synchronization technique receives discovered topology

information, metrics, KPIs, HIs and events from BSM, OMi 10 and Operations Agent. In an environment with OMi 10, OBR uses RTSM to obtain topology information, KPIs, HIs and metrics from Operations Agent or SiteScope systems that are configured with OMi.

Additionally, you can configure OBR to collect data directly from NNMi and NNM iSPI Performance for Metrics. You can access network performance reports based on the components and interfaces in your IT environment.

OBR with BSM 9.24 (and earlier)/OMi 9.2x

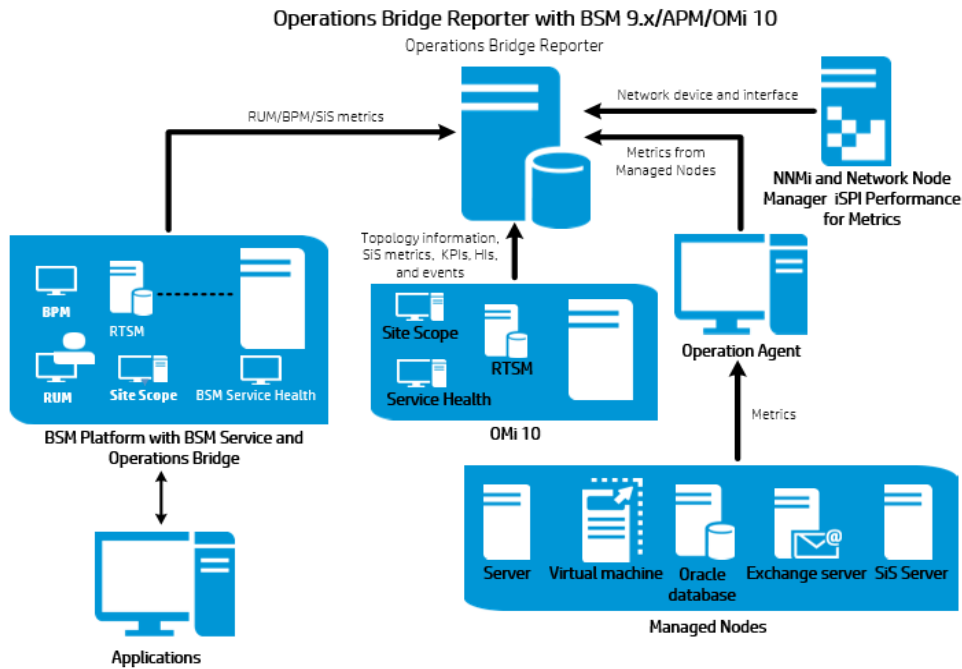
The following diagram shows the flow of data from Operations Agent, NNMi (direct), NNM iSPI Performance for Metrics, and topology information from RTSM with underlying OM servers.



OBR with BSM 9.x/APM/OMi 10

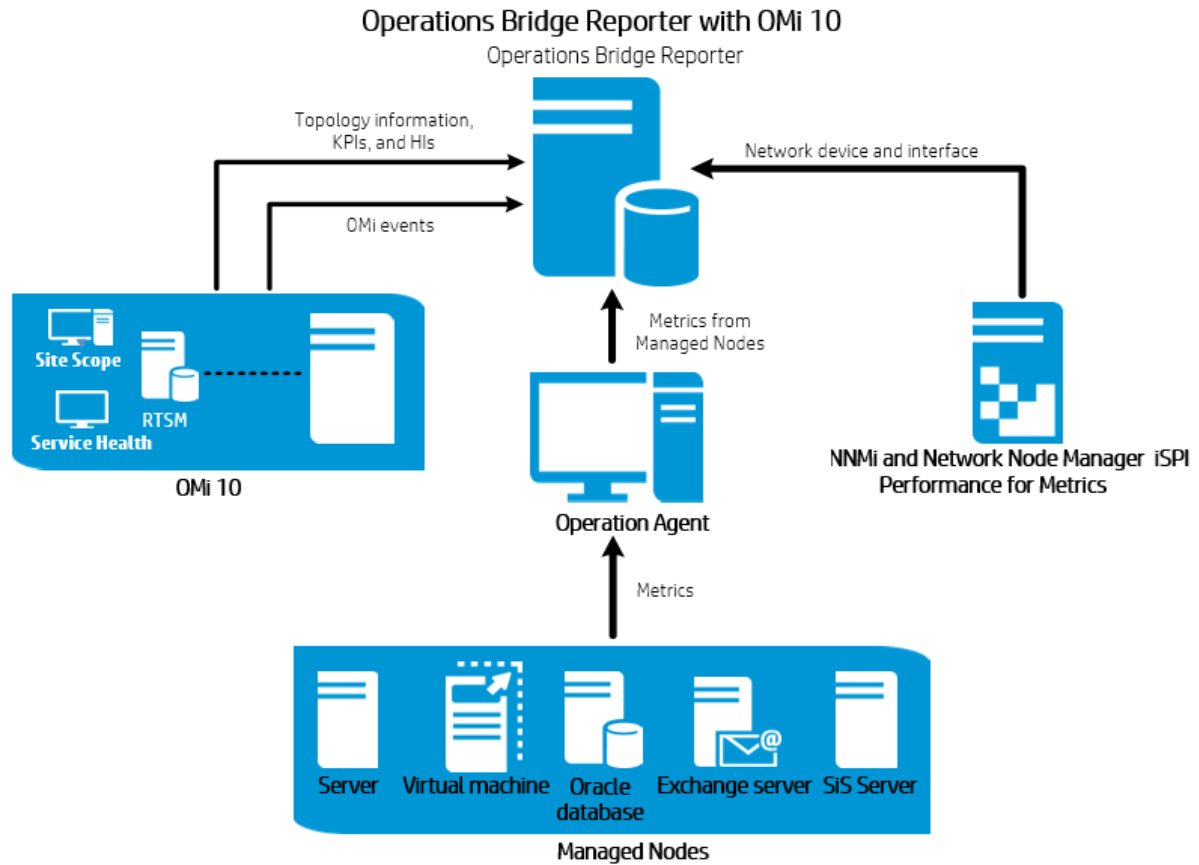
The following diagram shows the flow of data from Operations Agent, OMi 10, NNMi (direct), NNM iSPI Performance for Metrics, and topology information from RTSM in an BSM/APM and OMi 10 environment.

You can configure BSM 9.x/APM and OMi 10 as standalone topology and data sources. You can also setup BSM 9.x/APM to synchronize topology data with the OMi 10 system. In this configuration, the OMi 10 system provides topology data for all nodes and fact data for operations, events and KPI. The BSM/APM system provides fact data from RUM, BPM, and SiteScope that are directly configured with it.



OBR with OMi 10.x

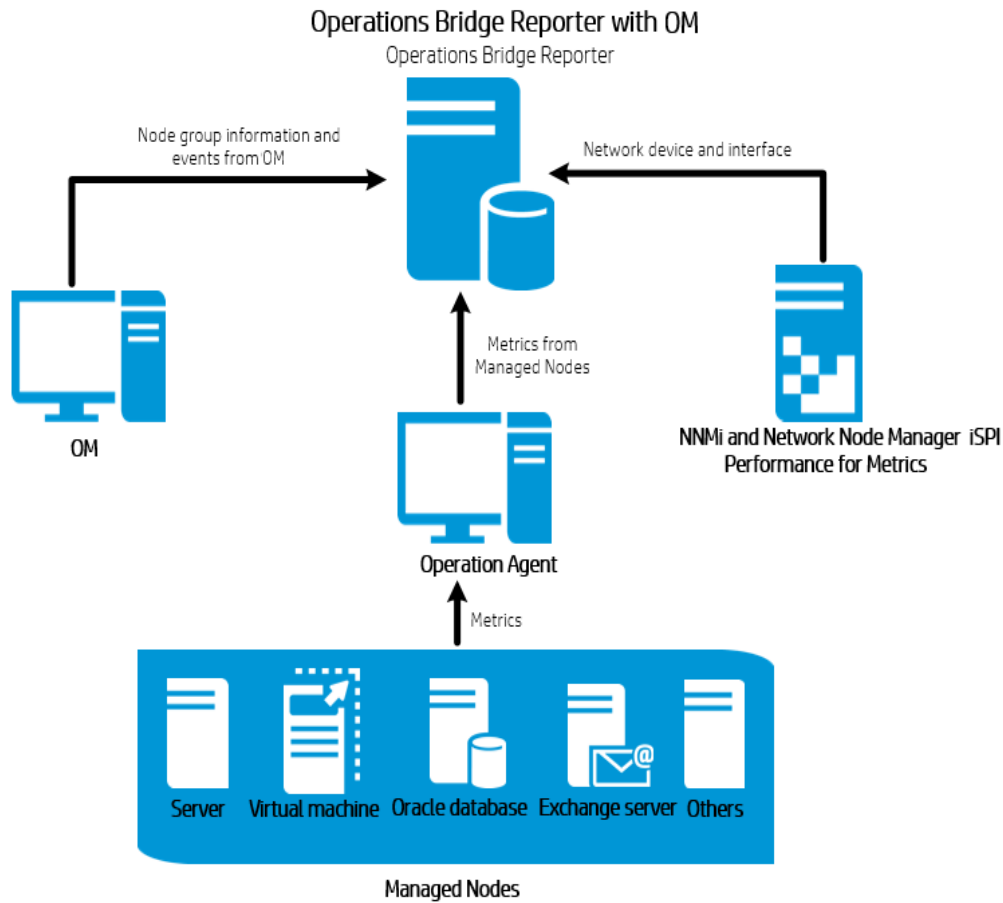
The following diagram shows the flow of data from Operations Agent, NNMi (direct), NNM iSPI Performance for Metrics, and topology information from RTSM in an OMi 10.x environment.



Operations Manager (OM)

In this deployment, the topology information is taken from OM that consists of logical node groups. A node group is a group of managed nodes defined in OM that are logically combined for operational monitoring. These logical node groups are created by OM users to classify the nodes as specific organizations or entities within their enterprise. For example, a group called **Exchange Servers** can be created in OM to organize the specific Exchange Servers for reporting or monitoring purposes. OBR uses the node groups from OM for its topology reporting.

You can configure OBR to collect data directly from NNMI and NNM iSPI Performance for Metrics. You can access network performance reports based on the components and interfaces in your IT environment.

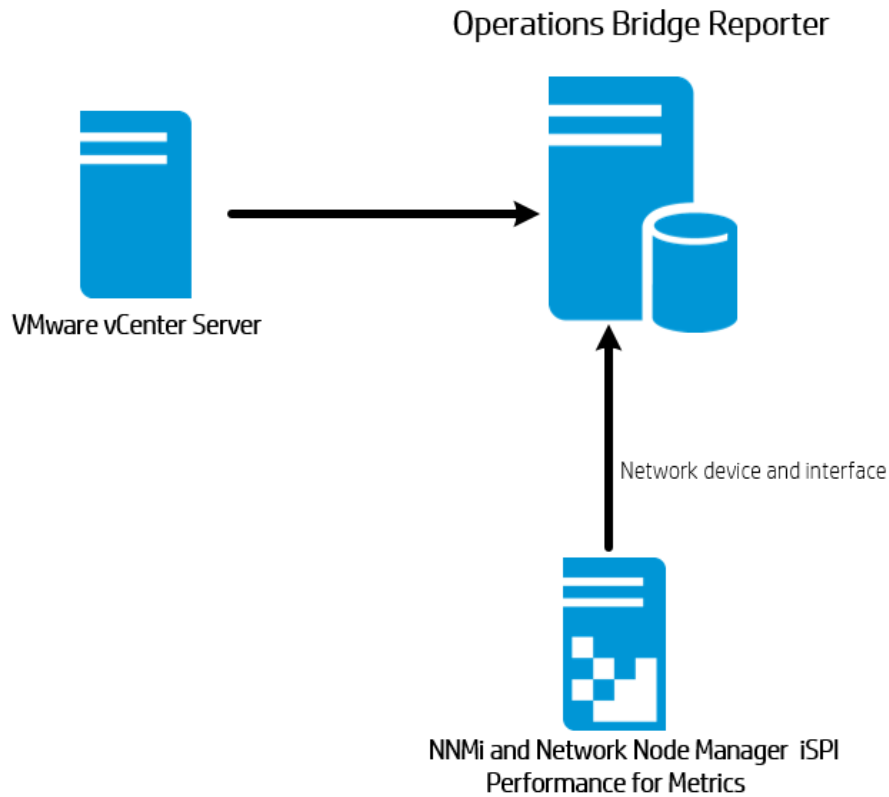


VMware vCenter

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.

In the VMware vCenter deployment scenario, the VMware vCenter server is the source of the topology information for OBR.

You can configure OBR to collect data directly from NNMi and NNM iSPI Performance for Metrics. You can access network performance reports based on the components and interfaces in your IT environment.



Other Deployments

Apart from the basic deployment scenarios, you can collect data - irrespective of the topology source configured - from the following sources independently:

- Deployment with NNMi

OBR integrates with and collects historical network-related data for the network nodes from NNM iSPI Performance for Metrics. OBR supports the collection of network data by extending the functionality of the database collector. The Network Content Pack identifies the list of metrics or fact data that OBR must collect from each of these data sources. The corresponding dimension data is collected from the RTSM or OM topology source, depending on the deployment scenario. If NNMi is integrated with BSM/OMi RTSM then use the **NetworkPerf_ETL_PerfiSPI_RTSM** Content Pack component. Otherwise, use the **NetworkPerf_ETL_PerfiSPI_NonRTSM** Content Pack component.

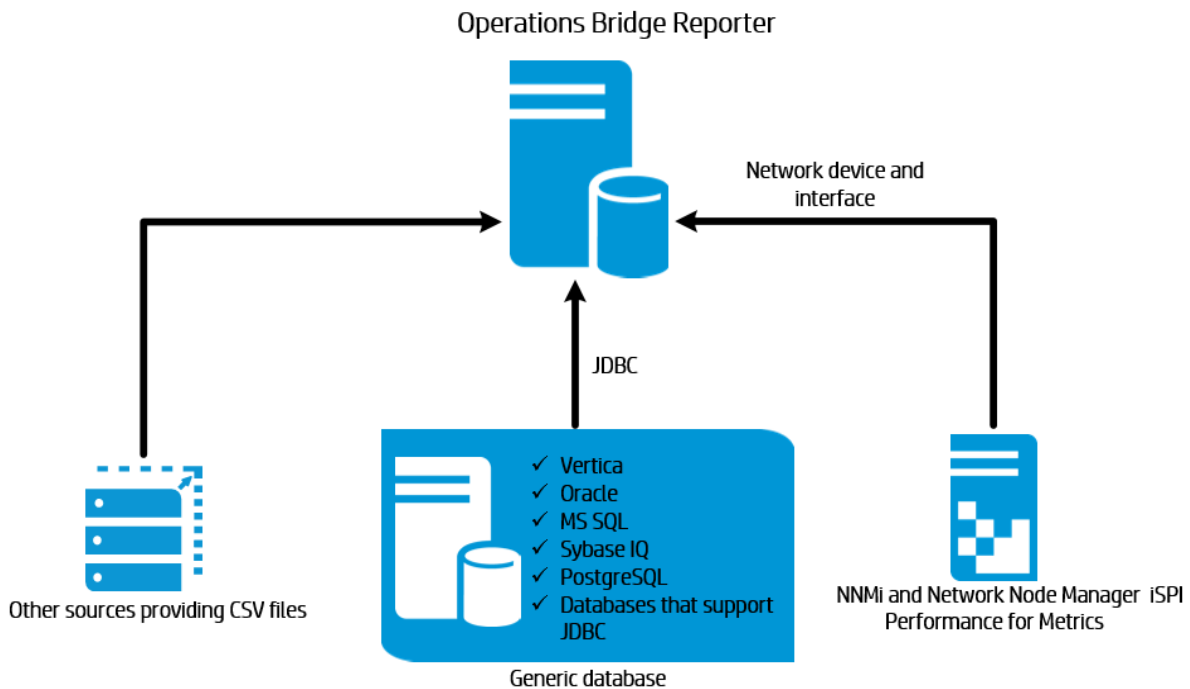
OBR also collects network performance data directly from Network Node Manager i (NNMi). The Network Component Health Content Pack and Interface Health Content Pack identifies the metrics that OBR must collect from the data sources.

- Deployment with other applications using JDBC

OBR includes Java Database Connectivity (JDBC) drivers to connect to Oracle, Microsoft SQL, Sybase IQ and Vertica databases. You can configure OBR to collect data from other databases that support JDBC connection. OBR provides Content Development Environment (CDE) and Content Designer to create content and generate reports.

- Deployment with other applications using CSV

OBR also collects data from set of Comma Separated Variables (CSV) files. The format of the CSV file should be as defined in the Domain Content Pack. The Content Development Environment (CDE) and Content Designer tools help you to create content and generate reports.



Know the Data Sources

OBR collects data from other HPE monitoring products like SiteScope, Operations Agent (OA), Operations Manager (OM), Business Process Management (BPM), Application Performance

Management (APM), Real User Monitoring (RUM), Network Node Manager i (NNMi), Operations Management i (OMi), and third party sources like VMware vCenter.

Based on the deployment scenario and the topology sources, you can configure OBR to collect data from the HPE monitoring products and third party data source. OBR can then report on the data collected from the configured data sources.

OBR also supports creating new content using the Content Development Environment (CDE). The Content Development Environment consists of a set of tools that you use during the process of new content development.

You must know the data sources from which you want OBR to collect the data from and also list down Content Packs you want to deploy. You must plan for new custom content and reports that you want to generate.

Determine the Readiness

In this stage, you must determine the readiness of the HPE monitoring products deployed in your environment before you integrate them with OBR. Ensure that OBR supports the versions of the HPE products deployed in your environment.

For more information on the versions supported by OBR, see *Operations Bridge Reporter Release Notes*.

The following table lists the readiness checks you must perform before integrating with OBR:

HPE Monitoring Products	Readiness Check List
BSM/APM/OMi	<p>You must ensure that the Configuration Item (CI) discovery products like OA, Sitescope, NNMi populates the CIs in RTSM. You must confirm the number of CI instances in OBR views in RTSM is as expected and the CI attributes that OBR depends on contains proper values.</p> <p>Depending on the deployment scenario, OBR collects data from Management database, Profile database, Operations database, and/or Event database. You must ensure that connectivity is available between these databases and the OBR system.</p>
Operations Manager (OM)	You must ensure that a proper connection is established between OM database and OBR system.
Operations Agent (OA)	You must ensure that all the required SPI and MP policies are deployed and a proper connection exists between the OA and OBR systems.

HPE Monitoring Products	Readiness Check List
SiteScope	<p>You must ensure that all the required monitors are deployed in SiteScope. A list of SiteScope monitors are provided in the Appendix section, see "SiteScope Monitors for OBR " on page 287.</p> <p>You must ensure to integrate Sitescope with BSM to collect system performance data from SiteScope. You must either install SysPerf_ETL_SiS_DB for OBR to collect data from the BSM Profile database or install the SysPerf_ETL_SiS_API to collect data logged from the SiteScope API.</p> <p>For more information on ETLs, see Appendix C: Listing of ETLs.</p>
NNMi	<p>OBR collects network data directly from NNMi and iSPI Performance for Metrics. You must ensure that you have NNMi configured in your environment. If BSM is deployed in your environment, you have the option of integrating NNMi with BSM or OMi to view Business Service based reports in OBR.</p> <p>If OBR is directly integrated with NNMi, you have to ensure that HPE_PMDB_Platform_NRT_ETL service is up and running. Also ensure that the ComponentHealth_Reports and InterfaceHealth_Reports Content Packs are installed.</p>
VMware vCenter	<p>You must ensure that a proper connection is established between VMware vCenter server and OBR system.</p>

Licensing Requirement for OBR

This section provides information on licensing requirements for OBR. This section also provides information on various OBR editions and license to use. It provides procedure to obtain a permanent license key and install it. It also provides procedure to reactivate license for SAP BusinessObjects.

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 are as follows:

- **Operations Bridge Reporter (Base License)**

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 (Node License)**

A node is a real or virtual computer system, or a device (for example a printer, router, or bridge) on a network or an entity defined in custom content (for example software instance, port). Additional data collection and reporting entitlements can be added to grow the solution to fit your environment.

Note: If you have obtained the node license, you must also obtain and install the base license with it.

Licenses to Use (LTUs)

Operations Bridge Reporter Standard and *Operations Bridge Reporter Advanced* editions are included in the **Operations Bridge Premium** and **Operations Bridge Ultimate** editions respectively. To benefit from the OBR advanced functionality, you can buy *Operations Bridge Reporter Upgrade (TD906AAE)* edition in addition to the **Operations Bridge Premium** edition or *Operations Bridge Reporter Standard* edition.

Operations Bridge Reporter Advanced edition

Stock-keeping Unit (SKU): TJ756AAE

The Operations Bridge Reporter Advanced edition includes the following:

- All Content Packs. Following are the out-of-the-box content available for this edition:
 - System Performance Content Pack
 - Virtual Environment Performance Content Pack
 - Health and Key Performance Indicators Content Pack
 - Cross-Domain Operations Events Content Pack
 - Operations Events Content Pack
 - Microsoft Active Directory Content Pack
 - Microsoft Exchange Server Content
 - Microsoft SQL Server Content Pack
 - Oracle Content Pack Reference
 - Oracle WebLogic Server ContentPack
 - IBM WebSphere Application ServerContent Pack

- Network Performance Content Pack
- Network Component Health Content Pack
- Network Interface Health Content Pack
- Real User Transaction Monitoring Content Pack
- Synthetic Transaction Monitoring Content Pack
- Ability to create custom 3rd party content packs and generate reports on the custom content.
- **Operations Bridge Ultimate** edition which includes *Operations Bridge Reporter Advanced*, entitles customers to 1 TB of HPE Vertica for every 50 **Operations Bridge Nodes** for the use with **HPE Operations Bridge**. Storing any other data other than that of HPE Operations Bridge requires additional appropriate HPE Vertica license to be acquired separately.
- When bought as stand-alone, *Operations Bridge Reporter Advanced* edition, entitles customers to 1 TB of HPE Vertica for every 50 **Operations Bridge Reporter Nodes** for the use with Operations Bridge Reporter . Storing any other data other than that of Operations Bridge Reporter requires additional appropriate HPE Vertica license to be acquired separately

Operations Bridge Reporter Standard edition

Stock-keeping Unit (SKU): TD905AAE

The Operations Bridge Reporter Standard edition includes the following:

- Content on Systems and Virtualization and Enterprise Application Management and Events (OMi, OM). Following are the out-of-the-box content available for this edition:
 - System Performance Content Pack
 - Virtual Environment Performance Content Pack
 - Health and Key Performance Indicators Content Pack
 - Cross-Domain Operations Events Content Pack
 - Operations Events Content Pack
 - Microsoft Active Directory Content Pack
 - Microsoft Exchange Server Content
 - Microsoft SQL Server Content Pack
 - Oracle Content Pack

- Oracle WebLogic Server Content Pack
- IBM WebSphere Application Server Content Pack
- Ability to create custom 3rd party content packs and generate reports on the custom content.
- **Operations Bridge Premium** edition which includes *Operations Bridge Reporter Standard* edition, entitles customers to 1 TB of HPE Vertica for every 50 **Operations Bridge Nodes** for the use with **HPE Operations Bridge**. Storing any other data other than that of HPE Operations Bridge requires additional appropriate HPE Vertica license to be acquired separately.
- When bought as stand-alone, *Operations Bridge Reporter Standard edition*, entitles customers to 1 TB of HPE Vertica for every 50 **Operations Bridge Reporter nodes** for the use with Operations Bridge Reporter. Storing any other data other than that of Operations Bridge Reporter requires additional appropriate HPE Vertica license to be acquired separately.

Operations Bridge Reporter Upgrade edition

Stock-keeping Unit (SKU): TD906AAE

You can upgrade Operations Bridge Reporter from Standard to Advanced for **Operations Bridge Premium** edition nodes or Operations Bridge Reporter nodes SW E-LTU

Operations Bridge Reporter additional 50 Operations Bridge Reporter Nodes

Stock-keeping Unit (SKU): TJ757AAE

This is an add-on pack to add entitlement for 50 additional nodes for OBR.

For information on custom content license, see *Operations Bridge Reporter Content Development Guide*.

Obtaining a Permanent License Key

To obtain a permanent license, you can either use the new Software Entitlement system website or log on to Administration Console and go to **Additional Configurations > Licensing > Launch HPE Password Center**. HPE partners and employees can still continue to use the HPE Licensing for Software website.

To view the OBR License Details, log on to Administration Console and go to **Additional Configurations > Licensing**. You can view active license type, days to license expiry, license entitlement, license usage, nodes remaining, Vertica entitlement, and Vertica usage.

Note: If you uninstall Content Pack, run the DLC to get the correct license usage count in the **Additional Configurations > Licensing** page of Administration Console.

To obtain a permanent license key, follow these steps:

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

```
https://<OBR_Server_FQDN>:21412/OBRApp
```

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

Note: By default HTTPs is enabled for OBR. You can also launch Administration Console using `http://<OBR_Server_FQDN>:21411/OBRApp` if you have disabled HTTPs.

2. Enter user name in the **User Name** field and password in the **Password** field.
3. Click **Log On**.
The **Dashboard** page is displayed.
4. Click **Additional Configurations > Licensing**. The **Licensing** page appears with HPE OBR License Details.
5. Click **Launch HPE Password Center** link OR go to the [HPE Software Licensing website](#).
6. 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.
7. Follow the instructions provided on the website to obtain license keys.

Installing the Permanent License Key

To install the permanent license, follow these steps:

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 where you have saved 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 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:

- a. Type the following command at the command prompt:

RHEL 6.x/SUSE Linux Enterprise Server 11: `service HPE_PMDB_Platform_Administrator restart`

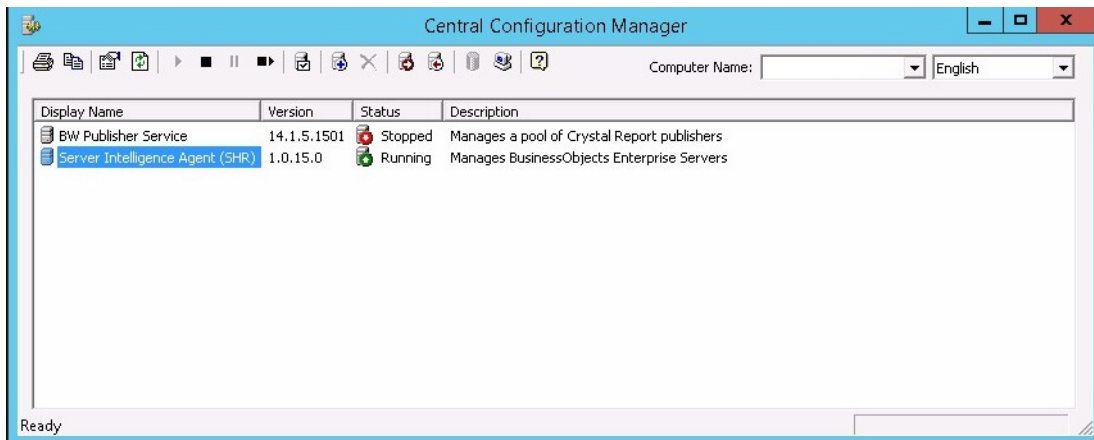
RHEL 7.x: `systemctl restart HPE_PMDB_Platform_Administrator.service`

SAP BusinessObjects License Reactivation

The SAP BusinessObjects license depends on the validity of the OBR license. If the OBR license expires, the SAP BusinessObjects license is automatically deactivated and all the SAP BusinessObjects servers are disabled. After you renew the OBR license and access the Administration Console, OBR automatically reactivates the SAP BusinessObjects license. However, the SAP BusinessObjects servers remain in the disabled state. To ensure that SAP BusinessObjects works, you must manually enable the servers by performing the following steps:

On Windows:

1. Log on to SAP BusinessObjects Central Configuration Manager.
2. Click **Start > 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. Type the user credentials in the **User name** and **Password** fields of the SAP BusinessObjects server.

The default user name is **administrator**.

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 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:

`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. You can also launch CMC using `http://<System_FQDN>:8080/CMC` if you have disabled HTTPs.


The log in page is displayed.

2. Log on as user with administrator privileges.

The **System Configuration Wizard** is displayed. Click **Close** to close the wizard. The **Central Management Console** home page is displayed.

Note: If you do not want the **System Configuration Wizard** to appear each time you log on to CMC, click the check box **Don't show this wizard when cms is started**.



3. Click  **Servers** and select the **Servers list** in the left menu.
4. Hold down the **Shift** or **Ctrl** key and click on server to select multiple servers.
5. Right-click on the selected group of servers and then click **Enable Server**.

Note: If there are two pages of server listings, proceed to the second page to enable all the servers.

Note: If the SAP BusinessObjects servers are still not enabled, restart the HPE_PMDB_Platform_IM service.

Part II: Configuring OBR

This section provides information on post-install configuration and other data source configuration required to setup OBR.

Chapter 2: Post-Install Configuration

This section contains sub sections that describes tasks to complete post-install configuration of OBR using the Configuration Wizard and the Data Source Selection Wizard from the Administration Console.

Note: Make sure to install the OBR 10.22 patch before you move ahead with the configurations. For steps to install the OBR 10.22 patch, see the *Operations Bridge Reporter Release Notes* for 10.22.

If you have not completed all the tasks of the post-install configuration then you can refer **Pending Configuration** page to configure or install remaining packages, see "[Pending Configuration](#)" on [page 144](#). If you want to install additional Content Packs or configure data source, see "[Install and Uninstall the Content Packs](#)" on [page 103](#) and "[Data Source Configuration](#)" on [page 117](#) respectively.

Note: You must perform all the post-install configuration tasks described in this chapter immediately after installing OBR, and before installing the Content Packs through the Content Pack Deployment page.

Note: You can manually create users/group for SAP BO, Postgres database and Vertica database and assign the users during the post-install configuration. For more information to create users/group manually, see *Operations Bridge Reporter Interactive Installation Guide*.

Secure Communication

You can configure JDBC or ODBC connections over TLS for the following:

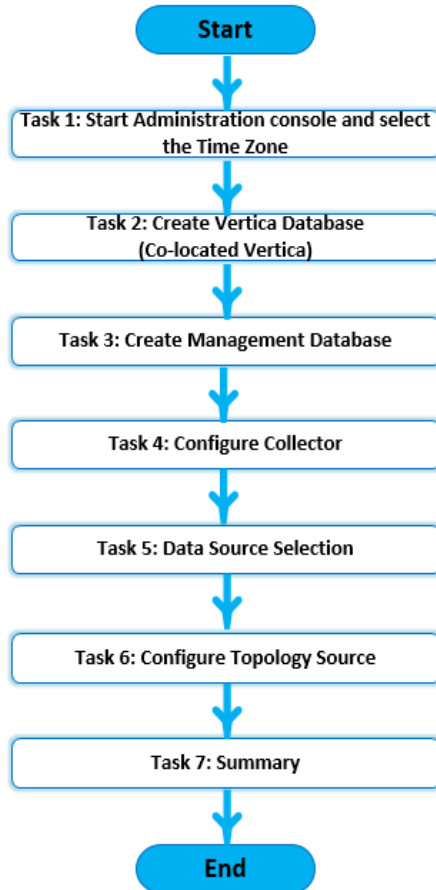
- Vertica and OBR server /SAP BusinessObjects
- OBR collector and BSM/APM/OMi Oracle database
- OBR collector and BSM/APM/OMi RtSM

Using the Administration Console, **Data Source Configuration** page, you can enable TLS for OM and BSM/APM/OMi to connect with Oracle database using ODBC or JDBC. For more information, see "[Data Source Configuration](#)" on [page 117](#).

Using the Administration Console, **Additional Configurations > Vertica Database & Time Zone** page, you can enable TLS for Vertica database. For more information, see "[Configuring TLS for Vertica](#)" on [page 209](#).

Flow of tasks for typical scenario

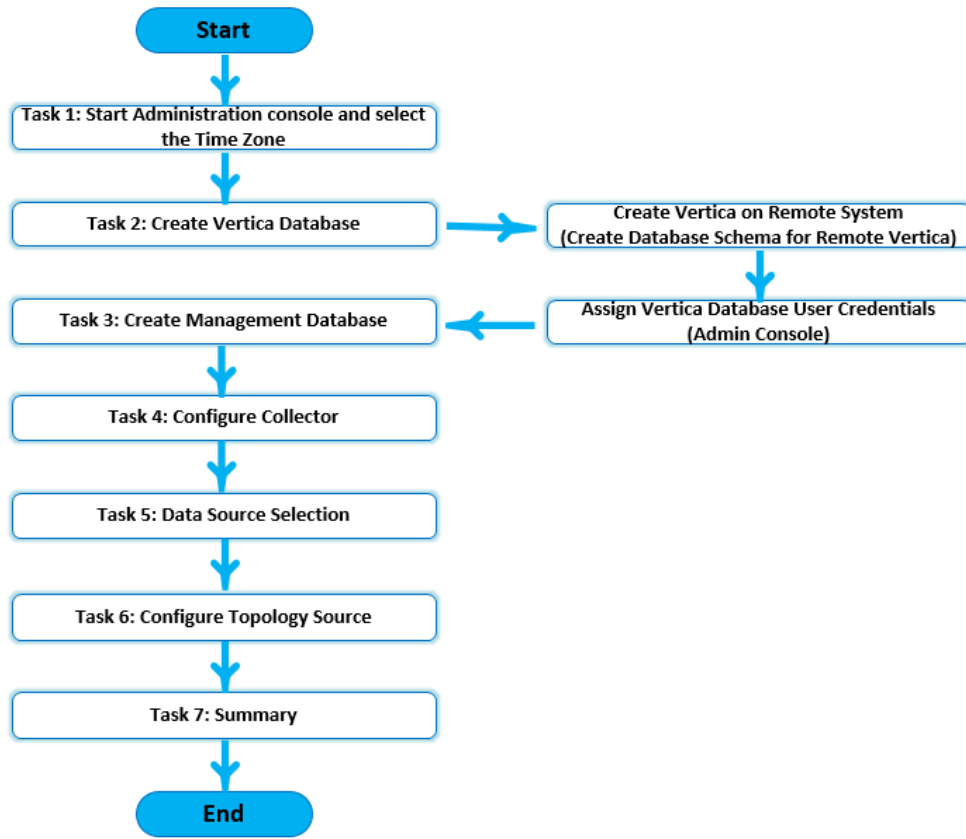
The following flowchart gives you an overview of the post-install tasks for OBR where the OBR and Vertica database are installed on the same system.



Flow of tasks for distributed scenario

The following flowchart gives you an overview of the post-install tasks for OBR where the Vertica database is installed on a remote system.

Note: You must have installed and created the Vertica database schema on remote system before you begin with the post-install tasks. To create Vertica on remote system, see ["Creating Database Schema for Remote Vertica"](#) on page 39.



Configuration Wizard

After OBR is installed, launch the Administration Console for post-install configuration. The Administration console helps you to configure OBR system to collect the required data, manage the platform and install the Content Packs. 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 the Configuration Wizard, you can complete the post-install configuration of OBR databases and collectors for OBR system.

Note: Make sure to install the OBR 10.22 patch before you move ahead with the configurations. For steps to install the OBR 10.22 patch, see the *Operations Bridge Reporter Release Notes* for 10.22.

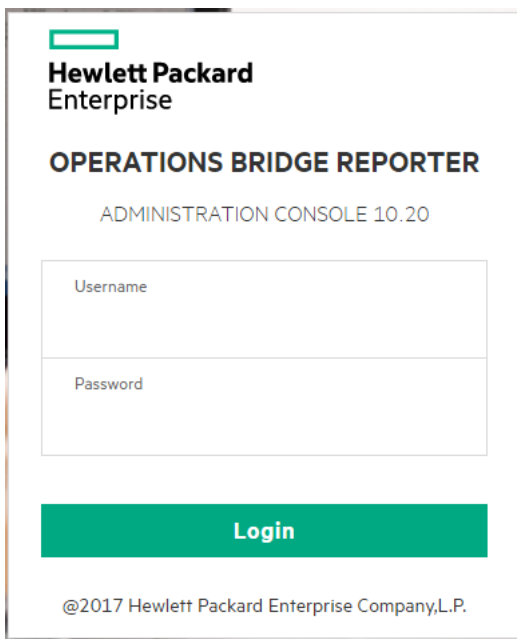
Task 1: Launching the Administration Console

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

`https://<OBR_Server_FQDN>:21412/OBRApp`

Note: By default HTTPs is enabled for OBR. You can also launch Administration Console using `http://<OBR_Server_FQDN>:21411/OBRApp` if you have disabled HTTPs.

The Operations Bridge Reporter Administration Console log on page is displayed.



The screenshot shows the login interface for the Hewlett Packard Enterprise Operations Bridge Reporter Administration Console. At the top left is the HP logo. Below it, the text reads "Hewlett Packard Enterprise". The main heading is "OPERATIONS BRIDGE REPORTER" in bold, followed by "ADMINISTRATION CONSOLE 10.20". There are two input fields: "Username" and "Password". Below these fields is a prominent green button labeled "Login". At the bottom of the page, it says "@2017 Hewlett Packard Enterprise Company,L.P."

2. a. Type the user name and the password and click **Login** to continue.

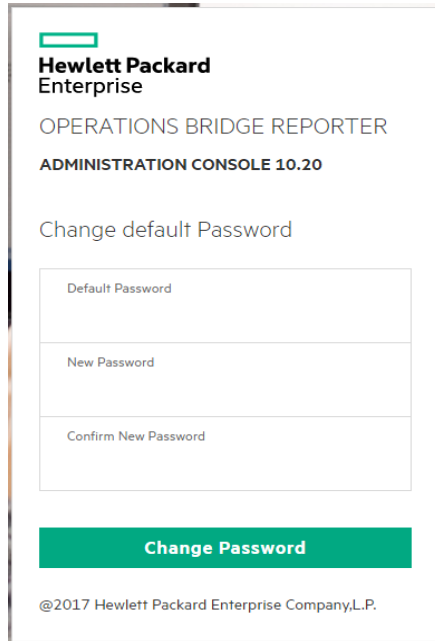
The Administration Console page is displayed.

Note: If you use any other user account to access the Administration Console, make sure that the user account has administrator privileges.

- b. If you have logged on to Administrator Console for the first time as **administrator** with a default password as **1ShrAdmin**, follow these steps:
 - i. Enter **administrator** in the user name field and default password in the password field. Click **Login**.

You have to reset the default administrator user password.

- ii. Click **CHANGE PASSWORD**. The following screen to change the password is displayed.



Hewlett Packard Enterprise
OPERATIONS BRIDGE REPORTER
ADMINISTRATION CONSOLE 10.20

Change default Password

Default Password

New Password

Confirm New Password

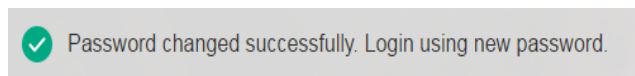
Change Password

@2017 Hewlett Packard Enterprise Company,L.P.

- iii. Enter default password in **Default Password** field.
- iv. Enter new password in **New Password** field.

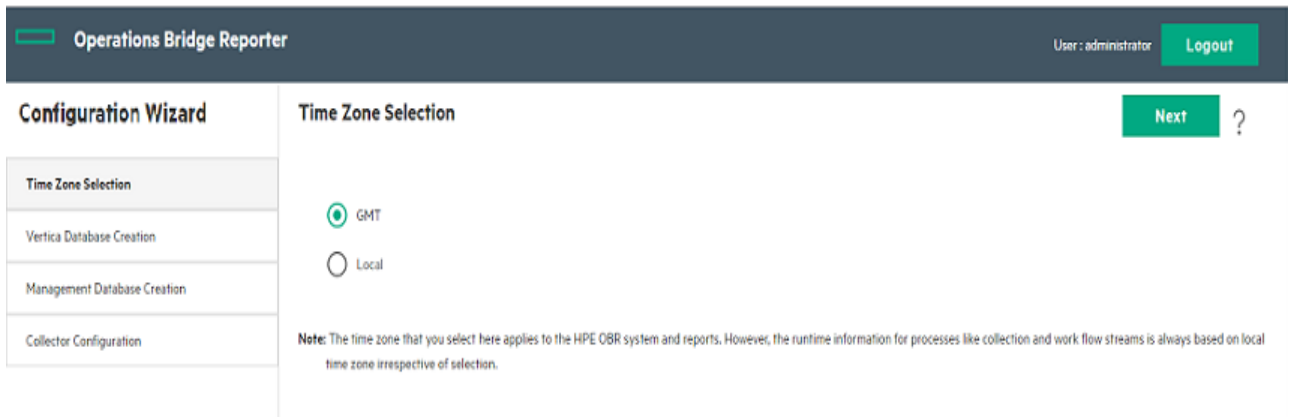
Note: The password should be an alphanumeric value, with a combination of lower, upper cases, and number. The password must be minimum of six characters and maximum of 25 characters in length.

- v. Retype the new password in the **CONFIRM PASSWORD** field. Click **CHANGE PASSWORD**. The following message is displayed.



- vi. Click the link and log on to Administration Console with your new password.

The following OBR 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. The wizard supports session-state-persistence, which enables you to resume and continue a previously-interrupted configuration session.



3. In the **Time Zone Selection** page, select the time zone, that is, GMT or Local, under which you want OBR to operate.
 - Select **GMT** if you want OBR to follow the GMT time zone.
 - Select **Local** if you want OBR to follow the local system time zone.

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.

4. Click **Next**. The **Vertica Database Creation** page is displayed.

Task 2: Creating the Vertica Database Schema

On the **Vertica Database Creation** page, specify the Vertica database user credentials and provide the location for Vertica database and catalog files.

The screenshot shows the 'Vertica Database Creation' page in the Operations Bridge Reporter Configuration Wizard. The page is titled 'Vertica Database Creation' and includes a 'Previous' button and a 'Next' button. The main content area is divided into several sections:

- Remote Database:** A checkbox labeled 'Remote Database' is unchecked. A note states: 'Note: If OBR and Vertica are installed on different systems then create a Vertica database before you continue.'
- Enable TLS:** A checkbox labeled 'Enable TLS' is checked. Below it are two radio button options: 'Generated certificates' (unselected) and 'Provided certificates' (selected). A note for 'Provided certificates' states: 'The Vertica database connection will be secured using your own certificates.'
- Enter Vertica Database Information:** This section contains five input fields:
 - Host name: mtpvm3017.hpeswlab.net
 - Port: 5433
 - Database file location: (empty)
 - Catalog file location: (empty)
 - Database name: pmdb
- Enter Vertica Database User (DBA Privilege) Information:** This section contains three input fields:
 - DBA user name: verticadba
 - Password: (empty)
 - Confirm password: (empty)
- Enter Vertica Database User Information:** This section contains three input fields:
 - User name: (empty)
 - Password: (empty)
 - Confirm password: (empty)
- Enter TLS Configuration Information:** This section contains five input fields:
 - Truststore file: (empty)
 - Truststore password: (empty)
 - Confirm password: (empty)
 - Server certificate file: (empty)
 - Server private key file: (empty)

If Vertica database is embedded with OBR, complete the task mentioned under "[Creating Database Schema for Co-located Vertica](#)" below.

If Vertica database is located remotely, complete the task mentioned under "[Creating Database Schema for Remote Vertica](#)" on page 39.

You can configure OBR to support external Vertica database. For information on configuring external Vertica database based on the scenarios, see "[Configuring OBR for External Vertica](#)" on page 187.

Creating Database Schema for Co-located Vertica

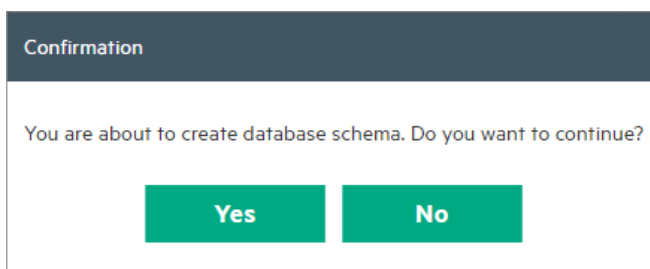
To create the database schema for Vertica database that is installed on the OBR server, follow these steps:

1. On the **Create Vertica Database** page, type the Vertica database configuration parameter as follows:

Field	Description
Remote Database	Select this option only if OBR is installed with remote Vertica database and proceed with the steps given in Creating Database Schema for Remote Vertica .
Enable TLS	Select to enable Vertica connection over TLS. By default, this field is selected.
Generated certificates	Select to enable the configuration wizard to generate default SSL certificates. When Generated certificates is selected, the <code>serverca.crt</code> and <code>server.key</code> file will be created in <code>{PMDB_HOME}/config</code> folder on the database host.
Provided certificates	Select to provide your own certificates to secure database connection. Make sure the self provided certificates are imported to the truststore on OBR server. For more information on the Vertica recommendations for Certificates, see Vertica Documentation . For Example: The default trust store path <code>{PMDB_HOME}/keystore</code> created by OBR may be used. Tip: It is recommended to use the CA certificates than the self-signed certificates.
<i>Enter Vertica Database Information</i>	
Host name	Name of the host where the Vertica database server is running.
Port	Port number to query the database server. The default port is 5433.
Database file location	Location or path where you want to store the database files.
Catalog file location	Location or path where the database metadata information will be stored.
Database name	Name of the Vertica database. By default, it is PMDB. You can edit the Vertica database name.
<i>Enter Vertica Database User (DBA Privilege) Information</i>	
DBA user name	Vertica database user name with DBA privilege to log on to Vertica database.

Field	Description
Password	Vertica database password to log on to the Vertica database.
Confirm Password	Retype the password to confirm it.
<i>Enter Vertica Database User Information</i>	
User name	Enter the Vertica database user name.
Password	Enter the Vertica database user name password.
Confirm Password	Retype the password for Vertica database user name to confirm.
<i>Enter TLS Configuration Information</i>	
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.
Confirm password	Re-type the password provided to access the truststore. This option is displayed when Enable TLS is selected.
Server certificate file	Type the path of the server .crt file if the Provided certificates is selected.
Server private key file	Type the path of the server .key file if the Provided certificates is selected.

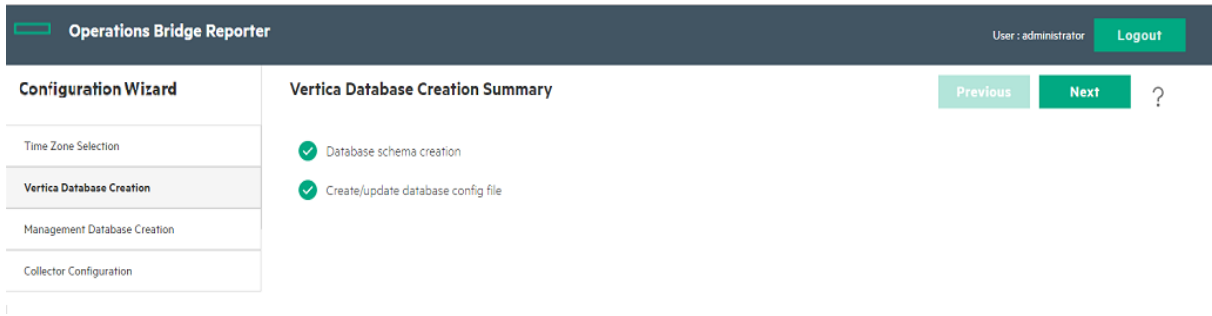
A confirmation dialog box is displayed.



The image shows a confirmation dialog box with a dark header bar containing the word "Confirmation". Below the header, the text reads "You are about to create database schema. Do you want to continue?". At the bottom of the dialog, there are two green buttons: "Yes" on the left and "No" on the right.

2. Click **Yes**.

The **Vertica Database Creation Summary** appears.



The Vertica database is created in the specified path given in **Database File Location**.

3. (Optional - Perform this step only if you have Enabled TLS) Complete the additional certificate configurations for SAP BusinessObjects. Follow these steps:

- a. Go to the location `/opt/HP/BSM/BOE4/sap_bobj/enterprise_xi40/dataAccess/connectionServer`
- b. Open the `cs.cfg` file and add/edit the lines to file as follows:

```
<JavaVM>
<!-- The default JVM configuration can be overridden here -->
<!-- Use an absolute path for the JVM -->
<!--
<LibraryName JNIVersion="JNI_VERSION_1_4">ABSOLUTE_
PATH/jvm.dll</LibraryName>
-->
<Options>
<Option Processor="64">-Xmx2048m</Option>
<Option>-Xrs</Option>
<Option>-Djavax.net.ssl.trustStore=<PATH_TO_TrustStore></Option>
<Option>-Djavax.net.ssl.trustStorePassword=<Password></Option>
</Options>
</JavaVM>
```

where, `<PATH_TO_TrustStore>` is the path to the truststore to which certificate is imported. For Example: The default trust store path `{PMDB_HOME}/keystore` created by OBR may be used.

`<Password>` is the Password to the truststore. For Example: `shradmin`

- c. Go to `/etc/init.d` directory and restart the `SAPBOBJEnterpriseXI40` service using the following commands:

On RHEL 6.x/SUSE Linux Enterprise Server 11:

- i. `service SAPBOBJEnterpriseXI40 stop`
- ii. `service SAPBOBJEnterpriseXI40 start`

On RHEL 7.x:

- i. `systemctl stop SAPBOBJEnterpriseXI40.service`
- ii. `systemctl start SAPBOBJEnterpriseXI40.service`

4. Click **Next**. The **Management Database Creation** page is displayed.

Note: If you do not proceed to **Management Database Creation** page even after clicking **Next**, refresh the browser and continue with post installation steps.

Tip: You may disable the TLS for Vertica. For information to disable, see [Disable TLS for Vertica](#).

Creating Database Schema for Remote Vertica

If OBR and Vertica are installed on different system then create the Vertica database before you begin the guided or post-install configuration.

Follow these tasks to create the Remote Vertica database:

1. Run the script on remote system where Vertica is installed
2. Perform post-install configuration on system where OBR is installed
3. Complete the additional certificate configurations

Note: You must ensure that bash is the default SHELL to run the commands for Vertica.

Task 1: Run the script on remote system where Vertica is installed

The `CreateVerticaDatabase.sh` script helps to create vertica database on a remote system. This script provides the option to enable TLS for Vertica database.

```
$PMDB_HOME/bin/CreateVerticaDatabase.sh <Vertica DBA User Name> <DBA User Password>  
<Database File Location> <Catalog File Location> <Vertica Database User name >  
<Vertica Database User name Password> <Database Name> t1son/t1soff
```

```
generatedcertificates/providedCertificates <server certificate file  
Location><server key file Location>
```

where,

- *<Vertica DBA User Name>* is the Vertica database user name with DBA privilege to log on to Vertica database
- *<DBA User Password>* is the Vertica database password to log on to the Vertica database
- *<Database File Location>* is the path to create the Vertica database
- *<Catalog File Location>* is the path to create the Vertica catalog
- *<Vertica Database User name>* is the Vertica Database user name
- *<Vertica Database User name Password>* is the password for Vertica Database user name
- *<Database Name>* is the name of Vertica database. This is an optional parameter. By default, the name of the Vertica database is PMDB.
- *tlson/tlsoff* is the option for Vertica with or without TLS.
- *generatedcertificates* is the option for Vertica with TLS and Certificate generated by OBR. When *generatedcertificates* is selected, the *serverca.crt* and *server.key* file will be created in *{PMDB_HOME}/config* folder on the database host.
- *providedcertificates* is the option for Vertica with TLS and self provided certificate. Type the complete path to the *<server certificate file location>* certificate path and *<server key file location>* key location.
- *<server certificate file location>* is the path of the self provided certificate file. Type the complete path of the file if you have opted for *providedcertificates*.
- *<server key file location>* is the path of the self provided certificate key file. Type the complete path of the file if you have opted for *providedcertificates*.

Run the `CreateVerticaDatabase.sh` script on the system where vertica is installed based on the scenarios described as follows:

Scenario 1: TLS is enabled with OBR generated certificates

```
$PMDB_HOME/bin/CreateVerticaDatabase.sh <Vertica DBA User Name> <DBA User Password>  
<Database File Location> <Catalog File Location> <Vertica Database User name >  
<Vertica Database User name Password> <Database Name> tlson generatedCertificates
```

Example:

```
$PMDB_HOME/bin/CreateVerticaDatabase.sh verticadba password /opt/data /opt/catalog  
verticausr password pmdb tlson generatedCertificates
```


Scenario 2: TLS is enabled with self provided certificates

```
$PMDB_HOME/bin/CreateVerticaDatabase.sh <Vertica DBA User Name> <DBA User Password>  
<Database File Location> <Catalog File Location> <Vertica Database User name >  
<Vertica Database User name Password> <Database Name> tlon providedCertificates  
<server certificate file location> <server key file location>
```

Example:

```
$PMDB_HOME/bin/CreateVerticaDatabase.sh verticadba password /opt/data /opt/catalog  
verticausr password pmdb tlon providedCertificates <server certificate file  
location> <server key file location>
```

Scenario 3: TLS is not enabled

```
$PMDB_HOME/bin/CreateVerticaDatabase.sh <Vertica DBA User Name> <DBA User Password>  
<Database File Location> <Catalog File Location> <Vertica Database User name >  
<Vertica Database User name Password> <Database Name> tloff
```

Example:

```
$PMDB_HOME/bin/CreateVerticaDatabase.sh verticadba password /opt/data /opt/catalog  
verticausr password pmdb tloff
```

Task 2: Perform post-install configuration on system where OBR is installed

During post install configuration, to configure Vertica database on system where OBR is installed, log on to the Administration Console on OBR system.

The screenshot shows the 'Vertica Database Creation' step in the 'Configuration Wizard'. The sidebar on the left lists the steps: Time Zone Selection, Vertica Database Creation (highlighted), Management Database Creation, and Collector Configuration. The main area contains the following sections:

- Remote Database:** A checked checkbox with a note: "Note: If OBR and Vertica are installed on different systems then create a Vertica database before you continue."
- Enable TLS:** A checked checkbox. Below it are two radio button options: "Generated certificates" (unselected) and "Provided certificates" (selected). A note for "Provided certificates" states: "The Vertica database connection will be secured using your own certificates."
- Enter Vertica Database Information:** Input fields for Host name (btpvm3017.hpswlab.net), Port (5433), Database file location, Catalog file location, and Database name (pmdb).
- Enter Vertica Database User (DBA Privilege) Information:** Input fields for DBA user name, Password, and Confirm password.
- Enter Vertica Database User Information:** Input fields for User name, Password, and Confirm password.
- Enter TLS Configuration Information:** Input fields for Truststore file, Truststore password, Confirm password, Server certificate file, and Server private key file.

1. In the **Configuration Wizard > Create Vertica Database** step, type the Vertica database configuration parameter as follows:

Field	Description
Remote Database	Select this option as Vertica database is created on a remote system.
Enable TLS	Select to enable Vertica connection over TLS. By default, this field is selected.
Generated certificates	Select to enable the configuration wizard to generate default SSL certificates. When Generated certificates is selected, the <code>serverca.crt</code> and <code>server.key</code> file will be created in <code>{PMDB_HOME}/config</code> folder on the database host. Follow these steps if you have selected Enable TLS and Generated certificates : a. Make sure that you have run the <code>CreateVerticaDatabase.sh</code> script to create

Field	Description
	<p>Vertica database.</p> <ol style="list-style-type: none"> From the Vertica server <code>\$PMDB_HOME/config</code> directory, copy the <code>serverca.crt</code> file. On the OBR server, go to <code>\$PMDB_HOME/config</code> directory and paste the <code>serverca.crt</code> file. Import the <code>serverca.crt</code> to the truststore of OBR. Run the following command: <pre>keytool -import -file serverca.crt -alias importcert -keystore <File name> -storepass <Password></pre> <p>where, <code><File name></code> is the trust store file name with path. For Example: The default trust store path <code>{PMDB_HOME}/keystore</code> created by OBR may be used.</p> <p><code><Password></code> is the password. For example: <code>shradmin</code></p>
Provided certificates	<p>Select to provide your own certificates to secure database connection.</p> <p>Follow these steps if you have selected Enable TLS and Provided certificates:</p> <ol style="list-style-type: none"> Make sure that you have run the <code>CreateVerticaDatabase.sh</code> script to create Vertica database. Make sure the self provided certificates are imported to the truststore on OBR. <p>For Example: The default trust store path <code>{PMDB_HOME}/keystore</code> created by OBR may be used.</p> <p>For more information on the Vertica recommendations for Certificates, see Vertica Documentation.</p> <p>Tip: It is recommended to use the CA certificates than the self-signed certificates.</p>
<i>Enter Vertica Database Information</i>	
Host name	Name of the host where the Vertica database server is running.
Port	Port number to query the database server. The default port is 5433.
Database File Location	Location or path where you want to store the database files. This field is disabled.
Catalog File Location	Location or path where the database metadata information will be stored. This field is disabled.

Field	Description
Database Name	Name of the Vertica database. By default, the database name is PMDB. You can edit the Vertica database name.
<i>Enter Vertica Database User (DBA Privilege) Information</i>	
DBA User Name	Vertica database user name with DBA privilege to log on to Vertica database. This field is disabled.
Password	Vertica database password to log on to the Vertica database. This field is disabled.
Confirm Password	Retype the password to confirm it. This field is disabled.
<i>Enter Vertica Database User Information</i>	
User Name	Enter the Vertica database user name.
Password	Enter the Vertica database user name password.
Confirm Password	Retype the password for Vertica database user name to confirm.
<i>Enter TLS Configuration Information</i>	
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.
Confirm password	Re-type the password provided to access the truststore. This option is displayed when Enable TLS is selected.
Server	Type the path of the server . crt file if the Provided certificates is selected.

Field	Description
certificate file	This field is disabled if the Remote Database is selected.
Server private key file	Type the path of the server .key file if the Provided certificates is selected. This field is disabled if the Remote Database is selected.

2. (Optional - Perform this step only if you have Enabled TLS) ["Task 3: Complete the additional certificate configurations"](#) below.
3. Click **Next**. The **Management Database Creation** page appears.

Note: If you do not proceed to **Management Database Creation** page even after clicking **Next**, refresh the browser and continue with post installation steps.

Caution: In a distributed scenario, if OBR is installed on Windows, irrespective of BO installed on Windows or Linux or on the same system or different system, you must configure DSN on OBR system (installed on Windows) to connect to Vertica database. If OBR is installed on Linux then installer automatically handles the DSN configuration and connection to Vertica database.

To configure DSN, see ["Configuring DSN on Windows for Vertica Database Connection"](#) on page 178.

Tip: You may disable the TLS for Vertica. For information to disable, see [Disable TLS for Vertica](#).

Task 3: Complete the additional certificate configurations

Follow these steps according to the OBR installation scenarios listed below:

- ["For OBR and SAP BusinessObjects server on a single Linux system"](#) below
- ["For OBR and SAP BusinessObjects server on a single Windows system"](#) on the next page
- ["For remote OBR server"](#) on page 48
- ["For remote SAP BusinessObjects server"](#) on page 48

For OBR and SAP BusinessObjects server on a single Linux system

1. To configure SSL for the ODBC Clients, run the following command on a command prompt:

```
echo 'SSLMode = require' >> $PMDB_HOME/config/odbc.ini
```
2. To configure TLS for SAP BusinessObjects, follow these steps:

- a. Go to the location `/opt/HP/BSM/BOE4/sap_bobj/enterprise_xi40/dataAccess/connectionServer`
- b. Open the `cs.cfg` file and add/edit the lines to file as follows:

```

<JavaVM>
<!-- The default JVM configuration can be overridden here -->
<!-- Use an absolute path for the JVM -->
<!--
<LibraryName JNIVersion="JNI_VERSION_1_4">ABSOLUTE_
PATH/jvm.dll</LibraryName>
-->
<Options>
<Option Processor="64">-Xmx2048m</Option>
<Option>-Xrs</Option>
<Option>-Djavax.net.ssl.trustStore=<PATH_TO_TrustStore></Option>
<Option>-Djavax.net.ssl.trustStorePassword=<Password></Option>
</Options>
</JavaVM>

```

where, `<PATH_TO_TrustStore>` is the path to the truststore to which certificate is imported. For Example: The default trust store path `{PMDB_HOME}/keystore` created by OBR may be used.

`<Password>` is the Password to the truststore. For Example: `shradmin`

- c. Go to `/etc/init.d` directory and restart the `SAPBOBJEnterpriseXI40` service using the following commands:

On RHEL 6.x/SUSE Linux Enterprise Server 11:

- i. `service SAPBOBJEnterpriseXI40 stop`
- ii. `service SAPBOBJEnterpriseXI40 start`

On RHEL 7.x:

- i. `systemctl stop SAPBOBJEnterpriseXI40.service`
- ii. `systemctl start SAPBOBJEnterpriseXI40.service`

For OBR and SAP BusinessObjects server on a single Windows system

1. To configure SSL for the ODBC Clients, perform the steps mentioned in "[Configure SSL for ODBC clients](#)" on page 221.

