IBM Network Performance Insight 1.3.1
Document Revision R2E1

Network Management Operations
Note
Before using this information and the product it supports, read the information in “Notices” on page 27.
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network management operations</td>
<td>v</td>
</tr>
<tr>
<td>Intended audience</td>
<td>v</td>
</tr>
<tr>
<td>Network Performance Insight architecture</td>
<td>v</td>
</tr>
<tr>
<td>IBM Community</td>
<td>viii</td>
</tr>
<tr>
<td>Network Performance Insight technical training</td>
<td>ix</td>
</tr>
<tr>
<td>Support information</td>
<td>ix</td>
</tr>
<tr>
<td>Conventions used in this publication</td>
<td>ix</td>
</tr>
<tr>
<td>Typeface conventions</td>
<td>ix</td>
</tr>
<tr>
<td><strong>Chapter 1. Discovering the network</strong></td>
<td>1</td>
</tr>
<tr>
<td>Discovery-related files and folders</td>
<td>1</td>
</tr>
<tr>
<td>Discovery process</td>
<td>2</td>
</tr>
<tr>
<td>Discovery methods</td>
<td>4</td>
</tr>
<tr>
<td>Configuring the discovery</td>
<td>4</td>
</tr>
<tr>
<td>Optional: Adding and deleting resource types</td>
<td>5</td>
</tr>
<tr>
<td>Troubleshooting discovery</td>
<td>6</td>
</tr>
<tr>
<td><strong>Chapter 2. Polling the network</strong></td>
<td>7</td>
</tr>
<tr>
<td>Configuring the metric polling interval</td>
<td>7</td>
</tr>
<tr>
<td>SNMP metric collection scope</td>
<td>8</td>
</tr>
<tr>
<td>Resource scoping</td>
<td>8</td>
</tr>
<tr>
<td>Enabling and disabling formulas</td>
<td>10</td>
</tr>
<tr>
<td>Troubleshooting network polling</td>
<td>12</td>
</tr>
<tr>
<td>Verifying the scope from Ambari</td>
<td>12</td>
</tr>
<tr>
<td><strong>Chapter 3. Rapid SNMP device onboarding</strong></td>
<td>13</td>
</tr>
<tr>
<td>Technology Pack Development Tool</td>
<td>14</td>
</tr>
<tr>
<td>Installing the tool</td>
<td>15</td>
</tr>
<tr>
<td>Preparing your environment</td>
<td>16</td>
</tr>
<tr>
<td>Creating discovery formulas</td>
<td>17</td>
</tr>
<tr>
<td>Creating collection formulas</td>
<td>20</td>
</tr>
<tr>
<td>Creating metrics</td>
<td>22</td>
</tr>
<tr>
<td>Validating the pack content</td>
<td>22</td>
</tr>
<tr>
<td>Packaging the Technology Pack bundle</td>
<td>24</td>
</tr>
<tr>
<td>Deploying the custom Technology Pack</td>
<td>25</td>
</tr>
<tr>
<td>Troubleshooting Technology Pack Development Tool</td>
<td>26</td>
</tr>
<tr>
<td><strong>Notices</strong></td>
<td>27</td>
</tr>
<tr>
<td>Trademarks</td>
<td>28</td>
</tr>
<tr>
<td>Terms and conditions for product documentation</td>
<td>29</td>
</tr>
</tbody>
</table>
Network management operations

This information helps you to understand the network management operations that can be performed by Network Performance Insight, V1.3.1.

Network Performance Insight complements Tivoli® Network Manager to interrogate and poll the resources from network devices to collect the Performance Metric OOTB Device Support metrics. Performance Metric OOTB Device Support are the device health metrics from Cisco, Huawei and Juniper devices. For IP SLA-configured devices, discovery is performed by Tivoli Network Manager and polling is done by Network Performance Insight. The metric data is stored in the timeseries database for easy and fast retrieval for visualizations.

Network Performance Insight performs second-level discovery on the SNMP devices that are discovered by Tivoli Network Manager to collect the resource metadata. This data is stored in INVENORY schema tables.

To enable Network Performance Insight to perform the network management, ready-to-use Cisco, Huawei, and Juniper Technology Packs are provided with the following content:

• Discovery formulas
• Collection formulas
• Metrics
• Required MIB files

Intended audience

The audience who is network administrators or operations specialist responsible for installing the Network Performance Insight product suite on an enterprise network.

To use the Technology Pack Development Tool to create your custom Technology Pack, you must have a thorough understanding of the following subjects:

• Network Performance Insight 1.3.1 system
• Basic principles of network protocols and network management
• Discovery concepts
• Polling concepts
• IBM Netcool® Operations Insight
• IBM Tivoli Network Manager IP Edition
• SQL concepts

Network Performance Insight architecture

IBM Network Performance Insight is a network performance monitoring system. It offers both real-time and historical trends in network performance and interactive view on the network data that helps in reduced network downtime and optimized network performance.

Network Performance Insight provides IBM Netcool Operations Insight with comprehensive IP network device performance monitoring and session traffic analysis.

The following diagram shows how data is flowing through the various components in Network Performance Insight:
Network Performance Insight services

Network Performance Insight services are running on microservice architecture that has the software application as a suite of independently deployable, small, modular services in which each service runs a unique process and communicates through a well-defined, lightweight mechanism. Currently, Network Performance Insight 1.3.1 consists of the following microservices:

**Foundation services**
- Dashboard
- DNS
- Event
- Manager
- Storage
- UI

**Entity Metric services**
- Cacti Collector
- Exporter
- Formula Service
- Entity Analytics
- SNMP Collector
- Threshold
• Tivoli Network Manager Collector

**Flow Metric services**

• Flow Analytics
• Flow Collector

For more information about these services, see their respective sections in *IBM Network Performance Insight: Product Overview*.

**Network Performance Insight additional components**

Some of the additional components that are introduced in Network Performance Insight, V1.3.1 for enhanced functions are described here:

**Technology Packs**

A set of ready-to-use Technology Packs is provided to perform second-level discovery and polling of resources to collect entity metric data. These Technology Packs can help to collect standard SNMP metrics, IP SLA metrics, and Performance Metric OOTB Device Support metrics.

For more information, see *Installing the Technology Packs* section in *Installing and Configuring IBM Network Performance Insight*.

**Network Performance Insight Dashboards**

These interactive dashboards are the built-in, JSON-based dashboards suite that can display aggregated network data from Network Performance Insight database with the help of REST API calls. It supports a combination of data from multiple data sources.

This feature provides a wide variety of dashboards for Network Operators, Network Engineers, and Network Capacity Planners. These dashboards help in pinpointing the troubled resources and general resource performance. A number of web-based configuration options are available to control the data that is displayed on the dashboards.

For more information, see *Network Performance Insight Dashboards* section in *IBM Network Performance Insight: Product Overview*.

**Note:** Networks for Operations Insight is a solution extension of Netcool Operations Insight that includes the following components and products:

• Tivoli Network Manager
• Tivoli Netcool Configuration Manager
• Network Performance Insight
• Network Health Dashboard
• Device Dashboard
• Topology Search

**Hortonworks Data Platform components**

Hortonworks Data Platform (HDP®) can be used to help process and analyze the volume, variety, and velocity of data that continually enters your organization every day. Network Performance Insight is installed as a service extension to the installed HDP® stack.

The features of HDP® that are used in Network Performance Insight:

• HDP®
• Default support for rolling upgrades for Hadoop services
• Support for long-running applications within YARN for enhanced reliability
• Spark in-memory distributed compute engine for dramatic performance increase
• Apache Ambari operational framework. Apache Ambari is an open framework for provisioning, managing, and monitoring Apache Hadoop clusters. Ambari provides an intuitive and easy-to-use Hadoop management web UI backed by its collection of tools and APIs that simplify the operation of Hadoop clusters.
• Essentially includes the following open source technologies for working with Network Performance Insight:
  - Apache Hadoop
  - Apache Kafka
  - Apache Ambari
  - Apache Spark
  - Apache ZooKeeper
  
  Note: Because Zookeeper requires a majority, it is best to use an odd number of machines. For example, with four machines ZooKeeper can handle the failure of a single machine; if two machines fail, the remaining two machines do not constitute a majority. However, with five machines ZooKeeper can handle the failure of two machines.

