Server Automation

Software Version: 10.50

Integration Guide

Hewlett Packard Enterprise

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

© Copyright 2000-2016 Hewlett Packard Enterprise Development LP

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

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

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

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

Support

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

This website provides contact information and details about the products, services, and support that HPE Software offers.

HPE Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support website to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HPE support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

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

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

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

Contents

Overview

This document provides information to integrate SA with other HPE products.

- "Integrating with DMA" on page 111

- "Integrating with OBR" on page 112

- "Integrating with HPELN" on page 88

- "Integrating with uCMDB Connector" on page 57

- "Integrating with OO" on page 29

- "Integrating with NA" on the next page

Integrating with NA

This section provides you information about Integrating SA with NA.

Overview

Implementing changes in an IT environment often requires a coordinated effort between network administrators, system administrators, and application architects who manage an application environment that consist of servers with different operating systems as well as network devices that include firewalls, load balancers, switches, servers, Web applications, and so on.

For example, in certain environments, you are required to make changes to network devices of an application environment, such as load balancers, firewalls, switches, and so on.

NA/SA Integration makes this process easier by enabling you to see how servers are connected to network devices and enables them to closely examine managed servers. With this information, you can determine how all devices are related and can coordinate and implement required changes accordingly.

The following figure illustrates some of the coordinated tasks you can perform using NA/SA Integration.

Overview of coordinating tasks using SA-NA Integration
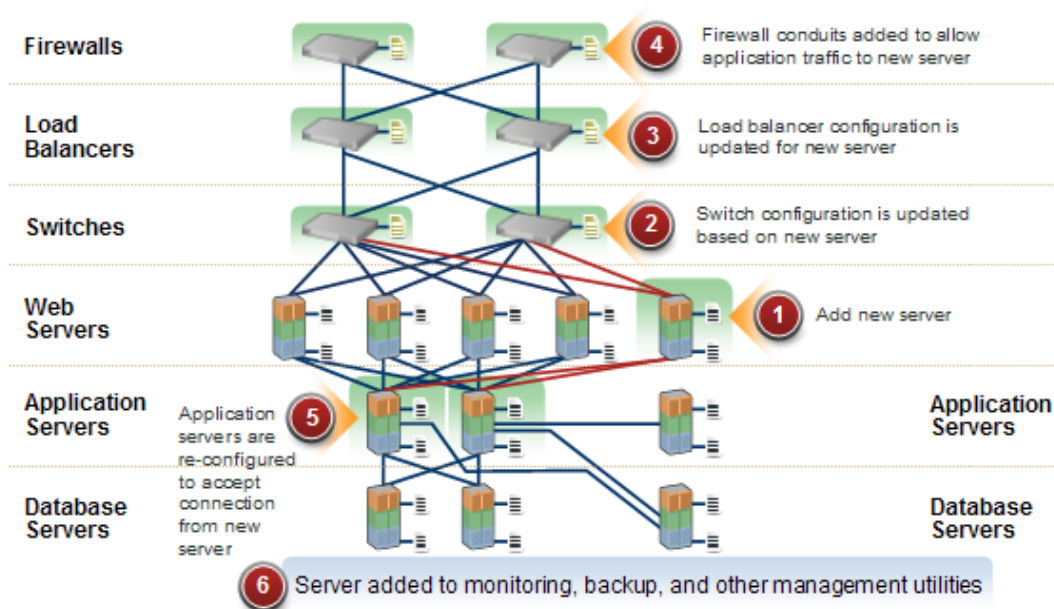
After integration is established, you can view device details, examine connections between network devices and servers, identify duplex mismatches, and view combined device history information. It also provides information about implementing changes across the environment and generating network reports.

To support an integrated approach to making changes in your environment, such as server reallocation, ensuring compliance across servers and network devices, and detecting and resolving duplex mismatches, NA/SA Integration provides the following interface points:

- HPE Server Automation (SA)

- Network Automation (NA)

- SA Global Shell

- HPE Server Automation Visualizer (in SA)

- HPE Reports (in SA)

NA/SA Integration features

After NA/SA Integration is configured, you can perform the following tasks:

- View the detailed hardware information about SA Managed Servers and their attached network devices, and about their network connections (interfaces and ports).

- Use the SA Global File System (OGFS) to:

  ○ Navigate between managed servers and connected network devices by tracing their associated physical connections

  ○ Find network device configurations

  ○ Run scripts across servers and network devices.

- Call NA scripts from SA scripts to automate operations across servers and network devices.

- Use features in SA and NA to create diagrams that illustrate the managed servers, network devices, and layer 2 (and inferred layer 1) connections in your environment.

- Use SA to identify, troubleshoot, and remediate configuration duplex mismatches between managed servers and network devices.

- Use SA to perform actions on SA Device Groups that can contain both servers and network devices.

- Use SA to review a combined server and network device event history log that records changes

made to applications in your environment.

- Use SA to export combined event history logs to CSV and/or HTML files.

- Use NA to directly access additional network device details and event history.

- Use SA to run network reports that identify layer 2 and inferred layer 1 connections and configuration mismatches (duplex compliance).

> **Note:** References to *connections* in this document refer to *physical connections*, except where noted.

NA data collection

The NA/SA Integration feature uses the NA Topology Data Gathering and NA Duplex Data Gathering diagnostic tools to collect information about network devices.

NA topology data gathering diagnostic

The NA Topology Data Gathering diagnostic instructs NA to collect MAC addresses for all switches. Using MAC addresses, you can discover and add physical connections to the SA data model.

For example, when you add a server to a switch, the information is collected the next time the NA Topology Data Gathering diagnostic runs. You can also manually run the NA Topology Data Gathering diagnostic or the NA Duplex Data Gathering diagnostic for specific network devices. For more information about these diagnostics, see the SA 10.50 User Guide.

> **Note:** For NA performance reasons, you should not run these diagnostics on multiple devices more frequently than once in a week. If you are required to refresh the NA data more frequently, contact your support representative. These diagnostics can be run on single devices more frequently.

NA duplex data gathering diagnostic

For network devices, speed and duplex is gathered by the NA Duplex Data Gathering diagnostic, which runs after a device is initially added to NA and subsequently according to a schedule that you define.

To ensure that you have the latest speed and duplex information about network devices, SA recommends that you set up a recurring schedule that runs the diagnostic. For more information about this diagnostic and scheduling, see "Duplex mismatch" and the SA 10.50 User Guide.

NA database/SA database

The NA and SA databases are not integrated – NA and SA each manage their own data.

Authentication

For SA/NA integrated functionality, authentication is handled by SA. For more information, see "Prerequisites". NA-only functionality continues to be authenticated using NA credentials.

Setting up the integration

The SA administrators must perform certain tasks on SA Core servers to enable NA/SA Integration.

The set up includes changing certain configuration settings in both NA and SA, running diagnostics for NA topology data, and configuring certain user permissions.

The integration does not support failover of the NA core. If the integrated NA core fails over in a different NA core, update the HPE SA twist.conf and edit the twist.nasdata.host to the new NA core for connecting to the new NA core. For more details, see **Specify the NA server name** in SA configuration changes.

SA Client communication with NA

Ensure that the SA Client can communicate with NA. If the SA Client cannot communicate with the NA server, see "Resetting the NA host in the SA Client".

SA configuration changes

Complete the following tasks to prepare SA for NA integration:

- **Specify the NA server name**

  NA – SA integration works only when SA twist.conf (`/etc/opt/opsware/twist/twist.conf`) is configured with NA FQDN in the twist.nasdata.host=<NA Server FQDN>.

  For more information about modifying this file, see the SA Administering.

  If you have installed multiple Slice Component bundles, you must edit the `twist.conf` file on all slices. Then, you must restart all NA services and the Web Service Data Access Engine for each Slice component bundle.

- **Specify the NA Port (Windows-only) in SA**

  If NA is running on a Windows server, you must change the port setting parameter from
  `nas.port=8022` to `nas.port=22` in the `/etc/opt/opsware/hub/hub.conf file.`

  A default Windows server installation runs the proxy SSH/Telnet servers on port 22/23 rather than
  the Unix default of port 8022/8023.

  After you make this configuration change, you must restart the server hosting the Slice Component
  bundle.

- Enable the spin.cronbot.check_duplex.enabled Parameter

  The `spin.cronbot.check_duplex.enabled system configuration` parameter must be enabled
  for NA integration.

  To enable this system configuration parameter, perform the following steps:

  a. Select the **Administration** tab in the SA Client.

  b. Select System Configuration in the navigation pane. This displays the SA components,
     facilities and realms that have system configuration parameters.

  c. In the list of SA components, select Data Access Engine. This displays the system
     configuration parameters for this component.

  d. Locate the parameter `spin.cronbot.check_duplex.enabled`.

  e. In the Value column, select the new value button and set the value to 1.

  f. Select the Revert button to discard your changes or the Save button to save your changes.

For more information about system configurations, see the SA 10.50 Administration Guide.

Configuring NA for integration

> **Note:** To configure NA Integration with the current SA version, you must have a compatible
> version of Network Automation (NA) installed. For more information, see the NA*Support Matrix* on
> SSO (https://softwaresupport.hpe.com/).

The NA administrator should perform the following tasks on your NA server.

SA **gateway requirements**

NA must be configured to use the Master Gateway for the SA Core you are integrating with. For more information about specifying the SA Core Master Gateway in NA, see the *NA Satellite Guide* on on SSO (https://softwaresupport.hpe.com/)..

User permissions

Access permissions for NA/SA Integration are based on two separate databases: a NA database and a SA database. NA uses its own database for authorization. SA uses a different security mechanism for authorization. However, for NA integration, all authentication (for both NA and SA) is processed by SA.

When NA is configured to use SA authentication, NA tries to authenticate against SA first. If NA fails to authenticate against SA, it falls back to the NA database. If there is an account in the NA database, the fallback is only allowed if that user is configured to allow fallback authentication. See the NA User Guide for more information on NA authentication.

When a new user is authenticated through SA, an account is created in NA. The account is placed in the Default User Group that was specified when SA authentication was enabled in the Administrative Settings in NA. This user group, which is configurable, controls the default permissions that the system administrator has assigned to SA users.

> You must have the required set of permissions to view servers and network devices. To obtain these permissions, contact your SA administrator, or for more information, see the SA 10.50 Administration Guide.

NA authentication configuration

To set up NA/SA Integration, you must configure NA to use SA Authentication. Before beginning this configuration, you must have this information (see Server Automation Software Authentication):

Twist Server: the IP address or Hostname of the server hosting the Web Services Data Access Engine (`twist`: part of the Slice Component bundle which is typically installed on the SA Core host but can be installed on a different host).

- **Twist Port Number:** The port number that the Web Services Data Access Engine listens on.
- **Twist Username:** The Web Services Data Access Engine user name.
- **Twist Password:** The Web Services Data Access Engine user's password.
- **OCC Server:** The IP address or hostname of the server hosting the Command Center (OCC).
- **Default User Group:** The default user group for new SA users.

To change the authentication settings in NA, perform the following tasks:

1. Log in to NA.

2. Select **Admin > Administrative Settings > User Authentication** to display the Administrative Settings — User Authentication page.

3. In the External Authentication Type section, use the radio button to select HPE Server Automation software & TACACS+ (if used) as shown in the following figure.

External authentication type in NA

4. Scroll down and complete all fields in the HPE Server Automation software Authentication section shown in the following figure.

   NA uses the Web Services Data Access Engine (`twist`) Username and Password when it gathers layer 2 data. NA gathers server interface information by MAC address using the Twist user's permissions. The Twist user must have read access to server information.

HPE Server Automation software authentication

5. Click **Save** to save your configuration changes.

See the NA User Guide for more information on NA configuration.

Gathering topology data

After SA-NA Integration tasks are completed, you must run the NATopology Data Gathering and NA Duplex Data Gathering diagnostics. For instructions about running these utilities, see the NA User Guide.

Troubleshooting

To test whether SA is communicating with NA, check the following conditions:

- You can log in to NA with your SA credentials. This verifies that NA can communicate with SA.

- The SA credentials specified in the NA Administrative Settings under External Authentication Type are set to SA. This ensures that NA can look up server MAC addresses.

- The NA Topology Gathering Diagnostic has run successfully. To verify this condition, search for tasks and check their results. This ensures that NA has gathered MAC addresses and tried to look them up in SA.

Prerequisites

To perform integration, the following prerequisites must be met:

- Time requirements

- Port requirements

Time requirements

The SA and NA core servers must be synchronized and have the same time and time zone settings.

NA Integration port requirements

Before you configure NA Integration, ensure that SA and NA can communicate with each other over the following ports:

- **Port 1032 (NA to SA)**

  NA must be able to access port 1032 on the server that is running the SA Web Services Data Access Engine component (part of the Component Slice bundle). By default, the Web Services Data Access Engine listens on port 1032.

- **Port 8022 (Unix) / Port 22 (Windows) (SA to NA)**

  For the Global File System (OGFS) feature to be able to display data about network devices, SA must have access to port 8022 (Unix-based NA Servers) or 22 (Windows-based NA Servers).

- **RMI Ports for NA API**

  The NA API uses Java RMI to connect to the NA server. SA uses the NA API for the NA integration. RMI requires that the following ports be open:

  - **Port 1099**

    JNDI

  - **Port 4444(for** NA **versions 9.10 and earlier)**

    RMI Object

○ **Port 4446 (for** NA **versions 9.20 and later)**

RMI Object

○ **Port 1098**

RMI Method

Resetting the NA host in the SA Client

Some NA/SA Integration features require that the SA Client (Java) opens the NA Web interface (directly from SA) so that you can access additional details about certain NA events. If your administrator has completed the setup tasks in the *SA Installing*, but the SA Client is unable to communicate directly with the server running the NA host (server) Web interface, you might need to change the NA option in the SA Client. For example, if a firewall is preventing the SA Client from reaching the NA host, you need to specify the name of a server that is acting as a proxy for the NA host. This will override the default setting. This task must be performed on every desktop running a SA Client that cannot communicate with the NA host.

To reset the NA host in the SA Client:

1. From the **Tools** menu in the SA Client window, select **Options**.

2. In the Views pane, select HPE Network Automation.

3. In the Host field, enter the name of a server that is acting as a proxy for the NA host, such as m208, which is the proxy for the m208.example.com NA host.

4. (Optional) Click **Restore Default** to restore the previously saved NA host name.

5. (Optional) Click **Test** to open the NA login window.

6. Click **Save**.

Use cases

After you have successfully configured SA-NA Integration, the following capabilities are available:

- Connections between network devices and servers

- Network Device Information in SA

- "Viewing network interfaces" on page 20

- Viewing Network Ports

- Network Device Information in NA

- Duplex Mismatch

- Network Reports

- NA and the SA Global Shell

- Inferred Physical Connections

- Device Groups and NA

Connections between network devices and servers

The NA/SA Integration features are based on layer 2 connections and inferred layer 1 connections of the OSI Seven Layer Model.

OSI seven layer model
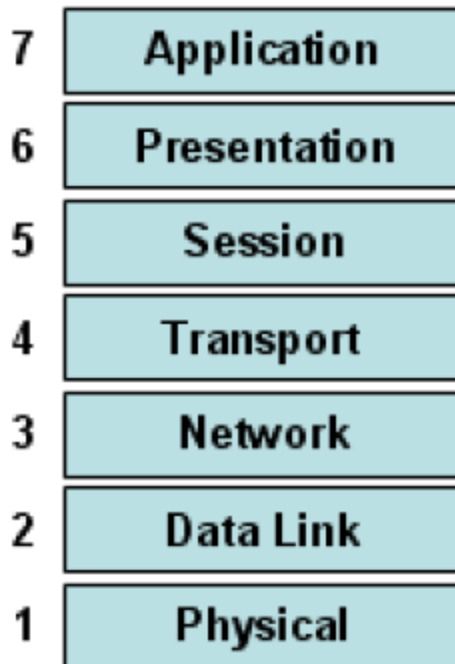
Data link connections

The NA/SA Integration feature includes functionality that detects Data Link (layer 2) connections and reports on physical (layer 1) and data link connections. These data link connections include switches

that are directly connected to a managed server and switches that are indirectly connected through other switches. These connections are discovered by correlating the MAC addresses reported by the device with the known MAC addresses for servers and switches.

Physical connections

The Physical connections are inferred from the Data Link connections (see "Inferred physical connections". Physical connections represent direct connections (cables) between server and switches.

In the SA Client, you can see Physical connections in the Server Explorer, the Network Device Explorer and in detailed layout diagrams in Service Automation Visualizer (SAV). In the NA diagramming feature, you can see physical, data link or network (layer 3) connections.

Network device information in SA

In addition to basic hardware details about managed servers and network devices, the NA/SA Integration feature also reports the following information about network interfaces and network ports:

- On the server side, network interfaces have the following properties:
  - MAC address
  - Subnet mask
  - interface type
  - IP address
  - DHCP setting
  - Connected switch port
  - Speed
  - Duplex (excluding Windows)
- On the network device side, network ports have the following properties:
  - Port name
  - Speed
  - Duplex settings
  - Devices connected
  - Interface type.

Note: For most devices, auto-negotiation works best when both sides of the connection (server

and network device) are set to auto-negotiate mode. For example, a duplex policy could specify that a port should be set to full, half, or auto, and not to full (auto). A full (auto) duplex setting indicates that the port was set to auto-negotiate and it negotiated to full duplex.

The following tasks describe how you can access detailed hardware information for servers and network devices directly in SA. See "Network device information in NA" for instructions on how to access hardware information about network devices directly in NA.

Viewing network interfaces

To view hardware information about a server, including network interfaces:

1. Log in to the SA Client.

2. From the Navigation pane, select **Devices > All Managed Servers.**

3. From the View drop-down list, select **Network**.

4. Double-click on a server in the Content pane to display hardware details in the Server Explorer (see the following figure).

Hardware view in the Server Explorer

Viewing network ports

To view hardware information about a network device, including network ports:

1. Log in to the SA Client.

2. From the Navigation pane, select **Devices > Device Groups > Public** and then select a device group.

3. Double-click on a network device in the Content pane to display the Network Device Explorer.

4. In the Views pane, select **Hardware** to display information about the selected network device. See the following figure.

Hardware view in the Network Device Explorer

Network device information in NA

To help you with troubleshooting tasks that involve network devices in your environment, you can examine additional network device details and network device event history by logging directly in to NA. The NA/SA Integration feature provides a login option to access detailed information about network devices and their event history as recorded in NA.

Viewing a network device

1. From the Navigation pane, select Devices > Device Group > Public.

2. In the Content pane, select a network device.

Network device details in NA

Viewing event history

In the Event Details window, click on the Device link to view additional information, such as timestamps for when the device was added, the last snapshot and the last configuration change.

Event details for a network device in NA

Duplex mismatch

The NA/SA Integration feature provides automatic detection of duplex mismatches. A duplex mismatch is a configuration mismatch between the speed and duplex of a managed server and a connected network device.

For servers' network interfaces, speed and duplex information is gathered during every hardware registration, which occurs every 24 hours.

Due to the lack of a device independent method of determining duplex for servers running a Windows operating system, the Server Agent for Windows does not report duplex settings out-of-the-box. A custom script can be added to the Server Agent to collect and report the speed and duplex setting for a certain network interface. For instructions on how to create and integrate the script with the Agent, contact your support representative.

Speed and duplex information for servers is *not* updated when you select **View > Refresh** or press F5 in the SA Client. This data gets updated when the NA Duplex Data Gathering diagnostic runs. See "NA duplex data gathering diagnostic".

