IBM Network Performance Insight 1.1.0
Document Revision R2E1

Integrating IBM Tivoli Netcool/OMNibus

IBM
<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Before using this information and the product it supports, read the information in “Notices” on page 49.</td>
</tr>
</tbody>
</table>
Contents

Integrating with Tivoli Netcool/OMNIbus v
   Intended audience v
   Organization v
   Network Performance Insight overview vi
   Service Management Connect vii
   Network Performance Insight technical training vii
   Support information viii
   Conventions used in this publication viii
      Typeface conventions viii

Chapter 1. Introduction to Tivoli Netcool/OMNIbus 1
   Tivoli Netcool/OMNIbus Web GUI menu 1
   The ObjectServer 2

Chapter 2. Prerequisites 3
   Supported configurations 3
   Software requirements and dependencies 5

Chapter 3. Preparing your environment 7
   Installing Jazz for Service Management 7
   Groups and users 8
      Creating users and groups in a repository 9
      Granting roles to npiAdmin user 10
   Single sign-on 10
      Configuring single sign-on on the Jazz for Service Management server 11
   Installing and configuring Network Performance Insight 12
      Configuring the Network Performance Insight for communicating with Jazz for Service Management 13
   Installing and configuring Tivoli/Netcool OMNIbus 15
      Quick reference to Tivoli Netcool/OMNIbus installation 15
      Starting an ObjectServer 17
      Stopping an ObjectServer 18
   Configuring the SSL communication for integration 18
      Generating the SSL certificate for Network Performance Insight system 19
      Exporting SSL personal certificate for Network Performance Insight system 20
      Copying Jazz for Service Management root certificate to Network Performance Insight 21
      Adding the root certificate to your browser 22
      Adding the root certificate to JRE keystore on your desktop 22

Chapter 4. Integration with Tivoli Netcool/OMNIbus Web GUI 23
   Quick reference to integration 24
   Logging in to the Dashboard Application Services Hub portal 24
   Configuring Network Performance Insight console integration on Jazz for Service Management 25
   Configuring thresholds from Console Integrations 26
   Configuring launch-in-context integration with Network Performance Insight 28
      Creating a launch-in-context tool 28
      Configuring launch-in-context menu 29
      Sending Network Performance Insight Threshold Events to OMNIbus 29
   Configuring the OMNIbus REST APIs in Network Performance Insight 30
   Encrypting Object Server password 32
   Changing ObjectServer user password 32

Chapter 5. Monitoring events from Web GUI on Dashboard Application Services Hub 35
   Event severity levels 36

Chapter 6. Troubleshooting integration with Tivoli Netcool/OMNIbus 37
   Cannot view the Event List from AEL if the list of events is large 37
   Do not use Google Chrome to view Tivoli Netcool/OMNIbus Web GUI events on Dashboard Application Services Hub 37
   Timezone settings on Event Viewer and Network Performance Insight dashboards on Dashboard Application Services Hub are not the same 37

Appendix A. Adding the LDAP user registry as a federated repository 39

Appendix B. npid command reference 43

Appendix C. Common directory locations for Jazz for Service Management 45

Notices 49
   Trademarks 51
   Terms and conditions for product documentation 52
Integrating with Tivoli Netcool/OMNibus

How to integrate IBM® Network Performance Insight with IBM® Tivoli® Netcool/OMNibus component of IBM Netcool® Operations Insight.

Provides step-by-step instructions on how to integrate Network Performance Insight with Tivoli Netcool/OMNibus.

**Important:** Before you install and use Network Performance Insight, read the *IBM Network Performance Insight: Release Summary*. The Release Summary can contain information specific to your installation that is not contained in this information. Failure to consult the Release Summary might result in a corrupted, incomplete, or failed installation and integration.

**Intended audience**

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

To integrate Network Performance Insight with successfully, you must have a thorough understanding of the following subjects:

- Network Performance Insight 1.1.0 system
- Basic principles of network protocols and network management
- Flow concepts
- Fault management capabilities of IBM Tivoli Netcool/OMNibus
- Jazz for Service Management 1.1.2.1

**Organization**

Read this summary to help you find the information that you need.

- Chapter 1, “Introduction to Tivoli Netcool/OMNibus,” on page 1
- Chapter 2, “Prerequisites,” on page 3
- Chapter 3, “Preparing your environment,” on page 7
- Chapter 4, “Integration with Tivoli Netcool/OMNibus Web GUI,” on page 23
- Chapter 5, “Monitoring events from Web GUI on Dashboard Application Services Hub,” on page 35
- Chapter 6, “Troubleshooting integration with Tivoli Netcool/OMNibus,” on page 37
Network Performance Insight overview

IBM Network Performance Insight is a flow-based network traffic performance monitoring system.

Network Performance Insight provides comprehensive, flexible, and scalable traffic data management with visualization and reporting to support complex, multi-vendor, multi-technology networks. It offers a range of dashboard views with robust security features that are designed to meet the needs of executive management and converging network and IT operations teams.

Network Performance Insight offers near real-time and interactive view on the traffic data that helps in reduced network repair times and optimized network performance.

Network Performance Insight provides IBM Netcool Operations Insight with network performance monitoring capabilities to address modern network management challenges around application-oriented, software-defined-networks in the enterprise data centers and intranet.

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

The flow records that are sent by the configured flow exporters are collected by Collector, segregated, and sent to Inventory or Analytics component based on the information that they contain.

Analytics component performs flow session categorization and aggregation. These results are then stored in Network Performance Insight database.

Additionally, you can control the flow interface to enable collection and perform administrative tasks on the web-based user interface on Jazz for Service Management portal. The dashboards provide up-to-date actionable information to increase insight into network problems and streamline root cause analysis.
The database can be queried to display the results on the Dashboard Application Services Hub portal in the form of specialized report tables, graphs, and charts that are ready for immediate use. The database is designed for high performance.

You can integrate Network Performance Insight with Tivoli Netcool/OMNIbus to take advantage of its fault management capabilities.

Network Performance Insight documentation consists of the following:
- Release summary
- Installing Network Performance Insight
- Configuring Network Performance Insight
- Integrating with Tivoli Netcool/OMNIbus component of Netcool Operations Insight.
- Using Network Performance Insight
- Troubleshooting Network Performance Insight
- References
- Technical notes

Related information:

IBM Network Performance Insight on IBM Knowledge Center

**Service Management Connect**

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

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

Related information:

IBM Network Performance Insight community on developerWorks

**Network Performance Insight technical training**

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

**Support information**

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


IBM Support Assistant

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

Troubleshooting Guide

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

Conventions used in this publication

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

Typeface conventions

This publication uses the following typeface conventions:

**Bold**

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

**Italic**

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

**Monospace**

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

**Bold monospace**

- Command names, and names of macros and utilities that you can type as commands
- Environment variable names in text
- Keywords
- Parameter names in text: API structure parameters, command parameters and arguments, and configuration parameters
- Process names
- Registry variable names in text
- Script names
Integrating IBM Tivoli Netcool/OMNibus
Chapter 1. Introduction to Tivoli Netcool/OMNibus

Tivoli Netcool/OMNibus is a service level management (SLM) system that delivers real-time, centralized monitoring of complex networks and IT domains.

IBM Netcool Operations Insight uses real-time alarm and alert analytics, which are combined with broader historic data analytics. Netcool Operations Insight is powered by the fault management capabilities of IBM Tivoli Netcool/OMNibus and IBM's leading big data technologies within IBM Operations Analytics - Log Analysis, providing powerful event search and historical analysis in a single solution.

Currently, Network Performance Insight integrates with Tivoli Netcool/OMNibus component of IBM Netcool Operations Insight.

Tivoli Netcool/OMNibus tracks alert information in a high-performance, in-memory database, and presents information of interest to specific users through filters and views that can be configured individually. Tivoli Netcool/OMNibus has automation functions that can perform intelligent processing on managed alerts.

Components of Tivoli Netcool/OMNibus:
- ObjectServer
- Probes
- Gateways
- Desktop tools
- Administration tools
- Web GUI

Related information:

Solution overview - IBM Netcool Operations Insight v1.3.1
Supported products and components in IBM Netcool Operations Insight v1.3.1
Introduction to Tivoli Netcool/OMNibus

Tivoli Netcool/OMNibus Web GUI menu

The Web GUI is a web-based application that presents event data from multiple data sources in various graphical formats in supported web browsers and mobile devices. The Web GUI includes most features of the Tivoli Netcool/OMNibus desktop components.

Although the Web GUI typically receives event data from ObjectServers, it can connect to any data source from which event information can be obtained. The Web GUI uses a client/server architecture and it is hosted inside Dashboard Application Services Hub, which is part of Jazz™ for Service Management.

Clients connect to Dashboard Application Services Hub to access the Web GUI. You can install the Web GUI into an existing Jazz for Service Management.

Related information:
The ObjectServer

The ObjectServer is the in-memory database server at the core of Tivoli Netcool/OMNIbus.

Event information is forwarded to the ObjectServer from external programs such as probes and gateways. This information is stored and managed in database tables, and displayed in the Web GUI event lists, or in the desktop event list.

Related information:
Chapter 2. Prerequisites

Ensure that you fulfill the prerequisites for integrating Network Performance Insight with Tivoli Netcool/OMNIbus Web GUI.

