HP Operations Orchestration Software

Software Version: 9.00.05

HP Network Node Manager (i series) Integration

Document Release Date: April 2011

Software Release Date: April 2011

Legal Notices

Warranty

The only warranties for HP 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. HP 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 HP 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 Notices

Trademark Notices

For information on open-source and third-party software acknowledgements, see in the documentation set for this release, Open-Source and Third-Party Software Acknowledgements (3rdPartyOpenNotices.pdf).

On the Web: Finding OO support and documentation

There are two Web sites where you can find support and documentation, including updates to OO Help systems, guides, and tutorials:

- The OO Support site
- HP Live Network

Support

Documentation enhancements are a continual project at Hewlett-Packard Software. You can obtain or update the HP OO documentation set and tutorials at any time from the HP Software Product Manuals Web site. You will need an HP Passport to log in to the Web site.

To obtain HP OO documentation and tutorials

1. Go to the HP Software Product Manuals Web site (*http://support.openview.hp.com/selfsolve/manuals*).
2. Log in with your HP Passport user name and password.

   OR

   If you do not have an HP Passport, click **New users – please register** to create an HP Passport, then return to this page and log in.

   If you need help getting an HP Passport, see your HP OO contact.
3. In the **Product** list box, scroll down to and select **Operations Orchestration**.
4. In the **Product Version** list, click the version of the manuals that you're interested in.
5. In the **Operating System** list, click the relevant operating system.
6. Click the **Search** button.
7. In the **Results** list, click the link for the file that you want.

HP Live Network

For support information, including patches, troubleshooting aids, support contract management, product manuals and more, visit the following site: *https://www.www2.hp.com/*.

This is the **HP Live Network** Web page. To sign in:

1. Click **Login**.
2. On the **HP Passport sign-in** page, enter your HP Passport user ID and password and then click **Sign-in**.
3. If you do not already have an HP Passport account, do the following:
   a. On the **HP Passport sign-in** page, click **New user registration**.
   b. On the **HP Passport new user registration** page, enter the required information and then click **Continue**.
   c. On the confirmation page that opens, check your information and then click **Register**.
   d. On the **Terms of Service** page, read the Terms of use and legal restrictions, select the **Agree** button, and then click **Submit**.
4. On the **HP Live Network** page, click **Operations Orchestration Community.**

The Operations Orchestration Community page contains links to announcements, discussions, downloads, documentation, help, and support.

Note: Contact your OO contact if you have any difficulties with this process.

In OO: How to find Help, PDFs, and tutorials

The HP Operations Orchestration software (HP OO) documentation set is made up of the following:

- Help for Central

  Central Help provides information to the following:

  - Finding and running flows
  - For HP OO administrators, configuring the functioning of HP OO
  - Generating and viewing the information available from the outcomes of flow runs

  The Central Help system is also available as a PDF document in the HP OO home directory, in the \Central\docs subdirectory.

- Help for Studio

  Studio Help instructs flow authors at varying levels of programming ability.

  The Studio Help system is also available as a PDF document in the HP OO home directory, in the \Studio\docs subdirectory.

- Animated tutorials for Central and Studio

  HP OO tutorials can each be completed in less than half an hour and provide basic instruction on the following:

  - In Central, finding, running, and viewing information from flows
  - In Studio, modifying flows

  The tutorials are available in the Central and Studio subdirectories of the HP OO home directory.

- Self-documentation for operations and flows in the Accelerator Packs and ITIL folders

  Self-documentation is available in the descriptions of the operations and steps that are included in the flows.

Table of Contents

Overview of HP Network Node Manager integration

With this integration, administrators can build HP Operations Orchestration (OO) flows that are integrated into HP Network Node Manager i Series (NNMi), and also launch OO flows via the NNMi Event Console.

This document explains how this integration has been implemented and how to launch OO flows from within NNMi. It also explains how the integration's operations communicate between OO and NNMi.

Use cases and scenarios

The following are among the possible use cases for which integration of OO with NNMi is well-suited:

1. To launch an OO flow from within the NNMi console.

   This allows administrators to connect specific events to OO flows. This type of integration is a simple Incident Management/Runbook use case, in which the following takes place:

   a. NNMi detects an error and raises an alarm on the console.
   b. Context-sensitive runbook is launched to remediate the fault.
   c. OO automatically acknowledges the event and runs the runbook.
   d. OO remediates the problem.
   e. OO updates and resets the alarm.
2. To create operations that automate the gathering and processing of NNMi node information.

