System Automation for z/OS
Version 4 .Release 1

Service Management Unite Automation Installation and Configuration Guide

SC27-8747-00

Note!

Before using this information and the product it supports, read the information in Appendix A, "Notices," on page 263.

Edition Notes

This edition applies to IBM® System Automation for z/OS (Program Number 5698-SA4) Version 4 Release 1, an IBM licensed program, and to all subsequent releases and modifications until otherwise indicated in new editions or technical newsletters.

Contents

Figures

Tables

Accessibility

Accessibility features help users with physical disabilities, such as restricted mobility or limited vision, to use software products successfully. System Automation for z/OS supports several user interfaces. Product functionality and accessibility features vary according to the interface.

The major accessibility features in this product enable users in the following ways:

- Use assistive technologies such as screen reader software and digital speech synthesizer, to hear what is displayed on screen. Consult the product documentation of the assistive technology for details on using those technologies with this product and screen magnifier software
- Operate specific or equivalent features using only the keyboard
- Magnify what is displayed on screen.

The product documentation includes the following features to aid accessibility:

- All documentation is available to both HTML and convertible PDF formats to give the maximum opportunity for users to apply screen-reader software
- All images in the documentation are provided with alternative text so that users with vision impairments can understand the contents of the images.

Using assistive technologies

Assistive technology products, such as screen readers, function with the user interfaces found in z/OS®. Consult the assistive technology documentation for specific information when using such products to access z/OS interfaces.

Keyboard navigation of the user interface

Users can access z/OS user interfaces using TSO/E or ISPF. Refer to *z/OS TSO/E Primer*, *z/OS TSO/E User's Guide*, and *z/OS ISPF User's Guide Vol 1* for information about accessing TSO/E and ISPF interfaces. These guides describe how to use TSO/E and ISPF, including the use of keyboard shortcuts or function keys (PF keys). Each guide includes the default settings for the PF keys and explains how to modify their functions.

How to send your comments to IBM

We appreciate your input on this publication. Feel free to send us any comments you might have.

If you have feedback to the manuals

If you have comments on the manuals, like clarity, accuracy, and completeness of the information, use the Feedback channel on IBM Knowledge Center to send your comments.

1. Click **Feedback** > **Email IBM Knowledge Center support** at the bottom of IBM Knowledge Center.
2. Log in to the invoked mailbox; or if the Launch Application window is displayed, choose one mailbox and log in. A new email is displayed after login.
3. In the email body, write down your feedback. Please include the specific book and topic name that you're commenting on.
4. Send the email to the default recipient.
5. SA z/OS team will respond to you by email as soon as possible.

If you have a technical problem

Use one of the following feedback methods:

- Contact your IBM service representative.
- Call IBM technical support.
- Visit the IBM zSeries support web page at www.ibm.com/systems/z/support/.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

IBM or any other organizations will only use the personal information that you supply to contact you about the issues that you submit.

Related Publications

The System Automation for z/OS Library

Table 1 on page xv shows the information units in the System Automation for z/OS library. These manuals can be downloaded from IBM Documentation.

Table 1. System Automation for z/OS library

Title	Form Number	Description
Get Started Guide	SC27-9532	This book is intended for SA z/OS beginners. It contains the information about early planning, configuring the product, making it secure, customizing your automation environment, and the basic operational tasks that you perform on a daily basis.
Planning and Installation	SC34-2716	Describes SA z/OS new capabilities and how to plan, install, configure, and migrate SA z/OS.
Customizing and Programming	SC34-2715	Describes how to adapt the standard installation, add new applications to automation, write your own automation procedures, and add new messages for automated applications.
Defining Automation Policy	SC34-2717	Describes how to define and maintain the automation policy.
User's Guide	SC34-2718	Describes SA z/OS functions and how to use SA z/OS to monitor and control systems.
Messages and Codes	SC34-2719	Describes the problem determination information of SA z/OS, including messages, return codes, reason codes, and status codes.
Operator's Commands	SC34-2720	Describes the operator commands available with SA z/OS, including their purpose, format, and specifics of how to use them.
Programmer's Reference	SC34-2748	Describes the programming interfaces of SA z/OS and the definitions for the status display facility (SDF).
End-to-End Automation	SC34-2750	Describes the end-to-end automation adapter for z/OS and how it enables end-to-end automation and how it connects to Service Management Unite Automation.
Service Management Unite Automation Installation and Configuration Guide	SC27-8747	Describes how to plan, install, set up, configure, and troubleshoot Service Management Unite Automation.

Table 1. System Automation for z/OS library (continued)

Title	**Form Number**	**Description**
Product Automation Programmer's Reference and Operator's Guide	SC34-2714	Describes how to customize and operate product automation components (CICS, Db2, and IMS automation) with SA z/OS to provide a simple and consistent way to monitor and control all of the CICS, Db2, and IMS regions, both local and remote, within your organization.
TWS Automation Programmer's and Operator's Reference Guide	SC34-2749	Describes how to customize and operate TWS Automation.

Related Product Information

For information that supports System Automation for z/OS, visit the z/OS library in IBM Knowledge Center (www.ibm.com/support/knowledgecenter/SSLTBW/welcome).

Chapter 1. New in this release

This information contains an overview of the major changes to Service Management Unite Automation for Version 1.1.6, V1.1.5, and V1.1.4.

SMU Automation V1.1.6 provides the following key new features:

- Enhancements to the Docker scripts:

  The SMU Automation Docker image and the **eezdocker.sh** script are enhanced to deploy, configure, and upgrade SMU Automation in a Docker environment more easily. See Installing Service Management Unite Automation with Docker.
- Enhancements to the Web Configuration Tool:

  With the enhanced web configuration tool, you can configure properties to enable and establish connection with Zowe™ in the SMU dashboard.
- Enhancements to SMU exploitation and integration with Zowe:
  - Zowe V1.0.1, V1.1.0, V1.2.0, V1.3.0, and V1.4.0 are supported.
  - The SMU plug-in is packaged as a **.tar** file for easier decompression.
  - In the JES Explorer dashboard, a dialogue is provided to assist you in easily accepting the certificate to avoid security issues when accessing Zowe micro-services.

SMU Automation V1.1.5 provides the following key new features:

- SMU Automation V1.1.5 is integrated with Zowe:
  - A Zowe application plug-in is provided for SMU Automation to allow you to use SMU directly on Zowe Desktop and leverage free and commercial APIs in Zowe Application Framework.
  - A new **JES Explorer** dashboard is provided to allow you to view job content and job output to isolate environmental issues. The **JES Explorer** dashboard can be started from SA APL resources.

  See Chapter 11, “SMU exploitation and integration with Zowe™,” on page 253 for more information.
- A web-based configuration tool is added as a modern alternative of the configuration dialogue **cfgsmu**. See “[Use Web Config Tool] Configuring the SMU server” on page 59 and “[Use Web Config Tool] Configuring the Universal Automation Adapter” on page 71.
- The installation is simplified and consolidated to provide minimal time-to-value:
  - The tool to install SMU Automation is replaced by Installation Manager, which requires fewer user inputs and provides a consolidated installation experience. See “Installing SMU Automation” on page 27.
  - The SMU Docker image and the **eezdocker.sh** script are enhanced to deploy and configure SMU in a Docker environment more easily. See “Installing and uninstalling SMU Automation with Docker” on page 18.
- Enhancements to SA Server Groups (with APAR OA54684 installed in System Automation for z/OS V4.1):

  You can now modify the **satisfactory target** and **availability target** of a server group in an easy-to-use dialogue from an SA dashboard.

SMU Automation V1.1.4 provides the following key new features:

- The installation of SMU is simplified with a prebuilt Docker image. See Installing and uninstalling SMU Automation with Docker.
- "Ask Watson" dashboard is added as an open beta feature to provide a cognitive documentation search.
- To ensure a reliable system with high performance and less downtime, you can set up SMU with high availability. See Chapter 5, “Setting up Service Management Unite with High Availability,” on page 35.

- With APAR OA55386 installed in System Automation for z/OS V4.1, SMU Automation can automate applications that run on non-z/OS systems using Universal Automation Adapters. See Universal Automation Adapter concept in Service Management Unite Automation architecture.
- SA operations experience is enhanced:
  - For a stop, start, or suspend request, you can choose the new **REMOVE=SYSGONE** option to automatically remove the request when the system where the selected resource runs, leaves the sysplex.
  - The resource status of a system is now represented as the worst compound status of all top-level resources running on that system. This can be combined with a Resource name filter or Resource class filter as data set parameter. In this case, the worst resource state is derived by the worst compound state of all resources on the system that match the specified filter criteria.
  - A **Hide operational tasks** option is added into the automation domain topology and automation node list data sets. Choose this option if the context menu of nodes that are contained in these data sets should not include any operational tasks, such as excluding a node.

Chapter 2. Overview of Service Management Unite Automation

IBM Service Management Unite Automation is the new customizable dashboard interface that is available with IBM System Automation for z/OS V4.1.0. It provides a single point of control for multiple SAplexes to operate in your environment.

Operators can quickly and confidently analyze, isolate, and diagnose problems by providing all relevant data including important logs in a single place. SMU Automation also enables operators to interact directly with the system by issuing commands and viewing results without going to a different console. Additionally, it allows the customization of own dashboards, providing exactly the information needed by the operations in your specific environment.

SMU Automation can be installed on Linux on z Systems or Linux on System x and uses the E2E adapter for secure communication with SA z/OS. You can download SMU Automation from IBM's download portal: http://ibm.biz/smu-auto-download.

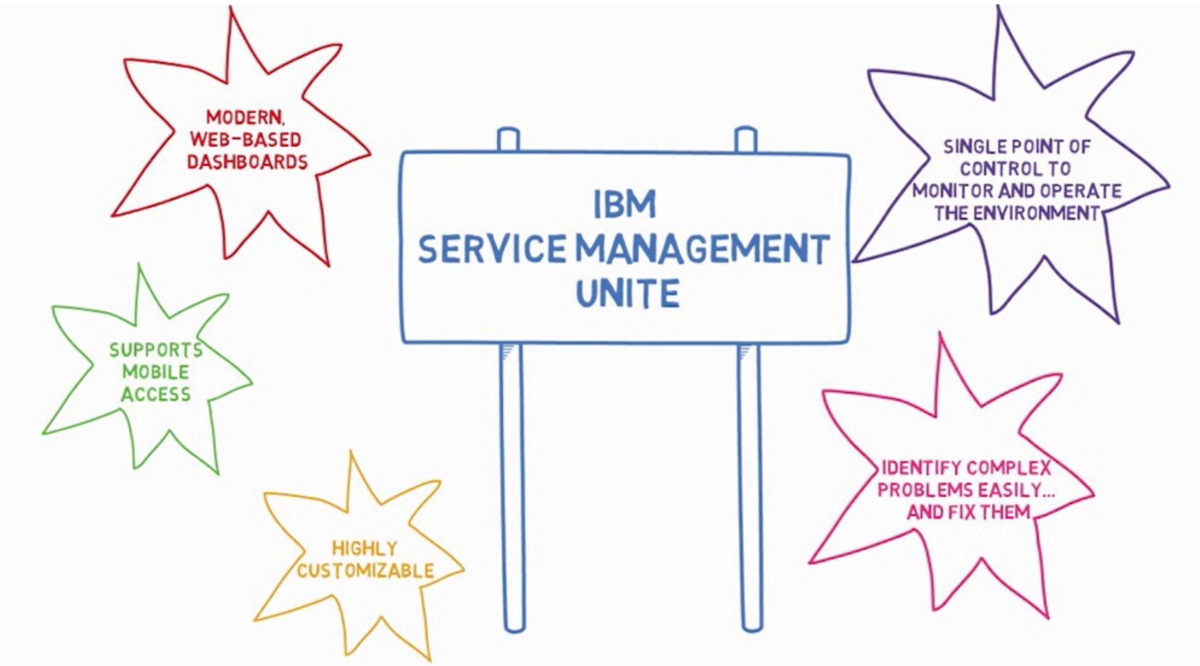

MODERN, WEB-BASED DASHBOARDS
IBM SERVICE MANAGEMENT UNITE
SINGLE POINT OF CONTROL TO MONITOR AND OPERATE THE ENVIRONMENT
SUPPORTS MOBILE ACCESS
HIGHLY CUSTOMIZABLE
IDENTIFY COMPLEX PROBLEMS EASILY... AND FIX THEM

Figure 1. Highlights of Service Management Unite

For related information, refer to the following resources:

Table 2. Related documentation for Service Management Unite Automation

Related documentation	**Location**
Service Management Unite Automation - Installation and Configuration Guide	Download link
Service Management Unite Automation's embedded online help	Within Service Management Unite Automation, click the question mark icon (?) on a dashboard's console toolbar to get detailed information about the usage and how to customize dashboards

Service Management Unite Automation architecture

The following diagram depicts a simple topology of the various principal components that form the Service Management Unite Automation infrastructure, and how they interact with each other.

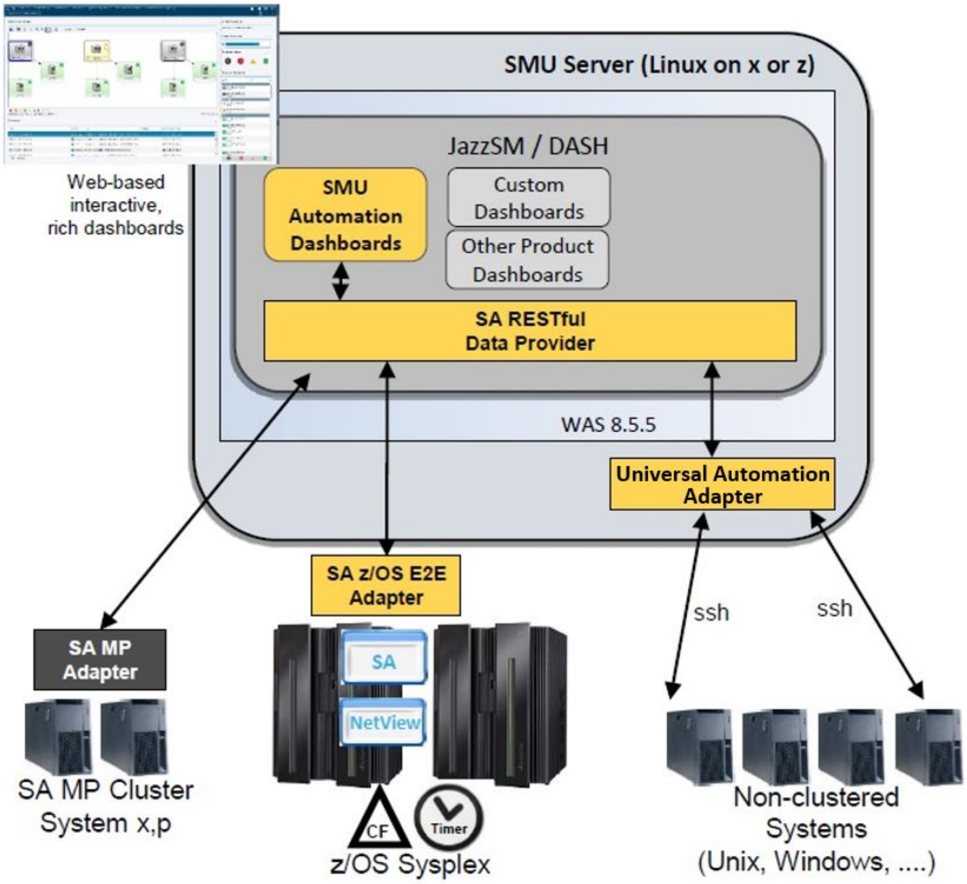


Figure 2. IBM Service Management Unite Automation architecture

The Service Management Unite Server

Service Management Unite Automation can be installed on Linux on z Systems or Linux on System x.

Service infrastructure

Service Management Unite Automation uses a service infrastructure that incorporates key products and services to run the dashboards and provide flexible integration and customization capabilities. The service infrastructure is provided with Service Management Unite Automation and needs to be installed before the Service Management Unite Automation dashboards. It consists of the following components:

IBM Dashboard Application Services Hub (DASH) / Jazz for Service Management (JazzSM)

IBM Dashboard Application Services Hub (DASH) provides visualization and dashboard services based on Jazz for Service Management (JazzSM). The DASH integration platform supports data processing and content rendering from multiple sources. The data is integrated and presented in interactive dashboards. DASH has a single console for administering IBM products and related applications.

IBM WebSphere Application Server

IBM WebSphere Application Server provides the application server runtime environment for DASH and the Service Management Unite Automation dashboards.

Service Management Unite Automation

Service Management Unite Automation provides the dashboards to monitor and operate resources that are automated by IBM System Automation for z/OS, issue z/OS and NetView commands, and access system logs. It also provides the Universal Automation Adapter to automate non-z/OS systems from IBM System Automation for z/OS.

Connectivity to backend systems

Connect Service Management Unite Automation with z/OS Systems

Use the following main components to interact with z/OS systems:

IBM System Automation for z/OS

IBM System Automation for z/OS is a policy-based, self-healing, high availability solution. It maximizes the efficiency and the availability of critical systems and applications. It also reduces administrative and operational tasks.

System Automation for z/OS end-to-end (E2E) adapter

The SA for z/OS E2E adapter connects an SA for z/OS domain to Service Management Unite Automation. It enables Service Management Unite Automation to read data like the status of automated resources and run actions like sending requests. It also provides the capability to issue NetView and z/OS commands and access system logs. In addition, the E2E adapter is used as the connection target by System Automation to provide cross-sysplex end-to-end automation.

For more information about the E2E adapter, refer to the End-to-End Automation manual.

Connect Service Management Unite Automation with non-z/OS Systems

Universal Automation Adapter (UAA)

The Universal Automation Adapter enables Service Management Unite Automation to monitor, operate, and automate resources that run on non-z/OS systems. It can be used as the connection target by IBM System Automation for z/OS to provide end-to-end automation.

The Universal Automation Adapter is installed with IBM Service Management Unite Automation. No additional software needs to be installed on the system that hosts the monitored application. The UAA connects to remote systems using SSH. In a policy that you can edit from your Service Management Unite dashboard, you define the resources on the remote systems and which commands to use to monitor, start, and stop the resources. Remote systems and resources that are managed by the UAA are automatically displayed in the Service Management Unite Automation dashboards.

For more information about how to configure UAA, see "[Optional] Configuring access to the Universal Automation Adapter" on page 69.

Authentication and Authorization concepts

Go through the basic concepts to understand users, groups, and user roles in Service Management Unite.

Authentication

In the Service Management Unite architecture, you must configure user authentication for the following main components:

WebSphere Application Server

When you log in to Dashboard Application Services Hub (DASH) to access the Service Management Unite dashboards, you need a user ID to authenticate against the user repository that is configured for WebSphere Application Server. The user repository can either be the default file-based user repository or a Lightweight Directory Access Protocol (LDAP) repository.

Use the WebSphere administrative console to configure the security setup and manage users and user groups.

z/OS Systems to issue NetView or System Automation commands

All requests are routed through the E2E adapter that run in the SA for z/OS automation domain. The user is authenticated with the configured System Authorization Facility (SAF) product such as the z/OS Resource Access Control Facility (RACF). Depending on the security setup of your System Automation environment, the detailed situation varies. For more information about the required security definitions for the user ID, see "Requirements for user IDs that access z/OS systems from Service Management Unite" on page 11.

Use the configuration tool **cfgsmu** to define which user IDs are used by the Service Management Unite automation framework.

Non-z/OS Systems that are accessed by the Universal Automation Adapters

Non-z/OS Systems use the Universal Automation Adapters to connect to Service Management Unite through Secure Shell (SSH). You need a user ID that is configured on the remote system to authenticate through SSH.

Use the configuration tool **cfgsmu** to define which user IDs are used by the Universal Automation Adapter to access remote systems.

For an overview of the usage of the different user IDs, see User credentials.

Authorization

Authorization defines the content that you can view and the actions that you can perform.

Service Management Unite Automation uses the following user role names:

- EEZMonitor
- EEZOperator
- EEZConfigurator
- EEZAdministrator

For more details about the permissions that are granted by these user roles, see User roles.

Three layers are used to control authorization:

DASH Roles

The DASH roles define the views, menus, and dashboards that you can see when you work with DASH. You can assign DASH roles to individual users or user groups.

When you install Service Management Unite Automation, the default user groups are created in the user repository that is configured for WebSphere Application Server. DASH roles with the role names of EEZMonitor, EEZOperator, EEZConfigurator, and EEZAdministrator are assigned to these default user groups. For more information about the default user roles, role mapping, and how to assign roles to users or user groups, see "Authorizing users and groups within the Dashboard Application Services Hub" on page 105.

WebSphere Application Server: EJB-Level Roles

The automation framework that runs as Enterprise Java Beans (EJB) in WebSphere Application Server provides the interface to automation domains. At EJB application level, the functions that the EJB-Level role can access are defined. For example, if you have only the EEZMonitor role, you are not allowed to issue a System Automation request.

Similar to the role mapping of the DASH roles, the SMU user roles are assigned to the default groups during the installation. You can follow the steps to view and edit the EJB-level role mapping using the WebSphere administrative console:

1. Log in to the WebSphere administrative console.
2. In the navigation bar, click **Applications** > **Application types** > **WebSphere enterprise applications**.
3. In the **Enterprise Applications** window, click **EEZEAR**.

4. Under section **Detail Properties**, click **Security role to user/group mapping**. The list of role mapping is displayed.

z/OS Backend Authorization using the configured System Authorization Facility (SAF)

When you issue a command or a query against a z/OS domain, the user ID that you use to log in to the corresponding automation domain is checked against the configured SAF product such as RACF. This check process ensures that the z/OS user ID is authorized to issue the corresponding NetView, MVS, or System Automation commands and to work with the resources. For more details about the security requirements for user IDs on z/OS, see "Requirements for user IDs that access z/OS systems from Service Management Unite" on page 11.

During the installation, the DASH roles and the EJB-Level roles are assigned to the default user groups that can be used for Service Management Unite. Use the WebSphere administrative console to add the user IDs to the corresponding user groups. All the users in a user group inherit the roles that are defined at the group level.

Overview of System Automation dashboards

IBM Service Management Unite (SMU) provides a single point of control for multiple SAplexes to operate in your environment.

With the predefined System Automation dashboards, you can view the overall health status and easily manage your automation environment.

System Automation dashboards

Table 3. System Automation dashboards

Dashboard name	Description	Accessing this dashboard
Domain and Automation Health	You can see statistics about the health of top-level resources of a selected domain or node. You can also drill down to operational views of displayed domains, nodes, and resources.	In the navigation bar, click **System Status and Health** > **Domain and Automation Health**.
Explore Automation Domains	You can navigate through a large number of automation domains, systems, and their resources and run operational tasks.	In the navigation bar, click **Administration** > **Explore Automation Domains**.
Explore Automation Nodes	You can find a specific node and understand which resources are hosted by it if you want to run maintenance actions on that node.	In the navigation bar, click **Administration** > **Explore Automation Nodes**.
Domain Page	You can view all resources that belong to the active automation policy of an automation domain. You can use this dashboard to drill down to a specific resource and run operational tasks or view the resource relationships.	• In the navigation bar, click **Administration** > **View Default Automation Domain**. • Right-click a System Automation for z/OS domain or node, and click **View Domain Page**. • Right-click a System Automation for z/OS resource, and click **View in Domain Page**.

Table 3. System Automation dashboards (continued)

Dashboard name	Description	Accessing this dashboard
Issue Command	You can execute NetView® and MVS™ commands on the associated system.	- In the navigation bar, click **Administration** > **Issue Command**. - Right-click a resource and click **Issue Command**.
System Log	You can view the log messages for a specific system.	Right-click a node or a resource and click **View System Log**. The dashboard is automatically connected with the system associated with this node or resource and show its log messages.
Adapter Log	You can view the log messages for a specific adapter.	Right-click an automation domain and select **View Adapter Log**. The **Adapter Log** dashboard is automatically connected with the adapter associated with this automation domain and show its log messages.
Problem Isolation with INGWHY	You can view the analysis for a specific resource using the SA z/OS operator command INGWHY.	Right-click a System Automation for z/OS resource and click **Isolate Problem with INGWHY**. The **Problem Isolation with INGWHY** dashboard is opened in context of the selected resource and shows its analysis.
Captured Messages	The Captured Messages dashboard shows the captured messages for a specific node or resource. You can use SA z/OS to capture messages and view the messages in the context of the automation resource that issued the message.	Right-click a node or a resource and click **View Captured Messages**. The **Captured Messages** dashboard is automatically connected with the node or resource and shows its captured messages.
Monitoring History	The Monitoring History dashboard shows the monitoring history for a specific monitor resource. You can use IBM System Automation for z/OS to capture messages and view the messages in the context of the monitor resource that issued the message.	Right-click a monitoring resource and click **View Monitoring History**. The **Monitoring History** dashboard is automatically connected with the monitoring resource and shows its monitoring history.
Manage Automation Policies	You can view all the Universal Automation Adapter domains and corresponding policies, and list, edit, activate, and deactivate policies.	In the navigation bar, click **System Configuration** > **Manage Automation Policies**.

Table 3. System Automation dashboards (continued)

Dashboard name	**Description**	**Accessing this dashboard**
Edit Automation Policy	You can view the Universal Automation Adapter policy and remote applications information, and create or edit the policies.	- In dashboard **Manage Automation Policies**, right-click the policy from the **Policies** widget and click **Edit Policy**. - In dashboard **Manage Automation Policies**, from the **Policies** widget, select **Actions** > **New...**.
JES Explorer	You can view JES job information and output when Zowe™ is installed and configured to connect with the SMU server.	1. In the Navigation bar, click **Administration** → **Explore Automation Domains**. 2. Right-click an application resource in the **Resources** widget and select **View Job Information**.
Configure Service Management Unite	You can configure the SMU server and the Universal Automation Adapter.	In the navigation bar, click **System Configuration** → **Configure Service Management Unite**.

Chapter 3. Planning

Effective preparation and planning make your installation and deployment go more quickly and smoothly. Review the following preinstallation requirements and familiarize yourself with the installation tools to prepare for your installation.

Environment requirements

To successfully install and configure Service Management Unite Automation, your environment must meet certain prerequisites.

Your environment must include at least two systems:

- A system running z/OS V2.2 or later
- A physical or virtual image running Linux® on system x or Linux on System z®

  For the distributed systems, the language setting in system locale must be 'English' to install SMU Automation.

Note:

- Installing multiple SMU Automation instances on one server is not supported.
- To use the new capabilities offered by SMU integration with Zowe, APAR OA54684 must be installed in System Automation for z/OS.

Service Management Unite Automation supports these components:

- System Automation for z/OS 4.1.0
- System Automation for z/OS 3.5.0 (with APAR OA51668 installed)

Planning for a user repository

Information about users and groups is stored in a user registry. By default, the WebSphere® Application Server that is installed with Jazz for Service Management is configured to use a local file-based user repository.

Optionally, you can also set up an LDAP server and create an LDAP user repository to use with Service Management Unite Automation.

For more information, refer to "Setting up an LDAP user registry" on page 87.

Requirements for user IDs that access z/OS systems from Service Management Unite

Access to z/OS systems is routed through the E2E adapter that runs in the System Automation for z/OS domain. The following two types of user IDs need access to the System Automation for z/OS domain from Service Management Unite:

Personal user ID

The personal user ID is used to log in to an SA domain and work with the automation resources after you log in to Dashboard Application Services Hub to access the Service Management Unite dashboards.

In the domain's login dialog, enter the z/OS user credential. The user ID is linked to your WebSphere user ID for DASH login. It can optionally be stored in the your credential store, which can store the user ID and password on a per domain basis so that you don't need to provide the credential to this domain again for login purpose.

Functional user ID

The functional user ID is used to access an SA domain on behalf of the automation framework that runs in the WebSphere Application Server. It is used for querying the SA resources that run in the SA plex independent of an actual user that is logged in to Service Management Unite. For example, the functional user ID is used to populate the resource cache in Service Management Unite during the startup of the Service Management Unite server. Only queries and no actions (for example, to start or stop a resource) are issued through the functional user ID.

Configure the functional z/OS user ID in the configuration tool **cfgsmu** or the Web Configuration Tool. For more details about how to configure the functional user IDs, see "User Credentials tab" on page 65 in **cfgsmu** or "User Credentials" on page 60 in the web configuration tool.

Requirements for User IDs on z/OS

Make the following security definitions depending on the purpose of the user ID and the rights that the users should have:

- **Functional User ID**
  - The functional user ID must be defined to RACF and must have at least an OMVS segment.
  - Authorization requirements:
    - Ensure the following RACF profile configuration to authorize the user ID for SA queries:
      - Class: NETCMDS
      - Permission: READ
      - Profile: netid.netvdom.INGRXTX0
- **Personal User ID**
  - The personal user ID must be defined to RACF and must have at least an OMVS segment.
  - Authorization requirements:
    - Ensure the following RACF profile configuration to authorize the user ID for SA queries:
      - Class: NETCMDS
      - Permission: READ
      - Profile: netid.netvdom.INGRXTX0
    - Define the following RACF profiles for the user ID depending on the actions that the user needs to perform:
      - Class: NETCMDS
      - Permission: READ
      - Profile:
        - netid.netvdom.INGRYRU0 for issuing start or stop requests (**INGREQ**)
        - netid.netvdom.INGRYSE0 for canceling requests (**INGSET**)
        - netid.netvdom.INGRYMVX for issuing a move of sysplex application groups (**INGMOVE**)
        - netid.netvdom.AOFRASTA for resetting a resource (**SETSTATE**)
        - netid.netvdom.INGRYGRA for changing group targets (**INGGROUP**)
        - For any NetView command that a user needs to submit from the "Issue Command" dashboard: the profile of the corresponding command
    - If System Automation resource security that is used to check if an action is allowed on a specific resource is enabled, define the following RACF profiles for the user ID depending on which resources the user can work with (defined by profile) and whether the user needs to specify advanced parameters with start and stop requests (defined by permission):
      - Class: SYSAUTO

- Permission: UPDATE or CONTROL
- Profile: AGT.sysplex.xcfgrp.RES.name.type.system

  Note:

  – Use AGT.*.*.RES.** to authorize the user for all System Automation resources.

  – If the user needs to specify advanced parameters for start and stop requests (**`INGREQ`**), such as "Override dependencies", the user needs to have CONTROL access. Otherwise, UPDATE is sufficient.

For details about System Automation resource security, see Resources in IBM System Automation for z/OS manual.

Port requirements

Review the following tables for the port requirements.

Ports used by JazzSM

The values of the ports that are used by JazzSM to access web server consoles are stored in the `JazzSM_installation_directory/profile/properties/portdef.props` file.

Table 4. Ports that are used by JazzSM

Connectivity to...	Ports used
WAS Admin Console	**`WC_adminhost_secure`**=16316 **`WC_adminhost`**=16315
DASH Web GUI	**`WC_defaulthost_secure`**=16311 **`WC_defaulthost`**=16310

Ports used by the SMU backend

Table 5. Ports that are used by the SMU backend

Connectivity to...	Ports used
The System Automation E2E Adapter on z/OS	2001 (outgoing) 2002 (incoming)

Ports used by the Universal Automation Adapter

Table 6. Ports that are used by the Universal Automation Adapter

Target systems for the Universal Automation Adapter	Ports used
Systems that can be accessed via SSH protocol	22 (default ssh port)

Other optional ports – depending on your installation

Table 7. Optional ports

Connectivity from SMU server to...	Ports used
LDAP Server (if LDAP user registry is used)	389 (default non-SSL port) 636 (default SSL port)

Table 7. Optional ports (continued)

Connectivity from SMU server to...	Ports used
TDI (if TDI is installed on a separate server)	1099
IBM Operations Analytics - Log Analyzer (IOLA) (if IOLA is used)	9987

Supported operating systems

IBM Service Management Unite supports various versions of Linux operating systems.

The following table lists the minimum supported versions:

Table 8. Supported operating systems for IBM Service Management Unite Automation

Operating system	IBM System x[1]	IBM System z
SUSE Linux Enterprise Server 11 (64 bit)	√	√
SUSE Linux Enterprise Server 12 (64 bit)[2]	√	√
Red Hat Enterprise Linux 5.6 (64 bit)[3]	√	√
Red Hat RHEL Linux 6 (64 bit)	√	√
Red Hat RHEL Linux 7 (64 bit)	√	√

The following Service Pack or technology levels are supported, unless one of the notes indicates a more specific minimum requirement:

- Service Pack levels of the listed supported SUSE versions, or later
- Service Pack levels of the listed supported Red Hat versions, or later

Note:

1. IBM System x with IA32, EM64T, or AMD64 architecture.

   Any other systems with IA32, EM64T, or AMD64 architecture are also supported.

   Systems with IA64 architecture are not supported.

   All supported operating systems are also supported when running under VMware.

   All listed Linux operating systems running under the Red Hat Enterprise Virtualization Hypervisor (RHEV-H) KVM version 5.4 or later are also supported. However, the live migration functionality provided by this hypervisor is not supported.
2. For SUSE Linux Enterprise Server 12, the supported minimum level is Dashboard Application Services Hub 3.1.3 (part of JazzSM 1.1.3) and WebSphere Application Server 8.5.5.9 or later.
3. The supported minimum level is Red Hat Enterprise Linux 5.6.

Supported web browsers and mobile OS

IBM Service Management Unite Automation is supported using various web browsers and mobile devices.

It's recommended that you use Chrome or Firefox to use the SMU dashboards.

Hardware requirements

Before you begin installation and configuration, be sure to identify and address all the required hardware prerequisites.

Processor

2 processors are needed for the installation.

Memory

Make sure that enough memory is available for the installation. The minimum required memory (RAM) is 4 GB to install WebSphere Application Server and IBM Service Management Unite on the same server. It's highly recommended that 8GB is available on the server.

Disk space

Make sure that enough disk space is available for the installation. In general, 12 GB free disk space is needed for the SMU server:

- 4 GB for directory `/tmp`
- 6 GB for installation media
- 2 GB for the installed code

You can use the prerequisite scanner for the Jazz for Service Management installation package to list the precise requirements that arise from your operating system. To run the prerequisite scanner, issue the following commands:

```
export JazzSM_FreshInstall=True
JazzSM_Image_Home/PrereqScanner/prereq_checker.sh "ODP,DSH" detail
```

The scanner prints the expected disk space and other prerequisites.

TCP/IP Connectivity

Provide TCP/IP connections between the SMU Automation server and the System Automation E2E Adapter on z/OS (By default, ports 2001 and 2002) .

Software prerequisites

Prerequisite software must be installed in your environment before you install and configure IBM Service Management Unite Automation. Prerequisite checks are run automatically at various points in the installation process.

Prerequisites for the SMU server

You must install the following products before you install the SMU components. Visit the download portal at http://ibm.biz/smu-auto-download to get the installation packages.

- Jazz™ for Service Management V1.1.3.0 or later (with 1.1.3.2 recommended), including Dashboard Application Services Hub (DASH) V3.1.3

  Note:

  – It's recommended to update DASH with fix pack 2 (DASH 3.1.3.2 included in JazzSM 1.1.3.2) after you install the base package from the download page. Download the fix pack from Fix Central: https://ibm.biz/Bd2tdB.

  – Ensure that your existing environment meets current Jazz for Service Management requirements including prerequisites like the IBM Installation Manager. For more information about the requirements, see Detailed system requirements for Linux.

- WebSphere® Application Server V8.5.5.x, including WebSphere Application Server Java SDK V1.7 or V1.8

  Note:

  – It's recommended to update the WebSphere Application Server with fix pack 14 after you install the base package from the download page. Download the fix pack from Fix Central: https://ibm.biz/Bd2tdc.

  – The minimum fix pack level for DASH 3.1.3 is WebSphere Application Server V8.5.5.9.

Prerequisites for SMU Automation:

To make product data available to Service Management Unite Automation, you must install the following products and adapters, as applicable to your environment:

- IBM System Automation for z/OS® V4.1 with APAR OA54684 installed
- System Automation for z/OS end-to-end adapter
- Universal Automation Adapter
- NetView for z/OS V6.2.1

Preinstallation checklist

Use this checklist to organize the required information for installing Service Management Unite Automation.

Review the following information before you begin the installation process:

__ Ensure the "Environment requirements" on page 11, "Hardware requirements" on page 15, and "Software prerequisites" on page 15 are met.
__ Verify the administrator ID and password for WebSphere Application Server.
__ Verify the name of the WebSphere Application Server used by the Jazz for Service Management profile.
__ Determine the Service Management Unite installation directory, if you don't use the default path.
__ Determine whether any Tivoli Common Directory setup and whether another product uses it.
__ Determine the functional user ID to be used for Service Management Unite Automation internally.
__ Determine the Service Management Unite Automation Administrator user ID.

Chapter 4. Installing and uninstalling SMU Automation

Installing Service Management Unite Automation requires meeting the prerequisites, installing the required and optional software. Select the installation method and follow the steps to install SMU Automation.

Installation method	SMU Automation
Docker	Install SMU Automation with Docker.
Root	1. Install JazzSM and WebSphere Application Server as root. 2. Install SMU Automation as root.
Non-root	1. Install JazzSM and WebSphere Application Server as non-root. 2. Install SMU Automation as non-root.
Silent	1. Install JazzSM and WebSphere Application Server in silent. 2. Install SMU Automation in silent.

Obtaining installation files

Visit the download portal to get the Service Management Unite installation files.

Procedure

1. Go to the download portal (http://ibm.biz/smu-auto-download) to download SMU Automation installation files.

   You need an IBM ID to log in, if you don't have one, access this website (https://www.ibm.com/account/us-en/signup/register.html?Target=https://myibm.ibm.com/) to sign up.
2. Provide the access key to get the installation files.

   You have two options to find the access key:

   - If you have APAR OA56692 installed in IBM System Automation for z/OS, you can find the access key and additional download information on your z/OS system in dataset SINGSAMP(INGESMU).
   - View the PDF which is supplied with the product materials on a CD titled "**Accessing IBM System Automation for z/OS Service Management Unite**".
3. Select the packages and click **Download now** to get the installation files.

   - If you prefer to install SMU Automation using a prebuilt Docker image, select **IBM Service Manageme Unite Automation - Docker image for Linux on System x** or **IBM Service Management Unite Automation - Docker image for Linux on System z** depending on your system. The Docker image contains all the software prerequisites that you need to install SMU Automation.
   - If you install SMU Automation manually using the provided installers, select the SMU Automation and prerequisite software packages depending on your system. For example,
     - IBM Service Management Unite Automation - Installation image for Linux on System x or z
     - Jazz for Service Management 1.1.3.0 for Linux (Launchpad, PRS, Jazz Repository, TDI)
     - IBM WebSphere Application Server V8.5.5.9 for Linux

Installing and uninstalling SMU Automation with Docker

Starting from Service Management Unite V1.1.4, Docker technology is introduced to reduce the time and effort in installing Service Management Unite.

Docker is an open platform for developing, shipping, and running applications. To simplify the installation, a Service Management Unite Docker image is provided as an alternative to the classic installation package. With the Docker image, you can create a Docker container that includes everything that is needed for Service Management Unite to run, including an operating system, user-added files, metadata, and the related dependencies.

The Docker image contains all runtime components that are needed to run Service Management Unite:

- IBM Service Management Unite Automation
- IBM WebSphere Application Server
- IBM Jazz for Service Management with IBM Dashboard Application Services Hub

Installing Service Management Unite Automation

Load and run the Docker image to install Service Management Unite Automation.

Before you begin

Before you install Service Management Unite Automation by using the Docker image, you must ensure that you have Docker installed on the server. Refer to the following information to install Docker on Linux on System x or Linux on System z:

- Installing Docker on zLinux.
- Installing Docker on xLinux.

Procedure

1. Download the SMU Docker archive depending on the architecture of your host system, for example `SMU_Automation_v1.1.6.0_Docker_Image_xLinux.tar` for the SMU Docker image running on xLinux (x86_64).

   The SMU Docker archive is a compressed file. Run the command to extract the contained files to a target directory:

   ```
   tar -xvf <SMU_Docker_archive.tar> --directory <target_dir>
   ```

   Note: The target directory must exist before **`tar`** can extract the files into it.

   The package contains the following files:

   - An exported Docker image that includes all prerequisite software and must be loaded into your Docker environment: `smu_image_v1160.tar`.
   - The IBM SMU Docker Command Line Utility: A shell script with other necessary files that help you to manage the SMU Automation Docker image and perform common tasks like loading the Docker image or starting and stopping the SMU Docker container.

     This utility consists of the following files:

     - **`eezdocker.sh`**: The key script that allows you to manage the Docker image and container.

       Run command **`eezdocker.sh help`** for more details.

       Note: The script must be ran from a user who is allowed to use Docker, for example, root.
     - **`eezdocker.cfg`**: A file that allows you to overwrite the default settings used by **`eezdocker.sh`**. It must be in the same directory where **`eezdocker.sh`** is located. If it doesn't exist, **`eezdocker.sh`** will use its default settings.
     - **`util`**: A folder that contains utility files for the **`eezdocker.sh`** script.

- A readme file with additional information about the SMU Docker image.

2. Edit file **eezdocker.cfg** if you want to change the default settings of **eezdocker.sh**. For more information, see "Customizing the SMU Docker Command Line Utility" on page 20.
3. Use the IBM SMU Docker Command Line Utility to load the SMU Docker image into your Docker environment by issuing the following command:

   ```
   ./eezdocker.sh load
   ```

   To verify if the Docker image is loaded, issue command **eezdocker.sh status**.

   If the load is successful, you can delete the `smu_image_v1160.tar` because it is not needed anymore.
4. Use the IBM SMU Docker Command Line Utility to start the SMU Docker container by issuing the following command:

   ```
   ./eezdocker.sh start
   ```

   If you run this command for the first time, a new SMU Docker container will be automatically created from the SMU Docker image.

   The Tivoli Directory Integrator server and WebSphere Application Server are automatically started when a Docker container is started from the SMU Docker image.

   Note: The Docker container is started with the Docker option '–restart on-failure', which means it will be automatically restarted when the SMU Docker container crashes or if the Docker runtime environment or the host system is restarted.

   To verify if the Docker container from the SMU Docker image is started, issue command **eezdocker.sh status**.

Results

When the Docker container is successfully started, you can access the SMU dashboard via the following URL:

```
https://<hostname>:16311/ibm/console
```

The default SMU administrative user ID and password are `eezadmin/eezadmin`.

Note: It might take up to 1 minute after the Docker container is started until all services are initialized and available.

Access the WebSphere administrative console via the following URL:

```
https://<hostname>:16316/ibm/console
```

The default WebSphere Application Server administrative user ID and password are `wasadmin/wasadmin`.

You can use the WebSphere administrative console to define more user IDs or change the password.

What to do next

Follow the steps to configure SMU to connect to backend systems:

- Define the functional user IDs that are used to connect to automation domains with the configuration tool **cfgsmu**.

  To start the GUI of **cfgsmu** from within the running Docker container, the container's variable *$DISPLAY* must point to the X Display server of your host system. Run the command:

  ```
  eezdocker.sh cfgsmu
  ```

Note: If command '**eezdocker.sh cfgsmu**' doesn't work as expected, run the command '**xhost +local:all**' before you run '**eezdocker.sh cfgsmu**' to ensure that the Docker process can access the user's X session.

- Set up the IBM System Automation for z/OS (SA z/OS) E2E automation adapter to connect an SA z/OS automation domain to SMU.

For more information on how to configure SMU for your environment, refer to Chapter 7, “Configuring and administering SMU Automation,” on page 59.

Customizing the SMU Docker Command Line Utility

You can use the Service Management Unite (SMU) Docker Command Line Utility to manage and control the SMU Docker containers.

About this task

The **eezdocker.sh** is preconfigured and can be used in most cases. For special scenarios, you can optionally uncomment or change the values of the variables in file **eezdocker.cfg** to customize the **eezdocker.sh** script.

If file **eezdocker.cfg** exists and is located in the same directory as the **eezdocker.sh** script, the SMU Docker Command Line Utility will read it and override its default configuration with the configuration provided by the config file.

Procedure

1. Open the config file **eezdocker.cfg**.
2. Edit the values of the options as needed.

SMU_CURRENT_VERSION

The version of SMU that the script handles.

It can be set to an earlier version to let the script handle the older SMU version instead of the latest one. Same as the '**-v**' option.

The version must be in format *<MAJOR><MINOR><REVISION><SUBREVISION>*, for example, 1150.

Note: Only SMU Docker containers version 1140 and later are supported.

DOCKER_CMD

The Docker executable to use. A path can be included.

Change the value if the Docker command is not in your environment variable *$PATH*, or if you want to use another Docker executable than the default one in your environment.

DOCKER_NETWORK

The network to which the SMU Docker container is connected.

The value of this option is provided as **--network** option to the **docker create** command. For more details, see the official Docker documentation at https://docs.docker.com/network/.

Note: If you change this value, you must issue command **eezdocker.sh reconfigure** to make the changes take effect.

DOCKER_NETWORK_CONFIG

Additional configuration (parameters) related to the network type.

It's required when you specify the DASH and WAS Admin Console port mapping and the Docker container's host name. For more details, see the official Docker documentation at https://docs.docker.com/network/.

DOCKER_RESTART_POLICY

The restart policy that is used to run the SMU Docker container.

The value of this option is provided as **--restart** option to the **docker create** command. For more details, see the official Docker documentation at https://docs.docker.com/config/containers/start-containers-automatically/.

Note: If you change this value, you must issue command **eezdocker.sh reconfigure** to make the changes take effect.

DOCKER_CREATE_FLAGS
Other flags or options that are used to run the SMU Docker container.

The value of this option is provided as is to the **docker create** command. For more details, see the official Docker documentation at https://docs.docker.com/engine/reference/commandline/create/.

Note: If you change this value, you must issue command **eezdocker.sh reconfigure** to make the changes take effect.

DOCKER_VOLUMES
Docker volumes that are used for the SMU Docker container.

The value(s) of this option is provided as is to the **docker create** command. For more details see the official Docker documentation at https://docs.docker.com/storage/volumes/.

Note: No volumes are used in the default configuration so that you can create and distribute snapshots of SMU Docker containers. Volumes are not stored when a container is committed to a new image. If you change this value, you must issue command **eezdocker.sh reconfigure** to make the changes take effect.

MIGRATION_COPY_CUSTOM_FOLDERS
Array of the customized files or folders that should be copied over from the old SMU Docker container to the new container during **eezdocker.sh migrate**. The array of files or folders must be indexed starting with 0.

Note: During a migration, the required SMU and DASH / JazzSM configuration is copied over regardless of the setting of this option. This array allows to specify additional files or folders like holding custom files or modifications that should not get lost during a migration to a new version of SMU Docker container.

3. Save the changes and exit the file.

Managing the SMU Docker container

This section describes the lifecycle of an IBM SMU Docker container and the commands available for managing the container.

The lifecycle of an SMU Docker container

When you download the SMU Docker archive, extract the package, and initially run command **eezdocker.sh load**, the SMU Docker image is loaded into your local Docker environment.

The image is like a blueprint for you, containing SMU and all its prerequisites but missing your custom configuration. To use SMU in your environment, you need to create a Docker container from the SMU Docker image. A container is a concrete, runnable instance of an image. Theoretically, you can create more than one container instance from the same image in parallel and configure each container individually.

When you first run command **eezdocker.sh start**, the SMU Docker Command Line Utility automatically creates a new SMU Docker container from the SMU Docker image for you. The created Docker container can be started and stopped as often as you like and also survives from a restart of the Docker environment or a restart of the host system.

Unless you explicitly delete the SMU Docker container (**eezdocker.sh reset** or **eezdocker.sh uninstall**), the SMU Docker Command Line Utility operates on the same SMU Docker container instance. For example, if you stop the SMU Docker container (**eezdocker.sh stop**) and start it again (**eezdocker.sh start**), it will be the same SMU Docker container instance.

Every SMU and WebSphere Application Server configuration change that you perform on a running SMU Docker container is stored within this container instance, but not in the SMU Docker image. For example, if you create an own custom dashboard in DASH, the change is stored within the SMU Docker container and will be there until the container is deleted. The dashboard will also still be there if the SMU Docker container is restarted or even if the host system is restarted.

Therefore, the easiest way to reset SMU to factory defaults is to delete the SMU Docker container and create a new one from the SMU Docker image (**`eezdocker.sh reset`**).

Note: In SMU V1.1.4, Docker volumes are used to store the SMU and WebSphere Application Server configuration outside of the SMU Docker container in a specific directory on the host system. From SMU V1.1.5, the SMU Docker container does not use any Docker volumes anymore. All configuration is stored within the SMU Docker container and won't get lost unless you delete the container.

In addition, a migration command is provided that allows you to migrate your custom configuration from an SMU Docker container of an old version to a new version. For more information, see "Upgrading SMU with Docker" on page 55.

Commands provided by the SMU Docker Command Line Utility

Run the following commands to manage the SMU Docker container:

eezdocker.sh load

Loads the IBM provided SMU Docker image into your local Docker environment.

You only need to run this command once. If the image is successfully loaded, you can delete the `smu_image.tar` file.

eezdocker.sh start

Starts the SMU Docker container if it is stopped.

If no SMU Docker container exists, it creates a new SMU Docker container from the loaded SMU Docker image.

eezdocker.sh stop

Stops the running SMU Docker container.

eezdocker.sh restart

Restarts the running SMU Docker container.

It stops the SMU Docker container and starts it again. For example, you can run the command if you need to restart the WebSphere Application Server after a configuration change.

eezdocker.sh shell

Opens a Bash shell to the running SMU Docker container.

It allows you to access the internal of the container, for example, if the configuration files need to be edited manually.

To exit the shell, issue command **`exit`** in the shell. It only exits the shell connection into the SMU Docker container, and the container and SMU continue to run.

eezdocker.sh cfgsmu

Starts the SMU Automation **`cfgsmu`** tool and sets up the necessary X-Forwarding so that the tool's GUI can be displayed with the host's Window Manager.

If **`cgfsmu`** cannot be ran out of the Docker container, it might be necessary to allow access to the X11 session on the host system. Run command `xhost+local:all` before you run `eezdocker.sh cfgsmu` to ensure that the Docker process can access the user's X session.

eezdocker.sh collect_logs

Collects and bundles all relevant log files from the running SMU Docker container and copies them to the host system's `/tmp` folder.

For example, you can run this command if you have a problem and the IBM Support team requests the log information.

eezdocker.sh reconfigure

Some Docker configuration can only be specified during the creation of the SMU Docker container, for example the network configuration. If you need to change such a configuration option, issue this command to make the configuration changes take effect.

Internally, the current SMU Docker container is committed into a snapshot of the SMU Docker image, from which a new container is created. By this means, the new container has all the configuration and customization of the old container, but runs with the new configuration. When you issue command **`eezdocker.sh reconfigure`**, a new snapshot is created. Keep the snapshot image because an image cannot be removed if there are containers derived from it. The image doesn't take up too much disk space because only the changes, compared to the official SMU Docker image, are stored in it.

eezdocker.sh migrate

Migrates all of your custom configuration from the old SMU Docker container into the new container of a new SMU release. See "Upgrading SMU with Docker" on page 55.

eezdocker.sh reset

Deletes the current SMU Docker container. If you run command **`eezdocker.sh start`** afterwards, a new SMU Docker container is created.

⚠ **Warning:** All custom configuration will get lost! Run the command if you need to rest to factory defaults.

eezdocker.sh uninstall

Deletes the current SMU Docker container and the SMU Docker image.

⚠ **Warning:** All custom configuration will get lost! Run the command if you need to remove SMU from your Docker environment.

Network and ports information

As default configuration, the SMU Docker container uses a network bridge and maps the required ports to the Docker host system. The Docker container's host name is set to the Docker host system's name.

The Docker container opens and maps the following ports in listen mode for services that are offered by Service Management Unite:

Table 9. Default ports information

Port number	Description
16311	Port to access the DASH that hosts the SMU dashboards
16316	Port to access the WebSphere administrative console
2002	Port that is used by automation adapters to connect to SMU and send update events for resources
2005	Port that is opened by the Universal Automation Adapter to receive requests from the E2E agent

If you want to restrict access to a port (for example, the WebSphere administrative console, port 16316), you need to configure appropriate firewall rules on the host system.

Note: If you plan to use the Universal Automation Adapter (UAA) to manage resources that are running on the same host system where the SMU Docker container is running, a special configuration is required.

It is not possible to use the SMU Docker container host's host name as node name in the UAA Policy, because this host name will be resolved to the Docker container's internal IP address by the SMU Docker container - and not to the Docker host's IP address as required. To resolve this issue, you need to use another host name than the one that is set to the SMU Docker container, but resolving to the intended IP address.

In **eezdocker.cfg**, you can add **--add-host=<my_host_name>_host:<my_host_ip>** as an option to **DOCKER_NETWORK_CONFIG**. The Docker parameter **--add-host** allows you to introduce host name IP address mappings for a Docker container. For example, if the host name where your SMU Docker container runs is **smu**, this will (inside the SMU Docker container) introduce the host name **smu_host**, which resolves to the same IP address than **smu**. In the UAA's policy, you specify the resource's node to this new host name **smu_host**.

Uninstalling Service Management Unite

To uninstall Service Management Unite Automation, remove the SMU Docker image and all SMU Docker containers from the host system.

Procedure

1. Any SMU Docker container must be stopped before the uninstallation. Issue the command to stop the SMU Docker container:

   ```
   ./eezdocker.sh stop
   ```

2. Issue the command to remove SMU Docker container and Docker image:

   ```
   ./eezdocker.sh uninstall
   ```

Results

The SMU instance is successfully removed from your server.

What to do next

After you remove the SMU Docker image and containers, delete the `eezdocker.sh` script and its belonging files.

Installing Jazz for Service Management and WebSphere Application Server

Jazz for Service Management and WebSphere Application Server are software prerequisites that you need to install before you install Service Management Unite. You can either use root or non-root user authority to install the software prerequisites.

[Root] Installing Jazz for Service Management and WebSphere Application Server

Follow the steps described in this topic to install Jazz for Service Management and WebSphere Application Server.

1. Create a common directory to store the extracted Jazz for Service Management installation media, referred to as the `JazzSM_Image_Home directory`.

   Restriction: Ensure that the path to the common root directory does not contain any spaces or special characters.

2. Extract the contents of the following deliverable into this directory:

   Jazz for Service Management Version 1.1.3:

   - Linux: Jazz for Service Management 1.1.3.0 for Linux (Launchpad, PRS, Jazz Repository, TDI) `IBM-jazzsm-launchpad-113-linux64.zip`
   - Linux on System z: Jazz for Service Management 1.1.3.0 for Linux on System z (Launchpad, PRS, Jazz Repository, TDI) `IBM-jazzsm-launchpad-113-linuxZSeries64.zip`

WebSphere Application Server Version 8.5.5.x:

- Linux: IBM WebSphere Application Server V8.5.5.x for Linux `IBM-was-8.5.5.x-linux64.zip`
- Linux on System z: IBM WebSphere Application Server V8.5.5.x for Linux on System z `IBM-was-8.5.5.x-linuxZSeries64.zip`

3. Install JazzSM Services by using Installation Manager:

   a. Browse to the `JazzSM_Image_Home/im.platform_name/` directory and run the installation command, for example:

   ```
   ./install
   ```

   If the installation does not start due to missing prerequisites, check whether all required libraries are installed. For more information about Jazz for Service Management prerequisites, see Jazz for Service Management Detailed System Requirements (http://www-01.ibm.com/support/docview.wss?uid=swg27038732).

   b. The **Installation Manager** window opens. Select the following packages to be installed:

      i) IBM Installation Manager Version 1.8.2 or later

      ii) IBM WebSphere Application Server Version 8.5.5.4 or later

      iii) IBM WebSphere SDK Java™ Technology Edition Version 7.0 or later

      iv) Jazz for Service Management extension for IBM WebSphere 8.5 Version 1.1.3.0 or later

      v) IBM Dashboard Application Services Hub Version 3.1.3.0

   c. Click **Next**. The **Installation Manager > Licenses** window opens. Review and accept the License Agreements.

   d. Click **Next** and specify the directories that are used by the Installation Manager.

   e. Click **Next** and specify the installation directories for WebSphere Application Server and Jazz for Service Management.

   f. Click **Next**. The **Installation Manager > Features – languages** window opens.

   g. Accept the default translated languages that are selected in the **Translations Supported by All Packages** window. Click **Next**. The **Installation Manager > Features** window opens.

   h. Click **Next** and specify the configuration for your WebSphere Application Server installation. Define the WebSphere administrative user ID. Click **Validate**.

   i. Click **Next**. The **Installation Manager > Summary window** opens.

   j. Review the software packages to be installed and their installation directories. Click **Install** to start the installation.

   k. When the installation completed, a success window is displayed. You can now click **Finish** to close the Installation Manager.

