



HPE Operations Bridge Reporter

Software Version: 10.21

Network Interface Health Content Pack Reference

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


Hewlett Packard
Enterprise

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

© 2015 - 2017 Hewlett Packard Enterprise Development LP

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

Documentation Updates

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

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

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

Support

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

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

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

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

About this PDF Version of Online Help

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

Contents

About This Document	4
Getting Started	5
HPE Operations Bridge Reporter (OBR) Overview	5
Deployment Scenarios	5
Types of Reports	6
Network Interface Health Content Pack Overview	8
Target Audience	8
Data Sources for Network Interface Health Data	8
Operating System Combination in Distributed Installation	9
Install the Content Pack	10
Check Availability and Integrity of Data Sources	10
Selecting the Content Pack Components	13
Install the Content Pack	15
Uninstalling the Content Pack Components	16
Data Source Collection Configuration	17
Report Navigation	20
Use Cases	22
Appendix	24
Appendix A: Terminology	24
Send documentation feedback	26

About This Document

This document provides an overview of HPE OBR and Network Interface Health Content Pack. This document provides the list of Network Interface Health reports available with the Network Interface Health Content Pack.

This document helps you to install and configure the data source for the Network Interface Health Content Pack. It provides information on report navigation and related terminology.

For information on HPE Operations Bridge Reporter tools and contents, go to [Marketplace](#).

Getting Started

This section provides HPE OBR overview, deployment scenarios, and types of reports.

HPE Operations Bridge Reporter (OBR)

Overview

HPE OBR is a cross-domain historical infrastructure performance reporting solution. It displays top-down reports from Business Service Management (BSM) Business Service and Business Application, Operations Manager (OM) Node Group or OMi10 perspective to the underlying infrastructure. It also displays bottoms-up reports from the infrastructure to the impacted Business Services and Business Applications or Node Groups. It leverages the topology information to show how the underlying infrastructure health, performance and availability affects your Business Services and Business Applications or Node Groups in the long term. You can navigate from higher level cross domain reports to detailed domain level reports.

Deployment Scenarios

Following are the deployment scenarios supported on HPE OBR:

- **Deployment with BSM/OMi** - In this deployment, Run-time Service Model (RTSM) is the source of topology information. HPE OBR discovers and synchronizes topology information from OMi. In a BSM environment with underlying OM servers, this synchronization technique receives discovered topology data from multiple OM systems and updates the Configuration Items (CIs) and CI relationships in the RTSM as soon as changes are discovered. However, you can also use the OM D-MoM dynamic topology synchronization technique to discover and synchronize the topology information in RTSM. In an environment with OMi 10.00, HPE OBR uses RTSM to obtain topology information and metrics from Operations Agent or SiteScope systems that are configured with OMi.
- **Deployment with Operations Manager** - In this deployment, the topology information is a group of managed nodes defined in OM that are logically combined for operational monitoring. These logical node groups are created by OM users to classify the nodes as specific organizations or entities within their enterprise. For example, a group called Exchange Servers can be created in OM to

organize the specific Exchange Servers and Active Directory nodes for reporting or monitoring purposes. HPE OBR uses the node groups from OM for its topology computation.