Installation and configuration instructions

For NNM 7.5, you must install a RAS on your NNM server (Windows) or be able to reach your NNM server by SSH or Telnet (Unix). If integrating to a Unix installation of NNM, you must also update the path to the NNM \bin folder on the steps of your flow. This folder is set correctly for a default Windows installation of NNM.

For NNM 8.1x, you need a RAS that can open up an HTTP or HTTPS command to the port on which the NNM WS-I Web service is running. By default, this is port 8080.

Versions

Operations Orchestration Version	NNMi Version
9.00.05	7.5, 8.10, 9.0, and 9.1

Architecture

NNMi 8.1x

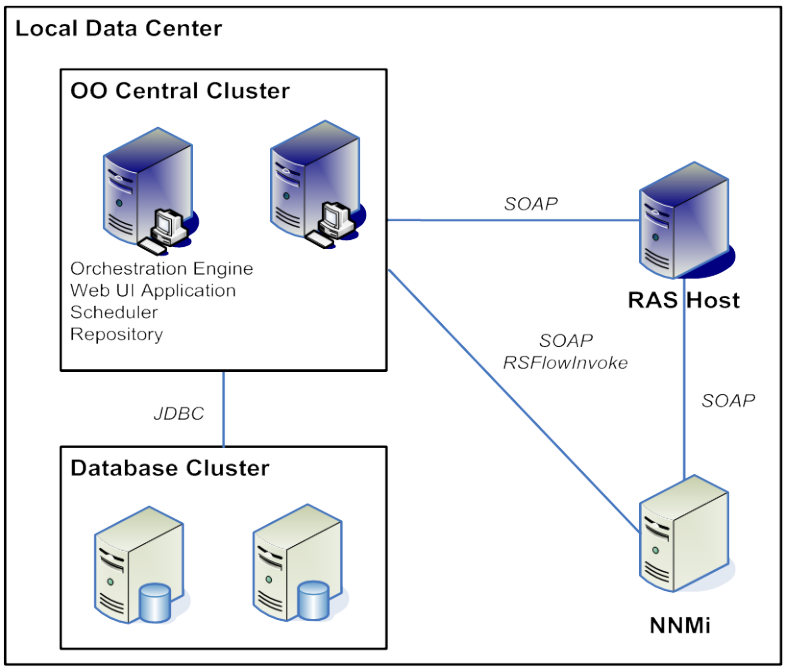

Figure 1 - NNMi 8.10 and later architecture

NNMi 7.5

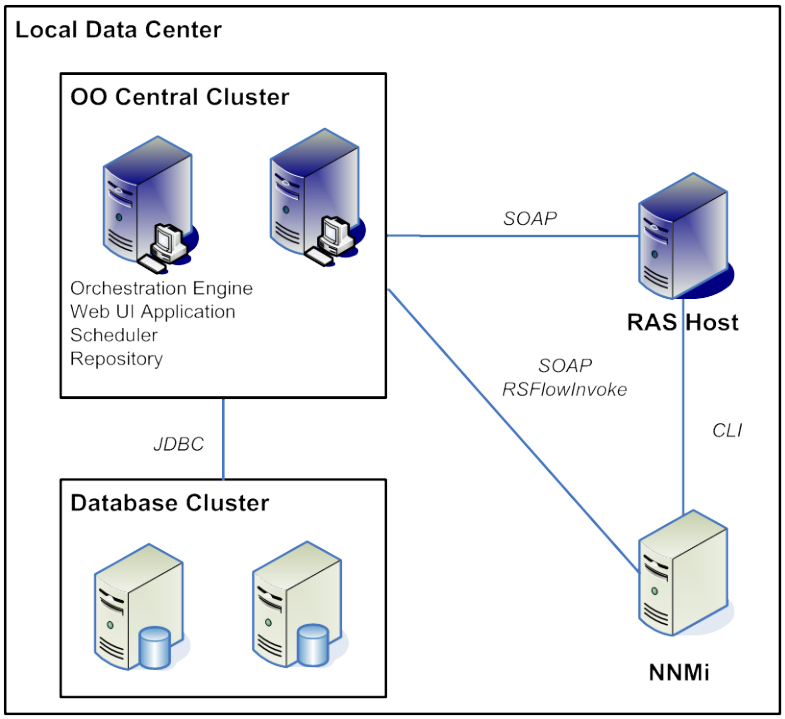

Figure 2 - NNMi 7.5 architecture

HP Network Node Manager integration operation and flow infrastructure

The NNMi integration includes the following operations and flows in the OO Studio Library/Integrations/Hewlett-Packard/Network Node Manager/ folder.