4. Important: Activate Java 7 or Java 8 for the WebSphere Application Server profile.

   For example, to activate Java SDK 7, issue the following command:

```
was_root/bin/managesdk.sh -enableProfile -sdkName 1.7_64 -profileName JazzSMProfile -enableServers
```

   JazzSMProfile is the profile name that is used for Jazz for Service Management. Default name: JazzSMProfile.

   Note: More information about configuring Java 7 is provided at the following links:

   - Find out how to install and configure Java 7 at the IBM Education Assistant -WebSphere software.
   - Check the Java SDK Upgrade Policy for the IBM WebSphere Application Server before you apply the fixes to WebSphere Application Server, to ensure that the fix matches to the installed Java version.
   - The page Verify Java SDK version shipped with IBM WebSphere Application Server fix packs describes which version of WebSphere Application Server corresponds to which Java SDK level.

You are now ready to install Service Management Unite Automation.

[Non-root] Installing Jazz for Service Management and WebSphere Application Server

By default, the IBM WebSphere Application Server that hosts IBM Service Management Unite Automation runs as root. However, it can also be installed and run by using a non-root user ID. In that case, Service Management Unite Automation as well as the prerequisite WebSphere Application Server and Dashboard Application Services Hub must be all installed using the same non-root user ID.

About this task

The root or non-root installer who owns the currently installed files is the only user who can perform subsequent installation or removal operations on that installation.

To install Jazz for Service Management using a non-root user, complete the steps as follows:

Procedure

1. Log in to the system where you want to install Service Management Unite using the non-root user ID that should be the owner of this WebSphere Application Server runtime environment.
2. Follow the instructions that are described in Installing Jazz for Service Management and WebSphere Application Server, but instead of running the command `install` in step 3, use the command `userinst` to start IBM Installation Manager in "user mode".
3. In the Installation Manager, choose installation directories that are located below your user's home directory, for example, accept the default directories such as `/home/<user>/IBM/WebSphere/AppServer`.

Planning for the Universal Automation Adapters

The Universal Automation Adapters enables Service Management Unite to monitor, operate, and automate resources that run on non-z/OS systems. It can be used as the connection target by IBM System Automation for z/OS to provide end-to-end automation.

The Universal Automation Adapter is automatically installed together with the IBM Service Management Unite Automation product as described in "Installing SMU Automation" on page 27. Only one instance of the Universal Automation Adapter can be installed on any remote node on Linux systems.

For more information, refer to "Tuning the number of domains and resources of the Universal Automation Adapter" on page 81.

Requirements for target machines managed by the Universal Automation Adapter

The Universal Automation Adapter uses the Secure Shell (SSH) protocol to start, stop, and monitor resources on remote nodes. This topic describes the requirements that must be fulfilled by remote nodes that host the resources defined for a Universal Automation Adapter domain. These nodes are referred to as target-nodes.

Unix, Linux, and Windows targets

The Universal Automation Adapter does not supply SSH code for UNIX machines. Ensure SSH is installed and enabled on any target you want to access using the Universal Automation Adapter.

OpenSSH 3.7.1 or higher contains security enhancements not available in earlier releases. The Universal Automation Adapter cannot establish connections with any UNIX target that has all remote access protocols (`rsh`, `rexec`, or `ssh`) disabled.

In all UNIX environments except Solaris, the Bourne shell (sh) is used as the target shell. On Solaris targets, the Korn shell (ksh) is used instead due to problems encountered with sh.

In order for the Universal Automation Adapter to communicate with Linux and other SSH targets using password authentication, you must:

1. Edit the file `/etc/ssh/sshd_config` on target machines and set:

   ```
   PasswordAuthentication yes (the default is ’no’)
   ```

2. Now stop and restart the SSH daemon using the following commands:

   ```
   /etc/init.d/sshd stop
   /etc/init.d/sshd start
   ```

z/OS targets

z/OS targets require z/OS UNIX System Services (USS) and IBM Ported Tools for z/OS (OpenSSH).

- Documentation for OpenSSH can be found here:

  z/OS UNIX System Services
- Make sure that the SSHD process is available, for example, using AUTOLOG.
- Edit `/etc/ssh/sshd_config`, uncomment the UsePrivilegeSeparation parameter and change it to *no*.
- Verify that port 22 is open using the netstat -P 22 command.

Installing SMU Automation

After you installed Jazz for Service Management and WebSphere Application Server, you can select the method (root, non-root, or silent mode) to install Service Management Unite Automation.

Default directories

During the installation, default directories are used to install Service Management Unite Automation. Default directories are defined in variables. Verify and confirm all used variables and any related default directory.

The following table lists the default directory paths for which variables are used in this documentation. The paths in your environment may differ, for example, if you changed the default path during the installation of the application or component.

Table 10. Default directories

Variable used in this guide	**Default path**
`<EEZ_CONFIG_ROOT>`	`/etc/opt/IBM/smsz/ing/cfg`
`<EEZ_INSTALL_ROOT>`	`/opt/IBM/smsz/ing` The configuration properties files are located in the directory `<EEZ_CONFIG_ROOT>`.
`<Tivoli_Common_Directory>`	`/var/ibm/tivoli/common` The path to the Tivoli® Common Directory is specified in the properties file `log.properties`. The file `log.properties` is located in the following directory `/etc/ibm/tivoli/common/cfg`.
`<was_root>`	`/opt/IBM/WebSphere/AppServer`
`JazzSM_root`	`/opt/IBM/JazzSM`

Root installation

Run a wizard-based graphical installation to install SMU Automation as root.

Before you begin

You must ensure that an X Window session is available for displaying the graphical installation panels.

About this task

The installation comprises the following phases:

1. In the preinstallation phase, you need to specify the installation parameters.
2. The installation phase begins when you click **Install** on the last preinstallation window. In this phase, all files are installed to the disk. The installation step can be canceled at any time. It can also be resumed by starting the installer again.

Procedure

1. Extract the installation package `SMU_Automation_v1.1.6.0.tar`.
2. Start the installer from the command line:

   a. Change to the extracted directory that contains the installation script `SMUAUTO1160`.

   b. Issue the command to start IBM Installation Manager:

   ```
   ./smu_install.sh
   ```

   IBM Installation Manager should be available on your server if you installed the prerequisite software IBM WebSphere Application Server.

   The script tries to detect the location of IBM Installation Manager and launches it. Additionally, it will automatically configure IBM Installation Manager with the SMU Automation installer repository that is included in the extracted installation package.

   If the script launches Installation Manager successfully and the SMU Automation installer repository is pre-configured, you can skip step 3 and continue with step 4.
3. Skip this step if the script **`smu_install.sh`** launches IBM Installation Manager successfully.

   If the **`smu_install.sh`** script fails to detect Installation Manager on the server or fails to automatically configure the SMU Automation installer repository, follow the steps to manually start Installation Manager and load the repository:

   a) Issue the command to start Installation Manager:

   ```
   /opt/IBM/InstallationManager/eclipse/IBMIM
   ```

   b) Select **File** → **Preferences...** to open the **Preferences** window.

   i) Click **Add Repository...**.

   ii) Click **Browse...**. Browse to the location where you extracted the installation package and navigate to the `SMUAUTO1160/repositories/disk1_smu_auto` directory.

   iii) Select the `diskTag.inf` file and click **OK** to add the repository.

   iv) Click **OK** to exit the **Preferences** window.
4. On the IBM Installation Manager start page, click **Install** to start your installation.
5. On the **Install Packages** page, select **IBM Service Management Unite Automation Version 1.1.6.0** and click **Next**.

   Installation Manager checks for the prerequisite packages on your server. If your server does not meet the prerequisites check, the **Validation Results** page shows the missing prerequisites.
6. Carefully read the terms of the license agreement.

To accept the terms of the license agreement, select **I accept the terms in the license agreement** and click **Next**.

7. Specify the directory where you want to install SMU Automation or accept the default location `/opt/IBM/smsz/ing`, and then click **Next**.

   The **Create a new package group** option is selected by default and only this option is supported for the installation of SMU Automation.

8. Specify the directory where the Tivoli application log files are to be written, or accept the default location `/var/ibm/tivoli/common`, and then click **Next**.

   Note: If the installation program detects an existing Tivoli Common Directory on your system, click **Next** to use the existing one. For example, when another Tivoli product is already installed, the directory must also be used for SMU Automation.

9. On the **WebSphere Configuration** page:

   a) Decide whether to create users and user groups in the WebSphere Application Server's user repository.

      - Click **Yes** to use the default file-based user repository for managing WebSphere® Application Server users. The installer creates users and groups in the WebSphere Application Server's configured user repository.
      - Click **No** to use a central LDAP user repository, and the users and groups exist in this repository. The installer does not make any changes to users and groups. For further information, refer to "Configuring an LDAP user registry (optional)" on page 86.

      Note: For a high available environment, click **Yes** to create users and groups when you install the first SMU Automation server, and click **No** for the rest of the SMU servers.

   b) Provide the WebSphere Application Server administrative user ID and password.

      - Enter the username in field **WAS Admin User ID**. The user ID is detected and pre-filled.
      - Enter the password in field **WAS Admin User Password**.

   c) Click **Next**. If the credentials are incorrect, you will get an error message after the validation and cannot proceed.

10. On the **System Automation Functional user ID** page, specify password for the functional user ID `eezdmn`, and then click **Next**.

    Note: Do not copy and paste the password and the password confirmation. Enter the password and the confirmation directly.

    This functional user ID is needed for several purposes:

    - The operations console uses the credentials to populate the internal resource cache.
    - The automation framework uses the credentials to access JMS, as defined in the WebSphere Application Server JAAS authentication alias `EEZJMSAuthAlias`.
    - The automation framework uses the credentials for all asynchronous internal work that is associated with the `EEZAsync` role, as defined in the EEZEAR application's "User RunAs role" mapping.

11. On the **System Automation Administration user ID** page, specify the user ID and password of the System Automation administrator, and then click **Next**. The default user ID is `eezadmin`.

    Note: Do not choose the same name for both the System Automation Administration user ID and the WebSphere Application Server administrator user ID. Otherwise, problems might occur if you uninstall SMU Automation. For example, do not specify `smadmin` for both users.

12. When you specified all the required information on the installation panels, click **Install** to start the installation.

13. When the installation of SMU Automation is complete, the Installation Complete page is displayed. To check the installation log, click **View Log File**. Or click **Finish** to return to the main IBM Installation Manager dialog. For information about verifying the installation, refer to Verifying the Installation.

Results

SMU Automation is successfully installed.

Non-root installation

To install SMU Automation using a non-root user ID, ensure that you've installed Jazz for Service Management and WebSphere Application Server using the same non-root user ID that SMU Automation uses. For more information, refer to "[Non-root] Installing Jazz for Service Management and WebSphere Application Server" on page 26.

Before you begin

If you plan to install SMU Automation and want to use the Universal Automation Adapter, you need to make the following preparations:

- Make the Tivoli Common Directory (TCD) available for your non-root user.

  The TCD is a common location in which problem determination information for IBM products is saved. In Service Management Unite, the TCD is used by the Universal Automation Adapter as location for trace and log files. You need to ensure that your non-root user has write access to the following directories:

  - TCD Config Directory
    - The properties file for the TCD is stored in `/etc/ibm/tivoli/common/cfg`. Create this directory if it does not exist yet:

      `mkdir /etc/ibm/tivoli/common/cfg`.
    - Allow full access to this directory for all users:

      `chmod 777 /etc/ibm/tivoli/common/cfg`
  - Tivoli Common Directory

    If the TCD does not exist yet, you are prompted for the location of the Tivoli Common Directory during the installation of SMU Automation. As preparation, create a TCD to which your non-root user has write-access. By default, the directory is: `/var/ibm/tivoli/common`.

    - Create the directory:

      `mkdir /var/ibm/tivoli/common`
    - Allow full access to this directory for all users:

      `chmod 777 /var/ibm/tivoli/common`

Procedure

1. Log in to the system where you want to install SMU Automation using the non-root user ID that you also used for installing the (non-root) WebSphere Application Server runtime environment.
2. Issue the command to launch the non-root Installation Manager:

   ```
   /home/<userid>/IBM/InstallationManager/eclipse/IBMIM
   ```
3. Select **File** → **Preferences...** to open the **Preferences** window.

   a. Click **Add Repository...**.

   b. Click **Browse...**. Browse to the location where you extracted the installation package and navigate to the `SMUAUTO1160/repositories/disk1_smu_auto` directory.

   c. Select the `diskTag.inf` file and click **OK** to add the repository.

   d. Click **OK** to exit the **Preferences** window.
4. Continue with step 4 and all the following steps that are described in root installation of SMU Automation.

   Note:

- Ensure to choose an installation directory for which your non-root user ID has write-access during the installation, for example, a directory below the user's home directory: `/home/<user>/IBM/smsz/ing`.
- If you install SMU Automation as non-root user, the shortcut to the command `cfgsmu` is not created. To open the configuration tool `cfgsmu`, you either have to run it using a fully qualified path name (for example, `/home/<user>/IBM/smsz/ing/bin/cfgsmu.sh`) or create a shortcut for your non-root user manually.

Silent mode installation

You can install SMU Automation by running a silent installation. In silent mode, the installation program does not display a user interface, instead, it reads settings from a response file, runs a prerequisites check, and installs the software if the check succeeds.

About this task

You can use a response file to run a silent installation, the installation program does not display any installation windows. The response file contains parameters and values that you specify to tell the SMU Automation installation program how to run the installation.

If you are familiar with IBM Installation Manager, you can record your own response files for silent installation. As a convenience, Service Management Unite provides a response file template **`responsefile_auto.xml`** to help install or update in silent mode.

Procedure

1. Extract the installation package `SMU_Automation_v1.1.6.0.tar` into a temporary directory.
2. Change to the extracted directory SMUAUTO1160`/responsefiles`.
3. Edit the response file **`responsefile_auto.xml`** to match your environment.

   Tip: Create a backup copy of the response file before you change the content.
4. Change or add values for some of the properties, which are indicated by the "**xxxxxxxx**" string.

   In the response file, many properties have default values, but you can edit **`data key=properties`** if you need to change values for your environment. See the comments in the file for more details.

   Note: The *repository location* indicates the directory where the SMU Automation repository file – `diskTag.inf` is located. You must specify the relative path to the **`responsefile_auto.xml`** file. For example, `<repository location='../repositories/disk1_smu_auto'/>`.
5. Save your changes to the response file.

   The response file contains passwords. You need to secure the file after the passwords are entered into the file.
6. Issue the command to silently install SMU Automation:

   ```
   ./smu_install.sh SILENT AUTO
   ```
7. If the prerequisite checker fails, or the installation fails, refer to the `packageinstall.log` file that is created in the same directory where script **`smu_install.sh`** is located. Fix the issues and rerun the **`smu_install.sh`** script.

   Note: The installation process might create informational and warning messages that appear in the log and terminal session that can usually be ignored. For example, Installation Manager message **`CRMA1014W`** that indicates an existing shared resources directory cannot be changed. Installation Manager message **`CRIMA1263W`** warns against the use of symbolic links in installation directory path names.

Results

SMU Automation is successfully installed in silent mode.

Verifying the installation

This topic describes the tasks you should complete in order to verify that the automation manager and the operations console have been installed successfully.

Verifying the automation framework

To verify that the automation framework is installed successfully on Linux, complete the following steps:

Procedure

1. In a web browser window, specify the following address to display the Login window of the WebSphere administrative console:

   ```
   https://<your_host_name>:<your_was_port>/ibm/console
   ```

   The default WebSphere administrative console port is 16316.
2. On the login window, enter the user ID and password of the WebSphere Application Server administrator user. The default user ID is `smadmin`. Click **Log in**.
3. Navigate to **Applications > Application Types > WebSphere enterprise applications**. The list of installed applications must contain the entry **EEZEAR**.

Verifying that the automation database accepts WebSphere Application Server requests

Perform the following task to verify that the automation database accepts WebSphere Application Server requests:

Procedure

1. In a web browser window, specify the following address to display the Login window of the WebSphere administrative console:

   ```
   https://<your_host_name>:<your_was_port>/ibm/console
   ```

   The default WebSphere administrative console port is 16316.
2. On the login window, enter the user ID and password of the WebSphere Application Server administrator user. The default user ID is `smadmin`. Click **Log in**.
3. Navigate to **Resources > JDBC > Data sources > EAUTODBDS**. Click **Test connection** to verify that the automation database accepts WebSphere Application Server requests. If the test is successful, the following message displays:

   ```
   The test connection operation for data source EAUTODBDS on server server1 at node JazzSMNode01 was
   successful
   ```

Verifying the operations console

Perform the following steps to verify that the operations console was installed successfully:

Procedure

1. In a web browser window, specify the following address to display the Login window of the Dashboard Application Services Hub:

   ```
   https://<your_host_name>:<your_dash_port>/ibm/console
   ```

   The default IBM Dashboard Application Services Hub port is 16311.

2. In the Login window, enter the System Automation administrator user ID. The default user ID is `eezadmin`. Click **Go**.
3. The Welcome Page showing the System Automation dashboards appears. Select one of the System Automation dashboards. The installation is successful if the selected dashboard opens.

Uninstalling SMU Automation

Use Installation Manager to uninstall SMU Automation.

Procedure

1. Issue the following command to start IBM Installation Manager:

   ```
   /opt/IBM/InstallationManager/eclipse/IBMIM
   ```

2. On the Installation Manager start page, click **Uninstall**.
3. In the **Uninstall Packages - select packages to uninstall** panel, select **IBM Service Management Unite Automation** and click **Next**.
4. In the **Uninstall Packages - Common Configurations** panel, verify the fields that are filled in and provide the password for WAS Admin User ID, and then click **Next**.
5. Review the package that you want to uninstall and click **Uninstall**.
6. When the uninstallation is complete, a summary window is displayed. Click **Finish** to return to the main IBM Installation Manager dialog.

   To check the uninstallation log, click **View Log File**.
7. To exit IBM Installation Manager, click **File** → **Exit**.

Results

SMU Automation is successfully removed from your server.

Chapter 5. Setting up Service Management Unite with High Availability

To ensure a reliable system with high performance and less downtime, use this information to set up Service Management Unite Automation with high availability.

What is High Availability (HA)?

Availability refers to the time when a service or system is available. High availability is a quality of a system that assures a high level of operational performance for a given period.

Related concepts:

Load balanced cluster
A group of servers that act as a single system and provide continuous uptime.

Downtime
Time periods when a system is unavailable or unresponsive.

Load balancing
An effective way to increase the availability of web-based applications. When server failure instances are detected, the traffic is automatically redistributed to servers that are still running. It facilitates higher levels of fault tolerance within service applications.

Failover
The process by which one node takes over the job of another when it becomes unavailable.

Why is High Availability important?

When a server goes down, the entire system always becomes unavailable. However, in an HA environment, if a node in the cluster stops working, other active nodes in the cluster can take over services to keep on working. In other words, systems with high availability can avoid this kind of problems by eliminating single point of failure and thus increase reliability.

An SMU environment with high availability has the following capabilities:

Data Synchronization
After the load balancer is set up, all changes in the SMU console are stored in a common repository. In a cluster, updates that require synchronization are first committed to the database. At the same time, the node that submits the update notifies all other nodes in the cluster about the change. When other nodes in the cluster are notified, they get the updates from the database and commit the changes to the local configuration.

If data fails to be committed on a node, a warning message is written in the log file. The node is prevented from making its own updates to the database. Restarting the Jazz for Service Management application server instance on the node resolves most synchronization issues. Otherwise, the node must be removed from the cluster for corrective actions. For more information, see "Maintaining a load balanced cluster" on page 53.

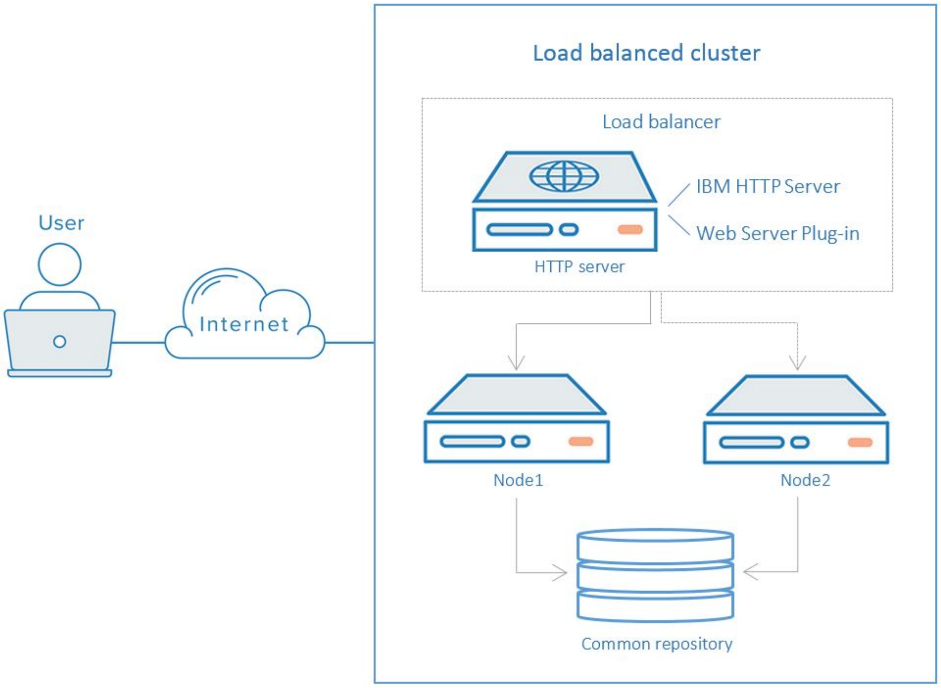
Load balancing
The web server plug-in dispatches workload to different nodes by using the round robin method. When a browser connects to the HTTP server, it is directed to one of the configured nodes. When another browser connects to this HTTP server, it is directed to a different node.

SMU failover
When one of the nodes in the cluster fails, the workload is redirected to other active nodes, and thus eliminate single point of failure in the infrastructure.

Note: Workload is distributed by session, not by request. If a node in the cluster fails, users who are in session with that node must log back in to access the Dashboard Application Services Hub. Any unsaved work is not recovered.

What makes SMU High Availability?

To set up a high available Service Management Unite, you need at least two servers for running Dashboard Application Services Hub (DASH), and one server for DB2, IBM HTTP Server and Web Server Plug-ins. The following diagram shows a Service Management Unite instance deployed in a high availability environment:



To set up a high available environment, complete the following steps:

1. Go through the tasks that are described in Chapter 4, “Installing and uninstalling SMU Automation,” on page 17 to install Service Management Unite Automation on at least two servers.
   a. Install Jazz for Service Management and WebSphere Application Server.
   b. Optional: Configure Jazz for Service Management to use the LDAP for a central user registry.

      Note:

      - For ease of operation, it's highly recommended to configure the LDAP registry before you install Service Management Unite Automation.
      - Each node in the cluster must be enabled to use the same LDAP with the same user and group configuration.

   c. Install SMU Automation.

      Note:

      - When you install Service Management Unite and the related prerequisites, you must ensure all the user IDs and passwords are the same on different servers.
2. Go through the information in this chapter to complete the other steps.

Creating a common repository

In an HA environment, a common repository is used to store the console changes. These changes are synchronized to all of the nodes in the cluster using a common database.

Before you begin

If you do not have an existing supported DB2 installation, install the IBM DB2 server. See Installing DB2 database servers in the IBM DB2 Knowledge Center.

The DB2® database manager must be running before you create database instances. Issue the following command to start the database manager:

```
db2start
```

Procedure

1. Log in to the DB2 server. The default user ID is **db2inst1**.
2. Issue the following command to create a DB2 database:

   ```
   db2 create database database_name
   ```

   The database is shared as a common repository for SMU servers. The database administrator must have the authority to create tables.
3. To view the detailed information of the database that you create, issue the following command:

   ```
   db2 list database directory
   ```

Preparing the DASH nodes for load balancing

A load balanced cluster includes at least two nodes that share information through common repository. Use this information to create and configure a load balanced cluster.

1. "Setting up a load balanced cluster" on page 37.
2. "Adding other nodes to a load balanced cluster" on page 39.
   a. "Exporting data from a DASH server" on page 41.
   b. "Importing data to the cluster" on page 41.
3. "Enabling server-to-server trust" on page 42.
4. "Verifying the load balancing implementation in DASH" on page 43.

For more background information on configuring load balancing for the Dashboard Application Service Hub, refer to Load balancing for Dashboard Application Services Hub.

Setting up a load balanced cluster

Load balancing is ideal for Dashboard Application Services Hub installations with a large user population. When a node in a cluster fails, new user sessions are directed to other active nodes. To enable load balancing, you must create a load balanced cluster first.

Procedure

1. Check that you have the JDBC driver for DB2 on the server where Dashboard Application Services Hub is installed. The JDBC driver is available at:

   JazzSM_HOME/lib/db2

   The default directory of *JazzSM_HOME* is /opt/IBM/JazzSM.
2. Log in to **WebSphere Administrative Console**.
3. Create a JDBC provider for the DASH server.
   a) On the navigation bar, click **Resources** > **JDBC** > **JDBC providers** to open the **JDBC providers** page.
   b) From the drop-down list of **Scope**, select the server scope where Dashboard Application Services Hub is installed, for example, Node=JazzSMNode01, Server=server1.
   c) Click **New...** to open the **Create a new JDBC Provider** pane.
   d) Complete the fields to set the basic configuration of a JDBC provider and click **Next**.

    - Select DB2 as the database type.
    - Select `DB2 Universal JDBC Driver Provider` as the provider type.
    - Select `Connection pool data source` as the implementation type.
    - Accept the default name of the provider or specify a new name.

   e) In pane **Step 2: Enter database class path information**, set the class path, directory location, and native library path.

      For example:

    - Class path:

      ```
      ${DB2UNIVERSAL_JDBC_DRIVER_PATH}/db2jcc.jar
      ${UNIVERSAL_JDBC_DRIVER_PATH}/db2jcc_license_cu.jar
      ${DB2UNIVERSAL_JDBC_DRIVER_PATH}/db2jcc_license_cisuz.jar
      ```

    - Directory location for "db2jcc_license_cisuz.jar": *JazzSM_HOME*`/lib/db2`.
    - Native library path: *JazzSM_HOME*`/lib/db2`.

   f) Click **Next** to go over a summary of the actions. If all the settings are correct, click **Finish**.

   g) Click **Save** to save all your changes.

      A new JDBC provider is created.

4. Create a data source for the DASH server.

   a) On the navigation bar, click **Resources** > **JDBC** > **Data sources** to open the **Data sources** page.

   b) From the drop-down list of **Scope**, select the server scope where Dashboard Application Services Hub is installed, for example, `Node=JazzSMNode01, Server=server1`.

   c) Click **New...** to open the **Create a data source** pane.

   d) Complete the fields to set the basic configuration of a data source, and then click **Next** to proceed.

    - In the **Name** field, type `tipds`.
    - In the **JNDI Name** field, type the name of Java™ Naming and Directory Interface (JNDI), for example, `jdbc/tipds`.

      The application server uses the JNDI name to bind resource references for an application to this data source.

   e) In pane **Step 2: Select JDBC provider**, select the JDBC provider that you created, for example, `DB2 Universal JDBC Driver Provider`.

   f) In pane **Step 3: Enter database specific properties for the data source**, set the following properties:

      i) Driver type: 4

      ii) Type the database name, server name, and port number that is created in DB2 server.

      iii) Check the **CMP** check box.

   g) In pane **Step 4: Setup security aliases**,

      right-click the link **Global J2C authentication alias** and click **Open Link in New Tab**. The J2C authentication data pane is displayed.

      i) Click **New** to define a new alias.

      ii) Specify the properties for Java Connector security to use. The J2C authentication alias must be created using a DB2 user ID that has the authority to create and modify database tables.

      iii) Click **OK** to save your settings.

   h) Go back to the **Create a data source** pane, and select the authentication values for the data resource. For example,

    - Select `JazzSMNode01/db2inst1` as the Component-managed authentication alias.
    - Select `DefaultPrincipalMapping` as the Mapping-configuration alias.

- Select JazzSMNode01/db2inst1 as the Container-managed authentication alias.

i) Go through the summary of actions, and click **Finish** to save the configuration and exit the pane.

j) Click **Save** to save all the changes to the master configuration.

5. Restart the DASH server.

   For example, in the *JazzSM_HOME*/profile/bin directory, for a server that is named *server1*, issue the following commands to stop and start the server:

```
./stopServer.sh server1
./startServer.sh server1
```

Results

The load balanced cluster is created and the DASH node is added to the cluster as the first node.

What to do next

Add other DASH nodes to the cluster.

Adding other nodes to a load balanced cluster

A load balanced cluster includes more than one node so that user sessions can be evenly distributed. Add other nodes after you set up the cluster.

Before you begin

- If you add a node that contains custom data, ensure that you export all of its data first. For information about how to export data from a server, see “Exporting data from a DASH server” on page 41.
- Make sure that a load balanced cluster is created as described in Setting up a load balanced cluster.
- If the cluster uses any customization changes in consoleProperties.xml, copy the customized consoleProperties.xml to the same location on the node that you want to add.

Procedure

1. Check that you have the JDBC driver for DB2 on the server where Dashboard Application Services Hub is installed. The JDBC driver is available at:

   JazzSM_HOME/lib/db2

   The default directory of *JazzSM_HOME* is /opt/IBM/JazzSM.
2. Log in to **WebSphere Administrative Console**.
3. Create a JDBC provider for the DASH server.

   a) On the navigation bar, click **Resources** > **JDBC** > **JDBC providers** to open the **JDBC providers** page.

   b) From the drop-down list of **Scope**, select the server scope where Dashboard Application Services Hub is installed, for example, Node=JazzSMNode01, Server=server1.

   c) Click **New...** to open the **Create a new JDBC Provider** pane.

   d) Complete the fields to set the basic configuration of a JDBC provider and click **Next**.

   - Select DB2 as the database type.
   - Select DB2 Universal JDBC Driver Provider as the provider type.
   - Select Connection pool data source as the implementation type.
   - Type the name of the provider in the **Name** field.

   e) In pane **Step 2: Enter database class path information**, set the class path, directory location, and native library path.

   For example:

- Class path:

  ```
  ${DB2UNIVERSAL_JDBC_DRIVER_PATH}/db2jcc.jar
  ${UNIVERSAL_JDBC_DRIVER_PATH}/db2jcc_license_cu.jar
  ${DB2UNIVERSAL_JDBC_DRIVER_PATH}/db2jcc_license_cisuz.jar
  ```

- Directory location for "db2jcc_license_cisuz.jar": *JazzSM_HOME*`/lib/db2`.
- Native library path: *JazzSM_HOME*`/lib/db2`.

f) Click **Next** to go over a summary of the actions. If all the settings are correct, click **Finish**.

g) Click **Save** to save all your changes.

A new JDBC provider is created.

4. Create a data source for the DASH server.

a) On the navigation bar, click **Resources** > **JDBC** > **Data sources** to open the **Data sources** page.

b) From the drop-down list of **Scope**, select the server scope where Dashboard Application Services Hub is installed, for example, `Node=JazzSMNode01, Server=server1`.

c) Click **New...** to open the **Create a data source** pane.

d) Complete the fields to set the basic configuration of a data source, and then click **Next** to proceed.

- In the **Name** field, type `tipds`.
- In the **JNDI Name** field, type the name of Java™ Naming and Directory Interface (JNDI), for example, `jdbc/tipds`.

  The application server uses the JNDI name to bind resource references for an application to this data source.

e) In pane **Step 2: Select JDBC provider**, select the JDBC provider that you created, for example, `DB2 Universal JDBC Driver Provider`.

f) In pane **Step 3: Enter database specific properties for the data source**, set the following properties:

i) Driver type: 4

ii) Type the database name, server name, and port number that is created in DB2 server.

iii) Check the **CMP** check box.

g) In pane **Step 4: Setup security aliases**,

right-click the link **Global J2C authentication alias** and click **Open Link in New Tab**. The J2C authentication data pane is displayed.

i) Click **New** to define a new alias.

ii) Specify the properties for Java Connector security to use. The J2C authentication alias must be created using a DB2 user ID that has the authority to create and modify database tables.

iii) Click **OK** to save your settings.

h) Go back to the **Create a data source** pane, and select the authentication values for the data resource. For example,

- Select `JazzSMNode01/db2inst1` as the Component-managed authentication alias.
- Select `DefaultPrincipalMapping` as the Mapping-configuration alias.
- Select `JazzSMNode01/db2inst1` as the Container-managed authentication alias.

i) Go through the summary of actions, and click **Finish** to save the configuration and exit the pane.

j) Click **Save** to save all the changes to the master configuration.

5. Restart the DASH server.

For example, in the *JazzSM_HOME*/profile/bin directory, for a server that is named *server1*, issue the following commands to stop and start the server:

```
./stopServer.sh server1
./startServer.sh server1
```

Results

The DASH node is successfully added to the cluster.

Exporting data from a DASH server

You can export data from an existing stand-alone DASH server to create a data file that can be imported to a load balanced cluster.

About this task

Before you add a node that contains custom data to an existing cluster, you must export the data first. The exported data is later imported to one of the nodes in the cluster so that it is replicated across the other nodes in the cluster.

Procedure

1. Browse to the directory: *DASH_HOME*/bin/. The default directory of *DASH_HOME* is /opt/IBM/JazzSM/ui.
2. Issue the following command (as one line) to export the custom data from the DASH server:

   ```
   ./consolecli.sh export --username console_admin_user_ID --password console_admin_password
    --destination data_file
   ```

   Where:

   console_admin_user_ID
   Specifies the administrator user ID.

   console_admin_password
   Specifies the password that is associated with the administrator user ID.

   data_file
   Specifies the path and file name of the exported data, for example, /opt/IBM/JazzSM/data.tar.

What to do next

After you export the custom data, join the node to the cluster and then import custom data to the nodes in the cluster.

Importing data to the cluster

After you export custom data from a node and add the node to the cluster, you can import the data to any node in the cluster. The data will be replicated across the cluster.

Procedure

1. Browse to the directory: *DASH_HOME*/bin/. The default directory of *DASH_HOME* is /opt/IBM/JazzSM/ui.
2. Issue the following command (as one line) to import the custom data from the node:

   ```
   ./consolecli.sh import --username console_admin_user_ID --password console_admin_password
    --source data_file
   ```

   Where:

console_admin_user_ID
Specifies the administrator user ID.

console_admin_password
Specifies the password that is associated with the administrator user ID.

data_file
Specifies the path and file name of the data file to be imported, for example, `/opt/IBM/JazzSM/data.tar`.

Results

The data is imported and replicated across the other cluster nodes.

Enabling server-to-server trust

To enable nodes to connect to each other and send notifications, you must update SSL properties files for all nodes and retrieve signers to enable trust.

Procedure

1. Browse to the directory *JazzSM_WAS_Profile*/`properties` and open the `ssl.client.props` file.

   The default directory of *JazzSM_WAS_Profile* is `/opt/IBM/JazzSM/profile`.
2. Uncomment the section that starts with `com.ibm.ssl.alias=AnotherSSLSettings`, for example,

```
com.ibm.ssl.alias=AnotherSSLSettings
com.ibm.ssl.protocol=SSL_TLS
com.ibm.ssl.securityLevel=HIGH
com.ibm.ssl.trustManager=IbmX509
com.ibm.ssl.keyManager=IbmX509
com.ibm.ssl.contextProvider=IBMJSSE2
com.ibm.ssl.enableSignerExchangePrompt=true
com.ibm.ssl.keyStoreClientAlias=default
com.ibm.ssl.customTrustManagers=
com.ibm.ssl.customKeyManager=
com.ibm.ssl.dynamicSelectionInfo=
com.ibm.ssl.enabledCipherSuites=
```

3. Uncomment the section that starts with `# TrustStore information`, for example,

```
# TrustStore information
com.ibm.ssl.trustStoreName=AnotherTrustStore
com.ibm.ssl.trustStore=${user.root}/etc/trust.p12
com.ibm.ssl.trustStorePassword={xor}CDo9Hgw=
com.ibm.ssl.trustStoreType=PKCS12
com.ibm.ssl.trustStoreProvider=IBMJCE
com.ibm.ssl.trustStoreFileBased=true
com.ibm.ssl.trustStoreReadOnly=false
```

4. Update the value of **`com.ibm.ssl.trustStore`** in the `# TrustStore information` section. This property value represents the location of the trust store that the signer should be added to, for example,

```
com.ibm.ssl.trustStore=${user.root}/config/cells/JazzSMNode01Cell/nodes/JazzSMNode01/
trust.p12
```

5. Save and exit the `ssl.client.props` file.
6. Restart the server.

   In the *JazzSM_HOME*/`profile/bin` directory, for a server that is named *server1*, issue the following command to stop and start the server:

```
./stopServer.sh server1
./startServer.sh server1
```

7. Repeat steps 1-6 on all the nodes before you continue with the next steps.
8. Issue the following command (as one line) on each node to enable trust with each other in the cluster.

```
JazzSM_WAS_Profile/bin/retrieveSigners.sh NodeDefaultTrustStore AnotherTrustStore
 -host myremotehost -port remote_SOAP_port
```

Where

myremotehost
The name of the computer to enable trust with

remote_SOAP_port
The SOAP connector port number. The default value is 16313. If you installed with non-default ports, check the value of **SOAP_CONNECTOR_ADDRESS** in file `JazzSM_WAS_Profile/properties/portdef.props`.

9. Restart the servers.

Verifying the load balancing implementation in DASH

After you add all the nodes into the cluster and enable server-to-server trust, verify that the DASH load balancing setup is working correctly.

About this task

You can verify the following functions through the verification process:

- The database that is used for the load balanced cluster is properly created and initialized.
- Every node in the cluster uses the database instead of its own local file system as its repository.
- Server-to-server trust is properly enabled between nodes in the cluster.

Procedure

1. Ensure that each JazzSM application server on every node in the cluster is running.

   To check the server status, change to the directory *JazzSM_HOME*`/profile/bin` and issue the following command:

   ```
   ./serverStatus.sh server1
   ```

2. Log in to the web console of any DASH node.
3. Customize the console as needed, for example, create a new page and save the changes.
4. Log in to other nodes in the cluster and check if the newly created page is available.

Preparing the HTTP server for load balancing

IBM HTTP Server uses a web server plug-in to dispatch HTTP requests to the Jazz for Service Management application server. Install and configure the HTTP server and web server plug-in to act as the load balancing server to pass requests (HTTPS or HTTP) to the nodes in the cluster.

Procedure

1. "Installing IBM HTTP Server and Web Server Plug-ins" on page 44.
2. "Creating web server definitions" on page 45.
3. "Creating a CMS-type key database" on page 46.
4. Create a self-signed certificate to allow SSL connections between nodes.
5. "Enabling SSL communication" on page 47.
6. "Verifying SSL communication" on page 48.

Installing IBM HTTP Server and Web Server Plug-ins

Use IBM Installation Manager to install IBM® HTTP Server and Web Server Plug-ins for IBM WebSphere Application Server.

Before you begin

Before you install IBM HTTP Server and Web Server Plug-ins, ensure that you installed IBM Installation Manager.

Procedure

1. Add the product repositories to Installation Manager preferences.

   Note: Jazz for Service Management bundles the WebSphere Application Server Version 8.5 Supplements installation media, which contains the installation packages for IBM HTTP Server and the IBM HTTP Server plug-in for IBM WebSphere Application Server. If you do not have the DVDs, you can download the electronic images for Jazz for Service Management, see Downloading Jazz for Service Management.

   a) Start Installation Manager.

   b) Select **File** > **Preferences**, and then click **Add repository**.

   c) Browse to the directory where you extracted the installation packages of IBM HTTP Server and Web Server Plug-ins, and select the following repository files:

   - `diskTag.inf` from the JDK directory, for example, `/`*`WAS_DIR`*`/`*`version_number`*`/java8/disk1/diskTag.inf`. It is used to install the required Java SDK.

     Note: For new installations of IBM HTTP Server version 8.5.5.11 and later, the default Java SDK is Java SE 8. Java 8 is the recommended Java SDK because it provides the latest features and security updates. You can continue to use Java SE 6, but no service can be provided after the end of support in April 2018, which might expose your environment to security risks.
   - `repository.config` from `/`*`WAS_DIR`*`/`*`version_number`*`/supplements/ihs/`, which is used to install IBM® HTTP Server.
   - `repository.config` from `/`*`WAS_DIR`*`/`*`version_number`*`/supplements/plugins/`, which is used to install Web Server Plug-ins.
   - `repository.config` from `/`*`WAS_DIR`*`/`*`version_number`*`/supplements/wct/`, which is used to install WebSphere Customization Toolbox.

     Note: For IBM HTTP Server for WebShere Application Server V8 and later, you must install WebSphere Customization Toolbox together to do further configuration.

   d) Click **OK** to save and exit the **Preferences** pane.
2. In the Installation Manager pane, click **Install**.

   Installation Manager searches its defined repositories for available packages.
3. In the **Install Packages** pane, select the following products to install, and then click **Next**.
   - IBM HTTP Server for WebSphere Application Server
   - Web Server Plug-ins for IBM WebSphere Application Server
   - WebSphere Customization Toolbox
4. Accept the terms in the license agreements and click **Next**.
5. Specify a path in the **Shared Resources Directory** field, or use the default path `/opt/IBM/IMShared`, and then click **Next**.

   The shared resources directory is the directory where installation artifacts are stored so that they can be used by one or more product package groups. You can specify the shared resources directory only when you install a package for the first time.
6. Specify the installation root directory for the product binary files, which are also referred to as the core product files or system files. The default directory is `/opt/IBM/HTTPServer`.

7. If you install IBM HTTP Server on a 64-bit system, choose a 32-bit or 64-bit HTTP server environment and click **Next**.

   Note:

   - This option is displayed only if you install on a 64-bit system. You cannot modify this installation later and change this selection.
   - This option does not apply to Solaris x86 64-bit systems.
8. Select the translations to install and click **Next**.
9. Select the features to install and click **Next**.

   By default, all the features are selected. You can deselect the products if you don't need them. For example, if you don't need to build and process definitions for creating or migrating WebSphere Application Server profiles, clear the selection of Profile Management Tool (z/OS only) and z/OS Migration Management Tool.
10. In the **Common Configurations** pane, specify the HTTP port number for IBM HTTP Server to communicate, and then click **Next**. The default port is 80.
11. Review the summary information and click **Install**.

    A message indicating that installation is successful is displayed if no errors occurr. Otherwise, click **View Log File** to troubleshoot the problem.
12. Click **Finish** to exit.

Results

IBM HTTP Server and Web Server Plug-ins are successfully installed.

Creating web server definitions

Use the WebSphere Customization Toolbox to configure the web server plug-in. The Web Server Plug-ins Configuration Tool creates web server definitions in a default profile.

Procedure

1. Browse to the default directory `/opt/IBM/WebSphere/Toolbox/WCT` and issue the following command to start WebSphere Customization Toolbox:

   ```
   ./wct.sh
   ```
2. Select **Web Server Plug-ins Configuration Tool** and click **Launch Selected Tool**.
3. In tab **Web Server Plug-in Runtime Locations**, click **Add** to add a web server plug-in location to the working set.
   a) Type the name of the web server plug-in in the **Name** field.
   b) Click **Browse** to select the location of the installed web server plug-ins. For example, the default path is `/opt/IBM/WebSphere/Plugins`.
   c) Click **Finish**.
   The web server plug-in location is successfully added.
4. In tab **Web Server Plug-in Configurations**, click **Create** to create a web server definition.
5. In the **Web Server Plug-ins Configuration Tool** wizard, select the web server (IBM HTTP Server) to configure and click **Next**.
6. Select the architecture of the installed web server and click **Next**.
7. Select the web server configuration file and identify the web server port, and then click **Next**. For example,

   - Select the IBM HTTP Server configuration file: `/opt/IBM/HTTPServer/httpd.conf`.
   - Specify the web server port: 80.
8. Set up IBM HTTP Server Administrator Server.

- Select the check box **Set up IBM HTTP Server Administrator Server**.
- Specify a port number for IBM HTTP Server administration server to communicate, for example, `8008`.
- Create a user ID for IBM HTTP Server Administrator authentication. You need to use the credentials created here to connect to IBM HTTP Server Administrator from WebSphere Administrator Console.

9. Specify a system user ID and group. For example,
   - User ID: `1001`.
   - Group: `1001`.
10. Specify a unique web server definition name and click **Next**.
11. Select and specify the configuration scenario.
    - Choose the remote configuration scenario if the web server and the application server are not on the same computer. In the remote scenario, specify the host name of the application server.
    - Choose the local configuration scenario if the web server and the application server are on the same computer. In the local scenario, the web server definition is defined automatically in the application server.
12. Review the plug-in configuration summary and click **Configure**.

    You get a success message if no errors occur during the configuration.

Creating a CMS-type key database

A key database is a file that the web server uses to store one or more key pairs and certificates.

Procedure

Issue the following command (as one line) to create a new key database:

```
<ihsinst>/bin/gskcmd -keydb -create -db <filename> -pw <password>
-type <cms | jks | jceks | pkcsk> -expire <days> -stash
```

Where:

<ihsinst>
The root directory for IBM® HTTP Server. The default value is `/opt/IBM/HTTPServer`.

-keydb -create
The creation of a key database

-db <filename>
The name of the database.

-pw <password>
The password to access the key database.

-type <cms | jks | jceks | pkcsk>
The database type.

Note: IBM HTTP Server supports CMS-type database only.

-expire <days>
The number of days before the password expires. This parameter is valid for only CMS key databases.

-stash
stashes the password for the key database. When the `-stash` option is specified during the key database creation, the password is stashed in a file with a name as follows:

```
<filename_of_key_database>.sth
```

This parameter is valid for only CMS key databases. If the database being created is named `keydb.kdb`, the stash file name is `keydb.sth`.

Note: Stashing the password is required for IBM HTTP Server.

Creating a self-signed certificate

A self-signed certificate provides a certificate to enable Secure Sockets Layer (SSL) sessions between clients and the server. Creating a self-signed certificate generates a self-signed X509 certificate in the identified key database.

Procedure

Issue the following command (as one line) to create a self-signed certificate:

```
<ihsinst>/bin/gskcmd -cert -create -db <filename> -pw <password>
-size <2048 | 1024 | 512> -dn <distinguished_name>
-label <label> -default_cert <yes | no> - expire <days> -ca <true | false>
```

Where:

-cert -create
The creation of a self-signed certificate.

-db <filename>
The name of the database.

-pw <password>
The password to access the key database.

-dn <distinguished_name>
Indicates an X.500 distinguished name. Enter a quoted string of the following format:

"CN=weblinux.raleigh.ibm.com,O=IBM,OU=IBM HTTP Server,L=RTP,ST=NC,C=US", of which only CN, O, and C are required.

-label <label>
A descriptive comment that is used to identify the certificate in the database.

-size <2048 | 1024 | 512>
Indicates a key size of 2048, 1024, or 512. The default key size is 1024. The 2048 key size is available if you are using Global Security Kit (GSKit) Version 7.0.4.14 and later.

-default_cert <yes | no>
Specifies whether this is the default certificate in the key database.

-expire <days>
The number of days before the new self-signed digital certificates expires. The minimum is 1 day and the maximum is 7300 days.

-ca <true | false>
specifies the basic constraint extension to the self-signed certificate. If you set CA:true, the extension is added with a CA:true and PathLen:<max int>. Otherwise, they are not added.

Enabling SSL communication

SSL ensures the data that is transferred between a client and a server remains private. To set up SSL communication, enable the SSL directives in the IBM® HTTP Server configuration file.

Procedure

1. Browse to the directory where the IBM HTTP Server configuration file httpd.conf locates. The default directory is /opt/IBM/HTTPServer/conf/httpd.conf.
2. Open the configuration file and locate the line # End of example SSL configuration.
3. Before the line # End of example SSL configuration, add the following lines in the configuration file and ensure that KeyFile and SSLStashfile reference the key database files that are created in task "Creating a CMS-type key database" on page 46.

```
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
Listen 443
<VirtualHost *:443>
```

```
SSLEnable
SSLProtocolDisable SSLv2
ErrorLog "/opt/IBM/HTTPServer/logs/sslerror.log"
TransferLog "/opt/IBM/HTTPServer/logs/sslaccess.log"
KeyFile "/opt/IBM/HTTPServer/smuha.kdb"
SSLStashfile "/opt/IBM/HTTPServer/smuha.sth"
</VirtualHost>
SSLDisable
```

For more information about the `httpd.conf` file, see Securing with SSL communications.

4. Save and exit the configuration file.
5. Restart IBM® HTTP Server:

   In the *HTTP_SERVER_PATH*`/bin` directory, issue the following commands to stop and start the IBM HTTP Server:

   ```
   ./apachectl stop
   ./apachectl start
   ```

Verifying SSL communication

SSL enables the client to authenticate the identity of the server. To verify that the SSL communication is enabled, run SSL requests using HTTPS to request an SSL-protected document.

Procedure

Open the browser and enter the url `https://localhost`.

You can access to the IBM HTTP Server page if SSL is successfully enabled.

Setting clone IDs for DASH nodes

To distinguish different nodes in the cluster, set a unique clone ID for each node.

Procedure

1. Log in to the node for which you want to set the clone ID. .
2. Browse to the directory *JazzSM_WAS_Profile*`/config/cells/JazzSMNode01Cell/nodes/JazzSMNode01/servers/server1` and open `server.xml`.

   The default directory of *JazzSM_WAS_Profile* is `/opt/IBM/JazzSM/profile`.
3. Add the following line to the `<components xmi:type="applicationserver.webcontainer:WebContainer` section:

   ```
   <properties xmi:id="WebContainer_1183077764084" name="HttpSessionCloneId" value="12345"
   required="false"/>
   ```

   Where:

   `value` is the clone ID for the node. The clone ID must be unique. See the following example of an updated `<components>` section:

   ```
   <components xmi:type="applicationserver.webcontainer:WebContainer"
   xmi:id="WebContainer_1183077764084" enableServletCaching="false" disablePooling="false">
   <stateManagement xmi:id="StateManageable_1183077764087" initialState="START"/>
   <services xmi:type="applicationserver.webcontainer:SessionManager"
    xmi:id="SessionManager_1183077764084" enable="true" enableUrlRewriting="false"
    enableCookies="true" enableSSLTracking="false" enableProtocolSwitchRewriting="false"
    sessionPersistenceMode="NONE" enableSecurityIntegration="false"
    allowSerializedSessionAccess="false" maxWaitTime="5" accessSessionOnTimeout="true">
    <defaultCookieSettings xmi:id="Cookie_1183077764084"domain=""
   maximumAge="-1"secure="false"/>
    <sessionDatabasePersistence xmi:id="SessionDatabasePersistence_1183077764084"
    datasourceJNDIName="jdbc/Sessions" userId="db2admin" password="{xor}Oz1tPjsyNjE="
    db2RowSize="ROW_SIZE_4KB" tableSpaceName=""/>
    <tuningParams xmi:id="TuningParams_1183077764084" usingMultiRowSchema="false"
    maxInMemorySessionCount="1000" allowOverflow="true"
   ```

```
scheduleInvalidation="false"
 writeFrequency="TIME_BASED_WRITE" writeInterval="10"
writeContents="ONLY_UPDATED_ATTRIBUTES"
 invalidationTimeout="30">
 <invalidationSchedule xmi:id="InvalidationSchedule_1183077764084"
 firstHour="14" secondHour="2"/>
 </tuningParams>
 </services>
<properties xmi:id="WebContainer_1183077764084" name="HttpSessionCloneId" value="12345"
required="false"/>
</components>
```

4. Save the changes.
5. Repeat the previous steps for all the nodes in the cluster.

Updating the `plugin-cfg.xml` file

The `plugin-cfg.xml` file determines how the web server plug-in forwards requests. To configure the web server plug-in, update the `plugin-cfg.xml` file.

Procedure

1. Log in to one of the nodes in the cluster.
2. Browse to the directory *JazzSM_WAS_Profile*/bin/ and issue the following command:

   ```
   ./GenPluginCfg.sh
   ```

   This command generates a `plugin-cfg.xml` file and saves it to the *JazzSM_WAS_Profile*/config/cells directory.
3. Complete the previous steps for all the nodes in the cluster.
4. Log in to the HTTP server.
5. Browse to the directory *HTTP_web_server_install_dir*/plugins/config/webserver1 and replace the existing `plugin-cfg.xml` file with the one that is generated in step 2.
6. Edit the new `plugin-cfg.xml` file to include server information that is copied from the generated `plugin-cfg.xml` file on each node in the cluster.

   a. Copy the `<server>` section from the `plugin-cfg.xml` file on each DASH server and add the entry into the `ServerCluster` section.

      The value of `keyring` in the **<Property>** section must be HTTP_web_server_install_dir/plug-ins/etc/*xxx*.kdb and the value of `stashfile` in the **<Property>** attribute must be HTTP SERVER PATH /plug-ins/etc/*xxx*.sth.

   b. Add an entry in section `PrimaryServers` for each additional DASH server.

   See the following example of the updated section:

   ```
    <ServerCluster CloneSeparatorChange="false" GetDWLMTable="false"
   IgnoreAffinityRequests="false"
   LoadBalance="Round Robin" Name="server1_JazzSMNode01_Cluster" PostBufferSize="0"
   PostSizeLimit="-1" RemoveSpecialHeaders="true" RetryInterval="60" ServerIOTimeoutRetry="-1">
   <Server CloneID="19216820017" ConnectTimeout="0" ExtendedHandshake="false"
   MaxConnections="-1" Name="JazzSMNode01_server1" ServerIOTimeout="900"
   WaitForContinue="false">
            <Transport Hostname="smuha-server05" Port="16310" Protocol="http"/>
            <Transport Hostname="smuha-server05" Port="16311" Protocol="https">
               <Property Name="keyring" Value="/opt/IBM/WebSphere/Plugins/etc/plugin-key.kdb"/>
               <Property Name="stashfile" Value="/opt/IBM/WebSphere/Plugins/etc/plugin-
   key.sth"/>
            </Transport>
   </Server>
   <Server CloneID="19216820018" ConnectTimeout="0" ExtendedHandshake="false"
   MaxConnections="-1" Name="JazzSMNode02_server1" ServerIOTimeout="900"
   WaitForContinue="false">
            <Transport Hostname="smuha-server06" Port="16310" Protocol="http"/>
            <Transport Hostname="smuha-server06" Port="16311" Protocol="https">
               <Property Name="keyring" Value="/opt/IBM/WebSphere/Plugins/etc/plugin-key.kdb"/>
               <Property Name="stashfile" Value="/opt/IBM/WebSphere/Plugins/etc/plugin-
   key.sth"/>
   ```

```
         </Transport>
</Server>
      <PrimaryServers>
         <Server Name="JazzSMNode01_server1"/>
         <Server Name="JazzSMNode02_server1"/>
      </PrimaryServers>
   </ServerCluster>
```

For more information about the `plugin-cfg.xml` file, see plugin-cfg.xml file.

7. If the DNS server can't parse the names of the nodes, add the mapping relationship in the `hosts` file, for example,

```
192.168.200.17 smuha-server05 smuha-server05.cn.ibm.com
```

Configuring SSL from each node to the IBM HTTP Server

After you install and configure IBM HTTP Server for load balancing, configure SSL between the IBM HTTP Server plug-ins and each node in the cluster.

Procedure

1. Log in to the **WebSphere Administrative Console** of one node.
2. Follow these steps to extract signer certificate from the truststore in node:
   a) In the console navigation pane, click **Security** > **SSL certificate and key management**.
   b) In the **Related Items** area, click **Key stores and certificates**.
   c) In the table, select **NodeDefaultTrustStore**.
   d) In the **Additional Properties** area, click **Signer certificates**.
   e) In the table, select the **root** check box and click **Extract**.
   f) In the **File name** field, enter a certificate file name, for example, `/root/certificate_`*`hostname`*`.arm`.
   g) From the **Data Type** list, select **Base64-encoded ASCII data** and click **OK**.
   h) Copy the extracted signer certificate to the server that IBM HTTP Server is running.
3. Follow these steps to import the extracted signer certificate into the key database on the HTTP server.
   a) Browse to the directory `/`*`HTTP_SERVER_PATH`*`/bin` and issue the following command to start the Key Management Utility (iKeyman):

   ```
   ./ikeyman
   ```

   iKeyman is a component of the IBM SDK that generates keys, certification requests, and self-signed certificates. You can use iKeyman to create certificates to secure communications, and to encrypt and decrypt data.
   b) Select **Key Database File** > **Open**. The open box is displayed.
   c) Select the CMS key database file that is specified in the configuration file `plugin-cfg.xml` and click **OK**.

   For example,

   - **Key database type**: `CMS`
   - **File Name**: `plugin-key.kdb`
   - **Location**: `/opt/IBM/WebSphere/Plugins/etc`

   d) In the **Password Prompt** window, enter the password for the key database and click **OK**. The default value is `WebAS`.
   e) From the **Key database content** drop-down list, select **Signer Certificates**.
   f) Click **Add** and select the signer certificate that you copied from the node, and then click **OK**.
   g) In the prompt window, enter a descriptive label for the certificate and click **OK**.