2. To configure TLS for SAP BusinessObjects, follow these steps:

a. Go to the location <OBR install Directory>:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\dataAccess\connectionServer\

b. Open the cs.cfg file and add/edit the lines to file as follows:

```
<JavaVM>
<!-- The default JVM configuration can be overridden here -->
<!-- Use an absolute path for the JVM -->
<!--
<LibraryName JNIVersion="JNI_VERSION_1_4">ABSOLUTE_
PATH/jvm.dll</LibraryName>
-->
<Options>
<Option Processor="64">-Xmx2048m</Option>
<Option>-Xrs</Option>
<Option>-Djavax.net.ssl.trustStore=<PATH_TO_TrustStore></Option>
<Option>-Djavax.net.ssl.trustStorePassword=<Password></Option>
</Options>
</JavaVM>
```

where, <PATH_TO_TrustStore> is the path to the truststore to which certificate is imported. For Example: The default trust store path {PMDB_HOME}/keystore created by OBR may be used.

<Password> is the Password to the truststore. For Example: shradmin

c. Restart the SAP BusinessObjects services as follows:

- i. From the **Start**, type **Run** in **Search**. The Run dialog box appears.
- ii. Type **services.msc** in the open field, and then press **ENTER**. The Services window appears.
- iii. Right-click on the following services and click **Restart**:
 - Business Objects Webserver

Server Intelligent Agent (OBR)
SQL Anywhere for SAP Business Intelligence

For remote OBR server

1. Configure SSL for the ODBC Clients as follows:

On Linux: Run the command `echo 'SSLMode = require' >> $PMDB_HOME/config/odbc.ini`

On Windows: Perform the steps mentioned in ["Configure SSL for ODBC clients" on page 221](#).

For remote SAP BusinessObjects server

1. Import the certificate to the truststore available on SAP BusinessObjects. Run the following command:

```
keytool -import -file <serverca.crt> -alias importcert -keystore <File name>  
storepass <Password>
```

where, `serverca.crt` is the CA certificate file path

`<File name>` is the truststore path on SAP BusinessObjects server. For Example: The default trust store path `{PMDB_HOME}/keystore` created by OBR may be used.

`<Password>` is the Password to the truststore. For Example: `shradmin`

2. To configure TLS for SAP BusinessObjects, follow these steps:

- a. Go to the following location:

On Linux: `/opt/HP/BSM/BOE4/sap_bobj/enterprise_xi40/dataAccess/connectionServer`

On Windows: `<OBR install Directory>:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\dataAccess\connectionServer\`

- b. Open the `cs.cfg` file and add/edit the lines to file as follows:

```
<JavaVM>  
  
<!-- The default JVM configuration can be overridden here -->  
  
<!-- Use an absolute path for the JVM -->  
  
<!--  
  
<LibraryName JNIVersion="JNI_VERSION_1_4">ABSOLUTE_  
PATH/jvm.dll</LibraryName>  
  
-->
```



```

<Options>
<Option Processor="64">-Xmx2048m</Option>
<Option>-Xrs</Option>
<Option>-Djavax.net.ssl.trustStore=<PATH_TO_TrustStore></Option>
<Option>-Djavax.net.ssl.trustStorePassword=<Password></Option>
</Options>
</JavaVM>

```

where, *<PATH_TO_TrustStore>* is the path to the truststore to which certificate is imported. For Example: The default trust store path {PMDB_HOME}/keystore created by OBR may be used.

<Password> is the Password to the truststore. For Example: shradmin

- c. Restart the SAP BusinessObjects services as follows:

On Linux:

Go to /etc/init.d directory and run the following commands:

On RHEL 6.x/SUSE Linux Enterprise Server 11:

- i. service SAPBOBJEnterpriseXI40 stop
- ii. service SAPBOBJEnterpriseXI40 start

On RHEL 7.x:

- i. systemctl stop SAPBOBJEnterpriseXI40.service
- ii. systemctl start SAPBOBJEnterpriseXI40.service

On Windows:

- i. From the **Start**, type **Run** in **Search**. The Run dialog box appears.
- ii. Type **services.msc** in the open field, and then press **ENTER**. The Services window appears.
- iii. Right-click on the following services and click **Restart**:
 - Business Objects Webserver
 - Server Intelligent Agent (OBR)
 - SQL Anywhere for SAP Business Intelligence

Verification on the system where Vertica is installed

Check Vertica Service Status

To check the status of the Vertica service, run the following commands on the command line interface:

On RHEL 6.x/SUSE Linux Enterprise Server 11: `service HPE_PMDB_Platform_Vertica status`

On RHEL 7.x: `systemctl status HPE_PMDB_Platform_Vertica.service`

Verify Connectivity of Vertica User to Vertica Database

To verify the connectivity of the Vertica user to the Vertica database, follow these steps:

1. Run the following commands:

```
su - <Vertica User Name>
```

where, *<Vertica User Name>* is the Vertica database user name

```
vsq1
```

2. Type the Vertica database password and press Enter.

The Vertica user is connected to the Vertica database.

Verify Vertica Log Files

To verify the Vertica log files created by the Vertica, go to the following locations:

- `/opt/vertica/log` - This log directory has all the log files of Vertica application.
- `<Catalog File Location directory>/vertica.log` - This log file is created after the Vertica catalog directory is created.
- `$PMDB_HOME/temp/VerticaDbCreation.log` - This log file lists the logs related to the Vertica database creation.

Verification on the OBR system

Verify Network Connectivity in Distributed Scenario

In a distributed scenario, to check the connectivity between Vertica database installed on a remote system and OBR system, run the following command on OBR system:

```
/opt/vertica/bin/vs1 -U <Vertica User Name> -p 5433 -w <Vertica Database User name Password> -h <Verticahostname>
```

where, *<Vertica User Name>* is the Vertica database user name

<Vertica Database User name Password> is the Vertica database password

<Verticahostname> is the host name of the system where Vertica is installed

Task 3: Creating the Management Database User Account

The management database refers to the Online Transaction Processing (OLTP) store used by OBR to store its run-time data such as data process job stream status, runtime information for individual steps, and data source information.

On the **Management Database Creation** page, provide the user details for the management database.

The screenshot shows the 'Management Database Creation' page in the Operations Bridge Reporter. The page is part of a 'Configuration Wizard' and is currently on the 'Management Database Creation' step. The wizard steps are: Time Zone Selection, Vertica Database Creation, Management Database Creation (selected), and Collector Configuration. The main content area is titled 'Management Database Creation' and contains two sections: 'Enter Management Database User (DBA Privilege) and Password' and 'Enter Management Database User Information'. The first section has fields for 'User name' (postgres), 'New DBA Password', and 'Confirm New DBA Password'. The second section has fields for 'User name' (pmdb_admin), 'New DBA Password', and 'Confirm New Password'. Navigation buttons 'Previous', 'Next', and '?' are visible.

To create the management database user account, follow these steps:

1. In the **Enter Management Database User (DBA Privilege) and Password**, type the following values:

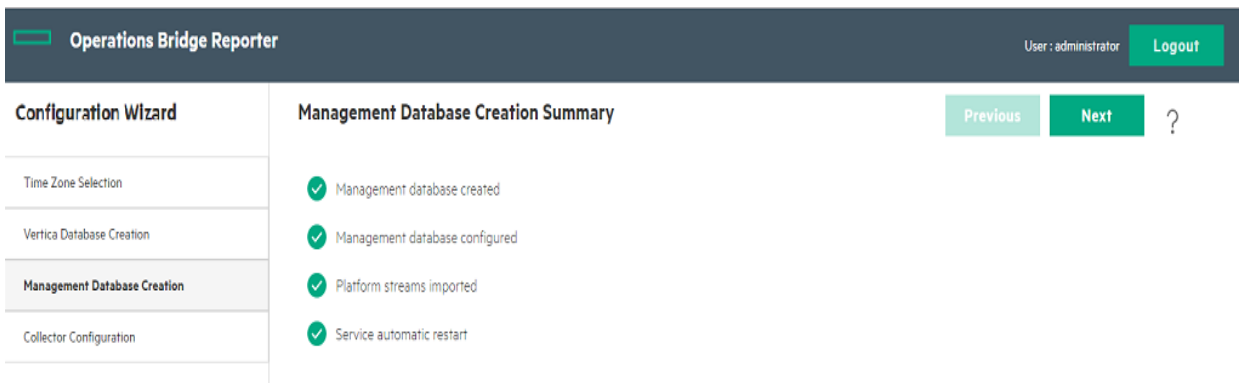
Field	Description
User name	Name of the PostgreSQL database administrator. The default value is postgres. You cannot edit this field.

Field	Description
New DBA Password	Enter the new password for PostgreSQL database administrator.
Confirm New DBA Password	Retype the same password to confirm it.

- In the **Enter Management Database User Information**, type the following values to change the password of the management database user:

Field	Description
User name	Name of the management database user. The default value is <code>pmdb_admin</code> . You cannot edit this field.
New Password	Enter new password for management database user.
Confirm New Password	Retype the same password to confirm it.

- Click **Next**. The confirmation dialog box appears.
- Click **Yes**. The **Management Database Creation Summary** page appears.
- Review the tasks completed as part of database connection and management database details and then click **Next**. The **Configure Collectors** page appears.



Check the status of HPE_PMDB_Platform_NRT_ETL service

Note: Perform the following steps only if the management database is created successfully and the **HPE_PMDB_Platform_NRT_ETL** service is not started automatically.

If the management database creation status is successful, the **HPE_PMDB_Platform_NRT_ETL** service is started automatically. If the service has not been started automatically, start the service manually.

To start the **HPE_PMDB_Platform_NRT_ETL** service manually, follow these steps:

1. Log on to the OBR system.
2. Start the service manually:

On Windows:

- Open the **Services** window, right-click the **HPE_PMDB_Platform_NRT_ETL** service, and then click **Start**.

On Linux:

- Go to the `/etc/init.d` directory, and then run the following command:

RHEL 6.x/SUSE Linux Enterprise Server 11: `service HPE_PMDB_Platform_NRT_ETL start`

RHEL 7.x: `systemctl start HPE_PMDB_Platform_NRT_ETL.service`

Task 4: Configuring the Remote Collectors

Before you proceed to configure the collector, it is mandatory to run the following command on the remote collector system:

On Windows:

```
"perl %PMDB_HOME%\bin\scripts\configurePoller.pl <OBR server system name>"
```

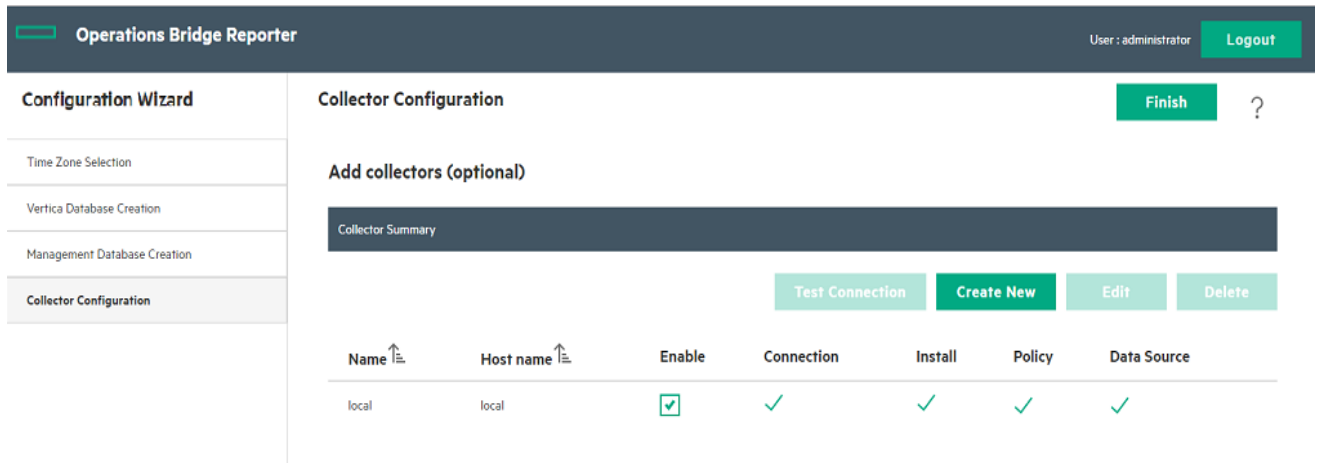
On Linux:

```
"perl $PMDB_HOME/bin/scripts/configurePoller.pl <OBR server system name>"
```

Note: The command above ensures that a certificate is exchanged between the OBR server system and the collector system; this exchange sets up the communication channel between OBR and the remote collector system. You can configure an instance of collector to use only one instance of OBR. Configuring a collector with multiple instances of OBR is not supported.

On the **Collector Configuration** page, you can create and configure remote collector(s).



Note: By default, the installer in OBR configures the local collector(s).



1. On the **Configure Collectors** page, click **Create New**.

The **Configuration Parameters** section appears, type the following values:

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: The name cannot be changed once configured.
Host name	IP address or FQDN of the database server to enable or disable the remote collector. If any data source has already been assigned to any remote collector for data collection, then the application will not allow you to disable the remote collector.

2. Click **Save** to complete the creation of the collector.
3. In the **Collector Configuration** page, click  icon in **Policy** to synchronize the policy for a newly created remote collector.
4. Click  icon in **Data Source** to synchronize the policy for a newly created remote collector.
5. Click **Test Connection** to check the status of the connection.

If the status report shows Test Connection Failed, follow these steps:

- a. Log on to the collector system.
- b. Check that the **HPE_PMDB_Platform_Collection** is started.

If the service is not started, manually start the service.

- c. To start the service manually, follow these steps:

On Windows:

- Open the **Services** window, right-click the **HPE_PMDB_Platform_Collection** service, and then click **Start**.

On Linux:

- Go to the `/etc/init.d` directory, and then run the following command:

On RHEL 6.x/SUSE Linux Enterprise Server 11: `service HPE_PMDB_Platform_Collection start`

On RHEL 7.x: `systemctl start HPE_PMDB_Platform_Collection.service`

Note: Once you complete the remote collector configuration, ensure to restart the **HPE_PMDB_Platform_Collection** service manually on the collector system.

6. Click **Finish**. The dialog box appears, click **Yes** to continue with the Data Source Selection or click **No** to go to Dashboard.



You can continue to select the data sources later from the **Administration Console > Data Source Selection Wizard** tab.

Note: Once you complete the remote collector configuration, ensure to restart the **HPE_PMDB_Platform_Collection** service manually on the collector system.

Data Source Selection Wizard

After completing tasks in Configuration Wizard, the Data Source Selection Wizard appears immediately after you select **Yes** in the pop-up. You can perform the following selections using this wizard:

- Data Source Selection based on your deployment scenarios
- Topology Source Configuration

- Content Type Selection
- OMi Management Packs/OM SPIs Selection
- Content Pack Deployment
- Data Source Configuration

Tip: You may go to the Dashboard after completing the Configuration Wizard and configure the data sources later. The Data Source Selection Wizard appears in the left pane of the Administration Console.

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 <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/APM/OMi BSM 9.2x or OMi 10.x	<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

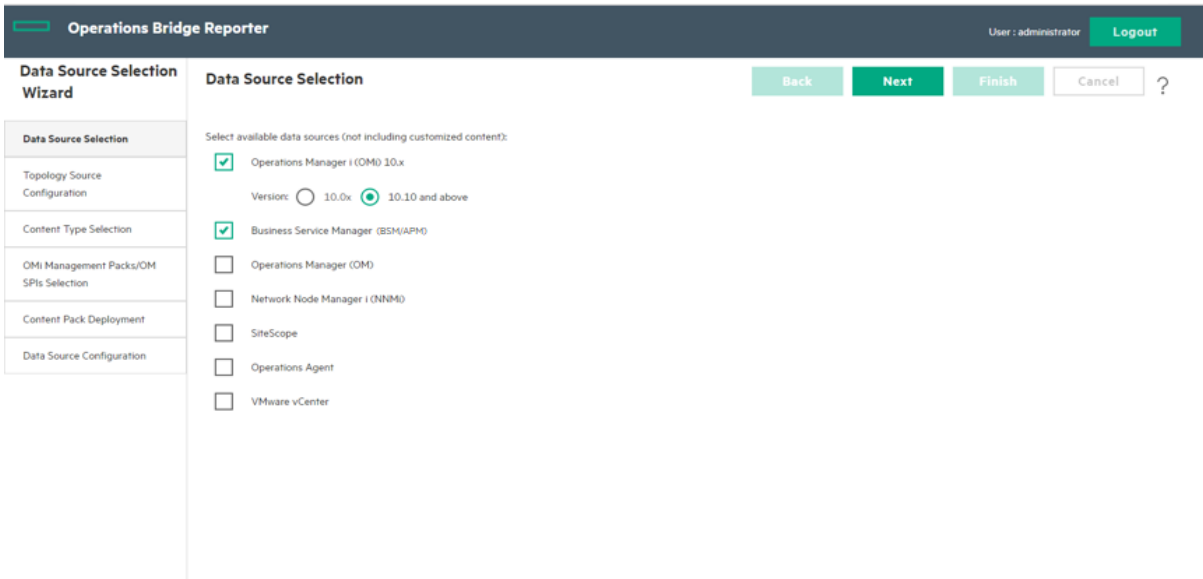
Deployment Scenario	Areas of Monitoring
	<ul style="list-style-type: none"> ○ OMi Events ○ Service Health ● End User Monitoring <ul style="list-style-type: none"> ○ Real User Monitor ○ Business Process Monitor ● Enterprise Application Performance <ul style="list-style-type: none"> ○ Microsoft SQL Server ○ Microsoft Exchange Server ○ Microsoft Active Directory ○ Oracle ○ Oracle Weblogic Server ○ IBM Webshpere Application Server
VMware vCenter only	<ul style="list-style-type: none"> ● Virtual Environment Performance ● Network Performance
Others	<ul style="list-style-type: none"> ● Network Performance

Tip: Plan and select the Data Source based on your deployment scenarios and content requirement. Also, remember to select all the dependencies (data source and content packs) during data source configuration and content packs installation.

For example, to report on Real User Transaction Monitoring, select Service Health in the Content Type and HIKPI_Reports_ServiceHealth Content pack and all other dependent content packs in the Content Pack deployment page.

Task 1: Data Source Selection

On the **Data Source Selection** page, select the data sources that you want OBR to collect the data according to your deployment scenario.



Tip: If you are not selecting the data source in post-install configuration, you can select it later on the **Data Source Selection Wizard** page in the Administration Console. Click **Next** to go to the end of the Wizard and click **Finish**.

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 <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 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

Data Sources for the OM Deployment Scenario

To collect data for OM, follow these steps:

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**.

Data Sources for the BSM/APM or OMi Deployment Scenario

You must configure the following data collectors in OBR:

- **Database collector** - to collect historical Synthetic Transaction Monitoring (BPM) and Real User Monitoring (RUM) data from the BSM database. It also collects events, messages, availability, and performance Key Performance Indicators (KPIs) from the databases of data sources such as Profile database, OM, and OMi databases.
- **Operations Agent collector** - to collect system performance metrics and data related to applications, databases, and system resources. The data is collected by the Operations Agents that are installed on the managed nodes.

To collect data for BSM/APM and/or OMi, follow these steps:

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.

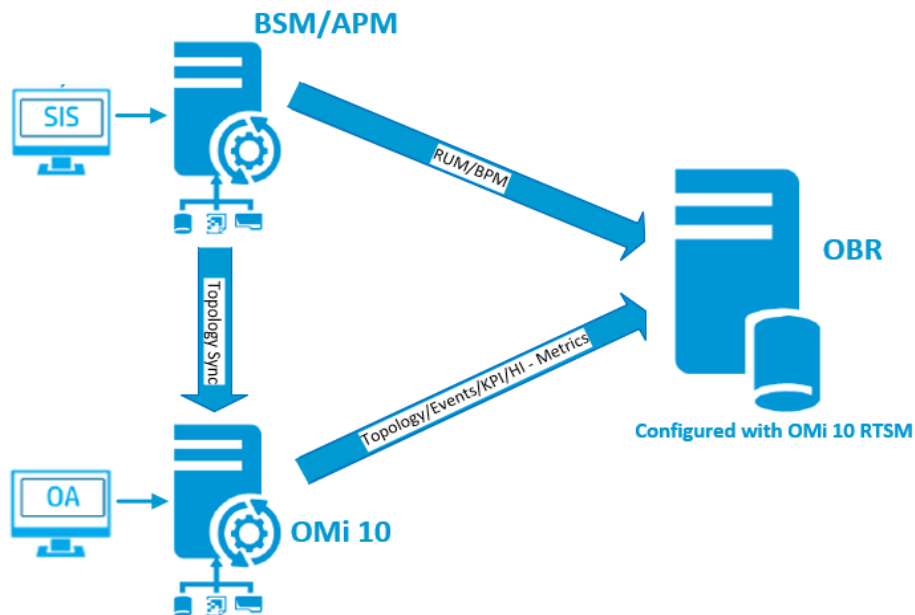
If you have BSM/APM deployed in your environment, select **Business Service Manager (BSM/APM)**. If you have only OMi 10.x deployed in your environment, select **Operations Manager i (OMi) 10.x**. If you have both BSM/APM and OMi 10.x deployed in your environment and BSM/APM and OMi 10 systems are integrated,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

For additional deployment configurations using BSM/APM and OMi, see:

- ["OMi10 Topology Source with Integrated BSM/APM"](#)
 - [" OMi10 Topology Source after BSM Upgrade"](#)
3. (Optional). You may select **SiteScope** for system performance, **Operations Agent** and **VMware vCenter** data source for the virtual environment
 4. Click **Next**

OMi10 Topology Source with Integrated BSM/APM

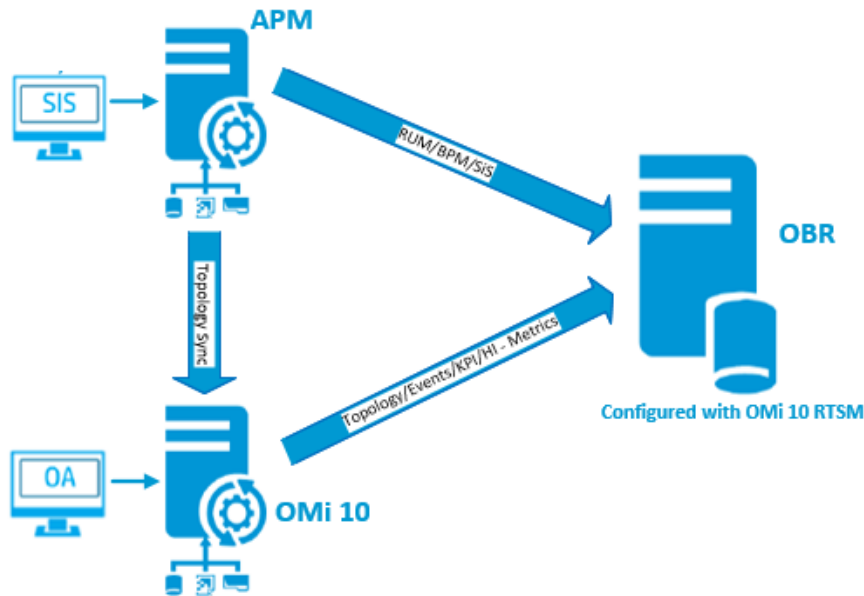
While you can configure BSM/APM and OMi10 as standalone topology and data sources, you can also setup BSM/APM to synchronize topology data with the OMi10 system.



In this configuration, the OMi10 system provides topology data and fact data for Operations Events and KPI. The BSM/APM system provides fact data from RUM and BPM that are directly configured with it. For enabling topology sync between BSM/APM and OMi10, see the respective documentation.

Note: Use the NPS RTSM ETL (**NetworkPerf_ETL_PerfiSPI_RTSM**) Content Pack component, if NNMi is integrated to OMi RTSM. Otherwise, use the non NPS RTSM ETL (**NetworkPerf_ETL_PerfiSPI_NonRTSM**) Content Pack component. In an APM only deployment scenario, the NetworkPerf_ETL_PerfiSPI_RtSM integration is not supported.

OMi10 Topology Source with Integrated APM

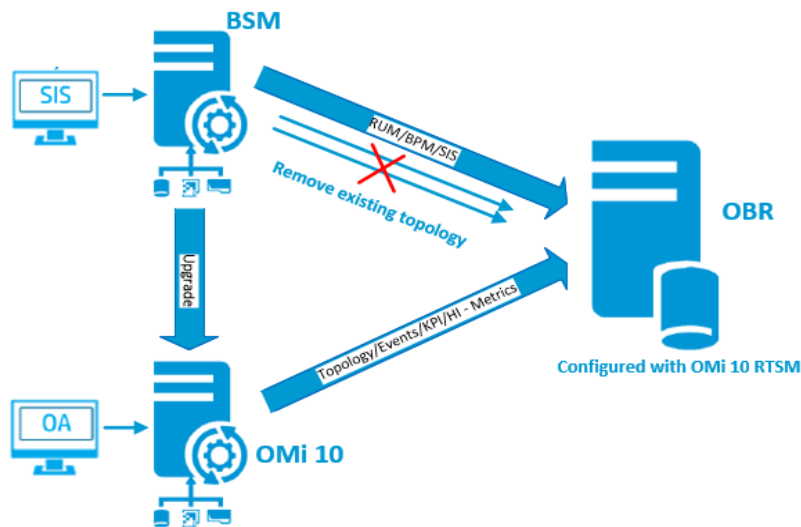


In this configuration, the OMi10 system provides topology data and fact data for Operations Events and KPI. The APM system provides fact data from RUM, BPM, SiteScope and Service Health that are directly configured with it. For enabling topology sync between APM and OMi10, see the respective documentation.

To configure the topology source in OBR, see ["Configuring RTSM Topology Source" on page 67](#)

OMi10 Topology Source after BSM Upgrade

While you can configure BSM and OMi10 as standalone topology and data sources, you can also upgrade your BSM system to an OMi10 system.



In this configuration, the existing topology synchronized between BSM system and OBR system is removed and the OMi10 system provides topology data for all nodes and fact data for Operations Events and KPI. The BSM system provides fact data from RUM, BPM, and SiteScope that are directly configured with BSM.

Note: In this scenario, if you are already using NPS RTSM ETL (**NetworkPerf_ETL_PerfiSPI_RTSM**) when OBR was connected to BSM 9.2x then ensure that NNMI is integrated to OMi 10 RTSM after BSM is upgraded to OMi 10 and BSM 9.24.

In this configuration, after the BSM system is upgraded to OMi, all topology and fact data is collected from OMi. To perform the upgrade, follow these steps:

Important: Perform the following steps only if the CIIDs for the CI(s) are unchanged after OMi upgrade.

For more information on OMi upgrade, see *Operations Manager i Installation and Upgrade Guide*.

1. Stop collection service manually from the BSM systems.
Wait until all data is loaded into OBR tables
2. Complete the BSM to OMi10 upgrade process.
3. From the **Administration Console > Content Pack Deployment** page:
 - a. Uninstall the older ETL component of BPM (SynTrans_ETL_BPM) and install the newer (SynTrans_ETL_BPM_OMi10) ETL component.
 - b. Uninstall the older ETL component of RUM (RealUsrTrans_ETL_RUM) and install the newer (RealUsrTrans_ETL_RUM_OMi10) ETL component.

- c. If SiteScope is integrated with OMi10 then install the SiteScope Direct API (SysPerf_ETL_SiS_API) ETL.
4. To modify the RTSM topology source for OMi, follow these steps:
 - a. Log on to Postgres database from OBR system using the command line interface:

```
psql -U pmdb_admin -p 21425 -d dwabc
```
 - b. Enter the password given at the time of management database creation during post-install configuration.
 - c. Run the following commands:

```
update dwabc.dict_cmdb_ds set hostname='<omi10hostname>';  
commit;
```

where <omi10hostname>, is the hostname of your OMi10.
5. Log in to **Administration Console > Data Source Configuration > Topology Source**, and click **Configure** to modify the user name, password, and port as relevant for OMi10.
6. Add Operations database connection of OMi in **Administration Console > Data Source Configuration > BSM/APM/OMi** page. For more details, see ["Configuring the Management and Profile Database Data Source" on page 132](#).
7. Enable HI/KPI Data Collection and optionally SiteScope.
8. Make the collection service manual and start the collection service.

Note: Ensure to configure the topology source to OMi10 in OBR soon after the upgrade and before starting the collection service. Otherwise OBR will continue to point and collect the data from BSM system even after upgrading to OMi10. During this period, if a new CI is discovered in BSM and this new CI is collected by OBR, it will end up being a duplicate in OBR when the topology is changed to OMi10. If you come across such situation, then use DLC to clean up the duplicates.

Data Source for the VMware vCenter Deployment Scenario

To collect data from VMware vCenter, follow these steps:

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**.

Data Sources for Other Database Deployment Scenario

To collect data for other databases, follow these steps:

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

Task 2: Configuring the Topology Source

Before you configure OBR for data collection, you must configure the topology source.

Note: If you are not configuring the topology source in post-install configuration, you can configure it on the **Data Source Configuration > Topology Source** page in the Administration Console. Click **Next** to go to the end of the Wizard and click **Finish**.

The topology source configuration tasks are organized into the following categories:

- If OBR is deployed in the OM environment, see "[Configuring OM Topology Source](#)" below.
- If OBR is deployed in the BSM or Operations Manager i, see "[Configuring RTSM Topology Source](#)" on page 67.
- If OBR is deployed in the VMware vCenter environment, see "[Configuring VMware vCenter Topology Source](#)" on page 71.

Note: OBR uses the identifier of the Configuration Items (CI) from the topology source to uniquely identify them for reporting. Changing the topology source can result in duplicate CIs because different topology sources do not use the same identifier for a certain CI. So, once a certain topology source (RTSM, OM, or VMware vCenter) is configured, you cannot change it later.

Configuring OM Topology Source

To configure OM topology source, follow these steps on the **Topology Source Configuration** page:

1. Click **Create New**. The **Connection Parameter** section appears.
2. In the **Connection Parameter**, type the following details:

Caution: 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.

Field	Description
Enable TLS	Enable JDBC connection over TLS.
Truststore Path	Full path along with the trust store file name. This option appears only if you have selected Enable TLS . Tip: It is recommended to have a common trust store file.
Truststore Password	The password to access the trust store. This option appears only if you have selected Enable TLS .
Datasource Type	Select the type of OM that is configured in your environment. The options include: 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.
Windows Authentication	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. This option only appears if OM for Windows is selected as the data source type.
Database name	Name of the database.
Database in Oracle RAC	This option appears only if you have selected Oracle 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.

Field	Description
Host name	IP address or fully-qualified domain name (FQDN) of the OM database server. The OM database is configured on a remote system, provide the machine name of the remote system. Host name is not displayed when the database type is Oracle and Management DB on Oracle RAC is selected.
Port	Port number to query the OM database server. To check the port number for the database instance, such as OVOPS, see "Checking for the OM Server Port Number" on page 102 .
Database instance	System Identifier (SID) of the database instance in the data source. The default database instance is OVOPS. If MSSQL Server is configured to use default (unnamed) database instance, leave this field empty.
User name	Name of the OM database user. For the OM for Windows data source type, if the Windows Authentication option is selected, this field is disabled and appears empty.
Password	Password of the OM database user. For the OM for Windows data source type, if the Windows Authentication option is selected, this field is disabled and appears empty.
Collection station	If you installed collectors on remote systems, you can choose either the local collector or a remote collector. To configure a remote collector with this topology source, select one of the available remote systems in the drop down list. To use the collector that was installed by default on the OBR system, select local.

3. Click **OK**.
4. Click **Save** to save the information.
5. Click **Test Connection**.
6. A success message appears in the information message panel.

You can configure additional OM data sources by repeating the same steps.

For more information about configuring OM topology sources, see *Managing the enterprise topology* section in the *Operations Bridge Reporter Online help for Administrators*.

Note: To collect data from non-domain hosts, appropriate DNS resolutions must be made by

the OM administrator for these hosts so that they are reachable by OBR, which is installed in the domain.

7. Click **Next**. The Content Type Selection page appears.

Supported Data Source Selections

In this deployment scenario, you can configure the following data sources to collect fact data:

- ["Configuring the Operations Manager Data Source" on page 119](#)
- ["Configuring the Operations Agent Data Source" on page 131](#)
- ["Configuring the Generic Data Source" on page 127](#)
- ["Configuring OBR with Network Node Manager i \(NNMi\)" on page 173](#)
- ["Configuring the VMware vCenter Data Source" on page 130](#)

Configuring RTSM Topology Source

To configure RTSM topology source, follow these steps on the **Configure Topology Source** page:

1. Click **Create New**. The **Connection Parameter** appears.
2. In the **Connection Parameter**, type the following details:

Field	Description
Host name	IP address or FQDN of the BSM/APM or OMi server. If your BSM/APM installation is distributed, type the name of the gateway server in the field. Note: In a distributed BSM/APM 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 default port number is 80. If the port number has been changed, contact your BSM/APM administrator for more information.
User name	Name of the RTSM web service user. The default user name is admin. Note: You can use the user with only <i>RTSMOpenApiUser</i> role assigned to it.

Field	Description
Password	Password of the RTSM web service user.
Collection station	<p>If you installed collectors on remote systems, you can choose either the local collector or a remote collector.</p> <p>To configure a remote collector to collect data from this RTSM 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>

3. Click **OK**.
4. Click **Save** to save the information.
5. Click **Test Connection**.

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

6. A success message appears in the information message panel.

You can configure additional RTSM data sources by repeating the same steps.

For more information about configuring RTSM topology sources, see *Managing the enterprise topology* section in *Operations Bridge Reporter Online help for Administrators*.

7. Click **Next**. The Content Type Selection page appears.

Configure Data Collection When HTTPS is Enabled for RTSM

Note: In case of remote collector, follow the same configuration steps on the system where remote collector is installed.

If RTSM is HTTPS enabled, follow these steps:

1. Set the port to 443 when RTSM is HTTPS enabled during topology source configuration.
2. Export the BSM/OMi 10 root CA certificate. You can use the `opr-cert-mgmt` command-line interface to get certificates. For more information about other options that OMi provides to get the certificates, see *OMi Administration Guide*.

Note: If FIPS is enabled, export the certificate in PKCS12 format, else export in PEM format.

3. *Import the BSM/OMi 10 root CA certificate into OBR server trust store. To import the CA certificates, follow these steps:*

a. **On Windows**

```
keytool -import -trustcacerts -keystore <Path to store> -file "<filename with path>"
```

b. **On Linux**

```
keytool -import -trustcacerts -keystore <Path to store> -file "<filename with path>"
```

where, <filename with path> is the location and file name of the BSM/OMi CA certificates.

<Path to store> is the path to the trust store. You have to mention the same path in the collection service.

For Example: The default trust store path {PMDB_HOME}/keystore created by OBR may be used.

4. On the collector system chosen in above configuration, add the following fields in config.prp, located at %PMDB_HOME%\data (**on Windows**) \$PMDB_HOME/data (**on Linux**):

Field	Value
ucmdb.protocol	https Important: You must make sure to add ucmdb.protocol value in {PMDB_HOME}/data/config.prp file on the OBR server.
shr.truststorepath	Full path to the keystore file. Example: C:\\\HPE-OBR\\PMDB\\keystore\\SHR_CERT_HTTPS.jks
shr.truststorepassword	Password of the keystore
shr.truststoretype	Type of the trust store - JKS or PKCS12

5. Follow these steps to add the entries in collection service scripts:

a. **On Windows**

- i. Open the Services window, right-click the **HPE_PMDB_Platform_Collection** service, and then click **Stop**.
- ii. Add -Djavax.net.ssl.trustStore=<Path to store> -Djavax.net.ssl.trustStorePassword=<password> to JVM_ARGS in %PMDB_HOME%\bin\CollectionServiceCreation.bat file.

where, <Path to store> is the path to the trust store. Example: C:\\HPE-OBR\\PMDB\\keystore\\SHR_CERT_HTTPS.jks

- iii. Recreate the collection service, follow these steps:
 - A. Open the command line console, run the following commands:

```
CollectionServiceCreation.bat -remove <OV Install Directory>  
<Product Install Directory>  
  
CollectionServiceCreation.bat -install <OV Install Directory>  
<Product Install Directory>  
  
where, <OV Install Directory> is %OVIInstallDir%  
  
<Product Install Directory> is %PMDB_HOME%\..
```
 - iv. Open the Services window, right-click the **HPE_PMDB_Platform_Collection** service, and then click **Start**.

b. On Linux

- i. Go to /etc/init.d directory, and run the following command:
On RHEL 6.x/SUSE Linux Enterprise Server 11: service HPE_PMDB_Platform_Collection stop
On RHEL 7.x: systemctl stop HPE_PMDB_Platform_Collection.service
- ii. Add -Djavax.net.ssl.trustStore=<Path to store> -Djavax.net.ssl.trustStorePassword=<password> to JVM_ARGS in \$PMDB_HOME/bin/hpbsm_pmdb_collector_start.sh files.
where, <Path to store> is the path to the trust store.
- iii. Go to /etc/init.d directory, and run the following command:
On RHEL 6.x/SUSE Linux Enterprise Server 11: service HPE_PMDB_Platform_Collection start
On RHEL 7.x: systemctl start HPE_PMDB_Platform_Collection.service

6. Stop and start the HPE_PMDB_Platform_Administration service as follows:

On Windows:

- a. Open the Services window, right-click the **HPE_PMDB_Platform_Administration** service, and then click **Stop**.
- b. Wait for the service to stop.
- c. Open the Services window, right-click the **HPE_PMDB_Platform_Administration** service, and then click **Start**.

On Linux:

- a. Go to the `/etc/init.d` directory, and run the following command:

On RHEL 6.x/SUSE Linux Enterprise Server 11: `service HPE_PMDB_Platform_Administration stop`

On RHEL 7.x: `systemctl stop HPE_PMDB_Platform_Administration.service`

- b. Wait for the service to stop and then run the following command:

On RHEL 6.x/SUSE Linux Enterprise Server 11: `service HPE_PMDB_Platform_Administration start`

On RHEL 7.x: `systemctl start HPE_PMDB_Platform_Administration.service`

Supported Data Source Selections

In this deployment scenario, you can configure the following data sources to collect fact data:

- ["Configuring the Management and Profile Database Data Source" on page 132](#)
- ["Configuring the OMi Data Source" on page 140](#)
- ["Configuring the Operations Manager Data Source" on page 119](#)
- ["Configuring the Operations Agent Data Source" on page 131](#)
- ["Configuring the Generic Data Source" on page 127](#)
- ["Configuring OBR with Network Node Manager i \(NNMi\)" on page 173](#)
- ["Configuring the VMware vCenter Data Source" on page 130](#)
- ["Configuring the SiteScope Data Source" on page 122](#)

Configuring VMware vCenter Topology Source

To configure VMware vCenter topology source, follow these steps on the **Configure Topology Source** page:

1. Click **Create New**. The **Connection Parameter** section appears.
2. In the **Connection Parameter**, type the following details:

Field	Description
Host name	IP address or FQDN of the VMware vCenter server.

Field	Description
User name	Name of the VMware vCenter web service user. The <code>administration@vsphere.local</code> is the default user name.
Password	Password of the VMware vCenter web service user.
Collection station	<p>If you installed collectors on remote systems, you can choose either the local collector or a remote collector.</p> <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>

3. Click **OK**.
4. Click **Save** to save the information.
5. Click **Test Connection**.
6. A success message appears in the information message panel.

You can configure additional VMware vCenter data sources by repeating the same steps.

7. Click **Next**. The Content Type Selection page appears.

Restart the collector service

If you configured a remote collector with the service definition, make sure to restart the collector service on the collector system after installing Content Packs.

To restart the service manually, follow these steps:

On Windows:

- Open the Services window, right-click the **HPE_PMDB_Platform_Collection** service, and then click **Restart**.

On Linux:

- Go to the `/etc/init.d` directory, and then run the following command:

On RHEL 6.x/SUSE Linux Enterprise Server 11: `service HPE_PMDB_Platform_Collection restart`

On RHEL 7.x: `systemctl restart HPE_PMDB_Platform_Collection.service`

VMware stats Logging Levels

It is recommended to set the VMware stats logging level to 2. However, 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 following URL:

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

Supported Data Source Selections

In this deployment scenario, you can configure the following data sources to collect fact data:

- "Configuring the Generic Data Source" on page 127
- "Configuring OBR with Network Node Manager i (NNMi)" on page 173
- "Configuring the VMware vCenter Data Source" on page 130

Task 3: Content Type Selection

Based on the data sources selected, the content types will be listed in the Content Type Selection page.

Tip: If you are not selecting the content type in post-install configuration, you can select it later on the **Data Source Selection Wizard > Content Type Selection** page in the Administration Console. Click **Next** to go to the end of the Wizard and click **Finish**.

Follow these steps to select the content type according to your data sources:

OM Deployment Scenario

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**.

BSM or OMi Deployment Scenario

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 VMwareo IBM LPARo Microsoft Hyper-Vo Solaris Zones

5. Click **Next**.

VMware vCenter Deployment Scenario

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

Other Database Deployment Scenario

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.

For more information, see *Operations Bridge Reporter Performance, Sizing, and Tuning guide*.

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**.

Task 4: 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.

Tip: If you are not selecting the OMi Management Packs/OM SPIs in post-install configuration, you can select it later on the **Data Source Selection Wizard > OMi Management Packs/OM SPIs Selection** page in the Administration Console. Click **Next** to go to the end of the Wizard and click **Finish**.

Perform the following steps for each of the deployment scenario:

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 **Next**.

Task 5: Content Pack Deployment

The Data Source Selection Wizard provides Content Pack Deployment utility to install the content the required content packs during post-installation.

The **Content Pack Deployment** page is displayed with Content Packs selected based on the selections made in the [Data Source Selection](#).

For information to install Content Packs, see "[Install and Uninstall the Content Packs](#)" on page 103. Click **Next** to move ahead with the data source configuration.

Note: If you are not deploying the content packs in post-install configuration, you can configure it

on the **Content Pack Deployment** page from the Administration Console. Click **Next** to go to the end of the Wizard and click **Finish**.

Task 6: Data Source Configuration

After installing Content Packs, you must configure OBR to collect required data from various data collectors. The 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 where the collectors can collect the data using the Administration Console.

For information on configuring the data sources to collect the data, see ["Data Source Configuration" on page 117](#). After completing the configurations, click **Finish** to complete the data source selection using the wizard.

Note: If you are not configuring the data sources in post-install configuration, you can configure it on the **Data Source Configuration** tabs in the Administration Console. Click **Finish** to exit from the wizard.

You may install and configure additional Data Processors after completing the post-install configurations using Data Source Selection Wizard. For more information, see *Operations Bridge Reporter Interactive Installation Guide*.

Logon Banner

You can configure log on banner after post install configuration of OBR for Administration Console and SAP BusinessObjects. You can configure the text that is displayed on log on banner. The text should warn the users against unauthorized entry. Once you click **OK** on this screen, the usual log on screen is displayed.

For information on enabling and disabling the log on banner, see ["Configuring Logon Banner for OBR" on page 193](#).

Chapter 3: Configure OBR for BSM/APM/OMi Deployment Scenario

If you plan to configure OBR to work with a BSM/APM or OMi installation, you must make sure:

- BSM/APM/OMi is installed and configured successfully.
- If you are monitoring systems and applications using the Monitoring Automation component of OMi and Management Packs, make sure that necessary Management Pack policies are deployed.
- If you are monitoring systems and applications using underlying OM servers and Smart Plug-ins (SPIs), make sure that necessary SPI policies are deployed.
- Make sure to deploy necessary OMi views. See [Configuring RTSM Topology Source for OBR](#).

Configuring RTSM Topology Source for OBR

RTSM is a source of the topology information for OBR. The topology information includes all CIs as modeled and discovered in RTSM. Node resource (CPU, disk etc.) information is directly obtained from Operations Agent and SiteScope.

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 on Operations Agent:

- Microsoft Active Directory
- Microsoft Exchange
- Microsoft SQL Server
- Oracle
- Oracle WebLogic
- IBM WebSphere
- Systems Infrastructure
- Virtualization Infrastructure

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

In BSM/APM environment, RTSM is used to discover the CIs and generate the topology views. To configure OBR to collect domain-specific data, you first need to deploy those topology views for each Content Pack.

These topology views contain specific CI attributes that Contents Packs use to collect the relevant data. However, these topology views can vary from one Content Pack to another.

For example, the Exchange Server Content Pack might require a topology view that lists exchange servers, mailbox servers, mailbox and public folder stores, and so on. A System Management Content Pack, however, might require a different topology view that lists all the Business Applications, business services, and system resource, such as CPU, memory, disk, within the infrastructure. Based on these views, the CI attributes for each Content Pack may vary.

List of Content Pack and Topology Views to Deploy

On Windows:

Content Pack	View Name	Location
BPM (Synthetic Transaction Monitoring)	EUM_BSMR.zip(BSM only) EUM_OMi.zip(OMi 10 only)	%PMDB_ HOME%\packages\EndUserManagement\ETL_BPM.ap\source\cldb_views %PMDB_ HOME%\packages\EndUserManagement\ETL_BPM_OMi.ap\source\cldb_views Note: If BSM is the deployment scenario, then deploy only EUM_BSMR.zip view in the BSM server. If OMi 10 is the deployment scenario, then deploy only EUM_OMi.zip view in the OMi 10 server.
Real User Transaction Monitoring	EUM_BSMR.zip(BSM only) EUM_OMi.zip(OMi 10 only)	%PMDB_ HOME%\packages\EndUserManagement\ETL_RUM.ap\source\cldb_views %PMDB_ HOME%\packages\EndUserManagement\ETL_RUM_OMi.ap\source\cldb_views

Content Pack	View Name	Location
		<p>Note: If BSM is the deployment scenario, then deploy only EUM_BSMR.zip view in the BSM server.</p> <p>If OMi 10 is the deployment scenario, then deploy only EUM_OMi.zip view in the OMi 10 server.</p>
Network Performance	SHR_Network_Views.zip	%PMDB_HOME%\packages\Network\ETL_Network_NPS92_RTSM.ap\source\cmdb_views
Network Component_Health	No views	
Network Interface_Health	No views	
System Performance	SM_BSM9_Views.zip SM_SiS_Views.zip (APM 9.40 only)	<p>%PMDB_HOME%\packages\SystemManagement\ETL_SystemManagement_PA.ap\source\cmdb_views</p> <p>%PMDB_HOME%\packages\SystemManagement\ETL_SystemManagement_SiS_API.ap\source\cmdb_views</p> <p>%PMDB_HOME%\packages\SystemManagement\ETL_SystemManagement_SiS_API_NonRtSM.ap\source\cmdb_views</p> <p>%PMDB_HOME%\packages\SystemManagement\ETL_SystemManagement_SiS_DB.ap\source\cmdb_views</p> <p>Note: If APM 9.40 is the deployment scenario, then deploy only SM_SiS_Views.zip view in the APM server.</p>
Oracle	SHR_DBOracle_Views.zip SHR_DBOracle_OM.zip	%PMDB_HOME%\packages\DatabaseOracle\ETL_DBOracle_DBSPI.ap\source\cmdb_views
Oracle WebLogic Server	J2EEApplication.zip J2EEApplication_OM.zip	<p>For OM/SPI: %PMDB_HOME%\packages\ApplicationServer\ETL_AppSrvrWLS_WLSSPI.ap\source\cmdb_views</p> <p>For OMi/MP: %PMDB_</p>

Content Pack	View Name	Location
		HOME%\packages\ApplicationServer\ETL_AppSrvrWLS_WLSMP.ap\source\cldb_views
IBM WebSphere Application Server	J2EEApplication.zip J2EEApplication_OM.zip	For OM/SPI: %PMDB_HOME%\packages\ApplicationServer\ETL_AppSrvrWBS_WBSSPI.ap\source\cldb_views For OMi/MP: %PMDB_HOME%\packages\ApplicationServer\ETL_AppSrvrWBS_WBSMP.ap\source\cldb_views
Microsoft SQL Server	SHR_DBMSSQL_VIEWS.zip SHR_DBMSSQL_OM.zip	%PMDB_HOME%\packages\DatabaseMSSQL\ETL_DBMSSQL_DBSPI.ap\source\cldb_views
Microsoft Exchange Server	SHR_Exchange_Business_View.zip SHR_Exchange_OM.zip	Exchange Server 2007: %PMDB_HOME%\packages\ExchangeServer\ETL_Exchange_Server2007.ap\source\cldb_views Exchange Server 2010: %PMDB_HOME%\packages\ExchangeServer\ETL_Exchange_Server2010.ap\source\cldb_views Exchange Server 2013: %PMDB_HOME%\packages\ExchangeServer\ETL_Exchange_Server2013.ap\source\cldb_views
Microsoft Active Directory	SHR_AD_Business_View.zip SHR_ActiveDirectory_OM.zip	%PMDB_HOME%\packages\ActiveDirectory\ETL_AD_ADSPI.ap\source\cldb_views
Virtual Environment Performance	SM_BSM9_VIEWS.zip SM_SiS_VIEWS.zip (APM 9.40 only)	%PMDB_HOME%\packages\SystemManagement\ETL_SystemManagement_PA.ap\source\cldb_views %PMDB_HOME%\packages\SystemManagement\ETL_SM_VI_VMware_SiS_API.ap\source\cldb_views %PMDB_HOME%\packages\SystemManagement\ETL_SM_VI_VMware_SiS_DB.ap\source\cldb_views Note: If APM 9.40 is the deployment

Content Pack	View Name	Location
		scenario, then deploy only SM_SiS_Views.zip view in the APM server.
Health and Key Performance Indicators (Service Health)	All the views SM_SiS_Views.zip (APM 9.40 only)	%PMDB_HOME%\packages\ServiceHealth\ETL_SvcHealth_BSM.ap\source\cmdb_views Note: If APM 9.40 is the deployment scenario, then deploy only SM_SiS_Views.zip view in the APM server.
Server Automation	No views	
Cross-Domain Operations Events	All the views	
Operations Events	No views	

On Linux:

Content Pack	View Name	Location
BPM (Synthetic Transaction Monitoring)	EUM_BSMR.zip(BSM only) EUM_OMi.zip(OMi 10 only)	\$PMDB_HOME/packages/EndUserManagement/ETL_BPM.ap/source/cmdb_views \$PMDB_HOME/packages/EndUserManagement/ETL_BPM_OMi.ap/source/cmdb_views Note: If BSM is the deployment scenario, then deploy only EUM_BSMR.zip view in the BSM server. If OMi 10 is the deployment scenario, then deploy only EUM_OMi.zip view in the OMi 10 server.
Real User Transaction Monitoring	EUM_BSMR.zip(BSM only) EUM_OMi.zip(OMi 10 only)	\$PMDB_HOME/packages/EndUserManagement/ETL_RUM_OMi.ap/source/cmdb_views \$PMDB_HOME/packages/EndUserManagement/ETL_RUM_OMi.ap/source/cmdb_views Note: If BSM is the deployment scenario, then deploy only EUM_BSMR.zip view in the BSM server.

Content Pack	View Name	Location
		<p>If OMi 10 is the deployment scenario, then deploy only EUM_OMi.zip view in the OMi 10 server.</p>
Network Performance	SHR_Network_Views.zip	\$PMDB_HOME/packages/Network/ETL_Network_NPS92_RTSM.ap/source/cmdb_views
Network Component_Health	No views	
Network Interface_Health	No views	
System Performance	SM_BSM9_Views.zip SM_SiS_Views.zip (APM 9.40 only)	<p>\$PMDB_HOME/packages/SystemManagement/ETL_SystemManagement_PA.ap/source/cmdb_views</p> <p>\$PMDB_HOME/packages/SystemManagement\ETL_SystemManagement_SiS_API.ap/source/cmdb_views</p> <p>\$PMDB_HOME/packages/SystemManagement/ETL_SystemManagement_SiS_API_NonRtSM.ap/source/cmdb_views</p> <p>\$PMDB_HOME/packages/SystemManagement/ETL_SystemManagement_SiS_DB.ap/source/cmdb_views</p> <p>Note: If APM 9.40 is the deployment scenario, then deploy only SM_SiS_Views.zip view in the APM server.</p>
Oracle	SHR_DBOracle_Views.zip SHR_DBOracle_OM.zip	\$PMDB_HOME/packages/DatabaseOracle/ETL_DBOracle_DBSPI.ap/source/cmdb_views
Oracle WebLogic Server	J2EEApplication.zip J2EEApplication_OM.zip	<p>For OM/SPI: \$PMDB_HOME/packages/ApplicationServer/ETL_AppSrvrWLS_WLSSPI.ap/source/cmdb_views</p> <p>For OMi/MP: \$PMDB_HOME/packages/ApplicationServer/ETL_AppSrvrWLS_WLSMP.ap/source/cmdb_views</p>
IBM WebSphere	J2EEApplication.zip	For OM/SPI: \$PMDB_HOME/

Content Pack	View Name	Location
Application Server	J2EEApplication_OM.zip	packages/ApplicationServer/ETL_AppSrvrWBS_WBSSPI.ap/source/cmdb_views For OMi/MP: \$PMDB_HOME/packages/ApplicationServer/ETL_AppSrvrWBS_WBSMP.ap/source/cmdb_views
Microsoft SQL Server	SHR_DBMSSQL_VIEWS.zip SHR_DBMSSQL_OM.zip	\$PMDB_HOME/packages/DatabaseMSSQL/ETL_DBMSSQL_DBSPI.ap/source/cmdb_views
Microsoft Exchange Server	SHR_Exchange_Business_View.zip SHR_Exchange_OM.zip	Exchange Server 2007: \$PMDB_HOME/packages/ExchangeServer/ETL_Exchange_Server2007.ap/source/cmdb_views Exchange Server 2010: \$PMDB_HOME/packages/ExchangeServer/ETL_Exchange_Server2010.ap/source/cmdb_views Exchange Server 2013: \$PMDB_HOME/packages/ExchangeServer/ETL_Exchange_Server2013.ap/source/cmdb_views
Microsoft Active Directory	SHR_AD_Business_View.zip SHR_ActiveDirectory_OM.zip	\$PMDB_HOME/packages/ActiveDirectory/ETL_AD_ADSPI.ap/source/cmdb_views
Virtual Environment Performance	SM_BSM9_VIEWS.zip SM_SiS_VIEWS.zip (APM 9.40 only)	\$PMDB_HOME/packages/SystemManagement/ETL_SystemManagement_PA.ap/source/cmdb_views \$PMDB_HOME/packages/SystemManagement/ETL_SM_VI_VMware_SiS_API.ap/source/cmdb_views \$PMDB_HOME/packages/SystemManagement/ETL_SM_VI_VMware_SiS_DB.ap/source/cmdb_views Note: If APM 9.40 is the deployment scenario, then deploy only SM_SiS_VIEWS.zip view in the APM server.
Health and Key	All the views	\$PMDB_HOME/packages/ServiceHealth/ETL_

Content Pack	View Name	Location
Performance Indicators (Service Health)	SM_SiS_Views.zip (APM 9.40 only)	SvcHealth_BSM.ap/source/cmdb_views Note: If APM 9.40 is the deployment scenario, then deploy only SM_SiS_Views.zip view in the APM server.
Server Automation	No views	
Cross-Domain Operations Events	All the views	
Operations Events	No views	

BSM Server

To deploy the topology model views for the Content Packs in the BSM server, follow these steps:

1. In the web browser, type the following URL:

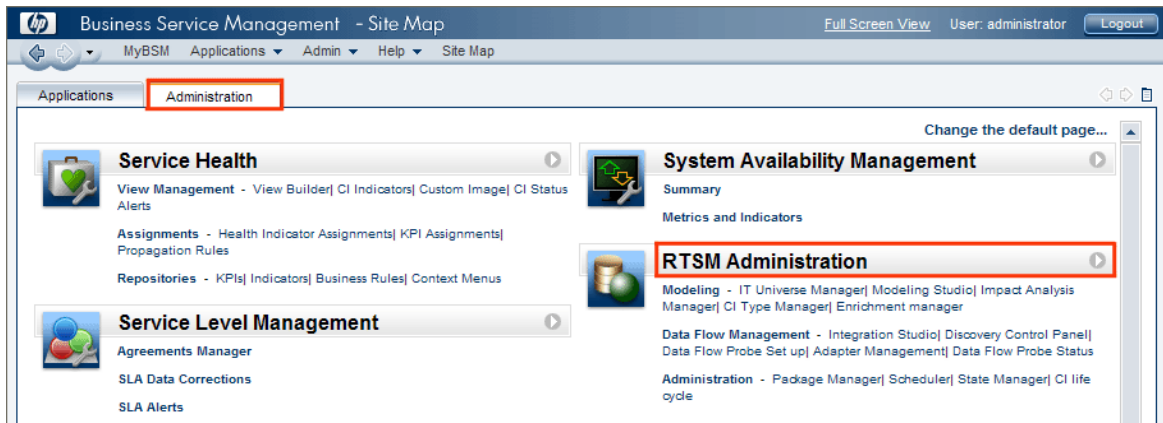
`http://<BSM system FQDN>/bsm`

where, <BSM system FQDN> is the FQDN of the BSM server.

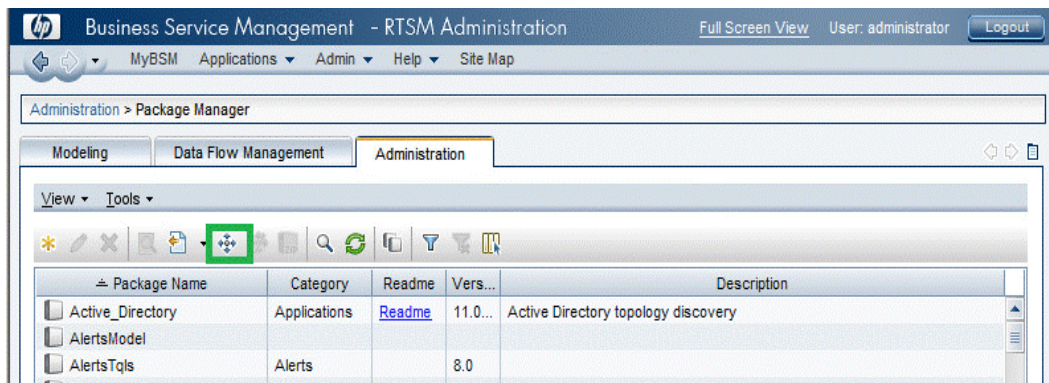
Note: You can launch the BSM server from a system where OBR is installed or any other local system. If you are launching from local system, ensure that you browse to the location mentioned in [List of Content Pack and Topology Views to Deploy](#) and copy the required views to your local system.

The Business Service Management Login page appears.

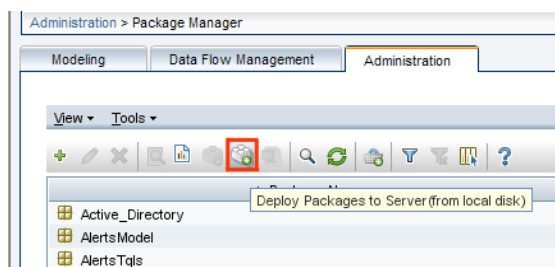
2. Type the login name and password and click **Log In**. The Business Service Management - Site Map appears.
3. Click **Administration > RTSM Administration**. The RTSM Administration page appears.



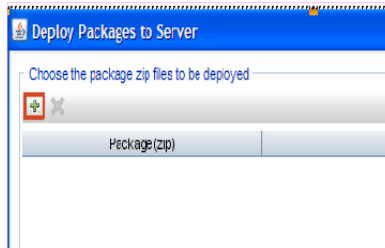
4. Click **Administration > Package Manager**. The Package Manager page appears.



5. Click the **Deploy Packages to Server (from local disk)** icon. The **Deploy Package to Server** dialog box appears.



6. Click the **Add** icon.



The **Deploy Package to Server (from local disk)** dialog box appears.

7. Browse to the location of the Content Pack zip files, select the required files, and then click **Open**.

You can view and select the TQL and ODB views that you want to deploy under **Select the resources you want to deploy** in the **Deploy Package to Server (from local disk)** dialog box. Ensure that all the files are selected.

8. Click **Deploy** to deploy the Content Pack views.

You have successfully deployed the Content Packs views based on the type of deployment scenario selected for OBR.