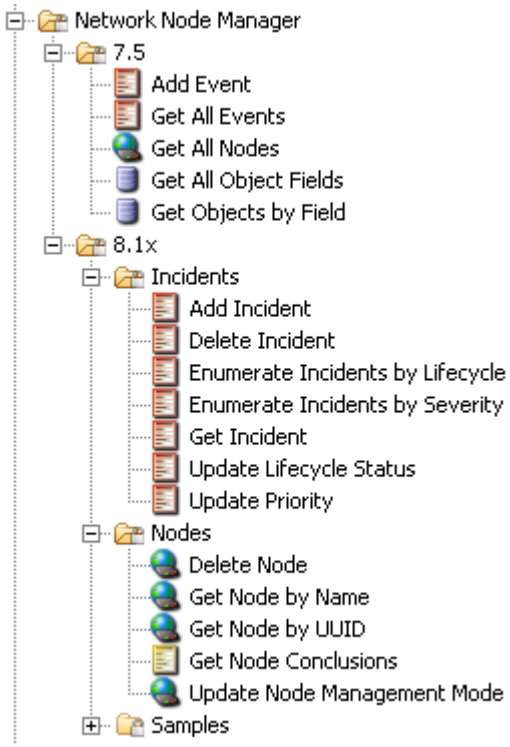

Figure 3 - NNMi integration operation and flow infrastructure

Operation and flow specifics

This section describes the NNMi integration's operations and flows, including any operation- or flow-specific inputs. The flows and operations are grouped first by version:

- 7.5
- 8.10 and later

The 8.1x flows and operations are grouped by their basic functionality:

- Incidents
- Nodes
- Samples

NNM 7.5 has operations and flows for getting lists of events and for adding events. NNM 7.5 also enables a user to get a list of nodes and to read any information from the NNM Database for a given node.

NNM 8.1x has a deeper integration. With the integration's operations, the user can:

- Add, delete, search, and modify NNM incidents.
- Query, delete, and update nodes.

NNMi 7.5 operations and flows

Add Event

The **Add Event** flow adds a new event to NNM.

The operation produces a **Success** response if the operation completes successfully. It produces a **Failure** response if the operation is unable to complete successfully.

Other results are:

stdOut

Contains the output of the command.

The inputs for the operation are:

host

The name or IP address of the NNM host.

username

The username for the host.

password

The password for the host username.

protocol

The protocol to use to connect to the host.

category

The NNM category for the event.

severity

The NNM severity for the event.

node

The NNM server to issue the event against.

oid

The OID (object identifier) of the event.

agent

The agent sending the event.

Get All Events

The **Get All Events** flow retrieves all events that have occurred recently.

The operation produces a **Success** response if the operation completes successfully. It produces a **Failure** response if the operation is unable to complete successfully.

Other results are:

date

A comma-delimited list of the dates when each event occurred.

host

A comma-delimited list of the hosts that sent the events.

message

A comma-delimited list of the messages corresponding to the events.

The inputs for the operation are:

host

The name or IP address of the NNM host.

username

The username for the host.

password

The password for the host username.

protocol

The protocol to use to connect to the host.

minutes

The number of minutes in the past to retrieve events for. All events that occurred in these minutes are returned.

Get All Nodes

The **Get All Nodes** flow retrieves a list of all of the nodes known to the NNM host.

The operation produces a **Success** response if the operation completes successfully. It produces a **Failure** response if the operation is unable to complete successfully.

Other results are:

objectIDs

A comma-delimited list of the retrieved object IDs.

nodeNames

A comma-delimited list of the retrieved node names or IP addresses.

The inputs for the operation are:

host

The name or IP address of the NNM host.

username

The username for the host.

password

The password for the host username.

protocol

The protocol to use to connect to the host.

Get All Object Fields

The **Get All Object Fields** flow retrieves all of the data fields of an NNM object.

The operation produces a **Success** response if the operation completes successfully. It produces a **Failure** response if the operation is unable to complete successfully.

Other results are:

fields

A newline-delimited list of fieldName=fieldValue pairs.

The inputs for the operation are:

host

The name or IP address of the NNM host.

username

The username for the host.

password

The password for the host username.

protocol

The protocol to use to connect to the host.

objectID

The ID of the NNM object to query.