- IBM JRE 7.0, 64-bit

**Note:** The Web GUI supports the IBM JRE 7.0. Always apply the latest updates to the JRE on the Web GUI host.

- Jazz for Service Management 1.1.2.1

- Supported browsers:
  - Internet Explorer 9, 10
  - Mozilla Firefox ESR 24, 31
  - Google Chrome 42, 43

The most up-to-date information about supported hardware, software, browsers, and operating systems is provided by the IBM Software Product Compatibility Reports website.

**Related information:**

- [Installing and updating Tivoli Netcool/OMNIbus](#)
- [Installing and updating the Web GUI component](#)

**Supported configurations**

The following configurations are supported in this solution. This installation scenario describes a fresh installation of Network Performance Insight that is integrated with Netcool Operations Insight. A sample three-server system architecture is presented.

A preferred distributed installation configuration for the integration is as follows:
Server 1
Hosts all the components of Network Performance Insight in a stand-alone installation.

Server 2
Hosts the Tivoli Netcool/OMNIbus V8.1.0.5 core components.

Note: Tivoli Netcool/OMNIbus Object Server is recommended to be installed on a separate server than Network Performance Insight and Tivoli Netcool/OMNIbus Web GUI.

Server 3
Hosts Dashboard Application Services Hub, which is a component of Jazz for Service Management and Tivoli Netcool/OMNIbus Web GUI V8.1.0.4 component.
Software requirements and dependencies

Ensure that you have all of the required software before you start the integration.

Ensure that the following software is available:

- IBM Network Performance Insight, Version 1.1.0
- IBM Tivoli Netcool/OMNIbus v8.1 for Netcool Operations Insight V1.3.1, Fix Pack 5
- IBM Tivoli Netcool/OMNIbus Web GUI v8.1 for Netcool Operations Insight V1.3.1, Fix Pack 4
- Dashboard Application Services Hub on Jazz for Service Management, V1.1.2.1

IBM Tivoli Netcool/OMNIbus Web GUI uses a client/server architecture and it is hosted inside Dashboard Application Services Hub, which is part of Jazz for Service Management. Clients connect to Dashboard Application Services Hub to access the Web GUI.

Related information:

- Jazz for Service Management Detailed System Requirements
- Planning for installation or upgrade of IBM Tivoli Netcool/OMNIbus 8.1.0
Chapter 3. Preparing your environment

Before you begin

Ensure that IBM Network Performance Insight, Version 1.1.0 is installed on your system. For more information, see Installing IBM Network Performance Insight.

Installing Jazz for Service Management

Install all the UI components that are based on Dashboard Application Services Hub onto a single host. All the products and components on this host are installed by IBM Installation Manager.

About this task

The UI components are installed in two stages. Install IBM WebSphere Application Server and Jazz for Service Management first, which provide the underlying UI technology, and then install the Web GUI. After installation, configure the Web GUI to integrate with Network Performance Insight.

For more information about Jazz for Service Management 1.1.2.1 installation, see Installing Network Performance Insight.

Note: Always use fully qualified domain name in the URLs when you access the Jazz for Service Management servers.

Related information:

Stopping Jazz for Service Management application servers

You can stop any Jazz for Service Management application server by using the IBM WebSphere stopServer command. You might need to restart the application server after you complete a configuration task for an integration service, or stop the application server for maintenance. To start the server again, use the startServer command.

Procedure

1. On the relevant Jazz for Service Management server, open a command window.
2. Change to the JazzSM_WAS_Profile/bin directory. The default location for JazzSM_WAS_Profile is /opt/IBM/JazzSM/profile.
3. Run the following command:

   ```
   ./stopServer.sh <server_name> -username <WAS_admin_user_name> -password <WAS_admin_password>
   ```

   Where

   **server_name**
   
   Enter the name of the application server that was specified when the application server profile was created. For example, server1.

   **WAS_admin_user_name**
   
   The default user name is smadmin.
**WAS_admin_password**
This is the password that is specified at the time of installation.

**Example**

stopServer.sh server1 -username smadmin -password jazzmpwd

**Starting Jazz for Service Management application servers**
You can start any Jazz for Service Management virtualization and reporting servers by using the IBM WebSphere startServer command. You might need to restart the application server after you complete a configuration task for an integration service, or after you stop the application server for maintenance.

**About this task**
The same procedure applies to any Jazz for Service Management application server.

**Procedure**

1. On the relevant Jazz for Service Management server, open a command window.
2. Change to the <JazzSM_WAS_Profile>/bin directory. The default location for <JazzSM_WAS_Profile> is /opt/IBM/JazzSM/profile.
3. Run the following command:

   ```bash
   ./startServer.sh server_name
   ```

   Where

   `server_name`
   
Enter the name of the application server that was specified when the application server profile was created. For example, server1.

---

**Groups and users**

All the required users and groups must be set up on the system before integration.

Create the following groups on the user repository that is used by the Jazz for Service Management server:

- npiuser
- npiadministrator
- ConsoleUser
- ConsoleAdmin
- WriteAdmin
- ReadAdmin
- manager-gui
- manager-script
- manager-jmx
- manager-status

A user who has access to all event management tasks that includes menu creation and tool creation must exist. If such a user does not exist, then create an
appropriate user. Ensure that the user is assigned to a group npiadministrator or Netcool_OMNIbus_User and user role as ncw_admin or ncw_user.

Create the following users:
- **npiadmin**
  Must be a part of all the groups that are created earlier.
- **npiuser**
  Must be a part of the ConsoleUser and npiuser groups that are created earlier.

**Creating users and groups in a repository**

Security relies on users and user groups. You define the groups to which the users belong in the application server. For this purpose, you can configure a federated repository as a user registry or WebSphere Application Server-based repository.

**Procedure**

1. Log in to Jazz for Service Management server.
   See “Logging in to the Dashboard Application Services Hub portal” on page 24.
2. Expand **Console Settings > WebSphere Administrative Console**.
3. Click **Launch WebSphere Administrative Console**.
4. In the side pane, open **Users and Groups > Manage Groups**.
5. Click **Create**.
6. Create all the groups that are specified in “Groups and users” on page 8.
7. Click **Close**.
   On the **Manage Groups** page, the table shows the existing groups.
8. In the side pane, open **Users and Groups > Manage Users**.
9. Click **Create**.
10. Create all the users that are specified in “Groups and users” on page 8.
11. Assign this new user to a group.
   a. Click **Group Membership**.
   b. On the Group Membership page, click **Search**.
   c. In the **Available** column, select a group and click **Add**.
   d. Click **Close**.
   e. Restart your application server.

**What to do next**

Alternatively you can use LDAP user registry, see Appendix A, “Adding the LDAP user registry as a federated repository,” on page 39.
Granting roles to npiadmin user

Console users are granted access to resources based on the role to which they have been assigned.

Procedure

1. Log in to Dashboard Application Services Hub portal as admin user. By default, smadmin.
2. In the navigation pane, select Console Settings > User Roles.
3. To assign a role to a user, click Search. A list of available users is displayed.
4. Click npiadmin user from the User ID column.
   A list of available roles for the selected user is displayed on a new page. Those roles that are currently associated with the selected user are checked.
5. Select all the roles and assign to npiadmin user.
   This grants all the Dashboard Application Services Hub roles to npiadmin user.
6. Click Save.

What to do next

Log off from Dashboard Application Services Hub and log in again to ensure all the privileges that include admin privileges are available to the npiadmin user.

Related tasks:

“Creating users and groups in a repository” on page 9

Security relies on users and user groups. You define the groups to which the users belong in the application server. For this purpose, you can configure a federated repository as a user registry or WebSphere Application Server-based repository.

Single sign-on

The single sign-on (SSO) capability in Tivoli products means that you can log on to one Tivoli application, and then start other Tivoli web-based or web-enabled applications without having to reenter your user credentials.

The repository for the user IDs can be the Tivoli Netcool/OMNIbus ObjectServer or a Lightweight Directory Access Protocol (LDAP) registry. A user logs on to one of the participating applications, at which time their credentials are authenticated at a central repository. With the credentials authenticated to a central location, the user can then start from one application to another to view related data or perform actions. Single sign-on can be achieved between applications that are deployed to Dashboard Application Services Hub servers on multiple machines.

Single sign-on capabilities require that the participating products use Lightweight Third Party Authentication (LTPA) as the authentication mechanism. When SSO is enabled, a cookie is created containing the LTPA token and inserted into the HTTP response.

When the user accesses other web resources (portlets) in any other application server process in the same Domain Name Service (DNS) domain, the cookie is sent with the request. The LTPA token is then extracted from the cookie and validated. If the request is between different cells of application servers, you must share the LTPA keys and the user registry between the cells for SSO to work. The realm names on each system in the SSO domain are case-sensitive and must match exactly.
Configuring single sign-on on the Jazz for Service Management server

Use these instructions to establish single sign-on support and configure a federated repository.

Before you begin

Configuring SSO is a prerequisite to integrating products that are deployed on multiple servers. All Jazz for Service Management server instances must point to the central user registry (such as a Lightweight Directory Access Protocol server).