OMi 10 Server

To deploy the topology model views for the Content Packs in the OMi 10 server, follow these steps:

1. In the web browser, type the following URL:

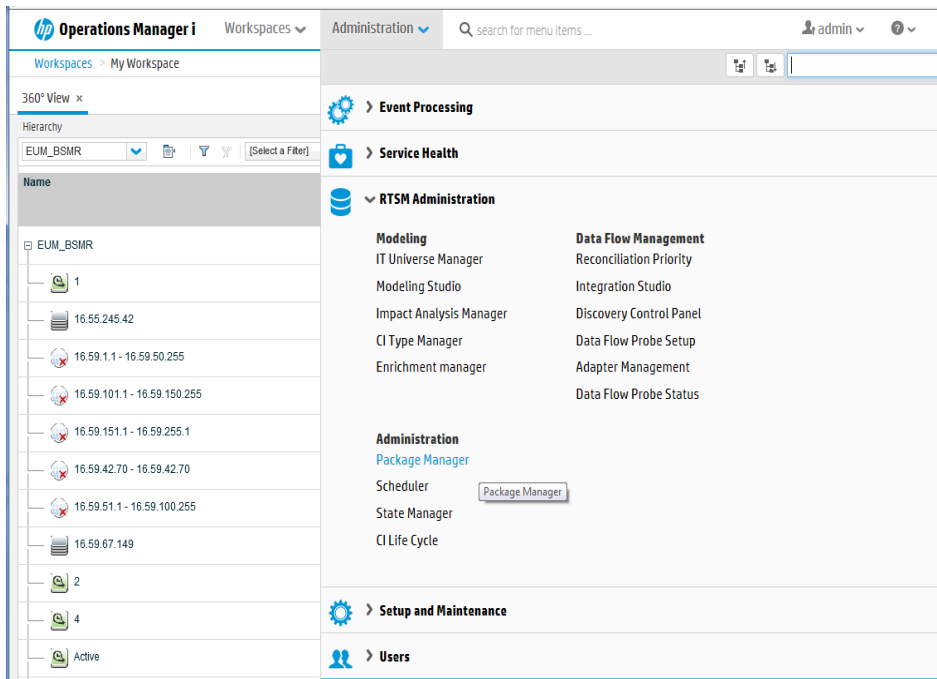
```
http://<OMi system FQDN>/omi
```

where, <OMi system FQDN> is the FQDN of the OMi server.

Note: You can launch the OMi server from a system where OBR is installed or any other local system. If you are launching from local system, ensure that you browse to the location mentioned in [List of Content Pack and Topology Views to Deploy](#) and copy the required views to your local system.

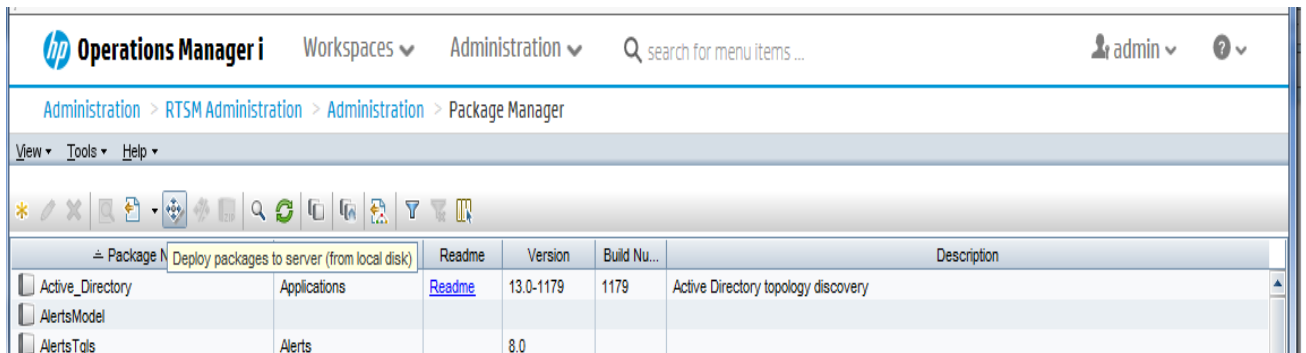
The Operations Manager i Login page appears.

2. Type the login name and password and click **Log In**. The Operations Manager i Workspace page appears.
3. Click **Administration > RTSM Administration > Package Manager**.

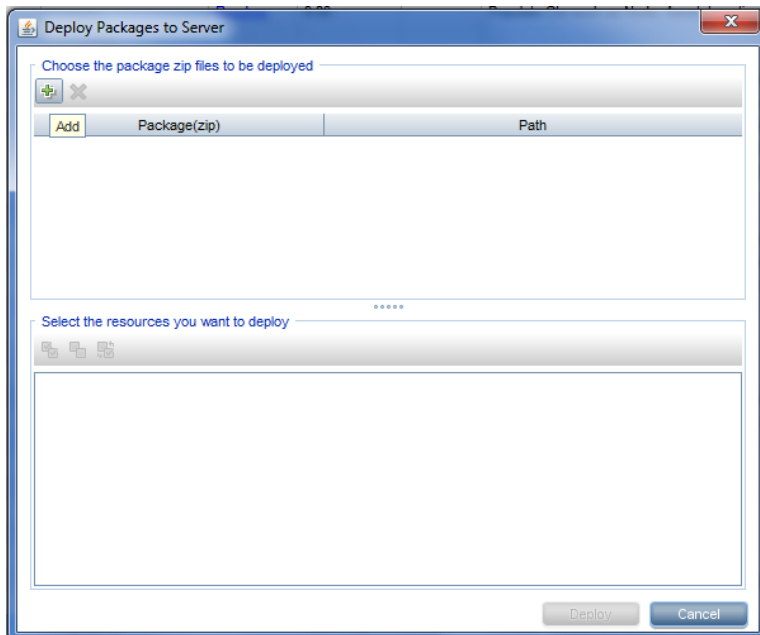


The Package Manager page appears.

4. Click the **Deploy Packages to Server (from local disk)** icon. The **Deploy Package to Server** dialog box appears.



5. Click the **Add** icon.



The **Deploy Package to Server (from local disk)** dialog box appears.

6. Browse to the location of the Content Pack zip files, select the required files, and then click **Open**.

You can view and select the TQL and ODB views that you want to deploy under **Select the resources you want to deploy** in the **Deploy Package to Server (from local disk)** dialog box. Ensure that all the files are selected.

7. Click **Deploy** to deploy the Content Pack views.

You have successfully deployed the Content Packs views based on the type of deployment scenario selected for OBR.

Enabling CI Attributes for a Content Pack

Note: To enable CI attributes for Content Pack in OMi 10 environment, follow the same configuration steps given in this section. However, use OMi server details instead of BSM server.

Each Content Pack view includes a list of CI attributes that are specific to that Content Pack. The CI attributes that are required for data collection are automatically enabled in each of the Content Pack views after you deploy them.

To enable additional CI attributes to collect additional information relevant to your business needs:

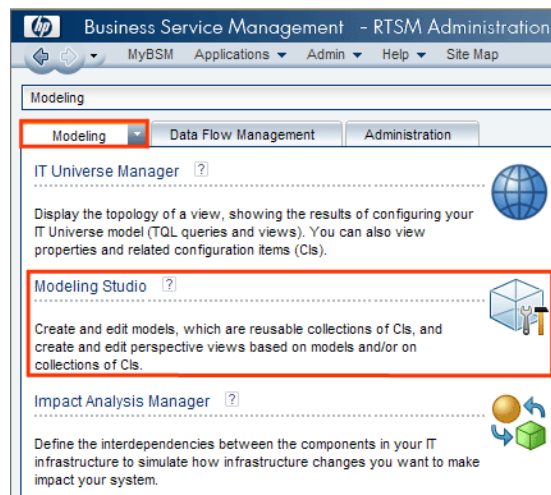
1. In the web browser, type the following URL:

`http://<BSM system FQDN>/bsm`

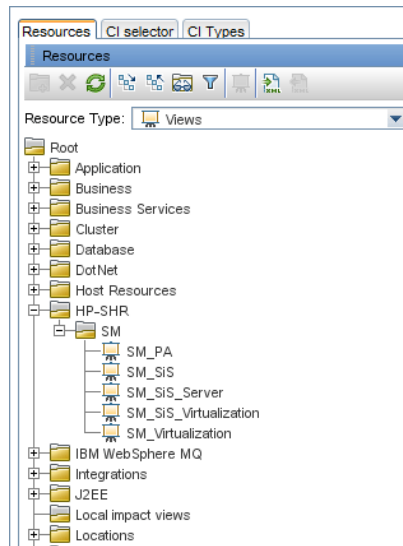
where, <BSM system FQDN> is the FQDN of the BSM server.

The Business Service Management Login page appears.

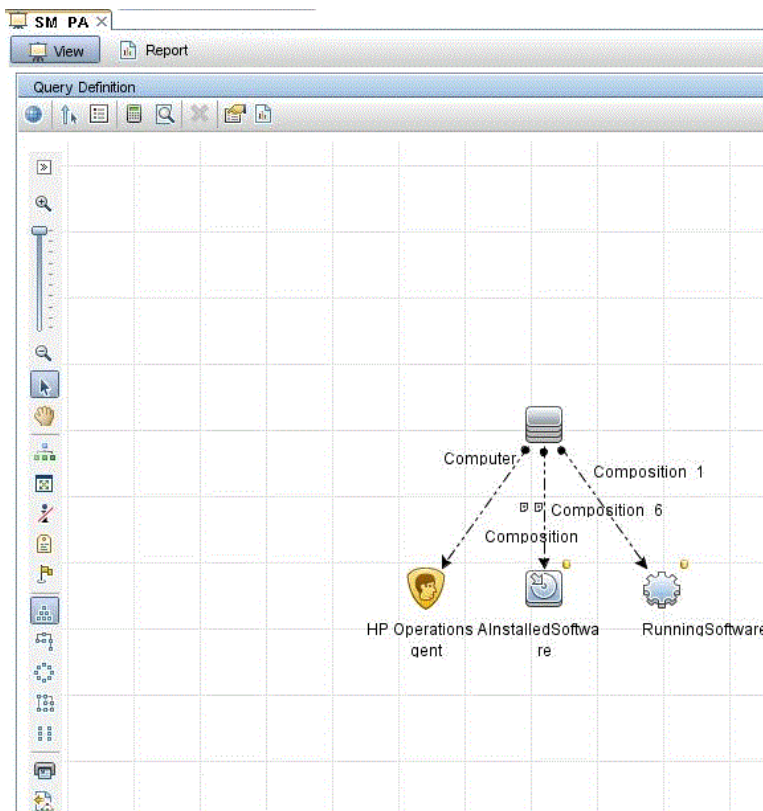
2. Type the login name and password and click **Log In**. The Business Service Management Site Map appears.
3. Click **Administration > RTSM Administration**. The RTSM Administration page appears.
4. Click **Modeling > Modeling Studio**. The **Modeling Studio** page appears.



5. In the **Resources** pane, expand HP-SHR, expand a Content Pack folder and double-click a topology view to open it.



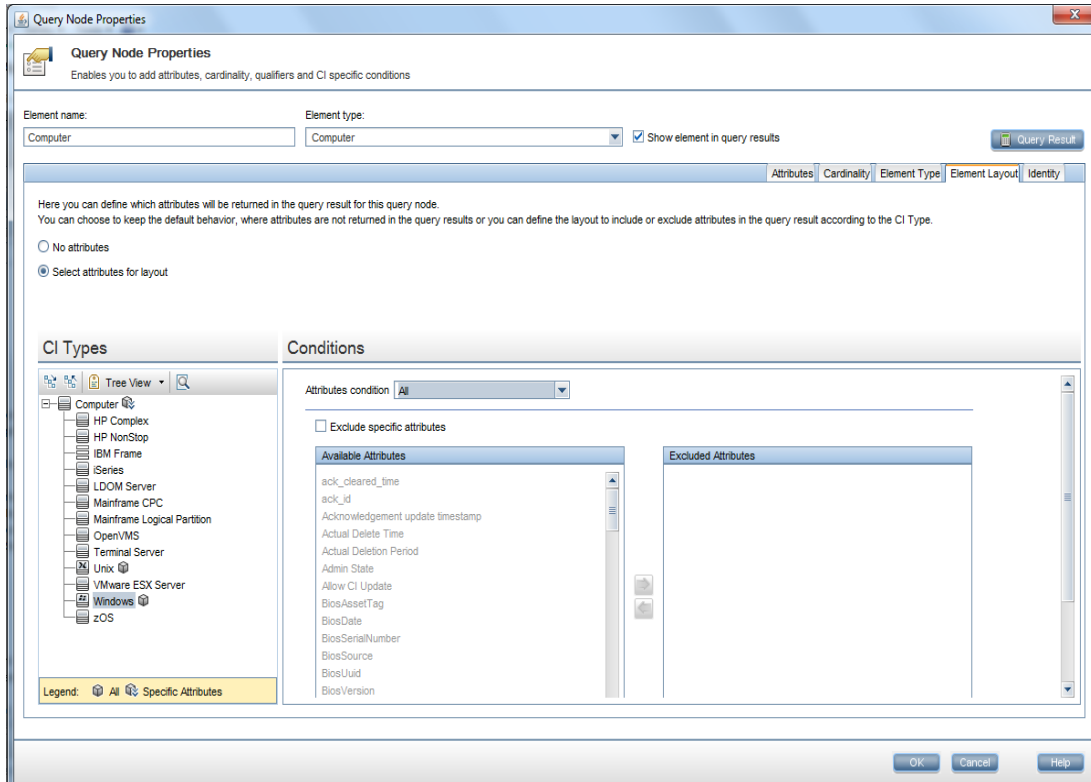
6. In the **Topology** pane, right-click any node in the topology diagram, and then click **Query Node Properties** to view the list of CI attributes for the selected node.



The **Query Node Properties** dialog box appears.

7. In **Query Node Properties** dialog box, perform the following:

- a. Click **Element Layout**.
- b. Click **Select attributes for layout** option.
- c. Select the required CI Type that you want to enable.
- d. In **Conditions**, select **All** for Attribute condition.
- e. Click **OK**.



Configure SiteScope to integrate with OBR

SiteScope is an agentless monitoring solution designed to ensure the availability and performance of distributed IT infrastructures—for example, servers, operating systems, network devices, network services, applications, and application components.

For OBR to collect data for the physical nodes from SiteScope, you must first create the monitors in SiteScope. Monitors are tools for automatically connecting to and querying different kinds of systems and applications used in enterprise business systems. These monitors collect data on various IT components in your environment and are mapped to specific metrics that are used by OBR such as CPU usage, memory usage, and so on. After you create the monitors, you must also enable SiteScope to log data in BSM profile database so that OBR can collect the required data from the agent. Perform this task only if you have SiteScope installed in your environment. Otherwise, proceed to the next task.

For the list of monitors (including the counters and measures) to be created in SiteScope, see "[SiteScope Monitors for OBR](#) " on page 287.

For more information about creating monitors in SiteScope, see the *Using SiteScope* and the *Monitor Reference* guides. This document is available at the following URL:

<https://softwaresupport.hpe.com/>

Enable integration between SiteScope and BSM or OMi 10 to transfer the collected topology data by the SiteScope monitors to BSM or OMi 10. For more information about SiteScope integration with BSM, see *Working with Business Service management (BSM)* of the *Using SiteScope* guide.

If BSM is the deployment scenario then you can integrate SiteScope with OBR using either [Configuring the Management and Profile Database Data Source](#) procedure or [Configuring the SiteScope Data Source](#) procedure.

If OMi10 is the deployment scenario then you can integrate SiteScope with OBR using [Configuring the SiteScope Data Source](#) procedure.

Chapter 4: Configure OBR for OM Deployment Scenario

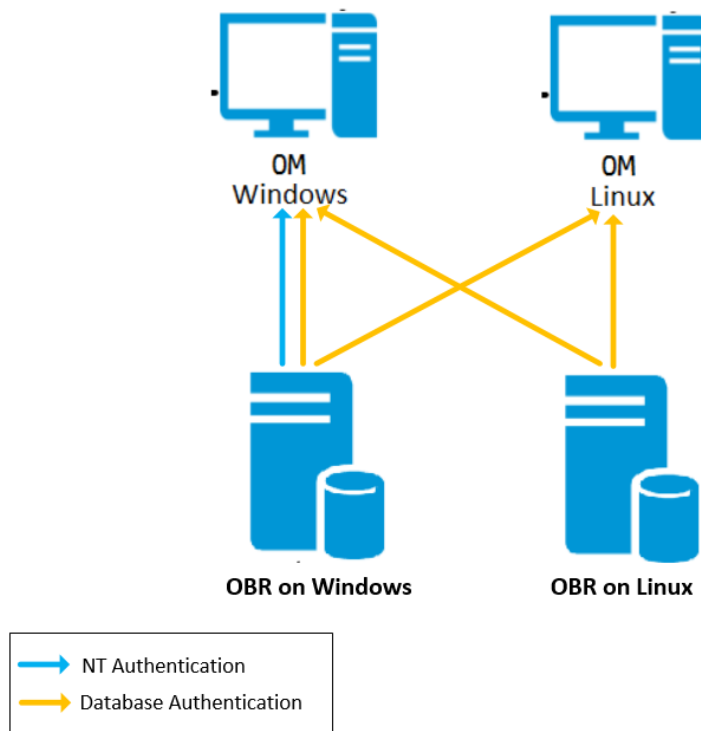
If you plan to configure OBR to work with an OM installation, you must:

- Install and configure OM successfully
- Deploy necessary SPI policies

Authentication for OBR connection with OM

OBR connects to OM to collect data. The NT authentication and database authentication are the two methods of authentication for OBR to connect to OM.

If OBR and OM are installed on Windows then both NT and database authentication is supported. For all the other deployment scenarios only database authentication is supported.



OBR connection with OM using NT authentication

If OBR is installed on a system which is part of a domain, and if you have logged into the system as a local user or domain user having administrator privileges (say DOMAIN\Administrator), start the *HPE PMDB Platform Administrator* and *HPE PMDB Platform Collection* service. You must configure the services for the domain before configuring the OM service definition source connection.

Task 1: Configure HPE PMDB Platform Administrator Service for the Domain

1. Click **Start > Run**. The **Run** dialog box appears.
2. Type `services.msc` in the **Open** field, and then press **Enter**. The **Services** window appears.
3. On the right pane, right-click **HPE_PMDB_Platform_Administrator**, and then click **Stop**.
4. Right-click **HPE_PMDB_Platform_Administrator** and then click **Properties**. The **OBR Service Properties** dialog box appears.
5. On the **Log on** tab, select **This account**.
6. Type **DOMAIN\Administrator** in the field (where Administrator is the local user having administrator privileges).
7. Type the user password in the **Password** field.
8. Retype the password in the **Confirm password** field.
9. Click **Apply** and then click **OK**.
10. On the right pane, right-click **HPE_PMDB_Platform_Administrator**, and then click **Start**.

Task 2: Configure HPE_PMDB_Platform_Collection Service for the Domain

Note: You have to perform the following steps on a collector system to which the OM is assigned for collection.

1. Click **Start > Run**. The **Run** dialog box appears.
2. Type `services.msc` in the **Open** field, and then press **ENTER**. The **Services** window appears.
3. On the right pane, right-click **HPE_PMDB_Platform_Collection_Service**, and then click **Stop**.
4. Right-click **HPE_PMDB_Platform_Collection_Service** and then click **Properties**. The **OBR Collection Service Properties** dialog box appears.
5. On the **Log on** tab, select **This account**.

6. Type **DOMAIN\Administrator** in the field (where Administrator is the local user having administrator privileges).
7. Type the user password in the **Password** field.
8. Retype the password in the **Confirm password** field.
9. Click **Apply** and then click **OK**.
10. On the right pane, right-click **HPE_PMDB_Platform_Collection_Service**, and then click **Start**.

After performing the configuration steps, proceed with the OM service definition connection configuration.

OBR connection with OM using database authentication

Creating database user account depends on how Microsoft SQL Server is set up in the OM environment and how you configure OBR to communicate with the OM database server. The following are the two possible scenarios:

- **Scenario 1:** OM for Windows 8.x or 9.x is installed on one system with Microsoft SQL Server 2005 or Microsoft SQL Server 2008 installed on the same system or a remote system. OBR, which is installed on another system, can be configured to connect to SQL Server either through Windows authentication or SQL Server authentication (mixed-mode authentication). The authentication method defined in SQL Server can be used in OBR to configure the OM database connection.
- **Scenario 2:** OM for Windows 8.x uses Microsoft SQL Server 2005 Express Edition that is embedded with it by default. Similarly, OM for Windows 9.x uses the embedded Microsoft SQL Server 2008 Express Edition by default. The authentication mode in this scenario is Windows NT authentication. However, in this case, a remote connection between SQL Server and OBR is not possible. Therefore, you must create a user account for OBR so that mixed-mode authentication is possible in this scenario.

Before you create the user account, enable the mixed-mode authentication. For information on the steps to enable the mixed-mode authentication, see the following URL:

<http://support.microsoft.com>

To create a user name and password for authentication purposes on OM system with embedded Microsoft SQL Server 2005, follow these steps:

Task 1: Create a user name and password

1. Log on to the OM system with embedded Microsoft SQL Server 2005.
2. Click **Start > Programs > Microsoft SQL Server 2005 > SQL Server Management Studio**. The **Microsoft SQL Server Management Studio** window opens.

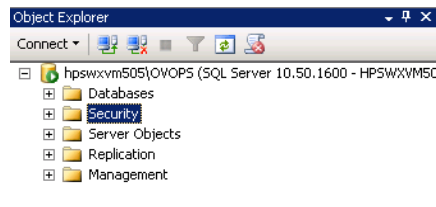
Note: If SQL Server Management Studio is not installed on your system, you can download it from the relevant section of Microsoft web site using the following URL:

<http://www.microsoft.com>

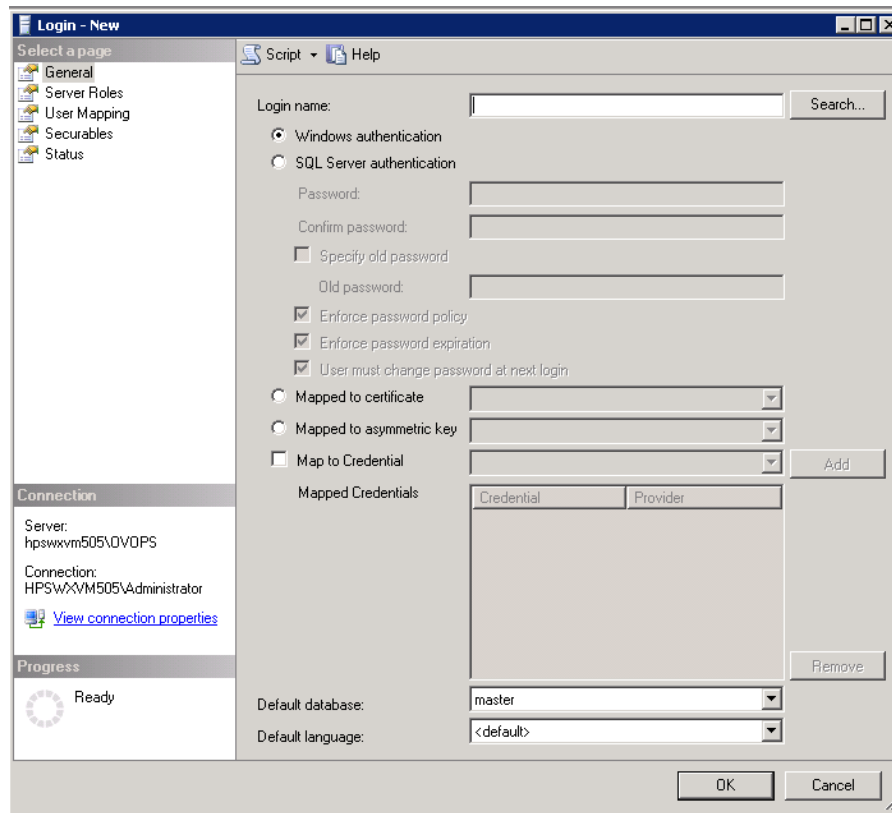
3. In the **Connect to Server** dialog box, select **NT Authentication** in the **Authentication** list, and then click **Connect**.



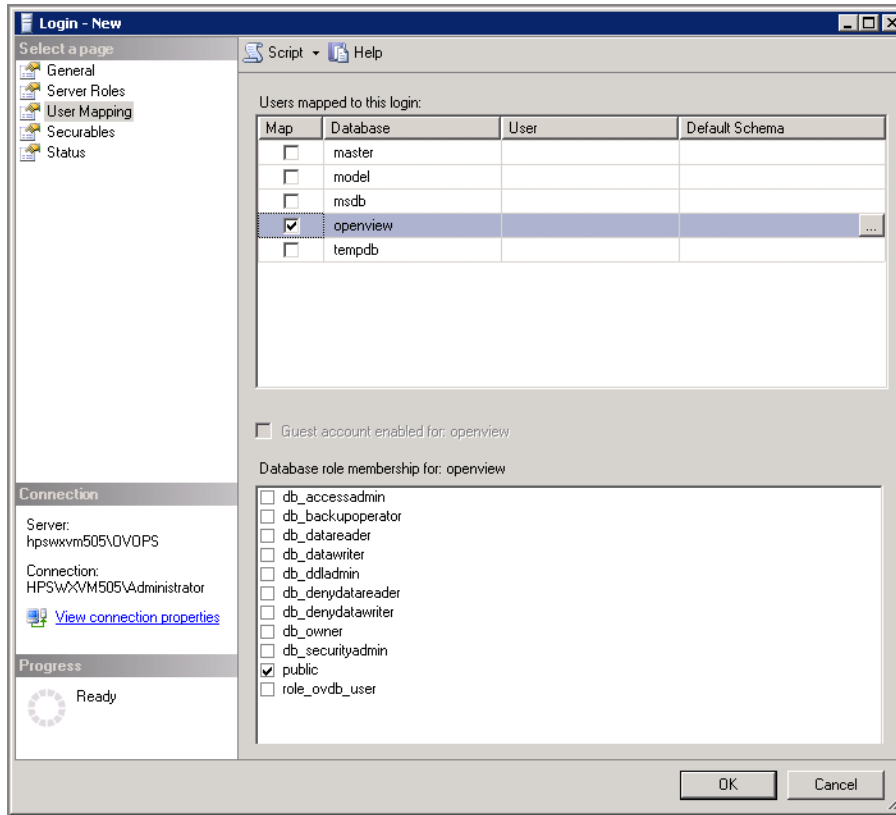
4. In the **Object Explorer** pane, expand **Security**.



5. Right-click **Login** and click **New Login**. The **Login - New** dialog box opens.



6. In **General**, type a user name for **Login name** field. Specify other necessary details.
7. Click **SQL Server authentication** option button.
8. In the **Password** field, type the password.
9. In the **Confirm password** field, retype the password. You can disable the password enforcement rules to create a simple password.
10. Click **User Mapping**.
11. In **Users mapped to this login**, select the **openview** check box.



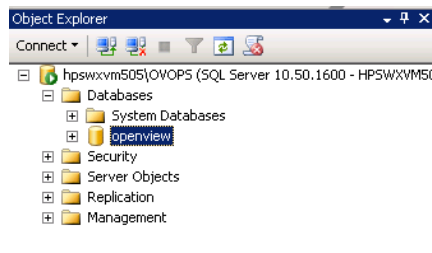
12. Click **OK** to create the user name and password.

Note: To create user name and password on OM system with embedded Microsoft SQL Server 2008, follow the same steps in [Task 1](#).

Task 2: Enable Connect and Select permissions

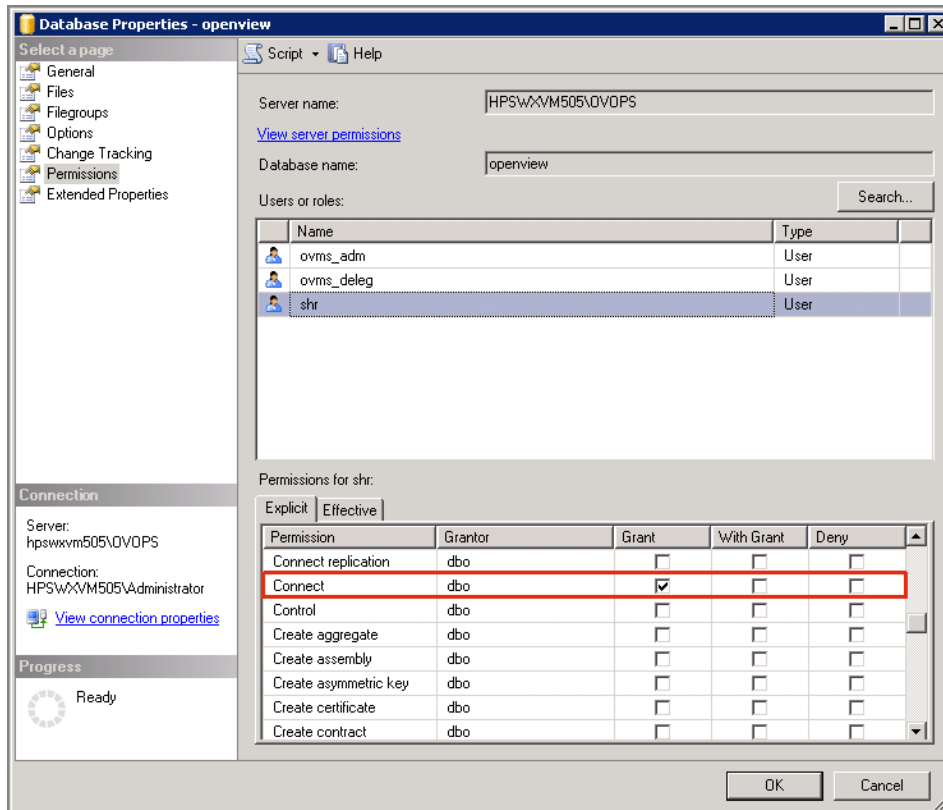
The database user must have at least the Connect and Select permissions. To enable Connect and Select permissions for the newly created user account, follow these steps:

1. In the **Object Explorer** pane, expand Databases.

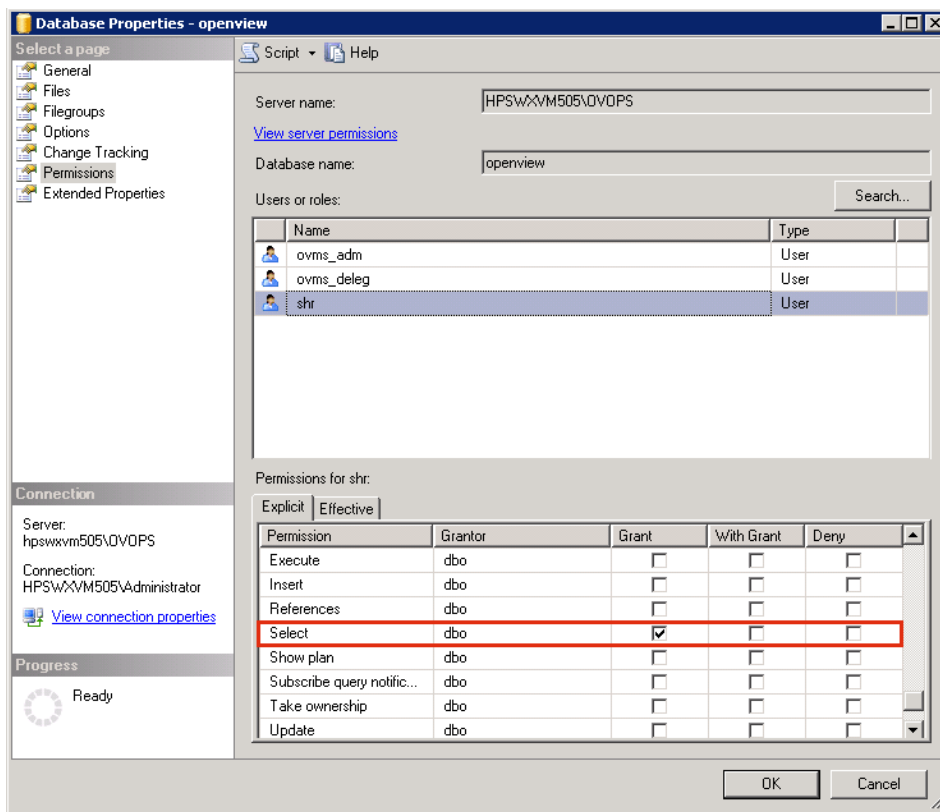


2. Right-click **openview** and then click **Properties**. The **Database Properties - openview** dialog box opens.

3. Click **Permissions**.



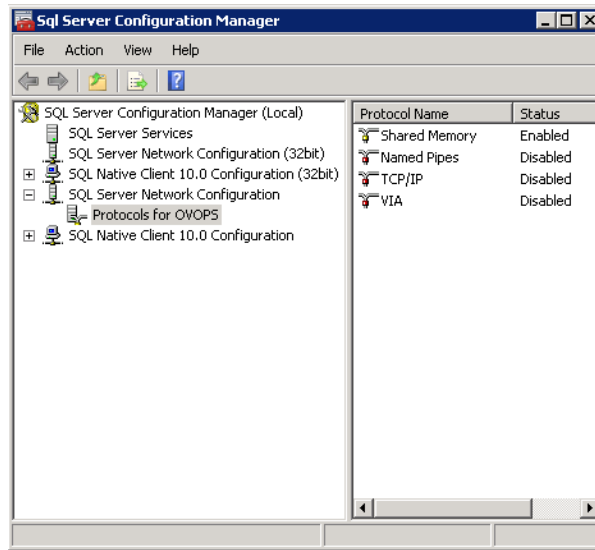
4. In the **Users or roles**, click the newly created user account.
5. In the **Explicit** tab of permissions for newly created user, scroll down to the **Connect** permission, and then select the **Grant** check box for this permission.
6. Scroll down to the **Select** permission and select the **Grant** check box for this permission.



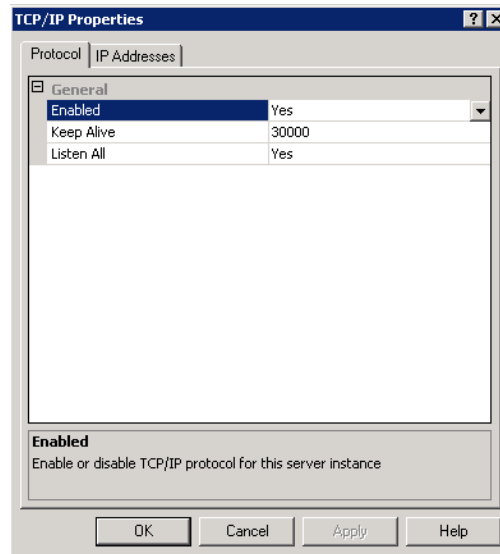
7. Click **OK**.

Task 3: Check for the OM server port number

1. Click **Start > Programs > Microsoft SQL Server 2005 > Configuration Tools > SQL Server Configuration Manager**. The **SQL Server Configuration Manager** window is displayed.
2. Expand **SQL Server Network Configuration** and select **Protocols for OVOPS**. If the instance name has been changed, select the appropriate instance name.



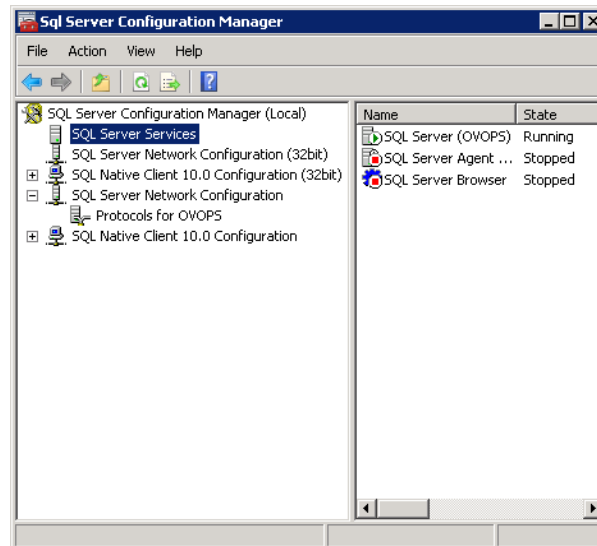
3. On the right pane, right-click **TCP/IP**, and then click **Enable**.
4. Right-click **TCP/IP** again, and click **Properties**. The **TCP/IP Properties** dialog box is displayed.



5. Click **IP Addresses** tab, under the IPAll, note down the port number.

Task 4: Restart the OM database server

1. In the **SQL Server Configuration Manager** window, click **SQL Server Services**.



2. On the right pane, right-click **SQL Server (OVOPS)**, and then click **Restart**.

You can use the newly created user name, password, and the observed instance name and port number when configuring the OM data source connection in the Administration Console.

Note: You can perform these steps by using the command prompt utility, `osql`. For more information, visit the Microsoft website at the following URL:

<http://support.microsoft.com>

Checking for the OM Server Port Number

If Microsoft SQL Server is the database type in OM, follow steps in [Task 3](#) to check for the OM server port number.

If Oracle is the database type in OM, follow these steps to check the port number:

1. Log on to the Oracle server.
2. Browse to the `$ORACLE_HOME/network/admin` or `%ORACLE_HOME%\NET80\Admin` folder.
3. Open the `listener.ora` file. Note the port number for the OM server listed in the file.

Chapter 5: Install and Uninstall the Content Packs

For installing the required Content Packs, OBR provides the Content Pack Deployment utility through the Administration Console. This web-based interface simplifies the process of installation by organizing the Content Packs based on the domain, the data source applications from where you want to collect data, and the specific Content Pack components you want to install to collect the data.

Before You Begin

Before you begin installing Content Packs, make sure that:

- Post-installation is complete
- Data source selections are complete
- In a distributed scenario, if OBR is installed on Windows, irrespective of BO installed on Windows or Linux or on the same system or different system, you must configure DSN on OBR system (installed on Windows) to connect to Vertica database. If OBR is installed on Linux then installer automatically handles the DSN configuration and connection to Vertica database.

To configure DSN, see ["Configuring DSN on Windows for Vertica Database Connection" on page 178](#).

Note: To install Content Packs on Windows Operating System, make sure that UAC is disabled on the system.

Check Availability and Integrity of Data Sources

OBR has Data Source Readiness Check tool that enables you to check the availability and integrity of RTSM and PA data sources before installing Content Packs. The tool is available on Windows and Linux operating systems. You can check the data source readiness using the property file or by database.

Check Data Source Related to RTSM

To check the availability and integrity of data source related to RTSM, follow these steps:

1. Log on to the OBR system.
2. Before you check the data source readiness, ensure the following:
 - a. The **dscheck** folder is available in PMDB_HOME.
 - b. The dscheckRTSM.sh script is available in %PMDb_HOME%\dscheck\bin (**On Windows**) and \$PMDb_HOME/dscheck/bin (**On Linux**).
 - c. Property file is created with the following entries:

```
## RTSM DB connection properties
rtsm.hostname=<hostname>
rtsm.username=<username>
rtsm.password=<password>
rtsm.port=<port>
```

3. To check the data source readiness, run the following command in the command prompt:
 - a. cd {PMDb_HOME}/dscheck/bin
 - b. Check the data source readiness using:

- i. **Property file:**

```
dscheckRTSM.sh -propFile <File_Path>/<property_file>
```

where, <File_Path> is the path where property file is created.

<property_file> is the name of the RTSM property file. For example, rtsm.prp.

OR

```
dscheckRTSM.sh -mode SHR rtsm -propFile <File_Path>/<property_file> -
hours <number of hours>
```

where, <File_Path> is the path where property files is created.

<property_file> is the name of the PA property file. For example, RTSM_db_config.prp.

<number of hours> is the hours for which the data is collected. This is an optional term.

- ii. **Database:**

```
./dscheckRTSM.sh
```

You can open the .html file created in **dscheck** folder to check the availability and integrity of the RTSM data source.

Status Summary						
DSM/OMI Version	Host Name	Connection Status	View Status	Mandatory CI Type Status	Mandatory CI Attributes Status	Number of Duplicate Nodes
Unknown	IIFVM02277.hpswlabns.adapps.hp.com	✔	✘	✘	✘	0

Select Views:			
<input type="checkbox"/> Not available in RTSM	<input type="checkbox"/> Missing Mandatory CI Types	<input type="checkbox"/> Missing Mandatory CI Attributes	

View Summary			
View Name	Available in RTSM?	Mandatory CI Types Missing	Mandatory CI Attributes Missing
SM_PA	Yes	0	4
SM_SIS_BusinessView	Yes	1	1
Exchange_Site_View	Yes	0	0
IJEF_Deployment	Yes	1	0
SM_HyperV_BusinessView	Yes	1	2
SM_SIS_Server	Yes	1	0
SM_Sol_Zones	Yes	0	1
ORA_Deployment	Yes	1	0
MSSQL_BusinessView	Yes	0	0
ORA_BusinessView	Yes	1	2
SM_Sol_Zones_BusinessView	Yes	0	12
SHR_Network	Yes	0	0
SM_LPAP	Yes	1	1
SM_SIS	Yes	0	1

The file displays the following information:

- i. Server status
- ii. Configuration details
- iii. Views available in RTSM
- iv. Mandatory CI types missing in the view
- v. Mandatory CI attributes missing with the CI type

Check Data Source Related to PA

To check the availability and integrity of data source related to PA, follow these steps:

1. Log on to the OBR system.
2. Before you check the data source readiness, ensure the following:
 - a. The **dscheck** folder is available in PMDB_HOME.
 - b. The dscheckPA.sh script is available in %PMDb_HOME%\dscheck\bin (**On Windows**) and \$PMDb_HOME/dscheck/bin (**On Linux**).
 - c. Property file with the entries of PA nodes is created.
3. To check the data source readiness, run the following command in the command prompt:
 - a. `cd {PMDb_HOME}/dscheck/bin`
 - b. Check the data source readiness using:
 - i. **Property file:**

```
dscheckPA.sh -propFile <File_Path>/<property_file>
```

where, <File_Path> is the path where property files is created.

<property_file> is the name of the PA property file. For example, pa.prp.

OR

```
dscheckPA.sh -mode SHR pa -propFile <File_Path>/<property_file> -hours <number of hours>
```

where, *<File_Path>* is the path where property files is created.

<property_file> is the name of the PA property file. For example, PA_node_list.prp.

<number of hours> is the hours for which the data is collected. This is an optional term.

ii. **Database:**

```
./dscheckPA.sh
```

You can open the .html file created in **dscheck** folder to check the availability and integrity of the PA data source.

The screenshot displays a web interface with two main sections. The top section, titled "Node Status Summary", contains a table with the following data:

Total	Not Reachable	Policy Missing	Data not logged for last 2 days	DSi/CODA Status
1	0	1	1	1

Below this is a "Select any" section with a "Node Name" input field and a "Domains" dropdown menu set to "-- Select All --".

The bottom section, titled "Node Status", contains a table with the following data:

Node Name	ICMP ping	BBC ping	CODA ping	Agent Version	Last Log Time	Number of Missing Policies	Domain	DSi/CODA
WFMVS017.HPSWLABS.HP.COM	✓	✗	✓	11.11.025	09/28/15 13:38:00	1		✗

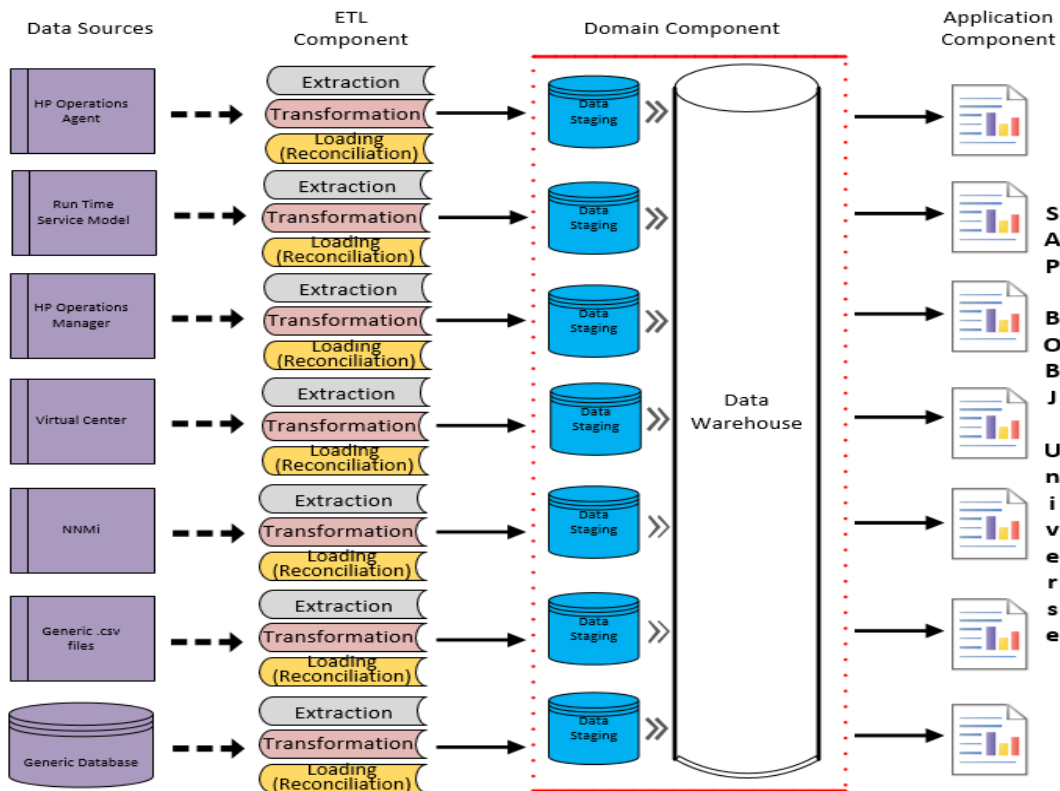
The file displays the following information:

- i. Node status summary
- ii. Node status

Selecting the Content Pack Components

A Content Pack is a data mart—a repository of data collected from various sources—that pertains to a particular domain, such as system performance or virtual environment performance, and meets the specific demands of a particular group of knowledge users in terms of analysis, content presentation, and ease of use. For example, the system performance content provides data related to the availability and performance of the systems in your IT infrastructure. Content Packs also include a relational data

model, which defines the type of data to be collected for a particular domain, and a set of reports for displaying the collected data.



Content Packs are structured into the following layers or components:

- **Domain component:** The 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 Application components (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 (Extract, Transform, and Load) 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 Operations Agent, you must install the SysPerf_ETL_PerformanceAgent component. If you want to collect system performance data from

SiteScope, you must install either `SysPerf_ETL_SiS_API` (sourcing data logged in SiteScope directly using API) or `SysPerf_ETL_SiS_DB` (sourcing data logged in BSM Profile database).

A single data source application can have multiple ETL components. For example, you can have one ETL component for each virtualization technology supported in Performance 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.

- **Application component:** The Report Content Pack component defines the application-specific aggregation rules, business views, SAP BusinessObjects universes, and the reports for a particular domain. Application components can be dependent on one or more Domain components. This component also provides the flexibility to extend the data model that is defined in one or more Domain components.

The list of Content Pack components that you can install depends on the topology source that you configured during the post-install configuration phase of the installation. Once the topology source is configured, the Content Pack Deployment page filters the list of Content Pack components to display only those components that can be installed in the supported deployment scenario. For example, if RTSM is the configured topology source, the Content Pack Deployment page only displays those components that can be installed in the Service and Operations Bridge (SaOB) and APM deployment scenarios.

For more information about each Content Pack and the reports provided by them, see the *Operations Bridge Reporter Online Help for Users*.

Installing the Content Pack Components

Use the Content Pack Deployment page in the Administration Console to install the Content Pack components.

Note: The Content Packs already selected in the Content Pack Deployment page may be mutually exclusive. For information on Content Packs that are mutually exclusive, see ["Listing of ETLs" on page 294](#).

To install the Content Packs, follow these steps:

1. To log on to Administration Console, follow these steps:

- a. Launch the following URL:

`https://<OBR_Server_FQDN>:21412/OBRApp`

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

- b. Type **administrator** in the **Login Name** field and password in the **Password** field. Click **Log In** to continue. The **Home** page appears.

Note: If you use any other user account to access the Administration Console, make sure that the user account has administrator privileges.

2. On the left pane, click **Content Pack Deployment**. The **Content Pack Deployment** page appears.

The Content Pack Deployment displays the Content Pack components that can be installed in the supported deployment scenario. You can modify the selection by clearing the selected content, the data source application, or the Content Pack components from the list.

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.

The following table lists the content that is specific to each deployment scenario:

List of Content Packs

Content	BSM/OMi	Operations Manager	Application Performance Management	VMware vCenter
Default	✓	✓	✓	✓
Cross-Domain Operations Events	✓			
Health and Key Performance Indicators	✓		✓	
IBM WebSphere Application Server	✓	✓		

Content	BSM/OMi	Operations Manager	Application Performance Management	VMware vCenter
Microsoft Active Directory	✓	✓		
Microsoft Exchange Server	✓	✓		
Microsoft SQL Server	✓	✓		
MSAppCore	✓	✓		
Network Performance ¹	✓	✓		
Network Component Health	✓	✓		
Network Interface Health	✓	✓		
Operations Events	✓	✓		
Oracle	✓	✓		
Oracle WebLogic Server	✓	✓		
Real User Transaction Monitoring	✓		✓	
Synthetic Transaction Monitoring	✓		✓	
System Performance	✓	✓		✓

¹You must use the NetworkPerf_ETL_PerfiSPI_NonRTSM ETL content in an RTSM deployment of OBR when Network Node Manager i (NNMi) is not integrated with BSM.

Content	BSM/OMi	Operations Manager	Application Performance Management	VMware vCenter
Virtual Environment Performance	✓	✓		✓

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

An **Installation Started** status appears in the **Status** column for Content Pack that is currently being installed. 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.

Note: The HPE_PMDB_Platform_Orchestration and the timer service will be stopped automatically during Content Pack(s) install/uninstall operation and will be started once operation is complete.

4. Click the  icon 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 install/uninstall process, Content Pack Deployment page does not allow you to interrupt the process. Instead, you must wait till the current process is complete before you can perform any other operations on the Content Pack Deployment page.

Note: If the **Status** of the Content Pack installation is in **Installation Started** for more than 1 hour and the Content Pack installation hangs, see *Installing of Content Packs Hangs (on Linux only)* in *Operations Bridge Reporter Troubleshooting Guide*.

You may install and configure additional Data Processors after completing the Content Pack installation. For more information, see *Operations Bridge Reporter Interactive Installation Guide*.

Note: Install the Network Performance Content Pack to collect performance data at hourly granular from NPS source. So executive summary reports display hourly/daily /monthly summarized view of Network devices collected from NPS. OBR collects performance data of only 'Switches and Routers' devices from NPS source.

Install the Network Component_Health and Network Interface_Health Content Pack to collect network performance data directly from NNMi. The data collection gives you detailed real time view of component or interface health in your network. You can view detailed health or utilization

reports. You have to revisit the hardware requirements, if you choose to install these Content Packs.

For more information, see *Operations Bridge Reporter Performance, Sizing, and Tuning guide*.

Based on your requirement, OBR recommends you to install either the Network Performance Content Pack or Network Component_Health/Network Interface_Health Content Packs. Installing both Network Performance Content Pack and Network Component_Health/Network Interface_Health Content Packs may lead to performance issues due to redundant data.

Note: If you have installed Component Health and / or Interface Health Content Pack, you have to configure OBR and NNMi to exchange network data. For configuration procedure, see ["Configuring OBR with Network Node Manager i \(NNMi\)" on page 173](#).

You have to ensure that the following prerequisites are met before you go ahead with the configuration procedure:

- The NNMi and NPS are installed and configured correctly.
- The **HPE_PMDB_Platform_NRT_ETL** service is up and running.

After you install Content Pack and open reports, you might come across Memory Full error in SAP BusinessObjects BI Launch Pad. To overcome this issue, you have to disable the memory analysis and APS service monitoring settings in CMC. See ["Disabling Memory Analysis and APS Service Monitoring" on the next page](#).

Uninstalling the Content Pack Components

Use the Content Pack Deployment page in the Administration Console to uninstall the Content Pack components.


To uninstall the Content Packs, follow these steps:

1. To log on to Administration Console, follow these steps:
 - a. Launch the following URL:
`https://<OBR_Server_FQDN>:21412/OBRApp`
 - b. Type **administrator** in the **Login Name** field and password in the **Password** field. Click **Log In** to continue. The Administration Console page appears.

Note: If you use any other user account to access the Administration Console, make sure that the user account has administrator privileges.

2. On the left pane, click **Content Pack Deployment**. The **Content Pack Deployment** page appears.

The Content Pack Deployment page displays the Content Pack components that are installed in the supported deployment scenario. For the list of Content Pack, see, "[List of Content Packs](#)" on page 109.

3. Click  icon for the required Content Pack to be uninstalled. A summary message is displayed.

Note: At a time, only one Content Pack and its dependent Content Packs are uninstalled.

4. Click **OK** to uninstall the Content Pack. The uninstall status is displayed in the **Status** column.

Note: If you uninstall Content Pack, run the DLC to get the correct license usage count in the **Additional Configurations > Licensing** page of Administration Console.