Integrated products

Products that are integrated with Network Performance Insight 1.3.1:

Cassandra
It is available as a microservice that can be installed along with other microservices in Network Performance Insight. All the inventory metadata is stored in Cassandra.

Jazz® for Service Management
Dashboard Application Services Hub provides visualization and dashboard services in Jazz for Service Management. It has a single console for administering IBM products and related applications. Visualization for Network Performance Insight is federated into Dashboard Application Services Hub.

IBM Tivoli Network Manager IP Edition
Tivoli Network Manager provides first-level device discovery and polling of some standard SNMP metrics.

Tivoli Netcool/OMNIbus component of IBM Netcool Operations Insight
Netcool Operations Insight is powered by the fault management capabilities of IBM Tivoli Netcool/OMNIbus. In Network Performance Insight, V1.3.1, Tivoli Netcool/OMNIbus is an important part of the solution for monitoring the network threshold violations.

Related information
IBM Network Performance Insight on IBM Knowledge Center
Hortonworks Data Platform
HDFS Architecture
Apache Hadoop YARN
Apache Kafka
Apache Zookeeper
IBM Networks for Operations Insight

IBM Community

Connect, learn, and share with professionals and product support technical experts who provide their perspectives and expertise.

Access the IBM Network Performance Insight community. Use IBM Community in the following ways:
• Become involved with transparent development, an ongoing, open engagement between other users and IBM developers of Tivoli products. You can access early designs, sprint demonstrations, product roadmaps, and prerelease code.
• Connect one-on-one with the experts to collaborate and network about Tivoli and the Network and Service Assurance community.
• Read blogs to benefit from the expertise and experience of others.
• Use wikis and forums to collaborate with the broader user community.

**Network Performance Insight technical training**

For Tivoli technical training information, see the following Network Performance Insight Training website at https://tnpmsupport.persistentsys.com/updated_trainings.

**Support information**

If you have a problem with your IBM Software, you want to resolve it quickly. IBM provides the following ways for you to obtain the support you need:

**Online**

**IBM Support Assistant**
The IBM Support Assistant is a free local software serviceability workbench that helps you resolve questions and problems with IBM Software products. The Support Assistant provides quick access to support-related information and serviceability tools for problem determination. To install the Support Assistant software, go to https://www.ibm.com/software/support/isa.

**Troubleshooting Guide**
For more information about resolving problems, see the problem determination information for this product.

**Conventions used in this publication**

Several conventions are used in this publication for special terms, actions, commands, and paths that are dependent on your operating system.

**Typeface conventions**

This publication uses the following typeface conventions:

**Bold**
- Lowercase commands and mixed case commands that are otherwise difficult to distinguish from surrounding text
- Interface controls (check boxes, push buttons, radio buttons, spin buttons, fields, folders, icons, list boxes, items inside list boxes, multicolumn lists, containers, menu choices, menu names, tabs, property sheets), labels (such as Tip:, and Operating system considerations:)
- Keywords and parameters in text

**Italic**
- Citations (examples: titles of publications, diskettes, and CDs)
- Words defined in text (example: a nonswitched line is called a point-to-point line)
- Emphasis of words and letters (words as words example: "Use the word that to introduce a restrictive clause."); letters as letters example: "The LUN address must start with the letter L.")
• New terms in text (except in a definition list): a view is a frame in a workspace that contains data.
• Variables and values you must provide: ... where myname represents....

**Monospace**
• Examples and code examples
• File names, programming keywords, and other elements that are difficult to distinguish from surrounding text
• Message text and prompts addressed to the user
• Text that the user must type
• Values for arguments or command options

**Bold monospace**
• Command names, and names of macros and utilities that you can type as commands
• Environment variable names in text
• Keywords
• Parameter names in text: API structure parameters, command parameters and arguments, and configuration parameters
• Process names
• Registry variable names in text
• Script names
Chapter 1. Discovering the network

Network discovery process gathers information about resources on your network. Make sure that you always have the most up-to-date inventory of the discovered resources and resource types.

Discovery in Network Performance Insight V1.3.1 complements the discovery from Tivoli Network Manager.

Network Performance Insight collects additional metadata that is related to Performance Metric OOTB Device Support metrics. All the information is stored in database. Tivoli Network Manager Collector Service is primary microservice that is used in discovery. Discovery formulas and the required MIB files are provided for discovery operations.

Discovery-related files and folders

Install the technology pack content that is bundled with Network Performance Insight installation media. The content is distributed in different microservices and used for both discovery and polling operations by Network Performance Insight.

All the content related to discovery process is available in Tivoli Network Manager Service and is distributed as follows:

- `/opt/IBM/npi/npi-itnm-collector/discovery/`
  - device
    - Contains the `system-objectid.discovery` file.
  - content/
    - Contains a copy of the `system-objectid.discovery` file.
  - `<vendor>/vendor-specific discovery formula files`
  - `<vendor>/mibs/vendor-specific MIB files`

Note: When Network Performance Insight is installed, `system-objectid.discovery` file is available in both locations.

Discovery formulas

Predefined discovery formulas that are available in the technology pack are used by Network Performance Insight to discover the vendor-specific devices and their resources based on the OIDs from their associated MIB files.

Typical content of a vendor-specific discovery formula is as follows:

```
when resource.type = "device" and resource.sysobjectid like "1.3.6.1.4.1.9"
select 'environment' as type,index,ciscoenvmontemperaturestate,
ciscoenvmontemperaturethreshold
as CiscoEnvMonitorCiscoTemperatureThreshold,
ciscoenvmontemperaturestatusindex
as envMonTempIndex from CiscoEnvMonMib.ciscoEnvMonTemperatureStatusTable
where ciscoenvmontemperaturestate !=5
set vendor = "Cisco"
set name = context.host + "_TemperatureTestPoint:<" + resource.index + ">"
```

Content of the `system-objectid.discovery` file is as follows:

```
when resource.type = "unknown" and resource.ipAddress is not ""
```
MIB files
All vendor-specific and dependent standard MIB files that are required for the predefined formulas are available and installed with the pack content.

Discovery process
Discovery is handled by both Tivoli Network Manager and Network Performance Insight and are complementary. Discovered devices and their resources are stored in Cassandra database.

During discovery, Tivoli Network Manager discovers the configured SNMP devices and Network Performance Insight discovers their resources from the devices. As these resources respond, their addresses and properties are stored in the database for use in the analysis phase. The analysis phase stores the resource information.

Stages in discovery
Discovery in Network Performance Insight is done in two stages.

• Typically, first-level discovery is done by Tivoli Network Manager where the configured devices are discovered and device IP addresses and their credentials are pulled by Tivoli Network Manager Collector Service via Kafka Connect.

  Note: Discovery for interfaces and IP SLA - enabled devices is handled by Tivoli Network Manager alone.

• The second-level discovery is performed by Network Performance Insight based on the device IDs of the discovered devices. Only device entities that are referred to as resources and their properties are discovered by Network Performance Insight. Network Performance Insight discovers the vendor-specific resources that are associated with the devices and stores the Inventory data in Cassandra.. Typically, discovery by Network Performance Insight is limited to resources for collecting Performance Metric OOTB Device Support metrics.

In Rapid SNMP device onboarding scenario, you can create your own discovery formulas, package and install them to start the discovery of both devices and their resource types independent of Tivoli Network Manager.

Important: Do not modify the preinstalled discovery files that are supplied by technology pack.

