HPE Operations Bridge Reporter

Software Version: 10.10

Configuration Guide

Document Release Date: January 2017
Software Release Date: January 2017

Hewlett Packard Enterprise

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

© 2015 - 2017 Hewlett Packard Enterprise Development LP

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

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

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

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

Contents

Part I: HPE OBR Overview and Planning 8
Revision History 8
Chapter 1: Configuration Planning 11
Know your Deployment Scenarios 11
Business Service Management/Operations Manager i 11
HP Operations Manager 14
VMware vCenter 15
Other Deployments 16
Know the Data Sources 17
Determine the Readiness 18
Licensing Requirement for HPE OBR 19
Licenses to Use (LTUs) 20
Obtaining a Permanent License Key 21
Installing the Permanent License Key 22
SAP BusinessObjects License Reactivation 24
Part II: Configuring HPE OBR 27
Chapter 2: Post-Install Configuration 28
Task 1: Launching the Administration Console 30
Task 2: Creating the Vertica Database Schema 34
Creating Database Schema for Co-located Vertica 35
Creating Database Schema for Remote Vertica 37
Task 3: Creating the Management Database User Account 40
Task 4: Configuring the Remote Collectors 43
Migrating Data from Older Versions (HP SHR 9.x) 45
Task 5: Data Source Selection 46
Data Sources for the HPOM Deployment Scenario 48
Data Sources for the BSM or OMi Deployment Scenario 49
OMi10 Topology Source with Integrated BSM 52
OMi10 Topology Source after BSM Upgrade 53
Data Source for the VMware vCenter Deployment Scenario 55
Data Sources for Other Database Deployment Scenario 56

Task 6: Configuring the Topology Source 57
Configuring RTSM Topology Source 58
Supported Data Source Selections 62
Configuring HPOM Topology Source 62
Supported Data Source Selections 65
Configuring VMware vCenter Topology Source 65
Supported Data Source Selections 66
Task 7: Summary 67
Disabling Memory Analysis and APS Service Monitoring 68
Logon Banner 71
Chapter 3: Configure OBR for BSM/OMi Deployment Scenario 72
Configuring RTSM Topology Source for HPE OBR 72
List of Content Pack and Topology Views to Deploy 73
HP BSM Server 77
HP OMi 10 Server 79
Enabling CI Attributes for a Content Pack 82
Chapter 4: Configure OBR for HPOM Deployment Scenario 86
Authentication for HPE OBR connection with HPOM 86
HPE OBR connection with HPOM using NT authentication 87
HPE OBR connection with HPOM using database authentication 88
Checking for the HPOM Server Port Number 95
Chapter 5: Install and Uninstall the Content Packs 96
Before You Begin 96
Check Availability and Integrity of Data Sources 96
Selecting the Content Pack Components 99
Installing the Content Pack Components 101
Uninstalling the Content Pack Components 105
Chapter 6: Data Source Configuration 106
Topology Source 107
Configuring the HP Operations Agent Data Source 108
Configuring the HP Operations Manager Data Source 108
Configuring the Generic Data Source 111
Configuring the VMware vCenter Data Source 114
Configuring the SiteScope Data Source 115
Configuring the Management and Profile Database Data Source 120

Configuring the HP OMi Data Source 127
Chapter 7: Pending Configuration 131
Part III: Additional Configuration and Administration 133
Chapter 8: Configuring the HP Operations Agent for Data Collection in Secure Mode 134
Chapter 9: Configuring the Report Drill Feature Settings 139
Chapter 10: Configuring the Internal Alerting Service 142
Chapter 11: Certificates for HPE OBR 146
Use Secure Sockets Layer (SSL) Certificate 146
Client Authentication Certificate for HPE OBR 147
Authentication and Authorization 147
Prerequisites of Certificate Based Authentication 147
Configuring Username Extraction Method 150
Configuring HPE OBR Administration Console 151
Configuring SAP BusinessObjects BI Launch Pad 155
Chapter 12: Configuring HPE OBR with Network Node Manager i (NNMi) 160
Chapter 13: Configuring DSN on Windows for Vertica Database Connection 165
Chapter 14: Discover Profile or Operations Database 169
Chapter 15: Configuring HPE OBR to Setup Vertica Cluster 172
Chapter 16: Configuring HPE OBR for External Vertica 173
For New HPE OBR Installation 174
Scenario 1: HPE OBR is the Only Product 174
Scenario 2: HPE OBR is Installed Before Other Product 175
Scenario 3: HPE OBR is Installed After Other Products 175
Scenario 4: HPE OBR is installed after the other product installation and then again other product is installed 177
For Existing HPE OBR Installation 177
Configuring HPE OBR for External Vertica after Post Installation 177
Chapter 17: Configuring Logon Banner for HPE OBR 179
Enabling the Logon Banner 179
Disabling the Logon Banner 181
Chapter 18: Configuring FIPS for HPE OBR 183
HPE OBR in FIPS Mode 183
Considerations When Running OBR in FIPS Mode 184

Configure HPE OBR for FIPS 140-2 Compliance 184
Prerequisites: 184
Chapter 19: Change the Vertica Data Storage Location 190
Chapter 20: Configuring TLS for Vertica 191
Configure TLS for Vertica in Typical Scenario 191
On Vertica: 191
On OBR: 195
Configure TLS for Vertica in Distributed Scenario 197
On Vertica: 197
On OBR: 200
On Remote Collector: 204
Part IV: Database Backup and Recovery 206
Chapter 21: Database Backup and Recovery 207
Backup of HPE OBR Components 208
Create Full Backup of HPE OBR on Windows 208
Create Full Backup of HPE OBR on Linux 214
Restore HPE OBR Components 215
Restore Backup of HPE OBR on Windows 215
For SAP BusinessObjects Database and File Store 215
For Management Database Table 228
Restore Backup of HPE OBR on Linux 229
For SAP BusinessObjects Database and File Store 229
For Management Database Table 242
Back up and Restore Vertica Database 243
Part V: Appendix 244
Appendix A: Status, Stopping and Starting HPE OBR Services 245
On Linux 245
On Windows 248
Appendix B: SiteScope Monitors for HPE OBR 252
Appendix C: Installing SAP BusinessObjects Dashboards (Earlier known as Xcelsius) 258
Hardware and Software Requirements 258
Installing SAP BusinessObjects Dashboards (Optional) 258
Appendix D: Listing of ETLs 259
Appendix E: System Management Reports with SiteScope data source 265

Send documentation feedback 269

Part I: HPE OBR Overview and Planning

HPE 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. HPE 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.

HPE Operations Bridge Reporter collects data from different data sources, processes the data, and generates reports with the processed data. HPE 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 HPE OBR collects data from RTSM, HPOM, BSM Profile database, BSM Management database, Operations Manager i (OMi), HP SiteScope, HP Network Node Manager i (NNMi) as well as from the NNM iSPI Performance for Metrics, HP Operations Agent, and HP Cloud Optimizer.

All the components of HPE Operations Bridge Reporter can be installed on a single system. If a single system is not capable of supporting all the components of HPE 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 HPE Operations Bridge Reporter collector on different systems. It reduces the network load and ensures connectivity to the data sources.

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

A topology model or view, logically maps and relates your business services to your IT elements. HPE 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
January 2017	Initial release.

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 4.1.
- 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:

    `/opt/HP/BSM/BOE4/sap_bobj/enterprise_xi40/warfiles/webapps/CMCDoc/en` (**On Linux**)
  - For information on BI Launchpad (creation of reports, report functions and other admin tasks like

scheduling), go to:

`/opt/HP/BSM/BOE4/sap_bobj/enterprise_xi40/warfiles/webapps/InfoViewDoc/en` (**On Linux**)

OMi Management Packs

- For information on OMi Management Packs and other contents, see HP Live Network Content Catalog.

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 17
3. "Determine the Readiness" on page 18
4. " Licensing Requirement for HPE OBR" on page 19

Know your Deployment Scenarios

The following deployment scenarios are supported by HPE OBR:

- Deployment with BSM/OMi
- Deployment with HP Operations Manager
- Deployment with VMware vCenter
- Other Deployments

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

> **Note:** HPE 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/Operations Manager i

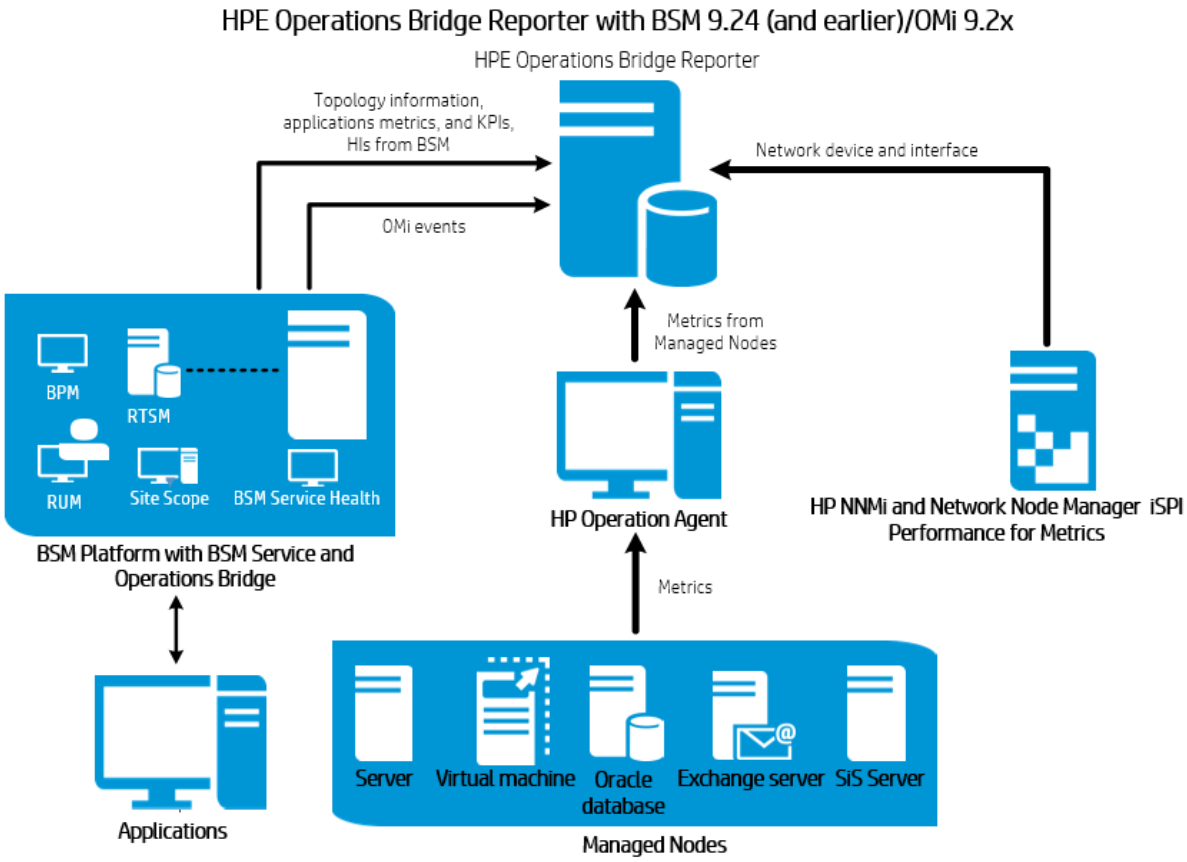
In this deployment, Run-time Service Model (RTSM) is the source of topology information. HPE OBR discovers and synchronizes topology information from RTSM. In a BSM with RUM, BPM, SiteScope and OMi 9.2x scenario, this synchronization technique receives data from HP Operations Agent, NNMi, NNM iSPI Performance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

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

Additionally, you can configure HPE 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.

HPE Operations Bridge Reporter with BSM 9.24 (and earlier)/OMi 9.2x

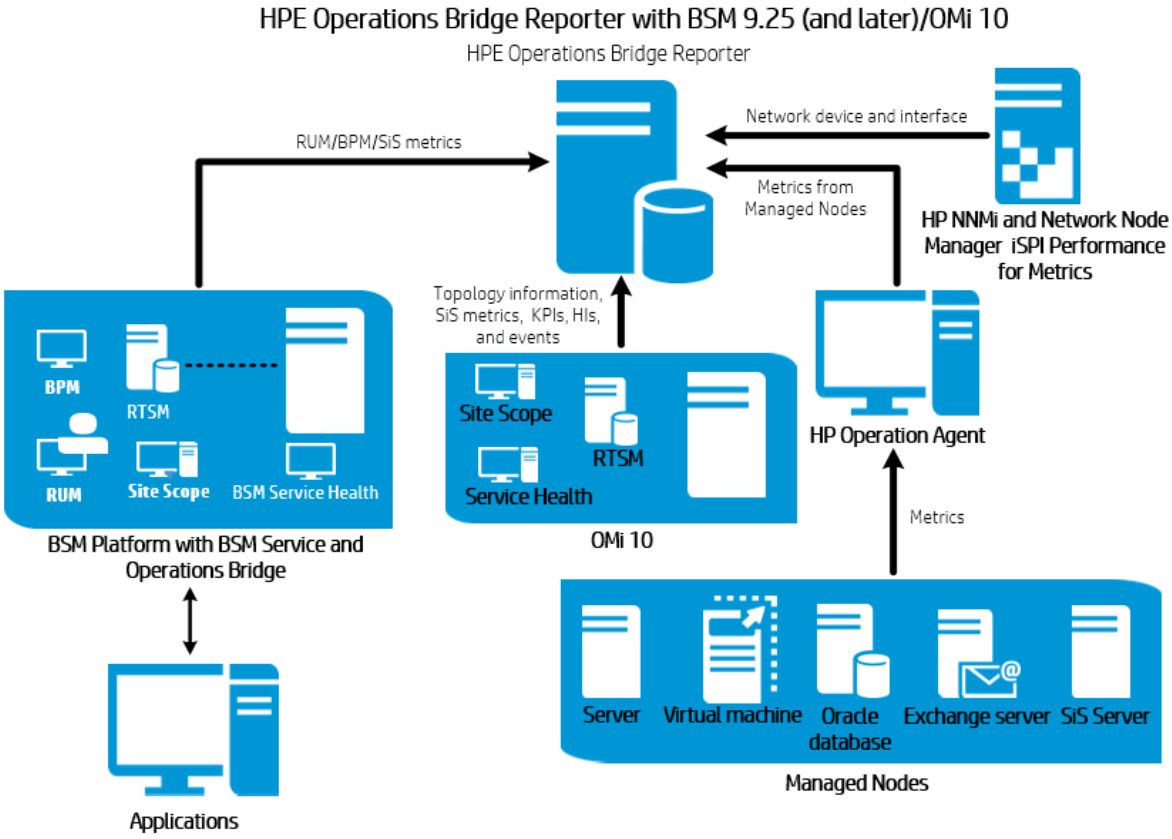
The following diagram shows the flow of data from HP Operations Agent, NNMi (direct), NNM iSPI Performance for Metrics, and topology information from RTSM in a BSM environment with underlying HPOM servers.



HPE Operations Bridge Reporter with BSM 9.25 (and later)/OMi 10

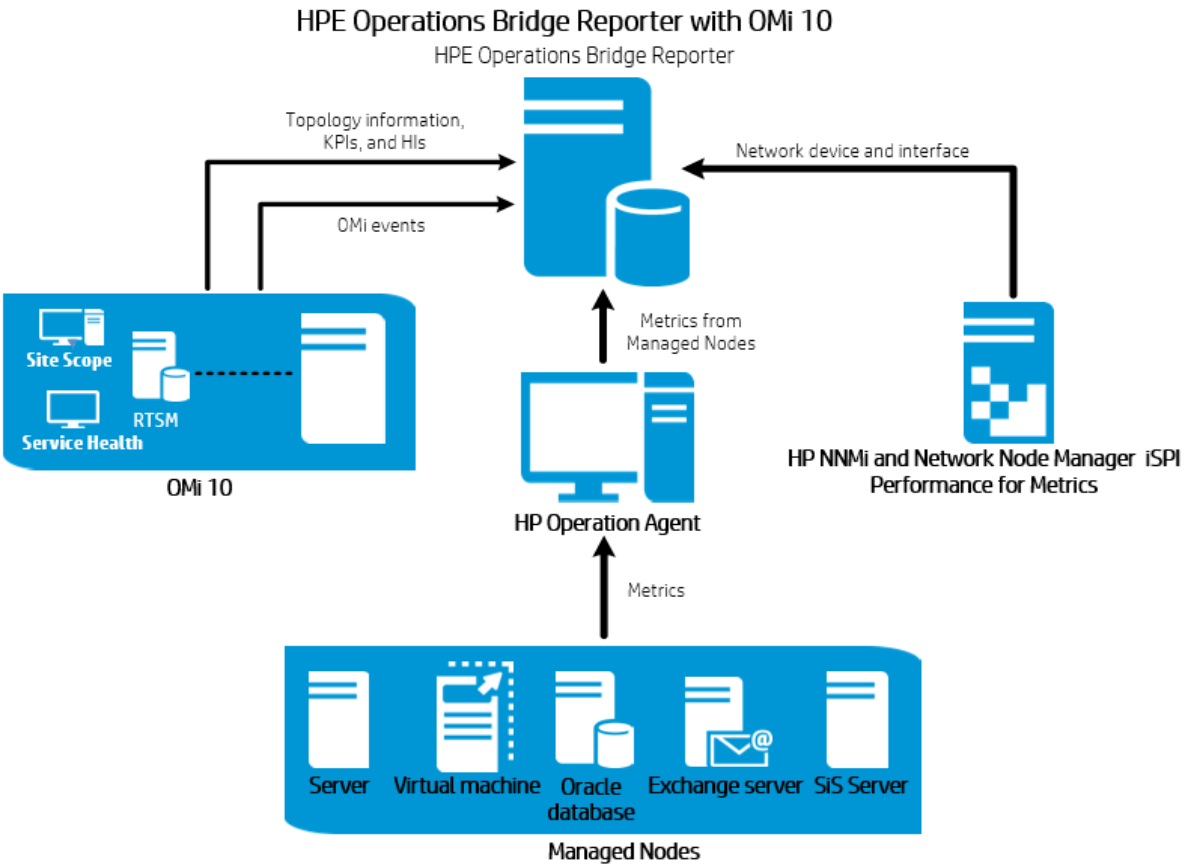
The following diagram shows the flow of data from HP Operations Agent, OMi 10, NNMi (direct), NNM iSPI Performance for Metrics, and topology information from RTSM in an BSM and OMi 10 environment.

You can configure BSM 9.25 (or later) and OMi 10 as standalone topology and data sources. You can also setup BSM 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 system provides fact data from RUM, BPM, and SiteScope that are directly configured with it.



HPE Operations Bridge Reporter with OMi 10

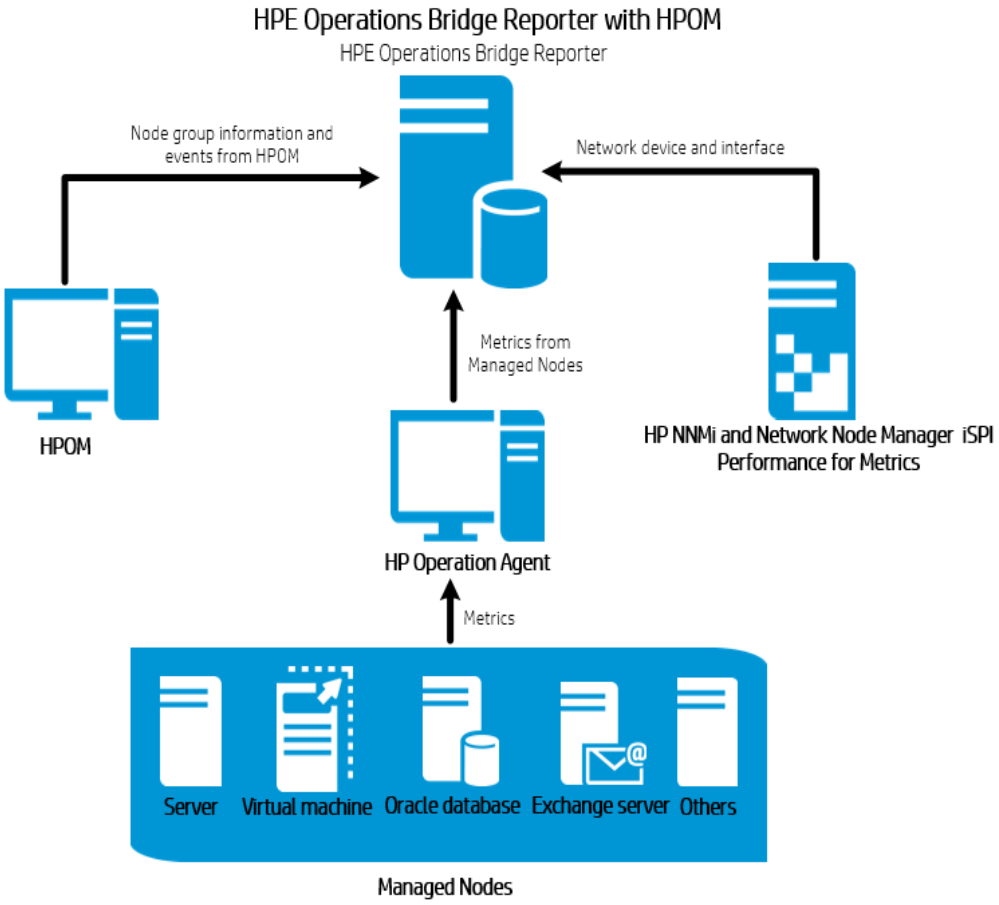
The following diagram shows the flow of data from HP Operations Agent, NNMi (direct), NNM iSPI Performance for Metrics, and topology information from RTSM in an OMi 10 environment.



HP Operations Manager

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

You can configure HPE 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.

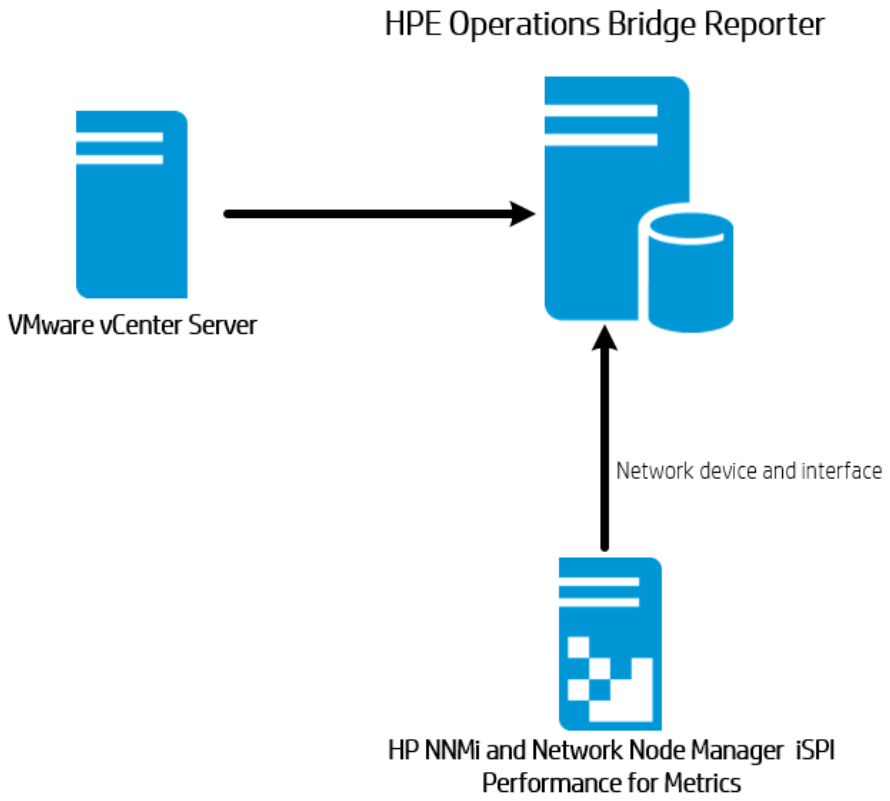


VMware vCenter

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 HPE OBR.

You can configure HPE 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

  HPE OBR integrates with and collects historical network-related data for the network nodes from NNM iSPI Performance for Metrics. HPE 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 HPE OBR must collect from each of these data sources. The corresponding dimension data is collected from the RTSM or HPOM 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.

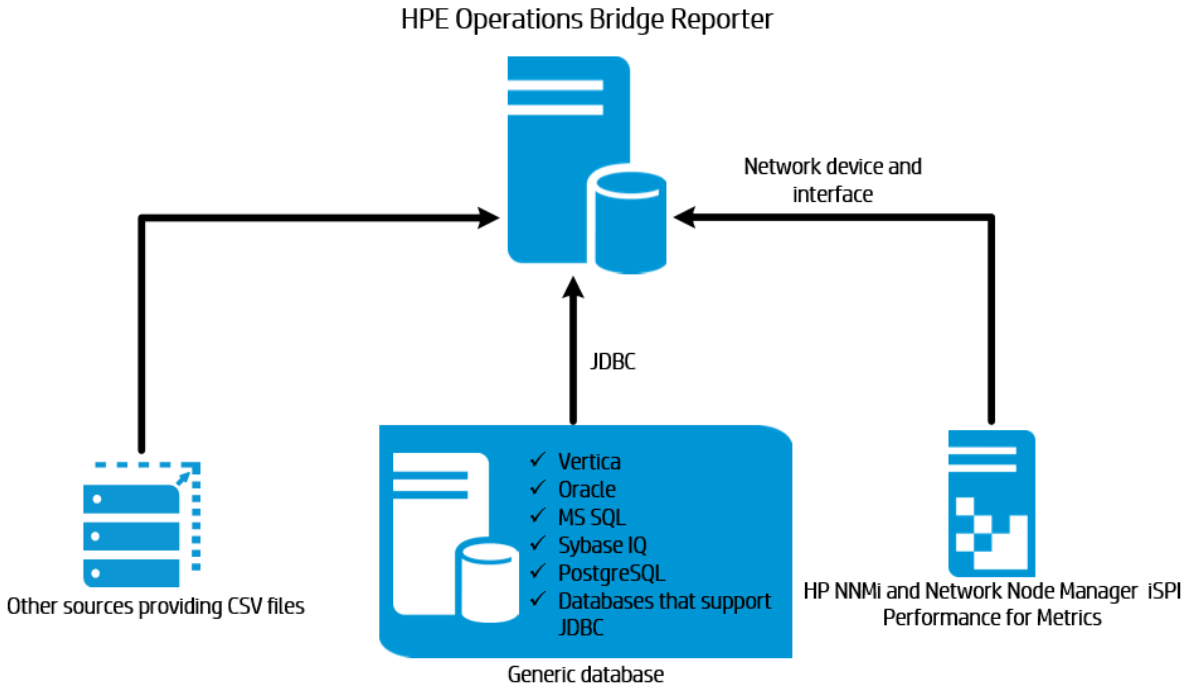
HPE OBR also collects network performance data directly from HP Network Node Manager i (NNMi). The Network Component Health Content Pack and Interface Health Content Pack identifies the metrics that HPE OBR must collect from the data sources.

- Deployment with other applications using JDBC

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

- Deployment with other applications using CSV

  HPE 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

HPE OBR collects data from other HP monitoring products like HP SiteScope, HP Operations Agent (OA), HP Operations Manager (OM), Business Process Management (BPM), 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 HPE OBR to collect data from the HP monitoring products and third party data source. HPE OBR can then report on the data collected from the configured data sources.

HPE 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 HPE 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 HP monitoring products deployed in your environment before you integrate them with HPE OBR. Ensure that HPE OBR supports the versions of the HP products deployed in your environment.

For more information on the versions supported by HPE OBR, see *HPE Operations Bridge Reporter Support Matrix*.

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

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

HPE Monitoring Products	Readiness Check List
HP SiteScope	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 HPE OBR " on page 252. You must ensure to integrate Sitescope with BSM to collect system performance data from HP SiteScope. You must either install SysPerf_ETL_SiS_DB for HPE OBR to collect data from the BSM Profile database or install the SysPerf_ETL_SiS_API to collect data logged from the SiteScope API. For more information on ETLs, see Appendix C: Listing of ETLs.
NNMi	HPE 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 HPE OBR. If HPE 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.
VMware vCenter	You must ensure that a proper connection is established between VMware vCenter server and HPE OBR system.

Licensing Requirement for HPE OBR

This section provides information on licensing requirements for HPE OBR. This section also provides information on various HPE 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:

- **HPE 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. *Operations Bridge Reporter Standard* and Operations Bridge Reporter*Advanced* editions can also be bought as stand-alone products. To benefit from the HPE 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 Advance edition

Stock-keeping Unit (SKU): TJ756AAE

The Operations Bridge Reporter Advance edition includes the following:

- All Content Packs
- 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 HPE Operations Bridge Reporter . Storing any other data other than that of HPE 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 Packs for System Performance and Events
- 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 HPE Operations Bridge Reporter. Storing any other data other than that of HPE 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 HPE OBR.

For information on custom content license, see *HPE 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 HP Password Center**. HPE partners and employees can still continue to use the HPE Licensing for Software website.

To view the HPE OBR License Details, log on to Administration Console and go to **Administration > 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 **Administration > 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/`

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

   > **Note:** By default HTTPs is enabled for HPE OBR. You can also launch Administration Console using `http://<OBR_Server_FQDN>:21411/` 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 **Home** page is displayed.
4. Click **Administration > Licensing**. The **Licensing** page appears with HPE OBR License Details.
5. Click **Launch HP Password Center**. The **Welcome to HP Licensing** page appears.
6. In *Licensing Support links*, click **Hewlett Packard Enterprise Software Licenses and Downloads**.
7. Log on to HP Passport with your user ID and password. If you do not have an account, you must create one before you can proceed.
8. Follow the instructions provided on the website to obtain license keys.

OR

1. Go to the HPE Software Licensing website.
2. Log on to HP Passport with your user ID and password. If you do not have an account, you must create one before you can proceed.
3. Follow the instructions provided on the website to obtain license keys.

Installing the Permanent License Key

To install the permanent license, follow these steps:

1. Log on to the HPE OBR system with the same user name used during the installation of HPE 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 BO Pack
   License Feature Id      :1004
   Active License Type     :Instant On
   Days to License Expiry  :60
   License Entitlement     :50
   (2) License Feature         :HPE Operations Bridge Reporter Server
   License Feature Id      :1002
   Active License Type     :Instant On
   Days to License Expiry  :60
   License Entitlement     :50
   (3) License Feature         :HPE Operations Bridge Reporter Collector
   License Feature Id      :1006
   Active License Type     :Instant On
   Days to License Expiry  :60
   License Entitlement     :50
   ```
4. You must restart the administrator service to apply the installed license. To restart the **HPE_PMDB_Platform_Administrator** service on the HPE OBR system, follow these steps:

   On Windows:

   a. Click **Start > Run**. The Run dialog box is displayed.

   b. Enter **service.msc** in **Open**. The **Services** windows is displayed.

   c. On the right pane, right-click on the **HPE_PMDB_Platform_Administrator** service and then

click **Restart**.

d. Close the Services window.

On Linux:

a. Type the following command at the command prompt:

RHEL 6.x: `service HPE_PMDB_Platform_Administrator restart`

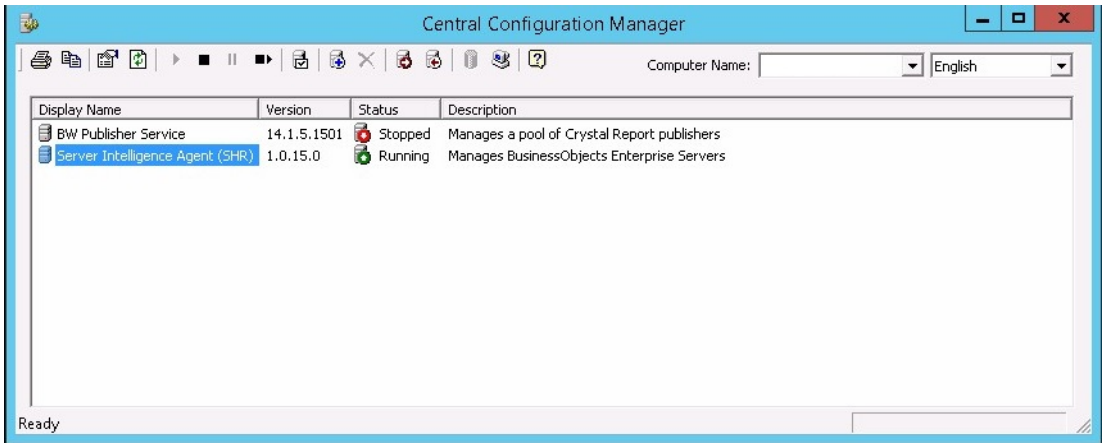
RHEL 7.x: `sytemctl restart HPE_PMDB_Platform_Administrator.service`

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 HPE 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 HPE OBR

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

Chapter 2: Post-Install Configuration

This section contains sub sections that describes tasks to complete post-install configuration of HPE OBR.

After HPE OBR is installed, launch the Administration Console for post-install configuration. The Administration console helps you to configure HPE 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 your HPE OBR system. You can also configure HPE OBR databases and collectors. After completing tasks in Configuration Wizard, the Deployment Manager page is displayed.

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 131. If you want to install additional Content Packs or configure data source, see "Install and Uninstall the Content Packs" on page 96 and "Data Source Configuration" on page 106 respectively.

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

> **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 *HPE Operations Bridge Reporter Interactive Installation Guide*.

Secure Communication

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

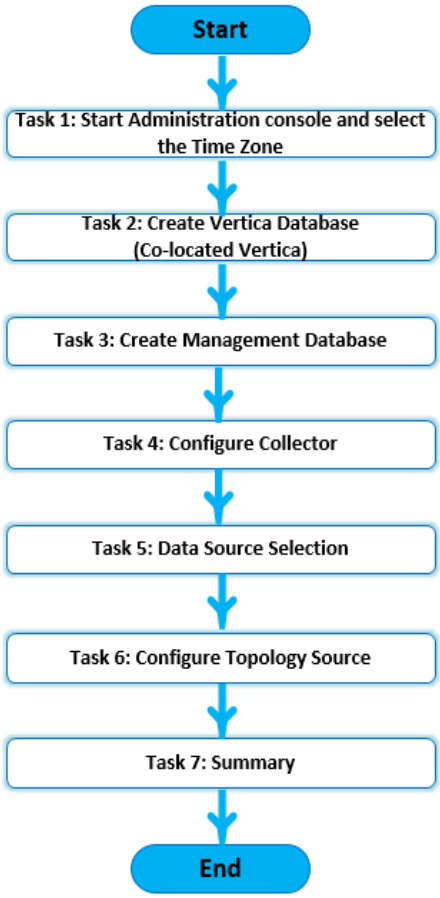
- Vertica and HPE OBR server /SAP BusinessObjects
- OBR collector and BSM/OMi Oracle database
- OBR collector and BSM/OMi RtSM

Using the Administration Console, **Administration > Data Source Configuration** page, you can enable TLS for HP OM and BSM/OMi to connect with Oracle database using ODBC or JDBC. For more information, see "Data Source Configuration" on page 106.

Using the Administration Console, **Administration > Database Configuration** page, you can enable TLS for Vertica database. For more information, see "Configuring TLS for Vertica" on page 191.

Flow of tasks for typical scenario

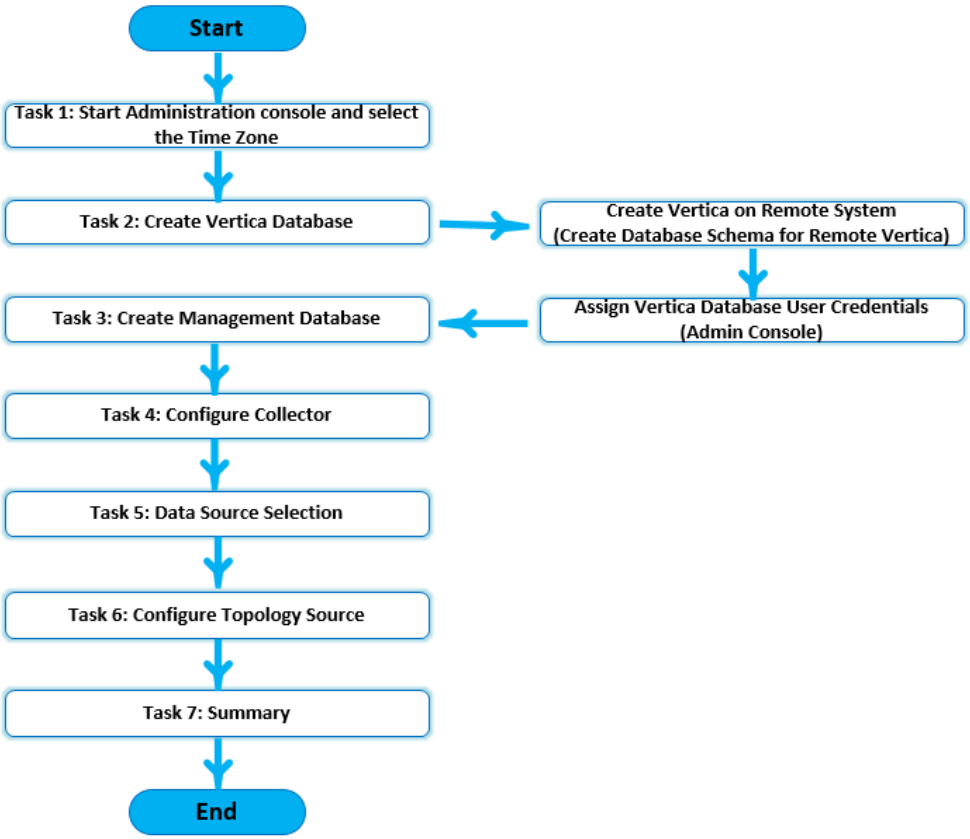
The following flowchart gives you an overview of the post-install tasks for HPE OBR where the HPE OBR and Vertica database are installed on the same system.



Flow of tasks for distributed scenario

The following flowchart gives you an overview of the post-install tasks for HPE 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 37.



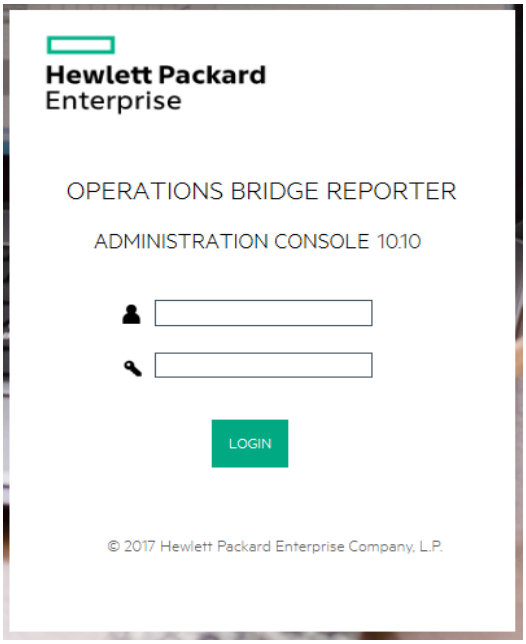
Task 1: Launching the Administration Console

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

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

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

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



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

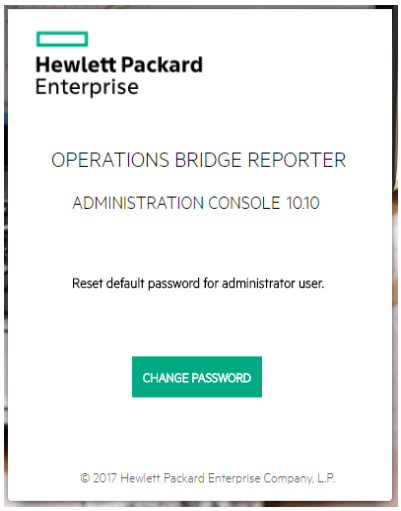
   The Administration Console page is displayed.

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

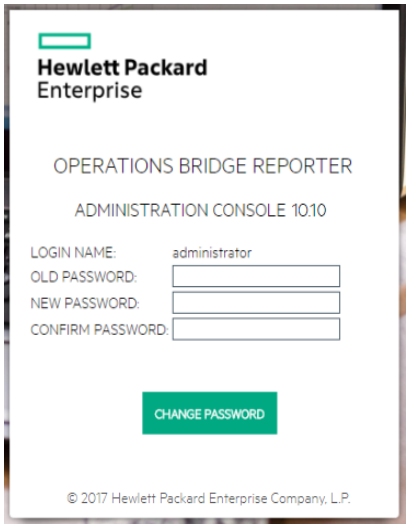
   b. If you have logged on to Administrator Console for the first time as **administrator** with a default password as **1ShrAdmin**, follow these steps:

      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.

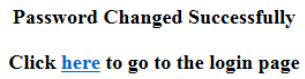


iii. Enter default password in **OLD PASSWORD** field.

iv. Enter new password in **NEW PASSWORD** field.

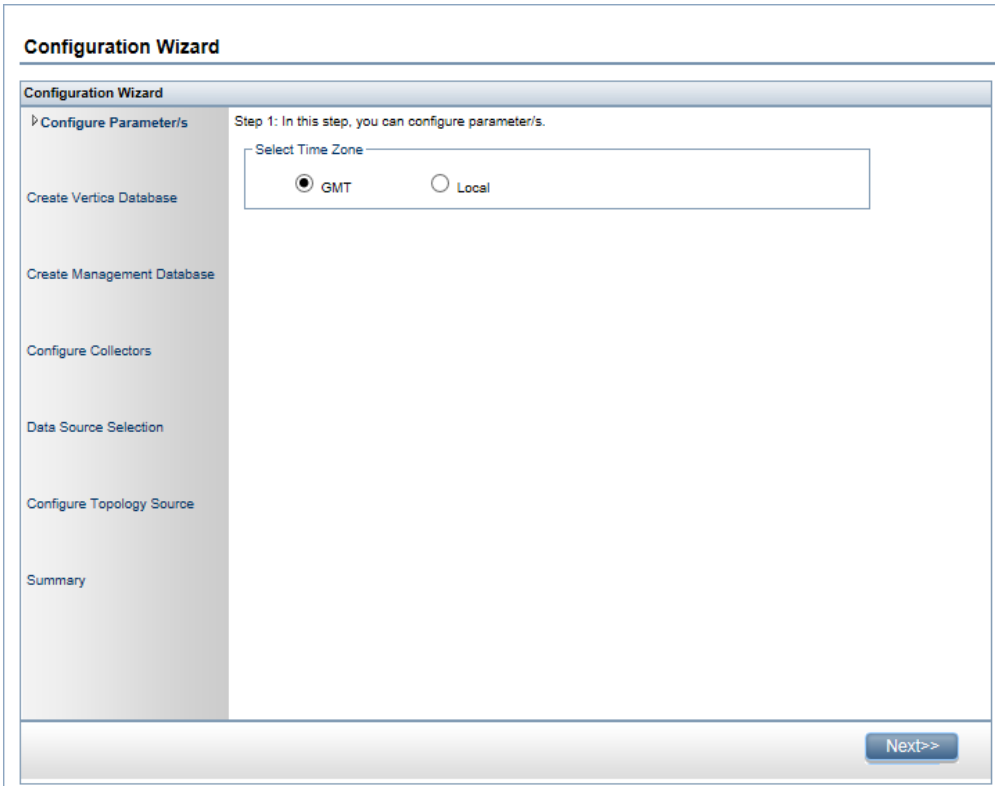
> **Note:** The password should be an alphanumeric value, with a combination of lower, upper cases, and number. The password must be minimum of six characters and maximum of 25 characters in length.

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 HPE 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.



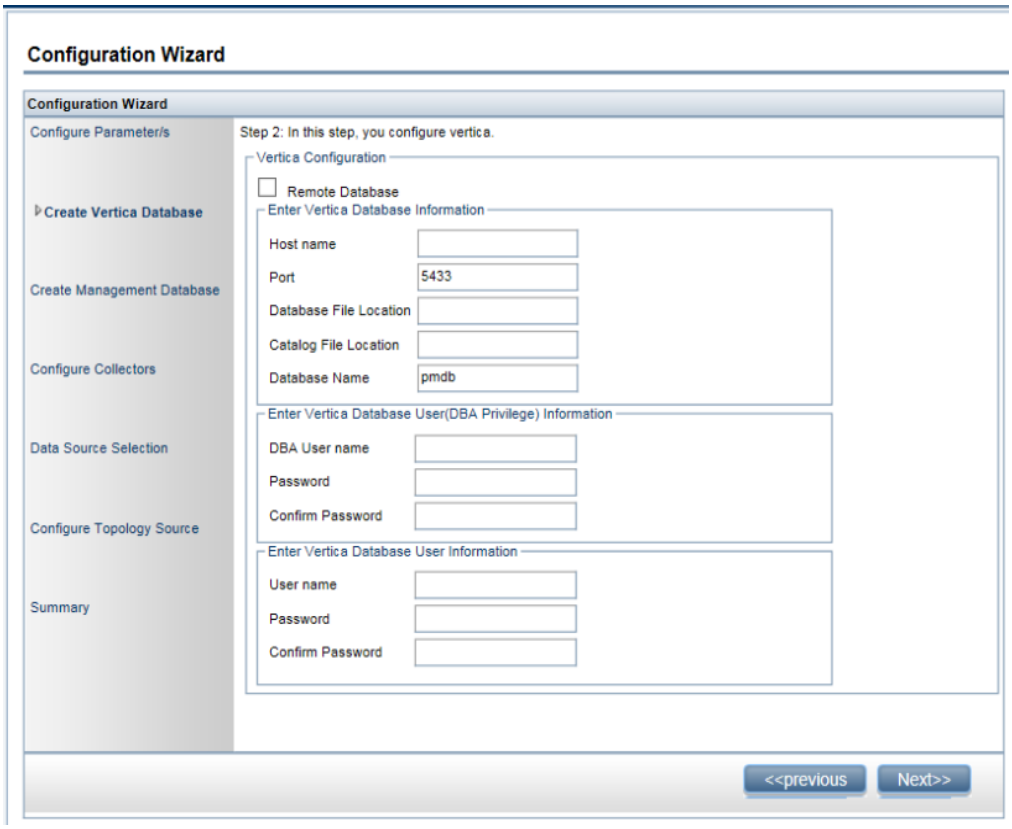
3. In the **Time Zone Selection** page, select the time zone, that is, GMT or Local, under which you want HPE OBR to operate.
   - Select **GMT** if you want HPE OBR to follow the GMT time zone.
   - Select **Local** if you want HPE OBR to follow the local system time zone.

   > **Note:** The time zone that you select here applies to the HPE 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 **Create Vertica Database** page is displayed.

Task 2: Creating the Vertica Database Schema

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



If Vertica database is embedded with HPE OBR, complete the task mentioned under "Creating Database Schema for Co-located Vertica" on the next page.

If Vertica database is located remotely, complete the task mentioned under "Creating Database Schema for Remote Vertica" on page 37.

You can configure HPE OBR to support external Vertica database. For information on configuring external Vertica database based on the scenarios, see "Configuring HPE OBR for External Vertica" on page 173.

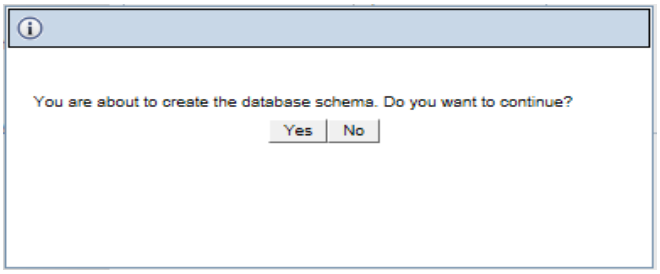
Creating Database Schema for Co-located Vertica

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

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

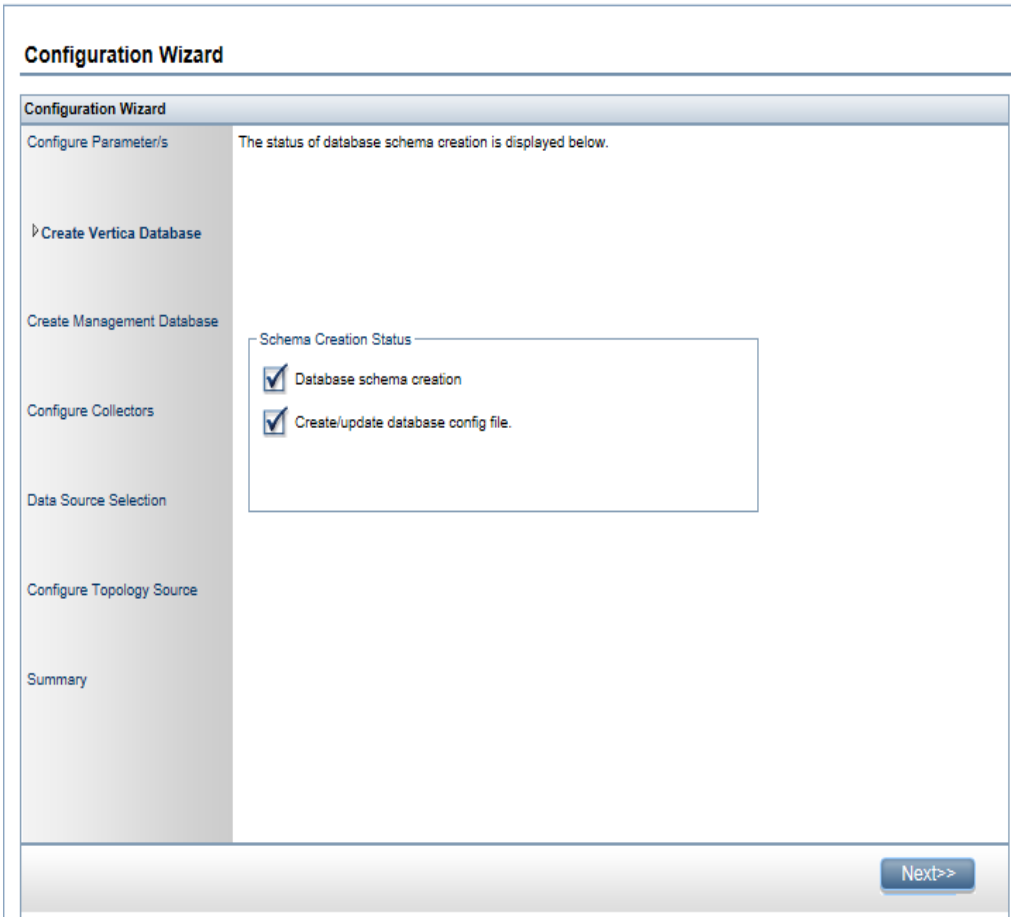
Field	Description
Remote Database	Select this option only if HPE OBR is installed with remote Vertica database and proceed with the steps given in Creating Database Schema for Remote Vertica.
Host name	Name of the host where the Vertica database server is running.
Port	Port number to query the database 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.
DBA User Name	Vertica database user name with DBA privilege to log on to Vertica database.
Password	Vertica database password to log on to the Vertica database.
Confirm Password	Retype the password to confirm it.
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.

A confirmation dialog box is displayed.



2. Click **Yes**.

   The **Schema Creation Status** is displayed.



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

3. Click **Next**. The **Create Management Database** page is displayed.

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

Creating Database Schema for Remote Vertica

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

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

On Remote System where Vertica is Installed:

To create vertica database on a remote system, run the following command on the 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>`

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

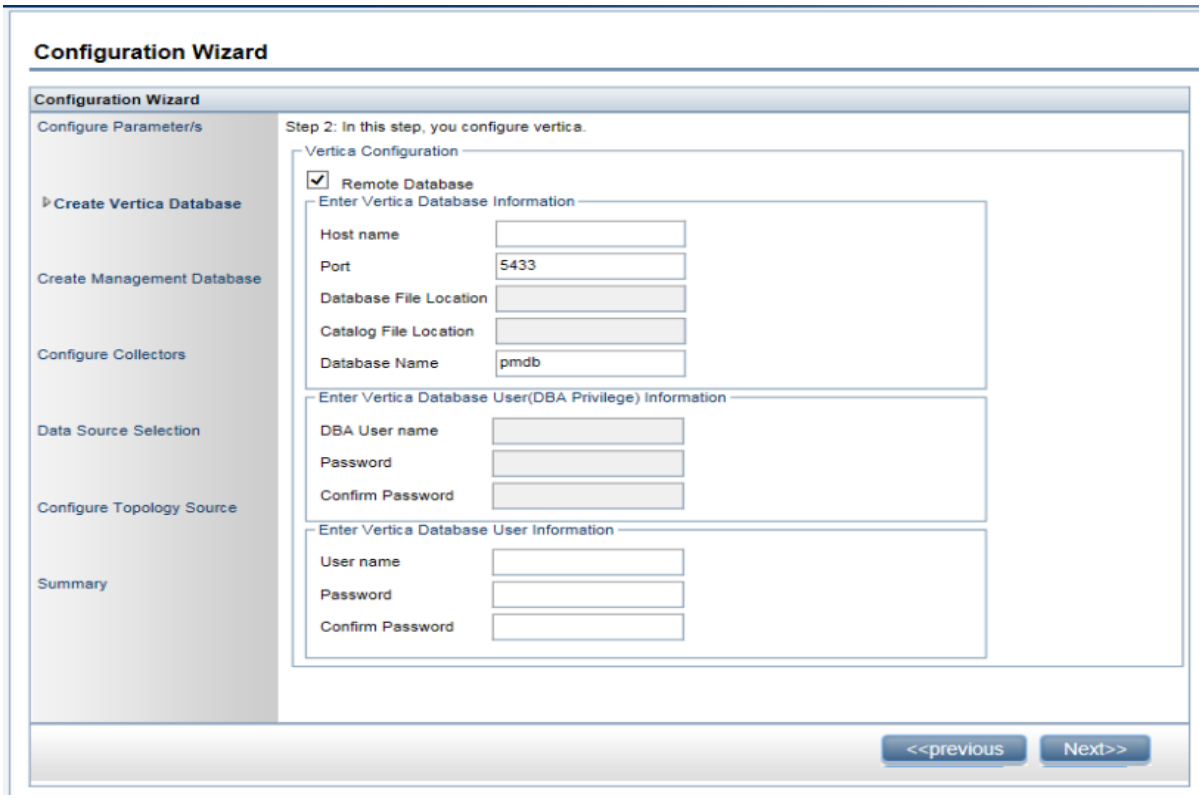
<Vertica Database User name> is the Vertica Database user name

<Vertica Database 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.

On System where HPE OBR is Installed:

During post install configuration, to configure Vertica database on system where OBR is installed, log on to the Administration Console on HPE OBR system. In the **Configuration Wizard > Create Vertica Database** step, enter the Vertica database configuration parameter as follows:



Field	Description
Remote Database	Select this option as Vertica database is created on a remote system.
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.
Database Name	Name of the Vertica database. By default, the database name is PMDB. You can edit the Vertica database name.
DBA User Name	Vertica database user name with DBA privilege to log on to Vertica database. 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.
User Name	Enter the Vertica database user name.

Field	Description
Password	Enter the Vertica database user name password.
Confirm Password	Retype the password for Vertica database user name to confirm.

Click **Next**. The **Create Management Database** page is displayed.

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

Caution: In a distributed scenario, if HPE 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 HPE OBR system (installed on Windows) to connect to Vertica database. If HPE 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 165.

Drop Vertica Database

To drop the Vertica database, follow these steps:

1. Open the command prompt and run the following commands:
   a. `su <Vertica User Name> -c "/opt/vertica/bin/adminTools -t stop_db -d <Database Name> -p <Vertica Database Password> -F"`
   b. `su <Vertica User Name> -c "/opt/vertica/bin/adminTools -t drop_db -d <Database Name>"`

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

   `<Vertica Database Password>` is the Vertica database password

   `<Database Name>` is the name of the Vertica database

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: `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

   `vsql`

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.

Verification on the HPE 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 HPE OBR system, run the following command on HPE OBR system:

`/opt/vertica/bin/vsql –U <Vertica User Name> –p 5433 –w <Vertica Database Password> –h <Verticahostname>`

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

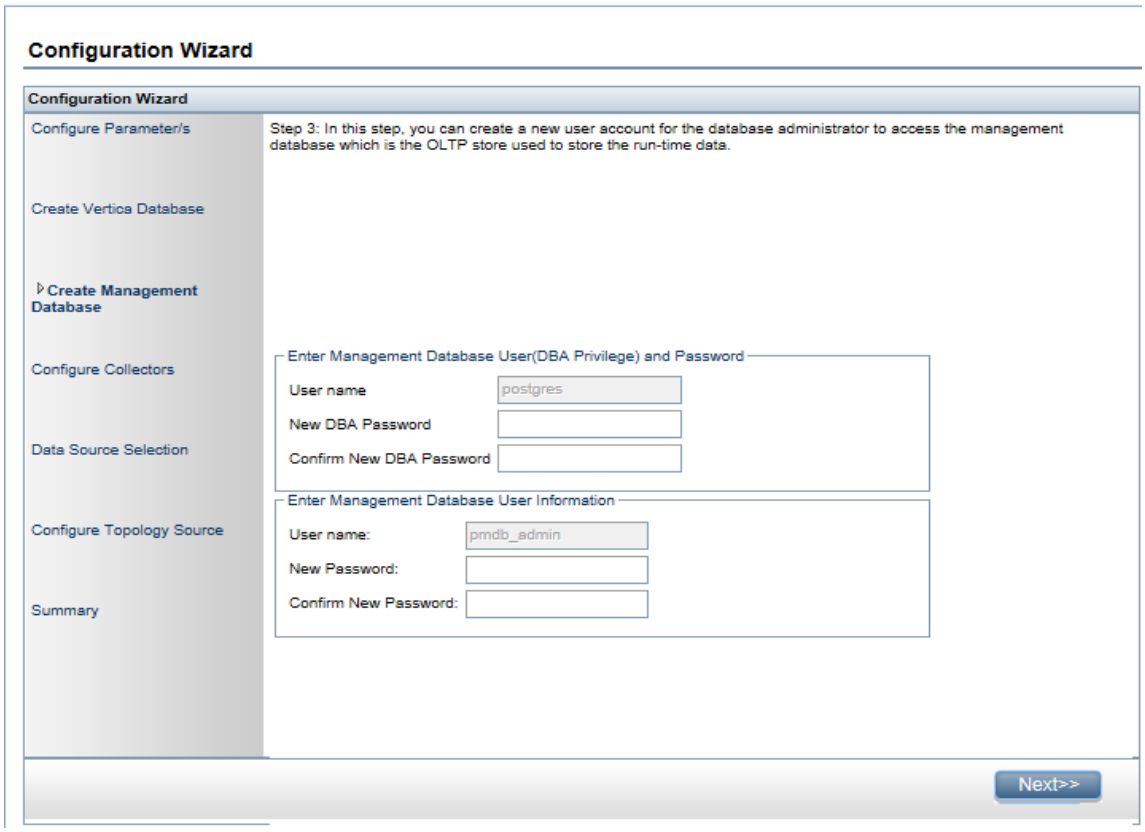
<Vertica Database Password> is the Vertica database password

<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 HPE 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 **Create Management Database** page, provide the user details for the management database.



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:

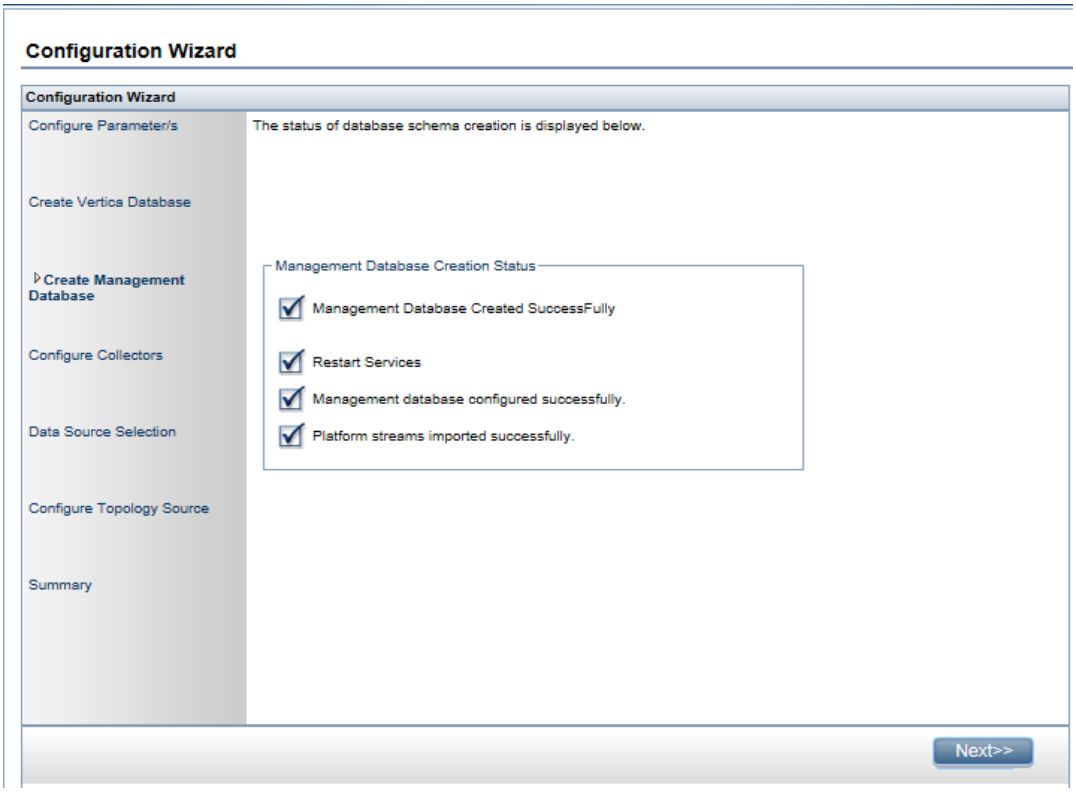
Field	Description
User name	Name of the PostgreSQL database administrator. The default value is `postgres`. You cannot edit this field.
New DBA Password	Enter the new password for PostgresSQL database administrator.
Confirm New DBA Password	Retype the same password to confirm it.

2. 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 `pmdb_admin`.

Field	Description
	You cannot edit this field.
New Password	Enter new password for management database user.
Confirm New Password	Retype the same password to confirm it.

3. Click **Next**. The **Management Database Creation Status** page is displayed.
4. Review the tasks completed as part of database connection and management database details and then click **Next**. The **Configure Collectors** page is displayed.



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 HPE 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: `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>"
```