Disabling Memory Analysis and APS Service Monitoring

To disable the memory analysis and APS service monitoring setting in CMC, follow these steps:

1. Log on to the **Central Management Console** by launching the following URL:

```
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. You can also launch CMC using

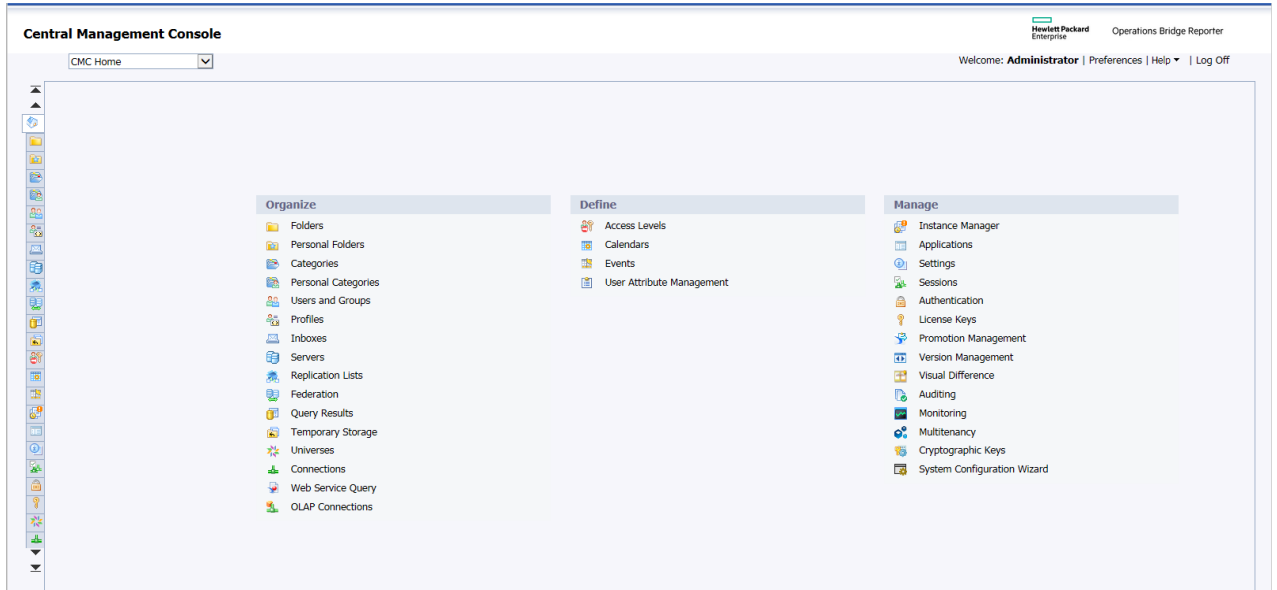
```
http://<System_FQDN>:8080/CMC if you have disabled HTTPS.
```


You can also access CMC from Administration Console. Click **Additional Configurations > Reporting Platform > Launch CMC**. The Log in page is displayed.

2. Log on as user with administrator privileges.

The **System Configuration Wizard** is displayed. Click **Close** to close the wizard. The **Central Management Console** home page is displayed.

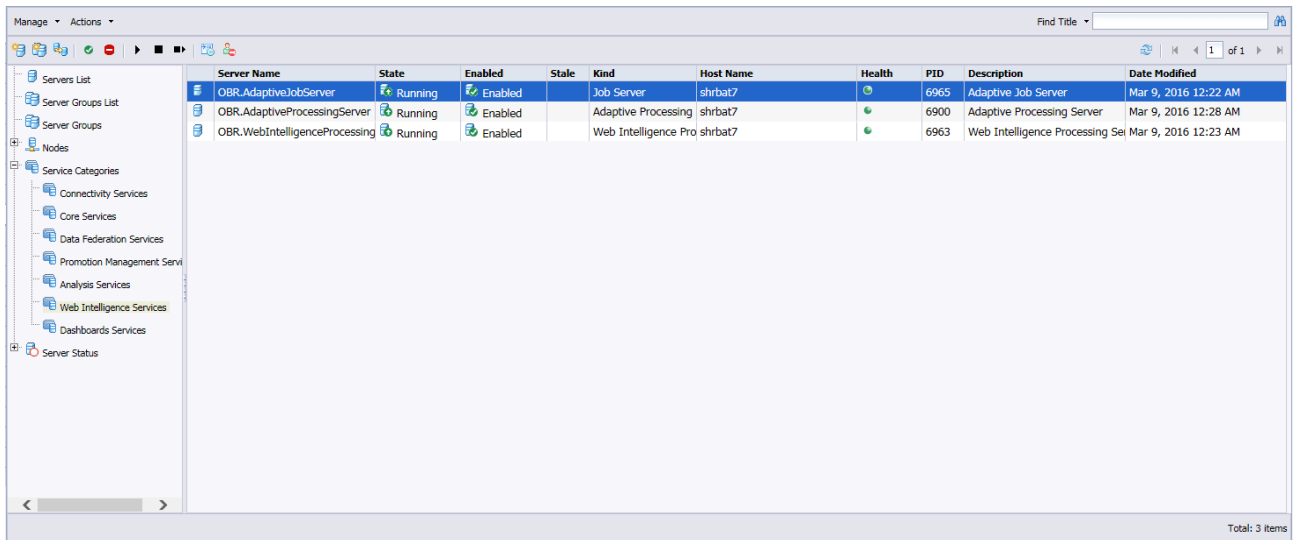
Note: If you do not want the **System Configuration Wizard** to appear each time you log on to CMC, click the check box **Don't show this wizard when cms is started**.



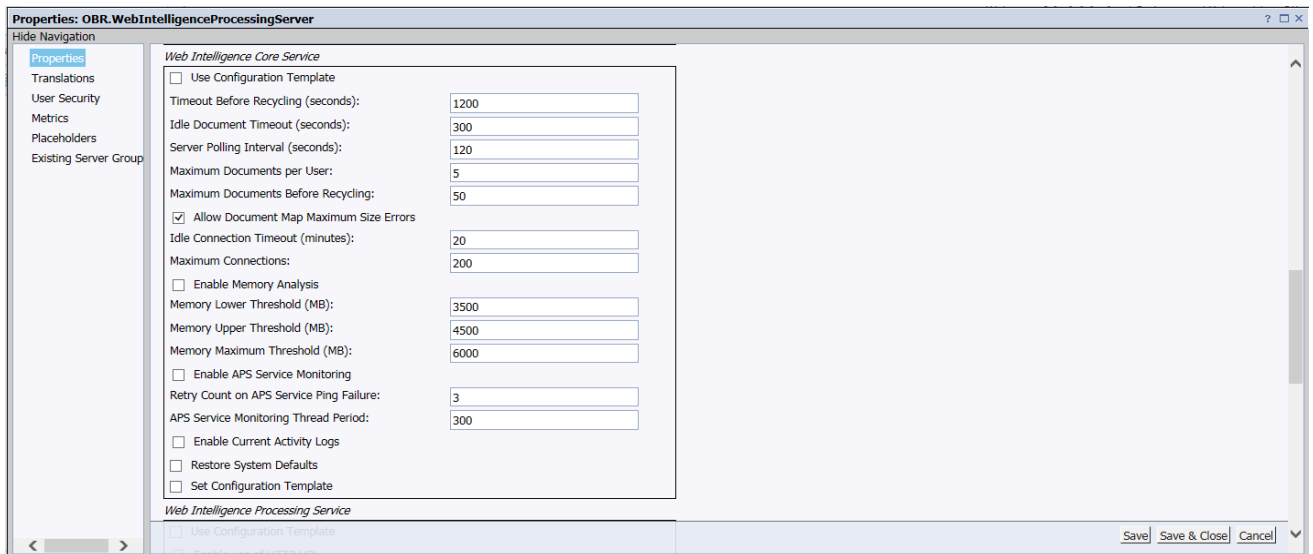
3. Click  **Servers** or select **Servers** from the drop down list. The Manage page is displayed.



4. Click **Web Intelligence Services**.



5. Right-click **Web Intelligence Processing Server** and click **Properties**.



6. Scroll down the page to clear the selection from **Enable Memory Analysis** and **Enable APS Service Monitoring**. Click **Save & Close**.

7. Right-click **Web Intelligence Processing Server** and click **Start Server**.

You can now view reports using SAP BusinessObject BI Launch Pad.

Upgrading Content Packs

After successfully upgrading to the latest version of OBR, you must upgrade all Content Packs installed on the OBR system with the help of the Content Pack Deployment page.

To upgrade Content Packs, follow these steps:

1. To log on to Administration Console, follow these steps:


- a. Launch the following URL:

```
https://<OBR_Server_FQDN>:21412/OBRApp
```

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

- b. Type **administrator** in the **Login Name** field and password in the **Password** field. Click **Log In** to continue. The **Home** page appears.

Note: If you use any other user account to access the Administration Console, make sure that the user account has administrator privileges.

2. On the left pane, click **Content Pack Deployment**. The Content Pack Deployment page appears.
3. 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.

Chapter 6: Data Source Configuration

After installing Content Packs, you must configure OBR to collect required data from various data collectors. The 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 where the collectors can collect the data using the Administration Console.

You can configure the data source based on the following deployment scenarios:

1. **OMi 9.2x deployment scenario**
 - a. [Configuring the Management and Profile Database Data Source](#)
 - b. [Configuring the OMi Data Source \(Events database\)](#)
 - c. [Configuring the Operations Agent Data Source](#)
 - d. [Configuring the Operations Manager Data Source](#)
 - e. [Configuring the Network Data Source \(using Generic Database\)](#)
 - f. [Configuring the Network Data Source \(using NNMi\)](#)
 - g. [Configuring the VMware vCenter Data Source](#)
 - h. [Configuring the SiteScope Data Source](#)
2. **OMi 10 deployment scenario**
 - a. [Configuring the OMi Data Source \(Operations database\)](#)
 - b. [Configuring the Operations Agent Data Source](#)
 - c. [Configuring the Network Data Source \(using Generic Database\)](#)
 - d. [Configuring the Network Data Source \(using NNMi\)](#)
 - e. [Configuring the VMware vCenter Data Source](#)
 - f. [Configuring the SiteScope Data Source](#)
3. **Operations Manager deployment scenario**
 - a. [Configuring the Operations Agent Data Source](#)
 - b. [Configuring the Operations Manager Data Source](#)
 - c. [Configuring the Network Data Source \(using Generic Database\)](#)

- d. [Configuring the Network Data Source \(using NNMi\)](#)
 - e. [Configuring the VMware vCenter Data Source](#)
4. **VMware vCenter deployment scenario**
- a. [Configuring the VMware vCenter Data Source](#)
 - b. [Configuring the Network Data Source \(using Generic Database\)](#)
 - c. [Configuring the Network Data Source \(using NNMi\)](#)
5. **Other deployment scenarios**
- a. [Configuring the Network Data Source \(using Generic Database\)](#)
 - b. [Configuring the Network Data Source \(using NNMi\)](#)

For information on listings of ETLs for Content Pack, see [Appendix C](#).

Topology Source

If you have not configured the topology source in post-install configuration, you can configuration it using the **Topology Source** page. However, if you have already configured the topology source during the post-install configuration, you can only test or modify the connection parameters of the topology source you already configured.

Topology Source ?

Topology Source

Selected Topology source (based on available data sources): RTSM

OBR collects entity (CI) and topology relationships from any of the following data sources – BSM/OMi, OM or VMware vCenter.

A topology source configured in OBR, serves as a single point of truth for topology data; once selected it cannot be altered .

[Create New](#) [Test Connection](#) [Edit](#) [Save](#)

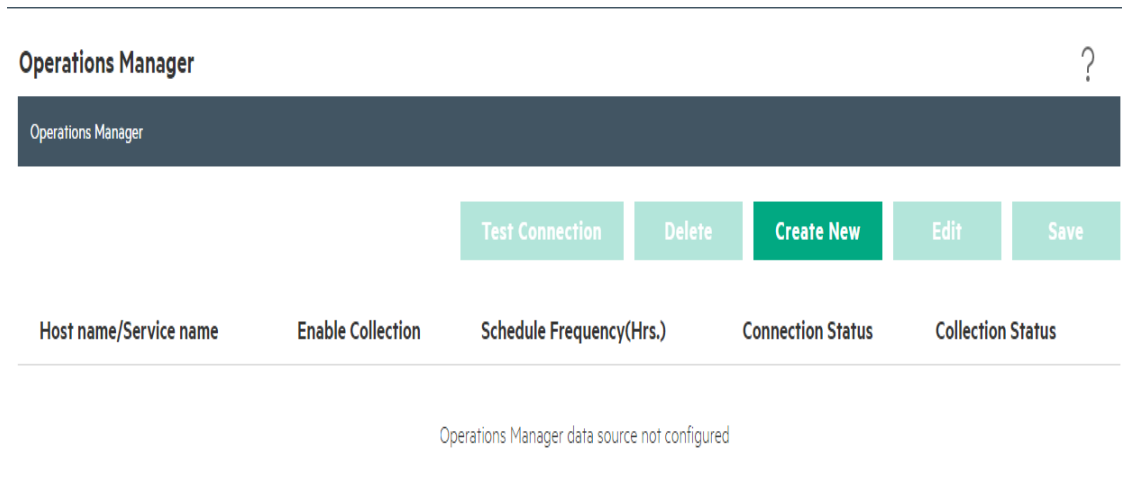
Collection Frequency (Hrs.) – +

Host name	Enable Collection	Connection Status	Collection Status
Topology Data Source not Configured			

For more information on topology source configuration, see "[Task 2: Configuring the Topology Source](#)" on [page 64](#).

Configuring the Operations Manager Data Source

If you have installed the Operations Manager (OM) Content Pack and created the topology source connection for OM, the same data source connection appears on the **Data Source Configuration > Operations Manager** page. You need not create a new data source connection. You can test the existing connection and save it.



However, updating the data source connection on the Topology Source page does not update the connection details on the Operations Manager page.

To configure the database connection, follow these steps:

1. In the **Administration Console**, click **Data Source Configuration > Operations Manager**. The **Operations Manager** page appears.
2. Click **Create New** to create the OM data source connection. The **Connection Parameters** dialog box appears.
3. Specify or type the following values in the **Connection Parameters** dialog box:

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

Field	Description
	system must be typed here.
Port	<p>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.</p> <p>To check the port number for the database instance, such as OVOPS, see "Checking for the OM Server Port Number" on page 102.</p>
Database Instance	<p>System Identifier (SID) of the database instance. The default database instance is OVOPS.</p> <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.

Field	Description
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. Tip: It is recommended to have a common trust store file.
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.
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 **OK**.
5. Select the host name and then click **Test Connection** to test the connection.
6. Click **Save** to save the changes. A *Saved Successfully* message appears in the Information message panel.

You can select the host name and click **Edit** to modify a specific OM data source connection.

7. To change the OM data collection schedule for one or more hosts, in the **Schedule Frequency** column, specify a collection time between 1 and 24 hours in the **Hrs** box.
8. Click **Save** to save the changes. A *Saved Successfully* message appears in the Information message panel.

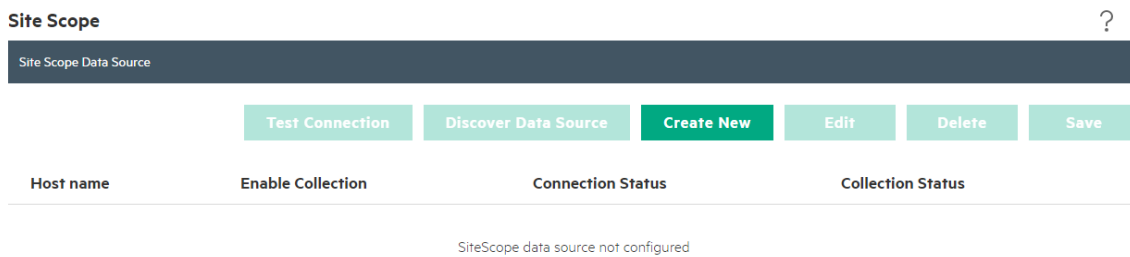
For more information about creating or configuring Operations Manager data source connections, see the *Operations Bridge Reporter Online help for Administrators*.

Configuring the SiteScope Data Source

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

You can also use this page to discover the host name of SiteScope Server. Click **Discover Data Source** to list the host name of SiteScope servers.

If you have configured the RTSM topology source, **Discover Data Source** discovers all the associated SiteScope servers. Also, you must have deployed the SiteScopeProfileView.zip from the location {PMDB_HOME}\packages\SystemManagement\ETL_SystemManagement_SiS_API.ap/source/cmdb_views.



If you have enabled SSL for SiteScope, perform the steps mentioned in "[SiteScope with SSL enabled](#)" on page 126.

To create a new SiteScope data source connection, follow these steps:

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:

Connection Parameters

Connection Settings

Host name*

Port*

Use SSL

User name*

Password*

Collection Station ▼

General Data Integration Settings

Create Integration

Integration name*

Encoding

Init String*

Use SSL

Reporting Interval (seconds) - +

Request timeout (seconds) - +

Connection timeout (seconds) - +

Number of retries - +

Authentication when requested

Authentication user name

Authentication password

Proxy address

Proxy user name

Proxy password

Create tag

Tag name

* Indicates Mandatory Fields

Save **Test Connection** **Cancel**

Field	Description
Connection Settings	
Host name	IP address or FQDN of the SiteScope server.
Port	Port number to query the SiteScope server. Note: The port number 8080 is the default port to connect to SiteScope server.
Use SSL	<i>(Optional)</i> . If selected, you must enable the SiteScope server to support communication over Secure Sockets Layer (SSL). If you have enabled SSL for SiteScope, perform the steps mentioned in "SiteScope with SSL enabled" on page 126 .
User name	Name of the SiteScope user.
Password	Password of the SiteScope user.
Collection Station	The collector to which the data source should be assigned to for the collection.
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. 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.	
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. Note: To obtain the Init String, log on to SiteScope server with your credentials and click on General Preferences > LW SSO .
Use SSL	<i>(Optional)</i> . If selected, you must enable the SiteScope server to support communication over Secure Sockets Layer (SSL). If you have enabled SSL for SiteScope, perform the steps mentioned in "SiteScope with SSL enabled" on page 126 .

	For OBR to obtain the data from SiteScope in HTTPs mode, perform the steps " Configuring OBR server to get data from SiteScope in HTTPs mode " on the next page, after completing the SiteScope data source configuration.
Reporting interval (seconds)	Frequency at which SiteScope pushes data to OBR.
Request timeout (seconds)	The time to wait before the connection times out. To configure infinite timeout, set it as 0.
Connection timeout (seconds)	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	<i>(Optional)</i> . 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 to monitors or groups from the SiteScope server.
Tag name	User defined name of the tag.

4. *(Optional)* If you have enabled SSL for SiteScope, click **Test Connection** to complete the certificate import.
5. Click **OK**.
6. Click **Save**.

A Saved Successfully message appears in the Information message panel.

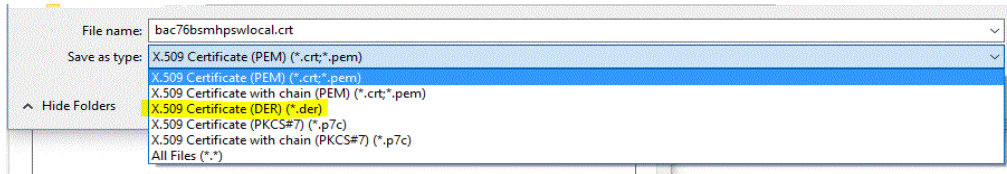
Data collection for the newly created SiteScope data source connection is enabled by default. In addition, the collection frequency is scheduled for every 15 minutes.

For more information about SiteScope data source page, see the *Operations Bridge Reporter Online help for Administrators*.

SiteScope with SSL enabled

If you have enabled SSL for SiteScope, perform these steps:

1. Log on to the SiteScope server user interface.
2. Export the SiteScope certificate from the browser. Make sure to export the certificate with X.509 encoding with .der format as shown in the following image:



3. Rename the certificate extension with .pem.
4. Copy the SiteScope certificate to OBR server {PMDB_HOME}/config folder.
5. Perform the steps ["Configuring the SiteScope Data Source" on page 122](#).

Note: To import the certificate to the .jks file, provide all the details in the **Administration Console > Data Source Configuration > SiteScope** page and select **Use SSL**. Click **Test Connection**.

6. On the OBR server, go to the location {PMDB_HOME}/stores and verify if cacert.jks file is created.
7. Run the command `keytool -v -list -keystore {PMDB_HOME}/stores/cacerts.JKS` to verify the certificate.

Note: The password is changeit.

The certificate should display the parameter `Owner: CN=<SiteScope Server name>`.

Configuring OBR server to get data from SiteScope in HTTPs mode

Perform these steps to configure the OBR server to get the data from SiteScope server in HTTPs mode after ["Configuring the SiteScope Data Source" on page 122](#):

1. From the location {PMDB_HOME}/config, open the file `collection.properties`.
2. Edit the following parameter values from false to true:

```
sis.gdi.http.server.use.ssl=true
```

```
sis.https.server.enable=true
```

Also, change the following parameter from true to false:

```
sis.http.server.enable=false
```

3. On the OBR Collector system, run the following command to export the OBR Collector CA certificate from keystore:

```
ovcert -exporttrusted -file <filename> -ovrg server
```

4. Copy the exported CA certificate to the SiteScope server.
5. On the SiteScope server, log on to the SiteScope user interface, click **Preferences > Certificate Management** and click **Import Certificates** button. Select **File** or **Host**, and enter the details of the source server.

From the Loaded Certificates table, select the server certificates to import and click **Import**. The imported certificates are listed on the Certificate Management page.

6. On the OBR server, restart the HPE_PMDB_Platform_Collection service.

Configuring the Generic Data Source

This page allows you to configure connections to generic databases that use Vertica, Oracle, Sybase IQ or SQL Server as the database system.

If you have installed “Network Performance” Content Pack, you must configure OBR to collect network performance data from NPS data base which is integrated with NNMI. OBR collects performance data of only ‘Switches and Routers’ devices from NPS source. Using the Generic Database page in the Administration Console, you can configure OBR to collect the required data from the NPS.

Sybase IQ as Data Source

If Sybase IQ is the database in your system, you have to manually copy the `jconn4.jar` file to the OBR system and then continue with the generic database configuration.

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

1. Copy the `jconn4.jar` from `%SYBASE%/jConnect-7_0/classes` (**On Windows**) and `$SYBASE\jConnect-7_0\classes` (**On Linux**) on Sybase IQ server to `$PMDB_HOME/lib` directory on OBR system.
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 %SYBASE%/jConnect-7_0/classes (**On Windows**) and \$SYBASE\jConnect-7_0\classes (**On Linux**) on Sybase IQ server to \$PMDB_HOME/lib directory on Collector system.
2. Restart the collection service.

Configure Generic Data Source

To configure the generic database, follow these steps:

Generic Database ?

Generic Database

Test Connection Create New Edit Delete Save

Host name	Enable Collection	Schedule Frequency	Connection Status	Collection Status
-----------	-------------------	--------------------	-------------------	-------------------

1. In the **Administration Console**, click **Data Source Configuration > Generic Database**. The **Generic Database** page appears.
2. Click **Create New** to create the NPS data source connection. The **Connection Parameters** dialog box appears.
3. Specify or type the following values in the **Connection Parameters** dialog box:

Field	Description
Host name	Address (IP or FQDN) of the NPS database server.
Port	Port number to query the NPS database server.
TimeZone	The time zone in which the database instance is configured. 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.
Database type	The type of database engine that is used to create the NPS database.

Field	Description
Domain	Select the domain(s) for which you want OBR to collect data from the selected database type.
URL	The URL of the database instance.
User name	Name of the NPS database user.
Password	Password of the NPS database user.
Collection Station	The collector to which the data source should be assigned to for the collection.

The Domain name `Network_Core` appears for selection only after the installation of **NetworkPerf_ETL_PerfiSPI_RTSM** or **NetworkPerf_ETL_PerfiSPI_NonRTSM**.

4. Click **OK**.
5. Click **Test Connection** to test the connection.
6. Click **Save** to save the changes. A Saved Successfully message appears in the Information message panel.
7. To change the data collection schedule for one or more hosts, in the **Schedule Frequency** column, specify a collection time between 1 and 24 hours in the **Hrs** box.
8. Click **Save** to save the changes. A Saved Successfully message appears in the Information message panel.

Data collection for all the newly created data source connections is enabled by default. For more information about configuring network data source connections, see the *Operations Bridge Reporter Online help for Administrators*.

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%/jConnect-7_0/classes` (**On Windows**) and `$SYBASE\jConnect-7_0\classes` (**On Linux**) on Sybase IQ server to `$PMDB_HOME/lib` directory on OBR system.
2. Restart the collection service.

Configuring the VMware vCenter Data Source

You can configure VMware vCenter as the data collection source to collect virtualization metrics.

To configure VMware vCenter, follow these steps:

1. In the **Administration Console**, click **Data Source Configuration > VMware vCenter**. The **VMware vCenter Data Source** page appears.
2. Click **Create New** to create the connection. 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 application server.
User name	Name of the VMware vCenter application user.
Password	Password of the VMware vCenter application user.
Collection Station	To specify whether it is a Local / Remote Collector.

Note: You can configure additional VMware vCenter data sources using [step 2 on page 109](#) for each VMware vCenter connection that you wish to create.

4. To change the VMware vCenter data collection schedule for one or more hosts, in the **Schedule Frequency** column, specify a collection time between 5 and 60 minutes in the **Mins** box.
5. Click **Save** to save the changes. A `Saved Successfully` message appears in the Information message panel.
6. In the VMware vCenter server, grant the user the following permissions:
 - Set the datastore permission to Browse Datastore.
 - Set the datastore permission to Low Level File Operations.
 - Set the sessions permission to Validate session.
7. In the VMware vCenter server, set the Statistics Level:
 - a. In the vSphere Client, click **Administration > vCenter Server Settings**.
 - b. In the **vCenter Server Settings** window, click **Statistics**. The **Statistics Interval** page is displayed. This page displays the time interval after which the vCenter Server statistics will be saved, the time duration for which the statistics will be saved and the statistics level.

- c. Click **Edit**.
- d. In the **Edit Statistics Interval** window, set the Statistics Interval from the drop-down list. For the statistics level that you select, the **Edit Statistics Interval** window appears. This displays the type of statistics which will be collected for that level. You must set the minimum statistic level as 2.

For more information about configuring VMware vCenter data source connections, see the *Operations Bridge Reporter Online help for Administrators*.

Configuring the Operations Agent Data Source

If you configure OM or RTSM as the topology source, you do not have to create new Operations Agent data source connections. Because, by default, all the nodes on which Operations Agent is installed are automatically discovered when the topology information is collected. These data sources or nodes are listed in the Operations Agent Data Source page of the Administration Console.

To view the list of Operations Agent data sources, follow these steps:

1. In the **Administration Console**, click **Data Source Configuration > Operations Agent**. The **Operations Agent** page appears.
2. To view detailed information about the Operations Agent data sources, click the ETL Content Pack component name or the number in the **Host collection status summary** table. The **Hosts:** table appears.
3. To change the data collection schedule for a 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**.

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

For more information about configuring Operations Agent data source connections, see the *Operations Bridge Reporter Online help for Administrators*.

Configuring the Management and Profile Database Data Source

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 OM, OMi, BPM, RUM, and Service Health.

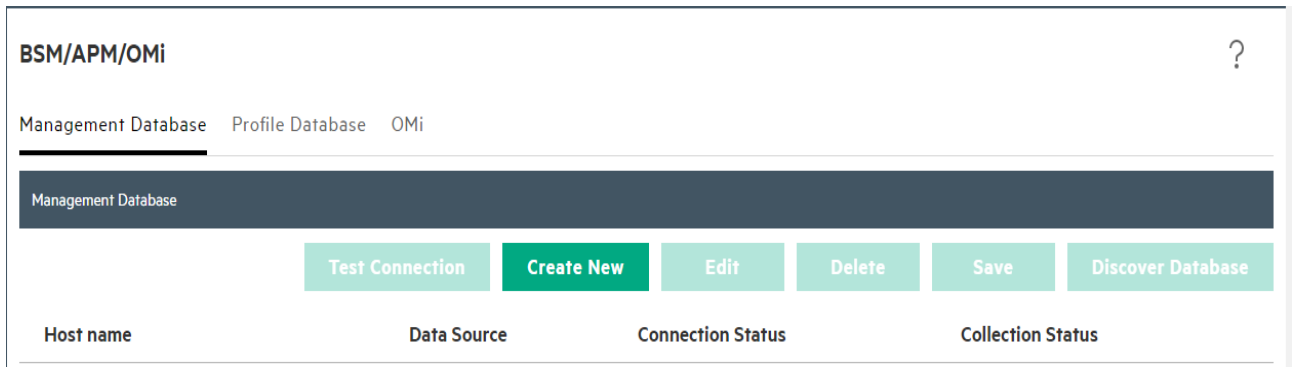
In your BSM deployment, you might have to set up multiple Profile databases for scaling because one database might not be enough to store all the data. You may also require multiple Profile database to store critical and non-critical data. The information on different Profile databases deployed in your environment is stored in the Management database.

Before you configure the multiple Profile database connections, you also need to configure the Management database on the BSM/APM/OMi page.

To configure a new Management Database, follow these steps:

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

Note: To discover Profile or Operations database in OBR system, you must copy the `seed.properties` and `encryption.properties` files from BSM/OMi server to OBR system. For more information, see "[Discover Profile or Operations Database](#)" on page 182.



2. Click **Create New**. The **Connection Parameters** dialog box appears.
3. Based on the topology source, select **Data Source** as **BSM** or **OMi**.
4. Enter appropriate values in the fields of **Connection Parameters** dialog box:

Field	Description
<ul style="list-style-type: none"> o BSM o 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. Tip: It is recommended to have a common trust store file.
Truststore Password	The password to access the truststore. This option is displayed when Enable TLS is selected.

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

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

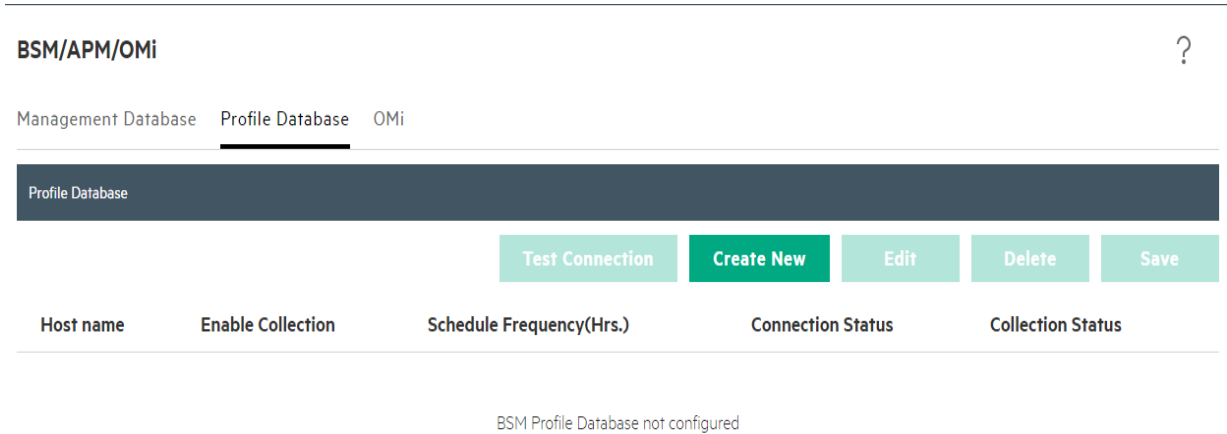
Note: If management database and profile database are on the same system as the BSM system (local database), clicking **Discover Database** will automatically discover the corresponding Profile database. If the databases are on different systems (remote database), you have to manually configure the Profile database using the **Profile Database** tab. You have to manually provide configuration details with user name and password for each profile database.

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. You have to manually provide configuration details with user name and password for each profile database.

8. Click **Save** to save the changes. A Saved Successfully message appears in the Information message pane.

To configure a new Profile database, follow these steps:

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



2. Click **Create New**. The **Connection Parameters** dialog box appears.
3. Type the following values in the **Connection Parameters** dialog box:

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

Field	Description
	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
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	<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

Field	Description
	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.
Enable TLS selected:	
Truststore Path	<p>Full path to the truststore path. This option is displayed when Enable TLS is selected.</p> <p>Tip: It is recommended to have a common trust store file.</p>
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

Field	Description
	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.

4. Click **OK**.
5. Click **Test Connection** to test the connection.
6. Click **Save** to save the changes made on this page. A *Saved Successfully* message appears in the Information message pane.

After you save the newly created Management database connection, OBR (local collector or remote collector) retrieves the Profile database information from the Management database data source and lists all the existing Profile database data sources under the Profile Database section of the page.

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

In case of a Remote Collector, the collection station has to be selected from the Database type drop down box provided in the Profile Database section of the page.

For more information about configuring Profile database data source connections, see the *Operations Bridge Reporter Online help for Administrators*.

Enable KPI Data Collection for Service Health CIs

KPIs are high-level indicators of a CI's performance and availability. The KPI data pertaining to certain logical Service Health CIs, such as Business Service, Business Application, Business Process, and Host, are logged by default in the Profile database. OBR collects this data from the database for reporting.

However, the KPI data for other CI types are not automatically logged in the Profile database. To enable the logging of the KPI data for these CI types, you must configure the CIs in the BSM. For more information, see the *Persistent Data and Historical Data* section of the *Business Service Management - Using Service Health* guide. This guide is available for the product, *Application Performance Management (BAC)*, at the following URL:

<https://softwaresupport.hpe.com/>

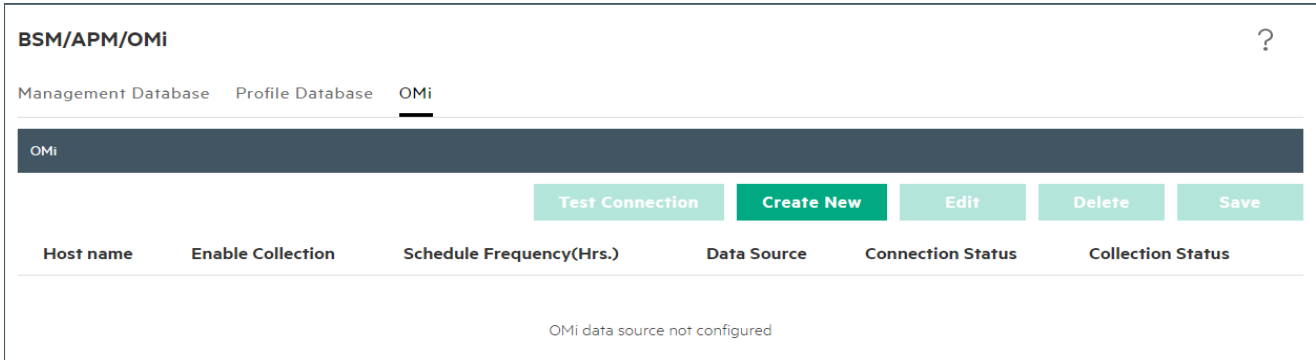
Configuring the OMi Data Source

If you install the OMi Content Pack, you must configure the OMi database connection for data collection. You can configure OBR to collect data from the following OMi data repositories:

- **Events database:** The events database stores data obtained from OMi (9.x versions) data source.
- **Operations database:** The operations database stores data obtained from OMi10 (and later versions) data source.

Note: Before you create a new OMi data source connection, make sure that a data source connection for the Management database exists on the Management DB / Profile DB page, see "[Configuring the Management and Profile Database Data Source](#)" on page 132. This data connection is required to retrieve Assigned User/Group information for OMi, which is stored in 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 BSM RTSM that was configured as the topology source.



To configure the OMi data source connections, follow these steps:

1. In the **Administration Console**, click **Data Source Configuration > BSM/APM/OMi > OMi**.
2. Click **Create New** to create a new OMi data source connection. The **Connection Parameters** dialog box appears.
3. Specify or type the following values in the **Connection Parameters** dialog box:

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.

Field	Description
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. 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.

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 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 **OK**.

Note: You can create only one OMi data source connection. After the connection is created, the **Create New** button is disabled by default. Make sure that you type in the correct values.

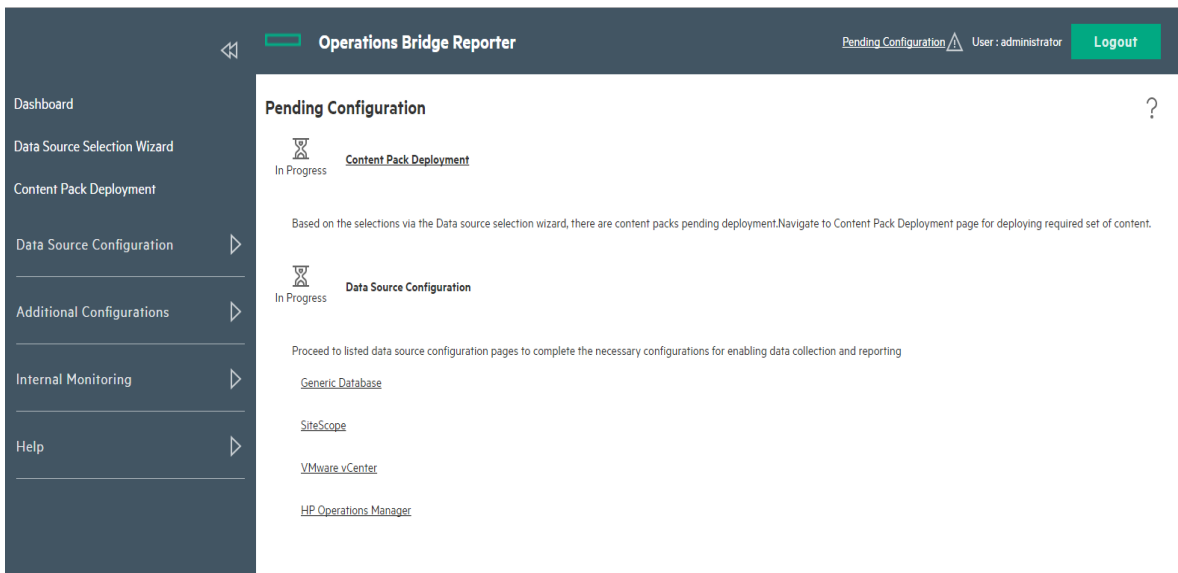
5. Click **Test Connection** to test the connection.
6. Click **Save** to save the changes. A *Saved Successfully* message appears in the Information message panel.
7. To change the OMi data collection schedule for one or more hosts, in the **Schedule Frequency** column, specify a collection time between 1 and 24 hours in the **Hrs** box.
8. Click **Save** to save the changes. A *Saved Successfully* message appears in the Information message panel.

For more information about configuring OMi data source connections, see the *Operations Bridge Reporter Online help for Administrators*.

Chapter 7: Pending Configuration

This page displays status of Content Pack Component Installation, and Data Source Configuration. Based on the status you can decide to install the remaining Content Pack or configure the data sources.

The following image shows the pending configurations based on the data source selected. Click on the links provided in the console to complete the pending configurations.



Part III: Additional Configuration and Administration

This section provides information and procedures to configure and administer OBR. This section helps you to configure Operation Agent for data collection in secure mode, report drill feature, set up internal alters, certificates, create keystore file using keytool, Vertica cluster, external Vertica, and logon banner.

Chapter 8: Configuring the Operations Agent for Data Collection in Secure Mode

The Operations Agent supports HTTP 1.1-based communications interface for data access between client and server applications. However, you can also configure data collection from Operations Agent-managed nodes via the secure (HTTPS) mode. Because HTTPS communication is certificate-based, certificates must be installed on the OBR system and on the managed nodes. The OBR system acts as a certificate client and the certificate server (certificate authority) is provided by the OM.

If the `SSL_SECURITY` is enabled in agents, then the collection from the agent to OBR fails with **No trusted certificate found** error. The collection happens only with HTTPS protocol and proper certificates installed. To get data, the certificates from certificate server corresponding to the agent(s) should be installed on OBR system or on the remote collector.

To check if the `SSL_SECURITY` is enabled, run the following command:

```
ovconfget
```

If `SSL_SECURITY` is set to `ALL` or `REMOTE` then it is enabled.

To install certificates from the server to OBR or remote collector, follow these steps:

Task 1: Configuration on OBR system

1. Log on to OBR machine.
2. To list the installed certificate on OBR machine, run the following command:

```
ovcert -list
```

3. To delete the certificate on OBR machine, run the following command:

```
ovcert -remove <certificate no>
```

where, *certificate no* is the certificate alias number.

4. Enter `Y` in the following prompt to remove the certificate. A status message is displayed.

5. To change the certificate server to OM server, run the following command:

```
ovconfchg -ns sec.cm.client -set CERTIFICATE_SERVER <OM_SERVER>
```

where, *<OM_SERVER>* is the name of the OM system

or

Run the following command and change the certificate server values manually:

```
ovconfchg -edit
```

6. To request for certificate, run the following command:

```
ovcert -certreq
```

7. Log on to OM system and run the following command to list the certificate:

```
ovcm -listpending -l
```

8. Run the following command to get the certificate ID corresponding to OBR machine:

```
ovcm -grant <certificate ID> -host <obr_hostname>
```

where, <certificate ID> is the certificate ID corresponding to OBR system

<obr_hostname> is the name of the OBR system

9. Run the following commands to verify that the certificates are installed properly:

```
ovcert -list
```

```
ovcert -check
```

10. Run the following command on the OBR system:

```
ovcert -exporttrusted -file <filename> -ovrg server
```

11. Run the following command on the OBR system:

```
ovcert -importtrusted -file <filename>
```

where, <filename> is the name of the file mentioned in the above step.

12. Run the following command to trust the OM server keystore and import the certificate to the OBR local keystore:

```
ovcert -trust <OM_SERVER> -ovrg server
```

where, <OM_SERVER> is the name of the OM server

13. Run the following command to restart the ovc:

```
ovc - restart
```

The collection happens from the agents that are enabled, that is, where SSL_SECURITY is set to ALL or REMOTE.

Note: If you are configuring HTTPS for new remote collector, perform the following ["Task 2a: Configuring HTTPS on new remote collector" on the next page](#). If you are configuring HTTPS for

already existing remote collector, perform the following ["Task 2b: Configuring HTTPS on an existing remote collector"](#) on the next page.

Task 2a: Configuring HTTPS on new remote collector

Perform the following steps once the new remote collector is installed.

1. Go to %PMDB_HOME%\bin\script (on Windows) and \$PMDB_HOME/bin/script (on Linux) and run the following command to configure the poller with OM server:

```
perl configurePoller.pl <OM_Server>
```

2. Ensure that you have added the new remote collector in OM server and the certificate request is accepted.
3. Run the following commands on the remote collector to verify that the certificates are installed properly:

```
ovcert -list
```

```
ovcert -check
```

4. Log on to OBR system and run the following command:

```
C:\>ovcert -exporttrusted -file C:\trusted_cert -ovrg server
```

5. Copy the certificate file generated in the above step to the new remote collector.
6. Run the following command on the remote collector to import the trusted certificate file:

```
ovcert -importtrusted -file C:\trusted_cert
```

7. To get the coreID from OBR system, follow these steps:

- a. Log on to OBR system and run the following command:

```
ovcoreid
```

You have to note the core ID displayed by the above command.

8. Run the following command on the remote collector and edit the MANAGER and MANAGER_ID parameters:

```
ovconfchg -edit
```

Set the MANAGER parameter to <OBR server name> and MANAGER_ID to the core ID you noted in the above step.

9. Restart the ovc.

10. Log on to the Administration Console. Go to **Additional Configurations > Collectors** and

configure the new remote collector.

For information on configuring the new remote collector, see "[Task 4: Configuring the Remote Collectors](#)" on page 53.

Task 2b: Configuring HTTPS on an existing remote collector

1. Run the following commands on the remote collector to check the existing certificate and remove it:

```
ovcert -list
```

```
ovcert -remove
```

2. Run the following command to change the certificate server from OBR Server to OM Server:

```
ovconfchg -ns sec.cm.client -set CERTIFICATE_SERVER <OM_SERVER>
```

where, <OM_SERVER> is the name of the OM system

or

Run the following command and change the certificate server values manually:

```
ovconfchg -edit
```

3. To request for certificate, run the following command:

```
ovcert -certreq
```

4. Log on to OM system and run the following command to list the certificate:

```
ovcm -listpending -l
```

5. Run the following command to get the certificate ID corresponding to remote collector :

```
ovcm -grant <certificate ID> -host <Remotecollector_hostname>
```

where, <certificate ID> is the certificate ID corresponding to OBR system

<Remotecollector_hostname> is the host name of remote collector

6. Run the following commands on remote collector to verify that the certificates are installed properly:

```
ovcert -list
```

```
ovcert -check
```

7. Log on to OBR system and run the following command:

```
ovcert -exporttrusted -file <file_name> -ovrg server
```

where, *<file_name>* is the trusted certificate file name

8. Copy the certificate file generated in the above step to the remote collector.
9. Run the following command on the remote collector to import the trusted certificate file:

```
ovcert -importtrusted -file <file_name>
```

where, *<file_name>* is the trusted certificate file name exported in the [Step 7](#).

10. Log on to the Administration Console.
11. To verify that proper collection is happening, go to **Additional Configurations > Collectors** and click **Test** and then click **Save**.

Chapter 9: Configuring the Report Drill Feature Settings

OBR includes the SAP BusinessObjects BI launch pad portal that enables you to view the generated reports. SAP BusinessObjects BI launch pad provides a Drill feature that you can use to view information at a daily, monthly, and yearly level. However, when drilling up or down within a report, sections of the report might not display the relevant data for the specified level. This is because the report blocks lose the synchronization between the Drill options in the report. To ensure that the reports display the correct data, you need to re-establish the synchronization by configuring the SAP BusinessObjects BI launch pad Preference settings.

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 is displayed.

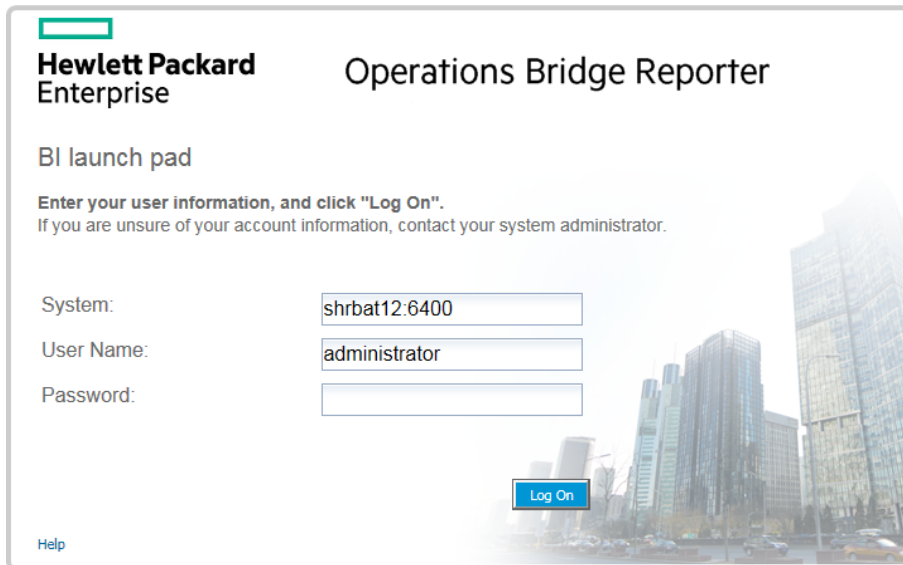
2. Enter user name as **administrator** in the **User Name** field and password in the **Password** field.
3. Click **Log On**.

The **Home** page is displayed.

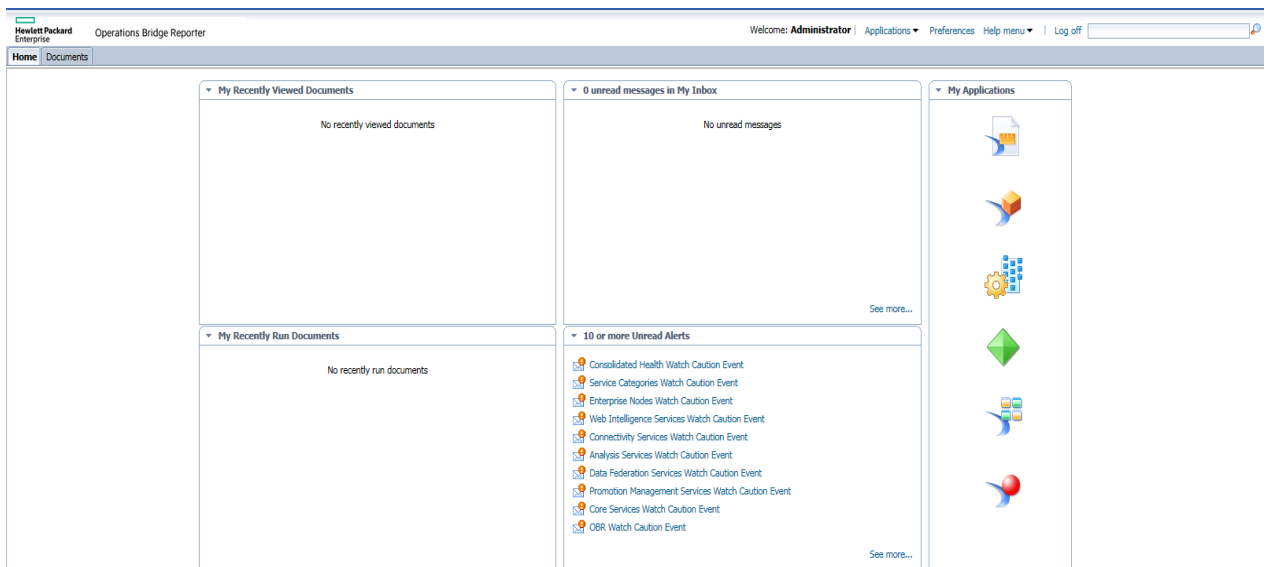
4. In the Administrator Console, click **Additional Configurations > Reporting Platform**.

The **Reporting Platform** page is displayed.

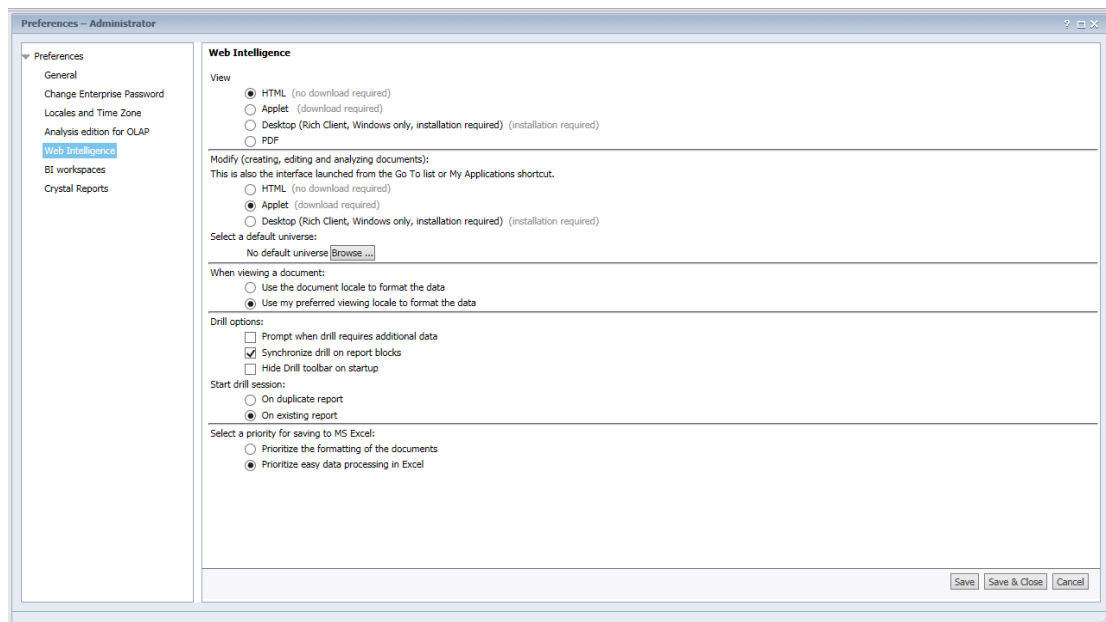
5. Click **Launch BI launch pad**. The SAP BusinessObjects BI launch pad log on page is displayed.



6. Enter user name as **administrator** in the **User Name** field and password in the **Password** field.
7. Click **Log On**. The SAP BusinessObjects BI launch pad Home page is displayed.



8. Click **Preferences**. The Preferences page opens.



9. Click **Web Intelligence**.
10. Under **Drill options**, select the **Synchronize drill on report blocks** option, and Click **Save & Close**.
11. Close the web browser.

Chapter 10: Configuring the Internal Alerting Service

The Home page of Administration Console displays the connectivity status, runtime file distribution, content health summary, collection status and alerts. OBR can be configured to send traps or emails when there is a failure in OBR system. You can also view the alerts in administration console of OBR. Alerts are sent when a service stops or when there is a failure in data processing.

The **HPE_PMDB_Platform_IA** service is responsible for internal alerting. Internal Alerting (IA) is a supportability tool used to alert when some parts of OBR are non operative. IA also sends alerts for current status of the services mentioned below. You can receive the following types of alerts from IA:

- Email
- SNMP trap
- Health alerts on Administration Console

Understanding how the Internal Alert rules work

The IA framework reads `SHR_Deployment.conf` file first and gets information on the OBR components that are installed on the system. Based on this information, IA framework loads the corresponding rules in the individual `.rule` files in the location `{PMDB_HOME}/bin/scripts/perl/InternalAlerting`.

For example:

- If IA is enabled on the system where all the OBR components are installed, then `SHRServer_IA.rule`, `BO_IA.rule`, `VerticaIA.rule` will be loaded.
- If IA is enabled on the system where the OBR server and SAP BusinessObjects components are installed, then `SHRServer_IA.rule` and `BO_IA.rule` will be loaded.

Following `.rule` files can be found in the location `{PMDB_HOME}/bin/scripts/perl/InternalAlerting`:

- `SHRServer_IA.rule`
- `BO_IA.rule`
- `Vertica_IA.rule`
- `Custom_IA.rule`
- `RC_IA.rule`

You can check the rules that have been loaded from `{PMDB_HOME}/log/IAEngine.log`.

The following services are monitored by IA:

1. Collection Configuration
2. Duplicate Dimensions
3. Server Runtime Data on Disk
4. Collector Runtime Data on Disk
5. Data Latency
6. Service Down
7. Connectivity
8. Collector Certificate
9. System Resource

Scheduled Execution

The OBR services are monitored every hour. However, all the other features are monitored at 8:00 AM local time every day.

Configure Internal Alerting Service

To configure the internal alerting service, follow these steps:

1. Open the `IA_Config.prp` file in a text editor from `%PMDB_HOME%\data` (on Windows) or `$PMDB_HOME/data` (on Linux).

To configure e-mail, follow these steps:

- a. Enter the e-mail ID where you want to receive the alerts in `email.to` parameter.
- b. Enter the domain name of the system where OBR is installed in `email.from` parameter.
- c. Enter the domain name of the mail server in `email.host` parameter.

To configure OBR to send SNMP traps to the third party SNMP Trap receiver, follow these steps:

Note: Copy the `hp-shr.mib` and `hp-nnm1.mib` files from `%PMDB_HOME%\config` (on Windows) and `$PMDB_HOME/config` (on Linux) to the system where SNMP Trap Receiver is installed. Load these `.mib` files to the SNMP Trap Receiver.

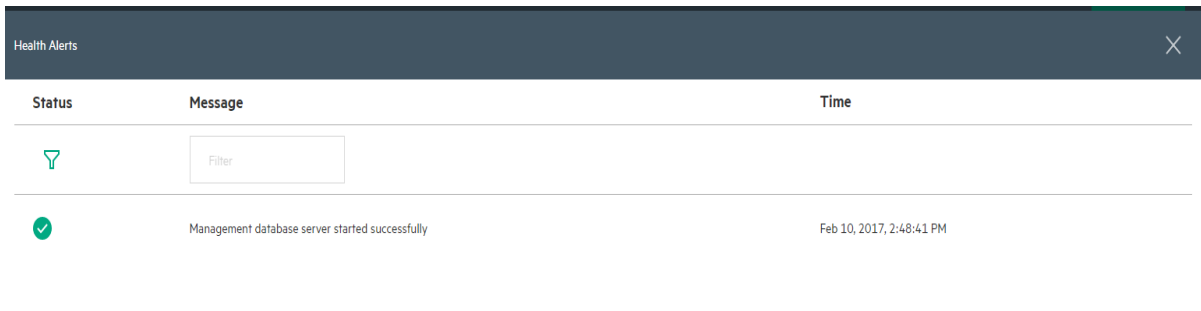
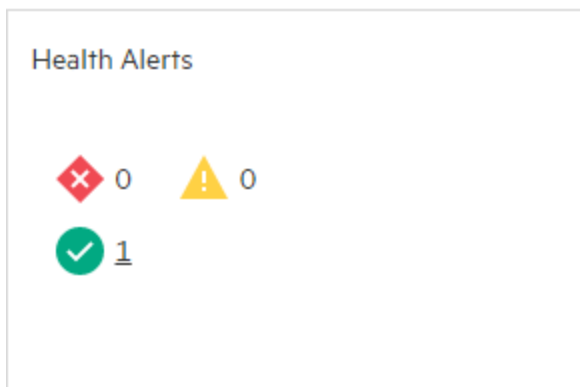
- a. Enter the IP address of the system where SNMP Trap Receiver is installed in `snmp.TargetHost` parameter.


- b. Enter the port number of the system where SNMP Trap Receiver is installed in `snmp.TargetPort` parameter.
2. Save and close the `IA_Config.prp` file.
3. On a system where OBR is installed, open the command prompt and run the following command to enable the internal alerting service:

```
enableIA
```
4. Restart the **HPE_PMDB_Platform_IA** service.

You can also view the OBR Health alerts in the Administration Console.

1. Log on to Administration Console. The **Dashboard** is displayed.
2. Click **Health Alerts** links to view the internal alerts.



Status	Message	Time
	Management database server started successfully	Feb 10, 2017, 2:48:41 PM

Change threshold value for free space of the disk

You will get an alert if the free space falls below 15% of the disk space. If you receive an alert when the free space falls below 15% of the disk space, reset the threshold value by editing the `im.disk.space.warnLimit` (Free Space Threshold) parameter in `config.prp` located at `{PMDB_HOME}/data/`.

Customizing IA rules

You can create new customized rules in `Custom_IA.rule`. Do not change or edit `SHRServer_IA.rule`, `BO_IA.rule`, `Vertica_IA.rule`, `RC_IA.rule`.

Caution: You must make sure that the custom rules does not consume more resources.

The following image shows a sample rule:

```
type=Calendar
time=0 1-23/1 ****
desc=Running ServiceStatus perl script
action=shellcmd perl IA_HOME_PATHServiceStatus.pl -output_file=IAEvent -output_dir=IA_PMDB_PATH

type=Single
ptype=RegExp
pattern=(\S+):STOPPED
desc=If Service stopped it will save the context in Storable module
context=SERVER_STOPPED_CONTEXT_$1
action=shellcmd echo $1;shellcmd sendemail -s "Service Status Test" -b "Service $1 is down";shellcmd shralert "Service $1 is down"; shellcmd sendtrap ServiceStatusTest -args [$1=down];create SERVER_STOPPED_CONTEXT_$1;event SAVE_CONTEXT;

type=Single
ptype=RegExp
pattern=(\S+):RUNNING
desc=If Service running it will save the context in Storable module and delete stopped or failed context
context=SERVER_STOPPED_CONTEXT_$1
action=shellcmd echo "HPE_PMDB_Platform ${1} is RUNNING";shellcmd sendemail -s "Service Status Test" -b "Service $1 is up";shellcmd shralert "Service $1 is up"; shellcmd sendtrap ServiceStatusTest -args [$1=up];delete SERVER_STOPPED_CONTEXT_$1;event SAVE_CONTEXT;
```

Description of the fields used in the sample:

- `type`: Rule type (Calendar or Single)
- `time`: Time frequency of running the rule
- `ptype`: Pattern type (value is case insensitive)
- `pattern`: Pattern for recognizing input events
- `context`: context expression
- `desc`: operation description string
- `action`: action list

For more information on the fields, see <https://simple-evcorr.github.io/man.html>.

The sample rule has three parts. The first part is the rule type that runs at the specified time and checks the service and writes the information in the `IAEvent.log` file. The part two and three looks for the type of pattern mentioned in **pattern**, updates the **context** accordingly and performs the corresponding action as mentioned in **action** field.

In the sample rule, the first part checks for the service status and logs the status in `IAEvent.log`. Part two and three will search for a pattern and execute their actions based on the **context**. The alert information will be sent as an email as described in the **action** field.

Chapter 11: Certificates for OBR

This chapter provides information on Client Authentication certificate for OBR and recommends the use of SSL.

Use Secure Sockets Layer (SSL) Certificate

The Secure Sockets Layer (SSL) is a networking protocol that manages server authentication, client authentication and encrypted communication between servers and clients. The SSL secures communication by encrypting data and provides authentication. Without SSL encryption, the information that travels over network is vulnerable to attacks, such as Man In The Middle (MITM). Setting up the SSL certificate to enable secure connection between two systems communicating over the network is critical.

Note: OBR highly recommends the use of Certificate Authority (CA) signed certificate. To configure OBR to use the CA signed certificate, see *Generating a Certificate Authority Signed Certificate* section in *Operations Bridge Reporter Interactive Installation Guide*.

OBR does not recommend the use of self-signed certificate when setting up the SSL connection.

Following are the default certificate locations for SSL communication used by OBR:

Name	Location	File name	Description
Keystore	{PMDB_HOME}/keystore	SHR_CERT_HTTPS	As part of OBR installation, the SHR_CERT_HTTPS file is created by default and used for Administration Console and SAP Business Objects (BI Launch pad, CMC) URLs.
Stores	{PMDB_HOME}/stores	cacert	When SSL is configured for SiteScope through the Administration Console for OBR integration with SiteScope Server over https, the trust store file cacert is created in this location.
cacert	{JAVA_HOME}/security/	cacert	This location is used by OBR for CAC communication.

Client Authentication Certificate for OBR

OBR provides certificate based client authentication. OBR verifies the identity by validating the certificate and authorizes the user using SAP BusinessObjects.

Authentication and Authorization

OBR uses SAP BusinessObjects for authentication and authorization. SAP BusinessObjects user accounts are managed by SAP BusinessObjects Central Management console. You must be a SAP BusinessObjects administrator to access OBR Administration console. By default, OBR uses username/password based authentication mechanism. You can also configure OBR to use client certificate based authentication by following the steps in ["Configuring OBR Administration Console "](#) for Administration console and ["Configuring SAP BusinessObjects BI Launch Pad"](#) for SAP BusinessObjects BI Launch Pad. OBR verifies the identity of the user by validating the certificate and authorizes the user using SAP BusinessObjects.

Prerequisites of Certificate Based Authentication

Before you configure certificate based authentication ensure that the following prerequisites are met.

Task 1: Create a keystore file containing OBR server certificate and private key

The keystore file is password protected. OBR enables you to configure keystore location and password using keystorepath and keystorepasswd properties. Keystorepath should be specified in the properties files in ["Task 4: Configuring for Certificate-based Authentication" on page 164](#) for Administration Console and ["Task 4: Set up the Certificate-based configuration" on page 169](#) for SAP BusinessObjects BI Launch Pad. Keystoretype property enables you to specify the type of the keystore, supported values are **JKS** and **PKCS12**. The certificate alias in the keystore is specified using the keyalias property as shown in the following table:

Property name	Example
Keystorepath	\\certs\serverkeystore.jks (Linux) C:\\certs\\serverkeystore.jks (Windows)
Keystorepasswd	changeit

Property name	Example
Keyalias	shserver
Keystoretype	JKS

For more information, see *Generating a Certificate Authority Signed Certificate* in Next Steps section of *Operations Bridge Reporter Interactive Installation Guide*.

Task 2: Create a keystore file containing the Certifying Authority (CA) certificates

You must create a keystore file containing the CA certificates trusted by the OBR server. This file is password protected. OBR enables you to configure truststore by setting the `truststorepath`, `truststorepasswd`, and `truststoretype` properties to values as shown in the following table. The `truststorepath` should be specified in the properties files in "[Task 4: Configuring for Certificate-based Authentication](#)" and "[Task 4: Set up the Certificate-based configuration](#)".

Property name	Example of values
truststorepath	\\certrelated\Trustkeystore (Linux) C:\\certrelated\\Trustkeystore (Windows)
truststorepasswd	changeit
truststoretype	JKS

For more information, see *Generating a Certificate Authority Signed Certificate* in Next Steps section of *Operations Bridge Reporter Interactive Installation Guide*.

Task 3: Determine if certificate revocation check should be enabled

You should set `com.sun.net.ssl.checkRevocation` to true, to enable certificate revocation check. OBR supports two methods of checking for revoked certificates.

- Certificate Revocation List (CRL) - A CRL contains information about revoked certificates and is downloaded from the CA. OBR extracts the CRL distribution point URL from the certificate. You should set `com.sun.security.enableCRLDP` to true to enable this check.
- Online Certificate Status Protocol (OCSP) - OCSP is a protocol for checking revocation of a single certificate using an online service called an OCSP responder. You should set `ocsp.enable` to true to enable revocation check using OCSP protocol. OBR extracts the OCSP URL from the certificate for validating the certificate. If you want to configure a local OCSP responder service, OBR enables you to configure it using `ocsp.responderURL` property.

For details on how to enable certificate revocation, CRL and OCSP on OBR Administration Console, see "[Task 4: Configuring for Certificate-based Authentication](#)" in "[Configuring OBR Administration Console](#)"

For details on how to enable certificate revocation, CRL and OSCP on SAP BusinessObjects BI Launch Pad, see "Task 4: Set up the certificate-based configuration" in "[Configuring SAP BusinessObjects BI Launch Pad](#)".

Task 4: Determine the proxy server address if there is a proxy between the OBR server and internet

In case of a proxy server, you must set it to enable OBR server to download the CRL. You can configure the proxy server as:

http.proxyHost	set the http proxy Hostname
http.proxyPort	set the http proxy Port number
https.proxyHost	set the https proxy Hostname
https.proxyPort	set the https proxy Port number

For more details, see "[Task 4: Configuring for Certificate-based Authentication](#)" in Configuring OBR Administration Console.

Task 5: Determine the username extraction mechanism

The username extraction mechanism depends on the format of your certificate. The user name extracted from the certificate should match the user names configured in SAP BusinessObjects. OBR enables you to extract username using SubjectDN and Subject Alternative Name (SAN) mechanisms.

To configure the username extraction mechanism, set the following properties in `server.xml` as shown given in the below table:

Properties	Value
field	SubjectDN
entry	set to CN to indicate CN as the username or set to OU to indicate OU as the username

For example,

```
<Realm className="com.hp.bto.bsmr.SHRSecureAuth.auth.SHRRealm" field="SubjectDN" entry="CN" Type="" oid="" pattern="" useSubjectDNNonMatchFail="true"/>
```

- To extract username from SubjectDN, set the following values to the properties

The entry property enables you to specify the entry that should be considered as username in SubjectDN. You can also use a pattern to extract username from SubjectDN instead of using entry

parameter. To configure a pattern to extract username from SubjectDN, use pattern parameter. For example, if the pattern is configured as EMAILADDRESS=(.+@) and if abc@hpe.com is the value of emailaddress field, then abc is extracted as the username.

- To extract username from Subject Alternative Name (SAN)

Set the property field to the value SAN. You can configure rcf822Name or otherName part of the SAN username using the property Type.

To configure rcf822Name, set the value of the property Type to rcf822Name.

To configure otherName set the value of the property Type to otherName and set the value of object identifier (OID) to OID.

By default, OBR extracts username from CN of SubjectDN.

You can configure OBR to allow a user to log on using smart card only. To enable smart card logon, you must set the property smartcard.enable to true.

The location of the file server.xml is given in the table below:

For configuring	Path
Administrator console	\$PMDB_HOME/adminserver/conf (for Linux) %PMDB_HOME%\adminserver\conf (for Windows)
SAP BusinessObjects BI Launch Pad	\$PMDB_HOME/BOWebServer/conf (for Linux) %PMDB_HOME%\BOWebServer\conf (for Windows)

Task 6: Import Certificate and Configure Browser

- Import the certificate that has been issued by the root CA to the OBR server. Import it to your web browser using the **Trusted Root Certificate** tab available in the Internet Explorer. For details, see the Internet Explorer help.
- Configure your web browser to accept the protocol TLSv1, here v1 indicates the version.

Note: For High Availability, configure both servers.

OBR enables you to configure certificate based authentication for Administration Console and SAP BusinessObjects BI Launch Pad.

Configuring Username Extraction Method

Username extraction can be configured by editing the `server.xml` file, for details, see [Task 5: Determine the username extraction mechanism](#).

Configuring OBR Administration Console

Before you proceed, ensure that the post-install configuration of OBR is successful. To configure OBR Administration Console for Certificate Based Authentication, follow these steps:

Task 1: Configuring trusted authentication

Shared secret is used to establish trusted authentication. You must enter the shared secret in character format only.

1. Type `https://<OBR_Server_FQDN>:21412/OBRApp` on the browser to log on to the Administration Console of OBR.

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

2. Go to **Additional Configurations > Security > BO Trusted Authentication**

Security

LW-SSO **BO Trusted Authentication** Logon Banner

BO Trusted Authentication Configuration

BO Enabled Disabled

Shared Secret

Save

3. Select the **Enabled** option.
4. Type the **Shared Secret**.
5. Click **Save**.

After successful configuration, the message given below is displayed:



Task 2: Stop the HPE_PMDB_Platform_Administrator service

• On Windows

To stop the **HPE_PMDB_Platform_Administrator** service, follow these steps:

- Click **Start > Run**. The Run dialog box opens.
- Type `services.msc` in the Open field, and then press **Enter**. The Services window opens.
- On the right pane, right-click `HPE_PMDB_Platform_Administrator`, and then click **Stop**.

• On Linux

Go to `/etc/init.d` and run the following command:

On RHEL 6.x/SUSE Linux Enterprise Server 11: `service HPE_PMDB_Platform_Administration stop`

On RHEL 7.x: `systemctl stop HPE_PMDB_Platform_Administration.service`

Task 3: Configuring the config.prp file

In the file `config.prp`, located at `%PMDB_HOME%\data` folder (for Windows) and `$PMDB_HOME/data` (for Linux) set the given value to the following fields:

Field	Value
<code>shr.loginMethod</code>	<code>certbased</code>
<code>shr.auth.classes</code>	<code>com.hp.bto.bsmr.security.auth.BOTrustedAuthenticator</code>

Task 4: Configuring for Certificate-based Authentication

Specify following parameters in `adminserverclientauth.prp` file located at `$PMDB_HOME/data` (for Linux) and `%PMDB_HOME%\data` folder (for Windows). Edit the following fields and set the values according to the given description:

Field	Description
<code>truststorepath</code>	Full path of the truststore file, which is to use to validate client certificates.
<code>truststorepasswd</code>	The password to access the trust store.

Field	Description
truststoretype	The type of keystore used for the trust store.
keystorepath	Full path of the keystore file where you have stored the server certificate to be loaded.
keystorepasswd	The password used to access the server certificate from the specified keystore file.
keystoretype	The type of keystore file to be used for the server certificate.
keyAlias	The alias used to for the server certificate in the keystore
smartcard.enable	Set to true to enable smart card logon and to false to disable smart card logon.
http.proxyHost	HTTP proxy Host name.
http.proxyPort	HTTP proxy Port number.
https.proxyHost	HTTPS proxy Host name.
https.proxyPort	HTTPS proxy Port number.
com.sun.net.ssl.checkRevocation	Set it as true for enabling revocation and to false to disable revocation.
com.sun.security.enableCRLDP	Set it to true to enable CRL revocation, otherwise set it to false.
crlFile	Enter the CRL file path.
ocsp.enable	Set it to true to enable OSCP based revocation, otherwise set it to false.
ocsp.responderURL	Set the OCSP responder URL.

Note: You must set the OSCP based revocation to false, when the CRL based revocation is set to true and vice versa.

After setting the properties value, do the following:

- **On Windows**

- a. Go to the %PMDB_HOME%\bin folder.
- b. Run the following command:

```
perl adminserverclientauth.pl -authType clientcert -configFile <config file location>
```

where *<config file location>* indicates the full path of `adminserver.prp` file

For example, `%PMDB_HOME%\data\adminserverclientauth.prp`.

- **On Linux**

- a. Go to `$PMDB_HOME/bin` folder.
- b. Run the following command:

```
perl adminserverclientauth.pl -authType clientcert -configFile <config file location>
```

where *<config file location>* indicates the full path of `adminserver.prp` file.

For example, `$PMDB_HOME/data/adminserverclientauth.prp`

Task 5: Configure Username Extraction

Ensure that CN entry in the SubjectDN field is extracted as username by OBR. In case you need different username extraction mechanism, modify the `server.xml` file as described in [Task 5: Determine the username extraction mechanism](#).

Task 6: Start the HPE_PMDB_Platform_Administrator service

To start the `HPE_PMDB_Platform_Administrator` service, follow these steps:

- **On Windows**

- a. Click **Start > Run**. The Run dialog box opens.
- b. Type `services.msc` in the Open field, and then press **Enter**. The Services window opens.
- c. On the right pane, right-click `HPE_PMDB_Platform_Administrator`, and then click **Start**.

- **On Linux**

Go to `/etc/init.d` and run the following command:

On RHEL 6.x/SUSE Linux Enterprise Server 11: `service HPE_PMDB_Platform_Administration start`

On RHEL 7.x: `systemctl start HPE_PMDB_Platform_Administration.service`

Task 7: Verify certificate based authentication

1. Type `https://<OBR_Server_FQDN>:21412/OBRApp` on the Web browser to log on to the Administration Console of OBR.

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

2. Click **LOG ON WITH A DIGITAL CERTIFICATE**.

Revert back to Password-based authentication from Certificate-based authentication

To revert back to Password-based authentication from Certificate-based authentication, follow these steps:

On Windows:

1. Follow these steps to stop the HPE_PMDB_Platform_Administrator service.
 - a. Click **Start > Run**. The Run dialog box opens.
 - b. Type `services.msc` in the Open field, and then press **Enter**. The Services window opens.
 - c. On the right pane, right-click HPE_PMDB_Platform_Administrator, and then click **Stop**.

2. Go to the `%PMDB_HOME%\bin` folder.

3. Run the following command:

```
perl adminserverclientauth.pl -authType password
```

4. Edit the following parameters in `%PMDB_HOME%\data\config.prp`:

```
shr.loginMethod=default
```

```
shr.auth.classes=com.hp.bto.bsmr.security.auth.BOAuthenticator
```

5. Follow these steps to start the HPE_PMDB_Platform_Administrator service.
 - a. Click **Start > Run**. The Run dialog box opens.
 - b. Type `services.msc` in the Open field, and then press **Enter**. The Services window opens.
 - c. On the right pane, right-click HPE_PMDB_Platform_Administrator, and then click **Start**.

On Linux:

1. Follow these steps to stop the HPE_PMDB_Platform_Administrator service.

Go to `/etc/init.d` and run the following command:

```
On RHEL 6.x/SUSE Linux Enterprise Server 11: service HPE_PMDB_Platform_Administration stop
```

On RHEL 7.x: `systemctl stop HPE_PMDB_Platform_Administration.service`

2. Go to the `$PMDB_HOME/bin` folder.
3. Run the following command:

```
perl adminserverclientauth.pl -authType password
```

4. Edit the following parameters in `$PMDB_HOME/data/config.prp`:

```
shr.loginMethod=default
```

```
shr.auth.classes=com.hp.bto.bsmr.security.auth.BOAuthenticator
```

5. Follow these steps to start the `HPE_PMDB_Platform_Administrator` service.

Go to `/etc/init.d` and run the following command:

On RHEL 6.x/SUSE Linux Enterprise Server 11: `service HPE_PMDB_Platform_Administration start`

On RHEL 7.x: `systemctl start HPE_PMDB_Platform_Administration.service`

Configuring SAP BusinessObjects BI Launch Pad

Note: In a custom installation of OBR with a remote SAP BusinessObjects system, copy the `SHRTrustedPrinciple.conf` file from `<Install_Dir>/PMDB/adminServer/conf` to `<Install_Dir>/PMDB/BOWebServer/conf` on the system where SAP BusinessObjects is installed.

Task 1: Stop the SAP BusinessObjects WebServer service

Note: In a custom installation of OBR, perform this tasks on the system where SAP BusinessObjects is installed.

- **On Windows**

To stop the SAP BusinessObjects WebServer service:

- a. Log on to the host system as administrator.
- b. Click **Start > Run**. The Run dialog box opens.
- c. Type `services.msc` in the **Open** field, and then press **Enter**. The Services window opens.
- d. Right-click the **Business Object WebServer** service and select **Stop** to stop the service.

- **On Linux**

- a. Go to `$PMDB_HOME/BOWebServer/bin`
- b. Run the following command:

```
./shutdown.sh
```

Task 2: Stop the HPE_PMDB_Platform_Administrator service

• On Windows

To stop the **HPE_PMDB_Platform_Administrator** service, follow these steps:

- a. Click **Start > Run**. The Run dialog box opens.
- b. Type `services.msc` in the **Open** field, and then press **Enter**. The **Services** window opens.
- c. On the right pane, right-click **HPE_PMDB_Platform_Administrator**, and then click **Stop**.

• On Linux

Go to `/etc/init.d` and run the following command:

On RHEL 6.x/SUSE Linux Enterprise Server 11: `service HPE_PMDB_Platform_Administration stop`

On RHEL 7.x: `systemctl stop HPE_PMDB_Platform_Administration.service`

Task 3: Edit the config.prp file

In the file `config.prp`, located at `%PMDB_HOME%\data` folder (for Windows) and `$PMDB_HOME/data` (for Linux) set the given value to the field.

Field	Value
<code>bo.protocol</code>	<code>https</code>

Task 4: Set up the Certificate-based configuration

Note: In a custom installation of OBR, perform this tasks on the system where SAP BusinessObjects is installed.

Set the following fields in the file `BOclientauth.prp`, located at `$PMDB_HOME/data` (for Linux) and `%PMDB_HOME%\data` folder (for Windows) to the values as given in the description.

Field	Description
<code>truststorepath</code>	Full path to the truststore file
<code>truststorepasswd</code>	The password to access the trust store

Field	Description
truststoretype	The type of key store used for the trust store
keystorepath	Full path of the keystore file where you have stored the server certificate to be loaded.
keystorepasswd	The password used to access the server certificate from the specified keystore file.
keystoretype	The type of keystore file to be used for the server certificate.
keyAlias	The alias used to for the server certificate in the keystore.
smartcard.enable	Set it to true for enabling smart card logon or else set it to false.
http.proxyHost	HTTP proxy Host name
http.proxyPort	HTTP proxy Port number
https.proxyHost	HTTPS proxy Host name
https.proxyPort	HTTPS proxy Port number
com.sun.net.ssl.checkRevocation	Set it to true to enable revocation or else set it to false.
com.sun.security.enableCRLDP	Set it to true to enable CRL revocation or else set it to false.
crlFile	Enter the CRL file path.
ocsp.enable	Set it to true for OSCP based revocation or else set it to false.
ocsp.responderURL	Set the OSCP responder URL.

Note: You must set the OSCP-based revocation to false, when the CRL based revocation is set to true and vice versa.

After setting the properties, follow these steps:

- **On Windows**

- a. Go to the %PMDB_HOME%\bin folder.
- b. Run the following command:

```
perl B0clientauth.pl -authType clientcert -configFile <config file location>
```

where <config file location> indicates the full path of B0clientauth.prp file.

For example, %PMDB_HOME%\data\B0clientauth.prp.

- **On Linux**

- a. Go to the `$PMDB_HOME/bin` folder.
- b. Run the following command:

```
perl BOclientauth.pl -authType clientcert -configFile <config file location>
```

where *<config file location>* indicates the full path of `BOclientauth.prp` file.

For example, `$PMDB_HOME/data/BOclientauth.prp`.

Run the following commands to clean up the work directory folders:

- `rm -rf $PMDB_HOME/adminServer/work/Catalina/localhost/*`
- `rm -rf $PMDB_HOME/BOWebServer/work/Catalina/localhost/`

Task 5: Start the SAP BusinessObjects WebServer service

Note: In a custom installation of OBR, perform this tasks on the system where SAP BusinessObjects is installed.

- **On Windows**

- a. Log on to the host system as administrator.
- b. Click **Start > Run**.
- c. Type `services.msc` in the Open field, and then press **Enter**. The Services window opens.
- d. Right-click the **SAP BusinessObjects WebServer** service and select **Start** to start the service.

- **On Linux**

- a. Go to the `$PMDB_HOME/BOWebServer/bin` folder.
- b. Run the command `./startup.sh`

Task 6: Start the HPE_PMDB_Platform_Administrator service

- **On Windows**

To start the `HPE_PMDB_Platform_Administrator` service, follow these steps:

- a. Click **Start > Run**. The Run dialog box opens.
- b. Type `services.msc` in the Open field, and then press **Enter**. The Services window opens.

- c. On the right pane, right-click **HPE_PMDB_Platform_Administrator**, and then click **Start**.

- **On Linux**

Go to `/etc/init.d` and run the following command:

On RHEL 6.x/SUSE Linux Enterprise Server 11: `service HPE_PMDB_Platform_Administration start`

On RHEL 7.x: `systemctl start HPE_PMDB_Platform_Administration.service`

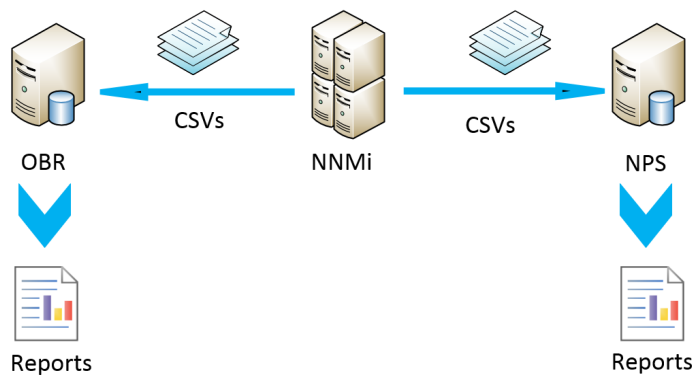
Task 7: Verify certificate based authentication

1. Type `https://<HostName>:8443/BI` on the web browser and log on to the BI launch pad of OBR.
2. A log on page is displayed. Click **Login with Digital Certificate** to log on to BI launch pad with digital certificate.

Chapter 12: Configuring OBR with Network Node Manager i (NNMi)

Note: You have to perform the following configuration steps only if you have installed Component Health and/or Interface Health Content Pack.

The OBR is integrated with NNMi to collect network performance data. The NNMi passes the network performance data as .csv files to both OBR and Network Performance Server (NPS). The OBR stores these .csv files from NNMi to data ware house to generate reports.



Prerequisite

You have to ensure that the following prerequisites are met before you go ahead with the configuration procedure:

- The NNMi and NPS are installed and configured correctly.
- The **HPE_PMDB_Platform_NRT_ETL** service is up and running.

Note: The Network Performance Content Pack collects performance data at hourly granular from NPS source. So executive summary reports display hourly/daily /monthly summarized view of Network devices collected from NPS. OBR collects performance data of only 'Switches and Routers' devices from NPS source.

The Network Component_Health and Network Interface_Health Content Pack 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 can view detailed health or utilization reports. You have to revisit the hardware requirements, if you choose to install these Content Packs.

For more information, see *Operations Bridge Reporter Performance, Sizing, and Tuning guide*.

Based on your requirement, OBR recommends you to install either the Network Performance Content Pack or Network Component_Health/Network Interface_Health Content Packs. Installing both Network Performance Content Pack and Network Component_Health/Network Interface_Health Content Packs may lead to performance issues due to redundant data.

To configure OBR and NNMi to collect network data, follow these steps:

Task 1: On the NNMi system

To configure OBR with NNMi, ensure the following:

1. The NNMi and NPS are up and running.
2. You must have the shared drive details.

You may get the details from your system administrator or check the recent output of the `nmenableperfspi.ovpl` script in `/opt/OV/newconfig` folder (**On Linux**) and `C:\Program Files (x86)\HP\HP BTO Software\newconfig` folder (**On Windows**).

Check for the most recently written file name with `nrmEnableNps.20xxxxxxxxxxxx.cfg`.

where, `xxx` is the most recent time stamp.

3. Set the `exportToSHR` property to `TRUE` in `$OvDataDir/shared/perfSpi/conf/nmsAdapter.conf` and restart NNMi.

Enable NFS Mount

NNMi by default uses CIFS to share files. Perform these steps only to configure NFS shared drive:

On Linux:

1. Edit the `/etc/exports` file.

In the `/var/opt/OV/shared/perfSpi/datafiles <Mounted System hostname>(rw, sync, no_root_squash)` parameter, add the `<OBR Server Name>(rw, sync, no_root_squash)` parameter at the end.

where, `<Mounted System hostname>` is the host name of the system that is already mounted.

`<OBR Server Name>` is the host name of the OBR system.

For example, `/var/opt/OV/shared/perfSpi/datafiles iwtest.hpeswlab.net(rw, sync, no_root_squash) iwobr.hpeswlab.net(rw, sync, no_root_squash)`

2. Run the following command to export the mount host:

```
exportfs -va
```

The exporting message appears with the mount host name and the path.

3. To check if NFS is enabled for the OBR server that is edited in the file earlier, run the following command:

```
exportfs
```

The path and the mount host name appears.

4. Set the `exportToSHR` property to `TRUE` in `$OvDataDir/shared/perfSpi/conf/nmsAdapter.conf` and run the following commands restart NNMi:

```
/opt/OV/bin/ovstop
```

```
/opt/OV/bin/ovstart
```

Run the command to check the NNMi status: `/opt/OV/bin/ovstatus`

Task 2: On the OBR system

To configure OBR to retrieve the collected network performance data from NNMi, follow these steps:

On Windows:

1. Edit the `HPE_PMDB_Platform_NRT_ETL` property. To edit the property, follow these steps:
 - a. Click **Start > Run**. The **Run** dialog box appears.
 - b. Type `services.msc` in the **Open** field, and then press **Enter**. The **Services** window appears.
 - c. On the right pane, right-click `HPE_PMDB_Platform_NRT_ETL`, and then click **Stop**.
 - d. Right-click `HPE_PMDB_Platform_NRT_ETL` and then click **Properties**. The **HPE_PMDB_Platform_NRT_ETL Service Properties** dialog box appears.
 - e. On the **Log on** tab, select **This account**.
 - f. Type `DOMAIN\Administrator` in the field (where `Administrator` is the local user having administrator privileges).
 - g. Type the user password in the **Password** field.
 - h. Retype the password in the **Confirm password** field.
 - i. Click **Apply** and then click **OK**.
2. Run the following script on the command line interface:

```
perl %PMDB_HOME%\bin\mountSharedDirectory.ovpl -n <host name>
```

where, *<host name>* is the host name of the NNMi system.

Note: The *<host name>* must be in uppercase only.

The remotely shared directory is mounted on the OBR system.

3. Edit the `%PMDB_HOME%\config\NRT_ETL\rconfig\NNMPerformanceSPI.cfg` file.

In the `PRSPI_NNMDIR //NNMHOSTNAME/PerfSpi` parameter, replace the `NNMHOSTNAME` with the actual host name of the NNMi system.

For example, `PRSPI_NNMDIR //IWFTEST.HPSWLABS.ADAPPS.HP.COM/PerfSpi`

4. In the **Services** window, on the right pane, right-click the **HPE_PMDB_Platform_NRT_ETL**, and then click **Start** to start the service.

On Linux:

Follow these steps to mount CIFS shared drive:

1. Run the following script on the command line interface:

```
perl $PMDB_HOME/bin/mountSharedDirectory.ovpl -n <host name>
```

where, *<host name>* is the host name of the NNMi system.

Note: The *<host name>* must be in uppercase only.

The remotely shared directory is mounted on the OBR system.

2. Edit the `$PMDB_HOME/config/NRT_ETL/rconfig/NNMPerformanceSPI.cfg` file.

In the `PRSPI_NNMDIR /mnt/NNMHOSTNAME/PerfSpi` parameter, replace the `NNMHOSTNAME` with the actual host name of the NNMi system.

For example, `PRSPI_NNMDIR /mnt/IWFTEST.HPSWLABS.ADAPPS.HP.COM/PerfSpi`

3. Run the following script to start the ETL:

```
perl $PMDB_HOME/bin/startETL.ovpl
```

Note: To check the status of the ETL, run `perl $PMDB_HOME/bin/statusETL.ovpl` script.

To start and stop the ETL service, run `perl $PMDB_HOME/bin/startETL.ovpl` and `perl $PMDB_HOME/bin/stopETL.ovpl`, respectively.

If the status of the service is returned as `DEAD`, then stop and start the ETL service.

For more information you can check the `$PMDB_HOME/log/NRT_ETL.log` file.

Follow these steps to mount NFS shared drive:

1. Run the following command to mount the NFS shared drive:

```
mount -t nfs <host name>://var/opt/OV/shared/perfSpi/datafiles /mnt/<host name>
```

where, <host name> is the host name of the NNMi system.

2. Edit the \$PMDB_HOME/config/NRT_ETL/rconfig/NNMPerformanceSPI.cfg file.

In the PRSPI_NNMDIR parameter, add /mnt/<NNMi host name>.

where, <NNMi host name> is the actual host name of the NNMi system.

For example, PRSPI_NNMDIR /mnt/IWFTEST.HPSWLABS.ADAPPS.HP.COM/

3. Run the following script to start the ETL:

```
perl $PMDB_HOME/bin/startETL.ovpl
```

Note: To check the status of the ETL, run `perl $PMDB_HOME/bin/statusETL.ovpl` script. To start and stop the ETL service, run `perl $PMDB_HOME/bin/startETL.ovpl` and `perl $PMDB_HOME/bin/stopETL.ovpl`, respectively.

If the status of the service is returned as DEAD, then stop and start the ETL service.

For more information you can check the \$PMDB_HOME/log/NRT_ETL.log file.

Note: If the collection has not yet started, you have to restart the service manually.

Note: The NNMPerformanceSPI.cfg file controls the operation of the iSPI Performance for Metrics.

The file contains values written by the Configuration Utility, as well as many other options with their standard and recommended settings. You should NOT modify the contents of this file directly. Doing so can affect the functionality and performance of NPS and render it unsupported.

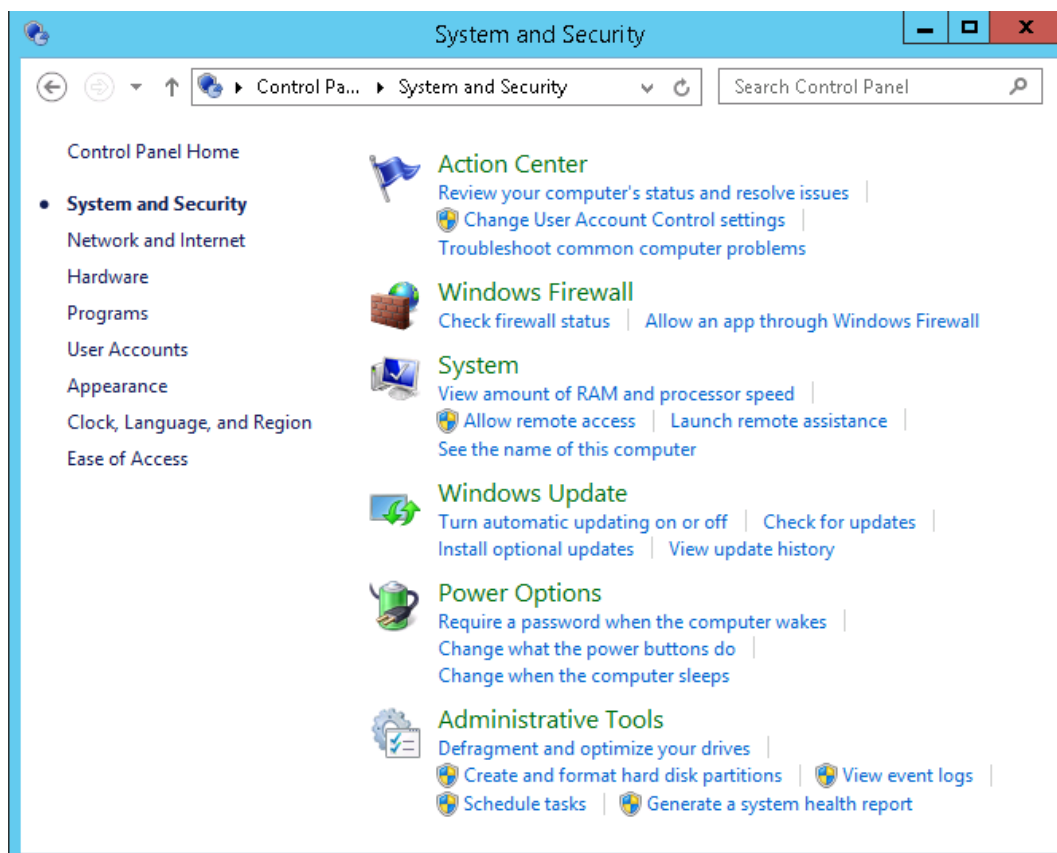
You have now successfully completed the configuration of OBR with NNMi system.

Chapter 13: Configuring DSN on Windows for Vertica Database Connection

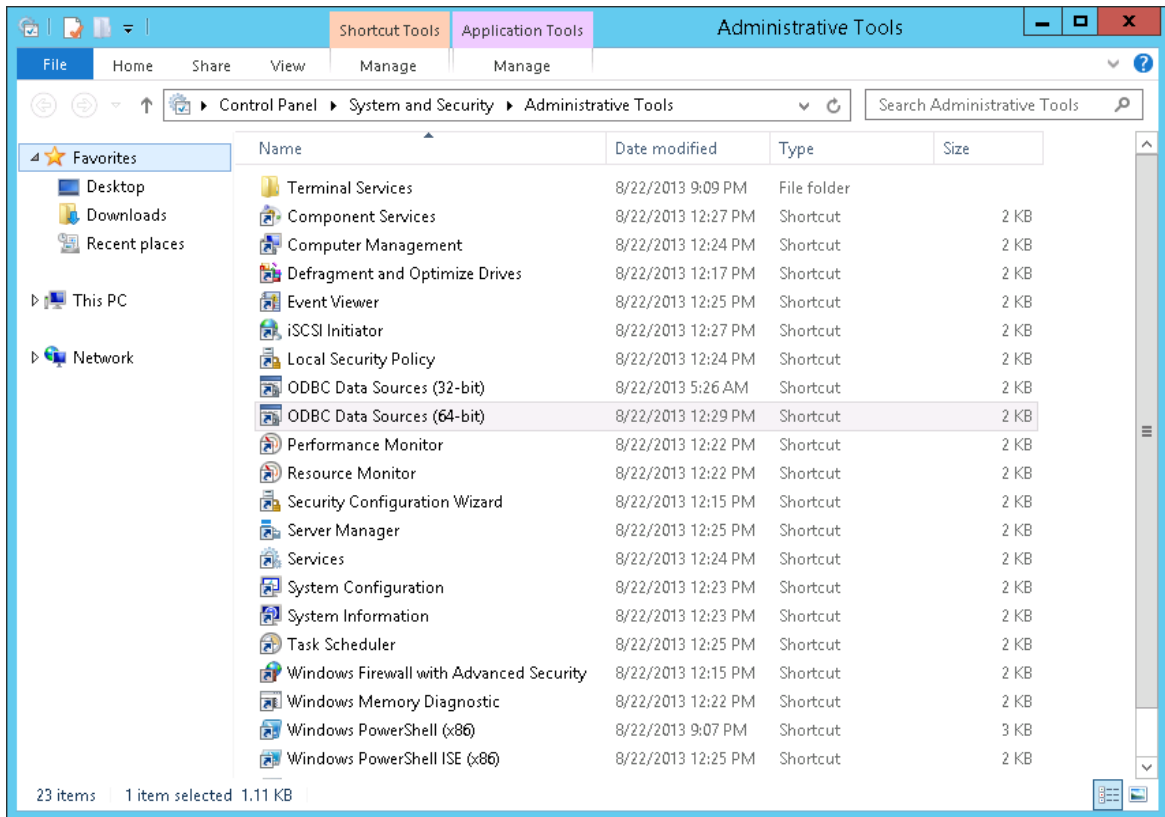
You must configure DSN only if OBR is installed on Windows. If OBR is installed on Linux then the installer automatically handles the DSN configuration and connection to Vertica database.

To configure DSN to connect to Vertica database, follow these steps on OBR system installed on Windows:

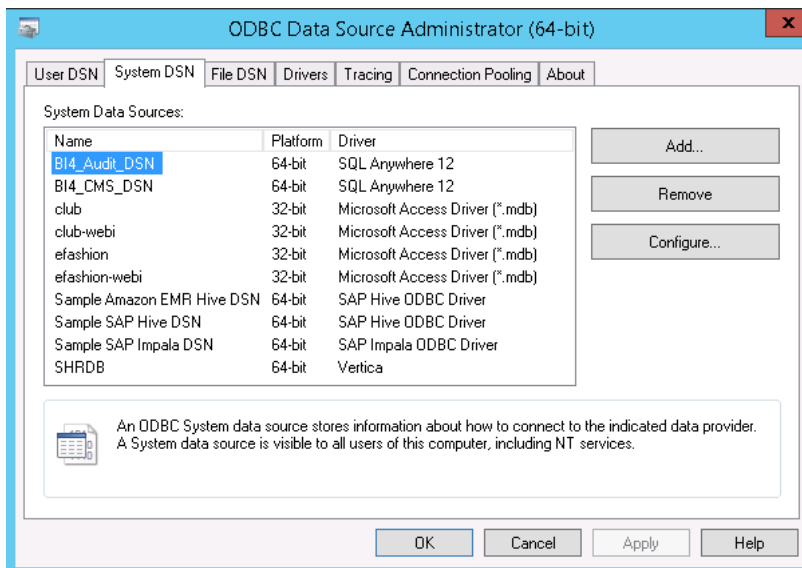
1. Log on to OBR system installed on Windows.
2. Click **Start > Control Panel** and then click **System and Security**. The **System and Security** windows is displayed.



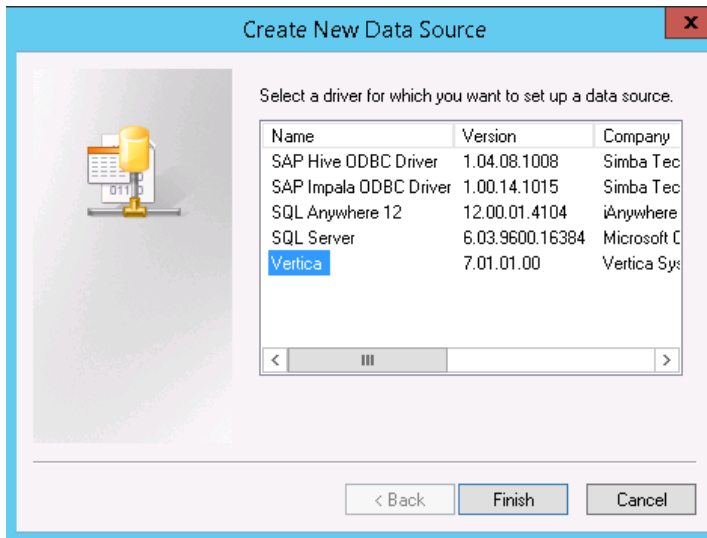
3. Click **Administrative Tools**. The Administrative Tools window is displayed.



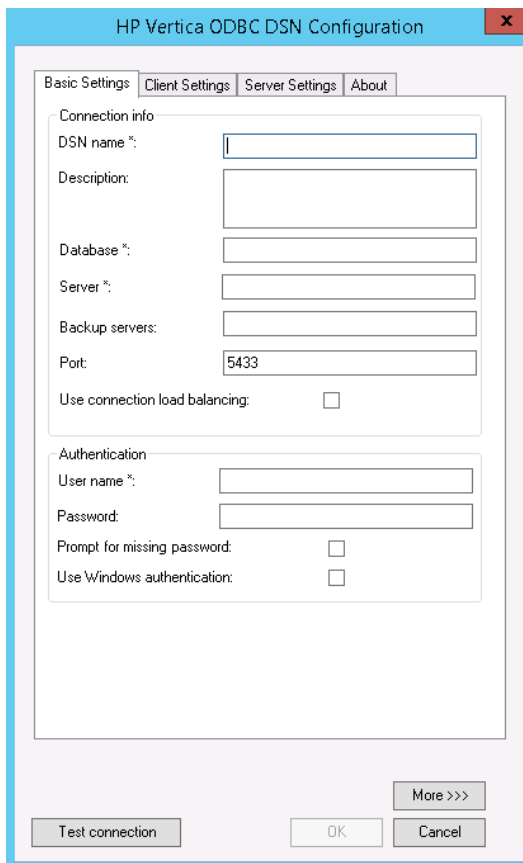
4. Double-click **ODBC Data Sources (64-bit)**. The **ODBC Data Source Administrator (64-bit)** window is displayed.



5. Click **System DNS** tab and then click **Add**. The **Create New Data Source** windows is displayed.



6. Click **Vertica** and then click **Finish** or double-click **Vertica**. The **Vertica ODBC DSN Configuration** window is displayed.



7. Enter the **DSN name as SHRDB**.

8. Enter the **Database** as **pmdb**.
9. Enter the database host name in **Server**.
10. Enter OBR schema user name in **User name**.
11. Enter OBR schema password in **Password**.
12. Click **Test connection** and then click **OK**.

The DSN connection is established between OBR system and Vertica database.

Note: You can configure DSN connection over TLS. For steps to configure, see "[Configure SSL for ODBC clients](#)" on page 221.

Chapter 14: Discover Profile or Operations Database

OBR supports the configuration of data collection from multiple Profile databases that are deployed in your BSM/OMi environment.

Note: Perform the following steps only if the topology source is RTSM.

Note: In case of OMi 10 (and later versions) perform this task for Operations Database support and then configure the database. To configure the Operations Database, see "[Configuring the OMi Data Source](#)" on page 140.

If management database and profile database are on the same system as the BSM system (local database), clicking **Discover Database** in the Administration Console 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 in the Administration Console. You have to manually provide configuration details with user name and password for each profile database.

After you configure management database with **Database in Oracle RAC** option selected and the **Test Connection** is successful, clicking **Discovery Database** in the Administration Console does not automatically discover the corresponding Profile database(s). You have to manually configure the profile database using the **Profile Database** tab. You have to manually provide configuration details with user name and password for each profile database.

To ensure that OBR identifies and displays all the existing Profile databases in the Administration Console, follow these steps:

Task 1: Start the HPE_PMDB_Platform_Administrator service on the OBR system

If the status of HPE_PMDB_Platform_Administrator service is stopped, run the following command:

On Windows:

1. Click **Start > Run**. The Run dialog box is displayed.
2. Enter **service.msc** in **Open**. The **Services** windows is displayed.
3. On the right pane, right-click on the **HPE_PMDB_Platform_Administrator** service and then click **Start**.
4. Close the Services window.

On Linux:

1. Type the following command at the command prompt:

```
cd /etc/init.d
```

On RHEL 6.x/SUSE Linux Enterprise Server 11: `service HPE_PMDB_Platform_Administration start`

On RHEL 7.x: `systemctl start HPE_PMDB_Platform_Administration.service`

Task 2: Copy the configuration files from the BSM/OMi host system to OBR system

1. Log on to the BSM/OMi host system through remote access.

Note: If your BSM setup is distributed, you can access through the gateway server as well as the data processing server. OBR recommends that you use the gateway server.

2. Browse to the %topaz_home%\Conf folder.
3. Copy the following files from the %topaz_home%\Conf folder to %PMDB_HOME%\config folder on the OBR system:
 - a. encryption.properties
 - b. seed.properties

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.

Note: You must ensure to create the sub folders with same name as management database (FQDN) in upper case.

Note: If you are configuring the Management/Profile database based on Oracle RAC, you need to copy the file tnsnames.ora to the %PMDB_HOME%\config (**On Windows**) and %PMDB_HOME%/config (**On Linux**) folder on the OBR system.

If you are configuring the collection against a remote collector system then ensure to copy the tnsnames.ora file to the config folder on that remote collector system acting as polling station.

Task 3: Restart the HPE_PMDB_Platform_Administrator service on the OBR system**On Windows:**

1. Click **Start > Run**. The Run dialog box is displayed.
2. Enter **service.msc** in **Open**. The **Services** windows is displayed.
3. On the right pane, right-click on the **HPE_PMDB_Platform_Administrator** service and then click **Restart**.
4. Close the Services window.

On Linux:

1. Type the following command at the command prompt:

```
cd /etc/init.d
```

On RHEL 6.x/SUSE Linux Enterprise Server 11: `service HPE_PMDB_Platform_Administration restart`

On RHEL 7.x: `systemctl restart HPE_PMDB_Platform_Administration.service`

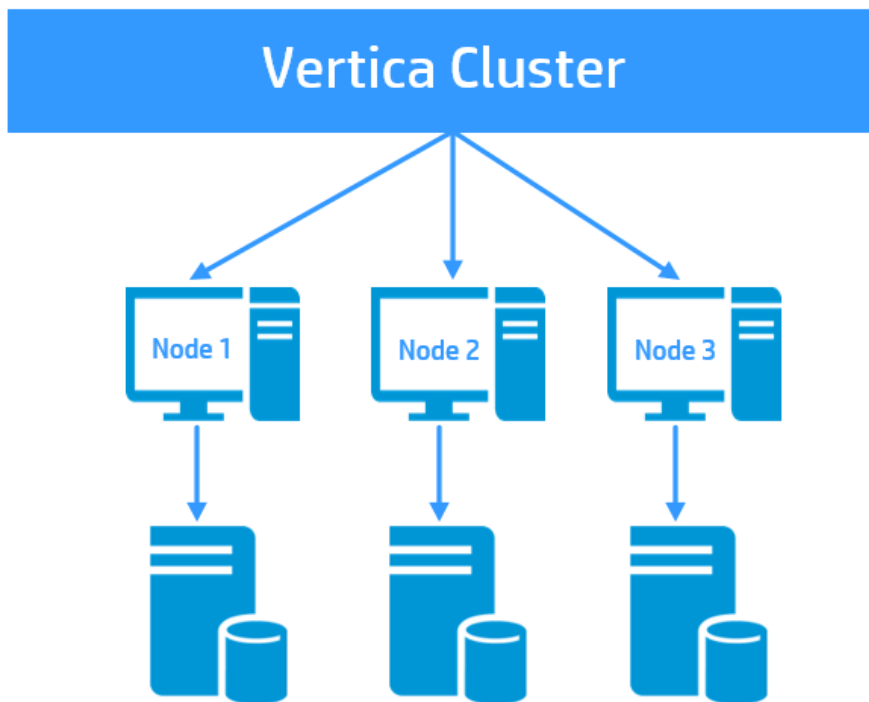
Caution: Ensure to take a backup of the OBR database in case you need to restore it later. If you fail to take a data back up, you risk losing it permanently. For more information, see the "[Part IV: Database Backup and Recovery](#)" on page 227.

Chapter 15: Configuring OBR to Setup Vertica Cluster

Vertica is, cluster based, analytic database management system. The architecture of Vertica is designed to distribute physical storage and allows parallel query execution on a large collection of data. Vertica manages large, fast-growing volumes of data and provides fast query performance for data warehouses and other query-intensive applications.

Cluster in Vertica is physical and linearly scalable, that means you can have minimum of three nodes in the Vertica Cluster. A cluster is a collection of nodes and a node is the host that runs an instance of Vertica. Every node has its own computing power, CPU, RAM and storage. A cluster of nodes, when active, can perform distributed data storage and SQL statement execution through administrative, interactive, and programmatic user interfaces.

The following image shows Vertica cluster with three nodes:



For more information on Vertica cluster, see *Vertica Analytic Database Concepts Guide*.

Prerequisites for the nodes of Cluster

The following are the prerequisites for all the nodes of a cluster:

- Ensure that the system configuration of all the nodes of a cluster are identical.
- All the nodes share the same network.
- Ensure that Date & Time is synchronized on all the nodes of a cluster.

Set up Vertica Cluster and Scale Out

After post install configuration or content pack installation, to set up Vertica cluster, follow the corresponding sections in *Operations Bridge Reporter High Availability Guide*:

1. *Stopping the OBR services*
2. *Setting up Vertica Cluster*

Note: In this section, Skip step 1 on creating the Vertica database, and proceed from step 2.

3. *Configuring Vertica Cluster*
4. *Configuring connectivity changes for Vertica Cluster*

For more information on scale out, see *Operations Bridge Reporter High Availability Guide*.

Chapter 16: Configuring OBR for External Vertica

OBR supports configuring Vertica database in a common environment with other HPE products. In your IT environment if you already have products that use Vertica as its database then you can configure OBR to the same Vertica database. Else, if you already have Vertica installed with OBR then you can configure the same Vertica database for other products that also use Vertica as its database with their own specific schema.

Note: You must ensure to install OBR before you perform steps to configure OBR for external Vertica.

For New OBR Installation

If you are installing OBR for the first time then the steps to configure external Vertica can be based on the following scenarios:

- [Scenario 1: OBR is the only product with Vertica as database.](#)
- [Scenario 2: OBR is installed before the other products are installed.](#)
- [Scenario 3: OBR is installed after the other product installation.](#)
- [Scenario 4: OBR is installed after the other product installation and then again other product is installed.](#)

For Existing OBR Installation

If you have already installed OBR, post install configuration is also complete and you want to configure OBR for external vertica, see "[Configuring OBR for External Vertica after Post Installation](#)" on [page 192](#).

For New OBR Installation

Scenario 1: OBR is the Only Product

If OBR is the only product using Vertica database then to configure OBR to support external Vertica, follow these steps:

1. **Typical scenario:** If OBR is installed in typical scenario, follow these steps:
 - a. During post-installation configuration, in step 2 of Initial Setup, creating the Vertica database, enter the OBR schema user name.
 - b. Enter the password for OBR schema user.
 - c. Confirm the password for OBR schema user.

The OBR schema user and the password is enabled and `config.prp` is updated with OBR schema user credentials.

For more information, see [Creating Database Schema for Co-located Vertica](#).

2. **Distributed scenario:** If OBR is installed in a distributed scenario, follow these steps:
 - a. Open the command prompt and run the following command on a system where Vertica is installed:

```
$PMDB_HOME/bin/CreateVerticaDatabase.sh <Vertica DBA User Name> <DBA User Password> <Database File Location> <Catalog File Location> <Vertica Database User name > <Vertica Database User name Password> <Database Name> tlon/tloff <generatedcertificates>/<providedCertificates <server certificate file location><server key file location>>
```

where, *<Vertica DBA User Name>* is the Vertica database user name with DBA privilege to log on to Vertica database

<DBA User Password> is the Vertica database password to log on to the Vertica database

<Database File Location> is the path to create the Vertica database

<Catalog File Location> is the path to create the Vertica catalog

<Vertica Database User name> is the Vertica Database user name

<Vertica Database User name Password> is the password for Vertica Database user name

<Database Name> is the name of Vertica database. This is an optional parameter. By default, the name of the Vertica database is PMDB.

tlson/tlsoff is the option for Vertica with or without TLS.

generatedcertificates is the option for Vertica with TLS and Certificate generated by OBR. When *generatedcertificates* is selected, the *server.crt* and *server.key* file will be created in *{PMDb_HOME}/config* folder on the database host.

providedcertificates is the option for Vertica with TLS and self provided certificate. Type the complete path to the *<server certificate file location>* certificate path and *<server key file location>* key location.

<server certificate file location> is the path of the self provided certificate file. Type the complete path of the file if you have opted for *providedcertificates*.

<server key file location> is the path of the self provided certificate key file. Type the complete path of the file if you have opted for *providedcertificates*.

For more information, see [Creating Database Schema for Remote Vertica](#).

- b. During post-installation configuration, in step 2 of the Initial Setup, provide the OBR schema user name and password details.

The OBR schema user and the password is enabled and *config.prp* is updated with OBR schema user credentials.

Scenario 2: OBR is Installed Before Other Product

If you have installed OBR before installing other products then to configure external Vertica, follow these steps:

1. Install OBR and configure external Vertica as per steps given in "[Scenario 1: OBR is the Only Product](#)" on the previous page.
2. Install other products.
3. Check the number of connections for OBR and update the connections and LockTimeout settings in OBR system accordingly. By default, the number of connections for OBR is 150. So, update the connection as 150 + other products connections in the OBR system.

You can set the proper value of connections and lock timeout in `config.prp` using the following commands:

- a. `SET_CONFIG_PARAMETER('MaxClientSessions',150)`
 - b. `SET_CONFIG_PARAMETER('LockTimeout',21600)`
 - c. `SET_LOAD_BALANCE_POLICY('ROUNDROBIN')`
4. OBR is already installed and to change the schema from public to OBR, follow steps given in section ["Configuring OBR for External Vertica after Post Installation" on page 192](#).

Scenario 3: OBR is Installed After Other Products

If you have installed OBR after installing other products then to configure external Vertica, follow these steps:

On Other Product(s)

1. Install other product(s) with Vertica as database.
2. Log in as DBA user and run the following commands:
 - a. `CREATE USER <OBR User> IDENTIFIED BY <'OBR User Password'>;`
where, <OBR User> is the user of OBR system
<'OBR User Password'> is the password for OBR user
 - b. `CREATE ROLE OBR_ROLE;`
 - c. `GRANT OBR_ROLE TO <OBR User> WITH ADMIN OPTION;`
where, <OBR User> is the user of OBR system
 - d. `GRANT CREATE ON DATABASE <Database name> TO OBR_ROLE;`
where, <Database name> is the name of Vertica database
 - e. `GRANT SELECT ON ALL TABLES IN SCHEMA PUBLIC TO <OBR User>;`
where, <OBR User> is the user of OBR system
 - f. `ALTER USER <OBR User> DEFAULT ROLE OBR_ROLE;`
where, <OBR User> is the user of OBR system
 - g. `GRANT PSEUDOSUPERUSER TO OBR_ROLE;`

You have to check the maximum client sessions (MaxClientSessions) and lock timeout (LockTimeout) of other products and then update these parameters accordingly in the `config.prp` in OBR system.

Database Schema Creation for OBR System

1. Log on to OBR system as OBR user.
2. Open the command prompt and run the following commands:
 - a. `CREATE SCHEMA OBR;`
 - b. `ALTER USER <OBR User> SEARCH_PATH OBR,PUBLIC;`
where, `<OBR User>` is the user of OBR system
 - c. Open the `config.prp` in the OBR system from `/opt/HP/BSM/PMDB/data/` and update the value of `database.dbname` to the running DB name. For example, `database.dbname=opsadb`.

You can now continue with the post install configuration of OBR system using the same OBR user.

Scenario 4: OBR is installed after the other product installation and then again other product is installed

If you install other products first, then OBR and later again install other products that use Vertica as its database, you have to follow steps of both scenario 3 and scenario 2 to configure OBR for external Vertica.

To configure OBR for external Vertica, follow these steps:

1. Perform the steps given in scenario 3, see ["Scenario 3: OBR is Installed After Other Products" on the previous page](#).
2. Perform the steps given in scenario 2, see ["Scenario 2: OBR is Installed Before Other Product" on page 189](#).

For Existing OBR Installation

If you have already installed OBR and post install configuration is complete then in Vertica, PMDB database is created with public schema. To Configure the existing OBR for external Vertica, you have to move the public schema to OBR schema.

Configuring OBR for External Vertica after Post Installation

To configure OBR for external Vertica, follow these steps:

1. Install OBR.
2. Go to %PMDB_HOME%\bin folder (**On Windows**) and \$PMDB_HOME/bin folder (**On Linux**).
3. Open the command prompt and run the following script:

```
SchemaChange.sh <Vertica Database User Name> <Vertica Database User Name  
Password>
```

where, <Vertica Database User Name> is the user name for Vertica database

<Vertica Database User Name Password> is the password for Vertica database user

The tables, sequences and views from public schema are moved to OBR schema.

Chapter 17: Configuring Logon Banner for OBR

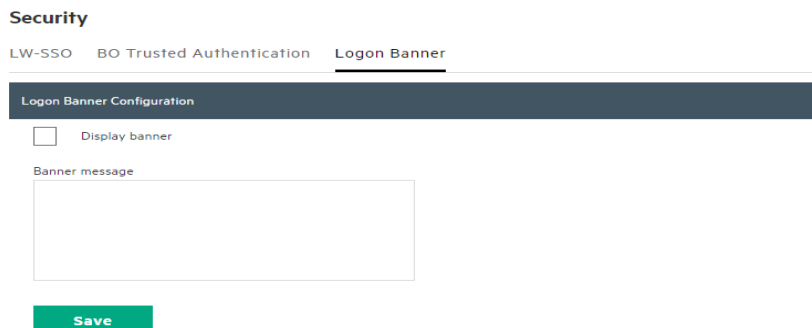
You can configure logon banner after post install configuration for Administration Console, SAP BusinessObjects and CMC in Operations Bridge Reporter. You can configure the text that is displayed on logon banner. The text that is displayed is the first screen and warns the users against unauthorized entry. Click Ok on this screen and the usual login screen is displayed.

Enabling the Logon Banner

To enable the logon banner, follow these steps:

1. Log on to Administration Console and click **Additional Configurations > Security**.

The **Security** page is displayed.



The screenshot shows the 'Security' page with three tabs: 'LW-SSO', 'BO Trusted Authentication', and 'Logon Banner'. The 'Logon Banner' tab is selected. Below the tabs is a dark header bar labeled 'Logon Banner Configuration'. Underneath, there is a checkbox labeled 'Display banner' which is currently unchecked. Below the checkbox is a text area labeled 'Banner message' which is empty. At the bottom of the form is a green 'Save' button.

2. Click **Logon Banner** tab and select the **Display banner** check box.

Security

LW-SSO BO Trusted Authentication Logon Banner

Logon Banner Configuration

Display banner

Banner message

Welcome to Operations Bridge Reporter
Administration Console

Save

In the **Banner Message** text box, a default warning message is provided. If you want to change the default message, click in the text box and enter your own logon banner message that must appear as the first screen to warn the user. You can also use HTML tags for formatting the message.

3. Click **Save**. A status message is displayed.
4. Click **Logout** to log out from Administration Console.
5. Launch the Administration Console in a web browser using the following URL:
https://<OBR_Server_FQDN>:21412/OBRApp
6. The logon banner warning message is displayed. Click **OK** to login again.

Welcome to Operations Bridge Reporter Administration Console.

OK

7. Enter the username and password to log on and proceed with Administration Console tasks.

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 remote SAP BusinessObject scenario, after you enable the logon banner in Administration Console, copy the {PMDB_HOME}/data/config.prp manually from OBR system to {PMDB_HOME}/data/config.prp in remote SAP BusinessObjects system.

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. Log on to Administration Console and click **Additional Configurations > Security**.

The **Security** page is displayed.

2. Click **Logon Banner** tab, uncheck the **Display banner** check box and click **Save**. A status message is displayed.

The screenshot shows the 'Security' page with the 'Logon Banner' tab selected. The 'Logon Banner Configuration' section contains a checkbox labeled 'Display banner' which is currently unchecked. Below this is a text area for 'Banner message' which is empty. At the bottom of the configuration area is a green 'Save' button.

3. Click **Logout** to log out from Administration Console.
4. Log on to the Administration Console from the url `https://<OBR_Server_FQDN>:21412/OBRApp`. The log on screen is displayed.

In typical scenario, after you disable the logon banner in Administration Console and launch the SAP BusinessObjects or CMC from the web browser, the respective SAP BusinessObjects or CMC log on screen is displayed. Enter the user credentials to log on and proceed with the tasks.

In remote SAP BusinessObject scenario, after you disable the logon banner in Administration Console, again copy the `{PMDB_HOME}/data/config.prp` manually from OBR system to `{PMDB_HOME}/data/config.prp` in remote SAP BusinessObjects system.

Launch the SAP BusinessObjects or CMC from the web browser, the respective SAP BusinessObjects or CMC log on screen is displayed. Enter the user credentials to log on and proceed with the tasks.

Chapter 18: Configuring FIPS for OBR

This section provides information on how to configure OBR to be compliant with Federal Information Processing Standards (FIPS) 140-2.

FIPS 140-2 is a standard for security requirements for cryptographic modules defined by the National Institute of Standards and Technology (NIST). To view the publication for this standard, go to: <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>.

OBR in FIPS Mode

When you configure OBR to run in FIPS mode, the following components are also configured to operate in FIPS mode:

- Tomcat server
- Java Runtime Environment
- SAP BusinessObjects
- Vertica

OBR automatically uses FIPS-compliant cryptographic methods for the following:

- HTTPS communication (if configured) between browser and Administration Console/SAP BusinessObjects.
- TLS communication (if configured) between Vertica and OBR server /SAP BusinessObjects.
- HTTPS communication (if configured) between OBR server and OBR collector.
- HTTPS communication (if configured) between OBR collector and agent.
- TLS communication (if configured) between OBR collector and BSM/OMi Oracle database.
- TLS communication (if configured) between OBR collector and BSM/OMi RtSM.

Considerations When Running OBR in FIPS Mode

When run in FIPS mode, OBR uses the following RSA BSAFE Crypto module FIPS certified algorithms for encryption and storage of OBR sensitive data:

- Supported Encryption Keystore format: PKCS 12
- Supported asymmetric algorithm for OBR Encryption Keystore: RSA (recommended size 2048)
- Supported symmetric key algorithm used by OBR: AES (128-bit (default), 192-bit, and 256-bit key sizes)
- Supported Random Number Generation algorithm used by OBR for encryption is HMAC DRBG (128-bit)

- **Integrations:**

Typically, FIPS is not enabled for a single application only. Instead, all integrated systems must be FIPS compliant for the entire deployment to be FIPS-compliant. For OBR, this means that all clients, data sources and databases must be configured for FIPS compliance.

Configure OBR for FIPS 140-2 Compliance

Prerequisites:

You have to ensure that the following HTTPS and TLS configuration are enabled:

1. HTTPS communication is configured between browser and Administration Console/SAP BusinessObjects.
2. HTTPS communication is configured between OBR server and OBR collector.
3. HTTPS communication is configured between OBR collector and agent. ["Configuring the Operations Agent for Data Collection in Secure Mode" on page 146.](#)
4. TLS communication is configured between Vertica and OBR server /SAP BusinessObjects. See ["Configuring TLS for Vertica" on page 209.](#)
5. TLS communication is configured between OBR collector and BSM/OMi Oracle database. See

["Data Source Configuration" on page 117.](#)

6. TLS communication is configured between OBR collector and BSM/OMi RtSM. See ["Data Source Configuration" on page 117.](#)

To enable FIPS, follow these steps:

1. Task 1: Enable FIPS

On SAP BusinessObject System

If you are enabling FIPS on the system where SAP BusinessObject is installed, perform the following steps to enable SSL handshake before you enable FIPS:

- a. Go to `<BO install Directory>:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\dataAccess\connectionServer\` **(On Windows)** and `/opt/HP/BSM/BOE4/sap_bobj/enterprise_xi40/dataAccess/connectionServer/` **(On Linux)** and open the `cs.cfg` file.
- b. Enable TLS for Vertica. For steps, see [Configure TLS for Vertica](#).
- c. Import the server CA certificate from Vertica server to OBR server truststore location `{PMDB_HOME}/keystore` using the following command:

```
keytool -import -file <serverca.crt> -alias importcert -keystore <File name>  
storepass <Password>
```

where, `serverca.crt` is the CA certificate file

`<File name>` is the truststore path on OBR server. For Example: The default trust store path `{PMDB_HOME}/keystore` created by OBR may be used.

`<Password>` is the Password to the truststore. For Example: `shradmin`

- d. Locate the `<JavaVM>` and add the following parameters in `cs.cfg` file:

```
<Option>-Djavax.net.ssl.trustStore=<PATH_TO_TrustStore></Option>
```

```
<Option>-Djavax.net.ssl.trustStorePassword=<Password></Option>
```

The following is an example of the sample `cs.cfg` after adding the parameters:

```
<JavaVM>
```

```
<!-- The default JVM configuration can be overridden here -->
```

```
<!-- Use an absolute path for the JVM -->
```

```
<!--
```

```
<LibraryName JNIVersion="JNI_VERSION_1_4">ABSOLUTE_
PATH/jvm.dll</LibraryName>

-->

<Options>
<Option Processor="64">-Xmx2048m</Option>
<Option>-Xrs</Option>
<Option>-Djavax.net.ssl.trustStore=<PATH_TO_TrustStore></Option>
<Option>-Djavax.net.ssl.trustStorePassword=<Password></Option>
</Options>
</JavaVM>
```

<PATH_TO_TrustStore> is the truststore path on OBR server. For Example: The default trust store path {PMDB_HOME}/keystore created by OBR may be used.

<Password> is the Password to the truststore. For Example: shradmin

Enabling FIPS on any OBR component

To enable FIPS, run the following commands on the command prompt:

- a. cd {PMDB_HOME}/bin
- b. perl FIPS.pl enable

The following status message is displayed.

```
Enabling FIPS, Please wait...
File copy started.
Required files copied.
FIPS enabled.
```

2. Task 2: Create encryption keystore in the PKCS 12 format and import the certificates

- a. cd {PMDB_HOME}/keystore
- b. Run the following command to create the keystore:

```
keytool -genkey -alias SHR -keyalg RSA -keysize 2048 -keypass <Password> -
storepass <Password> -keystore SHR_CERT_PKCS.p12 -storetype pkcs12
```

where, *<Password>* is the password. For example: shradmin

- c. Copy all the certificates (OMi CA certificate, Oracle server certificate, SiS certificate) to the FIPS enabled OBR server to a common location.
- d. Run the following command to import the certificates to truststore:


```
keytool -importcert -trustcacerts -keystore {PMDB_HOME}/keystore/SHR_CERT_
PKCS.p12 -file <individual certificate path> -alias <certificate alias> -
storepass <Password>
```

where, <Password> is the password. For example: shradmin

3. Task 3: Stop the HPE_PMDB_Platform_Administrator service and edit server.xml

Note: You have to perform these steps on the system where OBR is installed.

- a. To stop the HPE_PMDB_Platform_Administrator service, follow these steps:

On Windows:

- i. Click **Start > Run**. The Run dialog box opens.
- ii. Type `services.msc` in the Open field, and then press **Enter**. The Services window opens.
- iii. On the right pane, right-click `HPE_PMDB_Platform_Administrator`, and then click **Stop**.

On Linux:

- i. Go to `/etc/init.d` and run the following command:
- ii. **On RHEL 6.x/SUSE Linux Enterprise Server 11:** `service HPE_PMDB_Platform_Administration stop`
On RHEL 7.x: `systemctl stop HPE_PMDB_Platform_Administration.service`

- b. To edit the `server.xml`, follow these steps:

- i. Go to `%PMDB_HOME%\adminserver\conf` (**On Windows**) or `$PMDB_HOME/adminserver/conf` (**On Linux**) and open the `server.xml` in an editor and locate the `Connector port="21412"`
- ii. Update the `keystoreFile`, `keystorePass`, and `keystoreType` parameter values as per the newly created encryption keystore in [Task 2](#).
- iii. Delete the `keyAlias` parameter.

After editing `server.xml`, the sample code snippet for `Connector port` should look similar to the following:

```
<Connector port="21412"
protocol="org.apache.coyote.http11.Http11Protocol"
maxHttpHeaderSize="8192" connectionTimeout="20000"

maxThreads="150" minSpareThreads="25" maxSpareThreads="75"

enableLookups="false" disableUploadTimeout="true"
```

```

acceptCount="100" scheme="https" secure="true"

clientAuth="false"
sslEnabledProtocols="SSLv2Hello,TLSv1,TLSv1.1,TLSv1.2"
SSLEnabled="true"

keystoreFile="../keystore/SHR_CERT_PKCS.p12" keystorePass="shradmin"
keystoreType="pkcs12" xpoweredBy="false" server="SHR"/>

```

- iv. Save the `server.xml` and exit the editor.
- v. Start the `HPE_PMDB_Platform_Administrator` service, follow these steps:

On Windows:

- A. Click **Start > Run**. The Run dialog box opens.
- B. Type `services.msc` in the Open field, and then press **Enter**. The Services window opens.
- C. On the right pane, right-click `HPE_PMDB_Platform_Administrator`, and then click **Start**.

On Linux:

- A. Go to `/etc/init.d`.
- B. Run the following command:

On RHEL 6.x/SUSE Linux Enterprise Server 11: `service HPE_PMDB_Platform_Administration start`

On RHEL 7.x: `systemctl start HPE_PMDB_Platform_Administration.service`

4. Task 4: Stop the SAP BusinessObjects WebServer service and edit `server.xml`

Note: You have to perform these steps on the system where SAP BusinessObjects is installed.

- a. To stop the SAP BusinessObjects WebServer service, follow these steps:

On Windows:

- i. Log on to the host system as administrator.
- ii. Click **Start > Run**. The Run dialog box opens.
- iii. Type `services.msc` in the **Open** field, and then press **Enter**. The Services window opens.

- iv. Right-click the **Business Object WebServer** service and select **Stop** to stop the service.

On Linux:

- i. Go to \$PMDB_HOME/BOWebServer/bin
- ii. Run the following command:

```
./shutdown.sh
```

- b. To edit the server.xml, follow these steps:

- i. Go to %PMDB_HOME%\BOWebServer\conf (**On Windows**) or \$PMDB_HOME/BOWebServer/conf (**On Linux**) and open the server.xml in an editor and locate the Connector port="8443"
- ii. Update the keystoreFile, keystorePass, and keystoreType parameter values as per the newly created encryption keystore in [Task 2](#).
- iii. Delete the keyAlias parameter.

After editing server.xml, the sample code snippet for Connector port should look similar to the following:

```
<Connector port="8443"
protocol="org.apache.coyote.http11.Http11Protocol"
maxHttpHeaderSize="8192" connectionTimeout="20000"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100" scheme="https" secure="true"
clientAuth="false"
sslEnabledProtocols="SSLv2Hello,TLSv1,TLSv1.1,TLSv1.2"
SSLEnabled="true"
keystoreFile="../keystore/SHR_CERT_PKCS.p12" keystorePass="shradmin"
keystoreType="pkcs12" xpoweredBy="false" server="SHR"/>
```

- iv. Save the server.xml and exit the editor.

- c. Start the SAP BusinessObjects WebServer service, , follow these steps:

On Windows:

- i. Log on to the host system as administrator.
- ii. Click **Start > Run**. The Run dialog box opens.

- iii. Type `services.msc` in the **Open** field, and then press **Enter**. The Services window opens.
- iv. Right-click the **Business Object WebServer** service and select **Start**.

On Linux:

- i. Go to `$PMDB_HOME/BOWebServer/bin`
- ii. Run the following command:

```
./start.sh
```

5. Task 5: Stop the HPE_PMDB_Platform_Collection service and edit Collection start and stop scripts

To stop the HPE_PMDB_Platform_Collection service, follow these steps:

On Windows:

- a. Click **Start > Run**. The Run dialog box opens.
- b. Type `services.msc` in the Open field, and then press **Enter**. The Services window opens.
- c. On the right pane, right-click HPE_PMDB_Platform_Collection, and then click **Stop**.

On Linux:

- a. Go to `/etc/init.d` and run the following command:
- b. **On RHEL 6.x/SUSE Linux Enterprise Server 11:** `service HPE_PMDB_Platform_Collection stop`

On RHEL 7.x: `systemctl stop HPE_PMDB_Platform_Collection.service`

To add the path in collection service, follow these steps:

- a. **On Windows**

Add the following argument to `CollectionServiceCreation.bat` file:

```
-Djavax.net.ssl.trustStore=%PMDB_HOME%\keystore\SHR_CERT_PKCS.p12 -
Djavax.net.ssl.trustStorePassword=<Password> -
Djava.security.manager=com.hp.opr.foundation.securitymanager.DenyDataDirectS
ecurityProviderInsertion
```

where, `<Password>` is the password. For example: `shradmin`

- b. **On Linux**

- i. In `$PMDB_HOME/bin/hpbsm_pmdb_collector_start.sh` files, locate `jvm_args` and add the following argument at the last line:

```
-Djavax.net.ssl.trustStore=$PMDB_HOME/keystore/SHR_CERT_PKCS.p12 -
Djavax.net.ssl.trustStorePassword=<Password> -
Djava.security.manager=com.hp.opr.foundation.securitymanager.DenyDataDi
rectSecurityProviderInsertion
```

where, <Password> is the password. For example: shradmin

```
PVM_ARGS="-Xmx4096m -XX:MetaspaceSize=128m -XX:MaxMetaspaceSize=256m -Dbsm.home=$PMDBDIR -Dpmdb.home=$PMDBDIR -Dfile.encoding=UTF-8 -Dcom.sun.management.jmxremote -D
com.sun.management.jmxremote.port=21409 -Dcom.sun.management.jmxremote.authenticate=false -Dcom.sun.management.jmxremote.local.only=true -Dcom.hp.ov.installDir=$OVDIR
-Dcom.hp.ov.DataDir=/var/sovdDir/ -Dcom.sun.management.jmxremote.ssl=false -XX:+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=$PMDBDIR/log/collection.hprof -Djavax.net
ssl.trustStore=/opt/HP/BSM/PMDB/keystore/SHR_CERT_PKCS.p12 -Djavax.net.ssl.trustStorePassword=shradmin"
```

- ii. In \$PMDB_HOME/bin/hpbsm_pmdb_collector_stop.sh, locate nohup and add the following argument:

```
-Djavax.net.ssl.trustStore=$PMDB_HOME/keystore/SHR_CERT_PKCS.p12 -
Djavax.net.ssl.trustStorePassword=<Password> -
Djava.security.manager=com.hp.opr.foundation.securitymanager.DenyDataDi
rectSecurityProviderInsertion
```

where, <Password> is the password. For example: shradmin

```
nohup $JAVA_HOME/JRE64/bin/java -Djavax.net.ssl.trustStore=/opt/HP/BSM/PMDB/keystore/SHR_CERT_PKCS.p12 -Djavax.net.ssl.trustStorePassword=shradmin
```

- c. Go to the location {PMDB_HOME}/data, open the config.prp file and add the following :

```
ucmdb.protocol=https
shr.truststorepassword=<Password>
```

where, <Password> is the password. For example: shr.truststorepassword=shradmin

(On Windows) shr.truststorepath=%PMDB_HOME%\keystore\SHR_CERT_PKCS.p12

(On Linux) shr.truststorepath=/opt/HP/BSM/PMDB/keystore/SHR_CERT_PKCS.p12

```
shr.truststoretype=PKCS12
```

- d. Start the HPE_PMDB_Platform_Collection service, follow these steps:

On Windows:

- i. Click **Start > Run**. The Run dialog box opens.
- ii. Type services.msc in the Open field, and then press **Enter**. The Services window opens.
- iii. On the right pane, right-click HPE_PMDB_Platform_Collection, and then click **Start**.

On Linux:

- i. Go to /etc/init.d and run the following command:
- ii. **On RHEL 6.x/SUSE Linux Enterprise Server 11:** service HPE_PMDB_Platform_

Collection start

On RHEL 7.x: `systemctl start HPE_PMDB_Platform_Collection.service`

You should be able to log on to Administration Console and SAP BusinessObjects without any errors.

Chapter 19: Change the Vertica Data Storage Location

You have to change the vertica data storage location, if the current data storage disk is full.

To change the data storage location, follow these steps:

1. Log on as the Vertica DBA user. Run the following command to get the current storage location:

```
/opt/vertica/bin/vsql -c "select storage_path from disk_storage where storage_usage='DATA,TEMP';" -U <Vertica DBA Username> -w <Vertica DBA Password>
```

2. To create a new location, run the following command from the command prompt as root user:

```
mkdir -p <storage path>
```

where, *<storage path>* is the complete path of the new storage location. The format of the new location must be similar to the previous location.

For Example: Previous location - /disk1/pmdb/pmdb_node001_data

New location - /disk2/pmdb/pmdb_node001_data

3. Run the following command to change the owner and group to Vertica user for the newly created storage disk.