Data flow during discovery is diagrammatically represented as follows:

1. Tivoli Network Manager (ITNM) discovers SNMP, IP SLA enabled devices, Interfaces, and configured probes.
2. Tivoli Network Manager Collector Service pulls SNMP devices and their credentials from ITNM via the Kafka Connect JDBC connection.
3. Tivoli Network Manager Collector Service writes the device discovery information to Kafka.
4. Tivoli Network Manager Collector Service runs the predefined discovery formulas to obtain the resources on the discovered devices.
5. Tivoli Network Manager Collector Service writes the resource information such as resource ID and properties to Kafka.
6. Discovered resources information is retrieved from Kafka and stored in Cassandra.

**Discovered resources and their IDs**

When a device is discovered, an ID is generated by Tivoli Network Manager. Network Performance Insight inherits the device ID and discovers the resources that are associated with the device and performs the following tasks:

- `system-objectid.discovery` file is run to obtain the `sysObjectId` of the device.

  `sysObjectId` is the vendor's identification number of OID of an SNMP-managed object type. It represents the type of device and can also indicate the model number. It uses dotted decimal format. For example, some vendor IDs are as follows:

<table>
<thead>
<tr>
<th>Vendor</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco</td>
<td>1.3.6.1.4.1.9</td>
</tr>
<tr>
<td>Huawei</td>
<td>1.3.6.1.4.1.2011</td>
</tr>
<tr>
<td>Juniper</td>
<td>1.3.6.1.4.1.2636</td>
</tr>
<tr>
<td>Juniper Networks/Unispher</td>
<td>1.3.6.1.4.1.4874</td>
</tr>
</tbody>
</table>

  For more information, see IANA-registered Private Enterprise Numbers.

- All the discovery files that match with the same `sysObjectId` are run to obtain the resources from those devices.

- The discovered resources are assigned an ID and stored in the inventory data in Cassandra.

  Before these resources are stored, a validation check or reconciliation is done based on the resource name. The resource name is expected to be an invariant field and it is used to compare if the resource is a rediscovered one. If there is any change to the resource, the record is updated. The status is set to U in the tables. Otherwise, it is ignored as an existing resource.

  During a scheduled discovery, if some existing resources for a device are not discovered, those resources are deleted and the status is set to D in the tables.

- If a device is deleted from Tivoli Network Manager system, during Network Performance Insight scheduled discovery, reconciliation is done at device level and the deleted device, it's resources, and properties are removed from inventory data in Cassandra.

**Resource types**

When you install the required technology packs, the resource types are displayed for all types of devices in the Resource Type page in System Configuration. The resource types and their polling intervals are stored in the RESOURCE_TYPE configuration table.

See Configuring resource types section in Installing and Configuring IBM Network Performance Insight.

During discovery, Tivoli Network Manager Collector does the following tasks:

- Checks if the discovered resource type is available in the configuration table or not.
- If it is available, it is written to inventory data in Cassandra.
- If the resource type is not available, the record is dropped.
High scale capability for Tivoli Network Manager Collector Service

High scale capability for the collector is automatically turned on if the following conditions are fulfilled:

• If the path specified in the `entity.discovery-content-path` setting exists in your file system.
• Only one discovery definition for producing device resource is defined.
• At least one discovery definition is available besides the system object ID.

You might see the following message in the `/var/log/npi-itnm-collector.log` file:

Collector started with Highscale Entities Polling enabled

Discovery methods

The two types of discovery methods that are used by Network Performance Insight for your network. Predefined discovery formulas are used in discovering the network devices and their resources.

Ad hoc discovery

Whenever a new device is discovered by Tivoli Network Manager and the device ID is returned to Tivoli Network Manager Collector Service, Network Performance Insight runs the discovery on these devices to get resources and their properties.

Scheduled discovery

You can schedule a full discovery based on the configuration settings on Ambari for `collector.itnm.entity.import-interval` parameter. By default, this interval is one day to indicate that once in a day, a batch discovery is performed on the full list of devices and their resources. When the discovery is run on the full list of devices and their resources, reconciliation is performed to check if the resources must be added, updated, or deleted based on the existing information.

Note: If the Tivoli Network Manager Collector Service is restarted for any reason, the scheduled discovery is started at that point.

Configuring the discovery

Configure discovery from Ambari web interface by using some parameters that govern how the discovery is performed.

Procedure

1. Log in to Ambari user interface on the node to restart the service as follows:

   Use the following default URL:
   
   `http://<myserver.ibm.com>:8080`

   The default user name is `admin`, and the default password is `admin`.

2. Click `Services` > `NPI` > `Configs` > `Advanced`.

3. Expand the `Advanced npi-env` pane and add the following lines in `content` text area:

   ```
   collector.itnm.entity.discovery-content-path = "/opt/IBM/npi/npi-itnm-collector/discovery/content"
   collector.itnm.entity.import-interval = 1d
   ```

   Table 2. Discovery configurations

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>collector.itnm.entity.discovery-content-path</code></td>
<td><code>/opt/IBM/npi/npi-itnm-collector/discovery/content</code></td>
<td>Default path where the Technology Pack content is installed.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>collector.itnm.entity.import-interval</td>
<td>1 day</td>
<td>By default, discovery is scheduled to look up the newly discovered devices from Tivoli Network Manager. Everyday, Network Performance Insight gets the full list of discovered devices from Tivoli Network Manager via Kafka Connect.</td>
</tr>
</tbody>
</table>

### Optional: Adding and deleting resource types

The resource types that are discovered are displayed on the Resource Type configuration page in read-only mode. You cannot add or delete the resource types from the page.

#### About this task

Use this information to control the resource types that are available in the database and also on the Resource Type configuration page. You can list, add, or delete the resource types by using the `/opt/IBM/basecamp/basecamp-inventory/bin/content-manager` script as root user.

#### Procedure

1. List all the resource types in the installed technology packs and their status by using the following command:

   ```bash
cd /opt/IBM/basecamp/basecamp-inventory
./bin/content-manager list
```

2. At the prompt, enter the following inputs:

   - **NPI UI Host**: `<myserver.ibm.com>`
     - Host name where the UI Service is available.
   - **NPI Username**: npiadmin
   - **NPI Password**: netcool
     - Password for npiadmin user
   - **NPI Port**: 9443
     - https port on which Network Performance Insight application console can be accessed.

   You can see the following output:

   ```
   <myserver.ibm.com> 9443 npiadmin netcool
device               ADDED
   interface            ADDED
   probe                ADDED
   fan                  ADDED
   memory               ADDED
   card                 ADDED
   powerSupply          ADDED
   cpu                  ADDED
   chassis              ADDED
   temperature          ADDED
   wirelessController   ADDED
   channel              ADDED
   ssid                 ADDED
   ap                   ADDED
   radioSlot            UNAVAILABLE
   environment         NEW
   ```
Note:

- All the resource types that are available in the Resource Type configuration page are displayed by this command. The status of these resource types is shown as ADDED.
- The status of the resource types that have the model files from the installed technology packs but are not displayed on the Resource Types page is shown as NEW. It is applicable to scenarios where you have installed new technology packs.
- The status of the resource types that do not have the associated model files from the technology packs but are still displayed on the Resource Type configuration page are shown as UNAVAILABLE. It is applicable to scenarios where you have deleted some installed technology packs.

3. Add a resource type by using the following command:

```bash
cd /opt/IBM/basecamp/basecamp-inventory
./bin/content-manager add
```

All the resource types that have the associated model files from your installed technology packs but are not displayed on the Resource Type configuration page are added by this command. The status of these resource types is changed to ADDED from NEW.

4. Delete a resource type by using the following command:

```bash
cd /opt/IBM/basecamp/basecamp-inventory
./bin/content-manager delete
```

All the resource types that do not have the associated model files are removed from the Resource Type configuration page by this command.