Get Objects by Field

The **Get Objects by Field** flow retrieves a list of NNM objects of a specific field set.

The operation produces a **Success** response if the operation completes successfully. It produces a **Failure** response if the operation is unable to complete successfully.

Other results are:

objectIDs

A newline-delimited list of object IDs.

fieldValues

A newline-delimited list of field values.

The inputs for the operation are:

host

The name or IP address of the NNM host.

username

The username for the host.

password

The password for the host username.

protocol

The protocol to use to connect to the host.

field

The field to query.

attribute

The name of the attribute in the specified field by which to objects are retrieved.

value

The value the attribute must have for the object to be retrieved.

NNMi 8.1x operations and flows

Incidents

Add Incident

The **Add Incident** operation adds a new incident.

Note: This operation sends an event to NNM with the specified name. This may return **Success** without creating an incident if NNM is not configured to create an incident from the specified event name. You can use the returned UUID in follow-on operations, but these operations may fail if the event has not yet been processed. We recommend that you use the **Sleep** operation for at least a few seconds before trying to retrieve the incident to update additional fields.

The operation produces a **Success** response if the operation completes successfully. It produces a **Failure** response if the operation is unable to complete successfully.

Other results are:

returnResult

The universally unique identifier (UUID) of the created incident. For example, `6fa77cce-bbb5-4dc8-a4fb-becb6603f8d6`.

The inputs for the operation are:

nnmProtocol

The protocol to use to connect to the NNM server. The valid values are **HTTP** and **HTTPS**.

nnmHost

The DNS name or IP address of the NNM server.

nnmPort

The number of the port to use to connect to your NNM server.

nnmUsername

The username for NNM authentication.

nnmPassword

The password for NNM authentication.

name

The name of the incident to add.

priority

The priority of the incident. The default setting for assigning a value to this input is a prompt for the user to select the priority from the **NNM Priority** selection list.

sourceNodeUUID

The UUID of the originating node.

Delete Incident

The **Delete Incident** operation deletes an incident from NNM.

The operation produces a **Success** response if the operation completes successfully. It produces a **Failure** response if the operation is unable to complete successfully.

The inputs for the operation are:

nnmProtocol

The protocol to use to connect to the NNM server. The valid values are **HTTP** and **HTTPS**.

nnmHost

The DNS name or IP address of the NNM server.

nnmPort

The number of the port to use to connect to your NNM server.

nnmUsername

The username for NNM authentication.

nnmPassword

The password for NNM authentication.

incidentUUID

The UUID of the incident to delete.

Enumerate Incidents by Lifecycle

The **Enumerate Incidents by Lifecycle** operation retrieves all incidents in the specified lifecycle.

The operation produces a **Success** response if the operation completes successfully. It produces a **Failure** response if the operation is unable to complete successfully.

Other results are:

assignedTo

The person to whom the object is assigned.

category

The category to which the object belongs.

family

The family to which the object belongs.

firstOccurrenceTime

The date and time that the event first occurred.

duplicateCount

The number of duplicates of the object.

id

The ID of the object.

lastOccurrenceTime

The most recent date and time that the event occurred.

lifecycleState

The current state of the object.

name

The name of the object.

nature

The nature of the object. The valid values are **ROOTCAUSE**, **SECONDARYROOTCAUSE**, **SYMPTOM**, **SERVICEIMPACT**, **STREAMCORRELATION**, **NONE**, and **INFO**.

notes

Any notes associated with the object.

origin

Where the object originated. The valid values are **MANAGEMENTSOFTWARE**, **MANUALLYCREATED**, **REMOTELYGENERATED**, **SNMPTRAP**, **SYSLOG**, and **OTHER**.

originOccurrenceTime

The time that this instance of the object originated.

priority

The priority of the object.

severity

The severity of the issue. The valid values are **NORMAL**, **WARNING**, **MINOR**, **MAJOR**, and **CRITICAL**.

sourceName

The name of the object's source.

sourceNodeName

The name of the node on which the incident occurred.

sourceNodeUuid

The UUID of the node on which this incident occurred.

sourceType

The type of the source on which this incident occurred.

sourceUuid

The UUID of the object's source.

uuid

The UUID of the object.