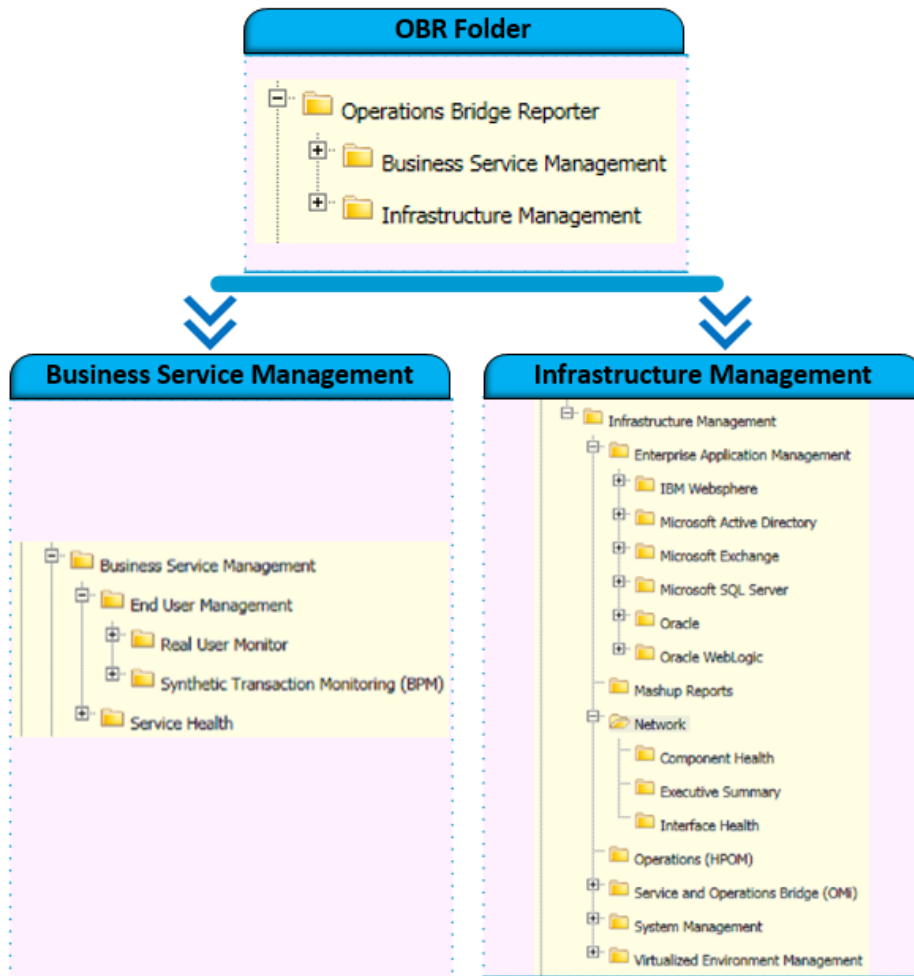
- **Deployment with VMware vCenter** - VMware vCenter is a distributed server-client software solution that provides a central and a flexible platform for managing the virtual infrastructure in business-critical enterprise systems. VMware vCenter centrally monitors performance and events, and provides an enhanced level of visibility of the virtual environment, thus helping IT administrators to control the environment with ease.
- **Other deployments** - Apart from the basic deployment scenarios, you can collect data from the following sources independently:
 - Deployment with NNMI
 - Deployment with a generic database
 - Deployment with other applications using CSV

Types of Reports

The reports available in HPE Operations Bridge Reporter (OBR) are divided into two broad categories:

- Business Service Management
- Infrastructure Management

The following image shows the supported list of reports folders under both these categories:



To view a map of all the reports available in the Network Interface Health Content Pack, see [Report Navigation](#).

For more information on Operations Bridge Reporter concepts, see *HPE Operations Bridge Reporter Concepts Guide* and *HPE Operations Bridge Reporter Content Development Guide*.

Network Interface Health Content Pack Overview

The Network Interface Health reports provide performance data for network interfaces. Using these reports you can determine the status of the interfaces on your network.

Target Audience

The target audience for the Network Interface Health reports is Network Administrators who are responsible for the maintenance of the network infrastructure of their organization. They can use the Network Interface Health reports to determine if a component is over-utilized or needs an upgrade. By analyzing the performance, availability, and health information displayed in the reports, Network Administrators can help ensure continuous improvement of these business services and business applications.

Data Sources for Network Interface Health Data

OBR collects network data directly from NNMI and NNM iSPI Performance for Metrics. The **InterfaceHealth_Reports Content Pack** identifies the list of metrics that OBR must collect from each of these data sources. This data is stored in the database as individual records. HPE OBR then performs aggregation routines on these records and converts the data to daily data. This aggregated data is displayed in the reports.

The Network Performance Server (NPS) extends NNMI's functionality by providing a platform for performance data storage, analysis and reporting. NPS provides the infrastructure that is used in conjunction with NNMI to monitor the operational performance of the network infrastructure. With the performance data collected by different NNMI Software Smart Plug-ins (iSPIs) such as NNM iSPI Performance for Metrics, the NPS builds data tables, runs queries in response to user selections, and displays query results in web-based reports that help you diagnose and troubleshoot problems in your network environment. The NPS enables you to effectively store, access, and track performance data.

Operating System Combination in Distributed Installation

The table below illustrates the combination of operating systems that are supported between NNMi and NPS in a distributed installation environment.

Note: Ensure that you use the same version levels for both NNMi and NPS.

		NPS	
		Windows	Linux
NNMi	Windows	Supported	Not Supported
	Linux	Supported	Supported

Install the Content Pack

This section provides information on the components of Content Pack, select and install the Content Pack.

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.