About this task

To configure Global Security to enable SSO, follow these steps:

Procedure

1. Log in to Jazz for Service Management server as admin user.
   See “Logging in to the Dashboard Application Services Hub portal” on page 24.
2. In the navigation pane, click Console Settings > Websphere Administrative Console and click Launch Websphere administrative console.
3. In the WebSphere Application Server administrative console navigation pane, click Security > Global security.
4. In the Administrative Security section, select the Enable administrative security check box.
5. In the Application Security section, select the Enable application security check box.
6. In the Authentication section, expand Web and SIP security and click Single sign-on (SSO).
7. Click Enabled option if the SSO is disabled.
8. Click Requires SSL if all the requests are expected to use HTTPS.
9. Enter the fully qualified domain names in the Domain name field where SSO is effective. For example, .ibm.com
   If the domain name is not fully qualified, the Jazz for Service Management Server does not set a domain name value for the LtpaToken cookie and SSO is valid only for the server that created the cookie. Single sign-on feature is necessary for different components of Netcool Operations Insight to interact with each other. For SSO to work across the Tivoli applications, their application servers must be installed in same domain (use the same domain name).
10. Set the LTPA V2 Cookie name to LtpaToken2.
11. Optional: Enable the Interoperability Mode option if you want to support SSO connections in WebSphere Application Server version 5.1.1 or later to interoperate with previous versions of the application server.
12. Select the Web inbound security attribute propagation check box to propagate information from the first login application server to the other application servers.
13. Clear the Set security cookies to HTTPOnly to help prevent cross-site scripting attacks check box.
14. Click OK to save your changes.
15. Stop and restart all the Jazz for Service Management server instances.
What to do next

When you start Jazz for Service Management, you must use a URL in the format protocol://host.domain:port/*. If you do not use a fully qualified domain name, Jazz for Service Management cannot use SSO between Tivoli products.

The configured single sign-on uses SSO tokens that are set in HTTP cookies to carry authenticated sessions. By default, these cookies expire after 120 minutes. To change this value, follow these steps:

1. In the WebSphere Application Server administrative console navigation pane, click Security > Global security.
2. In the Authentication section, click LTPA.
3. Change the LTPA timeout value to a different value.
   This value must be greater than the Cache timeout.

The credentials expire after the specified period you might have to revalidate your credentials.

Related tasks:

- "Stopping Jazz for Service Management application servers" on page 7
  You can stop any Jazz for Service Management application server by using the IBM WebSphere stopServer command. You might need to restart the application server after you complete a configuration task for an integration service, or stop the application server for maintenance. To start the server again, use the startServer command.
- "Starting Jazz for Service Management application servers" on page 8
  You can start any Jazz for Service Management virtualization and reporting servers by using the IBM WebSphere startServer command. You might need to restart the application server after you complete a configuration task for an integration service, or after you stop the application server for maintenance.

Related information:

- Configuring Jazz for Service Management for SSO
- Release Summary for IBM Network Performance Insight

Installing and configuring Network Performance Insight

Describes installation and configurations that are needed on the server where Network Performance Insight is installed for integrating with Tivoli Netcool/OMNibus component of IBM Netcool Operations Insight.

Procedure

Install Network Performance Insight.
See Installing IBM Network Performance Insight.

Related information:

- Release Summary for IBM Network Performance Insight
Configuring the Network Performance Insight for communicating with Jazz for Service Management

This configuration in npi.conf file helps Network Performance Insight server to communicate with the server where Jazz for Service Management is installed.

About this task

You can use the template file npi-dash.template that is available in <NPI_Home>/conf folder.

Procedure

1. Create or edit npi.conf file and enter the following details:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Recommended value</th>
</tr>
</thead>
<tbody>
<tr>
<td>https.port</td>
<td>Secure port on which Network Performance Insight application console can be accessed</td>
<td>9443</td>
</tr>
<tr>
<td>https.keystore.file</td>
<td>Full path for the keystore file that stores SSL certificate that is used by Network Performance Insight.</td>
<td>conf/security/security.keystore</td>
</tr>
<tr>
<td>https.keystore.password</td>
<td>Password for SSL keystore that is used by Network Performance Insight.</td>
<td>WebAS Note: Use the encrypted password. To encrypt, follow the steps in Encrypting Object Server password in Integrating with Tivoli/Netcool OMNibus.</td>
</tr>
<tr>
<td>https.key.password</td>
<td>Password for SSL Key that is used by Network Performance Insight</td>
<td>WebAS Note: Use the encrypted password. To encrypt, follow the steps in Encrypting Object Server password in Integrating with Tivoli/Netcool OMNibus.</td>
</tr>
<tr>
<td>security.dash.hostname</td>
<td>Full DNS name for Jazz for Service Management server. If this parameter is left blank, Network Performance Insight integration with Netcool Operations Insight does not work. This entry must be added before you start Dashboard Application Services Hub for the first time.</td>
<td>&lt;myserver.ibm.com&gt;</td>
</tr>
</tbody>
</table>
Table 1. Configurations for Network Performance Insight (continued)

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Recommended value</th>
</tr>
</thead>
<tbody>
<tr>
<td>security.dash.port</td>
<td>HTTPS port on which Jazz for Service Management server communicates.</td>
<td>The default Dashboard Application Services Hub HTTPS port is 16311.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Copy Dashboard Application Services Hub root signer certificate file by using the name WebSphereCACert.pem to <code>&lt;NPI_Home&gt;/conf/security</code> folder. Without this file, Network Performance Insight cannot connect to Dashboard Application Services Hub secure port.</td>
</tr>
<tr>
<td>security.dash.username</td>
<td>Administrator user name for Jazz for Service Management</td>
<td>smadmin</td>
</tr>
<tr>
<td>security.dash.password</td>
<td>Password for Jazz for Service Management administrator user. This password can be encrypted.</td>
<td>smadmin</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: Use the encrypted password. To encrypt, follow the steps in Encrypting Object Server password in Integrating with Tivoli/Netcool OMNIbus.</td>
</tr>
<tr>
<td>security.dash.domain</td>
<td>Domain name of the server. This entry must be added before you start Dashboard Application Services Hub for the first time.</td>
<td>.ibm.com</td>
</tr>
</tbody>
</table>

Example entries:

```
https.port=9443

https.keystore.file="conf/security/security.keystore"
https.keystore.password="86qTwzkzrq3gJcKwGbI1HlO=="
https.key.password="86qTwzkzrq3gJcKwGbI1HlO=="
security.dash.hostname="<myserver.ibm.com>"
security.dash.port=16311
security.dash.username="smadmin"
security.dash.password="UZceWXqtBV1rfu5OFfWmg=="
security.dash.domain=".your-domain.com"
```

2. Save this file to `<NPI_home>/conf` directory.

`<NPI_home>` is where Network Performance Insight is installed. For example, `/opt/IBM/NPI`.

3. Restart your system.

**Controlling Network Performance Insight system**

Commands to control the Network Performance Insight application processes.

**Procedure**

Run the `npid` command to start, stop, and restart Network Performance Insight by using the following commands:
Installing and configuring Tivoli/Netcool OMNIbus

Describes installation and configurations that are needed on the Tivoli Netcool/OMNIbus server and IBM Tivoli Netcool/OMNIbus Web GUI that is required for integrating with Network Performance Insight.

Quick reference to Tivoli Netcool/OMNIbus installation

Use this information as a quick reference if you are new to Tivoli Netcool/OMNIbus and want to perform a quick installation and configuration to obtain a running ObjectServer.

The following table lists the high-level steps for installing Tivoli Netcool/OMNIbus.

Table 2. Quick reference for installing Tivoli Netcool/OMNIbus

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prepare for installation by checking the prerequisites and obtaining the installation package.</td>
<td>IBM Prerequisite Scanner</td>
</tr>
<tr>
<td>Install Tivoli Netcool/OMNIbus and accept all the default installable features.</td>
<td>Installing Tivoli Netcool/OMNIbus</td>
</tr>
<tr>
<td>If necessary, set the following environment variables:</td>
<td>Setting environment variables</td>
</tr>
<tr>
<td>• $NCHOME</td>
<td>Checking shared library paths</td>
</tr>
<tr>
<td>By default, /opt/IBM/tivoli/netcool</td>
<td></td>
</tr>
<tr>
<td>• $OMNIHOME</td>
<td></td>
</tr>
<tr>
<td>By default, $NCHOME/omnibus</td>
<td></td>
</tr>
<tr>
<td>• $PATH</td>
<td></td>
</tr>
<tr>
<td>By default, $NCHOME/omnibus/bin</td>
<td></td>
</tr>
<tr>
<td>• Solaris</td>
<td></td>
</tr>
<tr>
<td>$LD_LIBRARY_PATH</td>
<td></td>
</tr>
<tr>
<td>By default, /opt/IBM/tivoli/netcool/platform/&lt;arch&gt;/lib64</td>
<td></td>
</tr>
<tr>
<td>• AIX</td>
<td></td>
</tr>
<tr>
<td>$LIBPATH</td>
<td></td>
</tr>
<tr>
<td>By default, /opt/IBM/tivoli/netcool/platform/&lt;arch&gt;/lib64</td>
<td></td>
</tr>
</tbody>
</table>

Note: <arch> refers to the operating system.
Table 2. Quick reference for installing Tivoli Netcool/OMNibus (continued)