The inputs for the operation are:

nnmProtocol

The protocol to use to connect to the NNM server. The valid values are **HTTP** and **HTTPS**.

nnmHost

The DNS name or IP address of the NNM server.

nnmPort

The number of the port to use to connect to your NNM server.

nnmUsername

The username for NNM authentication.

nnmPassword

The password for NNM authentication.

lifecycleState

The lifecycle state the incidents are currently in. The default setting for assigning a value to this input is a prompt for the user to select the lifecycle state from the **NNM Lifecycle State** selection list.

Enumerate Incidents by Severity

The **Enumerate Incidents by Severity** operation retrieves all non-closed incidents of the specified severity.

The operation produces a **Success** response if the operation completes successfully. It produces a **Failure** response if the operation is unable to complete successfully.

Other results are:

assignedTo

The person to whom the object is assigned.

category

The category to which the object belongs.

family

The family to which the object belongs.

firstOccurrenceTime

The date and time that the event first occurred.

duplicateCount

The number of duplicates of the object.

id

The ID of the object.

lastOccurrenceTime

The most recent date and time that the event occurred.

lifecycleState

The current state of the object.

name

The name of the object.

nature

The nature of the object. The valid values are **ROOTCAUSE**, **SECONDARYROOTCAUSE**, **SYMPTOM**, **SERVICEIMPACT**, **STREAMCORRELATION**, **NONE**, and **INFO**.

notes

Any notes associated with the object.

origin

Where the object originated. The valid values are **MANAGEMENTSOFTWARE**, **MANUALLYCREATED**, **REMOTELYGENERATED**, **SNMPTRAP**, **SYSLOG**, and **OTHER**.

originOccurrenceTime

The time that this instance of the object originated.

priority

The priority of the object.

severity

The severity of the issue. The valid values are **NORMAL**, **WARNING**, **MINOR**, **MAJOR**, and **CRITICAL**.

sourceName

The name of the object's source.

sourceNodeName

The name of the node on which the incident occurred.

sourceNodeUuid

The UUID of the node on which this incident occurred.

sourceType

The type of the source on which this incident occurred.

sourceUuid

The UUID of the object's source.

uuid

The UUID of the object.

The inputs for the operation are:

nnmProtocol

The protocol to use to connect to the NNM server. The valid values are **HTTP** and **HTTPS**.

nnmHost

The DNS name or IP address of the NNM server.

nnmPort

The number of the port to use to connect to your NNM server.

nnmUsername

The username for NNM authentication.

nnmPassword

The password for NNM authentication.

severity

The severity of the incidents. The valid values are **NORMAL**, **WARNING**, **MINOR**, **MAJOR**, and **CRITICAL**.

Get Incident

The **Get Incident** operation retrieves detailed information about an incident.

The operation produces a **Success** response if the operation completes successfully. It produces a **Failure** response if the operation is unable to complete successfully.

Other results are:

assignedTo

The person to whom the object is assigned.

category

The category to which the object belongs.

family

The family to which the object belongs.

firstOccurrenceTime

The date and time that the event first occurred.

duplicateCount

The number of duplicates of the object.

id

The ID of the object.

lastOccurrenceTime

The most recent date and time that the event occurred.

lifecycleState

The current state of the object.

name

The name of the object.

nature

The nature of the object. The valid values are **ROOTCAUSE**, **SECONDARYROOTCAUSE**, **SYMPTOM**, **SERVICEIMPACT**, **STREAMCORRELATION**, **NONE**, and **INFO**.

notes

Any notes associated with the object.

origin

Where the object originated. The valid values are **MANAGEMENTSOFTWARE**, **MANUALLYCREATED**, **REMOTELYGENERATED**, **SNMPTRAP**, **SYSLOG**, and **OTHER**.

originOccurrenceTime

The time that this instance of the object originated.

priority

The priority of the object.

severity

The severity of the issue. The valid values are **NORMAL**, **WARNING**, **MINOR**, **MAJOR**, and **CRITICAL**.

sourceName

The name of the object's source.

sourceNodeName

The name of the node on which the incident occurred.

sourceNodeUuid

The UUID of the node on which this incident occurred.

sourceType

The type of the source on which this incident occurred.

sourceUuid

The UUID of the object's source.

uuid

The UUID of the object.

The inputs for the operation are:

nnmProtocol

The protocol to use to connect to the NNM server. The valid values are **HTTP** and **HTTPS**.

nnmHost

The DNS name or IP address of the NNM server.

nnmPort

The number of the port to use to connect to your NNM server.

nnmUsername

The username for NNM authentication.

nnmPassword

The password for NNM authentication.

incidentUUID

The UUID of the incident to retrieve.