The signer certificate is successfully imported into the key database.

h) Select **Key Database File** > **Stash Password** and click **OK** in the prompt window. The password has been encrypted and saved in the stash file.

4. Repeat the previous steps for all the nodes in the cluster.
5. Restart all the nodes in the cluster.

   In the `*JazzSM_HOME*/profile/bin` directory, for a server that is named *server1*, issue the following commands to stop and start the server:

   ```
   ./stopServer.sh server1
   ./startServer.sh server1
   ```

6. Restart IBM HTTP Server:

   In the `*HTTP_SERVER_PATH*/bin` directory, issue the following commands to stop and start IBM HTTP Server:

   ```
   ./apachectl stop
   ./apachectl start
   ```

Results

You can access the load balanced cluster through `https://*http_server_hostname*/ibm/console` if the cluster is configured successfully.

Configuring an Event Integration Facility Event Dispatcher

The Event Integration Facility (EIF) event dispatcher forwards events that come from end-to-end adapter (E2E adapter) to the Service Management Unite servers. Use this information to customize the EIF configuration files.

Procedure

1. On the server where Service Management Unite is installed, browse to the following directory: `/opt/IBM/smsz/ing/EIFEventDispatcher`.
2. Extract the file `eezeifeventdispatcher.tar.gz` to a server where both the E2E adapter and the Service Management Unite servers can access, for example, the HTTP server.
3. Specify the following parameters in `receive.conf` to configure settings for the EIF event dispatcher to receive data from the E2E adapter:

   ServerLocation

   The host name of the server where the EIF Event Dispatcher is running. Typically, you can leave the default value: `localhost`.

   SpaceReplacement

   The spaces in the EIF event log are replaced by an underscore if you set `SpaceReplacement=TRUE`.

   ServerPort

   The port number on which the EIF event dispatcher listens for EIF events from the E2E adapter. The default value is `2002`.

   ConnectionMode

   The mode of IP connection. The supported values are as follows:

   - `connection_less`: A new connection is established and ended for each event that is sent.
   - `Connection_oriented`: A connection is established when the event dispatcher is initialized, and is maintained for all events that are sent. A new connection is established only if the connection is lost.

   EventMaxSize

   The maximum number of EIF event messages.

BufEvtPath
The location of an EIF buffer cache where the event dispatcher writes events.

4. Configure settings for the EIF event dispatcher to forward data to SMU servers.
   a) Go to the directory `EEZEIFEventDispatcher`, and rename file `send.conf` to `send.conf.bak`.
   b) Create a folder and name it as `send.conf`.
   c) Create as many copies of the `send.conf.bak` file as the number of SMU servers, and then save as the *`xxx`*`.conf` files in the `send.conf` folder.

      The extension name of the new files must be `.conf`.
   d) Specify the parameters **`ServerLocation`**, **`ServerPort`**, and **`BufEvtPath`**in the configuration file *`xxx`*`.conf` for each SMU server.

      ServerLocation
      The host name of the server where the SMU server is running.

      ServerPort
      The port number on which the EIF event dispatcher forwards data to the SMU server. The default value is `2002`.

      BufEvtPath
      The location of an EIF buffer cache where the event dispatcher writes events.

      Note: For each SMU server, specify its own EIF buffer cache file. Different SMU servers cannot share the same EIF buffer cache file.
5. Issue the command to start the EIF event dispatcher service:

```
./eifEventDispatcher.sh receive.conf send.conf
```

Verifying the implementation of HA setup

To verify the implementation of HA setup, trace logs to check whether load balancing and failover can be fulfilled.

Before you begin

To collect detailed logs from the web server, you must define the trace information. To enable tracing logs, complete the following steps:

1. Log in to the HTTP server.
2. Browse to the directory where `plugin-cfg.xml` locates and open this file.

   The default directory is `/opt/IBM/WebSphere/Plugins/config/webserver1`.
3. Locate the line `<Log LogLevel = "Error"` and change the value of **`LogLevel`** from `Error` to `Trace`.
4. Restart IBM HTTP Server.
5. Issue the following command to start tracing:

```
tail -f <plugins_root>/logs/http_plugin.log | grep STATS
```

   The default directory of `<plugins_root>` is `/opt/IBM/WebSphere/Plugins`.

Procedure

1. To verify the implementation of load balancing, check whether the requests are directed to different nodes when multiple users log in to SMU console.
   a) On different servers, log in to SMU consoles through `https://`*`<httpserver_hostname>`*`/ibm/console`.
   b) Check the logs in `http_plugin.log` to see which nodes the requests are directed to.

The load balancing is fulfilled if the requests are directed to different nodes.

2. To verify the implementation of failover, check whether the requests are directed to other active nodes when a running node fails.

   a) Log in to SMU console.

   b) Check the logs in `http_plugin.log` to see which node the requests are directed to.

   c) Stop the node that the requests are directed to.

   d) Select and click any menu in SMU console.

   The failover is fulfilled if the login page is displayed, and the requests are directed to another active node.

Maintaining a load balanced cluster

Use the load balancing **consolecli** commands to analyze and update the nodes in the cluster.

The consolecli.sh commands for maintaining the cluster are available at *DASH_HOME*/bin. The default directory of *DASH_HOME* is /opt/IBM/JazzSM/ui.

- To list the component modules in the cluster, issue the **ListHAModules** command (as one line):

  ```
  ./consolecli.sh ListHAModules --username console_admin_user_ID --password
  console_admin_password [--nodename true|false]
  ```

  Where:

  nodename is an optional parameter to the **ListHAModules** command. When you set it as true, the local component modules are also listed. Otherwise, only modules from the database are listed.

- To list the current nodes in the cluster, determine whether they are active or not, view their synchronization status and their version level of Dashboard Application Services Hub, issue the **ListHANodes** command:

  ```
  ./consolecli.sh ListHANodes --username console_admin_user_ID --password console_admin_password
  ```

- To refresh the node with the latest content from the database, issue the **ForceHARefresh** command:

  ```
  ./consolecli.sh ForceHARefresh --username console_admin_user_ID --password
  console_admin_password
  ```

  The **ForceHARefresh** command exports data from the database and imports it to the local node. The database module version for Dashboard Application Services Hub must be lower than the local node for export and import.

- To force a database update after you run the **ForceHARefresh** command, issue the **ForceHAUpdate** command as an administrator:

  ```
  ./consolecli.sh ForceHAUpdate --username console_admin_user_ID --password
  console_admin_password
  ```

  The **ForceHAUpdate** command pushes the local node configuration to the database and updates the modules table to match the local node's module versions. Notifications are sent to other nodes to synchronize. Notified nodes with module versions that match those of the originating nodes are synchronized. Notified nodes with module versions that do not match, go into maintenance mode until an administrator updates their modules accordingly.

- To remove a node from the cluster, issue the **RemoveHANode** command (as one line):

  ```
  ./consolecli.sh RemoveHANode --username console_admin_user_ID --password
  console_admin_password
   [--nodename node_name]|[-- active true|false|unreachable]
  ```

  Where:

active is an optional parameter that is used for cleanup purposes. Supported values are **true**, **false** and **unreachable**.

- true: All the active nodes that are reachable in the database are deleted.
- false: All the inactive nodes in the database are deleted.
- unreachable: All the nodes that are unreachable from that node are deleted.

The **RemoveHANode** command is used to permanently remove a node from the cluster before you delete the WebSphere Application Server data source. If the data source was deleted beforehand, this command can be run from another node to remove a separate node by specifying the relevant server name.

- To remove a node from the cluster without removing it from the cluster, in the WebSphere Application Server administrative console, set the value for com.ibm.isc.ha custom property to false. For more information about the detailed steps, see Disabling a node without removing it from the cluster.

Chapter 6. Upgrading

This information provides the following topics to help you upgrade Service Management Unite to a higher version.

Upgrading SMU with Docker

Use the SMU Docker Command Line Utility to upgrade SMU into a new version.

About this task

To upgrade the SMU components including the prerequisites like WebSphere Application Server with the IBM provided SMU Docker image, theoretically, you only need to load the new IBM provided SMU Docker image into your local Docker environment and create a new SMU Docker container from it. However, as described in "Managing the SMU Docker container" on page 21, the new created SMU Docker container will be factory reset and not automatically contain all the custom configuration that you made to your old SMU Docker container.

As a result, the IBM SMU Docker Command Line Utility provides a migration command that helps you to migrate all of your custom configuration from the old SMU Docker container into the new container from the new SMU release.

The migration process doesn't have any impact to the old SMU Docker image and Docker container. If the migration fails or the new SMU Docker container doesn't run as expected, you can immediately return to the old SMU Docker container – keeping the mean down time of SMU as short as possible.

Starting from SMU V1.1.5, the name of the SMU Docker images will be in the format `<smu_flavor>:<smu_version>`, and the name of the SMU Docker container will be in the format `<smu_flavor>_<smu_version>`,

where *<smu_flavor>* is `smu_auto` (Docker images containing SMU Automation only).

You can keep all the old SMU releases (images and containers) in your Docker environment if you want to return to an older version one day. However, the Docker images and containers consume several GB disk space, it's recommended to remove them if the latest version is successfully migrated and runs as expected.

Note:

- For SMU V1.1.4, the SMU Docker image uses name `<smu_flavor>:latest`, the container uses name `<smu_flavor>` (without a version suffix).
- The name tag '`latest`' is only used for SMU 1.1.4.0. So after a successful migration to the SMU 1.1.5.0 or later Docker image/container, the name `<smu_flavor>:latest` still points to the old SMU 1.1.4.0 Docker – not to the real latest version.

Procedure

1. Download and extract the new SMU Docker image to a temporary folder on the host system.

   Note: The new version of the SMU Docker Command Line Utility (**`eezdocker.sh`**) is included in the package. Use this new utility to migrate, but do NOT overwrite the old **`eezdocker.sh`** from the previous version. You might need the old script if you want to use the old SMU Docker image/container if there is a problem with the migration or the new SMU release.
2. Ensure the old SMU Docker container is running so that the DASH settings can be exported, but no administrative tasks should be done during the migration process.
3. Use the new SMU Docker Command Line Utility to load the SMU Docker image into your Docker environment:

```
eezdocker.sh load
```

4. Use the new SMU Docker Command Line Utility to start the migration process:

   ```
   eezdocker.sh -f 1150 migrate
   ```

   The **`-f`** option tells the **`eezdocker.sh`** script from which version of SMU it migrates. This is for example required to detect the running SMU Docker container of that old version. The migration process automatically completes the following steps:

   a. Exports all the required configuration from the old SMU Docker container.
   b. Stops the old Docker container.
   c. Creates a new Docker container from the new image.
   d. Imports the exported configuration into the new container.
   e. Starts the new container.

   Note: The following configuration data is migrated over from the old SMU Docker container to the new SMU Docker container:

   - All DASH settings.
   - The following files and folders:
     - /opt/IBM/JazzSM/ui/db/restdb
     - /opt/IBM/WebSphere/AppServer/derby/EAUTODB
     - /etc/opt/IBM/smsz/ing
     - /opt/IBM/JazzSM/profile/Tivoli/EEZ
     - /opt/IBM/JazzSM/profile/config/cells/JazzSMNode01Cell/fileRegistry.xml
     - /opt/IBM/JazzSM/profile/config/cells/JazzSMNode01Cell/security.xml
     - /opt/IBM/JazzSM/profile/config/cells/JazzSMNode01Cell/admin-authz.xml
     - /opt/IBM/JazzSM/profile/config/cells/JazzSMNode01Cell/nodes/JazzSMNode01/servers/server1/server.xml
     - /opt/IBM/JazzSM/profile/config/cells/JazzSMNode01Cell/applications/EEZEAR.ear/deployments/EEZEAR/META-INF/ibm-application-bnd.xml
     - /opt/IBM/JazzSM/profile/config/cells/JazzSMNode01Cell/applications/isc.ear/deployments/isc/isclite.war/WEB-INF/isc.dir
     - /opt/IBM/JazzSM/profile/config/cells/JazzSMNode01Cell/wim/config/wimconfig.xml
     - /opt/IBM/JazzSM/profile/config/cells/JazzSMNode01Cell/nodes/JazzSMNode01/key.p12
     - /opt/IBM/JazzSM/profile/config/cells/JazzSMNode01Cell/nodes/JazzSMNode01/trust.p12
     - /opt/IBM/JazzSM/profile/config/cells/JazzSMNode01Cell/applications/isc.ear/deployments/isc/isclite.war/WEB-INF/tipRoleUser.dat
     - /opt/IBM/JazzSM/profile/config/cells/JazzSMNode01Cell/applications/isc.ear/deployments/isc/isclite.war/WEB-INF/tipRoleGroup.dat

   If you manually modified any other configuration files in your old SMU Docker container, specify these files or folders in the **`eezdocker.cfg`** using the *MIGRATION_COPY_CUSTOM_FOLDERS* configuration option. For more details, see "Customizing the SMU Docker Command Line Utility" on page 20.

5. If the migration is successful, you can remove the old SMU Docker container by using the **old** version of the IBM SMU Docker Command Line Utility:

   ```
   eezdocker.sh uninstall
   ```

   After a successful uninstallation of the old SMU, you can also delete the old script **`eezdocker.sh`**.

Upgrading SMU Automation

Use IBM Installation Manager to upgrade SMU Automation from earlier versions to the latest version.

The upgrade scenarios vary with your installed version:

- To upgrade SMU Automation from V1.1.5, see "Upgrading SMU Automation from V1.1.5 to V1.1.6" on page 57.
- To upgrade SMU Automation from V1.1.4 or earlier versions, see "Upgrading SMU Automation from V1.1.4 or earlier versions to V1.1.6" on page 57.

Upgrading SMU Automation from V1.1.5 to V1.1.6

1. Launch IBM Installation Manager using the **`smu_install.sh`** script or manually add the SMU Automation repository to Installation Manager as described in Installating SMU Automation in step 1-3.
2. On the Start page of Installation Manager, click **Update**.
3. In the **Update Packages** page, select **IBM Service Management Unite Automation** and click **Next**.
4. Select the desired version, for example, **Version 1.1.6.0** and click **Next**.
5. Carefully read the terms of the license agreement. To accept the terms of the license agreement, select **I accept the terms in the license agreement** and click **Next**.
6. On the **WebSphere configuration** page, provide the password in field **WAS Admin User Password**, and click **Next**. The WAS user ID is detected and pre-filled.
7. When you specified all the required information on the installation panels, click **Update** to start the upgrade.

   Note: WebSphere Application Server might present a prompt to verify the **WebSphere User ID** and **password**. If this occurs, reenter the user ID and password.

   When the update process completes, a message that confirms the success of the process is displayed. Click **View Log File** to open the log file.
8. When the upgrade of SMU Automation is complete. Click **Finish** to exit.

Upgrading SMU Automation from V1.1.4 or earlier versions to V1.1.6

1. Launch IBM Installation Manager using the **`smu_install.sh`** script or manually add the SMU Automation repository to Installation Manager as described in Installating SMU Automation in step 1-3.
2. On the Start page of Installation Manager, click **Install** to start your upgrade.
3. On the **Install Packages** page, select **IBM Service Management Unite Automation Version 1.1.6.0** and click **Next**.

   The installer detects that this is an update installation if a previous version of SMU Automation is found on the system. Click **Next** to proceed.
4. Carefully read the terms of the license agreement. To accept the terms of the license agreement, select **I accept the terms in the license agreement** and click **Next**.
5. Specify the directory where you want to install SMU Automation or accept the default location `/opt/IBM/smsz/ing`, and then click **Next**.

   The **Create a new package group** option is selected by default and only this option is supported for the installation of SMU Automation.
6. On the **Tivoli Directory** page, no action is needed. Click **Next** to proceed.
7. On the **WebSphere configuration** page, provide the password in field **WAS Admin User Password**, and click **Next**. The WAS user ID is detected and pre-filled.
8. On the **System Automation Functional User ID** page, provide the password for the functional user ID `eezdmn`, and then click **Next**.

9. On the **System Automation Administration User ID** page, specify the user ID and password of the System Automation administrator, and then click **Next**. The default user ID is `eezadmin`.

   Note: Do not choose the same name for both the System Automation Administration user ID and the WebSphere Application Server administrator user ID. Otherwise, problems might occur if you uninstall SMU Automation. For example, do not specify `smadmin` for both users.

10. When you specified all the required information on the installation panels, click **Install** to start the upgrade.

    Note: WebSphere Application Server might present a prompt to verify the **WebSphere User ID** and **password**. If this occurs, re-enter the user ID and password.

    When the update process completes, a message that confirms the success of the process is displayed. Click **View Log File** to open the log file.

11. When the upgrade of SMU Automation is complete. Click **Finish** to exit.

Chapter 7. Configuring and administering SMU Automation

This section introduces how to configure and administer Service Management Unite Automation.

Configuring SMU Automation

After you installed IBM Service Management Unite and the prerequisites, complete the basic configuration tasks to fully prepare your infrastructure environment.

1. Quick startup of End-to-End Automation Adapter.
2. Configure the SMU Automation host. You can use the **cfgsmu** or the new web configuration tool to customize your configuration:
   - “[Use cfgsmu] Configuring the SMU Automation host” on page 61.
   - “[Use Web Config Tool] Configuring the SMU server” on page 59.
3. “Securing the connection to automation adapters” on page 66.
4. [Optional] Configuring access to Universal Automation Adapters.
   - “[Use cfgsmu] Configuring the Universal Automation Adapter” on page 75.
   - “[Use Web Config Tool] Configuring the Universal Automation Adapter” on page 71.

Note: If you use the configuration tool **cfgsmu**, you must ensure that an X Window is available for displaying the graphical configuration panels. At a minimum, you must use the configuration tool after an initial installation to define at least one functional user ID and password to access a connected automation domain.

You can also configure the Service Management Unite Automation in silent mode by using an input properties file. For more information, see “Starting silent configuration” on page 83.

[Use Web Config Tool] Configuring the SMU server

Use the **Configure Service Management Unite** dashboard to configure the Service Management Unite (SMU) server.

Procedure

1. In the navigation bar, click **System Configuration** → **Configure Service Management Unite** to open the **Configuration** dashboard.
2. Go through the following tabs under section **Service Management Unite Server**, and customize the configuration.
   - Host name and Port
   - User Credentials
   - Security
3. Click **Save** to save your changes.

   All your definitions and changes of SMU host configuration settings and properties will be written to the corresponding configuration files.

Starting the web configuration tool

As an alternative of the **cfgsmu** configuration dialogue, the **Configure Service Management Unite** dashboard is a web-based dashboard that allows you to configure the SMU server and the Universal Automation Adapter.

Procedure

1. Log on to the Service Management Unite console.
2. In the navigation bar, click **System Configuration** → **Configure Service Management Unite**.

Results

The dashboard **Configure Service Management Unite** is displayed.

Host name and Port

Use the **Host name and Port** tab to configure settings of the host system where Service Management Unite is running.

Host name or IP address
The host name or IP address of the IBM Service Management Unite server .

Event port number
The port number on which the Service Management Unite server receives events from automation adapters. This port has to match the port number that you must specify as target for events when configuring an automation adapter. The default port is 2002.

User Credentials

Use the **User Credentials** tab to configure the user credentials used by functional user. The automation framework uses these credentials to authenticate itself.

The characters that are used for all user IDs entered on this tab are limited to the following ASCII characters: A–Z, a-z, 0–9, and _ (underscore).

- Generic Credentials for Accessing Automation Domains

  Generic user ID for automation domains
  Backend user ID used by the SMU functional user to access all automation domains for which no specific credentials are defined below.

  - For System Automation for z/OS domains, this is a z/OS user ID.
  - For Universal Automation Adapter domains, this is a system user ID of the server hosting the Universal Automation Adapter.

  Generic password for automation domains
  The generic user ID’s password for accessing all automation domains.

  Confirm Generic password for automation domains
  Identical value as specified in the password field to confirm password correctness.

- Specific Credentials for Accessing Automation Domains

  Specific automation domain user credentials can be defined explicitly for each automation domain that is monitored by the SMU server. The automation domain list shows the name and user ID of each domain for which specific access credentials are currently defined.

  - Click **Add new** to create a new credential:

    1. In the new row, specify the following parameters:

       Domain Name
       The name of the new domain. Ensure that this domain name is unique in the set of all automation domains you are working with. The maximum length of the domain name is 64 characters.

User ID
The user ID that is used by the SMU server to access the new domain.

Password
The password that is used by the SMU server to access the new domain.

Confirm Password
Identical value as specified in the password field to confirm password correctness.

2. Click **OK** to save the new credential. You can click **Cancel** to cancel the changes.

- To modify the existing credential, click ✎.
- To delete the credential, click 🗑.

Security

Use the **Security** tab to configure the properties for the Secure Sockets Layer (SSL) connection to the automation domains.

Enable SSL
Check to use the SSL protocol for data transport between the SMU server and automation adapters.

If you deselect this check box, all the following fields within this tab are disabled. Furthermore, all entry fields are cleared and the **Enforce use of SSL for all automation domains** check box is deselected as well.

Keystore
The name of the keystore file used for SSL. For more information on how to generate Keystore and Truststore files, refer to Creating keystores and truststores with SSL public and private keys.

Keystore password
The password of the keystore file.

Confirm Keystore password
Identical value as specified in the keystore password field.

Truststore
The name of the truststore file used for SSL.

Certificate alias
The alias name of the certificate that is used by Service Management Unite.

Enforce use of SSL for all automation domains
Check if you want to enforce that automation adapters must be properly configured for using SSL at the transport layer before they successfully connect to the SMU server. If not checked, each adapter might or might not be configured for using SSL on an individual basis.

[Use `cfgsmu`] Configuring the SMU Automation host

Use the configuration dialogue **`cfgsmu`** to configure the SMU Automation host.

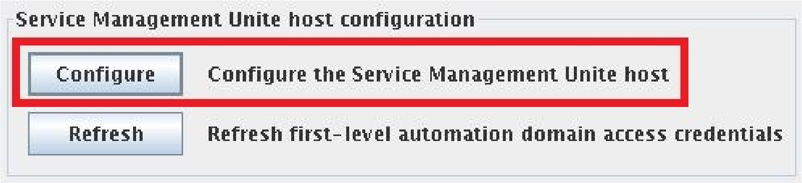
About this task

The initial configuration of IBM Service Management Unite is processed during the installation of the product. To browse or change the properties, use the IBM Service Management Unite configuration dialog or silent configuration. Do not manually edit the configuration properties files in which the configuration parameters are stored.

Procedure

1. Start the configuration dialog. See Starting the Service Management Unite Automation configuration dialog or see “Starting cfgsmu in the Docker container” on page 64 if you installed SMU using the predefined Docker image.

2. In the configuration dialogue panel, click **Configure** on the Service Management Unite host configuration section.



Service Management Unite host configuration

Configure — Configure the Service Management Unite host

Refresh — Refresh first-level automation domain access credentials

3. Switch between tabs to customize the configuration.
4. Click **Save** to save your changes to the SMU common configuration properties files.

   On completion, a configuration update status window is displayed, showing which configuration files are updated. If errors occurred during the update, the corresponding error messages are also displayed.

What to do next

After the configuration properties are edited, the configuration settings can be dynamically activated by clicking the **Refresh** on the main menu of the Service Management Unite host configuration section. See also "Refreshing the SMU common configuration" on page 66.

Overview of the cfgsmu configuration tool

The `cfgsmu` configuration tool is used to configure Service Management Unite Automation.

The `cfgsmu` configuration dialog

The initial window of the configuration dialog is called task launcher and provides all configuration tasks. The task launcher opens when you start the configuration dialog. There are two main sections in this panel:

- The **Service Management Unite host configuration** section includes the following functions:

  Configure
  Click **Configure** to open Service Management Unite Automation common settings dialog. You can specify configuration settings that are common for different components of Service Management Unite Automation. For more information, see "[Use cfgsmu] Configuring the SMU Automation host" on page 61.

  Refresh
  Click **Refresh** to update configuration settings of Service Management Unite Automation. For more information, see Refreshing the Service Management Unite common configuration.

- The **Universal Automation Adapter configuration** includes the following function:

  Enable Universal Automation Adapter configuration
  Select this check box to enable the configuration of Universal Automation Adapter The configuration files of the Universal Automation Adapter are updated if they are affected by the changes that you apply to the Service Management Unite configuration. The configuration dialog remembers the enable or disable status of the Service Management Unite configuration across multiple invocations.

  Configure
  Click **Configure** to open the Universal Automation Adapter configuration dialog. For more information, see "[Use cfgsmu] Configuring the Universal Automation Adapter" on page 75.

More detailed information about all configuration tasks is available in the Service Management Unite online help. To start the online help, click **Help** in the configuration dialog.

The `cfgsmu` command

Format

```
cfgsmu [-s
[-z] [-g|-gr] [-l  silent path]
-eu [-g|-gr] [-l  silent path]
-ru -o host [-g|-gr] [-l  silent path]
-ru -o host -ra
-ru -o host -rr
-ru -o host -rd -u uid -p pwd
]
```

Flags

`<no option>`
Invoke configuration dialog.

`-s`
Perform silent configuration (all following options and parameters only for silent configuration).

`-z`
Configure the Service Management Unite host settings (this is the default configuration task).

`-eu`
Configure the Universal Automation Adapter for non-clustered nodes.

Silent configuration properties file options (for 'Configure' function of all configuration tasks):

`-g`
Generate silent configuration properties file from defined values.

`-gr`
Like -g, but replace existing file.

`-l`
Silent input properties file location is different from default silent path.

`silent_path`
Location of silent input properties file; default is the directory where the target properties files are located.

Starting the `cfgsmu` configuration tool

The `cfgsmu` command configures the settings of different Service Management Unite Automation components that run on the Service Management Unite Automation server and the Universal Automation Adapters.

Before you begin

The user ID that you use to start the dialog must meet the following requirements:

- The user ID must be in same group as the user ID you used for installing Service Management Unite Automation. The group permissions for the `cfgsmu` script must be set to **EXECUTE**.
- The user ID must have write access to the following directory: `<EEZ_CONFIG_ROOT>` .

About this task

The command offers a graphical user interface to specify parameters, which are stored in various property files that are required by the Service Management Unite Automation components. Most parameters that are configured with this command control the behavior of the Service Management Unite Automation components and do not need to be changed frequently.

In addition, the `cfgsmu` command is used to add or change user IDs and passwords that are used to communicate with other automation domains and remote nodes.

Procedure

1. Log on to the system where Service Management Unite Automation is installed.
2. Run the command to start the graphical configuration tool:

   ```
   cfgsmu
   ```

   The configuration dialog task launcher is displayed.

Starting cfgsmu in the Docker container

Start the **cfgsmu** configuration tool to configure the SMU host, the Universal Automation Adapter, and the credentials for the functional user that are needed to access backend systems.

About this task

You can run **cfgsmu** in graphical mode or silent mode. For ease of use, the graphical mode is recommended.

Procedure

1. Log on to the system where Service Management Unite Automation is installed.
2. Start the configuration tool **cfgsmu** in graphical mode or silent mode:
   - To use **cfgsmu** in graphical mode, use a VNC client to access the docker host system, and then issue the following command:

     ```
     eezdocker.sh cfgsmu
     ```

     Note: If command '**eezdocker.sh cgfsmu**' doesn't work as expected, run the command '**xhost +local:all**' before you run '**eezdocker.sh cfgsmu**' to ensure that the Docker process can access the user's X session.
   - To use **cfgsmu** in silent mode, issue the following commands:
     a. Issue the command to access a shell to the running SMU Docker container:

        ```
        eezdocker.sh shell
        ```

        The commands in the following steps must be run in this opened SMU Docker container shell.

     b. Generate a silent configuration input properties file:

        ```
        cfgsmu -s -g
        ```

     c. Edit the input properties file. For example, you can specify values for **cred-generic-userid** and **cred-generic-password** to define credentials for the backend access to z/OS automation domains.

     d. Run the silent configuration according to the values from the input properties file:

        ```
        cfgsmu -s
        ```

     e. Issue the command to exit the SMU Docker container shell:

        ```
        exit
        ```

     f. Restart the WebSphere Application Server to activate the configuration changes by restarting the SMU Docker container:

        ```
        eezdocker.sh restart
        ```

Operations Console Host tab

Use the Operations Console Host tab to configure the IBM Service Management Unite server and the host where the IBM Service Management Unite host is running.

Controls and fields on the Operations Console Host tab:

Host name or IP address
Name or IP address of the system that hosts the operations console host.

Event port number
The port on which the EIF message converter listens for events from the first-level automation domains. This port number must match the port number for the operations console host in all adapter configurations. You can configure the event port number for the operations console host during the configuration of the automation adapters on first-level automation domains.

For the System Automation for z/OS adapter, the event port number is the event port that is specified in the adapter configuration parameter `eif-send-to-port` in the adapter plug-in properties file.

WAS bootstrap port number
The bootstrap port of the WebSphere Application Server instance that hosts the operations console host.

User Credentials tab

Use the User Credentials tab to configure the user credentials of Service Management Unite Automation. The automation framework uses these credentials to authenticate itself. The characters that are used for all user IDs entered on this tab are limited to the following ASCII characters: A–Z, a-z, 0–9, and _ (underscore).

Controls and fields on the User Credentials tab:

Generic user ID
The user ID the automation framework uses to authenticate itself to a first-level automation domain when no credentials are specified for the domain in the **Credentials for accessing specific FLA domains** table.

Generic password
The password for the generic user ID. Click **Change** to change the password.

Credentials for accessing specific first-level automation domains
Click **Add** to specify a user ID that is valid for a specific domain. The user ID is not required to be `root`, but to be authorized to run operations on resources in the first-level automation domain that are supported by the automation framework. For example, bringing an automated resource online.

- Click **Remove** or **Change** to remove or modify the credentials for the selected domain.
- Click **Validate** to validate the user ID and password that you specified for the selected domain. The domain is contacted, and the validation is performed on the system where the automation adapter that manages the domain is running.

Security tab

Use the Security tab to configure the properties for the Secure Sockets Layer (SSL) connection to the first-level automation domains.

Controls and fields on the Security tab:

Truststore
The fully qualified file name of the truststore file that is used for SSL. Click **Browse** to select a file.

For more information on how to generate Keystore and Truststore files, refer to "Creating keystores and truststores with SSL public and private keys" on page 66.

Keystore
The fully qualified file name of the keystore file that is used for SSL. Click **Browse** to select a file.

Keystore password
The password of the keystore file. The password is required if a keystore file was specified. Click **Change** to change the password.

Note: If the truststore is in a different file than the keystore, the passwords for the files must be identical.

Certificate alias
The alias name of the certificate to be used by the server. The characters that are used for the certificate alias are limited to the following ASCII characters: A – Z, a-z, 0–9, and _ (underscore).

Enforce use of SSL for all first-level automation domains
Select this check box if you want to enforce that all first-level automation domains are properly configured to use SSL at the transport layer. Then, all first-level automation domains can successfully connect to the automation framework. If not selected, first-level automation domains are configured to use SSL on an individual basis.

Refreshing the SMU common configuration

Click **Refresh** on the Service Management Unite main menu of the configuration dialog task launcher to trigger configuration settings changes. The settings are reloaded by the automation framework. Use this task in the following cases:

- Click **Refresh** after you changed the credentials for accessing specific first-level automation domains on the **User Credentials** tab of the IBM Service Management Unite common configuration.
- To clear the list of first-level automation domains that cannot be accessed anymore due to unrecoverable access errors.

Securing the connection to automation adapters

Complete the steps to secure the connection between the Service Management Unite server and the automation adapters connected to it.

About this task

Follow this procedure to secure the connection between the SMU server and the automation adapters using SSL encryption and SSL certificate based authentication.

Creating keystores and truststores with SSL public and private keys

Use the Java keytool to create keystores and truststores for automation adapters and Service Management Unite.

About this task

The process generates the following files:

Truststore
Contains the public keys for Service Management Unite and the automation adapters.

Service Management Unite keystore
Contains the private key for Service Management Unite.

Automation adapter keystore
Contains the private key for the automation adapter.

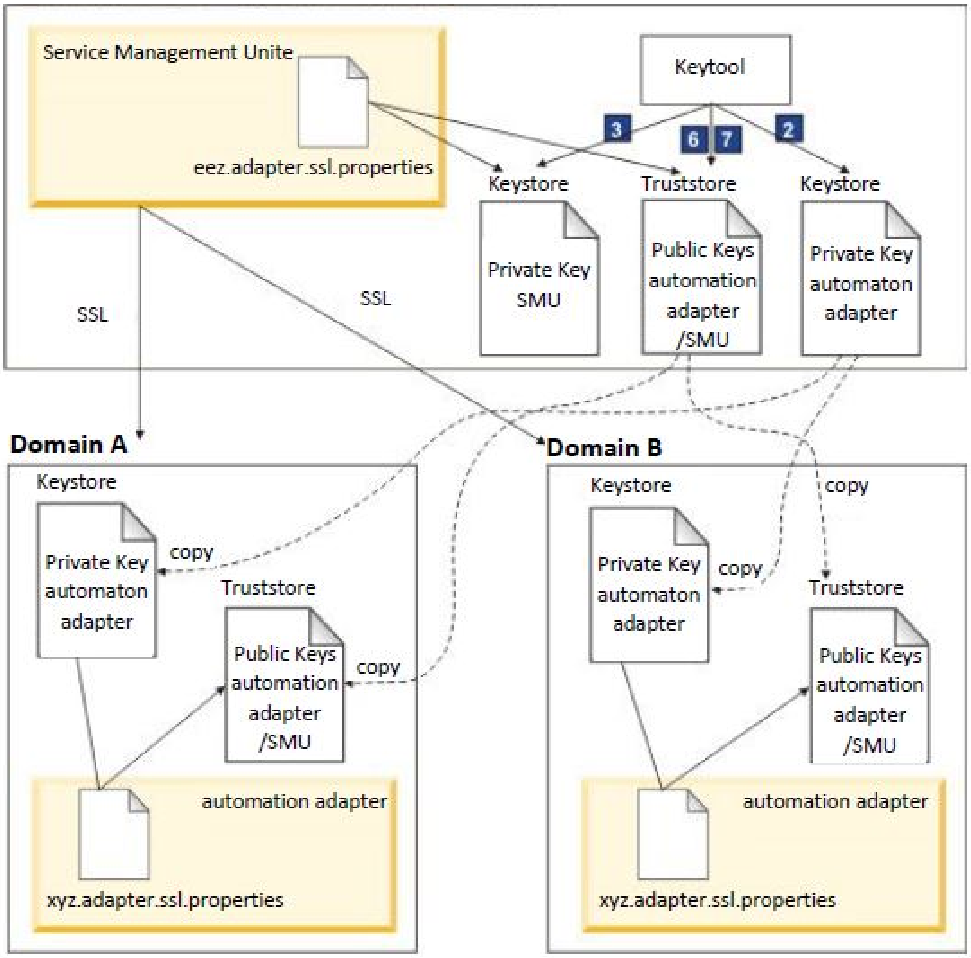

Service Management Unite
eez.adapter.ssl.properties
Keytool
3
6
7
2
Keystore
Truststore
Keystore
Private Key SMU
Public Keys automation adapter /SMU
Private Key automaton adapter
SSL
SSL
Domain A
Domain B
Keystore
Private Key automaton adapter
copy
Truststore
Public Keys automation adapter /SMU
copy
automation adapter
xyz.adapter.ssl.properties
Keystore
copy
Private Key automaton adapter
copy
Truststore
Public Keys automation adapter /SMU
automation adapter
xyz.adapter.ssl.properties

Figure 3. Keystore and truststore generation using SSL

Procedure

1. Set the following environment variables. They will be used as parameters to the keytool:

```
# java keytool from WebSphere installation directory
JAVA_KEYTOOL=/opt/IBM/WebSphere/AppServer/java/jre/bin/keytool
# SMU SSL config file directory
EEZ_CONFIG_DIR=/etc/opt/IBM/smsz/ing/cfg/ssl
# keys will expire in 25 years
KEY_VALIDITY_DAYS=9125
# passphrase at least 6 characters
PASSPHRASE=passphrase
```

2. Create a keystore with public and private keys for the automation adapter:

```
${JAVA_KEYTOOL} -genkey -keyalg RSA -validity ${KEY_VALIDITY_DAYS} \
-alias eezadapter -keypass ${PASSPHRASE} -storepass ${PASSPHRASE} \
-dname "cn=E2E Adapter, ou=System Automation, o=IBM, c=US" \
-keystore "${EEZ_CONFIG_DIR}/eez.ssl.adapter.keystore.jks"
```

3. Create a keystore with public and private keys for Service Management Unite:

```
${JAVA_KEYTOOL} -genkey -keyalg RSA -validity ${KEY_VALIDITY_DAYS} \
-alias eezsmu -keypass ${PASSPHRASE} -storepass ${PASSPHRASE} \
-dname "cn=SMU Server, ou=System Automation, o=IBM, c=US" \
-keystore "${EEZ_CONFIG_DIR}/eez.ssl.smu.keystore.jks"
```

4. Export the certificate file with the public key for the automation adapter:

```
${JAVA_KEYTOOL} -exportcert -alias eezadapter \
-file "${EEZ_CONFIG_DIR}/eezadapter.cer" -storepass ${PASSPHRASE} \
-keystore "${EEZ_CONFIG_DIR}/eez.ssl.adapter.keystore.jks"
```

5. Export the certificate file with the public key for Service Management Unite:

   ```
   ${JAVA_KEYTOOL} -exportcert -alias eezsmu \
   -file "${EEZ_CONFIG_DIR}/eezsmu.cer" -storepass ${PASSPHRASE} \
   -keystore "${EEZ_CONFIG_DIR}/eez.ssl.smu.keystore.jks"
   ```

6. Create the authorized keys truststore and import the certificate with the public key for the automation adapter:

   ```
   ${JAVA_KEYTOOL} -importcert -noprompt -alias eezadapter \
   -file "${EEZ_CONFIG_DIR}/eezadapter.cer" -storepass ${PASSPHRASE} \
   -keystore "${EEZ_CONFIG_DIR}/eez.ssl.authorizedkeys.truststore.jks"
   ```

7. Create the authorized keys truststore and import the certificate with the public key for Service Management Unite server:

   ```
   ${JAVA_KEYTOOL} -importcert -noprompt -alias eezsmu \
   -file "${EEZ_CONFIG_DIR}/eezsmu.cer" -storepass ${PASSPHRASE} \
   -keystore "${EEZ_CONFIG_DIR}/eez.ssl.authorizedkeys.truststore.jks"
   ```

8. Delete the certificate files that are no longer needed at run time for the automation adapter and Service Management Unite.

   ```
   rm ${EEZ_CONFIG_DIR}/eezadapter.cer
   rm ${EEZ_CONFIG_DIR}/eezsmu.cer
   ```

Enabling SSL security in the SMU Automation configuration

Complete the steps to enable SSL security in SMU Automation.

Procedure

1. Start the SMU Automation configuration tool **`cfgsmu`**.

   For the detailed instructions, see "Starting the cfgsmu configuration tool " on page 63
2. In the configuration dialogue, click **Configure** to open Service Management Unite Automation common settings dialogue.
3. In the **Security** tab, specify the values for the following parameters.

   Sample values are provided for your reference:

   - **`Truststore`**: `/etc/opt/IBM/smsz/ing/cfg/ssl/eez.ssl.authorizedkeys.truststore.jks`
   - **`Keystore`**: `/etc/opt/IBM/smsz/ing/cfg/ssl/eez.ssl.smu.keystore.jks`
   - **`Keystore password`**: passphrase
   - **`Certificate alias`**: eezsmu
4. Click **Save** to save the configuration changes.
5. Restart the WebSphere® Application Server. For detailed instructions, see Starting and stopping WebSphere Application Server.

Enabling SSL security in the automation adapter configurations

Complete the steps to enable SSL security for automation adapter configurations.

Procedure

1. Copy the authorized keys truststore file to the nodes in the automation domain where the automation adapter runs:

```
scp ${EEZ_CONFIG_DIR}/eez.ssl.authorizedkeys.truststore.jks \
root@<adapter-nodename>:<E2E_CUSTOM_ROOT>/ssl/eez.ssl.authorizedkeys.truststore.jks
```

2. Copy the adapter keystore file to the nodes in the automation domain where the automation adapter runs:

   ```
   scp ${EEZ_CONFIG_DIR}/eez.ssl.adapter.keystore.jks \
   root@<adapter-nodename>:<E2E_CUSTOM_ROOT>/ssl/eez.ssl.adapter.keystore.jks
   ```

3. Update the adapter SSL configuration to match the copied file names, passphrase, and alias name. For System Automation for z/OS End-to-End adapter, update the configuration in the properties file: `ing.adapter.ssl.properties`.
4. Enable SSL communication for the adapter. For System Automation for z/OS End-to-End adapter, set the property `eez-remote-contact-over-ssl=true` in the properties file: `ing.adapter.properties`.

Optional: Enforcing usage of SSL for all automation domains

To enforce usage of SSL for all automation domains, activate the corresponding setting in the configuration dialogue.

Before you begin

You must complete the SSL setup for all automation adapters before you start the following steps. If there are still automation adapters running without SSL setup, then these domains go offline and can not get reconnected after you activate the setting in the following steps.

Procedure

1. Start the SMU Automation configuration tool **`cfgsmu`**.
2. In the configuration dialogue, click **Configure** to open Service Management Unite Automation common settings dialog.
3. In the **Security** tab, select the check box **Enforce use of SSL for all first-level automation domains**, and click **Save** to save the changes.
4. In the configuration dialogue, click **Refresh** to activate the SSL configuration changes.

[Optional] Configuring access to the Universal Automation Adapter

Use the Universal Automation Adapter to access and integrate non-clustered nodes into an automation environment.

About this task

You can use the configuration dialog **`cfgsmu`** or the web configuration tool to configure the Universal Automation Adapter on the system where the Service Management Unite Automation is installed.

Figure 1 displays how configuration for the Universal Automation Adapter is maintained.

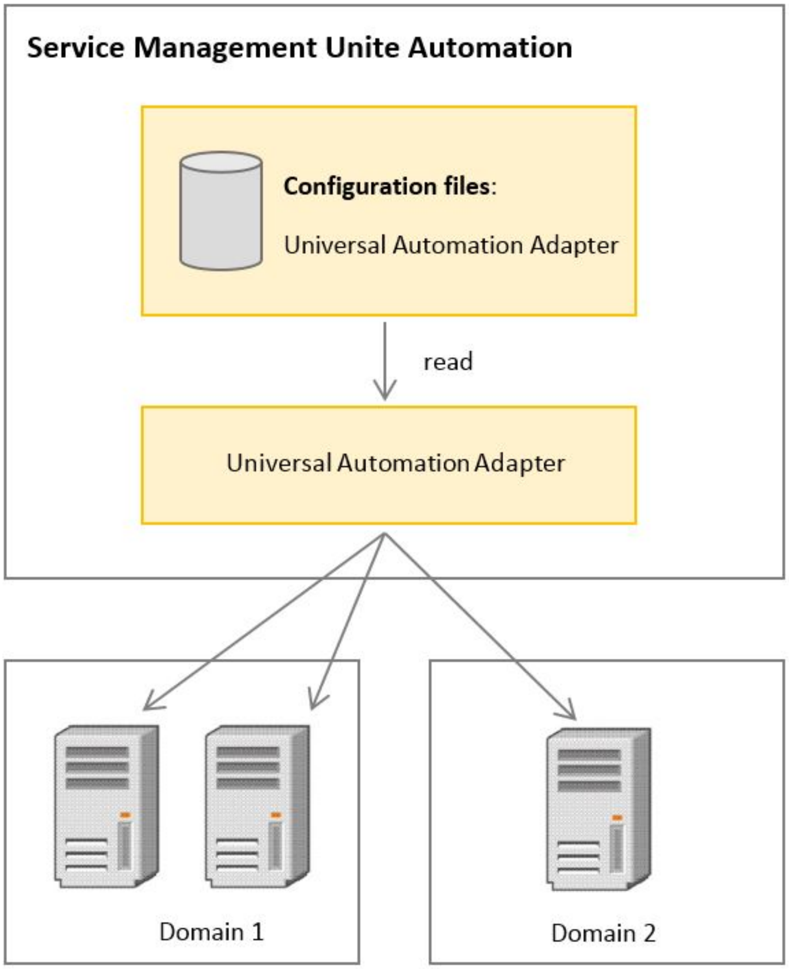

Service Management Unite Automation
Configuration files:
Universal Automation Adapter
read
Universal Automation Adapter
Domain 1
Domain 2

Figure 4. Maintaining configurations for multiple Universal Automation Adapters

Procedure

1. Start the configuration dialog **`cfgsmu`** or the web configuration tool.
   - Starting the Service Management Unite Automation configuration dialog
   - If you installed SMU using the predefined Docker image: “Starting cfgsmu in the Docker container” on page 64
   - “Starting the web configuration tool” on page 60.
2. Change to the Universal Automation Adapter configuration tabs and switch between tabs to customize the configuration.
3. Click **Save** to save your changes to the SMU common configuration properties files.

What to do next

If you use the configuration dialogue **`cfgsmu`**, after the configuration properties are edited, the configuration settings can be dynamically activated by clicking **Refresh** on the main menu. See “Refreshing the SMU common configuration” on page 66 for detailed instructions.

[Use Web Config Tool] Configuring the Universal Automation Adapter

Use the **Configure Service Management Unite** dashboard to configure the Universal Automation Adapter.

Procedure

1. In the navigation bar, click **System Configuration** → **Configure Service Management Unite** to open the Configuration dashboard.
2. Click **Universal Automation Adapter** to switch the tab.
3. The **Enable Universal Automation Adapter** check box is selected by default. To disable the configuration of Universal Automation Adapter, deselect the check box.
4. Go through the following tabs under section **Universal Automation Adapter**, and customize the configuration.
   - "Adapter" on page 71
   - "SA z/OS E2E Agent" on page 72
   - "User Credentials" on page 72
   - "Security" on page 73
   - "Logger" on page 74
5. Click **Save** to save your changes.

   All your definitions and changes of the Universal Automation Adapter configuration settings will be written to the corresponding configuration files.

Adapter

Use the **Adapter** tab to configure the Universal Automation Adapter host.

- Universal Automation Adapter Host

  Request port number
  The port of the Universal Automation Adapter listens for requests from the automation host. The default port is 2005.

- Universal Automation Policy

  Policy pool location
  The directory where all the XML policy files for the Universal Automation Adapter are stored.

- Automation domains managed by the universal automation adapter
  - Click **Add new** to add a new domain that is managed by the Universal Automation Adapter.
    1. In field **Doamin Name**, specify the the name of the new domain. Ensure that this domain name is unique in the set of all automation domains you are working with. The maximum length of the domain name is 64 characters.
    2. Click **OK** to save the new credential. You can click **Cancel** to cancel the changes.
  - To modify the existing domain name, click ✎.
  - To delete the domain name, click 🗑.

- Advanced Universal Automation Adapter Settings

  If you click **Default**, the default settings are restored.

  Adapter stop delay(seconds)
  The time delay before the Universal Automation Adapter stops. This gives the adapter a chance to deliver the domain leave event properly. The default value is 5, the value ranges between 3 through 60.

Remote contact activity interval(seconds)

The time after which the automation adapter stops if there is no communication with the SA z/OS E2E agent or the SMU server. The default value is 360, the value ranges between 0 through 360.

If you specify a value of 0 seconds, this means that the adapter never stops. It continues to run and waits until it is contacted again by the SA z/OS E2E agent or the SMU server.

Initial contact retry interval(minutes)

During this period the Universal Automation Adapter tries to contact the SA z/OS E2E agent host and the SMU server. This continues until it succeeds or the specified time has elapsed.

The default value 0 means that the adapter tries contacting the SA z/OS E2E agent host and the SMU host forever. The value ranges between 0 through 1440.

EIF event reconnect attempt interval(seconds)

The time the Universal Automation Adapter waits until it tries to reconnect if the connection to the SA z/OS E2E agent host or the SMU server is interrupted. The default value is 30.

Enable EIF event caching

If this check box is selected, all events that can not be sent are cached. This can help to recover in cases where the connection to the SA z/OS E2E agent host or the SMU server is interrupted for a short time so that cached events can be sent when the connection is available again. If the cache limit is exceeded, cached events are discarded and the adapter sends a "domain offline" followed by a "domain online" event to the SA z/OS E2E agent host or the SMU server host.

If this check box is not selected, all events that can not be sent are discarded immediately.

SA z/OS E2E Agent

Use the **SA z/OS E2E Agent** tab to configure the SA z/OS E2E agent host which uses the universal automation adapter to manage automation domains.

Host name or IP address

The name or the IP address of the host on which the SA z/OS E2E agent runs.

Event port number

The number of the port on which the SA z/OS E2E agent listens for events from the automation adapter. This port has to match the corresponding event port number that you specify when configuring the SA z/OS E2E agent. The default port is 2002.

If you do not want the SA z/OS E2E agent to perform end-to-end automation for any domain that is managed by the Universal Automation Adapter, you can leave the host field empty.

The Universal Automation Adapter potentially also sends events to the Service Management Unite server. You have defined the corresponding host name or IP address and port number on the Host name and Port tab.

User Credentials

Use the **User Credentials** tab to configure the credentials that the Universal Automation Adapter uses to access remote non-z/OS systems.

The user ID that you specify for a resource in a Universal Automation Adapter policy is used to determine how authentication is performed on the remote node where that resource resides. The Universal Automation Adapter uses the following priority to determine how authentication on remote nodes is performed:

- The user ID that is specified for a resource in the Universal Automation Adapter policy is defined in the specific non-z/OS nodes credentials list on this tab: The universal automation adapter uses the password that is associated with this specific user ID.
- The user ID that is specified for a resource in the Universal Automation Adapter policy is defined as generic user ID on this tab: The Universal Automation Adapter uses the password that is associated with this generic user ID.

- User authentication is performed using SSH public and private keys for the user ID that is specified for a resource in the Universal Automation Adapter policy. In this case SSH key authentication must be enabled and configured on the Security tab.
- Generic Credentials for Accessing Remote Non-z/OS Systems

  Generic user ID
  User ID for accessing remote non-z/OS systems. The user ID is used by the Universal Automation Adapter to access all remote systems for which no specific credentials are defined below.

  Generic password
  The generic user ID’s password for accessing all remote systems.

  Confirm Generic password
  Identical value as specified in the password field to confirm password correctness.

  Generic credentials are optional. If you want to remove the already configured generic credentials, leave the generic user ID field empty.
- Specific Credentials for Accessing Remote Non-z/OS Systems

  You can define specific user credentials explicitly for each non-z/OS system that is accessed by the Universal Automation Adapter for which no SSH key authentication is used. The list shows the pairs of node name and user ID for which specific access credentials are currently defined.

  – Click **Add new** to create a new credential:

    1. In the new row, specify the following parameters:

       Node Name
       The name of the new non-z/OS node. You might define more than on user ID and password pair for a particular node.

       User ID
       The user ID that is used by the Universal Automation Adapter to access the new node.

       Password
       The password that is used by the SMU server to access the new domain.

       Confirm Password
       Identical value as specified in the password field to confirm password correctness.
    2. Click **OK** to save the new credential. You can click **Cancel** to cancel the changes.

  – To modify the existing credential, click ✎.

  – To delete the credential, click 🗑.

Security

Use the **Security** tab to configure the security settings for the communication between the Universal Automation Adapter and other systems.

- Communication between Service Management Unite Host and Universal Automation Adapter

  Enable SSL for data transport between the automation host and the universal automation adapter
  Check to use SSL for data transport between the SA z/OS E2E agent or the SMU server and the Universal Automation Adapter.

  Note: If you selected **Enforce use of SSL for all automation domains**, you must enable SSL here. Check the security settings of the Service Management Unite host configuration for the setting of the SSL enforcement flag.

  Keystore
  The name of the keystore file used for SSL.

  Keystore password
  The password of the keystore file.

Confirm keystore password
Identical value as specified in the keystore password field to confirm password correctness.

Truststore
The name of the truststore file used for SSL.

Certificate alias
The alias name of the certificate that is used by the Universal Automation Adapter.

Enforce user authentication between the automation host and the universal automation adapter
Check to enable the authentication of users on the system where the Universal Automation Adapter is running when the Universal Automation Adapter is contacted by the SMU server.

Uncheck it if you want to bypass the authentication.

- Communication between Universal Automation Adapter and Remote Non-z/OS systems

Enable user authentication with SSH public and private keys
Check to use SSH keys for authentication of users for which you have defined neither generic nor specific access credentials on the User Credentials tab.

SSH private key file
The fully qualified name of the private key file that is generated by the ssh-keygen utility. The default names of files that are generated by ssh-keygen are `id_dsa` or `id_rsa`. Ensure that the user ID under which the Universal Automation Adapter is running has read access to this file.

Private key passphrase
The passphrase that you used to generate the private key file using the ssh-keygen utility.

Confirm Private key passphrase
Identical value as specified in the key passphrase field to confirm passphrase correctness.

Logger

Use the **Logger** tab to configure the message logging, tracing, and FFDC options for the Universal Automation Adapter.

Maximum log/trace file size
The maximum disk usage in kilobytes that a log file can reach. If the limit is reached, another log file is created for roll over purposes. The maximum number of log files is two, which means that the least recent file gets overwritten after both files are filled up.

Message logging level

- Error
- Warning
- Information

Trace logging level

- Off: Trace logging is disabled.
- Minimum: Only a minimum of trace data is logged.
- Medium: A medium amount of trace data is logged. This is the default trace logging level.
- Maximum: The maximum amount of trace data is logged.

Recording level

- Off: FFDC recording is disabled.
- Minimum: Only a minimum of FFDC data is recorded.
- Medium: A medium amount of FFDC data is recorded. This is the default FFDC recording level.
- Maximum: The maximum amount of FFDC data is recorded.

Maximum disk space
The maximum disk space in bytes that will be used to store FFDC data. The default maximum disk space is 10485760 bytes (10 MB).

Space exceeded policy

- Ignore: Issue a warning, but do not enforce the FFDC disk space limitation.
- Auto-delete: Automatically delete FFDC files to enforce the FFDC disk space limitation. This is the default space exceeded policy.
- Suspend: Halt further FFDC actions until disk space is freed manually.

Filter mode

- Passthru: All log events with messages that are specified in the message ID list will pass the filter and FFDC data is written. This is the default filter mode.
- Block: All log events with messages that are specified in the message ID list will be blocked.

Message ID list

The message IDs that control for which log events FFDC data is written, depending on the filter mode. The comparison of message IDs is case sensitive. Each message ID must occur in a new line. Note that you can use `*` as a wildcard character for a generic specification of a set of message IDs that follow a certain pattern, for example "*E". The default value is `EEZR*E EEZA*E`.

[Use `cfgsmu`] Configuring the Universal Automation Adapter

The Service Management Unite Automation Universal Automation Adapter configuration dialog helps you to configure the Universal Automation Adapter settings.

To open the configuration dialog, select the check box of **Enable Universal Automation Adapter configuration**, and then click **Configure** in the **Universal Automation Adapter** section of the task launcher window.

Adapter tab

Use the **Adapter** tab to configure the parameters of the host system on which the adapter is running and the parameters that are required for the Universal Automation Adapter policy.

Specify values for the following parameters:

Request port number

The number of the port on which the Universal Automation Adapter listens for requests from the SA z/OS E2E agent or the operations console. The default port is 2005.

Policy pool location

The fully qualified path name of the directory that contains the Universal Automation Adapter policies. These policies define resources on non-clustered nodes that are managed by the Universal Automation Adapter. Click **Browse** to select the policy pool.

Automation domains managed by the Universal Automation Adapter

The list of automation domain names. Each domain represents a set of resources on unclustered nodes that are managed by the Universal Automation Adapter. A domain name must match the domain name value that is defined in the policy file. This policy file defines the corresponding set of resources.

Use **Add**, **Remove**, and **Rename** to main the entries in the domain list.

- **Add**

  Click **Add** to add a domain that is managed by the Universal Automation Adapter.
- **Remove**

  Select the domain from the list and click **Remove** to remove from the domain list.
- **Rename**

  Select the domain from the list and click **Rename** to change the name of the domain that is managed by the Universal Automation Adapter. Ensure that this domain name is unique in the set of all automation domains you work with. The maximum length of the domain name is 64 characters.

Note: You must recycle the Universal Automation Adapter if a domain is added or removed within the configuration tool.

Advanced
The advanced settings of the Universal Automation Adapter.

- **Adapter stop delay**

  The time that the stop of adapter is delayed. It allows the adapter to properly deliver the domain leave event. The default value is 5. The value ranges between 3 through 60 seconds.

- **Remote contact activity interval**

  The time after which the automation adapter stops if there is no communication with the SA z/OS E2E agent or the operations console. The default value is 360. The value changes between 0 through 360. If you specify '0', the adapter never stops. It continues to run and waits until it is contacted again by the SA z/OS E2E agent or the operations console.