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create an ObjectServer by running the database initialization utility as follows:</td>
<td>Creating an ObjectServer</td>
</tr>
<tr>
<td>$NCHOME/omnibus/bin/nco_dbinit -server servername</td>
<td></td>
</tr>
<tr>
<td>Where servername is the ObjectServer name, which must consist of 29 or fewer uppercase letters and cannot begin with an integer.</td>
<td></td>
</tr>
<tr>
<td>The default database tables and data, users, groups, roles, and properties file are created. (You can use the default user root, which is created with a blank password, to log in to the ObjectServer).</td>
<td></td>
</tr>
<tr>
<td>Note: To update the root password, see “Changing ObjectServer user password” on page 32</td>
<td></td>
</tr>
<tr>
<td>Configure server communication information for the ObjectServer on the host computer.</td>
<td>Configuring server communication information</td>
</tr>
<tr>
<td>1. Update the ObjectServer communication information by editing the connections data file ($NCHOME/etc/omni.dat), and generate the interfaces file for Tivoli Netcool/OMNibus communications by running the following command:</td>
<td>“Starting an ObjectServer” on page 17</td>
</tr>
<tr>
<td>$NCHOME/bin/nco_igen</td>
<td></td>
</tr>
<tr>
<td>The interfaces file $NCHOME/etc/interfaces.arch is created, where arch represents the operating system name.</td>
<td></td>
</tr>
<tr>
<td>Note: The example entries in the communication details use the default host name omnihost. Change this to the name of the computer on which each server is run.</td>
<td></td>
</tr>
<tr>
<td>Start the ObjectServer by running the following command:</td>
<td></td>
</tr>
<tr>
<td>$NCHOME/omnibus/bin/nco_objserv -name servername</td>
<td></td>
</tr>
<tr>
<td>Prepare to install the Web GUI by checking the prerequisites, deciding on the type of installation that is required, and gathering the required information.</td>
<td>Planning for installation or upgrade</td>
</tr>
<tr>
<td>Install the Web GUI by using the wizard, console mode, or silent mode. Use the information that is gathered from the previous step to specify the parameters of the installation.</td>
<td>Installing and updating the Web GUI component</td>
</tr>
<tr>
<td></td>
<td>Gathering installation information</td>
</tr>
<tr>
<td></td>
<td>Installing the Web GUI</td>
</tr>
</tbody>
</table>

Integrating IBM Tivoli Netcool/OMNibus
Table 2. Quick reference for installing Tivoli Netcool/OMNIbus (continued)

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perform the configuration for the required user registry, for example LDAP, against the Dashboard Application Services Hub installation.</td>
<td>Configuring user authentication</td>
</tr>
</tbody>
</table>

Starting an ObjectServer

You must have an ObjectServer running before you can use the components of Tivoli Netcool/OMNIbus.

About this task

You can start an ObjectServer:

- Automatically, using process control on UNIX
  - If started by the process agent, the ObjectServer automatically restarts if it fails.
  - By starting the process agent when the system starts, you can make the ObjectServer start automatically
- Manually, from the command line

Procedure

1. To start an ObjectServer as a process, enter the following command:
   
   `nco_pa_start -process ObjectServer`

   **Note:** You can start the ObjectServer from a remote computer. The name that you specify with the `-server` option is compared to the process agent names that are configured in the Server Editor. The host computer and port are identified and the command is sent to the correct process agent.

2. Use the `nco_objserv` command to start the ObjectServer manually. Use the following command:
   
   `$NCHOME/omnibus/bin/nco_objserv [ -name servername ]`

   In this command, `servername` is the ObjectServer name. If you do not specify the `-name` command-line option, `nco_objserv` attempts to start the NCOMS ObjectServer. You can start the ObjectServer with extra command-line options.

   **Note:** An ObjectServer that is started from the command line is not under process control, and must be restarted manually if it is shut down.

   On start, the ObjectServer attempts to open the `$NCHOME/omnibus/etc/servername.props` properties file, where `servername` is the name of the specified ObjectServer.

Related information:

[Starting an ObjectServer](#)
Stopping an ObjectServer

You can stop an ObjectServer by using process control. You can also stop an ObjectServer from the SQL interactive interface.

About this task

You can stop an ObjectServer:

- Automatically, using process control on UNIX by using the process agent. The ObjectServer must be defined as a process.
- From the SQL interactive interface.

If you manually started an ObjectServer from the command-line, you must manually stop the ObjectServer by using the SQL interactive interface. You must have the appropriate permissions to stop the ObjectServer.

Procedure

1. To stop an ObjectServer as a process, enter the following command:
   `nco_pa_stop -process ObjectServer`
   a. To stop the ObjectServer from a remote computer, enter the following command:
      `nco_pa_stop -server NAME_PA -process ObjectServer`
      In this example, the NAME_PA value that you specify with the -server option is compared to the process agent names that are configured in the Server Editor. The host machine and port are identified, and the command is sent to the correct process agent on a remote computer.

2. To stop an ObjectServer that was started manually:
   a. Connect to an ObjectServer by running the appropriate command for your operating system:
      `NCHOME/omnibus/bin/nco_sql [ -server servername ] [ -user username ]`
   b. Provide the requested password.
   c. When the SQL prompt is displayed, enter the following commands:
      1> alter system shutdown;
      2> go

      The nco_sql command does not allow white space preceding the go keyword. Any white space causes the SQL statements to fail.

Related information:

Stopping an ObjectServer

Configuring the SSL communication for integration

The Secure Sockets Layer (SSL) protocol provides secure communications between remote server processes or endpoints. SSL security can be used for establishing communications inbound to and outbound from an endpoint. To establish secure communications, a certificate and an SSL configuration must be specified for the endpoint.

Before you begin

Configure SSL communication after you install Network Performance Insight.
About this task

You must configure the SSL one time only. If you are reinstalling or upgrading Network Performance Insight, back up the /opt/IBM/NPI/conf/security folder from previous installation and restore it in new installation. Follow these steps to complete the SSL configuration for the integration of Network Performance Insight with Tivoli Netcool/OMNIbus.

Generating the SSL certificate for Network Performance Insight system

SSL uses digital certificates for key exchange and authentication. When a client initiates an SSL connection, the server presents the client with a certificate that is signed by a Certificate Authority (CA). A CA is a trusted party that guarantees the identity of the certificate and its creator. The server certificate contains the identity of the server, the public key, and the digital signature of the certificate issuer.

Procedure

1. Log in to the Jazz for Service Management server as admin user.
   
   See “Logging in to the Dashboard Application Services Hub portal” on page 24.

2. Expand Console Settings > WebSphere Administrative Console.

3. Click Launch WebSphere Administrative Console.

4. Expand Security and select SSL certificate and key management > Keystores and certificates > NodeDefaultKeyStore.

5. Click Personal certificates from the Additional Properties section.

6. Select Chained Certificate from the Create list.

   A chained personal certificate is a personal certificate that is created by using another certificate’s private key to sign it.

   Provide the following mandatory details as needed:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Suggested value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias</td>
<td>Specifies the alias name to identify the certificate in the key store and is used to label the certificate object.</td>
<td>NPI</td>
</tr>
<tr>
<td>Root certificate used to sign the certificate</td>
<td>Specifies the personal certificate in the key store that is used to create the chained personal certificate</td>
<td>root</td>
</tr>
<tr>
<td>Key size</td>
<td>Specifies the key size of the private key that is used by the personal certificate</td>
<td>1024</td>
</tr>
<tr>
<td>Common name</td>
<td>Specifies the common name portion of the distinguished name. Fully qualified DNS name of the Network Performance Insight server where the certificate is available.</td>
<td>&lt;myserver.ibm.com&gt;</td>
</tr>
<tr>
<td>Validity period</td>
<td>Specifies the length in days, when the certificate is valid. The default is 365 days.</td>
<td>732</td>
</tr>
<tr>
<td>Organization</td>
<td>Specifies the organization portion of the distinguished name.</td>
<td>IBM</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Suggested value</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Organization unit</td>
<td>Specifies the organization unit portion of the distinguished name. This is an optional value.</td>
<td>JazzSMNode01</td>
</tr>
<tr>
<td>Country or region</td>
<td>Specifies the country portion of the distinguished name.</td>
<td>US</td>
</tr>
</tbody>
</table>

7. Click **Apply**, and then click the **Save** link in the **Messages** box.
   The new personal certificate is created with the alias name as **NPI**.

**What to do next**

Export the certificate to key store.

**Related tasks:**

- **Exporting SSL personal certificate**
  
  Configure security for Secure Socket Layer (SSL) and key management, certificates, and notifications. The SSL protocol provides secure communications between remote server processes or endpoints. SSL security can be used for establishing communications inbound to and outbound from an endpoint. To establish secure communications, a certificate and an SSL configuration must be specified for the endpoint.

**Exporting SSL personal certificate for Network Performance Insight system**

Configure security for Secure Socket Layer (SSL) and key management, certificates, and notifications. The SSL protocol provides secure communications between remote server processes or endpoints. SSL security can be used for establishing communications inbound to and outbound from an endpoint. To establish secure communications, a certificate and an SSL configuration must be specified for the endpoint.