Update Lifecycle Status

The **Update Lifecycle Status** operation changes the status of an incident.

The operation produces a **Success** response if the operation completes successfully. It produces a **Failure** response if the operation is unable to complete successfully.

The inputs for the operation are:

nnmProtocol

The protocol to use to connect to the NNM server. The valid values are **HTTP** and **HTTPS**.

nnmHost

The DNS name or IP address of the NNM server.

nnmPort

The number of the port to use to connect to your NNM server.

nnmUsername

The username for NNM authentication.

nnmPassword

The password for NNM authentication.

id

The ID of the incident.

lifecycleState

The new lifecycle state for the incident. The default setting for assigning a value to this input is a prompt for the user to select the lifecycle state from the **NNM Lifecycle State** selection list.

Update Priority

The **Update Priority** operation updates the priority of an incident.

The operation produces a **Success** response if the operation completes successfully. It produces a **Failure** response if the operation is unable to complete successfully.

The inputs for the operation are:

nnmProtocol

The protocol to use to connect to the NNM server. The valid values are **HTTP** and **HTTPS**.

nnmHost

The DNS name or IP address of the NNM server.

nnmPort

The number of the port to use to connect to your NNM server.

nnmUsername

The username for NNM authentication.

nnmPassword

The password for NNM authentication.

id

The ID of the incident.

priority

The new priority for the incident. The default setting for assigning a value to this input is a prompt for the user to select the priority from the **NNM Priority** selection list.

Nodes

Delete Node

The **Delete Node** operation deletes a node from NNM.

The operation produces a **Success** response if the operation completes successfully. It produces a **Failure** response if the operation is unable to complete successfully.

The inputs for the operation are:

nnmProtocol

The protocol to use to connect to the NNM server. The valid values are **HTTP** and **HTTPS**.

nnmHost

The DNS name or IP address of the NNM server.

nnmPort

The number of the port to use to connect to your NNM server.

nnmUsername

The username for NNM authentication.

nnmPassword

The password for NNM authentication.

nodeUUID

The UUID of the node to delete.

Get Node by Name

The **Get Node by Name** operation retrieves the node or nodes with the specified name, and returns details about them.

The operation produces a **Success** response if the operation completes successfully. It produces a **Failure** response if the operation is unable to complete successfully.

Other results are:

createdDate

The date the object was created.

contact

The contact person for the object (systemContact).

deviceCategory

The category to which the device belongs.

deviceDescription

The description of the device.

discoveryState

The discovery state of the object. The valid values are **NEWLY_CREATED**, **DISCOVERY_COMPLETED**, and **REDISCOVERY_IN_PROGRESS**.

family

The family to which the object belongs (deviceFamily).

id

The ID of the object.

isEndNote

Specifies whether there are other nodes beyond this node. The valid values are **true** and **false**.

isSnmpSupported

Specifies whether the node supports SNMP (snmpSupported). The valid values are **true** and **false**.

location

The location of the object (systemLocation).

longName

The long name of the object.

managementMode

The management mode the object is currently in. The valid values are **INHERITED**, **MANAGED**, **NOTMANAGED**, and **OUTOFSERVICE**.

model

The model of the device (deviceModel).

modified

The date on which the object was last modified.

name

The name of the object.

notes

Any notes associated with the object.

snmpVersion

The version of SNMP that the object is using.

status

The status of the object. The valid values are **NORMAL**, **WARNING**, **MINOR**, **MAJOR**, **CRITICAL**, **DISABLED**, **NOSTATUS**, and **UNKNOWN**.

systemDescription

The description of the system.

systemId

The object ID of the system (systemObjectId).

systemName

The name of the system.

uuid

The UUID of the object.

vendor

The vendor of the device (deviceVendor).

The inputs for the operation are:

nnmProtocol

The protocol to use to connect to the NNM server. The valid values are **HTTP** and **HTTPS**.

nnmHost

The DNS name or IP address of the NNM server.

nnmPort

The number of the port to use to connect to your NNM server.

nnmUsername

The username for NNM authentication.

nnmPassword

The password for NNM authentication.

name

The **name** property value of the node to retrieve; The **Name** in the user interface.

Get Node by UUID

The **Get Node by UUID** operation retrieves the node with the specified UUID and returns detailed information about it.

The operation produces a **Success** response if the operation completes successfully. It produces a **Failure** response if the operation is unable to complete successfully.