- **Initial contact retry interval**

  The time within which the Universal Automation Adapter tries to contact the SA z/OS E2E agent host and the operations console host until it succeeds or the specified time elapses. The default value is 0, which means the adapter tries to contact the SA z/OS E2E agent host and the operations console host indefinitely. The value ranges between 0 through 1440.

- **Enable EIF event caching**

  If you select this check box, all events that can not be sent are cached.

  This can help to recover in cases where the connection to the SA z/OS E2E agent host or the operations console host is interrupted for a short period so that cached events can be sent when the connection is available again. If the cache limit is exceeded, cached events are discarded and the adapter sends a "domain offline" followed by a "domain online" event to the SA z/OS E2E agent host or the operations console host.

  If this check box is not selected, all events that can not be sent are discarded immediately.

- **EIF reconnect attempt interval**

  The time that the Universal Automation Adapter waits until it tries to reconnect if the connection to the SA z/OS E2E agent host or the operations console host is interrupted. The default value is 30.

Click **OK** to save the settings internally and the settings are stored in the corresponding configuration file if you click **Save** in the Universal Automation Adapter window.

Click **Defaults** to restore the settings to the default values.

Click **Cancel** to close the dialog without saving the settings.

Click **Help** to display the online help information.

SA z/OS E2E Agent tab

Use the SA z/OS E2E Agent tab to configure the Universal Automation Adapter to manage first level domains for unclustered nodes.

Host name or IP address
The name or the IP address of the host on which the SA z/OS E2E agent runs.

Event port number
The number of the port on which the SA z/OS E2E agent listens for events from the automation adapter. This port has to match the corresponding event port number that you specify when configuring the SA z/OS E2E agent. The default port is 2003.

If you do not want the SA z/OS E2E agent to perform end-to-end automation for any domain that is managed by the Universal Automation Adapter, you can leave the host and port fields empty.

The Universal Automation Adapter also sends events to the Service Management Unite operations console. You have defined the corresponding host name or IP address and port number on the host tab of the Service Management Unite operations console configuration.

User Credentials tab

Use the **User Credentials** tab to configure credentials of the Universal Automation Adapter. These credentials are used to access remote nodes that host remote resources that are managed by the Universal Automation Adapter.

The user ID that you specify for a resource in a Universal Automation Adapter policy is used to determine how authentication is performed on the remote node where that resource resides. The following is the priority sequence in which the Universal Automation Adapter determines how authentication on remote nodes is performed:

- The user ID that is specified for a resource in the universal automation adapter policy is defined in the specific non-clustered nodes credentials list on this tab: The universal automation adapter uses the password that is associated with this specific user ID.
- The user ID that is specified for a resource in the universal automation adapter policy is defined as generic user ID on this tab: The universal automation adapter uses the password that is associated with this generic user ID.
- User authentication is performed using SSH public and private keys for the user ID that is specified for a resource in the universal automation adapter policy. In this case, SSH key authentication must be enabled and configured on the Security tab.

Generic user ID

The generic user ID to access non-clustered nodes for which no specific credentials are defined and no SSH key authentication is used.

Generic password

The generic password to access non-clustered nodes.

Click **Change** to specify and confirm the generic password that is used by the Universal Automation Adapter. Note this will not change a password on any of the non-clustered nodes.

Generic credentials are optional. If you want to remove already configured generic credentials, leave the generic user ID field empty.

Credentials for accessing specific non-clustered nodes

Specific user credentials can be defined explicitly for each non-clustered node that is accessed by the universal automation adapter for which no SSH key authentication is used. The non-clustered nodes list shows the pairs of node name and user ID for which specific access credentials are currently defined. Use the Add, Remove, and Modify buttons to maintain the entries in the node list.

Add

Click **Add** to define a new user ID and password to access remote nodes.

Remove

Select a user ID and click **Remove** to remove an entry from the list, s.

Modify

Select an entry from the list and click **Modify** to edit the node name, user ID, or password.

Node name

The name of the non-clustered node for that you want to change credentials.

User ID

The user ID that is used by the Universal Automation Adapter to access the selected node.

Password

The password that is used by the Universal Automation Adapter to access the selected node. Click **Change** to specify and confirm the password.

Note:

1. If an IPv6 host name is specified as node name, the DNS server must be configured to return IPv6 records only.
2. If the DNS server is configured to return IPv4 and IPv6 records, only the IPv4 address is used. To use IPv6, explicitly specify the IPv6 address as node name instead of the host name.

Use the tools that are provided by the operating system to resolve your IPv6 host name to the IPv6 address in that case. For example, on Linux use the host or nslookup commands:

```
host -a <ipv6_hostname>
```

Or to display DNS records:

```
nslookup <ipv6_hostname>
```

You can decide to use SSH public and private keys for user authentication between the Universal Automation Adapter and remote non-clustered nodes on the Security tab. In this case, do not define specific credentials for any pair of node name and user ID for which you want to use the SSH key authentication approach.

Security tab

Use the **Security** tab to configure security settings for the communication between the Universal Automation Adapter and other systems.

Secure Sockets Layer (SSL) for transport

Configure SSL for data transport between the Universal Automation Adapter and the operations console.

Enable SSL for data transport between the automation host and the Universal Automation Adapter

Check to use SSL for data transport between the SA z/OS E2E agent or the operations console and the Universal Automation Adapter. If you select to enforce that all first-level automation adapters including Universal Automation Adapters must be properly configured to use SSL at the transport layer before they successfully connect to the operations console, you must enable SSL here.

Truststore

The name of the truststore file that is used for SSL.

Click **Browse** to select the truststore file.

For more information on how to generate Keystore and Truststore files, refer to “Creating keystores and truststores with SSL public and private keys” on page 66.

Keystore

The name of the keystore file that is used for SSL.

Click **Browse** to select a keystore file.

Keystore password

The password of the keystore file.

Click **Change** to change the password.

Note: Passwords must be identical if truststore and keystore are in two different files.

Certificate alias

The alias name of the certificate that is used by the Universal Automation Adapter.

User authentication

Enforce user authentication between the automation host and the Universal Automation Adapter

Check to enable the authentication of users on the system where the universal automation adapter is running when the universal automation adapter is contacted by the operations console. If not checked, user authentication is bypassed.

Communication between the Universal Automation Adapter and remote non-clustered nodes

The user ID that you specify for a resource in a Universal Automation Adapter policy is used to determine how authentication is performed on the remote node where that resource resides. The following is the priority sequence in which the Universal Automation Adapter determines how authentication on remote nodes is performed:

- The user ID that is specified for a resource in the Universal Automation Adapter policy is defined in the specific non-clustered nodes credentials list on the User Credentials tab: The Universal Automation Adapter uses the password that is associated with that specific user ID.
- The user ID that is specified for a resource in the Universal Automation Adapter policy is defined as generic user ID on the User Credentials tab: The Universal Automation Adapter uses the password that is associated with that generic user ID.
- User authentication is performed using SSH public and private keys for the user ID that is specified for a resource in the Universal Automation Adapter policy. In this case, SSH key authentication must be enabled and configured on this tab.

Enable user authentication with SSH public and private keys

Check to use SSH keys for authentication of users for which you define neither generic nor specific access credentials on the User Credentials tab.

SSH private key file

The fully qualified name of the private key file that is generated by the **`ssh-keygen`** utility. The default names of files that are generated by **`ssh-keygen`** are `id_dsa` or `id_rsa`. Ensure that the user ID under which the Universal Automation Adapter is running has read access for this file.

Click **Browse** to select a key file.

Private key passphrase

The passphrase that you use to generate the private key file using the **`ssh-keygen`** utility.

Click **Change** to specify and confirm the passphrase. The passphrase is optional, because you can omit it when you use the **`ssh-keygen`** utility. To remove a passphrase, leave the entry fields in the dialog empty and click **OK**.

Logger tab

Use the **Logger** tab to specify settings for logging, tracing, and First Failure Data Capture (FFDC) for the Universal Automation Adapter.

Maximum log/trace file size

The maximum disk usage in KB that a log file can reach. If the limit is reached, another log file is created. The maximum number of log files is two, which means that the oldest file gets overwritten after both files are filled up. The default maximum file size is 1024 KB.

Message logging level

Error

Only error messages are logged.

Warning

Only error and warning messages are logged.

Information

Error, warning, and information messages are logged. This is the default message logging level.

Trace logging level

Off

Trace logging is disabled.

Minimum

Only a minimum of trace data is logged.

Medium

A medium amount of trace data is logged. This is the default trace logging level.

Maximum

The maximum amount of trace data is logged.

First failure data capture (FFDC) recording level

Select the FFDC recording level, depending on the severity of the incidents for which you want FFDC data to be collected.

Off

FFDC recording is disabled.

Minimum

Only a minimum of FFDC data is recorded.

Medium

A medium amount of FFDC data is recorded. This is the default FFDC recording level.

Maximum

The maximum amount of FFDC data is recorded.

First failure data capture (FFDC) disk space

Maximum disk space

The maximum disk space in bytes that is used to store FFDC data. The default maximum disk space is 10485760 bytes (10 MB).

Space exceeded policy

The maximum disk space in bytes that is used to store FFDC data. The default maximum disk space is 10485760 bytes (10 MB).

Select the space exceeded policy

Ignore

Issue a warning, but do not enforce the FFDC disk space limitation.

Auto-delete

Automatically delete FFDC files to enforce the FFDC disk space limitation. This is the default space exceeded policy.

Suspend

Halt further FFDC actions until disk space is freed manually.

First failure data capture (FFDC) message IDs

Filter mode

Passthru

All log events with messages that are specified in the message ID list will pass the filter and FFDC data is written. This is the default filter mode.

Block

All log events with messages that are specified in the message ID list are blocked.

Message ID list

First failure data capture (FFDC) message ID list

The message IDs that control for which log events FFDC data is written, depending on the filter mode. The comparison of message IDs is case sensitive. Each message ID must occur in a new line. Note you may use "*" as a wildcard character for a generic specification of a set of message IDs that follows a certain pattern, for example "*E". The default value is "EEZR*E EEZA*E".

Controlling the Universal Automation Adapter

Use the `eezuaadapter` command to start, stop, and monitor the Universal Automation Adapter. To control the Universal Automation Adapter, run the command on the system where the Service Management Unite Automation operations console is installed.

Configuring Universal Automation Adapters in silent mode

You can configure Universal Automation Adapters in silent mode as an alternative to using the configuration dialogs.

Use the silent mode when you configure the Universal Automation Adapter. Refer to "Configuring SMU Automation in silent mode" on page 81 for a detailed description of the silent mode configuration tasks.

Tuning the number of domains and resources of the Universal Automation Adapter

The number of resources that can be managed by Universal Automation Adapter without performance degradation depends on the hardware. Your performance depends in particular on processor power and CPU cycles that are available on the system where the Universal Automation Adapter runs. Make sure that CPU and memory utilization is not higher than 80% after policy activation.

Depending on your hardware capabilities, the numbers that are given in the following recommendations may vary slightly. Adhering to these recommendations provides good performance using Universal Automation Adapter.

Recommendations for the Universal Automation Adapter:

1. Do not define more than 20 domains.
2. Do not include more than 50 resources in each domain.
3. Do not define more than 150 remote resources in total.

For the Universal Automation Adapter, balance the number of resources per domain by including a similar number of resources in each domain.

Configuring SMU Automation in silent mode

You can configure Service Management Unite Automation and the automation adapters without starting the configuration dialogs by using the configuration tool in silent mode. If you use the silent configuration mode, you do not need to have an X Window session available.

- You can use the silent mode to perform the following configuration tasks:
  - Configuring Service Management Unite Automation common settings
  - Refreshing the Service Management Unite Automation common configuration.
- You can use the configuration tool in silent mode to configure the following components:
  - Service Management Unite Automation operations console host
  - Universal Automation Adapters

You configure these components by editing configuration parameter values in an associated properties file. The parameter values in each properties file correspond directly to the values that you enter in the configuration dialog. You must first start the configuration tool to generate silent mode input properties files before you process a configuration update.

To use the configuration tool in silent mode, you need to follow these steps for each component that you want to configure:

1. Generate or locate the silent mode input properties file.
2. Edit the parameter values in the file.
3. Start the configuration tool in silent mode to update the target configuration files.
4. If the configuration tool does not complete successfully, deal with any errors that are reported and start the configuration tool again.

Processing tasks manually

No silent configuration support is available to refresh first level automation (FLA) domain access credentials. After you have added or changed your FLA domain access credentials, you can use the refresh function of the configuration dialog to initiate a reload of the credentials by the operations console. If you do not want to use the configuration dialogs, you must recycle the WebSphere Application Server that hosts the operations console instead.

Generating silent mode input properties file

This information provides information about how to generate a silent mode input properties file from the values that are currently configured, and use it to modify configuration settings in silent mode.

The silent input properties file has the following advantages:

- You can generate properties files immediately after installation and before you process the customization.
- If you customize with the configuration dialog and in silent mode, you can first generate an up-to-date input file before you apply changes in silent mode.
- You can easily recover from the accidental deletion of the silent mode input properties file.

To generate a silent mode input properties file, use one of the following options when you start silent configuration:

-g
Generate the input properties file only if it does not exist.

-gr
Generate the input properties file and replace it if it exists.

-l *location*
The input properties file for silent configuration is in the directory that is specified with *location*. If `-l` is omitted, the input properties file is in the default directory <`EEZ_CONFIG_ROOT`>.

Depending on the target configuration, Table 11 on page 82 shows the silent input properties files that are generated if the **`-g`** or **`-gr`** option is specified.

Table 11. Generated input properties files

Component	Target configuration	Silent input properties file
IBM Service Management Unite operations console	**`cfgsmu -s -z -g	-gr`**	**`<EEZ_CONFIG_ROOT>/ silent.smuhost.properties`**
	**`cfgsmu -s -z -g	-gr -l`** *location*	*location***`/ silent.smuhost.properties`**
Universal Automation Adapter	**`cfgsmu -s -eu -g	-gr`**	**`<EEZ_CONFIG_ROOT>/ silent.eezaladapt.properties`**
	**`cfgsmu -s -eu -g	-gr -l`** *location*	*location***`/ silent.eezaladapt.properties`**

If you update configuration settings in silent mode, the silent properties file is used as input for the update task. If you want the configuration tool to retrieve the input file from a location other than in the <`EEZ_CONFIG_ROOT`> directory, use the **`-l`** *location* option.

Editing the input properties file

Modify the values in the input properties file to change the configuration in silent mode.

The input properties files that are generated for each of the components contain configuration parameter keyword-value pairs. The structure, terminology, and wording of the properties content and the configuration dialog are identical. This fact makes it easy to switch between modes and minimizes errors when you edit the properties file.

The names of tabs, for example **Host name or IP address**, on the configuration dialog are used as identifiers in the properties file, for example:

```
# ===============================================================================
# ... Host name or IP address
```

Each field name on the configuration dialog, for example **Host name or IP address**, is contained in the properties file, followed by a brief description and the keyword for that field, for example:

```
#     ----------------------------------------------------------------------
#  ... Host name or IP address
#      The name or IP address of the WebSphere Application Server hosting the operations
#      console. Although this has to be on the local system, do not specify 'localhost'.
#      Instead use the host name of this server or its IP address.
host-oc-hostname=my.oc.host
#
```

To edit the properties file, locate the keyword that is associated with the value that you want to change and overwrite the value.

If you set the value of a required keyword to blank or comment out the keyword, the value that is defined in the target configuration file remains unchanged.

Note:

1. If a keyword is specified several times, the value of the last occurrence in the file is used.
2. Each value must be specified on one single line.

Starting silent configuration

Use the command **`cfgsmu -s`** to start silent configuration.

About this task

Because silent configuration is an alternative to the configuration dialog, silent mode is started by using the same command. For each component, you specify the `-s` option after the command to start the configuration tool.

Procedure

1.
2. Issue the following commands to configure
   a) Process configuration tasks for the IBM Service Management Unite common configuration:

   ```
   cfgsmu -s -z [-r]
   ```

   b) Configure the IBM Service Management Unite Universal Automation Adapter:

   ```
   cfgsmu -s -eu
   ```

Output in silent mode

Inspect the output that is generated by the configuration tool in silent mode.

Start the configuration tool in silent mode by using one of the commands described in "Generating silent mode input properties file" on page 82. This task leads to output that closely matches the output that is displayed in interactive mode in the update status dialogs or in the message boxes. The silent mode output falls into one of the following categories:

No update
: There are no configuration updates to be saved. All parameters in all target configuration files already match the specified silent input parameters. No errors were detected when the silent input parameters were checked. If additional information is available or any warning conditions are detected, the information and warnings are reported. If warnings are reported, the configuration tool issues return code "1" rather than "0". You might need to observe the return code when you start silent configuration, for example within a shell script.

Successful completion
At least one of the target configuration files is updated and all configuration files and their update status are listed. No errors are detected when you check the silent input parameters. If additional information is available or any warning conditions are detected, the information and warnings are reported. If warnings are reported, the configuration tool issues return code "1" rather than "0". You might need to observe the return code when you start silent configuration, for example within a shell script.

Unsuccessful completion
No target configuration file is updated. Any errors that are detected when you check the silent input parameters are reported. The configuration tool stops and issues return code "2".

Silent input properties file generation
Values from the target configuration files are used to generate the input file. No target configuration file is updated.

Unrecoverable error
Error messages report the reason for the error. The configuration tool stops and issues a return code greater than "2".

Configuring properties files

Configuration properties files are used to store the settings of the IBM Service Management Unite Automation operations console host and Universal Automation Adapters.

SMU Automation configuration properties files

To change the values of the properties, use the Service Management Unite Automation `cfgsmu` configuration tool. The **`cfgsmu`** command ensures that the files are not corrupted during manual editing and that the change history in the files is updated whenever a property is changed.

It also ensures that dependencies between parameter values in different properties files are observed.

For more information about the `cfgsmu` configuration tool, refer to "Overview of the cfgsmu configuration tool" on page 62.

The configuration properties files of Service Management Unite Automation are in the following directory:

`<EEZ_CONFIG_ROOT>`

The following list describes the properties files that are changed when you modify a property value by using the `cfgsmu` configuration tool:

`eez.automation.engine.properties`
The properties in this file are used to configure the operations console host. The configuration properties specify, for example, the operations console host name or IP address.

`eez.automation.engine.dif.properties`
The domain identification file contains the user IDs and the passwords to authenticate to first-level automation domains.

`eez.fla.ssl.properties`
This file contains the configuration properties for the SSL connection to the first-level automation domains.

`eez.aladapter.properties`
The properties in this file are used to configure the Universal Automation Adapter. For example, the host and port the Universal Automation Adapter listens on, or the host and port of the automation framework it communicates with.

`eez.aladapter.dif.properties`
The properties in this file are used to configure the user IDs and the corresponding passwords that the Universal Automation Adapter uses to access remote non-clustered nodes. The resources that the Universal Automation Adapter starts, stops, and monitors are on remote nodes.

eez.aladapter.ssh.properties
The properties in this file are used to configure security settings that are related to SSH private keys. SSH keys can be configured for user authentication on remote non-clustered nodes as an alternative to configuring credentials in the `eez.aladapter.dif.properties` file for the Universal Automation Adapter.

eez.aladapter.ssl.properties
The properties in this file are used to configure Secure Sockets Layer (SSL) for transport between the automation framework and the Universal Automation Adapter.

eez.aladapter.jaas.properties
This file contains the configuration of the LoginModule that is used for user authentication between the automation framework and the Universal Automation Adapter.

eez.aladapter.jlog.properties
The properties in this file determine which information is written to the log and trace files of the Universal Automation Adapter.

eez.aladapter.plugin.properties
The properties in this file are used to configure settings that are unique for the Universal Automation Adapter: for example, the location of the XML policy pool.

eez.aladapter.plugin.<domain>.properties
For each Universal Automation Adapter domain, a domain-specific copy of `eez.aladapter.plugin.properties` is created:

User-based configuration properties files

Some configuration properties of Service Management Unite Automation are stored for a user.

Refer to “Administering users, groups, and roles” on page 99. For each user, a unique configuration properties file can be stored. Additionally, a global configuration properties file can be specified, allowing the administrator to configure a default behavior for Service Management Unite Automation.

The user-based configuration properties files are located in the following directory where `JazzSM_root` depends on your installation:

```
<JazzSM_root>/profile/Tivoli/EEZ
```

Refer to “Default directories” on page 27 for the default path of `JazzSM_root`.

The global configuration properties file is `properties.dat`. The name of a user-based configuration properties file is `<user_name>_properties.dat`, where `<user_name>` is the name of the user with all "." and "/" replaced by "_".

If there are no properties configured (globally or for a specific user), the files are optional.

The user-based configuration properties files are written by Service Management Unite Automation and are not intended for manual editing. The global configuration properties file `properties.dat` can be edited by an administrator with an editor of his choice. A restart of the WebSphere Application Server is necessary to enable changes to this file.

The following precedence is used by Service Management Unite Automation to search for a property:

1. `<user_name>_properties.dat` of the current user
2. `properties.dat`
3. default configuration (hard-coded)

This means that user-based configurations in general overwrite the global configurations.

If, for example, the property "a" is defined in the `<user_name>_properties.dat` for the current user and in the `properties.dat`, the value of the user-based configuration properties file is taken. If another user has no `<user_name>_properties.dat` or it does not contain the property "a" for this user, the value of the global configuration properties file is taken.

Some of the configurations are not allowed to be changed on a user basis, in general due to security restrictions. For these configuration properties Service Management Unite Automation only searches the global configuration properties and the default configuration.

The following properties values are currently available:

Property	User-based	Description
`prefdom`	yes	*Preferred automation domain*. The domain that is selected per default when the user opens the *Domain and Automation Health* dashboard.
`syslog_global_limit`	no	*Maximum number of system log messages* that are loaded per request from its source into the *System Log* dashboard.
`mandatory_comments`	no	Defines if comments in request dialogs are mandatory or not. Possible values: `true` - The comment in a request dialog, for example, to issue an offline request or suspend automation for a resource, is mandatory. You have to enter a comment. Otherwise the OK button of the dialog is not enabled. `false` - The comment field is optional. You can click OK in the dialog even if no comment has been specified. This is the default.

Configuring an LDAP user registry (optional)

If you don't want to use the default file-based user repository for managing WebSphere Application Server users, you can configure a central user registry, such as a Lightweight Directory Access Protocol (LDAP) registry, for user management and authentication.

Configure WebSphere Application Server to use the LDAP user registry as a federated repository. The WebSphere Application Server uses this registry for user authentication and the retrieval of information about users and groups to run security-related functions.

For more information about how to configure a federated user repository in WebSphere Application Server, see Managing the realm in a federated repository configuration.

Procedure for pre-defined LDAP setup

1. Install Jazz for Service Management including WebSphere Application Server and Dashboard Application Services Hub (DASH).
2. LDAP configuration
   a. Add the LDAP user registry as a federated repository to the WebSphere Application Server.
   b. Configure the supported entity types so that new users and groups are created in the LDAP user repository.
3. Install IBM Service Management Unite Automation.

4. Optional: Configure the connection to the LDAP server for secure communications. For more information, see Configuring an SSL connection to an LDAP server.

Procedure for post-defined LDAP setup

1. Install Jazz for Service Management including WebSphere Application Server and Dashboard Application Services Hub (DASH).
2. Install IBM Service Management Unite Automation.
3. LDAP configuration
   a. Add the LDAP user registry as a federated repository to the WebSphere Application Server.
   b. Configure the supported entity types so that new users and groups are created in the LDAP user repository.
4. Port from a file-based repository to an LDAP repository
   a. Create users and groups to use with IBM Service Management Unite Automation in the LDAP repository if they do not exist.
   b. Authorize the LDAP groups within the Dashboard Application Services Hub.
   c. Remove duplicate users from the file-based user repository.
5. Optional: Configure the connection to the LDAP server for secure communications. For more information, see Configuring an SSL connection to an LDAP server.

The core LDAP configuration is done in the same way for both pre-defined and post-defined setup. This LDAP configuration is described in the next sections.

Setting up an LDAP user registry

Information about users and groups is stored in a user registry. By default, the WebSphere Application Server that is installed with Jazz for Service Management and is used by IBM Service Management Unite Automation is configured to use a local file-based user repository.

Companies often use a central user registry that is based on the Lightweight Directory Access Protocol (LDAP) to manage users and groups company-wide and provide single sign-on to every service. Examples for LDAP servers:

- IBM Tivoli Directory Server
- Resource Access Control Facility (RACF®)
- Windows Server Active Directory
- OpenLDAP

You can set up an LDAP server and create an LDAP user registry to use with IBM Service Management Unite Automation. The WebSphere Application Server uses this registry for user authentication and the retrieval of information about users and groups to run security-related functions.

There are two different setup types:

Pre-defined

The LDAP user repository is configured in the WebSphere Application Server before the installation of IBM Service Management Unite Automation.

The installer of IBM Service Management Unite Automation can already use the configured LDAP repository for user creation and role assignments.

Post-defined

The LDAP user repository is configured in the WebSphere Application Server after the installation of the IBM Service Management Unite Automation.

If you reconfigure the user repository after you installed IBM Service Management Unite Automation, you must complete extra steps to port from a file-based repository to an LDAP user repository.

Adding the LDAP user registry as a federated repository

Federated repositories can access and maintain user data in multiple repositories, and federate that data into a single federated repository. For example, use the default file-based repository and an LDAP repository that is combined under a single realm.

Pre-requisites for this task:

Set up an LDAP server and create an LDAP user registry. Ensure that WebSphere Application Server supports the LDAP user registry as a federated repository, for example, IBM Tivoli Directory Server or Microsoft Active Directory Server.

Before you configure a central user registry, make sure that the user registry or registries that you plan to identify are started. The user registry must be accessible from the computer where you set up the Jazz for Service Management application server.

Configuring an LDAP user repository

Configure the LDAP user repository by running the following steps:

Procedure

1. Open your web browser and connect to the WebSphere administrative console.
2. Enter the WebSphere administrator user ID and password, and click **Log in**.
3. Select **Security > Global security**.
4. From the **Available realm definitions** list, select **Federated repositories** and click **Configure**.
5. In the **Related Items** area, click the **Manage repositories** link and then click **Add > LDAP repository** to configure a new LDAP user repository.
6. In the **Repository identifier** field, provide a unique identifier for the repository. The identifier uniquely identifies the repository within the cell.
   For example, `LDAP1`.
7. From the **Directory type** list, select the type of LDAP server. The type of LDAP server determines the default filters that are used by WebSphere Application Server. If you choose one of the predefined LDAP servers, you get default definitions for the mapping of entity types to corresponding object classes and for the attribute name that is used to determine group membership. If you choose **Custom** as directory type, you must specify these definitions as **Additional Properties** depending on your specific LDAP server. For more information, see "Configuring custom LDAP servers" on page 89.
8. In the **Primary host name** field, enter the fully qualified host name of the primary LDAP server. The primary host name and the distinguished name must contain no spaces. You can enter either the IP address or the domain name system (DNS) name.
9. In the **Port** field, enter the server port of the LDAP user registry.

   The default port value is 389, which is not a Secure Sockets Layer (SSL) connection port. Use port 636 for a Secure Sockets Layer (SSL) connection. For some LDAP servers, you can specify a different port. If you do not know the port to use, contact your LDAP server administrator.
10. Optional: In the **Bind distinguished name** and **Bind password** fields, enter the bind distinguished name (DN) (for example, `cn=root`) and password.

    The bind DN is required for write operations or to obtain user and group information if anonymous binds are not possible on the LDAP server. In most cases, a bind DN and bind password are needed, except when an anonymous bind can satisfy all of the functions. Therefore, if the LDAP server is set up to use anonymous binds, leave these fields blank.
11. Optional: In the **Login properties** field, enter the property names used to log in to the WebSphere Application Server. This field takes multiple login properties, delimited by a semicolon (;).
    For example, `uid`.
12. Optional: From the **Certificate mapping** list, select your preferred certificate map mode. You can use the X.590 certificates for user authentication when LDAP is selected as the repository.

The **Certificate mapping** field is used to indicate whether to map the X.509 certificates to an LDAP directory user by `EXACT_DN` or `CERTIFICATE_FILTER`. If you select `EXACT_DN`, the DN in the certificate must match the user entry in the LDAP server, including case and spaces.

13. Click **Apply** and then **Save**.

Configuring custom LDAP servers

If you chose `Custom` as directory type and not one of the predefined LDAP servers, define manually the mapping of entity types to corresponding object classes and the attribute name that is used to determine group membership.

Procedure

- **Set the object class for an entity type.**
  If you chose `Custom` as directory type and not one of the predefined LDAP servers, you must manually specify the object classes that are used in your LDAP server for the entity types `PersonAccount` and `Group`. A `PersonAccount` represents a user, whereas a `Group` represents a group of users.
  a) On the configuration page of your LDAP repository in the **Additional Properties** area, click **Federated repositories entity types to LDAP object classes mapping**.
  b) Click **New** to define a new entity type to class mapping.
  c) Specify a mapping for the **PersonAccount** entity type. As object classes, specify the object classes that are mapped to this entity type. Multiple object classes are delimited by a semicolon (;). For example, enter `PersonAccount` in the **Entity type** field, and enter `iNetOrgPerson` in the **Object classes** field to define that LDAP entries that have the object class `iNetOrgPerson` are mapped to the `PersonAccount` entity type.
  d) Click **Apply** and then **Save**.
  e) Specify a mapping for the `Group` entity type. As object classes, specify the object classes that are mapped to this entity type. Multiple object classes are delimited by a semicolon (;). For example, enter `Group` in the **Entity type** field, and enter `groupOfNames` in the **Object classes** field to define that LDAP entries that have the object class `groupOfNames` are mapped to the `Group` entity type.
  f) Click **Apply** and then **Save**.
- **Define group membership attribute**
  If you chose `Custom` as directory type and not one of the predefined LDAP servers, you must manually configure how group membership is modeled in your LDAP server. Model the group membership in the **Group attribute definition** properties of the repository. There are two main ways of specifying group membership. Configure the group membership depending on which group membership definition is supported by your LDAP server:

Option	Description
Static group membership that is defined in Group entity.	The `Group` entity has an attribute, for example member, which points to its members. The member attribute in this example is called the group member attribute. All LDAP server implementations support static group membership. If the group member attribute of the group is used, specify the name of the object class, and the attribute name that is used to indicate the group membership in **Group attribute definition -> Member attributes**. If the group `objectclass` for the user is `groupOfUniquePersons`, and within that `objectclass` members are listed as `persons`, then the static group `Member attributes` property is set as follows: 1. On the configuration page of your LDAP repository in the **Additional Properties** area, click **Group attribute definition**. 2. Under **Additional properties**, click **Member attributes**.

Option	Description
	3. Click **New** to specify a new member attribute. Set the **Name of member attribute** field to persons. Set the **Object class** field to groupOfUniquePersons. 4. Click **Apply** and then **Save**.
Direct group membership.	The PersonAccount entity has an attribute, for example, memberof, which points to the groups that this person belongs. The memberof attribute in this example is called the group membership attribute. Some LDAP servers support this kind of linking user objects to the groups to which they belong, for example Microsoft Active Directory Server. Use direct group membership if it is supported by the LDAP server. If the group membership attribute in the PersonAccount entity is used, specify the group membership attribute in **Group attribute definition -> Name of group membership attribute**. For example, if a PersonAccount entity (that is, a user) contains attributes called ingroup that contain each group membership, then you specify the direct group membership as follows: 1. On the configuration page of your LDAP repository in the **Additional Properties** area, click **Group attribute definition**. 2. Set the **Name of group membership attribute** field to ingroup. 3. Click **Apply** and then **Save**.

Adding configured LDAP repository as federated repository to the security realm

To add an already configured LDAP user repository as federated repository to the security realm, complete the following steps:

Procedure

1. On the **Global security > Federated repositories** page, click **Add repositories (LDAP, custom, etc)...**.
2. To add an entry to the base realm:
   a) Ensure that the LDAP federated repository is selected from the **Repository** list.
   b) In the field, enter the distinguished name (DN) of a base entry that uniquely identifies this set of entries in the realm. This base entry must uniquely identify the external repository in the realm.

      Note: If multiple repositories are included in the realm, use the **DN** field to define an extra distinguished name that uniquely identifies this set of entries within the realm. For example, repositories LDAP1 and LDAP2 might both use o=ibm,c=us as the base entry in the repository. So o=ibm,c=us is used for LDAP1 and o=ibm2,c=us for LDAP2. The specified DN in this field maps to the LDAP DN of the base entry within the repository, such as o=ibm,c=us b. The base entry indicates the starting point for searches in this LDAP server, such as o=ibm,c=us c).
3. In the administrative console, select **Security > Global security**.
4. From the **Available realm definitions** list, select **Federated repositories** and click **Set as current** to mark the federated repository as the current realm.
5. Restart the WebSphere Application Server.
6. Verify that the federated repository is correctly configured:
   a) In the administrative console, click **Users and Groups > Manage Users**.
   b) Confirm that the list of displayed users includes users from both the LDAP federated repository and the local file registry.
   c) Click **Users and Groups > Manage Groups**.
   d) Confirm that the list of displayed groups includes groups from both the LDAP federated repository and the local file registry.

Note: Verify that the default administrative user (for example, `wasadmin`) that is created during installation of Jazz for Service Management is in the local file registry. If IBM Service Management Unite Automation is installed before the LDAP repository is configured, also the users and groups that are generated during the installation are in the local file registry.

Configuring supported entity types

Configure the supported entity types before you can create users and groups in your LDAP repository in the administrative console.

This configuration specifies which RDN property is used for the default entity types, for example users and groups, and where in the repository name space these entities are created.

The supported entity types are `Group`, `OrgContainer`, and `PersonAccount`. A `Group` entity represents a simple collection of entities that might not have any relational context. An `OrgContainer` entity represents an organization, such as a company or a division. A `PersonAccount` entity represents a user that logs in. You cannot add or delete the supported entity types, because these types are predefined.

1. In the administrative console, click **Security > Global security**.
2. From the **Available realm definitions** list, select **Federated repositories** and click **Configure**.
3. Click **Supported entity types** to view a list of predefined entity types.
4. Click the name of a predefined entity type to change its configuration.
5. In the **Base entry for the default parent** field, provide the distinguished name of a base entry in the repository. This entry determines the default location in the repository where entities of this type are placed on write operations by user and group management.
6. Supply the relative distinguished name (RDN) properties for the specified entity type in the **Relative Distinguished Name properties** field. Possible values are `cn` for `Group`, `uid` or `cn` for `PersonAccount`, and `o`, `ou`, `dc`, and `cn` for `OrgContainer`. Delimit multiple properties for the `OrgContainer` entity with a semicolon (;).
7. Click **Apply** and then **Save**.
8. Repeat all steps for all predefined entity types.
9. Restart the WebSphere Application Server.

You can now manage your LDAP repository users in the console through the **Users and Groups > Manage Users** menu item.

Note: When you add a user, check that the user ID you specify does not exist in any of the user repositories. You can avoid difficulties when the new user attempts to log in.

What to do next:

Pre-defined setup:

The LDAP repository is configured and connected to the WebSphere Application Server. Next, install IBM Service Management Unite Automation .

On the **User and Group Administration** page of the installer click **Yes**. The default users and groups for IBM Service Management Unite Automation are created in your configured LDAP user repository. If you already created the default user groups and users for IBM Service Management Unite Automation in the LDAP repository through a previous installation or by adding them manually, click **No**. In this case, the installer does not make changes to users and groups.

Post-defined setup:

If you already installed IBM Service Management Unite Automation and you did not define the default users and groups for IBM Service Management Unite Automation in the LDAP repository, create these users and groups in your LDAP repository as the next step. Assign roles to the new LDAP groups and remove the old groups that are no longer used from the file-based repository.

These steps are explained in "Porting from a file-based repository to an LDAP repository in a post-defined setup" on page 92.

Porting from a file-based repository to an LDAP repository in a post-defined setup

If you configured WebSphere Application Server to use an LDAP repository after you installed IBM Service Management Unite Automation, complete extra steps to port from a file-based repository to an LDAP user repository.

Run the following steps to port the users, groups, and roles that are created during the installation of IBM Service Management Unite Automation to an LDAP-based configuration:

1. Create users and groups to use with IBM Service Management Unite Automation in the LDAP repository if they do not exist. For more information, see "Creating default users and groups" on page 92.
2. Authorize the LDAP groups within the Dashboard Application Services Hub. For more information, see "Authorizing LDAP groups within the Dashboard Application Services Hub" on page 94.
3. Remove duplicate users from the file-based user repository. For more information, see "Removing duplicate users from the file-based user repository" on page 95.

Creating default users and groups

IBM Service Management Unite Automation requires a set of default users and groups. These users and groups are created during the installation of IBM Service Management Unite Automation.

If you configured a new LDAP user repository after IBM Service Management Unite Automation is installed, the default users and groups are created in the local file-based user repository by the installer. In this case, manually create the default users and groups also in the LDAP repository and later delete the old definitions from the file-based repository.

During installation, users and groups are created and mapped to a group role automatically. Table 1 lists these user IDs and user groups and shows which group role they are assigned to.

Table 12. Default user IDs and groups of the Service Management Unite Automation

Default user IDs	**Default groups**	**Group roles**
`eezadmin, eezdmn`	`EEZAdministratorGroup`	`EEZAdministrator`
	`EEZOperatorGroup`	`EEZOperator`
	`EEZConfiguratorGroup`	`EEZConfigurator`
	`EEZMonitorGroup`	`EEZMonitor`

The following steps describe how to set up the default users (for example `eezadmin`), and groups (for example `EEZAdministratorGroup`) in the LDAP repository. If you choose to use different names for users and groups, adjust the described steps.

Procedure

1. Log in to the administrative console.
2. Click **Users and Groups > Manage Users** to create users.
3. Click **Create . . .** to create a new user. Enter the user ID for `eezadmin` and `eezdmn`.
4. Click **Create** to create both users.
5. Click **Users and Groups > Manage Groups** to create groups.
6. Click **Create . . .** to create a new group. Enter the group name of the following groups:
   - `EEZAdministratorGroup`
   - `EEZConfiguratorGroup`
   - `EEZMonitorGroup`
   - `EEZOperatorGroup`

7. Click **Create** to create all groups.
8. To add eezadmin to the following group, click the **Group** name of the following groups and proceed as follows:
   - EEZAdministratorGroup
9. Select the **Members** tab on the selected group page.
10. Click **Add Users . . .**
11. Enter the user name eezadmin into the **Search** field or enter * to see all users.
12. Click **Search**.
13. Select eezadmin and click **Add**.
14. Repeat step 8 - 13 to add **eezadmin** to more than one group.
15. To add eezdmn to the **EEZAdministratorGroup**, click the **Group** name.
16. Select the **Members** tab on the selected group page.
17. Click **Add Users . . .**.
18. Enter the user name **eezdmn** into the search field or enter ***** to see all users.
19. Click **Search**.
20. Select eezdmn and click **Add**.

You created the default users and groups. Since an LDAP repository is shared across multiple IBM Service Management Unite Automation installations, the users and groups must be created only once and can then be used by all IBM Service Management Unite Automation installations that are configured for this LDAP repository.

What to do next

- If you chose non-default group names, the role mapping for the EEZEAR application must be updated, see "Updating the user and role mapping for the EEZEAR application" on page 93.
- Next, assign roles to these groups, so that users that belong to a group have the expected access rights to work with System Automation dashboards in the Dashboard Application Services Hub, see "Authorizing LDAP groups within the Dashboard Application Services Hub" on page 94.

Updating the user and role mapping for the EEZEAR application

If your LDAP user repository uses non-default group names, roles that are used by the IBM Service Management Unite Automation must be adjusted to the group names. If your LDAP user repository uses the default group names, no further action is required.

Procedure

1. Log in to the administrative console as a WebSphere administrative user.
2. Click **Applications > Application Types > WebSphere enterprise application** in the navigation tree on the left side.
3. Click **EEZEAR**.
4. Click **Security role to user/group mapping**.
5. To change the mapping according to your settings, select a role and click **Map Groups.....**
6. Enter in the **Search** field the name of the group you are looking for, or use * to see all available groups.
7. Select the appropriate group and move it to the **Selected** list by using the arrow button **>>**.
8. Remove the groups that you don't use. Otherwise, errors can occur in the WebSphere logs.
9. Save the settings to the master configuration and restart the WebSphere Application Server.

Adapting installation variables

If you ported from a file-based user repository to a central LDAP user repository that is shared by multiple IBM Service Management Unite Automation installations, adapt an installation variable that defines whether a local or an external user repository is used. Otherwise, a later uninstallation of this IBM Service Management Unite Automation installation deletes the default users and groups from the LDAP repository.

Procedure

Change the variable EXTERNAL_USER_REP_ACTIVATE in file <EEZ_INSTALL_ROOT>/uninstall/installvariables.properties to false: EXTERNAL_USER_REP_ACTIVATE=false.

Authorizing LDAP groups within the Dashboard Application Services Hub

Users must have specific roles to work with dashboards that are available in the Dashboard Application Services Hub (DASH). This role assignment is configured in the DASH. Assign the required roles on the user group level, so that all users that belong to a group inherit the same roles.

Roles are assigned to user groups and users during the installation of IBM Service Management Unite Automation.

If you configured a new LDAP user repository after IBM Service Management Unite Automation is installed (see post-defined setup), assign the expected roles to the groups and users that are available in the LDAP repository. At the time of the installation of IBM Service Management Unite Automation, the roles are assigned to the groups, and users are created in the local file-based user repository.

Table 13. Role to group assignments:

Role	Group name
EEZMonitor	EEZMonitorGroup
EEZOperator	EEZOperatorGroup
EEZConfigurator	EEZConfiguratorGroup
EEZAdministrator	EEZAdministratorGroup

The iscadmins role is assigned to the default System Automation administrator (for example eezadmin) and to the default WebSphere administrative user (for example wasadmin):

Table 14. Role to user ID assignment

Role	User ID
iscadmins	eezadmin, wasadmin

You must have at least one user that has the iscadmins role.

Procedure

1. Log in to the **Dashboard Application Services Hub** by using the WebSphere administrative user ID that you specified during installation of Jazz for Service Management (for example wasadmin). This user is in the file-based repository and has the iscadmins role that allows this user to change role assignments.
2. Click Console Settings > Roles in the navigation bar.
3. Click the EEZAdministrator role and then expand the **Users and Groups** section. The **Users and Groups** tables display the current list of users and groups to which the EEZAdministrator role is assigned. If you configured LDAP after IBM Service Management Unite Automation is installed (post-defined setup), the **Groups** table displays the following entry: cn=EEZAdministratorGroup,o=defaultWIMFileBasedRealm. This default configuration is made by the installer that assigns the EEZAdministrator role to the EEZAdministratorGroup that is created in the file-based user repository.
4. Click + (Add Group) in the toolbar of the **Groups** table to add the corresponding EEZAdministratorGroup that exists in the LDAP repository. The **Available Groups** window opens.

5. Enter EEZ* in the **Group ID** field and click **Search** to list all groups that begin with EEZ from the configured federated repositories. The results table lists all EEZ* groups from both the file-based repository and the LDAP repository.
6. Select the `EEZAdministratorGroup` that is defined in LDAP and click **Add** and then **Save**.

   Note: Ensure that you select the group that is defined in LDAP and not the one with the same name that still exists in the file-based repository by examining the distinguished name. If you use other group names in LDAP than you previously used in the file-based repository, you can also assign the EEZ-roles to groups named differently. In this case also adjust the group configuration for the EEZEAR application.
7. Repeat steps 3 – 6 for all EEZ* roles (`EEZAdministrator, EEZConfigurator, EEZMonitor, EEZOperator`). Adjust the mappings so that they match the expected role assignments as listed in the table.
8. Finally, assign the `iscadmins` role to either one of your LDAP groups or to individual LDAP users. For example, if you want all your `EEZAdministrator` users to modify existing dashboards or define new dashboards in the DASH, assign the `iscadmins` role to the LDAP-based `EEZAdministratorGroup`.

Removing duplicate users from the file-based user repository

During the porting from a file-based user repository to an LDAP-based user repository, you might have users and groups that have the same name in both repositories. This setting leads to problems when you try to log on with one of the users that exists in both user repositories.

Procedure

For example, if the functional user id used by the IBM Service Management Unite Automation (default: `eezdmn`) is in the file-based and in the LDAP repository, the EEZEAR application does not start. This prevents the EEZEAR application from being started.

Therefore, you must remove the old System Automation users and groups from the file-based repository.

1. Log in to the **WebSphere administrative console**.
2. Click **Users and Groups > Manage Users**. The users from both the file-based and the LDAP repository are listed.
3. Select the following users:
   a) `eezadmin` with the unique name: `uid=eezadmin,o=defaultWIMFileBasedRealm`
   b) `eezdmn` with the unique name: `uid=eezdmn,o=defaultWIMFileBasedRealm`
4. Click **Delete**. Click **Delete** again in the confirmation dialog to delete both users.
5. Click **Users and Groups > Manage Groups**. The groups from both the file-based and the LDAP repository are listed.
6. Select the following groups:
   a) `EEZAdministratorGroup with the unique name: cn=EEZAdministratorGroup,o=defaultWIMFileBasedRealm`
   b) `EEZConfiguratorGroup with the unique name: cn=EEZAdministratorGroup,o=defaultWIMFileBasedRealm`
   c) `EEZMonitorGroup with the unique name: cn=EEZMonitorGroup,o=defaultWIMFileBasedRealm`
   d) `EEZOperatorGroup with the unique name: cn=EEZOperatorGroup,o=defaultWIMFileBasedRealm`
7. Click **Delete**. Click **Delete** again in the confirmation dialog to delete the selected groups from the file-based repository.
8. Restart WebSphere Application Server and verify that you can log on with your LDAP users into the DASH. See the dashboards for which they are enabled according to their role and group assignments. Also, verify that you can still log in to the WebSphere Application Server administrative console by using your administrative user. The administrative user (for example `wasadmin` by default) is still in the file-based repository.

Results

You now ported the default groups and users that are used by IBM Service Management Unite Automation to an LDAP user repository. You can continue to create further users in your newly configured LDAP repository.

What to do next

Optionally, you can define a different user who is in your LDAP repository as an WebSphere administrative user. Assign the following administrative roles to any of your LDAP users by using the WebSphere Application Server administrative console:

1. Admin Security Manager
2. Administrator
3. ISC Admins

Go to **Users and Groups > Administrative user roles** to assign these roles to a new user.

Working with console preference profiles

Preference profiles are a collection of portal behavior preferences for using the portal. These preferences include the visibility of the navigation tree, contents of the view selection list, and the default view. The portal administrator assigns preference profiles to roles to manage how the navigation area and view selections are displayed to users.

⚠ **Attention:** Each role is limited to one preference profile.

Creating preference profiles

Preference profiles are a collection of console behavior preferences for using the console that are created by the console administrator. Complete the following steps to create a preference profile and assign it to a role:

Procedure

1. Click **Settings > Console Preference Profiles** in the console navigation.

   The **Console Preference Profiles** page is displayed with the list of preference profiles that have already been created in the console.
2. Click **New**.

   The properties panel for the new preference profile is displayed.
3. Required: Enter a descriptive name for the preference profile.

   Consider how the name reflects the roles that have been assigned to it or the console settings that are defined.
4. Optional: Edit the system-provided unique name for the preference profile. Accept the default value or provide a custom value.
5. Optional: Select a theme for the preference profile. IBM recommends the "IBM Design" theme.

   A theme dictates how elements of the console are displayed, such as background colors and contrast. You can select a theme, click **Preview**, and go to areas of the console to assess the impact of your selection. The theme that you select is committed only when you save the preference profile; you can preview other themes before deciding which one is appropriate.
6. Indicate whether the navigation tree should be hidden.

   This option might be preferable when the user has few pages to access and display space in the console is better reserved for page content.
7. Optional: Use the Console Bidirection Options to set the direction to display console content and text.

The default option lets the browser dictate the text and content direction. For example, for Arabic and Hebrew the text is displayed right-to-left, whereas for other languages the text is displayed left-to-right. Alternatively, you can decide to set the text and content direction to either left-to-right or right-to-left. In the **Text direction** list, you can also select **Contextual Input** so that for portlets that include text entry fields, the direction of text is dependent on the language used to enter data.

8. Select which view options should be available for users in the role.
9. Expand the section **Roles Using this Preference Profile**.
10. Click **Add** and select one or more roles to use this preference profile.

    When assigning roles, you might notice some roles missing from the list. This means they are assigned to another preference profile. The role must be removed from the other profile before it can be assigned to this one.
11. Select the default console view for this preference profile.

    The default view is the one that is selected when users in this role log in to the console. This field is enabled when at least one role has been added for this preference profile.
12. Click **Save** to save your changes and return to **Console Preference Profiles**.

Results

The new preference profile is created and listed on the main panel for **Console Preference Profiles**.

Editing console preference profiles

Preference profiles are a collection of console behavior preferences for using the console that are created by the console administrator. Complete the following steps to change the properties or roles assigned to a preference profile:

Procedure

1. In the navigation pane, click **Settings > Console Preference Profiles**.

   The **Console Preference Profiles** page is displayed with the list of preference profiles that have already been created in the console.
2. Click the name of the preference profile that you want to edit.

   The properties panel for the preference profile is displayed.
3. Enter a descriptive name for the preference profile.
4. Edit the system-provided unique name for the preference profile. Accept the default value or provide a custom value.
5. Optional: Select a theme for the preference profile.

   A theme dictates how elements of the console are displayed, for example, background colors and contrast. You can select a theme, click **Preview**, and navigate to areas of the console to assess the impact of your selection. The theme that you select is committed only when you save the preference profile; you can preview other themes before deciding which one is appropriate.
6. Indicate whether the navigation tree should be hidden.

   This might be preferable when the user has few pages to access and display space in the console is better reserved for page content.
7. Optional: Use the Console Bidirection Options to set the direction to display console content and text.

   The default option lets the browser dictate the text and content direction. For Arabic and Hebrew, for example, the text is displayed right-to-left, whereas for other languages the text is displayed left-to-right. Alternatively, you can decide to set the text and content direction to either left-to-right or right-to-left. In the **Text direction** list, you can also select **Contextual Input** so that for portlets that include text entry fields, the direction of text is dependent on the language used to enter data.
8. Select which view options should be available for users in the role.
9. Expand the section **Roles Using this Preference Profile**.

Option	Description
To add roles	Click **Add** and select one or more roles to add to the list. Click **OK** when you have made all of your selections. **Note:** If a role is not listed, it likely means that it has been assigned to another preference profile.
To remove roles	Select one of more roles in the list and click **Remove**. Be certain of your selections. When you delete, there is no warning prompt and the action cannot be undone.
To assign a default view	Select from the **Default console view** section to the side of the role list.

10. Click **Save** to save your changes.

Deleting console preference profiles

Preference profiles are a collection of console behavior preferences for using the console that are created by the console administrator. Complete the following steps to delete a preference profile:

Procedure

1. Click **Settings > Console Preference Profiles** in the navigation pane.

   The **Console Preference Profiles** page is displayed with the list of preference profiles that have already been created in the console.
2. Locate the preference profile that you want to delete in the table provided.

   You can use the filter in the table to type in the preference profile name and quickly display it.
3. In the **Select** column select one or more preference profiles.
4. Click **Delete**.

   A message is displayed at the top prompting you to confirm the deletion.
5. Click **OK**.

Configuring time intervals for Jazz for Service Management

Jazz for Service Management defines default values for the time intervals within which the browser polls for new content. These default values are higher than the values that are required by System Automation to ensure timely visualization when an automation resource changes its state.

During initial installation of IBM Service Management Unite Automation, the timeout values are adjusted automatically. But when service for Jazz for Service Management is installed afterwards, the original default values are restored.

Perform the following steps after installing service for Jazz for Service Management:

1. Open file `/opt/IBM/JazzSM/ui/properties/ActiveMQBroker.properties`.
2. Set the following properties:

   ```
   ActiveMQBroker.timeout=25
   ActiveMQBroker.pollDelay=0
   ActiveMQBroker.pollErrorDelay=5
   ```
3. Save the file and restart WebSphere Application Server.

Modifying the Lightweight Third Party Authentication (LTPA) settings

After the installation of IBM Service Management Unite Automation, you should check whether the LTPA settings are appropriate for your environment.

During installation, the following LTPA parameters are automatically set in WebSphere Application Server:

- LTPA Password is set to the password of the IBM Dashboard Application Services Hub administrator user ID
- LTPA Timeout for forwarded credentials between servers is set to 1440 minutes

  LTPA Timeout is a security-related timeout. Because this timeout is absolute, a user will be logged out and forced to log in to the IBM Dashboard Application Services Hub again when the LTPA timeout is reached even if the user is working with the operations console at the time.

To change the LTPA settings (for example, password and timeout) you use the WebSphere Application Server administrative console. In the administrative console, select **Security > Global Security > Authentication > LPTA**.

Administering users, groups, and roles

Manage users, groups, and roles to work with Service Management Unite Automation and the WebSphere Application Server.

Roles, such as the administrator role, define the rights that each user has. You need to work with your system. One or many users can be members of a group. You can define users and groups in a user registry or repository. Roles define the rights a user has. An example for a role is the administrator. You need to map a user or a group to a role, to grant the user any rights to work with the WebSphere Application Server or the Dashboard Application Services Hub. Users and groups are mapped to `Roles` in the Dashboard Application Services Hub.

If you want to use a central, LDAP-based user repository to hold your users and groups, see "Configuring an LDAP user registry (optional)" on page 86.

User credentials

The following table gives you an overview of the usage of the different user IDs that are used to operate on resources hosted by various automation adapters.

Table 15. User credentials to operate on resources hosted by different automation adapters

#	Description	Location	Configuration	Details
1	Credential to log on to the IBM Dashboard Application Services Hub running on WebSphere Application Server.	**web browser:** See details. **Automation Framework:** Depends on the user repository that is used for WebSphere Application Server, for example WAS-based security or LDAP.	**web browser:** See details. **Automation Framework:** The administrator user of WebSphere Application Server can log in to the WebSphere administrative console to add or delete users. You can find these tasks in **Users and Groups -> Manage Users.**	Web browsers allow you to store user ID and password in the browser password cache. For more information, see your browser documentation.

Table 15. User credentials to operate on resources hosted by different automation adapters (continued)

#	Description	Location	Configuration	Details
2	Credential to access the domains hosted by the adapter from within the automation framework and the operations console.	**Automation Framework:** Queries performed by functional user: `<EEZ_CONFIG_ROOT>/eez.automation.engine.dif.properties` **Operations Console:** Queries and requests performed by a user who is logged on to the Dashboard Application Services Hub: Credential Store. **Adapter:** Operating system security or LDAP.	**Automation Framework:** Use the configuration tool `cfgsmu`. In the Service Management Unite Host Configuration, on the **User Credentials** tab, define the credentials used by the functional user to access automation domains. **Operations Console:** A Dashboard Application Services Hub user can store credentials when logging on to an automation domain in the credential store. Edit and delete these domain credentials using the **User > Credential Store** page within the Dashboard Application Services Hub. **Adapter:** Use the adapter's configuration utility to configure user authentication details.	If security configuration is enabled, the automation framework authenticates each user that accesses domains and resources of the individual automation adapter using the operations console. If a user cannot be authenticated by the configured security backend of the adapter, it cannot access domains and resources of the automation adapter.
3	Credential for the Universal Automation Adapter to access remote nodes. The user ID is specified for each resource in the Universal Automation Adapter policy.	**Adapter:** `<EEZ_CONFIG_ROOT>/eez.aladapter.dif.properties` **Remote node:** • SSH access: SSHd - OS security or LDAP	**Adapter:** Use the configuration tool, for example `cfgsmu` for the Universal Automation Adapter: in the Service Management Unite Host Configuration, on the **User credentials** and **Security** tab. **Remote node:** • SSH access: refer to SSHd documentation.	This credential is used by a Universal Automation Adapter to access remote nodes for resources of class IBM.RemoteApplication. The credential is not used for resources of class IBM.ITMResource which are defined for the Universal Automation Adapter. Depending on what you configured, different authentication methods are used.

Table 15. User credentials to operate on resources hosted by different automation adapters (continued)

#	Description	Location	Configuration	Details
4	Credential for the Universal Automation Adapter to access Tivoli Monitoring resources via a hub monitoring server. A user ID can be specified for each resource in the Universal Automation Adapter policy or a generic Tivoli Monitoring user is used.	**Adapter:** `<EEZ_CONFIG_ROOT>/eez.aladapter.dif.properties` **Hub TEMS**: • TEMS SOAP server configuration and configured security backend	**Adapter:** Use the configuration tool `cfgsmu` for the Universal Automation Adapter: in the Universal Automation Adapter configuration on the **Monitoring** tab. **Hub TEMS:** • In the configuration of the hub TEMS	This credential is used by a Universal Automation Adapter to access the SOAP server on the hub monitoring server (TEMS) for the resources of class IBM.ITMResource.