For network devices, speed and duplex is gathered by the NA Duplex Data Gathering diagnostic, which runs according to a schedule that you define. To ensure that you have the latest speed and duplex information about network devices, it is recommended that you set up a recurring schedule that runs the diagnostic. See the SA 10.50 User Guide.

If the network interface information (speed and duplex) for a server does not match the network port information (speed and duplex) for a connected network device, the device is considered to be non-compliant.

In the NA/SA Integration feature, you can see duplex mismatches identified at a top level by using the Dashboard. You can also see duplex mismatches identified by server and network device by using the Server Explorer and Network Device Explorer, respectively.

Viewing duplex mismatches in the dashboard

See the SA 10.50 Administration Guide for information about duplex compliance levels and how they are displayed in the Dashboard.

Viewing duplex mismatches by server

To view duplex mismatches using the Server Explorer:

1. From the Navigation pane, select **Devices > All Managed Servers**.

2. In the Content pane, select a server.

3. Double-click on the server to display the Server Explorer.

4. In the Views pane, select **Hardware**.

5. In the Network Interfaces section, review the Duplex column for detected mismatches. Mismatches are identified by an ✖ icon that precedes the duplex setting (Full, Half, Auto), in the Duplex column.

Viewing duplex mismatches by network device

To view duplex mismatches using the Network Device Explorer:

1. From the Navigation pane, select **Devices > Device Groups > Public**.

2. In the Content pane, select a network device.

3. Double-click on the network device to display the Network Device Explorer.

4. In the Views pane, select **Hardware**.

5. In the Network Ports section, review the Duplex column for detected mismatches. Mismatches are identified by an ✖ icon that precedes the duplex setting (Full, Half, Auto), in the Duplex column.

Network reports

To help troubleshoot problems that involve physical connections and duplex compliance, you can run and examine network reports. By using the Reports feature in the SA Client, you can produce the following network reports that identify layer 1 connections between managed servers and network devices in your environment:

Connections by network device

This report lists all physical connections to a selected network device.

Connections by server

This report lists all physical connections to a selected managed server.

> **Note:** See the SA 10.50 Administration Guide for information about how to run, export, and print these reports.

Network diagrams

You can use Service Automation Visualizer (SAV) functions in SA and the Diagramming feature in NA to create detailed diagrams that illustrate managed servers, network devices, and layer 2 and layer 1 connections in your environment. You can also export these network diagrams to `.png`, `.png`, and `.svg` files, annotate, and use them in other applications.

Launching HPE Server Automation Visualizer

To access SAV, perform the following steps:

1. From the Navigation pane, select **Devices > All Managed Servers**.

2. In the Content pane, select one or more servers.

3. From the **Tools** menu, select **HPE Server Automation Visualizer** and then select one of the following options:
   - Select **New** to open the SAV window.
   - Select **Open** to open a previously saved topology.

4. To create and export topology diagrams, see the procedures for using HPE Server Automation Visualizer in the SA 10.50 User Guide.

Launching NA diagramming

See the SA 10.50 User Guide for instructions on launching and using the NA Diagramming feature.

NA and the SA Global Shell

You can use the SA Global File System (OGFS) to navigate between servers and connected network devices by tracing their physical connections in the `/opsw/Servers/@` and `/opsw/Network/@` directories in the OGFS.

You can also run three types of NA scripts in the OGFS:

- Command

- Advanced

- Diagnostic

These scripts correspond to the three directories in the OGFS under `/opsw/Scripts/Network`. See Network Directories in the SA 10.50 User Guide.

You can also write Bourne shell and Python scripts that can perform the following tasks when run in the OGFS:

- Find servers and network devices.

- Find all servers that are connected to a specified switch.

- Find servers with a duplex mismatch.

- Display the network interfaces of a specified server.

- Get the IP addresses of all devices.

- Compare two files to identify changes in a network device's configuration.

- Change device details, such as the `snmp-location`.

Launching OGFS

To access the OGFS in the Global Shell feature:

1. From the **Tools** menu, select **Global Shell** to launch a terminal window. See the SA 10.50 User Guide for more details about using OGFS.

2. To navigate between servers and connected network devices, use the guidelines described in the SA Global Shell and OGFS Directories sections in Use.

Remote terminal (rosh)

The `rosh` utility enables you to log in to devices (servers and network devices) and run native commands. You invoke `rosh` from within a Global Shell session. You can run `rosh` and enter native commands interactively, or you can specify the native commands as an option of `rosh`. For example, you can log in to a switch with `rosh` and run the `show vlan` command to view all VLAN details.

See the SA 10.50 User Guide for more information about using the `rosh` utility.

Inferred physical connections

The NA/SA Integration feature also includes functionality that detects and reports on inferred physical (layer 1) connections. These connections are inferred from data (such MAC addresses that are seen by switches), captured, and then added to the SA data model.

These physical connections (inferred layer 1 data) are based on heuristics. In the OSI model, each layer is an abstraction designed to hide the layer below. Therefore, the layer 2 data gathered from devices cannot generate 100% accurate layer 1 data. In particular, layer 1 data may be incorrect if any of the following conditions exist:

- The device does not return the port number where MAC addresses are seen.

- There was no traffic between the devices within a few minutes of when NA gathered the topology data (where MAC addresses are seen).

- There is an unmanaged device between two managed devices.

- There is a hub between two managed devices.

In the SA Client, you can see inferred layer 1 connections by navigating network device directories in Global Shell.

Device groups and NA

A device group helps you categorize your devices (servers and network devices) in ways that make sense for your organization. For example, you can group devices by customer, facility, usage, application, and so on, and then perform actions on all of the devices in the group.

In SA, a device group can contain managed servers *and* network devices, or *only* managed servers. In NA, a device group contains only network devices. You create and edit network device groups only in NA. See the SA 10.50 User Guide for more information about using the `rosh` utility.

To monitor an application that is running on multiple servers and relies on multiple network devices in your environment, HPE recommends that you model it as a device group that contains all servers and network devices the application runs on. This enables you to troubleshoot the application by using SA.

Associating a NA device group

When you associate a public device group in SA with a device group in NA, you will be able to monitor information about all servers and network devices that you are interested in. You associate device groups by using identical group names.

Associated device groups have the following requirements:

- The SA device group is public.

- The SA device group is static.

- The names of the associated NA and SA device groups are identical.

To associate device groups in SA and NA:

1. From the Navigation pane, select **Devices > Device Groups > Public**.

2. In the Content pane, select a device group.

3. Right-click on the device group and then select Open to display the Device Group Explorer.

4. From the View drop-down list, select **Properties**.

5. Check the "Associate with a NA device group of the same name" check box to enable this functionality.

6. From the **File** menu, select **Save**.

Troubleshooting SA-NA integration

To test whether SA is communicating with NA, check the following conditions:

- You can log in to NA with your SA credentials. This verifies that NA can communicate with SA.

- The SA credentials specified in the NA Administrative Settings under External Authentication Type are set to SA. This ensures that NA can look up server MAC addresses.

- The NA Topology Gathering Diagnostic has run successfully. To verify this condition, search for tasks and check their results. This ensures that NA has gathered MAC addresses and tried to look them up in SA.

Integrating with OO

Overview

This section describes how system integrators and flow managers can use Server Automation (SA) to set up and run flows using SA. It also describes how users can run flows. Flows are operations that perform some of the most common automated tasks. SA-Operations Orchestration (OO) integration allows flow authors to build OO flows that are integrated with SA and users to run flows from SA. See OO documentation for more information about flows.

Before Integrating SA with OO, you must be familiar with SA, OO, OO flows, and OO jobs to implement the procedures described in the following section.

The section includes the following topics:

- "Setting up the integration"

- "Use cases: SA-OO flows"

- "Use cases: SA-OO jobs"

For more information about flows, refer OO documentation on SSO (https://softwaresupport.hpe.com/).

Supplementary information

This section contains supplementary information (such as tables and lists) related to SA-OO flows and jobs.

SA-OO flows

SA-OO integration flows

This section lists flow inputs. Flow authors can define the input name, input type, and template in OO. After these inputs are defined and flows are run, SA automatically populates their values into the OO-SA Library `SACoreInputs` table - you do not have to input these values manually.

For these inputs:

- If the input has a text, encrypted field, or free form list field, and OO provides a default value, the field will be filled with the default value. If there is no default value, then, if you followed the guidelines in the following table, SA will fill the text field with one of the known inputs, which you can modify.

- If the input has a single-select list field or multi-select list field, OO provides the values - you cannot modify these values.

For more information on defining flow inputs, see the OO documentation.

Flow inputs

Flow Inputs	Related to	Automatically assigned values (by SA)
coreHost and coreIPAddress	SA Core	Host and IP address of the SA core associated with the SA user who is logged in to the SA Client
coreUsername or coreUser	SA Core	User name associated with the SA user who is logged in to the SA Client
corePassword	SA Core	Password associated with the SA user who is logged in to the SA Client. SA will provide the password value only if the password is obfuscated in OO. The contents of the field are encrypted.
coreVersion	SA Core	Current SA core version SA provides these values
saServerIdentifier	SA Managed Server	Selected server identifiers: You can set two possible values (in OO): • Not Assigned (for one value) • List of Values (for multiple values) - Define the input as a freeFormList type in OO.
saServerScriptName	SA Managed Server	Name of the server script that is available in the SA core for that particular server's operating system Automatically assigned values: None Instead, the SA Client provides a widget that enables users to select a server script (excluding the OGFS script).
saServerName/hostName	SA Managed Server	DNS name of the selected server This value is filled in only if one server is selected. You can set two possible values (in OO):

Flow inputs, continued

Flow Inputs	Related to	Automatically assigned values (by SA)
		- Not Assigned (for one value) - List of Values (for multiple values) Define the input as a `freeFormList` type in OO.
platformName	SA Managed Server	Operating system name of the selected server This value is filled in only if one server is selected.
customerName	SA Managed Server	Customer name of the selected server selected This value is filled in only if one server is selected.
facilityName	SA Managed Server	Name of the facility where the selected server is located This value is filled in only if one server is selected.
`saJobId`	OO	Job ID of the SA job that was used to run the OO flow (tracked in OO using the reports feature) This input is not displayed.

SA-OO jobs

Java methods for handling blocked jobs

The `JobService` Java interface in the SA API provides Java methods for handling blocked jobs. These methods are the callbacks into SA that enable job approval integration.

> Users who invoke these methods must have the following required permissions: Edit or Cancel Any Job and View All Jobs.

What SA job types can be blocked?

The following table describes the SA job types that can be blocked.

Blockable SA job types

Job Type	Function
`Add Host to Virtualization Service`	Adds a host to the virtualization service.

Blockable SA job types, continued

Job Type	Function
`Add Virtualization Service`	Adds a virtualization service (to what is this added?).
`Clone Virtual Machine`	Clones a virtual machine on a VMware server.
`Convert Virtual Machine to VM Template`	Converts a virtual machine to a VM template.
`Create Snapshot`	Creates a snapshot that captures the configuration of a managed server at a particular point in time.
`Create Virtual Machine`	Creates a virtual machine.
`Create Virtual Zone`	Provisions a Solaris virtual machine (non-global zone) on a global zone (Hypervisor).
`Delete Virtual Machine`	Deletes a virtual machine.
Delete VM Template	Deletes the VM template.
`Deploy Virtual Machine from VM Template`	Deploys a virtual machine from a VM template.
`Edit Virtualization Service`	Edit the virtualization service.
`Install Patch`	Installs a patch on a managed server.
Install SA Agent	Install the SA Agent.
`Install Software`	Installs software on a managed server.
`Migrate Virtual Machine`	Migrate a virtual machine.
Modify Virtual Machine	Modify a virtual machine.
`Modify Virtual`	Modifies the properties of a Solaris virtual machine.

Blockable SA job types, continued

Job Type	Function
Zone	
Power Control Virtual Machine	Power control a virtual machine.
Push Configurations	Modifies configuration files on a managed server.
Reboot Servers	Reboots servers.
Reload Virtualization Data	Reloads the virtualization data.
Remediate Audit Results	Remediates servers based on the findings of an audit operation.
Remediate Policies	Remediates servers based on a software policy or a patch policy.
Remediate Snapshot Results	Remediates servers based on a snapshot. A snapshot captures the configuration of a managed server at a particular point in time.
Remove Virtual Zone	Removes a Solaris virtual machine (non-global zone) from a global zone (Hypervisor).
Remove Virtualization Service	Remove the virtualization service.
Restore Configurations	Restores a previous version of configuration files on a server. Every time you push configurations to a server, the previous configurations are saved and can be restored.
Rollback Software	Rolls back the software.
Run Agent Upgrade	Launches the SA Agent upgrade process.
Run Audit	Runs an audit.
Run Chef Recipe	Runs Chef recipes on a server.
Run Custom Extension	Runs a custom extension.

Blockable SA job types, continued

Job Type	Function
Run ISM Control	Runs an ISM (Intelligent Software Module) control. An ISM is an installable software package created with the ISM Development Kit (IDK). An ISM can contain control scripts that perform day-to-day, application-specific tasks, such as starting software servers.
Run OGFS Script	Runs an OGFS (Global File System) script on a server. The OGFS scripts allows you to execute scripts in the Global Shell from the SA Client.
Run OS Build Plan	Runs an OS builds plan.
Run OS Sequence	Provisions a server and installs an operating system using an OS sequence. An OS sequence defines what to install on an unprovisioned server, including OS build information from the OS installation profile, software and patch policies, and remediation settings.
Run Program Extension	Runs a custom feature added to SA. HPE can extend the functionality of SA by creating custom extensions to provide for specific customer needs.
Run Server Script	Runs a script on a server.
Uninstall Patch	Uninstalls a patch on a server.
Uninstall Software	Uninstalls software on a server.

The following table describes the SA JobService Java methods that you can use to handle blocked jobs.

SA JobService Java methods

Java method	Method description	SA CLI method examples
JobService. approveBlockedJob	Authorizes the job and unblocks it, allowing it to execute.	Within a Global Shell session: cd /opsw/api/com/opsware/job/JobService/method./approveBlockedJob self:i=$job_id
JobService. updateBlockedJob	Changes the	cd /opsw/api/com/opsware/job/JobService/ method./updateBlockedJob self:i=$job_id

SA JobService Java methods, continued

Java method	Method description	SA CLI method examples
	value of the `Ticket ID` field (corresponding to the `userTag` parameter) and `Reason` field (corresponding to the `blockReason` parameter) of the blocked job in the Job Status window of the SA Client. **Note:** You cannot change these fields using the SA interface.	userTag=$ticket_id \blockReason= "This type of job requires approval of CMB."
JobService. cancelScheduledJob	Cancels a blocked job and prevents it from executing. Changes the status of the blocked job from Awaiting Approval to Cancelled.	(Note that the ID parameter is jobRef, not self) cd /opsw/api/com/opsware/job/JobService/method./cancelScheduledJob jobRef:i=$job_id \reason="Job was scheduled to run outside of change window." A job that is currently running (`job_status` = `"ACTIVE"`) cannot be canceled.

SA JobService Java methods, continued

Java method	Method description	SA CLI method examples
JobService. findJobRefs	Searches all existing jobs and returns the IDs of all blocked jobs or jobs in other states, such as jobs in progress, expired jobs, and scheduled jobs. Can view jobs launched by other users.	Specify the job_status string in the filter, not the JobInfoVO.status integer. cd /opsw/api/com/opsware/job/JobService/method./.findJobRefs: i filter='job:{job_status = "BLOCKED" }'

The `job_id` attribute is required when a flow must come back to SA and interact with the job. Job blocking requires this attribute to be sent from SA to OO.

Job status values

This section describes the job-status values, which you can use in the `job_status` searchable attribute, as well as the corresponding integer values for the `JobInfoVO.status`, which you can examine if your client code has already retrieved the value object (VO).

"Job-Status Values" below lists allowed job-status values.

In a Java client, you can compare `JobInfoVO.status` with field constants such as `STATUS_ACTIVE`, instead of using the integers listed in this table.

Job-Status Values

Value of the job_ status searchable attribute	Value of JobInfoVO.status	Job status displayed in the SA Client	Job status description
ABORTED	0	Command Engine Script Failure	Job has finished running. A Command Engine failure has been detected.

Job-Status Values, continued

Value of the job_ status searchable attribute	Value of JobInfoVO.status	Job status displayed in the SA Client	Job status description
ACTIVE	1	In Progress	Job is currently running.
BLOCKED	11	Pending Approval	Job has been launched, but requires approval before it can run.
CANCELLED	2	N/A	Schedule has been deleted.
DELETED	3	Canceled	Job was scheduled but was later canceled.
EXPIRED	13	Expired	Current date is later than the job schedule's end date, so the job schedule is no longer in effect.
FAILURE	4	Completed with Errors	Job has finished running and an error has been detected.
PENDING	5	SCHEDULED	Job is scheduled to run once in the future.
RECURRING	12	RECURRING	Job is scheduled to run repeatedly in the future.
STALE	10	STALE	Opportunity for the blocked job to run has expired because it did not receive approval.
STATUS	15	TERMINATING	Job is in the process of shutting down in response to a user request to end the job.
STATUS	16	TERMINATED	Job ended early in response to a user request.
SUCCESS	6	COMPLETED	Job has finished running successfully.
TAMPERED	9	TAMPERED	Job has been tampered with.
UNKNOWN	7	Unknown	An unknown error occurred.
WARNING	8	Completed With Warnings	Job has finished running and a warning has been detected.
ZOMBIE	14	Orphaned	Job became orphaned.

Inputs Not Defined or Server Only Accepts One Device

When you try to run a flow, you might receive the following error:

```
SA will not pass the selected Device(s) to this flow. Either the flow does not have
the required ServerIdentifier input defined or the input only accepts a single
device.
```

If you receive this error, ask your administrator to check the `ServerIdentifier` input.

Setting up the integration

This section describes how administrators can build OO flows and jobs that are integrated with SA.

- Setting Up OO Flows

- Setting Up OO Jobs

Setting up OO flows

As an SA-OO integration administrator, you need to set user permissions, check that your system has the required environment, and import the required OO SDK Client Certificate.

Set user permissions

Users of OO flows must have the following OO permissions:

Required OO flow user permissions

Permission	Verify Permission Settings in the SA Client	
AdministerFlowIntegrations (ability to configure the OO integration settings)	Select Administration in the navigation panel. If the Flow Integrations option appears in the list of choices in the navigation tree, the permission has been granted.	
RunFlowOption (ability to run OO flows)	Select Devices in the navigation panel. Select Servers > All Managed Servers. Right-click a server name and choose Run. If the `Flow...` option is visible, the permission has been granted.	

Check the environment

Your system must have the following:

- SA version 10.0

- HPE Operations Orchestration (OO) version 10.x.

- OO installation server networked to an SA core server

- Valid OO SDK Client Certificate to communicate with OO (see Importing the OO SDK Client Certificate)

Import the OO SDK client certificate

You must import the certificate before users can run OO flows from SA.

> **Note:** If your architecture includes a master core and one or more secondary cores, follow the steps in this section for the master core and for *each* of the secondary cores. Similarly, if your SA computer has a sliced-core installation with one or more slices, repeat the steps for *each* slice.

To import the certificate:

1. Stop the Web Services Data Access Engine (Twist):

   `/etc/init.d/opsware-sas stop twist`

2. Transfer the OO Central Certificate to SA:

   (When you are prompted for a password for the next steps, use: `changeit`)

   a. Export the OO Central Certificate:

   The procedure to export the certificate may differ, depending on the OS version you have on your OO server. For more details see the OO documentation.