Other results are:

createdDate

The date the object was created.

contact

The contact person for the object (systemContact).

deviceCategory

The category to which the device belongs.

deviceDescription

The description of the device.

discoveryState

The discovery state of the object. The valid values are **NEWLY_CREATED**, **DISCOVERY_COMPLETED**, and **REDISCOVERY_IN_PROGRESS**.

family

The family to which the object belongs (deviceFamily).

id

The ID of the object.

isEndNote

Specifies whether there are other nodes beyond this node. The valid values are **true** and **false**.

isSnmpSupported

Specifies whether the node supports SNMP (snmpSupported). The valid values are **true** and **false**.

location

The location of the object (systemLocation).

longName

The long name of the object.

managementMode

The management mode the object is currently in. The valid values are **INHERITED**, **MANAGED**, **NOTMANAGED**, and **OUTOFSERVICE**.

model

The model of the device (deviceModel).

modified

The date on which the object was last modified.

name

The name of the object.

notes

Any notes associated with the object.

snmpVersion

The version of SNMP that the object is using.

status

The status of the object. The valid values are **NORMAL**, **WARNING**, **MINOR**, **MAJOR**, **CRITICAL**, **DISABLED**, **NOSTATUS**, and **UNKNOWN**.

systemDescription

The description of the system.

systemId

The object ID of the system (systemObjectId).

systemName

The name of the system.

uuid

The UUID of the object.

vendor

The vendor of the device (deviceVendor).

The inputs for the operation are:

nnmProtocol

The protocol to use to connect to the NNM server. The valid values are **HTTP** and **HTTPS**.

nnmHost

The DNS name or IP address of the NNM server.

nnmPort

The number of the port to use to connect to your NNM server.

nnmUsername

The username for NNM authentication.

nnmPassword

The password for NNM authentication.

nodeUUID

The UUID of the node to retrieve.

Get Node Conclusions

The **Get Node Conclusions** operation retrieves a summary of what NNM has concluded about the date of the specified node.

The operation produces a **Success** response if the operation completes successfully. It produces a **Failure** response if the operation is unable to complete successfully.

Other results are:

conclusion

The conclusion text of an individual conclusion object.

incidentUuid

The UUID of the associated incident.

status

The status of the object. The valid values are **NORMAL**, **WARNING**, **MINOR**, **MAJOR**, **CRITICAL**, **DISABLED**, **NOSTATUS**, and **UNKNOWN**.

timestamp

The time that the object was created or modified.

uuid

An individual conclusion object UUID.

The inputs for the operation are:

nnmProtocol

The protocol to use to connect to the NNM server. The valid values are **HTTP** and **HTTPS**.

nnmHost

The DNS name or IP address of the NNM server.

nnmPort

The number of the port to use to connect to your NNM server.

nnmUsername

The username for NNM authentication.

nnmPassword

The password for NNM authentication.

id

The ID of the node from which to retrieve conclusions.

Update Node Management Mode

The **Update Node Management Mode** operation changes the management mode of a node. You can use this operation for tasks such as disabling monitoring.

The operation produces a **Success** response if the operation completes successfully. It produces a **Failure** response if the operation is unable to complete successfully.

The inputs for the operation are:

nnmProtocol

The protocol to use to connect to the NNM server. The valid values are **HTTP** and **HTTPS**.

nnmHost

The DNS name or IP address of the NNM server.

nnmPort

The number of the port to use to connect to your NNM server.

nnmUsername

The username for NNM authentication.

nnmPassword

The password for NNM authentication.

id

The ID of the node whose management mode you want to change.

mode

The management mode. The default setting for assigning a value to this input is a prompt for the user to select the management mode from the **NNM Node Management Nodes** selection list.

Launching flows

You can interact with HP OO using the various REST-based services:

- `https://ooserver:port/PAS/services/http/list`
  Retrieves a list of flows from OO.
- `https://ooserver:port/PAS/services/http/execute/<Library Path>`
  Executes a flow by name (waits for the flow to finish before returning).
- `https://ooserver:port/PAS/services/http/execute/<Flow UUID>`
  Executes a flow by UUID (waits for the flow to finish before returning).
- `https://ooserver:port/PAS/services/http/execute_async/<Library Path>`
  Executes a flow by name (returns immediately after the flow is launched).
- `https://ooserver:port/PAS/services/http/execute_async/<Flow UUID>`
  Executes a flow by UUID (returns immediately after the flow is launched).