The scenarios described in the following topics describe which credentials are used depending on how you work with resources, either hosted by a Universal Automation Adapter or by any other automation adapter:

Resources hosted directly by a Universal Automation Adapter

Describes which user credentials are required to operate resources hosted directly by the Universal Automation Adapter.

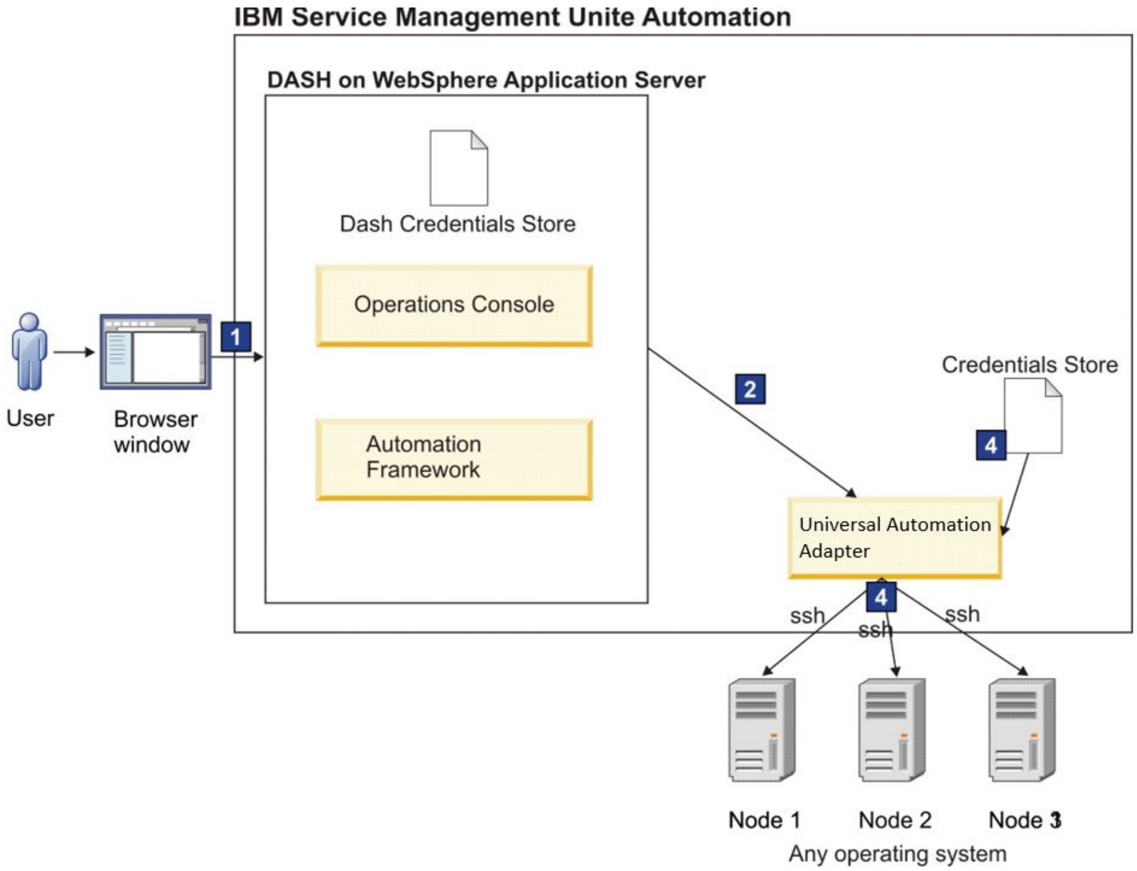


Figure 5. Operating resources directly on single nodes

The numbers in the pictures refer to the numbers of the credentials in "User credentials" on page 99.

Procedure

1. Log on to the IBM Dashboard Application Services Hub. Specify your user ID and password (Credential 1) for the IBM Dashboard Application Services Hub.
2. After successful login, stop a resource hosted by a Universal Automation Adapter. As soon as you select the Universal Automation Adapter domain, the operations console prompts for a credential to access the Universal Automation Adapter domain (Credential 2).
3. Select the resource that you want to stop, and run a stop command against it. The Universal Automation Adapter checks which user ID is specified for the resource in the Universal Automation Adapter policy and then authenticates itself using the configured authentication method (Credential 4).

User roles

Assign access roles that determine which Service Management Unite Automation tasks are available to a user in the Dashboard Application Services Hub.

Access roles are created during the installation of Service Management Unite Automation and assigned to the user groups that are listed in the **Group Name** column of the table. To assign access roles to individual users, add the users' IDs to the corresponding user groups in the WebSphere administrative console.

Table 16. Access roles for Service Management

Role	Permissions	Group name
`EEZMonitor`	Grants minimum access rights. Users who have the `EEZMonitor` role can run query-type operations. This role cannot activate and deactivate automation policies or run actions that modify the state of resources: for example, they cannot submit start requests. The following dashboards are available to `EEZMonitor` users: • Welcome Page • Domain and Automation Health • Explore Automation Nodes • Explore Automation Domains • Information and Support • Domain Adapter Log	`EEZMonitorGroup`

Table 16. Access roles for Service Management (continued)

Role	Permissions	Group name
EEZOperator	In addition to the permissions granted by the EEZMonitor role, users who have this role can send requests against resources. With this role, users cannot run tasks that change the configuration, such as activating and deactivating policies. The following dashboards are available to EEZOperator users: • Welcome Page • Domain and Automation Health • Explore Automation Nodes • Explore Automation Domains • Information and Support • Domain Adapter Log • System Log • Command Execution	EEZOperatorGroup
EEZConfigurator	In addition to the permissions granted by the EEZMonitor role, users who have this role can run tasks that change the configuration, such as activating and deactivating policies. Users who have only this role cannot submit requests against resources. The role is required to be able to work with policies. The following dashboards are available to EEZConfigurator users: • Welcome Page • Domain and Automation Health • Explore Automation Nodes • Explore Automation Domains • Information and Support • Domain Adapter Log • Activate Automation Policies • Create a New Automation Policy • Edit an existing Policy	EEZConfiguratorGroup

Table 16. Access roles for Service Management (continued)

Role	Permissions	Group name
EEZAdministrator	Extends the EEZOperator and EEZConfigurator roles, granting maximum access rights. Users who have this role can run all operations available on the operations console. The following dashboards are available to EEZAdministrator users: • Welcome Page • Domain and Automation Health • Explore Automation Nodes • Explore Automation Domains • Information and Support • Domain Adapter Log • System Log • Command Execution • Activate Automation Policies • Create a New Automation Policy • Edit an Existing Automation Policy	EEZAdministratorGroup

The EEZ* access roles authorize users only to access and work with Service Management Unite Automation tasks and dashboards. Other administrative console tasks of the Dashboard Application Services Hub are only available to users who have the `iscadmins` access role.

You also need the `iscadmins` role to be able modify existing or create new dashboards in the Dashboard Application Services Hub.

By default, the `iscadmins` role is assigned to the default System Automation administrator (for example `eezadmin`) during the installation of Service Management Unite Automation.

Creating and modifying users and groups

The following steps describe how to set up the user account repository with the default setup and names, for example, eezadmin. If you choose to use different names for users and groups, adjust the described steps accordingly.

Procedure

Note: By default, these steps are performed during the installation of Service Management Unite Automation and you do not have to perform these steps manually. This is only required if you selected to not create automatically the users and groups during installation.

1. Log in to the WebSphere administrative console.
2. Click **Users and Groups > Manage Users** to create users.
3. Click **Create . . .** to create a new user.
4. Enter the **User ID**, **First name**, **Last name**, and passwords for the following users: eezadmin, eezdmn
5. Click **Create** to create both users.
6. Click **Close**.
7. Click **Users and Groups > Manage Groups** to create groups.

8. Click **Create . . .** to create a new group.
9. Enter the **Group name** of the following groups:
   - EEZAdministratorGroup
   - EEZConfiguratorGroup
   - EEZMonitorGroup
   - EEZOperatorGroup
10. Click **Create** to create the group and click **Close**.
11. Repeat steps 7 and 8 to create all of the groups that are listed in step 9.
12. To add eezadmin to the following groups, click the Group name EEZAdministratorGroup and proceed as follows:
13. Select the **Members** tab on the selected group page.
14. Click **Add Users . . .**
15. Enter the user name **eezadmin** into the **Search** field or enter * to see all users.
16. Click **Search**.
17. Select **eezadmin** and click **Add**.
18. Repeat steps 13 - 17 to add **eezadmin** to all groups listed in step 9.
19. To add **eezdmn** to the EEZAdministratorGroup, click the **Group** name and proceed as follows:
20. Select the **Members** tab on the selected group page.
21. Click **Add Users . . .**
22. Enter the user name **eezdmn** into the Search field or enter * to see all users.
23. Click **Search**.
24. Select **eezdmn** and click **Add**.

Results

After new users are added to the user repository and assigned to a group, access rights are granted. If you want to setup your external user repository with the default users and groups, adjust the steps to the administrative interfaces of the external user repository.

Authorizing users and groups within the Dashboard Application Services Hub

Users must have specific roles to work with dashboards that are available in the Dashboard Application Services Hub (DASH). This role assignment is configured in the DASH. Assign the required roles on the user group level, so that all users that belong to a group inherit the same roles.

The roles are assigned to user groups and users during the installation of Service Management Unite Automation as follows:

Table 17. Role to group assignment

Role	Group name
`EEZMonitor`	`EEZMonitorGroup`
`EEZOperator`	`EEZOperatorGroup`
`EEZConfigurator`	`EEZConfiguratorGroup`
`EEZAdministrator`	`EEZAdministratorGroup`

In addition, the `iscadmins` role is assigned to the default System Automation administrator (for example `eezadmin`) and to the default WebSphere administrative user (for example `wasadmin`):

Table 18. Role to user ID assignment

Role	User ID
`iscadmins`	`eezadmin, wasadmin`

You must have at least one user that has the `iscadmins` role.

For a list of the available user roles for System Automation and their meaning, see "User roles" on page 102

If you want to create more role assignments, proceed as follows:

1. Log in to the **Dashboard Application Services Hub** by using the WebSphere administrative user that you specified during the installation of Jazz for Service Management (for example `wasadmin`) or any other user that has the `iscadmins` role.
2. Use one of the following entries in the navigation bar to manage your roles:

   Console Settings > Roles
   List all roles and assign groups or individual users to a selected role.

   Console Settings > User Roles
   List all users and assign roles to selected users.

   Console Settings > Group Roles
   List all groups and assign roles to selected groups.

Authorizing users to create dashboards

By default, Dashboard Application Services Hub (DASH) users have limited authority to edit existing dashboards and no authority to create new dashboards.

To authorize individual users to create and edit dashboards, perform the following steps:

1. Log in to the **Dashboard Application Services Hub**.
2. Click **Console Settings > User Roles** in the navigation bar.
3. Click **Search** to list the available groups.
4. Click the entry for the user ID you want to modify.
5. Ensure that **`iscadmins`** is selected in the **Available Roles** list.
6. Click **Save**.
7. Close the **User Roles** tab.

To authorize a complete group to create and edit dashboards, perform the following steps:

1. Log in to the **Dashboard Application Services Hub**.
2. Click **Console Settings > Group Roles** in the navigation bar.
3. Click **Search** to list the available users.
4. Click the entry for the group you want to modify, for example EEZAdministratorGroup.
5. Ensure that **`iscadmins`** is selected in the **Available Roles** list.
6. Click **Save**.
7. Close the **Group Roles** tab.

Modifying the functional user ID of the automation framework

The automation framework functional user ID (default user ID: eezdmn) may be modified in the following two areas:

Procedure

1. The Java EE framework uses the automation framework functional user ID to access the WebSphere Application Server JMS Provider. This JMS Provider is used to send and receive asynchronous messages (events). Modify the functional user ID as follows:
   a) Log in to the **WebSphere administrative console**.
   b) Navigate to **Security > Global security**. In the **Authentication** group, expand **Java Authentication and Authorization Service** and select **J2C authentication data**.
   c) In the table, select the Alias `EEZJMSAuthAlias`.
   d) Make your changes and click **OK**.
   e) Click **Save** to save and activate the new configuration.
2. The Java EE framework uses the automation framework functional user ID to perform asynchronous tasks. Modify the functional user ID as follows:
   a) Select **Applications** > **Application Types** > **WebSphere enterprise applications**.
   b) Select the application **EEZEAR** in the table.
   c) Select **User RunAs roles** in the Details Properties area.
   d) Select the role **EEZAsync.**
   e) Change the settings and click **Apply**.
   f) Click **OK** and save the new configuration.
   g) Select **Security role to user/group mapping** in the Details Properties area of the EEZEAR application.
   h) Select the row for role **EEZFunctionalUser** and click **Map Users....**
   i) Search and select the functional user, such that it appears in the **Selected** list.
   j) Click **OK** to return to the **Security role to user/group mapping** table.
   k) Click **OK** and save the new configuration.
   l) Select the application **isc** in the table.
   m) Select **User RunAs** roles in the Details Properties area.
   n) Select the role **EEZFunctionalUser**.
   o) Change the settings and click **Apply**.
   p) Click **OK** and save the new configuration.
   q) Restart **WebSphere Application Server**.

Modifying the user credentials for accessing first-level automation domains

Use the `cfgsmu` configuration utility to specify user credentials for accessing first-level automation domains. Domain user credentials are defined on the **User Credentials** tab of the configuration utility. For more information, refer to "User Credentials tab" on page 65.

The automation framework uses the credentials to authenticate to first-level automation domains.

Chapter 8. Scenarios and how-tos

This section provides step by step scenarios and specific tasks to help you better use the Service Management Untie dashboards.

How-to: Log on to the Service Management Unite console

After your environment is installed and configured correctly, log on to Service Management Unite(SMU) dashboard and learn about its user interface.

Procedure

1. Open the web browser and enter to the following URL:

   `https://`*`hostname`*`:16311/ibm/console/logon.jsp`

   Where: *hostname* is the server where you installed SMU.
2. Provide your credentials to log on to the dashboard. The default username is `eezadmin`.
3. When the logon completes successfully, the **Welcome page** is displayed.

What to do next

The **Welcome page** provides quick access to common Service Management Unite dashboards and shows version information. Start from the **Welcome page** to launch into high level dashboards to see overall health and specific dashboards to see detailed monitoring data.

How-to: Manage automation schedules

You can use the **Manage schedules** function provided by Service Management Unite dashboard to preview defined base schedules, modify schedules and create new schedules for a resource.

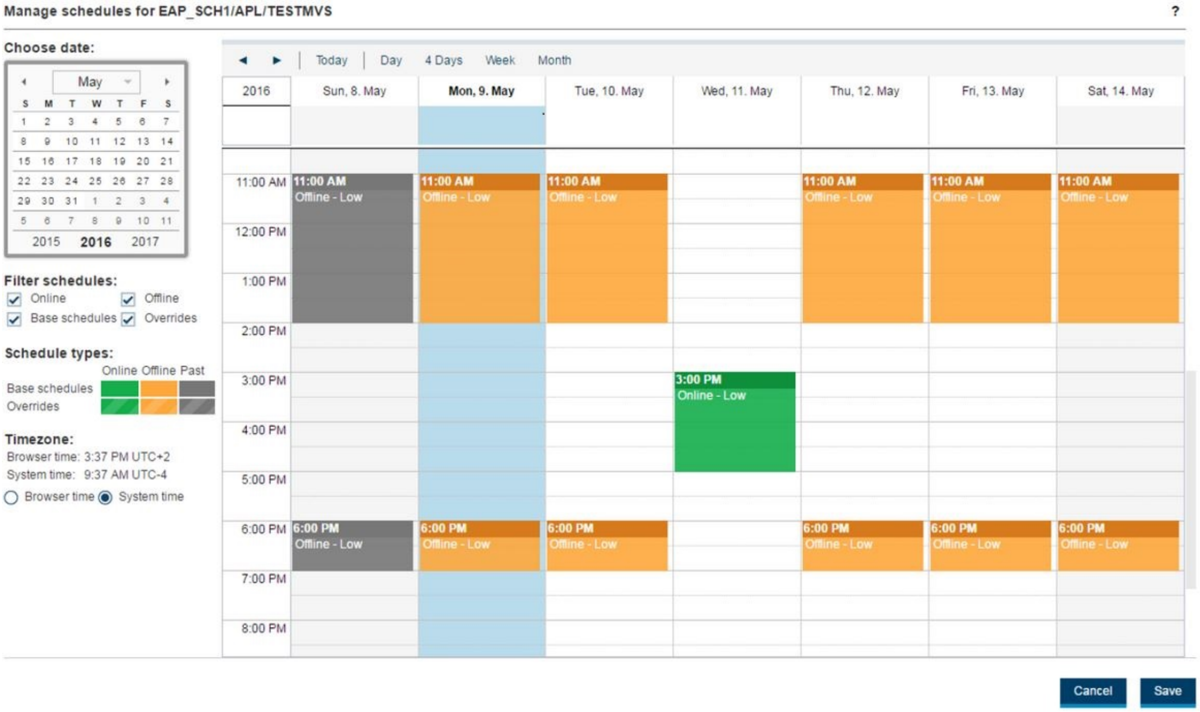
About this task

Schedules are time periods where a resource is kept online or offline by the automation. For example, during a maintenance window, it is required to stop a business application to apply service. Using schedules, this planned downtime can be defined ahead of time by an operator and System Automation will ensure that the application is stopped at the beginning of the maintenance window and started again at the end of the maintenance window.

Procedure

1. Open the **Explore Automation Domains** page.
2. In the **Domains** widget, select the desired domain, for example, using domain *TESTPLX INGXSGA0* for demo purpose.
3. In the **Resources** widget, enter the name of the resources in the **Search** field to filter the view to only show matching resources.
4. From the drop-down menu of one of the resources, select **Manage Schedules**.

   The **Manage Schedules** dialog appears and shows the base schedules that are defined for the resource. Offline schedules are marked as orange, Online schedules are marked as green.



Filter schedules:
☑ Online ☑ Offline
☑ Base schedules ☑ Overrides

Schedule types:

	Online	Offline	Past
Base schedules	🟩	🟧	⬛
Overrides	▨	▨	▨

Timezone:
Browser time: 3:37 PM UTC+2
System time: 9:37 AM UTC-4
○ Browser time ● System time

5. In this dialogue, you can create, modify, delete, review, or restore the schedules.

    - Navigate in the **Manage Schedules** dialog.

        a. With the calendar toolbar, users can switch between the following views: Today, Day, 4 Days, Week, and Month.

        b. Clicking on **Today** switches the view to a 'single day view' and navigates to the current date.

        c. Clicking on the left and right arrow buttons, navigates to the following or previous day/week/month, depending on the current view.

    - Create new schedules:

        a. In the calendar view, double-click an entry that is not occupied. It automatically creates a new one-hour schedule.

        b. Double-click the entry to customize the default schedule to match your needs.

    - Delete schedules:

      Right-click a schedule, and select **Delete**. The selected schedule is removed.

    - Modifying schedules:

        – Drag and drop the schedule box to move a schedule to a new start date.

          Note: You cannot move a schedule to a time in the past.

        – To change the start time or end time of a schedule, drag the upper or bottom line of the schedule box.

      Alternatively, you can double click the schedule box, and then modify the properties in the schedule information panel. This is always required when you want to change the priority.

    - Check details of the defined schedule:

      Double click a schedule to open a panel that shows detailed information about it.

    - Restore base schedules:

      The base schedule is defined in the policy. Whenever you create a schedule, or modify an existing base schedule, you create a schedule that replaces the base schedules. In the first row of the calendar widget, you can see an entry that indicates the base schedules exist for the selected day.

    - Restore base schedules:

    a. Double-click a schedule, a panel is displayed that shows information about the existing base schedules.
    b. Click **Restore Base Schedules** to reset to the base schedule.

6. Click **Cancel** on the Manage Schedules dialog, the modifications to schedules are not saved to the backend. Otherwise, if you click **Save**, all the changes in the dialogue are set active in System Automation for z/OS.

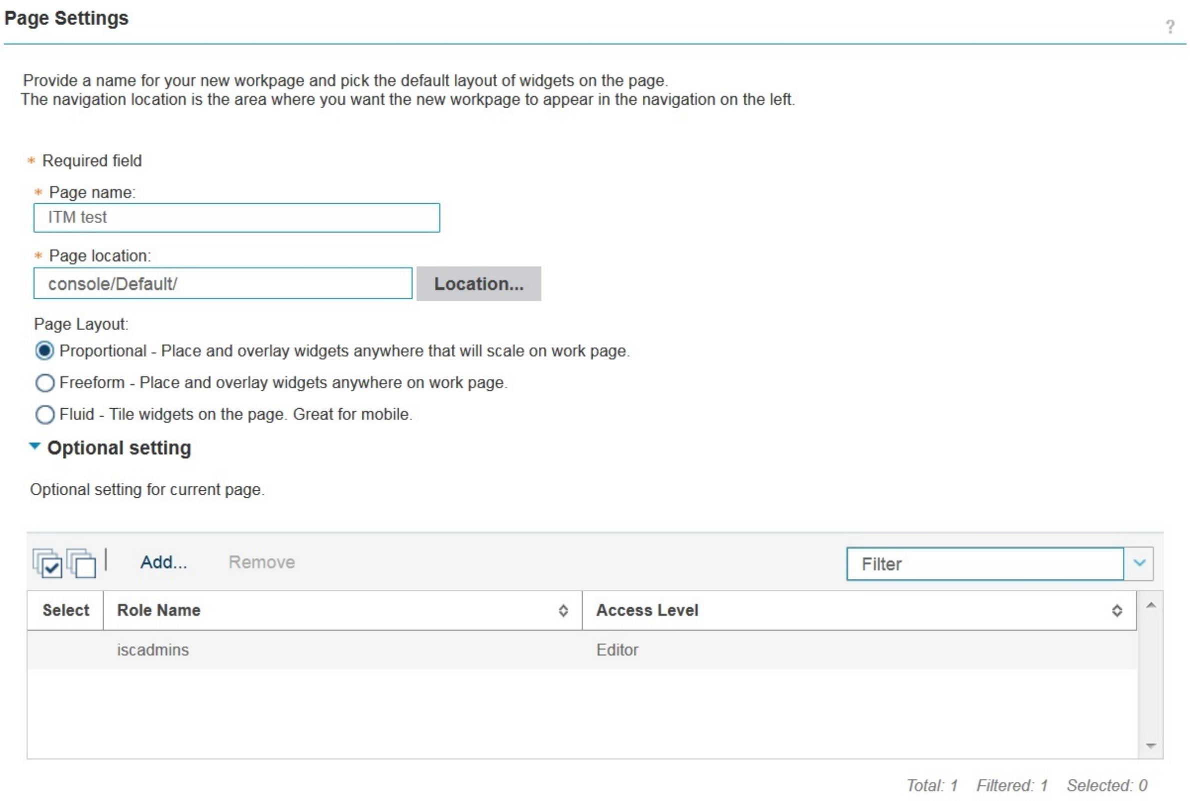
How to: Create a dashboard with SA data

Service Management Unite (SMU) utilizes Dashboard Application Services Hub (DASH) to allow you to create customized dashboards with interactive widgets.

Procedure

1. On the welcome page of SMU, click + **Create New Page**.
2. On **Page Settings**, specify the following settings:
    a. Specify a page name.
    b. Specify the page location.
    c. Specify the page layout:
    - Proportional:
        - The page and its widgets change size with the size of the browser;
        - Widgets might overlap;
        - Page never scrolls;
        - Most versatile;
    - Freeform:
        - The page and its widgets are fixed size;
        - Widgets might overlap;
        - The page gets scrollbars when it's too small;
    - Fluid:
        - The page and its widgets change size with the size of the browser;
        - Widgets do not overlap;
        - The page never scrolls;
        - Layout adapts to browser window size;
        - Designed for mobile;

    d. In **Optional settings**, specify the roles that should be able to access the new page.



Page Settings

Provide a name for your new workpage and pick the default layout of widgets on the page.
The navigation location is the area where you want the new workpage to appear in the navigation on the left.

* Required field

* Page name: ITM test

* Page location: console/Default/ Location...

Page Layout:

● Proportional - Place and overlay widgets anywhere that will scale on work page.

○ Freeform - Place and overlay widgets anywhere on work page.

○ Fluid - Tile widgets on the page. Great for mobile.

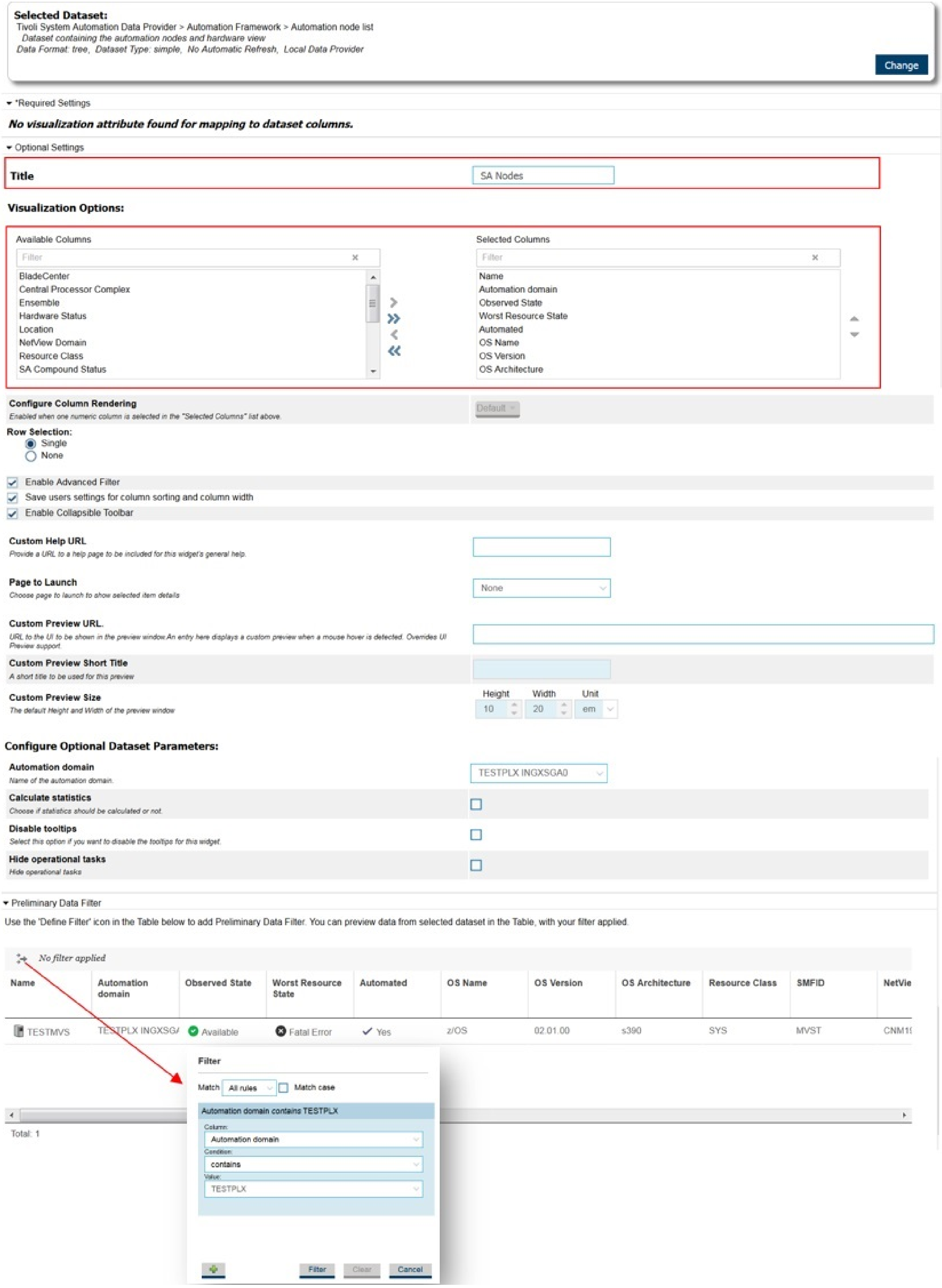
Optional setting

Optional setting for current page.

Select	Role Name	Access Level
	iscadmins	Editor

Total: 1 Filtered: 1 Selected: 0

3. Click **OK** to save the settings.
4. The widget palette provides SA specific and other widgets. Drag and drop a widget from the widget palette to the page canvas. For example, select **System Automation Table** and place it to the canvas.
5. Click **Edit** from the widget menu to configure the data provider and data set that should be displayed by the widget.
6. On page **Select a Dataset**, click **Show All** to list all the available data sets. Or search for the specific data set. For example, select **Automation node list** to show nodes in System Automation.
   a. Specify the title of the widget.
   b. For 'Table' or 'Tree Table' widget, select which columns you want to display.
   c. Use the Preliminary Data Filter section to filter on specific items in a data set that should be displayed in the widget.
   d. Specify other parameters as needed.



Selected Dataset:
Tivoli System Automation Data Provider > Automation Framework > Automation node list
Dataset containing the automation nodes and hardware view
Data Format: tree, Dataset Type: simple, No Automatic Refresh, Local Data Provider

▾ *Required Settings

No visualization attribute found for mapping to dataset columns.

▾ Optional Settings

Title: SA Nodes

Visualization Options:

Available Columns	Selected Columns
BladeCenter	Name
Central Processor Complex	Automation domain
Ensemble	Observed State
Hardware Status	Worst Resource State
Location	Automated
NetView Domain	OS Name
Resource Class	OS Version
SA Compound Status	OS Architecture

Configure Column Rendering: Default
Enabled when one numeric column is selected in the "Selected Columns" list above.

Row Selection:
● Single
○ None

☑ Enable Advanced Filter
☑ Save users settings for column sorting and column width
☑ Enable Collapsible Toolbar

Custom Help URL
Provide a URL to a help page to be included for this widget's general help.

Page to Launch: None
Choose page to launch to show selected item details

Custom Preview URL.
URL to the UI to be shown in the preview window.An entry here displays a custom preview when a mouse hover is detected. Overrides UI Preview support.

Custom Preview Short Title
A short title to be used for this preview

Custom Preview Size: Height 10, Width 20, Unit em
The default Height and Width of the preview window

Configure Optional Dataset Parameters:

Automation domain: TESTPLX INGXSGA0
Name of the automation domain.

Calculate statistics □
Choose if statistics should be calculated or not.

Disable tooltips □
Select this option if you want to disable the tooltips for this widget.

Hide operational tasks □
Hide operational tasks

▾ Preliminary Data Filter

Use the 'Define Filter' icon in the Table below to add Preliminary Data Filter. You can preview data from selected dataset in the Table, with your filter applied.

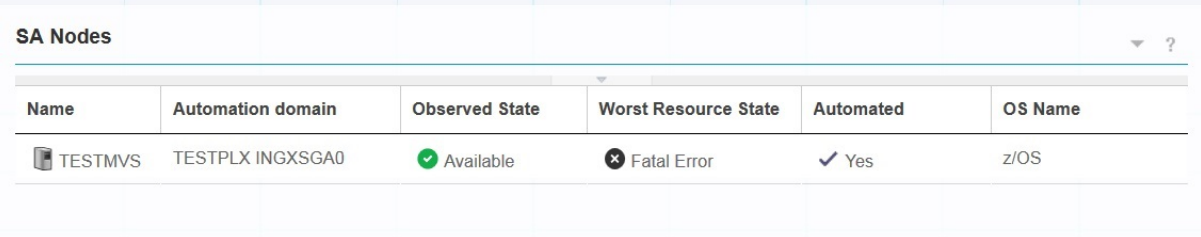
No filter applied

Name	Automation domain	Observed State	Worst Resource State	Automated	OS Name	OS Version	OS Architecture	Resource Class	SMFID	NetVie
TESTMVS	TESTPLX INGXSG/	Available	Fatal Error	✓ Yes	z/OS	02.01.00	s390	SYS	MVST	CNM1!

Total: 1

Filter
Match: All rules □ Match case
Automation domain contains TESTPLX
Column: Automation domain
Condition: contains
Value: TESTPLX

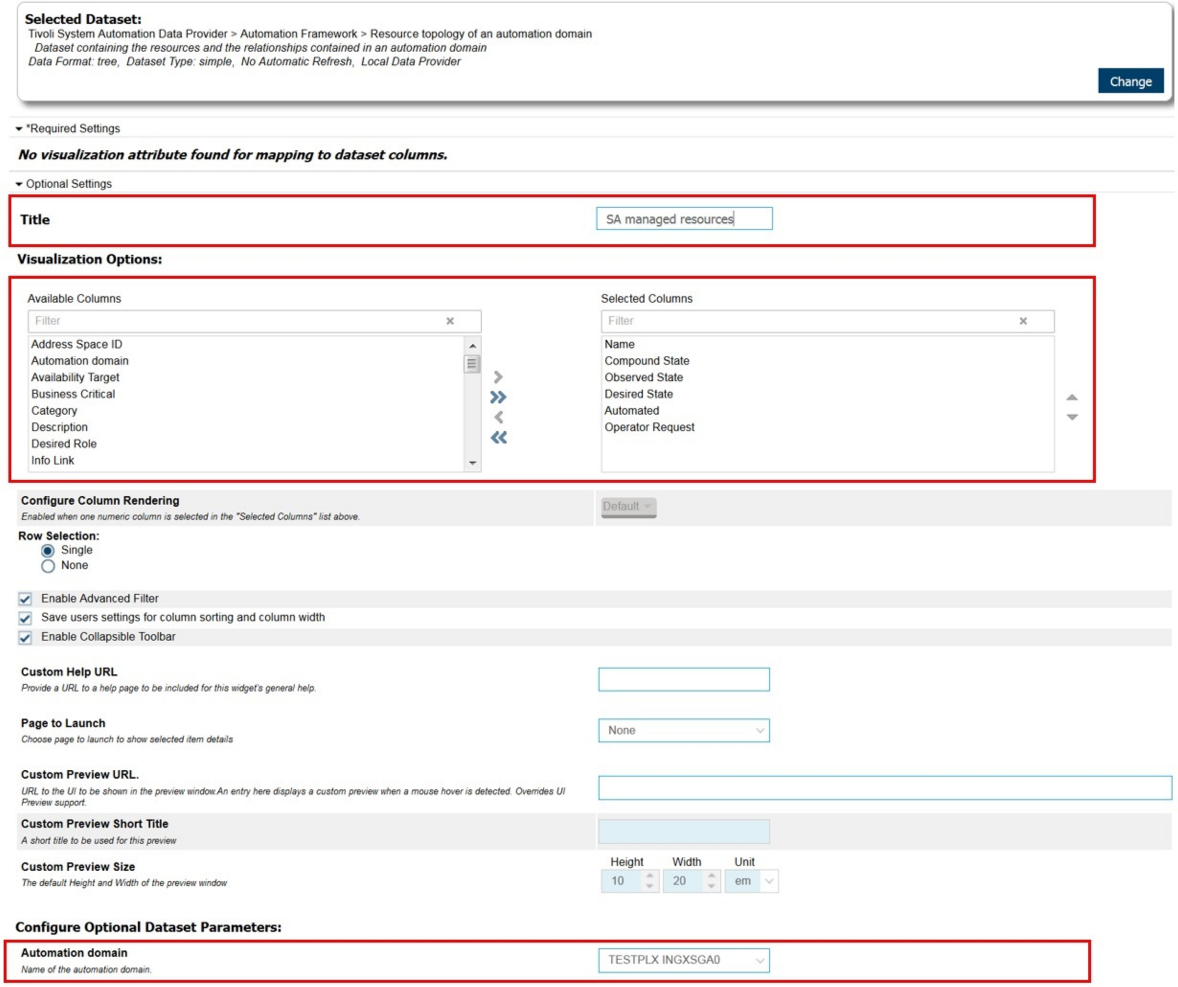
7. Click **OK** to save the settings. The widget is added to the page.



SA Nodes

Name	Automation domain	Observed State	Worst Resource State	Automated	OS Name
TESTMVS	TESTPLX INGXSGA0	✓ Available	☒ Fatal Error	✓ Yes	z/OS

8. Repeat steps 5 - 8 to add another widget to show automation resources on the node.



Selected Dataset:
Tivoli System Automation Data Provider > Automation Framework > Resource topology of an automation domain
Dataset containing the resources and the relationships contained in an automation domain
Data Format: tree, Dataset Type: simple, No Automatic Refresh, Local Data Provider

*Required Settings

No visualization attribute found for mapping to dataset columns.

Optional Settings

Title: SA managed resources

Visualization Options:

Available Columns: Address Space ID, Automation domain, Availability Target, Business Critical, Category, Description, Desired Role, Info Link

Selected Columns: Name, Compound State, Observed State, Desired State, Automated, Operator Request

Configure Column Rendering
Enabled when one numeric column is selected in the "Selected Columns" list above.

Row Selection:
● Single
○ None

☑ Enable Advanced Filter
☑ Save users settings for column sorting and column width
☑ Enable Collapsible Toolbar

Custom Help URL
Provide a URL to a help page to be included for this widget's general help.

Page to Launch: None
Choose page to launch to show selected item details

Custom Preview URL.
URL to the UI to be shown in the preview window.An entry here displays a custom preview when a mouse hover is detected. Overrides UI Preview support.

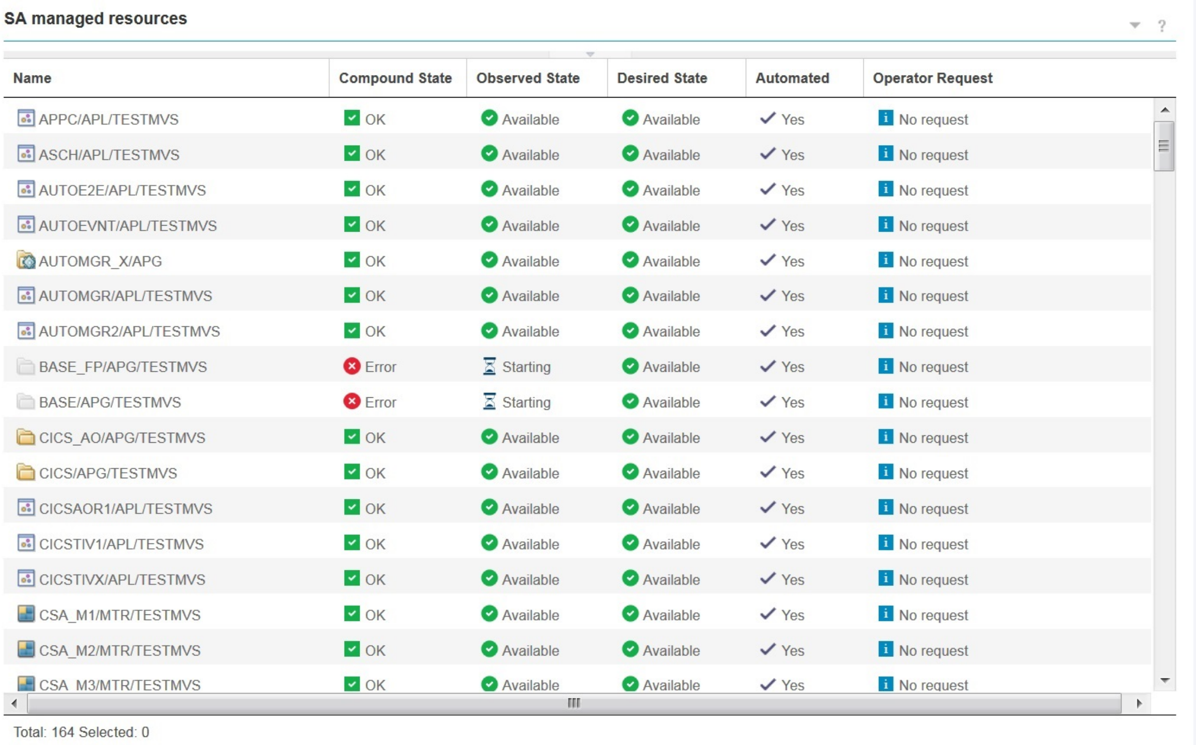
Custom Preview Short Title
A short title to be used for this preview

Custom Preview Size: Height 10, Width 20, Unit em
The default Height and Width of the preview window

Configure Optional Dataset Parameters:

Automation domain: TESTPLX INGXSGA0
Name of the automation domain.

The resources topology widget is added to the page:



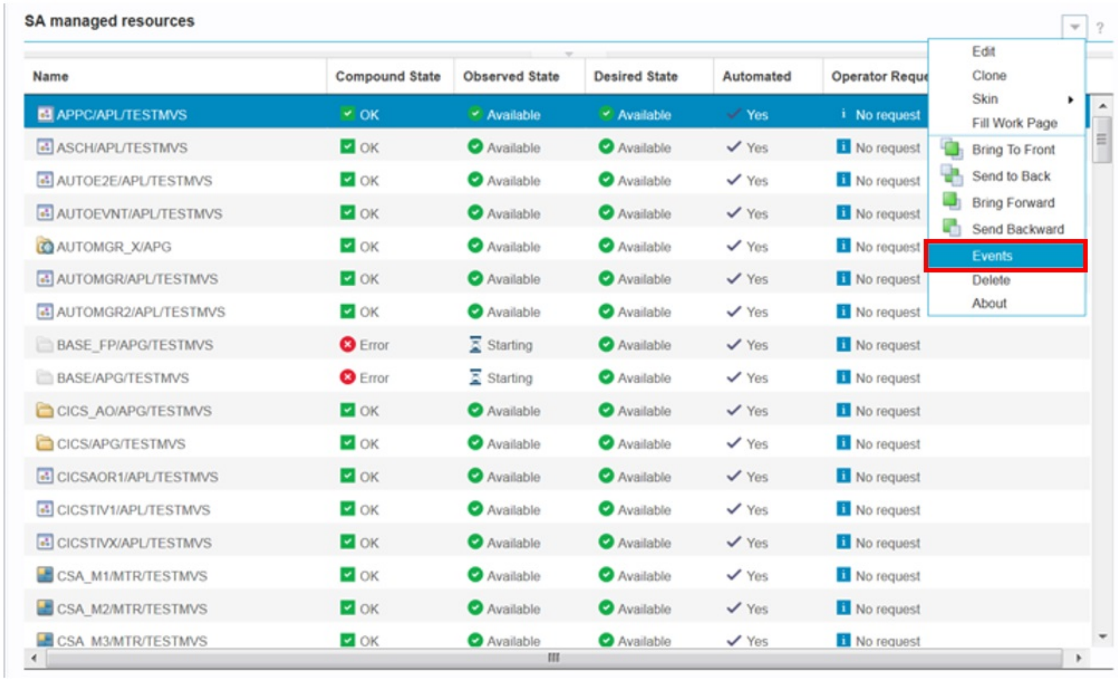
SA managed resources

Name	Compound State	Observed State	Desired State	Automated	Operator Request
APPC/APL/TESTMVS	OK	Available	Available	✓ Yes	No request
ASCH/APL/TESTMVS	OK	Available	Available	✓ Yes	No request
AUTOE2E/APL/TESTMVS	OK	Available	Available	✓ Yes	No request
AUTOEVNT/APL/TESTMVS	OK	Available	Available	✓ Yes	No request
AUTOMGR_X/APG	OK	Available	Available	✓ Yes	No request
AUTOMGR/APL/TESTMVS	OK	Available	Available	✓ Yes	No request
AUTOMGR2/APL/TESTMVS	OK	Available	Available	✓ Yes	No request
BASE_FP/APG/TESTMVS	Error	Starting	Available	✓ Yes	No request
BASE/APG/TESTMVS	Error	Starting	Available	✓ Yes	No request
CICS_AO/APG/TESTMVS	OK	Available	Available	✓ Yes	No request
CICS/APG/TESTMVS	OK	Available	Available	✓ Yes	No request
CICSAOR1/APL/TESTMVS	OK	Available	Available	✓ Yes	No request
CICSTIV1/APL/TESTMVS	OK	Available	Available	✓ Yes	No request
CICSTIVX/APL/TESTMVS	OK	Available	Available	✓ Yes	No request
CSA_M1/MTR/TESTMVS	OK	Available	Available	✓ Yes	No request
CSA_M2/MTR/TESTMVS	OK	Available	Available	✓ Yes	No request
CSA_M3/MTR/TESTMVS	OK	Available	Available	✓ Yes	No request

Total: 164 Selected: 0

9. Configure the resource topology widget to listen for NodeClickedOn events.

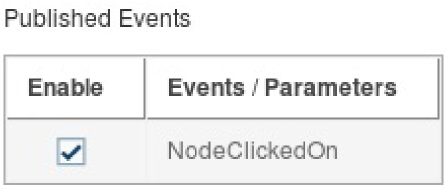
   a. Select **Events** on the widget toolbar.



SA managed resources

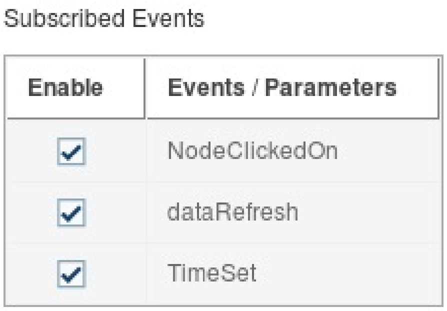
Name	Compound State	Observed State	Desired State	Automated	Operator Reque
APPC/APL/TESTMVS	OK	Available	Available	✓ Yes	No request
ASCH/APL/TESTMVS	OK	Available	Available	✓ Yes	No request
AUTOE2E/APL/TESTMVS	OK	Available	Available	✓ Yes	No request
AUTOEVNT/APL/TESTMVS	OK	Available	Available	✓ Yes	No request
AUTOMGR_X/APG	OK	Available	Available	✓ Yes	No request
AUTOMGR/APL/TESTMVS	OK	Available	Available	✓ Yes	No request
AUTOMGR2/APL/TESTMVS	OK	Available	Available	✓ Yes	No request
BASE_FP/APG/TESTMVS	Error	Starting	Available	✓ Yes	No request
BASE/APG/TESTMVS	Error	Starting	Available	✓ Yes	No request
CICS_AO/APG/TESTMVS	OK	Available	Available	✓ Yes	No request
CICS/APG/TESTMVS	OK	Available	Available	✓ Yes	No request
CICSAOR1/APL/TESTMVS	OK	Available	Available	✓ Yes	No request
CICSTIV1/APL/TESTMVS	OK	Available	Available	✓ Yes	No request
CICSTIVX/APL/TESTMVS	OK	Available	Available	✓ Yes	No request
CSA_M1/MTR/TESTMVS	OK	Available	Available	✓ Yes	No request
CSA_M2/MTR/TESTMVS	OK	Available	Available	✓ Yes	No request
CSA_M3/MTR/TESTMVS	OK	Available	Available	✓ Yes	No request

   b. Check **NodeClickedOn** to enable the widget to listen for NodeClickedOn events so that the selection of node in SA Nodes widget filters applications displayed.



Published Events

Enable	Events / Parameters
☑	NodeClickedOn



Subscribed Events

Enable	Events / Parameters
☑	NodeClickedOn
☑	dataRefresh
☑	TimeSet

Results

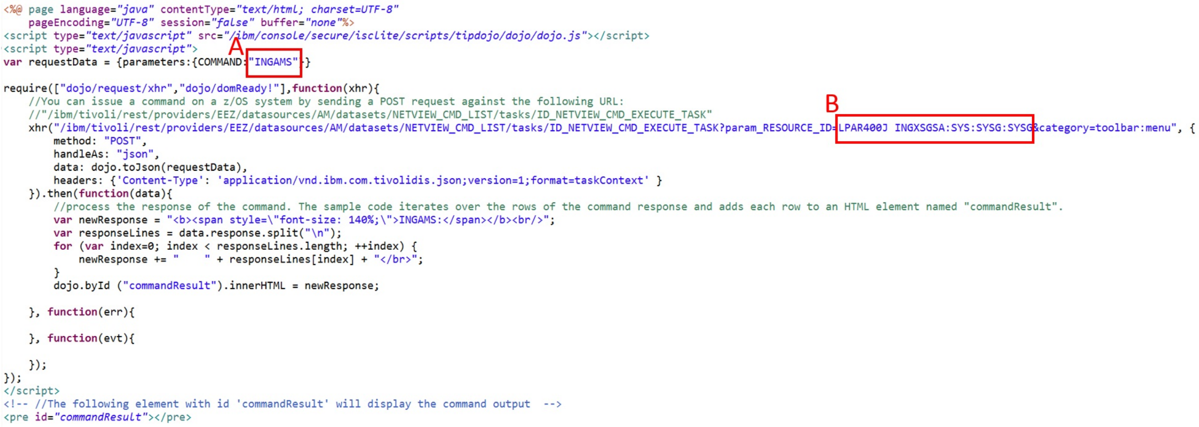
Now the page with SA nodes and resources information is created.

How to: Render command output in a widget

You can customize a JSP file by using REST APIs to issue a command and render its response in a widget.

Procedure

1. Create a JSP file that you will use in a web widget. In the JSP file, issue the command and render the output response as HTML output.



```
<%@ page language="java" contentType="text/html; charset=UTF-8"
    pageEncoding="UTF-8" session="false" buffer="none"%>
<script type="text/javascript" src="/ibm/console/secure/isclite/scripts/tipdojo/dojo/dojo.js"></script>
<script type="text/javascript">
var requestData = {parameters:{COMMAND:"INGAMS"}}

require(["dojo/request/xhr","dojo/domReady!"],function(xhr){
    //You can issue a command on a z/OS system by sending a POST request against the following URL:
    //"/ibm/tivoli/rest/providers/EEZ/datasources/AM/datasets/NETVIEW_CMD_LIST/tasks/ID_NETVIEW_CMD_EXECUTE_TASK"
    xhr("/ibm/tivoli/rest/providers/EEZ/datasources/AM/datasets/NETVIEW_CMD_LIST/tasks/ID_NETVIEW_CMD_EXECUTE_TASK?param_RESOURCE_ID=LPAR400J INGXSGSA:SYS:SYSG:SYSG&category=toolbar:menu", {
        method: "POST",
        handleAs: "json",
        data: dojo.toJson(requestData),
        headers: {'Content-Type': 'application/vnd.ibm.com.tivolidis.json;version=1;format=taskContext' }
    }).then(function(data){
        //process the response of the command. The sample code iterates over the rows of the command response and adds each row to an HTML element named "commandResult".
        var newResponse = "<b><span style=\"font-size: 140%;\">INGAMS:</span></b><br/>";
        var responseLines = data.response.split("\n");
        for (var index=0; index < responseLines.length; ++index) {
            newResponse += "    " + responseLines[index] + "</br>";
        }
        dojo.byId ("commandResult").innerHTML = newResponse;

    }, function(err){

    }, function(evt){

    });
});
</script>
<!-- //The following element with id 'commandResult' will display the command output  -->
<pre id="commandResult"></pre>
```

   a. In field **A**, specify the command that you want to issue on a system.

      In the sample code, the command **INGAMS** is used to display the environment information about the SA plex.

   b. In field **B**, specify parameter **RESOURCE_ID** of the REST URL. The **RESOURCE_ID** identifies the target system on which the command will be ran. The format is as follows:

      <DOMAIN_NAME>:SYS:*<SYSTEM_NAME>*:*<SYSTEM_NAME>*

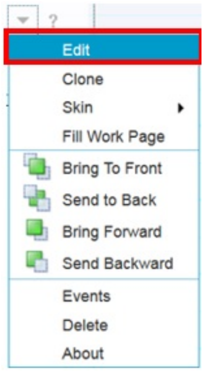
      You can get the value for *DOMAIN_NAME* and *SYSTEM_NAME* on the **Explore Automation Domains** page.

2. Copy the JSP file onto the SMU server so that you can address it in the web widget. For example, you can copy it to the following path:

   ```
   /opt/IBM/JazzSM/profile/installedApps/JazzSMNode01Cell/isc.ear/
   EEZUIWebClient.war/jsp/SampleCommandInWidget.jsp
   ```

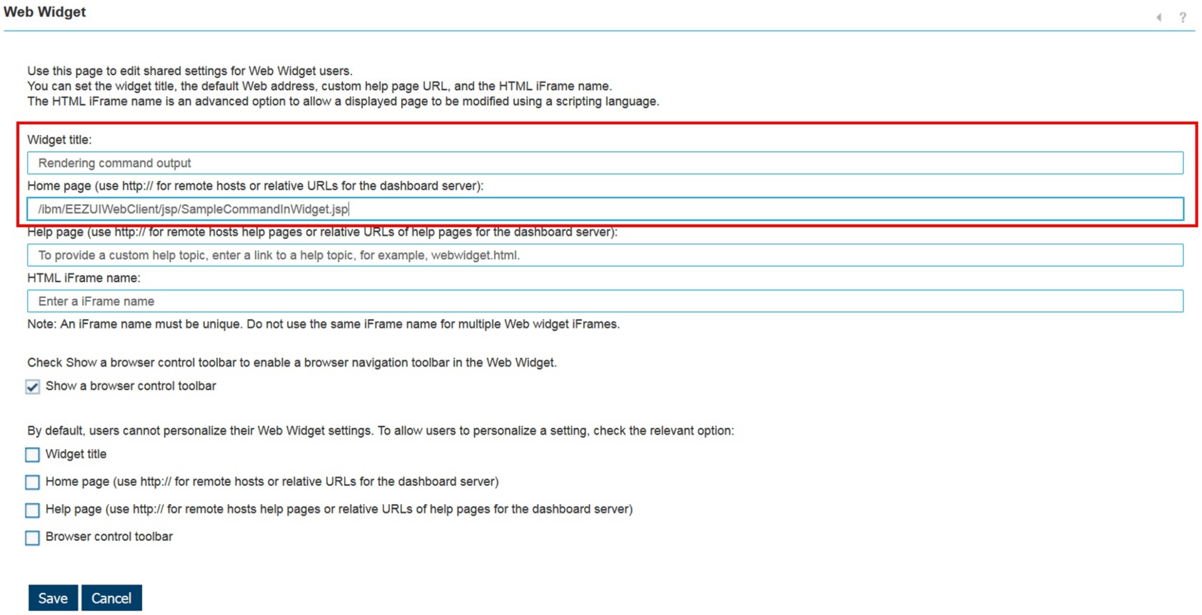
   In this way, the JSP file is located below the SMU Automation war file and you can locate it using the SMU Automation context root.

3. Create a **Web Widget** to a dashboard. In the edit mode, select **Dashboard Widgets** → **Web Widget**. Drag the widget to the page canvas.
4. Click **Edit** from the widget menu to configure the widget properties.



5. Specify the widget title and the following URL for the JSP file: `/ibm/EEZUIWebClient/jsp/SampleCommandInWidget.jsp`

   Where, `/ibm/EEZUIWebClient` is the context root of the `EEZUIWebClient.war` file.



Web Widget

Use this page to edit shared settings for Web Widget users.
You can set the widget title, the default Web address, custom help page URL, and the HTML iFrame name.
The HTML iFrame name is an advanced option to allow a displayed page to be modified using a scripting language.

Widget title:
Rendering command output

Home page (use http:// for remote hosts or relative URLs for the dashboard server):
/ibm/EEZUIWebClient/jsp/SampleCommandInWidget.jsp

Help page (use http:// for remote hosts help pages or relative URLs of help pages for the dashboard server):
To provide a custom help topic, enter a link to a help topic, for example, webwidget.html.

HTML iFrame name:
Enter a iFrame name

Note: An iFrame name must be unique. Do not use the same iFrame name for multiple Web widget iFrames.

Check Show a browser control toolbar to enable a browser navigation toolbar in the Web Widget.

☑ Show a browser control toolbar

By default, users cannot personalize their Web Widget settings. To allow users to personalize a setting, check the relevant option:

☐ Widget title

☐ Home page (use http:// for remote hosts or relative URLs for the dashboard server)

☐ Help page (use http:// for remote hosts help pages or relative URLs of help pages for the dashboard server)

☐ Browser control toolbar

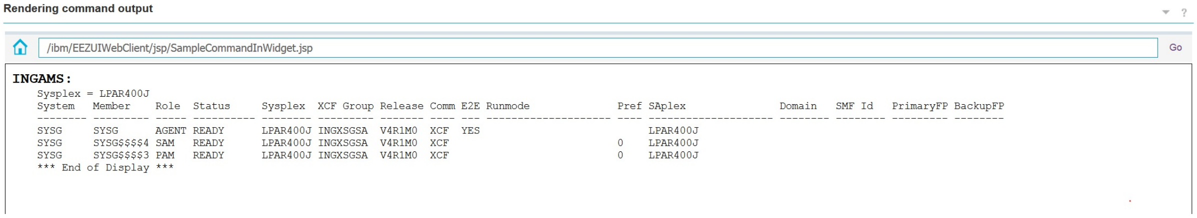
   Alternatively, you could also put the customized JSP file in directory `myBox.war` or create your own war file by using the 'Content Box' mechanism.