   > **Note:** The certificate export command must be run on the OO server (the client certificate is not bundled with SA).

   Example command, exporting from an OO 10.x instance installed on a Windows server:

   `<OO_INSTALL_DIR>\java\bin\keytool.exe -exportcert -alias tomcat -file C:\oocentral.crt -keystore <OO_INSTALL_DIR>\central\var\security\key.store`

   Next, make sure you copy the `C:\oocentral.crt` file to the SA core, under `/tmp/oocentral.crt`.

   b. Import the OO Central Certificate to the SA Java Runtime Environment (JRE) Keystore:

   `/opt/opsware/jdk1.8/jre/bin/keytool -importcert -alias oocert -file /tmp/oocentral.crt -keystore /opt/opsware/jdk1.8/jre/lib/security/cacerts`

   > **Note:** The example above uses the alias: oocert. However, any alias can be used when importing the certificate, as long as it is not already used in that keystore.

3. Check that the OO Central Certificate was imported successfully:

```
/opt/opsware/jdk1.8/jre/bin/keytool –list –alias oocert –keystore
/opt/opsware/jdk1.8/jre/lib/security/cacerts
```

Example output:

```
oocert, Feb 3, 2010, trustedCertEntry,
Certificate fingerprint (MD5): DF:DD:22:1B:A2:1E:A9:9C:1C:AF:8F:E0:14:1F:B5:E0
```

4. Restart the Web Services Data Access Engine (Twist):

```
/etc/init.d/opsware-sas restart twist
```

> **Note:** If a `jssecacerts` file is present in the same location as `cacerts`
> (`/opt/opsware/jdk1.8/jre/lib/security/`), either remove the `jssecacerts` file or make sure
> to import the certificate in `jssecacerts` instead of `cacerts`.

Setting up OO jobs

As an SA-OO jobs administrator, you need to create the following permissions so users can work with jobs in SA:

User Permissions

Permission	Description	Check in the SA Client	
AdministerFlowIntegrations	Configure the OO integration settings	Select Administration in the navigation panel. If the Flow Integrations option appears in the list of choices in the navigation tree, the permission has been granted.	
RunFlowOption (for users who want to run flows)	Run OO flows	Select Devices in the navigation panel. Select **Servers** > **All Managed Servers**. Right-click a server name and choose Run. If the Flow.. option is visible, the permission has been granted.	

Use cases: SA-OO flows

This section discusses use cases associated with SA-OO flows. The section is divided into two subsections: use cases for administrators, and use cases for end users.

Administrators: Configuring OO flows

As an administrator, you will need to configure OO flows and verify your changes and settings before your users can run flows in SA.

To configure flows:

1. In the SA Client navigation panel, select Administration >Flow Integrations.

2. In the Flow Integrations panel, click **Edit Settings** to display the Edit Flow Integration Settings window.

The Flow Integrations panel displays real-time information for the following users:

a. For Job Blocking: OO user who has permission to run the Approval Flow.

b. For Running Flows: OO user whose credentials are used to run flows from SA.

Any changes to user accounts (such as a disabled account or changes to OO credentials (user name, password, or URL)) are displayed instantaneously while this panel is open.

3. For running a flow, enter or change the following information:

   ○ OO URL - the location of the OO server in the following format:
   ```
   <protocol>://<hostname or host IP address>:<port number>/
   ```

   Examples:
   ```
   https://10.255.166.110:8443/
   https://10.255.166.110:8443/PAS/
   ```

   ○ OO user name and password ()

   For information about blocking jobs and the blocking job section of this window, see the SA-OO - blocking jobs section.

   A hyphen designates an unconfigured status, a red check mark designates an invalid status, and a green check mark designates a valid status. Both valid and invalid statuses are displayed with their latest verification timestamp.

4. Click **Verify Connection** to check the validity of the credentials you entered.

   If the connection status is valid, a check mark appears.

5. Click **Apply** to save the flow-integration settings changes.

   > **Note:** The **Apply** button is disabled if no data exists in the Edit Flow Integration Settings panel, if the data in the fields is incorrect, or if a check mark does not appear next to the connection status.

To verify flow changes and settings:

1. Log on to the SA Client.

2. In the navigation panel, select **Administration**.

3. In the navigation tree, select **Flow Integrations**.
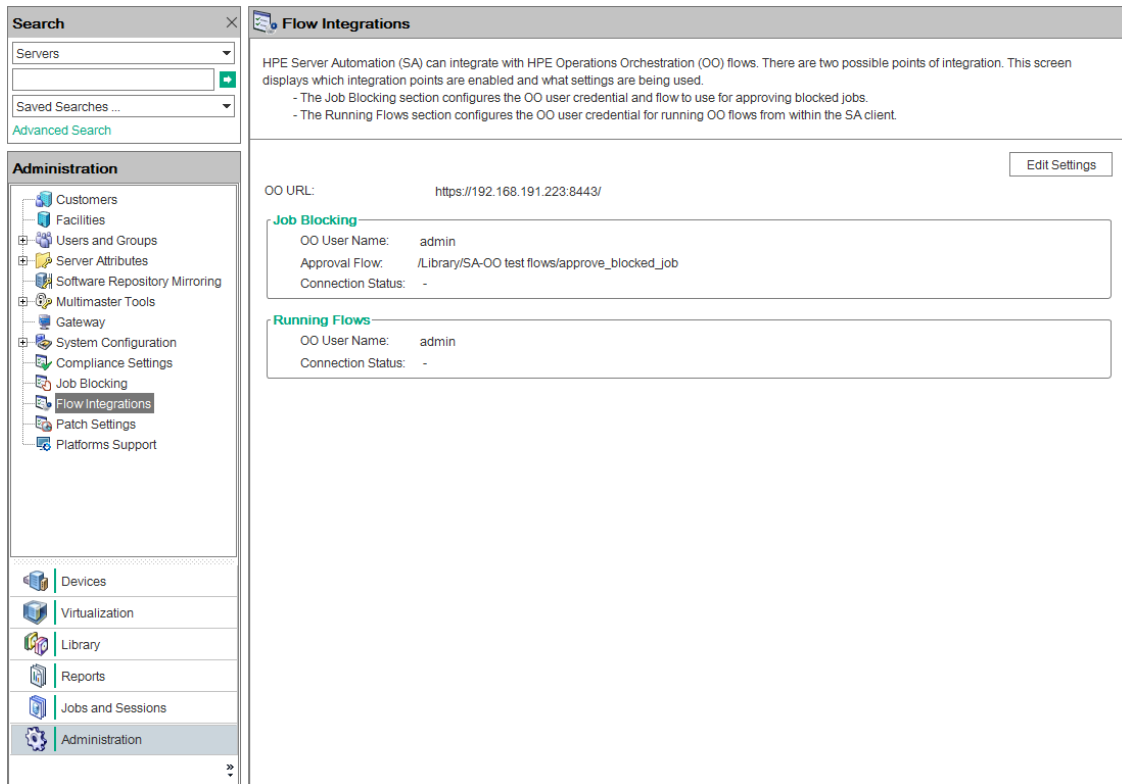
The Flow Integrations panel displays real-time information for the following users:

a. For Job Blocking: OO user who has permission to run the Approval Flow.

b. For Running Flows: OO user whose credentials are used to run flows from SA.

Any changes to user accounts (such as a disabled account or changes to OO credentials (user name, password, or URL)) are displayed instantaneously while this panel is open.

When the flow or job-blocking action is complete, a check mark appears next to the status.

Users: Running OO flows

Flows are operations that perform some of the most common automated tasks. SA-OO integration allows users to run flows from SA.

As a user, you can choose servers and flows; enter or choose a flow input, a runtime option, a scheduling option, and notification parameters; and add or delete servers.

To run flows:

1. In the SA Client navigation panel, select **Devices**.

2. In the top panel, select **Servers** > **All Managed Servers**.

    You must select a server before you can select a flow.

3. Right-click a server name.
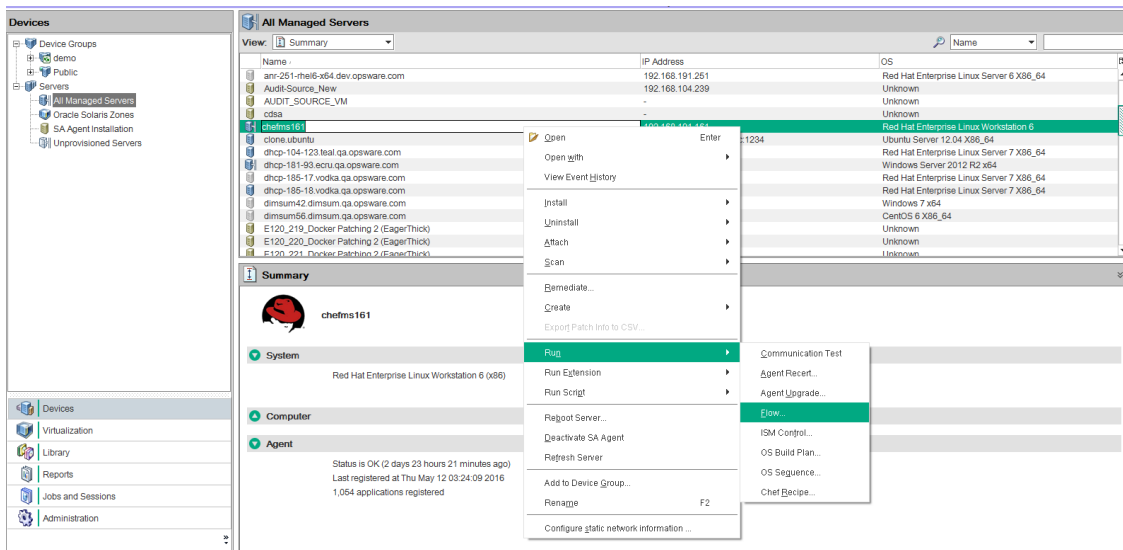
4. Select **Run** > **Flow**... to display the Select Flow OO window.
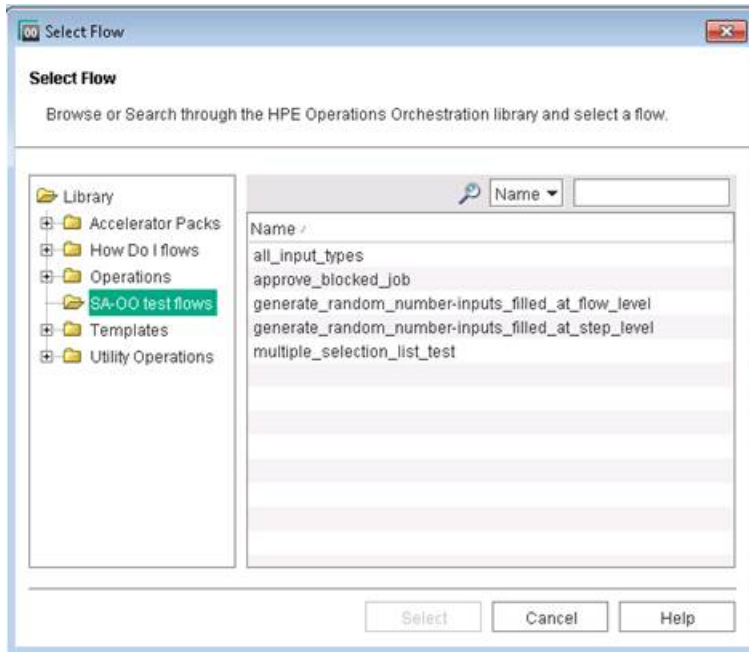
5. In the Select Flow window, select a flow category from the library tree to display its component flows.

6. In the name list, select a flow and click **Select** to display flow details in the Run Flow window.
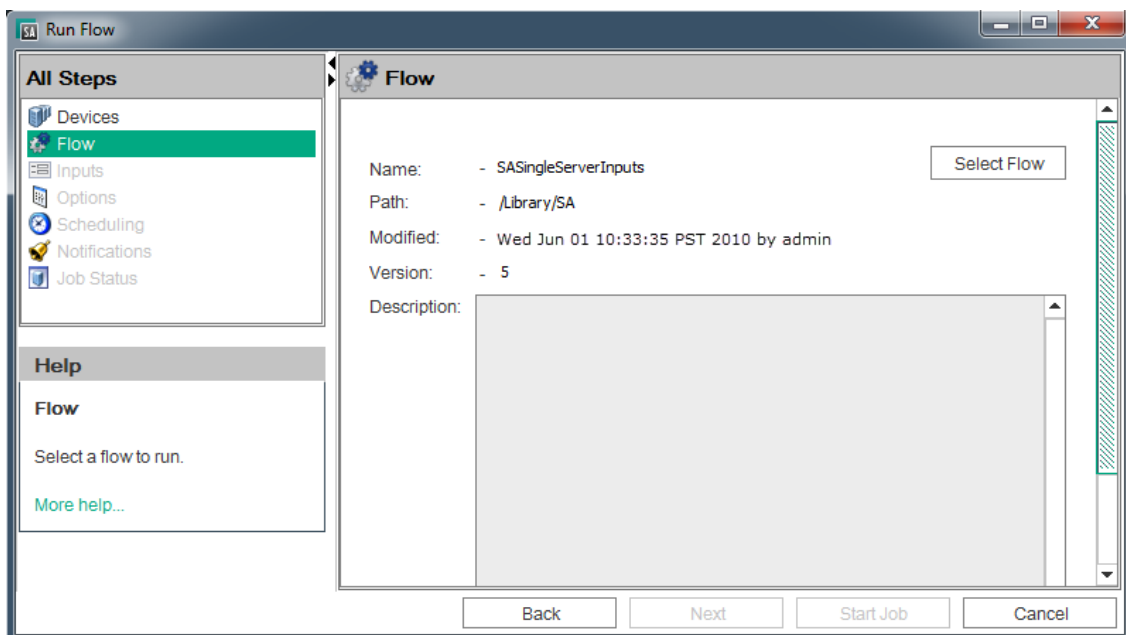
In the All Steps panel of the Run Flow Window, select each of the categories in turn (Inputs, Options, Scheduling, and Notification) to enter values for their parameters, as the rest of this procedure explains. Alternatively, you can choose **Next** from each panel to view the categories.

7. To enter values for flow inputs, select Inputs in the All Steps panel and enter values for the inputs that the panel displays (some values are automatically filled in for you).

   For example:

   a. `saServerScriptName` or click **Select Script** to display a list of scripts.

   b. `saServerName`

   c. `saServerIdentifier`

   See Flow inputs in Additional information for more information on inputs.

8. To enter values for runtime options, select Options from the All Steps panel, and enter a value for the job timeout. This is the number of minutes that the server will run a job before it times out. The default value is: 180 minutes and the timeout value is between 1 and 1440 minutes.

9. To select scheduling options, select Scheduling in the All Steps panel and enter values for:
   a. Schedule frequency

   b. Time and Duration

10. To enter notification information, click Notifications in the All Steps panel and add values for:
    a. Recipient email address

    b. Notifier (click **Add Notifier**)

    c. Ticket identification number (there are no conventions for the identification number - you can choose any number)

11. Click **Start Job** to start the job, or click Cancel to erase the choices you made in this session.

12. Click **Job Status** to view the status of the SA job. (optional)
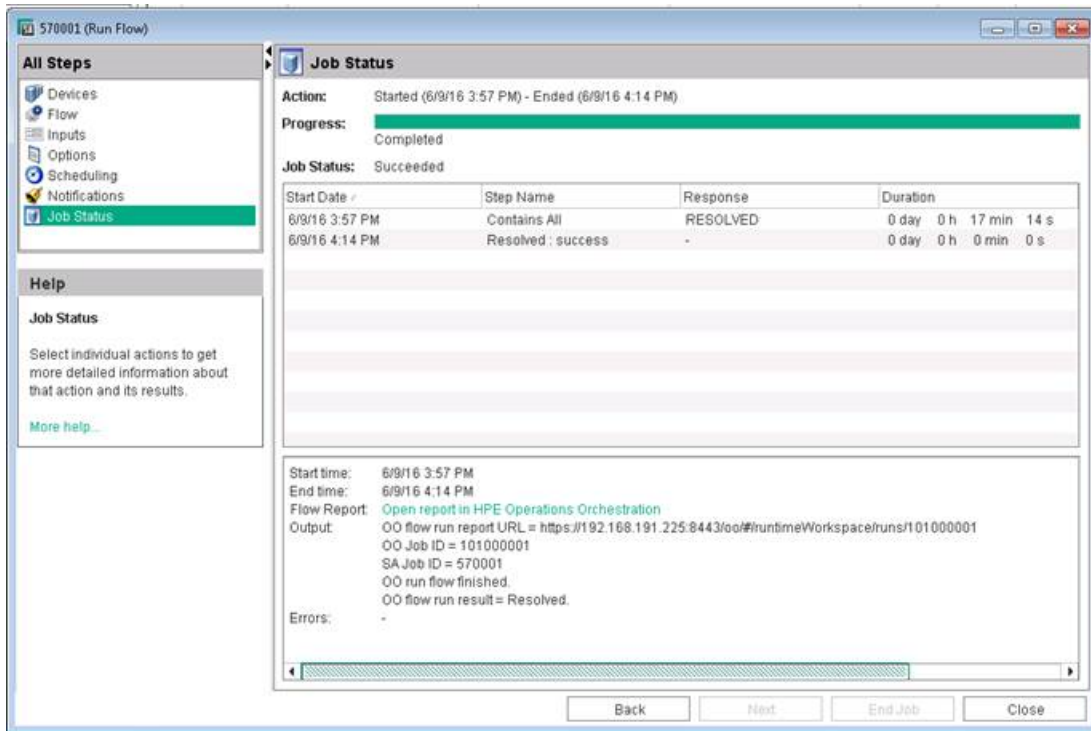
> The Job Status window does *not* display the flow run status, but rather the status of the SA job that starts and monitors the flow in OO.

When the SA job is complete, this window displays the status of each step in the flow (in the Response field) and a URL that points to more detailed flow-related information on OO.

It is possible that SA job monitoring succeeded even if at least one step failed. The OO API does not provide a call that precisely determines success or failure of the entire OO flow. Therefore, you cannot determine the success or failure of your OO flow from the SA Job Status screen or from the information provided at the URL.

To add or delete servers:

1. Run the flows.

2. In the All Steps navigation panel of the Run Flow Window, select **Devices**.

3. Right-click a server icon and choose **Add** or **Delete**, or click the plus or minus sign.

   The Select Servers and Device Groups window is displayed.

4. Click **Select** to add a server to the list of servers.

The Run Flow window displays the new server in the Devices panel, or shows that the removed server is absent.

Troubleshooting SA-OO integration

SA-OO connection error

If SA cannot connect to OO, administrators can:

- Check that the settings in the Edit Flow Integration Settings window fields are correct. See "Use cases: SA-OO flows" on page 40 for more information.)

- Examine the following log file for error messages on the Command Engine server:

  `/var/log/opsware/waybot/waybot.err`

  The error messages do not appear in the SA Client.

- Check that the OO URL, user name, and password are correct.

- Make sure the specified OO user has correct permissions to run the flow.

To check a flow status, see the Flow Integration Panel. For more information on this panel, see "Use cases: SA-OO flows" on page 40.

If you are a user and you see this error, check with your administrator.

Flow run error

This section describes errors you might encounter when you run a flow as a user.

Incorrect inputs

When you try to run a flow, you might receive one of the following error:

- SA will not pass the selected Device(s) to this flow.