```
chown -R <Vertica DBA Username>:<Vertica DBA group> <Location of new disk mounted>
```

where, *<Vertica DBA User>* is the vertica user name with DBA privilege to log on to Vertica database.

<Vertica group> is the group vertica DBA user belongs to.

Note: The Vertica group is same as Vertica DBA user name.

<Location of new disk mounted> is the location where new disk is mounted.

For Example, the location of new disk mentioned in the example of step 2 is /disk2.

4. Log on as the Vertica DBA user. Run the following command to create the new disk location:

```
/opt/vertica/bin/vsql -c "CREATE LOCATION '<storage path>';" -U <Vertica DBA Username> -w <Vertica DBA Password>
```

where, *<storage path>* is the complete path of the new storage location.

For Example: `/opt/vertica/bin/vsql -c "CREATE LOCATION '/disk2/pmdb/pmdb_node001_data';" -U verticadba -w password`

5. To verify the new disk added, run the following SQL query:

```
/opt/vertica/bin/vsql -c "select * from disk_storage;" -U <Vertica DBA Username> -w <Vertica DBA Password>
```

For more information, refer the following URLs:

https://my.vertica.com/docs/8.0.x/HTML/index.htm#Authoring/SQLReferenceManual/Functions/VerticaFunctions/ADD_LOCATION.htm

<https://my.vertica.com/docs/8.0.x/HTML/index.htm#Authoring/AdministratorsGuide/StorageLocations/AddingStorageLocations.htm>

Chapter 20: Configuring TLS for Vertica

You can configure JDBC or ODBC connections over TLS for Vertica. The following sections help you through the steps to configure TLS for Vertica based on the type of scenario (typical or distributed).

Configure TLS for Vertica in Typical Scenario

On Vertica:

Perform the following steps on the system where Vertica is installed. To enable TLS for Vertica, log on to the vertica system and run the following commands on the command prompt:

1. To create a CA private key and public certificate, follow these steps:
 - a. `openssl genrsa -out servercakey.pem 2048`
 - b. `openssl req -newkey rsa:2048 -x509 -days 3650 -key servercakey.pem -out serverca.crt`

Enter the values for the following prompts:

- i. Country Name (2 letter code) [XX]:
Enter the country code. For example, IN.
- ii. State or Province Name (full name) []:
Enter full name of state. For example, KA.
- iii. Locality Name (eg, city) [Default City]:
Enter name of your city. For example, BLR.
- iv. Organization Name (eg, company) [Default Company Ltd]:
Enter name of your organization or default company name. For example, HPE.
- v. Organizational Unit Name (eg, section) []:
Enter name of the section or organizational unit. For example, HPE.
- vi. Common Name (eg, your name or your server's hostname) []:

Enter your name or server's hostname as common name. For example, test.hpeswlab.net.

vii. Email Address []:

Enter your email address. For example, test123@hpe.com.

2. To create the server private key and certificate, follow these steps:

a. `openssl genrsa -out server.key 2048`

b. `openssl req -new -key server.key -out server_reqout.txt`

Enter the values for the following prompts:

i. Country Name (2 letter code) [XX]:

Enter the country code. For example, IN.

ii. State or Province Name (full name) []:

Enter full name of state. For example, KA.

iii. Locality Name (eg, city) [Default City]:

Enter name of your city. For example, BLR.

iv. Organization Name (eg, company) [Default Company Ltd]:

Enter name of your organization or default company name. For example, HPE.

v. Organizational Unit Name (eg, section) []:

Enter name of the section or organizational unit. For example, HPE.

vi. Common Name (eg, your name or your server's hostname) []:

Enter your name or server's hostname as common name. For example, test.hpeswlab.net.

vii. Email Address []:

Enter your email address. For example, test123@hpe.com.

viii. Please enter the following 'extra' attribute to be sent with your certificate request. A challenge password []:

Enter password.

ix. An optional company name []:

Enter an optional company name. For example, HPE.

3. To sign the server's certificate using the CA private key file and public certificate, run the following

command:

```
openssl x509 -req -in server_reqout.txt -days 3650 -sha1 -CAcreateserial -CA  
serverca.crt -CAkey servercakey.pem -out serverca.crt
```

Note: Run the above command in single line.

4. Run the following command to log on to vsq1:

```
vsq1 -h <Host name> -U <User name> -p <Port> -d <Database Name>
```

where, <Host name> is the host name of the system where Vertica is installed

<User name> is the Vertica user with DBA privileges

<Port> is the port number

<Database Name> is the name of Vertica database

5. Set the Enable SSL flag to 1:

```
SELECT SET_CONFIG_PARAMETER('EnableSSL', '1');
```

6. To set the private key in Vertica using the contents of server.key file, follow these steps:

- a. `SELECT SET_CONFIG_PARAMETER('SSLPrivateKey', '<contents of server.key file>');`

The following is an example of the command with sample content of server.key file:

```
SELECT SET_CONFIG_PARAMETER('SSLPrivateKey', '-----BEGIN RSA PRIVATE KEY-----  
MIICXgIBAAKBgQDtWLT9FGTpsxXc9Yo0n4LbLgy0shp0q8T0hzwRnz31izqeOasT  
KH4CCwXDOGQprcdELdS+Mr3NHGEni8ya+Cs9ZCCQJB+fzSk6Y7j40bBvIIwpV9s  
Na+YmpDnP9BM6qgniW/pn0i871Z+sHUIJHZ386R08cttPqKJLHdpixZy+RwIDAQAB  
AoGBAJk/HGUH5PxL6ELpuxmtIGV6fz0wh4prWcBr6uoJ4oyHIAsHeyD81Re1j7IT  
2ABdNvsbiHBh/NDRkR1ik3I/6FIV3kuZd6DNIiecfY8y7BfMtInw3Whm9gRAkron  
VGbRiSA330e0KTTt6wz2PY+ZVWH492gf33K6PZqXfR4+iG7RAKEA+R0DRnm5crwX  
LQ1ygMhwRn1p2b4LmYYmMosnUkW00ueC5I+dTPTFNVGktb9We3csRIy1RHXUJJU2  
yvT60/F5zwJBAPPoa3phaF3JE0Vy5DZS/r5+DKom14F5MeYsokPbqr2SG+xZOCm9  
cFjM0AneF/zHcW8qVNwb1wQIY6oIuRgEqgkCQQCccTjuwGE7BYkz9N70u2uvCPGh  
mbT1LBbu507DvwSsP1m30e2aN5mn0J7AtrGUBepZ/1eT779TYiqwWJqRbHuHAKEA  
7VyIC8bzcFCUb+ne351TqiYZpX6L5PkDZ3uI5+In4erC00ij0xAgwnqlx+9tE/b  
glVt0+575v7LDtQCX09dEQJAPjhGY/wyzJ8aS7KTF6Lm+8WuM2xD7d9y4NU6Shs2
```

```
tsb+QrM5jYg79AuwdwP4YceZLIp34QB19BSF/E7WAOXEUQ==
-----END RSA PRIVATE KEY-----
');
```

7. To set the certificate in Vertica using the contents of `server.crt` file, follow these steps:

- a. `SELECT SET_CONFIG_PARAMETER('SSLCertificate','<contents of serverca.crt file>');`

The following is an example of the command with sample content of `serverca.crt` file:

```
SELECT SET_CONFIG_PARAMETER('SSLCertificate','-----BEGIN CERTIFICATE-----
MIICmjCCAgoAgAwIBAgIJAMnZqpMfBVTjMA0GCSqGSIb3DQEBBQUAMGYxCzAJBgNV
BAYTAK10MQswCQYDVQQIDAJLQTEMMAoGA1UEBwwDQkxSMQwwCgYDVQQKDANIUEUx
DDAKBgNVBAsMA0hQRTEMMAoGA1UEAwwDT0JSMRIwEAYJKoZIhvcNAQkBFgnjb20w
HhcNMTYwMzI5MDkyMDU1WhcNMjYwMzI3MDkyMDU1WjBmMQswCQYDVQQGEWJTTjEL
MAKGA1UECAwCS0ExDDAKBgNVBACMA0JMUjEMMAoGA1UECgwDSFBFMQwwCgYDVQQQL
DANIUEUxDDAKBgNVBAMMA09CUjESMBAGCSqGSIb3DQEJARYDY29tMIGfMA0GCSqG
SIb3DQEBAQUAA4GNADCBiQKBgQDtWLT9FGTpsXc9Yo0n4LbLgy0shp0q8TOhzwR
nz31izqe0asTKH4CCWDOGQprcdELds+Mr3NHGEni8ya+C9ZCCQJB+fzSk6Y7j4
0bBvIIwPV9sNa+YmpDnP9BM6qgniW/pn0i871Z+sHUIJHZ386R08cttPqKJLHdpi
xZy+RwIDAQAB01AwTjAdBgNVHQ4EFgQUUNAaMPP9V4sEpHwWONurFx1aDr1QwHwYD
VR0jBBgwFoAUNAaMPP9V4sEpHwWONurFx1aDr1QwDAYDVDR0TBAUwAwEB/zANBgkq
hkig9w0BAQUFAA0BgQCe0d8077n7eTftVw+xrE0qhBG3owUURhqTgWrxBAH0y3V5
mL/TAapJhPSy05CDeFgD78jabpymSuLSGBaKQHYW2mx9ko2bwI6qFN72rzsT828U
4TmnqHjVye67JQcLBpvsxhi5Hgqe8vqD5v6k7MffizngJCnUkDkkmF2jYHVn5g==
-----END CERTIFICATE-----
');
```

8. From `admintools`, restart the Vertica database as `vertica DBA` user and to verify the settings, follow the step:

Tip: Make sure that the `admintools` is running.

```
vsq1 -h <Host name> -U <User name> -p <Port> -d <Database Name>
```

where, `<Host name>` is the host name of the system where Vertica is installed

`<User name>` is the Vertica user with DBA privileges

<Port> is the port number

<Database Name> is the name of Vertica database

A status message similar to the following will be displayed:

```
SSL connection (cipher: DHE-RSA-AES256-SHA, bits: 256)''
```

On OBR:

Perform the following steps on the system where OBR is installed.

Configure SSL for JDBC clients

To configure SSL for JDBC clients, run the following steps on the command prompt:

1. Log on as `root` and create the truststore in the same location as the `cert.crt`:

```
keytool -genkey -alias cacert -keyalg RSA -keysize 2048 -keypass <Password> -  
storepass <Password> -keystore <File name> -storetype pkcs12
```

where, *<File name>* is the trust store file name `SHR_CERT_PKCS.p12` with the path. For Example:
The default trust store path `{PMDB_HOME}/keystore` created by OBR may be used.

<Password> is the password. For example: `shradmin`

2. `keytool -import -file serverca.crt -alias importcert -keystore <File name> -
storepass <Password>`

where, *<File name>* is the trust store file name `SHR_CERT_PKCS.p12` with the path

<Password> is the password. For example: `shradmin`

Configure SSL for ODBC clients

To configure SSL for ODBC clients, run the following steps on the command prompt:

1. Run the following command on a command prompt:

```
echo 'SSLMode = require' >> $PMDB_HOME/config/odbc.ini
```

2. To check if the connection is working over TLS, run the following command:

```
isql -v SHRDB <Vertica DBA User> <Vertica DBA Password>
```

where, *<Vertica DBA User>* is the Vertica user with DBA privileges

<Vertica DBA Password> is the password for Vertica user

A connection status message is displayed.

On SAP BusinessObjects:

1. To configure TLS for BO, follow these steps:

- a. Go to the following location:

```
/opt/HP/BSM/BOE4/sap_bobj/enterprise_xi40/dataAccess/connectionServer
```

- b. Open the `cs.cfg` file and add/edit the lines to file as follows:

```
<JavaVM>  
<!-- The default JVM configuration can be overridden here -->  
<!-- Use an absolute path for the JVM -->  
<!--  
<LibraryName JNIVersion="JNI_VERSION_1_4">ABSOLUTE_  
PATH/jvm.dll</LibraryName>  
  
-->  
<Options>  
<Option Processor="64">-Xmx2048m</Option>  
<Option>-Xrs</Option>  
<Option>-Djavax.net.ssl.trustStore=<PATH_TO_TrustStore></Option>  
<Option>-Djavax.net.ssl.trustStorePassword=<Password></Option>  
</Options>  
</JavaVM>
```

where, <PATH_TO_TrustStore> is the path to the truststore to which certificate is imported. For Example: The default trust store path {PMDB_HOME}/keystore created by OBR may be used.

<Password> is the Password to the truststore. For Example: shradmin

- c. Restart the SAP BusinessObjects services as follows:

Go to `/etc/init.d` directory and run the following command:

On RHEL 6.x/SUSE Linux Enterprise Server 11:

- i. `service SAPBOBJEnterpriseXI40 stop`
- ii. `service SAPBOBJEnterpriseXI40 start`

On RHEL 7.x:

- i. `systemctl stop SAPBOBJEnterpriseXI40.service`
- ii. `systemctl start SAPBOBJEnterpriseXI40.service`

Enable TLS for Vertica in Administration Console

1. In the Administration Console, select **Additional Configurations > Vertica Database & Time Zone**.
2. In the **Vertica Database > TLS**, select the **Enable** option.

Vertica Database & Time Zone

Vertica Database & Time Zone

Time zone: GMT

Vertica Database:

Database type:	vertica
Host name:	btprvm0918.hpeswlab.net
Port:	5433
User name:	hpobr918
TLS:	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled

Save **Change Password**

A confirmation dialog box is displayed.

3. Click **Yes**. **Enable TLS** pane is displayed.
4. Enter trust store file name with path in **TrustStore File**, trust store password in **TrustStore Password**, and re-enter password to confirm in **TrustStore Confirm Password**.
5. Click **OK**. A confirmation message is displayed.

Configure TLS for Vertica in Distributed Scenario

On Vertica:

Perform the following steps on the system where Vertica is installed. To enable TLS for Vertica, log on to the vertica system and run the following commands on the command prompt:

1. To create a CA private key and public certificate, follow these steps:

- a. `openssl genrsa -out servercakey.pem 2048`
- b. `openssl req -newkey rsa:2048 -x509 -days 3650 -key servercakey.pem -out serverca.crt`

Enter the values for the following prompts:

- i. Country Name (2 letter code) [XX]:
Enter the country code. For example, IN.
- ii. State or Province Name (full name) []:
Enter full name of state. For example, KA.
- iii. Locality Name (eg, city) [Default City]:
Enter name of your city. For example, BLR.
- iv. Organization Name (eg, company) [Default Company Ltd]:
Enter name of your organization or default company name. For example, HPE.
- v. Organizational Unit Name (eg, section) []:
Enter name of the section or organizational unit. For example, HPE.
- vi. Common Name (eg, your name or your server's hostname) []:
Enter your name or server's hostname as common name. For example, test.hpeswlab.net.
- vii. Email Address []:
Enter your email address. For example, test123@hpe.com.

2. To create the server private key and certificate, follow these steps:

- a. `openssl genrsa -out server.key 2048`
- b. `openssl req -new -key server.key -out server_reqout.txt`

Enter the values for the following prompts:

- i. Country Name (2 letter code) [XX]:
Enter the country code. For example, IN.
 - ii. State or Province Name (full name) []:
Enter full name of state. For example, KA.
 - iii. Locality Name (eg, city) [Default City]:
Enter name of your city. For example, BLR.
 - iv. Organization Name (eg, company) [Default Company Ltd]:
Enter name of your organization or default company name. For example, HPE.
 - v. Organizational Unit Name (eg, section) []:
Enter name of the section or organizational unit. For example, HPE.
 - vi. Common Name (eg, your name or your server's hostname) []:
Enter your name or server's hostname as common name. For example, test.hpeswlab.net.
 - vii. Email Address []:
Enter your email address. For example, test123@hpe.com.
 - viii. Please enter the following 'extra' attribute to be sent with your certificate request. A challenge password []:
Enter password.
 - ix. An optional company name []:
Enter an optional company name. For example, HPE.
3. To sign the server's certificate using the CA private key file and public certificate, run the following command:

```
openssl x509 -req -in server_reqout.txt -days 3650 -sha1 -CAcreateserial -CA serverca.crt -CAkey servercakey.pem -out server.crt
```

Note: Run the above command in single line.

4. Run the following command to log on to vsq1:

```
vsq1 -h <Host name> -U <User name> -p <Port> -d <Database Name>
```

where, *<Host name>* is the host name of the system where Vertica is installed

<User name> is the Vertica user with DBA privileges

<Port> is the port number

<Database Name> is the name of Vertica database

5. Set the `Enable SSL` flag to 1:

```
SELECT SET_CONFIG_PARAMETER('EnableSSL', '1');
```

6. To set the private key in Vertica using the contents of `server.key` file, follow these steps:

- a. `SELECT SET_CONFIG_PARAMETER('SSLPrivateKey', '<contents of server.key file>');`

The following is an example of the command with sample content of `server.key` file:

```
SELECT SET_CONFIG_PARAMETER('SSLPrivateKey', '-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQDtWL T9FGTpsxXc9Yo0n4LbLgy0shp0q8T0hzwRnz31izqeOasT
KH4CCwXDOGQprcdELdS+Mr3NHGENi8ya+Cs9ZCCQJB+fzSk6Y7j40bBvIIwpVW9s
Na+YmpDnP9BM6qgniW/pn0i871Z+sHUJHZ386R08cttPqKJLHdpixZy+RwIDAQAB
AoGBAJk/HGUH5PxL6ELpuxmtIGV6fz0wh4prWcBr6uoJ4oyHIAsHeyD81Re1j7IT
2ABdNvsbiHBh/NDRkR1ik3I/6FIV3kuZd6DNIiecfY8y7BfMtInw3Whm9gRAkron
VGbRiSA330e0KTTt6wz2PY+ZVVH492gf33K6PZqXfR4+iG7RAkEA+R0DRnm5crwX
LQ1ygMhwRn1p2b4LmYYmMosnUkW00ueC5I+dTPTFvGKtb9We3csRIy1RHXUJJu2
yvT60/F5zwJBAPPoa3phaF3JE0Vy5DZS/r5+DKom14F5MeYsokPbqr2SG+xZOCm9
cFjM0AneF/zHcW8qVNwb1wQIY6oIuRgEqgkCQQCccTjuWGE7BYkz9N70u2uvCPGh
mbT1LBbu507DvwSsP1m30e2aN5mn0J7AtrGUBepZ/1eT779TYiqwWJqRbHuHAKEA
7VyIC8bzcFCUb+ne351TqiYZpX6L5PkDZ3uI5+In4erC00ij0xAgwnqlx+9tE/b
glVt0+575v7LDtQCX09dEQJAPjhGY/wyzJ8aS7KTF6Lm+8WuM2xD7d9y4NU6Shs2
tsb+QrM5jYg79AuwdwP4YceZLIp34QB19BSF/E7WAOXEUQ==
-----END RSA PRIVATE KEY-----
');
```

7. To set the certificate in Vertica using the contents of `serverca.crt` file, follow these steps:

- a. `SELECT SET_CONFIG_PARAMETER('SSLCertificate','<contents of serverca.crt file>');`

The following is an example of the command with sample content of `serverca.crt` file:

```
SELECT SET_CONFIG_PARAMETER('SSLCertificate','-----BEGIN CERTIFICATE-----
MIICmjCCAgOgAwIBAgIJAMnZqpMfBVTjMA0GCSqGSIb3DQEBBQUAMGYxCzAJBgNV
BAYTAK10MQswCQYDVQQIDAJLQTEMMAoGA1UEBwwDQkxSMQwwCgYDVQQKDANIUEUx
DDAKBgNVBAsMA0hQRTEMMAoGA1UEAwDT0JSMRIwEAYJKoZIhvcNAQkBFgnjb20w
HhcNMTYwMzI5MDkyMDU1WhcNMjYwMzI3MDkyMDU1WjBmMQswCQYDVQQGEWJTTjEL
MAKGA1UECAwCS0ExDDAKBgNVBACMA0JMUjEMMAoGA1UECgwDSFBFMQwwCgYDVQQL
DANIUEUxDDAKBgNVBAMMA09CUjESMBAGCSqGSIb3DQEJARYDY29tMIGfMA0GCSqG
SIb3DQEBAQUAA4GNADCBiQKBgQDtWLT9FGTpsXc9Yo0n4LbLgy0shp0q8T0hzwR
nz31izqe0asTKH4CCWXdOGQprcdELdS+Mr3NHGEni8ya+C9ZCCQJB+fzSk6Y7j4
0bBvIIwpVV9sNa+YmpDnP9BM6qgniW/pn0i871Z+sHUIJHZ386R08cttPqKJLHdpi
xZy+RwIDAQAB01AwTjAdBgNVHQ4EFgQUUNAaMPP9V4sEpHwWONurFx1aDr1QwHwYD
VR0jBBgwFoAUNAaMPP9V4sEpHwWONurFx1aDr1QwDAYDVR0TBAAUwAwEB/zANBgkq
hkiG9w0BAQUFAAOBgQCe0d8077n7eTftVw+xE0qhBG3owUURhqTgWrxBAH0y3V5
mL/TAapJhPSy05CDeFgD78jabpymSuLSGBaKQHYW2mx9ko2bwI6qFN72rzsT828U
4TmqHjVye67JQcLBpvsxhi5Hgqe8vqD5v6k7MfFizngJCnUkDkkmF2jYHVn5g==
-----END CERTIFICATE-----
');
```

8. From `admintools`, restart the Vertica database as `vertica DBA` user and to verify the settings, follow the step:

Tip: Make sure that the `admintools` is running.

```
vsq1 -h <Host name> -U <User name> -p <Port> -d <Database Name>
```

where, `<Host name>` is the host name of the system where Vertica is installed

`<User name>` is the Vertica user with DBA privileges

`<Port>` is the port number

`<Database Name>` is the name of Vertica database

A status message similar to the following will be displayed:

```
SSL connection (cipher: DHE-RSA-AES256-SHA, bits: 256)''
```

On OBR:

Perform the following steps on the system where OBR is installed.

On Linux:

Configure SSL for JDBC clients

To configure SSL for JDBC clients, run the following steps on the command prompt:

1. Copy the certificate `cert.crt` from the system where Vertica installed to the OBR system.
2. On the OBR system, log on as `root` and create the truststore in the same location as the `cert.crt`:

```
keytool -genkey -alias cacert -keyalg RSA -keysize 2048 -keypass <Password> -  
storepass <Password> -keystore <File name> -storetype pkcs12
```

where, *<File name>* is the trust store file name `SHR_CERT_PKCS.p12` with the path. For Example:
The default trust store path `{PMDB_HOME}/keystore` created by OBR may be used.

<Password> is the password. For example: `shradmin`

3. `keytool -import -file serverca.crt -alias importcert -keystore <File name> -
storepass <Password>`

where, *<File name>* is the trust store file name `SHR_CERT_PKCS.p12` with the path

<Password> is the password. For example: `shradmin`

Configure SSL for ODBC clients

To configure SSL for ODBC clients, run the following steps on the command prompt:

1. Run the following command on a command prompt:

```
echo 'SSLMode = require' >> $PMDB_HOME/config/odbc.ini
```

2. To check if the connection is working over TLS, run the following command:

```
isql -v SHRDB <Vertica DBA User> <Vertica DBA Password>
```

where, *<Vertica DBA User>* is the Vertica user with DBA privileges

<Vertica DBA Password> is the password for Vertica user

A connection status message is displayed.

On Windows:

Configure SSL for JDBC clients

To configure SSL for JDBC clients, run the following steps on the command prompt:

1. Copy the certificate `cert.crt` from the system where Vertica installed to OBR system.
2. Open the command prompt and create the truststore in the same location as the `cert.crt`:

```
keytool -genkey -alias cacert -keyalg RSA -keysize 2048 -keypass <Password> -storepass <Password> -keystore <File name> -storetype pkcs12
```

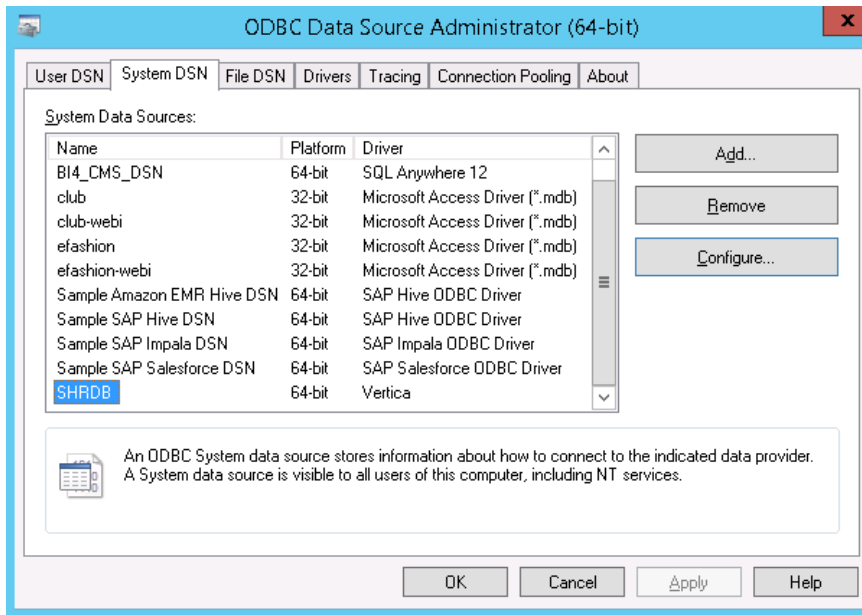
where, `<File name>` is the trust store file name with path. For example, `Verticatrustore.p12`
`<Password>` is the password. For example: `shradmin`
3.

```
keytool -import -file serverca.crt -alias importcert -keystore <File name> -storepass <Password>
```

where, `<File name>` is the trust store file name with path. For example, `Verticatrustore.p12`
`<Password>` is the password. For example: `shradmin`

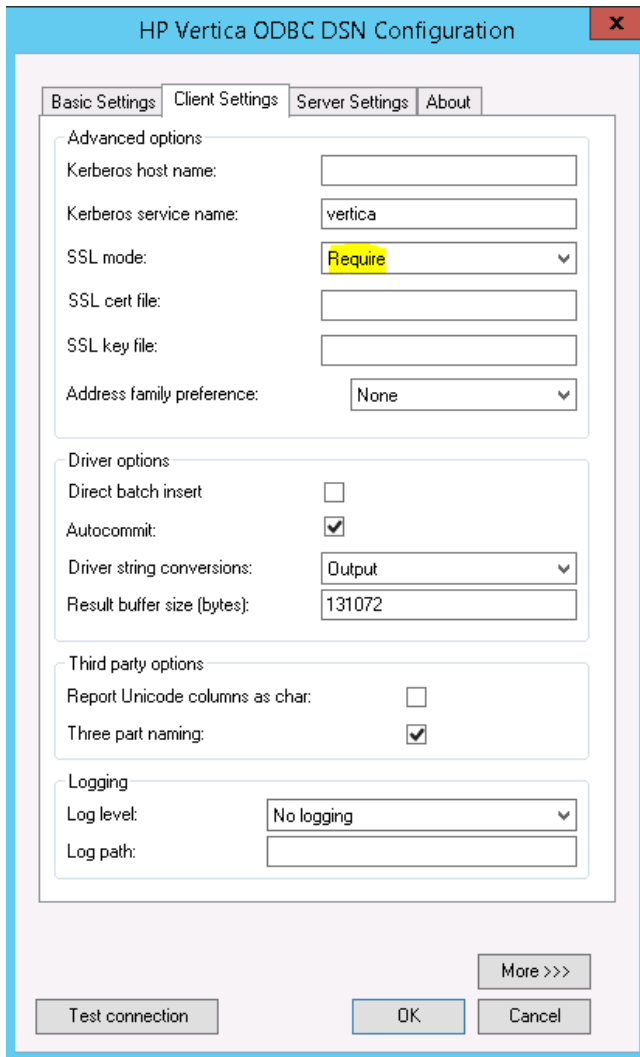
Configure SSL for ODBC clients

1. Log on to OBR system.
2. Click **Start > Control Panel** and then click **System and Security**. The **System and Security** windows is displayed.
3. Click **Administrative Tools**. The Administrative Tools window is displayed.
4. Double-click **ODBC Data Sources (64-bit)**. The **ODBC Data Source Administrator (64-bit)** window is displayed.
5. Click **System DNS** tab, select **SHRDB** and click **Configure**.



The Vertica ODBC DSN Configuration window is displayed.

6. Click **Client Settings** tab and select **Require** for **SSL mode** from the drop down list.



7. Click **Test connection**.

A connection succeeded message is displayed.

8. Click **OK**.

The SSL for DSN is enabled.

Enable TLS for Vertica in Administration Console

1. In the Administration Console, select **Additional Configurations > Vertica Database & Time Zone**.
2. In the **Vertica Database > TLS**, select the **Enable** option.

Vertica Database & Time Zone

Vertica Database & Time Zone

Time zone: GMT

Vertica Database:

Database type:	vertica
Host name:	btpvm0918.hpeswlab.net
Port:	5433
User name:	hpobr918
TLS:	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled

Save **Change Password**

A confirmation dialog box is displayed.

3. Click **Yes**. **Enable TLS** pane is displayed.
4. Enter trust store file name with path in **TrustStore File**, trust store password in **TrustStore Password**, and re-enter password to confirm in **TrustStore Confirm Password**.
5. Click **OK**. A confirmation message is displayed.

On SAP BusinessObjects:

1. Import the certificate to the truststore available on SAP BusinessObjects. Run the following command:

```
keytool -import -file <serverca.crt> -alias importcert -keystore <File name>  
storepass <Password>
```

where, `serverca.crt` is the CA certificate file path

`<File name>` is the truststore path on SAP BusinessObjects server. For Example: The default trust store path `{PMDB_HOME}/keystore` created by OBR may be used.

`<Password>` is the Password to the truststore. For Example: `shradmin`

2. To configure TLS for BO, follow these steps:

- a. Go to the following location:

On Linux: `/opt/HP/BSM/B0E4/sap_bobj/enterprise_xi40/dataAccess/connectionServer`

On Windows: <OBR install Directory>:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\dataAccess\connectionServer\

- b. Open the `cs.cfg` file and add/edit the lines to file as follows:

```
<JavaVM>
<!-- The default JVM configuration can be overridden here -->
<!-- Use an absolute path for the JVM -->
<!--
<LibraryName JNIVersion="JNI_VERSION_1_4">ABSOLUTE_
PATH/jvm.dll</LibraryName>
-->
<Options>
<Option Processor="64">-Xmx2048m</Option>
<Option>-Xrs</Option>
<Option>-Djavax.net.ssl.trustStore=<PATH_TO_TrustStore></Option>
<Option>-Djavax.net.ssl.trustStorePassword=<Password></Option>
</Options>
</JavaVM>
```

where, `<PATH_TO_TrustStore>` is the path to the truststore to which certificate is imported. For Example: The default trust store path `{PMDB_HOME}/keystore` created by OBR may be used.

`<Password>` is the Password to the truststore. For Example: `shradmin`

- c. Restart the SAP BusinessObjects services as follows:

On Linux:

Go to `/etc/init.d` directory and run the following command:

On RHEL 6.x/SUSE Linux Enterprise Server 11:

- i. `service SAPBOBJEnterpriseXI40 stop`
- ii. `service SAPBOBJEnterpriseXI40 start`

On RHEL 7.x:

- i. `systemctl stop SAPBOBJEnterpriseXI40.service`
- ii. `systemctl start SAPBOBJEnterpriseXI40.service`

On Windows:

- i. From the **Start**, type **Run** in **Search**. The Run dialog box appears.
- ii. Type **services.msc** in the open field, and then press **ENTER**. The Services window appears.
- iii. Right-click on the following services and click **Restart**:
 - Business Objects Webserver
 - Server Intelligent Agent (OBR)
 - SQL Anywhere for SAP Business Intelligence

On Remote Collector:

1. To enable FIPS, run the following commands on the command prompt:

- `cd {PMDB_HOME}/bin`
- `perl FIPS.pl enable`
- `cd {OVINSTALLDIR}/lbin/secco/`
- `ovconfchg -ns sec.cm -set ASYMMETRIC_KEY_LENGTH 2048`
- `MigrateSymKey -sym_key_algo eAES128`
- `MigrateSymKey -hash_algo eSHA256`
- `FIPS_tool -enable_FIPS`

Run the command `ovbbccb -status` to check the FIPS status of OVBBC.

2. From the OBR server, copy the `{PMDB_HOME}/keystore/SHR_CERT_PKCS.p12` to the Remote Collector server to the location `{PMDB_HOME}/keystore/SHR_CERT_PKCS.p12`
3. Stop the `HPE_PMDB_Platform_Collection` service.
4. Perform the steps for the collector changes as mentioned in ["Task 5: Stop the HPE_PMDB_Platform_Collection service and edit Collection start and stop scripts"](#) on page 204.
5. Start the collector `HPE_PMDB_Platform_Collection` service.
6. Log on to the Administration Console and add the collector.

Part IV: Database Backup and Recovery

This section provides you information to back up and restore the OBR databases. It also provides information on how you can plan for back up using the database backup options in OBR.

Chapter 21: Database Backup and Recovery

OBR enables you to back up and recover the database to prevent data loss in the event of a database failure. It is recommended that you take regular backup of the database before you begin using OBR in production.

Disaster recovery of OBR includes planning for taking regular back up of OBR databases, and creating a backup of key configuration and license files. Regular back up helps you to recover data and prevent data loss in the event of a disaster.

Important Considerations

- You must schedule the full back up tasks to run at regular intervals.
- While planning for database backup, the OBR system with SAP BusinessObjects installed on same system requires 5 GB for the backup storage space.

In case of distributed (custom) scenario, 5 GB for the backup storage space is required in the OBR system and SAP BusinessObjects system respectively.

For Vertica storage space, see [Vertica Backup and Restore](#).

- You must ensure to change the Administration Console password on the systems before you move ahead with back up and restore steps.

Also, change the SAP BusinessObjects Central Management Console (CMC) database (SQL Anywhere) password on the systems before you move ahead with back up and restore steps.

- It is recommended to take a daily backup.

If you have scheduled a daily backup, the backup files will be saved with the three letter prefix of the day the backup is taken.

For example, if the backup script is run on a Monday the backup file will be saved with the name `/<backup path>/SHR_DR_FullBackup/Mon`.

However the previous backup will be overwritten by the next week's backup files. Similarly, for a twelve-hour backup, the backup files may get overwritten if the backup script is run on the same day. You must ensure that you create separate folders for such instances if you prefer to retain the old back ups.

- In the event of a OBR server failure, you can recover the OBR database from the backup location. The backup system and the primary system must be identical with same hardware specifications,

operating systems, OBR version, file path, topology, post installation configurations and deployed content packs.

- If you have changed any of the configuration files (Example: CAC), performance tuning in the primary setup then perform all those changes for the disaster recovery setup.

Caution: OBR must have a static IP address. You must set up the OBR Disaster Recovery environment (remote or local) with the same IP address and host name similar to the primary OBR server to restore the permanent license. No additional license is required for restoring OBR.

Terminologies used in this guide

Following are the terminologies used in this guide:

Terminology	Explanation
SIA	Server Intelligence Agent
CMC	Central Management Console
CCM	Central Configuration Manager
OBR server1	Initial OBR system where the existing data back up is taken.
OBR server2	New OBR installed system where the data is restored.
SHR_DR_Backup	Name of the backup file.

Backup of OBR Components

It is recommended that you take regular back up of the OBR components before you begin using OBR in production.

OBR's full back up script enables you to take a complete back up of the following components (including the database files and transaction logs):

- SAP BusinessObjects (File store)
- SAP BusinessObjects Central Management Console (CMC) database (SQL Anywhere)
- Management database tables (PostgreSQL)
- Configuration Files

Note: In a Custom Installation scenario, perform the following steps to take a backup of OBR on the systems where you have installed the OBR components.

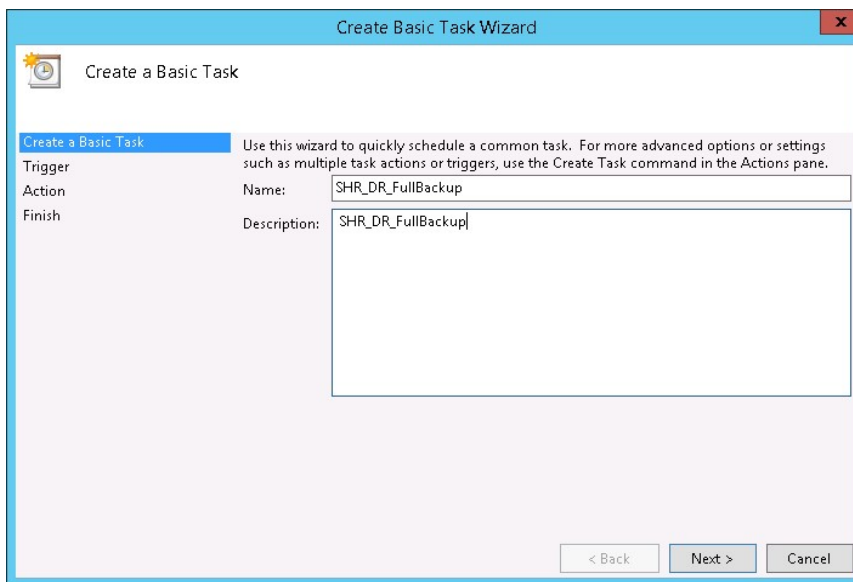
Create Full Backup of OBR on Windows

The %PMDB_HOME%\DR\SHR_full_Backup.pl script helps you take a full backup of the OBR components mentioned in "[Backup of OBR Components](#)" on the previous page.

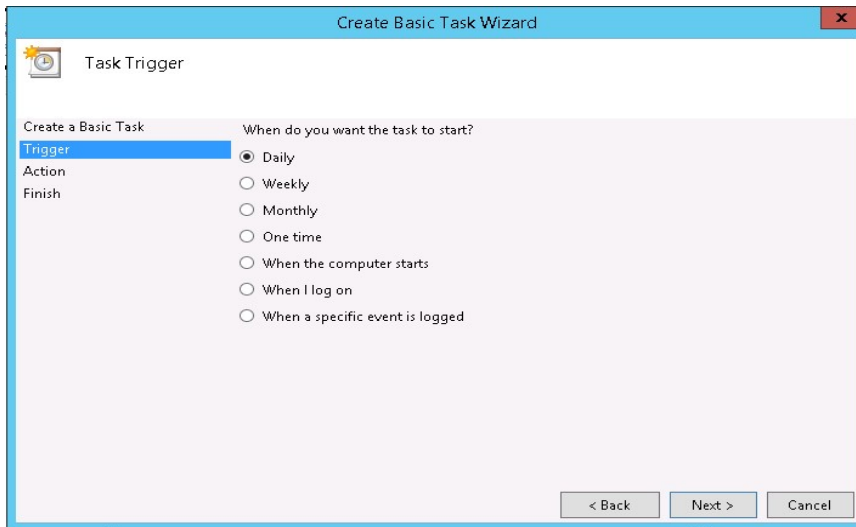
The script generates the DR.log file in the path %PMDB_HOME%\log.

Log on to OBR server1 where you have installed the OBR components and perform the following steps to schedule the backup:

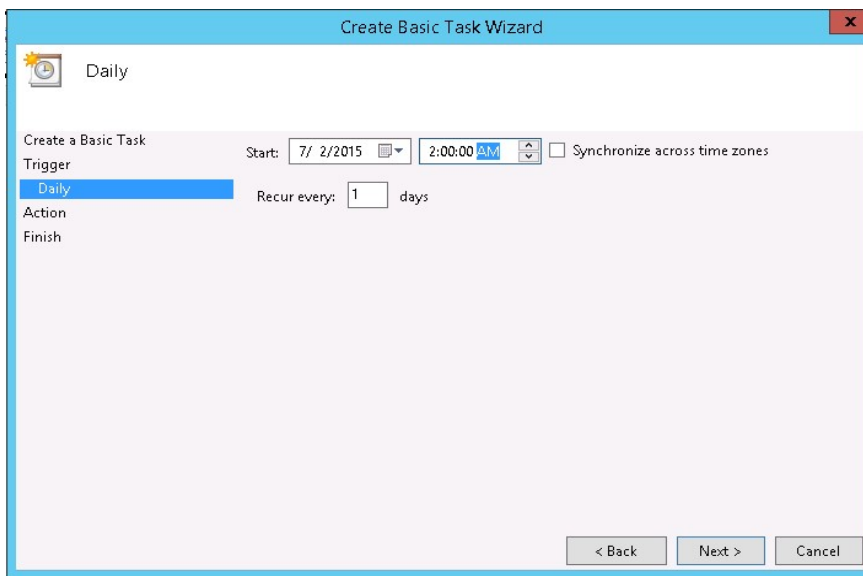
1. Go to **Start** and type **Task Scheduler** in **Search**. Double-click on the Task Scheduler to open it.
2. In the Task Scheduler window, click **Create Basic Task**. The Create Basic Task wizard appears.
3. Type **SHR_DR_FullBackup** for the Name and Description, and then click **Next**.



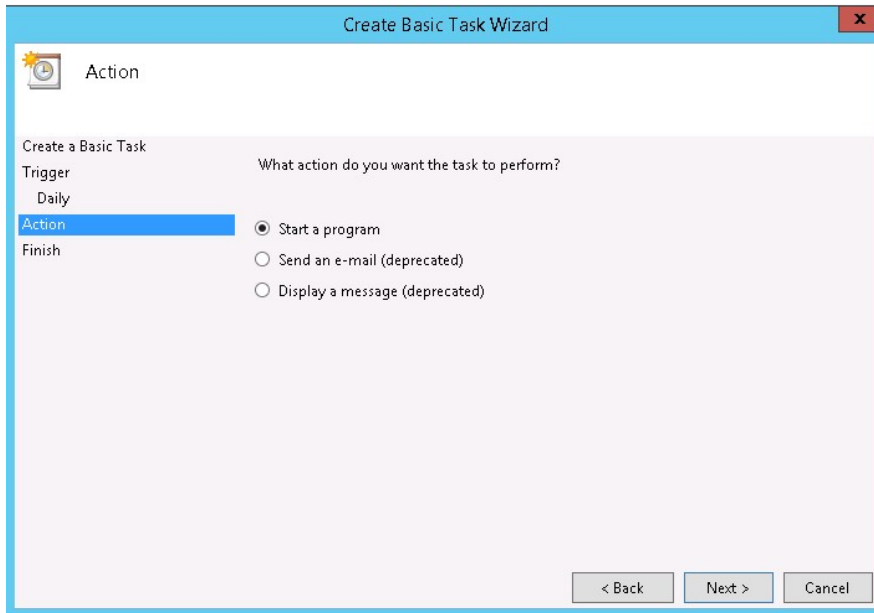
4. Select **Daily**, and then click **Next**.



5. Select the start time, type 1 in the **Recur every** text box, and then click **Next**.



6. Select **Start a program** in Action page, and then click **Next**.



7. Type `perl` and then Browse to `%PMDB_HOME%\DR`, select **SHR_full_Backup.pl**, and then click **Next**.

In the Add arguments field, type the following details:

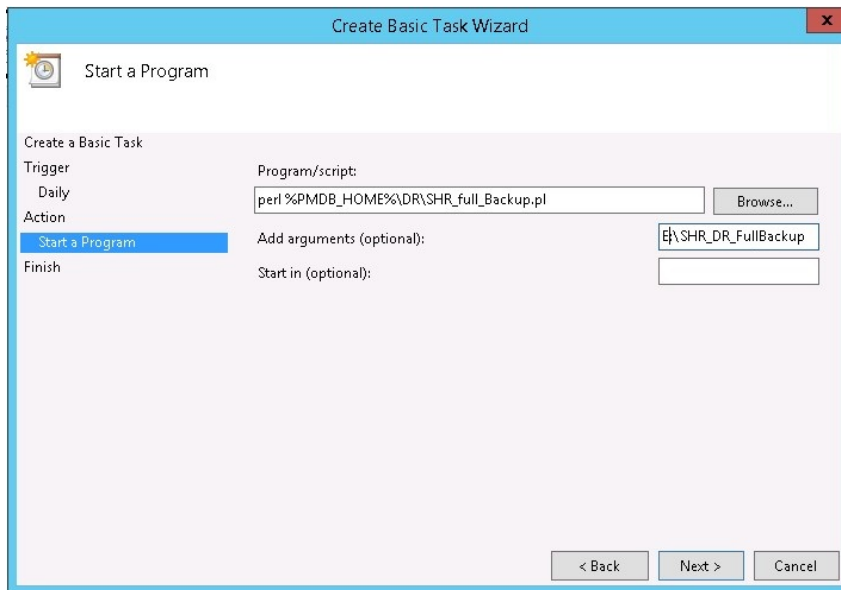
`<backup_path>`

In this instance:

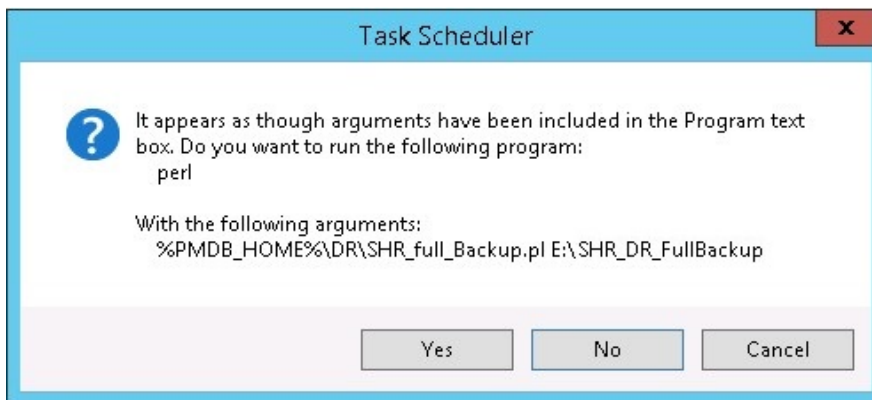
- `<backup_path>` is the location where you want to store the backup files and data.

Example: `E:\SHR_Full_Backup`

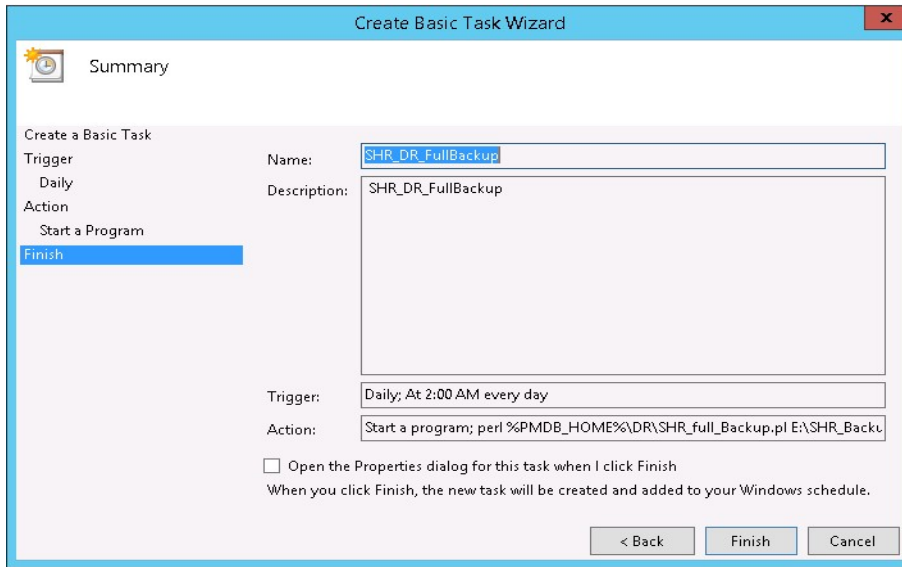
Note: If you want to backup the files to a custom folder, you must create it before you enter the path in **Add arguments** text box.



8. The following Task Scheduler message appears, click **Yes**.

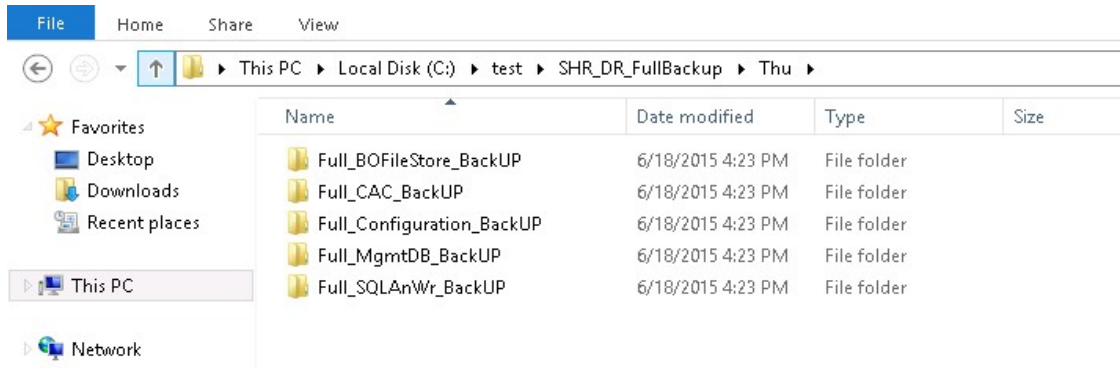


9. Click **Finish** in the Summary page.



You can check the task created in the **Active Tasks** of the Task Scheduler window.

Following image is the example of the backup files:



Create Full Backup of OBR on Linux

The `$PMDB_HOME/DR/SHR_full_Backup.pl` script helps you take a full back up of the OBR components mentioned in "[Backup of OBR Components](#)" on page 229.

The script generates the `DR.log` file in the path `$PMDB_HOME/log`.

Log on to the OBR server1 where you have installed the OBR components and follow these steps to schedule the back up:

1. Log on to the OBR system as root.
2. To edit your crontab file, type the following command at the command prompt:

```
crontab -e
```

3. Add a line to the crontab file to invoke the `$PMDB_HOME/DR/SHR_full_Backup.pl` script once every day.