Before you begin to install the Content Packs, check the availability and integrity of the data sources:

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 {PMD_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.

Status Summary

BSM/OMI Version	Host Name	Connection Status	View Status	Mandatory CI Type Status	Mandatory CI Attributes Status	Number of Duplicate Nodes
Unknown	IWFV/M02277.hpsw/abs.adapps.hp.com	✔	✘	✘	✘	0

Select Views:

Not available in RTSM
 Missing Mandatory CI Types
 Missing Mandatory CI Attributes

View Summary

View Name	Available in RTSM?	Mandatory CI Types Missing	Mandatory CI Attributes Missing
SM_PA	Yes	0	4
SM_SIS_BusinessView	Yes	1	1
Exchange_Site_View	Yes	0	0
JZEE_Deployment	Yes	1	0
SM_HyperV_BusinessView	Yes	1	3
SM_SIS_Server	Yes	1	3
SM_Sol_Zones	Yes	1	1
ORA_Deployment	Yes	1	0
MSSQL_BusinessView	Yes	0	0
ORA_BusinessView	Yes	1	0
SM_Sol_Zones_BusinessView	Yes	0	12
SHR_Network	Yes	0	0
SM_LPAR	Yes	1	1
SM_SIS	Yes	0	1

The file displays the following information:

- i. Server status
- ii. Configuration details

- iii. Views available in RTSM
- iv. Mandatory CI types missing in the view
- v. Mandatory CI attributes missing with the CI type

Check Data Source Related to PA

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

1. Log on to the 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.

Node Status Summary

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

Select any

Node Name: Domains:

Node Status

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

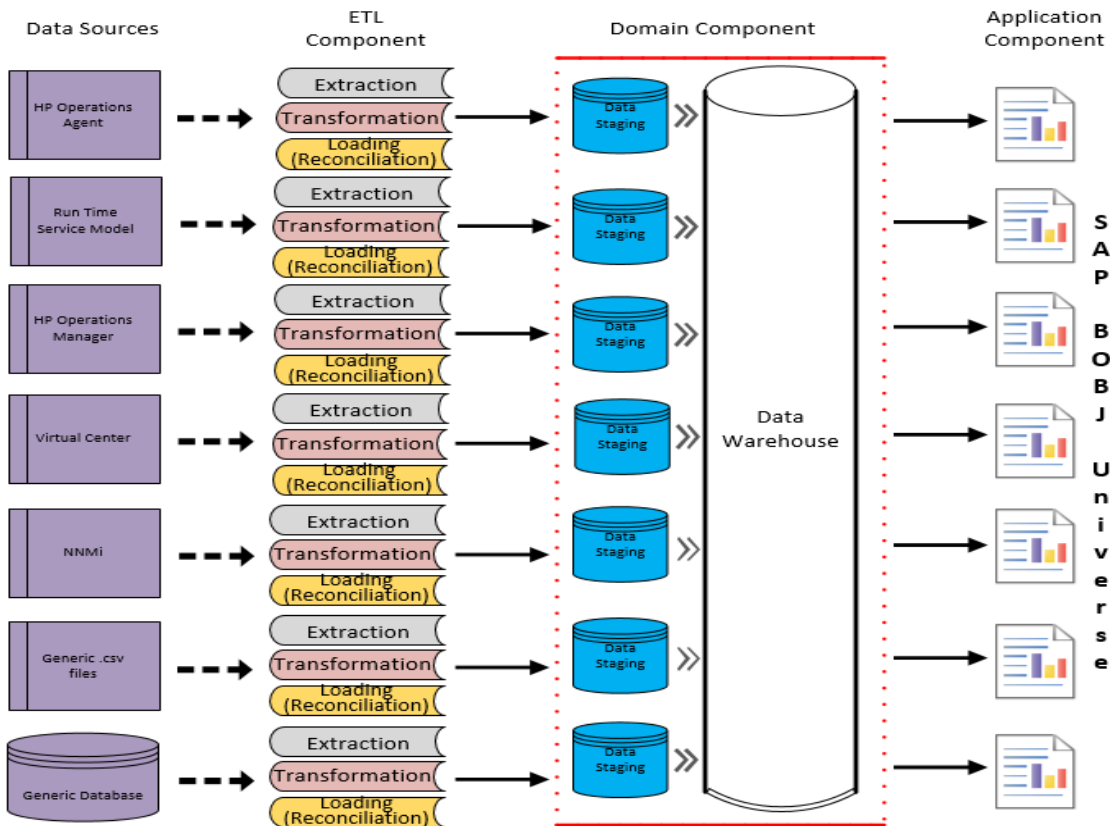
The file displays the following information:

- i. Node status summary
- ii. Node status

Selecting the Content Pack Components

A typical Content Pack consists of three components - the Domain, Extraction Transformation Loading (ETL), and Application components.