- SA-OO Integration Configuration Error: Flow Integration Settings are incorrect. Please verify that the flow Integration URL, username, and password are correct.

Typically, these errors are displayed when one or more of the following occurred:

- You (as a user) selected the wrong flow to run.

- The OO server is not responding. Ask your administrator for help.

- The inputs an administrator entered in the Edit Flow Integration Settings window are incorrect. Ask your administrator to check the information in the Edit Flow Integrations Settings window. See "Use cases: SA-OO flows" on page 40 for more information.

- The flow author must modify the flow definition to use the naming conventions.

Use cases: SA-OO jobs

SA jobs are major processes, such as installing patches or checking compliance, that you run in the SA Client.

Administrators: Configuring OO jobs

As an administrator, you block jobs in accordance with configure

This section describes how system integrators and software developers can block SA jobs in SA, and approve or cancel jobs in SA using flows that call the SA API.

For more information on SA jobs, see the SA 10.50 Developer Guide.

You must be familiar with SA, Operations Orchestration (OO), SA jobs, and OO flows to block and unblock jobs.

The section includes the following topics:

- "Blocking jobs"

- "Approving and deleting blocked jobs"

For more information about jobs, see the SA 10.50 Developer Guide. For more information on working with OO, see the OO documentation on SSO on SSO (https://softwaresupport.hpe.com/).

Blocking jobs

You can block SA jobs from running if they might need to be reviewed and approved before they are executed. This section defines blocked jobs, describes several scenarios for blocking jobs, the types of jobs that can be blocked, the permissions needed to block jobs, how to block a job, how to disable job blocking, and how to view information related to a blocked job.

What are blocked jobs?

A blocked job is a job that:

- Belongs to a job type that can be blocked.

- Belongs to a job type that has been enabled for blocking by a system administrator.

- Has a block placed on it.

- Needs review before it should be run.

- Must get approved before it should be run.

Why should I block a job?

This section contains three sample scenarios of jobs that are candidates for job blocking and illustrate instances where job blocking might be needed.

Scenario 1

A job's approval should be postponed until the job can be run in the early morning hours if running it requires a system reboot. If the job were to run during regular business hours, it would disrupt normal work processes.

Scenario 2

Some jobs require further review before they can be run. For example, if a job updates a particular software application on a server, a Change Advisory Board (CAB) might need to review the proposed upgrade to make sure it does not conflict with other applications running in the environment. The board would determine if the job should run and when.

Scenario 3

In many IT environments, certain operations must be assigned tickets, assessed, and approved before they can be executed or cancelled. These jobs need to be blocked so the ticket can be created in the ticketing system, evaluated, and resolved.

How do I block and unblock jobs?

This section describes how to designate job types to block and how to disable job blocking.

How do I designate job types to be blocked?

1. In the SA Client, select **Administration** in the navigation pane.

2. Select **Job Blocking** in the navigation tree. The list of job types is displayed in the right pane with a check box next to each type.

   Blocking SA job types
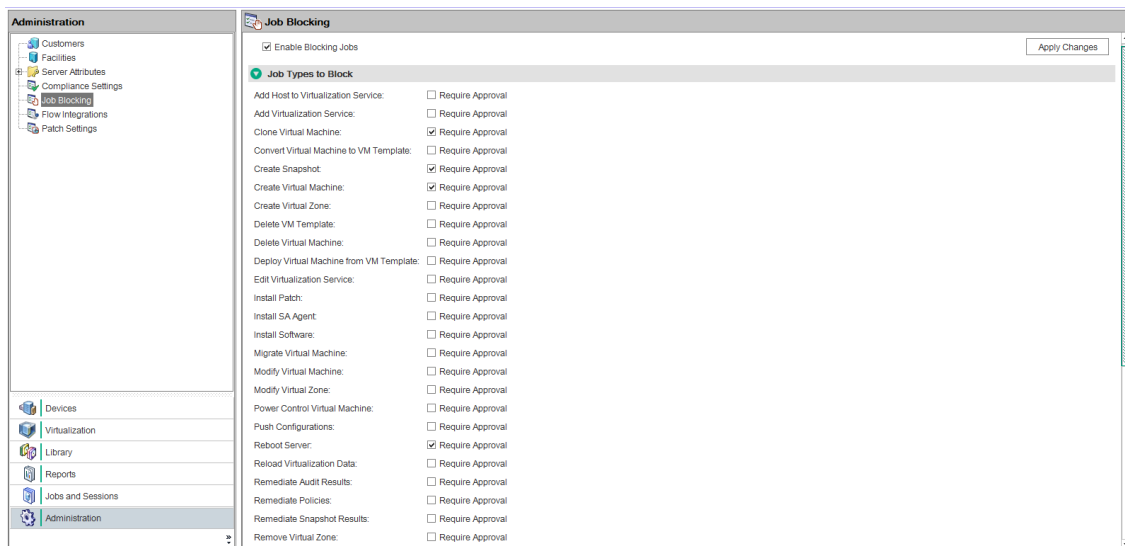
   See Blockable SA job types to see which types of jobs are available.

3. Select the check box: Enable Blocking Jobs.

   This action sets up the potential to block all job types listed in the panel.

4. In the panel below the Enable **Blocking Jobs** check box, select the check box next to each job type you want to block. Jobs that correspond to the blocked job type will be unable to run until they receive the appropriate approval.

This action designates individual job types to block.

5. Click Apply **Changes** to block jobs belonging to the job types you selected.

> **Note:** When you block jobs of a particular type, you block all future jobs that belong to that type until you deselect the Required Approval box for that job.

How do I disable job blocking?

1. In the SA Client, select **Administration** in the navigation pane.

2. Select **Job Blocking** in the navigation pane.

3. Deselect the check box corresponding to the job that you no longer want to block.

   This action disables job blocking for individual job types.

4. Above the list of job types, deselect the **Enable Blocking Jobs** check box. See the above figure.

   This action disables job blocking for all job types.

5. Click **Apply Changes**.

> **Note:** When you deselect the **Enable Blocking Jobs** check box, the checks next to the job types designated for blocking remain checked for your convenience.

How do I view blocked job information?

You can view OO connection information in the Flow Integrations panel and check job-status information in the job log.

Checking OO connection information in the SA flow integrations panel

Choose Administration > Flow Integrations to access the Flow Integrations Panel.
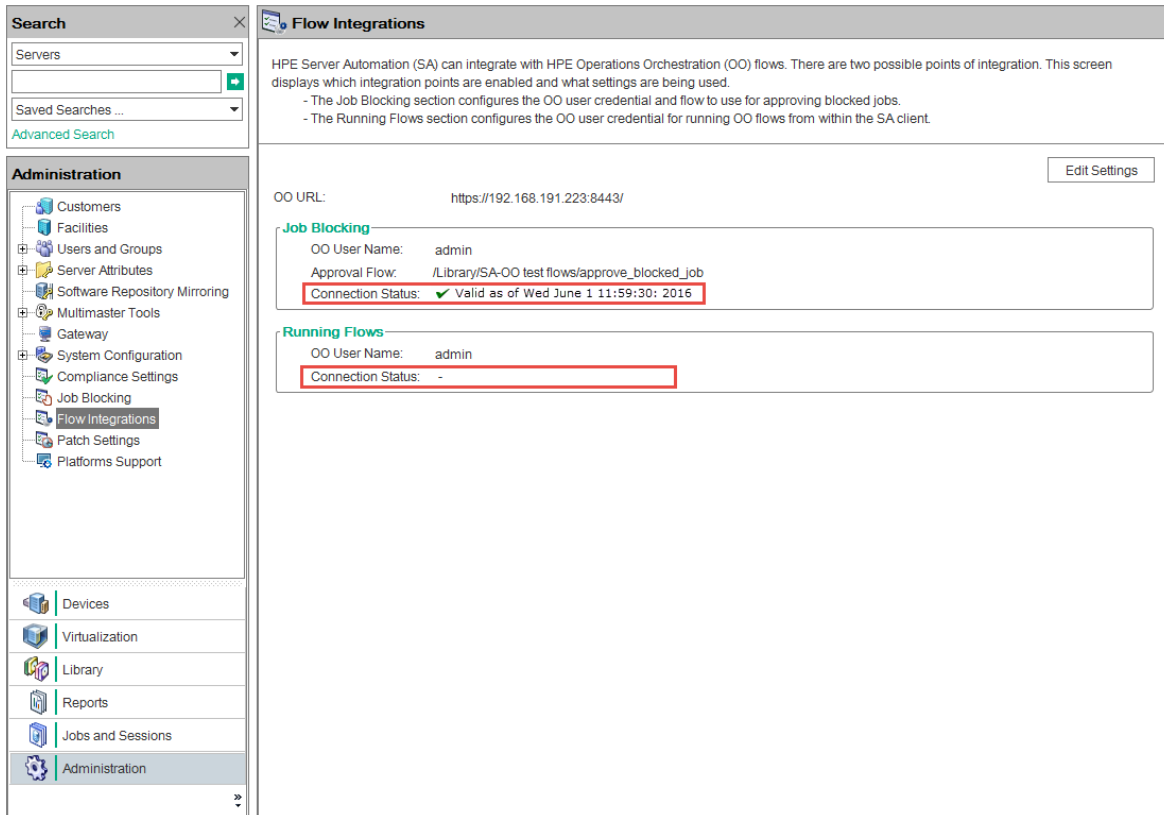
The Flow Integrations panel displays real-time information for the following users:

- **For Job Blocking**: OO user who has permission to run the Approval Flow

- **For Running Flows**: OO user whose credentials are used to run flows from SA

Any changes to user accounts (such as a disabled account or changes to OO credentials (user name, password, or URL)) are displayed instantaneously while this panel is open.

A check mark appears next to the status if the connection to OO is active.

Checking blocked job status in the job log

If you know a job has been blocked and you want to see whether the job block has been lifted, check the job log (choose Jobs and Sessions >Job Logs > Any Status).

For a list of possible job status values and what they mean, see Job-Status Values.

Configuring or editing a flow setting

To edit or configure a flow setting, you must be logged in to OO and SA.

In the SA Client navigation panel:

1. Select Administration > Flow Integrations.

2. In the Flow Integrations panel, click **Edit Settings** to display the Edit Flow Integration Settings window.
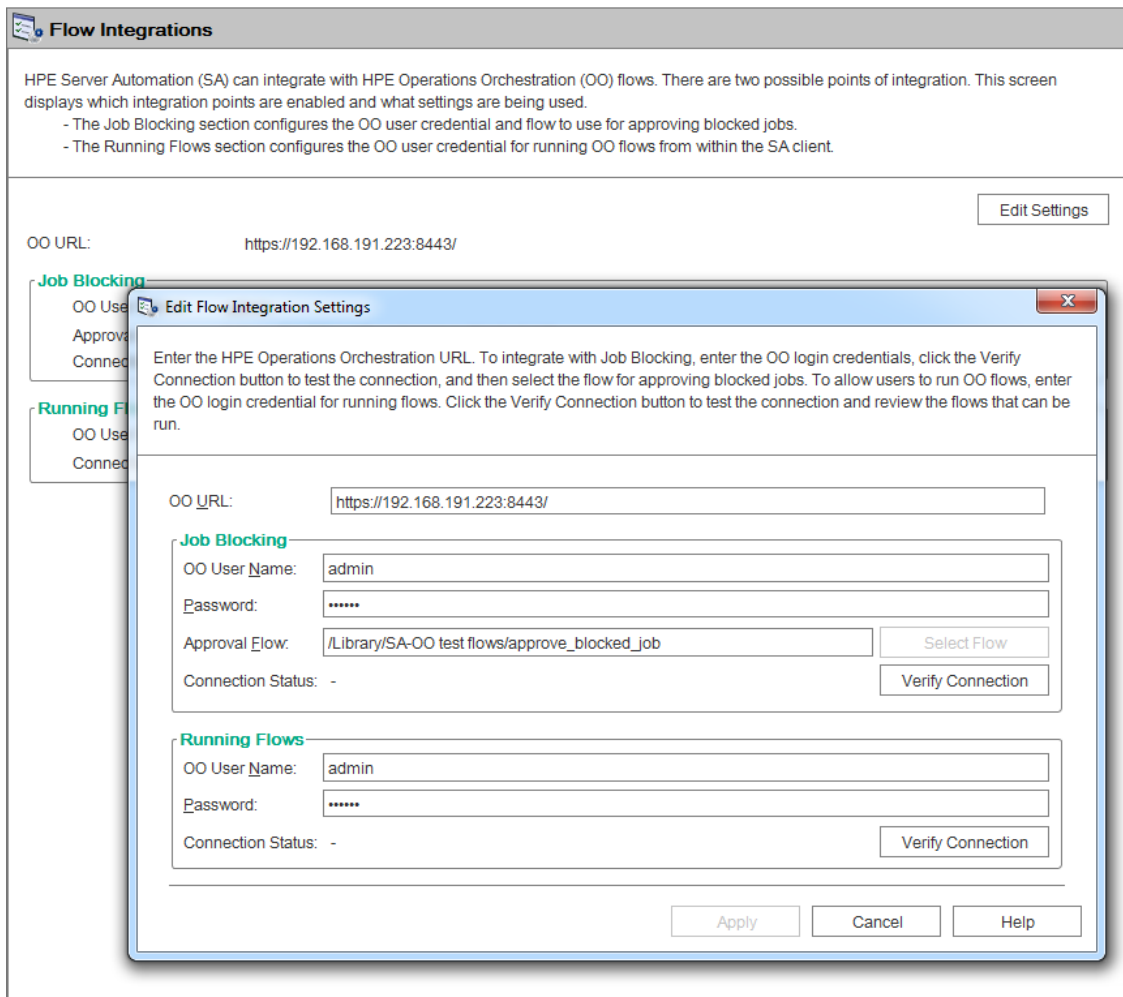
The Flow Integrations panel displays real-time information for the following users:

○ For Job Blocking: OO user who has permission to run the Approval Flow.

> **Note:** You can leave this value blank without affecting the integration.

○ For Running Flows: OO user whose credentials are used to run flows from SA.

Any changes to user accounts (such as a disabled account or changes to OO credentials (user name, password, or URL)) are displayed instantaneously while this panel is open.

> **Note:** Running Flows and Job Blocking can be set independently. However, you must enter the OO URL and all other inputs for at least one of these (Running Flows or Job Blocking). After Verify Connection is validated, the Apply button becomes enabled.

3. For running a flow, enter or change the following information:
   ○ OO URL - the location of the OO server in the following format:

   ```
   <protocol>://<hostname or host IP address>:<port number>/
   ```

   Examples:
   ```
   https://10.255.166.110:8443/
   https://10.255.166.110:8443/PAS/
   ```

   ○ Approval Flow - the location of the approval flow

   ○ OO user name and password of the user who is authorized to communicate with OO

   A hyphen designates an unconfigured status, a red check mark designates an invalid status, and a green check mark designates a valid status. Both valid and invalid statuses are displayed with their latest verification timestamp.

4. Click **Verify Connection** to check the validity of the credentials you entered.

   If the connection status is valid, a check mark appears.

5. Click **Apply** to save the flow-integration settings changes.

   > **Note:** The **Apply** button is disabled if no data exists in the Edit Flow Integration Settings panel, if the data in the fields is incorrect, or if a check mark does not appear next to the connection status.

Approving and deleting blocked jobs

You can use the SA Application Programming Interface (SA API) to approve or delete jobs. This API is the only way to manage blocked jobs. You cannot approve a blocked job through the SA Client. For information about using the SA API, see the SA 10.50 Developer Guide.

For information on blocking jobs using OO, see the OO documentation on SSO (https://softwaresupport.hpe.com/).

Integrating with uCMDB Connector

Overview

This topic describes the Universal Configuration Management Database (uCMDB) - Server Automation (SA) integration using the SA-uCMDB Connector. SA stores a large amount of information about your servers and software in the SA database. The SA-uCMDB Connector copies some of this data to the HPE uCMDB. Whenever the data in SA changes, the SA-uCMDB Connector automatically sends the updated data to the uCMDB Server.

You must be familiar with SA and uCMDB to implement the procedures described in this section.

> For up-to-date support and compatibility information, see the SA 10.5 Support and Compatibility Matrix for the relevant product release.

The topic includes the following topics:

- "Setting up SA-uCMDB integration "
- "Use cases"
- "Troubleshooting SA-uCMDB integration"

Setting up SA-uCMDB integration

To set up this integration as an administrator:

- Download the SA-uCMDB Connector
- Enable and start the SA-uCMDB Connector

set up the SA-uCMDB Connector, customize SA data sent to the SA-uCMDB Connector, transfer SA custom attributes to uCMDB, and customize data conversion functions.

Downloading the SA-uCMDB Connector

With the SA-uCMDB Connector, the SA Client provides the ability to launch the uCMDB Browser-Impact widget against an SA managed server.

The SA-uCMDB Connector is installed when you install SA. No separate installation is required.

If you are upgrading to Server Automation 10.5, the uCMDB Server must already be upgraded to release 10.01 or later.

To download the latest Cumulative Update Package:

This SA version requires uCMDB 10.01 or later. uCMDB 10.01 includes Content Pack 12.

The latest CUP HPE Software Patch is available on the SSO Portal at the following locations:

Linux: https://softwaresupport.hpe.com/group/softwaresupport/search-result/-/facetsearch/document/LID/UCMDB_00150

Windows: https://softwaresupport.hpe.com/group/softwaresupport/search-result/-/facetsearch/document/LID/UCMDB_00150

This site requires that you register for an HPE Passport and sign in.

For version support information, see the SA 10.5 Support and Compatibility Matrix on the HPE Software Support site.

Run the **enable** command to configure the SA-uCMDB Connector with the new uCMDB server.

> The syntax of the **enable** command varies depending on your environment. See "The enable command" on the next page in this document for an explanation of the **enable** command syntax and options.

Enter the following command to start the SA-uCMDB Connector:

```
/etc/init.d/opsware-sas start telldaemon
```

Optionally check the status of the SA-uCMDB Connector with the following command:

```
/etc/init.d/opsware-sas status telldaemon
```

Enabling and starting the SA-uCMDB connector

Before starting the SA-uCMDB connector, you must enable it to provide the following information: uCMDB server name or IP address, port number, login, and password. The **enable** command is located on your SA core server in the directory `/opt/opsware/tell/bin`.

To enable and start the SA-uCMDB connector, run the **enable** command to change the configurations of the SA-uCMDB Connector. There are multiple options for the **enable** command depending on your configuration.

The following is a simple example of this command:

```
enable --host myserver01.hpe.com --port 8888 --user ucmdb-admin

 --password leM93A3dme
```

For more information about the complete set of parameters, syntax, and options, see "The enable command" below.

Run the **start** command to restart the SA-uCMDB Connector:

```
/etc/init.d/opsware-sas start telldaemon
```

(Optional) Check the status of the SA-uCMDB Connector with the following command:

```
/etc/init.d/opsware-sas status telldaemon
```

For more information, see "Displaying the status of the SA-uCMDB connector" on page 73.

The enable command

Before you can start the SA-uCMDB Connector, you must enable it with the **enable** command. When you enable it, you provide the uCMDB server name or IP address, port number, login, and password.

Use the **enable** command to configure and enable the SA-uCMDB Connector. This section describes the **enable** command. You must enable the SA-uCMDB Connector before you can start it.

The **enable** command does the following:

Creates a custom SA-uCMDB Connector configuration file, /etc/opt/opsware/tell/tell_custom.conf, if it does not already exist. (By default, the custom configuration file does not pre-exist upon deployment unless one has been created manually.)