Integrating Central into the NNM Actions menu

This integration allows you to add a menu item which launches Central interactively to the HP Network Node Manager (NNM) interface.

To add a command that launches Central

1. Open the NNM Web User Interface.
2. Select **Configuration > URL Actions**.
3. Click **New**.
4. Enter a menu label, such as **Launch Network Diagnostic**.
5. Enter a unique key.
   The recommended format is:
   `com.<Company name/Group>.nnm.urlAction.<MenuLabel>)`
   For example:
   `com.hp.pas.nnm.urlAction.LaunchNetworkDiagnostic`
   The key can be up to 80 characters in length.
6. Specify the allowed target types.
   Each type requires the URL that is launched. This should be:
   `https://<HPOOhost>:8443/PAS/app?service=RCLinkService/FlowLinkDispatch&sp=SAUTOMATIC&sp=uuid&sp=l0&host=${name}&uuid=${uuid}`
   Where `<HPOOhost>` is the name of the HP OO server.
7. Replace the UUID with the UUID of the flow that will be launched.
   The arguments `host=${name}` and `uuid=${uuid}` allow information to be passed from NNM to the flow automatically.

The `host=` and `uuid=` portion of these arguments specify the HP OO input that is being supplied.

To test the integration

1. Open an instance of the object to which you associated the menu.
2. Click **Actions**.
3. Click the action name you specified in step 4 of the preceding procedure.

Automated incident integration

This integration allows you to automatically launch a flow when a specific Incident type changes its lifecycle.

To automatically trigger a flow from an event

1. From the **Configuration** menu, select **Incident Configuration**.
2. Click **Management Event Configuration**.
3. Open the event of interest.
4. Click the **Action Configuration** tab.
5. Click **New**.
6. Specify the triggering lifecycle state.

   The **Registered** lifecycle state triggers on new incidents.
7. Specify **Command Type** as **Script** or **Executable**.
8. Specify the command as a .bat file that runs RSFlowInvoke.

   The command that makes up the .bat file should be of the following form:

   ```
   RSFlowInvoke.exe –u <username> -ep <encrypted password>
   https://<HPOOserver:port>/PAS/services/http/execute/<full library path for flow>
   ```

   To execute the command using a non-encrypted password, the first part of the command would be as follows:

   ```
   RSFlowInvoke.exe –u <username> –p <password>
   ```
9. To pass the UUID of the incident to the command, add either `%1` or `${uuid}`:

   If the command is in a batch file and you have added `${uuid}` in the run field of the NNM UI as described above, add `%1` to the end of the command. `%1` reads the first argument passed to a batch file:

   ```
   RSFlowInvoke.exe –u <username> -ep <encrypted password>
   https://<HPOOserver:port>/PAS/services/http/execute/<full library path for flow>
   %1
   ```

   If you use the command by itself, add `${uuid}` (note that this uses curly braces) to the end of the command:

   ```
   RSFlowInvoke.exe –u <username> -ep <encrypted password>
   https://<HPOOserver:port>/PAS/services/http/execute/<full library path for flow>
   ${uuid}
   ```

The .bat file must be located in the C:\Program Files\Hp Openview\data\shared\nnm\actions\ folder.

Troubleshooting

General troubleshooting procedures

If an operation is not working, make sure that it can connect to the NNM server, and that you are using valid credentials.

Troubleshooting the operations

There are currently no known frequent issues with these operations.

Errors that the operations return

Connection refused - The RAS cannot reach the NNM server.

Bad Username or Password - Check your credentials.

Unauthorized -- Ensure that your user has been given access inside NNM.

Customizing the integration

The NNM 7.5 integration uses the following NNM Command Line interfaces:

- ovevent
- ovdumpevents
- ovobjprint

If the operations need to be customized, additional information on these CLIs can be found in the NNM online documentation.

The NNM 8.1x integration is made through the NNM Web service. This Web service is static and does not change.

Security

The username/password used in the flow must have full access to NNM.

Tools

Following are OO tools that you can use with the HP NNMi integration:

RSFlowInvoke.exe and **JRSFlowInvoke.jar**

RSFlowInvoke (RSFlowInvoke.exe or the Java version, JRSFlowInvoke.jar) is a command-line utility that allows you to start a flow without using Central (although the Central service must be running). RSFlowInvoke is useful when you want to start a flow from an external system, such as a monitoring application that can use a command line to start a flow.