6. Save the settings.

   You can also customize the web widget format, for example, set it to be transparent and have no borders, no controls, and so on.

Results

You can see the output of the **INGAMS** command is displayed in the widget.



Rendering command output

/ibm/EEZUIWebClient/jsp/SampleCommandInWidget.jsp

```
INGAMS:
    Sysplex = LPAR400J
    System   Member    Role  Status     Sysplex  XCF Group Release Comm E2E Runmode              Pref SAplex               Domain   SMF Id   PrimaryFP BackupFP
    -------- --------- ----- ---------- -------- --------- ------- ---- --- -------------------- ---- -------------------- -------- -------- --------- --------
    SYSG     SYSG      AGENT READY      LPAR400J INGXSGSA  V4R1M0  XCF  YES                           LPAR400J
    SYSG     SYSG$$$$4 SAM   READY      LPAR400J INGXSGSA  V4R1M0  XCF                           0    LPAR400J
    SYSG     SYSG$$$$3 PAM   READY      LPAR400J INGXSGSA  V4R1M0  XCF                           0    LPAR400J
    *** End of Display ***
```

What to do next

When you process the command response in the JSP file, you could do any parsing and formatting that you would like to do and render the output in a fancier way by using HTML stylesheets .

You could customize and enhance the above sample code to listen for click events. For example, you could have a list of systems displayed on the same page, and when you select a specific system, the click event is captured by the web widget and the JSP code, and thus the **INGAMS** command output on that system is displayed. For detailed instructions on how to implement event handling, see JazzSM Dashboard Widgets Interaction - Eventing Demystified.

You can also use the **POST** request described above against the REST API to issue a command in a Tivoli Directory Integrator assembly line, and then return the output as DASH data set that can be used by many other DASH widgets, like a table widget, chart, etc.

Chapter 9. Troubleshooting and support

Troubleshooting Service Management Unite includes reviewing messages and debugging information.

The following sections contain messages and troubleshooting information for Service Management Unite Automation. Support information and resources are also included.

Jazz for Service Management and WebSphere Application Server installation failed with errors

Use the prerequisite scanner to debug errors when the Jazz for Service Management and WebSphere Application Server installation fail with errors.

Problem

When you install Jazz for Service Management and WebSphere Application Server, the installation fails with errors. The errors might be related to dick space, memory, or Java errors.

Cause

The prerequisites for Service Management Unite are not met.

Solution

Use the prerequisite scanner for the Jazz™ for Service Management installation package to list all the requirements.

1. Issue the following commands to run the prerequisite scanner:

   ```
   export JazzSM_FreshInstall=True
   JazzSM_Image_Home/PrereqScanner/prereq_checker.sh "ODP,DSH" detail
   ```

   The prerequisites including the expected disk space are listed.
2. Go through the output and ensure that each item gets a **PASS** result. Otherwise, fix the problems until you get all **PASS** results.

Docker container enters a 'loop situation'

Use this information to solve the problem when Docker container enters a 'loop situation'.

Problem

WAS is not running and SMU console cannot be accessed via the browser.

Cause

The SMU Docker container is looping.

A 'loop situation' might occur if SMU (WAS) can't start successfully. If WAS cannot be started, the SMU Docker container stops. However, the Docker environment is configured to automatically start a new SMU Docker container in that case, as a result, it enters a loop situation: The SMU Docker container tries to start WAS when it is created, if it fails and results in the container to be stopped, immediately a new container is created with WAS started again, and thus enters a 'loop situation'.

Solution

1. Check whether the SMU Docker container is 'looping'.

    a. Run the command **docker ps** several times.
    b. Compare the 'status' field for the SMU Docker container. If the uptime of the SMU Docker container is always several seconds (but varying), even if the container was started quite some time ago, it is likely to have a 'loop situation'.
2. Run the command **eezdocker.sh stop** to stop looping SMU Docker container.
3. Run the command **eezdocker.sh debug** to start a new SMU Docker container in debug mode. This starts a new container without automatically starting SMU (WAS), instead, only a shell is opened in the container.

   A started SMU Docker container with only a running shell makes it possible to start WAS manually. You can see the reported errors and search the log files for further problem identification. The default directory of WAS's log is `/opt/IBM/JazzSM/profile/logs/server1/SystemOut.log`.

   You need to commit these changes in the container to the SMU Docker image so that the newly started SMU Docker containers will have these changes included. Run command **docker commit --help** for more information.

Unable to start WAS in Docker environment

Use this information to solve the problem when WebSphere Application Server (WAS) cannot be started in the Docker environment.

Problem

WebSphere Application Server cannot be started and enters a 'loop situation'.

Symptom

SMU Docker container is in a 'loop situation', and you see the following exception in WAS's `SystemOut.log` when starting WAS manually in the SMU Docker container debug mode:

```
com.ibm.wsspi.runtime.variable.UndefinedVariableException: Undefined variable
HOST
```

Cause

The host name of the Docker host isn't configured correctly. For example, only a subname is set instead of the fully qualified name (FQN). The SMU Docker container might not be able to resolve this host name. For example, if the FQN of the Docker host server is *mydocker.mycompany.com*, but the host name is set only to *mydocker*, the SMU Docker container inherits this host name but not be able to resolve it. As a result, WAS will not be able to start successfully, resulting in a 'loop situation'.

Solution

To solve this problem, configure your docker host's host name to the FQN so that the Docker container can resolve it properly.

Unable to log in to the automation domain with the TSO user ID

Use this information to solve the problem when you are unable to log in to the automation domain with the TSO user ID.

Problem

The authentication for user ID *user name* is unsuccessful.

Symptom

```
ICH420I PROGRAM INGIOC FROM LIBRARY ING.V3R5M0.SINGMOD1 CAUSED THE
ENVIRONMENT TO BECOME UNCONTROLLED.
BPXP014I ENVIRONMENT MUST BE CONTROLLED FOR DAEMON (BPX.DAEMON)
PROCESSING
+EEZA0013E Authentication for user ID <user_id> was unsuccessful
```

Cause

The profile `BPX.DEAMON` is defined in the RACF class FACILITY. In addition, profiles in the class PROGRAM are defined in RACF. However, the dynamic load libraries that are used by the automation adapter are not defined to the RACF class PROGRAM, or the user ID running the started task INGXADPT or IHSAEVNT is not permitted to access the profile `BPX.DAEMON`. For more information, refer to Prerequisites for USS.

Solution

1. Verify whether the user ID that you use to run the started tasks INGXADPT and IHSAEVNT is permitted to access the `BPX.DAEMON` profile in the class FACILITY. If not, grant this user ID READ access to the profile.
2. Add the CSSLIB, SINGMOD1, SCEERUN, SCEERUN2, SCLBDLL libraries to the appropriate profile in class PROGRAM.
3. For the user ID that you use to run the INGXADPT and IHSAEVNT started tasks, grant it READ access to the appropriate profile in the class PROGRAM.
4. Run a SETROPTS refresh for class PROGRAM.

   See the following example of the commands that you might use:

   Note:

   - Before you use these commands, refer to the RACF related information and consult your local security administrator for advice.
   - The following example shows the commands for a generic profile definition '*'. The defined profiles in your enterprise might differ.
   - Before you use the sample commands, adapt the high-level qualifier data set and verify its location. If the data set is not on the IPL volume, then use the appropriate VOLSER instead of the '******' pointing to the IPL volume.

   ```
   PE BPX.DAEMON CL(FACILITY) ID(stc_userid) ACCESS(READ)
   RALT PROGRAM * ADDMEM('hlq.SCEERUN'/******/NOPADCHK) UACC(READ)
   RALT PROGRAM * ADDMEM('hlq.SCEERUN2'/******/NOPADCHK) UACC(READ)
   RALT PROGRAM * ADDMEM('hlq.SCLBDLL'/******/NOPADCHK) UACC(READ)
   RALT PROGRAM * ADDMEM('hlq.SINGMOD1'/******/NOPADCHK) UACC(READ)
   RALT PROGRAM * ADDMEM('hlq.CSSLIB'/******/NOPADCHK) UACC(READ)
   SETR REFRESH RACLIST(FACILITY)
   SETROPTS WHEN(PROGRAM) REFRESH
   ```

5. Recycle the started tasks INGXADPT and IHSAEVNT.

Unable to display widgets with DASH FP 3.1.3.2

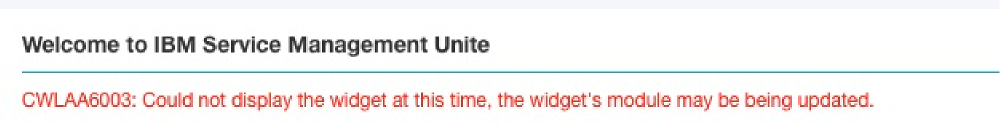
After you upgrade DASH to fix pack 3.1.3.2, you need to redefine the shared library reference for application `isc` to fix the display error.

Problem

After you update DASH to the latest fix pack 3.1.3.2, the widgets cannot be displayed properly.

Symptom

The following error message is displayed in the dashboard:



Welcome to IBM Service Management Unite

CWLAA6003: Could not display the widget at this time, the widget's module may be being updated.

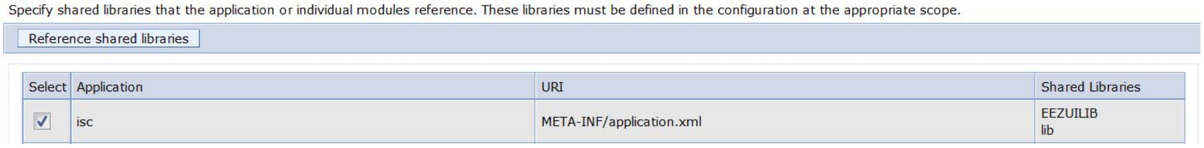
Cause

After the upgrade, the shared library `EEZUILIB` is no longer defined for the `isc` application.

Solution

Complete the following steps to define the shared library reference again for the `isc` application:

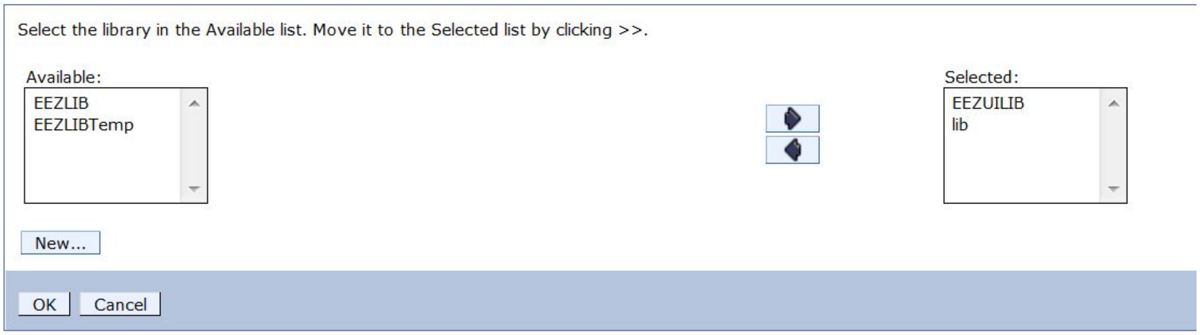
1. Log in to the WebSphere Admin console.
2. Click **Applications** > **Application Types** > **WebSphere enterprise applications** > **isc**.
3. Select **Shared library references**.
4. Select the row for **isc**, and then click **Reference shared libraries**.



Specify shared libraries that the application or individual modules reference. These libraries must be defined in the configuration at the appropriate scope.

Select	Application	URI	Shared Libraries
☑	isc	META-INF/application.xml	EEZUILIB lib

5. Move the `EEZUILIB` entry from the **Available** list to the **Selected** list.

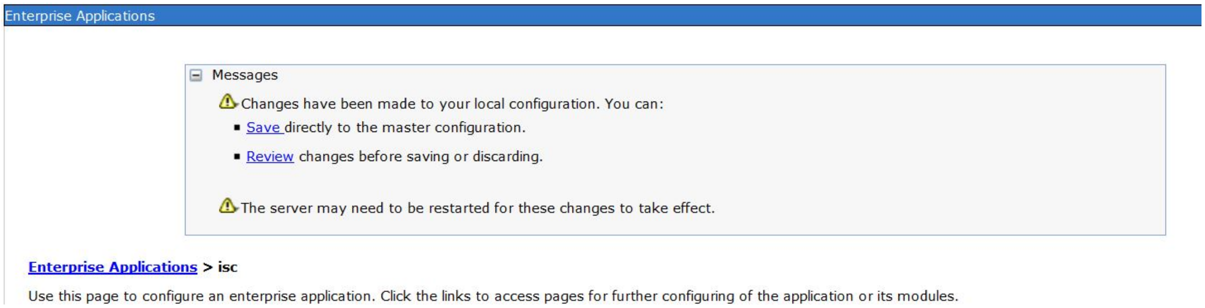


Select the library in the Available list. Move it to the Selected list by clicking >>.

Available:
EEZLIB
EEZLIBTemp

Selected:
EEZUILIB
lib

6. Click **OK** until you go back to the following page:



Enterprise Applications

Messages

⚠ Changes have been made to your local configuration. You can:
- Save directly to the master configuration.
- Review changes before saving or discarding.

⚠ The server may need to be restarted for these changes to take effect.

Enterprise Applications > isc

Use this page to configure an enterprise application. Click the links to access pages for further configuring of the application or its modules.

7. Click **Save** to save the configuration changes.
8. Restart the WebSphere Application Server.

Column 'Worst Resource State' is not shown after upgrading to SMU V1.1.4

The new column 'Worst Resource State' is not shown in dashboard 'Explore Automation Domains' and dashboard 'Explore Automation Nodes' after you upgrade to SMU V1.1.4.

Problem

In IBM Service Management Unite Version 1.1.4, the following default columns in dashboard 'Explore Automation Nodes' and dashboard 'Explore Automation Domains' are changed:

- In dashboard 'Explore Automation Nodes', the column 'Resource Class' is removed, and the column 'Worst Resource State' is added.
- In dashboard 'Explore Automation Domains', the column 'Domain Health State' is renamed to 'Worst Resource State'.

When you upgrade from a previous version of IBM Service Management Unite, these column changes don't take effect automatically. You still see the column definitions that are used in the previous release.

Solution

To apply these column changes after you update to SMU V.1.1.4, follow these steps to reset the two pages to the product defaults:

1. In the SMU navigation bar, click **Administration** > **Explore Automation Nodes**.
2. Select **Page Actions** > **Edit Page...**.
3. Click **Save and Exit** without changing anything.
4. In the SMU navigation bar, click **Console Settings** > **Pages**.
5. In dashboard **Pages**, under **Administration**, select **Explore Automation Nodes**. The page properties for dashboard Explore Automation Nodes are displayed.
6. Click **Restore**, and then click **Save**.
7. Repeat the above steps for dashboard 'Explore Automation Domains' to update to the new column 'Worst Resource State'.

Open dashboard 'Explore Automation Nodes' or 'Explore Automation Domains', you can see the columns as defined in the new product defaults.

Creating a Request For Enhancement (RFE) for Service Management Unite

Use the RFE community to create a request for Service Management Unite.

Problem

When you submit a new request for Service Management Unite via the RFE community, **Service Management Unite** is not provided in the RFE product list .

Solution

1. Open the Submit a request page in the RFE community.
2. In the **Product** field, specify **Service Management Suite for z/OS**.
3. The Component field is automatically filled with **Service Management Unite**.
4. Complete the other fields.
5. Submit your request.

Troubleshooting SMU Automation

Troubleshooting and support information for Service Management Unite Automation helps you understand, isolate, and resolve problems. Troubleshooting and support information contains instructions for using the problem-determination resources that are provided with your IBM products. To resolve a problem on your own, you can find out how to identify the source of a problem, how to gather diagnostic information, where to get fixes, and which knowledge bases to search. If you need to contact IBM Support, you can find out what diagnostic information the service technicians need to help you address a problem.

Communication flow between components

The following topic provides an overview of the communication flows between the components of Service Management Unite Automation. Understanding the communication flows helps you, if you try to solve communication-related problems with help of different log and trace files. All WebSphere components (such as the automation framework, adapters, or UI components) write trace statements, assuming trace is enabled. Trace statements are written to the corresponding WebSphere trace file. The location of the trace file is configured in the WebSphere Administrative Console.

Other components, for example, the Universal Automation Adapters, or Automation adapters are located on the FLA domains. They write trace and log files in the Tivoli Common Directory that can be found on the system where the particular component runs.

If you want to follow the communication flows described in this , gather all distributed trace and log files. Gathering all trace and log files of all components is also required when you contact IBM service in order to debug problems.

Starting a resource on a single node using remote command execution

The following scenario shows the communication flow that occurs if an operator starts a resource hosted by the Universal Automation Adapter:

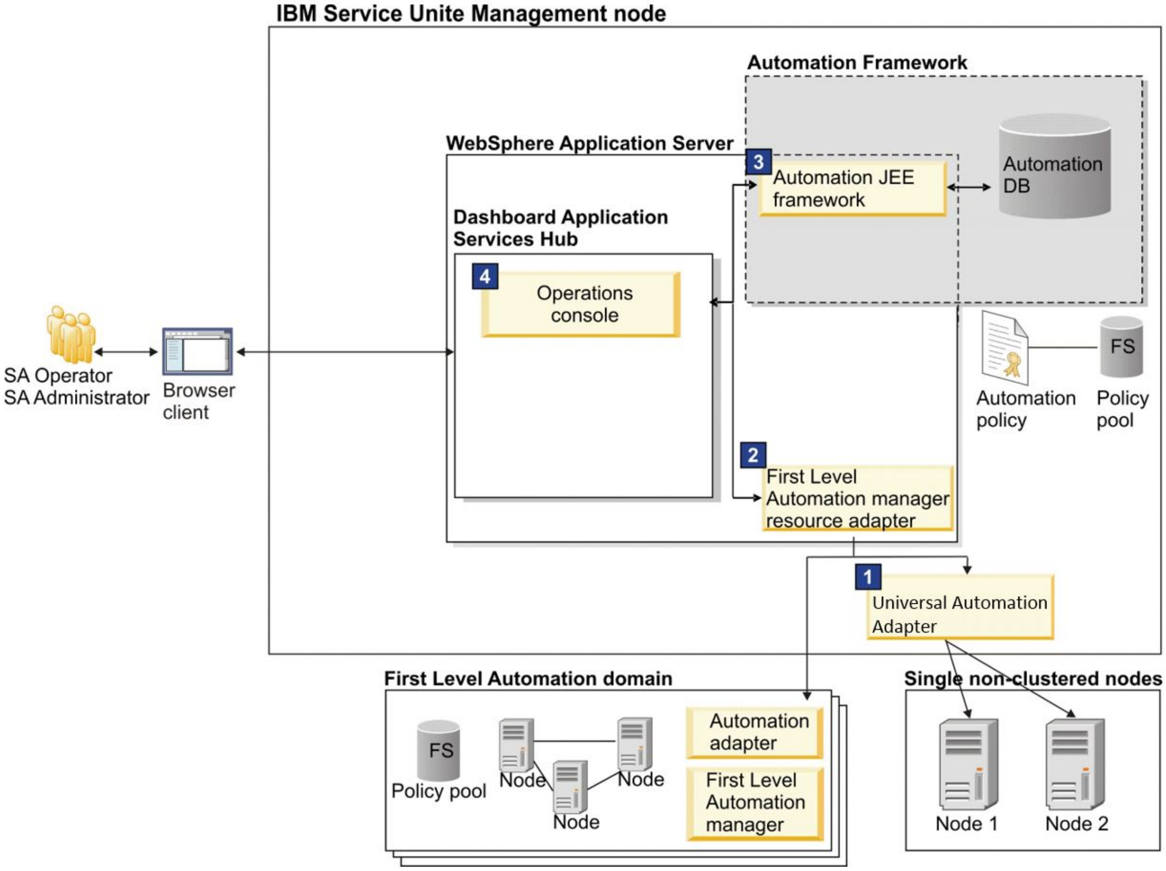

IBM Service Unite Management node
Automation Framework
WebSphere Application Server
3
Automation JEE framework
Automation DB
Dashboard Application Services Hub
4
Operations console
SA Operator
SA Administrator
Browser client
Automation policy
FS
Policy pool
2
First Level Automation manager resource adapter
1
Universal Automation Adapter
First Level Automation domain
FS
Policy pool
Node
Node
Node
Automation adapter
First Level Automation manager
Single non-clustered nodes
Node 1
Node 2

Figure 6. Communication flow: Start a resource on a single node

1. An operator submits a start request against a resource configured for a UAA domain using the System Automation operations console.
2. The System Automation operations console forwards the request to the automation JEE framework.
3. The request is passed through the first-level automation manager resource adapter.
4. The request is passed to the UAA.
5. The UAA remotely executes the start script on the remote node. The scripts and the node are specified in the UAA policy.

Resource status changes are not reflected in the Service Management Unite dashboard

Use this information to solve the problem where the resources status changes are not reflected in the Service Management Unite dashboard.

Problem

After you start or stop a resource from the Service Management Unite dashboard, the status of the resource is not changed in the dashboard.

Cause

The NetView for z/OS message adapter service is not configured properly. The message adapter service of the NetView for z/OS event/automation service (E/AS) is used to convert and forward messages from NetView for z/OS to the E2E automation adapter.

Diagnose

Issue the **INGE2E** command with the `Verify` option to check the E2E configuration:

```
NETVASIS INGE2E VERIFY JOBEAS=eas-jobname CPATH=/custom-root/adapter
```

If the E/AS message adapter does not show **active**, or **ERROR**, or a **Verification failed** message is shown, complete the following steps to review and edit the configuration file.

Solution

1. Go to the user data set `hlq.SCNMUXCL` and edit the message adapter configuration file `IHSAMCFG`.
2. Ensure the value of parameter **ServerLocation** is the host name where Service Management Unite is installed, and is the same as the value of **eif-send-to-hostname** in the E2E adapter's `ing.adapter.properties`.
3. Ensure the value of parameter **ServerPort** is the same as the value of **eif-receive-from-port** in the E2E adapter's `ing.adapter.properties` file.
4. Uncomment the line that starts with `AdapterFmtFile`.
5. Specify the name of the NetView message adapter format file: `AdapterFmtFile=INGMFMTE`.

   Parameters need to be set as follows:

   ```
   ServerLocation=127.0.0.1
   -  -  -  -  -  -  -  -  -  -  -  -  -  -
   ServerPort=5529
   -  -  -  -  -  -  -  -  -  -  -  -  -  -
   ConnectionMode=connection_oriented
   -  -  -  -  -  -  -  -  -  -  -  -  -  -
   BufferEvents=no
   -  -  -  -  -  -  -  -  -  -  -  -  -  -
   BufEvtPath=/etc/Tivoli/tec/cache_nv390msg
   -  -  -  -  -  -  -  -  -  -  -  -  -  -
   AdapterFmtFile=INGMFMTE
   ```

6. Issue the following command to display the configuration parameters of the NetView message adapter:

   ```
   MVS F <EASJOBNAME>,SETTINGS,TASK=MESSAGEA
   ```

   If the problem still exists, enable the trace mode of the E2E adapter to identify if there's any connection problem between the adapter and the Service Management Unite server. For detailed instructions on how to enable the trace mode, refer to Syntax and User-Defined USS File System for the Automation Adapter in IBM System Automation for z/OS End-to-End Automation. Check the logs and also check the messages EEZA0116I and EEZA0118I. The messages provide information about the connection status of the adapter and the Service Management Unite server. For example,

   ```
   EEZA0116I The status of the event sender changed: Address=<SMU_hostname>/<SMU_IP> Port=2002,
   Status=1
   EEZA0118I The connection to the management server <SMU_hostname> : 2002 has been established.
   ```

   If the **Status** in message EEZA0116I is not '1', check the status of the port or firewall to fix the communication problem between the adapter and Service Management Unite.

Troubleshooting for administration

Find out all the help that is offered if you require support or want to solve an issue while administering Service Management Unite Automation.

Known problems and solutions

This section contains know problems and solutions of troubleshooting for administration.

Log and trace file location

Locate the log and trace files that are relevant for automation management.

Log and trace files of the operations console and the automation framework

The operations console and the automation framework of IBM Service Management Unite Automation use the log files and the tracing function of WebSphere Application Server.

By default, the information is written to the following log and trace files:

- `SystemOut.log`
- `SystemErr.log`
- `trace.log`

The files are in the following directory:

```
<JazzSM_root>/profile/logs/<server_name>
```

Use the WebSphere administrative console to set the parameters for logging and tracing:

- To specify log file parameters, for example, the log file names, the maximum size, and the number of history log files to be preserved, open the WebSphere administrative console and go to **Troubleshooting > Logs and Trace >** <server_name> **> Diagnostic Trace**.
- To set the parameters for tracing, for example, to switch tracing on or off or to define for which components traces should be recorded, open the WebSphere administrative console and go to **Troubleshooting > Logs and Trace > Diagnostic Trace> Change Log Detail Levels**.

Traceable components

For the components of IBM Service Management Unite Automation that run in WebSphere Application Server, it is possible to enable logging and tracing with different scopes, varying from all component groups (com.ibm.eez.*) to fine-grained individual components.

You change the logging and tracing levels for the components of IBM Service Management Unite Automation on the **Change Log Detail Levels** page in the WebSphere administrative console. The names of the components start with the string *com.ibm.eez*. To change the log detail levels for all traceable user interface components, change the settings for the component group *com.ibm.eez.ui.**. For tracing all Service Management Unite Automation components, you would enter in the field *=info: *com.ibm.eez.*=all*.

Tivoli Common Directory location

Message and trace logs for Tivoli products are located under a common parent that is called the Tivoli Common Directory. The log and trace files of all components of IBM Service Management Unite Automation that are not running within WebSphere Application Server, for example, the log and trace files of the automation framework and of the automation adapters, are written to the product-specific subdirectory of the Tivoli Common Directory.

The path to the Tivoli Common Directory is specified in the properties file `log.properties`. The file `log.properties` is located in the `/etc/ibm/tivoli/common/cfg` directory.

In the `log.properties` file, the path to the Tivoli Common Directory is defined in the property `tivoli_common_dir=<path_to_Tivoli_Common_Directory>`.

The path `/var/ibm/tivoli/common` is the default value.

These are the relevant subdirectories for automation management:

Subdirectory	Description
`<Tivoli_Common_Directory>/eez/logs`	message log files, trace files
`<Tivoli_Common_Directory>/eez/ffdc`	FFDC files

For information about the log and trace files of the automation adapters, refer to the adapter-specific documentation.

Restart workflow fails

If the restart workflow fails, it can have one of the following three reasons.

1. The restart workflow is rejected. The workflow does not start or terminates immediately. The following reasons apply:
   - The observed state of the resource is not Online.
   - The desired state of the resource is NoChange.
   - The restart of the resource is already running.
   - The automation domain throws an exception while processing the initial offline request.
2. The restart workflow is interrupted. The following reasons apply:
   - Another request with a higher priority changes the observed state of the resource.
   - The restart workflow timed out. The offline or online request does not complete within a given timeframe. The default timeout range is 48 hours. For more information, see Resolving timeout problems.
3. All restart workflows are interrupted for the whole domain or node. The following reasons apply:
   - Activation of an automation policy.
   - Start or stop the first-level automation adapter.
   - Exclude the first-level cluster node.
   - Stop the WebSphere Application Server which affects all ongoing restart workflows.

Resources do not appear because credentials for accessing automation domains are not configured

The System Automation operations console implements a cache of automated resources which is populated automatically after the startup of WebSphere Application Server. It is populated using the functional user ID that is configured in the configuration dialog as described in this topic.

In addition, any queries against automation domains are issued using functional credentials. Note that operational tasks, like issuing requests or commands, are always issued using the credentials of the user that has logged in to the domain from within the dashboards and never using the functional user credentials configured in the configuration dialog.

Indicators are:

- No nodes displayed for the first-level automation domain.
- Message EEZJ0076E in WAS SystemOut.log and as message in dashboard views.

For all connected first-level automation domains, credentials must be configured using the configuration utility.

1. From the command line, open the configuration dialog using `cfgsmu`.
2. In the **Service Management Unite host configuration** section, click **Configure**.

3. Navigate to the **User Credentials** tab.
4. Configure the credentials for accessing first-level domains.

You can configure generic credentials if you use the same user ID and password for many domains, and you can configure specific configuration for domains that have different credentials.

OutOfMemory exception when trying to view the domain log

The size of log files of your automation domain grows up to a specified limit. When this limit is reached, the current log file is automatically saved as a different file name.

Logging continues with a new empty file with the same name. When you experience OutOfMemory problems when trying to view the log file this problem can be circumvented by reducing the maximum size of the file using the IBM Service Management Unite Automation configuration tool (**Logger** tab of the Universal Automation Adapter configuration dialog). You may consider to copy your current log file on a regular basis to a different location, for example once a week into a folder named OldLogFiles. You achieve a well structured log file history as you start each week with an empty log file.

Using multiple browser windows to connect to the same IBM Dashboard Application Services Hub from the same client system

If you are using a browser other than Microsoft Internet Explorer, opening multiple browser windows on the same client machine to connect to the same IBM Dashboard Application Services Hub causes unexpected results.

This is because only Microsoft Internet Explorer establishes a separate HTTP session for each browser instance. Other browser types share a single session between multiple browser instances on the same system if these instances connect to the same IBM Dashboard Application Services Hub.

The same situation occurs if you open multiple Microsoft Internet Explorer browser windows using **File > New Window** (or Ctrl + N) from an existing IBM Dashboard Application Services Hub session, because in this case the new browser window and the one from which it was opened also share the same session.

Topology widget graph area is blank

Graph area of a topology dashboard widget may be blank when using Internet Explorer 9 or 10 (64-bit only). The topology widget requires the Adobe flash plugin. Even with the Adobe flash plugin installed there might be a conflict between the video driver and the flash plugin when using Internet Explorer.

From a 64-bit Internet Explorer browser, this behavior may be caused by a conflict between the IE Adobe plugin and your video driver. To resolve the issue:

1. Open Internet Explorer and in the **Tools** menu, select **Internet Options**.
2. Click the **Advanced** tab, and locate the **Accelerated Graphics** section.
3. Change the setting for **Use software rendering instead of GPU rendering** check box.
4. Click **Apply** to commit your changes.
5. Click **OK** to exit **Internet Options Dialog**.
6. To enable the updated setting, restart Internet Explorer.

Topology node selection with browser or desktop zoom level greater than 100% does not work reliably

Resources which are displayed using the graphical topology widget, for example in the Relationships view on the domain page, are not selectable and the right-click context menu cannot be opened reliably.

The topology widget reads the zoom level of the widget using the toolbar actions, but it cannot read the zoom level set in the browser or on the desktop. Also for a browser, when zoom levels are set to greater than 100%, the topology widget does not register the changed settings and the mouse cursor position is incorrectly mapped.

Browser Zoom Level

Set a browser zoom level. Use the following keystroke combinations to adjust the browser zoom level.

- Press Ctrl and 0 to reset browser zoom level.
- Press Ctrl and = to zoom in.
- Press Ctrl and - to zoom out.

Desktop Zoom Level

Follow your operating system documentation to set zoom levels to 100%.

- In Microsoft 7, for example, change the zoom level for the desktop in **Control Panel** through **Appearance and Personalization -> Display** and select the **Smaller** option. If you set the zoom level to Medium or Larger, it equates to 125% and 150% respectively. The topology widget does not register the new settings and therefore the mouse cursor position is not correctly mapped to the coordinates of the topology widget nodes.
- In Microsoft Windows XP, right-click on your desktop and select **Display Properties**. In the **Settings** tab, click **Advanced** and set the **Display DPI** setting to Normal (96 DPI).

A first-level automation domain is not displayed in the topology tree after an outage

After a planned or unplanned outage of the automation framework, it may happen that first-level automation domains that were previously visible on the topology tree in the operations console do not appear again. This may occur if the automation database was cleared for some reason, or if the timeout defined by the environment variable com.ibm.eez.aab.domain-removal-hours was exceeded.

For more information, see "Resolving timeout problems" on page 133.

To resolve the problem, stop and restart the first-level automation adapter. If the first-level automation domain is still not displayed in topology tree, check the instructions in "A System Automation for Multiplatforms domain is not displayed in the topology tree" on page 130.

A System Automation for Multiplatforms domain is not displayed in the topology tree

If a first-level automation domain does not appear in the topology tree on the operations console, perform the following steps to analyze and resolve the problem:

Procedure

1. Check if the adapter is running by issuing the following command on one of the nodes of the domain:

   ```
   samadapter status
   ```

   If the adapter is running, a message similar to the following example comes up:

   ```
   samadapter is running on sapb13
   ```

   Make a note of the name of the node on which the adapter runs (in the example this is sapb13) and proceed with step 4.
2. If the adapter is not running, issue the following command to check if the domain is online:

   ```
   lsrpdomain
   ```

   A message like in the following example comes up:

   ```
   Name    OpState RSCTActiveVersion MixedVersions TSPort GSPort
   domain1 Online  2.4.4.2           No            12347  12348
   ```

   If `OpState` is not `Online`, start the domain.
3. If the domain is online, start the adapter with the following command:

   ```
   samadapter start
   ```

   After the start message has appeared, reissue the following command:

   ```
   samadapter status
   ```

4. If the adapter is running, check again on the operations console if the domain now appears in the topology tree. Note that it may take time until the contact to the automation framework is established after the adapter is started.
5. If the domain still does not appear in the topology tree, you need the connection information that you specified in the adapter configuration dialog to resolve the problem. Perform the following steps:
   a) Launch the adapter configuration dialog of System Automation by issuing the following command on a node in the domain:

   ```
   cfgsamadapter
   ```

   b) On the entry window of the configuration dialog, click **Configure**.

   c) Open the Adapter page on the Configure window and write down the values that appear in the following fields:

   - **Host name or IP Address**
   - **Request port number**

   This is the connection information the operations console host uses to reach the adapter on any of the nodes in the domain.

   d) Open the page Host using adapter and write down the values that appear in the following fields:

   - **Host name or IP Address**
   - **Event port number**

   This is the connection information the adapter on any of the nodes in the domain uses to reach the operations console host.
6. Check if the operations console host can be reached from each node in the domain.

   A simple test is `ping <operations console host>`.

   If there is a firewall between the nodes of the domain and the operations console host, check with the network administrator if the firewall permits a connection between the node (page Adapter: **Host name or IP Address**) and the operations console host (page Host using adapter: **Host name or IP Address** and **Event port number**).
7. The adapter determines whether SSL must be used for the communication with the operations console host.

   To check the SSL settings of the adapter, launch the adapter configuration dialog using the command `cfgsamadapter`. On the Security page, verify that the SSL settings are correct.

   Note: If the operations console host is configured for using SSL, the adapter must be configured for SSL as well. The SSL configuration of the end-to-end automation manager is performed using the `cfgsmu` configuration utility.
8. On the operations console host, use **netstat** to find out if it is listening for events on the event port defined in **Event port number**.

   When the event port number is set to 2002 host, **`netstat -an`** displays a message like in the following example:

   ```
    Active Internet connections (servers and established)
    Proto Recv-Q Send-Q Local Address       Foreign Address     State
    tcp        0      0 :::2002             :::*                LISTEN
    tcp        0      0 10.0.0.1:2002       10.0.0.2:59261      ESTABLISHED
   ```

   If **netstat** does not display any information about the event port defined in **Event port number**, open the file `/etc/hosts` and verify that the loopback address (`127.0.0.1`) is not related to the actual host name. The loopback address should be related to localhost only. For example, the entry in `/etc/hosts` may look like the following:

   ```
   127.0.0.1               localhost.localdomain localhost
   ```
9. Check if each node in the domain can be reached from the operations console host.

A simple test is `ping <host name or IP Address>`.

If there is a firewall between the operations console host and the nodes of the domain, check with the network administrator if the firewall permits a connection between the operations console host (page Host using adapter: **Host name or IP Address** and **Request port number**) and the node (page Adapter: **Host name or IP Address**).

10. On the node on which the adapter is running, use **netstat** to find out if it is listening on the port defined in **Request port number**.

    For example, when the request port number is set to 2001, **`netstat`** displays a message like the following:

    ```
    sapb13:~ # netstat -atn |grep 2001
    tcp        0      0 9.152.20.113:2001       :::*                    LISTEN
    ```

11. When the communication between all ports has been established correctly (see the descriptions above), check whether the EEZ Publisher is running. The EEZ Publisher must be running on the master node of the System Automation for Multiplatforms domain. To check if the publisher is running, perform the following steps:

    a) Issue the following command on one of the nodes of the first-level automation domain:

    ```
    lssamctrl
    ```

    If the publisher is enabled, you will receive output like in the following example:

    ```
    safli03:~ # lssamctrl | grep Publisher
    EnablePublisher        = EEZ
    ```

    b) Issue the following command on the master node of the System Automation for Multiplatforms domain:

    ```
    ps axw | grep SAMAdapter
    ```

    You should receive output like in the following example:

    ```
    32739 ? Sl 0:01 /usr/sbin/rsct/bin/SAMAdapter
    /etc/opt/IBM/tsamp/sam/cfg/sam.adapter.properties EEZ false 1
    ```

12. If the domain still does not appear on the operations console contact IBM support and provide diagnostic information:

    a) On each node in the domain, find out where the trace files are located.

    The trace files can be found in the `/eez/logs` subdirectory of the Tivoli Common Directory. To find the path to the Tivoli Common Directory, issue the following command:

    ```
    cat /etc/ibm/tivoli/common/cfg/log.properties
    ```

    The command returns the path to the Tivoli Common Directory, for example:

    ```
    tivoli_common_dir=/var/ibm/tivoli/common
    ```

    This means that the trace files can be found in the following directory:

    ```
    /var/ibm/tivoli/common/eez/logs
    ```

    b) Use `tar` to package all files in the directory and provide the archive to IBM support.

Command Execution

IBM Service Management Unite Automation provides the **Issue Command** dashboard that allows a user to issue NetView commands. If issues occur with any return codes of your executed command, you can use information in this topic for root cause analysis.

Reserved Return Codes

The adapter, used to issue NetView commands on a remote system, utilizes the reserved codes to signal to IBM Service Management Unite Automation a problem with the execution of the command.

If the issued command itself exits with one of these defined return codes, IBM Service Management Unite Automation interprets this return code and shows an error message, even if the issued command implies another meaning with this return code.

It is a good practice to issue only commands that will not return the reserved return codes.

Table 19. Reserved return codes for Command Execution

Reserved Return Code	Meaning for IBM Service Management Unite Automation	EEZ Message
9001	User not authorized to execute command.	EEZU0049E
9002	Command does not exist.	EEZU0050E
9003	Unknown misbehavior during execution of command.	EEZU0056E
9004	Operator task not defined.	EEZU0051E

Resolving timeout problems

If you experience timeout problems when accessing first-level automation domains, this could mean that the default values of some optional JEE framework environment variables are not appropriate for your environment.

The following table lists the environment variables that you might need to change to resolve the problems.

More information about the environment variables is provided in the following topics.

Table 20. Environment variables of the automation JEE framework

Variable name	Minimum value	Default value	Maximum value
com.ibm.eez.aab.watchdog-interval-seconds	60	300	86400
com.ibm.eez.aab.watchdog-timeout-seconds	2	10	60
com.ibm.eez.aab.domain-removal-hours	1	48	1000
com.ibm.eez.aab.resource-restart-timeout-hours	1	1	3600
com.ibm.eez.aab.invocation-timeout-seconds	30	60	3600

Rules:

- If the value of an environment variable is below the minimum value for that variable, the minimum value is used.
- If the value of an environment variable is above the maximum value for that variable, the maximum value is used.
- Cross-dependency: To ensure that domains are removed only after the health state has moved to some timeout or failed state, the value of the variable:

  ```
  com.ibm.eez.aab.domain-removal-hours
  ```

  must be greater than the value of:

  ```
  com.ibm.eez.aab.watchdog-interval-seconds/3600
  ```

  If you specify values that violate this rule, the user-specified value for:

  ```
  com.ibm.eez.aab.domain-removal-hours
  ```

is ignored and the value of:

```
com.ibm.eez.aab.domain-removal-hours
```

is set to

```
com.ibm.eez.aab.watchdog-interval-seconds/3600 +1
```

Watchdog - A mechanism for monitoring the domain communication states

The automation framework includes a watchdog mechanism to determine the health state of the communication with each domain. If the automation framework and the domain in question have not communicated successfully during the time interval defined by the environment variable:

```
com.ibm.eez.aab.watchdog-interval-seconds
```

(default value: 300), the automation framework invokes a test operation on the domain. This test operation may only take a limited amount of time, as defined by the environment variable:

```
com.ibm.eez.aab.watchdog-timeout-seconds
```

Depending on the outcome of this test operation, the domain communication health state is updated and reflected in the operations console accordingly.

If a very large number of domains is to be monitored or the domain contains a very large number of resources and the value of:

```
com.ibm.eez.aab.watchdog-interval-seconds
```

is not sufficiently large, the watchdog might not be able to contact all domains and receive their reply events within the given time. This results in incorrect communication state changes for the affected domains:

- In the WebSphere Application Server message log, pairs of messages EEZJ1003I can be found for each of these domains, indicating that the domain's communication state was changed from "OK" to "AsyncTimeout" and back to "OK" within a short time.
- In addition, the operations console icons for the affected domains change accordingly for a short time from "The domain is online" to "Resource events cannot be received" and back to "The domain is online".

To resolve the problem, increase:

```
com.ibm.eez.aab.watchdog-interval-seconds
```

to a value that is approximately double that of the number of domains. For example, if there are 200 domains, the value of:

```
com.ibm.eez.aab.watchdog-interval-seconds
```

should be set to `400`.

If the number of resources to be monitored on the operations console is very large, increase the value of:

```
com.ibm.eez.aab.watchdog-interval-seconds
```

in steps of 200 seconds until the result is satisfactory.

Database cleanup timeout for automation domains

The automation framework contains a mechanism for removing automation domains from the database after a period of inactivity. The domains themselves are not removed, just the representation of the domains in the automation framework is removed.

When the automation framework detects that no communication with a particular domain has occurred for a time interval that is longer than the clean-up timeout interval defined in the environment variable:

```
com.ibm.eez.aab.domain-removal-hours
```

it removes the related domain information from the database.

If the automation framework are stopped for a time, such domains will be removed only after attempts to contact them failed.

Whenever the automation framework removes a domain, the operations console is notified about the change and refreshed accordingly.

Restart request timeout

The automation framework observes resource restart requests until they are completed. After the restart, the resource is online. In some other situations, the restart does not finish. For example, a restart request is sent to resource A. Resource A has a dependency relationship to resource B. This dependency relationship inhibits to stop resource A. In this case, the restart request waits until B changes its state. Pending restart requests are removed after they timed out. You can find the timeout value in the environment variable:

```
com.ibm.eez.aab.resource-restart-timeout-hours
```

Method invocation timeout between the automation framework and the automation adapters

A timeout value can be set to control how long an operation between the automation framework and the automation adapters might take. The environment variable *com.ibm.eez.aab.invocation-timeout-seconds* is used to define this timeout value.

The value of this environment variable should be at least 15 seconds less than the value of the WebSphere ORB request timeout property. Otherwise, "CORBA.NO_RESPONSE: Request timed out" errors could be encountered by the operations console if an operation takes longer than the time interval specified by the ORB request timeout. The default value for the WebSphere ORB request timeout is 180 seconds. The ORB request timeout property can be changed from the WebSphere administrative console. To view or change the property, open the WebSphere administrative console and go to **Servers > Server Types > WebSphere application servers > server1 > Container Services > ORB service**. For more information about the ORB request timeout property, see the WebSphere documentation.

The *com.ibm.eez.aab.invocation-timeout-seconds* variable is used for the communication with all automation adapters. There is no individual timeout value per automation adapter.

Note: The communication with the automation framework does not support method invocation timeout. This means that either the connection cannot be established, in which case the operation returns with an exception immediately, or the operation continues until a connection is established.

Modifying the environment variables for the automation framework

The current value of each variable is displayed when the application EEZEAR is started. Look for messages EEZJ1004I, EEZJ1005I, EEZJ1006I in the WebSphere Application Server log (`SystemOut.log`).

If the default values of the environment variables are not appropriate for your environment, you can change them by running these steps in the WebSphere administrative console:

1. Log on to the WebSphere administrative console.
2. Go to **Servers > Server Types > WebSphere application servers > server1 > Server Infrastructure > Java and Process Management > Process Definition > Additional Properties > Java Virtual Machine > Additional Properties > Custom Properties**.

   Click **New** to create a new variable, or select an existing variable to change its value.

3. Enter values for **Name** (com.ibm.eez.aab.<variable_name>) and **Value** (<new_value>). You can also enter a description.
4. Save your changes.

WebSphere Application Server must be restarted for the changes to take effect.

OutOfMemoryError in the WebSphere Application Server log file

An OutOfMemoryError may occur if a large amount of data is returned from a first-level automation domain. Depending on the situation, the error may become visible on the operations console or in the WebSphere Application Server message log file.

Perform the following steps to increase the JVM heap size:

1. Log on to the **WebSphere administrative console**.
2. Navigate to **Servers > Server Types > WebSphere application servers > server1 > Server Infrastructure > Java and Process Management > Process definition > Additional Properties > Java Virtual Machine**.
3. Set the value to at least 768 MB. Refer to the WebSphere Application Server online documentation for more information about how to determine the optimum value for the maximum heap size, depending on the available physical memory.
4. Save your changes. WebSphere Application Server must be restarted for the changes to take effect.

Modifying available heap size

After the installation of IBM Service Management Unite Automation, modify the heap size settings of the WebSphere Application Server to the following recommended values:

- Minimum heap size: 768 MB
- Maximum heap size: 2048 MB

Perform the following steps to increase the JVM heap size:

1. Log on to the **WebSphere administrative console**.
2. Go to **Servers > Server Types > WebSphere application servers > server1 > Server Infrastructure > Java and Process Management > Process Definition > Additional Properties > Java Virtual Machine**.
3. Enter **2048** for the Maximum Heap Size and **768** for the Minimum Heap Size to avoid `OutOfMemoryErrors`. Refer to the WebSphere Application Server online documentation for more information about how to determine the optimum value for the maximum heap size, depending on the available physical memory.
4. **Save** your changes. Restart WebSphere Application Server for the changes to take effect.

EEZBus is not started

The EEZBus is a sub-component of the automation JEE framework that runs within WebSphere Application Server. There are several potential reasons why the EEZBus cannot be started. The reasons and proposed actions are described in this topic.

EEZBus is not started due to a security problem

If the EEZBus cannot be started, this may indicate a problem with the DB2® instance account for the automation framework databases, regardless of whether you are using DB2 or LDAP as the user registry.

In such a case, one or more of the following symptoms may occur:

- On the messaging engine panel of the WebSphere administrative console **Service integration > Buses > EEZBus > Topology > Messaging engines**, you can see that the EEZBus is not started. When you try to start the bus, the following error message is displayed:

```
The message engine <node_name.server_name> EEZBus cannot be started.
```

- If you are using DB2 as the user registry, the following exception appears in the WebSphere Application Server log file:

```
00000f1d FreePool      E   J2CA0046E:
Method createManagedConnectionWithMCWrapper caught an exception
during creation of the ManagedConnection for resource jms/
       EEZTopicConnectionFactory,
throwing ResourceAllocationException.
Original exception: javax.resource.ResourceException:
CWSJR1028E: An internal error has occurred.
The exception com.ibm.websphere.sib.exception.SIResourceException:
CWSIT0006E: It is not possible to contact a messaging engine in bus EEZBus.
was received in method createManagedConnection.
```

- If you are using LDAP as the user registry, the following exception appears in the WebSphere Application Server log file:

```
000000a2 FreePool      E   J2CA0046E:
Method createManagedConnectionWithMCWrapper caught an exception
during creation of the ManagedConnection for resource jdbc/EAUTODBDS,
throwing ResourceAllocationException.
Original exception: com.ibm.ws.exception.WsException:
DSRA8100E: Unable to get a XAConnection from the DataSource.
with SQL State : null SQL Code : -99999
```

To eliminate a problem with the DB2 instance account as the cause, check the database connection from the WebSphere administrative console:

1. Select the data source.
2. Click **Test connection**.

If the DB2 instance account for the automation framework databases causes the problem, you receive the following message:

```
Test connection failed for data source EAUTODBDS
on server <serverName> at node <nodeName> with the following exception:
java.lang.Exception: java.sql.SQLException:
      Connection authorization failure occurred.
Reason: password invalid. DSRA0010E: SQL State = null, Error Code = -99,999.
```

The automation framework fails to initialize

The message `EEZJ0030E The end-to-end automation manager is not fully initialized and refuses to accept requests. The following subcomponents are not yet initialized: [EventHandlerBean]` may appear when logging in on the operations console. This message indicates that the initialization phase of the automation framework has not yet completed after a restart. Normally, this message will not show up again if you log in again after a short period of time. Internally, the automation framework regularly tries to initialize the missing components.

However, there are situations when this initialization step never completes.

A transaction timeout may occur before the communication timeout is reached. In addition, the WebSphere Application Server process may be restarted automatically.

Solution:

The following table shows the sub-components that may be listed within message EEZJ0030E, and the respective troubleshooting actions:

Table 21. Sub-components implicated by message EEZJ0030E

Subcomponent name	Solution
AutomationProperties	Ensure that the automation framework has read access to the properties file `eez.automation.engine.properties` that is located in the `EEZ_CONFIG_ROOT` directory.

Table 21. Sub-components implicated by message EEZJ0030E (continued)

Subcomponent name	Solution
DB2	If remote DB2 is used, ensure that the DB2 instance is started. See "WebSphere Application Server cannot connect to DB2" on page 138 for details.
EventHandlerBean	See "EEZBus is not started" on page 136.
FLAEventReceiver	Transient state only. Indicates that the subcomponent that receives events from first-level automation domains has not been initialized yet. If the problem persists, restart WebSphere Application Server. If this does not solve the problem, check the WebSphere Application Server logs and the IBM Service Management Unite Automation installer logs for more details related to the first-level automation resource adapter.
ManagedDomainsRegistry	Transient state only, or accompanied by subcomponent "DB2". Check the solution for that subcomponent first.
ServerConfigCache	Transient state only. Indicates that the automation framework has not yet read the WebSphere Application Server configuration properties that the automation framework needs to know.
StartupBean	Transient state only. If it persists, restart WebSphere Application Server.
WatchdogBean	Transient state only. The WatchdogBean is the last component that gets started. After all other components are started successfully, then this component refreshes the states of the automation domains and verifies if the previously known nodes still exist.
RestartRegistry	Transient state only. Indicates that the in-memory registry of pending restart requests has not yet been initialized.

WebSphere Application Server cannot connect to DB2

When you receive an error message indicating that WebSphere Application Server could not establish a connection to the automation framework database, check first if the database server is started.

If it was not started, start the database server. If the System Automation operations console does not recover within two minutes, restart WebSphere® Application Server.

If the DB2 database server was started already this may indicate that the DB2 port number is not specified correctly in the WebSphere administrative console.

To verify if the DB2 port number is specified correctly, run the following steps:

1. On the DB2 server system, check which port number DB2 is using. On Linux, for example, use the **`netstat`** command to obtain the following information:

   ```
   sys1:~ #
   netstat -atnp | grep db2
   tcp  0  0 0.0.0.0:50001     0.0.0.0:*         LISTEN      8714/db2sysc
   tcp  0  0 x.x.x.x:50001     y.y.y.y:38306     ESTABLISHED 8714/db2sysc
   tcp  0  0 x.x.x.x:50001     z.z.z.z:42614     ESTABLISHED 8714/db2sysc
   ```

   In the example, the correct DB2 port number is `50001`.
2. In the WebSphere administrative console, navigate to **Resources>JDBC>Data sources >EAUTODBDS** and check whether the port number is specified correctly in the field **Port number**.

"Unable to set up the event path..." error message is displayed in the IBM Dashboard Application Services Hub

When you try to connect the operations console the following error message is displayed in the IBM Dashboard Application Services Hub:

```
Unable to set up the event path between the operations console
  and the management server:
CWSIA024E: An exception was received during the call to the method
   JmsManagedConnectionFactoryImpl.createConnection:
   com.ibm.websphere.sib exception SIRexourceException:
CWSIT0006E: It is not possible to contact a messaging engine in bus EEZBus
```

This may indicate a problem with the DB2 instance account for the automation framework databases. To check if this is the case, check whether the password for the DB2 instance account has expired or is incorrect.

Mozilla Firefox browser displays special characters incorrectly when editing policies

If special characters are incorrectly displayed when you edit policies, select **View > Character Encoding > Auto Detect > Universal** in the browser menu.

Troubleshooting the Universal Automation Adapter

Universal Automation Adapter does not start

If there is no UAA domain already defined, the UAA will not start successfully. Define at least one domain using the configuration utility and retry to start the UAA.

Universal Automation Adapter log files

Location of the adapter log files:

Tivoli Common Directory

The log files are written to the following sub-directories of the Tivoli Common Directory:

- `eez/ffdc` – Contains the First Failure Data Capture files (if the FFDC recording level is not set to Off in the adapter configuration dialog)
- `eez/logs` – Contains the Universal Automation Adapter log files:
    - `msgEEZALAdapter.log`
    - `eventEEZALAdapter.log` and `traceFlatEEZALAdapter.log` (if the trace logging level is not set to Off)

Default Universal Automation Adapter installation directory

`/opt/IBM/smsz/ing/eez/bin`

Universal Automation Adapter fails to connect to the operations console host

For a Universal Automation Adapter (UAA) installation check if ports are configured as expected, and TCP sessions are established.

Check with `netstat` if TCP sessions are established:

- Whether the UAA listens on the request port (default port is 2001).
- Whether the operations console host listens on the event port (default port is 2002).

For UAA, if no sessions are established try to set up TCP sessions, for example using `telnet`:

- `telnet <operations console host> 2002` from the system running the UAA.
- `telnet <Universal Automation Adapter address> 2001` from the system running the IBM Service Management Unite Automation installation.

Where `<operations console host>` is the IP address or fully qualified domain name of the system hosting the IBM Service Management Unite installation. `<Universal Automation Adapter address>` is the IP address or fully qualified domain name of the UAA. If a session setup is not possible using `telnet` check again that the firewall allows this.

Universal Automation Adapter domain and resource states are not refreshed as expected

If the states of remote resources that are managed by the Universal Automation Adapter do not reflect the actual state of the resources within a reasonable time frame then consider to tune the Universal Automation Adapter domain topology. For more information, see "Tuning the number of domains and resources of the Universal Automation Adapter" on page 81.

Analyzing the states of remote resources

If the states of remote resources that are managed via the Universal Automation Adapter indicate some issue, see the Monitor command for hints about the potential root cause of the issue based on the combination of the monitor command return codes and the resource states.

Resource states that are affected by the state of the target node

The following table lists resource states caused by communication problems with the target node.

Table 22. Resource states that are affected by the state of the target node

Scenario	Root cause	Resource Observed State	Resource Operational State	Resource Compound State	Monitoring consequences for resources and target node states
Waiting for state information	• after eezaladapter started (last policy activated) • after new policy activated • after subscription is deleted (unsubscribed)	Unknown	NoContact	Warning	Next resource monitor is started with next subscription or after next resource query. Target node is also not being monitored until next resource monitor is started.
Communication has been interrupted or timed out.	• network problem • monitor command timeout	Unknown	LostCommunication	Error	Next resource monitor is started after MonitorCommandPeriod. Same for target node monitor.

Table 22. Resource states that are affected by the state of the target node (continued)

Scenario	Root cause	Resource Observed State	Resource Operational State	Resource Compound State	Monitoring consequences for resources and target node states
Hosting node is not available.	• target node offline • wrong hostname in policy • no IP address found for hostname • firewall prevents access to host • sshd stopped	Unknown	SupportingEntityInError	Error	Next resource monitor is started after MonitorCommandPeriod. Same for target node monitor.
User credentials are incorrect	• wrong user ID or password in configuration • password expired • user ID does not exist • wrong ssh public keys in configuration	Unknown	BrokenResource	Fatal	Next resource monitor is started after next reset action. Target node will no longer be monitored to avoid user IDs to be revoked.
Unable to run a command defined for the resource.	• command not found • user ID has no permissions to execute command	Unknown	InvalidResource	Fatal	Next resource monitor is started after next reset action. Target node will continue to be monitored.
Non recoverable error	• MP monitor command rc = 3 or 4 • start/stop command timeout • start/stop command rc != 0 (Failed)	see UNIX command and System Automation for Multiplatforms monitor command return styles (Using Monitor Command).	NonRecoverableError	Fatal	Next resource monitor is started after next reset action. Target node will continue to be monitored.

Observed states that are affected by the state of the target node

The following table lists all observed states for a target node.