Modifies the custom configuration file, /etc/opt/opsware/tell/tell_custom.conf, and enters the uCMDB server's host name or IP address, port number, and login into this file.

Saves the user's password.

Modifies the file /opt/opsware/oi_util/startup/components.config and uncomments the lines for the telldaemon, which is the process for the SA-uCMDB Connector.

If you modify any of the uCMDB configuration parameters while the SA-uCMDB Connector is running, you must stop and restart the SA-uCMDB Connector for your changes to take effect.

Location of the enable Command

The enable command is located on your SA core server in the directory /opt/opsware/tell/bin.

New syntax in the enable command

In SA 9.14, additional parameters were added to the SA-uCMDB Connector's **enable** command in order to support the new uCMDB Browser. The new parameters are described in this section and in "New parameters for the enable command" below.

```
enable [--protocol <ucmdb_protocol>] [--host <ucmdb_host_ip>] [--port <ucmdb_host_
port_number>] [--browser_protocol <ucmdb_browser_protocol>] [--browser_host <ucmdb_
browser_host_ip>] [--browser_port <ucmdb_browser_host_port>] [--user <ucmdb_admin_
user>] [--password <ucmdb_admin_password>] [--help]
```

New parameters for the enable command

Parameter	Description	New
`--protocol <ucmdb_protocol>`	uCMDB server protocol, http or https. Default is http.	New
`--host <ucmdb_host_ip>`	This option gives the IP address or host name of your HPE uCMDB server. The default value is localhost.	—
`--port <ucmdb_host_port_number>`	This option gives the port number of your HPE uCMDB server. The default value is 8080.	—
`--browser_protocol <ucmdb_browser_protocol>`	uCMDB Browser server protocol, http or https. Default is http.	New
`--browser_host <ucmdb_browser_host_ip>`	This option gives the IP address or host name of your HPE uCMDB Browser host name or IP. The default value is localhost.	New
`--browser_port <ucmdb_browser_host_ port>`	This option gives uCMDB Browser host port. The default value is 8080.	New

New parameters for the enable command, continued

Parameter	Description	New
`--user <ucmdb_admin_user>`	This option gives the user name of an administrative user for your HPE uCMDB server. The default value is admin.	—
`--password <ucmdb_admin_password>`	This option gives the password for the user provided in the `--user` option. The default value is admin.	—

Example of **enable** command without SSL enabled:

enable —protocol http --host 192.168.8.93 --port 9999 —browser_protocol http —browser_host 192.168.8.100 —browser_port 8888 --user john-ucmdb --password mypass1234

Example of **enable** command with SSL enabled for the uMCDB Server and the uCMDB Browser:

enable —protocol https --host 192.168.8.93 --port 9999 —browser_protocol https —browser_host 192.168.8.100 —browser_port 8888 --user john-ucmdb --password mypass1234

Customizing SA data sent to the uCMDB server

Mapping file

The SA-uCMDB Connector XML mapping file describes the data being transferred by the SA-uCMDB Connector and enables you to customize the data mappings.

The initial mapping.xml is generated when the connector first runs. After it is generated, you can find the new mapping file at:

`/etc/opt/opsware/tell/metadata/mapping.xml`

The mapping file allows you to control:

- Data types and attributes that populate uCMDB

- Mappings between the optional SA custom attributes and the uCMDB Data Model Configuration Item (CI) attributes.

See for the complete original mapping file contents.

Customizing the mapping file

In order to customize how data is mapped, you need to create and modify the *mapping_custom.xml* file, and then restart the Connector.

> The **mapping_custom.xml** file is not used by default, so you need to restart the Connector to engage the customized mapping file.

To customize the uCMDB Connector mappings:

1. If the uCMDB Connector is running, you must stop and disable the Connector before editing the mapping file.

   See "Stopping and disabling the SA-uCMDB connector" on page 72 for instructions.

   IMPORTANT: Make sure the connector is stopped and disabled. If the connector is not stopped and disabled when you edit the mapping file, you may encounter problems when you try to restart the Connector.

2. Create the custom mapping file:
   a. Go to: `/etc/opt/opsware/tell/metadata`

   b. Copy the mapping.xml file to the same folder and name the copy mapping_custom.xml.

   The mapping_custom.xml file must be in the same specified folder as the mapping.xml file to function properly.

3. Edit the `/etc/opt/opsware/tell/metadata/mapping_custom.xml` as needed.

   See "Editing the mapping file" on the next page for details on how to edit the mapping file for different purposes.

4. Run the **enable** command to change the configurations of the SA-uCMDB Connector.

   The syntax of the **enable** command varies depending on your environment. See "The enable command" on page 59 in this document for an explanation of the **enable** command syntax and options.

5. Run the **start** command to restart the SA-uCMDB Connector:
   `/etc/init.d/opsware-sas start telldaemon`

6. Optionally check the status of the SA-uCMDB Connector with the following command:
   `/etc/init.d/opsware-sas status telldaemon`

Editing the mapping file

All customized mappings are defined in the **mapping_custom.xml** configuration file, so administrators can easily view and edit them. The XML mapping file can be modified to change the data being transferred by the SA-uCMDB connector. The mapping file also provides the ability to choose to omit specific CI and attributes. If the **mapping_custom.xml** does not exist, the connector by default will honor the out of box **mapping.xml**.

Permissions: In order to view or edit the **mapping_custom.xml** file, you must first log in to the SA Core as root in order to have read/write privileges.

> **Note:** This section describes your editing options within the customized mapping file. For instructions on the process for customizing the mapping file, including when you need to stop and start the connecter in order to make the changes take effect, see "Customizing the mapping file" on the previous page.

Illustration of a mapping file

Here is a snippet of the out-of-the-box mapping file:

```
<Model-Definition model-name='hosts'>
      <CI ucmdb-ci-type-name='node' enable='true' base-class='node'
            <Attribute source='Node/Name' target-attr='name' enable='true'/>
            <Attribute source='Node/Description' target-attr='description'
      enable='true'/>
      </CI>
</Model-Definition>
```

where the highlighted text indicates editable fields.

> **Note:** See "Example– SA-uCMDB Connector Mapping File" on page 83 for a complete out-of-the-box mapping file.

Each Model Definition tag in the mapping file defines a specific model name. In this example, this Model-Definition defines the 'hosts' model.

Each model can contain many Configuration Items (CIs). Each CI tag defines the composition of the CI. In this example, 'node' is the CI being defined.

For each attribute, **source** indicates the default attribute name in the source database.

- The **target-attr** field specifies the uCMDB attribute name that the source is mapping to.

- The **enable** field defines whether to map the attribute. The default value for **enable** is 'true'; which means the attribute will be loaded into the uCMDB. When you set **enable** to 'false', you are choosing not to map the attribute; which means the attribute will not be loaded to uCMDB.

XML attribute values

This section shows the XML attribute values, indicating the editable and non-editable values:

> **Caution:** Do not change non-editable attribute values. It is crucial that the non-editable values, such as, source='Node/Name', remain unchanged. Changing these values can prevent the synchronization from running properly and can lead to errors.

XML attributes

XML attribute tag	Attributes	Sample attribute values and notes	Editable?
Model-Definition	model-name	'hosts', 'sa', 'software', 'compliance', 'hypervisor', 'vmrelations', 'compliance_status'	NOT editable
	enable	'true' to enable this attribute; 'false' to disable	Editable
CI	ucmdb-ci-type-name	Specifies the uCMDB CI type. For example: 'node', 'ip_address'	Editable
	enable	'true' to enable this attribute; 'false' to disable	Editable
Attribute	source	Specifies the SA custom attribute name. For example: 'Node/Name', 'Node/Description', 'Node/BiosAssetTag', 'Node/BiosSerialNumber', 'Node/Facility', 'Node/VirtualizationTypeId' **Caution:** Do not edit the source value. Modifying the source value will damage the mapping and may cause errors.	NOT editable
	target-attr	Specifies the uCMDB attribute name that the source is mapping to. For example: 'name', 'description' NOTE: target-attr value must be a unique name.	Editable
	enable	'true' to enable this attribute; 'false' to disable.	Editable
	conversion-name	Only used for conversion functions. See "Customizing the data-conversion function " on page 68 for details. For example:	Editable

XML attribute tag	Attributes	Sample attribute values and notes	Editable?
		'com.hpe.tell.ConversionMethod$com.hpe.tell. MyConvertVirtualizationType'	
Attribute-Custom	sa-custom-attribute-key-value	Specifies the SA custom attribute name. For example: 'HW_RACK', 'DEVICE_RACK' NOTE: See "How to work with SA custom attributes " on the next page.	Editable
	target-attr	Specifies the uCMDB attribute name that the source is mapping to. For example: 'serial_number', 'facility' NOTE: target-attr value must be a unique name.	Editable
	enable	'true' to enable this attribute; 'false' to disable.	Editable
CI-Filter	enable	'true' to enable this attribute; 'false' to disable. NOTE: See "Filter support for queries " on page 67 for modifying CDATA block.	Editable
Relation	ucmdb-relation-type-name	Specifies uCMDB relationship between the CIs. For example: 'containment', 'aggregation'	Editable
	ucmdb-relation-from-ci-type-name	Specifies uCMDB relationship between the CIs of the 'from' CI. For example, if specifying a containment relationship from node to ip_address, the 'node' would be the 'from' CI in this relationship.	Editable
	ucmdb-relation-to-ci-type-name	Specifies uCMDB relationship between the CIs of the 'to' CI. For example, if specifying a containment relationship from node to ip_address, the 'ip-address' would be the 'to' CI in this relationship.	Editable
	enable	'true' to enable this attribute; 'false' to disable.	Editable
	ucmdb-relation-id-link	'true' if the relationship contains an ID link. This 'true' value requires the 'from' CI to exist, 'false' if the relationship does not contain an ID link.	Editable

Model definitions

"Model definitions" below shows model definitions. There are 7 models defined in the mapping file that define how data objects are represented in uCMDB. For example, the SA model would represent SA in uCMDB.

Model definitions

Model definition model-name	Description
'sa'	generates installed_software.xml
'hosts'	generates node.xml
'software'	generates installed_software.xml
'compliance'	generates policy-xml
'hypervisor'	generates hypervisor.xml
'vmrelations'	generates hypervisor.Relationxml
'compliance_status'	generates policyResult.xml

Note: These XML files are generated internally based on the mapping file and should not be edited directly. Editing the generated XML files directly is not supported. Any changes made to the generated files will be overwritten.

How to work with SA custom attributes

Note: All editing of mapping files must be done in the mapping_custom.xml file. Do not edit the out-of-the-box mapping.xml file. Editing the mapping.xml file directly can prevent the synchronization from running properly and can lead to errors.

Transferring SA custom attributes to uCMDB

Custom attributes can also be loaded to uCMDB.

In addition to the SA attributes that are synchronized with uCMDB, the mappings in the **mapping_custom.xml** file enable you to specify any SA Custom Attributes defined with an SA Device or inherited from SA Facilities.

Custom Attributes can be specified in the **mapping_custom.xml** file as follows:

The following example shows how a user could configure the mapping file to extract the custom attribute, *DEVICE_RACK*, and load it to the *my_location_rack* destination in uCMDB. The **enable** attribute is set to 'true,' showing that the user chose to load this attribute to uCMDB.

```
<CI ucmdb-ci-type-name='node' enable='true' base-class='node'>
      <Attribute-Custom sa-custom-attribute-key-value='DEVICE_RACK' targetattr='
      my_location_rack' enable='true' />
</CI>
```

where the highlighted text indicates editable fields.

Filter support for queries

The **mapping_custom.xml** file provides the capability to filter specific criteria.

To filter by specific criteria:

- Embed the filtering clause in the CDATA section under CI-Filter tag.

- Specify whether the filter is enabled by supplying the value for **enable** attribute ('true' to enable, 'false' to disable).

  Note: The CI-Filter specification is based on the SA database and requires knowledge of the SA schema. You can only supply one CI-Filter per CI type. If multiple filters are needed, you can specify a simple filter expression using AND and OR clauses.

Example of a single filter (out-of-the-box mapping in mapping.xml file):

```
<CI ucmdb-ci-type-name='node' enable='true' base-class='node'>
      <Attribute source='Node/Name' target-attr='name' enable='true' />
      <CI-Filter enable='true'><![CDATA[(DEVICES.OPSW_LIFECYCLE =
'MANAGED')]]></CI-Filter>
</CI>
```

In the above example, the filter selects SA devices with State: 'managed'. By default, the SA-uCMDB Connector only synchronizes Managed device objects.

Example of a filter which includes an AND clause (modified mapping in mapping_custom.xml):

```
<CI-Filter enable='true'><![CDATA[(DEVICES.DVC_MODEL = 'POWEREDGE 2950') and
(DEVICES.DVC_ID > 300000000)]]></CI-Filter>
```

In the above example, the filter selects SA devices with BOTH the Model, 'POWEREDGE 2950', and the ID greater than '300000000'.

Extended out-of-the-box mappings

The mapping file is provided to enable you to:

- Change names of attributes being populated in uCMDB

- Change how data is populated in uCMDB

- Specify which uCMDB CI type gets populated

Additional out-of-the-box mappings

The **Facility** and **VirtualizationType** attributes are disabled by default in the out-of-the-box mapping file. However, they may be enabled, as shown below:

ServerVO.getFacility()

```
<Attribute source='Node/Facility' target-attr='facility' enable='true'/>
```

ServerVO.getVirtualizationType()

```
<Attribute source='Node/VirtualizationTypeId' target-attr='virtualization_type_id'
enable='true'/>
```

Customizing the data-conversion function

If data to be populated in uCMDB needs to be tailored during synchronization, Custom conversion methods can be written and provided to the SA-uCMDB Connector. The SA-uCMDB Connector can, then, apply these functions to transform the data from the SA syntax to the desired uCMDB syntax. For example, you can write custom conversion methods to convert lower case to upper case, or bytes to megabytes, and so on.

Customized conversion functions should be provided to the SA-uCMDB Connector via a jar file named tell_conversions.jar, and placed in `/etc/opt/opsware/tell/lib` prior to the connector startup. After you restart the connector, the custom conversion java class should extend the **ConversionMethod** class and import the **com.hpe.tell.ConversionMethod** package.

To customize data conversion:

1. If the SA-uCMDB Connector is running, you must stop and disable the Connector before editing the mapping file.
   - Run the **stop** command to stop the SA-uCMDB Connector:
     ```
     /etc/init.d/opsware-sas stop telldaemon
     ```
   - Run the disable command to disable the SA-uCMDB Connector:
     ```
     disable
     ```

     Note: Make sure the connector is stopped and disabled. If the connector is not stopped and disabled when you edit the mapping file, you may encounter problems when you try to restart the Connector.

2. Write the customized conversation function code in java.

   For example, see "Sample conversion file – MyConvertVirtualizationType.Java" on the next page. In this example, the conversion file's name is MyConvertVirtualizationType.java.

3. Modify the mapping_custom.xml file to utilize the conversion file that you just created.

   For example, you would place the following line in the mapping_custom.xml file to point to the java file, **MyConvertVirtualizationType.java**:

Original text in mapping file

```
<Attribute source='Node/VirtualizationTypeId' target-attr='virtualization_type_id'
enable='false'/>
```

Customized text in mapping file

```
<Attribute source='Node/VirtualizationTypeId' target-attr='device_isVirtual'
enable='true' conversion-
name='com.hpe.tell.ConversionMethod$com.hpe.tell.MyConvertVirtualizationType'/>
```

This modified line of XML has the following values:

- '**device_isVirtual**' is the new attribute value for target-attr. Because this conversion changes the data type, it should be mapped to a different uCMDB attribute. However, if you are not changing the data type, then you should map to the same target-attr value.*

- conversion-name is the XML name for the conversion attribute. This is a verbatim label and cannot be substituted.

- '**com.hpe.tell.ConversionMethod$com.hpe.tell.MyConvertVirtualizationType**' is the attribute value for conversion-name, and MyConvertVirtualizationType.java is the java conversion code file name.

The target-attr value is critical to the success of the conversion operation:

Changing data types

If the conversion is changing an attribute's data type, make sure that the destination attribute (specified by **target-attr**) has the same or compatible requirements, such as length and format. In the previous example, we modified the **target-attr** value because the conversion changes the actual data type. If, for example, you were merely converting the unit of measure (UOM), then you could specify the same **target-attr** value, because the actual data type did not change.

Unique filename per target-attr

Each **target-attr** conversion requires a unique java conversion code filename. The java conversion file represents a singular target-attr (output). For example, you can have multiple **target-attr** conversion scenarios for a single source attribute; however, each **target-attr** must be stated on an individual attribute tag in the mapping file, as shown in the following example:

```
<Attribute source='Node/VirtualizationTypeId' target-attr='virtualization_type_id1'

enable='true' conversion-
name='com.hpe.tell.ConversionMethod$com.hpe.tell.MyConvertVirtualizationType1'/>

<Attribute source='Node/VirtualizationTypeId' target-attr='virtualization_type_id2'

enable='true' conversion-
name='com.hpe.tell.ConversionMethod$com.hpe.tell.MyConvertVirtualizationType2'/>
```

4. Compile the customized conversion file (MyConvertVirtualizationType.java in this example). This generates the executable binaries.

5. Compress all of the conversion binaries into a jar file with the following name: tell_conversions.jar.

   Note: You must use this exact jar filename for the SA-uCMDB Connector to recognize it.

6. Place the jar file in the SA Core directory, /etc/opt/opsware/tell/lib, prior to the starting up the uCMDB Connector.

   Note: You must use this exact directory path for the SA-uCMDB Connector to recognize it.

7. Start the SA-uCMDB Connector.

The conversion function will convert the data dynamically, at the time the SA-uCMDB Connector is restarted.

Sample conversion file – MyConvertVirtualizationType.Java

This sample conversion file provides sample java code to use as a guideline. This java sample converts an SA **VirtualizationType** from Type: Numeric into Type: String for uCMDB.

Note: You can only have one attribute conversion per java file. To convert multiple attributes, you need to have multiple java files. Each target attribute can only have one conversion.

Tip: Name the conversion file based on the attribute being modified. As in this example, the java filename is MyConvertVirtualizationType because it is modifying the VirtualizationType attribute.

```
package com.hpe.tell;

import java.math.BigDecimal;
```

```java
import com.hpe.tell.ConversionMethod;

public class MyConvertVirtualizationType extends ConversionMethod {

        public Object convert(Object value) throws Exception{

                Integer vType = putInteger(value);

                String vValue;

                /*
                 * Function to convert SA VirtualizationType (numeric) to string type For uCMDB.
                 */

                if (vType > 0) {

                        vValue = "True";

                } else {

                        vValue = "False";

                }

                return vValue;

        }

        private Integer putInteger(Object o) throws Exception {

        if (o instanceof String) {

            return Integer.valueOf((String) o);

        }

        if (o instanceof BigDecimal) {

          return ((BigDecimal)o).intValue();

        }

        if (o instanceof Integer) {

          return (Integer)o;

        }

        throw new Exception("Invalid conversion in putInteger "+o.getClass
().toString());

    }

}
```

Use cases

This section contains information you will need to work with the SA-uCMDB Connector after it is set up.

Stopping and disabling the SA-uCMDB connector

If the SA-uCMDB Connector is running, you must stop and disable the Connector before making any kind of configuration change.