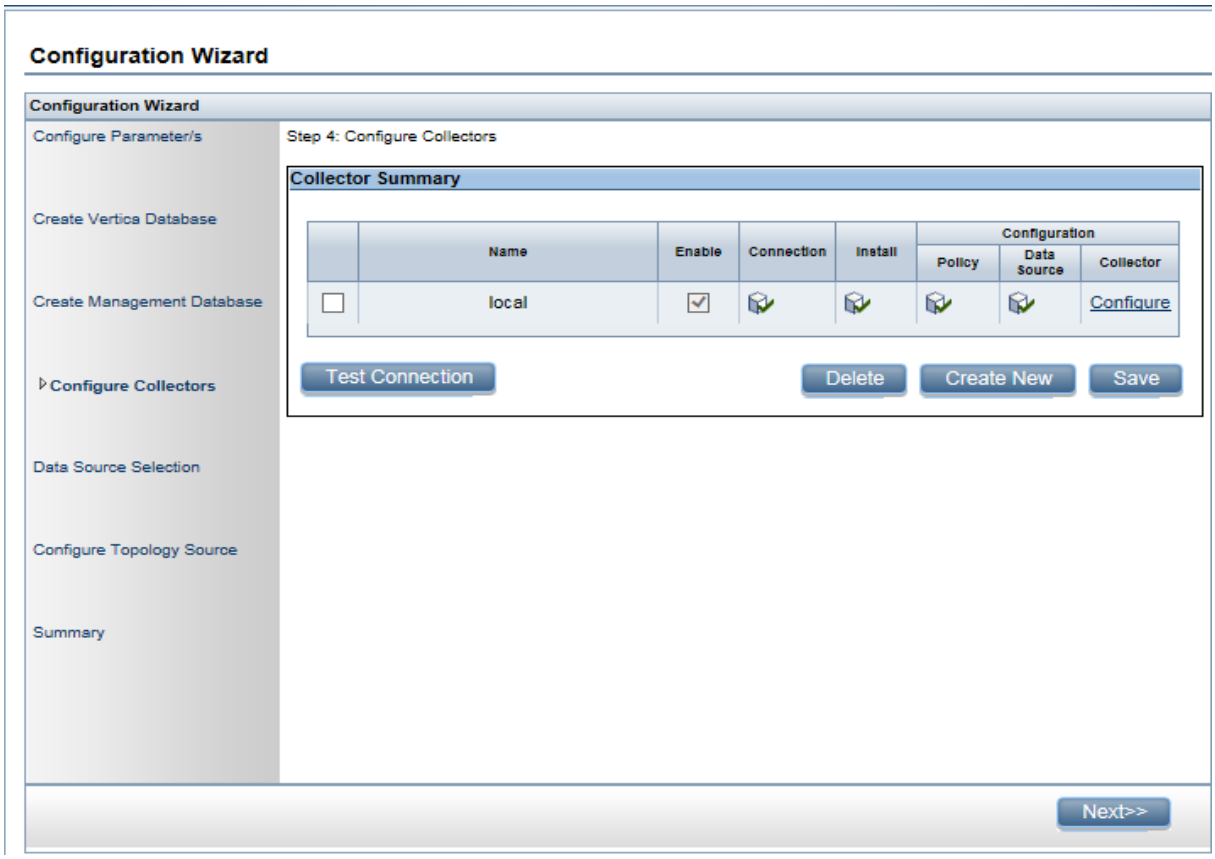
On Linux:

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

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

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

> **Note:** By default, the installer in HPE 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 **OK** to complete the creation of the collector and click **Save**.
3. 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: `service HPE_PMDB_Platform_Collection start`

     On RHEL 6.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.

4. Click **Next**. The **Data Source Selection** page is displayed.

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

Migrating Data from Older Versions (HP SHR 9.x)

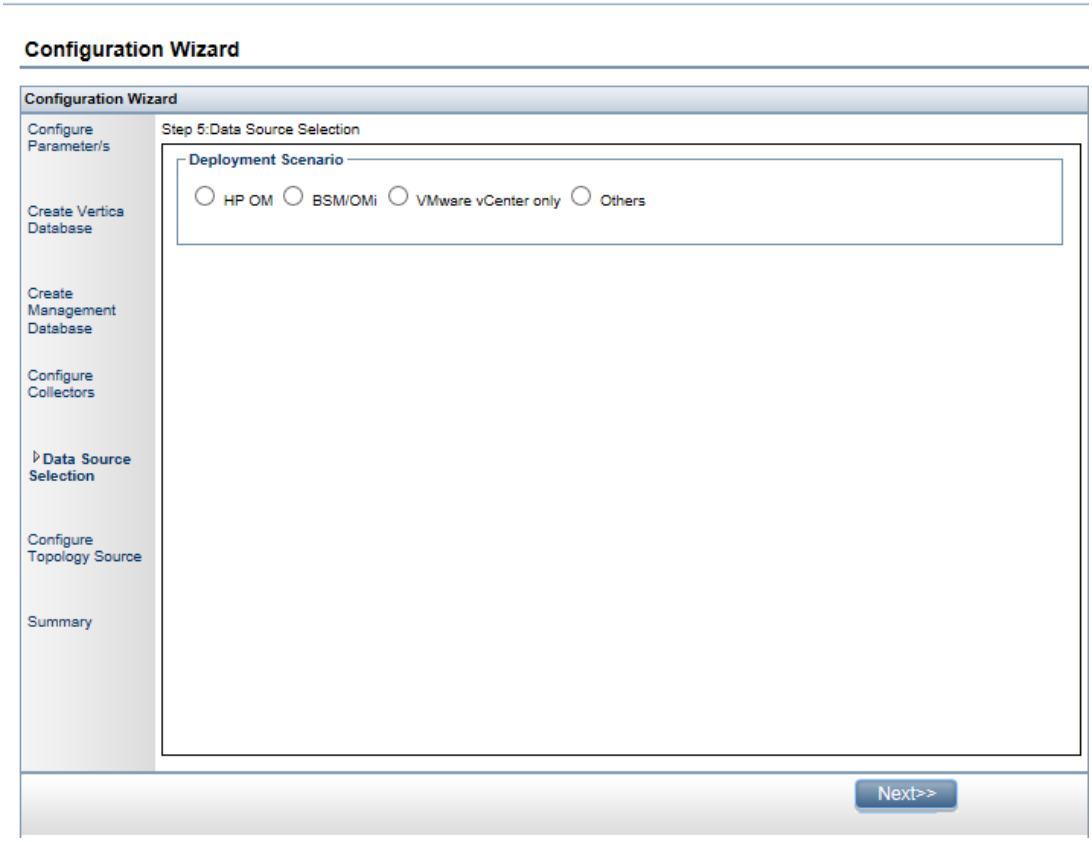
If you are migrating from older versions (HP SHR 9.x) then do not configure the data sources and topology source. Click **Next** to skip the **Data Source Selection** and **Configure Topology Source** steps and proceed with Content Pack deployment using the **Deployment Manager** page.

In the **Deployment Manager** page, select the Content Packs you want to install and click **Install/Upgrade**. For information on installing the Content Packs and list of ETLs available, see "Install and Uninstall the Content Packs" on page 96 and "Listing of ETLs" on page 259 respectively.

For information on migrating your data, see *HPE Operations Bridge Reporter Migration Guide*.

Task 5: Data Source Selection

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



Select one of the **Deployment Scenarios** - **HP OM**, **BSM/OMi**, **VMWare vCenter only**, or **Others**.

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

Deployment Scenario	Areas of Monitoring

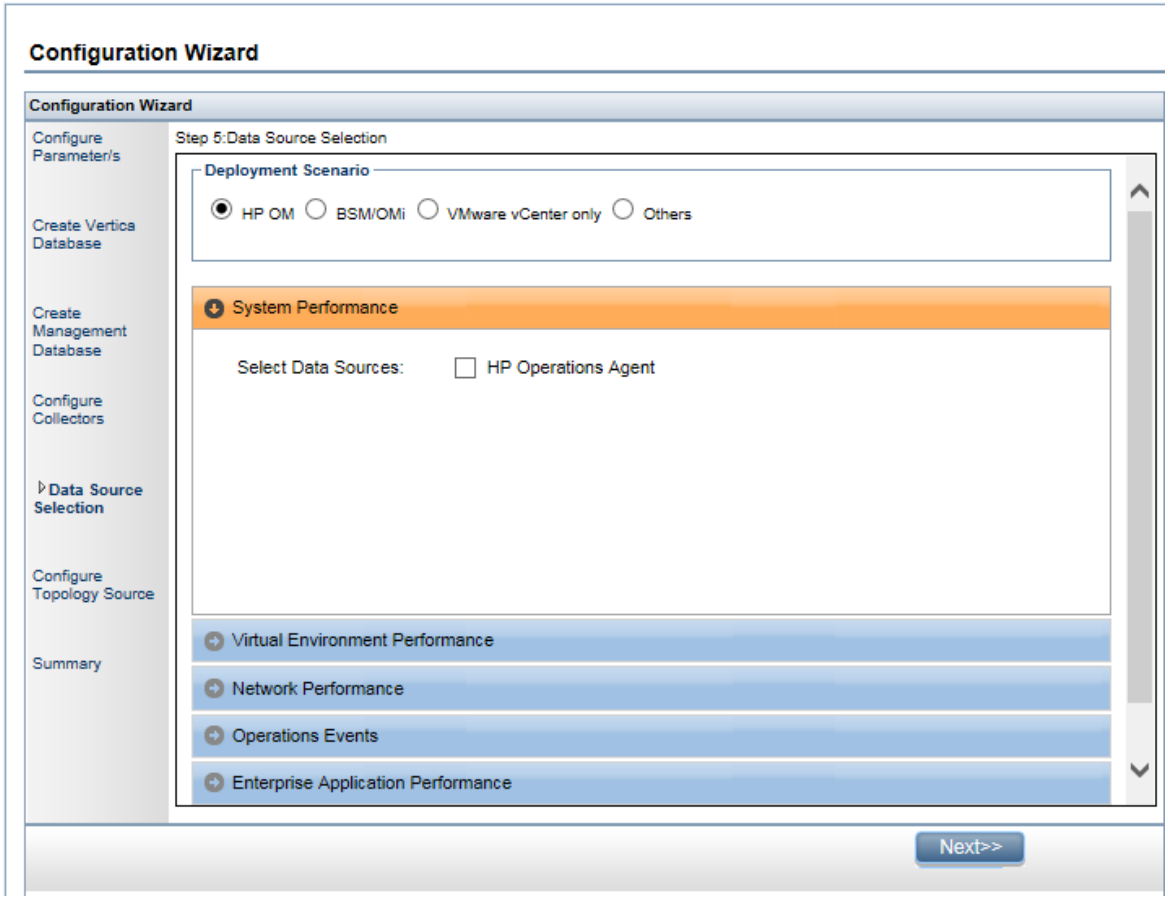
HP OM	• System Performance
	  ◦ HP Operations Agent
	• Virtual Environment Performance
	  ◦ HP Operations Agent
	  ◦ VMware vCenter
	• Network Performance
	• Operations Events

Deployment Scenario	Areas of Monitoring
	◦ HPOM Events • Enterprise Application Performance ◦ Microsoft SQL Server ◦ Microsoft Exchange Server ◦ Microsoft Active Directory ◦ Oracle ◦ Oracle Weblogic Server ◦ IBM Webshpere Application Server
BSM/OMi **BSM 9.2x or OMi 10**	• System Performance ◦ HP Operations Agent ◦ SiteScope • Virtual Environment Performance ◦ HP Operations Agent ◦ SiteScope ◦ VMware vCenter • Network Performance • Operations Events and KPI ◦ HPOM Events ◦ OMi Events ◦ HP Service Health • HP End User Monitoring ◦ HP Real User Monitor ◦ HP Business Process Monitor • Enterprise Application Performance ◦ Microsoft SQL Server ◦ Microsoft Exchange Server ◦ Microsoft Active Directory ◦ Oracle ◦ Oracle Weblogic Server ◦ IBM Webshpere Application Server
VMware vCenter only	• Virtual Environment Performance • Network Performance
Others	• Network Performance

Data Sources for the HPOM Deployment Scenario

To collect data for HPOM, follow these steps:

1. In the **Deployment Scenario**, click **HP OM**.



2. In the **System Performance**, select **HP Operations Agent**.
3. *(Optional)*. In the **Virtual Environment Performance**, select the data source for virtual environment.
4. *(Optional)*. In the **Network Performance**, select **Network Performance** if NNMi and the NNMi SPI Performance is available in your environment.
5. In the **Operations Event**, select **HPOM Events** for events.
6. In the **Enterprise Application Performance**, select the application.

   The **Select Technology** section appears.

7. 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.

   > **Note:** If you select **Microsoft Exchange Server** application then you must **Select Version of MS Exchange Server**.

8. Click **Save**. A summary of all the selection is displayed.
9. Click **Next**. The **Configure Topology Sources** page appears.

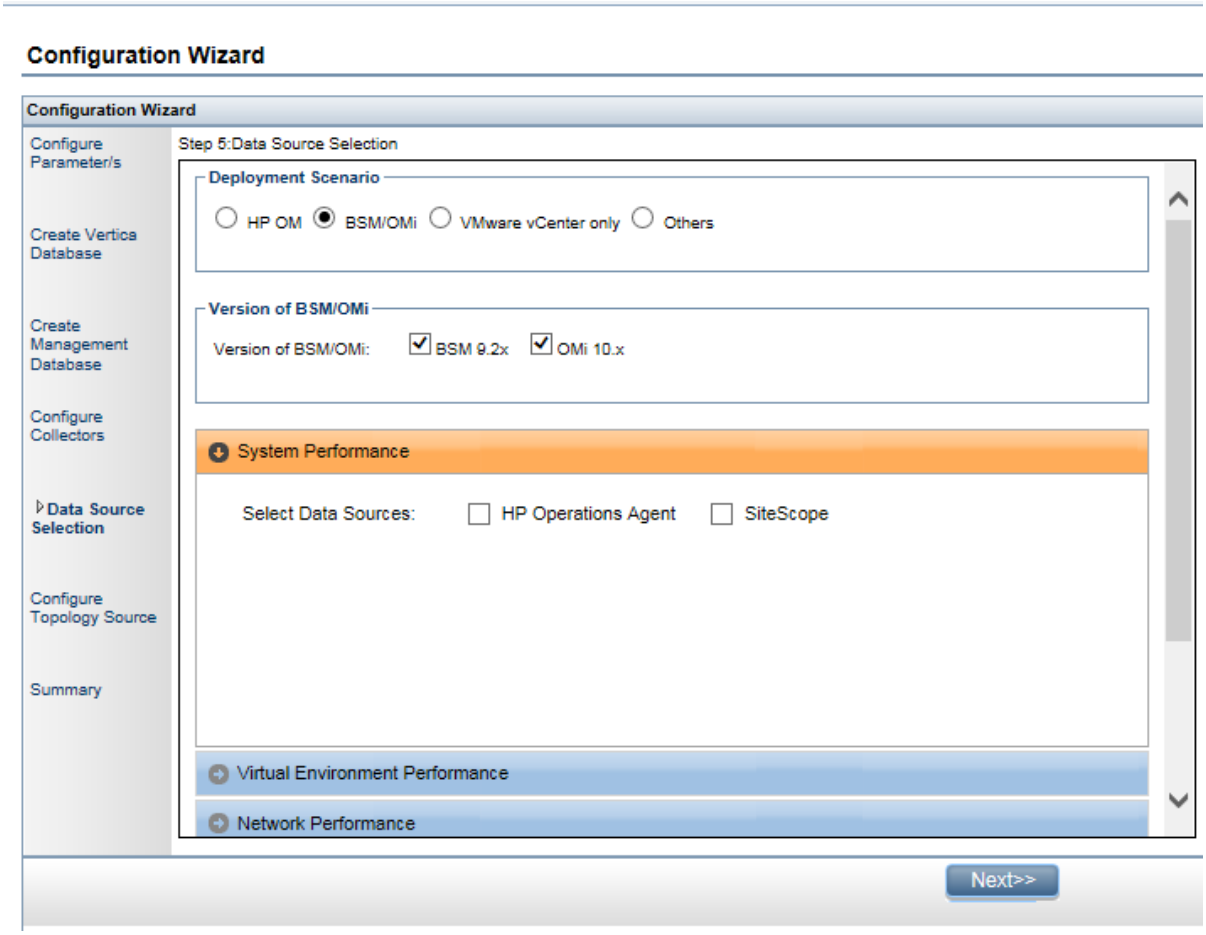
Data Sources for the BSM or OMi Deployment Scenario

You must configure the following data collectors in HPE 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, HPOM, and HP OMi databases.
- **HP Operations Agent collector** - to collect system performance metrics and data related to applications, databases, and system resources. The data is collected by the HP Operations Agents that are installed on the managed nodes.

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

1. In the **Deployment Scenario**, click **BSM/OMi**.



2. In the **Version of BSM/OMi**, select the version of the application.

   If you have only BSM deployed in your environment, select **BSM 9.2x**. If you have only OMi 10.x deployed in your environment, select **OMi 10.x**. If you have both BSM and OMi 10.x deployed in your environment and BSM and OMi 10 systems are integrated, select both **BSM 9.2x** and **OMi 10.x**.

   For additional deployment configurations using BSM and OMi, see:

   - "OMi10 Topology Source with Integrated BSM"
   - " OMi10 Topology Source after BSM Upgrade"

3. In the **System Performance**, select the required data source for the system.

   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.

> **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)*. In the **Virtual Environment Performance**, select the data source for the virtual environment. Select the technology for the data source.

Data Source	Select Technology
HP Operations Agent	VMware IBM LPAR Microsoft Hyper-V Solaris Zones
SiteScope	VMware **Note:** For virtual environment performance, you must also select the metric channel. For OMi 10.x, you can collect data for SiteScope only through Direct API.
VMware vCenter	VMware

5. *(Optional)*. In the **Network Performance**, select **Network Performance** to collect metrics on your network environment.
6. In the **Operations Event and KPI**, select the data sources for required events.
7. In the **HP End User Monitoring**, select the data source for the components monitored by BSM.

> **Note:** If the deployment is for OMi 10.x, this parameter is disabled.

8. In the **Enterprise Application Performance**, select the application.

   The **Select Technology** section appears.

9. 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.

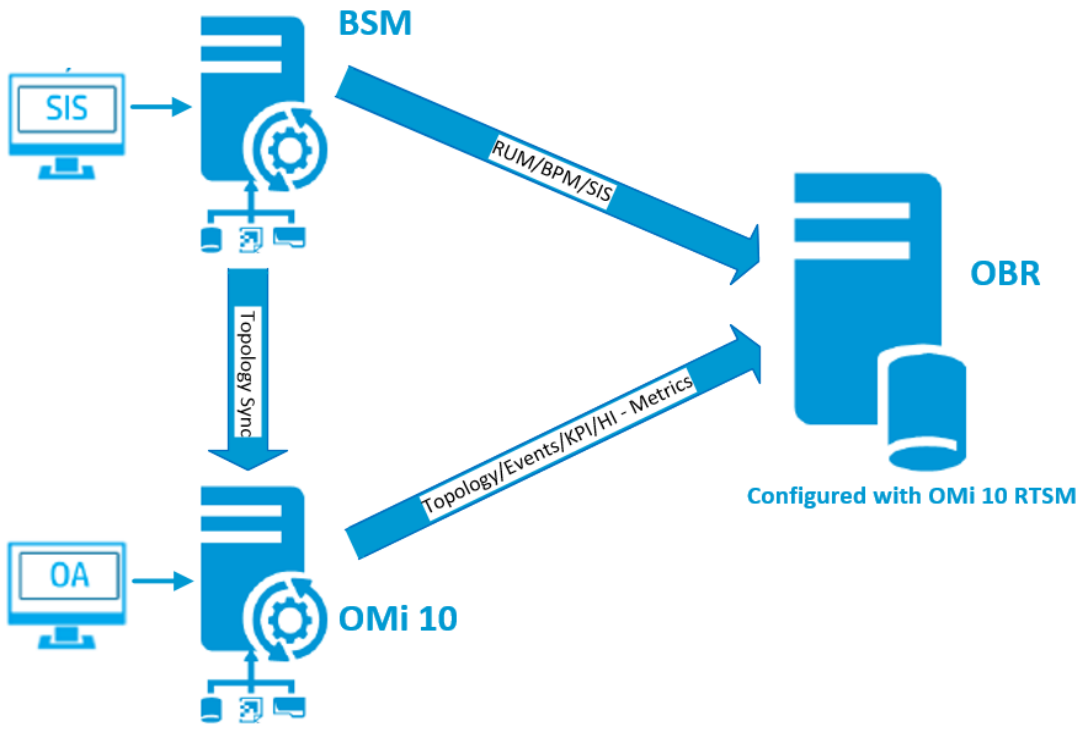
> **Note:** If you select **Microsoft Exchange Server** application then you must **Select Version of MS Exchange Server**.

10. Click **Save**. A summary of all the selection appears.

11. Click **Next**. The **Configure Topology Sources** page is displayed.

OMi10 Topology Source with Integrated BSM

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



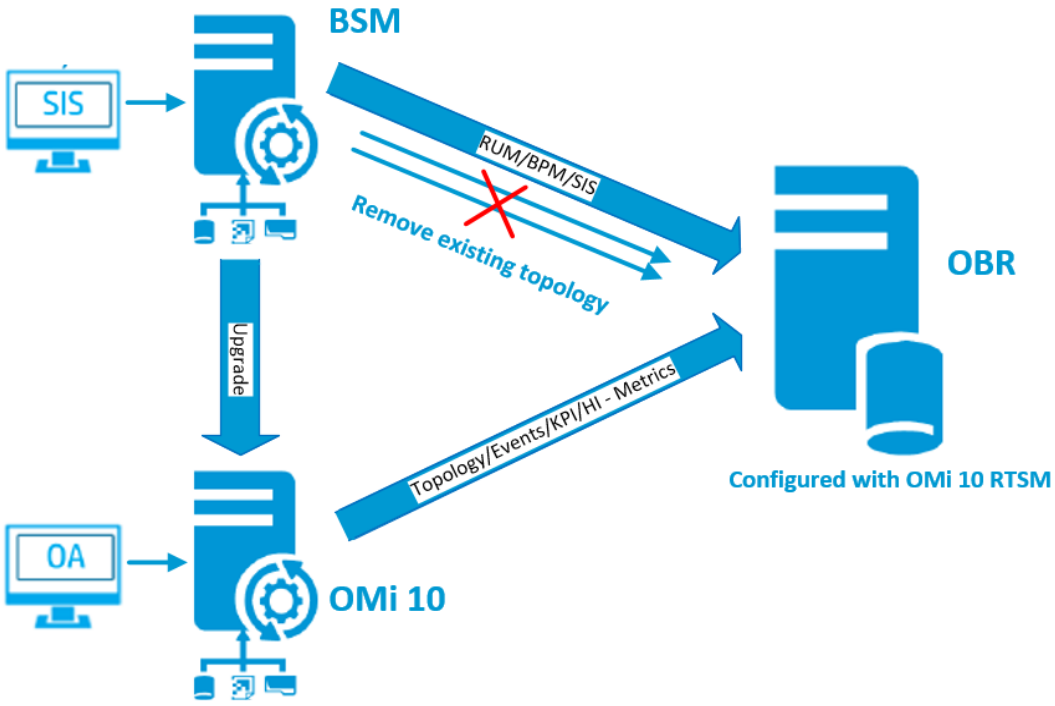
In this configuration, the OMi10 system provides topology data and fact data for Operations Events and KPI. The BSM system provides fact data from RUM, BPM, and SiteScope that are directly configured with it. For enabling topology sync between BSM and OMi10, see the respective documentation.

> **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.

To configure the topology source in OBR, see "Configuring RTSM Topology Source" on page 58

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 HPE 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 HPE 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 it. To perform the upgrade, follow these steps:

1. Stop collection service manually from the BSM systems.

   Wait until all data is loaded into HPE OBR tables

2. Complete the BSM to OMi10 upgrade process.

3. From the **Administration Console > Administration > Deployment Manager** 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 HPE 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;
      ```

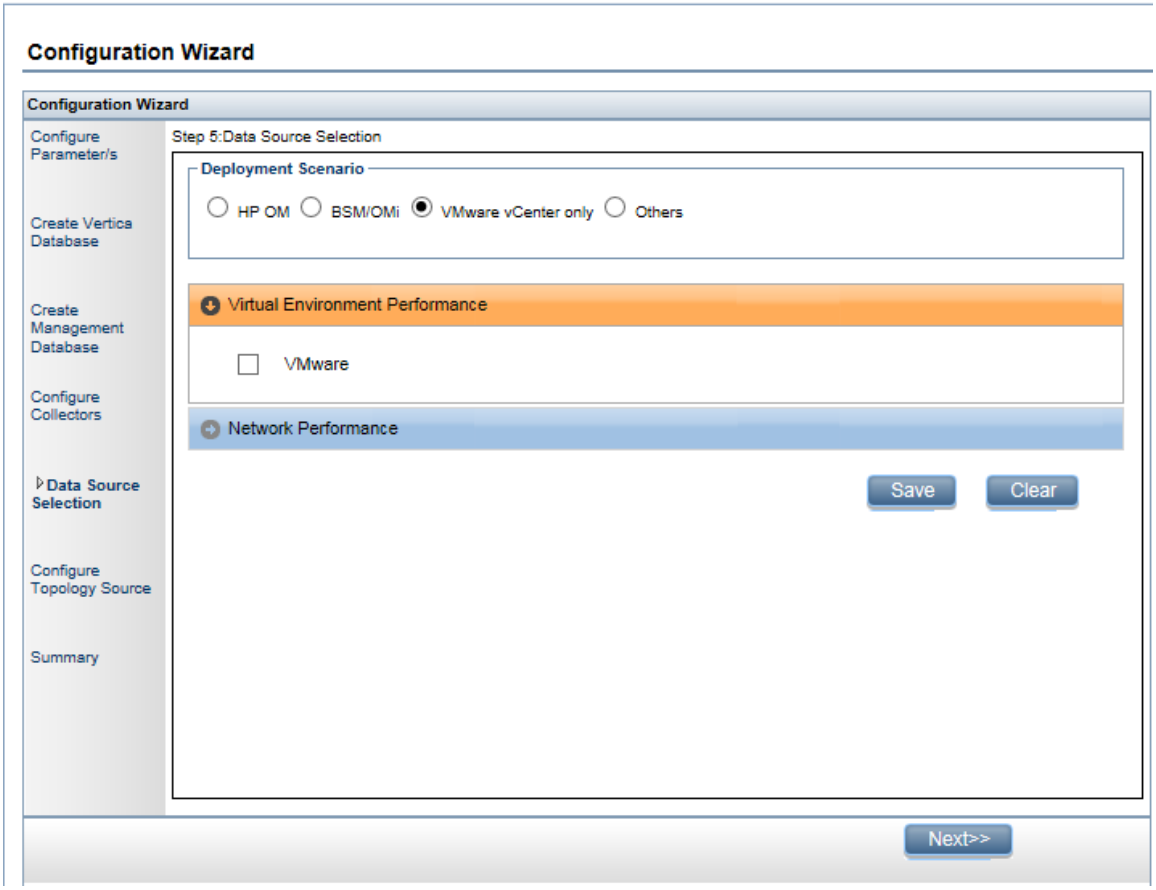
      where `<omi10hostname>`, is the hostname of your OMi10.
5. Log in to **Administration Console > Data Source Configuration > Topology Source**, and click **Configure** to modify the user name, password, and port as relevant for OMi10.
6. Add Operations database connection of OMi in **Administration Console > Data Source Configuration > BSM/OMi** page. For more details, see "Configuring the Management and Profile Database Data Source" on page 120.
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 HPE OBR soon after the upgrade and before starting the collection service. Otherwise HPE 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 HPE OBR, it will end up being a duplicate in HPE 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 the **Deployment Scenario**, click **VMware vCenter only**.

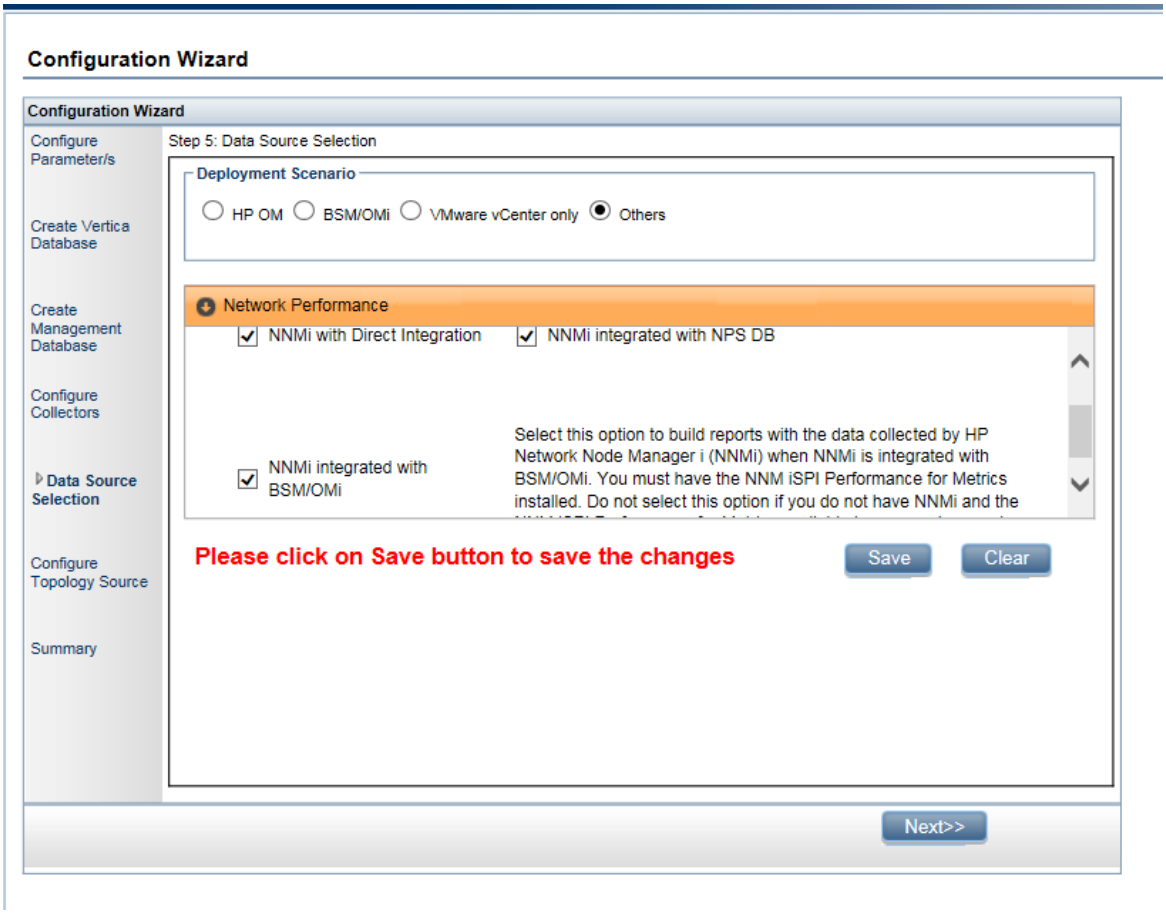


2. In the **Virtual Environment Performance**, select **VMware**.
3. *(Optional)*. In **Network Performance**, select **Network Performance** if NNMi and the NNMi iSPI Performance is available in your environment.
4. Click **Save**. The `Saved Successfully` message is displayed.
5. Click **Next**. The **Configure the Topology Sources** page appears.

Data Sources for Other Database Deployment Scenario

To collect data for other databases, follow these steps:

1. In the **Deployment Scenario**, click **Others**.



2. In the **Network Performance**, select **Network Performance** to collect metrics on your network environment.

   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.