**Procedure**

1. Export Jazz for Service Management SSL personal certificate.
   a. Log in to the Jazz for Service Management server.
   b. Expand **Console Settings > WebSphere Administrative Console**.
   c. Click **Launch WebSphere Administrative Console**.
   d. Expand **Security** and select **SSL certificate and key management > Keystores and certificates > NodeDefaultKeyStore > Personal certificates**.
   e. Select the new personal certificate from list and click **Export**.
   f. Provide the following details in the **General Properties** section.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Suggested value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key store password</td>
<td>Specifies the password of the keystore to use for the import or export.</td>
<td>WebAS</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you do not use this password, the export operation fails with an error CWPKI0663E.</td>
<td></td>
</tr>
<tr>
<td>Alias</td>
<td>Specifies the alias that the personal certificate is referenced by in the key store.</td>
<td>NPI</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Suggested value</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------</td>
</tr>
<tr>
<td>Key store file</td>
<td>Specifies to use a key store file for the import. Full path to the keystore file to be created.</td>
<td>/opt/IBM/JazzSM/security.keystore</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies the type of the keystore file.</td>
<td>JKS</td>
</tr>
<tr>
<td>Key file password</td>
<td>Specifies the password that is used to access the key store file.</td>
<td>WebAS</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you do not use this password, the export operation fails with an error CWPKI0663E.</td>
<td></td>
</tr>
</tbody>
</table>

g. Click **Apply**, and then click **OK**.

2. Restart the Jazz for Service Management server.
3. Locate the security.keystore file in `<JazzSM_Home>` directory.
4. Copy the security.keystore file to Network Performance Insight installation directory at the following location:
   `<NPI_Home>/conf/security`

Related information:

- [Configuring an SSL connection to an LDAP server](#)

### Copying Jazz for Service Management root certificate to Network Performance Insight

Procedure to extract the Jazz for Service Management root signer certificate from Jazz for Service Management keystore and add it to Network Performance Insight keystore as a signer certificate.

#### About this task
- Extract the certificate from Jazz for Service Management.
- Copy the certificate to the `<NPI_Home>/conf/security` directory.

#### Procedure
1. Log in to the Jazz for Service Management server.
2. Expand **Console Settings > WebSphere Administrative Console.**
3. Click **Launch WebSphere Administrative Console.**
4. Expand Security and select **SSL certificate and key management > Keystores and certificates > NodeDefaultTrustStore > Signer certificates.**
5. Click **Extract.**
6. Specify the file name as `WebSphereCACert.pem`.
7. Click **Apply** and click **OK.**
   The exported Signer certificate file is saved in the directory as `/opt/IBM/JazzSM/profile/etc/WebSphereCACert.pem`.
8. Copy the certificate file to the server where Network Performance Insight is available in `<NPI_Home>/conf/security` directory.
9. Restart the Network Performance Insight application.

Related tasks:
- “Controlling Network Performance Insight system” on page 14
- Commands to control the Network Performance Insight application processes.
Adding the root certificate to your browser

The WebSphereCACert.pem file that is extracted from Jazz for Service Management must be imported to browser’s Trusted CA Certificate store.

About this task

This task must be done on all computers that access Network Performance Insight data for visualization. These steps differ on different browsers. Instructions are provided for Internet Explorer and Firefox.

Procedure

1. For Internet Explorer, follow these steps:
   a. Click Tools > Internet Options.
   b. Click Content > Certificates > Trusted Root Certification Authorities.
   c. Click Import.
   d. Browse to the location of the exported WebSphereCACert.pem file.
   e. Click Next.
   f. Select to place the certificates in Trusted Root Certification Authorities option and click Finish.

2. For Firefox, follow these steps:
   a. Click Tools > Options.
   b. Click Advanced > Certificates > View Certificates.
   c. Click Authorities > Import.
   d. Browse to the location of the exported WebSphereCACert.pem file and click Open.
   e. Select all the check boxes on the Downloading Certificate page and click OK.
   f. Click OK to close the window.

Adding the root certificate to JRE keystore on your desktop

The Active Event List (AEL) is an interactive Java applet for displaying alert data from the ObjectServer. The Java applets use different certificate stores from browsers and must be configured separately. The root certificate must be added to the Signer CA store for the JRE by using the Java Control Panel on Windows clients or System Preferences on other platforms.

About this task

This certificate must be added to the computer that you use to view Network Performance Insight visualization dashboards.

Procedure

1. On a Windows computer, click Start > Control Panel > Java.
2. Click the Security tab, and then click Manage Certificates.
3. Click the User tab and select Signer CA from the Certificate type list.
4. Click Import.
5. Browse to the location where you exported the WebSphereCACert.pem file and click Open.
6. Click Close to close the Certificates window.
7. Click Apply and click OK to close the Java Control Panel.
Chapter 4. Integration with Tivoli Netcool/OMNibus Web GUI

Explains the tasks that are associated with integrating Network Performance Insight with the Tivoli Netcool/OMNibus Web GUI application. You can view network events in real time by using your Web browser. It works with the Tivoli Netcool/OMNibus application to retrieve real-time event data. The Tivoli Netcool/OMNibus Web GUI customizable dashboards display real-time performance information and event data.

Integrating Network Performance Insight with Tivoli Netcool/OMNibus Web GUI combines the ability of Network Performance Insight to generate alerts when threshold violations are detected, with the application function of Web GUI.

An event contains the Event ID, host name, and port information. When an event is selected, some of the data for the event is sent to Network Performance Insight and used to determine the best report to present. Network Performance Insight then builds a block of HTML content that redirects the browser to a Network Performance Insight display.

Right-click an event in Active Event List of Web GUI to display the tools that are added from the alerts menu. You select an option from this menu to display a detailed Network Performance Insight report for the time period of the threshold violation or an AEL report.

The high level steps that are needed for the integration of Network Performance Insight with IBM Tivoli Netcool/OMNibus are as shown in the diagram:
Quick reference to integration

Use this information as a quick reference if you are new to Tivoli Netcool/OMNIbus and want to perform an installation from scratch.

The following table lists the high-level steps for installing and configuring the integration components.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install Network Performance Insight.</td>
<td>Installing IBM Network Performance Insight, Version 1.1.0</td>
</tr>
<tr>
<td>Configure Network Performance Insight.</td>
<td>“Configuring the Network Performance Insight for communicating with Jazz for Service Management” on page 13</td>
</tr>
<tr>
<td>Prepare for the installation by checking the prerequisites.</td>
<td>Checking prerequisites</td>
</tr>
<tr>
<td>Install IBM Installation Manager on the hosts for IBM Tivoli Netcool/OMNIbus and Jazz for Service Management.</td>
<td>Fix central</td>
</tr>
<tr>
<td>Install the Tivoli Netcool/OMNIbus core components. Apply Fix Pack 5. Associated tasks include creating and starting ObjectServers.</td>
<td>Installing Tivoli Netcool/OMNIbus Creating and running ObjectServers</td>
</tr>
<tr>
<td>Install the Tivoli Netcool/OMNIbus Web GUI V8.1. Apply Fix Pack 4. Note: Installation Manager V1.8.2.1 or later is required before Web GUI V8.1 Fix Pack 4 installation.</td>
<td>Installing Dashboard Application Services Hub and the UI components</td>
</tr>
<tr>
<td>Configure the Web GUI for integration with Network Performance Insight.</td>
<td>“Configuring launch-in-context integration with Network Performance Insight” on page 28</td>
</tr>
<tr>
<td>Monitor events from Web GUI.</td>
<td>Chapter 5, “Monitoring events from Web GUI on Dashboard Application Services Hub,” on page 35</td>
</tr>
</tbody>
</table>

Logging in to the Dashboard Application Services Hub portal

Depending upon your organization’s deployment, you can access the reporting interface through Dashboard Application Services Hub.

Procedure

Access the reporting interface from Dashboard Application Services Hub as follows:

1. Open a web browser and enter the following URL for the Jazz™ for Service Management UI and reporting server:
   https://host.domain:port/DASH_context_root
   For example: https://<myserver.ibm.com>:16311/ibm/console
   Where:
   - host.domain is the fully qualified host name or IP address of the Jazz for Service Management UI and reporting server.
   - When single sign-on (SSO) is enabled, ensure that you use the fully qualified host name in the URL of the Jazz for Service Management reporting and UI
server. SSO requires that the browser pass LTPA cookies to the Jazz for Service Management application server, and these cookies contain the fully qualified host name.

- **port** is the secure HTTP port number that was specified during installation. The default value is 16311.
- **/DASH_context_root** is the context root for the console that was specified during installation. The default value is /ibm/console.

2. On the Dashboard Application Services Hub login page, enter the user ID and password. Click **Log in**. The Dashboard Application Services Hub Welcome page opens.

3. **Note:** Console Integration icon is available only after you complete the step **Configuring Network Performance Insight console integration on Jazz for Service Management** in Integrating IBM Tivoli Netcool/OMNIbus.

   In the navigation bar, click **Console Integration** icon ( ) and select the dashboard of your choice.

---

**Configuring Network Performance Insight console integration on Jazz for Service Management**

To display external content from a stand-alone console in the Dashboard Application Services Hub console, you can configure a new console integration.