The following figure shows the typical data flow between the components of the Content Pack:



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

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.

The ETL Content Pack component is data source dependent. Therefore, for a particular domain, each data source application has a separate ETL Content Pack component. For example, if you

want to collect system performance data from the Operations Agent, you must install the `SysPerf_ETL_PerformanceAgent` component. If you want to collect system performance data from SiteScope, you must install either `SysPerf_ETL_SiS_API` (sourcing data logged in API) or `SysPerf_ETL_SiS_DB` (sourcing data logged in BSM Profile database).

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

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

Install the Content Pack

To install the required Network Performance Content Pack, follow these steps:

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

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

2. In the Administration Console, click **Content Pack Deployment**.
The Content Pack Deployment page is displayed.

To install this content pack and to generate reports on network performance data from NNMi, make the following selections:


- `InterfaceHealth_Domain`
- `InterfaceHealth_Reports`

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

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

appears.

Note: The timer service will be stopped automatically during install/uninstall/upgrade operation and will be started once operation is complete.

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

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

Uninstalling the Content Pack Components


To uninstall the Content Packs, follow these steps:

1. Launch the Administration Console in a web browser:
 - 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 **Content Pack Deployment**. The **Content Pack Deployment** page appears.

The **Content Pack Deployment** displays the Content Pack components that are installed in the supported deployment scenario. For the list of Content Pack, see, [List of Content Pack and Topology Views to Deploy](#) .
3. Click  icon for the required Content Pack to be uninstalled. A summary message is displayed.

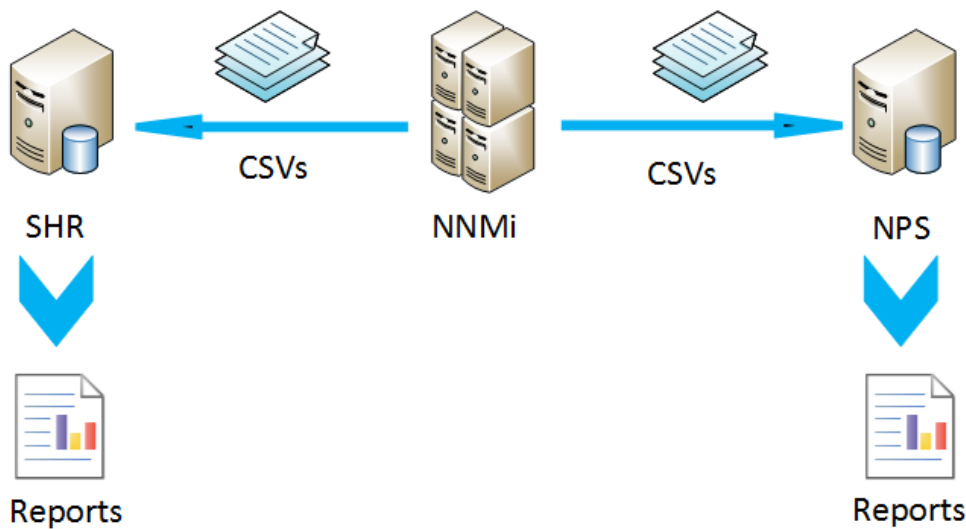
Note: At a time, only one Content Pack and its dependent Content Packs are uninstalled.

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

Data Source Collection Configuration

Note: You have to perform the following configuration steps only if you have installed Component Health and/or Interface Health Content Pack.

HPE OBR is integrated with NNMi to collect network performance data. NNMi passes the network performance data as .csv files to both HPE OBR and Network Performance Server (NPS). HPE OBR stores these .csv files from NNMi to data warehouse to generate reports.



Prerequisite

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

- NNMi and NPS are installed and configured correctly.
- HPE OBR is installed with Component Health and/or Interface Health Content Pack.
- The HPE_PMDB_Platform_NRT_ETL service is up and running.

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. NNMi and NPS are up and running.
2. You must have the shared drive details.

You may get the details from your system administrator or check the recent output of the `nmenableperfspi.ovpl` script in `/opt/OV/newconfig` folder (**On Linux**) and `C:\Program Files (x86)\HP\HP BTO Software\newconfig` folder (**On Windows**).