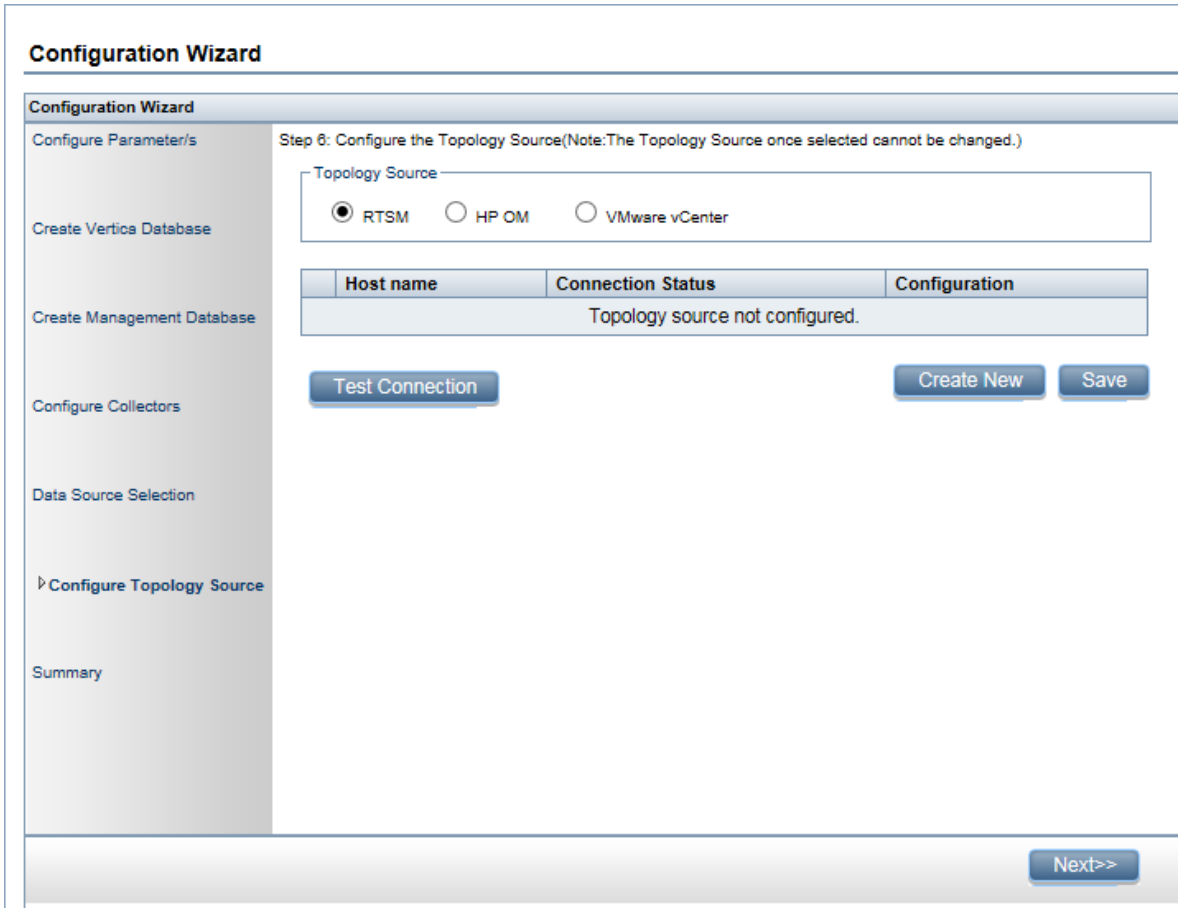
   The **NNMi with Direct Integration** collects network performance data directly from NNMi. The data collection gives you detailed real time view of component or interface health in your network. You have to install Network Comonent_Health/Network Interface_Health Content Packs. You

can view detailed health or utilization reports. You have to revisit the hardware requirements, if you choose to install these Content Packs.

3. Click **Save**. A summary of your selections is displayed.
4. Click **Next**. The **Configure Topology Sources** page appears.

Task 6: Configuring the Topology Source

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



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

- If HPE OBR is deployed in the BSM or Operations Manager i, see "Configuring RTSM Topology Source" on the next page.

- If HPE OBR is deployed in the HPOM environment, see "Configuring HPOM Topology Source" on page 62.
- If HPE OBR is deployed in the VMware vCenter environment, see "Configuring VMware vCenter Topology Source" on page 65.

> **Note:** HPE 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, HPOM, or VMware vCenter) is configured, you cannot change it later.
>
> If you are not configuring the topology source in post-install configuration, you can configure it on the **Data Source Configuration > Topology Source** page.

Configuring RTSM Topology Source

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

1. In the **Topology Source**, click **RTSM**.
2. Click **Create New**. The **Connection Parameter** appears.
3. In the **Connection Parameter**, type the following details:

Field	Description
Host name	IP address or FQDN of the BSM or OMi server. If your HP BSM installation is distributed, type the name of the gateway server in the field. **Note:** In a distributed BSM deployment with multiple gateway servers and load balancer configured, type the virtual IP address of the load balancer in this field.
Port	Port number to query the RTSM web service. The default port number is 80. If the port number has been changed, contact your BSM administrator for more information.
User name	Name of the RTSM web service user. The default user name is admin.
Password	Password of the RTSM web service user.
Collection	If you installed collectors on remote systems, you can choose either the local

Field	Description
station	collector or a remote collector. To configure a remote collector to collect data from this RTSM source, select one of the available remote systems in the drop down list. To use the collector that was installed by default on the HPE OBR system, select local.

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

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

7. In the message box, click **Yes**. A `Saved Successfully` message appears in the information message panel.

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

8. Click **Next** to continue. The **Summary** page appears.
9. Click **Finish** to complete the post-install configuration tasks. The **Deployment Manager** 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 HPE 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.

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`
`shr.truststorepath`	Full path to the keystore file
`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.

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 `%OVInstallDir%`

<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: `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: `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: `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: `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 120
- "Configuring the HP OMi Data Source" on page 127
- "Configuring the HP Operations Manager Data Source" on page 108
- "Configuring the HP Operations Agent Data Source" on page 108
- "Configuring the Generic Data Source" on page 111
- "Configuring HPE OBR with Network Node Manager i (NNMi)" on page 160
- "Configuring the VMware vCenter Data Source" on page 114
- "Configuring the SiteScope Data Source" on page 115

Configuring HPOM Topology Source

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

1. In the **Topology Source**, click **HP OM**.
2. Click **Create New**. The **Connection Parameter** section appears.
3. In the **Connection Parameter**, type the following details:

> **Caution:** If you are using the database method of authentication to connect to the HPOM 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**.

Field	Description
	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 HPOM that is configured in your environment. The options include: HPOM for Windows HPOM for Unix HPOM for Linux HPOM for Solaris
Database Type	Depending on the data source type that you select, the database type is automatically selected for you. For the HPOM for Windows data source type, the database type is MSSQL. For the HPOM for Unix, HPOM for Linux, or HPOM for Solaris, the database type is Oracle.
Windows Authentication	Option to enable Windows Authentication for accessing the HPOM database. The user can use the same credentials to access HPOM as that of the Windows system hosting the database. This option only appears if HPOM 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.
Host name	IP address or fully-qualified domain name (FQDN) of the HPOM database server. The HPOM 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 HPOM database server. To check the port number for the database instance, such as

Field	Description
	OVOPS, see "Checking for the HPOM Server Port Number" on page 95.
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 HPOM database user. For the HPOM for Windows data source type, if the Windows Authentication option is selected, this field is disabled and appears empty.
Password	Password of the HPOM database user. For the HPOM 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 HPE OBR system, select local.

4. Click **OK**.
5. Click **Save** to save the information.
6. Click **Test Connection**.
7. In the message box, click **Yes**. A `Saved Successfully` message appears in the information message panel.

   You can configure additional HPOM data sources by performing step 2 to step 7.

   For more information about configuring HPOM topology sources, see *Managing the enterprise topology* section in the *HPE Operations Bridge Reporter Administrators Guide*.

   > **Note:** To collect data from non-domain hosts, appropriate DNS resolutions must be made by the HPOM administrator for these hosts so that they are reachable by HPE OBR, which is installed in the domain.

8. Click **Next** to continue. The **Summary** page appears.
9. Click **Finish** to complete the post-install configuration tasks. The **Deployment Manager** page appears.

Supported Data Source Selections

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

- "Configuring the HP Operations Manager Data Source" on page 108
- "Configuring the HP Operations Agent Data Source" on page 108
- "Configuring the Generic Data Source" on page 111
- "Configuring HPE OBR with Network Node Manager i (NNMi)" on page 160
- "Configuring the VMware vCenter Data Source" on page 114

Configuring VMware vCenter Topology Source

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

1. In the **Topology Source**, click **VMware vCenter**.
2. Click **Create New**. The **Connection Parameter** section appears.
3. In the **Connection Parameter**, type the following details:

Field	Description
Host name	IP address or FQDN of the VMware vCenter server.
User name	Name of the VMware vCenter web service user. The `administration@vsphere.local` is the default user name.
Password	Password of the VMware vCenter web service 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 HPE OBR system, select local.

4. Click **OK**.

5. Click **Save** to save the information.
6. Click **Test Connection**.
7. In the message box, click **Yes**. A `Saved Successfully` message appears in the information message panel.

   You can configure additional vCenter data sources by performing step 2 to step 7.
8. Click **Next** to continue. The **Summary** page appears.
9. Click **Finish** to complete the post-install configuration tasks. The **Deployment Manager** 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: `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 HPE OBR reports. For information on logging levels and their corresponding metrics, use the following URL:

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

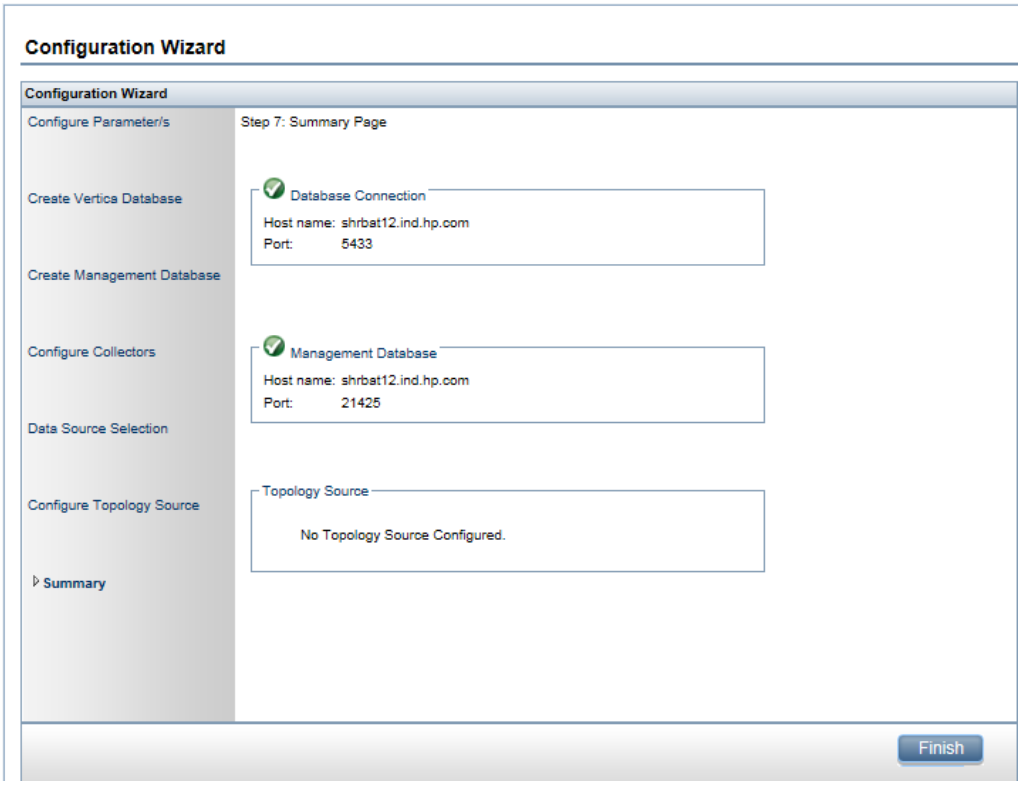
Supported Data Source Selections

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

- "Configuring the Generic Data Source" on page 111
- "Configuring HPE OBR with Network Node Manager i (NNMi)" on page 160
- "Configuring the VMware vCenter Data Source" on page 114

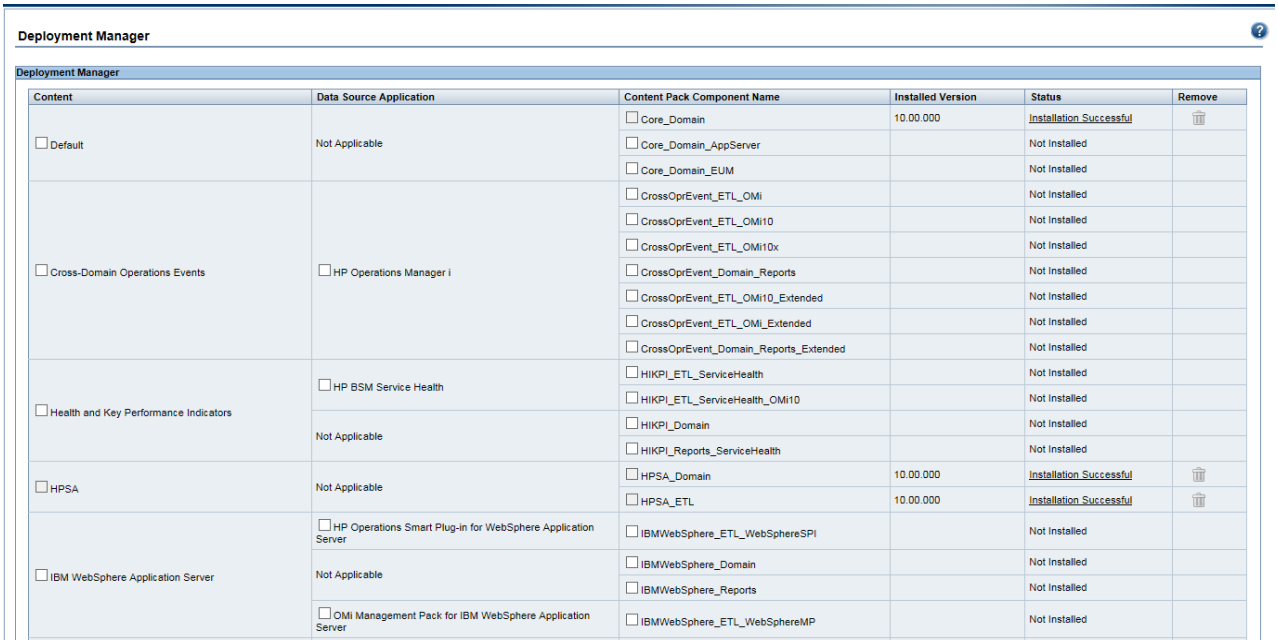
Task 7: Summary

The **Summary** page presents a summary of all selections. Click **Finish**.



You may install and configure additional Data Processors after completing the post-install configurations using Configuration Wizard. For more information, see *HPE Operations Bridge ReporterInteractive Installation Guide*.

The **Deployment Manager** page is displayed with Content Packs selected based on the selections made in the data source configuration.



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

> **Note:** The Content Packs already selected in the Deployment Manager may be mutually exclusive. For information on Content Packs that are mutually exclusive, see "Listing of ETLs" on page 259.

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.

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.

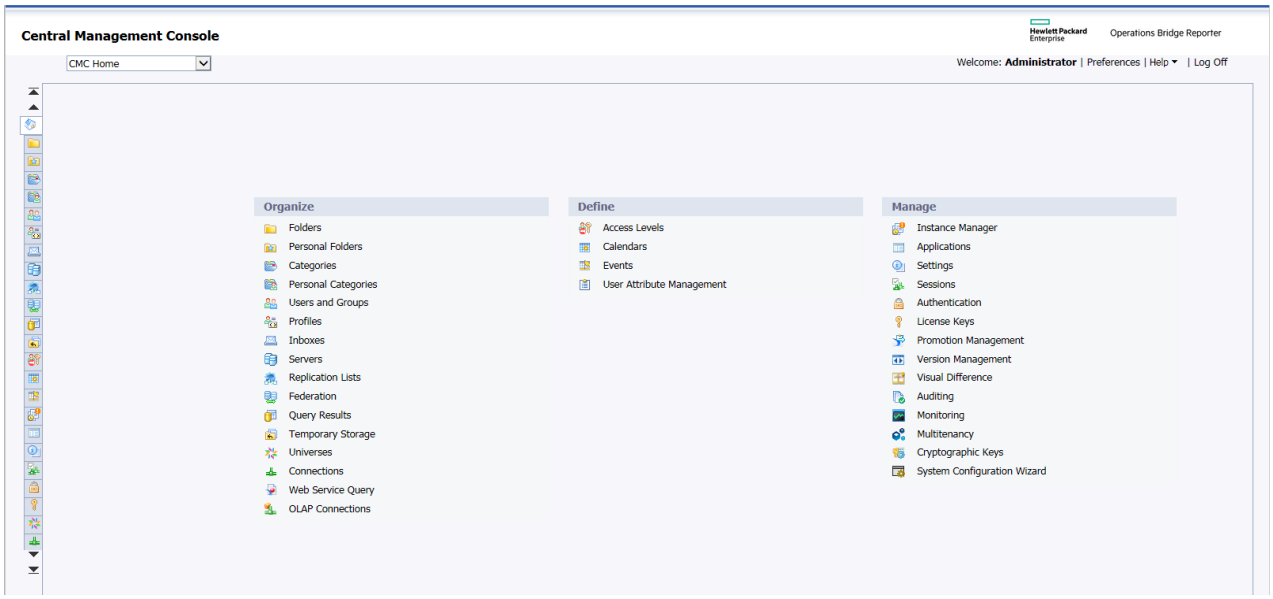
   > **Note:** By default HTTPs is enabled for HPE OBR. You can also launch CMC using `http://<System_FQDN>:8080/CMC` if you have disabled HTTPs.

You can also access CMC from Administration Console. Click **SAP BOBJ > Launch CMC**. The Log in page is displayed.

2. Log on as user with administrator privileges.

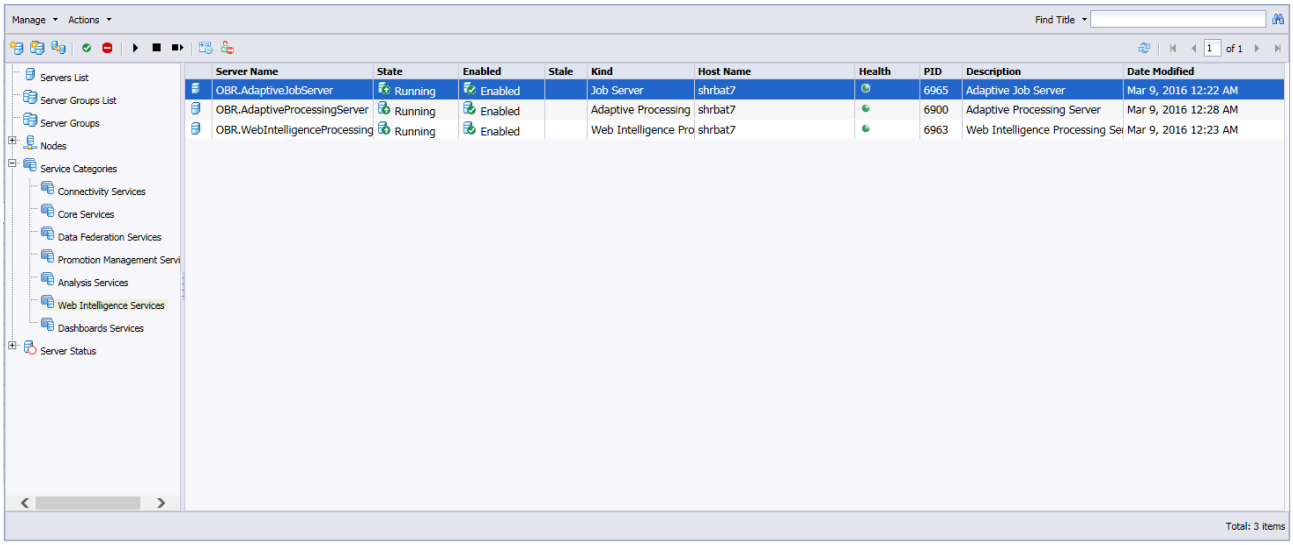
   The **System Configuration Wizard** is displayed. Click **Close** to close the wizard. The **Central Management Console** home page is displayed.

   > **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**.

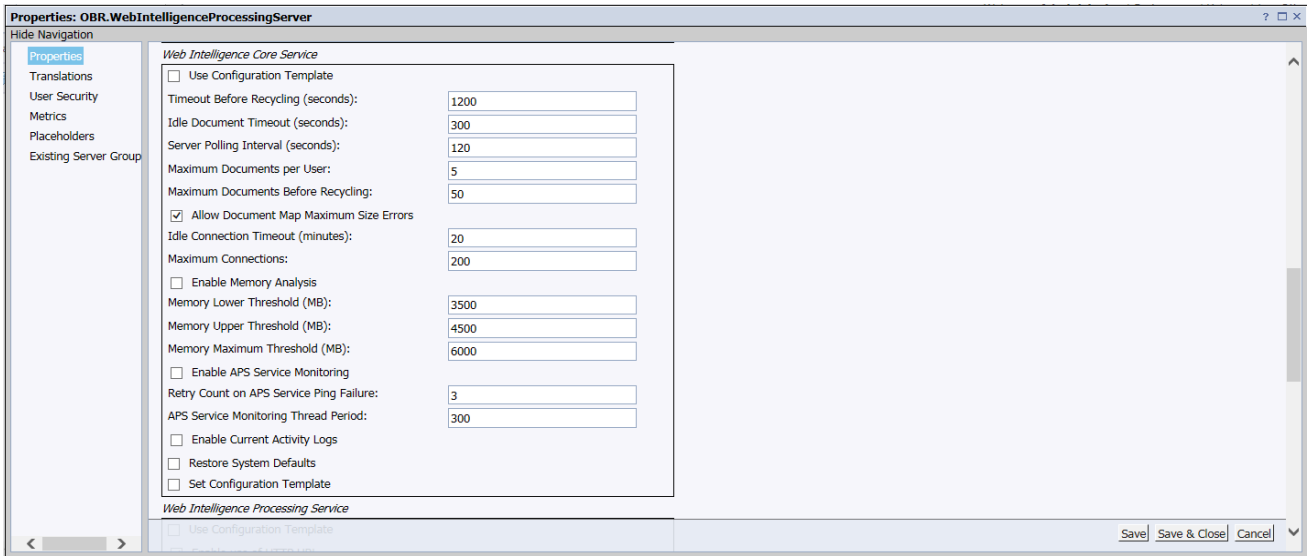


3. Click **Servers** or select **Servers** from the drop down list. The Manage page is displayed.

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.

Logon Banner

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

For information on enabling and disabling the logon banner, see "Configuring Logon Banner for HPE OBR" on page 179.

Chapter 3: Configure OBR for BSM/OMi Deployment Scenario

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

- BSM/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 HPOM 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 HPE OBR.

Configuring RTSM Topology Source for HPE 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 HP Operations Agent and HP SiteScope.

Prerequisite for Management Packs

To view reports for the following HPE OBR content packs that gather data from the OMi10 data source, the corresponding Management Packs must be installed on HP 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 HPE OBR reports for Service Health and OMi.

In the HP BSM 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\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.ap\source\cmdb_views` `%PMDB_HOME%\packages\EndUserManagement\ETL_RUM_OMi.ap\source\cmdb_views`

Content Pack	View Name	Location
		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.
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`	`%PMDB_HOME%\packages\SystemManagement\ETL_SystemManagement_PA.ap\source\cmdb_views`
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`	**For OM/SPI**: `%PMDB_HOME%\packages\ApplicationServer\ETL_AppSrvrWLS_WLSSPI.ap\source\cmdb_views` **For OMi/MP**: `%PMDB_HOME%\packages\ApplicationServer\ETL_AppSrvrWLS_WLSMP.ap\source\cmdb_views`
IBM WebSphere Application Server	`J2EEApplication.zip` `J2EEApplication_OM.zip`	**For OM/SPI**: `%PMDB_HOME%\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`

Content Pack	View Name	Location

		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`	`%PMDB_HOME%\packages\SystemManagement\ETL_SystemManagement_PA.ap\source\cmdb_views`
Health and Key Performance Indicators (Service Health)	All the views	
HPSA	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

Content Pack	View Name	Location
		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. If OMi 10 is the deployment scenario, then deploy only EUM_OMi.zip view in the OMi 10 server.
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	$PMDB_HOME/packages/SystemManagement/ETL_SystemManagement_PA.ap/source/cmdb_views
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	**For OM/SPI**: $PMDB_HOME/packages/ApplicationServer/ETL_AppSrvrWLS_WLSSPI.ap/source/cmdb_views **For OMi/MP**: $PMDB_HOME/packages/ApplicationServer/ETL_AppSrvrWLS_WLSMP.ap/source/cmdb_views
IBM WebSphere Application Server	J2EEApplication.zip J2EEApplication_OM.zip	**For OM/SPI**: $PMDB_HOME/packages/ApplicationServer/ETL_AppSrvrWBS_WBSSPI.ap/source/cmdb_views **For OMi/MP**:$PMDB_HOME/packages/ApplicationServer/ETL_

Content Pack	View Name	Location
		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	$PMDB_HOME/packages/SystemManagement/ETL_SystemManagement_PA.ap/source/cmdb_views
Health and Key Performance Indicators (Service Health)	All the views	
HPSA	No views	
Cross-Domain Operations Events	All the views	
Operations Events	No views	

HP BSM Server

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

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

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

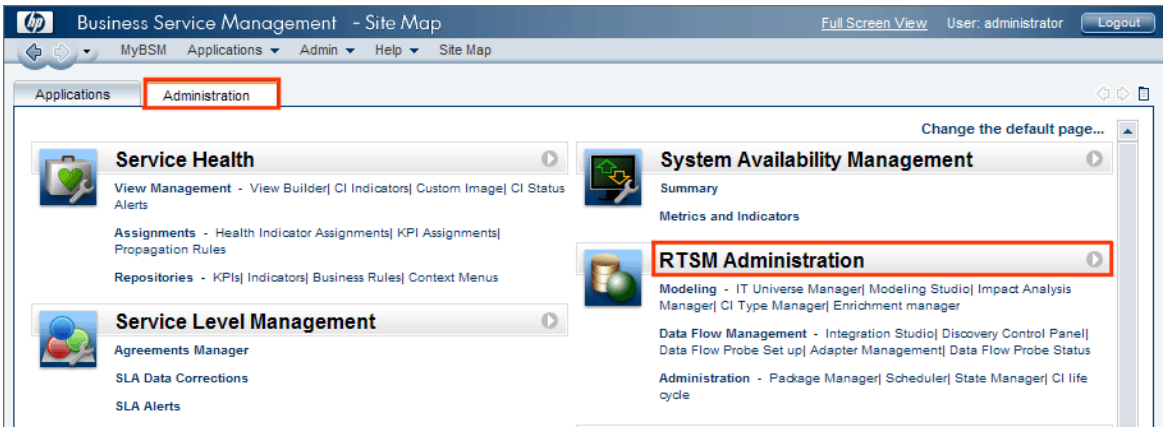
   where, *<BSM system FQDN>* is the FQDN of the HP BSM server.

   > **Note:** You can launch the HP BSM server from a system where HPE 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.

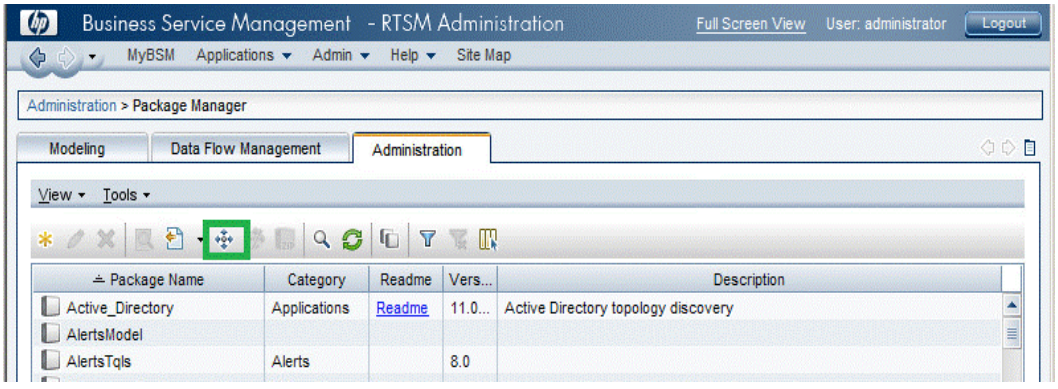
   The Business Service Management Login page appears.

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.

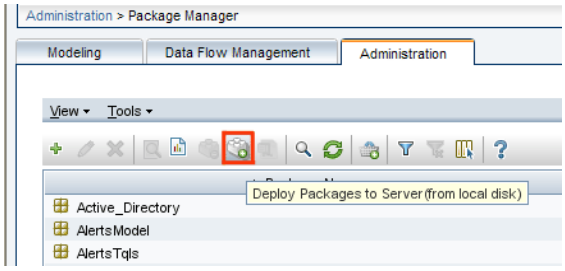


4. Click **Administration > Package Manager**. The Package Manager page appears.

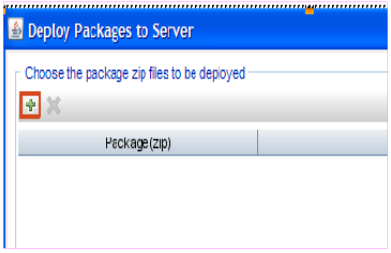


5. Click the **Deploy Packages to Server (from local disk)** icon. The **Deploy Package to Server**

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 HPE OBR.

HP OMi 10 Server

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

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

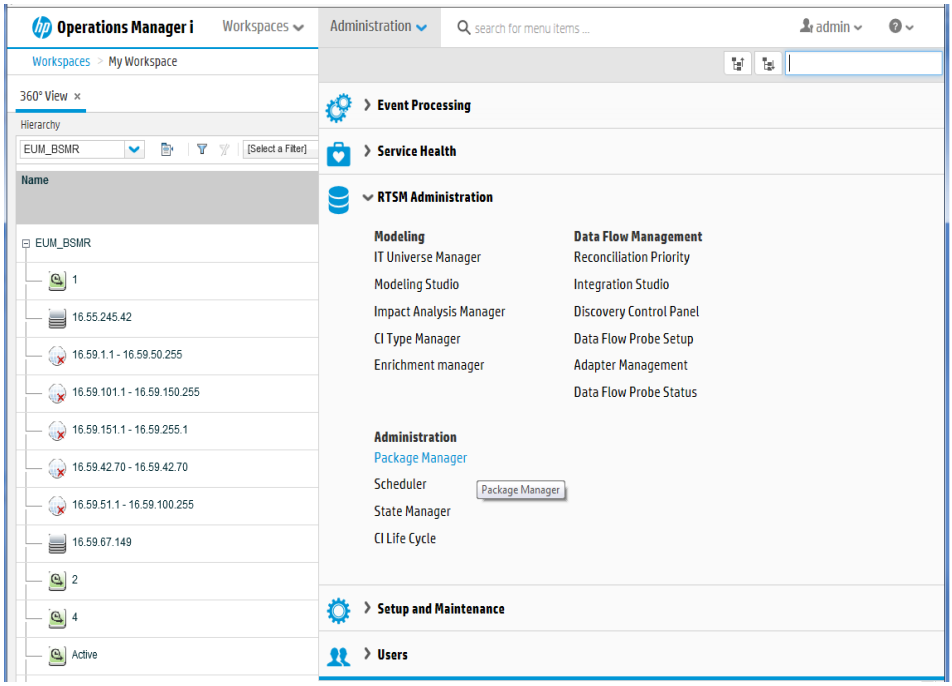
   `http://<OMi system FQDN>/omi`

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

> **Note:** You can launch the HP OMi server from a system where HPE 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.

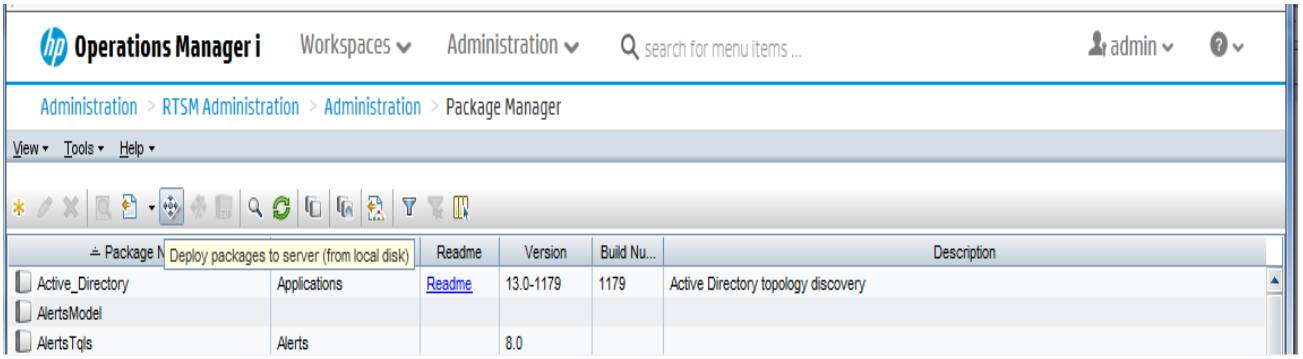
The Operations Manager i Login page appears.

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**.

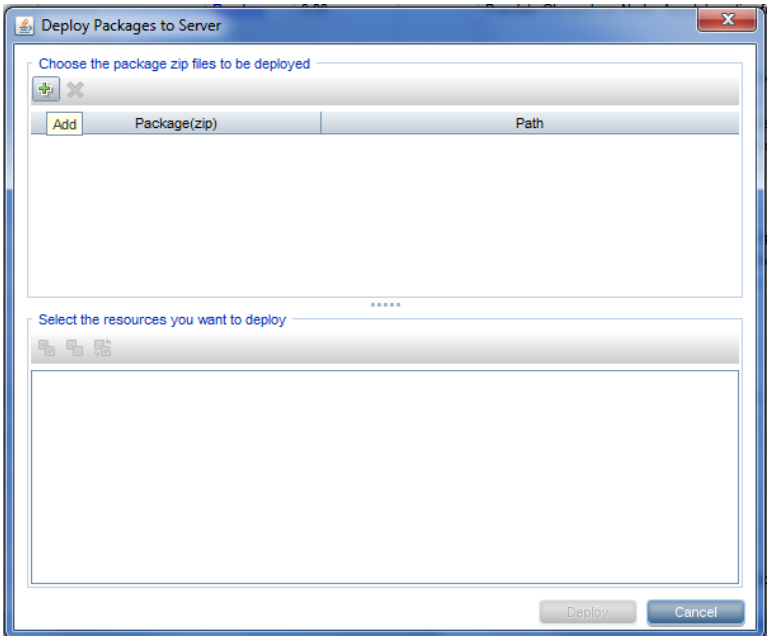


The Package Manager page appears.

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 HPE 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:

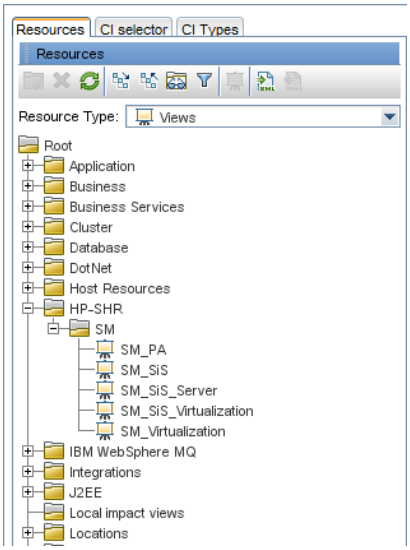
   `http://<BSM system FQDN>/bsm`

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

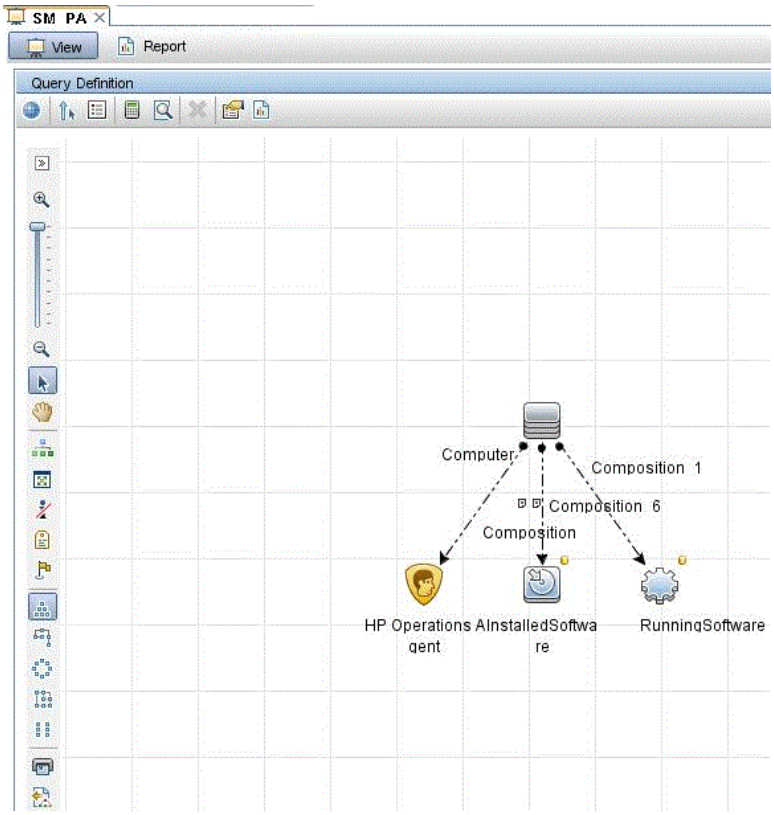
   The Business Service Management Login page appears.

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:

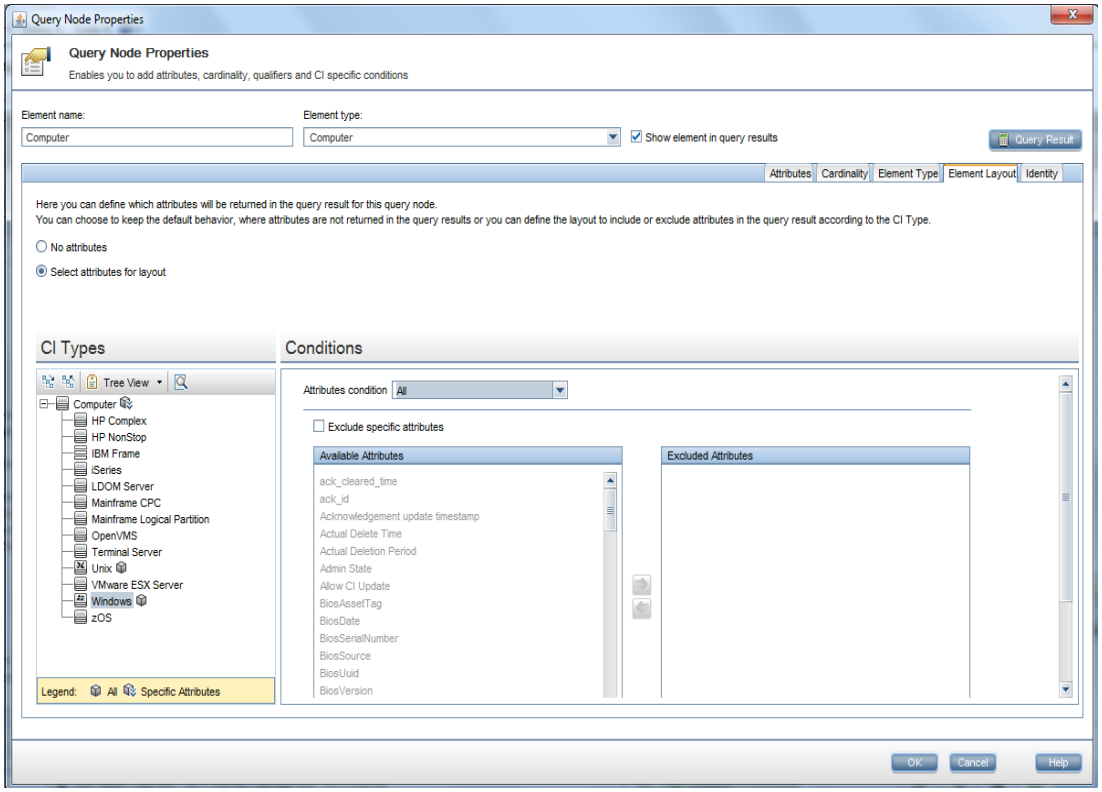
a. Click **Element Layout**.

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

HP 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 HPE OBR " on page 252.

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:

http://h20230.www2.hp.com/selfsolve/manuals

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 HP BSM is the deployment scenario then you can integrate SiteScope with HPE 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 HPE OBR using Configuring the SiteScope Data Source procedure.

Chapter 4: Configure OBR for HPOM Deployment Scenario

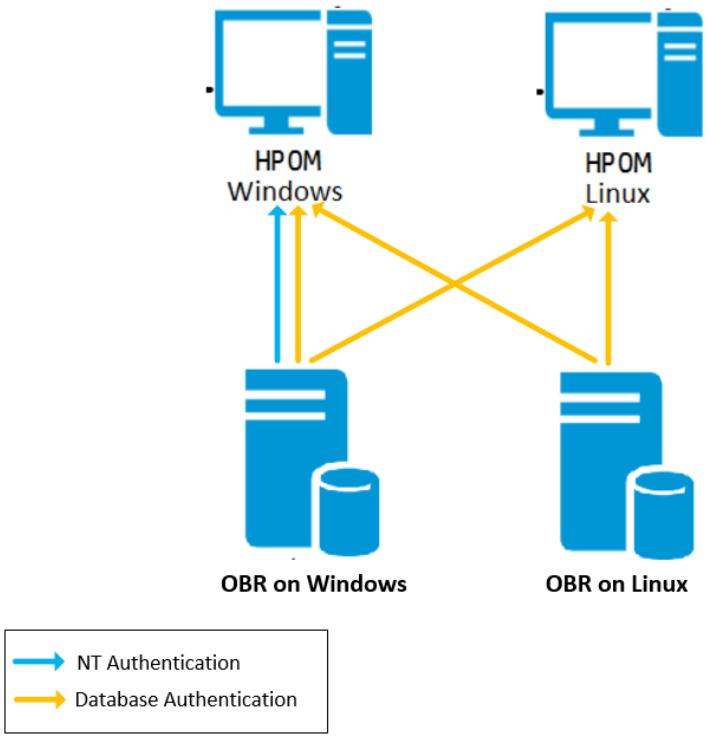
If you plan to configure OBR to work with an HPOM installation, you must:

- Install and configure HPOM successfully
- Deploy necessary SPI policies

Authentication for HPE OBR connection with HPOM

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

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



HPE OBR connection with HPOM 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 HPOM 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 HPOM service definition connection configuration.

HPE OBR connection with HPOM using database authentication

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

- **Scenario 1**: HPOM 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 HPOM database connection.
- **Scenario 2**: HPOM for Windows 8.x uses Microsoft SQL Server 2005 Express Edition that is embedded with it by default. Similarly, HPOM 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 HPOM system with embedded Microsoft SQL Server 2005, follow these steps:

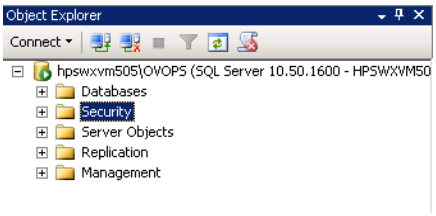
Task 1: Create a user name and password

1. Log on to the HPOM 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.

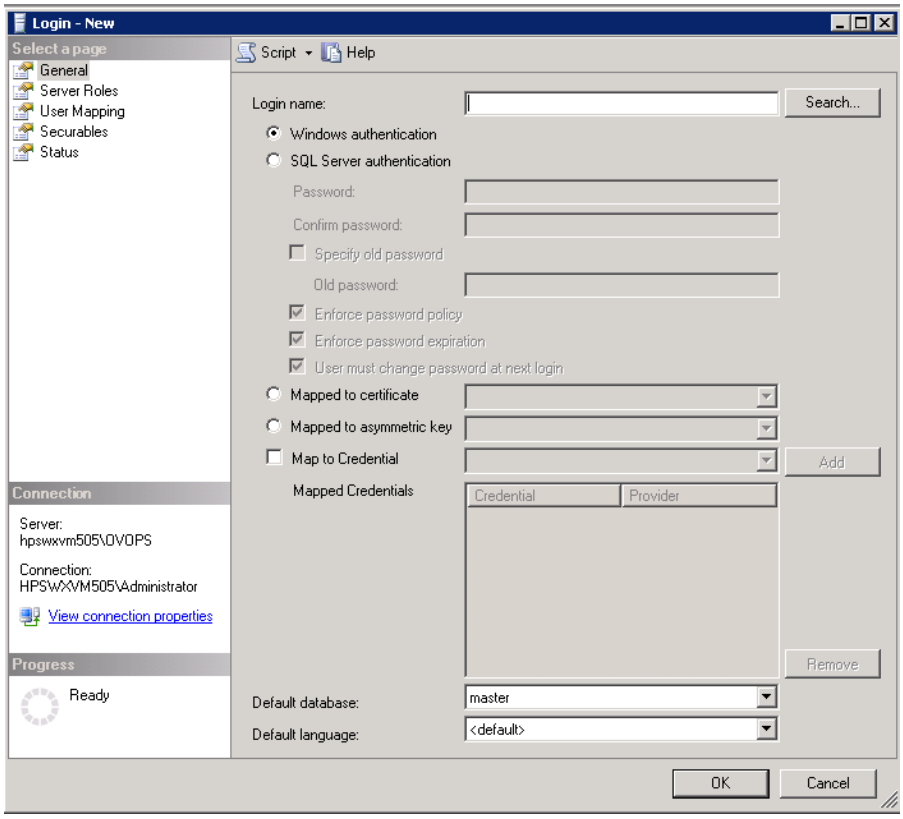
   > **Note:** If SQL Server Management Studio is not installed on your system, you can download it from the relevant section of Microsoft web site using the following URL: http://www.microsoft.com

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

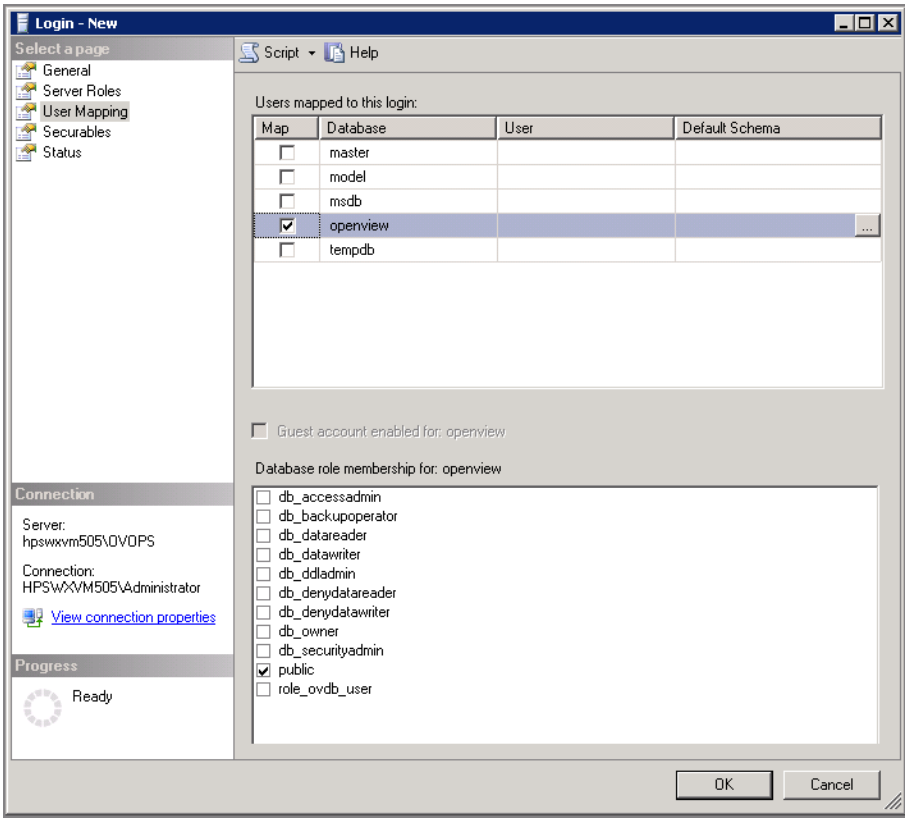
4. In the **Object Explorer** pane, expand **Security**.