The stop command

When you stop the SA-uCMDB Connector, it will stop transferring data from the SA database to uCMDB. To stop the SA-uCMDB Connector, enter the following command on an SA core server:

`/etc/init.d/opsware-sas stop telldaemon`

This stops the SA-uCMDB Connector.

If the SA-uCMDB Connector is disabled, the output will look like the following:

```
opsware-sas: One or more of the specified components does not exist in the
following file:
```

`/opt/opsware/oi_util/startup/components.config`

If you no longer need the SA-uCMDB Connector, you can disable it with the disable command. For more information, see "The disable command" on the next page.

The disable command

Use the **disable** command to disable the SA-uCMDB Connector. If the SA-uCMDB Connector is running, the **disable** command will stop it before disabling it. If the SA-uCMDB Connector is disabled, you will not be able to start it.

The **disable** command modifies the file /opt/opsware/oi_util/startup/components.config and comments out the lines for the **telldaemon**, which is the process for the SA-uCMDB Connector.

Location of the disable Command

The **disable** command is located on your SA core server in the directory /opt/opsware/tell/bin.

Syntax of the disable Command

/opt/opsware/tell/bin/disable

To stop and disable the SA-uCMDB Connector:

Run the **stop** command to stop the SA-uCMDB Connector:
```
/etc/init.d/opsware-sas stop telldaemon
```

Run the **disable** command to disable the SA-uCMDB Connector:
```
disable
```

> **Note:** Make sure the connector is stopped and disabled before making any configuration change. If the connector is not stopped and disabled, you may encounter problems when you try to restart the Connector.

Displaying the status of the SA-uCMDB connector

To display the status of the SA-uCMDB Connector, enter the following command on an SA core server:

```
/etc/init.d/opsware-sas status telldaemon
```

If the SA-uCMDB Connector is enabled but not running, the output will look like the following:

```
Verify "telldaemon" running: FAILURE (pidfile does not exist)
Failed to perform "status" operation on Opsware SAS components.
```

If the SA-uCMDB Connector is disabled, the output will look like the following:

```
opsware-sas: One or more of the specified components does not exist in the
following file:
/opt/opsware/oi_util/startup/components.config
```

SA-uCMDB data relationship and transfer

CI relationships maintained

The "CI relationships maintained" below table lists the Configuration Item (CI) relationships maintained by the SA-uCMDB Connector.

CI relationships maintained

From uCMDB CI	Via	From uCMDB CI
Node	containment	IpAddress
Node	composition	InstalledSoftware
Node	composition	Hypervisor
Node	aggregation	PolicyResult
Hypervisor	ExecutionEnvironment	Node
Policy	composition	PolicyResult
SaSystem	aggregation	Node
SaSystem	aggregation	Policy

Example: uCMDB showing an SA managed server

The "SA managed servers displayed in the uCMDB" below figure is from an HPE uCMDB screen and it shows:

- One SA managed server named "atari."

- The managed server's IP address 10.12.10.65.

- The managed server "atari" is running a VMware hypervisor.

- Two virtual machines are running on the hypervisor named "gofish" and "miracles."

SA managed servers displayed in the uCMDB
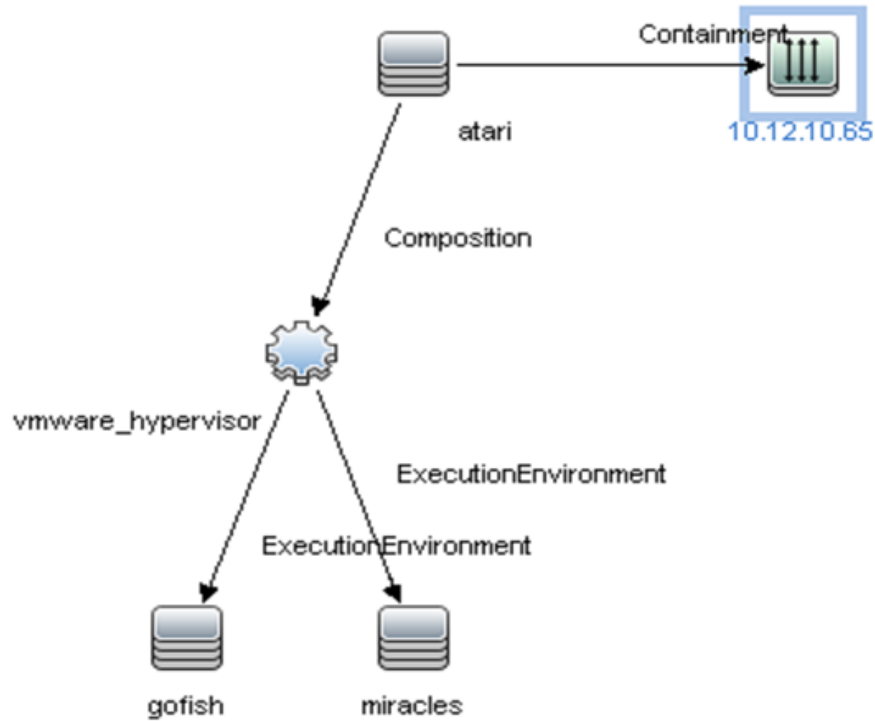
SA data transferred to uCMDB

The following data from the SA database is transferred to the uCMDB Configuration Items (CI) and Attributes (see the below table):

uCMDB CIs and attributes populated by SA

uCMDB CI	uCMDB Attribute
Node	Name
Node	Description
Node	BiosAssetTag
Node	DefaultGatewayIpAddress
Node	NodeModel
Node	SerialNumber
Node	BiosUuid
Node	NetBiosName
Node	MemorySize

uCMDB CIs and attributes populated by SA, continued

uCMDB CI	uCMDB Attribute
Node	OsDescription
Node	OsFamily
Node	TenantOwner
IpAddress	Name
IpAddress	RoutingDomain
InstalledSoftware	Name
InstalledSoftware	Vendor
InstalledSoftware	BuildNumber
InstalledSoftware	DmlProductName
Hypervisor	Name
Hypervisor	Description
Hypervisor	ProductName
Policy	Name
Policy	Description
Policy	PolicyCategory
Policy	PolicyDefinedBy
PolicyResult	Name
PolicyResult	PolicyResultDateTime
PolicyResult	ComplianceStatus
PolicyResult	RulesCompliant
PolicyResult	RulesNonCompliant
PolicyResult	ComplianceLevel
SASystem	Name
SASystem	Description
SASystem	Version

Frequency of data transfer to uCMDB

When the SA-uCMDB Connector first starts running, it queries the SA database, creates the CIs in the uCMDB and transfers the data from SA to the uCMDB. After that, whenever the data in the SA database changes, the SA-uCMDB Connector automatically detects the changes and transfers the modified data to the uCMDB. The connector logs information in the log file /var/log/opsware/tell/LOAD_STATS.0.log.

For the complete list of data transferred from SA to the uCMDB, see "SA data transferred to uCMDB" on page 75.

Accessing the uCMDB browser from the SA Client

uCMDB browser window

You can view server details in the uCMDB Browser window. To view server details:

1. Log in to the SA Client.

2. Go to **Devices** > **All Managed Servers**.

3. Select any server and click **Actions > Open with uCMDB Browser**.

   Optional: You can also use the context menu here or on the search panel. Select the server, then right-click and choose Open With > uCMDB browser.

   Sample URL that SA uses to open the uCMDB Browser for a specific Managed Server:

   ```
   http://my-ucmdb.mycomp.com:8080/ucmdb-api/ucmdb-
   browser/?locale=en&theme=LIGHT#refocus-selection=<global_ucmdb_id>
   ```

4. If you are not already logged in to the uCMDB Browser, this will invoke the uCMDB Browser Login screen. Complete using your uCMDB login credentials. You will only need to sign in once per session.

> **Tip:** If a blank page or a Page Not Found error occurs when you open the uCMDB Browser, it could mean that either uCMDB is not set up or the uCMDB server is not running or configured correctly. Make sure that the uCMDB server is configured and that the Tellconnector is running.

If the SA-uCMDB Connector has not been configured and you need to disable the 'Open with uCMDB Browser' menu item, go to System Configuration > Opsware > Tell and set the values to no value for uCMDB Browser URL and uCMDB URL.

Configuring the uCMDB browser

If the uCMDB Browser needs to be invoked from the SA Client, the uCMDB Browser's related parameters need to be specified after enabling the SA-uCMDB Connector using the following /opt/opsware/tell/bin/enable parameters:

--browser_protocol   - uCMDB Browser server protocol, http or https

--browser_host   - uCMDB Browser host name or IP

--browser_port   - uCMDB Browser host port

To use the uCMDB 10.01-based browser:

1. Stop the SA-uCMDB Connector by running the **stop** command:
   `/etc/init.d/opsware-sas stop telldaemon`

2. Disable the SA-uCMDB Connector by running the **disable** command:
   `disable`

   > **Note:** Make sure the connector is stopped and disabled. If the connector is not stopped and disabled when you revise the configuration file, you may encounter problems when you try to restart the Connector.

3. Update the uCMDB Browser suffix in the custom SA-uCMDB Connector configuration file /etc/opt/opsware/tell/tell_custom.conf according to your uCMDB browser version.

   For example:

   Change from the following default URL:
   `com.hpe.sa.tell.ucmdb.browser.path.suffix=/ucmdb-browser/?locale=en&theme=LIGHT`

   To a URL that works with uCMDB Browser 3.21 (or later):
   `com.hpe.sa.tell.ucmdb.browser.path.suffix=/ucmdb-browser/?locale=en`

   You can add, remove, or change other http GET parameters for your uCMDB setup as you see fit.

4. After the configuration file is updated, enable the SA-uCMDB Connector by running the **enable** command.

   The syntax of the **enable** command varies depending on your environment. See "The enable command" on page 59 in this document for an explanation of the **enable** command syntax and options.

5. Restart the uCMDB Connector. Enter the following command to start the SA-uCMDB Connector:
   ```
   /etc/init.d/opsware-sas start telldaemon
   ```

6. Optionally check the status of the SA-uCMDB Connector with the following command:
   ```
   /etc/init.d/opsware-sas status telldaemon
   ```

Global uCMDB IDs

With uCMDB 9.04 and earlier, only the local uCMDB IDs as known to that uCMDB server were synchronized in SA.

The uCMDB Servers can be configured as uCMDB Global ID generators, where the uCMDB IDs generated are *global* and *unique* in multi-uCMDB server environments. In such environments, these global IDs are needed to invoke the uCMDB Browser properly.

The SA 9.14 SA-uCMDB Connector was enhanced to automatically use the global uCMDB ID of CIs if the uCMDB Server is configured as a global ID generator. No special configuration is needed for the SA-uCMDB Connector.

SSL connectivity to the uCMDB server and the uCMDB browser

The SA-uCMDB Connector supports SSL protocol for the uCMDB Server and the uCMDB Browser.

When enabling Secure Sockets Layer Communication (SSL), the appropriate certificate and keystore need to be in place for the SA-uCMDB Connector.

To enable SSL:

Follow the instructions in the uCMDB Deployment Guide, "Enabling Secure Sockets Layer Communication," to create a uCMDB keystore and export the certificate to a file.

Import exported certificate from step 1 to where the SA-uCMDB Connector is installed. For example, the keystore must be placed in `/var/opt/opsware/crypto/tell` with the keystore filename: tell.keystore and the keystore password: **hppass**.

Example of import command:

```
/opt/opsware/jdk1.8/bin/keytool -import -noprompt -alias hpsaucmdb -file <path_to_
the_exported_hpcert> -keypass hppass -keystore
/var/opt/opsware/crypto/tell/tell.keystore -storepass hppass
```

Configurable files archived during upgrade

During upgrade, certain customizable and configurable files will be archived for preservation.

If you are upgrading from the SA-uCMDB Connector 9.14 to 10.0 following files will be archived in `/var/opt/opsware/install_opsware/config_file_archive/<respective path for file>`

- `tell.conf`
- `mapping.xml`
- `logging.properties`
- `tell_conversions.jar`
- `tell.pwd`
- `tell.keystore`

For example, the t**ell_custom.conf** residing in **/etc/opt/opsware/tell/tell_custom.com** will be archived to `/var/opt/opsware/install_opsware/config_file_archive/etc/opt/opsware/tell/tell_custom.com<time_stamp_of_upgrade>`

For the SA-uCMDB Connector 10.0 and future upgrades, **tell_custom.conf** and **mapping_ custom.xml** will also be archived for preservation.

Troubleshooting SA-uCMDB integration

Running the SA-uCMDB connector on a second core

In some cases, a particular core in a multi-master SA Mesh needs to be deactivated and it becomes necessary to run the SA-uCMDB Connector from a different core in that mesh. Sometimes this is also needed if network performance from another core to the uCMDB server is preferred. In those scenarios, the following steps are necessary:

To run the connector on a second core:

1. Stop the SA-uCMDB Connector on the first core and remove its affinity to it.
   /etc/init.d/opsware-sas stop telldaemon
   /opt/opsware/tell/bin/tell --release

2. On the second core, enable the SA-uCMDB Connector by running the **enable** command. The syntax of the **enable** command varies depending on your environment. See "The enable command" on page 59 in this document for an explanation of the enable command syntax and options.

3. Take responsibility of the SA-uCMDB integration, and then start the SA-uCMDB Connector.
   /opt/opsware/tell/bin/tell --take
   /etc/init.d/opsware-sas start telldaemon

To enable additional logging:

1. Start the SA-uCMDB Connector. Normal log files are stored in the /var/log/opsware/tell directory. Default file names include the following:
   tell.0.log   (normal startup log)
   ucmdb_failure.*.log   (uCMDB failures seen during synchronization)
   LOAD_STATS.*.log   (number of processed data)

2. To request additional logging details, specify the requested information in the `/etc/opt/opsware/tell/logging.properties` file as shown in the following table.

/etc/opt/opsware/tell/logging.properties fields

Field	Description
`java.util.logging.FileHandler.limit`	Specifies the maximum number of bytes to write to

/etc/opt/opsware/tell/logging.properties fields, continued

Field	Description
	any one file. Default value is 10000000.
`java.util.logging.FileHandler.count`	Specifies the number of files to use. Default value is 10.
`java.util.logging.FileHandler.append`	Specifies append mode, defaults to true.
`java.util.logging.FileHandler.pattern`	Specifies the pattern for naming the output file where the log file can be found. Defaults to **/var/log/opsware/tell/tell.%g.log**

Caution: Use caution when modifying the file limit. Large numbers might impact performance.

On-demand synchronization

Upon SA restart, the SA-uCMDB Connector normally continues synchronizing SA data to uCMDB from where it ended before the restart. The connector also runs a full sync, periodically. However, in some cases, such as when there are networking or server issues that prevent the updates from reaching the uCMDB server, you may need to trigger the full sync on demand.

To trigger the synchronization on demand:

1. Stop the SA-uCMDB Connector.

2. Restart the SA-uCMDB Connector with the following option:
   ```
   /opt/opsware/tell/bin/tell --startfresh
   ```

Viewing log files

The SA-uCMDB Connector generates the following text log files. You can view these log files in a text editor to get more information.

- /var/log/opsware/tell/tell.0.log is the main log file for information, warnings and errors encountered by the SA-uCMDB Connector.

- /var/log/opsware/tell/LOAD_STATS.0.log contains the status and statistics of the initial data load, and approximate times to complete the initial data load.

- /var/log/opsware/tell/ucmdb_failure.0.log contains uCMDB errors, primarily reconciliation errors if the SA data is incomplete, for example, if the required uCMDB keys are missing. This could happen

if a server did not have a serial number or an IP address, for example. This log file contains the uCMDB exception, the reason why it failed and a trace of the CIs that caused the exception.

SA-uCMDB connector daemon

The SA-uCMDB Connector runs the daemon /etc/opt/opsware/startup/telldaemon on your SA core server. Make sure this process is running on your SA core server.

If it is not running, start it as described in .

If it is running, check the status as described in .