```
<time schedule> </opt/OV/nonOV/perl/a/bin/perl> <location of the backup script> <backup path>
```

where, *<time schedule>* is the time of the day the script is invoked (the time schedule is as per the crontab format)

<location of the backup script> is the location of the `SHR_full_Backup.pl` back up script

<backup path> the location of the back up files

For example: `0 15 * * 0 /opt/OV/nonOV/perl/a/bin/perl $PMDB_HOME/DR/SHR_full_Backup.pl /root/SHR_DR_FullBackup`

In the above example, the `/opt/HP/BSM/PMDB/DR/SHR_full_Backup.pl` script is invoked on the first day of the week at 15:00 hours and the data file backup is stored at `/root/SHR_DR_FullBackup`.

4. Save the crontab file.
All the log files for crontab are in the location `/var/mail`.
5. After running the scheduled backup, note down the backup sub folder and file for Management DB

```
<backup path>/SHR_DR_FullBackup/<the day of backup>/Full_MgmtDB_BackUP
```

```
<backup path>/SHR_DR_FullBackup/<the day of backup>/Full_MgmtDB_BackUP/Mgmt_backup_AGGREGATE_CONTROL.dat
```

For example:

```
/root/SHR_DR_FullBackup/SHR_DR_FullBackup/Thu/Full_MgmtDB_BackUP
```

```
/root/SHR_DR_FullBackup/SHR_DR_FullBackup/Thu/Full_MgmtDB_BackUP/Mgmt_backup_AGGREGATE_CONTROL.dat
```

Restore OBR Components

After you complete the OBR installation and configuration, you must ensure to bring the Vertica database down before you restore the back up.

Transfer all backup data into a local directory of the system. OBR's restore script enables you to restore all of the backup data.

Note: In a Custom Installation scenario, perform the following restore steps on the systems where you have installed the OBR components.

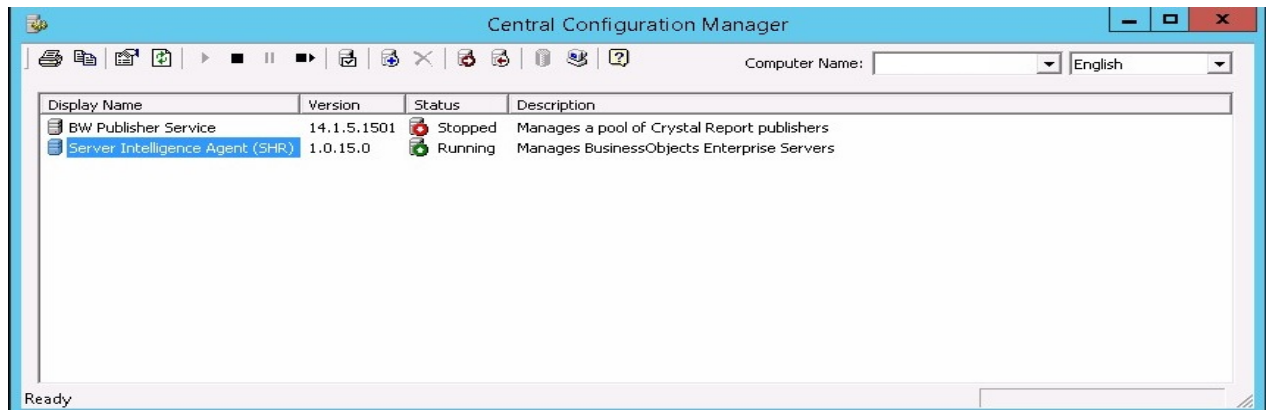
Restore Backup of OBR on Windows

For SAP BusinessObjects Database and File Store

Log on to the system where OBR is installed that is OBR server2 and follow these steps to restore the back up of the OBR components:

1. Copy the backup file SHR_DR_FULLBACKUP from the backup location of OBR server1 to OBR server2 where you want to restore the backup.
2. Go to **Start** and type **Central Configuration Manager** in **Search**. Double-click on the Central Configuration Manager.

The Central Configuration Manager window appears.



3. Right-click on **Server Intelligence Agent (SHR)** and click **Stop**.
4. From the **Services** window, click the **SLQ Anywhere for SAP Business Intelligence** service and click **Stop**.
5. Rename the existing file store folder.

The default location of the file store is <BusinessObjects installed drive>:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\FileStore.

For example: You can rename it to FileStore_old.

6. From the default location move the existing SQL Anywhere database to another location.

The default location of the SQL Anywhere database is <BusinessObjects installed drive>:\Program Files (x86)\SAP BusinessObjects\sqlanywhere\database.

7. Perform the following steps to run the restore script:

- a. Click **Start > Run**. The Run dialog box appears.
- b. Type `cmd`, and then press **ENTER**. The command prompt appears.
- c. Run the following command:

```
Perl <Location of the restore script><Location of the backup file>
```

where, <Location of the restore script> is the path of the restore script, and <Location of the backup file> is the path of the particular day's backup file that you want to restore.

For example: `Perl %PMDB_HOME%\DR\SHR_full_Restore.pl E:\SHR_Backup\SHR_DR_FullBackup\Thu`

8. Click **Start > Run**. The Run dialog box appears.
9. Type `dbisqlc` and then press **ENTER**. The Connect to SQL Anywhere window opens.
10. From the **Services** window, click the **SQL Anywhere for SAP Business Intelligence** service and click **Start**.



11. In the Connect to SQL Anywhere window, type the following details:

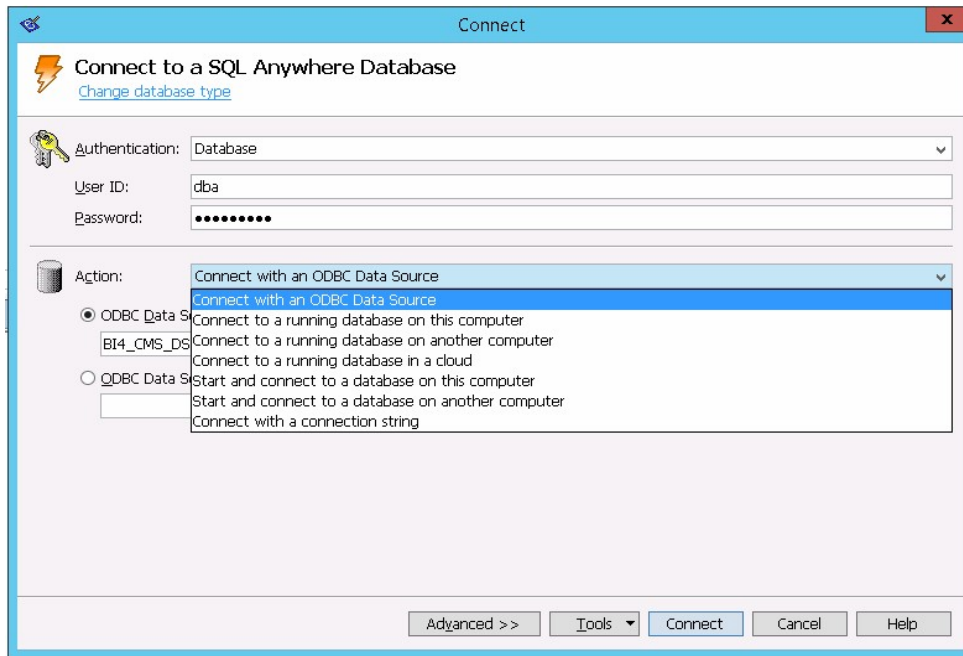
- User ID: Type the user as `dba`
- Password: `<password>`

where, `<password>` is the password used to log on to the CMC database (SQL Anywhere)

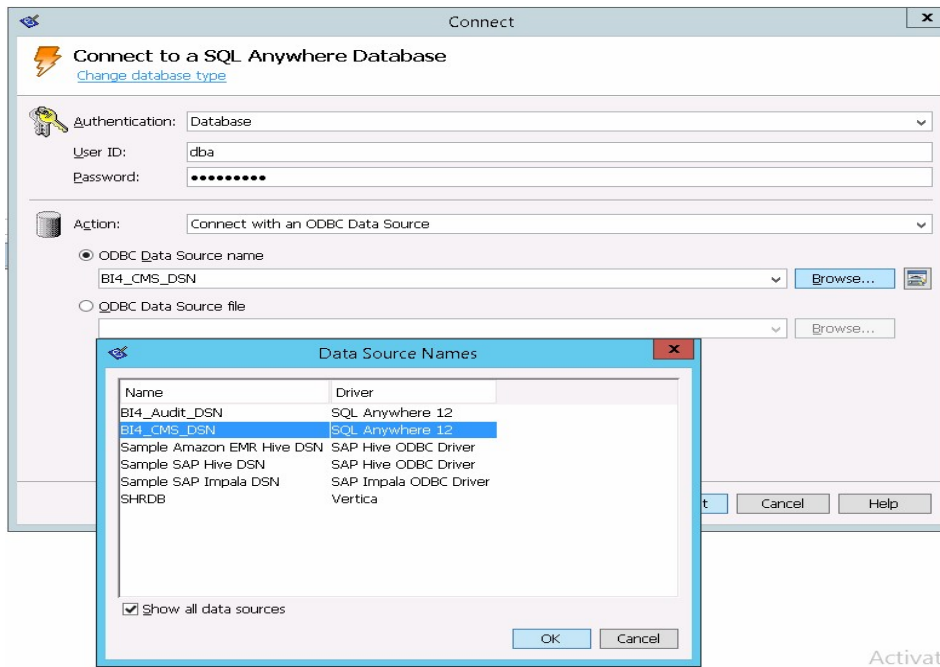
Note: If you have not changed the password in the server where the back up is taken, type the same password else, type the changed password.

Caution: Ensure that you change the default password before you start using OBR. For more information, refer *Changing Default Passwords* in the *Operations Bridge Reporter Online help for Administrators*.

- o Action: Select **Connect with an ODBC Data Source** from the drop down.

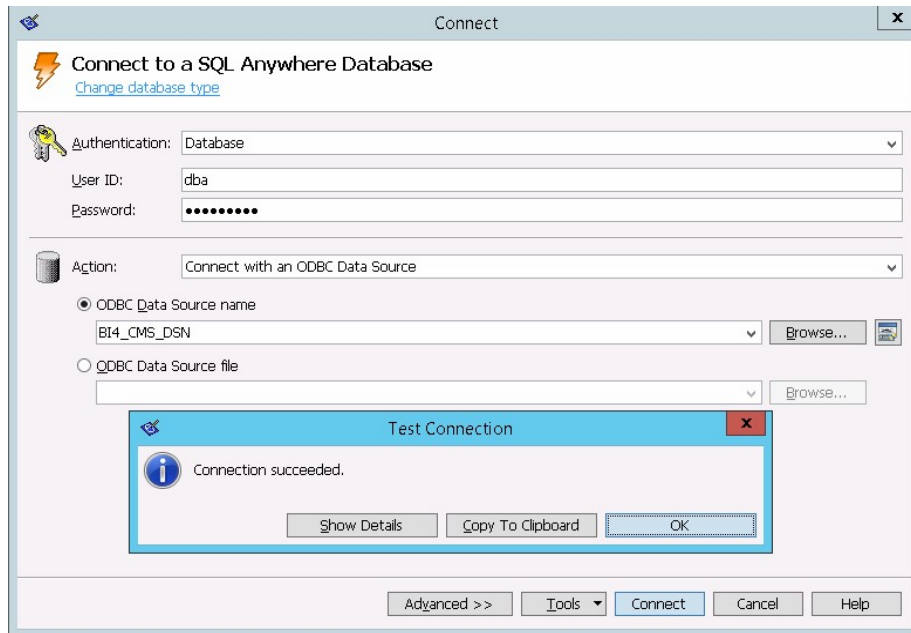


- o Select the **ODBC Data Source name** option, and then click **Browse** to enter the source name BI4_CMS_DSN.



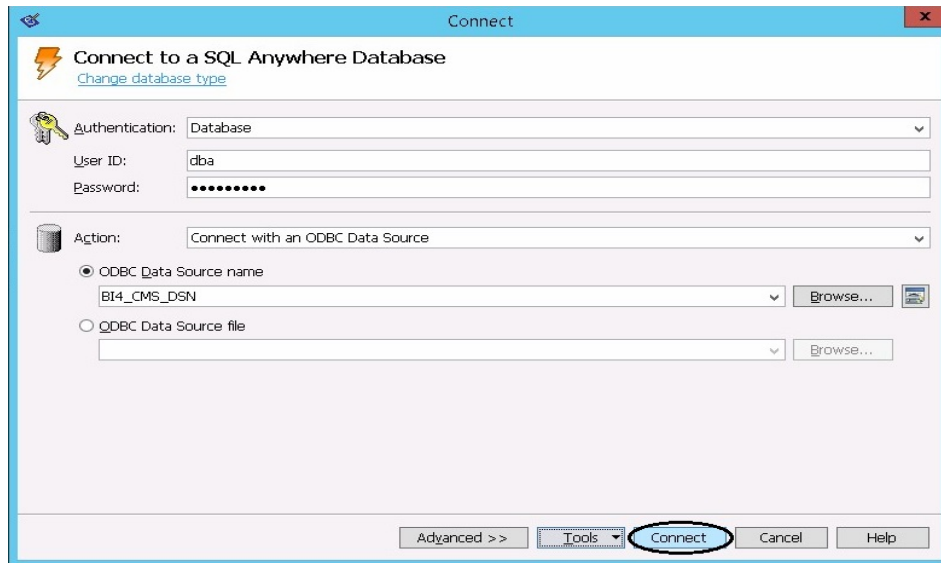
Activate

- o Check the connection as shown in the following image.



The Connection succeeded confirmation dialog box appears.

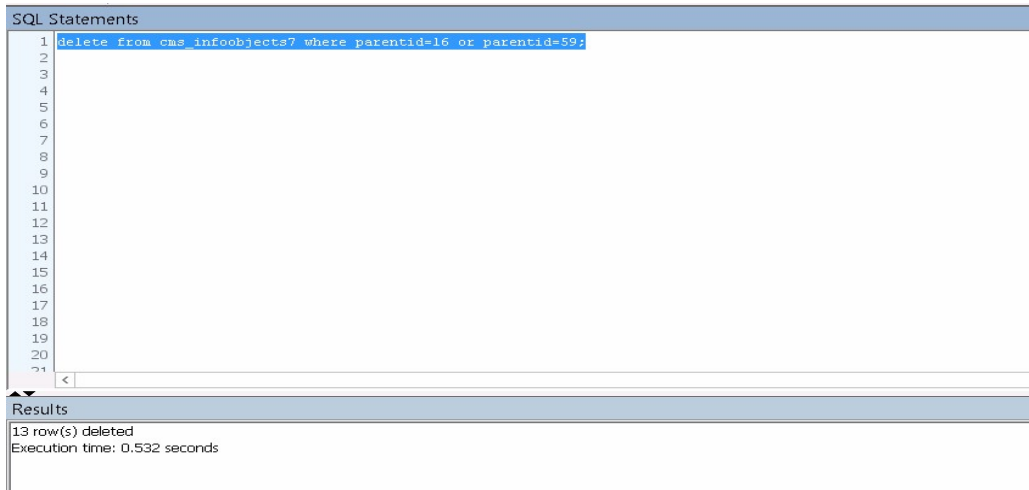
- o Click **Connect**.



12. In the SQL Statements pane, type the following query:

```
delete from cms_infoobjects7 where parentid=16 or parentid=59;
```


13. Click **Execute**. You will get a message that displays the number of records deleted as shown in the following image.

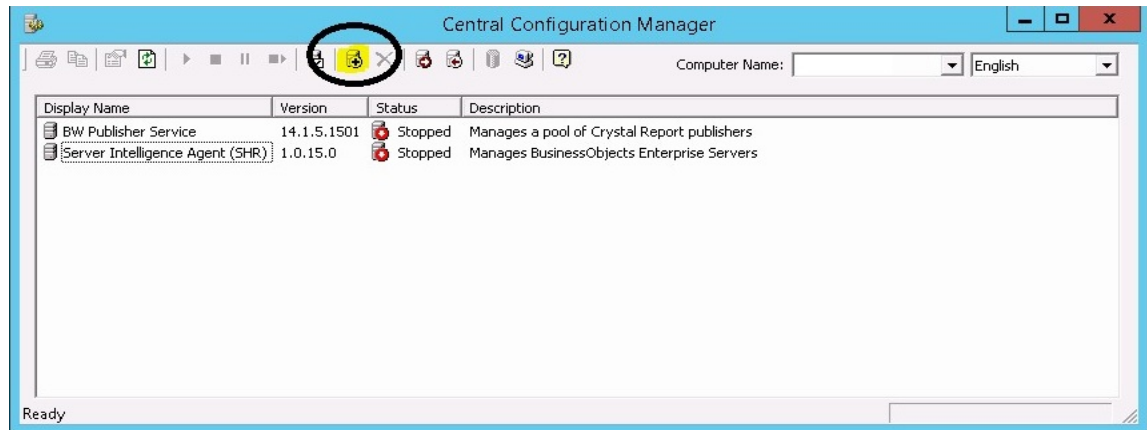


14. Commit the query execution and close the Connect to SQL Anywhere window.
15. Create a new SIA:

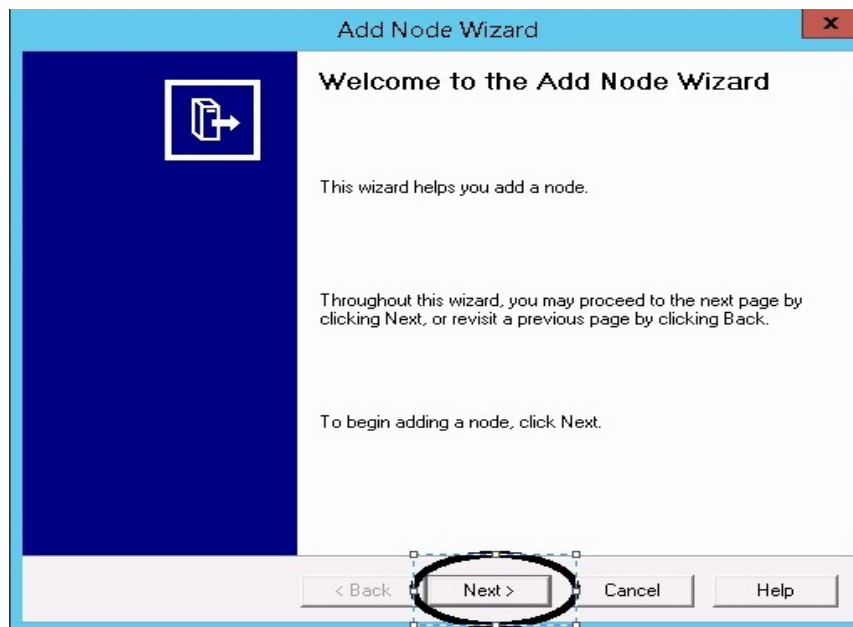
Note: Ensure that the SIA is not started before moving ahead.

- a. Go to **Start** and type **Central Configuration Manager** in **Search**. Double-click on the Central Configuration Manager to open it.

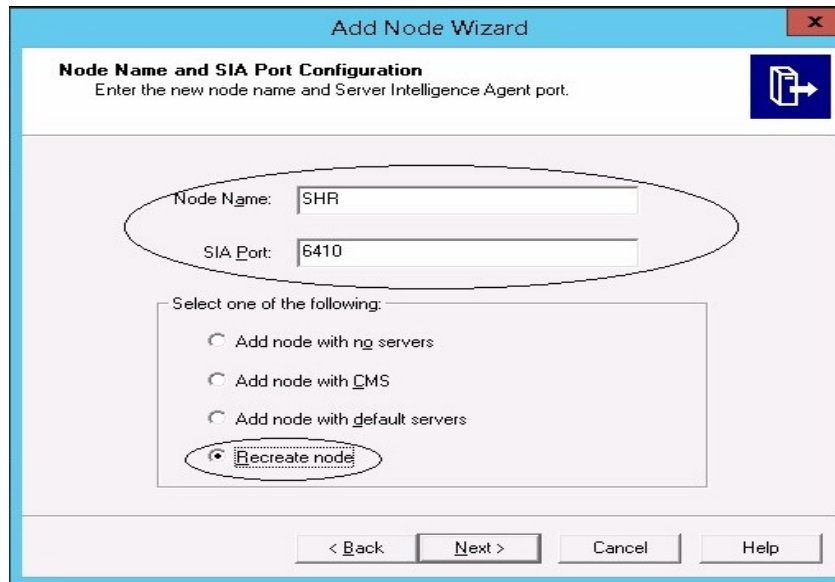
- b. Click on  to create a new SIA node. The Add Node Wizard appears.



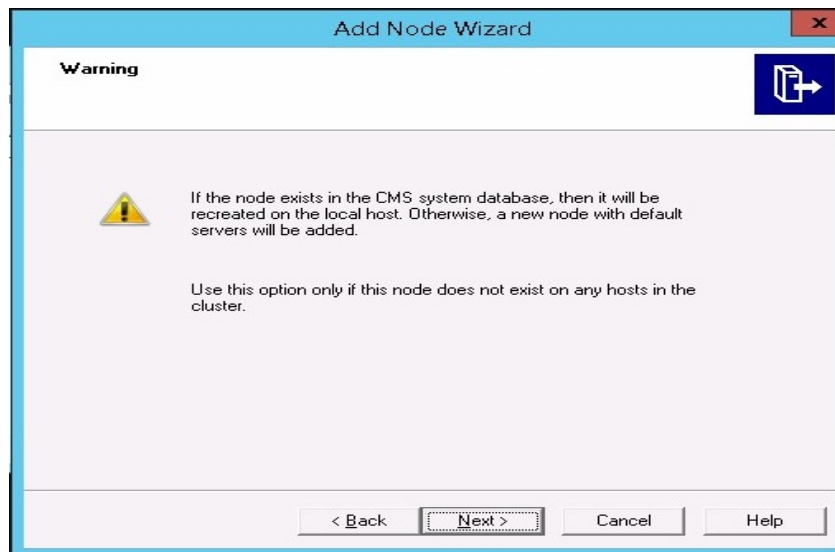
- c. Click **Next**. The Node name and SIA Port Configuration page appears.



- d. Type the following details:
- Node Name:
 - SIA Port: 6410
 - Select the **Recreate Node** option.
 - Click **Next**.

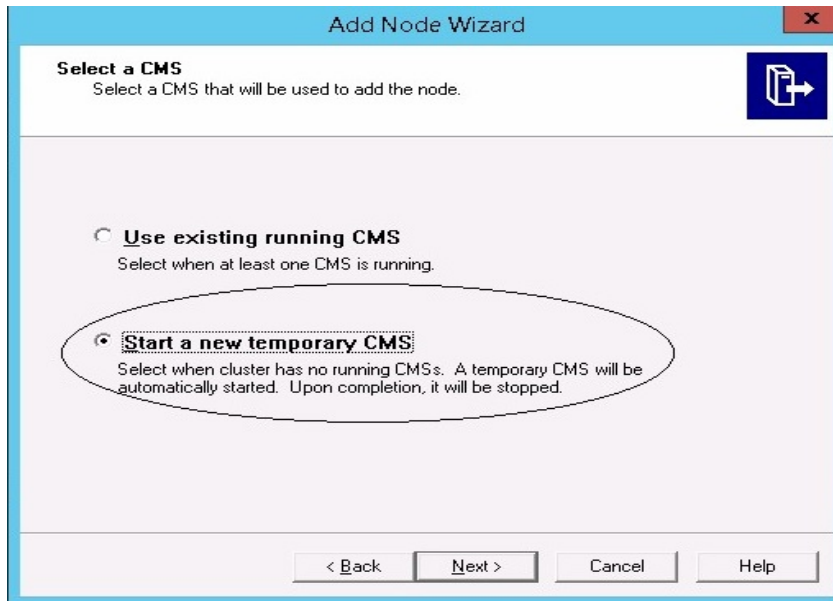


- e. A warning message appears as shown in the following image. Click **Next**.



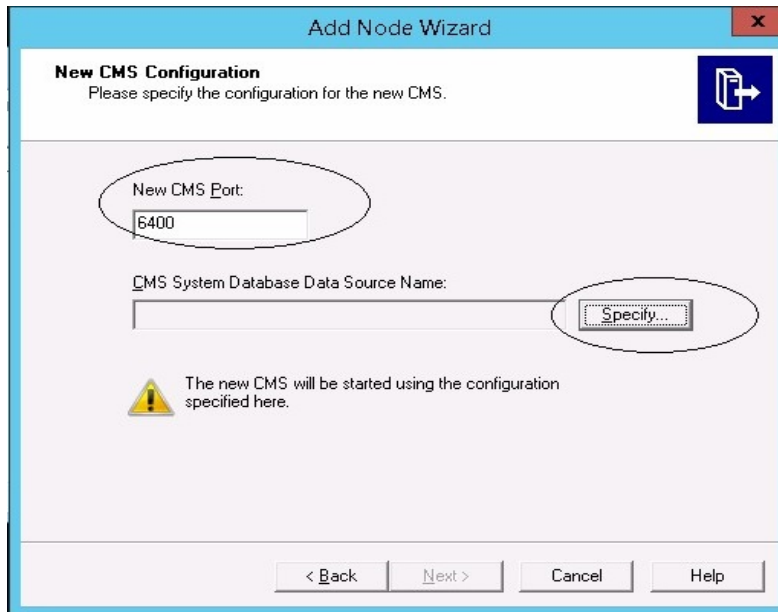
The Select a CMS page appears.

- f. Select **Start a new temporary CMS** option and click **Next**.

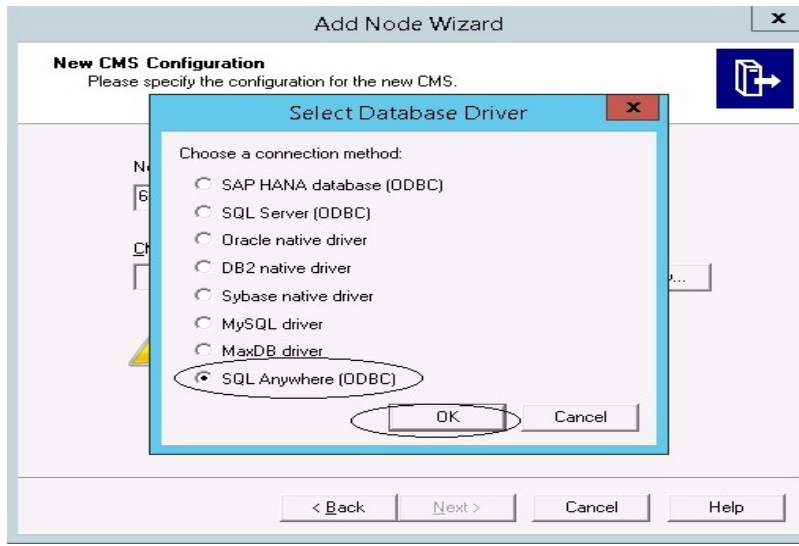


The New CMS Configuration page appears.

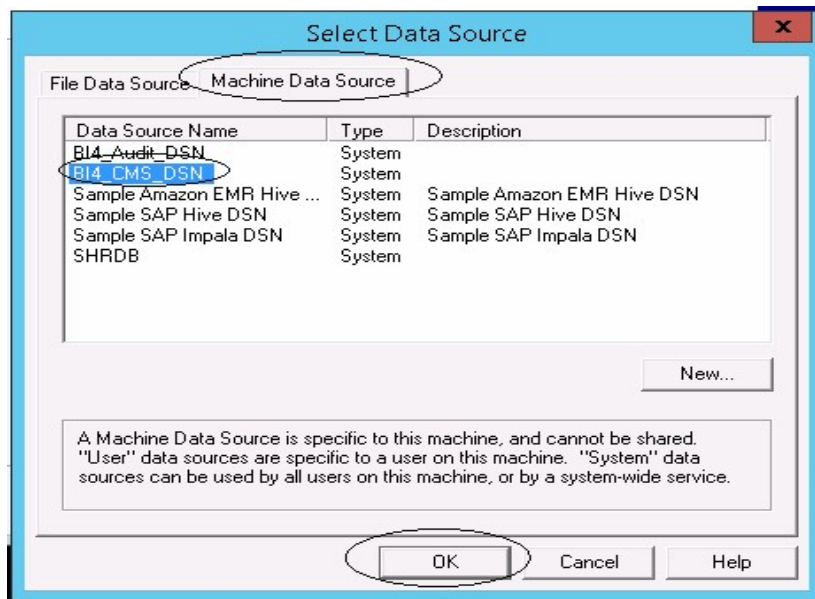
- g. Type 6400 for **New CMS Port**, and click on **Specify**.



- h. Select **SQL Anywhere (ODBC)** option in Select Database Driver page, and click **OK**.



- i. In Select Data Source page, click the **Machine Data Source** tab, and select **BI4_CMS_DSN**. Click **OK**.



- j. In Connect to SQL Anywhere wizard, type the following:

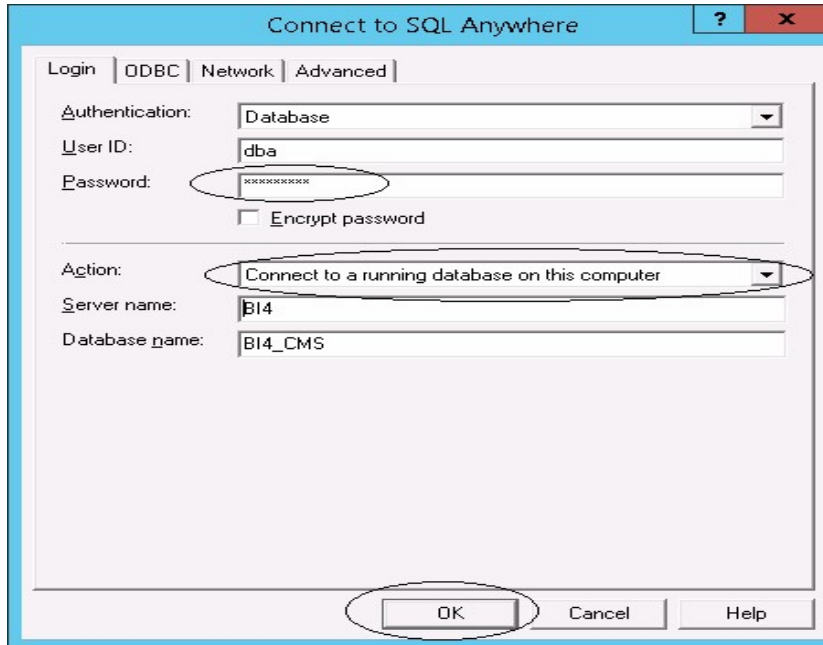
- User ID: dba
- Password: <password>

where, <password> is the password used to log on to the CMC database (SQL Anywhere)

Note: If you have not changed the password in the server where the back up is taken, type the same password else, type the changed password.

Caution: Ensure that you change the default password before you start using OBR. For more information, refer *Changing Default Passwords* in the *Operations Bridge Reporter Online help for Administrators*.

- Action: Select the **Connect to a running database on this computer** option. Click **OK**.

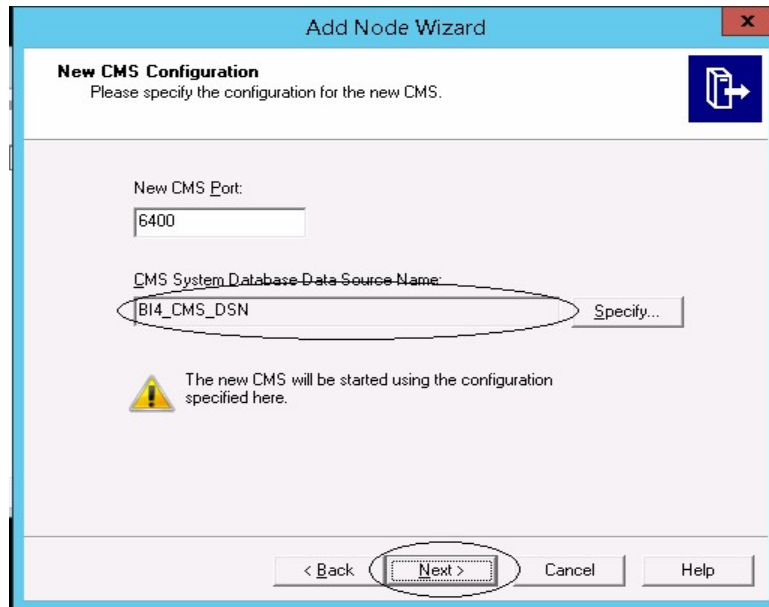


- k. In Specify Cluster Key page, type the cluster key as 1ShrAdmin. Click **OK**.

Note: The default cluster key is 1ShrAdmin, if you have changed the cluster key then enter the changed cluster key value.



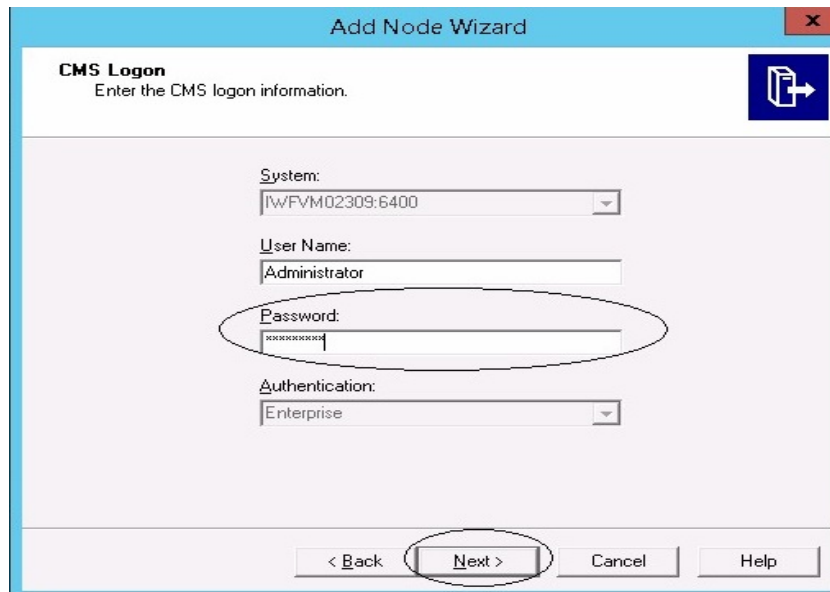
- l. The **CMS System Database Data Source name** will now be enabled in New CMS Configuration page. Click **Next**.



- m. Type the **Password** for the CMS Logon page, and click **Next**.

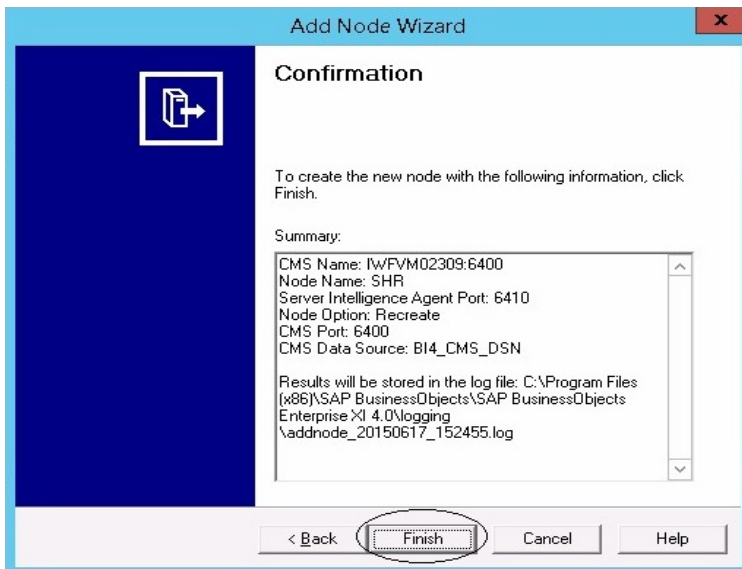
Note: If you have not changed the password in the server where the back up is taken, type the same password else, type the changed password.

Caution: Ensure that you change the default password before you start using OBR. For more information, refer *Changing Default Passwords* in the *Operations Bridge Reporter Online help for Administrators*.

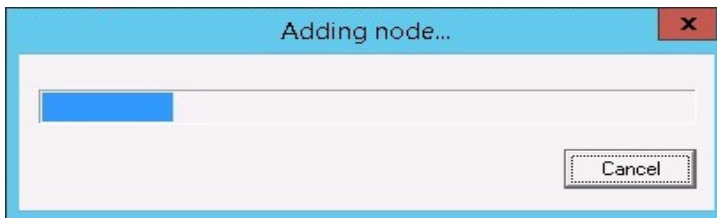


The Confirmation page appears.

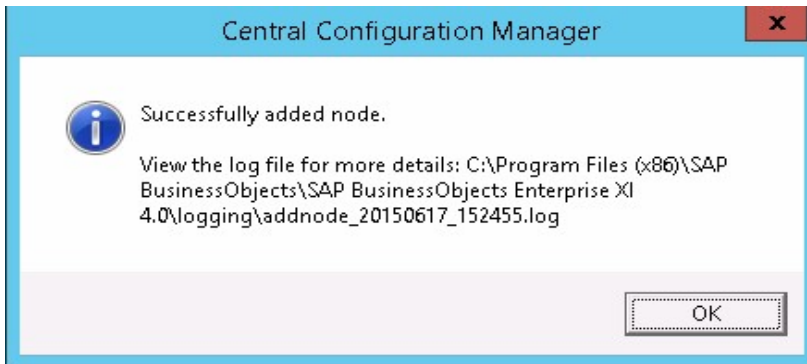
- n. Click **Finish**.



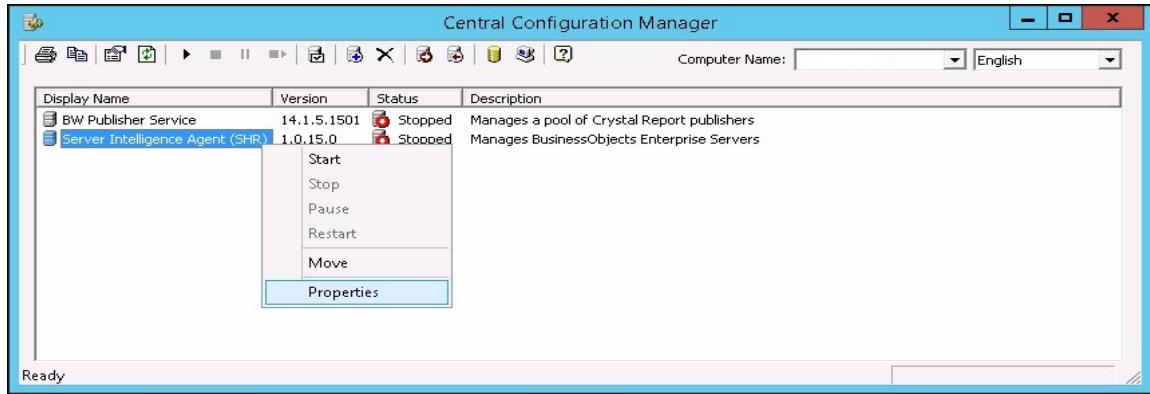
The Adding node... dialog box appears. Wait till the process gets completed.



A confirmation dialog appears as shown in the following image:



- o. In CCM, right-click on **Server Intelligence Agent (SIA)** and select **Properties**.

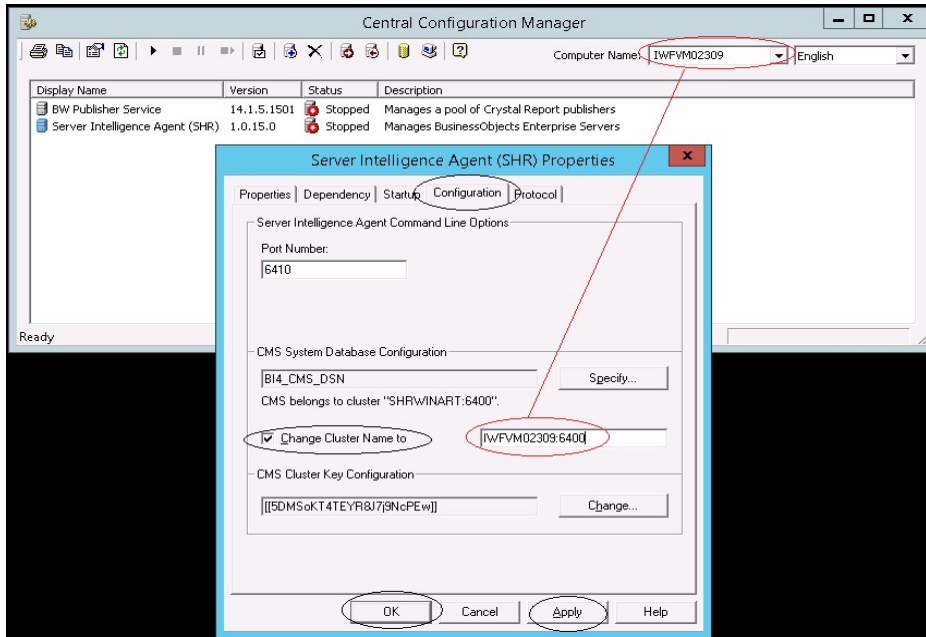


p. Select the **Configuration** tab and perform the following

- Select the **Change Cluster Name** to check box.
- Type the cluster name in the format `<Cluster Name>:6400`

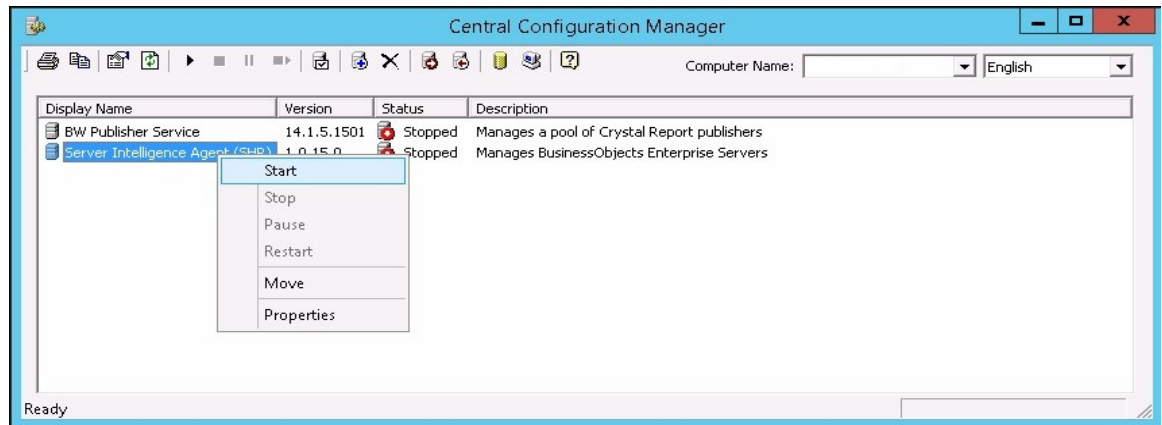
where, the `<Cluster Name>` is same as the **Computer Name** that appears in the Central Configuration Manager.

The following image shows the example for the Cluster Name:



- Click **Apply** and then click **OK**.

q. In CCM, right-click on **Server Intelligence Agent (SHR)** (SIA) and click **Start**.



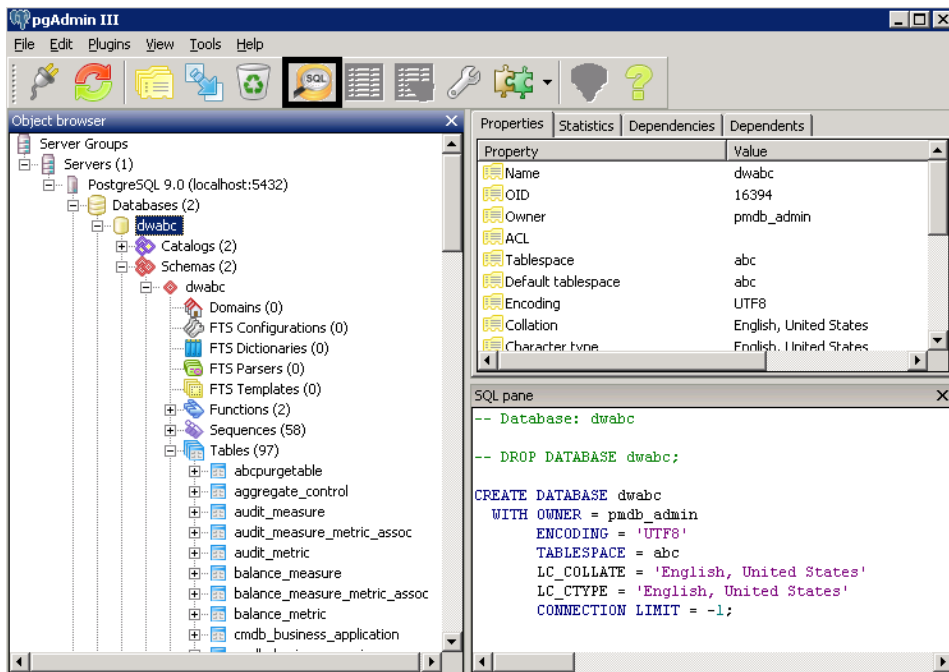
For Management Database Table

To restore the management database table, follow these steps:

1. Log on to the OBR system.
2. Go to **Start** and type **pgAdmin III** in **Search**. Double-click on the pgAdmin III to open it.
3. Connect to the database by providing the password. Launch the sql query analyzer by clicking the sql icon.

Note: If you have not changed the password in the server where the back up is taken, type the same password else, type the changed password.

Caution: Ensure that you change the default password before you start using OBR. For more information, refer *Changing Default Passwords* in the *Operations Bridge Reporter Online help for Administrators*.



- Run the following query to restore the database tables:

```
Delete From dwabc.aggregate_control
```

```
COPY dwabc.aggregate_control from '<Path of the backupfile>\\backup_AGGREGATE_
CONTROL.dat'
```

where, *<Path of the backupfile>* is the directory where you placed the Management database backup file.

For Example: COPY dwabc.aggregate_control from 'E:\SHR_DR_FullBackup\\backup_AGGREGATE_CONTROL.dat'

Restore Backup of OBR on Linux

For SAP BusinessObjects Database and File Store

Log on to the system where OBR is installed that is OBR server2 and follow these steps to restore the backup of the OBR components:

1. Copy the backup file SHR_DR_FULLBACKUP from the backup location of OBR server1 to OBR server2 where you want to restore the back up.

2. Log on to the system as root.

3. Run the following command to stop the web server:

```
sh /opt/HP/BSM/BOE4/sap_bobj/tomcatshutdown.sh
```

4. Move the SQL Anywhere Data Base files in OBR server2 from the following location to another location of your choice

```
$PMDB_HOME/./BOE4/sqlanywhere/database/*BI4*
```

Similarly, from the following location rename the frsinput and frsoutput directories

```
$PMDB_HOME/./BOE4/sap_bobj/data
```

5. Switch to the SAP BusinessObjects administrator by running the following command:

```
su - shrboadmin
```

6. Run the following command to stop all Server Intelligence Agent servers:

```
sh $PMDB_HOME/./BOE4/sap_bobj/stopservers
```

7. Stop the SQL Anywhere service:

```
sh $PMDB_HOME/./BOE4/sap_bobj/sqlanywhere_shutdown.sh
```

If prompted for password, specify the SQL Anywhere database password.

8. Switch back to root by running the following command:

```
exit
```

9. Copy the backup files (that you have taken a back up in the chapter *Back up OBR Database* "Create Full Backup of OBR on Linux" on page 234) perform the following:

```
perl <location of the restore script><location of the backup file>
```

where, <location of the restore script> is the path of the restore script, and <location of the backup file> is the path of the particular day's backup file that you want to restore.

For example: perl \$PMDB_HOME/DR/SHR_full_Restore.pl /root/SHR_DR_FullBackup/Thu

10. Run the following command:

```
chown shrboadmin:shrboadmin $PMDB_HOME/./BOE4/sqlanywhere/database/*BI4*
```

11. Ensure that you log in as shrboadmin user and not root.

```
su - shrboadmin
```

12. Start the SQL Anywhere service. Execute the following command to start SQL Anywhere.

```
sh $PMDB_HOME/./BOE4/sap_bobj/sqlanywhere_startup.sh
```

13. Go to the location `/opt/HP/BSM/BOE4/sap_bobj/enterprise_xi40/odbc.ini` and note down the ODBC Data Source name of the CMS database.

For example the ODBC Data Source name of the CMS database in the following image is BI4_CMS_DSN_1435083599

```
[ODBC Data Sources]
BI4_CMS_DSN_1435083599=SQLAnywhere 12.0
BI4_Audit_DSN_1435083599=SQLAnywhere 12.0

[BI4_CMS_DSN_1435083599]
UID=dba
DatabaseName=BI4_CMS
ServerName=BI4_1435083599
Host=localhost:2638
Driver=/opt/HP/BSM/BOE4/sqlanywhere/lib64/libdbodbc12.so

[BI4_Audit_DSN_1435083599]
UID=dba
DatabaseName=BI4_Audit
ServerName=BI4_1435083599
Host=localhost:2638
Driver=/opt/HP/BSM/BOE4/sqlanywhere/lib64/libdbodbc12.so
```

14. Create a new Server Intelligence Agent by running the following command:

```
sh $PMDB_HOME/./BOE4/sap_bobj/serverconfig.sh
```

The SAP BusinessObjects wizard appears in the command line console.

15. Type 1, and then press **Enter**.

```
-----  
SAP BusinessObjects  
What do you want to do?  
1 - Add node  
2 - Delete node  
3 - Modify node  
4 - Move node  
5 - Back up server configuration  
6 - Restore server configuration  
7 - Modify web tier configuration  
8 - List all nodes  
  
[quit(0)]  
-----  
[8]1
```

16. Type the name of the new Node, and then press **Enter**.

```
-----  
SAP BusinessObjects  
  
* Node Configuration *  
Enter the name of the new node.  
  
[back(1)/quit(0)]  
-----  
[IWFVM02570]SHRM2
```

17. Type 6410 as the port number, and then press **Enter**.

```
-----  
SAP BusinessObjects  
  
* Node Configuration *  
Enter the port of the new Server Intelligence Agent.  
  
[back(1)/quit(0)]  
-----  
[ ]6410
```

18. Type 3 (default server) to add node with default server, and then press **Enter**.

```
-----  
SAP BusinessObjects  
  
* Node Configuration *  
  
Select one of the following:  
  
no servers (Add node with no servers)  
cms (Add node with CMS)  
default servers (Add node with default servers)  
recreate (Recreate node)  
  
[no servers(5)/cms(4)/default servers(3)/recreate(2)/back(1)/quit(0)]  
-----  
  
[no servers]3
```

19. Type 2 to select a temporary CMS, and then press **Enter**.

```
-----  
SAP BusinessObjects  
  
* Select a CMS *  
  
Select a CMS that will be used to add the node.  
  
existing  
  (Select when at least one CMS is running.)  
temporary  
  (Select when cluster has no running CMSs. A temporary CMS will be automatically started. Upon completion, it will be stopped.)  
  
[existing(3)/temporary(2)/back(1)/quit(0)]  
-----  
  
[existing]2
```

20. Type 6400 for the CMS port number, and then press **Enter**.

```
-----  
SAP BusinessObjects  
  
* New OMS Configuration *  
Enter the port of the new OMS.  
  
Warning: The new OMS will start using the configuration specified here.  
  
[back(1)/quit(0)]  
-----  
[default (6400)]6400
```

21. Type 2 for SQL Anywhere, and then press **Enter**.

```
-----  
SAP BusinessObjects  
  
* New OMS Configuration *  
Specify new OMS 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
```

22. Enter the ODBC data source name that you have noted down earlier in [step 12](#), and then press **Enter**.

```
-----  
SAP BusinessObjects  
  
* New OMS Configuration *  
Specify new OMS database connection information.  
  
Enter the ODBC data source name (DSN) for connecting to your SQL Anywhere database.  
  
[back(1)/quit(0)]  
-----  
[BI4_OMS_DSN_1434393679]
```

23. Type the user name, and then press **Enter**.

Note: This must be the same user name that is used in the SAP BusinessObjects Server from where the back up is taken.

```
-----  
SAP BusinessObjects  
  
* New OMS Configuration *  
Specify new OMS database connection information.  
  
Enter the user name for connecting to your SQLAnywhere database.  
  
[back(1)/quit(0)]  
-----  
[dba]dba
```

24. Type the password, and then press **Enter**.

Note: If you have not changed the password in the server where the back up is taken, type the same password else, type the changed password.

Caution: Ensure that you change the default password before you start using OBR. For more information, refer *Changing Default Passwords* in the *Operations Bridge Reporter Online help for Administrators*.


```
-----  
SAP BusinessObjects  
  
* New CMS Configuration *  
Specify new CMS database connection information.  
  
Enter the password for connecting to your SQLAnywhere database.  
  
[back(1)/quit(0)]  
-----  
[]
```

25. Type the cluster key, and the press **Enter**.

Note: The default cluster key is 1ShrAdmin, if you have changed the cluster key then enter the changed cluster key value.

```
-----  
SAP BusinessObjects  
  
* New CMS Configuration *  
Enter the cluster key.  
  
[back(1)/quit(0)]  
-----  
[]
```

26. Type Administrator as the user name to connect to the CMS, and press **Enter**.

```
-----  
SAP BusinessObjects  
  
* OMS Logon *  
Enter the user name to connect to this OMS.  
Note that only Enterprise authentication is supported.  
  
[back(1)/quit(0)]  
-----  
[Administrator]█
```

27. Type the password, and then press **Enter**.

Note: If you have not changed the password in the server where the back up is taken, type the same password else, type the changed password.

Caution: Ensure that you change the default password before you start using OBR. For more information, refer *Changing Default Passwords* in the *Operations Bridge Reporter Online help for Administrators*.

```
-----  
SAP BusinessObjects  
  
* OMS Logon *  
Enter the password to connect to this OMS.  
  
[back(1)/quit(0)]  
-----  
[ ]█
```

28. Type yes to add a new node, and then press **Enter**.

```
-----  
SAP BusinessObjects  
  
* Confirmation *  
  
The following information will be used to create the new node.  
  
CMS Name: IWFVM02570:6400  
Node Name: SHRM2  
Server Intelligence Agent Port: 6410  
Node Option: Create default servers  
CMS Port: 6400  
CMS Data Source: BI4_CMS_DSN_1434393679  
  
Results will be stored in the log file: /opt/HP/BSM/BOE4/sap_bobj//logging/addnode_20150616_224929.log  
  
Do you want to create the node?  
  
[yes(3)/no(2)/back(1)/quit(0)]  
-----  
[yes]
```

The Confirmation screen for adding a node appears.

```
-----  
SAP BusinessObjects  
  
* Confirmation *  
  
The following information will be used to create the new node.  
  
CMS Name: IWFVM02570:6400  
Node Name: SHRM2  
Server Intelligence Agent Port: 6410  
Node Option: Create default servers  
CMS Port: 6400  
CMS Data Source: BI4_CMS_DSN_1434393679  
  
Results will be stored in the log file: /opt/HP/BSM/BOE4/sap_bobj//logging/addnode_20150616_224929.log  
  
Do you want to create the node?  
  
[yes(3)/no(2)/back(1)/quit(0)]  
-----  
[yes]  
Adding node...  
█
```

29. Press **Enter** to continue.

```
-----  
SAP BusinessObjects  
  
* Confirmation *  
  
The following information will be used to create the new node.  
  
OVS Name: IMFVM02570:6400  
Node Name: SHRM2  
Server Intelligence Agent Port: 6410  
Node Option: Create default servers  
OVS Port: 6400  
OVS Data Source: BI4_OVS_DSN_1434393679  
  
Results will be stored in the log file: /opt/HP/BSW/BCE4/sap_bobj//logging/addnode_20150616_224929.log  
  
Do you want to create the node?  
  
[yes(3)/no(2)/back(1)/quit(0)]  
-----  
  
[yes]  
Adding node...  
.....Successfully added node.  
View the log file for more details: /opt/HP/BSW/BCE4/sap_bobj//logging/addnode_20150616_224929.log  
  
Press Enter to continue...  
█
```

30. Type 0 to quit, and then press **Enter**.

```
-----  
SAP BusinessObjects  
  
What do you want to do?  
  
1 - Add node  
2 - Delete node  
3 - Modify node  
4 - Move node  
5 - Back up server configuration  
6 - Restore server configuration  
7 - Modify web tier configuration  
8 - List all nodes  
  
[quit(0)]  
-----  
  
[8]0█
```

31. Type 1 to confirm quit, and then press **Enter**.

```
-----  
SAP BusinessObjects  
  
Are you sure you want to quit?  
  
[yes(1)/no(0)]  
-----  
  
[no]1█
```

32. Take a back up of /opt/HP/BSM/BOE4/sap_bobj/ccm.config
33. Remove/ Delete the SHRLAUNCH section as shown in the following image:

```
#!/bin/sh
BOBJDIR="/opt/HP/BSM/BOE4/sap_bobj/"
BOBJDIRALLLOCAL="user"
BOBJTLA="en"
BOBJTELSEBEN="bc00U-1MVE5M-710XJ4-Gb200AC-7b"
BOBJTELSEBEN="shrbodmin"
BOBJVERSIO="XI_4_0"
CLUSTER_NAME_SERVER=""
CLUSTER_PORT_NUMBER="6400"
CNS_CLUSTER="no"
CNS_NAME_SERVER="DVPM02570"
CNS_PORT_NUMBER="6400"
CNS_SELECTOR="8080"
CNS_DATABASE="die"
DBTYPE_AU="sqlanywhere"
DBTYPE="sqlanywhere"
DEFAULT_NAME_SERVER="no"
INSTALL_DIR="/opt/HP/BSM/BOE4/sap_bobj/"
LOCAL_NAME_SERVER="DVPM02570"
NAME_SERVER="DVPM02570"
PIDDIR="/opt/HP/BSM/BOE4/sap_bobj/serverpids/"
PRODUCT_ID_NAME="BusinessObjects"
PRODUCT_ID_VER="14_0"
REBJRECTPORT="8443"
REGFILE="/opt/HP/BSM/BOE4/sap_bobj/data/.bobj"
REJIND="yes"
SERVCEUWE_AU="BI4_Audit"
SERVCEUWE="BI4_OMS"
SERVCEFOR="no"
SHUTDOWNPORT="8005"
SI#CDEUWE="SHR"
SI#PORTNUMBER="6410"
SI#ModeVal="undefined"
SHRLAUNCH="/opt/HP/BSM/BOE4/sap_bobj/enterprise_xi40/generic/bobjrestart.sh" -protect "/opt/HP/BSM/BOE4/sap_bobj/enterprise_xi40/generic/java launch.sh" "-bb
obj_product_languages_dirs/opt/HP/BSM/BOE4/sap_bobj/enterprise_xi40/Languages/" -djava.net.preferIPv4Stack=false -djava.ext.headless=true -bcsm.sap.vw.tag=SHR
M64M "-Xms256m" "-Xmx256m" "-XX:+ExitVMOnOutOfMemoryError" "-XX:+HeapDumpOnOutOfMemoryError" "-XX:+PrintGCHeapStops" "-XX:+PrintGCDateTis" "-XX:LogGCMaxFileCounts=3"
"-XX:LogGCMaxFileSize=5m" "-XX:HeapDumpPath=/opt/HP/BSM/BOE4/sap_bobj/logging/" "-XtraceFiles=/opt/HP/BSM/BOE4/sap_bobj/logging/SHR_jvm.SPID.log" "-XX:GCHistoryF
ilename=/opt/HP/BSM/BOE4/sap_bobj/logging/SHR_gc.prf" "-Xloggc:/opt/HP/BSM/BOE4/sap_bobj/logging/SHR_gc.log" "-XX:ErrorFiles=/opt/HP/BSM/BOE4/sap_bobj/logging/S
HR_dump.SPID.log" -jar "/opt/HP/BSM/BOE4/sap_bobj/enterprise_xi40/java/lib/SIA.jar" -boot "/opt/HP/BSM/BOE4/sap_bobj/enterprise_xi40/linux_x64/_boe_SHR_bootsnp
sp" -port "6410" -pidfile "/opt/HP/BSM/BOE4/sap_bobj/serverpids/SHR.pid" -loggingPath "/opt/HP/BSM/BOE4/sap_bobj/logging/" -traceInPath "/opt/HP/BSM/BOE4/sap
_bobj/enterprise_xi40/conf/BO_trace.in" -name "SHR" -dbinfo "/opt/HP/BSM/BOE4/sap_bobj/enterprise_xi40/linux_x64/_boe_SHR.dbinfo" -piddir "/opt/HP/BSM/BOE4/sap
_bobj/serverpids/" -noauditor
SHRLAUNCH="/opt/HP/BSM/BOE4/sap_bobj/enterprise_xi40/generic/bobjrestart.sh" -protect "/opt/HP/BSM/BOE4/sap_bobj/enterprise_xi40/generic/java launch.sh" "-bb
obj_product_languages_dirs/opt/HP/BSM/BOE4/sap_bobj/enterprise_xi40/Languages/" -djava.net.preferIPv4Stack=false -djava.ext.headless=true -bcsm.sap.vw.tag=SHRM
2 "-Xms256m" "-Xmx256m" "-XX:+ExitVMOnOutOfMemoryError" "-XX:+HeapDumpOnOutOfMemoryError" "-XX:+PrintGCHeapStops" "-XX:+PrintGCDateTis" "-XX:LogGCMaxFileCounts=3"
"-XX:LogGCMaxFileSize=5m" "-XX:HeapDumpPath=/opt/HP/BSM/BOE4/sap_bobj/logging/" "-XtraceFiles=/opt/HP/BSM/BOE4/sap_bobj/logging/SHRM2_jvm.SPID.log" "-XX:GCHistoryF
ilename=/opt/HP/BSM/BOE4/sap_bobj/logging/SHRM2_gc.prf" "-Xloggc:/opt/HP/BSM/BOE4/sap_bobj/logging/SHRM2_gc.log" "-XX:ErrorFiles=/opt/HP/BSM/BOE4/sap_bobj
/logging/SHRM2_dump.SPID.log" -jar "/opt/HP/BSM/BOE4/sap_bobj/enterprise_xi40/java/lib/SIA.jar" -boot "/opt/HP/BSM/BOE4/sap_bobj/enterprise_xi40/linux_x64/_boe
SHRM2_bootsnp" -port "6410" -pidfile "/opt/HP/BSM/BOE4/sap_bobj/serverpids/SHRM2.pid" -loggingPath "/opt/HP/BSM/BOE4/sap_bobj/logging/" -traceInPath "/opt/
HP/BSM/BOE4/sap_bobj/enterprise_xi40/conf/BO_trace.in" -name "SHRM2" -dbinfo "/opt/HP/BSM/BOE4/sap_bobj/enterprise_xi40/linux_x64/_boe_SHRM2.dbinfo" -piddir "/
opt/HP/BSM/BOE4/sap_bobj/serverpids/" -noauditor
```

Remove the below marked line

34. After removing/ deleting SHRLAUNCH section, save the file as shown in the following image:

```
#!/bin/sh
BOBJDIR="/opt/HP/BSM/BOE4/sap_bobj/"
BOBJDIRALLLOCAL="user"
BOBJTLA="en"
BOBJTELSEBEN="bc00U-1MVE5M-710XJ4-Gb200AC-7b"
BOBJTELSEBEN="shrbodmin"
BOBJVERSIO="XI_4_0"
CLUSTER_NAME_SERVER=""
CLUSTER_PORT_NUMBER="6400"
CNS_CLUSTER="no"
CNS_NAME_SERVER="DVPM02570"
CNS_PORT_NUMBER="6400"
CNS_SELECTOR="8080"
CNS_DATABASE="die"
DBTYPE_AU="sqlanywhere"
DBTYPE="sqlanywhere"
DEFAULT_NAME_SERVER="no"
INSTALL_DIR="/opt/HP/BSM/BOE4/sap_bobj/"
LOCAL_NAME_SERVER="DVPM02570"
NAME_SERVER="DVPM02570"
PIDDIR="/opt/HP/BSM/BOE4/sap_bobj/serverpids/"
PRODUCT_ID_NAME="BusinessObjects"
PRODUCT_ID_VER="14_0"
REBJRECTPORT="8443"
REGFILE="/opt/HP/BSM/BOE4/sap_bobj/data/.bobj"
REJIND="yes"
SERVCEUWE_AU="BI4_Audit"
SERVCEUWE="BI4_OMS"
SERVCEFOR="no"
SHUTDOWNPORT="8005"
SI#CDEUWE="SHR"
SI#PORTNUMBER="6410"
SI#ModeVal="undefined"
SHRLAUNCH="/opt/HP/BSM/BOE4/sap_bobj/enterprise_xi40/generic/bobjrestart.sh" -protect "/opt/HP/BSM/BOE4/sap_bobj/enterprise_xi40/generic/java launch.sh" "-bb
obj_product_languages_dirs/opt/HP/BSM/BOE4/sap_bobj/enterprise_xi40/Languages/" -djava.net.preferIPv4Stack=false -djava.ext.headless=true -bcsm.sap.vw.tag=SHRM
2 "-Xms256m" "-Xmx256m" "-XX:+ExitVMOnOutOfMemoryError" "-XX:+HeapDumpOnOutOfMemoryError" "-XX:+PrintGCHeapStops" "-XX:+PrintGCDateTis" "-XX:LogGCMaxFileCounts=3"
"-XX:LogGCMaxFileSize=5m" "-XX:HeapDumpPath=/opt/HP/BSM/BOE4/sap_bobj/logging/" "-XtraceFiles=/opt/HP/BSM/BOE4/sap_bobj/logging/SHRM2_jvm.SPID.log" "-XX:GCHistoryF
ilename=/opt/HP/BSM/BOE4/sap_bobj/logging/SHRM2_gc.prf" "-Xloggc:/opt/HP/BSM/BOE4/sap_bobj/logging/SHRM2_gc.log" "-XX:ErrorFiles=/opt/HP/BSM/BOE4/sap_bobj
/logging/SHRM2_dump.SPID.log" -jar "/opt/HP/BSM/BOE4/sap_bobj/enterprise_xi40/java/lib/SIA.jar" -boot "/opt/HP/BSM/BOE4/sap_bobj/enterprise_xi40/linux_x64/_boe
SHRM2_bootsnp" -port "6410" -pidfile "/opt/HP/BSM/BOE4/sap_bobj/serverpids/SHRM2.pid" -loggingPath "/opt/HP/BSM/BOE4/sap_bobj/logging/" -traceInPath "/opt/
HP/BSM/BOE4/sap_bobj/enterprise_xi40/conf/BO_trace.in" -name "SHRM2" -dbinfo "/opt/HP/BSM/BOE4/sap_bobj/enterprise_xi40/linux_x64/_boe_SHRM2.dbinfo" -piddir "/
opt/HP/BSM/BOE4/sap_bobj/serverpids/" -noauditor
```

35. Run the following command to start all Server Intelligence Agent servers:

```
/opt/HP/BSM/BOE4/sap_bobj/startservers
```

36. Run the following commands:

```
cd /etc/initd
```

- a. **On RHEL 6.x/SUSE Linux Enterprise Server 11:**

```
service SAPBOBJEnterpriseXI40 stop
```

```
service SAPBOBJEnterpriseXI40 start
```

- b. **On RHEL 7.x:**

```
systemctl stop SAPBOBJEnterpriseXI40.service
```

```
systemctl start SAPBOBJEnterpriseXI40.service
```

For Management Database Table

To restore the management database table, follow these steps:

1. Run the following commands to launch PgAdminIII:

- a. `cd $PMDB_HOME/./Postgres/bin`

- b. `./psql -U pmdb_admin -d dwabc -p 21425`

2. Connect to the database by providing the same password which was configured during post installation.
3. Launch the sql query analyzer.

Note: You must ensure that all the folders in the backup folder path have read permissions for all users.

4. Run the following query to restore the database tables:

```
Delete from aggregate_control
```

```
COPY aggregate_control from '<backup_path>/Mgmt_backup_AGGREGATE_CONTROL.dat';
```

In this instance, *<backup_path>* is the directory where you placed the Management database backup file.

For example: `COPY dwabc.aggregate_control from '/root/SHR_DR_FullBackup/SHR_DR_FullBackup/Thu/Full_MgmtDB_BackUP/Mgmt_backup_AGGREGATE_CONTROL.dat';`

Back up and Restore Vertica Database

OBR uses Vertica database for storing, processing, and managing the performance data of your IT environment. You must take a regular backup of Vertica database along with the other OBR database files.

For Vertica backup and restore documentation, see [Vertica Backup and Restore](#).

Points to note:

1. To start the Vertica database backup, log on as *<Vertica Database Administrator>* (For example, verticadba) in SSH.