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.



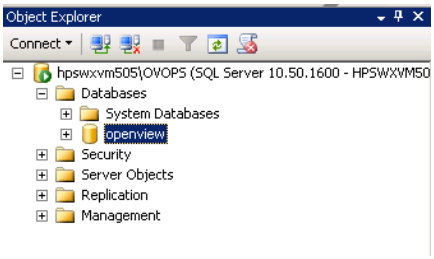
12. Click **OK** to create the user name and password.

> **Note:** To create user name and password on HPOM system with embedded Microsoft SQL Server 2008, follow the same steps in Task 1.

Task 2: Enable Connect and Select permissions

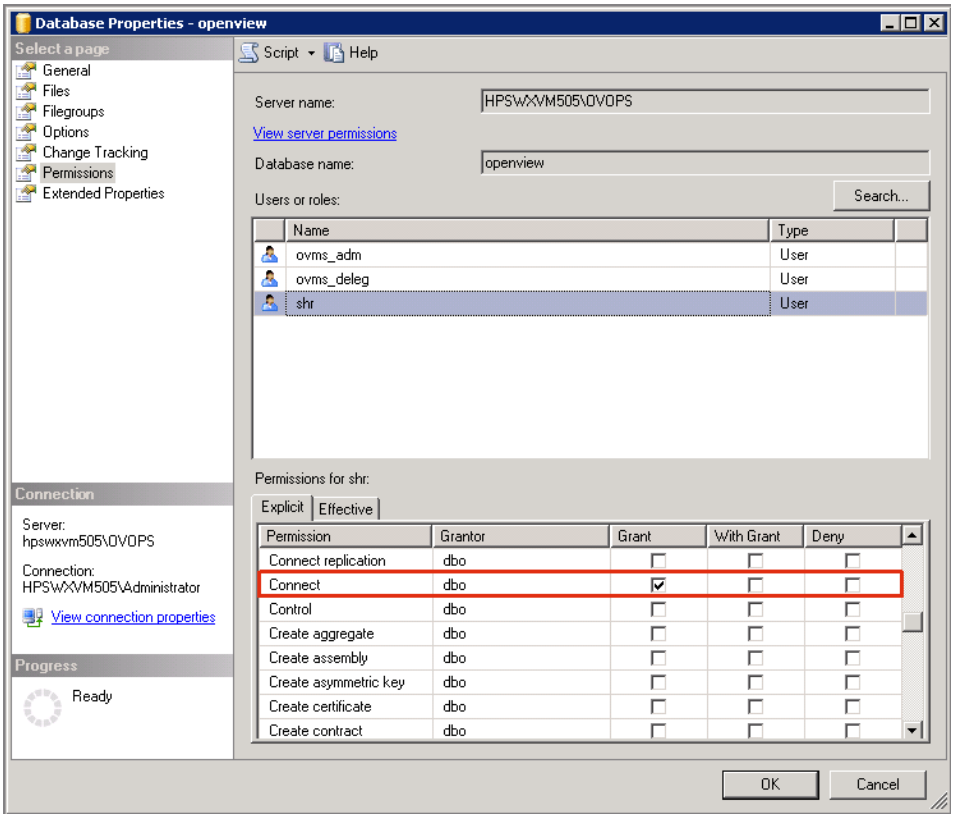
The database user must have at least the Connect and Select permissions. To enable Connect and Select permissions for the newly created user account, follow these steps:

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

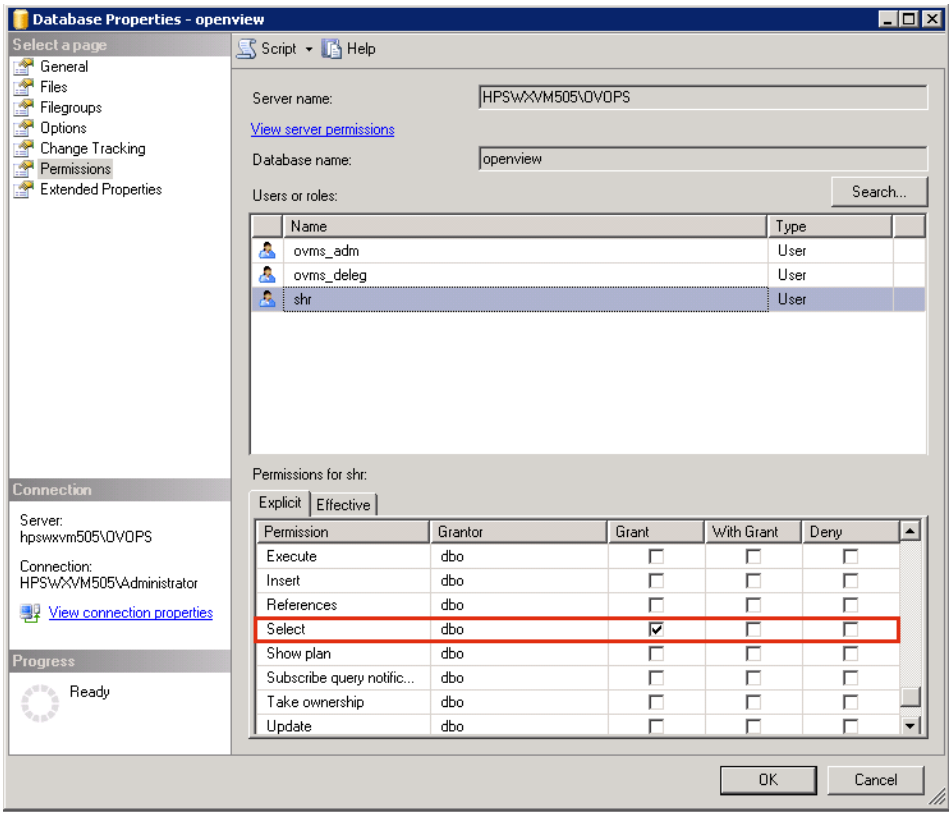


2. Right-click **openview** and then click **Properties**. The **Database Properties - openview** dialog box opens.

3. Click **Permissions**.



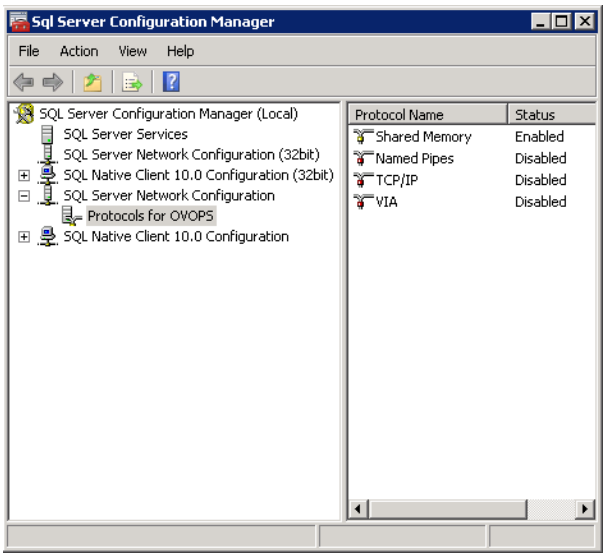
4. In the **Users or roles**, click the newly created user account.
5. In the **Explicit** tab of permissions for newly created user, scroll down to the **Connect** permission, and then select the **Grant** check box for this permission.
6. Scroll down to the **Select** permission and select the **Grant**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



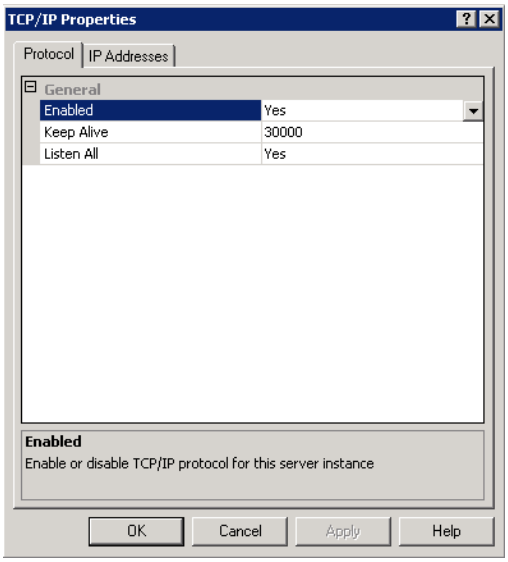
7. Click **OK**.

Task 3: Check for the HPOM 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.



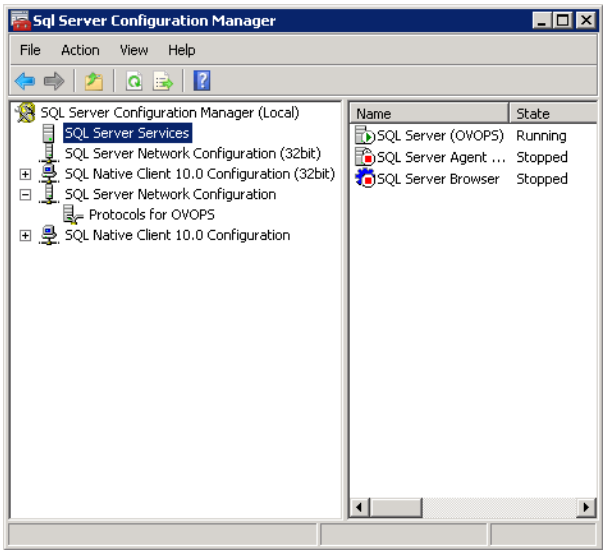
3. On the right pane, right-click **TCP/IP**, and then click **Enable**.
4. Right-click **TCP/IP** again, and click **Properties**. The **TCP/IP Properties** dialog box is displayed.



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

Task 4: Restart the HPOM 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 HPOM 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 HPOM Server Port Number

If Microsoft SQL Server is the database type in HPOM, follow steps in Task 3 to check for the HPOM server port number.

If Oracle is the database type in HPOM, 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 HPOM server listed in the file.

Chapter 5: Install and Uninstall the Content Packs

For installing the required Content Packs, HPE OBR provides the Deployment Manager 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 HPE 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 HPE OBR system (installed on Windows) to connect to Vertica database. If HPE 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 165.

> **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

HPE 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 HPE 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**:

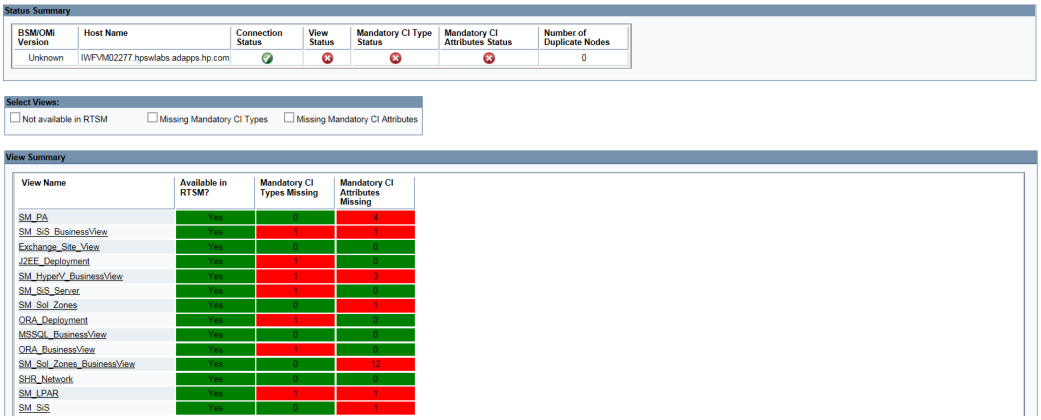
         `dscheckRTSM.sh -propFile <File_Path>/<property_file>`

         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`.
      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.



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 HPE 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>`

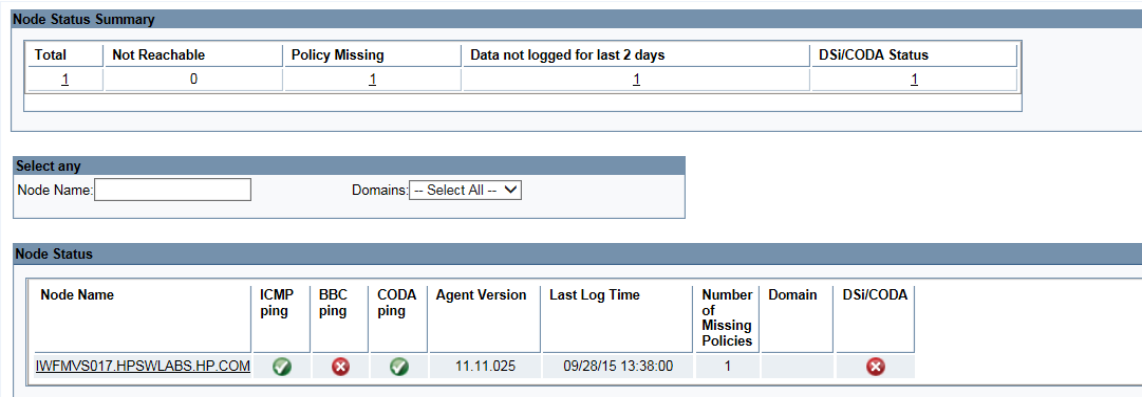
      where, <*File_Path*> is the path where property files is created.

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

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.



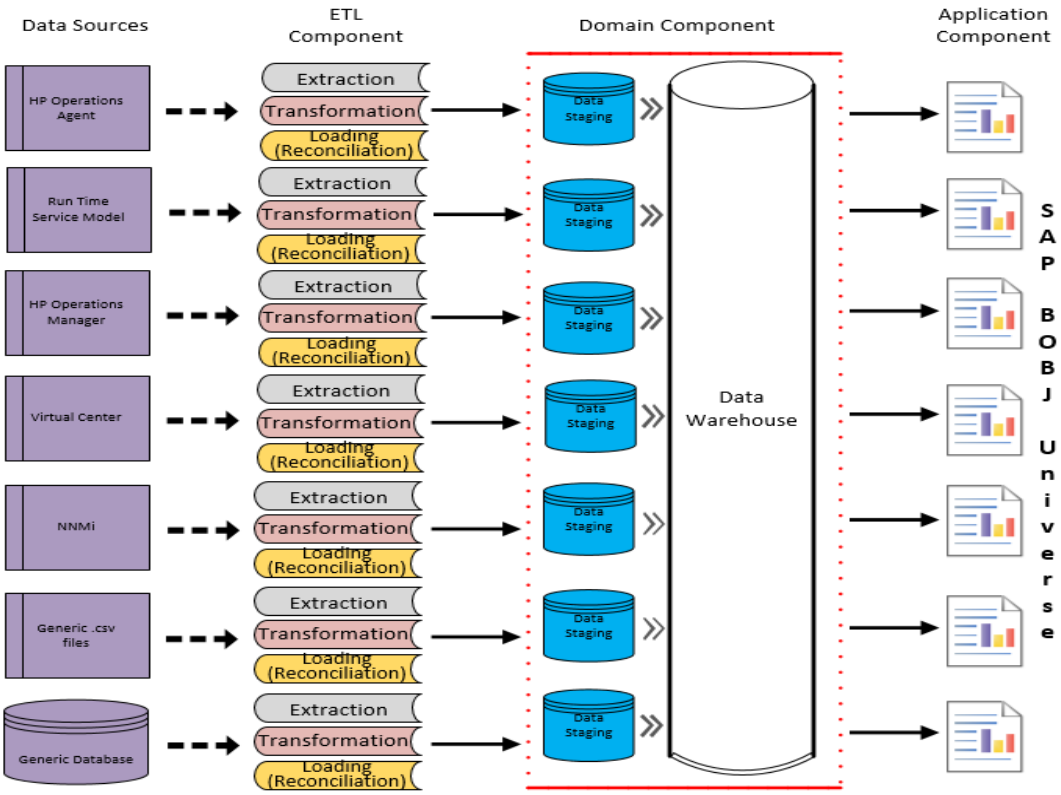
The file displays the following information:

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 HP Operations Agent, you must install the `SysPerf_ETL_PerformanceAgent` component. If you want to collect system performance data from HP 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 Deployment Manager 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 Deployment Manager 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 *HPE Operations Bridge Reporter Online Help for Users*.

Installing the Content Pack Components

Use the Deployment Manager utility to install the Content Pack components.

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/BSMRApp`

      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 **Administration**, and then click **Deployment Manager**. The **Deployment Manager** page appears.

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

   List of Content Packs

Content	BSM/OMi	HP Operations Manager	Application Performance Management	VMware vCenter
Default	✓	✓	✓	✓
Cross-Domain Operations Events	✓			
Health and Key Performance Indicators	✓		✓	
IBM WebSphere Application Server	✓	✓		
Microsoft Active Directory	✓	✓		
Microsoft Exchange Server	✓	✓		
Microsoft SQL Server	✓	✓		
MSAppCore	✓	✓		
Network Performance[1]	✓	✓		
Network Component	✓	✓		

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

Content	BSM/OMi	HP Operations Manager	Application Performance Management	VMware vCenter
Health				
Network Interface Health	✓	✓		
Operations Events	✓	✓		
Oracle	✓	✓		
Oracle WebLogic Server	✓	✓		
Real User Transaction Monitoring	✓		✓	
Synthetic Transaction Monitoring	✓		✓	
System Performance	✓	✓		✓
Virtual Environment Performance	✓	✓		✓

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

   The color of the status column changes for all the selected Content Packs. An **Installation Started** status appears in the **Status** column for Content Pack that is currently being installed. The Deployment Manager 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 timer service will be stopped automatically during install/uninstall operation and will be started once operation is complete.

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

> **Note:** During install/uninstall process, Deployment Manager 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 Deployment Manager 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)* section in *HPE Operations Bridge Reporter Troubleshooting Guide*.

You may install and configure additional Data Processors after completing the Content Pack installation. For more information, see *HPE 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. HPE 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.

Based on your requirement, HPE 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 HPE OBR and NNMi to exchange network data. For configuration procedure, see "Configuring HPE OBR with Network Node Manager i (NNMi)" on page 160.

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 page 68.

Uninstalling the Content Pack Components

Use the Deployment Manager utility 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/`

   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 **Administration**, and then click **Deployment Manager**. The **Deployment Manager** page appears.

   The Deployment Manager 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 102.

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 **Administration > Licensing** page of Administration Console.

Chapter 6: Data Source Configuration

After installing Content Packs, you must configure HPE OBR to collect required data from various data collectors. The data collectors work internally within the HPE 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. **BSM/OMi 9.2x deployment scenario**
    a. Configuring the Management and Profile Database Data Source
    b. Configuring the HP OMi Data Source **(Events database)**
    c. Configuring the HP Operations Agent Data Source
    d. Configuring the HP 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 HP OMi Data Source **(Operations database)**
    b. Configuring the HP 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. **HP Operations Manager deployment scenario**
    a. Configuring the HP Operations Agent Data Source
    b. Configuring the HP 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**

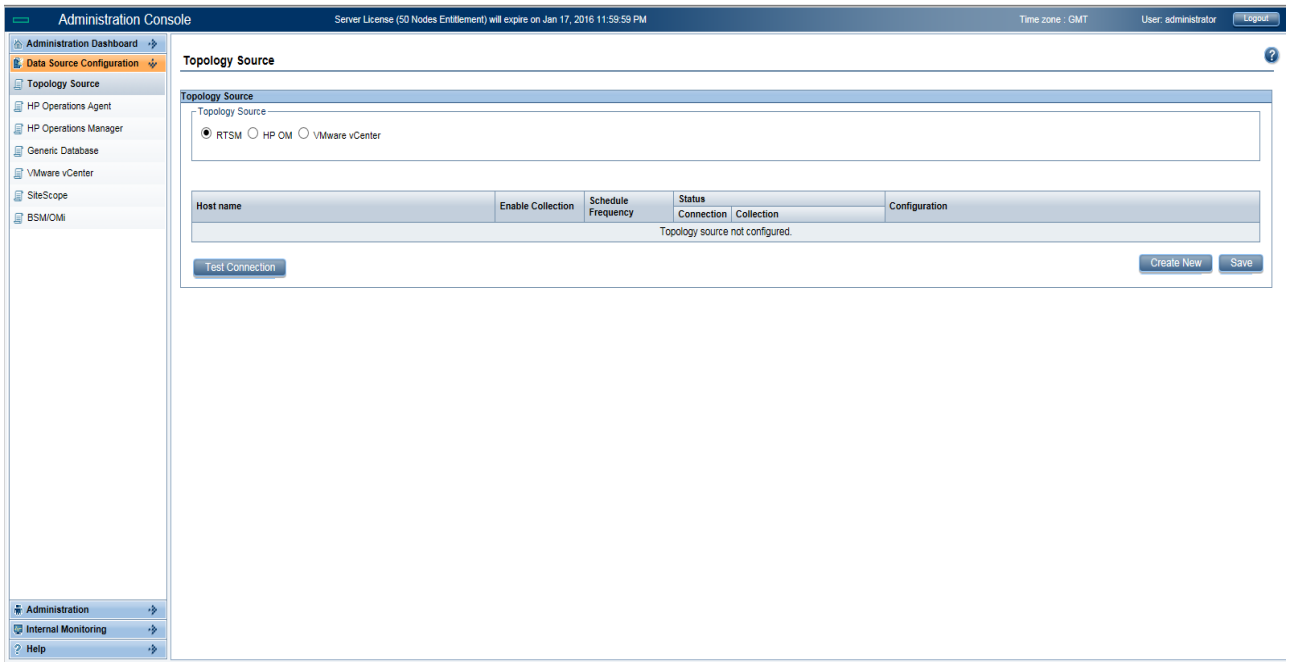
   a. Configuring the Network Data Source (using Generic Database)

   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.



For more information on topology source configuration, see "Task 6: Configuring the Topology Source" on page 57.

Configuring the HP Operations Agent Data Source

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

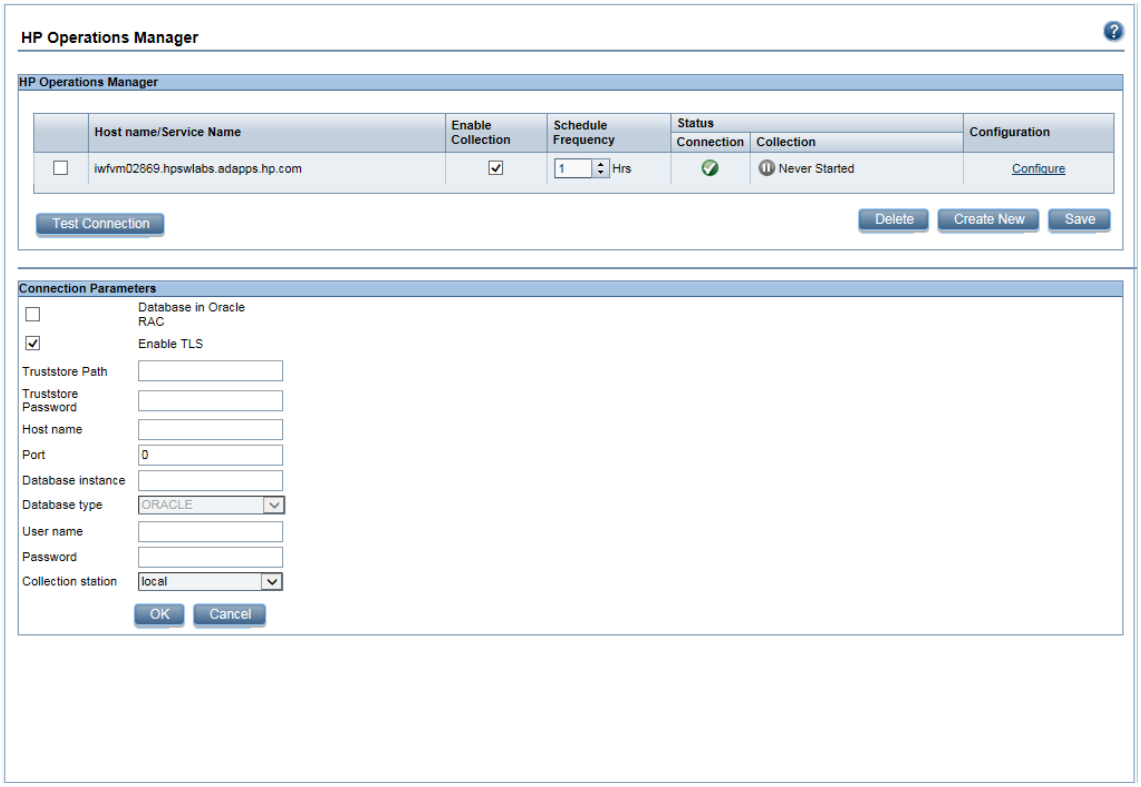
To view the list of HP Operations Agent data sources, follow these steps:

1. In the **Administration Console**, click **Data Source Configuration > HP Operations Agent**. The **HP Operations Agent Data Source** page appears.
2. To view detailed information about the HP Operations Agent data sources, click the Domain name or the number in the **HP Operations Agent Data Source Summary** table. The **HP Operations Agent Data Source Details** table appears.
3. To change the data collection schedule for one or more hosts, specify a polling time between 1 and 24 hours in the **Hrs** box in the **Schedule Polling Frequency** column.
4. Click **Save** to save the changes. A Saved Successfully message appears in the Information message panel.

For more information about configuring HP Operations Agent data source connections, see the *HPE Operations Bridge Reporter Administration Guide*.

Configuring the HP Operations Manager Data Source

If you have installed the HP Operations Manager (HPOM) Content Pack and created the topology source connection for HPOM, the same data source connection appears on the **Data Source Configuration > HP 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 HP Operations Manager page.

To configure the database connection, follow these steps:

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

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**.

Field	Description
Host name	IP address or fully-qualified domain name (FQDN) of the HPOM database server. The HPOM 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 HPOM database server. To check the port number for the database instance, such as OVOPS, see "Checking for the HPOM Server Port Number" on page 95.
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.
Database type	Depending on the data source type that you select, the database type is automatically selected for you. For the HPOM for Windows data source type, the database type is MSSQL. For the HPOM for Unix, HPOM for Linux, or HPOM for Solaris, the database type is Oracle.
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 (available at `${PMDB.HOME}/config` folder) contains connection information to the Oracle Real Application Cluster. This option appears only if **Database in Oracle RAC** is 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.
User name	Name of the HPOM database user. For the HPOM for Windows data source type, if the Windows Authentication option is selected, this field is disabled and appears empty.
Password	Password of the HPOM database user. For the HPOM for Windows data source type, if the Windows Authentication option is selected, this field is disabled and appears empty.

Field	Description
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 HPE OBR system, select local.

4. Click **OK**.
5. Select the check box next to 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 check box next to the host name and click **Configure** to modify a specific HPOM data source connection.
7. To change the HPOM 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 HP Operations Manager data source connections, see the *HPE Operations Bridge Reporter Administration Guide*.

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 HPE OBR to collect network performance data from NPS data base which is integrated with NNMi. HPE 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 HPE OBR to collect the required data from the NPS.

Sybase IQ as Data Source

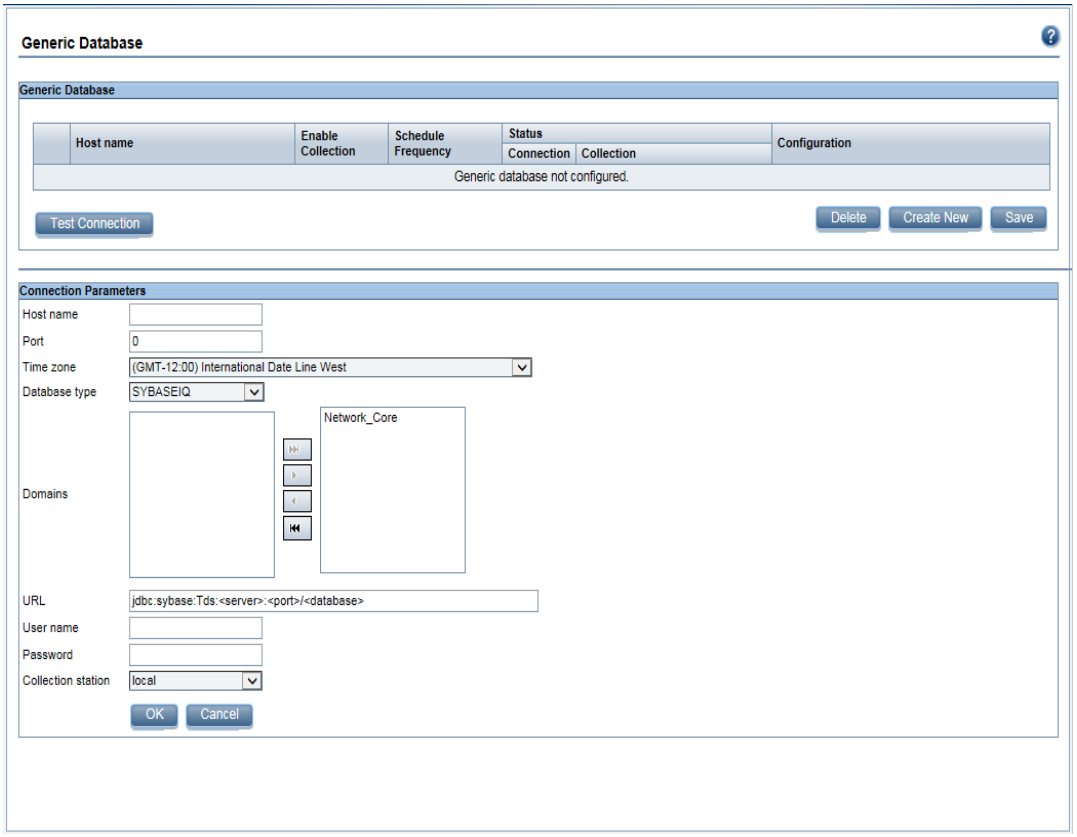
If Sybase IQ is the database in your system, you have to manually copy the `jconn4.jar` file to the HPE OBR system and then continue with the generic database configuration.

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 HPE OBR system.
2. Restart the collection service.

Configure Generic Data Source

To configure the generic database, follow these steps:



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.
Database type	The type of database engine that is used to create the NPS database.
Domain	Select the domain(s) for which you want HPE 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 *HPE Operations Bridge Reporter Administration Guide*.

> **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 HPE 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.

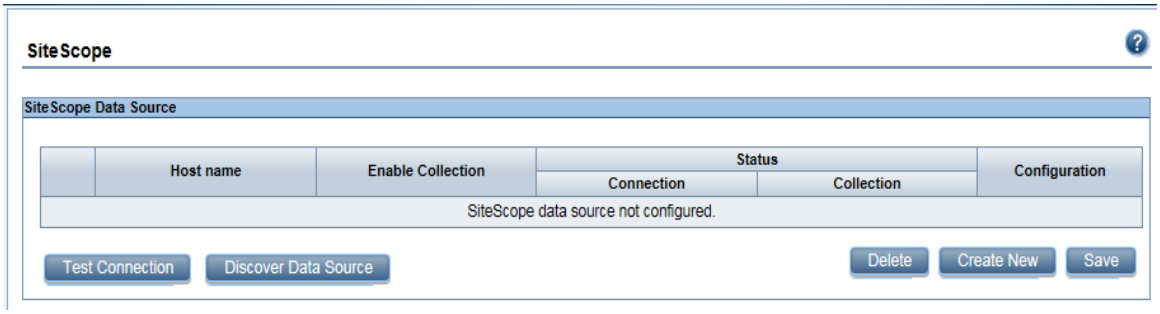
For more information about configuring VMware vCenter data source connections, see the *HPE Operations Bridge Reporter Administration Guide*.

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.

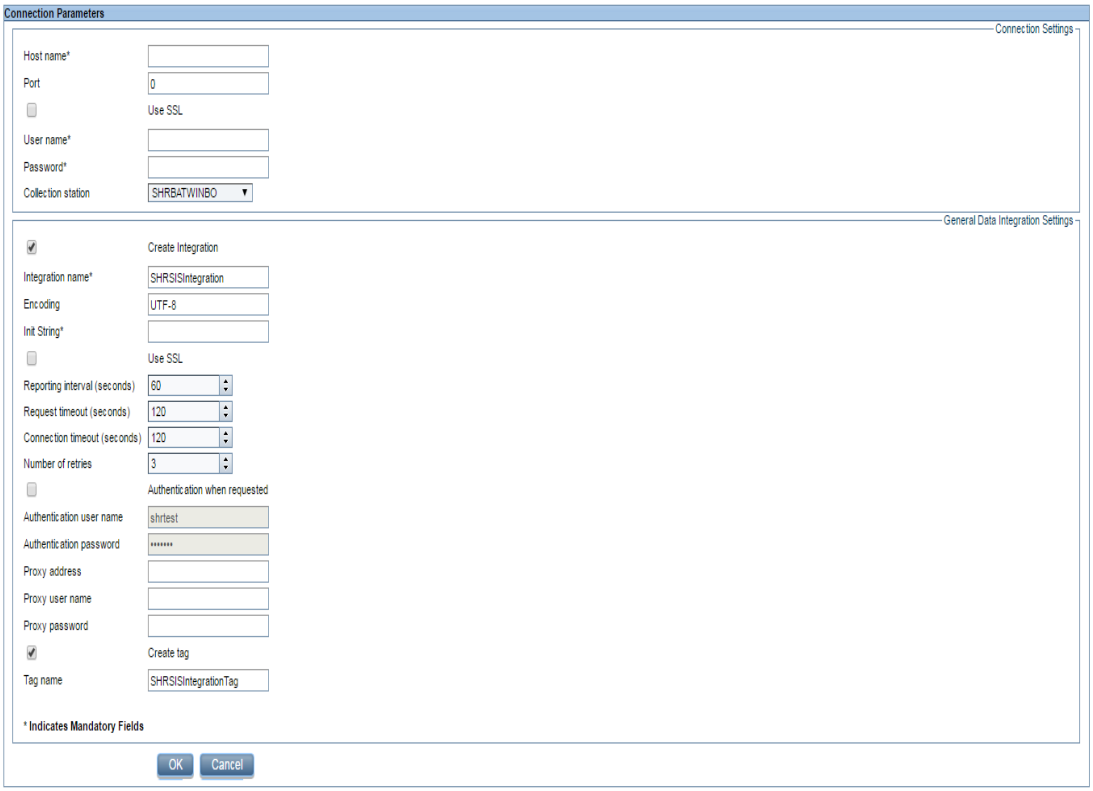
If you have configured the RTSM topology source, **Discover Data Source** discovers all the associated SiteScope servers. Also, you must have deployed the `SiteScopeProfileView.zip` from the location `{PMDB_HOME}\packages\SystemManagement\ETL_SystemManagement_SiS_API.ap/source/cmdb_views`.



If you have enabled SSL for SiteScope, perform the steps mentioned in "SiteScope with SSL enabled" on page 118.

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:



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	*(Optional).* If selected, you must enable the SiteScope server to

Field	Description
	support communication over Secure Sockets Layer (SSL). If you have enabled SSL for SiteScope, perform the steps mentioned in "SiteScope with SSL enabled" on the next page.
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 HPE OBR server. After the connection is successful, SiteScope servers push data to the HPE OBR server. Also, you must create a tag in HPE 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.	
Integration name	Enter the name of the integration. **Note**: You cannot change it later.
Encoding	The encoding type for communication between HPE 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	*(Optional).* 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 the next page. For HPE 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 page 119, after completing the Sitescope data source configuration.
Reporting interval (seconds)	Frequency at which SiteScope pushes data to HPE OBR.
Request timeout (seconds)	The time to wait before the connection times out. To configure infinite timeout, set it as 0.

Field	Description
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 HPE OBR.
Authentication when requested	*(Optional).* If selected, authentication is performed using the Web server user name and password.
Authentication user name	If HPE OBR is configured to use basic authentication, specify the user name to access the server.
Authentication password	If HPE 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. Click **OK**.
5. 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 *HPE Operations Bridge Reporter Administration Guide*.

SiteScope with SSL enabled

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

1. Copy the certificate from Sitescope server to HPE OBR server `{PMDB_HOME}/config` folder.
2. Rename the certificate extension with `.pem`.
3. Run the command `keytool -v –list –keystore <certificate name.pem>` to verify the certificate.

> **Note:** The password is `changeit`.

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

4. Perform the steps "Configuring the SiteScope Data Source" on page 115.
5. Go to the location `{PMDB_HOME}/stores` and verify if `cacert.jks` file is created.

Configuring OBR server to get data from SiteScope in HTTPs mode

Perform these steps to configure the OBR server to get the data from Sistescope server in HTTPs mode after "Configuring the SiteScope Data Source" on page 115:

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 HPE OBR Collector system, run the following command to export the HPE 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 HPE OBR server, restart the `HPE_PMDB_Platform_Collection` service.

Configuring the Management and Profile Database Data Source

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

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

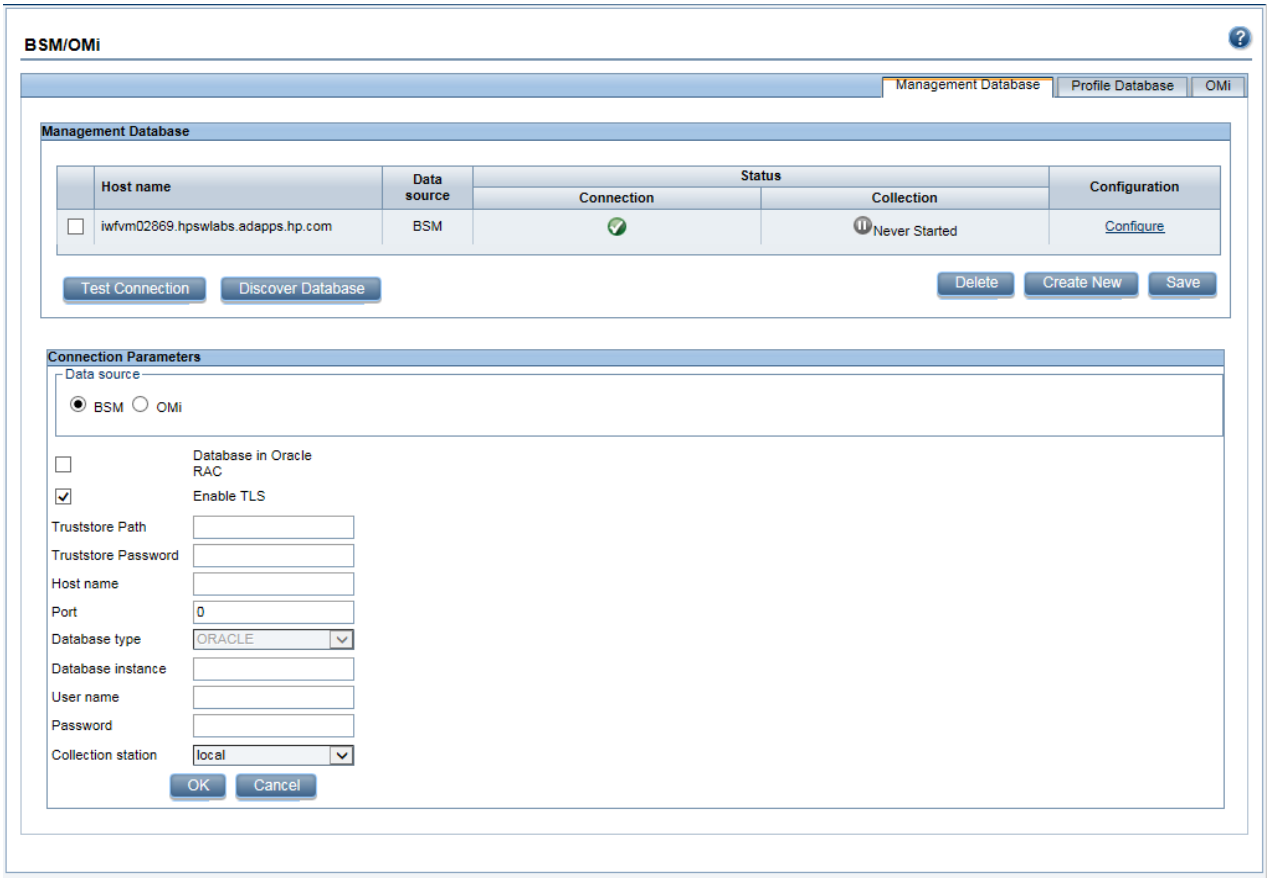
In your HP BSM deployment, you might have to set up multiple Profile databases for scaling because one database might not be enough to store all the data. You may also require multiple Profile database to store critical and non-critical data. The information on different Profile databases deployed in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

To configure a new Management Database, follow these steps:

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

   > **Note:** To discover Profile or Operations database in HPE OBR system, you must copy the `seed.properties` and `encryption.properties` files from HP BSM/OMi server to HPE OBR system. For more information, see "Discover Profile or Operations Database" on page 169.



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
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**.
Host name	IP address or FQDN of the Management Database server. Not displayed when **Database in Oracle RAC** is selected.

Field	Description
Port	Port number to query the Management Database server. Not displayed when **Database in Oracle RAC** is selected.
Database type	The type of database engine that is used to create the Management Database. If you have selected the **Data Source** as **BSM** then the database type can either be **Oracle** or **MSSQL**. If you have selected the **Data Source** as **OMi** then the database type can be **Oracle**, **MSSQL**, or **PostgreSQL**.
Windows Authentication	If you have selected MSSQL as the database type, you have the option to enable Windows authentication for MSSQL, that is, the user can use the same credentials to access SQL Server as that of the Windows system hosting the database.
Database 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 (available at `${PMDB.HOME}/config` folder) contains connection information to the Oracle Real Application Cluster. This option appears only if **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 HP Business Service Management administrator.
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, 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.

Field	Description
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 HPE 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).

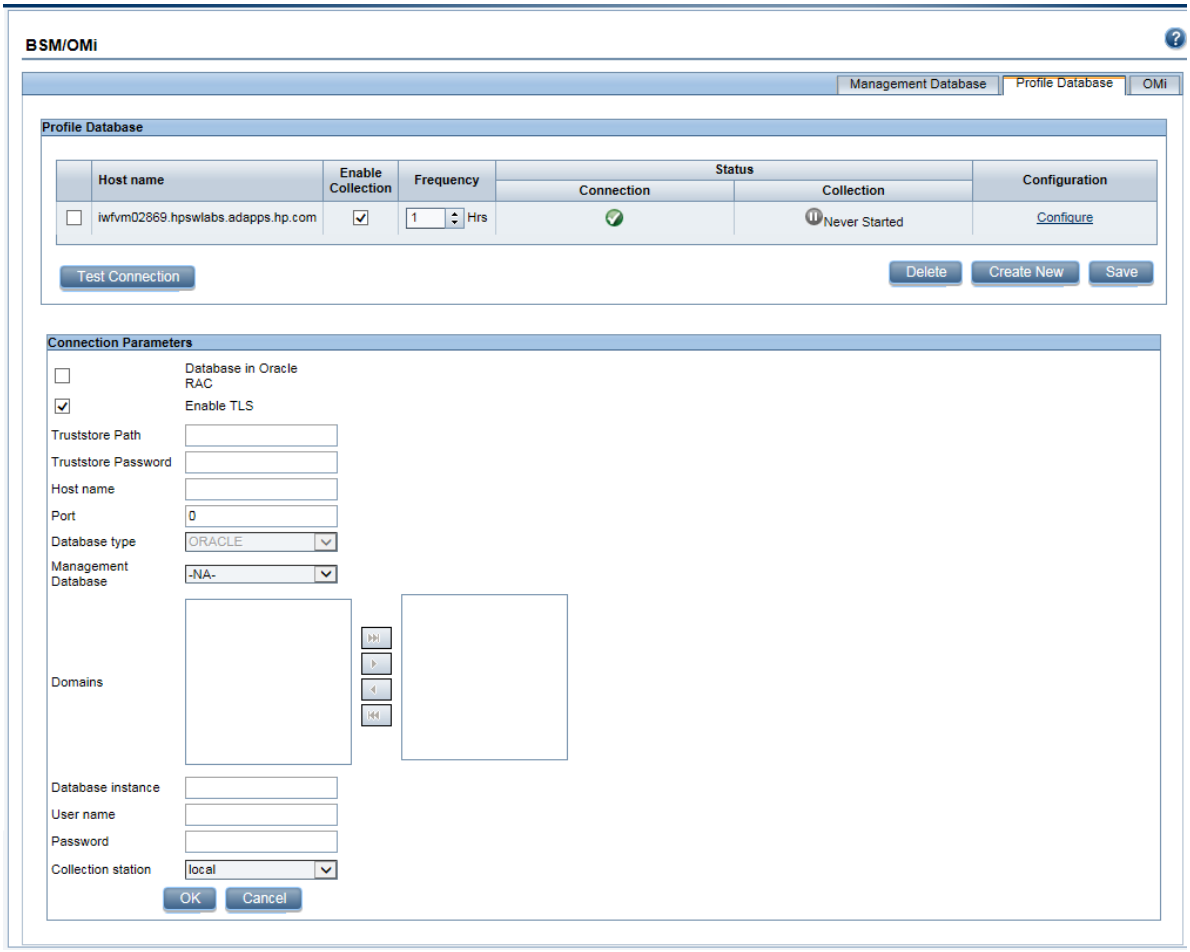
> **Note:** If management database and profile database are on the same system as the BSM system (local database), clicking **Discover Database** will automatically discover the corresponding Profile database. If the databases are on different systems (remote database), you have to manually configure 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/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
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**.
Host name	IP address or FQDN of the Profile Database server. Not displayed when **Database in Oracle RAC** is selected.