Example– SA-uCMDB Connector Mapping File

```
<DB-UCMBD-HIGHLEVEL-MAPPING>

    <!-- generates installed_software.xml -->

    <Model-Definition model-name='sa' enable='true'>

        <CI ucmdb-ci-type-name='server_automation_system' enable='true' base-
class='server_automation_system'>

            <Attribute source='SA/Description' target-attr='description'
enable='true'/>

            <Attribute source='SA/Name'  target-attr='name' enable='true'/>

            <Attribute-Default target-attr='version' target-attr-value='9.14'
enable='true'/>

        </CI>

    </Model-Definition>

    <!-- generates node.xml -->

    <Model-Definition model-name='hosts' enable='true'>

        <CI ucmdb-ci-type-name='server_automation_system' reference-ci='true'
enable='true'/>

        <CI ucmdb-ci-type-name='ip_address' enable='true' base-class='node'>

            <Attribute source='IpAddress/PrimaryIpName' target-attr='name'
enable='true'/>

            <Attribute source='IpAddress/RoutingDomain' target-attr='routing_
domain' enable='true'/>

        </CI>
```

```
        <CI ucmdb-ci-type-name='node' enable='true' base-class='node'>

            <Attribute source='Node/Name' target-attr='name' enable='true'/>

            <Attribute source='Node/Description' target-attr='description'
enable='true'/>

            <Attribute source='Node/BiosAssetTag' target-attr='bios_asset_tag'
enable='true'/>

            <Attribute source='Node/BiosSerialNumber' target-attr='serial_number'
enable='true'/>

            <Attribute source='Node/BiosUuid' target-attr='bios_uuid'
enable='true'/>

            <Attribute source='Node/DefaultGatewayIpAddress' target-attr='default_
gateway_ip_address' enable='true'/>

            <Attribute source='Node/NetBiosName' target-attr='net_bios_name'
enable='true'/>

            <Attribute source='Node/NodeModel' target-attr='node_model'
enable='true'/>

            <Attribute source='Node/MemorySize' target-attr='memory_size'
enable='true'/>

            <Attribute source='Node/OsDescription' target-attr='os_description'
enable='true'/>

            <Attribute source='Node/OsFamily' target-attr='os_family'
enable='true'/>

            <Attribute source='Node/TenantOwner' target-attr='TenantOwner'
enable='true'/>

            <Attribute source='Node/Facility' target-attr='facility'
enable='false'/>

            <Attribute source='Node/VirtualizationTypeId' target-
attr='virtualization_type_id' enable='false'/>

            <Attribute source='IpAddress/ManagementIpName' target-attr='ip_address'
enable='false'/>

            <CI-Filter enable='true'><![CDATA[(DEVICES.OPSW_LIFECYCLE =
'MANAGED')]]></CI-Filter>

        </CI>

        <Relation ucmdb-relation-type-name='containment' ucmdb-relation-from-ci-
type-name='node' ucmdb-relation-to-ci-type-name='ip_address' enable='true' ucmdb-
relation-id-link='true'/>
```

```
        <Relation ucmdb-relation-type-name='aggregation' ucmdb-relation-from-ci-
type-name='server_automation_system' ucmdb-relation-to-ci-type-name='node'
enable='true' ucmdb-relation-id-link='false'/>

    </Model-Definition>

    <!-- generates installed_software.xml -->

    <Model-Definition model-name='software' enable='true'>

        <CI ucmdb-ci-type-name='node' base-class='node' reference-ci='true'
enable='true'/>

        <CI ucmdb-ci-type-name='installed_software' enable='true' base-
class='installed_software'>

            <Attribute source='InstalledSoftware/DmlProductName' target-attr='dml_
product_name' enable='true'/>

            <Attribute source='InstalledSoftware/Name'  target-attr='name'
enable='true'/>

            <Attribute source='InstalledSoftware/Version' target-attr='version'
enable='true'/>

            <Attribute source='InstalledSoftware/Vendor' target-attr='vendor'
enable='true'/>

        </CI>

        <Relation ucmdb-relation-type-name='composition' ucmdb-relation-from-ci-
type-name='node' ucmdb-relation-to-ci-type-name='installed_software' ucmdb-
relation-id-link='true' enable='true'/>

    </Model-Definition>

    <!-- generates policy.xml -->

    <Model-Definition model-name='compliance' enable='true'>

        <CI ucmdb-ci-type-name='server_automation_system' reference-ci='true'
enable='true'/>

        <CI ucmdb-ci-type-name='policy' base-class='policy' enable='true'>

            <Attribute source='Policy/Name' target-attr='name' enable='true'/>

            <Attribute source='Policy/Description' target-attr='description'
enable='true'/>

            <Attribute-Default target-attr='policy_defined_by' target-attr-
value='SA' enable='true'/>

            <Attribute-Default target-attr='policy_category' target-attr-
value='audit' enable='true'/>

        </CI>
```

```
        <Relation ucmdb-relation-type-name='aggregation' ucmdb-relation-from-ci-
type-name='server_automation_system' ucmdb-relation-to-ci-type-name='policy'
enable='true' ucmdb-relation-id-link='false'/>

    </Model-Definition>

    <!-- generates hypervisor.xml -->

    <Model-Definition model-name='hypervisor' enable='true'>

        <CI ucmdb-ci-type-name='node' base-class='node' reference-ci='true'
enable='true'/>

        <CI ucmdb-ci-type-name='hypervisor' base-class='hypervisor' enable='true'>

            <Attribute source='Hypervisor/Name' target-attr='name' enable='true'/>

            <Attribute source='Hypervisor/Description' target-attr='description'
enable='true'/>

            <Attribute source='Hypervisor/ProductName' target-attr='product_name'
enable='true'/>

        </CI>

        <Relation ucmdb-relation-type-name='composition' ucmdb-relation-from-ci-
type-name='node' ucmdb-relation-to-ci-type-name='hypervisor' ucmdb-relation-id-
link='true' enable='true'/>

    </Model-Definition>

    <!-- generates hypervisorRelation.xml -->

    <Model-Definition model-name='vmrelations' enable='true'>

        <CI ucmdb-ci-type-name='hypervisor' base-class='hypervisor' reference-
ci='true' enable='true'/>

        <CI ucmdb-ci-type-name='node' base-class='node' reference-ci='true'
enable='true'/>

        <Relation ucmdb-relation-type-name='execution_environment' ucmdb-relation-
from-ci-type-name='hypervisor' ucmdb-relation-to-ci-type-name='node' ucmdb-
relation-id-link='false' enable='true'/>

    </Model-Definition>

    <!-- generates policyResult.xml -->

    <Model-Definition model-name='compliance_status' enable='true'>

        <CI ucmdb-ci-type-name='policy' base-class='policy' reference-ci='true'
enable='true'/>

        <CI ucmdb-ci-type-name='node' base-class='node' reference-ci='true'
enable='true'/>
```

```
        <CI ucmdb-ci-type-name='policy_result' base-class='policy_result'
enable='true'>

            <Attribute source='PolicyResult/Name' target-attr='name'
enable='true'/>

            <Attribute source='PolicyResult/ComplianceStatus' target-
attr='compliance_status' enable='true'/>

            <Attribute source='PolicyResult/PolicyResultDateTime' target-
attr='policy_result_date_time' enable='true'/>

            <Attribute source='PolicyResult/RulesCompliant' target-attr='rules_
compliant' enable='true'/>

            <Attribute source='PolicyResult/RulesNonCompliant' target-attr='rules_
non_compliant' enable='true'/>

            <Attribute source='PolicyResult/ComplianceLevel' target-
attr='compliance_level' enable='true'/>

        </CI>

        <Relation ucmdb-relation-type-name='composition' ucmdb-relation-from-ci-
type-name='policy' ucmdb-relation-to-ci-type-name='policy_result' ucmdb-relation-
id-link='false' enable='true'/>

        <Relation ucmdb-relation-type-name='aggregation' ucmdb-relation-from-ci-
type-name='node' ucmdb-relation-to-ci-type-name='policy_result' ucmdb-relation-id-
link='true' enable='true'/>

    </Model-Definition>

</DB-UCMBD-HIGHLEVEL-MAPPING>
```

Integrating with HPELN

Overview

The HPE Live Network connector (HPE LNc) is a dynamic content updating tool, integrated with several HPE software products including HPE Server Automation (HPE SA).

The HPE LNc provides you with security and compliance policies to help maximize your return on investment in HPE Software products, and to leverage the extensible automation platforms to deliver new automation capabilities on an ongoing basis.

The HPE LNc provides a direct link between your Business Service Automation products and HPELN. The LNc provides real-time downloads of content and content updates for HPE SA.

Using the LNc, subscription service content is delivered every day to HPE customers' enterprise data centers around the world.

LNc is customizable through plugins called profiles. Every product integrating with LNc needs a profile that customizes the LNc.

The Live Network Connector user guide, the LNc Release Notes and the HPE LNc installers can be found at https://hpln.hpe.com/contentoffering/hpe-live-network-connector if you are connected with HPE Passport credentials.

Live-Network-Connector usually comes installed along with the HPE SA Core in the following directory: **/opt/opsware/hpln/.**.

The live-network-connector binaries are available under **/opt/opsware/hpln/lnc/bin/**.

> **Note:** The latest edition of LNc guide can be found at:
> https://lnast01pcache.saas.hpe.com/asset/resources/co/1284/10f1459953792/HPELN_LNc_Users_Guide.pdf.

Setting up your integration

This section describes how to configure the LNc, as well as its Services and Streams. It also describes how to verify whether content was downloaded and where the LNc log file is located.

Prerequisites

The LNc must be installed on the SA core component server. On the SA core component server (assuming that the LNc script is your $PATH), type the command `live-network-connector` to launch the LNc.

By default, the LNc will:

- Connect over SSL

- Re-attempt a failed download once

- Download and import core updates for the specified products (if any)

- Import content from enabled streams

    Note: The first update can take a significant amount of time.

Configuring the Live Network connector

This section describes how to configure the LNc to connect to the HPE Live Network.

1. Add the following to your PATH variable:

    ○ <install_directory>/lnc/bin

    For example:

    `export PATH=$PATH:<install_directory>/lnc/bin`

2. Open a command prompt on the computer where the LNc is installed.

3. To set the user name and password, enter the following command:

    `live-network-connector write-config --username=<username>--password=<password>`

    The **--username** and **--password** commands can also be run separately.

    Note: Manual editing of any LNc configuration file is not supported and could lead to corruption or lost settings. Use the write-config command instead.

4. To check the URL that the LNc connects to in order to download content, execute the following

command: `live-network-connector read-config --url`

The output should display the following URL:

https://hpln.glb.itcs.hp.com

5. (Optional) If you need to use a proxy server to access the HPE Live Network, run the following command:

```
live-network-connector write-config --http-proxy=<HTTP_PROXY> --http-proxy-
    user=<HTTP_PROXY_USER> --http-proxy-pass=<HTTP_PROXY_PASS>
```

The **--http-proxy**, **--http-proxy-user**, and **--http-proxy-pass** commands can also be run separately.

6. The default path to the LNc log file is:

   ○ `<install_directory>/lnc/log/live-network-connector.log`

7. The default path to the LNc cache directory is

   ○ `<install_directory>/lnc/cache`

   ○ (Optional) You can change this value, but be aware that doing so can potentially cause the redownload and re-import of previously obtained content, so use with caution. To change this default value, execute the following command on the system where the LNc is installed:

   ```
   live-network-connector write-config --cache=<PATH>
   ```

8. The default path to the LNc lock file is:

   ○ `<install_directory>/lnc/live-network-connector.lock`

9. To configure the LNc for a specific product, specify it by using `--product`.

   To see a list of supported product values, including the long product name, you can run the following command: `live-network-connector list-products`

   This provides a listing of currently supported products, which should be used in the next configuration step.

   For example, to configure your LNc installation to support Server Automation (sas), execute the following command on the system where the LNc is installed:

   ```
   live-network-connector write-config --product=sas
   ```

   Important: To enable multiple products, a single **write-config** command must be executed with a **--product** for each product. Note that subsequent **write-config** commands will overwrite the previous values.

○ Manual editing of any LNc configuration file is not supported and could lead to corruption or lost settings. Use the write-config command instead.

○ Depending on the products enabled, some additional settings are required. For more information, see the product documentation or the product admin.

10. Once the product has been configured, you can see a list of available content (streams) for the selected product, run the list-streams command.

For example: `live-network-connector list-streams`

> **Note:** If no streams are returned, ensure that you have configured the system for a specific product.

11. Perform any additional queries against those streams as desired (such as through the describe command).

For example:

`live-network-connector write-config --stream=content.ms_patch_supp`

12. To set the values of username (sas_user) and password (sas_pass) of the SA user account used to access SA, run the following command:

`live-network-connector write-config`

`--setting=sas.sas_user=<sa_username>`

`--setting=sas.sas_pass=<sa_userpassword> --add`

13. To set the values of **cbt_path** and **cbt_config_path** to the path for the CBT executable and CBT configuration file, run the following command:

`live-network-connector write-config`

`--setting=sas.cbt_path=<cbt_pathname>`

`--setting=sas.cbt_config_path=<cbt_config_pathname> --add`

Services and streams

The HPE Live Network delivers content in the form of streams and services.

● **Stream**: A grouping of related content. A stream maintains multiple content objects that are related to each other in form, function, or use.

- **Service**: A grouping of streams. A service is a collection of streams that are all available to a customer based on a related entitlement, where entitlement is determined using assets and valid license or maintenance contracts for a given HPE Live Network account.

In the LNc configuration file, streams are grouped in blocks of services or products.

Viewing services and streams

To view a list of available services and streams, either use the **list-streams** command or the **describe** command.

> **Note:** Having the product set (either by using write-config --product, or by specifying --product in the command line) is mandatory for the command to succeed. To see the available products, use the list-products command.

- At a command prompt, enter the following command:

  ```
  live-network-connector list-streams
  ```

  The format of the value returned by the list-streams command is:

  ```
  product, service, stream (stream.name)
  ```

  An example of a stream returned by this command is:

  ```
  sas security vc_cisco (security.vc_cisco)
  ```

- At a command prompt, enter the following command:

  ```
  live-network-connector describe
  ```

  The format of the value returned by the describe command is:

  ```
  product, service, stream (stream.name), enabled/disabled status,

  description and/or url of that stream, the available tags.
  ```

  An example of the output returned by this command is:

  ```
  Product       Stream                       Enabled

  ========== =========================== ===========

  hpca       security.hpca_config          0

                                         Description

  _____
  ```

```
Configuration definition to allow for the HPCA product to add

new or adapt to changes in subscriptions services.
                                          Tags

_____

hpca_config
```

Configuring the content and security streams

Each stream in a service must be enabled in the LNc configuration using the **live-network-connector** command followed by **write-config** plus the specific parameters for each stream. A stream is activated when you set its value to 1.

For example, to activate the stream, enter the following command from a shell on the server where the LNc is installed:

```
live-network-connector write-config --stream=security.cc_library --enable
```

The LNc must be installed on the server the SA software repository component is installed on. The LNc must be configured as described in Configuring_the_Live_Network_connector.

> **Note:** If you run the **live-network-connector write-config** command and you receive a message that the configuration parameter does not exist, append the **--add** option to the command. Manual editing of any LNc configuration file is not supported and could lead to corruption or lost settings. Use the **write-config** command instead.

Configuring the Microsoft patch supplement stream

To configure the LNc to activate the Microsoft Patch Supplement stream:

1. On the system where the LNc is installed, run the following command to enable the Microsoft Patch Supplement stream:

   ```
   live-network-connector write-config --stream=content.ms_patch_supp --enable
   ```

2. (Optional) To disable the Microsoft Patch Supplement stream, run the command using the --disable command:

```
live-network-connector write-config --stream=content.ms_patch_supp --disable
```

3. (Optional) To enable the Microsoft Patch Supplement stream to overwrite the metadata when the content is imported into SA, set the `sas.force_win_patch_import` parameter.

   For example, to enable the option, run the following command:

   ```
   live-network-connector write-config --setting=
   sas.force_win_patch_import=1 --add
   ```

4. (Optional) To disable this option, run the following command:

   ```
   live-network-connector write-config --setting=
   sas.force_win_patch_import=0 --add
   ```

5. Enter the following command to launch the LNc:

   ```
   live-network-connector
   ```

Configuring the software discovery stream

To configure the LNc to activate the SA software discovery stream:

1. On the system where the LNc is installed, run the following command to enable the software discovery stream:

   ```
   live-network-connector write-config
   --stream=content.software_discovery --enable
   ```

2. (Optional) To disable the software discovery stream, run the command using the --disable option:

   ```
   live-network-connector write-config
   --stream=content.software_discovery --disable
   ```

3. Enter the following command to launch the LNc:

   ```
   live-network-connector
   ```

Configuring the SA DMA stream

To configure the LNc to activate the sa_dma stream:

1. On the system where the LNc is installed, run the following command to enable the sa_dma stream:

   ```
   live-network-connector write-config --stream=content.sa_dma --enable
   ```

2. (Optional) To disable the sa_dma stream, run the command using the --disable option:

   ```
   live-network-connector write-config --stream=content.sa_dma --disable
   ```

3. Enter the following command to launch the LNc:

   ```
   live-network-connector
   ```

Configuring the content operating system platform family streams

To configure the LNc to activate the platform streams (Linux, Unix, Windows and VMware):

1. On the system where the LNc is installed, run the following command to enable the platform_ <family_platform_type> stream:

   ```
   live-network-connector write-config --stream=content.platform_<family_platform_
   type> --enable
   ```

2. (Optional) To disable the platform_<family_platform_type> stream, run the command using the -- disable option:

   ```
   live-network-connector write-config --stream=content.platform_<family_platform_
   type> --disable
   ```

3. Enter the following command to launch the LNc:

   ```
   live-network-connector
   ```

Configuring the Solaris patch supplement stream

As a prerequisite for downloading this content, solpatch_import.conf file from:
`/etc/opt/opsware/solpatch_import/` should be edited (values for sa user/password, download user/password, proxy host and fujitsu_download_user/pass should be added).

Using the solpatch_import.conf, a db should be created.

To configure the LNc to activate the solaris_patching stream, perform the following steps:

1. On the system where the LNc is installed, run the following command to enable the solaris_ patching stream:

   live-network-connector write-config --stream=content.solaris_patching --enable

2. (Optional) To disable the solaris_patching stream, run the command using the --disable option:

   live-network-connector write-config --stream=content.solaris_patching --disable

3. Enter the following command to launch the LNc:

   live-network-connector

Configuring the security scanner stream

To configure the LNc to activate the security_scanner stream, perform the following steps:

1. On the system where the LNc is installed, run the following command to enable the security_ scanner stream:

   ```
   live-network-connector write-config

   --stream=security.security_scanner --enable
   ```

2. (Optional) To disable the security_scanner stream, run the command using the --disable option:

   ```
   live-network-connector write-config

   --stream=security.security_scanner --disable
   ```

3. Enter the following command to launch the LNc:

   ```
   live-network-connector
   ```

Configuring SA vulnerability content streams

To configure the LNc to activate the SA vulnerability content streams, perform the following steps:

1. Log in to the system where the LNc is installed.

2. From the command line, set specific LNc configuration parameters to 1 in order to activate each SA vulnerability content stream you want to receive updates from.

For example, if you have subscribed to vulnerability content for SA, run the following command:

```
live-network-connector write-config --stream=security.vc_winxp

--stream=security.vc_win2k3 --stream=security.vc_rhel3

--stream=security.vc_hpux11 --enable
```

3. (Optional) To disable a stream, execute the command using the --disable option:

```
live-network-connector write-config --stream=security.vc_winxp

--stream=security.vc_win2k3 --stream=security.vc_rhel3

--stream=security.vc_hpux11 --disable
```

Configuring SA compliance content streams

The security.cc_library stream is a prerequisite stream that enables all SA compliance streams, and should be run at least once on each SA system you want to download content onto. Each time you want to import new content from the HPELN, this stream should be enabled.

To configure the LNc to activate the SA compliance content streams, perform the following steps:

1. Log into the system where the LNc is installed.

2. From the command line, set specific LNc configuration parameters to 1 in order to activate each SA compliance content stream you want to receive updates from.

   For example, to enable compliance content for SA Audit and Remediation, run the following command:

   ```
   live-network-connector write-config —stream=security.cc_library

   --stream=security.ec_disa_stig --enable
   ```

3. (Optional) To disable a stream, run the command using the --disable option:

   ```
   live-network-connector write-config —stream=security.cc_library

   --stream=security.ec_disa_stig --disable
   ```

Use Cases

General troubleshooting tips

If you are encountering issues with LNc, follow these steps:

1. Read this document carefully, looking for answers to your specific problem, and ensure that all required settings are configured as expected, referencing your product and Content specific documentation, ensuring any additional required parameters have been configured properly.

2. Run the following command:

   ```
   live-network-connector read-config
   ```

   Check all values for username, product, and that desired streams are enabled without any spelling errors. Note that some passwords with non-alphanumeric characters may require special treatment.

   Passwords entered are interpreted by your operating system's command interpreter, and some characters have special meaning and must be escaped to be passed to the LNc correctly. For additional information on special characters and escaping or quoting them at the command line, Linux users can see the "man" page for bash (e.g. man bash), and other Unix users can reference the relevant "man" pages for their specific shell in use.

   A simple example is provided below for a Unix system:

   To pass the password my$?9FYI^ to the LNc, the special character(s) must be escaped as follows:

   ```
   live-network-connector write-config --password='my$?9FYI^'
   ```

3. Check that the following command runs successfully. This validates that your credentials and product settings are correct. If you receive an error, review your username, password and product settings and re-configure them as required:

   ```
   live-network-connector list-streams
   ```

4. Ensure that your account has full access by logging in to https://hpln.hpe.com with your user credentials, visiting the relevant Product or Content area, and ensuring that you are listed as a content viewer.

If not, check that your Service Agreement Identifiers are associated with your account at:

https://softwaresupport.hpe.com/.

5. If you are downloading content successfully but experiencing problems on import, this is generally a product- or content-specific configuration issue. Review the required settings and update your environment accordingly.

6. If none of these steps resolve your problem, follow the steps below:

    a. Save the output of the following commands:

    ```
    live-network-connector read-config

    live-network-connector list-status --product=all --stream=all
    ```

    b. Truncate, move or delete the existing LNc log file under <INSTALL_PATH>/lnc/log, and re-execute the command showing your issue, appending --debug to the end.

    For example, if you have configured LNc correctly with user credentials, proxy information as required, enabled a product and selected one or more streams for content subscription, and are simply trying to update and import that content, run the following command:

    ```
    live-network-connector download-import --debug
    ```

    After execution, compress or archive (zip, gzip, etc.) the live-network-connector.log file.

    c. Open a Support case as necessary. If you are experiencing a product or content specific configuration issue, or content is being downloaded but failing to import, open a Support case for the relevant product.

    If you are experiencing core LNc specific issues such as being unable to connect, download or import content at all, open a Support case for the HPE Live Network connector. Include a description of your problem, and the information from Step 6 above.