Table 23. Observed states that are affected by the state of the target node

Resource Observed State	Monitoring consequences for resources and target node states
Unknown	If all resources on that node have the operational state NoContact or BrokenResource.
Offline	If at least one resource on that node has the operational state SupportingEntityInError.
Online	All other cases.

Troubleshooting for installation

Use this topic for troubleshooting problems you experience when you install IBM Service Management Unite Automation.

Installation log files

Use this procedure to work with installation log files

Installation Manager log files are located in the Installation Manager `/data/logs` directory. The default location is `/var/ibm/InstallationManager/data/logs`. Otherwise, the `/data` directory location is available from the *appDataLocation* value in the `/etc/.ibm/registry/InstallationManager.dat` file.

Installation Manager logs are XML files in the `/logs` directory. Output files from the multiple system commands that are run during installation are located in the `logs/native` directory. If any command has failed and stopped the installation, the Installation Manager error window will identify the native log file containing output for the failed command.

Turning on debug for the installation

Enable the debug mode to debug problems when you install Service Management Unite Automation.

Procedure

1. Browse to the directory where the properties files are located. The default location is `/var/ibm/InstallationManager/logs`.
2. Open file `log.properties`.

   If it doesn't exist, manually create the file.
3. Add the following lines in the file to enable the debug mode:

```
com.ibm.smu.automation.common=DEBUG
com.ibm.smu.automation.locationcheck=DEBUG
com.ibm.smu.automation.panels=DEBUG
com.ibm.smu.automation.prereqs=DEBUG
```

Results

You've successfully enabled the debug mode for the installation process.

Cleaning up and restoring from a failed installation

If the installation or upgrade is aborted unexpectedly, you need to manually clean up files before you try again.

You can cancel the installation at any time and Installation Manager can reverse the changes and progress automatically.

However, if Installation Manager is stopped unexpectedly during the installation or upgrade phase, you must clean up and restore the files before you try again because Installation Manager cannot roll back if it's stopped unexpectedly.

- Installation Manager exits unexpectedly during the installation:

  Clean up all the files located in the installation directory, the default location is `/opt/IBM/smsz/ing`.
- Installation Manager exits unexpectedly during the upgrade:

  You must manually clean up the old files and restore to the back up ones:

  1. Browse to the installation directory, the default location is `/opt/IBM/smsz/ing`.
  2. Find the folders and replace them with the back up ones:
     - Replace files in folder `bin` with files in `bin.backup`
     - Replace files in folder `Derby` with files in `Derby.backup`
     - Replace files in folder `EIFEventDispatcher` with files in `EIFEventDispatcher.backup`
     - Replace files in folder `install` with files in `install.backup`
     - Replace files in folder `lib` with files in `lib.backup`
     - Replace files in folder `license` with files in `license.backup`
     - Replace files in folder `msg` with files in `msg.backup`
  3. Browse to the directory where the configuration files are stored. The default location is `/etc/opt/IBM/smsz/ing/cfg`.
  4. Find the files with postfix '`.saved`'. For example, find the file `eez.aladapter.properties.saved` and save it as `eez.aladapter.properties` to overwrite the existing one.
  5. Try again to upgrade Service Management Unite.

To check the log files, see installation log files.

WebSphere SDK not enabled for JazzSM profile

Use this procedure to debug WebSphere SDK not being enabled for the JazzSM profile.

Service Management Unite Automation requires version 1.7, or later, of the WebSphere Java SDK. The SDK must be installed and also enabled for the JazzSM WebSphere profile. If an error message indicates that the installed SDK is missing, it might require enablement.

To enable the SDK for the JazzSM profile, run the WebSphere managesdk.sh command with the -enableProfile option. For example:

```
was_root/bin/managesdk.sh -enableProfile -sdkName 1.7_64 -profileName
JazzSMProfile -enableServers
```

Known problems and solutions

This section contains know problems and solutions of troubleshooting for installation.

Installation Manager installed by non-root user

Use this procedure to enable running Installation Manager as root user.

If Installation Manager was installed by a user with non-root authority, Installation Manager might not run for a root user, or it might not detect an installed WebSphere and JazzSM. Use the **su** *userid* command to switch to the root user and run as authorized to address the problem.

Installer cannot detect non-default SOAP port

If the default SOAP port settings are changed in the WebSphere Administrator Console, the installer cannot detect these. This causes an error window to be displayed with the message that the cell could not be retrieved.

Changing the SOAP port via the WebSphere Administrator Console does not update the value used by the `wsadmin.sh` command. This will cause all commands which use `wsadmin.sh` and a SOAP connection to fail.

A quick workaround for this problem is to manually edit the file `/opt/IBM/JazzSM/profile/properties/wsadmin.properties` and adjust the value of the variable `com.ibm.ws.scripting.port`.

You can change the default ports of WebSphere using an Ant script. For more information, see http://www-01.ibm.com/support/knowledgecenter/SSEQTP_8.5.5/com.ibm.websphere.base.doc/ae/tins_updatePorts.html. Using the `Ant` script avoids the problem as it correctly updates the SOAP port for `wsadmin.sh`.

Troubleshooting for configuration

Use this topic for troubleshooting problems you experience when you configure IBM Service Management Unite Automation.

SSL configuration problems

If problems occur with the SSL setup, you can use the information in this topic for root cause analysis.

SSL configuration error messages are stored in the following paths:

- On the IBM Service Management Unite Automation side, the messages are stored in the WebSphere Application Server log file:

  ```
  <WAS_PROFILE>/logs/server1/SystemOut.log
  ```

- On the Adapter side in the log file:

  ```
  /var/ibm/tivoli/common/eez/logs/msg<ADAPTER_TYPE>Adapter.log
  ```

The following list describes the most common SSL errors with their corresponding error messages.

1. **Corrupt or empty SSL truststore file specified**

   a. Messages in the Adapter log:

   Table 24. Corrupt or empty SSL truststore file - Adapter messages

Message Identifier	Exception Text
EEZA0038E	Unrecognized keystore entry
EEZA0038E	Received fatal alert: certificate_unknown
EEZA0022E	No trusted certificate found
EEZA0038E	Certificate chain is null

   b. Messages in the Service Management Unite Automation WebSphere log:

   Table 25. Corrupt or empty SSL truststore file - Service Management Unite Automation messages

Message Identifier	Exception Text
EEZA0038E	Invalid keystore format
EEZA0022E	Received fatal alert: handshake_failure
EEZJ0101E	Embedded message EEZI0015E: Unable to connect to the adapter

   User response: Check SSL truststore files on Adapter and Service Management Unite Automation side.

2. **Corrupt or empty SSL keystore file specified**

a. Messages in the Adapter log:

Table 26. Corrupt or empty SSL keystore file - Adapter messages

Message Identifier	Exception Text
EEZA0038E	No trusted certificate found
EEZA0038E	Received fatal alert: certificate_unknown
EEZA0038E	Invalid keystore format
EEZA0032E	Embedded message EEZA0033E: Unable to create socket factory object
EEZA0105I	Embedded return code rc=20: Adapter has been stopped due to initialization failure

b. Messages in the Service Management Unite Automation WebSphere log:

Table 27. Corrupt or empty SSL keystore file - Service Management Unite Automation messages

Message Identifier	Exception Text
EEZA0038E	Received fatal alert: certificate_unknown
EEZA0038E	Invalid keystore format
EEZJ0101E	Embedded message EEZI0046E: SSL connection could not be established
EEZJ0101E	Embedded message EEZI0015E: Unable to connect to the adapter

User response: Check SSL keystore files on Adapter and IBM Service Management Unite Automation side.

3. **Wrong SSL keystore password specified**

a. Messages in the Adapter log:

Table 28. Wrong SSL keystore password specified - Adapter messages

Message Identifier	Exception Text
EEZA0038E	Keystore was tampered with, or password was incorrect
EEZA0032E	Embedded message EEZA0033E: Unable to create socket factory object
EEZA0105I	Embedded return code rc=20: Adapter has been stopped due to initialization failure

b. Messages in the Service Management Unite Automation WebSphere log:

Table 29. Wrong SSL keystore password specified - Service Management Unite Automation messages

Message Identifier	Exception Text
EEZA0038E	Keystore was tampered with, or password was incorrect
EEZA0033E	Unable to create socket factory object
EEZJ0101E	Embedded message EEZI0046E: SSL connection could not be established

User response: Check SSL keystore password on Adapter and IBM Service Management Unite Automation side.

4. **Wrong SSL certificate alias specified**

   a. Messages in the Adapter log:

Table 30. Wrong SSL certificate alias specified - Adapter messages

Message Identifier	Exception Text
EEZA0038E	Certificate chain is null
EEZA0047E	No available certificate corresponds to the SSL cipher suites which are enabled
EEZA0047E	No cipher suites in common
EEZA0105I	Embedded return code rc=12: Adapter has been stopped because initial contact failed

   b. Messages in the Service Management Unite Automation WebSphere log:

Table 31. Wrong SSL certificate alias specified - Service Management Unite Automation messages

Message Identifier	Exception Text
EEZA0022E	Received fatal alert: handshake_failure
EEZJ0101E	Embedded message EEZI0015E: Unable to connect to the adapter

User response: Check SSL certificate alias on Adapter and IBM Service Management Unite Automation side.

5. **Missing SSL configuration on one side**

   a. Messages in the Adapter log:

Table 32. Missing SSL configuration on one side - Adapter messages

Message Identifier	Exception Text
EEZJ0101E	Embedded message EEZI0021E: Using SSL is required for all first-level automation adapters but not enabled for this particular adapter

Reason: SSL was configured only at the IBM Service Management Unite side and enforce use of SSL was enabled, or the adapter was not restarted after SSL was configured.

User response: Check the SSL configuration on the adapter side and restart the adapter.

   b. Messages in the Service Management Unite Automation WebSphere log:

Table 33. Missing SSL configuration on one side - Service Management Unite Automation messages

Message Identifier	Exception Text
EEZA0038E	No such file or directory
EEZJ0101E	Embedded message EEZI0046E: SSL connection could not be established

Reason: SSL was only configured at the adapter side, or WebSphere was not restarted after SSL was configured.

User response: Check the SSL configuration at the IBM Service Management Unite Automation side and restart WebSphere.

Unable to start `cfgsmu` in Docker container

Use this information to solve the problem when you are unable to start **cfgsmu** in Docker container.

Problem

The configuration tool **cfgsmu** cannot be started after you run command **eezdocker.sh cfgsmu**.

Cause

cfgsmu is a GUI tool, and **eezdocker.sh cfgsmu** doesn’t work over SSH sessions to the Docker host machine.

Solution

- If the Docker host machine is accessed by an SSH session, you can select either of the following ways to start the tool:
  - Run command **eezdocker.sh shell** to open a shell inside the SMU container and do a silent configuration. For more information, see “Starting cfgsmu in the Docker container” on page 64.
  - Configure a VNC server on the host machine and log into the desktop environment using VNC to start **cfgsmu**.
- If **cgfsmu** cannot be ran out of the Docker container, it might be necessary to allow access to the X11 session on the host machine. Run the command '**xhost+local:all**' before you run '**eezdocker.sh cfgsmu**' to ensure that the Docker process can access the user's X session.

Chapter 10. Messages

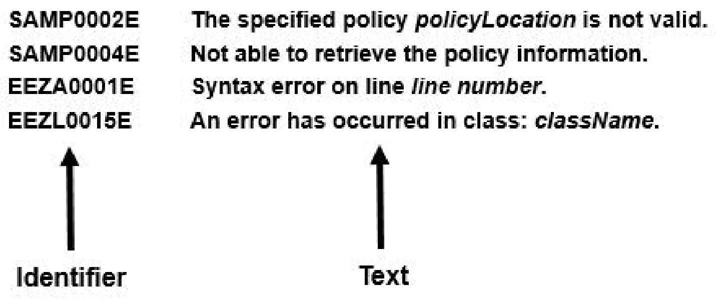
This section contains messages for Service Management Unite Automation.

Message formats

This section introduces the formats of Service Management Unite Automation messages.

- Message text formats

  Most messages are preceded by an identifier, as illustrated in Figure 1.



SAMP0002E The specified policy *policyLocation* is not valid.
SAMP0004E Not able to retrieve the policy information.
EEZA0001E Syntax error on line *line number*.
EEZL0015E An error has occurred in class: *className*.

Figure 7. Sample message format

- Message description formats

  A message consists of several sections. Not all categories are used for each message. For messages that are always issued as a group, the "Explanation" section of the first message usually contains a complete description of the other messages in the group.

SMU Automation messages

All messages that are generated by Service Management Unite Automation installation and configuration are included in this section, including the appropriate user responses.

This section also includes messages for any problems related to launching or using the Service Management Unite Automation dashboard console or the dashboard console online help.

Note: For all other administrative, user and other console-related messages, refer to the dashboard console online help.

EEZ message catalog

This section lists the messages that are generated by subcomponents of the IBM Service Management Unite Automation that have the prefix EEZ. The messages are sorted alphabetically by subcomponent prefix.

For information about additional messages you might encounter while working with the Service Management Unite Automation, see the remaining message sections of this document and to the documentation for the corresponding first-level automation product.

EEZ message code

Most messages that are generated by subcomponents of IBM Service Management Unite begin with a unique message code.

Example:

EEZS1234E

- **EEZ –** component identifier of the IBM Service Management Unite. The EEZ component identifier is also used for System Automation Application Manager.
- **S –** represents one of the following prefixes:
  - **A** - Messages issued by automation adapters

    Note: System Automation for z/OS adapter messages:

    - Within NetView an additional * may be appended to the end of the message text.
    - Because these messages are written to the syslog on z/OS, the message text must be in English.
  - **J, L, T –** Automation JEE framework messages
  - **C –** Messages issued by various utilities
  - **I –** Automation manager resource adapter messages
  - **K, X –** Automation Software Development Kit messages
  - **P –** Policy-related messages
  - **Q –** ITM integration messages
  - **R –** Universal Automation Adapter messages
  - **U –** Operations console messages

  Messages are sorted alphabetically by subcomponent prefix.
- **1234 –** unique four-digit number
- **E –** one of the following severity code identifiers:
  - **I** for Information
  - **W** for Warning
  - **E** for Error

Prefix EEZA

This section contains messages with prefix EEZA.

EEZA0001E **Syntax error on line *line number***

Explanation

A syntax error has occurred in the configuration file, for example a leading = on a line.

System action

The automation adapter stops.

Operator response

Analyze the configuration file for invalid syntax.

EEZA0002E **Wrong datatype in key *the key*. Expected *the desired type*, found value " *the value that was found* "**

Explanation

The value of the given key cannot be interpreted as the desired type. For example, the system expected a boolean value but found the string "hello".

System action

The automation adapter stops.

Operator response

Analyze the configuration file for invalid key/value pairs.

EEZA0003E **The key " *the key that was not found* " was not found and no default value was given**

Explanation

The system attempted to retrieve a value from the configuration file that did not exist and no default value was given.

System action

The automation adapter stops.

Operator response

Supply a value for the key in the configuration file.

EEZA0004E **Integer out of bounds in key " *the key* ". Expected value between *the lower bound expected* and *the upper bound expected*, found *the value parsed***

Explanation

The system expected an integer value between the given bounds (inclusive) for the given key, but found a value outside these bounds.

System action

The automation adapter stops.

Operator response

Supply a value within the given bounds for the key.

EEZA0005I **At least one system symbol cannot be resolved: *text-line***

Explanation

The text line in error contains the system symbol that cannot be resolved. A system symbol is considered unresolved if it is either not defined or empty.

System action

The automation adapter stops.

Operator response

If available, refer to message EEZA0031E that specifies the name of the configuration file in error. Check the text line in error for an invalid system symbol. The system symbol in the corresponding z/OS IEASYMxx parmlib member might not be defined. If you are authorized to do so, enter the z/OS DISPLAY SYMBOLS command to display the system symbols and associated substitution texts that are in effect, and then define the corresponding system symbol if it's missing.

EEZA0006E **Cannot create an instance of the class because class not found: *class name***

Explanation

The automation adapter cannot load the class.

System action

The automation adapter rejects the request.

Operator response

Check whether the class name is valid and is available in the corresponding classpath.

EEZA0007E **Cannot create an instance of the class because method not found: *class name***

Explanation

The automation adapter can load the class but cannot create an instance.

System action

The automation adapter rejects the request.

Operator response

Check whether the class is valid.

EEZA0008E **Cannot create an instance of the class because of an unknown error: *class name***

Explanation

The automation adapter cannot load the class or create an instance.

System action

The automation adapter rejects the request.

Operator response

Check whether the class is valid and analyze the attached original exception.

EEZA0009E **Invocation of adapter plug-in failed: plug-in=*plug-in name*, method=*method name*, internalRetcode=*internal return code*, taskRetcode=*task return code***

Explanation

The automation adapter client API was called to execute a task on the remote adapter. The call failed. There are three error categories: The client suffers an error on the connection or the execution of the task within the automation adapter backend failed or execution failed in the automation adapter plug-in.

System action

Execution of the remote task failed.

Operator response

Analyze the return code description. If it is an internal error, check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZA0010E **Request expires before the adapter passes it to the adapter plug-in. Timeout period is *timeout value* seconds**

Explanation

All requests have an associated expiration date. The request is scheduled to an execution thread that detected that the expiration time had expired.

System action

The automation adapter rejects the request.

Operator response

Analyze the reason (for example, high working load). Increase the timeout period if necessary.

EEZA0011E **The backend program specification is invalid**

Explanation

The backend program is not a Java program or the Java program name was not specified.

System action

The automation adapter rejects the request.

Operator response

Check the program that called the automation adapter client API.

EEZA0012E **Invalid parameter list**

Explanation

The automation adapter detected a request that is associated with an invalid parameter list.

System action

The automation adapter rejects the request.

Operator response

Check the program that called the automation adapter client API.

EEZA0013E **Authentication for user ID *user name* was unsuccessful**

Explanation

The request is associated with a user ID and password that have been validated unsuccessfully.

System action

The automation adapter rejects the request.

Operator response

Check whether the user ID is authorized for the system and check the security policy. Also check if you have stored a user ID and password for this domain in the credential store of the Dashboard Application Services Hub.

EEZA0014E **The original exception *original-class* needs to be transported to the remote caller**

Explanation

An exception from an underlying component needs to be transported to the remote caller.

System action

None.

Operator response

Analyze the original exception attached with this message.

EEZA0015E **Method not supported: *name of the missing method***

Explanation

The automation adapter detected an unknown method name. The list of all valid method names is defined in the EEZAdapterInteraction interface.

System action

The automation adapter rejects the request.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZA0017E **Request not supported: *name of the unsupported request***

Explanation

The automation adapter plug-in does not support the specified request.

System action

The request might be rejected depending on the behavior of the plug-in.

Operator response

Check if the automation domain supports this type of request.

EEZA0022E **Adapter client is unable to connect to the adapter at *host*:*port* due to exception: *the exception that was caught***

Explanation

The automation adapter client cannot connect to the server at the given host and port. The original exception text is provided.

System action

The connection is not established.

Operator response

Analyze the original exception.

EEZA0023E **Cache directory is invalid**

Explanation

The EIF cache directory is not a directory.

System action

The automation adapter stops.

Operator response

Correct the configuration file.

EEZA0024E **EIF sender and receiver must not be equal**

Explanation

The EIF configuration parameters are not allowed to point to each other.

System action

The automation adapter stops.

Operator response

Correct the configuration file.

EEZA0025E **Cannot find the plug-in configuration file: *configuration file name***

Explanation

The master configuration file contains the name of a plug-in configuration file that cannot be found.

System action

The automation adapter stops.

Operator response

Correct the configuration file.

EEZA0026E **No plug-in configuration file was specified**

Explanation

The master configuration file must contain at least one plug-in configuration file.

System action

The automation adapter stops.

Operator response

Correct the configuration file.

EEZA0027E **Cannot load configuration file: *configuration file name***

Explanation

The specified configuration file cannot be loaded.

System action

The automation adapter stops.

Operator response

Correct the configuration file.

EEZA0028E Plug-in configuration file does not contain all mandatory parameters: *configuration file name*

Explanation

The specified configuration file does not contain all mandatory parameters. The plug-in is not used.

System action

The automation adapter does not deploy the plug-in.

Operator response

Correct the configuration file.

EEZA0029E Cannot create the first instance of the plug-in class: *class name*

Explanation

An attempt was made to create the first instance of the plug-in during initialization. Creation failed.

System action

The automation adapter does not deploy the plug-in.

Operator response

Correct the configuration file.

EEZA0030E Cannot set up event subscription list for plug-in configuration file: *plug-in configuration file name*

Explanation

The specification of the EIF event classes in the plug-in configuration file is invalid.

System action

The automation adapter does not deploy the plug-in.

Operator response

Correct the configuration file.

EEZA0031E Cannot load configuration file from: *plug-in configuration file name*

Explanation

The automation adapter cannot load the specified configuration file because either no configuration file or an invalid one was specified.

System action

The automation adapter stops.

Operator response

Check whether the name of the configuration file is correct.

EEZA0032E Initialization of the adapter failed: *original exception*

Explanation

An error occurred in the initialization step of the automation adapter.

System action

The automation adapter stops.

Operator response

Analyze the associated exception. If there is no exception text for this message, try to find additional messages that were sent previously.

EEZA0033E Unable to create *type of factory* SocketFactory

Explanation

The automation adapter server or client cannot create a socket factory for remote contact.

System action

The automation adapter client cannot create a connection or the automation adapter server cannot receive connections.

Operator response

Analyze the reason using previous messages.

EEZA0036E The adapter suffered an unexpected interruption: *original exception*

Explanation

The automation adapter waits for a termination command. An unexpected interruption occurred.

System action

The automation adapter stops.

Operator response

Analyze original exception.

EEZA0037E **The adapter stops running because no plug-in has been successfully initialized**

Explanation

At least one plug-in must have been successfully initialized otherwise the automation adapter stops.

System action

The automation adapter stops.

Operator response

Analyze previous messages and exceptions issued by the failing plug-in.

EEZA0038E **A (SSL) socket configuration error occurred: *exception text***

Explanation

An error occurred during the loading or processing of (SSL) socket-related configuration data. An SSL handshake exception will only be reported during initial contact.

System action

The automation adapter client cannot create a connection or the automation adapter server cannot receive connections.

Operator response

Analyze the exceptions text. Check the SSL configuration file if necessary.

EEZA0039E **Not all data was read from socket: *number of bytes read* bytes read, *number of bytes expected* bytes expected to be read**

Explanation

The incoming request has a length in bytes, but not all bytes can be read.

System action

The automation adapter rejects the request.

Operator response

Check why the socket connection was broken while transfering data.

EEZA0040E **The adapter client cannot establish connection to the adapter: *string representation of the connection***

Explanation

Opening the connection failed. A request cannot be sent to the automation adapter. The string representation of the connection contains details about the connection.

System action

The automation adapter frontend failed.

Operator response

Analyze the connection information.

EEZA0041E **The adapter client cannot invoke an adapter request: InternalRC=*internal return code*, TaskRC=*task return code***

Explanation

A connection to the automation adapter has been successfully established. The automation adapter frontend might have sent a request to the automation adapter but the request failed. If the internal or task return codes are not applicable (n/a), some other unexpected exception occurred.

System action

The automation adapter frontend failed.

Operator response

Analyze the internal and task return codes (see EEZA0009E for an explanation of the return codes).

EEZA0042E **The adapter has thrown a remote exception: InternalRC=*internal return code*, TaskRC=*task return code*. The original message was: *message text***

Explanation

A connection to the automation adapter has been successfully established. The automation adapter frontend has sent a request to the automation adapter but the plug-in has thrown an exception.

System action

None.

Operator response

Analyze the internal and task return codes (see EEZA0009E for an explanation of the return codes).

EEZA0043E **A required command line parameter is missing**

Explanation

One of the required command line parameters is missing (such as -start, -stop or -terminate).

System action

The automation adapter frontend failed.

Operator response

Specify the required command-line parameters and try again.

EEZA0045E **The adapter cannot establish a server socket due to illegal arguments: *exception text***

Explanation

The automation adapter cannot establish a receiver thread and cannot accept incoming connections.

System action

The automation adapter stops.

Operator response

Analyze the configuration file for invalid IP address.

EEZA0047E **The adapter is unable to accept connections due to socket exception " *exception* "**

Explanation

An exception occurred as the automation adapter was about to accept an incoming connection.

System action

The automation adapter stops.

Operator response

Analyze the exception text.

EEZA0051W **Termination of the adapter failed due to exception: *error message***

Explanation

The attempt to stop the receiver thread failed because an exception occurred.

System action

None.

Operator response

Analyze the exception text.

EEZA0052E **Cannot create an in-storage EIF configuration file: *exception text***

Explanation

An instance of the Java class ByteArrayInputStream cannot be created or written.

System action

The automation adapter stops.

Operator response

This is probably an internal error. The exception text might give the reason for the problem.

EEZA0053E **Missing argument for command line parameter " *the parameter* "**

Explanation

A required argument for a command line parameter (such as -start) is missing. For example, "AdapterCmd -start" would be wrong, because "-start" requires an argument. A correct example would be: "AdapterCmd -start com.ibm.ing.saplugin.INGXPluginInvocation".

System action

Processing of this command ends.

Operator response

Check the documentation for information about valid command line arguments and their parameters.

EEZA0055E **Remote Contact inactivity threshold exceeded: elapsed**

seconds=*elapsed seconds* threshold=*threshold*

Explanation

The automation adapter calculates the elapsed time since the last synchronous request was received. The automation adapter stops itself if this time exceeds the number specfied in the parameter eez-remote-contact-activity-interval-seconds. Any incoming event is used as a trigger for the calculation.

System action

The automation adapter stops.

Operator response

You might want to increase the number of seconds specified by parameter eez-remote-contact-activity-interval-seconds. Setting this parameter to 0 (zero) means it never expires.

EEZA0056I Initial contact was enabled and the connection to the management server has been established

Explanation

The parameter eez-initial-contact was set to true and the automation adapter attempted to connect the management server. The handshake to the management server was successful.

System action

None.

Operator response

No action required.

EEZA0057E The connection to the management server cannot be established

Explanation

The automation adapter stops attempting to connect the management server because the timeout interval is over.

System action

The automation adapter stops.

Operator response

You might want to increase the number of minutes specified by parameter eez-initial-contact-retry-interval-minutes. Specify the value 0 (zero) in order to retry forever.

EEZA0058E The plug-in has not been deployed or is not yet started: *name of the Java plug-in class*

Explanation

An attempt was made by the automation server to issue a request to the automation adapter against an unknown plug-in or a plug-in that has not been started.

System action

The automation adapter rejects the request.

Operator response

Check the plug-in configuration file on the automation adapter site for the parameter plugin-impl-class. Compare it with the plugin class name specified in the message. If there is a mismatch an installation problem might be the reason for the problem. Analyze further adapter messages e.g. EEZA0115I.

EEZA0059E An internal error occurred

Explanation

The automation adapter detected an internal error.

System action

None.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZA0060I The termination of the adapter is delayed for *duration of the delay in seconds* seconds

Explanation

Stopping the automation adapter is delayed for a short while until it has sent the appropriate domain leave events. You can configure the duration of this delay with the eez-stop-delay-seconds parameter.

System action

The automation adapter attempts to send domain leave events.

Operator response

No action required.

EEZA0061E **Unable to bind a socket to address *eez-remote-contact-hostname* at port *eez-remote-contact-port*. Reason: *message of the exception***

Explanation

The automation adapter was unable to use this address or port. Possible causes of the problem are: 1) The port is already in use by another program. 2) The address could not be assigned.

System action

The automation adapter stops.

Operator response

Make sure that no program uses this port (that is, an automation adapter that is already running). If another program needs this port, then configure the automation adapter to use another port (with the eez-remote-contact-port parameter in the master configuration file). Ensure that the address is valid.

EEZA0062I **The start command of the automation plug-in *name of the Java plug-in class* was successful**

Explanation

The selected automation plug-in was successfully started.

System action

The automation adapter has started the automation plug-in.

Operator response

No action required.

EEZA0063I **The stop command of the automation plug-in *name of the Java plug-in class* was successful**

Explanation

The selected automation plug-in was successfully stopped.

System action

The automation adapter has stopped the automation plug-in.

Operator response

No action required.

EEZA0064I **The termination command for the adapter was successful**

Explanation

The automation adapter was successfully stopped.

System action

The automation adapter stops.

Operator response

No action required.

EEZA0070E **The host name *eez-remote-contact-hostname* is unknown**

Explanation

The automation adapter was unable to resolve the host name.

System action

The automation adapter stops.

Operator response

Specify a valid host name.

EEZA0071E **The domain name is either null or empty**

Explanation

The plug-in returned an invalid domain name since its is either null or empty.

System action

The plug-in cannot be started.

Operator response

Specify a valid domain name in the plug-in configuration file.

EEZA0100I The adapter has been started

Explanation

This is the first of a sequence of three messages until the automation adapter is ready. The automation adapter starts initialization and will try to connect to the management server if eez-initial-contact=true.

System action

None.

Operator response

No action required.

EEZA0101I The adapter is active

Explanation

The automation adapter becomes "active" after a connection has been successfully established to the management server. The automation adapter continues initialization, finds and starts up all plug-ins.

System action

None.

Operator response

No action required.

EEZA0102I The adapter is ready

Explanation

The automation adapter startup sequence is complete.

System action

None.

Operator response

No action required.

EEZA0103I The adapter is stopping

Explanation

An internal or an external stop command has been received.

System action

The automation adapter is about to stop.

Operator response

No action required.

EEZA0104I The adapter has been stopped

Explanation

The automation adapter termination is complete. All possible stop delay periods are over. The process stops immediately.

System action

The automation adapter has stopped.

Operator response

No action required.

EEZA0105I The adapter has been stopped due to a failure, rc=*return code*

Explanation

The automation adapter stopped because an error occurred. All possible stop delay periods are over. The process stops immediately.

System action

The automation adapter stops.

Operator response

Search for error messages that were issued previously. On z/OS return code 28 might be caused due to the 64-bit JVM. You should use the 32-bit JVM instead. If a stop command has been issued against the adapter, while the adapter is trying to establish an inital contact to the management server, the adapter will stop with return code 12 or 13 indicating that the adapter was not able to establish an inital contact within the time period before the stop command was received. See also message EEZA0057E.

EEZA0111I The plug-in is starting: *name of the Java plug-in class*

Explanation

The automation adapter has already successfully created an instance of the plug-in class and will now call function INIT_DOMAIN.

System action

None.

Operator response

No action required.

EEZA0112I **The plug-in has been started: *name of the Java plug-in class***

Explanation

The automation adapter plug-in has successfully initialized the domain (INIT_DOMAIN).

System action

None.

Operator response

No action required.

EEZA0113I **The plug-in is stopping: *name of the Java plug-in class***

Explanation

The automation adapter will call plug-in function TERM_DOMAIN.

System action

None.

Operator response

No action required.

EEZA0114I **The plug-in has been stopped: *name of the Java plug-in class***

Explanation

The automation adapter plug-in has successfully stopped the domain (TERM_DOMAIN).

System action

None.

Operator response

No action required.

EEZA0115I **The plug-in startup failed: *name of the Java plug-in class***

Explanation

This message might follow after EEZA0111I, but the attempt to start the plug-in via function INIT_DOMAIN failed. The automation adapter plug-in will not be started automatically.

System action

The plug-in will be disabled. A join event was not sent.

Operator response

You might want to restart the plug-in using the automation adapter start command. Analyze further plug-in messages.

EEZA0116I **The status of the event sender changed: Address=*Address*, Port=*Port*, Status=*Status***

Explanation

This message occurs if the status of the EIF connection changed. The reason could be that a new EIF connection is created or an existing EIF connection is lost. The reason can be found in the status. A status='connection timed out' is expected if the management server is stopped e.g. if the management server moves to another system and therefore the adapter needs to change the EIF sender destination.

System action

None.

Operator response

No action required.

EEZA0117I **The combination of hostname and port is invalid. Please check the adapter property file.**

Explanation

This message occurs if the combination of hostname and port is invalid.

System action

The automation adapter stops.

Operator response

Supply the correct hostname and port combination in the adapter property file

EEZA0118I The connection to the management server *Target* has been established.

Explanation

The automation adapter has successfully connected to the management server. This message appears only if parameter eez-initial-contact was set to false.

System action

None.

Operator response

No action required.

EEZA9991E The message file is not installed

Explanation

The English message file must be available.

System action

The automation adapter stops.

Operator response

Make sure that the message file is in the class path.

EEZA9992E EEZAdapterLogger is not available

Explanation

The automation adapter logging component has not been initialized.

System action

The automation adapter stops. Other processes using the automation adapter client API will be unable to write messages into log and trace files.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

Prefix EEZC

This section contains messages with prefix EEZC.

EEZC0001I Setting up Tivoli Common Directory at *location where Tivoli Common Directory is being set up*.

Explanation

The Tivoli Common Directory path was set to its default value, as shown in the message text.

System action

No system action required.

Operator response

No operator action required.

EEZC0002I Unable to determine Tivoli Common Directory. Diverting serviceability related output to *alternative location*.

Explanation

The system was not able to determine the Tivoli Common Directory.

System action

Processing continues. The application will attempt to divert serviceability related output to another location for this session.

Operator response

In order to manage its serviceability related output, the application should be granted read/write permission to the location /etc/ibm/tivoli/common.

EEZC0003I Base output directory for serviceability related files (for example, message log files and trace files) has been set to *new output directory*.

Explanation

The output directory for serviceability related files was set to its default value, as shown in the message text.

System action

From now on the application will write serviceability related information to the directory that is contained in the message text.

Operator response

No action is required if the base output directory for serviceability related files is acceptable. Otherwise, if it is required to relocate the base output directory, modify the entry in log.properties which should be located at /etc/ibm/tivoli/common/cfg/log.properties. Changes to this file will take effect once the corresponding component is restarted.

EEZC0004I **Changing base output directory for serviceability related files of *name of logger* from *old output directory* to *new output directory*.**

Explanation

Due to changes in configuration settings the output directory of serviceability related files has been relocated.

System action

From now on the system will write serviceability related information to the new location.

Operator response

No action is required if the base output directory for serviceability related files is acceptable. Otherwise, if it is required to relocate the base output directory, modify the entry in log.properties which should be located at /etc/ibm/tivoli/common/cfg/log.properties. Changes to this file will take effect once the corresponding component is restarted.

EEZC0006E **Remote replication operation failed for file " *fileName* ". A connection from local node " *localNode* " to remote node " *remoteNode* " could not be established.**

Explanation

An error occurred when attempting to replicate, create or delete a file on a remote node. Establishing a connection between the local node and the remote target node on which the replication, creation or deletion actually was supposed to be performed failed. The remote file operation could not be completed successfully.

System action

The failing remote file operation is skipped and processing continues.

Operator response

Make sure that the local as well as the remote node are known host names and that IP connectivity between those two systems is correctly set up. Check whether network problems were reported at the time where the failure occured.

EEZC0007E **Remote replication operation failed for file " *fileName* ". Authentication failed when establishing a connection from local node " *localNode* " to remote node " *remoteNode* " for user ID " *userID* ".**

Explanation

An error occurred when attempting to replicate, create or delete a file on a remote node. Establishing a connection between the local node and the remote target node on which the replication, creation or deletion actually was supposed to be performed failed due to incorrect user credentials. The remote file operation could not be completed successfully.

System action

The failing remote file operation is skipped and processing continues.

Operator response

Make sure that the user ID and password used to perform the remote file operation are correctly defined on the target node.

EEZC0008E **Replication of file " *fileName* " failed. The connection from local node " *localNode* " to remote node " *remoteNode* " was lost. The original exception was: " *excMessage* ".**

Explanation

An error occurred when attempting to replicate a file on a remote node. The connection between the local node and the remote target node on which the replication actually was supposed to be performed was lost during the replication operation. The replication of the file could not be completed successfully.

System action

The failing file replication is skipped and processing continues.

Operator response

Make sure that IP connectivity between those two systems is correctly set up. The failure may also occur due to timeouts. The original exception message may give some hints about the root cause of the problem.

EEZC0009E **Remote deletion of file "** ***fileName*** **" failed. The connection from local node "** ***localNode*** **" to remote node "** ***remoteNode*** **" was lost. The original exception was: "** ***excMessage*** **".**

Explanation

An error occurred when attempting to delete a file on a remote node. The connection between the local node and the remote target node on which the deletion actually was supposed to be performed was lost during the delete operation. The remote deletion of the file could not be completed successfully.

System action

The failing remote file deletion is skipped and processing continues.

Operator response

Make sure that IP connectivity between those two systems is correctly set up. The failure may also occur due to timeouts. The original exception message may give some hints about the root cause of the problem.

EEZC0010E **Remote creation of file "** ***fileName*** **" failed. The connection from local node "** ***localNode*** **" to remote node "** ***remoteNode*** **" was lost. The original exception was: "** ***excMessage*** **".**

Explanation

An error occurred when attempting to create a file on a remote node. The connection between the local node and the remote target node on which the creation actually was supposed to be performed was lost during the create operation. The remote creation of the file could not be completed successfully.

System action

The failing remote file creation is skipped and processing continues.

Operator response

Make sure that IP connectivity between those two systems is correctly set up. The failure may also occur due to timeouts. The original exception message may give some hints about the root cause of the problem.

EEZC0011E **An unexpected I/O Exception occurred when attempting to replicate file "** ***fileName*** **" from local node "** ***localNode*** **" on remote node "** ***remoteNode*** **". The original exception was: "** ***excMessage*** **".**

Explanation

An error occurred when attempting to replicate a file on a remote node. Writing the file on the remote target node failed with an unexpected I/O exception. The replication of the file could not be completed successfully.

System action

The failing file replication is skipped and processing continues.

Operator response

Make sure that the directory on the target node where the file is to be written is correctly defined and accessible in read/write mode. The original exception message may give some hints about the root cause of the problem.

EEZC0012E **An unexpected I/O Exception occurred when attempting to delete file "** ***fileName*** **" on remote node "** ***remoteNode*** **". The original exception was: "** ***excMessage*** **".**

Explanation

An error occurred when attempting to delete a file on a remote node. Deleting the file on the remote target node failed with an unexpected I/O exception. The remote deletion of the file could not be completed successfully.

System action

The failing remote file deletion is skipped and processing continues.

Operator response

Make sure that the directory on the target node where the file is to be deleted is correctly defined and accessible in read/write mode. The original exception message may give some hints about the root cause of the problem.

EEZC0013E **An unexpected I/O Exception occurred when attempting to create file "** ***fileName*** **" on remote node "** ***remoteNode*** **". The original exception was: "** ***excMessage*** **".**

Explanation

An error occurred when attempting to create a file on a remote node. The name of the remote file indicates either the file actually to be created or a temporary file that is supposed to be created before renaming it to the actual target file. Creating the file on the remote target node failed with an unexpected I/O exception. The remote creation of the file could not be completed successfully.

System action

The failing remote file creation is skipped and processing continues.

Operator response

Make sure that the directory on the target node where the file is to be created is correctly defined and accessible in read/write mode. The original exception message may give some hints about the root cause of the problem.

EEZC0014E **Remote creation of file "** ***fileName*** **" to remote node "** ***remoteNode*** **" failed. Renaming temporary file "** ***tempFile*** **" to actual target file "** ***targetFile*** **" failed with return code "** ***rc*** **". The issued rename command was: "** ***cmd*** **". The command result was: "** ***cmdResult*** **".**

Explanation

An error occurred when attempting to create a file on a remote node. The create operation consists of two steps: first creating a temporary file on the remote node and second renaming the temporary file to the file actually to be created. The creation of the temporary file completed successfully, but renaming it to the target file failed.

System action

The failing remote file creation is skipped, the temporary file is removed and processing continues.

Operator response

Inspect the result output that was produced by the rename command and that is included in the message text to determine the reason for the failure.

EEZC0015E **The server name "** ***serverNameAndOptionalPort*** **" could not be parsed successfully.**

Explanation

An error occurred while evaluating the server name. Allowed input are host names, or IPv4 addresses, or IPv6 addresses. The host name or the IP address can be followed by a colon and a port number. If a literal IPv6 address is supplied, it has to be enclosed with brackets, for example: [::1], or [::1]:2809

System action

Evaluation of the server name ends.

Operator response

Inspect the server name for syntactical correctness. If a host name has been specified, check if the host name can be resoved by DNS (for example, try to ping the host).

Prefix EEZI

This section contains messages with prefix EEZI.

EEZI0001E **The WebSphere infrastructure has reported a severe error situation:** ***runtimeExceptionMessage*****.**

Explanation

The application was interrupted by a RuntimeException and cannot complete its task.

System action

The current task ends. The transaction is rolled back.

Operator response

Check the description of the error situation if it indicates that the server database or another subsystem is unavailable.

EEZI0003E **A critical error has occurred in class: *className*, method: *methodName*. Unable to initialize Logger.**

Explanation

No Logger object could be initialized and accessed.

System action

The process cannot be completed. All parts of this component are affected

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZI0005E **Failing Logger initialization in: *variable text*, in class: *className*. Information: *someInfo***

Explanation

Critical error. No logger object could be obtained. The entire application might be affected.

System action

Method terminates with a ConfigurationFailedException.

Operator response

Ensure the correct classpath configuration.

EEZI0012E **Internal error. Null parameter passed in method: *methodName*, in class: *className*.**

Explanation

Method getConnection() must not be called with null parameters. This is an indication of a programming error on the EJB exploiter side.

System action

Method terminates with an IllegalArgumentException.

Operator response

Invoke getConnection() with a fully initialized EEZFLAConnectionSpec object as a valid parameter.

EEZI0013E **Internal error. Illegal parameter passed in method: *methodName*, in class: *className*.**

Explanation

The EEZFLAConnectionSpec parameter contained an uninitialized EEZFLAConfigData member object.

System action

Method terminates with an IllegalArgumentException.

Operator response

Invoke getConnection() with a fully initialized EEZFLAConnectionSpec object as a valid parameter.

EEZI0014E **Illegal invocation of method: *methodName*, in class: *className*.**

Explanation

Method invoke() must not be called with this parameter combination. It is not supported.

System action

Method terminates with an IllegalOperationException.

Operator response

Invoke invoke() with the signature(InteractionSpec, Record) as a valid parameter combination.

EEZI0015E **Critical error in class: *className*, method: *methodName*. A connection to the Adapter could not be established.**

Explanation

The call to EEZAdapterConnection.open(..) returned value 0.

System action

The method terminates with a ConnectionFailedException.

Operator response

See the WebSphere and automation adapter logs if they contain further details about this error situation.

EEZI0016E **Critical error in class: *className*, method: *methodName*. Unknown AdapterException return code in *variable text*.**

Explanation

The operation has terminated with an AdapterException, but the internal return code is unknown.

System action

The method terminates with a ExecutionFailedException.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZI0017E **Critical error in class: *className*, method: *methodName*. The operation could not be performed because of *exception*.**

Explanation

An exception other than a subtype of EEZApplicationException occurred during interaction with the backend.

System action

The method terminates with a ExecutionFailedException.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZI0018E **Internal error. Illegal parameter passed in method: *methodName*, in class: *className*.**

Explanation

The EEZFLAConnectionRequestInfo parameter contained an uninitialized EEZFLAConfigData member object.

System action

Method terminates with an IllegalArgumentException.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZI0019E **Internal error. Illegal invocation of method: *methodName*, in class: *className*.**

Explanation

Method createConnection() must not be called without parameters. This is an indication of an internal JCA error.

System action

Method terminates with an IllegalOperationException.

Operator response

Invoke createConnection() with a fully initialized ConnectionManager object as a valid parameter.

EEZI0021E **Security violation detected for an automation adapter at IP address " *ipAddress* " and port number " *portNumber* ". Using SSL is required for all first-level automation adapters but not enabled for this particular adapter.**

Explanation

According to the SSL configuration of the automation framework, it is required to use SSL for the connections to all first-level automation adapters. However, this particular adapter is not configured to communicate via SSL.

System action

The current task ends.

Operator response

If all communication between the automation framework and the first-level automation adapters should use SSL, then ensure that the failing first-level automation adapter is properly configured to use SSL. If it should be allowed that the automation framework and first-level automation adapters do not use SSL, then use the configuration dialog and change the property that enforces SSL connectivity. After having saved the change in the configuration dialog, restart the WebSphere Application Server.

EEZI0022E **Security violation detected in class: *className*, method: *methodName*. The SSL configuration file could not be found.**

Explanation

The connection factory of this J2C connector requires SSL-secure connections, but the file containing the necessary properties could not be found.

System action

The method terminates with a ConfigurationException.

Operator response

Check the custom properties of the EEZFLAConnectionFactory and ensure that the SSL configuration file exists at the correct location.

EEZI0023E **Security violation detected in class: *className*, method: *methodName*. The SSL configuration file could not be opened.**

Explanation

The ConnectionFactory of this JCA requires SSL-secure connections, but the file containing the necessary properties could not be opened and read.

System action

The method terminates with a ConfigurationException.

Operator response

Ensure the properties file is not corrupt and has the appropriate read access rights.

EEZI0031E **Connector exception detected in class: *className*, method: *methodName*. The content is: *exceptionDetails*. A Connection object could not be allocated.**

Explanation

The call to getConnection() returned with an exception that is not attributable to an internal application exception.

System action

The method terminates with a ResourceException.

Operator response

See the WebSphere logs for further details about this error situation.

EEZI0032E **Connector exception detected in class: *className*, method: *methodName*. A ConnectionFactory object could not be allocated.**

Explanation

The ManagedConnectionFactory of this JCA encountered an internal error. The ConnectionManager instance was null.

System action

The method terminates with a ConfigurationException.

Operator response

Ensure the properties file is not corrupt and has the appropriate read access rights.

EEZI0041E **Internal error. Illegal parameter passed in method: *methodName*, in class: *className*.**

Explanation

The parameter passed to this object was not initialized.

System action

Method terminates with an IllegalArgumentException.

Operator response

Invoke this method with a fully initialized object as a valid parameter.

EEZI0042E **Internal error. Illegal call to method *methodName*, in class *className*.**

Explanation

This method is specified and required by the J2C specification, but must not be called this way.

System action

Method terminates with an IllegalOperationException.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZI0044E **Critical error in *methodName*, in class *className*. SSL problem. Property *property* is null.**

Explanation

The SSL properties file could not be read correctly. One or more properties do not exist or are incorrect.

System action

The J2C Connector will fail to load and not be operational.

Operator response

Make sure all settings in the SSL properties file are correct and restart the server.

EEZI0046E **Critical error in *methodName*, in class *className*. SSL problem.**

Explanation

An SSL connection could not be established. One reason might be corrupt or incorrect SSL files.

System action

The current task ends.

Operator response

Make sure all settings in the SSL properties file are correct and that all SSL files are in the correct location and not corrupted.

EEZI0047E **A 'JMSSecurityException' was caught while trying to contact the JMS queue of the end-to-end automation manager.**

Explanation

The automation engine was unable to establish contact with the end-to-end automation manager. This contact is required to forward EIF events from other automation domains.

System action

The automation engine is unable to contact the server. It has to be restarted when the problem has been resolved.

Operator response

Check the correct configuration for WAS Access User ID and Password. Restart the automation engine.

EEZI0048E **An exception was caught while trying to contact the JMS queue of the end-to-end automation manager.**

Explanation

The automation engine was unable to establish contact with the end-to-end automation manager. This contact is required to forward EIF events from other automation domains.

System action

The automation engine is unable to contact the server. It has to be restarted when the problem has been resolved.

Operator response

Check the correct configuration for WAS Access User ID and Password. Restart the automation engine.

EEZI0049E **Rejected the *requestName* request against the resource " *resourceName* " in domain " *domainName* ".**

Explanation

The resource does not support this request.

System action

The request is not processed.

Operator response

No action required.

EEZI0050E **Rejected the *requestName* request against the resource " *resourceName* " in domain " *domainName* ".**

Explanation

The resource is currently in a state that does not support this request.

System action

The request is not processed.

Operator response

Bring the resource into a state where the request is supported and issue the request again.

EEZI0051E **Rejected the *requestName* request against the resource " *resourceName* " in domain " *domainName* ".**

Explanation

The resource addressed in the request is not existing in the domain.

System action

The request is not processed.

Operator response

Check the resource key of the request.

EEZI0052E **Rejected the SetRole request with requested role " *requestedRole* " against the resource " *resourceName* " in domain " *domainName* ".**

Explanation

The resource does not support the role specified in the request.

System action

The request is not processed.

Operator response

Specify a role in the SetRole request that is supported by the resource.

EEZI0501W **An exception was encountered and ignored in order to continue operation. Exception string: *exceptionString***

Explanation

The invoked method is designed to ignore exceptions and continue operation. It logs the exception for problem determination purposes.

System action

Ignores the exception.

Operator response

Evaluate the exception details.

EEZI0545W **Possible error in *methodName*, in class *className*. SSL problem. Property *property* equals null.**

Explanation

The SSL properties file could not be read correctly. One or more properties do not exist or are incorrect.

System action

The J2C Connector will start, but will only be operational for non-SSL operations.

Operator response

Make sure all settings in the SSL properties file are correct, and restart the server if SSL operations are desired.

EEZI2001I **Request: *Request Name* was issued by User ID: *User Id* against *Resource Class* with name: *Resource Name*. Following comment was specified: *Comment text***

Explanation

System action

The replication domain will handle this request.

Operator response

No action required.

EEZI2002I **SetRole request with requested role: *Requested Role* was issued by User ID: *User Id* against *Resource Class* with name: *Resource Name*. Following comment was specified: *Comment text***

Explanation

System action

The replication domain will handle this request.

Operator response

No action required.

Prefix EEZJ

This section contains messages with prefix EEZJ.

EEZJ0001E **The WebSphere infrastructure has reported a severe error situation: *RuntimeException message***

Explanation

The application was interrupted by a RuntimeException and cannot complete its task.

System action

The current task ends. The transaction is rolled back.

Operator response

Check the description of the error situation if it indicates that the server database or another subsystem is unavailable. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/.

EEZJ0002E **The WebSphere infrastructure has reported an error situation: *Exception message***

Explanation

The application was interrupted by an unexpected exception or error that is not a RuntimeException.

System action

The current task ends, but the database operations that have been performed already remain valid (no transaction rollback).

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/.

EEZJ0003E **Operation *operationName* encountered a FinderException because automation domain *domainName* is unknown in the scope of the management server. The operation continues processing of the other automation domains.**

Explanation

Possible causes of the problem are: 1) The automation domain name was incorrect. 2) The automation domain has been deleted in the meantime.

System action

The operation task ends as far as the indicated automation domain is concerned. The operation continues processing of the other automation domains.

Operator response

Refresh the list of existing automation domains and verify that the domain name is contained in the list of existing domains. If not, and if the domain still exists and participates in automation, then restart the end-to-end automation adapter for this domain.

EEZJ0004E **Expected a nonempty list of input data but received none in class: *className*, method: *methodName*, parameter: *parameterName***

Explanation

A null or empty list parameter was encountered. This is an indication of a programming error on the EJB client side.

System action

The server method ends without processing the request.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZJ0005E **Expected nonempty input but received no input in class: *className*, method: *methodName*, parameter: *parameterName***

Explanation

A parameter with a null value was encountered. This is an indication of a programming error on the EJB client side.

System action

The server method ends without processing the request.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZJ0006E **Domain type *domainType* of automation domain *domainName* is unknown.**

Explanation

The domain type of an automation domain is unknown.

System action

The server method ends without processing the request.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZJ0007E **Within the list of resource requests, a request was encountered that contains a null or empty automation domain name.**

Explanation

One of the requests within the parameter list contains a null or empty automation domain name.

System action

All requests in the list are ignored.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZJ0008E **The automation framework is unable to publish an event to JMS topic *topicName*. The topic connection factory is *topicConnectionFactoryName*. The following exception was encountered: *exceptionDetails***

Explanation

An invocation of the WebSphere Application Server's JMS service failed.

System action

The automation framework failed to publish a message to the topic. This may result in a loss of event data.

Operator response

Evaluate the exception details and retry the operation. Restart the WebSphere application server.

EEZJ0009E **Within the list of resource requests for automation domain *firstDomainName*, a request was encountered for automation domain *differentDomainName***

Explanation

Request lists must contain requests against a single automation domain only. The request list that causes the problem contains requests against multiple automation domains.

System action

All requests in the list are ignored.

Operator response

Select only resources that are contained by a single automation domain, and retry the operation.

EEZJ0010E **The EEZDomainNameList parameter received in class: *className*, method: *methodName* contains an element that is not a string.**

Explanation

An incorrect parameter value was detected. This is an indication of a programming error on the EJB client side.

System action

The method ends but the session continues to exist.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZJ0011E **The subscription method *methodName* in class *className* was called before the subscriber id was set in the session.**

Explanation

Before a subscribe or unsubscribe method can be called, the subscriber id must be set within the session. This is an indication of a programming error on the EJB client side.

System action

The method ends but the session continues to exist.

Operator response

Restart the application that failed and retry the operation.

EEZJ0013E **Subscriber *subscriberId* was unable to unsubscribe from some resources in domain *domainName* because the automation domain is not accessible at this time.**

Explanation

The automation domain is currently not accessible, so the unsubscribe request could not be forwarded to the domain. However, the subscription cleanup within the management server was successful. Appropriate cleanup mechanisms in the domain (at domain adapter startup, for example) will take care of the orphaned subscription at the domain level.

System action

The unsubscribe operation continues to unsubscribe from resources that reside within other automation domains.

Operator response

Determine why the automation domain is not accessible at this time. If necessary, restart the end-to-end automation adapter for that domain in order to trigger resynchronization. If the domain has left, no further action is required.

EEZJ0014E **Subscriber *subscriberId* was unable to unsubscribe from all resources in automation domain *domainName* because the domain is not accessible at this time.**

Explanation

The automation domain is currently not accessible, so the unsubscribe request could not be forwarded to the domain. However, the subscription cleanup within the management server was successful. Appropriate cleanup mechanisms in the domain (at domain adapter startup, for example) will take care of the orphaned subscription at the domain level.

System action

The unsubscribe operation continues to unsubscribe from all resources that the subscriber has subscribed to previously and that reside within domains other than the failing one.

Operator response

Determine why the automation domain is not accessible at this time. If necessary, restart the end-to-end automation adapter for that domain in order to trigger resynchronization. If the domain has left, no further action is required.

EEZJ0015E **An attempt to invoke operation *methodName* within automation domain *domainName* has been detected. The type of this domain does not support the requested operation.**

Explanation

A caller tried to invoke an operation that is not supported.

System action

The operation request is ignored.

Operator response

Restart the application that failed and retry the operation.

EEZJ0016E Unable to create an initial context.

Explanation

The JNDI naming directory is not accessible, and the attempt to create an initial context failed.

System action

The current task ends.

Operator response

Restart the application that logged this message. If this does not solve the problem, restart the WebSphere Application Server that provides the runtime environment for the automation manager.

EEZJ0017E Looking up object *jndiLookupName* in JNDI failed.

Explanation

Possible causes of the problem are: 1) The JNDI naming directory is not accessible. 2) The object was not bound to the JNDI correctly.

System action

The current task ends.

Operator response

Restart the WebSphere Application Server that provides the runtime environment for the automation manager.

EEZJ0018E Automation domain *domainName* does not exist.

Explanation

Possible causes of the problem are: 1) An invalid automation domain name was supplied. 2) The automation domain has been deleted in the meantime.

System action

The current task ends.

Operator response

Check if the automation adapter that corresponds to the automation domain is running. Restart the automation adapter and verify that the automation domain is listed in the operations console or the command shell.

EEZJ0019E Automation domain *domainName* is not accessible at this time.

Explanation

The automation domain exists, but it is currently not possible to communicate with it.

System action

The current task ends.

Operator response

Make sure that the automation domain is running. If it is a first-level automation domain, verify that the automation adapter is running. Retry the operation after the timeout period defined by the environment variable *com.ibm.eez.aab.watchdog-interval-seconds*.

EEZJ0020E Automation domain *domainName* seems to be not accessible at this time. Invocation of method *methodName* failed with a RemoteException.

Explanation

The automation domain exists, but it is currently not possible to communicate with it.

System action

The current task ends.

Operator response

Make sure that the automation domain is running. If it is a first-level automation domain, verify that the automation adapter is running. Retry the operation after the timeout period defined by the environment variable com.ibm.eez.aab.watchdog-interval-seconds. If the problem persists, restart the automation adapter (in case of a first-level automation domain) or the end-to-end automation engine (in case of an end-to-end automation domain).

EEZJ0021E Automation domain *domainName* cannot be accessed because of a problem within the JEE framework.

Explanation

An attempt to create a session failed within the JEE framework.

System action

The current task ends.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZJ0022E **An unrecoverable error occurred during startup of application *productName*. The application stops. Details about the error: *exceptionDetails*.**

Explanation

An exception was encountered.