Field	Description
Port	Port number to query the Profile Database server. Not displayed when **Database in Oracle RAC** is selected.
Database type	The type of database engine that is used to create the Profile Database. It can either be Oracle, or MSSQL.
Management Database	Links Profile Database to the Management Database. If you collect data from only SiteScope, no Management Database needs to be selected.
Domains	Select the domains for which you want to enable data collection. **Note:** You must select the domains from which you want to enable data collection. Content Pack is associated with a domain name. If you install any Content Pack after you have configured the data source then you must map the Content Pack with appropriate domain name. Therefore, if you have configured the data source and then installed the Content Pack, you must return here to select among the following domains to enable data collection: ◦ RUM ◦ BPM ◦ ServiceHealth ◦ SM ◦ SM_VMware_SiS
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 HP Business Service Management administrator.
Windows Authentication	If you have selected MSSQL as the database type, you have the option to enable Windows authentication for MSSQL, that is, the user can use the same credentials to access SQL Server as that of the Windows system hosting the database.
Database name	Name of the database.
Database in Oracle RAC	This option appears only if you have selected Oracle as the database type.

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.
User name	Name of the Profile 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 Profile 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.

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, HPE 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 *HPE Operations Bridge Reporter Administration Guide*.

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. HPE 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 HP BSM. For more information, see the *Persistent Data and Historical Data* section of the *HP Business Service Management - Using Service Health* guide. This guide is available for the product, *Application Performance Management (BAC)*, at the following URL:

http://h20230.www2.hp.com/selfsolve/manuals

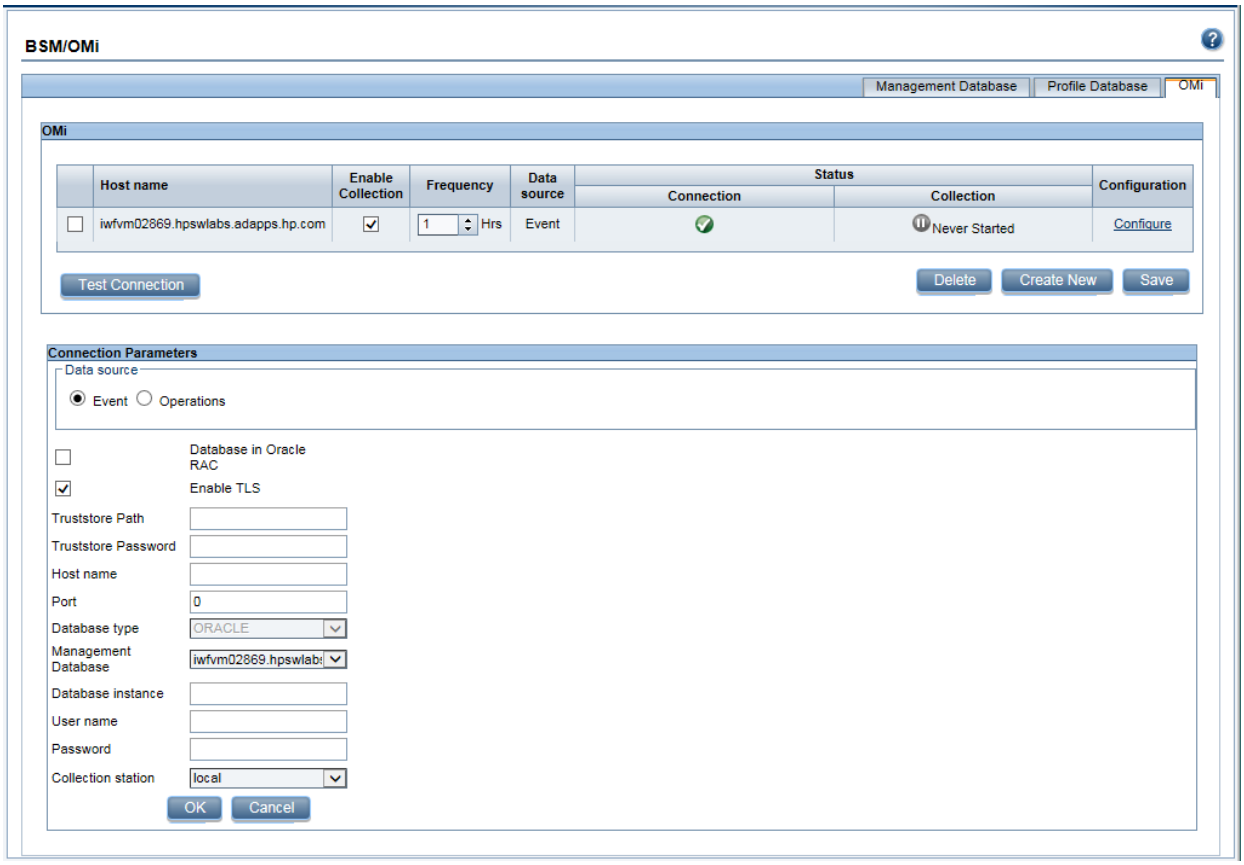
Configuring the HP OMi Data Source

If you install the HP OMi Content Pack, you must configure the HP OMi database connection for data collection. You can configure HPE 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 HP 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 120. This data connection is required to retrieve Assigned User/Group information for HP 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 HP BSM RTSM that was configured as the topology source.



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

1. In the **Administration Console**, click **Data Source Configuration > BSM/OMi > OMi**.
2. Click **Create New** to create a new HP 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
Data Source	Event or Operations **Note:** Select **Event** for OMi 9.x version and **Operations** for OMi 10.x and later versions.
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.

Field	Description
Truststore Password	The password to access the trust store. This option appears only if you have selected **Enable TLS**.
Host name	Address (IP or FQDN) of the HP OMi database server.
Port	Port number to query the HP OMi database server.
Database type	The type of database engine that is used to create the HP OMi database. If you have selected the **Data Source** as **Event** then the database type can either be **Oracle** or **MSSQL**. If you have selected the **Data Source** as **Operations** then the database type can be **Oracle**, **MSSQL**, or **PostgreSQL**.
Windows Authentication	If you 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.
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.
Management Database	Links Event or Operations Database to the Management Database. If you collect data from only SiteScope, no Management Database needs to be selected.
Database instance	System Identifier (SID) of the HP OMi database instance. If MSSQL Server is configured to use default (unnamed) database instance, leave this field empty. For information about the database hostname, port number and SID, contact your HP OMi database administrator.
User name	Name of the HP OMi database user. If the Windows Authentication option is selected, this field is disabled and appears empty.
Password	Password of the HP OMi database user. If the Windows Authentication option is selected, this field is disabled and appears empty.

Field	Description
Collection Station	To specify whether it is a Local / Remote Collector

4. Click **OK**.

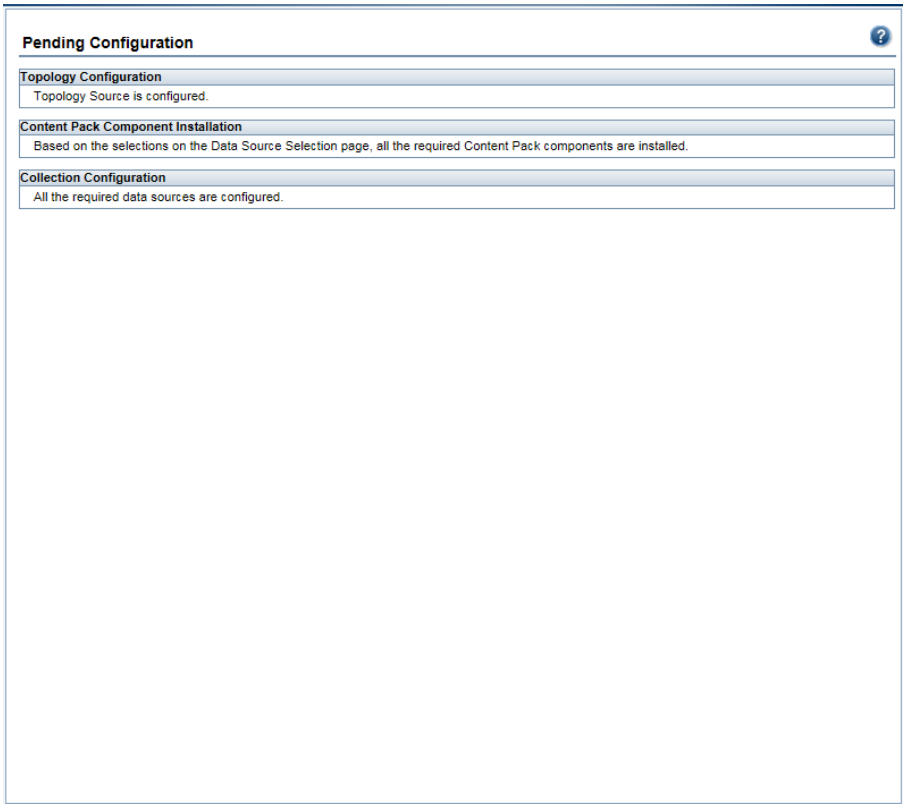
> **Note:** You can create only one HP OMi data source connection. After the connection is created, the **Create New** button is disabled by default. Make sure that you type in the correct values.

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 HP 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.

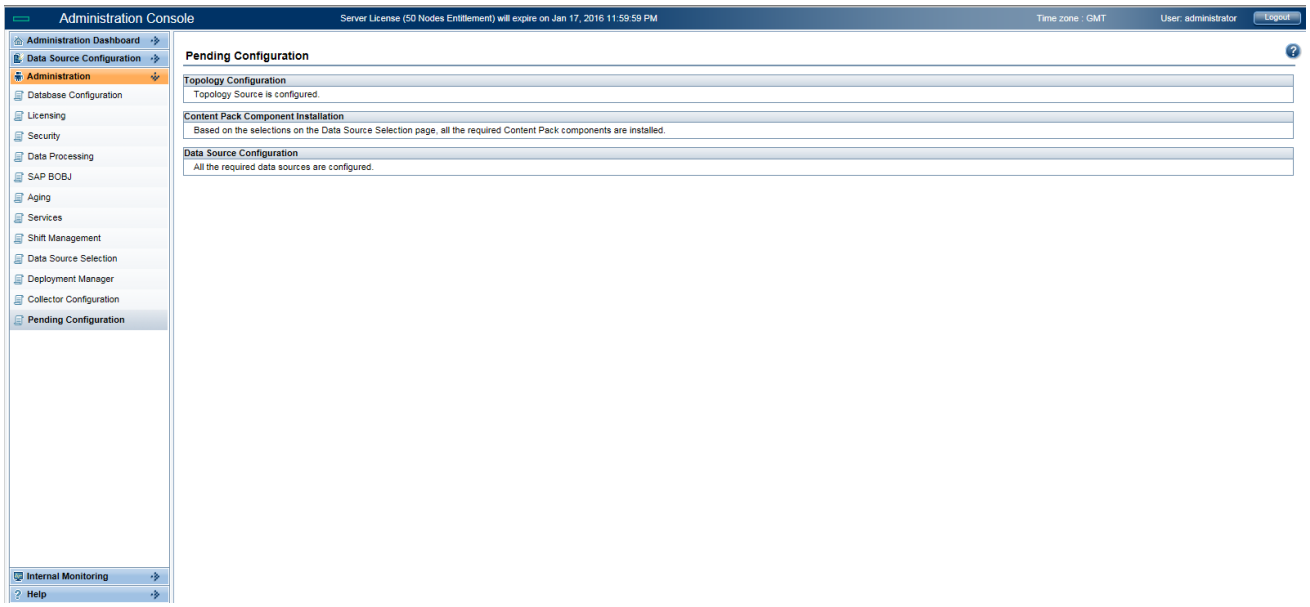
For more information about configuring HP OMi data source connections, see the *HPE Operations Bridge Reporter Administration Guide*.

Chapter 7: Pending Configuration

This page displays status of Topology Configuration, 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 corresponding links to complete the pending configurations.


Administration Console
Server License (50 Nodes Entitlement) will expire on Jan 17, 2016 11:59:59 PM
Time zone : GMT
User: administrator
Logout
Administration Dashboard
Data Source Configuration
Administration
Database Configuration
Licensing
Security
Data Processing
SAP BOBJ
Aging
Services
Shift Management
Data Source Selection
Deployment Manager
Collector Configuration
Pending Configuration
Internal Monitoring
Help
Pending Configuration
Topology Configuration
Topology Source is configured.
Content Pack Component Installation
Based on the selections on the Data Source Selection page, all the required Content Pack components are installed.
Data Source Configuration
All the required data sources are configured.

Part III: Additional Configuration and Administration

This section provides information and procedures to configure and administer HPE OBR. This section helps you to configure HP 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 HP Operations Agent for Data Collection in Secure Mode

The HP 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 HP Operations Agent-managed nodes via the secure (HTTPS) mode. Because HTTPS communication is certificate-based, certificates must be installed on the HPE OBR system and on the managed nodes. The HPE OBR system acts as a certificate client and the certificate server (certificate authority) is provided by the HPOM.

If the SSL_SECURITY is enabled in agents, then the collection from the agent to HPE 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 HPE 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 HPE OBR or remote collector, follow these steps:

Task 1: Configuration on HPE OBR system

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

   ```
   ovcert -list
   ```
3. To delete the certificate on HPE 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 HPE OBR machine:

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

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

   <obr_hostname> is the name of the HPE 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 HPE OBR system:

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

11. Run the following command on the HPE 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 HPE 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 HPE 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 HPE OBR system, follow these steps:
   a. Log on to HPE 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 **Administration > Collectors** and configure the new remote collector.

    For information on configuring the new remote collector, see "Task 5: Configuring the Collectors Installed on Remote Systems" on page 1.

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 HPE 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 HPE 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 HPE 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 **Administration > Collectors** and click **Test** and then click **Save**.

Chapter 9: Configuring the Report Drill Feature Settings

HPE 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/BSMRApp`

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

   The Log on page is displayed.

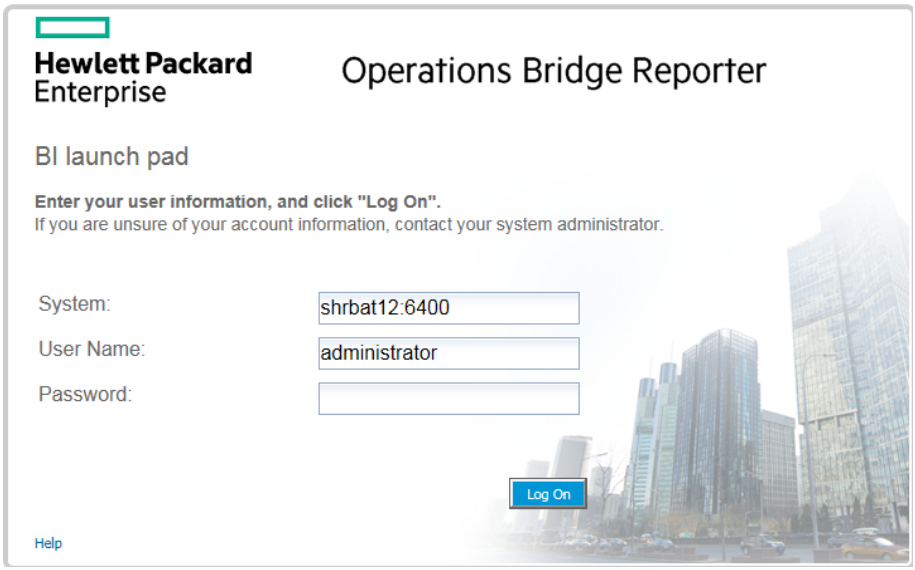
2. Enter user name as **administrator** in the **User Name** field and password in the **Password** field.
3. Click **Log On**.

   The **Home** page is displayed.

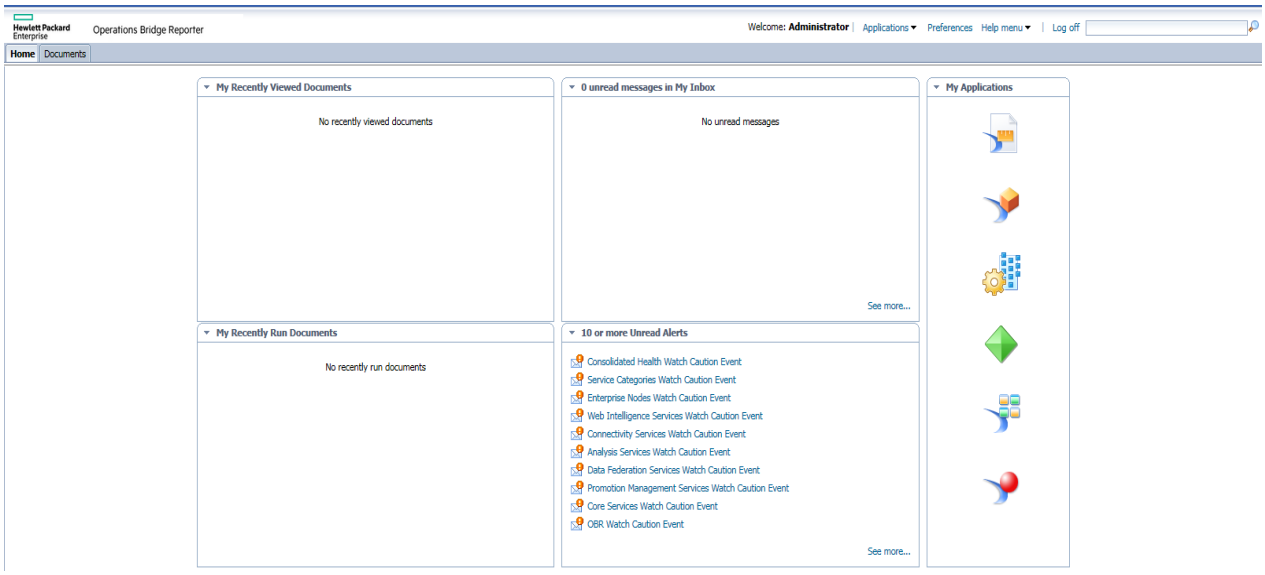
4. In the Administrator Console, click **Administration > SAP BOBJ**.

   The **SAP BOBJ** page is displayed.

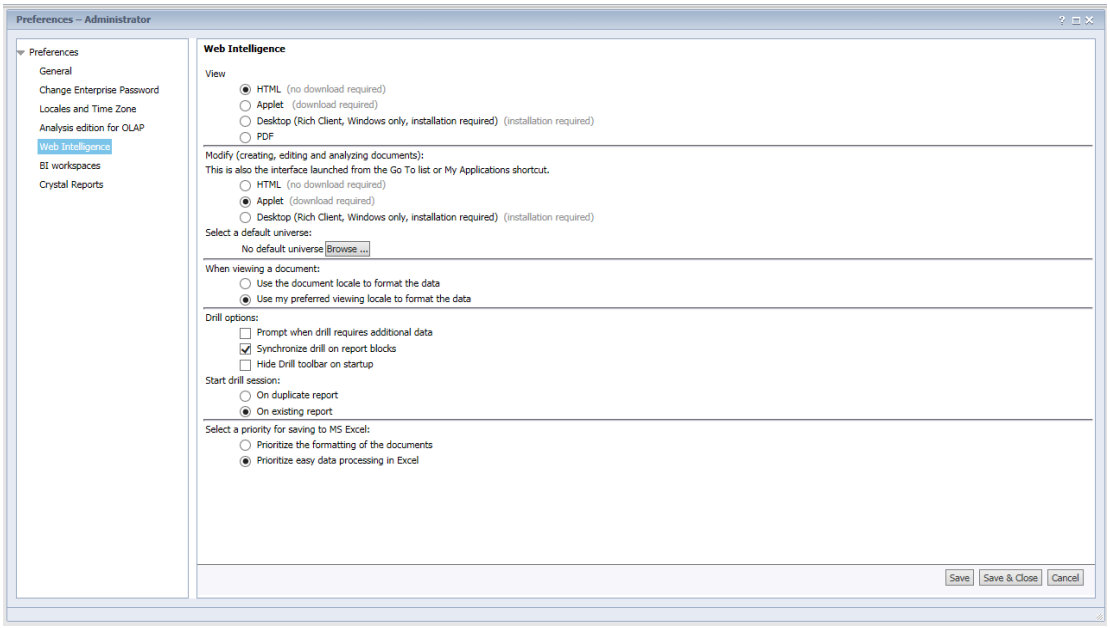
5. Click **Launch BI launch pad**. The SAP BusinessObjects BI launch pad log on page is displayed.



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. HPE OBR can be configured to send traps or emails when there is a failure in HPE OBR system. You can also view the alerts in administration console of HPE 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 HPE 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_Depolyment.conf` file first and gets information on the HPE 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 HPE 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 HPE 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 HPE 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 HPE OBR is installed in `email.from` parameter.

   c. Enter the domain name of the mail server in `email.host` parameter.

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

> **Note:** Copy the `hp-shr.mib` and `hp-nnnmi.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.

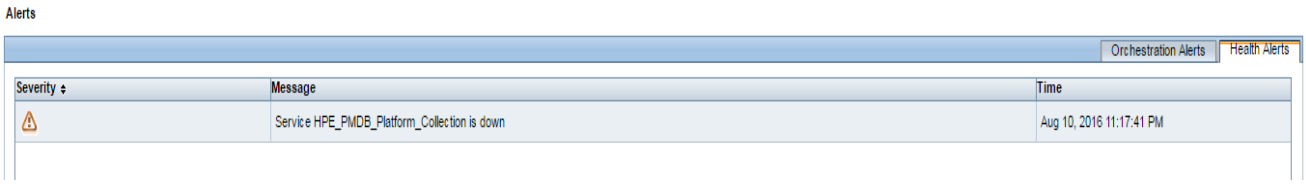
2. Save and close the `IA_Config.prp` file.
3. On a system where HPE OBR is installed, open the command prompt and run the following command to enable the internal alerting service:

   ```
   enableIA
   ```

4. Restart the **HPE_PMDB_Platform_IA** service.

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

1. Log on to Administration Console. The **Home** page is displayed.
2. Click **Health Alerts** tab to view the internal alerts.



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 HPE OBR

This chapter provides information on Client Authentication certificate for HPE 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:** HPE OBR highly recommends the use of Certificate Authority (CA) signed certificate. To configure HPE OBR to use the CA signed certificate, see *Generating a Certificate Authority Signed Certificate* section in *HPE Operations Bridge Reporter Interactive Installation Guide*.
>
> HPE OBR does not recommend the use of self-signed certificate when setting up the SSL connection.

Client Authentication Certificate for HPE OBR

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

Authentication and Authorization

HPE 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 HPE OBR Administration console. By default, HPE OBR uses username/password based authentication mechanism. You can also configure HPE OBR to use client certificate based authentication by following the steps in "Configuring HPE OBR Administration Console " for Administration console and "Configuring SAP BusinessObjects BI Launch Pad" for SAP BusinessObjects BI Launch Pad. HPE 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 HPE OBR server certificate and private key

The keystore file is password protected. HPE 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 152 for Administration Console and "Task 4: Set up the Certificate-based configuration" on page 156 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

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 HPE OBR server. This file is password protected. HPE 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

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. HPE 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. HPE 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 (OSCP) - OSCP is a protocol for checking revocation of a single certificate using an online service called an OSCP responder. You should set ocsp.enable to true to enable revocation check using OCSP protocol. HPE OBR extracts the OCSP URL from the certificate for validating the certificate. If you want to configure a local OCSP responder service, HPE OBR enables you to configure it using ocsp.responderURL property.

For details on how to enable certificate revocation, CRL and OSCP on HPE OBR Administration Console, see "Task 4: Configuring for Certificate-based Authentication" in "Configuring HPE 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 HPE OBR server and internet

In case of a proxy server, you must set it to enable HPE 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 HPE 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. HPE 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="" useSubjectDNonMatchFail="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@hp.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, HPE OBR extracts username from CN of SubjectDN.

  You can configure HPE 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 HPE 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.

HPE 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 HPE OBR Administration Console

Before you proceed, ensure that the post-install configuration of HPE OBR is successful. To configure HPE OBR Administration Console for Certificate Based Authentication, follow these steps:

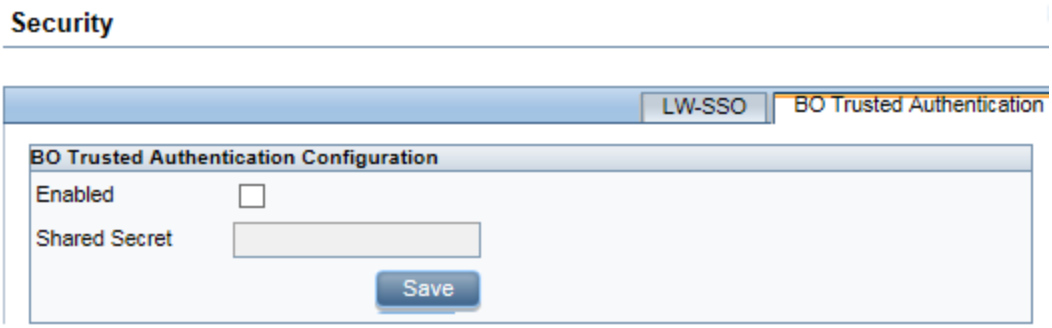
Task 1: Configuring trusted authentication

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/BSMRApp` on the browser to log on to the Administration Console of HPE OBR.

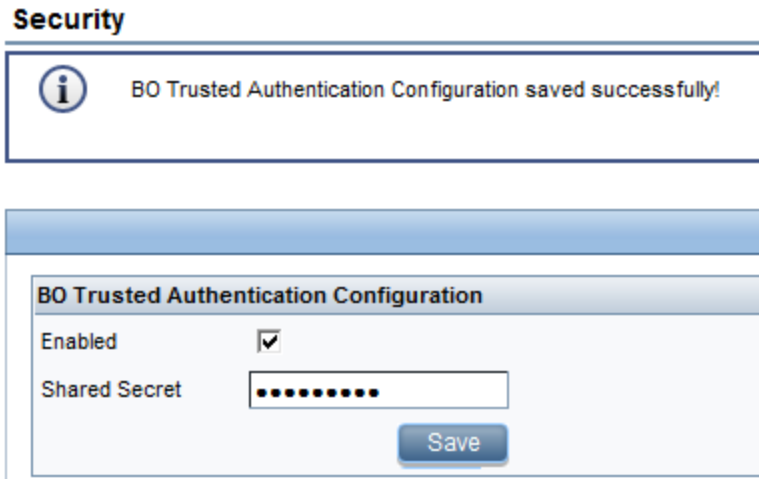
   where,*<OBR_Server_FQDN>* is the fully qualified domain name of the system where OBR is installed.

2. Go to **Administration > Security > BO Trusted Authentication**



3. Select the **Enabled** check box.
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:

  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: `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
`shr.loginMethod`	`certbased`
`shr.auth.classes`	`com.hp.bto.bsmr.security.auth.BOTrustedAuthenticator`

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
`truststorepath`	Full path of the truststore file, which is to use to validate client certificates.
`truststorepasswd`	The password to access the trust store.
`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 `adminsever.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 `adminsrver.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 HPE OBR. Incase 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:

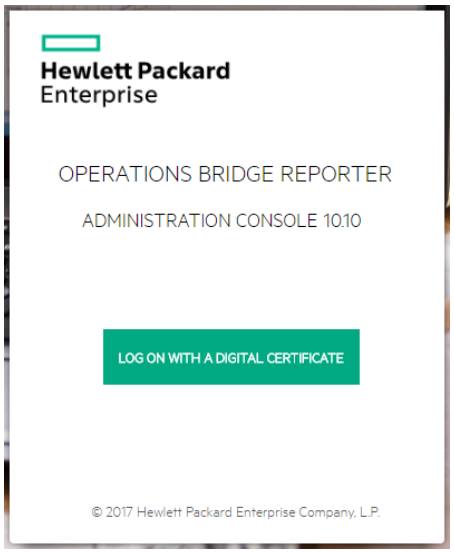
  On RHEL 6.x: `service HPE_PMDB_Platform_Administration start`

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

Task 7: Verify certificate based authentication

1. Type `https://<OBR_Server_FQDN>:21412/BSMRApp` on the Web browser to log on to the Administration Console of HPE 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**.

Configuring SAP BusinessObjects BI Launch Pad

> **Note:** In a custom installation of HPE 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 HPE 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 `/opt/HP/BSM/PMDB/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: `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
`bo.protocol`	`https`

Task 4: Set up the Certificate-based configuration

> **Note:** In a custom installation of HPE 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
truststorepath	Full path to the truststore file
truststorepasswd	The password to access the trust store
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 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`.

- **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`.

Task 5: Start the SAP BusinessObjects WebServer service

> **Note:** In a custom installation of HPE 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 `/opt/HP/BSM/PMDB/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: `service HPE_PMDB_Platform_Administration start`

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

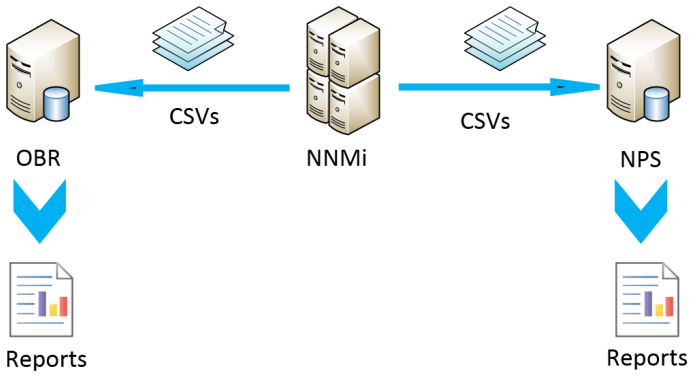
Task 7: Verify certificate based authentication

1. Type `https://<HostName>:8443/BI` on the web browser and log on to the BI launch pad of HPE 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 HPE 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 HPE OBR is integrated with NNMi to collect network performance data. The NNMi passes the network performance data as `.csv` files to both HPE OBR and Network Performance Server (NPS). The HPE 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. HPE 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.

> Based on your requirement, HPE 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 HPE OBR and NNMi to collect network data, follow these steps:

Task 1: On the NNMi system

To configure HPE 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 `nnmenableperfspi.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 `nnmEnableNps.20xxxxxxxxxx.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 is the 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 HPE OBR system

To configure HPE 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 HPE 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 HPE 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 unsupportable.

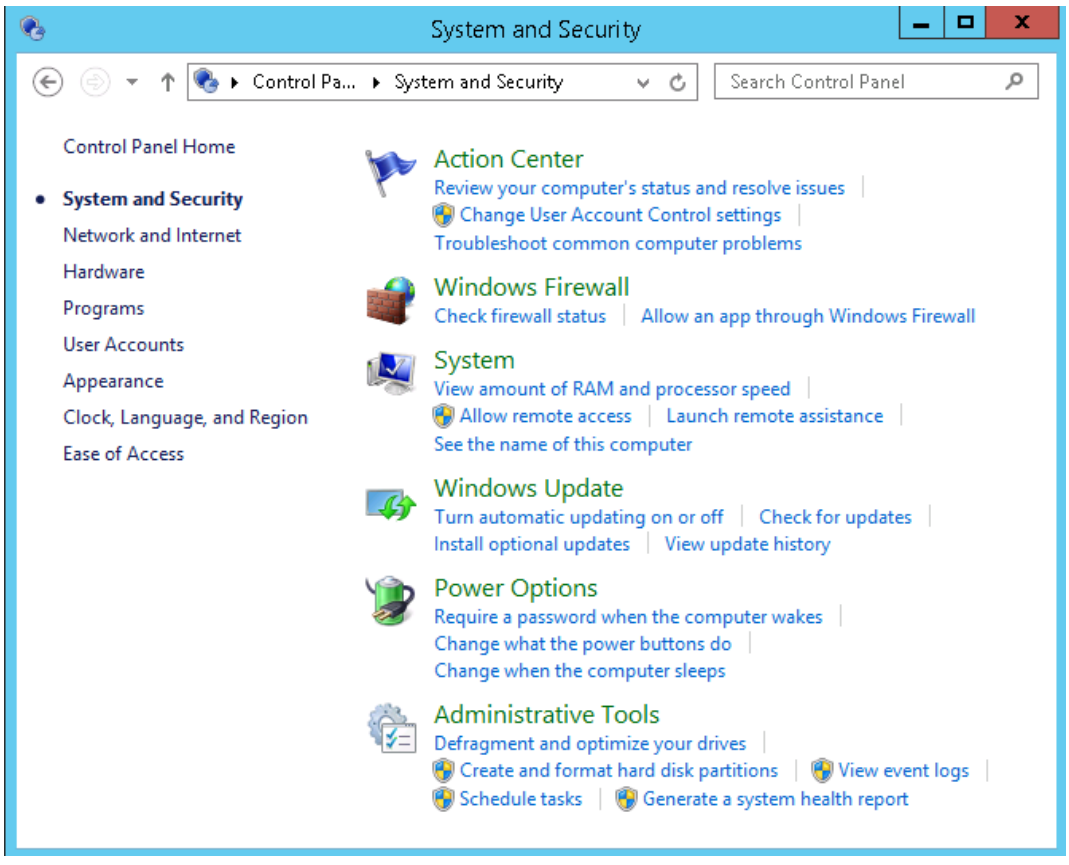
You have now successfully completed the configuration of HPE OBR with NNMi system.

Chapter 13: Configuring DSN on Windows for Vertica Database Connection

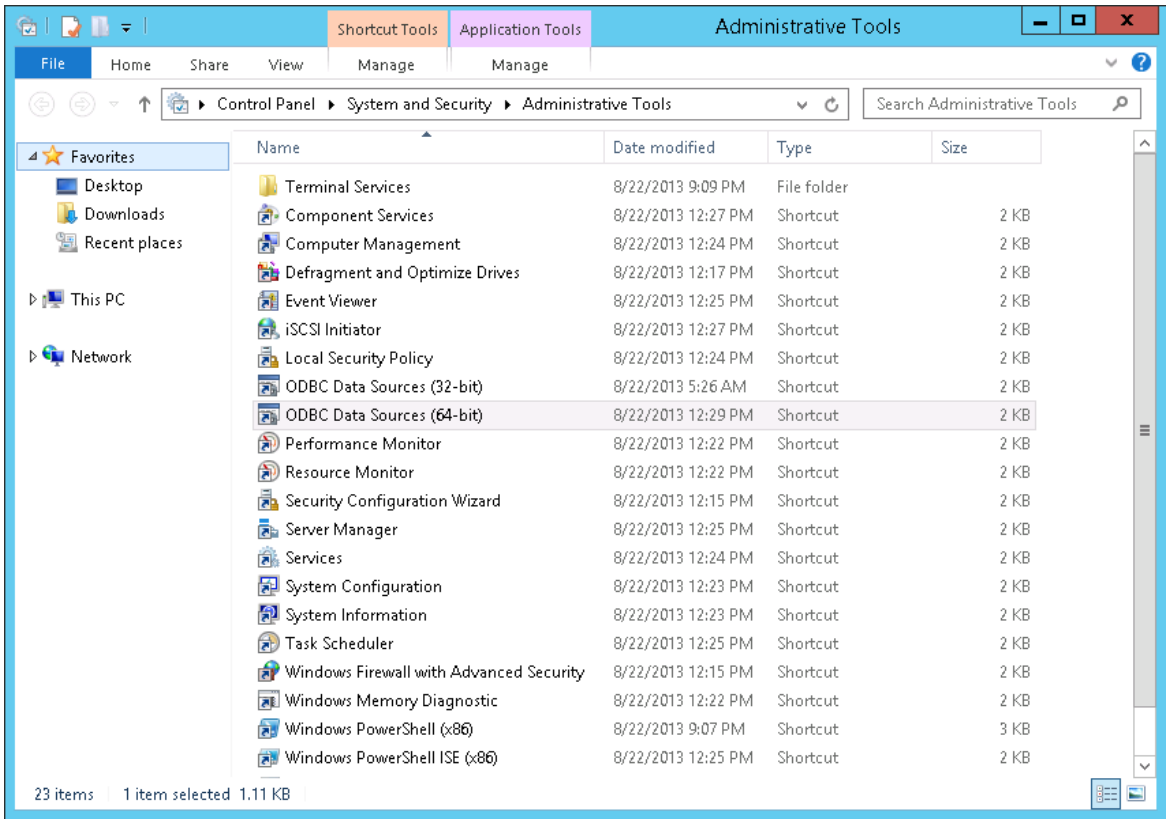
You must configure DSN only if HPE OBR is installed on Windows. If HPE OBR is installed on Linux then the installer automatically handles the DSN configuration and connection to Vertica database.

To configure DSN to connect to Vertica database, follow these steps on HPE OBR system installed on Windows:

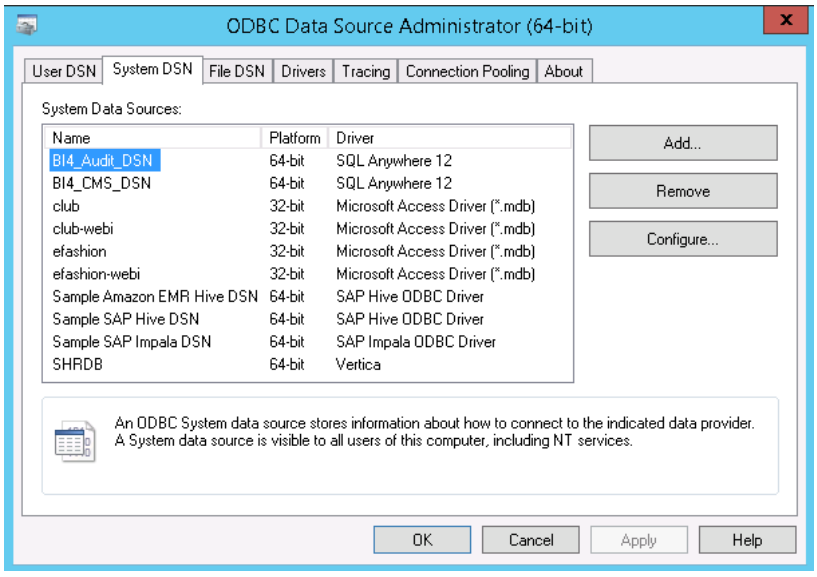
1. Log on to HPE OBR system installed on Windows.
2. Click **Start > Control Panel** and then click **System and Security**. The **System and Security** windows is displayed.



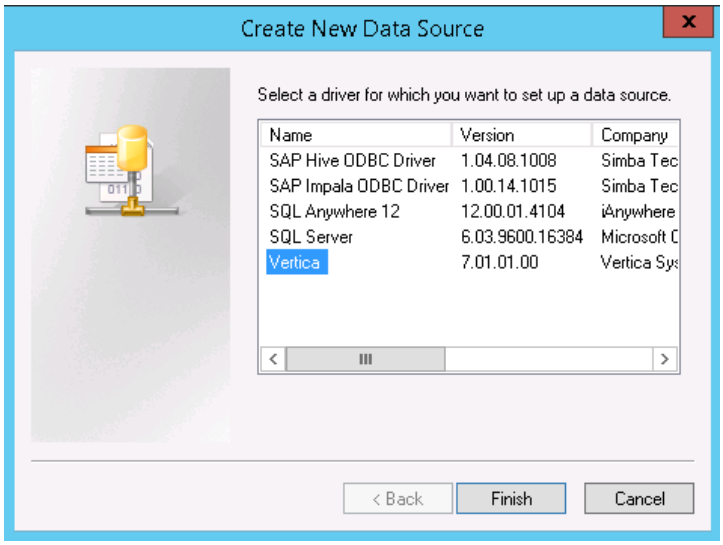
3. Click **Administrative Tools**. The Administrative Tools window is displayed.



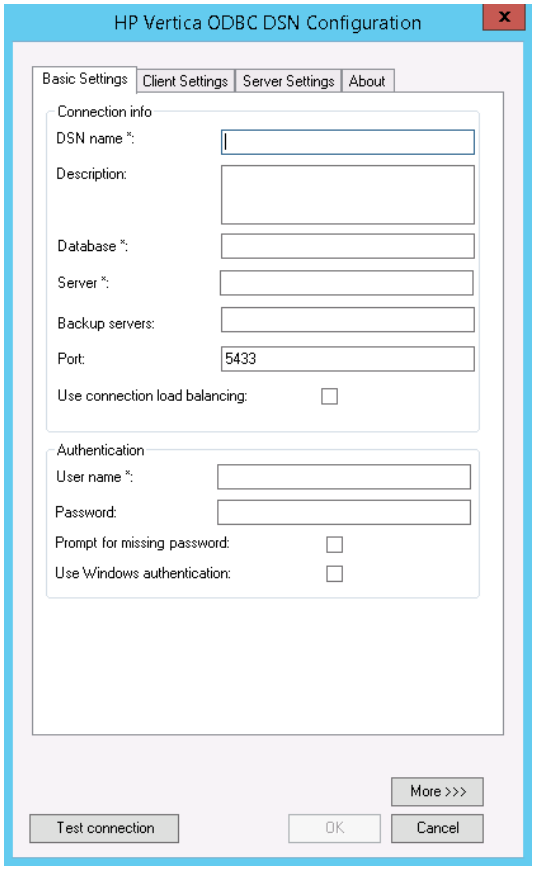
4. Double-click **ODBC Data Sources (64-bit)**. The **ODBC Data Source Administrator (64-bit)** window is displayed.



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 **HP 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 HPE 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 202.

Chapter 14: Discover Profile or Operations Database

OBR supports the configuration of data collection from multiple Profile databases that are deployed in your HP 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 HP OMi Data Source" on page 127.
>
> 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 HPE 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: `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 HPE OBR system

1. Log on to the HP BSM/OMi host system through remote access.

   > **Note:** If your HP BSM setup is distributed, you can access through the gateway server as well as the data processing server. HPE 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 HPE 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 HPE 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: `service HPE_PMDB_Platform_Administration restart`

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

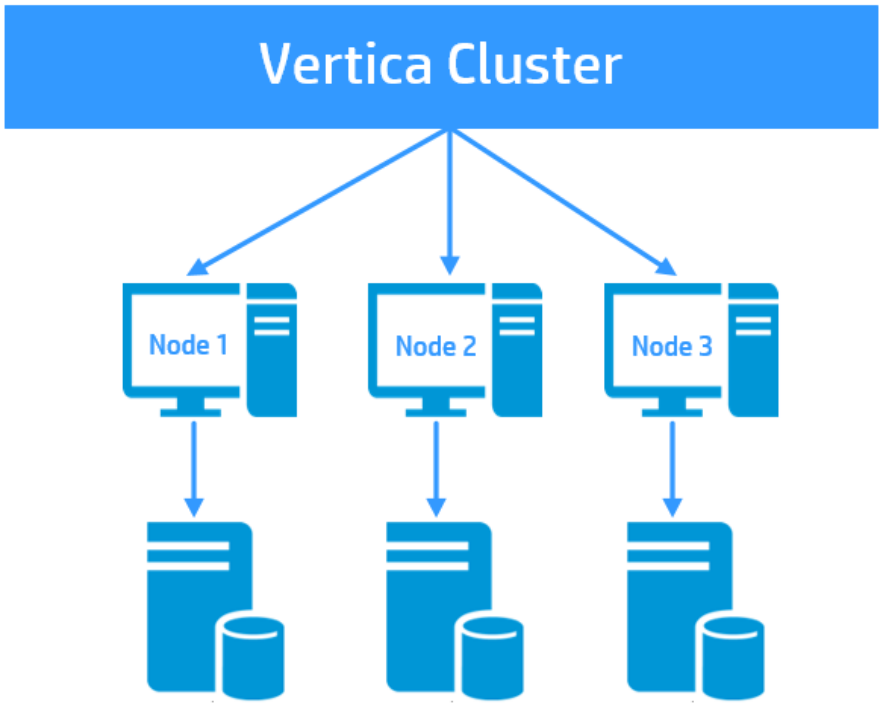
> **Caution:** Ensure to take a backup of the HPE OBR database in case you need to restore it later. If you fail to take a data back up, you risk losing it permanently. For more information, see the "Part IV: Database Backup and Recovery" on page 206.

Chapter 15: Configuring HPE OBR to Setup Vertica Cluster

HP 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 *HP Vertica Analytic Database Concepts Guide*.

Chapter 16: Configuring HPE OBR for External Vertica

HPE 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 HPE OBR to the same Vertica database. Else, if you already have Vertica installed with HPE 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 HPE OBR before you perform steps to configure HPE OBR for external Vertica.

For New HPE OBR Installation

If you are installing HPE OBR for the first time then the steps to configure external Vertica can be based on the following scenarios:

- Scenario 1: HPE OBR is the only product with Vertica as database.
- Scenario 2: HPE OBR is installed before the other products are installed.
- Scenario 3: HPE OBR is installed after the other product installation.
- Scenario 4: HPE OBR is installed after the other product installation and then again other product is installed.

For Existing HPE OBR Installation

If you have already installed HPE OBR, post install configuration is also complete and you want to configure HPE OBR for external vertica, see "Configuring HPE OBR for External Vertica after Post Installation" on page 177.

For New HPE OBR Installation

Scenario 1: HPE OBR is the Only Product

If HPE OBR is the only product using Vertica database then to configure HPE OBR to support external Vertica, follow these steps:

1. **Typical scenario**: If HPE OBR is installed in typical scenario, follow these steps:
   a. During post-installation configuration, in step 2 of Configuration Wizard, 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 HPE 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>`

      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 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.

b. During post-installation configuration, in step 2 of the Configuration Wizard, 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.

   For more information, see Creating Database Schema for Remote Vertica.

Scenario 2: HPE OBR is Installed Before Other Product

If you have installed HPE OBR before installing other products then to configure external Vertica, follow these steps:

1. Install HPE OBR and configure external Vertica as per steps given in "Scenario 1: HPE OBR is the Only Product " on the previous page.
2. Install other products.
3. Check the number of connections for HPE OBR and update the connections and LockTimeout settings in HPE OBR system accordingly. By default, the number of connections for HPE OBR is 150. So, update the connection as 150 + other products connections in the HPE 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. HPE OBR is already installed and to change the schema from public to OBR, follow steps given in section "Configuring HPE OBR for External Vertica after Post Installation" on page 177.

Scenario 3: HPE OBR is Installed After Other Products

If you have installed HPE 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 HPE 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 HPE OBR system using the same OBR user.

Scenario 4: HPE OBR is installed after the other product installation and then again other product is installed

If you install other products first, then HPE 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 HPE OBR for external Vertica.

To configure HPE OBR for external Vertica, follow these steps:

1. Perform the steps given in scenario 3, see "Scenario 3: HPE OBR is Installed After Other Products" on page 175.
2. Perform the steps given in scenario 2, see "Scenario 2: HPE OBR is Installed Before Other Product" on page 175.

For Existing HPE OBR Installation

If you have already installed HPE OBR and post install configuration is complete then in Vertica, PMDB database is created with public schema. To Configure the existing HPE OBR for external Vertica, you have to move the public schema to OBR schema.

Configuring HPE OBR for External Vertica after Post Installation

To configure HPE OBR for external Vertica, follow these steps:

1. Install HPE 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 User Name> <Vertica Database Password>`

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

`<Vertica Database 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 HPE OBR

You can configure logon banner after post install configuration for Administration Console, SAP BusinessObjects and CMC in HPE 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.