```
su - verticadba
```

2. To create vbr.py configuration files, run the `/opt/vertica/bin/vbr.py -setupconfig` command from the directory where the *<Vertica Database Administrator>* user (For example, verticadba) has read-write access.

For example, `cd /home/verticadba`

```
/opt/vertica/bin/vbr.py -setupconfig
```

After you restore the Vertica database backup successfully, bring the Vertica database up.

Part V: Appendix

This section lists the SiteScope monitors that are used to collect the virtualization metrics and also provides information to install Xcelsius application. Also, this section lists the services in OBR and the steps to start and stop these services on Red Hat Enterprise Linux (RHEL) 6.x and 7.x versions supported by OBR.

Appendix A: Topology Source Migration (OM to OMi)

Operations Bridge Reporter (OBR) fetches conformed dimensions from the topology source configured in OBR. After collecting data from a topology source instance, if the user modifies the topology source instance, the CIID of the dimensions changes. This change results in duplicate dimensions in the data warehouse. So, OBR does not allow changing the topology source once configured. But, when a customer migrate from Operations Manager (OM) to Operations Manager i (OMi), there is a need to change the topology source from OM to OMi in OBR.

This document captures the approach to modify the topology source from OM to OMi in OBR. This document contains the following information:

- ["Prerequisites" below](#)
- ["Topology Migration Steps" on the next page](#)
- ["Points to Note" on page 269](#)
- ["Limitations" on page 269](#)
- ["Topology Source Migration FAQs" on page 271](#)

Prerequisites

1. Ensure that the collector service `HPE_PMDB_Platform_Collection` is stopped on OBR system and Remote Collector systems (if remote collector is configured).
2. Wait until all the data flow from the OM datasource is processed and the folders other than archive folder do not have files. Ensure that the following folders are empty:
 - `{PMDB_HOME}\extract`
 - `{PMDB_HOME}\extract\extract\temp`
 - `{PMDB_HOME}\collect`
 - `{PMDB_HOME}\collect\temp`
 - `{PMDB_HOME}\collect\archive_download`
 - `{PMDB_HOME}\stage`

- {PMDB_HOME}\stage\failed_to_load
 - {PMDB_HOME}\stage\failed_to_reconcile
 - {PMDB_HOME}\stage\failed_to_stage
 - {PMDB_HOME}\stage\failed_to_transform
3. Ensure data from the stage tables has moved to the warehouse tables.
 4. Ensure OBR Vertica database backup is taken.

For more information, see *Operations Bridge Reporter Disaster Recovery Guide*.

5. Ensure OBR PostgreSQL Management database backup is taken.

Refer to the "[PostgreSQL Management DB Backup and Restore](#)" on page 270 section of this document for details.

6. Data from the old OM datasource has to be completely processed prior to initiating topology switch to OMi; else, it could result in older IDs getting loaded.

Note: To achieve step 2 and 3, stop the HPE_PMDB_Platform_Collection service and allow the following service to run for few hours so that all the collected data will be loaded to data warehouse:

- HPE_PMDB_Platform_Timer
- HPE _PMDB_Platform_JobManager
- HPE _PMDB_Platform_TaskManager
- HPE _PMDB_Platform_Orchestration

Topology Migration Steps

1. Topology Migration Precheck

Run the following command for topology migration precheck:

```
TopologyMigrationTool -precheck
```

In this step, the migration tool checks the following:

- **The HPE_PMDB_Platform_Collection service is stopped**

If the Collection service is running, the migration tool aborts with the following message:

PRECHECK FAILED: HPE_PMDB_Platform_Collection service is running. Please stop the HPE_PMDB_Platform_Collection service.

- **Files pending to be processed**

If there are files pending to be processed in the file system, the migration tool aborts with the following message:

PRECHECK FAILED: Files pending to be processed exists in PMDB extract, collect and stage directories. Please make sure no files exist pending to be processed.

- **Backup the reconcile_registry folder**

If the backup fails, the migration tool aborts with the following message:

PRECHECK FAILED: Could not back up reconcile_registry folder.

- **Stage tables contain no data**

If stage tables contain data, the migration tool aborts with the following message:

PRECHECK FAILED: Unprocessed data available in stage table.

- **Enter new OMi source details**

The migration tool prompts the user to enter the new OMi source details.

Note: If your OMi instance is HTTPS enabled, you need to configure CA certificate. For more information, refer to the *Configuring RTSM Topology Source* section in the *Operations Bridge Reporter Configuration Guide*.

- **Test connection for new OMi source.**

- **Check the status of all the OBR services.**

2. Generating the Mapping Files

Run the following command:

```
TopologyMigrationTool -migrate RTSM -generatemapping
```

In this step, the migration tool runs the precheck again and performs the following:

Topology Data Extract

The migration tool extracts the topology data.

Topology Management Database Update

The migration tool updates the Management Database (Postgre DB) with RTSM topology details.

Topology Build Registry

The migration tool builds the registry for the topology data.

Topology CIID Mapping Generator

The migration tool builds the CIID mapping of RTSM topology source and OM topology source and generates the mapping CSV files.

- The mapped CSV files are created in the `PMDB_HOME/csv/mappedcsvfolder`
- The unmapped CSV files are be created in `PMDB_HOME/csv/unmappedcsvfolder`.

Note: Unmapped CSV lists all the CI's which exist in the OM topology source which has not been synced in RTSM topology source. The unmapped CI's exist as is in the datawarehouse.

Topology Sync Data Source

In this step the migration tool syncs the Topology Data source to the available remote collectors.

3. Topology Invoke DLC

Run the following command:

```
TopologyMigrationTool -migrate RTSM - updatedb
```

In this step, the migration tool fetches the mapped CSV file and updates the Data ware house dimension tables with the RTSM CIID.

Topology Configuration Update

The migration tool updates the `config.prp` file with RTSM topology source configurations.

Start OBR Services

In this step the migration tool starts the below OBR services:

- `HPE_PMDB_Platform_Administrator`
- `HPE_PMDB_Platform_Collection`
- `HPE_PMDB_Platform_DB_Logger`

- HPE_PMDB_Platform_IM
- HPE_PMDB_Platform_JobManager
- HPE_PMDB_Platform_TaskManager
- HPE_PMDB_Platform_Orchestration
- HPE_PMDB_Platform_IA
- HPE_PMDB_Platform_NRT_ETL
- HPE_PMDB_Platform_Timer Service

Points to Note

1. If you are using OM content pack, switch to OMi event content pack according to your OMi version:

- CrossOprEvent_ETL_OMi10_Extended
- CrossOprEvent_ETL_OMi10x
- CrossOprEvent_ETL_OMi10
- CrossOprEvent_ETL_OMi
- CrossOprEvent_ETL_OMi_Extended
- CrossOprEvent_ETL_OMi10

For information about the latest content pack version available, refer to *OBR Content Packs Versions* document.

2. Ensure that you are using the appropriate version of Management Pack (MP)-based ETLs for Exchange/Weblogic ETLs.

For more information, refer to Oracle WebLogic Server Content Pack Reference and Microsoft Exchange Server Content Pack

Reference guides.

Limitations

Only the dimensions present in RTSM are migrated. If a dimension is not available in RTSM (dimension no longer exists in deployment), then the dimension continues to be available in OBR DATA

WAREHOUSE with previous CIID (CIID formed using OM topology source).

1. OA/PA data sources that are not available in RTSM will not be deleted in OBR management DB, but collection will be disabled for these data sources.
2. Node groups collected from OM will continue to exist in OBR and be present in reports (unless delete steps are explicitly run). Views will be added to group list post switch to OMi; node group/CI Collections are not collected from OMi.
3. OM Nodegroups will appear in report prompts post migration.

Download and install the VSQL client to run the queries listed here.

To clean up, run the below queries using the VSQL tool:

- Delete from K_CI_Group_Bridge where group_key in (Select dsi_key_id from K_group where type ='NODEGROUP')
- Delete from K_CI_Bridge where group_key in (Select dsi_key_id from K_group where type ='NODEGROUP')
- Delete from K_group where type='NODEGROUP'

PostgreSQL Management DB Backup and Restore

PostgreSQL Management DB backup

1. Open command prompt and navigate to {PMDB_HOME}/../ Postgres/bin directory.

Postgres directory is in the installed location of OBR.

Example: C:\HPE-OBR\Postgres\bin

2. Run the following command to take the backup:

```
pg_dump -h <hostname> -p 21425 -U pmdb_admin dwabc >c:\outfile.txt
```

Example: C:\HPE-OBR\Postgres\bin>pg_dump -h host001 -p 21425 -U pmdb_admin dwabc >c:\outfile.txt

Restore PostgreSQL Management DB

1. Open command prompt and navigate to {PMDB_HOME}/../Postgres/bin directory.

Postgres directory is in the installed location of OBR.

Example: C:\HPE-OBR\Postgres\bin

2. Run the following command to log on to psql:

```
psql -h <hostname> -p 21425 -U pmdb_admin dwabc
```

Example: C:\HPE-OBR\Postgres\bin>psql -h host001 -p 21425 -U pmdb_admin dwabc

3. Run the following command restore the database backup:

```
psql swayback < <absolute path of the backedup file name >
```

Example: psql dwabc < c:\outfile.txt

Note: Replace {PMDB_HOME} with

- %PMDB_HOME% for Windows
- \$PMDB_HOME for Linux

Topology Source Migration FAQs

1. What do I do if some rows from the old OM topology source are loaded?

Clean up the loaded rows using the DLC cleanup. For more information, see the *Managing Dimensions* section in the *Operations Bridge Reporter Administration Guide*.

Appendix B: Topology Source Migration (BSM to OMi)

OBR fetches conformed dimensions from the topology source configured. After collecting data from a topology source instance, if the user modifies the topology source instance, the CIID of the dimensions changes. This change results in duplicate dimensions in the data warehouse. So, OBR does not allow changing the topology source once configured. But, when a customer migrate from BSM to Operations Manager i (OMi), there is a need to change the topology source from BSM to OMi in OBR.

This section captures the approach to modify the topology source from BSM to OMi in OBR.

- ["Prerequisites" below](#)
- ["Topology Migration Steps" on the next page](#)
- ["Points to Note" on page 276](#)
- ["Limitations" on page 277](#)
- ["Topology Source Migration FAQs" on page 279](#)

Prerequisites

1. Ensure that the collector service `HPE_PMDB_Platform_Collection` is stopped on OBR system and Remote Collector systems (if remote collector is configured) .
2. Wait until all the data flow from the BSM datasource is processed and the folders other than archive folder do not have files. Ensure that the following folders are empty:
 - `{PMDB_HOME}\extract`
 - `{PMDB_HOME}\extract\extract\temp`
 - `{PMDB_HOME}\collect`
 - `{PMDB_HOME}\collect\temp`
 - `{PMDB_HOME}\collect\archive_download`
 - `{PMDB_HOME}\stage`
 - `{PMDB_HOME}\stage\failed_to_load`

- {PMDB_HOME}\stage\failed_to_reconcile
 - {PMDB_HOME}\stage\failed_to_stage
 - {PMDB_HOME}\stage\failed_to_transform
3. Ensure data from the stage tables has moved to the warehouse tables.
 4. Ensure OBR Vertica database backup is taken.

For more information, see *Operations Bridge Reporter Disaster Recovery Guide*.

5. Ensure OBR PostgreSQL Management database backup is taken.

Refer to the "[PostgreSQL Management DB Backup and Restore](#)" on page 278 section of this document for details.

6. Data from the old BSM datasource has to be completely processed prior to initiating topology switch to OMi; else, it may result in older IDs getting loaded.

Note: To achieve step 2 and 3, stop the HPE_PMDB_Platform_Collection service and allow the following service to run for few hours so that all the collected data will be loaded to data warehouse:

- HPE_PMDB_Platform_Timer
- HPE _PMDB_Platform_JobManager
- HPE _PMDB_Platform_TaskManager
- HPE _PMDB_Platform_Orchestration

Topology Migration Steps

1. Topology Migration Precheck

Run the following command for topology migration precheck:

```
TopologyMigrationTool -precheck
```

In this step, the migration tool checks the following:

- **The HPE_PMDB_Platform_Collection service is stopped**

If the Collection service is running, the migration tool aborts with the following message:

PRECHECK FAILED: HPE_PMDB_Platform_Collection service is running. Please stop the HPE_PMDB_Platform_Collection service.

- **Files pending to be processed**

If there are files pending to be processed in the file system, the migration tool aborts with the following message:

PRECHECK FAILED: Files pending to be processed exists in PMDB extract, collect and stage directories. Please make sure no files exist pending to be processed.

- **Backup the reconcile_registry folder**

If the backup fails, the migration tool aborts with the following message:

PRECHECK FAILED: Could not back up reconcile_registry folder.

- **Stage tables contain no data**

If stage tables contain data, the migration tool aborts with the following message:

PRECHECK FAILED: Unprocessed data available in stage table.

- **Enter new OMi source details**

The migration tool prompts the user to enter the new OMi source details.

Note: If your OMi instance is HTTPS enabled, you need to configure CA certificate. For more information, refer to the *Configuring RTSM Topology Source* section in the *Operations Bridge Reporter Configuration Guide*.

- **Test connection for new OMi source.**

- **Check the status of all the OBR services.**

2. Generating the Mapping Files

Points to note:

- Make sure that the view names in `topology_migration.properties` file located in `{PMDB_HOME}/config` directory have all the standard (out-of-the-box) and custom RTSM views deployed.

- The View name is case sensitive, if a new view is added, it should be with the same name that appears in **OMi console > RTSM Administration > Modeling > Modeling studio**.
- The OBR Topology migration tool maps the CIs from source RTSM to target RTSM based on Global Id attribute. As a pre-requisite, it is necessary to have unique Global Id values for all CIs gathered by OBR. For more details on topology integration between the two RTSM instances and populating Global Id, see the [OMi Documentation](#).
- The `topology_migration.properties` file located in `{PMDB_HOME}/config` directory captures the parameter `MappingProperty=global_id` as the default value.
- Make sure that `global_id` attribute is **Enabled** in all RTSM views used for OBR integration. For more information, see the *Operations Bridge Reporter Integration Guide*.

Run the following command:

```
TopologyMigrationTool -migrate RTSM -generatemapping
```

In this step, the migration tool runs the precheck again and performs the following:

Topology Data Extract

The migration tool extracts the topology data.

Topology Management Database Update

The migration tool updates the Management Database (Postgre DB) with RTSM topology details.

Topology Build Registry

The migration tool builds the registry for the topology data.

Topology CIID Mapping Generator

The migration tool builds the CIID mapping of RTSM topology source and BSM topology source and generates the mapping CSV files.

- The mapped CSV files are created in the `PMDB_HOME/csv/mappedcsvfolder`
- The unmapped CSV files are be created in `PMDB_HOME/csv/unmappedcsvfolder`.

Note: Unmapped CSV lists all the CI's which exist in the BSM topology source which has not been synchronized in RTSM topology source. The unmapped CI's exist as is in the data warehouse.

Topology Sync Data Source

In this step the migration tool syncs the Topology Data source to the available remote collectors.

3. Topology Invoke DLC

Run the following command:

```
TopologyMigrationTool -migrate RTSM - updatedb
```

In this step, the migration tool fetches the mapped CSV file and updates the Data ware house dimension tables with the RTSM CIID.

Topology Configuration Update

The migration tool updates the `config.prp` file with RTSM topology source configurations.

Start OBR Services

In this step the migration tool starts the below OBR services:

- HPE_PMDB_Platform_Administrator
- HPE_PMDB_Platform_Collection
- HPE_PMDB_Platform_DB_Logger
- HPE _PMDB_Platform_IM
- HPE _PMDB_Platform_JobManager
- HPE _PMDB_Platform_TaskManager
- HPE _PMDB_Platform_Orchestration
- HPE _PMDB_Platform_IA
- HPE _PMDB_Platform_NRT_ETL
- HPE _PMDB_Platform_Timer

Points to Note

1. If you are using BSM content pack, switch to OMi event content pack according to your OMi version:
 - CrossOprEvent_ETL_OMi10_Extended
 - CrossOprEvent_ETL_OMi10x

- CrossOprEvent_ETL_OMi10
- CrossOprEvent_ETL_OMi
- CrossOprEvent_ETL_OMi_Extended
- CrossOprEvent_ETL_OMi10

For information about the latest content pack version available, refer to *Operations Bridge Reporter Content Packs Versions* document.

2. Ensure that you are using the appropriate version of Management Pack (MP)-based ETLs for Exchange/Weblogic ETLs.

For more information, refer to Oracle WebLogic Server Content Pack Reference and Microsoft Exchange Server Content Pack Reference guides.

Limitations

Only the dimensions present in RTSM are migrated. If a dimension is not available in RTSM (dimension no longer exists in deployment), then the dimension continues to be available in OBR DATA WAREHOUSE with previous CIID (CIID formed using BSM topology source).

1. OA/PA data sources that are not available in RTSM will not be deleted in OBR management DB, but collection will be disabled for these data sources.
2. Node groups collected from BSM will continue to exist in OBR and be present in reports (unless delete steps are explicitly run). Views will be added to group list post switch to OMi; node group/CI Collections are not collected from OMi.
3. BSM Nodegroups will appear in report prompts post migration.

Download and install the VSQL client to run the queries listed here.

To clean up, run the below queries using the VSQL tool:

- Delete from K_CI_Group_Bridge where group_key in (Select dsi_key_id from K_group where type ='NODEGROUP')
- Delete from K_CI_Bridge where group_key in (Select dsi_key_id from K_group where type ='NODEGROUP')
- Delete from K_group where type='NODEGROUP'

PostgreSQL Management DB Backup and Restore

PostgreSQL Management DB backup

1. Open command prompt and navigate to {PMDB_HOME}/../ Postgres/bin directory.

Postgres directory is in the installed location of OBR.

Example: C:\HPE-OBR\Postgres\bin

2. Run the following command to take the backup:

```
pg_dump -h <hostname> -p 21425 -U pmdb_admin dwabc >c:\outfile.txt
```

Example: C:\HPE-OBR\Postgres\bin>pg_dump -h host001 -p 21425 -U pmdb_admin dwabc
>c:\outfile.txt

Restore PostgreSQL Management DB

1. Open command prompt and navigate to {PMDB_HOME}/../ Postgres/bin directory.

Postgres directory is in the installed location of OBR.

Example: C:\HPE-OBR\Postgres\bin

2. Run the following command to log on to psql:

```
psql -h <hostname> -p 21425 -U pmdb_admin dwabc
```

Example: C:\HPE-OBR\Postgres\bin>psql -h host001 -p 21425 -U pmdb_admin dwabc

3. Run the following command restore the database backup:

```
psql swayback < <absolute path of the backedup file name >
```

Example: psql dwabc < c:\outfile.txt

Note: Replace {PMDB_HOME} with

- %PMDB_HOME% for Windows
- \$PMDB_HOME for Linux

Topology Source Migration FAQs

1. What do I do if some rows from the old BSM topology source are loaded?

Clean up the loaded rows using the DLC cleanup. For more information, see the *Managing Dimensions* section in the *Operations Bridge Reporter Administration Guide*.

Appendix C: Status, Stopping and Starting OBR Services

This section provides instructions to check the status, stop and start OBR services.

In case of typical installation scenario, perform these steps on the OBR system. For custom installation, perform these steps on the individual servers as mentioned in the following sections.

On Linux

Status of the OBR services

Go to `/etc/init.d` directory and run the following commands on the command prompt to check the status of OBR services:

On RHEL 6.x/SUSE Linux Enterprise Server 11	On RHEL 7.x
On OBR Server	
<ul style="list-style-type: none">• <code>service HPE_PMDB_Platform_Administrator status</code>• <code>service HPE_PMDB_Platform_Collection status</code>• <code>service HPE_PMDB_Platform_DB_Logger status</code>• <code>service HPE_PMDB_Platform_IA status</code>• <code>service HPE_PMDB_Platform_IM status</code>• <code>service HPE_PMDB_Platform_NRT_ETL status</code>• <code>service HPE_PMDB_Platform_PostgreSQL status</code>• <code>service HPE_PMDB_Platform_JobManager status</code>• <code>service HPE_PMDB_Platform_</code>	<ul style="list-style-type: none">• <code>systemctl status HPE_PMDB_Platform_Administrator.service</code>• <code>systemctl status HPE_PMDB_Platform_Collection.service</code>• <code>systemctl status HPE_PMDB_Platform_DB_Logger.service</code>• <code>systemctl status HPE_PMDB_Platform_IA.service</code>• <code>systemctl status HPE_PMDB_Platform_IM.service</code>• <code>systemctl status HPE_PMDB_Platform_NRT_ETL.service</code>• <code>systemctl status HPE_PMDB_Platform_PostgreSQL.service</code>• <code>systemctl status HPE_PMDB_Platform_JobManager.service</code>• <code>systemctl status HPE_PMDB_Platform_</code>

<ul style="list-style-type: none"> TaskManager status • service HPE_PMDB_Platform_Orchestration status • service TrendTimer status 	<ul style="list-style-type: none"> TaskManager.service • systemctl status HPE_PMDB_Platform_Orchestration.service • systemctl status TrendTimer.service
On SAP BusinessObjects Server	
<ul style="list-style-type: none"> • service SAPBOBJEnterpriseXI40 status 	<ul style="list-style-type: none"> • systemctl status SAPBOBJEnterpriseXI40.service
On Remote Collector	
<ul style="list-style-type: none"> • service HPE_PMDB_Platform_Collection status 	<ul style="list-style-type: none"> • systemctl status HPE_PMDB_Platform_Collection.service
On Data Processor	
<ul style="list-style-type: none"> • service HPE_PMDB_Platform_TaskManager status 	<ul style="list-style-type: none"> • systemctl status HPE_PMDB_Platform_TaskManager.service
On Vertica Server	
<ul style="list-style-type: none"> • service HPE_PMDB_Platform_Vertica status 	<ul style="list-style-type: none"> • systemctl status HPE_PMDB_Platform_Vertica.service

Stopping OBR Services

Go to `/etc/init.d` directory and run the following commands on the command prompt to stop OBR services:

On RHEL 6.x/SUSE Linux Enterprise Server 11	On RHEL 7.x
On OBR Server	
<ul style="list-style-type: none"> • service HPE_PMDB_Platform_Administrator stop • service HPE_PMDB_Platform_Collection stop • service HPE_PMDB_Platform_DB_Logger stop • service HPE_PMDB_Platform_IA stop • service HPE_PMDB_Platform_IM stop • service HPE_PMDB_Platform_NRT_ETL stop • service HPE_PMDB_Platform_ 	<ul style="list-style-type: none"> • systemctl stop HPE_PMDB_Platform_Administrator.service • systemctl stop HPE_PMDB_Platform_Collection.service • systemctl stop HPE_PMDB_Platform_DB_Logger.service • systemctl stop HPE_PMDB_Platform_IA.service • systemctl stop HPE_PMDB_Platform_IM.service • systemctl stop HPE_PMDB_Platform_NRT_

<p>PostgreSQL stop</p> <ul style="list-style-type: none"> • service HPE_PMDB_Platform_Orchestration stop • service HPE_PMDB_Platform_TaskManager stop • service HPE_PMDB_Platform_JobManager stop • service TrendTimer stop 	<p>ETL.service</p> <ul style="list-style-type: none"> • systemctl stop HPE_PMDB_Platform_PostgreSQL.service • systemctl stop HPE_PMDB_Platform_Orchestration.service • systemctl stop HPE_PMDB_Platform_TaskManager.service • systemctl stop HPE_PMDB_Platform_JobManager.service • systemctl stop TrendTimer.service
On SAP BusinessObjects Server	
<ul style="list-style-type: none"> • service SAPBOBJEnterpriseXI40 stop 	<ul style="list-style-type: none"> • systemctl stop SAPBOBJEnterpriseXI40.service
On Remote Collector	
<ul style="list-style-type: none"> • service HPE_PMDB_Platform_Collection stop 	<ul style="list-style-type: none"> • systemctl stop HPE_PMDB_Platform_Collection.service
On Data Processor	
<ul style="list-style-type: none"> • service HPE_PMDB_Platform_TaskManager stop 	<ul style="list-style-type: none"> • systemctl stop HPE_PMDB_Platform_TaskManager.service
On Vertica Server	
<ul style="list-style-type: none"> • service HPE_PMDB_Platform_Vertica stop 	<ul style="list-style-type: none"> • systemctl stop HPE_PMDB_Platform_Vertica.service

Starting OBR Services

Go to `/etc/init.d` directory and run the following commands on the command prompt to start OBR services:

On RHEL 6.x/SUSE Linux Enterprise Server 11	On RHEL 7.x
On OBR Server	
<ul style="list-style-type: none"> • service HPE_PMDB_Platform_Administrator start • service HPE_PMDB_Platform_Collection start • service HPE_PMDB_Platform_DB_Logger start 	<ul style="list-style-type: none"> • systemctl start HPE_PMDB_Platform_Administrator.service • systemctl start HPE_PMDB_Platform_Collection.service • systemctl start HPE_PMDB_Platform_DB_Logger.service

<ul style="list-style-type: none"> • service HPE_PMDB_Platform_IA start • service HPE_PMDB_Platform_IM start • service HPE_PMDB_Platform_NRT_ETL start • service HPE_PMDB_Platform_PostgreSQL start • service HPE_PMDB_Platform_JobManager start • service HPE_PMDB_Platform_TaskManager start • service HPE_PMDB_Platform_Orchestration start • service TrendTimer start 	<ul style="list-style-type: none"> • systemctl start HPE_PMDB_Platform_IA.service • systemctl start HPE_PMDB_Platform_IM.service • systemctl start HPE_PMDB_Platform_NRT_ETL.service • systemctl start HPE_PMDB_Platform_PostgreSQL.service • systemctl start HPE_PMDB_Platform_JobManager.service • systemctl start HPE_PMDB_Platform_TaskManager.service • systemctl start HPE_PMDB_Platform_Orchestration.service • systemctl start TrendTimer.service
On SAP BusinessObjects Server	
<ul style="list-style-type: none"> • service SAPBOBJEnterpriseXI40 start 	<ul style="list-style-type: none"> • systemctl start SAPBOBJEnterpriseXI40.service
On Remote Collector	
<ul style="list-style-type: none"> • service HPE_PMDB_Platform_Collection start 	<ul style="list-style-type: none"> • systemctl start HPE_PMDB_Platform_Collection.service
On Data Processor	
<ul style="list-style-type: none"> • service HPE_PMDB_Platform_TaskManager start 	<ul style="list-style-type: none"> • systemctl start HPE_PMDB_Platform_TaskManager.service
On Vertica Server	
<ul style="list-style-type: none"> • service HPE_PMDB_Platform_Vertica start 	<ul style="list-style-type: none"> • systemctl start HPE_PMDB_Platform_Vertica.service

On Windows

Status of the OBR services

Follow these steps to check the status of OBR services:

1. Log on to the system.
2. From the **Start**, type **Run** in **Search**.
The Run dialog box appears.
3. Type **services.msc** in the open field, and then press **ENTER**.
The Services window appears.
4. The status of the following services is displayed as shown in the image:

On OBRServer:

- HPE_PMDB_Platform_Administrator
- HPE_PMDB_Platform_Collection
- HPE_PMDB_Platform_DB_Logger
- HPE_PMDB_Platform_IA
- HPE_PMDB_Platform_IM
- HPE_PMDB_Platform_NRT_ETL
- HPE_PMDB_Platform_PostgreSQL
- HPE_PMDB_Platform_JobManager
- HPE_PMDB_Platform_TaskManager
- HPE_PMDB_Platform_Orchestration
- HPE_PMDB_Platform_Timer

On SAP BusinessObjects Server:

- Business Objects Webserver
- Server Intelligence Agent (OBR)

On Remote Collector:

- HPE_PMDB_Platform_Collection

On Data Processor:

- HPE_PMDB_Platform_TaskManager

Stopping OBR Services

Follow these steps to stop OBR services:

1. Log on to the system.
2. From the **Start**, type **Run** in **Search**.
The Run dialog box appears.
3. Type **services.msc** in the open field, and then press **ENTER**.
The Services window appears.
4. Right-click the following services and click **Stop**:

On OBR:

- HPE_PMDB_Platform_Administrator
- HPE_PMDB_Platform_Collection
- HPE_PMDB_Platform_DB_Logger
- HPE_PMDB_Platform_IA
- HPE_PMDB_Platform_IM
- HPE_PMDB_Platform_NRT_ETL
- HPE_PMDB_Platform_PostgreSQL
- HPE_PMDB_Platform_Orchestration
- HPE_PMDB_Platform_TaskManager
- HPE_PMDB_Platform_JobManager
- HPE_PMDB_Platform_Timer

On SAP BusinessObjects:

- Business Objects Webserver
- Server Intelligence Agent (OBR)

On Remote Collector:

- HPE_PMDB_Platform_Collection

On Data Processor:

- HPE_PMDB_Platform_TaskManager

Starting OBR Services

Follow these steps to start OBR services:

1. Log on to the system.
2. From the **Start**, type **Run** in **Search**.
The Run dialog box appears.
3. Type **services.msc** in the open field, and then press **ENTER**.
The Services window appears.
4. Right-click the following services and click **Start**:

On OBR Server:

- HPE_PMDB_Platform_Administrator
- HPE_PMDB_Platform_Collection
- HPE_PMDB_Platform_DB_Logger
- HPE_PMDB_Platform_IA
- HPE_PMDB_Platform_IM
- HPE_PMDB_Platform_NRT_ETL
- HPE_PMDB_Platform_PostgreSQL
- HPE_PMDB_Platform_JobManager
- HPE_PMDB_Platform_TaskManager
- HPE_PMDB_Platform_Orchestration
- HPE_PMDB_Platform_Timer

On SAP BusinessObjects Server:

- Business Objects Webserver
- Server Intelligence Agent (OBR)

On Remote Collector:

- HPE_PMDB_Platform_Collection

On Data Processor:

- HPE_PMDB_Platform_TaskManager

Appendix D: SiteScope Monitors for OBR

The following table lists the monitors that are used to collect the virtualization metrics:

Monitor Name	Counter	Measure Name
VMware Performance	HostSystem\state	hardware.memorySize
VMware Performance	HostSystem\state	summary.hardware.numCpuCores
VMware Performance	HostSystem\state	summary.hardware.cpuMhz
VMware Performance	HostSystem\state	summary.hardware.numNics
VMware Performance	HostSystem\Realtime\sys	uptime.latest[]
VMware Performance	HostSystem\Realtime\mem	usage.average[]
VMware Performance	HostSystem\Realtime\mem	consumed average[]
VMware Performance	HostSystem\Realtime\cpu	usage.average[]
VMware Performance	HostSystem\Realtime\cpu	ready.summation[]
VMware Performance	HostSystem\Realtime\disk	usage.average[]
VMware Performance	HostSystem\Realtime\disk	read.average[]
VMware Performance	HostSystem\Realtime\disk	write.average[]
VMware Performance	HostSystem\Realtime\net	received.average[]
VMware Performance	HostSystem\Realtime\net	transmitted.average[]
VMware Performance	HostSystem\Realtime\net	packetsRx.summation[]
VMware Performance	HostSystem\Realtime\net	packetsTx.summation[]
VMware Performance	HostSystem\Realtime\net	usage.average[]
VMware Performance	HostSystem\Realtime\mem	usage.average
VMware Performance	HostSystem\Realtime\mem	consumed.average
VMware Performance	Virtual Machine\state	config.hardware.memoryMB
VMware Performance	Virtual Machine\state	config.cpuAllocation.shares.shares
VMware Performance	Virtual Machine\state	config.hardware.numcpu
VMware Performance	Virtual Machine\state	config.memoryAllocation.reservation

Monitor Name	Counter	Measure Name
VMware Performance	Virtual Machine\state	config.memoryAllocation.limit
VMware Performance	Virtual Machine\state	config.cpuAllocation.reservation
VMware Performance	Virtual Machine\state	config.cpuAllocation.limit
VMware Performance	Virtual Machine\mem	active.average[]
VMware Performance	Virtual Machine\Realtime\sys	uptime.latest[]
VMware Performance	Virtual Machine\Realtime\mem	usage.average[]
VMware Performance	Virtual Machine\Realtime\mem	consumed.average[]
VMware Performance	Virtual Machine\Realtime\mem	active.average[]
VMware Performance	Virtual Machine\Realtime\mem	overhead.average[]
VMware Performance	Virtual Machine\Realtime\mem	swapin.average[]
VMware Performance	Virtual Machine\Realtime\mem	swapout.average[]
VMware Performance	Virtual Machine\Realtime\mem	usage.average[]
VMware Performance	Virtual Machine\Realtime\mem	ready.summation[]
VMware Performance	Virtual Machine\Realtime\mem	usagemhz.average[]
VMware Performance	Virtual Machine\Realtime\mem	wait.summation[]
VMware Performance	Virtual Machine\Realtime\mem	read.average[]
VMware Performance	Virtual Machine\Realtime\mem	write.average[]
VMware Performance	Virtual Machine\Realtime\mem	received.average[]

Monitor Name	Counter	Measure Name
VMware Performance	Virtual Machine\Realtime\mem	transmitted.average[]
VMware Performance	Virtual Machine\Realtime\mem	packetsRx.summation[]
VMware Performance	Virtual Machine\Realtime\mem	packetsTx.summation[]
VMware Performance	Virtual Machine\Realtime\cpu	usage.average[]
VMware Performance	Virtual Machine\Realtime\cpu	ready.summation[]
VMware Performance	Virtual Machine\Realtime\cpu	usagemhz.average[]
VMware Performance	Virtual Machine\Realtime\cpu	wait.summation[]
VMware Performance	Virtual Machine\Realtime\net	received.average[]
VMware Performance	Virtual Machine\Realtime\net	transmitted.average[]
VMware Performance	Virtual Machine\Realtime\net	packetsRx.summation[]
VMware Performance	Virtual Machine\Realtime\net	packetsTx.summation[]
VMware Performance	Virtual Machine\Realtime\net	usage.average[]
VMware Performance	Virtual Machine\Realtime\disk	read.average[]
VMware Performance	Virtual Machine\Realtime\disk	write.average[]
VMware Performance	Virtual Machine\Realtime\disk	usage.average[]

The following table lists the monitors that are used to collect the system management metrics:

Monitor	Objects	Counter	System Type
Microsoft Windows Resources	Memory	% Committed Bytes In Use	Windows

Monitor	Objects	Counter	System Type
Microsoft Windows Resources	memory	Pages Output/sec	Windows
Microsoft Windows Resources	System	Processor Queue Length	Windows
Microsoft Windows Resources	System	System Up Time	Windows
Microsoft Windows Resources	Physical Disk	Total Disk Bytes/sec	Windows
Microsoft Windows Resources	Physical Disk	Disk Read Bytes/sec	Windows
Microsoft Windows Resources	Physical Disk	Disk Write Bytes/sec	Windows
Microsoft Windows Resources	Physical Disk	Disk Bytes/sec	Windows
Microsoft Windows Resources	Network Interface	%Packets Received/sec	Windows
Microsoft Windows Resources	Network Interface	%Bytes Received/sec	Windows
Microsoft Windows Resources	Network Interface	%Bytes Sent/sec	Windows
Microsoft Windows Resources	Network Interface	%Packets/sec	Windows
Microsoft Windows Resources	Network Interface	%Packets Sent/sec	Windows
Microsoft Windows Resources	Network Interface	BytesTotal/sec	Windows
Unix Resources	Queue length	Queue length\runq-sz	Linux/Solaris
Unix Resources	Queue Statistics	Queue Statistics\runq-sz	HP-UX/AIX
Unix Resources	Uptime	Uptime\Uptime	Linux/HP-UX
Unix Resources	File System	%\capacity	Linux/Solaris
Unix Resources	File System	%\kbytes	Linux/Solaris
Unix Resources	File System	avail	Solaris

Monitor	Objects	Counter	System Type
Unix Resources	File System	used	Solaris
Unix Resources	File System	%\Use\%	RHEL
Unix Resources	File System	%\Used	RHEL
Unix Resources	File System	%\Capacity	HP-UX
Unix Resources	File System	%\%Used	HP-UX, AIX
Unix Resources	File System	%\1024-blocks	AIX
Unix Resources	File System	1K-blocks	RHEL
Unix Resources	File System	Available	RHEL
Unix Resources	Network Interface	%packets	RHEL
Unix Resources	Network Interface	%ReceiveBytes	RHEL
Unix Resources	Network Interface	%TransmitBytes	RHEL
Unix Resources	Network Interface	%ipackets	Solaris
Unix Resources	Network Interface	%opackets	Solaris
Unix Resources	Network Interface	%rbytes	Solaris
Unix Resources	Network Interface	%obytes	Solaris
Unix Resources	Network Stats	%Ipkts	HP-UX
Unix Resources	Network Stats	%Opkts	HP-UX
Dynamic Disk space	Disk/FileSystem	%/MB free **	Linux/Windows
Dynamic Disk space	Disk/FileSystem	%/MB total **	Linux/Windows
Dynamic Disk space	Disk/FileSystem	%/percent full **	Linux/Windows
CPU	N/A	utilization	Linux/Windows
CPU	N/A	utilization cpu%	Linux/Windows
Memory	N/A	Percent used	Linux/Windows
Memory	N/A	virtual memory used %	Linux/Windows
Memory	N/A	physical memory used % *	Linux/Windows

Monitor	Objects	Counter	System Type
Memory	N/A	swap space used %	Linux/Windows
Memory	N/A	physical memory MB Free *	Linux/Windows
Memory	N/A	virtual memory MB Free	Linux/Windows
Memory	N/A	MB Free	Linux/Windows

* The counter is available only when Windows node is connected with WMI method.

** The counter is not available when Windows node is connected with WMI method.

Appendix E: Installing SAP BusinessObjects Dashboards (Earlier known as Xcelsius)

An SAP BusinessObjects Dashboards report is an interactive Flash-based report created by using the SAP. To create Dashboards as Flash-based reports in OBR, you must install the SAP BusinessObjects Dashboards application, which is included on the OBR installation media. SAP BusinessObjects Dashboards is not essential for viewing the OBR reports. Therefore, installation it is optional.

Note: Microsoft Excel, as a base, is a prerequisite for SAP BusinessObjects Dashboards.

Hardware and Software Requirements

For the list of hardware and software requirements of BusinessObjects Dashboard, see its documentation from SAP BusinessObjects.

Installing SAP BusinessObjects Dashboards (Optional)

The `setup` file for installing Installing SAP BusinessObjects Dashboards is bundled with the OBR installation media.

Follow these steps to obtain the `setup` executable:

1. On the OBR installation media, browse to the `\packages` folder.
2. Select the `BusinessObjects_Dashboards.ZIP` file, copy it to a location of your choice, and extract it.
3. From the extracted folder, browse to the `\DATA_UNITS\Xcelsius` folder and run the `setup` executable (`setup.exe`).

For more information on the installation, see the *Dashboards and Presentation Design Installation Guide* available from from SAP BusinessObjects.

Appendix F: Listing of ETLs

This section list the ETLs for the Content Packs. To generate reports, make sure to select atleast one domain Content Pack, ETL Content Pack, and report Content Pack. The dependent domain Content Pack get selected automatically, you have to select only the ETLs based on the data source.

The timer service will be stopped automatically during install/uninstall operation and will be started once operation is complete.

During install/uninstall process, Content Pack Deployment page does not allow you to interrupt the process. Instead, you must wait till the current process is complete before you can perform any other operations on the Content Pack Deployment page.

The following table list the ETLs for each content pack:

Content Pack Name	ETL	Comments
Cross-Domain Operations Events	CrossOprEvent_ETL_OMi	If the topology source is OMi 10, select the CrossOprEvent_ETL_OMi10 component for OMi 10.00 and OMi 10.01. Select the CrossOprEvent_ETL_OMi10x for OMi 10.10 and later versions.
	CrossOprEvent_ETL_OMi10	
	CrossOprEvent_ETL_OMi10x	
	CrossOprEvent_Domain_Reports	The Content Pack components 'CrossOprEvent_ETL_OMi' and 'CrossOprEvent_ETL_OMi10' are mutually exclusive. Ensure that only one of them is selected.
	CrossOprEvent_ETL_OMi10_Extended	The Content Pack components 'CrossOprEvent_ETL_OMi_Extended' and 'CrossOprEvent_ETL_OMi10_Extended' are mutually exclusive. Ensure that only one of them is selected.
	CrossOprEvent_ETL_OMi_Extended	
	CrossOprEvent_Domain_Reports_Extended	The Content Pack components 'CrossOprEvent_ETL_OMi10' and 'CrossOprEvent_ETL_OMi10x' are mutually exclusive. Ensure that only one of them is selected.
	CrossOprEvent_ETL_OMi10x_Extended	
	The Content Pack components 'CrossOprEvent_ETL_OMi10x_Extended' and 'CrossOprEvent_ETL_OMi10_Extended' are mutually exclusive. Ensure that only one of them is selected.	

Content Pack Name	ETL	Comments				
		<p>Note: You must upgrade CrossOprEvent_Domain_Report_Extended to the latest version to use CrossOprEvent_ETL_OMi10x_Extended component.</p> <p>Note: Select the Extended ETLs to generate customized reports that involves Event detail attributes.</p> <p>Note: You have to select one of the Health and Key Performance Indicators ETLs explicitly because Cross-Domain Operations Events Content Pack has a dependency on Health and Key Performance Indicators Content Pack.</p>				
Health and Key Performance Indicators	<table border="1"> <tr> <td data-bbox="495 953 875 1003">HIKPI_ETL_ServiceHealth</td> </tr> <tr> <td data-bbox="495 1008 875 1087">HIKPI_ETL_ServiceHealth_OMi10</td> </tr> <tr> <td data-bbox="495 1092 875 1142">HIKPI_Domain</td> </tr> <tr> <td data-bbox="495 1146 875 1197">HIKPI_Reports_ServiceHealth</td> </tr> </table>	HIKPI_ETL_ServiceHealth	HIKPI_ETL_ServiceHealth_OMi10	HIKPI_Domain	HIKPI_Reports_ServiceHealth	<p>If the topology source is OMi 10, select the HIKPI_ETL_ServiceHealth_OMi10 component.</p> <p>The Content Pack components 'HIKPI_ETL_ServiceHealth' and 'HIKPI_ETL_ServiceHealth_OMi10' are mutually exclusive. Ensure that only one of them is selected.</p>
HIKPI_ETL_ServiceHealth						
HIKPI_ETL_ServiceHealth_OMi10						
HIKPI_Domain						
HIKPI_Reports_ServiceHealth						
Server Automation	<table border="1"> <tr> <td data-bbox="495 1268 875 1318">SA_Core_ETL</td> </tr> <tr> <td data-bbox="495 1323 875 1373">SA_Core_Domain</td> </tr> </table>	SA_Core_ETL	SA_Core_Domain			
SA_Core_ETL						
SA_Core_Domain						
IBM WebSphere Application Server	<table border="1"> <tr> <td data-bbox="495 1386 875 1470">IBMWebSphere_ETL_WebSphereSPI</td> </tr> <tr> <td data-bbox="495 1474 875 1524">IBMWebSphere_Domain</td> </tr> <tr> <td data-bbox="495 1528 875 1579">IBMWebSphere_Reports</td> </tr> <tr> <td data-bbox="495 1583 875 1667">IBMWebSphere_ETL_WebSphereMP</td> </tr> </table>	IBMWebSphere_ETL_WebSphereSPI	IBMWebSphere_Domain	IBMWebSphere_Reports	IBMWebSphere_ETL_WebSphereMP	<p>If you have installed IBM WebSphere SPI ETL already and are migrating from OM to OMi10 or upgrading to latest OMi Management Pack for WebSphere, uninstall the IBM WebSphere SPI ETL and deploy the latest IBM WebSphere MP ETL.</p>
IBMWebSphere_ETL_WebSphereSPI						
IBMWebSphere_Domain						
IBMWebSphere_Reports						
IBMWebSphere_ETL_WebSphereMP						
Microsoft Active Directory	<table border="1"> <tr> <td data-bbox="495 1692 875 1776">MicrosoftActiveDirectory_ETL_ADSPI</td> </tr> <tr> <td data-bbox="495 1780 875 1864">MicrosoftActiveDirectory_Reports</td> </tr> </table>	MicrosoftActiveDirectory_ETL_ADSPI	MicrosoftActiveDirectory_Reports			
MicrosoftActiveDirectory_ETL_ADSPI						
MicrosoftActiveDirectory_Reports						

Content Pack Name	ETL	Comments
	MicrosoftActiveDirectory_Domain	
Microsoft Exchange Server	MicrosoftExchange_ETL_ExchangeSPI2007	The MicrosoftExchange_ETL_ExchangeSPI2007 collects data from Operations SPI for Exchange Server 2007.
	MicrosoftExchange_ETL_ExchangeSPI2010	The MicrosoftExchange_ETL_ExchangeSPI2010 collects data from Operations SPI and OMi management pack for Exchange Server 2010.
	MicrosoftExchange_ETL_ExchangeSPI2013	
	MicrosoftExchange_Domain	The MicrosoftExchange_ETL_ExchangeSPI2013 collects data from Operations SPI and OMi management pack for Exchange Server 2013.
	MicrosoftExchange_Reports	
Microsoft SQL Server	MicrosoftSQLServer_ETL_DBSPI	
	MicrosoftSQLServer_Domain	
	MicrosoftSQLServer_Reports	
Network Performance	NetworkPerf_ETL_PerfiSPI_NonRTSM	Install this Content Pack to collect network performance data from NPS. The data collection is based on hourly, daily and aggregate summary. You can view executive summary reports.
	NetworkPerf_ETL_PerfiSPI_RTSM	
	NetworkPerf_Domain	The Content Pack components 'NetworkPerf_ETL_PerfiSPI_NonRTSM' and 'NetworkPerf_ETL_PerfiSPI_RTSM' are mutually exclusive. Ensure that only one of them is selected.
	NetworkPerf_Reports	
	<p>Note: If the NNMi topology is integrated to BSM/OMi RTSM, select NetworkPerf_ETL_PerfiSPI_RTSM Content Pack component. If else, select NetworkPerf_ETL_PerfiSPI_NonRTSM Content Pack component.</p> <p>Note: The Network Performance Content Pack collects data only from Type2 NodeGroups, that is, routers and switches.</p>	

Content Pack Name	ETL	Comments
Network Component_Health	ComponentHealth_Reports	Install this Content Pack to collect network performance data directly from NNMi. The data collection gives you detailed real time view of component or interface health in your network. You can view detailed health or utilization reports.
	Core_ComponentHealth	
Network Interface_Health	InterfaceHealth_Reports	Install this Content Pack to collect network performance data directly from NNMi. The data collection gives you detailed real time view of component or interface health in your network. You can view detailed health or utilization reports.
	Core_InterfaceHealth	
Operations Events	OprEvent_ETL_OM	
	OprEvent_Domain_Reports	
Oracle	Oracle_ETL_DBSPI	
	Oracle_Domain	
	Oracle_Reports	
Oracle WebLogic Server	OracleWebLogic_ETL_WebLogicSPI	If you have installed WebLogic SPI ETL already and are migrating from OM to OMi10 or upgrading to latest OMi Management Pack for WebLogic, uninstall the Oracle WebLogic SPI ETL and deploy the latest Oracle WebLogic MP ETL.
	OracleWebLogic_Domain	
	OracleWebLogic_Reports	
	OracleWebLogic_ETL_WebLogicMP	
Real User Transaction Monitoring	RealUsrTrans_ETL_RUM	If the topology source is OMi 10, select the RealUsrTrans_ETL_RUM_OMi component.
	RealUsrTrans_ETL_RUM_OMi	
	RealUsrTrans_Domain_Reports	The Content Pack components 'RealUsrTrans_ETL_RUM' and 'RealUsrTrans_ETL_RUM_OMi' are mutually exclusive. Ensure that only one of them is selected.
Synthetic Transaction Monitoring	SynTrans_Domain_Reports	If the topology source is OMi 10, select the SynTrans_ETL_BPM_OMi component.
	SynTrans_ETL_BPM	
	SynTrans_ETL_BPM_OMi	The Content Pack components 'SynTrans_ETL_BPM' and 'SynTrans_

Content Pack Name	ETL	Comments
		ETL_BPM_OMI' are mutually exclusive. Ensure that only one of them is selected.
System Performance	SysPerf_ETL_PerformanceAgent	If Operations Agent is the data source, select the SysPerf_ETL_PerformanceAgent Content Pack component.
	SysPerf_ETL_SiS_API	
	SysPerf_ETL_SiS_API_NonRtSM	The SysPerf_ETL_SiS_DB is for Profile DB integration. If the topology source is BSM 9.x and you have already installed the SysPerf_ETL_SiS_DB, you can continue to use the same.
	SysPerf_ETL_SiS_DB	The SysPerf_ETL_SiS_API is for OMI 10.0 integration. You can use this Content Pack component even in the absence of Profile DB. The list of metrics collected by SysPerf_ETL_SiS_DB and SysPerf_ETL_SiS_API are same.
	SysPerf_Domain	
	SysPerf_Reports	<p>The SysPerf_ETL_SiS_API_NonRtSM is for direct integration with SiteScope. The list of metrics collected by this ETL are same as SysPerf_ETL_SiS_DB and SysPerf_ETL_SiS_API ETLs. However, some of the CI attributes are not collected by SysPerf_ETL_SiS_API_NonRtSM.</p> <p>The Content Pack components 'SysPerf_ETL_SiS_API_NonRtSM' and 'SysPerf_ETL_SiS_API' are mutually exclusive. Ensure that only one of them is selected.</p>
Virtual Environment Performance	VirtualEnvPerf_ETL_HyperV_PerformanceAgent	If the data source is Operations Agent or Performance Agent, select Performance Agent based Content Pack components.
	VirtualEnvPerf_ETL_IBMLPAR_PerformanceAgent	If the data source is VMware vCenter, select VMWare_vCenter based Content Pack components.
	VirtualEnvPerf_ETL_SolarisZones_PerformanceAgent	Select either VirtualEnvPerf_ETL_VMware_SiteScope or VirtualEnvPerf_ETL_VMware_SiS_API Content Pack component.
	VirtualEnvPerf_ETL_VMWare_PerformanceAgent	The VirtualEnvPerf_ETL_VMware_SiteScope is for Profile DB integration. If
	VirtualEnvPerf_ETL_VMware_	

Content Pack Name	ETL	Comments
	<p>SiS_API</p> <p>VirtualEnvPerf_ETL_VMware_SiteScope</p> <p>VirtualEnvPerf_Domain</p> <p>VirtualEnvPerf_Domain_VMWare</p> <p>VirtualEnvPerf_Reports</p> <p>VirtualEnvPerf_Reports_VMWare</p> <p>VirtualEnvPerf_ETL_VMWare_vCenter</p>	<p>the topology source is BSM 9.x and you have already installed the VirtualEnvPerf_ETL_VMware_SiteScope, you can continue to use the same. The VirtualEnvPerf_ETL_VMware_SiS_API is for OMi 10.0 integration. You can use this Content Pack component even in the absence of Profile DB. The list of metrics collected by VirtualEnvPerf_ETL_VMware_SiteScope and VirtualEnvPerf_ETL_VMware_SiS_API are same.</p> <p>The Content Pack components 'VirtualEnvPerf_ETL_VMWare_vCenter' and 'VirtualEnvPerf_ETL_VMWare_PerformanceAgent' are mutually exclusive. Ensure that only one of them is selected.</p> <p>Note: Use the VirtualEnvPerf_ETL_VMWare_PerformanceAgent and VirtualEnvPerf_ETL_HyperV_PerformanceAgent ETLs if the Operations Agent version is 11.x or earlier. Use Cloud Optimizer (earlier known as Virtualization Performance Viewer (vPV)) content if the Operations Agent version is 12.</p> <p>Note: The Operations Bridge Reporter supports Cloud Optimizer (earlier known as Virtualization Performance Viewer (vPV)). OBR collects data for reporting on performance, configuration, and capacity problems in the virtual environments from Cloud Optimizer. For more information on the integration of OBR with Cloud Optimizer, see User Guide from the following URL:</p> <p>https://hpin.hpe.com/contentoffering/hpe-obr-cloud-optimizer-content</p>

Appendix G: System Management Reports with SiteScope data source

The following table lists the System Management reports with the report fields with SiteScope API data source and RTSM topology:

Category	Report Name	Report Fields
Executive Summary	SM Executive summary	<ul style="list-style-type: none"> • OS • Physical Or Virtual • CPU Utilization • Memory Utilization • Filesystem Utilization • Availability • RunQ • BS (Business Service) • BV/Group (Business View)
Executive Summary	SM Heat chart	<ul style="list-style-type: none"> • CPU Utilization • Memory Utilization
Executive Summary	SM System availability summary	<ul style="list-style-type: none"> • Average Uptime • Average Downtime • Average Availability • Total Uptime in Hours • Total Downtime in Hours
Executive Summary	SM System Exception by Group	<ul style="list-style-type: none"> • CPU Utilization • Memory Utilization • SWAP Utilization
Executive Summary	SM System Forecast summary	<ul style="list-style-type: none"> • CPU Utilization • Memory Utilization • Number of standalone nodes • Number of Virtual Host

Executive Summary	SM System Grade of Service by Group	<ul style="list-style-type: none"> • CPU Utilization • Memory Utilization • SWAP Utilization
Executive Summary	SM System Inventory	<ul style="list-style-type: none"> • K_Location.Name • K_CI_System_Alias.DNS_Name • K_CI_System_Alias.isvirtual • K_CI_System_Alias.OS
Executive Summary	SM System Resource Outage Forecast Summary	<ul style="list-style-type: none"> • CPU Utilization • Memory Utilization
Executive Summary	SM Top and Bottom 10 Filesystems by Free Space Utilization	<ul style="list-style-type: none"> • filesystem Name • Utilization
Executive Summary	SM Top and Bottom 5 Systems	<ul style="list-style-type: none"> • By Availability • By CPU Utilization • By Memory utilization
Operational Reports	NRT Resource Utilization	<ul style="list-style-type: none"> • CPU • Memory • RunQ • SWAP
Operational Reports	Resource Utilization - Trend	<ul style="list-style-type: none"> • RunQ
Performance	SM Filesystem Utilization Detail	<ul style="list-style-type: none"> • Filesystem • Average space used in MB
Performance	SM system availability details	<ul style="list-style-type: none"> • Uptime % • Downtime % • Availability %
Performance	SM System exception details	<ul style="list-style-type: none"> • CPU Utilization • Memory Utilization • CPU RunQ • SWAP Utilization • Avg memory pageout

		<ul style="list-style-type: none"> rate • OS
Performance	SM system grade of service details	<ul style="list-style-type: none"> • OS • CPU Utilization • Memory Utilization • CPU RunQ • SWAP Utilization
Performance	SM system usage details	<ul style="list-style-type: none"> • OS • CPU Utilization • Memory Utilization

The following table lists the System Management reports with the report fields with SiteScope API data source and non-RTSM topology:

Category	Report Name	Report Fields
Executive Summary	SM Executive summary	<ul style="list-style-type: none"> • CPU Utilization • Memory Utilization • Filesystem Utilization • Availability • RunQ
Executive Summary	SM Heat chart	<ul style="list-style-type: none"> • CPU Utilization • Memory Utilization
Executive Summary	SM System availability summary	<ul style="list-style-type: none"> • Average Uptime • Average Downtime • Average Availability • Total Uptime in Hours • Total Downtime in Hours
Executive Summary	SM System Exception by Group	<ul style="list-style-type: none"> • CPU Utilization • Memory Utilization • SWAP Utilization
Executive Summary	SM System Forecast summary	<ul style="list-style-type: none"> • CPU Utilization • Memory Utilization
Executive	SM System Grade of Service by Group	<ul style="list-style-type: none"> • CPU Utilization

Summary		<ul style="list-style-type: none"> • Memory Utilization • SWAP Utilization
Executive Summary	SM System Inventory	<ul style="list-style-type: none"> • K_Location.Name • K_CI_System_Alias.DNS_Name
Executive Summary	SM System Resource Outage Forecast Summary	<ul style="list-style-type: none"> • CPU Utilization • Memory Utilization
Executive Summary	SM Top and Bottom 10 Filesystems by Free Space Utilization	<ul style="list-style-type: none"> • filesystem Name • Utilization
Executive Summary	SM Top and Bottom 5 Systems	<ul style="list-style-type: none"> • By Availability • By CPU Utilization • By Memory utilization
Operational Reports	NRT Resource Utilization	<ul style="list-style-type: none"> • CPU • Memory • RunQ • SWAP
Operational Reports	Resource Utilization - Trend	<ul style="list-style-type: none"> • RunQ
Performance	SM Filesystem Utilization Detail	<ul style="list-style-type: none"> • Filesystem • Average space used in MB
Performance	SM system availability details	<ul style="list-style-type: none"> • Uptime % • Downtime % • Availability %
Performance	SM System exception details	<ul style="list-style-type: none"> • CPU Utilization • Memory Utilization • CPU RunQ • SWAP Utilization • Avg memory pageout rate
Performance	SM system grade of service details	<ul style="list-style-type: none"> • CPU Utilization • Memory Utilization • CPU RunQ • SWAP Utilization

Performance	SM system usage details	<ul style="list-style-type: none">• CPU Utilization• Memory Utilization
-------------	-------------------------	--

Appendix H: Disable TLS for Vertica

Follow these steps to disable TLS for Vertica:

1. On the Vertica server, run the following command to log on to vsql:

```
vsqll -h <Host name> -U <Vertica DBA Username> -p <Port> -d <Database Name>
```

where, <Host name> is the host name of the system where Vertica is installed

<Vertica DBA Username> is the Vertica user with DBA privileges

<Port> is the port number

<Database Name> is the name of Vertica database

2. To disable TLS for Vertica, run the command:

```
SELECT SET_CONFIG_PARAMETER ('EnableSSL', '0');
```

3. Go to /etc/init.d directory and run the following command to restart the Vertica service:

On RHEL 6.x/SUSE Linux Enterprise Server 11:

```
service HPE_PMDB_Platform_Vertica restart
```

On RHEL 7.x:

```
systemctl restart HPE_PMDB_Platform_Vertica.service
```

4. Go to the location \$PMDB_HOME/data and open the config.prp file.
5. Delete the values for the database.trustStore and database.trustStorePassword parameters.
6. Edit the database.ssl parameter as follows:

```
database.ssl=false
```

7. Restart HPE_PMDB_Platform_Administrator service on OBR server as follows:

On Linux:

Go to /etc/init.d directory and run the following commands:

On RHEL 6.x/SUSE Linux Enterprise Server 11:

- a. service HPE_PMDB_Platform_Administrator stop
- b. service HPE_PMDB_Platform_Administrator start

On RHEL 7.x:

- a. `systemctl stop HPE_PMDB_Platform_Administrator.service`
- b. `systemctl start HPE_PMDB_Platform_Administrator.service`

On Windows:

- a. From the **Start**, type **Run** in **Search**. The Run dialog box appears.
 - b. Type **services.msc** in the open field, and then press **ENTER**. The Services window appears.
 - c. Right-click on the HPE_PMDB_Platform_Administrator service and click **Restart**.
8. Run the following command on OBR server:

```
BOAdapter -updateDataConnection
```

Appendix I: Drop Vertica Database

To drop the Vertica database, open the command prompt and run the following commands:

1. `su <Vertica Database User Name> -c "/opt/vertica/bin/adminTools -t stop_db -d <Database Name> -p <Vertica Database User name Password> -F"`
2. `su <Vertica Database User Name> -c "/opt/vertica/bin/adminTools -t drop_db -d <Database Name>"`

where, *<Vertica Database User Name>* is the Vertica database user name

<Vertica Database User name Password> is the Vertica database password

<Database Name> is the name of the Vertica database

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 Configuration Guide (Operations Bridge Reporter 10.22)

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!