Troubleshooting discovery

Device caching and synchronization are built-in mechanisms to avoid discovering the same device twice. You can also troubleshoot discovery by monitoring discovery events in the log file.

**Device caching**

After a device is discovered either by ad hoc discovery or scheduled discovery, it is cached for 30-minutes. During this period, discovery cannot be run on the device again. Device caching prevents the discovery to be run on the same device twice.

**Synchronization between credential record and device information**

If the Tivoli Network Manager Collector Service receives the record with device parent ID before the device credentials or vice-versa, it loops back the record 10 times with an interval of one minute. It waits for the credential information, failing which, it drops the record with a warning message.

**Log files associated with discovery**

Monitor the `npi-itnm-collector.log` file that is available in `/var/log/npi-itnm-collector.log`, which is a symbolic link to `/opt/IBM/npi/npi-itnm-collector/logs/npi-itnm-collector.log`. 
Chapter 2. Polling the network

Polling is for SNMP metric collection from the devices in your network and to store the data in the database. You can collect the metrics from different devices and entity types based on the data in the Management Information Base (MIB) variables of the devices.

About this task
Typically, network polling for resources is performed every 300 seconds, which is the default polling interval.

High-level tasks in polling the network in Network Performance Insight are as follows:
• Scoping
• Polling interval

Procedure
1. Install the Technology Pack content that comes with the predefined formulas, metrics, and MIB files.

   Network Performance Insight supports SNMP metrics, vendor-specific IP SLA metrics, and device health metrics for Cisco, Huawei, and Juniper devices. Apart from using the predefined metrics, you can also create or modify metrics and formulas. For more information, see Chapter 3, “Rapid SNMP device onboarding,” on page 13.

   For more information about installing the Technology Pack, see Installing and Configuring IBM Network Performance Insight.

2. Optional: Configure the polling interval from Polling Configuration page under System Configuration.

   By default, polling is initiated once in every 300 seconds. If you want to set a different value, use the Polling Configuration page.

   For more information, see Configuring metric polling interval section in Installing and Configuring IBM Network Performance Insight.

3. Configure the poll definitions for the resources to be polled.

Configuring the metric polling interval

Network polling depends on the polling formulas and metrics that are derived from the Technology Pack content, polling interval that can be configured on the Polling Configuration page, and polling scope.

About this task
Polling interval defines the frequency of polling and it can affect the polling performance. List of resource types and their resources are populated on this page from Inventory schema tables based on the available Technology Pack content.

Procedure
1. Click Console Integrations in the navigation bar and select Polling Configuration under System Configuration.

   You can see the following tabs:
   • Resource Config
Contains a list of all the resource types in the installed Technology Packs content and their polling intervals.

- **Entity Config**

  Contains a list of all the resources in the installed Technology Packs content and their polling intervals. You can also add more resources and set the polling interval.

2. Click the **Resource Config** tab.

3. Select a resource type from the table and click the **Edit** button ( ).

4. Specify the required polling interval for the resource type and click **Ok**.

   The default polling interval is 300 seconds.

   **Important:**
   - The polling interval for the resource type **Probe** cannot be configured from this page. Set the polling interval for probe on the device itself.
   - If you set polling interval to zero for a resource type, then polling from the resources for that resource type is stopped.

5. Click **Entity Config** tab.

6. Select a resource and click the **Edit** button ( )

7. Or, click **Edit** in the **Actions** column.

8. Specify the required polling interval for the resource and click **Ok**.

   Resource interval setting from the **Entity Config** page takes precedence over the resource type setting on the **Resource Config** page.

9. Click **Clear** in the **Actions** column to clear the polling interval setting on the selected resource.

---

**SNMP metric collection scope**

Scoping is used to define the zones in the network that you want to include for metric data collection. You can limit the collection from specific devices and IP ranges. In Network Performance Insight multi-host setup, you can use the scoping function to partition the list of resources to be polled by a specific host.

In Network Performance Insight, scoping is done with the help of command-line tool `snmp-scoping.sh` that is available in `/opt/IBM/basecamp/basecamp-installer-tools/snmp` directory.

**Resource scoping**

By default, metric collection scoping is disabled for all devices and no resources are configured for metric collection. You can manually define the resource scoping for each node in your network. It can then start SNMP polling for metric collection.

**About this task**

You can scope a single node or multiple nodes and the resource types on the nodes for metric collection.

**Note:** Run the `snmp-scoping.sh` script from Ambari server.

**Procedure**

Usage of scoping function.

1. Use the scoping function with the following commands:

   ```bash
   cd /opt/IBM/basecamp/basecamp-installer-tools/snmp
   ./snmp-scoping.sh
   ```

   You can see the usage of the function call as follows:
where:

- `<host_name_FQDN>` is the Fully Qualified Domain Name of the Network Performance Insight host in your cluster on which you want to scope the collection.
- `<scoping expression>` is the filtering options that you want to use to restrict the scoping. See "Scoping expressions" on page 10.

Listing the existing scopes.

2. To list the available scopes, run the following commands:

   ```
   cd /opt/IBM/basecamp/basecamp-installer-tools/snmp
   ./snmp-scoping.sh list
   ```

   For example, you can see existing scopes as follows:

   ```
   npi-<myserver.ibm.com> :
   { "formula.entity-scope" : "resource.type == 'interface' || resource.type == 'device'
   || resource.type == 'physicalcard'", }
   npi-<myserver.ibm.com> :
   { "formula.entity-scope" : "resource.agentIp == '10.55.239.235'" }
   ```

   **Note:** You can restrict the scope listing that is set on specific host by specifying the `<host_name_FQDN>` parameter.

Enabling polling on a specific Network Performance Insight host.

3. To enable polling on a specific node, run the following commands:

   ```
   cd /opt/IBM/basecamp/basecamp-installer-tools/snmp
   ./snmp-scoping.sh set <host_name_FQDN> true
   ```

Disabling polling on a specific Network Performance Insight host.

4. To disable polling on a selected host, run the following commands:

   ```
   cd /opt/IBM/basecamp/basecamp-installer-tools/snmp
   ./snmp-scoping.sh set <host_name_FQDN> false
   ```

Setting scope per Network Performance Insight host.

5. To set a scope for a node, run the following commands:

   ```
   cd /opt/IBM/basecamp/basecamp-installer-tools/snmp
   ./snmp-scoping.sh set <host_name_FQDN> <scoping expression>
   ```

Retrieving all the resources that can be polled by a specific scoping expression on a specific Network Performance Insight host.

6. To get all the resources that can be polled by a scoping expression on a host, run the following commands:

   ```
   cd /opt/IBM/basecamp/basecamp-installer-tools/snmp
   ./snmp-scoping.sh test <host_name_FQDN> <scoping expression>
   ```

Resources are filtered based on the scoping expression and the list of resources that can be polled by the scoping expression on the node are returned.

7. Restart Formula Service and on the node where the metric collection scope is set by using the following steps:

   a) Log in to Ambari user interface on the node to restart the service as follows:

   Use the following default URL:
   http://<myserver.ibm.com>:8080
   The default user name is admin, and the default password is admin.
b) Click **Services > NPI**.
c) Click **Service Actions > Restart Formula Services**.

### Scoping expressions

Use this information to see some example scoping expressions that can be used to set your scoping.