**Before you begin**

Make sure that all these components of Jazz for Service Management are installed:

- IBM Dashboard Application Services Hub
- Administration Services
- Administrative Services UI
- Security Services
- Registry Services

**Note:** If the Security Services are not installed, you might encounter an Authentication Service client error with the following message ID: CTGES0039E

**Procedure**

1. Log in to Jazz for Service Management server as admin user. See “**Logging in to the Dashboard Application Services Hub portal**” on page 24.

2. In the navigation bar, click **Console Settings > Console Integrations**.
   A Console Integrations page is displayed, and existing console integrations (if any) are listed in a table.

3. In the taskbar, click the **New** icon.
   The Console Integrations configuration page is displayed.

4. Required: In the **Console Integration Name** field, provide a meaningful name for the console integration that you are creating.
   For example, **NPI Console**.
   This name is visible to all the users on Dashboard Application Services Hub portal as a folder on the main menu.
5. In the **Console Integration URL** field, enter a URL for the content that you want to display in the Dashboard Application Services Hub console. For example, `https://<myserver.mydomain.com>:9443/Blaze/rest`  
   `<myserver.mydomain.com>` is the fully qualified server name where Network Performance Insight is installed.

   **Note:** When you specify a URL, you must provide a fully qualified URL that includes `https://` and a full host DNS name for SSO to work correctly.

6. To test the connection for the URL that you entered, click **Test Connection**. If the connection is unsuccessful an error message is displayed, otherwise a Connection Successful message is displayed. For successful connections, a table lists the tasks available from stand-alone console and attributes for each task.

7. Click **Save** to commit your settings. The new console integration is added to the list in the **Console Integrations** page.

8. Close the **Console Integrations** page.

**Results**

If the connection test was successful, the specified stand-alone console content is available in the navigation bar of the Dashboard Application Services Hub console through the ⭐ icon.

**Related information:**

[Stand-alone console content integration](#)

---

### Configuring thresholds from Console Integrations

A threshold is a metric value that is compared against a value to determine whether an interface has violated a specific constraint. Using thresholds as the measure against which data is evaluated lets you report on only those resources with pertinent data.

**About this task**

These thresholds are considered static thresholds because you set the value for them by using the configuration dialog box. You also define how you want the threshold to act.

**Note:** The database tables store the Threshold configuration settings data. For more information, see **Data storage in Network Performance Insight overview**.

**Procedure**

1. Log in to Jazz for Service Management server.

2. In the navigation, click **Console Integrations** (⭐) and select **Thresholds** under **System Configuration**. You can see Flow Thresholds table.

3. Select a row from the table and click the **Edit** (⭐) button to configure a Threshold for an Interface. Enter the following details:
a. Select the **Enabled** check box to enable a Threshold on the Interface.

b. Select the **Limit Type** list to **Over, Under, or Band**.
   - **Over** Detect violations when they exceed threshold values.
   - **Under** Detect violations when they fall short of threshold values.
   - **Band** Detect violations when they go outside a range (or band) between two threshold values.

c. Enter the **Upper Limit** for the traffic flow for triggering the Threshold.

d. Enter the **Lower Limit** for the traffic flow for triggering the Threshold.

e. Enter the number of events for triggering the Threshold.

**Note:** When the threshold violation limit is crossed, it displays the severity as **Critical** in the Threshold Violation table on Traffic Overview dashboard. For more information, see *Threshold levels* in *Network Performance Insight overview*.

4. Click ![Search](image) and type an Interface in the **Filter by Domain Name** field. You can view the details of that particular entity.

5. In the **Actions** column:
   - a. Click **Edit** to edit or configure the selected Threshold. Repeat step 3
   - b. Click **Enable or Disable** to enable or disable the Threshold for an entity.
   - c. Click **Traffic Details** to view the Traffic Details for an entity.

6. Click **OK** to save the settings.

7. In the lower-right corner, the numbers displayed are the number of interfaces to be displayed on each page. Select a number to change the number of items in the table. Click the arrow to go to a particular page.

8. In the **Go to Page**, enter a page number that you want to navigate to and click **Go**.

**Results**

Any interface that is violating the new threshold value is reported in the Active Event List.

**What to do next**

You must repeat the same process to enable and configure Thresholds for all Interfaces as needed.

**Note:** Currently, you cannot select multiple interfaces to configure the thresholds values at a time.
Configuring launch-in-context integration with Network Performance Insight

Launch-in-context integrations are supported between the Web GUI and compatible Tivoli products. A launch-out integration describes the starting of another product from a Web GUI widget. A launch-in integration describes the starting of the Web GUI from another product.

About this task

Launch-in-context is the concept of moving seamlessly from one Tivoli product UI to another Tivoli product UI (either in a different console or in the same console or portal interface) with single sign-on and with the target UI in position at the proper point for users to continue with their task.

Creating a launch-in-context tool

You can create tools that are run from right-click menus in event lists or when users click a widget. Different tool formats are supported.

Procedure

1. Log in to Jazz for Service Management server as npiadmin user.
2. Select Administration > Event Management Tools > Tool Configuration from the left pane.
3. Click Create Tool and enter the following details:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>npiFlowTvLiC</td>
</tr>
<tr>
<td>Type</td>
<td>script</td>
</tr>
<tr>
<td>Script Commands</td>
<td>Copy and paste the contents of the file npiFlowTvLiC.js that is available in $NPI_home\resources/webgui. Where, $NPI_home\ is Network Performance Insight installation directory.</td>
</tr>
</tbody>
</table>

4. Select the data source name OMNIBUS.
5. Clear the Execute for each selected row check box.
6. Click Save.

A confirmation message is displayed. Click OK to close the message.

Related information:

Tools overview
Configuring launch-in-context menu

In event lists, users access default and custom tools through menus. You can add tool entries to the menus, create new submenus, and modify or delete menu items.

About this task

The two supplied menus are the Alerts menu and the Tools menu. The Alerts menu can also be opened from the right-click menu when you select an event.

Procedure

1. Log in to Jazz for Service Management server as npiadmin user.
2. Select Administration > Event Management Tools > Menu Configuration from the left pane.
3. Select the alerts menu in the window, and then click the Modify button. The Menus Editor is displayed.
4. Select the npiFlowTvLiC tool in the Available items on the left, click the arrow to move it to the Current items section.
5. Select npiFlowTvLiC from the Current items section and click Rename.
6. In the Label text box, enter a meaningful name for the new button. For example, Flow Dashboard. Enter a value in the Mnemonic text box, if needed.
7. Click Save.
8. Use the button selections on the left to move the menu option up or down. Separators might also be added by selecting <Separator> in the Available Items area of the window. The separator might be moved up and down.
9. Click Save.
   The following message is displayed:
   Menu has been successfully modified.
10. Click OK to close the message.

Results

When you right-click any event in Active Event List, you can see the npiFlowTvLiC tool that is renamed to Flow Dashboard as a selectable option in the menu. Select the tool to see the Traffic Details report associated with the interface that violated the threshold and generated the event.

Sending Network Performance Insight Threshold Events to OMNIbus

You can edit the information that is contained in the properties files for ObjectServers. A properties file has a .props extension. ObjectServer properties file is NCOMS.props.

Procedure

1. From the Conductor window on UNIX, click Properties in the button bar. The Properties Editor window opens.
2. From Type list, select ObjectServer to edit the properties files of components such as ObjectServers and proxy servers.
   Typically, these files are available in <NCHOME>\omnibus\etc directory.
4. Edit the NCOMS.props file to add the following settings:

```
NHttpd.EnableHTTP: TRUE
NHttpd.ListeningPort: 8080
NRestOS.Enable: TRUE
```

5. Restart the ObjectServer.

**What to do next**

Verify the ObjectServer is providing the REST API with a `curl` command to get all active alerts. Follow these steps:

* curl --basic --user USERNAME:PASSWORD http://NODENAME:PORT/objectserver/restapi/alerts/status

Specify appropriate values for NODENAME, PORT, USERNAME, and PASSWORD

You can see an output in JSON format as follows:

```
"rowset": {
  "osname": "NCOMS",
  "dbname": "alerts",
  "tblname": "status",
  "affectedRows": 125,
  "coldesc": [{
    "name": "Identifier",
    "type": "string",
    "size": 255
  },
  ...
  ...
},
 ...
...
```

Related information:

- Starting the Conductor

**Configuring the OMIbus REST APIs in Network Performance Insight**

Modify the Network Performance Insight configuration file in `<NPI_Home>/conf/npi.conf`.