Check for the most recently written file name with `nmenableNps.20xxxxxxxxxxxx.cfg`.

where, `xxx` is the most recent time stamp.

3. Set the `exportToSHR` property to `TRUE` in `$OvDataDir/shared/perfSpi/conf/nmsAdapter.conf` and restart NNMi.

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.hpswlab.s.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:

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.hpswlab.s.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.

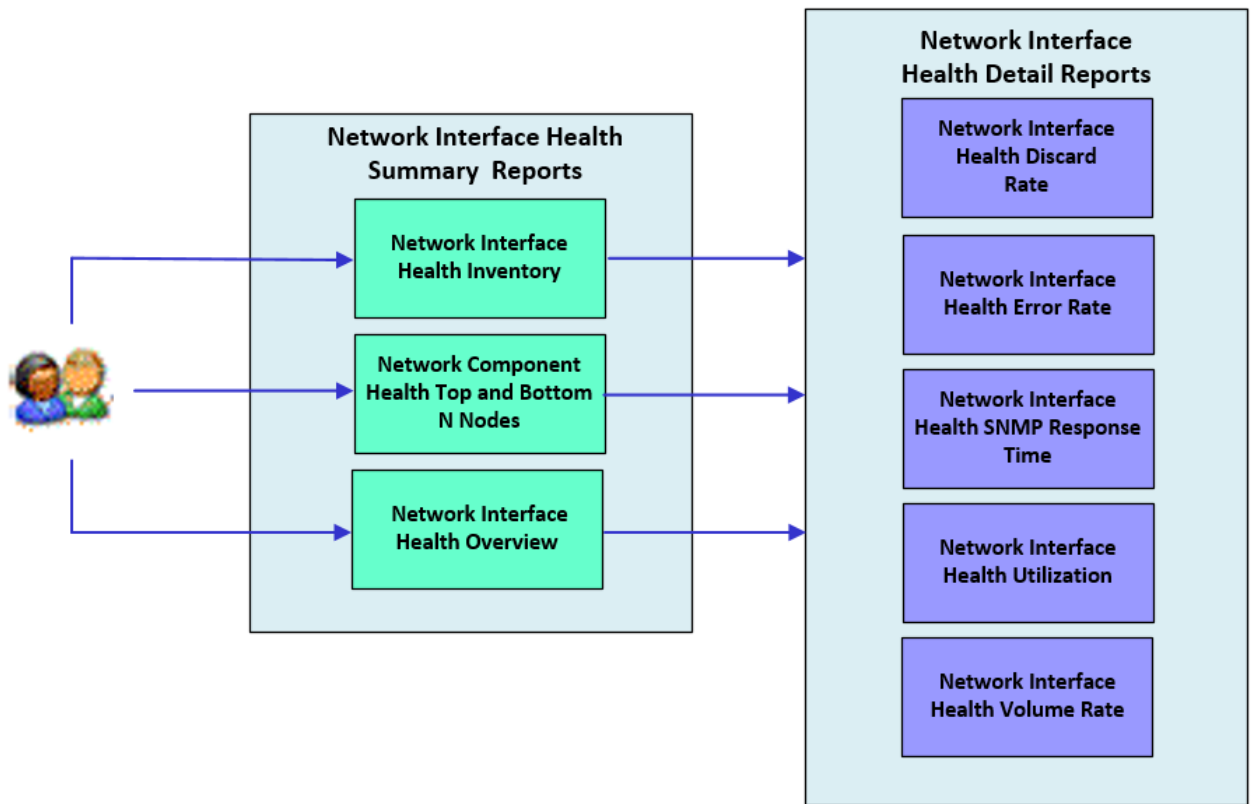
Note: If the collection has not yet started, you have to restart the service manually.

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

Report Navigation

The Network Interface Health reports help you to detect the component that has a health or performance problem, analyze the utilization of the NNMi-managed network components during a specific time range, and detect over-utilized and under-utilized components on the network.

The following diagram consolidates the reports in the Network Interface Health domain and depicts one possible way of navigating the reports:



Availability

Displays average node availability , average node reachability, average SNMP response time, and average ICMP response time for top and bottom N selected nodes based on availability and reachability.

Availability	Color
< 90	

Availability	Color
> 90 and < 95	Yellow
> 95	Green

Use Cases

This section provides information on use cases for Network Interface Health reports. The following table provides description, user, and report name for the use cases.