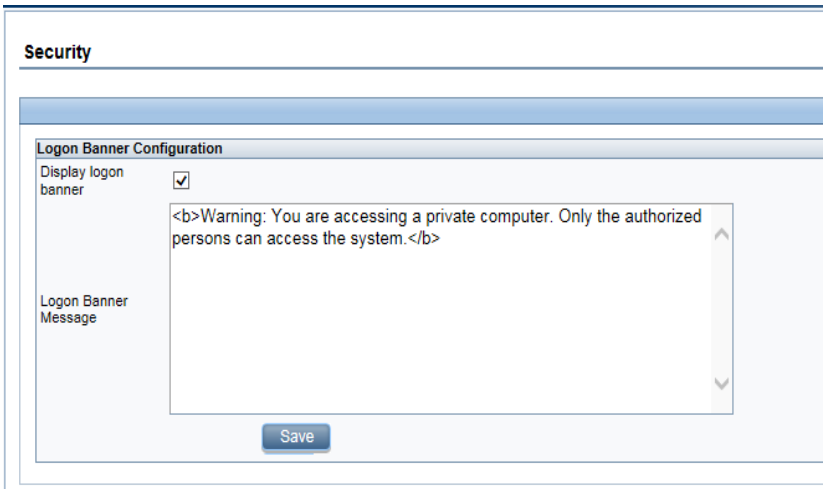
Enabling the Logon Banner

To enable the logon banner, follow these steps:

1. Log on to Administration Console and click **Administration > Security**.

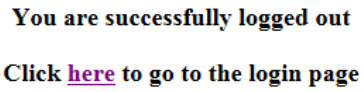
   The **Security** page is displayed.

2. Click **Logon Banner** tab and select the **Display logon banner** check box.

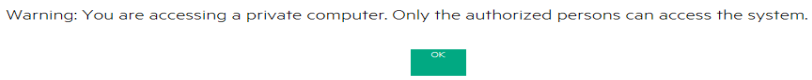


In the **Logon Banner Message** text box, a default warning message is provided. If you want to change the default message, click in the text box and enter your own logon banner message that must appear as the first screen to warn the user. You can also use HTML tags for formatting the message.

3. Click **Save**. A status message is displayed.
4. Click **Logout** to log out from Administration Console.



5. Click the link **here** to login again. The logon banner warning message is displayed.



6. Click **OK**. The usual log on screen is displayed.
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 or CMC from the web browser, 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 HPE OBR system to `{PMDB_HOME}/data/config.prp` in remote SAP BusinessObjects system.

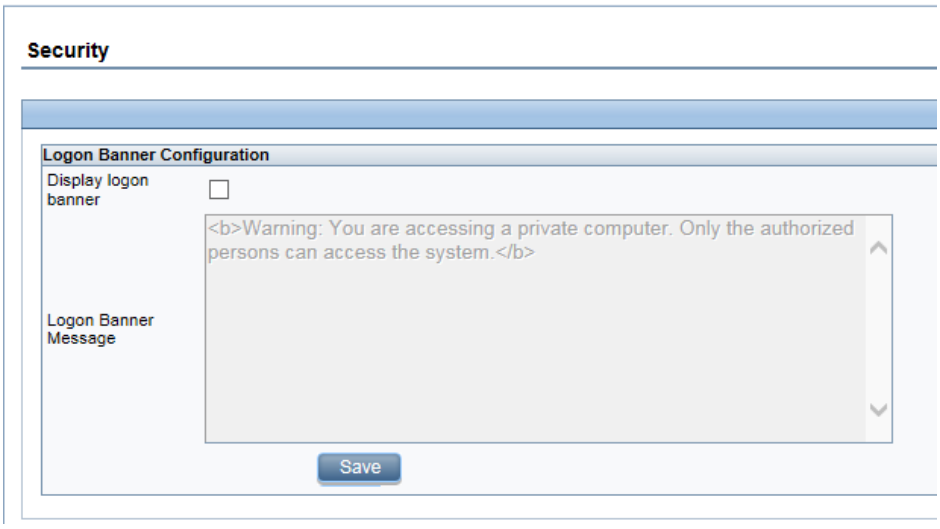
Launch the SAP BusinessObjects or CMC from the web browser, the logon banner warning message is displayed. Click **OK** and respective SAP BusinessObjects or CMC log on screen is displayed. Enter the user credentials to log on and proceed with the tasks.

Disabling the Logon Banner

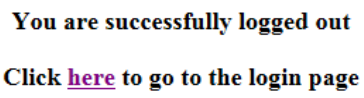
1. Log on to Administration Console and click **Administration > Security**.

   The **Security** page is displayed.

2. Click **Logon Banner** tab, uncheck the **Display logon banner** check box and click **Save**. A status message is displayed.



3. Click **Logout** to log out from Administration Console.



4. Click the link **here** to login again. The usual 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 HPE 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 HPE OBR

This section provides information on how to configure HPE 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.

HPE OBR in FIPS Mode

When you configure HPE 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

HPE 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 HPE 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, HPE OBR uses the following RSA BSAFE Crypto module FIPS certified algorithms for encryption and storage of HPE OBR sensitive data:

- Supported Encryption Keystore format: PKCS 12
- Supported asymmetric algorithm for HPE OBR Encryption Keystore: RSA (recommended size 2048)
- Supported symmetric key algorithm used by HPE OBR: AES (128-bit (default), 192-bit, and 256-bit key sizes)
- Supported Random Number Generation algorithm used by HPE 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 HPE 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 HP Operations Agent for Data Collection in Secure Mode" on page 134.
4. TLS communication is configured between Vertica and HPE OBR server /SAP BusinessObjects. See "Configuring TLS for Vertica" on page 191.

5. TLS communication is configured between OBR collector and BSM/OMi Oracle database. See "Data Source Configuration" on page 106.
6. TLS communication is configured between OBR collector and BSM/OMi RtSM. See "Data Source Configuration" on page 106.

To enable FIPS, follow these steps:

1. **Task 1: Enable FIPS**

   > **Note:** To enable FIPS in Vertica database, ensure to connect to Vertica database and perform only this task.

   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 and then run the `perl` command to 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. Locate the `<JavaVM>` and add the following parameters in `cs.cfg` file:

   ```
   <Option>-Djavax.net.ssl.trustStore=C:/HPE-OBR/verticatruststore.jks</Option>

   <Option>-Djavax.net.ssl.trustStorePassword=sslpassword</Option>
   ```

   The following is an example of the sample `cs.cfg` after adding the parameters:

   ```
   <JavaVM>

   <!-- The default JVM configuration can be overriden 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=C:/HPE-OBR/verticatruststore.jks</Option>
   ```

```
<Option>-Djavax.net.ssl.trustStorePassword=sslpassword</Option>
</Options>
</JavaVM>
```

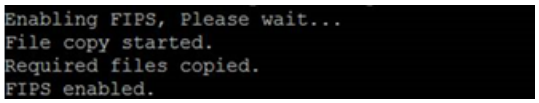
Enabling FIPS on any OBR component

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.



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 shradmin -
storepass shradmin -keystore SHR_CERT_PKCS.p12 -storetype pkcs12
```

c. Copy all the certificates (OMi CA certificate, Oracle server certificate, SiS certificate) to the FIPS enabled HPE 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 <cerficate alias> -
storepass 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 HPE 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**: `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.

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 `/opt/HP/BSM/PMDB/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.

5. **Task 5: Stop the HPE_PMDB_Platform_Collection service and edit Collection start and stop scripts**

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**: `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=shradmin -
Djava.security.manager=com.hp.opr.foundation.securitymanager.DenyDataDirectS
ecurityProviderInsertion
```

b. **On Linux**

Add the following argument to `$PMDB_HOME/bin/hpbsm_pmdb_collector_stop.sh` and `$PMDB_HOME/bin/hpbsm_pmdb_collector_start.sh`:

```
-Djavax.net.ssl.trustStore=$PMDB_HOME/keystore/SHR_CERT_PKCS.p12 -
Djavax.net.ssl.trustStorePassword=shradmin -
Djava.security.manager=com.hp.opr.foundation.securitymanager.DenyDataDirectS
ecurityProviderInsertion
```

c. Go to the location `{PMDB_HOME}/data`, open the `config.prp` file and add the following :

```
ucmdb.protocol=https

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.

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. Create a new storage disk.
2. Run the following command to change the owner and group to Vertica user for the newly created storage disk.

   `chown <Vertica User Name>:<vertica group> <Path of new disk mounted>`

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

   <vertica group> is the group vertica user belongs to

   > **Note:** The Vertica group is same as Vertica user name.

   <Path of new disk mounted> is the path where new disk is mounted
3. Open the sql prompt and run the following command to create the new disk location:

   `CREATE LOCATION '<Path of new disk mounted>' LABEL 'OBR';`

   where, *<Path of new disk mounted>* is the path where new disk is mounted
4. Run the following command to create the storage policy:

   `SELECT set_object_storage_policy ('<Vertica database name>','OBR');`

   where, *<Vertica database name>* is the name of the created database during post-install.

For more information, refer the following URLs:

https://my.vertica.com/docs/7.1.x/HTML/Content/Authoring/SQLReferenceManual/Functions/VerticaFunctions/ADD_LOCATION.htm

https://my.vertica.com/docs/7.1.x/HTML/Content/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 helps 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, 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
```

4. Log on to `vsql`.
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-----

      MIICXgIBAAKBgQDtWLT9FGTpsxXc9Yo0n4LbLgy0shp0q8TOhzwRnz31izqeOasT

      KH4CCWXDOGQprcdELdS+Mr3NHGEni8ya+Cs9ZCCQJB+fzSk6Y7j4ObBvIIwpVV9s

      Na+YmpDnP9BM6qgniW/pn0i871Z+sHUJHZ386RO8cttPqKJLHdpixZy+RwIDAQAB

      AoGBAJk/HGUH5PxL6ELpuxmtIGV6fzOwh4prWcBr6uoJ4oyHIAsHeyD8lRelj7IT

      2ABdNvsbiHBh/NDRkR1ik3I/6FIV3kuZd6DNIiecfY8y7BfMtInw3Whm9gRAkron

      VGbRiSA33Oe0KTTt6wz2PY+ZVVH492gf33K6PZqXfR4+iG7RAkEA+R0DRnm5crWX

      LQ1ygMhwRn1p2b4LmYYmMosnUkWOOueC5I+dTPTFnvGKtb9We3csRIy1RHXUJJu2

      yvT6O/F5zwJBAPPoa3phaF3JE0Vy5DZS/r5+DKom14F5MeYsokPbqr2SG+xZOCm9

      cFjMOAneF/zHcW8qVNwb1wQIY6oIuRgEqgkCQQCccTjuWGE7BYkz9N70u2uvCPGh

      mbTlLBbu5O7DvwSsP1m3Oe2aN5mn0J7AtrGUBepZ/leT779TYiqwWJqRbHuHAkEA

      7VyIC8bzrCFcUb+ne351TqiYZpX6L5PkDZ3uI5+In4erCO0ijOxAgwnqlx+9tE/b

      glVt0+575v7LDtQCXO9dEQJAPjhGY/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 server.crt file>');`

      The following is an example of the command with sample content of `server.crt` file:

```
SELECT SET_CONFIG_PARAMETER('SSLCertificate','-----BEGIN CERTIFICATE-----
MIICmjCCAgOgAwIBAgIJAMnZqpMfBVTjMA0GCSqGSIb3DQEBBQUAMGYxCzAJBgNV
BAYTAklOMQswCQYDVQQIDAJLQTEMMAoGA1UEBwwDQkxSMQwwCgYDVQQKDANIUEUx
DDAKBgNVBAsMA0hQRTEMMAoGA1UEAwwDT0JSMRIwEAYJKoZIhvcNAQkBFgNjb20w
HhcNMTYwMzI5MDkyMDU1WhcNMjYwMzI3MDkyMDU1WjBmMQswCQYDVQQGEwJJTjEL
MAkGA1UECAwCS0ExDDAKBgNVBAcMA0JMUjEMMAoGA1UECgwDSFBFMQwwCgYDVQQL
DANIUEUxDDAKBgNVBAMMA09CUjESMBAGCSqGSIb3DQEJARYDY29tMIGfMA0GCSqG
SIb3DQEBAQUAA4GNADCBiQKBgQDtWLT9FGTpsxXc9Yo0n4LbLgy0shp0q8TOhzwR
nz31izqeOasTKH4CCWXDOGQprcdELdS+Mr3NHGEni8ya+Cs9ZCCQJB+fzSk6Y7j4
ObBvIIwpVV9sNa+YmpDnP9BM6qgniW/pn0i871Z+sHUJHZ386RO8cttPqKJLHdpi
xZy+RwIDAQABo1AwTjAdBgNVHQ4EFgQUNAaMPP9V4sEpHWwONurFxlaDr1QwHwYD
VR0jBBgwFoAUNAaMPP9V4sEpHWwONurFxlaDr1QwDAYDVR0TBAUwAwEB/zANBgkq
hkiG9w0BAQUFAAOBgQCe0d8O77n7eTftVw+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:

   `vsql -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 privilages

   `<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)”`

To disable TLS for Vertica, run the `SELECT SET_CONFIG_PARAMETER('EnableSSL', '0');` command and restart the Vertica database.

On OBR:

Perform the following steps on the system where HPE 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

   <*Password*> is the password

2. `keytool -import -file server.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

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' >> /opt/HP/BSM/PMDB/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>`

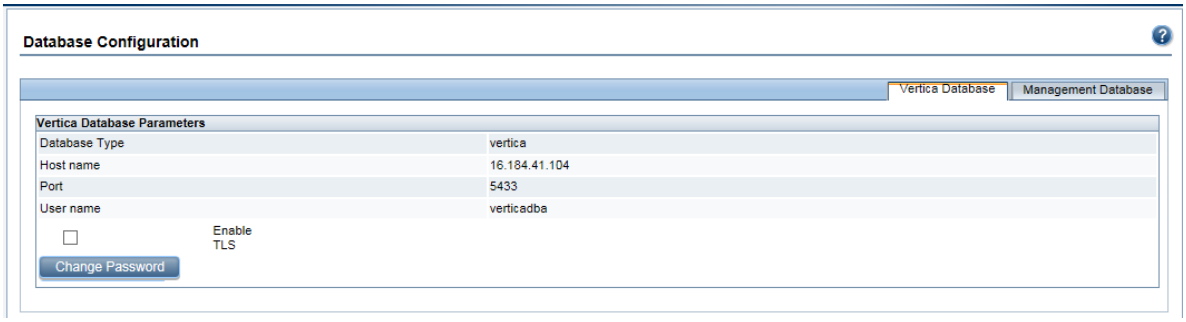
   where, <*Vertica DBA User*> is the Vertica user with DBA privileges

   <*Vertica DBA Password*> is the password for Vertica user

   A connection status message is displayed.

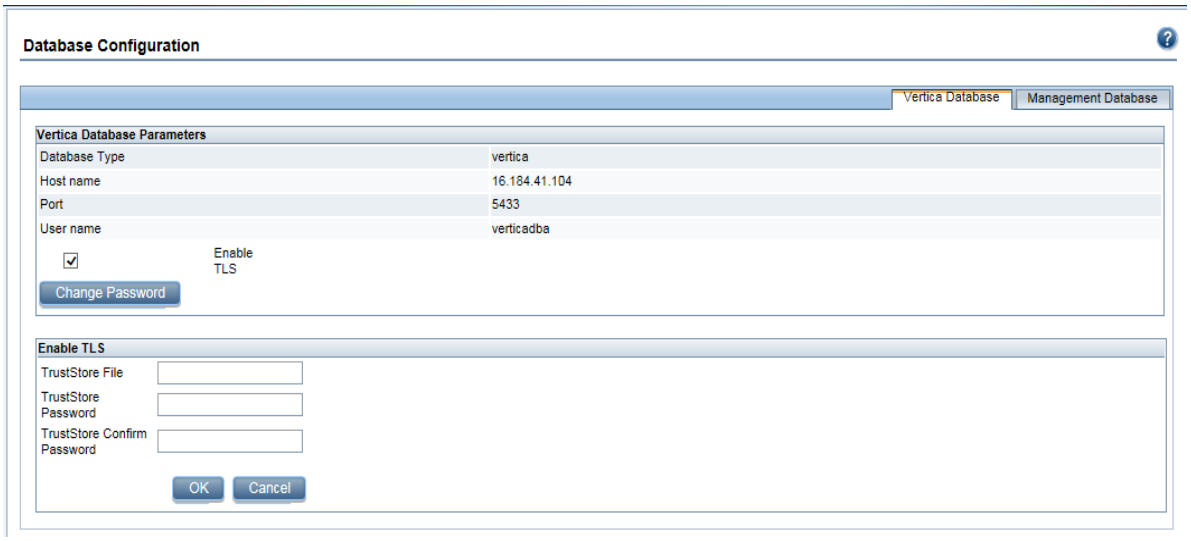
Enable TLS for Vertica in Administration Console

1. In the Administration Console, select **Administration > Database Configuration**.
2. In the **Vertica Database** tab, select the **Enable TLS** check box.



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, 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
```

4. Log on to `vsql`.

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-----
MIICXgIBAAKBgQDtWLT9FGTpsxXc9Yo0n4LbLgy0shp0q8TOhzwRnz31izqeOasT
KH4CCWXDOGQprcdELdS+Mr3NHGEni8ya+Cs9ZCCQJB+fzSk6Y7j4ObBvIIwpVV9s
Na+YmpDnP9BM6qgniW/pn0i871Z+sHUJHZ386RO8cttPqKJLHdpixZy+RwIDAQAB
AoGBAJk/HGUH5PxL6ELpuxmtIGV6fzOwh4prWcBr6uoJ4oyHIAsHeyD8lRelj7IT
2ABdNvsbiHBh/NDRkR1ik3I/6FIV3kuZd6DNIiecfY8y7BfMtInw3Whm9gRAkron
VGbRiSA33Oe0KTTt6wz2PY+ZVVH492gf33K6PZqXfR4+iG7RAkEA+R0DRnm5crWX
LQ1ygMhwRn1p2b4LmYYmMosnUkWOOueC5I+dTPTFnvGKtb9We3csRIy1RHXUJJu2
yvT6O/F5zwJBAPPoa3phaF3JE0Vy5DZS/r5+DKom14F5MeYsokPbqr2SG+xZOCm9
cFjMOAneF/zHcW8qVNwb1wQIY6oIuRgEqgkCQQCccTjuWGE7BYkz9N70u2uvCPGh
mbTlLBbu5O7DvwSsP1m3Oe2aN5mn0J7AtrGUBepZ/leT779TYiqwWJqRbHuHAkEA
7VyIC8bzrCFcUb+ne351TqiYZpX6L5PkDZ3uI5+In4erCO0ijOxAgwnqlx+9tE/b
glVt0+575v7LDtQCXO9dEQJAPjhGY/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 server.crt file>');`

   The following is an example of the command with sample content of `server.crt` file:

```
SELECT SET_CONFIG_PARAMETER('SSLCertificate','-----BEGIN CERTIFICATE-----
MIICmjCCAgOgAwIBAgIJAMnZqpMfBVTjMA0GCSqGSIb3DQEBBQUAMGYxCzAJBgNV
BAYTAklOMQswCQYDVQQIDAJLQTEMMAoGA1UEBwwDQkxSMQwwCgYDVQQKDANIUEUx
DDAKBgNVBAsMA0hQRTEMMAoGA1UEAwwDT0JSMRIwEAYJKoZIhvcNAQkBFgNjb20w
HhcNMTYwMzI5MDkyMDU1WhcNMjYwMzI3MDkyMDU1WjBmMQswCQYDVQQGEwJJTjEL
MAkGA1UECAwCS0ExDDAKBgNVBAcMA0JMUjEMMAoGA1UECgwDSFBFMQwwCgYDVQQL
```

```
DANIUEUxDDAKBgNVBAMMA09CUjESMBAGCSqGSIb3DQEJARYDY29tMIGfMA0GCSqG
SIb3DQEBAQUAA4GNADCBiQKBgQDtWLT9FGTpsxXc9Yo0n4LbLgy0shp0q8TOhzwR
nz31izqeOasTKH4CCWXDOGQprcdELdS+Mr3NHGEni8ya+Cs9ZCCQJB+fzSk6Y7j4
ObBvIIwpVV9sNa+YmpDnP9BM6qgniW/pn0i871Z+sHUJHZ386RO8cttPqKJLHdpi
xZy+RwIDAQABo1AwTjAdBgNVHQ4EFgQUNAaMPP9V4sEpHWwONurFxlaDr1QwHwYD
VR0jBBgwFoAUNAaMPP9V4sEpHWwONurFxlaDr1QwDAYDVR0TBAUwAwEB/zANBgkq
hkiG9w0BAQUFAAOBgQCe0d8O77n7eTftVw+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:

   `vsql -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 privilages

   `<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)”`

To disable TLS for Vertica, run the `SELECT SET_CONFIG_PARAMETER('EnableSSL', '0');` command and restart the Vertica database.

On OBR:

Perform the following steps on the system where HPE 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

   <*Password*> is the password
3. `keytool -import -file server.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

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' >> /opt/HP/BSM/PMDB/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

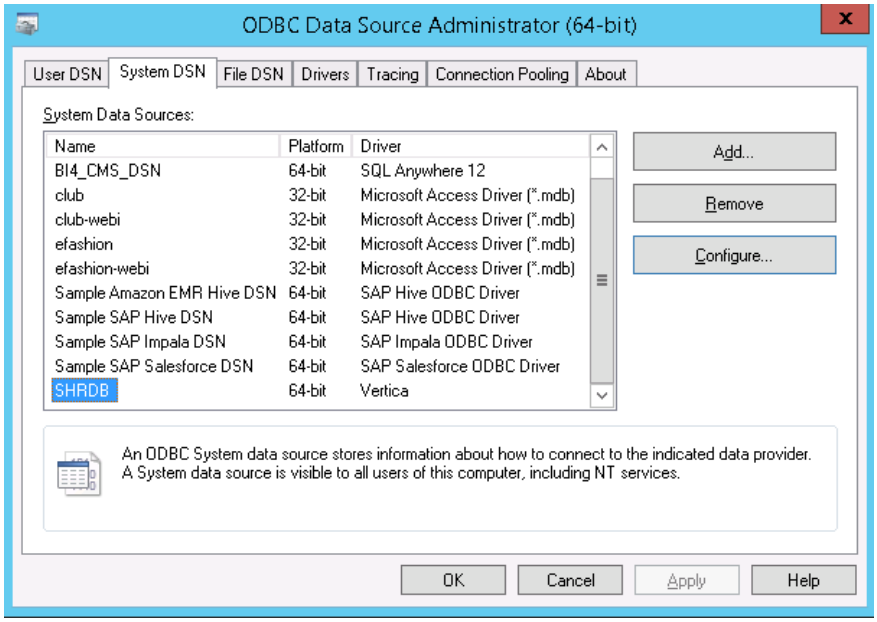
3. `keytool -import -file server.crt -alias importcert -keystore <File name> -storepass <Password>`

   where, <*File name*> is the trust store file name with path. For example, `Verticatrustore.p12`

   <*Password*> is the password

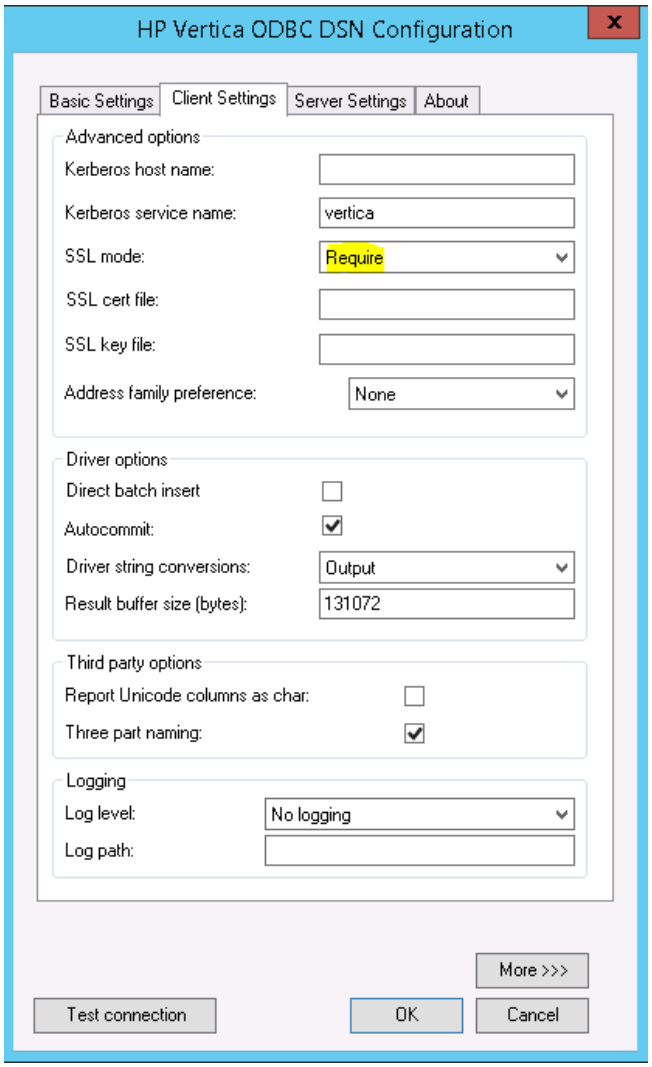
Configure SSL for ODBC clients

1. Log on to HPE 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 HP 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**.

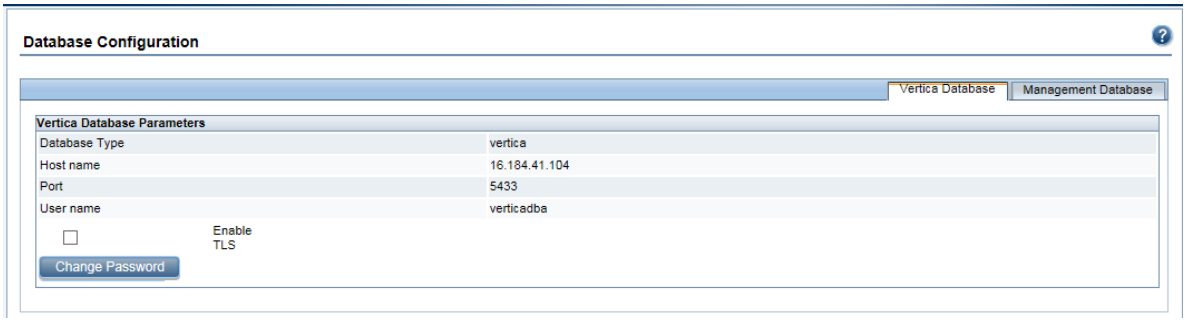
   A connection succeeded message is displayed.

8. Click **OK**.

   The SSL for DSN is enabled.

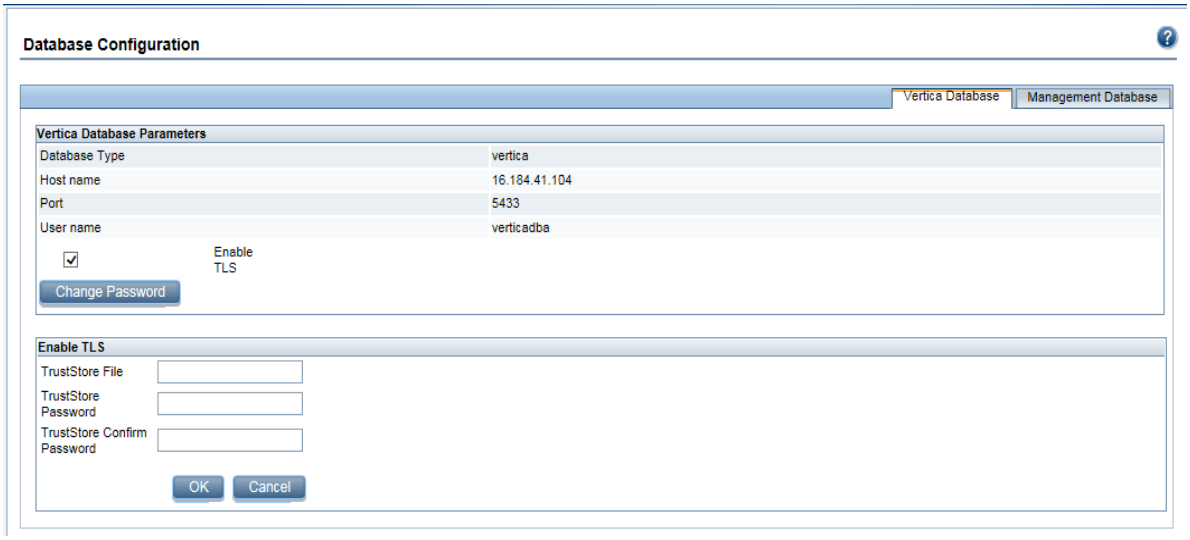
Enable TLS for Vertica in Administration Console

1. In the Administration Console, select **Administration > Database Configuration**.
2. In the **Vertica Database** tab, select the **Enable TLS** check box.



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 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 HPE 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 188.
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 HPE OBR databases.It also provides information on how you can plan for back up using the database backup options in HPE 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 HPE OBR databases, and creating a backup of key configuration and license files. HPE OBR enables you to back up and recover the SAP BusinessObjects database, and the SAP BusinessObjects file store to prevent data loss in the event of a disaster.

HPE OBR provides a full back up script. A full backup script enables you to take a complete back up of the following HPE OBR component (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

> **Tip:** It is recommended to take full backup every day as taking full backup is faster and consumes less disk space.

Important Considerations

- An important consideration before you plan for backup and recovery is to change the default password for HPE OBR Administrator user and SAP BusinessObjects Central Management Console (CMC) database (SQL Anywhere).

  For information on changing default passwords, refer to *Changing Default Passwords* section in the *HPE Operations Bridge Reporter Administration Guide*.

- You must schedule the full backup to run at regular intervals.
- 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 instance, if the backup script is run on a Monday the backup file will be saved with the name `/<backup path>/_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 database 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, HPE 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
HPE OBR server1	Initial HPE OBR system where the existing data back up is taken.
HPE OBR server2	New HPE OBR installed system where the data is restored.
SHR_DR_Backup	Name of the backup file.

Backup of HPE OBR Components

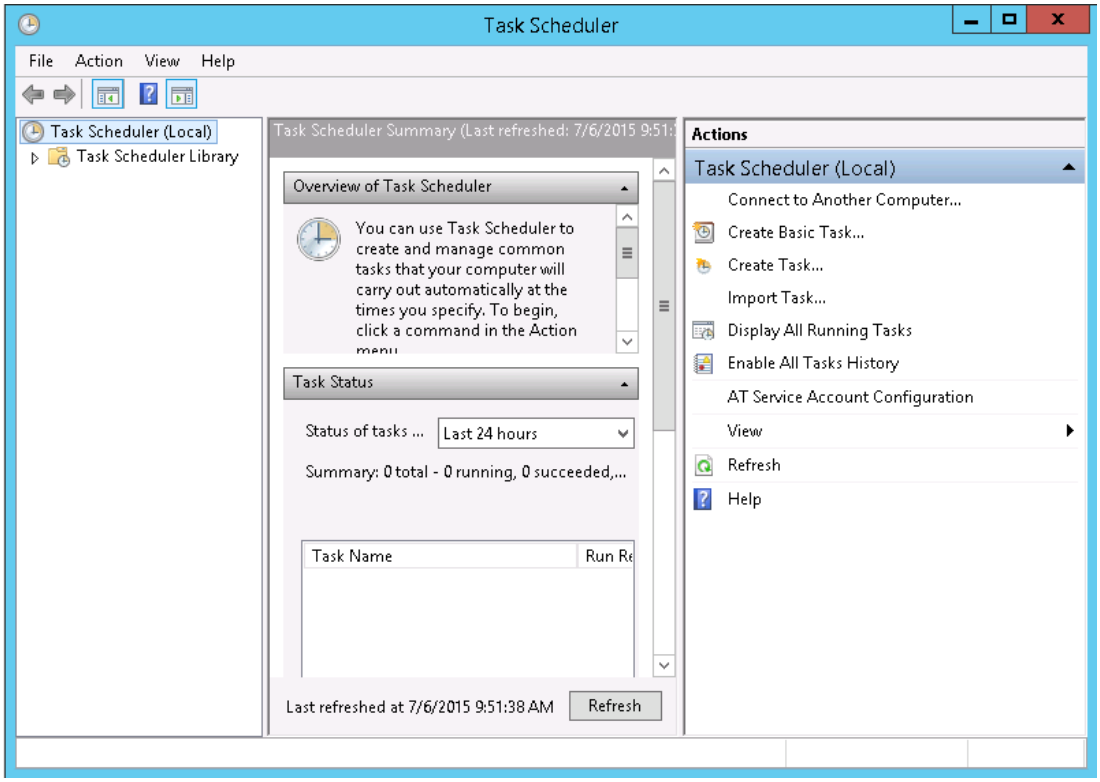
It is recommended that you take regular back up of the HPE OBR components.

Create Full Backup of HPE OBR on Windows

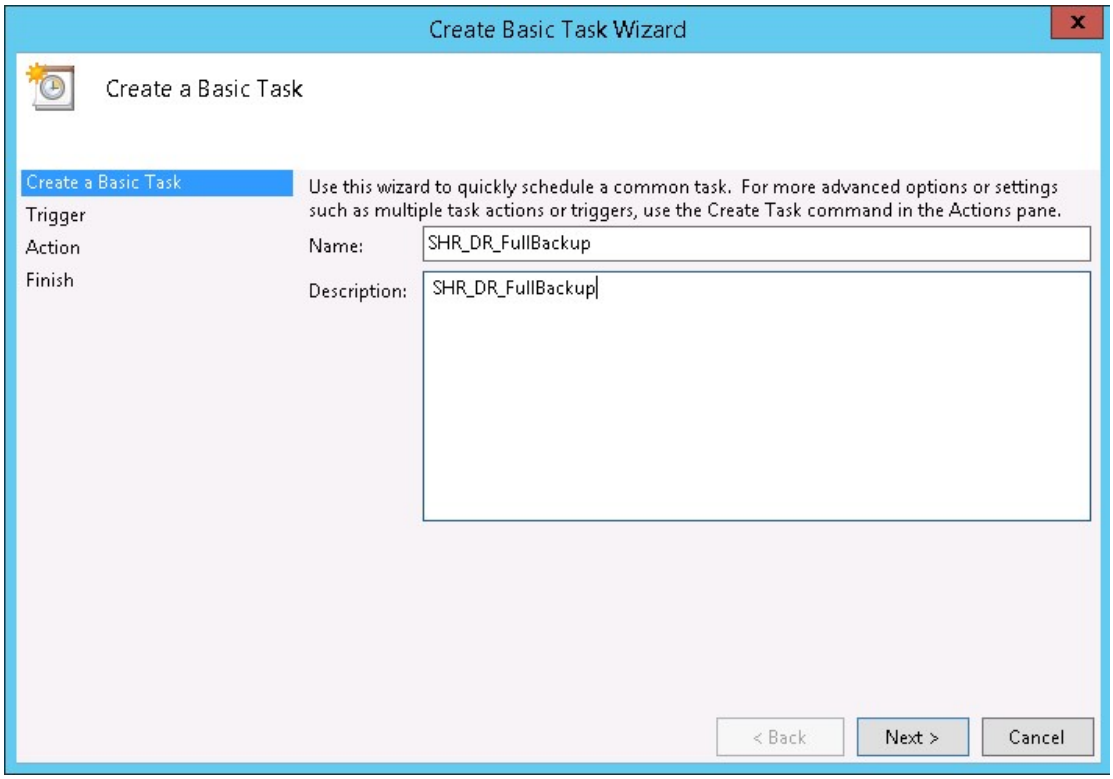
The `%PMDB_HOME%\DR\SHR_full_Backup.pl` script helps you to take full backup of the HPE OBR components. The script generates `DR.log` file in `%PMDB_HOME%\log`.

To schedule the backup of HPE OBR components, follow these steps:

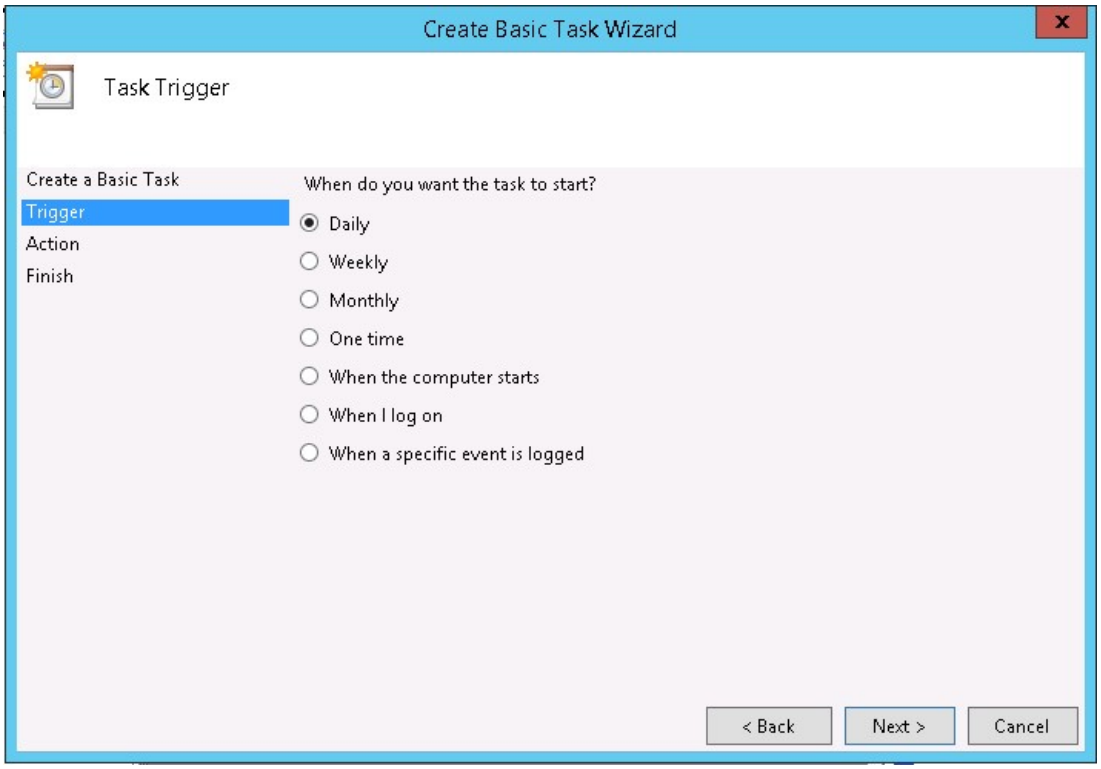
1. Go to **Start > Program > Administrative Tools > Task Scheduler** or go to **Start** and type **Task Scheduler** in **Search** and double-click on the **Task Scheduler**. The **Task Scheduler** window is displayed.



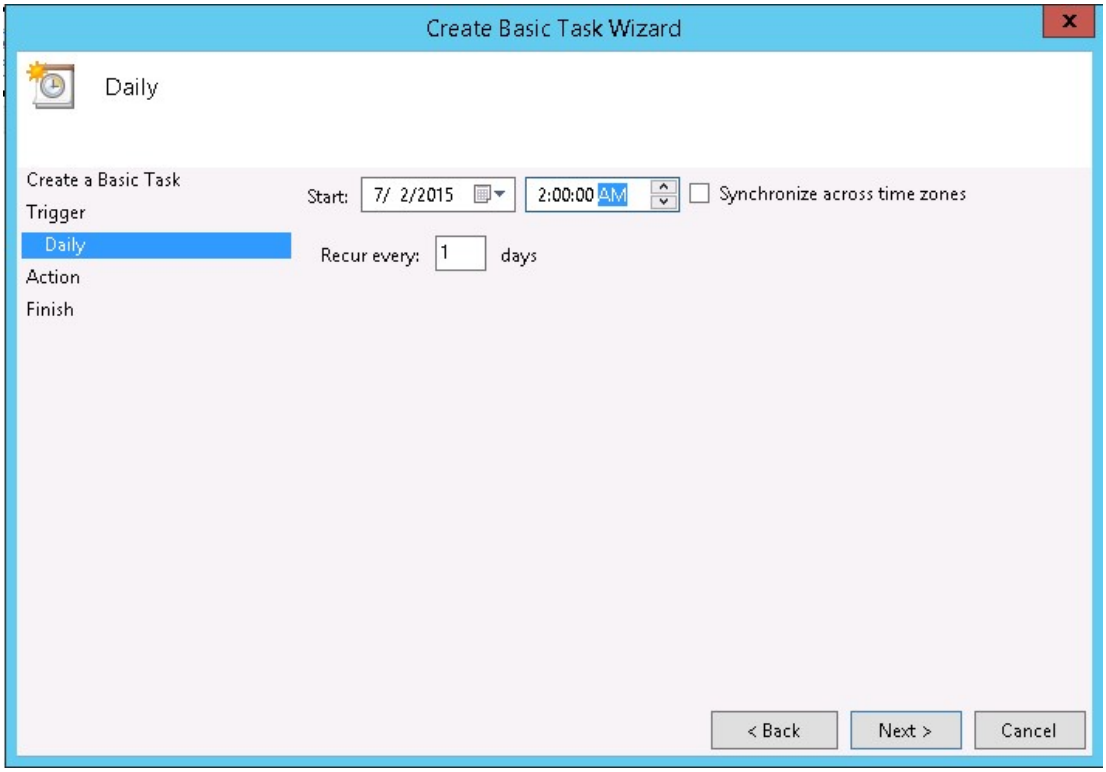
2. In the **Task Scheduler** window, click **Create Basic Task**. The **Create Basic Task wizard** is displayed.
3. Enter **SHR_DR_FullBackup** in **Name** and **Description**, and then click **Next**.



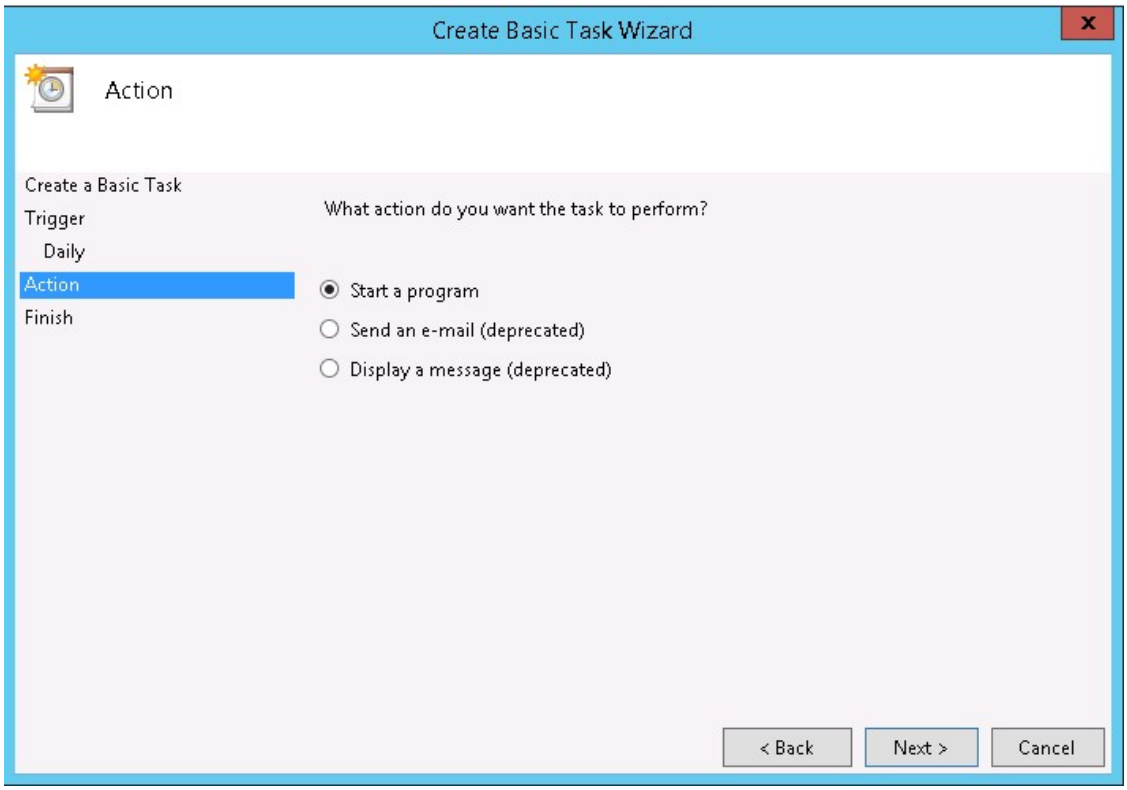
4. In **Trigger**, select **Daily** and click **Next**.



5. In **Daily**, select the start time and enter 1 in the **Recur every** text box, and then click **Next**.



6. In **Action**, select **Start a program** and click **Next**.

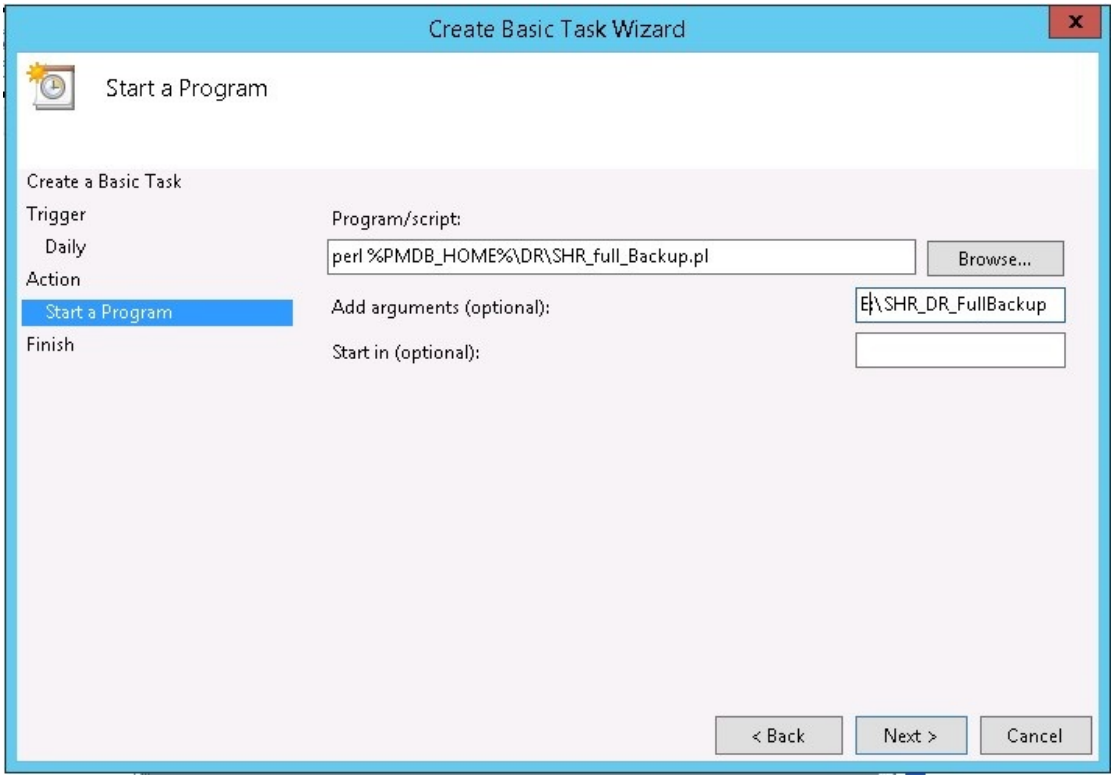


7. Enter `perl` in **Program/Script**, click **Browse** and go to `%PMDB_HOME%\DR`.
8. Select **SHR_full_Backup.pl** and then click **Next**.

   You can enter the location of custom folder where you want to store the backup files and data in the **Add arguments (optional)**

   For example: `E:\SHR_Full_Backup`

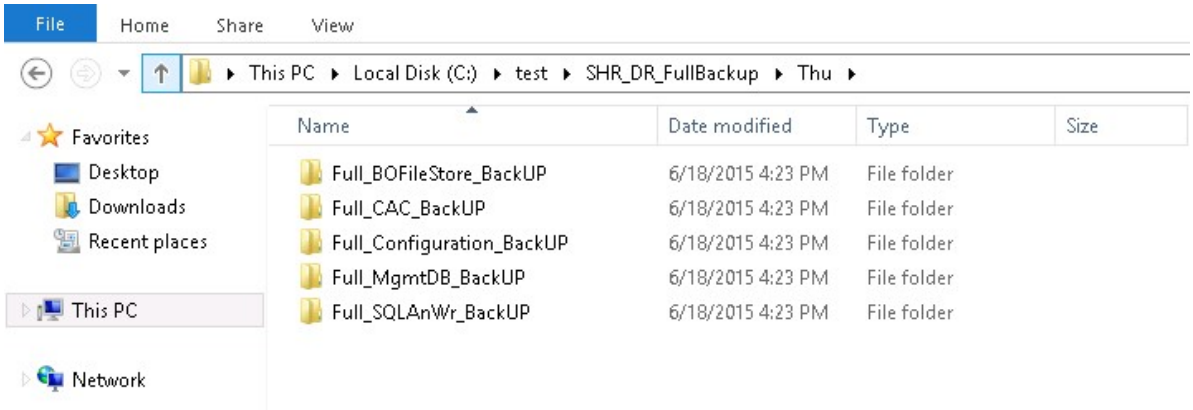
   > **Note:** Ensure that the custom folder is already created before you enter in the **Add arguments (optional)** text box.



9. Click **Yes** in the **Task Scheduler message** and click **Finish** in the **Summary** page.

You can check the task created in the **Active Tasks** of the **Task Scheduler** window.

The following image shows sample backup files created in **SHR_DR_FullBackup**:



Create Full Backup of HPE OBR on Linux

The `$PMDB_HOME/DR/SHR_full_Backup.pl` script helps you to take full backup of the HPE OBR components. The script generates `DR.log` file in `$PMDB_HOME/log`.

To schedule the backup, log on to OBR server1 where you have installed OBR components and follow these steps:

1. Log on to the OBR system as `root`.
2. Run the following command at the command prompt and edit the `crontab` file:

   ```
   crontab -e
   ```

3. Add a line in the following format to the `crontab` file to invoke the `/opt/HP/BSM/PMDB/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

   <location of the backup script> is the location of the full backup script (`SHR_full_Backup.pl`)

   <backup_path> is the location where you want to store the backup files and data

   For example:

   ```
   0 15 * * 0/opt/OV/nonOV/perl/a/bin/perl /opt/HP/BSM/PMDB/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 backup files are stored in `/root/SHR_DR_FullBackup`.