Connectivity issues

If LNc is reporting connectivity errors, check the firewall/proxy access permissions or required settings with your network administrator. Run ping/dig for each of the HPELN hosts and make sure IPs are resolved correctly and the hosts are accessible from your environment outside of LNc through various command line troubleshooting tools such as traceroute, wget, curl, and so on.

Command and command line options, importing content, and log files

This section describes the LNc commands and command line options, importing content, and the LNc log file.

Command options

To see the complete list of available commands, options, and online help, perform the following steps:

1. Open a command prompt.

2. Run the following command:

   ```
   live-network-connector --help
   ```

The following list shows some of the available modes that can be called at the command line when launching the LNc:

- **download**: Downloads content for the services and streams configured on the locally-installed LNc.

  > **Note:** The core updates for the specified products (if any) are also downloaded and imported.

- **download-import**: Default command mode. Running the LNc without specifying a command executes in this mode of operation. Downloads content for the services and streams configured on the locally-installed LNc, and imports the content.the locally-installed LNc, and imports the content.

  > **Note:** The core updates for the specified products (if any) are also downloaded and imported.

- **import**: Imports the content that has been previously downloaded using the download command.

  > **Note:** The core updates for the specified products (if any) are also imported.

- **encrypt-passwords**: Encrypts the passwords entered in plain text in the configuration file.

- **list-streams**: Shows the available services and streams. XML output is also available by using the **--format=xml** option.

> **Note:** The core updates for the specified products (if any) are also downloaded and imported.

- **list-products**: Displays the available products. The default output is in text format, and can be switched to XML output by appending the **--format=xml** option.

- **list-locales**: Displays the available content locales, for a given product and stream. If the product version cannot be detected, all available content locales are displayed.

  Options:

  `--product-version=<value>` filters the locale based on the given product version

  `--all-versions` no version filter will be applied.

  The default output is text format; it can be switched to XML output by appending the --format=xml option.

  For example:

  ```
  live-network-connector list-locales --product=hpca --stream=security.hpca_nvd

  Product Stream Locales

  ======= ========================== =============

  hpca security.hpca_nvd en_US
  ```

- **list-status**: Displays the latest content status. For displaying the import history add the **--history** parameter. For example:

  ```
  live-network-connector list-status --product=sas --stream=content.software_

  discovery
  ```

  which will display information similar to:

  ```
  Name Product Stream Version Date Status

  ====== ======= ========================== ============= ====================
  =======

  dssm sas content.software_discovery 37.0.0.0.29.0 2011-09-06 16:36:37 success
  ```

- **export**: Exports content that has been downloaded from HPE Live Network.

  > **Note:** The core updates for the specified products (if any) are also imported.

- **download-export**: Downloads and exports content from the HPE Live Network.

  > **Note:** The core updates for the specified products (if any) are also downloaded and imported.

- **read-config**: Shows the value of a configuration attribute in the LNc configuration file. For example, to display the value of username in the LNc configuration file, run the following command:

  ```
  live-network-connector read-config --username
  ```

- **write-config**: Sets the value of a configuration attribute in the LNc configuration file. For example, to set the value of username in the LNc configuration file to user plus an encrypted password, run the following command:

  ```
  live-network-connector write-config --username=<user>
  ```

  ```
  --password=<password>
  ```

  When you set a username and password in this manner, you will not need to use the encryptpasswords command.

  > **Note:** Manual editing of any LNc configuration file is not supported and could lead to corruption or lost settings. Use the **write-config** command described here instead.

- **describe**: Shows the available streams, their state (enabled/disabled), their associated description and/or url, and the available tags, if any are available.

Other options:

When `--content-object=<content object name>` is provided, the command also describes `<content object name>` for the configured product and/or stream.

When `--content-object=all` is provided, the command also describes all the content objects for the configured product and/or stream.

When `--stream=all` is provided, the command considers all available streams for the configured product, regardless of which streams were configured with `write-config`.

When `--extended` is provided, the command also displays stream extended data. When `--content-object=<content object name>` or `--content-object=all` is added, it also displays extended data for the configured content object.

Announcements and release notes are displayed as well, if you use the `--announcement` and `--release-notes` options, respectively . These options work only in conjunction with the --contentobject option.

> **Note:** The core updates for the specified products (if any) are also downloaded and imported.

- **search**: Searches the given text in the tags, name, description, and URL of the stream, as well as in the service name and the product name, and displays the result. To search only the stream tags, use the `--tag` option.

Command line options

The available command-line options for a specific command are listed when running the following command:

```
live-network-connector command --help
```

Option	Function	Command Compatibility
--http-proxy, --http-proxy-user, and --http-proxy-pass	Configures http proxy settings.	download, download-import, download-export
--export-to-directory	Exports content to a specific directory.	download-export, export
--import-from-directory	Imports content from a specific directory.	import
--product	Restricts the content to operate on a specific product. For example, --product=sas limits the content to content that is relevant to SA.	download, download-export, export, downloadimport, import, liststreams, list-status, list-locales, describe, search
--stream	Restricts the content to operate on one or more specific streams. When the value of this option is "all", the command will operate on all streams from any service within the configured product. **Note:** When used with write-config, this option enables all the streams from the configured product that are known since the last execution of a connected command (like download, downloadimport).	download, download-export, export, downloadimport, import, listproducts, liststatus, list-locales, describe, search, write-config
--platform	Specifies the platform of the isolated system in an air-gapped environment where the content will be used. For example: linux2, sunos5, win32.	download-export, export
--status-file	Indicates the status file of the isolated system in an air-	download-export,

Option	Function	Command Compatibility
	gapped environment, typically found in lnc/etc/ imports.js. Transfer this file to the connected node and use it to only download-export (or export) the necessary files.	export
--product-version	Specifies the version of the product core. For example, in an air-gapped environment, the LNc will not be able to detect the product version of the core. It is listed in the same order as the products with the --product flag.	download-export, export
--locale	Specifies the preferred content locale. If no value is specified, the default is considered to be en_US. If it is set to "all", the content is not filtered by locale. If the locale is changed, use --reload if the content was previously imported. Refer to your Product and Content documentation to see if localized content is available.	download download-import, import downloadexport, export
--secondary-product --secondary-version	• Specifies a product or a list of products, comma separated. • Specifies a version or a list of versions, comma separated. The two options need to be set together and have the same number of items. When set for content, the secondary product and version specify that the use (download, import, export) of this content will be allowed if the primary product version validation passes and also the secondary product version validation passes. The content itself will be consumed by the primary product only.	write-config, download, download-import, import, downloadexport, export
--release-notes	Displays the release notes for the configured content object (s) within the configured product and stream.	describe
--announcement	Displays the announcement for the configured content object (s) within the configured product and stream.	describe

Content preview (--preview)

The --preview option allows you to generate a preview of all new content for a requested stream before you initiate content download, download-import, import, download-export or export. Used with the download, download-import, import, download-export, and export commands, the --preview option

outputs a report of all new content available before you initiate a download, download-import, import, download-export, or export.

For example, if you are subscribed to one or more content streams and want to preview new updates before you download and import the new content, enter the following argument:

```
live-network-connector download-import --preview
```

This command will output a report containing all new content updates in all currently subscribed streams which are either available in the LNc cache or on a distribution server that have never been previously downloaded or imported.

If there is no new content available for your subscriptions, the preview report will contain no content objects.

By default, the report is output to STDOUT in plain text format, but if you want the preview report to be output in the XML format, use the --format=xml option to request XML output.

For example:

```
live-network-connector download-import --preview --format=xml
```

Options available for --preview

- **download --preview**: This report lists all content objects in all currently subscribed streams which have not been previously downloaded. The universe of considered content objects is limited to the set currently published on the distribution server.

- **download --preview --allow-update**: This report is similar to the download --preview report, but also updates the LNc and the configured product profile, without grabbing the actual content. Profile data that will be grabbed is based on the product configured in the LNc.

- **import --preview**: This report lists all content objects in all currently subscribed streams which are available in the LNc cache and have never been previously imported. The universe of considered content objects is limited to the set currently in the LNc cache. Specifically, the distribution server is not considered.

- **import --preview --allow-update**: This report is similar to the import --preview report, but also updates the LNc and the configured product profile, without grabbing the actual content. Profile data that will be grabbed is based on the product configured in the LNc.

- **download-import --preview**: This report lists the latest versions of all content objects in all currently subscribed streams which are either available on the distribution server and have not been previously downloaded, or are in the LNc cache and have never been previously imported. The universe of considered content objects includes both the set currently published on the distribution server and the set of content objects currently in the LNc cache.

- **download-import --preview --allow-update**: This report is similar to the download-import --preview report, but also updates the LNc and the configured product profile, without grabbing the actual content. Profile data that will be grabbed is based on the product configured in the LNc .

- **download-export --preview**: This report lists the latest available content appropriate to the current configuration in all currently subscribed streams which are available either on the distribution server or in the LNc cache, and which are available for export. The universe of considered content objects includes both the set currently published on the distribution server and the set of content objects currently in the LNc cache.

- **download-export --preview --allow-update**: This report is similar to the download-export --preview report, but also updates the LNc and the configured product profile, without exporting the actual content. Profile data that will be grabbed is based on the product configured in the LNc.

- **export --preview**: This report lists all content objects in all currently subscribed streams which are available in the LNc cache and are available for export. The universe of considered content objects is limited to the set currently in LNc cache. Specifically, the distribution server is not considered. Typically this option is used for exporting content to an air-gapped environment.

- **export --preview --allow-update**: This report is similar to the export --preview report, but also uses the already downloaded data to update the LNc and the configured product profile, without exporting the actual content. Profile data that will be grabbed is based on the product configured in the LNc.

- **--tags**: This report lists the search tags defined at content object level.

- **--release-notes**: This report lists the release notes available for each content object within the configured product and stream.

- **--announcement**: This report lists the announcement available for each content object within the configured product and stream.

Importing content

To help verify that the content was downloaded, the LNc calculates the SHA256 sum of downloaded files and checks the result against the SHA256 sum listed for the file in the stream. The LNc retains the files in the cache.

The LNc checks the return status of the import commands to see if the import succeeded. If the import succeeded, the LNc marks the file as imported and caches the information. Check the log file to make sure that the content was imported successfully.

Live network connector log file

The LNc checks the return status of the import commands to see if the import succeeded. If the import succeeded, the LNc marks the file as imported and caches the information. Check the log file to make sure that the content was imported successfully.

```
<install_directory>/lnc/log/live-network-connector.log
```

To change this default path, by using the write-config command, set the value of logfile_path to the preferred path and file name.

Standard content streams

The following table presents the names and descriptions of the streams currently available through the HPE Live Network.

> **Note:** The tables in this section are only a subset of the current list of available streams.

Activate a stream in this table by modifying the configuration file for the LNc on the specified server.

Name	Description
ms_patch_supp	Microsoft patch supplement.
platform_linux	Managed platform content - platform installers Linux.
platform_unix	Managed platform content - platform installers Unix.
platform_vmware	Managed platform content - platform installers VMware.
platform_windows	Managed platform content - platform installers Windows.
software_ discovery	Software discovery server module content.
solaris_patching	Solaris patching content.
security_scanner	Operational security assessment server module to scan system for known vulnerabilities.
sa_dma	Program APXs content to invoke the DMA client on managed servers when running DMA workflows.
sa_se_connector	Storage essentials connector.
os_provisioning	OS provisioning content.

SA vulnerability content streams

An SA vulnerability stream contains an audit and remediation (A&R) policy with checks for detecting platform vulnerability exposure based on CVE (Common Vulnerabilities and Exposures) and OVAL (Open Vulnerability and Assessment Language) data.

Name	Description
vc_aix43	Vulnerability content for SA on AIX 4.3
vc_aix51	Vulnerability content for SA on AIX 5.1
vc_aix52	Vulnerability content for SA on AIX5.2
vc_aix53	Vulnerability content for SA on AIX 5.3
vc_aix61	Vulnerability content for SA on AIX6.1
vc_aix71	Vulnerability content for SA on aix 7.1
vc_centos5	Vulnerability content for SA on Centos 5
vc_centos6	Vulnerability content for SA on Centos 6
vc_centos7	Vulnerability content for SA on Centos 7
vc_oel5	Vulnerability content for SA on OEL 5
vc_oel6	Vulnerability content for SA on OEL 6
vc_oel7	Vulnerability content for SA on OEL 7
vc_esx3	Vulnerability content for SA on VMware ESX 3.0
vc_esx35	Vulnerability content for SA on VMware ESX 3.5
vc_esx4	Vulnerability content for SA on VMware ESX 4.0
vc_esx41	Vulnerability content for SA on VMware ESX 4.1
vc_winxp	Vulnerability content for SA on Windows XP
vc_win2k	Vulnerability content for SA on Windows 2000
vc_win2k3	Vulnerability content for SA on Windows 2003
vc_win2k8	Vulnerability content for SA on Windows 2008
vc_win2k8r2	Vulnerability content for SA on Windows 2008 R2

Name	Description
vc_win2k12	Vulnerability content for SA on Windows 2012
vc_win2k12r2	Vulnerability content for SA on Windows 2012 R2
vc_sol7	Vulnerability content for SA on Solaris 7
vc_sol8	Vulnerability content for SA on Solaris 8
vc_sol9	Vulnerability content for SA on Solaris 9
vc_sol10	Vulnerability content for SA on Solaris 10
vc_hpux10	Vulnerability content for SA on HP-UX 10
vc_hpux11	Vulnerability content for SA on HP-UX 11
vc_rhel3	Vulnerability content for SA on RHEL3
vc_rhel4	Vulnerability content for SA on RHEL4
vc_rhel5	Vulnerability content for SA on RHEL5
vc_rhel6	Vulnerability content for SA on RHEL6
vc_rhel7	Vulnerability content for SA on RHEL7
vc_suse10	Vulnerability content for SA on SuSE Linux 10
vc_suse11	Vulnerability content for SA on SuSE Linux 11
vc_suse12	Vulnerability content for SA on SuSE Linux 12
vc_ubuntu	Vulnerability content for SA on Ubuntu

Compliance content streams

The following table lists all available compliance content streams.

Name	Description
Prerequisite	**Prerequisite content for installing additional policies**
cc_library	Configurable audit and remediation (A&R) compliance policy for both Windows and Unix
Audit and Remediation Dynamic Policies	**Customizable, actively supported dynamic policies**
cc_pci_windows	Dynamic A&R PCI policies for SA on Windows

Name	Description
cc_pci_unix	Dynamic A&R PCI policies for SA on UNIX
ec_cis_aix	Dynamic A&R CIS policies for SA on AIX
ec_cis_esx	Dynamic A&R CIS policies for SA on ESX
ec_cis_hpux	Dynamic A&R CIS policies for SA on HP-UX
ec_cis_rhel	Dynamic A&R CIS policies for SA on RHEL
ec_cis_solaris	Dynamic A&R CIS policies for SA on Solaris
ec_cis_suse	Dynamic A&R CIS policies for SA on SUSE
ec_cis_windows	Dynamic A&R CIS and MS policies for SA on Windows
ec_disa_stig	Dynamic A&R DISA policies for SA on UNIX and Windows
Basic Audit and Remediation Policies	**Non-customizable policies**
cc_fisma_ windows	A&R FISMA policies for SA on Windows
cc_fisma_unix	A&R FISMA policies for SA on UNIX
cc_hipaa_ windows	A&R HIPAA policies for SA on Windows
cc_hipaa_unix	A&R HIPAA policies for SA on UNIX
cc_sox_windows	A&R SOX policies for SA on Windows
cc_sox_unix	A&R SOX policies for SA on UNIX
cc_cis_ubuntu	A&R CIS policies for SA on Ubuntu
cc_cis_centos	A&R CIS policies for SA on Centos
cc_cis_oel	A&R CIS policies for SA on OEL
cc_iso_windows	A&R ISO policies for SA on Windows
cc_iso_unix	A&R ISO policies for SA on Unix

Integrating with DMA

This topic discusses the use of HPE Database and Middleware Automation (DMA) flows with HPE Server Automation(SA). DMA uses SA as its server management tool.

DMA overview

DMA addresses the shortfalls of custom scripting or using disparate ad hoc tools. It delivers industry-standard best-practices and subject matter expertise to address challenges around compliance, middleware and database patching, middleware and database provisioning and code release. DMA enables IT teams to enforce organizational standards across the enterprise. It supports database and middleware technologies from multiple vendors.

Integration tasks

The DMA integration with SA is covered in the HPE DMA Installation Guide available on SSO (https://softwaresupport.hpe.com/).

Refer to the appropriate section of the HPE DMA Installation Guide to accomplish the following tasks:

Tasks	Section
To install DMA—including all necessary integrations with SA	"How to Install HPE DMA"
To uninstall DMA—including uninstalling DMA from the SA managed servers	"How to Uninstall HPE DMA"
To upgrade to a new DMA version—including reinstalling the DMA APX on the SA Core	"How to Upgrade HPE DMA"
To link the current DMA version into SA	"How to Link HPE DMA into HPE Server Automation"

Integrating with OBR

HPE Server Automation (SA) is integrated with HPE Operations Bridge Reporter (OBR) for reporting requirements. The reports include:

1. SA Audit Compliance

2. SA Patch Compliance

3. SA Server Inventory

About HPE OBR

Operations Bridge Reporter (OBR) is the reporting solution for HPE Server Automation.

It provides advanced analysis on data center automation activities and enables you to leverage SA to make decisions based on day-day (current) and historical data. The data analyzed is collected from SA that performs automation and monitoring services in the data center.

HPE OBR allows you to perform the following functions:

- Create your own Content Packs. HPE OBR provides Content Development

- Environment (CDE) to create new Content Packs and customize existing Content Packs

- Customize and extend the out-of-the-box Content Packs provided in the product

- Create your own groups for reporting. For example, you can create groups based on the business management chain or business functions

OBR includes the following Software Components:

- SAP Business Objects for reporting

- HP Vertica database for storing, processing, and managing the performance data

Integrating with OBR

The following workflow provides an overview for configuring and integrating OBR with SA for generating reports:

Task	Details	Resources
Plan	• Refer to HPE OBR documentation for information about planning • Download the following HPE OBR core components: ○ HPE OBR ○ Vertica ○ Vertica license ○ SAP Business Object Enterprise (BOE) ○ Download HPE_Server-Automation Audit Compliance Content Pack from HPELN.	Locate the HPE OBR documentation sent on HPELN and navigate to **manuals** from **Document Type**.
Install OBR Core	1. Install the HPE OBR Core 2. Install Vertica and apply the Vertica license 3. Set up the data warehouse 4. Install SAP BOE	Locate the HPE OBR documentation sent on HPELN and navigate to **manuals** from **Document Type**.
Install Content Pack	Install the HPE OBR-SA Reports Content Packs	Obtain the content pack from HPELN.
Configure SA as the Data Source for OBR	Configure HPE SA as a data source to OBR	For details, see HPE OBR-SA Reports Content Pack Configuration Guide at HPELN. From HPELN, navigate to **Resource** > **File Repository**> **Documentation**.
Install Dataminer		For details, see HPE OBR-SA Reports Content Pack Configuration Guide at HPELN. From HPELN, navigate to **Resource** > **File Repository**> **Documentation**.

Task	Details	Resources
Ready for OBR SA Reporting		For details, see the Reports Guide at HPELN. From HPELN, navigate to **Resource** > **File Repository**> **Documentation**.

Send documentation feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Integration Guide (Server Automation 10.50)

Just add your feedback to the email and click send.

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

We appreciate your feedback!