Description	Report Category	Report Name
To view the health of the network interfaces available in your environment. Displays interfaces by their volume, discard rate, and errors. It also displays interfaces with low availability of less than 100% and greater than 1%, and interfaces with lowest availability.	Summary Report	Network Interface Health Overview
To view information on network health inventory such as interface name, interface type, tenant name, and security or group name for groups. It also provides inventory summary for a particular inventory with number of nodes, tenant name, qualified interface and interface type.	Summary Report	Network Interface Health Inventory Report
To view top and bottom N nodes based on node availability and SNMP response time. Also provide information on Top and Bottom N Availability and Top and Bottom N Node by SNMP Response tabs provides information such as average node availability, SNMP response time, utilization, throughput, discard rate, and error rate for top and bottom N node names based on node availability and SNMP response time.	Summary Report	Network Interface Health Top and Bottom N Nodes
To view the discard rate, discard rate in, and discard rate out for a node. The report must provide information on average, maximum and minimum discard rate for a node as table and as a chart. The report must also display average discard rate for selected interface of the node as a chart.	Detail Report	Network Interface Health Discard Rate
To view error rate, error rate in, and error rate out for a node. The report must provide information on average, maximum and minimum error rate for a node as table and as a chart. The report must also display average error rate for selected interface of the node as a chart.	Detail Report	Network Interface Health Error Rate
To view SNMP Response Time for a node. The report must provides information on average, maximum and minimum SNMP Response Time for a node as table and as a chart. The report must also display average SNMP Response Time for selected interface of the node as a chart.	Detail Report	Network Interface Health SNMP Response Time
To view utilization, utilization in, and utilization out for a node. The report must provide information on average, maximum and minimum utilization for a node as table and as a chart. The report must also display average	Detail Report	Network Interface Health

Description	Report Category	Report Name
utilization for selected interface of the node as a chart.		Utilization
To view graphical representation of interface health by volume rate for a specific time period. Displays the volume rate for bites and packets in terms of sum of bites in, bites out, packets in, and packets out.	Detail Report	Network Interface Health Volume Rate

Appendix

This section provides information on Terminology.

Appendix A: Terminology

Availability: The percentage of interfaces that are available.

Discard Rate: The percentage of discarded inbound and outbound packet count compared to the total number of packets received and sent.

Discard Rate In: The percentage of discarded inbound packet count compared to the total number of packets received.

Discard Rate Out: The percentage of discarded outbound packet count compared to the total number of packets sent.

Discards - Packets: The sum total of inbound and outbound data packets (without error) that are discarded.

Discards - Packets In: Total number of incoming packets (without error) that are discarded.

Discards - Packets Out: Total number of outgoing packets (without error) that are discarded.

Error Rate: The percentage of packets (inbound and outbound) with error.

Error Rate In: The percentage of inbound packets with error.

Error Rate Out: The percentage of outbound packets with error.

Errors - Packets: The sum total of inbound and outbound data packets with errors.

Errors - Packets In: Total number of inbound data packets with errors.

Errors - Packets Out: Total number of outbound data packets with errors.

Interface Name: The name of the interface.

Interface Speed: The speed of the interface

Interface Type: The type of the interface.

Node Name: Hostname of the node that hosts the interface.

Packet Size - Bytes: The average size of a packet in bytes.

Packet Size - Bytes In: The average size of an inbound packet in bytes.

Packet Size - Bytes Out: The average size of an outbound packet in bytes.

Qualified Interfaces: The fully qualified domain name of the interface.

Reboot: A device that is unable to perform the counter delta calculation due to a system restart.

SecGroups: Name of the security group where the interface belongs.

SNMP Response Time: Time (in milliseconds) for the SNMP agent to respond to polling request.

Tenants: Name of the tenant group where the interface belongs.

Throughput: Total inbound and outbound data (in bits) per second.

Throughput In: Total inbound data (in bits) per second.

Throughput Out: Total outbound data (in bits) per second.

Utilization: The percentage of the total inbound and outbound octets to the maximum number of possible inbound and outbound octets.

Utilization In: The percentage of total inbound octets compared to the maximum number of octets that can possibly arrive.

Utilization Out: The percentage of total outbound octets compared to the maximum number of octets that can be possibly sent.

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 Network Interface Health Content Pack Reference (Operations Bridge Reporter 10.21)

Just add your feedback to the email and click send.

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

We appreciate your feedback!