- **The functions for restricting the resource polling by IP address range and an array of IP addresses.** You can use `range` and `inArray` (an array of comma-separated list of IP addresses) functions:

  ```plaintext
  "range(resource.agentIp, '<start_IP_address>', '<end_IP_address>')"
  
  "inArray(resource.agentIp, ['<IP_address1>', '<IP_address2>', '<IP_address3>]')"
  
  **Examples:**
  
  "range(resource.agentIp, '10.55.239.57', '10.55.239.77')"
  
  "inArray(resource.agentIp, ['4.10.110.46', '4.50.100.23', '4.20.45.113'])"
  
- **Polling all resources that belong to a device or agent IP address.**

  "resource.agentIp == '<IP_address>'"

- **Polling all resources that belong to a resource type:**

  "resource.type == 'interface'"

**Note:** Some resource types based on vendors are as follows:

- interface
- probe
- device
- card
- cpu
- memory
- chassis

### Enabling and disabling formulas

Currently, the formulas that are available in the built-in technology packs are more than the ones that are used in Network Performance Insight Dashboards. By default, the formulas that are not required for data visualizations in dashboards are disabled by appending an `_` to the formula name. For example, `Probe.HTTP.Transaction.Succeeded.Percent.formula_`.

**About this task**

You can enable or disable the metrics to be collected and displayed in the dashboards and thereby control the system performance and resource utilization. Make sure to install all the required technology packs so that the required metrics are enabled.

Use this information to control the metric polling by enabling or disabling the metrics by using the `/opt/IBM/npi/npi-formula/bin/content-manager` script as root user.
## Procedure

1. List all the formulas in the installed technology packs and their status by using the following command:

```bash
cd /opt/IBM/npi/npi-formula
bin/content-manager list
```

You can see the following output:

<table>
<thead>
<tr>
<th>Metric Name</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>CiscoClassBasedQos/Class.Policing.Conformed.Throughput.bps</td>
<td>ENABLED</td>
</tr>
<tr>
<td>CiscoClassBasedQos/Class.Policing.Exceeded.Throughput.bps</td>
<td>ENABLED</td>
</tr>
<tr>
<td>CiscoClassBasedQos/Class.Policing.Violated.Throughput.bps</td>
<td>ENABLED</td>
</tr>
<tr>
<td>cisco_ipsla/tests/Probe.Duplicate.Poll.Count</td>
<td>DISABLED</td>
</tr>
<tr>
<td>cisco_ipsla/tests/Probe.missed.count</td>
<td>DISABLED</td>
</tr>
<tr>
<td>cisco_ipsla/tests/Probe.test-availability.percent</td>
<td>DISABLED</td>
</tr>
<tr>
<td>cisco_ipsla/tests/Probe.Tests.Missed.Count</td>
<td>DISABLED</td>
</tr>
<tr>
<td>cisco_ipsla/tests/Probe.Tests.Test.Availability.Percent</td>
<td>DISABLED</td>
</tr>
<tr>
<td>cisco_ipsla/tests/Probe.Tests.Test.Count</td>
<td>DISABLED</td>
</tr>
<tr>
<td>cisco_ipsla/voip/Probe.VOIP.ICPIF</td>
<td>DISABLED</td>
</tr>
</tbody>
</table>

2. Enable a metric by using the following command:

```bash
cd /opt/IBM/npi/npi-formula
bin/content-manager enable <formula_ID>
```

Where, `<formula_ID>` is a combination of group subdirectory path and metric name.

**Note:** You must use the subdirectory structure for the metric that you want to enable.

For example:

```bash
cd /opt/IBM/npi/npi-formula
bin/content-manager enable MIB-II/IP.Received.pps
```

3. Disable a metric by using the following command:

```bash
cd /opt/IBM/npi/npi-formula
bin/content-manager disable <formula_ID>
```

Where, `<formula_ID>` is a combination of group subdirectory path and the metric name.
Troubleshooting network polling

To troubleshoot network polling, monitor the polling events in Formula Service log files.

About this task
Monitor the npi-formula.log file that is available in /var/log/npi-formula, which is a symbolic link to /opt/IBM/npi-formula/logs/npi-formula.log. The npi-formula.log file shows the following events:
- All the initial poll definitions
- Changes to the existing definitions
- New poll definitions

Verifying the scope from Ambari

After you set the scope for SNMP metric collection, you can verify the scope from Ambari.

About this task

You can view the existing scope for metric collection from Ambari in two places.

Procedure
1. Log in to the Ambari server dashboard.
   Use the following default URL:
   http://<myserver.ibm.com>:8080
   The default user name is admin, and the default password is admin.
2. Click Services > NPI > Configs > Manage Config Groups.
   You can see the list of scoping that is available for the cluster node in Manage NPI Configuration Groups page.
3. To see the details in a scope, click the scope name on the left pane and click # properties.
   You can see the poll definition that is set in the scope in the Properties window.
   Note: Preferably, use the command-line scoping function to modify any poll definition.
4. You can also see the Kafka topic names.
   a) Click Services > NPI > Configs > Advanced > Custom npi-conf.
      You can see the following scope data according to the scoping that is set:
      • formula.entity-scope
      • snmp.consumer-group.suffix
      • snmp.npi.topic.data
      • snmp.npi.topic.definitions
Chapter 3. Rapid SNMP device onboarding

Rapid SNMP device onboarding is introduced to bring new devices such as routers, switches, and servers into a network environment smoothly and seamlessly. Accomplishing device onboarding accurately and consistently is critical to any enterprise.

An SNMP device is a device that is managed by using the Simple Network Management Protocol (SNMP). Rapid onboarding for new SNMP devices that are introduced in the network can be completed within 1 day. Within this period, the required discovery formulas, collection formulas, and metrics can be created and deployed for Network Performance Insight to start discovery and polling.

Rapid SNMP device onboarding solutions

Rapid SNMP device onboarding can be achieved with the help of Technology Pack Development Tool that is provided free of cost for Network Performance Insight customers.

You can do the following tasks in this solution:

• Create new discovery formulas.
• Create new collection formulas.
• Create new metrics.
• Package the custom Technology Pack content.
• Deploy the custom Technology Pack on Network Performance Insight system to start discovery and polling.

Components used in Rapid SNMP device onboarding:

Technology Pack Development Environment

For more information about SNMP formula language, see IBM Network Performance Insight: References
Technology Pack Development Tool

Technology Pack Development Tool is a command-line tool to design and develop Technology Pack that can be deployed in Network Performance Insight system. The content can then be used to discover and poll the resources from newly on-boarded devices.

Prepackaged Technology Pack content

Network Performance Insight V1.3.1 has the prepackaged Technology Pack content that can be used to discover the resources to collect the device health metrics that are termed as Performance Metric OOTB Device Support metrics.

Devices are discovered by Tivoli Network Manager as first-level discovery and resources from these devices are discovered and polled by Network Performance Insight to collect the device health metrics.

With the help of the Technology Pack Development Tool, you can create the following artifacts that are required to develop a Technology Pack that can be later deployed in the Network Performance Insight system:

• Discovery formulas
  Discovery formulas are used while discovering and analyzing the network. Discovery formulas are used against managed nodes or hosts only and their resource types and are designed to return a list of results.

• Collection formulas
  Collection formulas are used to collect information about the status of various devices in the network during polling. These formulas are applied against a resource type or managed item in the host to produce a result (numeric) that is saved in the database.

• Metrics
  A metric is a single data value, identified by the resource and displayed in a report.

All the required MIB files must be bundles and packaged.

Important: Do not use this tool to customize the built-in Technology Pack content that is provided with Network Performance Insight.

Overview of the Technology Pack Development Tool tasks

• Provides the development environment to run the various command-line tools. The following command-line tools are available:
  – Discovery tool
  – SNMP binding tool
  – Formula tool
  – SNMP MIB tool

• Validates the syntax during the development phase.

• Controls the versioning.

Process flow for creating a technology pack by using the Technology Pack Development Tool.
Software specifications for Technology Pack Development Tool

- Currently, the tool is supported on RHEL 7.x systems.
- Requires Open JDK x86_64 V1.8.0.

Installing the tool

Installation of the Technology Pack Development Tool is simple and fast.

Procedure

1. Download the latest version of the Technology Pack Development Tool from Network Performance Insight IBM Community from here:
   Rapid Device Onboarding - Technology Pack Development Tool
2. Extract the media to a location of choice with the following command:

   ```
   cd /<pack_dev_tool>
   $ tar zxvf npi-tpdt-0.5.0.0.tar.gz
   ```

   Where `<pack_dev_tool>` is the directory where you have extracted the tool media.

   You can see the following directories and files:
   - `bin`
     - device-discovery-tool
     - pack-tool
     - snmp-binding-tool
     - snmp-formula-tool
     - snmp-mib-tool
   - `lib`
Preparation of your environment

Use this information to understand the steps required to prepare the environment for your Technology Pack development.

About this task

Perform the following tasks:

1. “Creating a Technology Pack project” on page 16

A workspace that contains all the Technology Pack content is required from where you can bundle the content later.

2. “Validating the MIB files” on page 17

Copy and validate the required standard and prerequisite MIB files that are required for the Technology Pack content.

Creating a Technology Pack project

Create a workspace directory to keep the Technology Packs project files that are developed.

About this task

Use the pack_tool script to create a workspace for your project.

For more information about the pack_tool command usage, see IBM Network Performance Insight: References.

Procedure

1. Create a workspace directory for the workspace with the following command:

   ```
   cd /<pack_dev_tool>
   $ mkdir workspace
   ```

   Where, workspace is the project directory.

2. Optional: You can also create a softlink to the repository that you are using directly.

   For example, to convert your Git repository as the workspace directory to develop the packs, follow these commands:

   ```
   $ cd ~/git/
   $ git clone git@<repo_server.ibm.com>:<my_repo>/<my_file>.git
   $ cd ~/<pack_dev_tool>
   $ ln -s ~/git/<my_pack> workspace
   ```

   A new workspace by name <my_pack> is created that contains the new Technology Pack with the same name as the workspace.

3. Run the following command:

   ```
   cd /<pack_dev_tool>
   bin/pack-tool new <my_pack>
   ```

   New pro pack by name <my_pack> is created that contains the new Technology Pack with the same name as the workspace.
What to do next
Verify that the Technology Pack with the name `<my_pack>` is created as follows:

```
$ find workspace/<my_pack>/
```

Currently, you can ignore the `inventory` directory and its subdirectories.

**Note:** The `pack.properties` file contains the technology pack version. The default is 1.0.0.

### Validating the MIB files
A MIB file contains object definitions, which are organized to groups. Typically, the object definitions in a MIB file are organized in groups, such as System, Interface, or TCP. Use the `snmp-mib-tool` script to view a MIB file source and to validate the content in the MIB files.

#### About this task
The `snmp-mib-tool` script is available in `/<pack_dev_tool>/bin` directory. Follow these steps to validate the MIB files that are required for to develop your Technology Pack content.

#### Procedure
1. Copy all the required standard and prerequisite MIB files to the following directory:
   `/workspace/<my_pack>/snmp/mibs`
2. View the list of MIB files available in your Technology Pack content by using the following command:
   ```
   bin/snmp-mib-tool <my_pack> list
   ```
   You can see the list of MIB files that you have copied in step 1.
3. View a specific MIB file source by using the following command:
   ```
   bin/snmp-mib-tool <my_pack> show <MIB_name>
   ```
   For example:
   ```
   bin/snmp-mib-tool <my_pack> show CISCO-MEMORY-POOL-MIB
   ```
   You can see the content of the CISCO-MEMORY-POOL-MIB file.

### Creating discovery formulas
You can create your own discovery formulas for the resources from the devices discovered by Tivoli Network Manager. Network Performance Insight can then discover those resources.

#### About this task
You can create discovery formulas for new devices and their resources based on their resource types. These discovery formulas can work independent of Tivoli Network Manager for device discovery.
Procedure
1. Copy all the standard and dependent MIB files that are required for the discovery formulas that you plan to create.

Arrange the vendor-specific MIB files by creating sub directories as follows:

- workspace/<my_pack>/snmp/mibs/
- workspace/<my_pack>/snmp/mibs/cisco/CISCO-ENHANCED-MEMPOOL-MIB
- workspace/<my_pack>/snmp/mibs/cisco/CISCO-ENTITY-SENSOR-MIB
- workspace/<my_pack>/snmp/mibs/cisco/CISCO-ENVMON-MIB
- workspace/<my_pack>/snmp/mibs/cisco/CISCO-MEMORY-POOL-MIB
- workspace/<my_pack>/snmp/mibs/cisco/CISCO-PROCESS-MIB
- workspace/<my_pack>/snmp/mibs/cisco/CISCO-QOS-PIB-MIB
- workspace/<my_pack>/snmp/mibs/cisco/CISCO-SMI
- workspace/<my_pack>/snmp/mibs/cisco/CISCO-TC
- workspace/<my_pack>/snmp/mibs/cisco/CISCO-ENTITY-FRU-CONTROL-MIB
- workspace/<my_pack>/snmp/mibs/cisco/INET-ADDRESS-MIB
- workspace/<my_pack>/snmp/mibs/huawei/HUAWEI-ENTITY-EXTENT-MIB
- workspace/<my_pack>/snmp/mibs/huawei/HUAWEI-MIB
- workspace/<my_pack>/snmp/mibs/ietf/IANAifType-MIB
- workspace/<my_pack>/snmp/mibs/ietf/IF-MIB
- workspace/<my_pack>/snmp/mibs/ietf/SNMPv2-CONF
- workspace/<my_pack>/snmp/mibs/ietf/SNMPv2-MIB
- workspace/<my_pack>/snmp/mibs/ietf/SNMPv2-SMI
- workspace/<my_pack>/snmp/mibs/ietf/SNMPv2-TC
- workspace/<my_pack>/snmp/mibs/ietf/BRIDGE-MIB
- workspace/<my_pack>/snmp/mibs/ietf/ENTITY-MIB
- workspace/<my_pack>/snmp/mibs/ietf/HCNUM-TC
- workspace/<my_pack>/snmp/mibs/ietf/HOST-RESOURCES-MIB
- workspace/<my_pack>/snmp/mibs/ietf/IANA-ENTITY-MIB
- workspace/<my_pack>/snmp/mibs/ietf/P-BRIDGE-MIB
- workspace/<my_pack>/snmp/mibs/ietf/SNMP-FRAMEWORK-MIB
- workspace/<my_pack>/snmp/mibs/ietf/UUID-TC-MIB
- workspace/<my_pack>/snmp/mibs/ietf/RFC1155-SMI
- workspace/<my_pack>/snmp/mibs/ietf/RFC1158-MIB
- workspace/<my_pack>/snmp/mibs/ietf/RFC-1212
- workspace/<my_pack>/snmp/mibs/ietf/RFC1213-MIB
- workspace/<my_pack>/snmp/mibs/juniper/JUNIPER-MIBs
- workspace/<my_pack>/snmp/mibs/juniper/Juniper-System-MIB
2. Create the discovery formula file as follows:
   For example, to create a formula file by name, cisco-memorypool.discovery for a Cisco device:

   ```python
   when resource.type = 'device' and resource.sysobjectid like '1.3.6.1.4.1.9'
   select index, ciscomemorypooltype as memoryPoolType, ciscomemorypoolname
   as memoryPoolName, ciscomemorypoolvalid as memoryPoolValid from
   CiscoMemoryPoolMib.ciscoMemoryPoolTable
   where ciscomemorypoolvalid = 1
   set type = 'memory'
   set vendor = 'Cisco'
   set id = context.host + '_MemoryPool<' + resource.index + '>
   ```

3. Save the file in `/workspace/<my_pack>/discovery/<group>` folder. Arrange the discovery formulas in separate directories to avoid conflicts.

   **Note:** All the discovery formulas must have the file extension as `.discovery`.

4. Create all the required formulas to discover devices and their resources.

   **What to do next**

   Validate the content to make sure there are no errors in the formulas.

   For more information about writing custom discovery formulas, see *IBM Network Performance Insight: References*.

   **Running the discovery**

   You can directly run the discovery formulas from the custom Technology Pack by using the device-discovery-tool script.

   **About this task**

   device-discovery-tool is available in the `/<pack_dev_tool>/bin` directory. The script runs all the discovery formulas that are available in the custom Technology Pack that is created.

   The device-discovery-tool is useful in validating the formulas before the custom Technology Pack is deployed in Network Performance Insight system.

   **Procedure**

   Use the following command to run the discovery formulas from the custom Technology Pack that is created:

   ```bash
   $ bin/device-discovery-tool <my_pack> 'snmp://public@<device_IP>:161'
   ```
INFO: Discovered device is Resource [kind: device, name: 127.0.0.1, properties: Set(sysobjectid=1.3.6.1.4.1.2636, name=127.0.0.1, type=device)]
INFO: Found 1 supported definitions
INFO: Topology JSON =
{"resources": [{"type": "chassis", "name": "127.0.0.1_Chassis:<-1><1><0><0>", "properties": {"index": "1.1.0.0", "jnxccontainersdescription": "chassis frame", "jnnoxoperating13index": "0", "jnxccontentsserialno": "S/N TS4821", "jnnoxoperatingl1index": "1", "jnxccontentspartno": "710-013698", "jnnoxoperatingdescription": "midplane", "vendor": "Juniper", "name": "127.0.0.1_Chassis:<-1><1><0><0>", "jnnoxoperatingcontentsindex": "1", "jnxfilleddescription": "chassis frame", "jnxfilledstate": "3", "jnnoxoperatingl2index": "0", "type": "chassis", "jnxccontentsversion": "REV 03", "jnxccontainerslevel": "0", "jnxccontainersview": "1", "jnxccontainersindex": "1", "jnxfilledcontainerindex": "1", "jnxccontentscancontainerindex": "1"}]}], "relations": []}
INFO: Successfully completed discovery, found 1 resource(s)

Note: You can copy the JSON output into any JSON viewer to see the content more effectively. For example:

```json
{
  "resources": [
    {
      "type": "chassis",
      "name": "127.0.0.1_Chassis:<-1><1><0><0>",
      "properties": {
        "index": "1.1.0.0",
        "jnxccontainersdescription": "chassis frame",
        "jnnoxoperating13index": "0",
        "jnxccontentsserialno": "S/N TS4821",
        "jnnoxoperatingl1index": "1",
        "jnxccontentspartno": "710-013698",
        "jnnoxoperatingdescription": "midplane",
        "vendor": "Juniper",
        "name": "127.0.0.1_Chassis:<-1><1><0><0>",
        "jnnoxoperatingcontentsindex": "1",
        "jnxfilleddescription": "chassis frame",
        "jnxfilledstate": "3",
        "jnnoxoperatingl2index": "0",
        "type": "chassis",
        "jnxccontentsversion": "REV 03",
        "jnxccontainerslevel": "0",
        "jnxccontainersview": "1",
        "jnxccontainersindex": "1",
        "jnxfilledcontainerindex": "1",
        "jnxccontentscancontainerindex": "1"
      }
    }
  ]
}
```

Creating collection formulas
You can create your own collection formulas that you want Network Performance Insight to poll and collect the specific device performance metrics.

About this task
You can create custom collection formulas for any type of device and resources with in it.

Procedure
1. Copy all the standard and dependent MIB files that are required for the collection formulas that you plan to create and arrange them in vendor-specific directories to avoid conflicts.

   Note: Discovery and polling operations share the MIB files. So you must copy only those files that are not already available.

2. Generate the binding with all the required MIB files.
For example, create a binding with RFC1213-MIB for a formula that required the MIB as follows:

```
$ bin/snmp-binding-tool <my_pack> generate RFC1213-MIB
```

Generating bindings for mib RFC1213-MIB...
Generating bindings for mib RFC1213-MIB complete.

Class files are generated and arranged in separate MIB folders for all the OBJECT_TYPES in the MIB file.

3. Create the collection formula file as follows:
   For example, to create a formula file by name, interface.inbound.octets.formula.

   ```
   interface.inbound.octets = value(RFC1213_MIB.ifInOctets)
   when resource.type == 'interface'
   ```

4. Save the file in workspace/<my_pack>/snmp/formulas/<group> folder. Arrange the discovery formulas in separate directories to avoid conflicts.

   **Note:** All the collection formulas must have the file extension as .formula. If the file has more than one formula in it, save it as .formulas. As a best practice, create a formula file for a single metric. You cannot use the /opt/IBM/npi/npi-formula/bin/content-manager script to enable and disable formulas on .formulas files.

5. Create all the required formulas to poll the devices and their resources.

**What to do next**

Validate the content to make sure there are no errors in the formulas.

For more information about Writing custom collection formulas, see *IBM Network Performance Insight: References*.

**Running the collection formulas**

You can directly run the custom collection formulas from the custom Technology Pack by using the `snmp-formula-tool` script.

**About this task**

`snmp-formula-tool` is available in the `<pack_dev_tool>/bin` directory. The script runs all the collection formulas that are available in the custom Technology Pack that is created.

The `snmp-formula-tool` is useful in validating and running the formulas before the custom Technology Pack is deployed in Network Performance Insight system.

**Procedure**

1. Use the following command to list all the collection formulas in the custom Technology Pack that is created:

   ```
   $ bin/snmp-formula-tool <my_pack> list
   ```

   Formulas
   - interface.inbound.octets(ifInOctets: RFC1213_MIB.ifInOctets)

2. Use the following command to run the collection formulas from the custom Technology Pack that is created:

   ```
   $ bin/snmp-formula-tool <my_pack> execute
   1/interface/vendor=cisco RFC1213_MIB.ifInOctets=1000,2000,3500,5500
   ```
Executing with interface resource 1[vendor=cisco,agent=1:3030]...
1:3030/1.3.6.1.2.1.2.2.1.10.0[300000]
Calculated 1000.0 at timestamp 1535606392689 for interface.inbound.octets.
Calculated 2000.0 at timestamp 1535606452690 for interface.inbound.octets.
Calculated 3500.0 at timestamp 1535606512690 for interface.inbound.octets.
Calculated 5500.0 at timestamp 1535606572690 for interface.inbound.octets.
Execution complete in 1 seconds.

For example:

- If multiple properties are available in a formula, specify as:

  \[1/\text{interface}/\text{vendor=cisco, name='1.1.1.1\_If<1>}'\]

- If multiple OIDs are available in a formula, specify as:

  \[
  \text{CISCO\_MEMORY\_POOL\_MIB.ciscoMemoryPoolFree}=10, 50 \\
  \text{CISCO\_MEMORY\_POOL\_MIB.ciscoMemoryPoolLargestFree}=20, 40
  \]

**Creating metrics**

You can create your own specific device performance metric definitions that you want Network Performance Insight to poll and collect.

**Procedure**

1. Create the metric file as follows:
   For example, to create a metric file by name, `icmp-out-dest-unreached.metric`:

   ```
   name=icmp.out.dest.unreached
   description="The number of ICMP destination unreachable message sent"
   aliases=[]
   properties=
   ```

2. Save the file in `/my_project/<my_pack>/metrics/<group>` folder. Arrange the discovery formulas in vendor-specific directories to avoid conflicts.

   **Note:** All the metrics must have the file extension as `.metric`.

**What to do next**

Validate the content to make sure there are no error in the formulas.

**Validating the pack content**

As a best practice, test that the syntax of the formulas and metrics to make sure that they work correctly. Use the validate option in the `pack-tool` script.

**About this task**

You can perform this step intermittently during the Technology Pack development or at the end before packaging.

**Procedure**

Run the following command:

- Validating the discovery formulas:

  ```
  bin/pack-tool validate <my_pack>
  ```
Validating `<my_pack>` pack...
Validating inventory models...

Validating discovery...
  - Validating cisco-memorypool.discovery...

Validating metrics...

Validating snmp formulas...
Validating `<my_pack>` pack complete.

• Validating the collection formulas:

  $ bin/pack-tool validate `<my_pack>`

Validating `<my_pack>` pack...
Validating inventory models...

Validating discovery...
  - Validating cisco-memorypool.discovery...

Validating metrics...

Validating snmp formulas...
  - Validating interface.inbound.octets.formula...

Validating `<my_pack>` pack complete.

• Validating the metrics:

  $ bin/pack-tool validate `<my_pack>`

Validating `<my_pack>` pack...
Validating inventory models...

Validating discovery...
  - Validating cisco-memorypool.discovery...

Validating metrics...
  - Validating icmp-out-dest-unreached.metric...

  - Error in `/home/sherpa/sdk/workspace/pack-demo/metrics/icmp-out-dest-unreached.metric`:
/home/sherpa/sdk/workspace/pack-demo/metrics/icmp-out-dest-unreached.metric: 2:
Expecting a value but got wrong token: 'newline' (JSON does not allow unescaped newline in quoted strings, use a backslash escape)
(if you intended 'newline' (JSON does not allow unescaped newline in quoted strings, use a backslash escape) to be part of a key or string value, try enclosing the key or value in double quotes, or you may be able to rename the file .properties rather than .conf)

Validating snmp formulas...
  - Validating interface.inbound.octets.formula...

Validating `<my_pack>` pack complete.

**Note:** The validation error is due to missing double quotation marks in the metric definition. You can fix the errors during validation and rerun.
Packaging the Technology Pack bundle

You can generate the JAR file package of the custom Technology Pack with the content that you developed by using the Technology Pack Development Tool.

About this task

Use the build option in pack-tool script to package the Technology Pack that can be deployed on the Network Performance Insight system.

Procedure

Run the build command as follows:

```
$ bin/pack-tool build <my_pack>
```

Building pack `<my_pack>` [version 1.0.0]...
- Adding file snmp/mibs/cisco/CISCO-ENHANCED-MEMPOOL-MIB...
- Adding file snmp/mibs/cisco/CISCO-ENTITY-SENSOR-MIB...
- Adding file snmp/mibs/cisco/CISCO-ENVMON-MIB...
- Adding file snmp/mibs/cisco/CISCO-MEMORY-POOL-MIB...
- Adding file snmp/mibs/cisco/CISCO-PROCESS-MIB...
- Adding file snmp/mibs/cisco/CISCO-QOS-PIB-MIB...
- Adding file snmp/mibs/cisco/CISCO-SMI...
- Adding file snmp/mibs/cisco/CISCO-TC...
- Adding file snmp/mibs/cisco/CISCO-ENTITY-FRU-CONTROL-MIB...
- Adding file snmp/mibs/cisco/INET-ADDRESS-MIB...
- Adding file snmp/mibs/huawei/HUAWEI-ENTITY-EXTENT-MIB...
- Adding file snmp/mibs/huawei/HUAWEI-MIB...
- Adding file snmp/mibs/ietf/IANAIfType-MIB...
- Adding file snmp/mibs/ietf/IF-MIB...
- Adding file snmp/mibs/ietf/SNMPv2-CONF...
- Adding file snmp/mibs/ietf/SNMPv2-MIB...
- Adding file snmp/mibs/ietf/SNMPv2-SMI...
- Adding file snmp/mibs/ietf/SNMPv2-TC...
- Adding file snmp/mibs/ietf/BRIDGE-MIB...
- Adding file snmp/mibs/ietf/ENTITY-MIB...
- Adding file snmp/mibs/ietf/HCNUM-TC...
- Adding file snmp/mibs/ietf/HOST-RESOURCES-MIB...
- Adding file snmp/mibs/ietf/IANA-ENTITY-MIB...
- Adding file snmp/mibs/ietf/P-BRIDGE-MIB...
- Adding file snmp/mibs/ietf/SNMP-FRAMEWORK-MIB...
- Adding file snmp/mibs/ietf/UUID-TC-MIB...
- Adding file snmp/mibs/ietf/RFC1155-SMI...
- Adding file snmp/mibs/ietf/RFC1158-MIB...
- Adding file snmp/mibs/ietf/RFC-1212...
- Adding file snmp/mibs/ietf/RFC1213-MIB...
- Adding file snmp/mibs/juniper/JUNIPER-MIB...
- Adding file snmp/mibs/juniper/JUNIPER-SMI...
- Adding file snmp/mibs/juniper/Juniper-MIBs...
- Adding file snmp/mibs/juniper/Juniper-System-MIB...
- Adding file snmp/mibs/juniper/Juniper-TC...
- Adding file snmp/mibs/juniper/Juniper-UNI-SMI...
- Adding file snmp/formulas/rfc1213/interface.inbound.octets.formula...
- Adding file discovery/cisco/cisco-memorypool.discovery...
- Adding file pack.properties...

Building pack `<my_pack>` complete.

All the custom content that is available in the `<my_pack>` directory is bundled. The `<my_pack>-1.0.0.jar` file is available in the following directory:

```
$ cd <pack_dev_tool>
$ find build/
build/build/<my_pack>
```
**Deploying the custom Technology Pack**

Deploy the custom Technology Pack in Network Performance Insight system to start using the content to discover and poll the devices and resources. The collected metrics are stored in the database and can be rendered on Network Performance Insight Dashboards.

**About this task**

After the Technology Pack is bundled with the custom content, you can deploy and run discovery and polling from Network Performance Insight Dashboards as usual.

**Procedure**

1. Copy the custom Technology Pack bundle to Network Performance Insight system to a location of your choice.
   
   For example, `<DIST_DIR>`.

2. Install the Technology Pack by using the following commands:

   ```
   cd /opt/IBM/basecamp/basecamp-installer-tools/pack-installer
   ./pack-install.sh <DIST_DIR>/my_pack-1.0.0.jar
   ```

   The `<my_pack>-1.0.0.jar` file that is available in your `<DIST_DIR>` is extracted and the content is distributed to the following directories:

**Discovery formulas**

`/opt/IBM/npi/npi-itnm-collector/discovery/`

The discovery directory has all the collection formulas and their related files.

**Formulas**

`/opt/IBM/npi/npi-itnm-collector/discovery/content`

Contains all the discovery formula files that are arranged in separate vendor-specific directories from the custom Technology Pack.

**MIB files**

`/opt/IBM/npi/npi-itnm-collector/discovery/content/mibs`

Contains all the MIB files that are arranged in separate directories from the custom Technology Pack.

**Collection formulas**

`/opt/IBM/npi/npi-formula/content/`

The content directory has all the collection formulas and their related files.

**Bindings**

`/opt/IBM/npi/npi-formula/content/bindings`

Contains all the MIB object class files that are created by the snmp-binding-tool script.

**Formulas**

`/opt/IBM/npi/npi-formula/content/formulas`

Contains all the collection formula files from the custom Technology Pack.

**MIB files**

`/opt/IBM/npi/npi-formula/content/mibs`

Contains all the MIB files that are arranged in separate directories from the custom Technology Pack.

**Metrics**

`/opt/IBM/basecamp/basecamp-timeseries/content/metrics`

The metrics directory has all the metric files.
Troubleshooting Technology Pack Development Tool

You can use this troubleshooting and support information to troubleshoot problems with Technology Pack Development Tool.

For troubleshooting the usage of Technology Pack Development Tool for creating custom technology pack, see the related information.
This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user’s responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS"
WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO,
THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A
PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in
certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically
made to the information herein; these changes will be incorporated in new editions of the publication.
IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this
publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in
any manner serve as an endorsement of those websites. The materials at those websites are not part of
the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without
incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the
exchange of information between independently created programs and other programs (including this
one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US
Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

The client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM’s future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM’s suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided “AS IS”, without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_.

Trademark

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.
Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of The Minister for the Cabinet Office, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

## Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

### Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

### Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

### Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

### Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED,
INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.