**About this task**

You can use the template file npi-noi.template that is available in `<NPI_Home>/conf` folder.
Procedure

1. Open the npi.conf file from <NPI_Home>/conf folder.

2. Add the following settings for OMNibus REST APIs:

   ```plaintext
   event.netcool.omnibus.rest-api.host=<myserver.ibm.com>
   event.netcool.omnibus.rest-api.port=8080
   event.netcool.omnibus.rest-api.path=/objectserver/restapi/alerts/status
   event.netcool.omnibus.rest-api.username=root
   event.netcool.omnibus.rest-api.password=eTh66o0sJZrf1Ek1h/Xm+g==
   event.netcool.omnibus.rest-api.realm=omnibus
   ```

Where:

Table 3. Configurations for OMNibus REST APIs

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>event.netcool.omnibus.rest-api.host</td>
<td>Actual nodename where OMNibus ObjectServer is running (not NCOMS or omnihost).</td>
<td>&lt;myserver.ibm.com&gt;</td>
</tr>
<tr>
<td>event.netcool.omnibus.rest-api.port</td>
<td>OMNibus ObjectServer HTTP port number, as specified in NHttpd.ListeningPort.</td>
<td>8080</td>
</tr>
<tr>
<td>event.netcool.omnibus.rest-api.path</td>
<td>The URI that must be specified to get all the active alerts.</td>
<td>/objectserver/restapi/alerts/status</td>
</tr>
<tr>
<td>event.netcool.omnibus.rest-api.username</td>
<td>A privileged OMNibus user name (not the same as Jazz for Service Management user). For example, root.</td>
<td>root</td>
</tr>
<tr>
<td>event.netcool.omnibus.rest-api.password</td>
<td>OMNibus user's encrypted password</td>
<td>fe/KSX5GZ+/gJcKwGbIHlQ==</td>
</tr>
<tr>
<td>event.netcool.omnibus.rest-api.realm</td>
<td>A realm is a group of users from one or more user registries that form a coherent group within OMNibus.</td>
<td>omnibus</td>
</tr>
</tbody>
</table>

Note: To encrypt the password, follow the steps in Encrypting Object Server password in Integrating with Tivoli/Netcool OMNibus.

As a good security practice, passwords must not be left blank. If your OMNibus ObjectServer does not have a password, set a password in an encrypted form and add the encrypted password to the configuration settings.

Example entries:

```plaintext
   event.netcool.omnibus.rest-api.host=<myserver.ibm.com>
   event.netcool.omnibus.rest-api.port=8080
   event.netcool.omnibus.rest-api.path=/objectserver/restapi/alerts/status
   event.netcool.omnibus.rest-api.username=root
   event.netcool.omnibus.rest-api.password=fe/KSX5GZ+/gJcKwGbIHlQ==
   event.netcool.omnibus.rest-api.realm=omnibus
```
Encrypting Object Server password

Decide which level of security that you require and perform the configuration tasks that are required for that security level. Some configuration tasks are required, while others are required only for specific levels of protection. It is a good security practice to encrypt passwords that are used.

About this task

Encrypt the passwords that are created for Jazz for Service Management and also for Tivoli Netcool/OMNibus components.

Procedure

1. To create an encrypted password, use the bin/encrypt utility that is available in Network Performance Insight.
   
   use the following command:
   $ bin/encrypt <test_pass>

   You can see the encrypted password as:
   fe/KSX5GZ+/gJcKwGbIHlQ==

2. Copy the encrypted password in the configuration settings in npi.conf file as follows:

   security.dash.port=16311
   event.netcool.omnibus.rest-api.host="<myserver.ibm.com>"
   event.netcool.omnibus.rest-api.port="8080"
   event.netcool.omnibus.rest-api.path="/objectserver/restapi/alerts/status"
   event.netcool.omnibus.rest-api.username="root"
   event.netcool.omnibus.rest-api.password="fe/KSX5GZ+/gJcKwGbIHlQ=="
   event.netcool.omnibus.rest-api.realm="omnibus"


   Note: Check the Event Service log message in npi.log file for successful encryption. All the configuration settings must have values.

Changing ObjectServer user password

Instructions to set or change ObjectServer user password.

About this task

You must run the nco_config utility to start Netcool/OMNibus Administrator by using the following command:
$NCHOME/omnibus/bin/nco_config

Procedure

1. From the Netcool/OMNibus Administrator window, select File > Import.
2. Click Next.
3. Import the ObjectServer (NCOMS) and click Finish.
4. In the Netcool/OMNibus Administrator window, right-click the ObjectServer (NCOMS) and click Connect as.
5. Enter the user name as root and password.
   By default, the password is left blank.
6. Click OK.
7. From the Netcool/OMNibus Administrator window, select User.
8. Click Users.
   The Users pane opens.
9. To edit the root user, select root user to edit and then click Edit User in the toolbar.
   The User Details window opens.
10. Click Settings > Change.
11. Enter a new password and click Save.

What to do next

If the password of the user that authenticates the connection between the ObjectServer and the Web GUI is changed, update the password on the Web GUI server. For more information about setting the password for Web GUI, see Changing the password for the connection to the ObjectServer.
Chapter 5. Monitoring events from Web GUI on Dashboard Application Services Hub

You can monitor and manage Tivoli Netcool/OMNIbus by using the Web GUI that is started on the reporting interface of Jazz for Service Management.

About this task

You can access the events from:

- **Managing events in the Event Viewer**
  Use the JavaScript Event Viewer to monitor and manage events. You can access Event Viewers in any page in Dashboard Application Services Hub that hosts an Event Viewer widget.

- **Monitoring events in Active Event Lists**
  The Active Event List (AEL) is an interactive Java applet for displaying alert data from the ObjectServer. Communication between the ObjectServer and the AEL is bidirectional. The AEL presents alert information from the alerts.status table in the ObjectServer to operators. From the AEL, operators can perform actions against alerts that results in changes to the alert data in the alerts.status table.

Procedure

1. Log in to Jazz for Service Management server. See "Logging in to the Dashboard Application Services Hub portal" on page 24
2. In the navigation bar, click **Incident ( ) > Events > Active Event List (AEL).**
3. Right-click any event from the Active Event List (AEL) page and select **Flow Dashboard.**
   The Traffic Details report associated with the selected event is displayed in another window.
4. Optional: In the navigation bar, click **Incident ( ) > Events > Event Viewer.**
5. Right-click any event from the **Event Viewer** page and select **Flow Dashboard.**
   The Traffic Details report associated with the selected event is displayed in another window.

Related tasks:

- "Configuring launch-in-context menu" on page 29
  In event lists, users access default and custom tools through menus. You can add tool entries to the menus, create new submenus, and modify or delete menu items.

Related information:

- Monitoring events in the Web GUI
Event severity levels

A severity level is associated with each generated alert to help you to prioritize and manage alerts in the Event list. Severity levels are color-coded for easy identification.

There are six default severity levels, as shown in the following table.

<table>
<thead>
<tr>
<th>Level</th>
<th>Threshold type</th>
<th>Color</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Clear</td>
<td>Green</td>
</tr>
<tr>
<td>1</td>
<td>Intermediate</td>
<td>Gray</td>
</tr>
<tr>
<td>2</td>
<td>Warning</td>
<td>Blue</td>
</tr>
<tr>
<td>3</td>
<td>Minor</td>
<td>Yellow</td>
</tr>
<tr>
<td>4</td>
<td>Major</td>
<td>Orange</td>
</tr>
<tr>
<td>5</td>
<td>Critical</td>
<td>Red</td>
</tr>
</tbody>
</table>

You can customize the event data and how the event data is displayed.

Related information:

[Customizing event displays in the Web GUI](#)
Chapter 6. Troubleshooting integration with Tivoli Netcool/OMNIbus

Use this troubleshooting information to troubleshoot problems with the integration.

Cannot view the Event List from AEL if the list of events is large

**Symptoms**
Sometimes the Event list is not visible on AEL and you might encounter the following error:

W0025  HEMCDW0025

**Causes**
Typically, you encounter this issue if the Event list is large.

**Resolving the problem**
To workaround this issue, see the Technical Note: WebGUI AEL displays W0025 error when viewing a very large list of events.

Do not use Google Chrome to view Tivoli Netcool/OMNIbus Web GUI events on Dashboard Application Services Hub

Do not use Google Chrome to view the AEL or Event Viewer on Dashboard Application Services Hub.

**Note:** Tivoli Netcool/OMNIbus Web GUI v8.1.x versions on Dashboard Application Services Hub do not fully support the Chrome browser. For more information, see:


Timezone settings on Event Viewer and Network Performance Insight dashboards on Dashboard Application Services Hub are not the same

The time that is displayed in the Last Occurrence column in Event Viewer is different from Network Performance Insight dashboards. AEL and Network Performance Insight dashboards use the same timezone setting as the browser. Event Viewer always displays the time based on the timezone settings on the OMNIbus ObjectServer. Currently, this setting on Event Viewer cannot be changed.
Appendix A. Adding the LDAP user registry as a federated repository

This feature enables support for using an LDAP server as a user registry. This feature is an alternative to the use of Jazz for Service Management built-in file-based user repository. After you set up the LDAP server, you must add it as a federated repository. You can configure the Web GUI to authenticate users and groups against an LDAP directory.

Before you begin

Before you configure the user registry or repository, decide which user registry or repository to use.

About this task

Configure Lightweight Directory Access Protocol (LDAP) settings in a federated repository configuration. This step is not required if you have created your user repository on WebSphere Application Server as described in “Creating users and groups in a repository” on page 9.