4. Save the `crontab` file.

   All the log files for `crontab` are in the location `/var/mail`.

5. After the scheduled backup is complete, 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
```

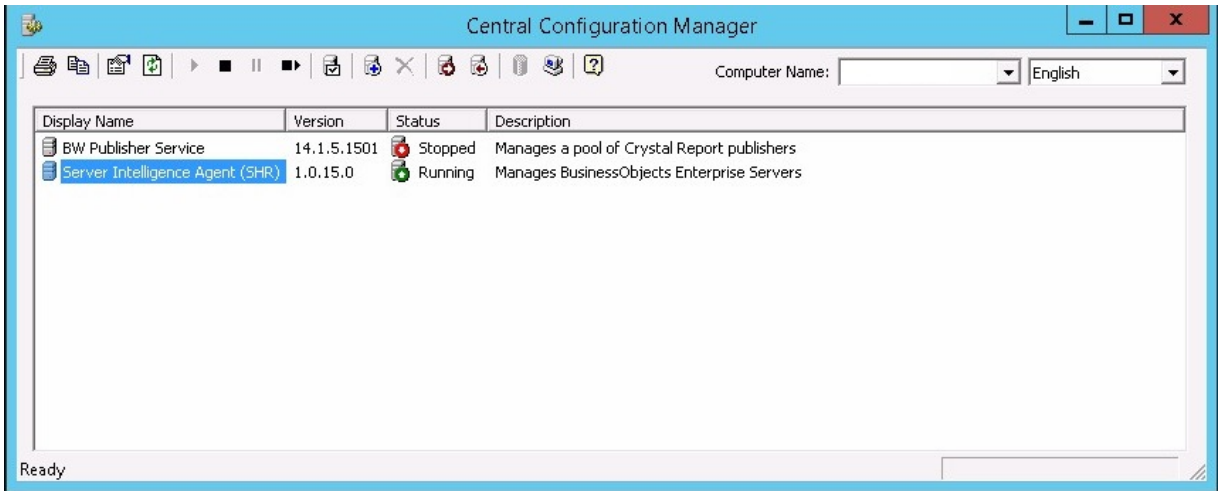
Restore HPE OBR Components

Restore Backup of HPE OBR on Windows

For SAP BusinessObjects Database and File Store

To restore the backup of HPE OBR components, follow these steps:

1. Log on to OBR server2 system where you have installed OBR components.
2. 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.
3. Log on to SAP BusinessObjects Central Configuration Manager. Click **Start > Central Configuration Manager**. The **Central Configuration Manager** window is displayed.



4. Right-click on **Server Intelligence Agent (OBR)** and click **Stop**.
5. Click **Start > Run**. The **Run** dialog box appears.

6. Type `services.msc` in the **Open** field and press **Enter**. The **Services** window appears.
7. From the **Services** window, click the **SQL Anywhere for SAP Business Intelligence** service and click **Stop**.
8. Rename the existing file store folder.

   The default location of the file store is `<BusinessObjects installed drive>:\Program Files (x86)\BusinessObjects\BusinessObjects Enterprise 12.0\FileStore`. You can rename it as `FileStore_old`.
9. Move the existing SQL Anywhere database from its default location to another location.

   The default location of the SQL Anywhere database is `<BusinessObjects installed drive>:\Program Files (x86)\SAP BusinessObjects\sqlanywhere\database`.
10. To run the restore script, follow these steps:
    a. Click **Start > Run**. The Run dialog box is displayed.
    b. Type `cmd` and press **Enter**. The command prompt is displayed.
    c. Run the following command:

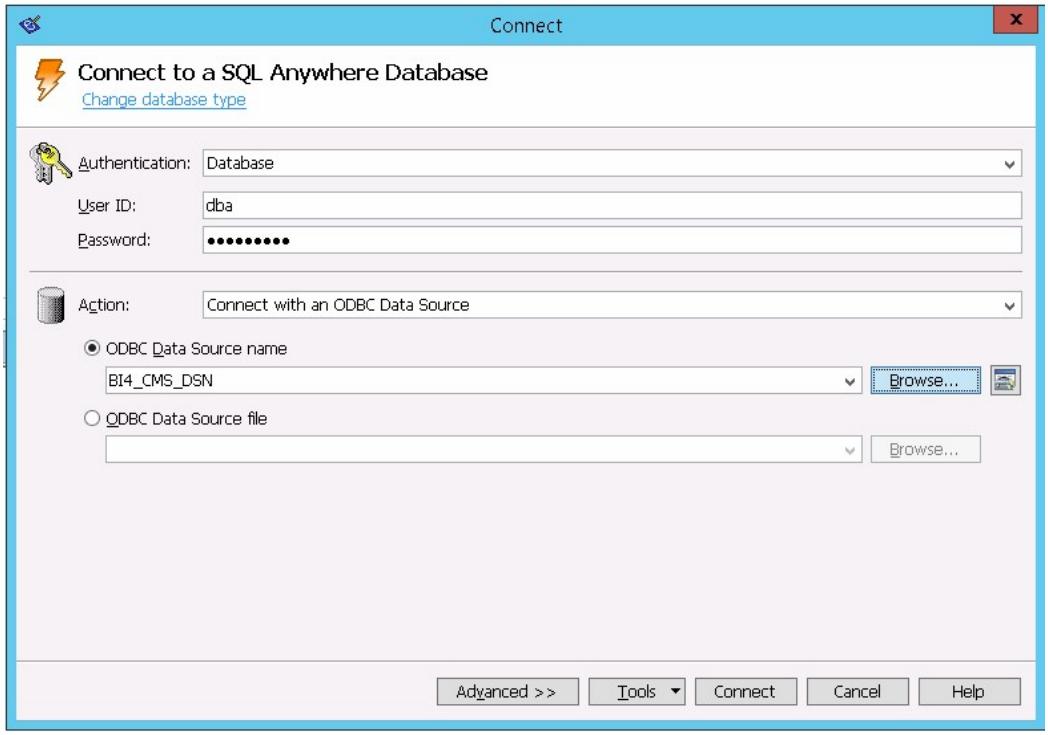
       `perl <location of the restore script> <location of the backup file>`

       where, *<location of the restore script>* is the location where the restore script is stored

       <location of the backup file> is the location of backup file of particular day that you want to restore

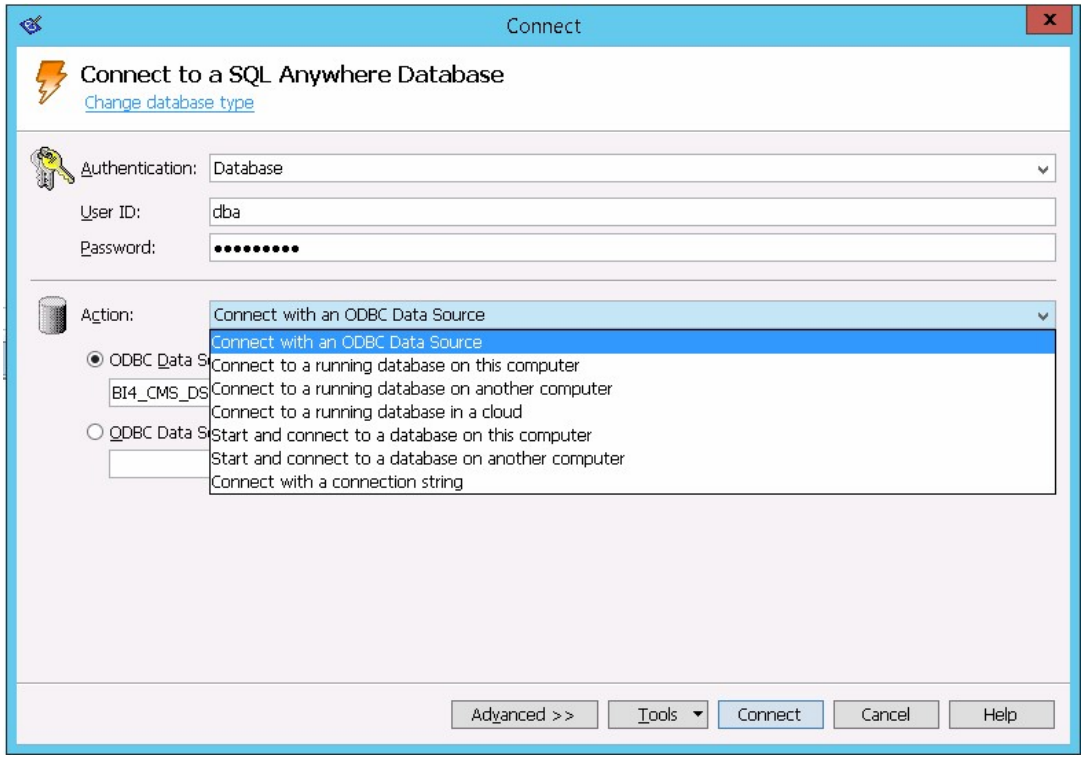
       For example:

       `perl %PMDB_HOME%\DR\SHR_full_Restore.pl E:\SHR_Backup\SHR_DR_FullBackup\Thu`
11. To Connect to SQL Anywhere, follow these steps:
    a. Open the Command prompt and type `dbisqlc` and press **Enter**. The **Connect to SQL Anywhere** window is displayed.

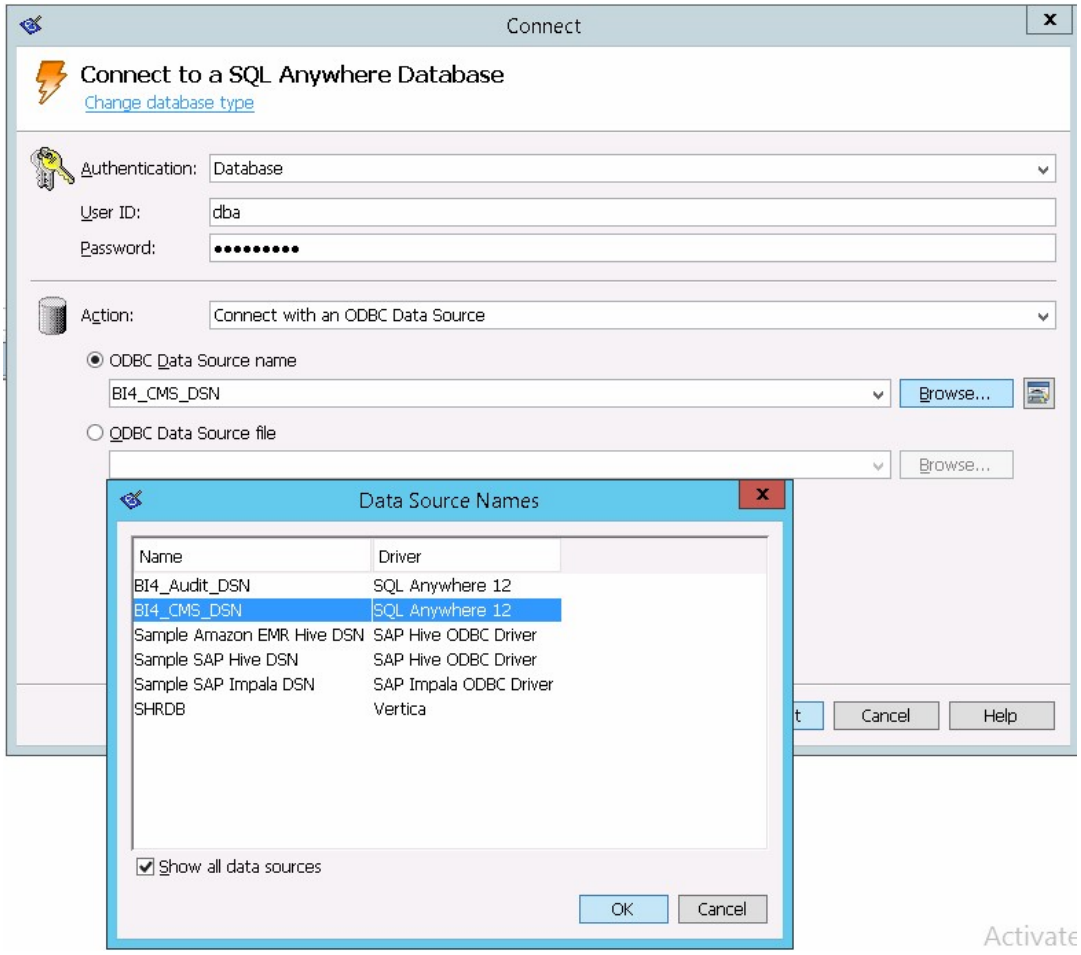


b. Enter **dba** in **User ID** field and password in **Password** field.

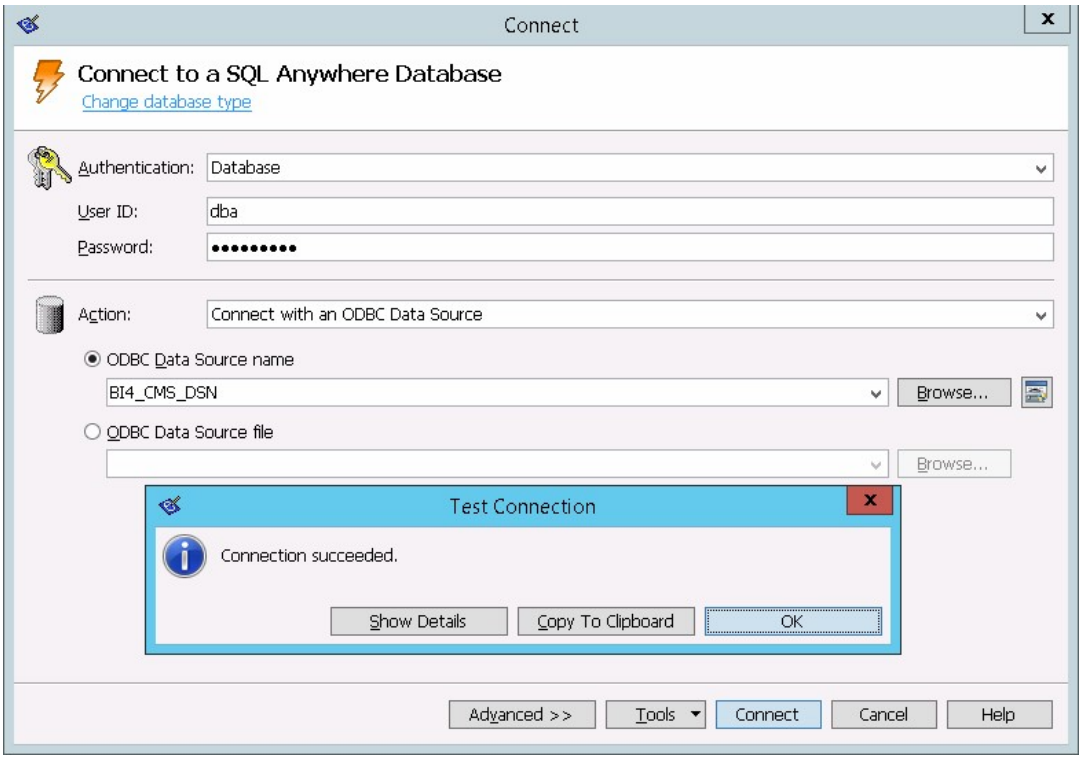
c. In **Action**, select the **Connect with an ODBC Data Source** from the drop down.



d. Select the **ODBC Data Source name** option and click **Browse**, and then select the source name **BI4_CMS_DSN**.

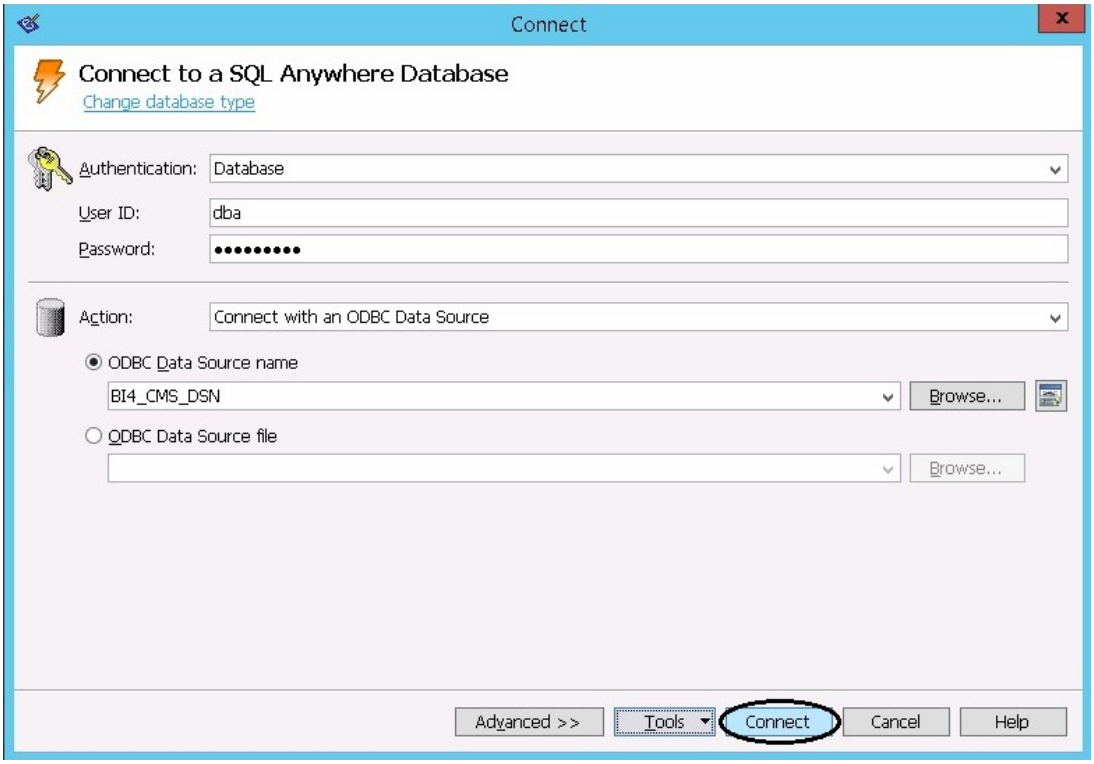


e. Check the connection as shown in the following image:



The connection succeeded confirmation dialog box is displayed. Click **OK**.

f. Click **Connect**.

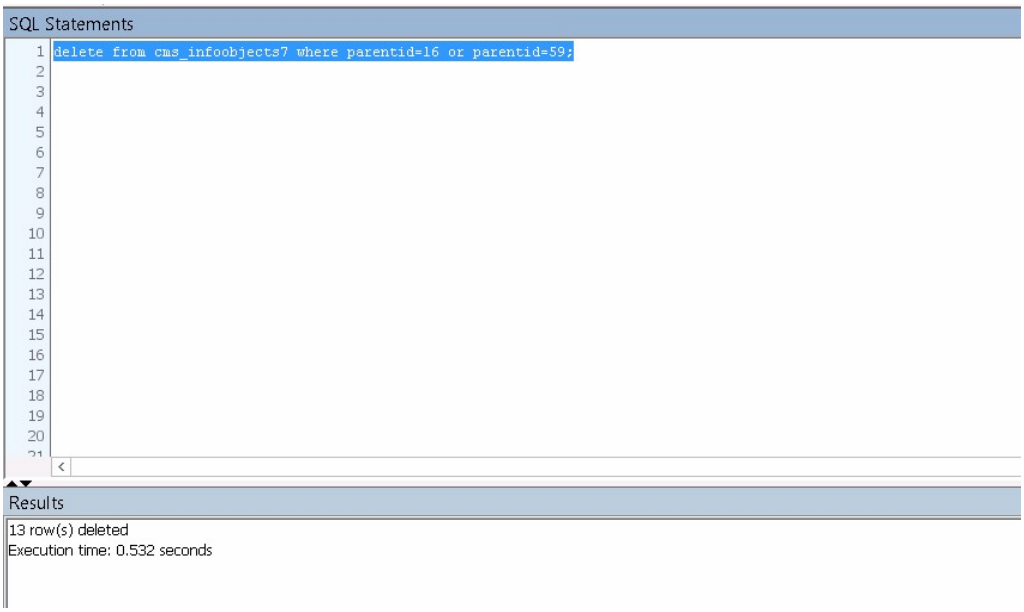


The SQL Statements pane is displayed.

g. In the SQL Statements pane, type the following query:

```
delete from cms_infoobjects7 where parentid=16 or parentid=59;
```

h. Click **Execute**. A message is displays with the number of records deleted as shown in the following image:



i. Commit the query execution and close the **Connect to SQL Anywhere** window.

12. Open **Start > Run** and type `services.msc`, and then press **Enter**. The **Services** windows is displayed.
13. From the **Services** window, click the **SQL Anywhere for SAP Business Intelligence** service and click **Start**.

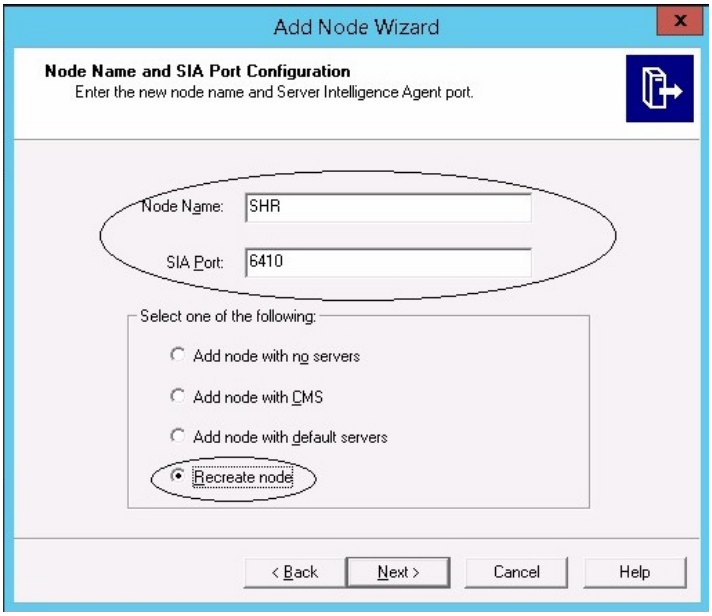
14. To create a new Server Intelligence Agent (SIA), follow these steps:

> **Note:** Before you proceed to the next step, ensure that the SIA is stopped.

a. Log on to SAP BusinessObjects Central Configuration Manager. The **Central Configuration Manager** window is displayed.

b. Click on to create a new SIA node. The **Add Node Wizard** is displayed.

c. Click **Next**. The Node name and SIA Port Configuration page appears.



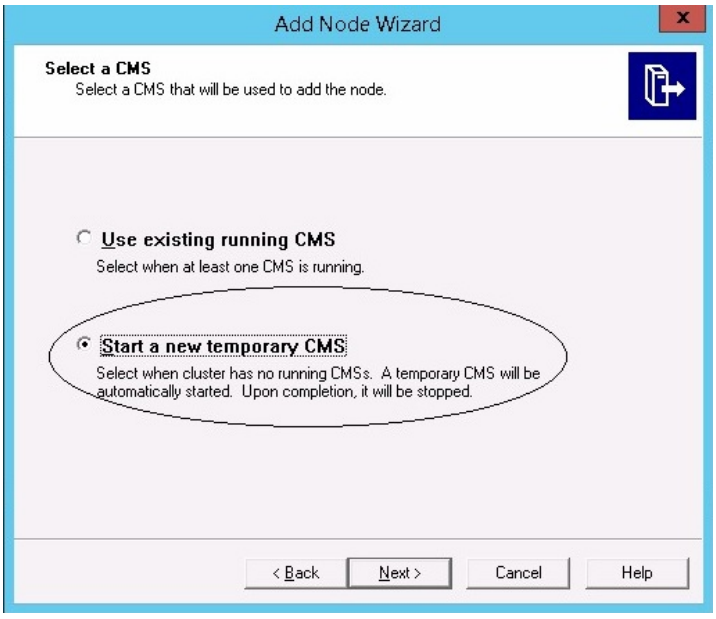
d. Enter **SHR** in the **Node Name** and **6410** in the **SIA Port**.

e. Select the **Recreate Node** and click **Next**.

   A warning message is displayed.

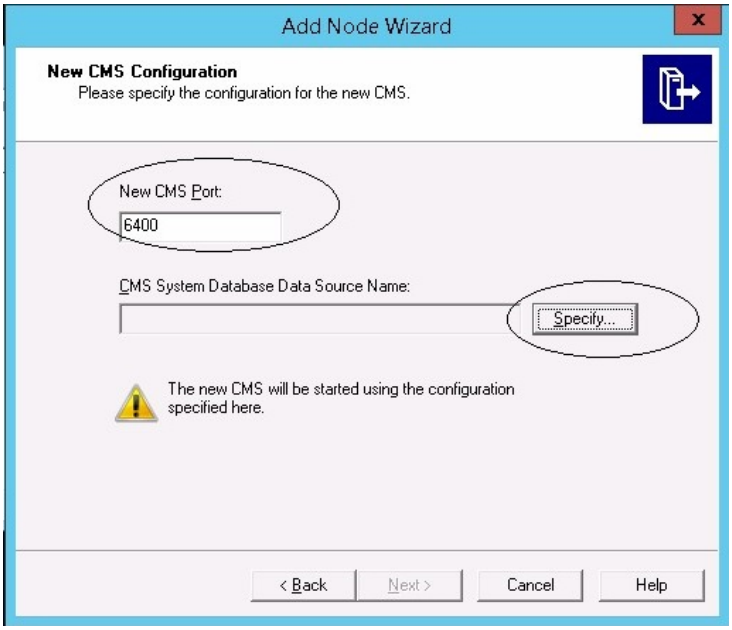
f. Click **Next**. The **Select a CMS** pane is displayed.

g. Select **Start a new temporary CMS** and click **Next**.



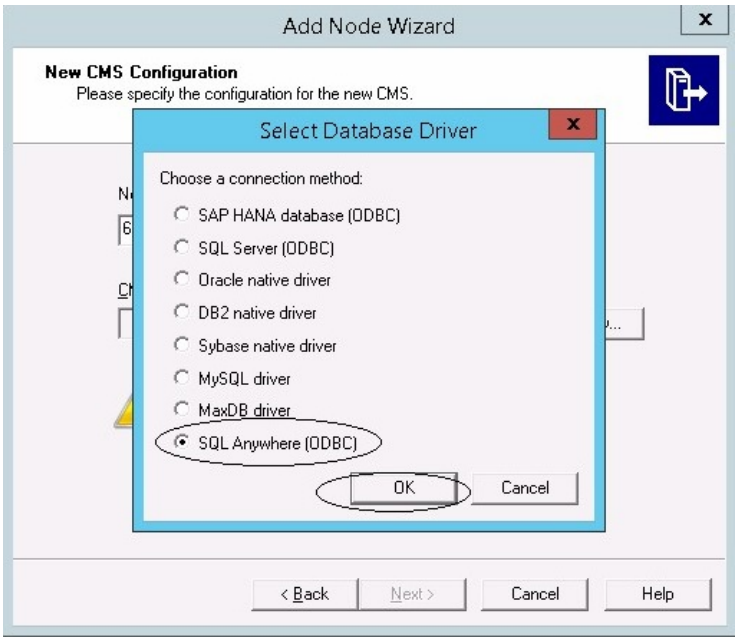
   The New CMS Configuration pane is displayed.

h. Enter **6400** in **New CMS Port** and click **Specify**.



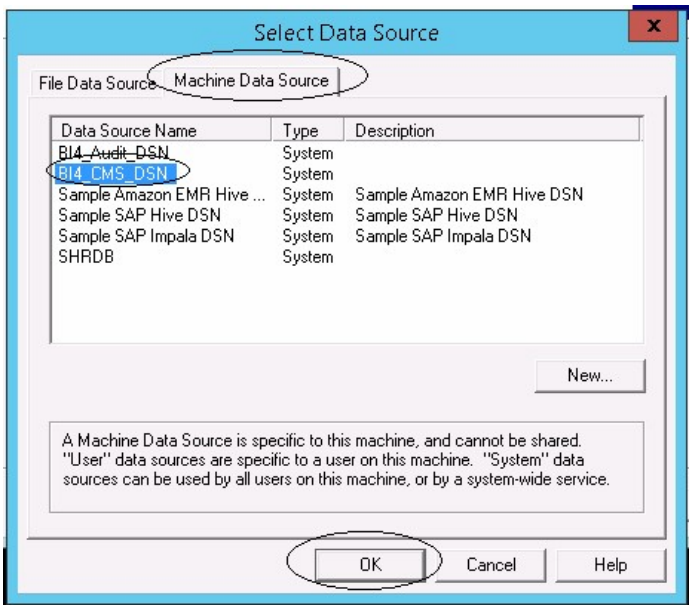
The **Select Database Driver** window is displayed.

i. Select **SQL Anywhere (ODBC)** and click **OK**.



The **Select Data Source** window is displayed.

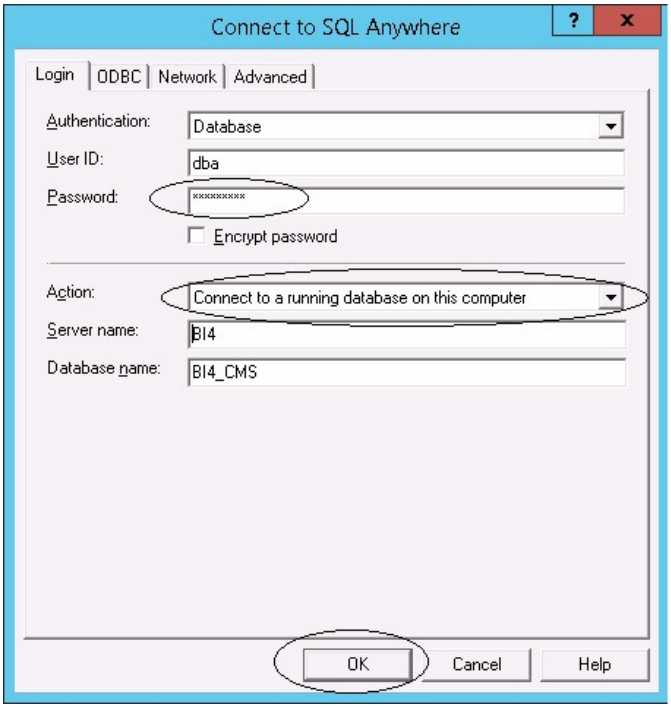
j. Click the **Machine Data Source** tab and select **BI4_CMS_DSN**, and then click **OK**.



k. Open the command prompt and type `dbisqlc`, and then press **Enter**. The **Connect to SQL Anywhere** window is displayed.

l. Enter **dba** in the **User ID** field and password in the **Password** field.

m. In **Action**, select the **Connect to a running database on this computer** and click **OK**.



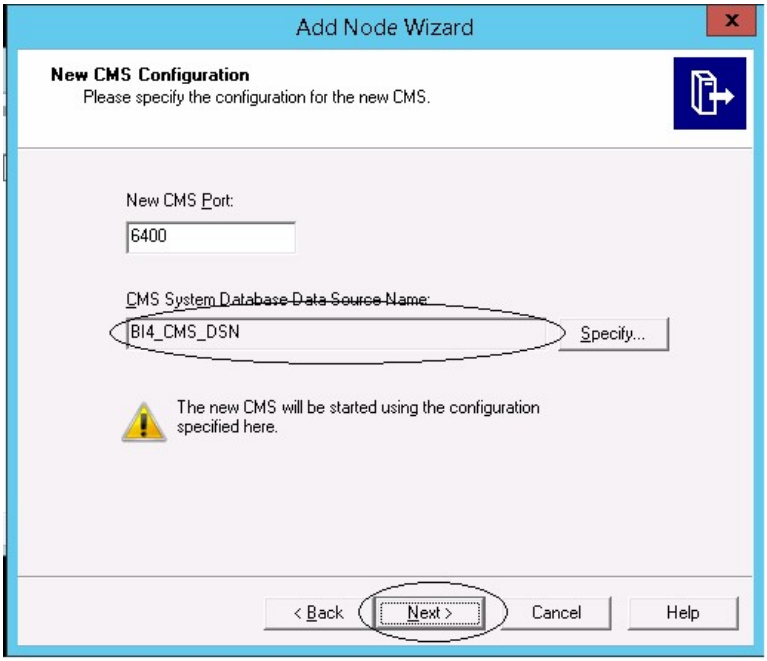
The **Specify Cluster Key** window is displayed.

n. Enter **1ShrAdmin** in **Enter the cluster key** and click **OK**.

> **Note:** The default cluster key is **1ShrAdmin**. If you have changed the cluster key then enter the changed cluster key value.

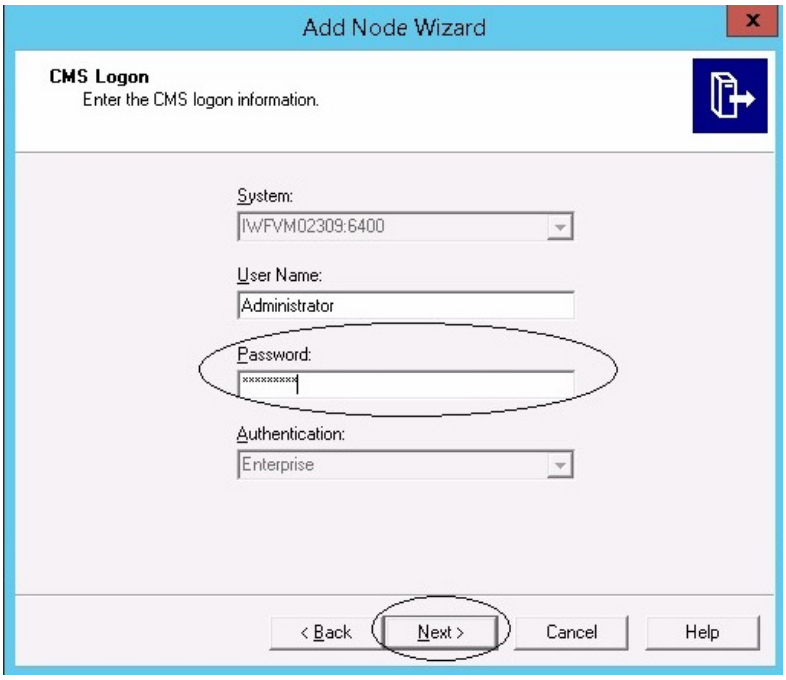
The **New CMS Configuration** pane is displayed.

o. The **CMS System Database Data Source Name** is enabled. Click **Next**.



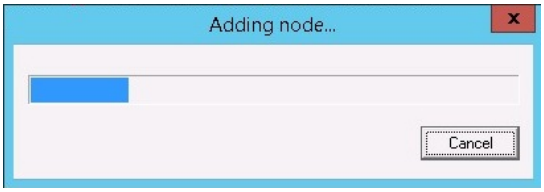
The **CMS Logon** pane is displayed.

p. Enter password in the **Password** field and click **Next**.



The Confirmation window is displayed.

q. Click **Finish**. The newly created node is added. Wait till the process is completed.



A confirmation dialog box is displayed. Click **OK**.

r. In the **Central Configuration Manager** window, right-click on **Server Intelligence Agent** (SIA) and select **Properties**.

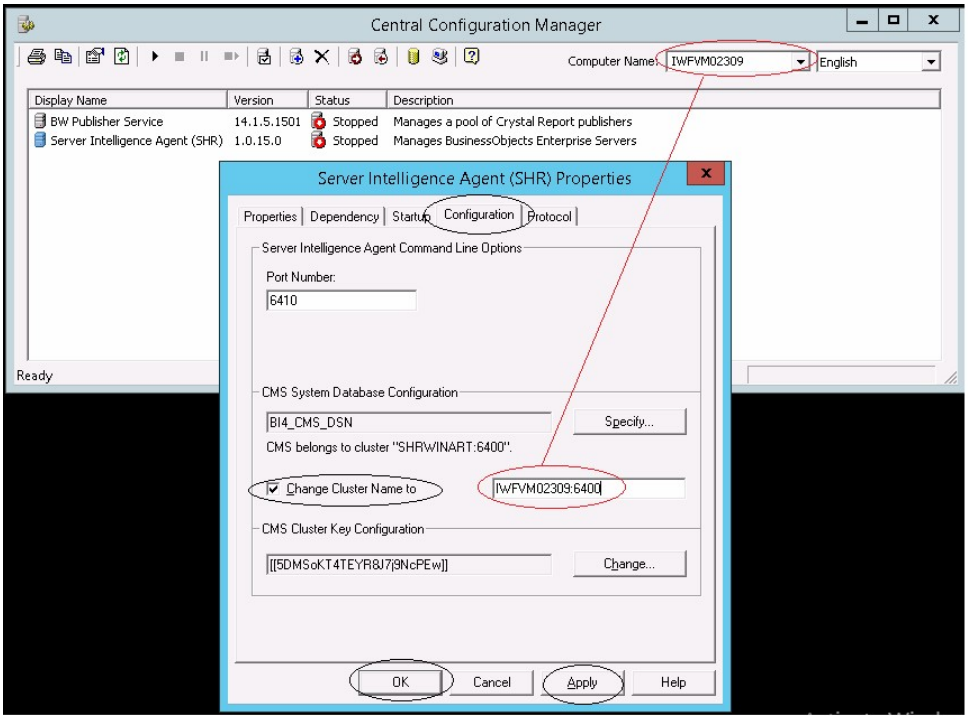
The **Server Intelligence Agent (OBR) Properties** window is displayed.

s. Click **Configuration** tab and select the **Change Cluster Name to** check box.

t. Enter the cluster name in the following format: *<Cluster Name>*:6400

where, *<Cluster Name>* is same as the **Computer Name** in the Central Configuration Manager window.

The following image shows an example of the Cluster Name:



u. Click **Apply** and then click **OK**.

v. In the **Central Configuration Manager** window, right-click on **Server Intelligence Agent** (SIA) and click **Start**.

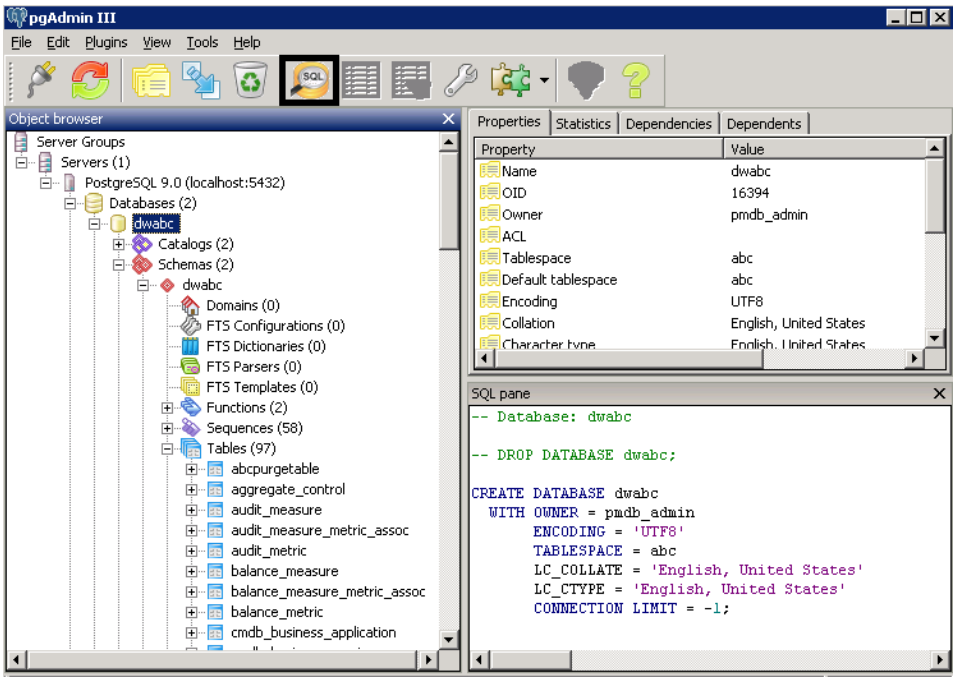
The **Server Intelligence Agent** is started.

15. Log on to Central Management Console (CMC) and check if the backup restored is successful.

For Management Database Table

To restore the management database table, follow these steps:

1. Log on to the HPE OBR system.
2. Go to **Start > Programs > PostgreSQL 9.3 > pgAdmin III** or go to **Start** and enter **pgAdmin III** in **Search** and double-click **pgAdmin III** to open it.
3. Enter password to connect to the database and click the **SQL** icon to launch the sql query analyzer.



4. 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 HPE OBR on Linux

For SAP BusinessObjects Database and File Store

To restore the backup of HPE OBR components, follow these steps:

1. Log on to OBR server2 system where you have installed OBR components.
2. 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.
3. Log on to the system as root.
4. Run the following command to stop the web server:

   ```
   sh /opt/HP/BSM/BOE4/sap_bobj/tomcatshutdown.sh
   ```

5. Move the SQL Anywhere Database files in OBR server2 from the following location to a different location of your choice:

   ```
   $PMDB_HOME/../BOE4/sqlanywhere/database/*BI4*
   ```

   Similarly, rename the `frsinput` and `frsoutput` directories in the following location:

   ```
   $PMDB_HOME/../BOE4/sap_bobj/data
   ```

6. Run the following command to switch to the SAP BusinessObjects administrator:

   ```
   su - shrboadmin
   ```

7. Run the following command to stop all the Server Intelligence Agent servers:

   ```
   sh $PMDB_HOME/../BOE4/sap_bobj/stopservers
   ```

8. Run the following command to stop the SQL Anywhere Database service:

   ```
   sh $PMDB_HOME/../BOE4/sap_bobj/sqlanywhere_shutdown.sh
   ```

   If prompted for password, specify the SQL Anywhere Database password.

9. Run the following command to switch to root user:

   ```
   su root
   ```

10. Copy the backup files taken in "Create Full Backup of HPE OBR on Linux" on page 214 and follow these steps:

    ```
    perl <location of the restore script> <location of the backup file>
    ```

    where, *<location of the restore script>* is the location where the restore script is stored

    <location of the backup file> is the location of backup file of particular day that you want to restore

    For example:

    ```
    perl $PMDB_HOME/DR/SHR_full_Restore.pl /root/SHR_DR_FullBackup/Thu
    ```

11. Run the following command to switch to SHRBOADMIN user and not as root user.

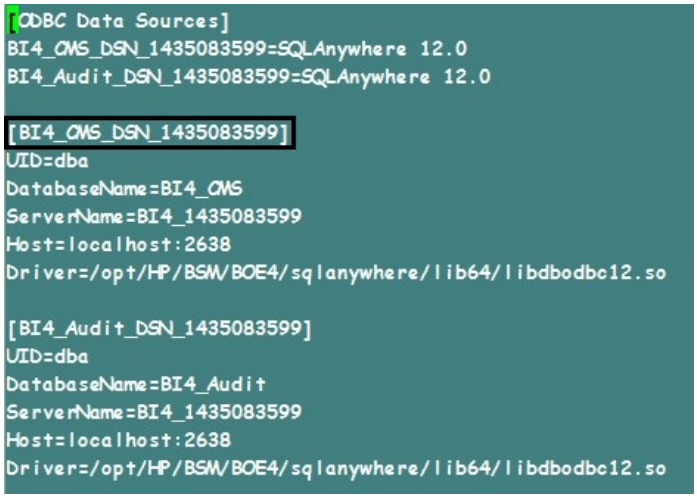
    ```
    su - shrboadmin
    ```

12. Run the following command to start the SQL Anywhere Database service:

    ```
    sh $PMDB_HOME/../BOE4/sap_bobj/sqlanywhere_startup.sh
    ```

13. Note the ODBC Data Source name of the CMS database from the location `/opt/HP/BSM/BOE4/sap_bobj/enterprise_xi40/odbc.ini`.

    For example, in the following image the ODBC Data Source name of the CMS database is `BI4_CMS_DSN_1435083599`

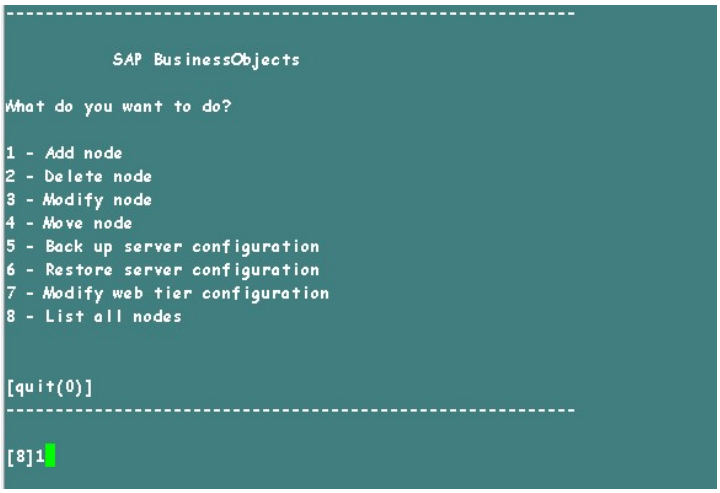
    

14. Run the following command to create a new Server Intelligence Agent (SIA):

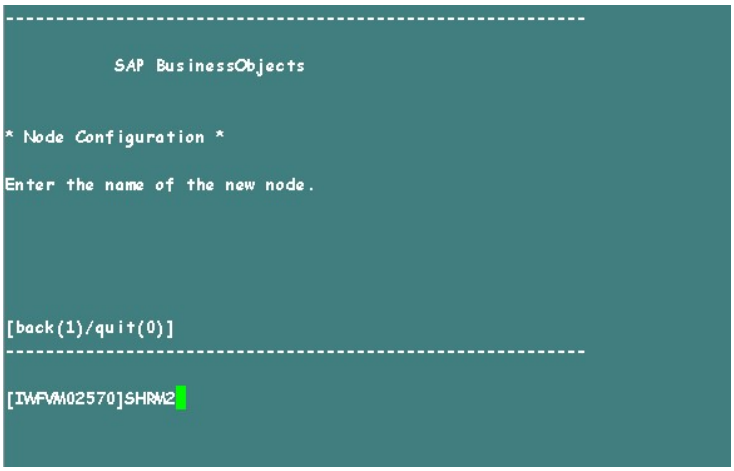
    ```
    sh $PMDB_HOME/../BOE4/sap_bobj/serverconfig.sh
    ```

    The SAP BusinessObjects wizard is displayed in the command line console.

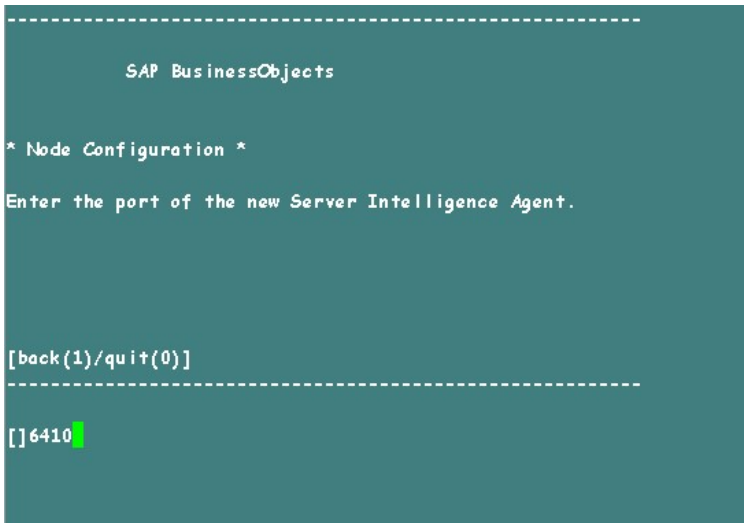
15. Type `1` and press **Enter**.



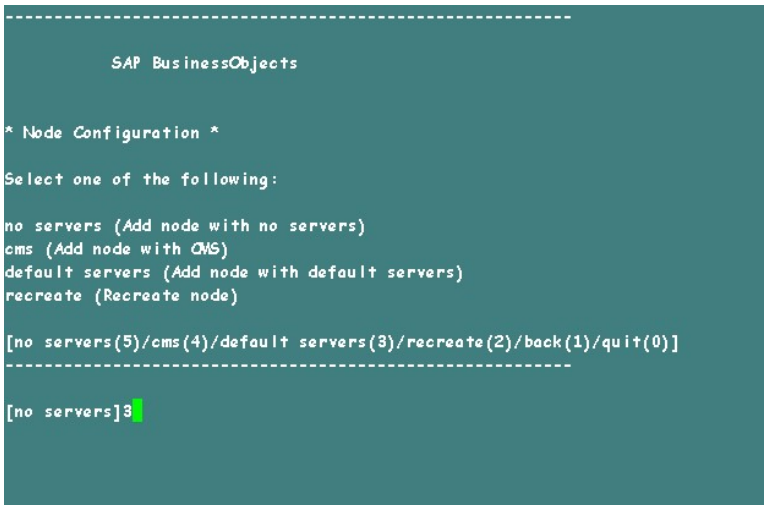
16. Enter the name of the new node and press **Enter**.



17. Enter `6410` as the port number and press **Enter**.

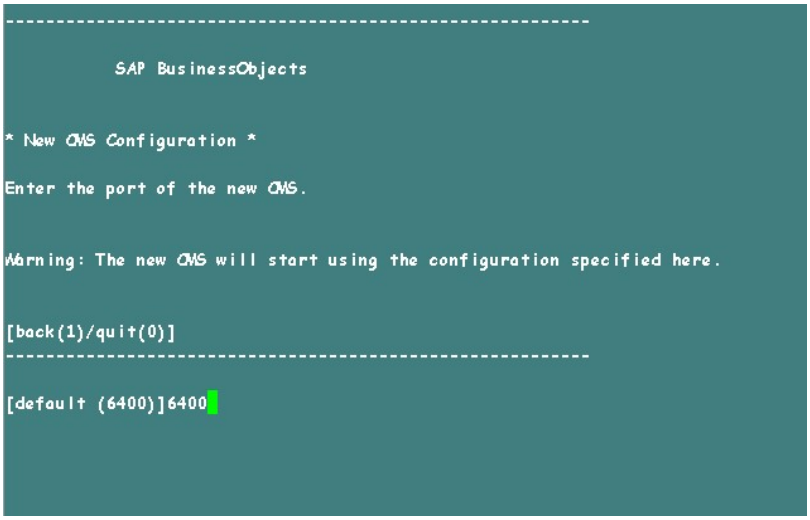


18. Type 3 to select default servers (Add node with default servers) and press **Enter**.

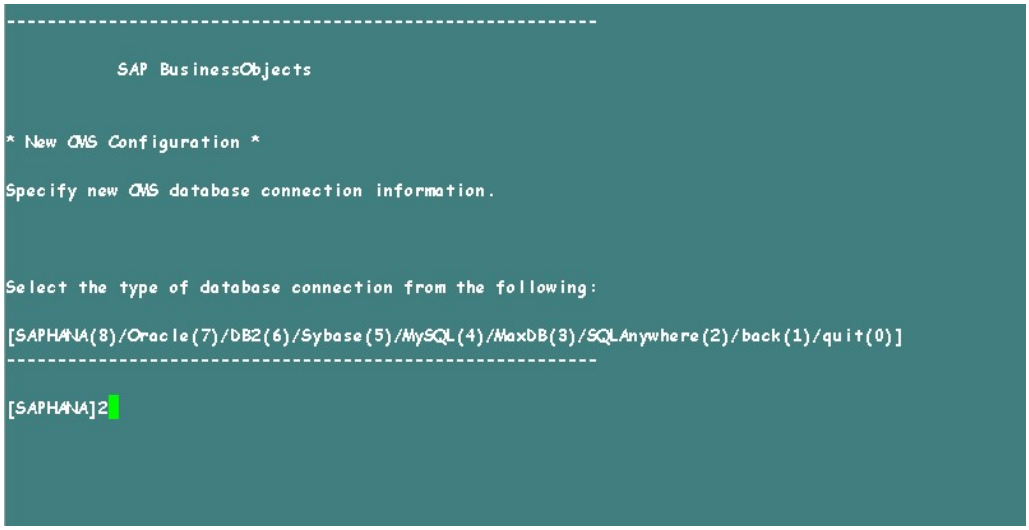


19. Type 2 to select temporary CMS and press **Enter**.

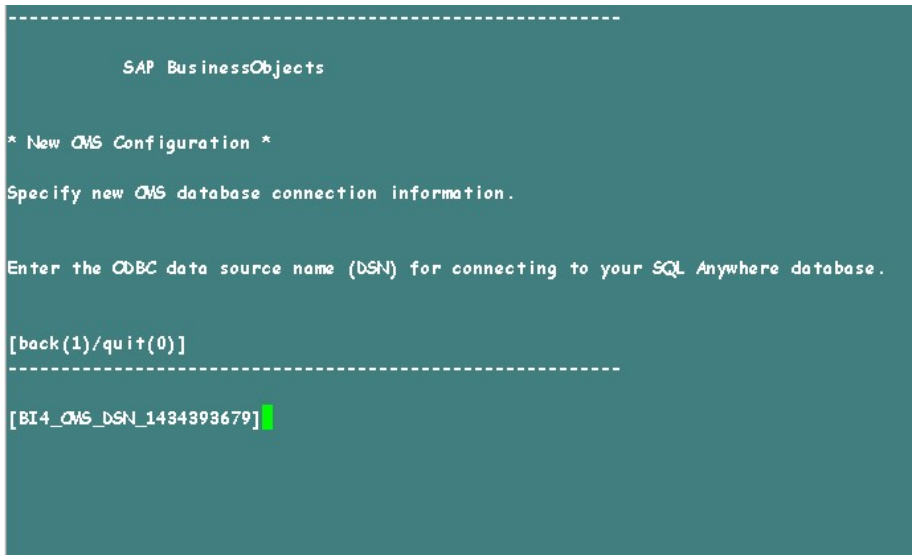
20. Enter the port number of the new CMS as `6400` and press **Enter**.



21. Type `2` to select SQL Anywhere and press **Enter**.

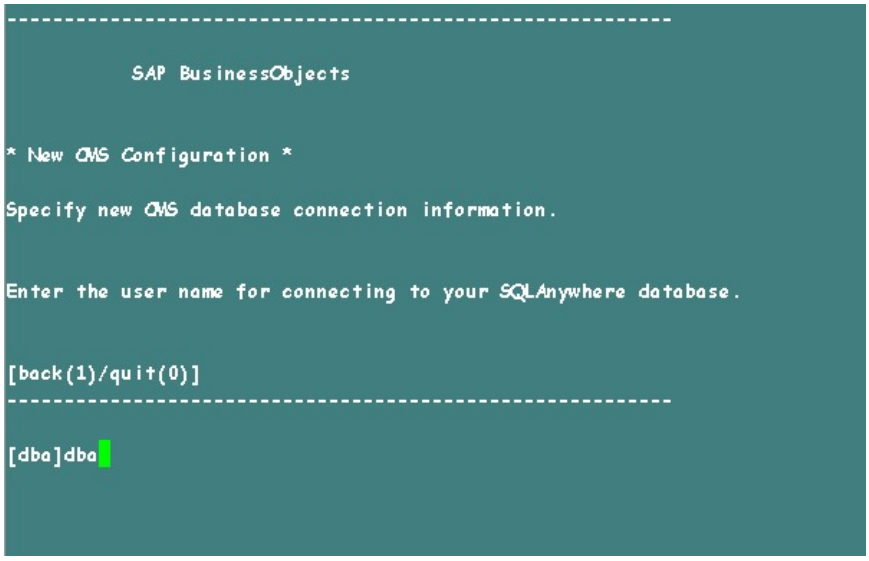


22. Enter the ODBC Data Source name that you noted in Step 13 and press **Enter**.

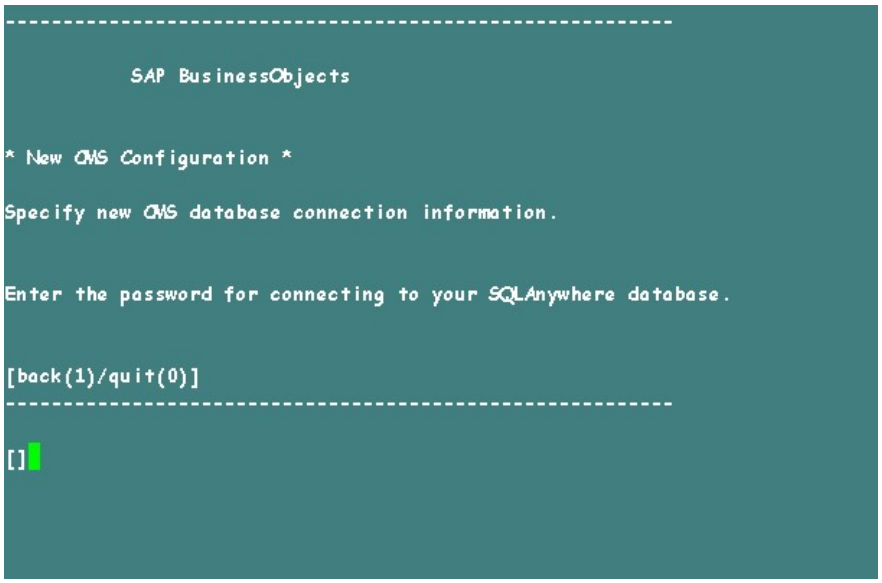


23. Enter the user name and press **Enter**.

> **Note:** Ensure that you enter same user name as is used in the SAP BusinessObjects Server from where the backup is taken.

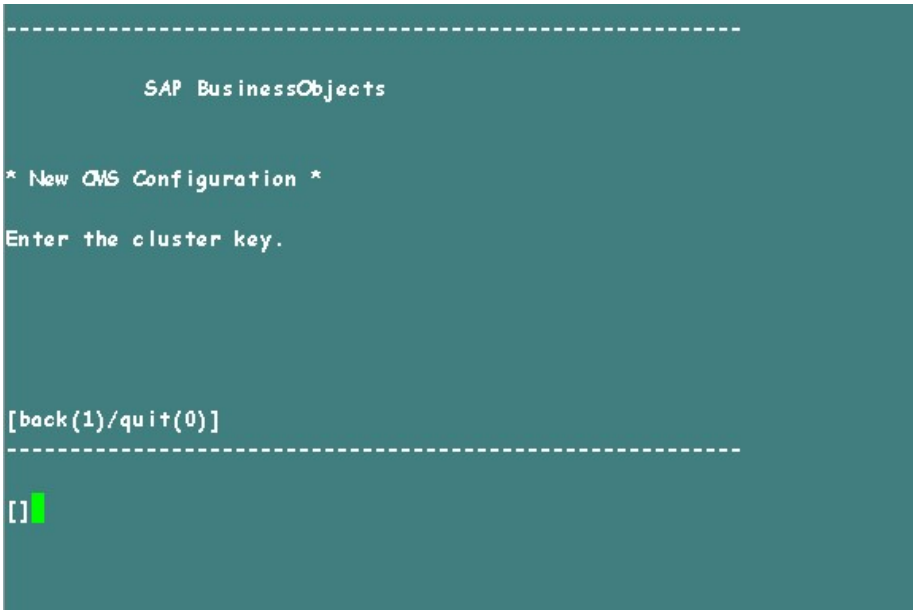


24. Enter the password and press **Enter**.



25. Type the cluster key and press **Enter**.

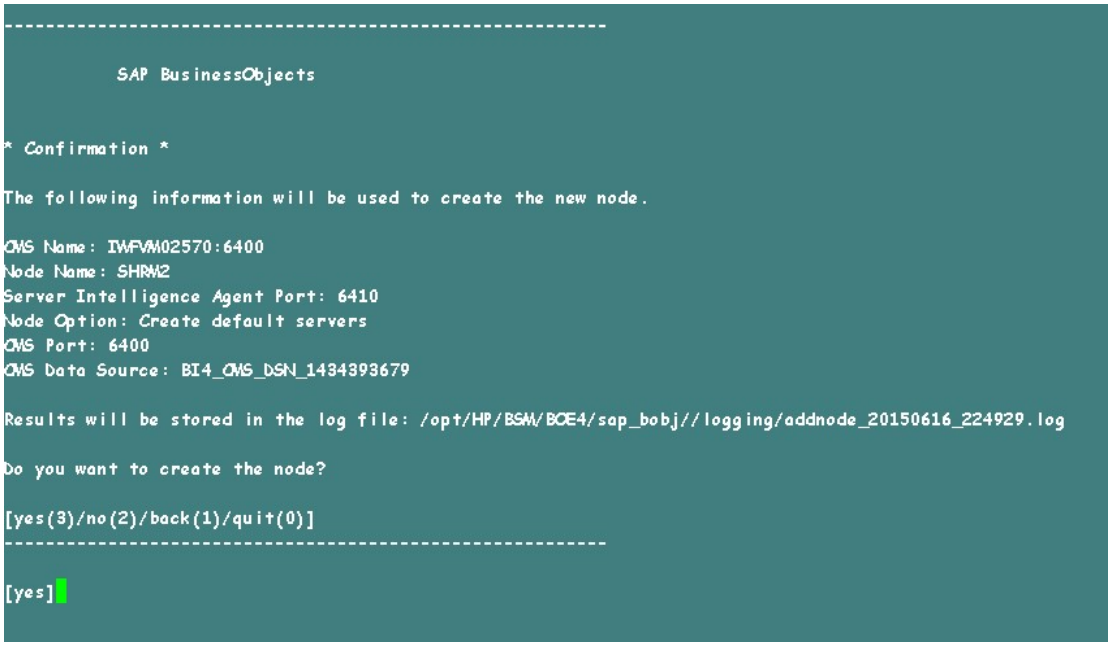
> **Note:** The default cluster key is `1ShrAdmin`. If you have changed the cluster key then enter the changed cluster key value.



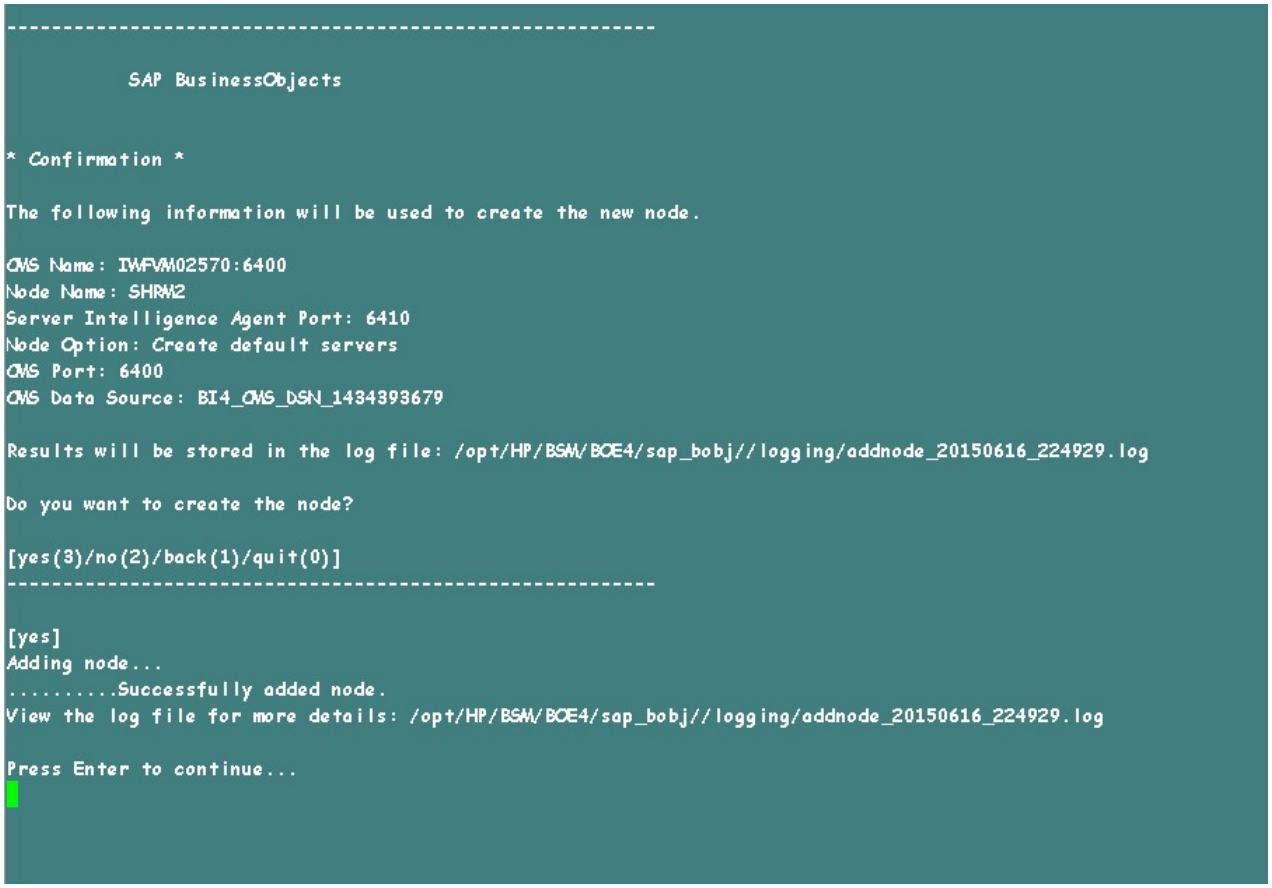
26. To connect to CMS, type the user name as `Administrator` and press **Enter**.

27. Enter the password and press **Enter**.

28. Type yes to add a new node and press **Enter**.

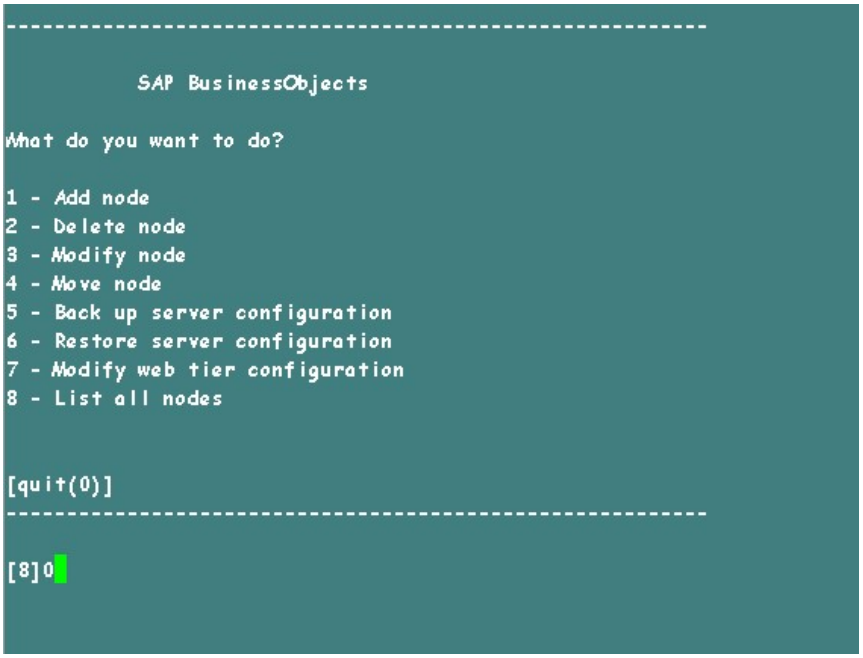


A confirmation message is displayed. Once the new node is successfully added, press **Enter**.



The SAP BusinessObjects menu is displayed.

29. Type `0` to quit and press **Enter**.



30. Type `1` to confirm quit and press **Enter**.
31. Take a back up of `/opt/HP/BSM/BOE4/sap_bobj/ccm.config`
32. Remove/ Delete the `SHRLAUNCH` section as shown in the following image:

33. After removing/ deleting SHRLAUNCH section , save the file as shown in the following image:

```
#!/bin/sh
BOBJEDIR="/opt/HP/BSM/BOE4/sap_bobj/"
BOBJEINSTALLLOCAL="user"
BOBJELANG="en"
BOBJELICENSEKEY="0C00U-1WUVE3M-710XUC4-Gb200MC-7b"
BOBJEUSERNAME="shrboadmin"
BOBJEVERSION="XI 4.0"
CLUSTER_NAMESERVER=""
CLUSTERPORTNUMBER="6400"
CMSCLUSTER="no"
CMSNAMESERVER="IWFVM02570"
CMSPORTNUMBER="6400"
CONNECTORPORT="8080"
DATABASEUID="dba"
DBTYPE_AUDIT="sqlanywhere"
DBTYPE="sqlanywhere"
DEFAULT_NAMESERVER="no"
INSTALL_DIR="/opt/HP/BSM/BOE4/sap_bobj/"
LOCALNAMESERVER="IWFVM02570"
NAMESERVER="IWFVM02570"
PIDDIR="/opt/HP/BSM/BOE4//sap_bobj/serverpids"
PRODUCTID_NAME="BusinessObjects"
PRODUCTID_VER="14.0"
REDIRECTPORT="8443"
REGFILE="/opt/HP/BSM/BOE4//sap_bobj/data/.bobj"
REINIT="yes"
SERVICENAME_AUDIT="BI4_Audit"
SERVICENAME="BI4_CMS"
SERVICEPORT="no"
SHUTDOWNPORT="8005"
SIANODENAME="SHR"
SIAPORTNUMBER="6410"
FIPSModeValue="undefined"
SHRM2LAUNCH='"/opt/HP/BSM/BOE4/sap_bobj/enterprise_xi40/generic/bobjrestart.sh" -protect "/opt/HP/BSM/BOE4/sap_bobj/enterprise_xi40/generic/javalaunch.sh" "-Dbobj.product.languages.dir=/opt/HP/BSM/BOE4/sap_bobj/enterprise_xi40/Languages/" -Djava.net.preferIPv4Stack=false -Djava.awt.headless=true -Dcom.sap.vm.tag=SHRM2 "-Xms64m" "-Xmx256m" "-XX:+ExitVMOnOutOfMemoryError" "-XX:+HeapDumpOnOutOfMemoryError" "-XX:+PrintGCTimeStamps" "-XX:+PrintGCDetails" "-XX:LogGcMaxFileCount=3" "-XX:LogGcMaxFileSize=5m" "-XX:HeapDumpPath=/opt/HP/BSM/BOE4/sap_bobj/logging/" "-XtraceFile=/opt/HP/BSM/BOE4/sap_bobj/logging/SHRM2_jvm_GPID.log" "-XX:GCHistoryFilename=/opt/HP/BSM/BOE4/sap_bobj/logging/SHRM2_gc.prf" "-Xloggc:/opt/HP/BSM/BOE4/sap_bobj/logging/SHRM2_gc.log" "-XX:ErrorFile=/opt/HP/BSM/BOE4/sap_bobj/logging/SHRM2_dump_GPID.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.bootstrap" -port "6410" -pidFile "/opt/HP/BSM/BOE4/sap_bobj/serverpids/SHRM2.pid" -loggingPath "/opt/HP/BSM/BOE4/sap_bobj/logging/" -traceinipath "/opt/HP/BSM/BOE4/sap_bobj/enterprise_xi40/conf/BO_trace.ini" -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 '
```

34. Run the following command to start all Server Intelligence Agent servers:

    ```
    /opt/HP/BSM/BOE4/sap_bobj/startservers
    ```

35. Run the following commands:

    ```
    cd /etc/initd
    ```

    a. **On RHEL 6.x**:

    ```
    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.
4. Run the following query to restore the database tables:

   ```
   Delete From aggregate_control

   COPY aggregate_control from '<backup_path>/backup_AGGREGATE_CONTROL.dat';
   ```

   where, *<backup_path>* is the directory where you placed the Management database backup file.

Back up and Restore Vertica Database

OBR uses HP Vertica database for storing, processing, and managing the performance data of your IT environment. You must take a regular back up of Vertica database along with the other HPE OBR database files.

> **Note:** After you restore the Vertica database backup successfully, bring up the Vertica database.

For more information on backup and restore of Vertica database, see HP Vertica Analytics Platform Version 7.1.x Documentation.

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 HPE OBR and the steps to start and stop these services on Red Hat Enterprise Linux (RHEL) 6.x and 7.x versions supported by HPE OBR.

Appendix A: Status, Stopping and Starting HPE OBR Services

This section provides instructions to check the status, stop and start HPE OBR services.

In case of typical installation scenario, perform these steps on the HPE OBR system. For custom installation, perform these steps on the individual servers as mentioned in the following sections.

On Linux

Status of the HPE OBR services

Go to `/etc/init.d` directory and run the following commands on the command prompt to check the status of HPE OBR services:

On RHEL 6.x	On RHEL 7.x
On OBR Server	
• `service HPE_PMDB_Platform_Administrator status` • `service HPE_PMDB_Platform_Collection status` • `service HPE_PMDB_Platform_DB_Logger status` • `service HPE_PMDB_Platform_IA status` • `service HPE_PMDB_Platform_IM status` • `service HPE_PMDB_Platform_JobManager status` • `service HPE_PMDB_Platform_NRT_ETL status` • `service HPE_PMDB_Platform_Orchestration status` • `service HPE_PMDB_Platform_PostgreSQL status`	• `systemctl status HPE_PMDB_Platform_Administrator.service` • `systemctl status HPE_PMDB_Platform_Collection.service` • `systemctl status HPE_PMDB_Platform_DB_Logger.service` • `systemctl status HPE_PMDB_Platform_IA.service` • `systemctl status HPE_PMDB_Platform_IM.service` • `systemctl status HPE_PMDB_Platform_JobManager.service` • `systemctl status HPE_PMDB_Platform_NRT_ETL.service` • `systemctl status HPE_PMDB_Platform_Orchestration.service` • `systemctl status HPE_PMDB_Platform_PostgreSQL.service`

• service HPE_PMDB_Platform_TaskManager status • service TrendTimer status	• systemctl status HPE_PMDB_Platform_TaskManager.service • systemctl status TrendTimer.service
On SAP BusinessObjects Server	
• service SAPBOBJEnterpriseXI40 status	• systemctl status SAPBOBJEnterpriseXI40.service
On Remote Collector	
• service HPE_PMDB_Platform_Collection status	• systemctl status HPE_PMDB_Platform_Collection.service
On Vertica Server	
• service HPE_PMDB_Platform_Vertica status	• systemctl status HPE_PMDB_Platform_Vertica.service

Stopping HPE OBR Services

Go to `/etc/init.d` directory and run the following commands on the command prompt to stop HPE OBR services:

On RHEL 6.x	On RHEL 7.x
On OBR Server	
• 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_JobManager stop • service HPE_PMDB_Platform_NRT_ETL stop • service HPE_PMDB_Platform_Orchestration stop • service HPE_PMDB_Platform_PostgreSQL stop	• 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_JobManager.service • systemctl stop HPE_PMDB_Platform_NRT_ETL.service • systemctl stop HPE_PMDB_Platform_Orchestration.service • systemctl stop HPE_PMDB_Platform_

• service HPE_PMDB_Platform_TaskManager stop • service TrendTimer stop	PostgreSQL.service • systemctl stop HPE_PMDB_Platform_TaskManager.service • systemctl stop TrendTimer.service
On SAP BusinessObjects Server	
• service SAPBOBJEnterpriseXI40 stop	• systemctl stop SAPBOBJEnterpriseXI40.service
On Remote Collector	
• service HPE_PMDB_Platform_Collection stop	• systemctl stop HPE_PMDB_Platform_Collection.service
On Vertica Server	
• service HPE_PMDB_Platform_Vertica stop	• systemctl stop HPE_PMDB_Platform_Vertica.service

Starting HPE OBR Services

Go to `/etc/init.d` directory and run the following commands on the command prompt to start HPE OBR services:

On RHEL 6.x	On RHEL 7.x
On OBR Server	
• service HPE_PMDB_Platform_Administrator start • service HPE_PMDB_Platform_Collection start • service HPE_PMDB_Platform_DB_Logger start • service HPE_PMDB_Platform_IA start • service HPE_PMDB_Platform_IM start • service HPE_PMDB_Platform_JobManager start • service HPE_PMDB_Platform_NRT_ETL start • service HPE_PMDB_Platform_Orchestration start	• systemctl start HPE_PMDB_Platform_Administrator.service • systemctl start HPE_PMDB_Platform_Collection.service • systemctl start HPE_PMDB_Platform_DB_Logger.service • systemctl start HPE_PMDB_Platform_IA.service • systemctl start HPE_PMDB_Platform_IM.service • systemctl start HPE_PMDB_Platform_JobManager.service • systemctl start HPE_PMDB_Platform_NRT_ETL.service • systemctl start HPE_PMDB_Platform_Orchestration.service

• service HPE_PMDB_Platform_PostgreSQL start • service HPE_PMDB_Platform_TaskManager start • service TrendTimer start	• systemctl start HPE_PMDB_Platform_PostgreSQL.service • systemctl start HPE_PMDB_Platform_TaskManager.service • systemctl start TrendTimer.service
On SAP BusinessObjects Server	
• service SAPBOBJEnterpriseXI40 start	• systemctl start SAPBOBJEnterpriseXI40.service
On Remote Collector	
• service HPE_PMDB_Platform_Collection start	• systemctl start HPE_PMDB_Platform_Collection.service
On Vertica Server	
• service HPE_PMDB_Platform_Vertica start	• systemctl start HPE_PMDB_Platform_Vertica.service

On Windows

Status of the HPE OBR services

Follow these steps to check the status of HPE 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_JobManager
- HPE_PMDB_Platform_NRT_ETL
- HPE_PMDB_Platform_Orchestration
- HPE_PMDB_Platform_PostgreSQL
- HPE_PMDB_Platform_TaskManager
- HPE_PMDB_Platform_Timer

On SAP BusinessObjects Server:

- Business Objects Webserver

On Remote Collector:

- HPE_PMDB_Platform_Collection

Stopping HPE OBR Services

Follow these steps to stop HPE 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_JobManager
- HPE_PMDB_Platform_NRT_ETL
- HPE_PMDB_Platform_Orchestration
- HPE_PMDB_Platform_PostgreSQL
- HPE_PMDB_Platform_TaskManager
- HPE_PMDB_Platform_Timer

On SAP BusinessObjects:

- Business Objects Webserver

On Remote Collector:

- HPE_PMDB_Platform_Collection

Starting HPE OBR Services

Follow these steps to start HPE 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_JobManager
- HPE_PMDB_Platform_NRT_ETL
- HPE_PMDB_Platform_Orchestration
- HPE_PMDB_Platform_PostgreSQL
- HPE_PMDB_Platform_TaskManager
- HPE_PMDB_Platform_Timer

On SAP BusinessObjects Server:

- Business Objects Webserver

On Remote Collector:

- HPE_PMDB_Platform_Collection

Appendix B: SiteScope Monitors for HPE 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	vmmemctltarget.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	ready.summation[]
VMware Performance	Virtual Machine\Realtime\mem	usage.average[]

Monitor Name	Counter	Measure Name
VMware Performance	Virtual Machine\Realtime\mem	read.average[]
VMware Performance	Virtual Machine\Realtime\mem	write.average[]
VMware Performance	Virtual Machine\Realtime\mem	received.average[]
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\mem	usage.average[]
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\cpu	ready.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[]

Monitor Name	Counter	Measure Name
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
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

Monitor	Objects	Counter	System Type
Microsoft Windows Resources	Network Interface	BytesTotal/sec	Windows
Unix Resources	Queue length	Queue length\runq-sz	Unix/Solaris
Unix Resources	Queue Statistics	Queue Statistics\runq-sz	HP-UX/AIX
Unix Resources	Uptime	Uptime\Uptime	Unix /Linux, HP-UX/AIX
Unix Resources	File System	%\capacity	Unix/Solaris
Unix Resources	File System	%\kbytes	Unix/Solaris
Unix Resources	File System	avail	Solaris
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	%\Free	
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

Monitor	Objects	Counter	System Type
Dynamic Disk space	Disk/FileSystem	%/MB free **	Unix/Windows
Dynamic Disk space	Disk/FileSystem	%/MB total **	Unix/Windows
Dynamic Disk space	Disk/FileSystem	%/percent full **	Unix/Windows
CPU	N/A	utilization	Unix/Windows
CPU	N/A	utilization cpu%	Unix/Windows
Memory	N/A	Percent used	Unix/Windows
Memory	N/A	virtual memory used %	Unix/Windows
Memory	N/A	physical memory used % *	Unix/Windows
Memory	N/A	swap space used %	Unix/Windows
Memory	N/A	physical memory MB Free *	Unix/Windows
Memory	N/A	virtual memory MB Free	Unix/Windows
Memory	N/A	MB Free	Unix/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 C: 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 HPE OBR, you must install the SAP BusinessObjects Dashboards application, which is included on the HPE OBR installation media. SAP BusinessObjects Dashboards is not essential for viewing the HPE 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 HPE OBR installation media.

Follow these steps to obtain the `setup` executable:

1. On the HPE 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 D: 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, Deployment Manager 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 Deployment Manager page.

The following table list the ETLs for each content pack:

Content Pack Name	ETL	Comments
Cross-Domain Operations Events	CrossOprEvent_ETL_OMi CrossOprEvent_ETL_OMi10 CrossOprEvent_ETL_OMi10x CrossOprEvent_Domain_ Reports CrossOprEvent_ETL_OMi10_ Extended CrossOprEvent_ETL_OMi_ Extended CrossOprEvent_Domain_ Reports_Extended	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. The Content Pack components 'CrossOprEvent_ETL_OMi' and 'CrossOprEvent_ETL_OMi10' are mutually exclusive. Ensure that only one of them is selected. The Content Pack components 'CrossOprEvent_ETL_OMi_Extended' and 'CrossOprEvent_ETL_OMi10_ Extended' are mutually exclusive. Ensure that only one of them is selected. The Content Pack components 'CrossOprEvent_ETL_OMi10' and 'CrossOprEvent_ETL_OMi10x' are mutually exclusive. Ensure that only one of them is selected. **Note:** Select the Extended ETLs to generate customized reports that involves Event detail attributes.

Content Pack Name	ETL	Comments
		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.
Health and Key Performance Indicators	HIKPI_ETL_ServiceHealth HIKPI_ETL_ServiceHealth_OMi10 HIKPI_Domain HIKPI_Reports_ServiceHealth	If the topology source is OMi 10, select the HIKPI_ETL_ServiceHealth_OMi10 component. The Content Pack components 'HIKPI_ETL_ServiceHealth' and 'HIKPI_ETL_ServiceHealth_OMi10' are mutually exclusive. Ensure that only one of them is selected.
HPSA	HPSA_ETL HPSA_Domain	
IBM WebSphere Application Server	IBMWebSphere_ETL_WebSphereSPI IBMWebSphere_Domain IBMWebSphere_Reports IBMWebSphere_ETL_WebSphereMP	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.
Microsoft Active Directory	MicrosoftActiveDirectory_ETL_ADSPI MicrosoftActiveDirectory_Reports MicrosoftActiveDirectory_Domain	
Microsoft Exchange Server	MicrosoftExchange_ETL_ExchangeSPI2007 MicrosoftExchange_ETL_ExchangeSPI2010 MicrosoftExchange_ETL_	The MicrosoftExchange_ETL_ExchangeSPI2007 collects data from HP Operations SPI for Exchange Server 2007. The MicrosoftExchange_ETL_ExchangeSPI2010 collects data from HP Operations SPI and OMi management pack for Exchange Server 2010.

Content Pack Name	ETL	Comments
	ExchangeSPI2013 MicrosoftExchange_Domain MicrosoftExchange_Reports	The MicrosoftExchange_ETL_ ExchangeSPI2013 collects data from HP Operations SPI and OMi management pack for Exchange Server 2013.
Microsoft SQL Server	MicrosoftSQLServer_ETL_ DBSPI MicrosoftSQLServer_Domain MicrosoftSQLServer_Reports	
Network Performance	NetworkPerf_ETL_PerfiSPI_ NonRTSM NetworkPerf_ETL_PerfiSPI_ RTSM NetworkPerf_Domain NetworkPerf_Reports	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. The Content Pack components 'NetworkPerf_ETL_PerfiSPI_NonRTSM' and 'NetworkPerf_ETL_PerfiSPI_RTSM' are mutually exclusive. Ensure that only one of them is selected. **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. **Note:** The Network Performance Content Pack collects data only from Type2 NodeGroups, that is, routers and switches.
Network Component_Health	ComponentHealth_Reports Core_ComponentHealth	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.
Network Interface_ Health	InterfaceHealth_Reports Core_InterfaceHealth	Install this Content Pack to collect network performance data directly from NNMi. The data collection gives you detailed real time view of component or

Content Pack Name	ETL	Comments
		interface health in your network. You can view detailed health or utilization reports.
Operations Events	OprEvent_ETL_HPOM OprEvent_Domain_Reports	
Oracle	Oracle_ETL_DBSPI Oracle_Domain Oracle_Reports	
Oracle WebLogic Server	OracleWebLogic_ETL_ WebLogicSPI OracleWebLogic_Domain OracleWebLogic_Reports OracleWebLogic_ETL_ WebLogicMP	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.
Real User Transaction Monitoring	RealUsrTrans_ETL_RUM RealUsrTrans_ETL_RUM_OMi RealUsrTrans_Domain_ Reports	If the topology source is OMi 10, select the RealUsrTrans_ETL_RUM_OMi component. 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 SynTrans_ETL_BPM SynTrans_ETL_BPM_OMi	If the topology source is OMi 10, select the SynTrans_ETL_BPM_OMi component. The Content Pack components 'SynTrans_ETL_BPM' and 'SynTrans_ ETL_BPM_OMi' are mutually exclusive. Ensure that only one of them is selected.
System Performance	SysPerf_ETL_ PerformanceAgent SysPerf_ETL_SiS_API SysPerf_ETL_SiS_API_ NonRtSM SysPerf_ETL_SiS_DB	If HP Operations Agent is the data source, select the SysPerf_ETL_ PerformanceAgent Content Pack component. 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

Content Pack Name	ETL	Comments
	SysPerf_Domain SysPerf_Reports	continue to use the same. 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. 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. 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.
Virtual Environment Performance	VirtualEnvPerf_ETL_HyperV_PerformanceAgent VirtualEnvPerf_ETL_IBMLPAR_PerformanceAgent VirtualEnvPerf_ETL_SolarisZones_PerformanceAgent VirtualEnvPerf_ETL_VMWare_PerformanceAgent VirtualEnvPerf_ETL_VMware_SiS_API VirtualEnvPerf_ETL_VMware_SiteScope VirtualEnvPerf_Domain VirtualEnvPerf_Domain_VMWare VirtualEnvPerf_Reports VirtualEnvPerf_Reports_	If the data source is HP Operations Agent or Performance Agent, select Performance Agent based Content Pack components. If the data source is VMware vCenter, select VMWare_vCenter based Content Pack components. Select either VirtualEnvPerf_ETL_VMware_SiteScope or VirtualEnvPerf_ETL_VMware_SiS_API Content Pack component. The VirtualEnvPerf_ETL_VMware_SiteScope is for Profile DB integration. If 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.

Content Pack Name	ETL	Comments
	VMWare VirtualEnvPerf_ETL_VMWare_vCenter	The Content Pack components 'VirtualEnvPerf_ETL_VMWare_vCenter' and 'VirtualEnvPerf_ETL_VMWare_PerformanceAgent' are mutually exclusive. Ensure that only one of them is selected. **Note:** Use the VirtualEnvPerf_ETL_VMWare_PerformanceAgent and VirtualEnvPerf_ETL_HyperV_PerformanceAgent ETLs if the HP Operations Agent version is 11.x or earlier. Use HPE Cloud Optimizer (earlier known as HP Virtualization Performance Viewer (vPV)) content if the HP Operations Agent version is 12. **Note:** The HPE Operations Bridge Reporter supports HPE Cloud Optimizer (earlier known as HP Virtualization Performance Viewer (vPV)). HPE OBR collects data for reporting on performance, configuration, and capacity problems in the virtual environments from HPE Cloud Optimizer. For more information on the integration of HPE OBR with HPE Cloud Optimizer, see User Guide from the following URL: https://hpln.hpe.com/contentoffering/hpe-obr-cloud-optimizer-content

Appendix E: 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	• OS • Physical Or Virtual • CPU Utilization • Memory Utilization • Filesystem Utilization • Availability • RunQ • BS (Business Service) • BV/Group (Business View)
Executive Summary	SM Heat chart	• CPU Utilization • Memory Utilization
Executive Summary	SM System availability	• Availability Heat Chart
Executive Summary	SM System availability summary	• Average Uptime • Average Downtime • Average Availability • Total Uptime in Hours • Total Downtime in Hours
Executive Summary	SM System Exception by Group	• CPU Utilization • Memory Utilization • SWAP Utilization
Executive Summary	SM System Forecast summary	• CPU Utilization • Memory Utilization • Number of standalone nodes • Number of Virtual Host Number of

		CPU(Virtual Host)
Executive Summary	SM System Grade of Service by Group	• CPU Utilization • Memory Utilization • SWAP Utilization
Executive Summary	SM System Inventory	• K_Location.Name, = Location enrichment • K_CI_System_Alias.DNS_Name • K_CI_System_Alias.isvirtual • K_CI_System_Alias.OS
Executive Summary	SM System Resource Outage Forecast Summary	• CPU Utilization • Memory Utilization
Executive Summary	SM Top and Bottom 10 Filesystems by Free Space Utilization	• filesystem Name • Utilization
Executive Summary	SM Top and Bottom 5 Systems	• By Availability • ByCPU Utilization • By Memory utilization
Operational Reports	NRT Resource Utilization	• CPU • Memory • RunQ • SWAP
Operational Reports	Resource Utilization - Trend	• RunQ
Performance	SM Filesystem Utilization Detail	• Filesystem • Average space used in MB
Performance	SM system availability details	• Uptime % • Downtime % • Availability %
Performance	SM System exception details	• CPU Utilization • Memory Utilization • CPU RunQ • SWAP Utilization • Avg memory pageout rate • OS

Performance	SM system grade of service details	• OS • CPU Utilization • Memory Utilization • CPU RunQ • SWAP Utilization
Performance	SM system usage details	• 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	• CPU Utilization • Memory Utilization • Filesystem Utilization • Availability • RunQ
Executive Summary	SM Heat chart	• CPU Utilization • Memory Utilization
Executive Summary	SM System availability	• Availability Heat Chart
Executive Summary	SM System availability summary	• Average Uptime • Average Downtime • Average Availability • Total Uptime in Hours • Total Downtime in Hours
Executive Summary	SM System Exception by Group	• CPU Utilization • Memory Utilization • SWAP Utilization
Executive Summary	SM System Forecast summary	• CPU Utilization • Memory Utilization
Executive Summary	SM System Grade of Service by Group	• CPU Utilization • Memory Utilization

		• SWAP Utilization
Executive Summary	SM System Inventory	• K_Location.Name, = Location enrichment • K_CI_System_Alias.DNS_Name
Executive Summary	SM System Resource Outage Forecast Summary	• CPU Utilization • Memory Utilization
Executive Summary	SM Top and Bottom 10 Filesystems by Free Space Utilization	• filesystem Name • Utilization
Executive Summary	SM Top and Bottom 5 Systems	• By Availability • By CPU Utilization • By Memory utilization
Operational Reports	NRT Resource Utilization	• CPU • Memory • RunQ • SWAP
Operational Reports	Resource Utilization - Trend	• RunQ
Performance	SM Filesystem Utilization Detail	• Filesystem • Average space used in MB
Performance	SM system availability details	• Uptime % • Downtime % • Availability %
Performance	SM System exception details	• CPU Utilization • Memory Utilization • CPU RunQ • SWAP Utilization • Avg memory pageout rate
Performance	SM system grade of service details	• CPU Utilization • Memory Utilization • CPU RunQ • SWAP Utilization
Performance	SM system usage details	• CPU Utilization • Memory Utilization

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 10.10)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to docfeedback@hpe.com.

We appreciate your feedback!