Procedure

1. Log in to Jazz for Service Management server.
2. Expand Console Settings > WebSphere Administrative Console.
3. Click Launch WebSphere Administrative Console.
5. Under User account repository, select Federated Repository and click the Configure button.
6. In the Global security > Federated repositories page, click Add Repositories (LDAP, custom,etc...).
7. In the Global security > Federated repositories > Repository reference page, select LDAP repository from the New Repository list.
8. In the Global security > Federated repositories > Repository reference > New page, specify the name of the LDAP repository and other details according to your requirements. For example, enter the following details:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Repository identifier</td>
<td>Specifies a unique identifier for the LDAP repository. This identifier uniquely identifies the repository within the cell, for example: LDAP1.</td>
</tr>
<tr>
<td>Directory type</td>
<td>Specifies the type of LDAP server to which you connect. Select Custom.</td>
</tr>
<tr>
<td>Primary host name</td>
<td>Specifies the host name of the primary LDAP server. This host name is either an IP address or a domain name service (DNS) name.</td>
</tr>
<tr>
<td>Port</td>
<td>Specifies the LDAP server port. For example, 10389</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Bind distinguished name</strong></td>
<td>Specifies the distinguished name (DN) for the application server to use when binding to the LDAP repository. For example, uid=admin,ou=system</td>
</tr>
<tr>
<td><strong>Bind password</strong></td>
<td>Specifies the password for the application server to use when binding to the LDAP repository.</td>
</tr>
</tbody>
</table>

9. Click OK and save the configuration.
10. In the Global security > Federated repositories > Repository reference page, specify the value for **Unique distinguished name of the base (or parent) entry in federated repositories**.
    For example, dc=customer,dc=com
11. Click OK.
12. In the Global security > Federated repositories page, select the link to the LDAP repository that you created.
13. In the Global security > Federated repositories > <LDAP Repository Name> page, under Additional Properties, select Federated repositories entity types to LDAP object classes mapping link.
    In the Global security > Federated repositories > <LDAP Repository Name> > Federated repositories entity types to LDAP object classes mapping page, ensure that each entity type listed is mapped to the correct object classes. Modify the values according to your requirements.
14. Click New to create an entity and enter the following details:
    • Entity type = Group
    • Object Classes = groupOfUniqueNames
    • Search bases = ou=groups,dc=customer,dc=com

    **Note:** Use the values that are specific to your server setup.
15. Click New to create another entity and enter the following details:
    • Entity type = PersonAccount
    • Object Classes = inetOrgPerson;organizationalPerson;person
    • Search bases = ou=people,dc=customer,dc=com

    **Note:** Use the values that are specific to your server setup.
16. Click OK.
17. In the Global security > Federated repositories page, select the link to the LDAP repository that you created. Under Additional Properties, select **Group attribute definition**.
18. In the Global security > Federated repositories > <LDAP Repository Name> > Group attribute definition page under Additional Properties, select **Member Attributes**.
19. Define a new attribute that is called unqiuemember with direct scope and object class as groupOfUniqueNames.
20. Click OK to save the configuration.

**Related information:**

[Selecting a registry or repository]
Configuring Lightweight Directory Access Protocol user registries
Appendix B. npid command reference

Usage for the npid command. Run the npid command to start, stop, and restart Network Performance Insight.

**Location**

\(<NPI\_Home>/bin\)

\(NPI\_Home\) is the location where Network Performance Insight is installed. For example, /opt/IBM/NPI.

**Syntax**

npid \{start | stop | restart | kill | status | version | help\}

**Parameters**

**start**

Starts Network Performance Insight application.

**stop**

Stops Network Performance Insight application.

**restart**

Stops and starts Network Performance Insight application.

**kill**

Kills the Network Performance Insight application process by using the command kill -9.

**status**

Checks if Network Performance Insight pid is running when you use the command ps -eaf.

**version**

Shows the version of Network Performance Insight that is installed.

**help**

Displays the usage for npid command.
Appendix C. Common directory locations for Jazz for Service Management

Jazz™ for Service Management topics use path name variables for paths to common directories, for example, home directories.

**Jazz for Service Management home directory**

The JazzSM_HOME variable describes the location where Jazz for Service Management is installed. This location can be specified during installation. If not specified, the following default locations are used:

- Root user installations: `/opt/IBM/JazzSM`
- Non-root user installations: `<user_home_directory>IBM/JazzSM`

**Jazz for Service Management profile directory**

The JazzSM_WAS_Profile variable describes the location of the application server profile that is used for Jazz for Service Management. This location is in the `/profile` subdirectory of the Jazz for Service Management home directory.

- Root user installations: `/opt/IBM/JazzSM/profile`
- Non-root user installations: `<user_home_directory>IBM/JazzSM/profile`

**Jazz for Service Management profile name**

The JazzSM_Profile_Name variable refers to the name assigned to the WebSphere® Application Server profile for Jazz for Service Management. The default name is JazzSMProfile.

**Installation images home directory**

The Install_Imgs_Home variable describes the common root directory that contains the extracted contents of the installation images depending on the installation scenario.

**Full installation**

IBM DB2®, IBM WebSphere Application Server.

**Attention:** You must extract the contents of the installation media for this software to the same common root directory, otherwise the full installation displays error messages for missing software.

**Custom installation**

IBM WebSphere Application Server, if you do not want to use an existing installation.

**Note:** It is not necessary to extract the contents of the installation media for this software to the same common root directory, but it is preferable to maintain all extracted installation media in a central location.
Jazz for Service Management installation images home directory

The JazzSM_Image_Home variable describes the common root directory in which the Jazz for Service Management is extracted. It contains the launchpad, IBM Installation Manager, IBM Prerequisite Scanner, the Installation Manager repository with the software packages for the integration services except Tivoli Common Reporting.

Tip: Ensure that the path to the JazzSM_Image_Home directory does not contain any spaces or special characters, otherwise the launchpad does not start.

IBM DB2 home

The DB2_HOME variable describes the location where IBM DB2 is installed. This location is specified during installation. If not specified, the following default locations are used:

- Root user installations: /opt/ibm/db2
- Non-root user installations: $HOME/sqllib

$HOME represents the non-root user's home directory.

WebSphere Application Server home directory

The WAS_HOME variable describes the location where WebSphere Application Server is installed. This location is specified during installation. If not specified, the following default locations are used:

- Root user installations: /opt/IBM/WebSphere/AppServer
- Non-root user installations: <user_home_directory>IBM/WebSphere/AppServer

Administration Services home directory

The ADMIN_HOME variable describes the location where Administration Services is installed. This location can be specified during installation. If not specified, the following default locations are used:

- Root user installations: /opt/IBM/JazzSM/admin
- Non-root user installations: /home/nonrootuser_name/IBM/JazzSM/admin

Administration Services UI home directory

The ADMINUI_HOME variable describes the location where Administration Services UI is installed. This location can be specified during installation. If not specified, the following default locations are used:

- Root user installations: /opt/IBM/JazzSM/adminui
- Non-root user installations: /home/nonrootuser_name/IBM/JazzSM/adminui

Registry Services home directory

The REGISTRY_HOME variable describes the location where Registry Services is installed. This location can be specified during installation. If not specified, the following default locations are used:

- Root user installations: /opt/IBM/JazzSM/registry
- Non-root user installations: /home/nonrootuser_name/IBM/JazzSM/registry
Security Services home directory

The SECURITY_HOME variable describes the location where Security Services is installed. This location can be specified during installation. If not specified, the following default locations are used:
- Root user installations: /opt/IBM/JazzSM/security
- Non-root user installations: /home/nonrootuser_name/IBM/JazzSM/security

Dashboard Application Services Hub home directory

The DASH_HOME variable describes the location where Dashboard Application Services Hub is installed. This location can be specified during installation. If not specified, the following default locations are used:
- Root user installations: /opt/IBM/JazzSM/ui
- Non-root user installations: <user_home_directory>IBM/JazzSM/ui

Dashboard Application Services Hub profile directory

The DASH_PROFILE variable describes the location of the application server profile that is used for Dashboard Application Services Hub. This location is in the/profiles subdirectory of the Jazz for Service Management home directory.
- Root user installations: /opt/IBM/JazzSM/profile
- Non-root user installations: <user_home_directory>IBM/JazzSM/profile

Full installation log directory

The Simple_install_log_dir directory into which general and offering specific logs are created during full installation:
- On UNIX systems: $HOME/jazzsm_launchpad/logs/

IBM Prerequisite Scanner installation directory

The ips_root directory that contains the contents of the extracted Prerequisite Scanner platform package. If not specified, the default locations are used:
- On UNIX systems: Install_Imgs_Home/PrereqScanner/UNIX_Linux

Related information:

[Common directory locations]
Notices

This information was developed for products and services that are offered in the USA. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

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

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

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

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

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

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

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

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.
Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

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

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

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

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

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

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

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

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

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

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

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

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

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

**COPYRIGHT LICENSE:**

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

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

© (your company name) (year).

Portions of this code are derived from IBM Corp. Sample Programs.

© Copyright IBM Corp. _enter the year or years_. All rights reserved.

---

### Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

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

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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

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

ITIL is a registered trademark, and a registered community trademark of The Minister for the Cabinet Office, and is registered in the U.S. Patent and Trademark Office.
UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

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

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

Terms and conditions for product documentation

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

Applicability

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

Personal use

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

Commercial use

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

Rights

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

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

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.
IBM makes no guarantee about the content of these publications. The publications are provided "as-is" and without warranty of any kind, either expressed or implied, including but not limited to implied warranties of merchantability, non-infringement, and fitness for a particular purpose.