System action

The current task ends.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZJ0023E **An attempt to activate policy *policyName* in automation domain *domainName* resulted in an error which indicates that the policy is invalid.**

Explanation

The automation domain indicates that an error was detected while processing the specified automation policy.

System action

The current task ends.

Operator response

Verify the correctness of the automation policy, and activate it again.

EEZJ0024E **An attempt to activate policy *policyName* in automation domain *domainName* resulted in an error which indicates that the policy cannot be found.**

Explanation

The automation domain indicates that the specified automation policy cannot be found in the file system.

System action

The current task ends.

Operator response

Verify that the automation policy file exists and contains a valid policy, and activate it again.

EEZJ0025E **The operation setPreferredMember has ended since the automation domain name specified by the choice group key: *choiceGroupDomainName* did not match the domain name specified by the preferred member key: *preferredMemberDomainName***

Explanation

The resource keys that were provided do not point to the same automation domain. It is necessary, however, that the choice group and its members reside within the same domain.

System action

The current task ends.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZJ0026E **Operation *operation name* is not supported by class *class name*.**

Explanation

A caller tried to invoke an operation that is not supported.

System action

The current task ends.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZJ0029E **An attempt to publish an event was stopped since there is an active transaction. Event automation domain name is *domainName* and event reason is *eventReason*.**

Explanation

The application does not support sending of JMS messages within a transactional boundary.

System action

The current task ends.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZJ0030E **The automation framework is not fully initialized and refuses to accept requests. The following subcomponents are not yet initialized: *listOfMissingComponents***

Explanation

The EEZEAR application is either starting or stopping. During these periods, no method requests are accepted.

System action

The current task ends.

Operator response

If the EEZEAR application is starting, retry the request. If the EEZEAR application is stopping, restart the application and retry the request. If the problem persists, review the System Automation documentation for specific information about the subcomponents that are included in this message.

EEZJ0031E **Refused to invoke operation *methodName* on end-to-end automation domain *domainName* because the user id *userIdName* is not in the EEZEndToEndAccess role.**

Explanation

The target of this operation is an end-to-end automation domain. This operation may be invoked against end-to-end automation domains only by operators that are in the EEZEndToEndAccess role.

System action

The operation request is ignored.

Operator response

If the operator is not allowed to invoke operations against end-to-end resources, no action is required. If the operator should be allowed to invoke operations against end-to-end resources, the operator's userid or a user group that contains the operator's userid has to be added to role EEZEndToEndAccess.

EEZJ0032E **Within the list of resource keys for automation domain *firstDomainName*, a resource key was encountered for automation domain *differentDomainName***

Explanation

In the context of this operation, each element of the list of resource keys must point to the same automation domain. This condition is not satisfied.

System action

The current task ends.

Operator response

Select only resources that are contained by a single automation domain, and retry the operation.

EEZJ0033E **Automation domain *domainName* requires user authentication.**

Explanation

The automation domain requires that authentication information be supplied for each task. The authentication information consists of a userid and a password. The failing task did not supply that information.

System action

The current task ends.

Operator response

Case 1: If user authentication checking is enabled in the automation domain, ensure that user credential information for the automation domain is supplied. If the failing task was invoked from the System Automation operations console, use the "Log In" task to enter the credential. If the failing task was invoked from the end-to-end automation engine, ensure that the user credentials in the configuration of the automation engine are correct. If you modified the credentials refresh the automation engine using the Refresh function of the configuration utility. Case 2: If user authentication checking has been disabled in the automation domain, restart the adapter for that automation domain.

EEZJ0034E **You are not authorized to perform the operation.**

Explanation

The authorization failed while accessing the automation framework.

System action

The requested operation is cancelled.

Operator response

Ensure that the permissions and user roles defined in the WebSphere Application Server are set up correctly. If the problem persists, contact your system administrator.

EEZJ0035E **You are not authorized to perform the operation. *error details*.**

Explanation

The authorization failed while accessing the automation framework.

System action

The requested operation is cancelled.

Operator response

Ensure that the permissions and user roles defined in the WebSphere Application Server are set up correctly. If the problem persists, contact your system administrator.

EEZJ0036E **A WebSphere user transaction with an unexpected status was encountered while operation *operationName* was processed. The expected status is *expectedStatus* but the actual status is *actualStatus*.**

Explanation

In the process of using a WebSphere user transaction, an unexpected transaction state was encountered.

System action

The current task ends.

Operator response

Retry the operation. If the problem persists, restart the WebSphere Application Server.

EEZJ0037E **No end-to-end automation domain is accessible at this time.**

Explanation

Either no end-to-end automation domain exists at all, or it exists but it is currently not accessible.

System action

The current task ends.

Operator response

Make sure that an end-to-end automation automation domain is running. If the problem persists, restart the end-to-end automation engine.

EEZJ0038E **An event has been successfully published to the subscribers *successfulSubscriberIdList*. However, event publishing failed for at least one subscriber: *failureDetailsPerSubscriberId***

Explanation

Publishing an event has failed for at least one event subscriber.

System action

The current task ends.

Operator response

Evaluate the message, which contains failure details for each subscriber the event could not be published to. Check if just before this message, other messages appear that may provide additional information on how to solve the problem.

EEZJ0039E **Sending events to OMNIbus is currently disabled since an earlier attempt to deliver an event has**

failed. The automation framework regularly tries to send an event and enables sending events again as soon as the retry operation succeeds.

Explanation

Publishing an event to OMNIbus has failed before. In order to avoid that failing attempts to send events block the event sender for a long time period, sending automation events to OMNIbus is currently disabled. The automation framework periodically tries to send an event to OMNIbus in order to check if it is available again.

System action

The current task ends.

Operator response

Check if OMNIbus is available. Use the configuration tool to check if the event server hostname and port are set to the correct values.

EEZJ0040E **Sending events to GDPS® is currently disabled since an earlier attempt to deliver an event to GDPS failed. The automation framework regularly tries to send an event and enables sending events to GDPS again as soon as the retry operation succeeds.**

Explanation

Publishing an event to GDPS has failed before. In order to avoid that failing attempts to send events to GDPS block the event sender for a long time period, sending automation events to GDPS is currently disabled. The automation framework periodically tries to send an event to GDPS in order to check if it is available again.

System action

The current task ends.

Operator response

Check if GDPS is available. Use the configuration tool to check if the GDPS server hostname and port are set to the correct values.

EEZJ0041E **The requests which should be stored in the automation database are based on different resource keys. The first resource key is "** ***firstResourceKey*** **". The other resource key is "** ***otherResourceKey*** **".**

Explanation

The administrative interface allows storing requests that are based on one single resource key only. In order to store requests related to multiple resource keys, the administrative interface has to be invoked multiple times.

System action

The current task ends. The requests have not been stored in the automation database.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZJ0042E **The requests which should be stored in the automation database cannot be serialized into a string with maximum length** ***maxLength*****. Even after all comment strings have been removed, there are still** ***numberOfExtraCharacters*** **characters beyond the maximum length.**

Explanation

The database column that is designed to store a serialized form of the requests accepts serialized strings up to the size defined by the maximum length value. But even after all superfluous information has been removed from the requests, the serialized string is too long.

System action

The current task ends. The requests have not been stored in the automation database.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZJ0043E **The request property name "** ***propertyName*** **" is not supported.**

Explanation

The automation JEE framework accepts a specific list of request property names only.

System action

The current task ends. The request has not been stored in the automation database.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZJ0044E **The request property " *propertyName* " does not support the value " *propertyValue* "**

Explanation

For some request property names there is a specified set of supported values.

System action

The current task ends. The request has not been stored in the automation database.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZJ0045E **The request property list contains duplicate property names: *propertyNameList***

Explanation

Duplicate property names within request property lists are not supported.

System action

The current task ends. The requests have not been stored in the automation database.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZJ0046E **The request properties which should be stored in the automation database cannot be serialized into a string with maximum length *maxLength*. There are *numberOfExtraCharacters* characters beyond the maximum length.**

Explanation

The database column that is designed to store a serialized form of the request properties accepts serialized strings up to the size defined by the maximum length value.

System action

The current task ends. The requests have not been stored in the automation database.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZJ0047E **The request list contains a request of type "vote".**

Explanation

Only regular requests are applicable for being stored in the automation database. Votes are indirect consequences of regular requests. They are automatically restored when the corresponding regular request is restored.

System action

The current task ends. The requests have not been stored in the automation database.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZJ0048E **The automation JEE framework encountered the unknown WebSphere Application Server property " *propertyName* ".**

Explanation

This property is not supported by the automation JEE framework.

System action

The current task ends.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZJ0049E The list of requests passed to class *className* and method *methodName* contains mismatching requests: *requestListWithError*

Explanation

A request list that contains restart requests and other requests was encountered. This is an indication of a programming error on the client side.

System action

The automation manager ignores the request list.

Operator response

Collect the traces of the automation JEE framework.

EEZJ0050E One or multiple restart requests are issued to resources that cannot be restarted at this time: *listOfResourceNamesWithAssociatedErrorReasons*

Explanation

The restart requests are invalid.

System action

The automation manager ignores the invalid requests and processes the valid requests.

Operator response

Resolve the problems indicated in the message text. Retry the operation.

EEZJ0051E A restart request by " *userName* " failed for resource " *resourceId* ". The following exception was encountered while trying to stop the resource: *errorReason*

Explanation

The restart was interrupted because the automation domain returned an exception during the stop request.

System action

Terminates the restart cycle of the resource.

Operator response

Review the exception details. Resolve the problem and issue the restart request again.

EEZJ0052E A restart request by " *userName* " failed for resource " *resourceId* " after *durationSeconds* seconds. The following exception was encountered while trying to start the resource: *errorReason*

Explanation

The restart was interrupted because the automation domain returned an exception during the start request.

System action

Terminates the restart cycle of the resource.

Operator response

Review the exception details. Resolve the problem and issue the restart request again.

EEZJ0053E A restart request by " *userName* " failed for resource " *resourceId* " after *durationSeconds* seconds. The state of the restart cycle is " *previousState* ". The reason code is: " *errorReason* ".

Explanation

The restart cycle was interrupted by an event.

System action

Terminates the restart cycle of the resource.

Operator response

Check the status of the affected resource. If needed issue a new request.

EEZJ0054E A restart request to resource " *resourceId* " already exists.

Explanation

A resource that is currently restarting cannot be restarted.

System action

Rejects the restart request.

Operator response

Wait until the previous restart request finishes. If needed, cancel the previous request and issue a new restart request.

EEZJ0055E **The automation framework cannot contact the database manager. Details about the exception: *ExceptionDetails***

Explanation

A connection to the database manager could not get established or an existing connection got disconnected.

System action

The current task ends. The transaction is rolled back.

Operator response

Ensure that the database manager is running. Verify the configuration of the data source that is used by the automation framework. If the problem persists, restart the automation framework.

EEZJ0056E **The operation " *operationName* " is not supported as a synchronous request.**

Explanation

Only the operations "Online", "Offline", "Restart", "CancelRequest", "Suspend", "Resume", and "SetRole" are supported as synchronous requests.

System action

The current task ends.

Operator response

Do not specify the operation as a synchronous request.

EEZJ0057E **The timeout value " *timeoutValue* " is too small. The timeout value must be at least equal to " *pollIntervalValue* ".**

Explanation

The timeout value must be at least equal to the polling interval length. The polling interval length is defined by the JVM property "com.ibm.eez.aab.monitor-interval-seconds". Default: 5, minimum: 2, maximum: 60 seconds.

System action

The current task ends.

Operator response

Adjust the timeout value for the request. If needed, set or modify the property com.ibm.eez.aab.monitor-interval-seconds.

EEZJ0058E **Unable to retrieve the current status of resource " *resourceId* ". Monitoring of request " *requestName* " ends.**

Explanation

The request has been issued successfully but now the resource cannot be found any more. Therefore it is no longer possible to monitor its state.

System action

The current task ends.

Operator response

Check if the resource has been removed in the meantime.

EEZJ0059E **The request " *requestName* " for resource " *resourceId* " did not finish within the specified timeout of " *timeout* " seconds.**

Explanation

The request has been issued successfully. The resource did not reach the expected state within the specified timeout interval.

System action

The synchronous monitoring of the resource ends. The resource might reach the expected state later.

Operator response

Increase the timeout value for future requests against this resource.

EEZJ0060E **The request " *requestName* " for resource " *resourceId* " has been forwarded to the automation domain but the response is empty.**

Explanation

The request has been issued without an exception but the automation domain did not return the updated request data.

System action

The synchronous monitoring of the resource ends. The resource might reach the expected state later.

Operator response

Check the status of the resource. If needed, issue the request again.

EEZJ0061E **An authentication exception occurred while looking up the JNDI name *jndiName*: *exceptionDetails***

Explanation

The client program uses invalid user credentials to access the Java Naming and Directory Interface (JNDI).

System action

The current task ends.

Operator response

Ensure that the JNDI client uses valid credentials. For example if the JNDI client is the end-to-end automation engine or the end-to-end automation manager configuration tool then verify that the System Automation Application Manager functional user credentials are valid.

EEZJ0062E **The resource " *resourceName* " cannot be stored because it is not a node resource. Its resource type is " *resourceType* ".**

Explanation

Only node resources can be stored by the operation.

System action

The current task ends. The resource does not get stored.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZJ0063E **The automation framework has not yet received an event from automation domain " *domainName* ". The automation framework does not allow access to that domain because the event path from the automation domain to the automation framework is not yet established. The end-to-end automation management host of the automation domain is " *managementHostName* ".**

Explanation

After the automation framework has been restarted it is required to receive an event from each automation domain. This ensures that the automation adapter has acknowledged the connection to this management server. The automation adapter might not be configured correctly to send events to this management server. In a DR setup, the adapter might be sending events to the management server instance on the other site, or it might have a version that does not support a site switch of the management server. If the value of the end-to-end automation management host is "undefined" this is a strong indication that the automation adapter version does not yet support a site switch.

System action

Access to the automation domain is rejected until an event is received from the respective automation adapter, except for viewing the domain log file. If the automation framework does not receive an event within the domain removal timeout (as defined by com.ibm.eez.aab.domain-removal-hours), the automation domain will be removed from the scope of this management server.

Operator response

Check if the automation adapter has been configured for the correct management server IP address and port. Check the adapter log. If you have a DR setup with an System Automation Application Manager at each site, ensure that the System Automation Application Manager at the other site is offline. Refer to the System Automation Application Manager documentation for the minimum required automation adapter version. Upgrade the automation adapter and configure it for System Automation Application Manager toggle.

EEZJ0064E **The policy directory name " *directoryName* " contains a path separator character.**

Explanation

The policy directory name must be a relative directory name. The system appends this directory name to the "snippets" subdirectory within the end-to-end automation policy pool directory. The system does not support further nesting of subdirectories.

System action

The current task ends.

Operator response

Specify a relative directory name without any path separator characters.

EEZJ0065E **The policy file name " *fileName* " contains a path separator character.**

Explanation

The policy file name must be a relative file name.

System action

The current task ends.

Operator response

Specify a policy file name without any path separator characters.

EEZJ0066E **The policy file name " *fileName* " does not end with ".xml".**

Explanation

The policy file name must end with ".xml".

System action

The current task ends.

Operator response

Specify a valid XML policy file name suffix.

EEZJ0067E **Event publishing failed for at least one subscriber: *failureDetailsPerSubscriberId***

Explanation

Publishing an event has failed for at least one event subscriber.

System action

The current task ends.

Operator response

Evaluate the message, which contains failure details for each subscriber the event could not be published to. Check if just before this message, other messages appear that may provide additional information on how to solve the problem.

EEZJ0068E **User " *wasUserName* " could not be authenticated in first-level automation domain " *automationDomainName* " using the first-level automation domain user " *automationUserName* ".**

Explanation

The automation domain requires user authentication, but no valid user credential has been supplied with the request.

System action

The current task ends.

Operator response

Case 1: If user authentication checking is enabled in the automation domain, ensure that user credential information for the automation domain is supplied. If the failing task was invoked from the System Automation operations console, the operations console asks for a new valid user credential. Enter the new credential directly and store it to the Domain Credential store, or navigate to "Settings - Stored Domain Credentials" and edit the credentials as needed. If the failing task was invoked from the end-to-end automation manager (either automation engine or automation framework within WebSphere Application Server), ensure that a user credential for the first-level automation domain is correctly defined in the configuration utility. After you modified the credentials use the Refresh function of the configuration utility. Case 2: If user authentication checking has been disabled in the automation domain, restart the adapter for that automation domain. Case 3: If you use the configuration utility to verify user credentials, either the user ID is not known in the first-level automation domain or the password is not correct.

EEZJ0069E **Creating the EIF event publisher based on the configuration file *publisherConfigurationFile* failed with exception *exceptionDetails***

Explanation

The EIF event publisher could not be created.

System action

The current task ends.

Operator response

Review the details of the exception. Use the configuration tool to modify EIF event publisher properties.

EEZJ0070E **The EIF event publisher configuration file " *publisherConfigurationFile* " for EIF event target " *eifTargetName* " does not exist.**

Explanation

The EIF event publisher cannot be created since the required configuration file cannot be found in the file system.

System action

The current task ends.

Operator response

Verify the EIF event publisher configuration file path.

EEZJ0071E **The EIF event publisher configuration file " *publisherConfigurationFile* " for EIF event target " *eifTargetName* " cannot be read.**

Explanation

The EIF event publisher configuration file exists but the automation JEE framework cannot read the file.

System action

The current task ends.

Operator response

Verify the file access permissions of the EIF event publisher configuration file.

EEZJ0072E **Reading the EIF event publisher configuration file " *publisherConfigurationFile* " for EIF event target " *eifTargetName* " failed with exception *exceptionDetails***

Explanation

The EIF event publisher configuration file exists but the automation JEE framework cannot read the file.

System action

The current task ends.

Operator response

Review the details of the exception. Use an editor to verify that the file is readable. Use the configuration tool to modify the content of the configuration file.

EEZJ0073E **The publisher for EIF event target " *eifTargetName* " failed to send an event with reason " *eventReason* " and message *eventMessage***

Explanation

The EIF event publisher method "sendEvent" returned error code "TECAgent.SEND_FAILURE".

System action

The current task ends. In order to avoid that failing attempts to send events block the event sender for a long time period, sending automation events to the EIF event target is disabled. The automation framework periodically tries to send an event to the EIF event target in order to check if it is available again.

Operator response

Check if the EIF event target is available. Use the configuration tool to check if the event target hostname and port are set to the correct values.

EEZJ0074E **The publisher for EIF event target " *eifTargetName* " with exception *exceptionDetails***

Explanation

The EIF event publisher failed to send the event.

System action

The current task ends.

Operator response

Check if the EIF event target is available.

EEZJ0075E **The publisher for EIF event target " *eifTargetName* " failed to send an event with reason " *eventReason* "**

and message *eventMessage* within *timeoutSeconds* seconds.

Explanation

The EIF event publisher method "sendEvent" did not complete within the expected time.

System action

The current task ends. In order to avoid that failing attempts to send events block the event sender for a long time period, sending automation events to the EIF event target is disabled. The automation framework periodically tries to send an event to the EIF event target in order to check if it is available again.

Operator response

Check if the EIF event target is available. Use the configuration tool to check if the event target hostname and port are set to the correct values.

EEZJ0076E **The functional user " *userName* " can not access the automation domain " *domainName* " because of the security issue " *securityExceptionMessage* ".**

Explanation

A security problem occurred while accessing the domain with the first-level automation domain credentials that are stored for the functional user.

System action

The system blocks all attempts of the functional user to retrieve data from the first-level automation domain until the security issue is cleared.

Operator response

Open the configuration utility and verify the credentials for the functional user and this first-level automation domain. Save the changes and refresh the end-to-end automation configuration. Review the adapter configuration for the affected first-level automation domain. For example, verify that the appropriate Pluggable Authentication Module (PAM) service is defined. Restart the automation adapter after having changed the adapter configuration.

EEZJ0100E **The processing of an event resulted in an exception: *exceptionDetails***

Explanation

The EventHandlerBean received an exception when processing an event.

System action

The current task ends.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZJ0101E **Cannot create or use a connection to the first-level automation domain *domainName*. Details about the exception: *exceptionDetails*.**

Explanation

The EventHandlerBean received an exception when processing an AdapterJoin event. It was not able to create or use a connection to a first-level automation domain.

System action

The processing of the AdapterJoin event ends.

Operator response

Resolve the problem that is described in the original exception.

EEZJ0102E **Not able to add a subdomain to the domain *domainName*. Details about the exception: *exception*.**

Explanation

The EventHandlerBean tried to locate this automation domain, but it received an exception. Therefore it is not able to add a subdomain to this automation domain.

System action

The current task ends but event processing continues.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZJ0103E **Encountered a FinderException for the domain *domainName*.**

Explanation

The EventHandlerBean tried to locate this automation domain, but it received a FinderException, because the automation domain is unknown in the scope of the automation framework.

System action

The current task ends.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZJ0104E **Received an exception related to a transaction when processing an event of domain *domainName*. Details about the exception: *exception*.**

Explanation

The transaction that was started when processing an event resulted in an exception.

System action

The current task ends.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZJ0105E **Not able to communicate with automation domain *domainName*. Details about the exception: *exception*.**

Explanation

The EventHandlerBean received a domain join event of an automation domain, but it was not able to communicate with this automation domain. An exception was thrown instead.

System action

The processing of the domain join event ends.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZJ0106E **Received a CreateException trying to create a domain for the domain name *domainName*.**

Explanation

The EventHandlerBean received a CreateException while trying to create an automation domain object.

System action

The current task ends.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZJ0107E **Forwarding an event to the end-to-end automation domain *domainName* failed. Details about the exception: *exception*.**

Explanation

The EventHandlerBean tried to forward an event to the automation engine. This operation failed.

System action

The current task ends. But the event processing continues.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZJ0108E **Activating policy *policyName* failed. Details about the exception: *exception***

Explanation

The EventHandlerBean tried to activate an end-to-end automation policy on an automation engine. This operation failed.

System action

The current task ends. But the event processing continues.

Operator response

Try to activate the policy using the operations console.

EEZJ0109E **Resynchronizing the end-to-end automation domain *domainName* failed. Details about the exception: *exception*.**

Explanation

The EventHandlerBean tried to resynchronize the automation engine. This operation failed.

System action

The current task ends. But the event processing continues.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZJ0110E **FinderException received while trying to find subscriptions for entity *entityName*.**

Explanation

The EventHandlerBean tried to find subscriptions for this entity, but it received a FinderException.

System action

The current task ends.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZJ0111E **CreateException received while trying to create a connection to the end-to-end automation domain *domainName*.**

Explanation

The EventHandlerBean received a CreateException while trying to create a connection to the automation engine.

System action

The current task ends.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZJ0112E **RemoteException received when communicating with the end-to-end automation domain *domainName*.**

Explanation

The EventHandlerBean received a RemoteException when it called a function of the automation engine.

System action

The current task ends.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZJ0113E **Calling checkHealth returned a null object for domain *domainName*.**

Explanation

The EventHandlerBean received a null object when calling checkHealth for an automation domain that just sent a domain join event. The domain join processing failed for this automation domain.

System action

The current task ends.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZJ0114E **The domain object returned by checkHealth has a different domain name than the according domain join event. The event domain name is *domainName*.**

Explanation

The EventHandlerBean received an incorrect object from checkHealth. The domain join processing failed for this automation domain.

System action

The current task ends.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZJ0115E **Exception received while trying to publish an event. Details about the exception: *exception details*.**

Explanation

The EventHandlerBean received an exception when it tried to publish an event.

System action

Processing continues.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZJ0116E **Exception received while trying to create the SSL session to connect to the OSLC registry. Details about the exception: *exception details*.**

Explanation

While trying to setup a secure connection to the OSLC registry, an error occurred which prevented the successful creation of the connection.

System action

Automation engine continues to work, but OSLC registration is aborted.

Operator response

Use the exceptions details to correct the configuration for OSLC registration. Re-activate the automation policy to trigger a new OSLC registration action.

EEZJ0117E **Exception received while trying to (de-)register the resource *resourceKey*. at the OSLC registry. Details about the exception: *exception details*.**

Explanation

While trying to register or deregister a resource to the OSLC registry, an error occurred which prevented the OSLC services to correctly register the resource.

System action

Automation engine continues to work, but the resource in question will not be registered.

Operator response

Use the exceptions details to learn more about the failure. Either re-activate the automation policy to trigger a new OSLC registration action or register the resource manually.

EEZJ0118E **The request list for the automation domain " *domainName* " contains the command " *nativeCommand* " and other requests.**

Explanation

Lists of requests that contain a platform-specific command must have one element only.

System action

All requests in the list are ignored.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZJ0119E **The automation domain " *domainName* " on host " *hostName* " and port " *portNumber* " can not be contacted. At least *numberOfAttempts* connection attempts have failed.**

Explanation

Several subsequent attempts to contact the automation domain are either hanging or have timed out.

System action

The automation domain is set to the communication state "domain has left". As a consequence, the end-to-end automation manager does not try to contact the automation domain any more until its automation adapter is restarted.

Operator response

Ensure that the network and firewall setup allow establishing connections from the end-to-end automation manager host to the first-level automation host. Ensure that the first-level automation adapter gets sufficient operating system resources to perform well. Restart the end-to-end adapter for the first-level automation domain.

EEZJ0501W **An exception was encountered and ignored in order to continue operation. Details about the exception: *exceptionString***

Explanation

The invoked method is designed to ignore exceptions and continue operation. It logs the exception for problem determination purposes.

System action

Processing continues.

Operator response

Evaluate the exception details.

EEZJ0509W **One or multiple restart requests for automation domain " *domainName* " have been interrupted. The reason code is " *eventReason* ". The following resources are affected: *resourceList***

Explanation

The cause of the event leads to terminating the restart cycle.

System action

Terminates the restart cycle of the resources regardless of their individual restart status.

Operator response

Check the status of the automation domain as mentioned in the reason code. Check the status of the affected resources.

EEZJ0510W **A restart request to resource " *resourceId* " requested by operator " *userName* " has timed out after *timeoutHours* hour(s). The state of the restart cycle is " *previousState* ".**

Explanation

The restart request has timed out. The timeout value is defined by the environment variable com.ibm.eez.aab.resource-restart-timeout-hours.

System action

Terminates the restart cycle of the resource.

Operator response

Check the status of the resource. For more information on how to change the timeout value refer to the Reference and Problem Determination Guide.

EEZJ0511W **Found *numberOfMatchingNodes* automation domain nodes for hostname *hostname*. All of these nodes are mapped to the virtual server *virtualServerName*. The nodes exist within automation domains *listOfDomainNames*.**

Explanation

Hostnames should be uniquely be mapped to automation domain nodes, so the automation domain nodes can be uniquely mapped to virtual servers.

System action

The system maps multiple automation domain nodes to a single virtual server.

Operator response

Check which nodes can be addressed using the same hostname. Verify if these nodes should be mapped to the same virtual server. If the mapping is not correct then reconfigure the nodes such that their hostnames are distinct. If the mapping is correct and if you want to suppress this message from being logged again, create a WebSphere Application Server JVM custom property with name "com.ibm.eez.aab.suppress_EEZJ0511W" and value "1". Restart WebSphere Application Server to enable the property.

EEZJ0514W **An exception for automation domain *domainName* was encountered and ignored. Details about the exception: *exceptionString***

Explanation

The invoked method is designed to ignore exceptions and continue operation. It logs the exception for problem determination purposes.

System action

Processing continues.

Operator response

Evaluate the exception details.

EEZJ0515W **A user security exception for first-level automation domain *domainName* has been encountered.**

Explanation

The automation domain requires user authentication, but no valid user credential has been supplied with the request.

System action

The current task ends.

Operator response

Case 1: If user authentication checking is enabled in the automation domain, ensure that user credential information for the automation domain is supplied. If the failing task was invoked from the System Automation operations console, the operations console asks for a new valid user credential. Enter the new credential directly and store it to the Domain Credential store, or navigate to "Settings - Stored Domain Credentials" and edit the credentials as needed. If the failing task was invoked from the management server (either automation engine or automation framework within WebSphere Application Server), ensure that a user credential for the first-level automation domain is correctly defined in the configuration. After you modified the credentials use the Refresh of the configuration utility. Case 2: If user authentication checking has been disabled in the automation domain, restart the adapter for that automation domain.

EEZJ0516W **The EIF event publisher failed to disconnect from EIF event target " *eifTargetName* " with exception *exceptionDetails***

Explanation

The automation JEE framework tries to disconnect from the EIF event target while the session that owns the EIF event publisher is removed.

System action

The current task ends.

Operator response

No operator action required.

EEZJ0600W **A RemoveException was received while trying to remove an entity from the database when processing an event received from automation domain *domainName*.**

Explanation

The EventHandlerBean received a RemoveException while trying to remove an entity after processing an event.

System action

Processing continues.

Operator response

Evaluate the exception details.

EEZJ0601W **The policy name stored in the JEE framework and the policy name supplied by a policy changed event are not equal. The policy name stored in the JEE framework is *aab policyName*. The policy name supplied by the event is *event policyName*.**

Explanation

The JEE framework received a policy changed event that contains a policy name that does not match the policy name that was stored previously in the JEE framework.

System action

Processing continues.

Operator response

Verify that the policy names are set correctly. If necessary, activate the policy again.

EEZJ0602W **Not able to communicate with automation domain *domainName*.**

Explanation

The EventHandlerBean tried to communicate with an automation domain, but it received an exception.

System action

Processing continues.

Operator response

Evaluate the exception details.

EEZJ0603W **Automation domain *oldDomainName* has left and automation domain *newDomainName* has joined. These domains have the same access data. Apparently the domain has been renamed.**

Explanation

The EventHandlerBean received a domain join event. The access data of this event, such as the hostname and port, is the same as that of an existing automation domain with a different name. The EventHandlerBean created a new object for the automation domain that joined and will soon remove the object for the automation domain that left.

System action

Processing continues.

Operator response

Verify that the automation domain has not been renamed by mistake.

EEZJ0604W **There are *numberOfThreads* active threads that are managed by component *componentName* and may be hung.**

Explanation

The component has detected that several of its threads did not terminate within the expected time frame and are still active.

System action

The component continues to create new threads as needed.

Operator response

Evaluate the message log for potential reasons why the threads do not terminate within the expected time frame. If the number of potentially hanging threads continues to increase consider to restart the WebSphere application server in order to avoid the server reaching its memory limitations eventually. Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZJ0605W **Ignoring a domain leave event for domain " *domainName* " since the stored host name or IP address " *ipAddressStored* " does not match the host name or IP address " *ipAddressInEvent* " that is defined within the event.**

Explanation

The domain leave event of the automation domain contains a different host name or IP address than the stored domain data. A domain leave event is published when a first-level domain's adapter is stopped, for example, when it moves from one node to another node in the first-level automation domain.

System action

The leave event is ignored.

Operator response

Check the first-level adapter configuration and verify that the adapter can be reached by using a single host name or IP address even if the adapter is made highly available. In this case, a virtual IP address should be used. Additionally check if there exist multiple first-level automation domains that use the same end-to-end domain name.

EEZJ1604I **All of the threads that are managed by component *componentName* have terminated.**

Explanation

The component has previously detected that several of its threads did not terminate within the expected time frame. In the meantime, all of them have terminated.

System action

The component continues to create new threads as needed.

Operator response

No operator action required.

EEZJ1000I **Application *productName* has started working.**

Explanation

The application starts its asynchronous work.

System action

No system action required.

Operator response

No operator action required.

EEZJ1001I **Application *productName* was shut down by the JEE container and has stopped working.**

Explanation

The application stops its asynchronous work.

System action

No system action required.

Operator response

If required, restart the application.

EEZJ1002I **Domain *domainName* has been inactive for a long period of time and has been removed from the automation scope.**

Explanation

The timeout defined by the environment variable com.ibm.eez.aab.domain-removal-hours has been reached for this automation domain.

System action

No system action required.

Operator response

No operator action required. When the automation domain that has been removed from the automation scope joins the automation scope again, it is recreated.

EEZJ1003I **The communication state of automation domain *domainName* has changed from *previousCommState* to *newCommState*.**

Explanation

The communication health state has changed.

System action

The system publishes a related event.

Operator response

Depending on the current state values and the desired communication state of the automation domain, it might be necessary to restart the automation adapter.

EEZJ1004I **The timeout for backend automation calls is *timeoutValue* seconds.**

Explanation

Controls how many seconds each call to the backend may take at most. Default: 60, minimum: 30, maximum: 3600.

System action

No system action required.

Operator response

If needed, set or modify the environment variable com.ibm.eez.aab.invocation-timeout-seconds.

EEZJ1005I **The timeout to determine domain communication health state is *timeoutValue* seconds.**

Explanation

Controls the number of seconds of inactivity after which the health of the communication to the automation domain is checked automatically. Default: 300, minimum: 60, maximum: 86400.

System action

No system action required.

Operator response

If needed, set or modify the environment variable com.ibm.eez.aab.watchdog-interval-seconds.

EEZJ1006I **The timeout before removing domains that have left is *timeoutValue* hour(s).**

Explanation

Controls the number of hours of inactivity after which the automation domain's representation in the management server is removed automatically. Default: 48, minimum: 1, maximum: 1000.

System action

No system action required.

Operator response

If needed, set or modify the environment variable com.ibm.eez.aab.domain-removal-hours.

EEZJ1008I **The domain state of domain *domainName* has changed from *previousDomainState* to *newDomainState***

Explanation

The state of the automation domain has changed.

System action

The system publishes a related event.

Operator response

Depending on the current state values and the desired state of the automation domain, it might be necessary to restart the domain.

EEZJ1013I **The automation framework does not send events to IBM Tivoli Netcool/OMNIbus as defined in the configuration.**

Explanation

The property that contols OMNIbus event creation is set to a value that prevents event creation.

System action

The automation framework does not send events to OMNIbus.

Operator response

If events should be sent to OMNIbus, start the configuration tool and enable the OMNIbus event generation checkbox.

EEZJ1014I **The automation framework sends events to IBM Tivoli Netcool/OMNIbus as defined in the configuration.**

Explanation

The property that contols OMNIbus event creation is set to a value that enables event creation.

System action

The automation framework sends events to OMNIbus.

Operator response

If events should not be sent to OMNIbus, start the configuration tool and disable the OMNIbus event generation checkbox.

EEZJ1015I **Restart of resource " *resourceId* " starts as requested by " *userName* ".**

Explanation

The restart request is validated successfully. The stopping phase of the restart cycle begins.

System action

The automation manager sends a stop request to the resource.

Operator response

No action required.

EEZJ1016I **The resource " *resourceId* " has reached the state "observed offline" after *durationSeconds* seconds. The starting phase of the restart cycle begins as requested by " *userName* ".**

Explanation

The stopping phase of the restart cycle is completed successfully. The starting phase of the restart cycle begins.

System action

The automation manager sends a start request to the resource.

Operator response

No action required.

EEZJ1017I **Restart of resource " *resourceId* " is completed successfully after *durationSeconds* seconds as requested by " *userName* ".**

Explanation

The resource is restarted successfully.

System action

None.

Operator response

No action required.

EEZJ1018I **The timeout before interrupting resource restart requests is *timeoutValue* hour(s).**

Explanation

Controls how many hours the resource restart workflow waits for the expected sequence of events. Default: 1, minimum: 1, maximum: 3600.

System action

When the timeout occurs, then the system interrupts the resource restart workflow. The system does not send any online or offline requests to the resource based on the timeout.

Operator response

When the timeout occurs, check the status and the request list of the affected resource in order to determine why either the stopping phase or the starting phase of the resource restart did not complete. To control the timeout value, set or modify the environment variable com.ibm.eez.aab.resource-restart-timeout-hours.

EEZJ1019I **The automation framework has connected successfully to the database manager.**

Explanation

Previously reported problems to connect to the database manager are resolved.

System action

Processing continues.

Operator response

No action required.

EEZJ1020I **The status of the EIF event target " *eifTargetName* " changed: Address=*Address*, Port=*Port*, Status=*Status***

Explanation

This message occurs if the status of the EIF connection changed. The reason could be that a new EIF connection is created or an existing EIF connection is lost. The reason can be found in the status. A status='connection timed out' is expected if the EIF event target is stopped, e.g. if the EIF event target moves to another system and therefore the EIF publisher needs to change the EIF destination. The following status values are supported: 1 - connection created, 2 - connection changed, 4 - connection closed, 8 - connection timed out.

System action

None.

Operator response

No action required.

EEZJ1100I **Attributes of domain *domainName* have changed: *listOfChangedAttributes***

Explanation

The domain join event of the automation domain contains different attribute values than the domain object. The domain object will be updated with the values of the event.

System action

Processing continues with the updated domain object.

Operator response

Review the modified attributes. If you find inappropriate values reconfigure the related automation adapter and restart the automation adapter.

EEZJ1101I **The host name or IP address of domain " *domainName* " has changed from " *ipAddressOld* " to " *ipAddressNew* ".**

Explanation

The domain join event of the automation domain contains a different host name or IP address than the stored domain data. A domain join event is published when a first-level domain's adapter is started, for example, when it moves from one node to another node in the first-level automation domain.

System action

The stored domain data will be updated with the data of the event. Processing continues with the updated domain object.

Operator response

Verify that this change of the host name or IP address is expected and authorized. For example, check if there exist multiple first-level automation domains with the same domain name.

Prefix EEZK

This section contains messages with prefix EEZK.

EEZK0003E **String *someString* is too long: the maximum length of *nameOfTheString* strings is *maxLength*.**

Explanation

Setting the string to the specified value did not succeed due to string length.

System action

The current task ends.

Operator response

Verify the input parameters.

EEZK0004E **String named *someStringName* must not be null and must not exceed the maximum length of *maxLength*.**

Explanation

Setting the string to null is not allowed.

System action

The current task ends.

Operator response

Verify the input parameters.

EEZK0005E **An exception that is not an instance of EEZApplicationException has been passed to the EEZApplicationTransientException . The type of the message is *exceptionType*. The exception message is: *exceptionMessage*.**

Explanation

This is an unexpected behavior.

System action

The current task will continue. The exception will be processed.

Operator response

If any other error occurs, please provide the logs and traces as an aid to analysis.

EEZK0006E **A string has been encountered that cannot be decomposed to a valid System Automation source token. The internal reason is: *internalReason***

Explanation

System Automation supports the concept of source tokens in order to identify automation domains and automation resources. Generally, source tokens are strings used to uniquely identify objects within the scope of a particular software product. For this purpose, source tokens have to conform to product-specific syntactical rules. In this case, at least one of the syntactical rules is violated.

System action

The current task ends.

Operator response

Evaluate the internal reason.

EEZK0007E **A problem occurred handling the encryption of a user credential. The original exception was: *original exception*.**

Explanation

System Automation uses credentials (user and password pairs) to authenticate actions against other components. Passwords are encrypted or decrypted as needed. One of these functions failed.

System action

The current task ends. System Automation is unable to use this credential for accessing another component.

Operator response

Evaluate the original exception. Ensure that you have correctly set up the user encryption for this System Automation component. Ensure that user name and password have been correctly specified and files storing credentials have not been modified.

EEZK0008E **A problem occurred handling the encryption of the credential for user with name *user*. The original exception was: *original exception*.**

Explanation

System Automation uses credentials (user and password pairs) to authenticate actions against other components. Passwords are encrypted or decrypted as needed. One of these functions failed for the specified user name.

System action

The current task ends. System Automation is unable to use this credential for accessing another component.

Operator response

Evaluate the original exception. Ensure that you have correctly set up the user encryption for this System Automation component. Ensure that user name and password have been correctly specified and files storing credentials have not been modified.

EEZK0009E **The input string *inputString* is too long. The maximum length of a string of type " *typeOfString* " is *maxLength* after it has been encoded to UTF-8. The number of characters of the input string is *numberOfCharacters*. The number of characters of the encoded input string is *numberOfUTF8Characters*.**

Explanation

The UTF-8 encoded input string is larger than the maximum supported length for strings of this type. The maximum length is defined by the end-to-end automation database table that is designed to store the input string in UTF-8 encoding format.

System action

The current task ends.

Operator response

Modify the input string such that it becomes shorter and repeat the current task.

Prefix EEZL

This section contains messages with prefix EEZL.

EEZL0001E **The WebSphere infrastructure has reported a severe error situation: *runtimeExceptionMessage***

Explanation

The application was interrupted by a RuntimeException and cannot complete its task.

System action

The current task ends. The transaction is rolled back.

Operator response

Check the description of the error situation if it indicates that the server database or another subsystem is unavailable. If the problem persists, check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/.

EEZL0002E **The WebSphere infrastructure has reported an error situation: *exceptionMessage***

Explanation

The application was interrupted by an unexpected exception or error that is not a RuntimeException.

System action

The current task ends, but the database operations that have been performed already remain valid (no transaction rollback).

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/.

EEZL0003E **A critical error has occurred in class: *className*, method: *methodName*. The logger object could not be initialized.**

Explanation

This component could not initialize and access a logger object. This indicates either a configuration or programming error.

System action

The process cannot be completed. All parts of this component are affected. The system is not operational.

Operator response

Check that the path settings are correct and all required libraries exist.

EEZL0004E **An error has occurred in class: *className*, method: *methodName*, parameter *parameterName*.**

Explanation

The method has been invoked with an empty or null parameter list. The method must be invoked with a parameter list that is not null and filled. This indicates a programming error.

System action

The current task ends.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/.

EEZL0005E **An error has occurred in class: *className*, method: *methodName*, parameter *parameterName*.**

Explanation

The method has been invoked with an empty or null parameter list. The method must be invoked with a parameter list that is not null and filled. This indicates a programming error.

System action

The current task ends.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/.

EEZL0015E **An error has occurred in class: *className*.**

Explanation

Configuration data object is null.

System action

The current task ends.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/.

EEZL0016E **An error has occurred in class: *className*.**

Explanation

First-level automation name has not been set.

System action

The current task ends.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/.

EEZL0017E **An error has occurred in class: *className*.**

Explanation

Host address has not been set.

System action

The current task ends.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/.

EEZL0018E An error has occurred in class: *className*.

Explanation

Adapter plugin class has not been set.

System action

The current task ends.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/.

EEZL0019E An error has occurred in class: *className*.

Explanation

Port has not been set.

System action

The current task ends.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/.

EEZL0020E An error has occurred in class: *className*.

Explanation

Timeout value has not been set.

System action

The current task ends.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/.

EEZL0021E An error has occurred in class: *className*.

Explanation

User Credentials object is null.

System action

The current task ends.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/.

EEZL0022E An error has occurred in class: *className*.

Explanation

Username has not been set.

System action

The current task ends.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/.

EEZL0023E An error has occurred in class: *className*.

Explanation

Password has not been set.

System action

The current task ends.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/.

EEZL0024E An error has occurred in class: *className*, method: *methodName*. Illegal return object.

Explanation

The JCA has returned an illegal argument to the EJB, which has caused a ClassCastException.

System action

The current task ends.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/.

EEZL0025E **An error has occurred in class: *className*, method: *methodName*. Illegal parameter at invocation of this method.**

Explanation

The method has been invoked with a null parameter. The method must be invoked with a parameter that is not null. This indicates a programming error.

System action

The current task ends.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/.

EEZL0030E **An *exception* has occurred in class: *className*, method *methodName*. The nested exception is null.**

Explanation

No exception object was linked to the **`ResourceException`** that has been caught. This is an unexpected behavior and indicates a programming error on the J2C side.

System action

The current task ends.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/.

EEZL0031E **An error has occurred in class: *className*, method *methodName*. Invalid nested exception: *nestedException*.**

Explanation

An invalid exception object was linked to the **`ResourceException`** that has been caught. This is an unexpected behavior and indicates a programming error on the J2C side.

System action

The current task ends.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/.

EEZL0032E **An error has occurred in class: *className*, method *methodName*. No Connection object could be obtained.**

Explanation

The call to **`EEZConnectionFactory.getConnection(..)`** returned null. This is an unexpected behavior and indicates a programming error at J2C side.

System action

The current task ends.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/.

EEZL0033E **An error has occurred in class: *className*, method *methodName*. No Interaction object could be obtained.**

Explanation

The call to **`EEZConnection.createInteraction()`** returned null. This is an unexpected behavior and indicates a programming error at J2C side.

System action

The current task ends.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/.

EEZL0034E **An error has occurred in class: *className*, method *methodName*. JNDI name: *jndiName* did not return a `ConnectionFactory` object.**

Explanation

The JNDI lookup of this J2C has encountered an internal error. The **`ConnectionFactory`** object could not be retrieved. This indicates a JNDI configuration error.

System action

The current task ends. No connection to the first-level automation will be possible until this problem is fixed.

Operator response

Ensure the JNDI settings for the J2C connection factories are correct and restart the server.

EEZL0040E **Error occurred during XML (de)serialization process. Exception: *exception* detected in *className*, method *methodName*.**

Explanation

The XML decoder has received an XML string that contained unsupported encoding.

System action

The method terminates with an **`ExecutionFailedException`**.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/.

EEZL0501W **An exception was encountered and ignored in order to continue operation. Exception string: *exceptionString*.**

Explanation

The invoked method is designed to ignore exceptions and continue operation. It logs the exception for problem determination purposes.

System action

Ignores the exception.

Operator response

Evaluate the exception details.

EEZL0510W **An exception was encountered at XML serialization in class *className*, method: *methodName*. Exception string: *exceptionDetails***

Explanation

This might be subject to back-level toleration and can be ignored.

System action

The exception is ignored. The process will be continued.

Operator response

Evaluate the exception details.

Prefix EEZP

This section contains messages with prefix EEZP.

EEZP0001E **The specified <Source> " *source* " in the <Relationship> " *source* " " *relationshipType* " " *target* " does not exist as a <ResourceReference>, <ResourceGroup> or <ChoiceGroup>.**

Explanation

The <Source> and <Target> of a <Relationship> must exist as exactly one <ResourceReference>, <ResourceGroup> or <ChoiceGroup>.

System action

This policy cannot be activated.

Operator response

Verify this <Relationship> in the policy.

EEZP0002E **The specified <Target> " *target* " in the <Relationship> " *source* " " *relationshipType* " " *target* " does not exist as a <ResourceReference>, <ResourceGroup> or <ChoiceGroup>.**

Explanation

The <Source> and <Target> of a <Relationship> must exist as exactly one <ResourceReference>, <ResourceGroup> or <ChoiceGroup>.

System action

This policy cannot be activated.

Operator response

Verify this <Relationship> in this policy.

EEZP0003E **The specified <*policyElement*> name " *nameOfElement* " was found more than once as the name of a <ResourceReference>, <ResourceGroup> or <ChoiceGroup>.**

Explanation

The value of the name attributes of <ResourceReference>, <ResourceGroup> and <ChoiceGroup> must be unique.

System action

This policy cannot be activated.

Operator response

Verify this name attribute in this policy.

EEZP0004E **The specified member " *groupMember* " of the <*groupElement*> name " *groupName* " does not exist as a <ResourceReference>, <ResourceGroup> or <ChoiceGroup>.**

Explanation

The member in a group must exist as exactly one <ResourceReference>, <ResourceGroup> or <ChoiceGroup>.

System action

This policy cannot be activated.

Operator response

Verify this member name in this policy.

EEZP0005E **Syntax error in line *lineNumber* column *columnNumber*. Original parser exception: *errorMessage***

Explanation

A syntax error occurred while parsing this policy.

System action

This policy cannot be activated.

Operator response

Correct the syntax error in this policy.

EEZP0006E **The specified policy file " *policyFile* " cannot be found.**

Explanation

The policy cannot be loaded from this location.

System action

This policy cannot be activated.

Operator response

Verify the policy XML file name and its path.

EEZP0007E **Original Parser Exception: *exceptionMessage***

Explanation

An internal problem occurred while parsing this policy.

System action

This policy cannot be activated.

Operator response

Verify that the product is correctly installed.

EEZP0008E **An unsupported character *character* was found in the string " *completeString* ". This string was found in the element <*elementName*> of the parent element <*parentElement*>.**

Explanation

The character found in the string is not supported.

System action

This policy cannot be activated.

Operator response

Remove the unsupported character from this string in this policy.

EEZP0009E **The specified name " *nameOfElements* " was found in the elements <*policyElement*> and <*otherPolicyElement*>.**

Explanation

The value of the name attribute must be unique.

System action

This policy cannot be activated.

Operator response

Verify this name attribute in this policy.

EEZP0010E **The specified <ResourceReference> " *referenceName* " was found as a member of multiple <ChoiceGroup> elements.**

Explanation

A <ResourceReference> can only be a member of one <ChoiceGroup>.

System action

This policy cannot be activated.

Operator response

Check that the <ResourceReference> is a member of at most one <ChoiceGroup> element in this policy.

EEZP0011E **The specified <*groupForm*> " *groupName* " was found as a member of multiple other groups.**

Explanation

A group can only be a member of one group.

System action

This policy cannot be activated.

Operator response

Check that the group is a member of at most one group element in this policy.

EEZP0012E **The two <ResourceReference> or <ReplicationReference> elements " *reference* " and " *otherReference* " point to the same referenced resource " *resource* ".**

Explanation

A first level resource cannot be referenced by more than one <ResourceReference> or <ReplicationReference> at a time.

System action

This policy cannot be activated.

Operator response

Check that every <ResourceReference> or <ReplicationReference> references a separate <ReferencedResource> or <ReferencedReplicationResource> as child element in this policy.

EEZP0013E **The specified member " *memberName* " was found multiple times in the same <*groupForm*> " *groupName* ".**

Explanation

All <Members> child elements must be unique in one group.

System action

This policy cannot be activated.

Operator response

Check that the group has no duplicate <Members> child elements in this policy.

EEZP0014E **The specified <ResourceReference> " *reference* " was found as a member of the <ResourceGroup> " *resourceGroupName* " and the <ChoiceGroup> " *choiceGroupName* ".**

Explanation

A <ResourceReference> can only be a member of multiple <ResourceGroup> elements or one <ChoiceGroup> element.

System action

This policy cannot be activated.

Operator response

Check that the <ResourceReference> is not a member of a <ResourceGroup> and a <ChoiceGroup> at the same time in this policy.

EEZP0015E **The specified <Relationship> <Type> " *relationType* " with <Source> " *Source* " and <Target> " *Target* " was found in a loop.**

Explanation

<Relationship> elements of the same <Type> where one <Relationship> element <Target> is the next <Relationship> element <Source> must not form a loop.

System action

This policy cannot be activated.

Operator response

Check that the <Relationship> elements are not defined as a loop in this policy.

EEZP0016E **The specified element <*childElement*> was found more than once as a child element of <*parentElement*> name " *parentName* ".**

Explanation

At most one element of this type is allowed in this group.

System action

This policy cannot be activated.

Operator response

Check that at most one element of this type is specified in this group in this policy.

EEZP0017E **The specified element <*parentElement*> name " *parentName* " was found without <Members> child elements.**

Explanation

At least one <Members> child element must be specified in this group.

System action

This policy cannot be activated.

Operator response

Check that at least one <Members> child element is specified in this group in this policy.

EEZP0018E **The policy document does not contain a <ResourceReference> or <include> element.**

Explanation

At least one <ResourceReference> element or an <include> element must be specified in this policy.

System action

This policy cannot be activated.

Operator response

Check that at least one <ResourceReference> element is specified in this policy or that another policy is included using an <include> element.

EEZP0019E **The specified element <ChoiceGroup> name " *groupName* " was found with more than one <Members> child element with the "preferred" attribute equal to "true".**

Explanation

One <ChoiceGroup> member must have the "preferred" attribute equal to "true".

System action

This policy cannot be activated.

Operator response

Check that exactly one <ChoiceGroup> member has the "preferred" attribute equal to "true".

EEZP0020E **The specified <Relationship> with the <Type> " *relationType* ", the <Source> " *source* " and the <Target> " *target* " was found multiple times in the policy document.**

Explanation

All <Relationship> elements must be unique.

System action

This policy cannot be activated.

Operator response

Check that at most one <Relationship> of this type is specified in this policy.

EEZP0021E **A 'UTFDataFormatException' was caughed in method *methodName* of class *className*. The received message was *message*.**

Explanation

The processing was interrupted by this exception and cannot complete.

System action

The policy cannot be loaded.

Operator response

Ensure the correct data format of the policy document by only using editors which create UTF-8-compliant documents.

EEZP0022E **The specified <*groupType*> name " *groupName* " was found in a loop.**

Explanation

Group elements cannot form a loop with their members.

System action

This policy cannot be activated.

Operator response

Check that the group <Members> child elements are not defined as a loop in this policy.

EEZP0023E **The specified element <ChoiceGroup> name " *groupName* " has no <Members> child element with the "preferred" attribute equal to "true".**

Explanation

One <ChoiceGroup> member must have the "preferred" attribute equal to "true".

System action

This policy cannot be activated.

Operator response

Check that exactly one <ChoiceGroup> member has the "preferred" attribute equal to "true".

EEZP0024E **The specified element <ResourceReference> name " *reference* " point to the same <AutomationDomainName> value specified for the element <PolicyInformation> in this policy.**

Explanation

A <ResourceReference> child element <AutomationDomain> cannot point to the same <AutomationDomainName> value specified for the element <PolicyInformation> in this policy.

System action

This policy cannot be activated.

Operator response

Check that no <ResourceReference> child element <AutomationDomain> has the same value as the <PolicyInformation> child element <AutomationDomainName> in this policy.

EEZP0025E **There is no <Site> specified with index "1".**

Explanation

There has to be specified a <Site> with index "1", which is the initially primary site.

System action

This disaster recovery policy cannot be activated.

Operator response

Specify a <Site> with attribute "index" set to "1" in this disaster recovery policy.

EEZP0026E **There are multiple <Site> elements specified with the same index " *siteIndex* " named *listOfSiteNames*.**

Explanation

<Site> indices have to be unique.

System action

This disaster recovery policy cannot be activated.

Operator response

Change the "index" attributes of <Site> elements in this disaster recovery policy so that they are unique or remove redundant <Site> specifications.

EEZP0027E **There are multiple <Domain> elements specified with the same name " *FLADomainName* ".**

Explanation

<Domain> names have to be unique.

System action

This disaster recovery policy cannot be activated.

Operator response

Change the <Domain> names in this disaster recovery policy so that they are unique or remove the redundant <Domain> specifications.

EEZP0029E **More than one <Domain> is specified on <Site> with index " *siteIndex* " in the Cluster Set " *ClusterSetName* ". Found: *listOfFLADomainNames*.**

Explanation

At most one <Domain> is allowed per <Site> in a Cluster Set.

System action

This disaster recovery policy cannot be activated.

Operator response

Ensure that in this disaster recovery policy, at most one <Domain> located at this <Site> specifies this Cluster Set in its attribute "clusterSetName".

EEZP0030E **There are multiple <Node> elements specified with the same name " *nodeName* " in the <Domain> " *FLADomainName* ".**

Explanation

The names for <Node> elements defined in a <Domain> have to be unique.

System action

This disaster recovery policy cannot be activated.

Operator response

Ensure that there are not multiple <Node> elements specified with equal pairs of "name" attributs and <Domain> subelements in this disaster recovery policy.

EEZP0032E **The <Site> which is referenced by <Node> " *nodeName* " in <Domain> " *FLADomainName* " is not defined.**

Explanation

Cannot assign a <Node> to a <Site> which is not specified in the disaster recovery policy.

System action

This disaster recovery policy cannot be activated.

Operator response

Ensure that the "index" attribute of the <Site> subelement of the <Node> matches with the "index" attribute of the corresponding <Site> in this disaster recovery policy.

EEZP0033E **The <Domain> " *FLADomainName* " which is referenced by <Node> " *nodeName* " is not specified in the disaster recovery policy.**

Explanation

The <Domain> referenced by a <Node> has to be specified in the disaster recovery policy.

System action

This disaster recovery policy cannot be activated.

Operator response

Add a specification for the <Domain> to this disaster recovery policy.

EEZP0034E **The <Domain> " *FLADomainName* " which is referenced by the member " *memberName* " of the disaster recovery choice group " *nodeName* " is not specified in the disaster recovery policy.**

Explanation

Each <Domain> referenced by a disaster recovery choice group member has to be specified in the disaster recovery policy.

System action

This disaster recovery policy cannot be activated.

Operator response

Add a specification to the disaster recovery policy for this <Domain>.

EEZP0035E **<ResourceReference> named " *resourceReferenceName* " is specified as "businessCritical", but its <Domain> " *FLADomainName* " is not associated with a Cluster Set.**

Explanation

Each <ResourceReference> specified in the disaster recovery scope has to be associated with a Cluster Set via its supporting <Domain>.

System action

This disaster recovery policy cannot be activated.

Operator response

Ensure that the supporting <Domain> is specified in the disaster recovery policy and that its "clusterSetName" attribute is set properly or remove the "businessCritical" attribute from the <ResourceReference>.

EEZP0036E **The members of the disaster recovery choice group " *DRChoiceGroupName* " are not all associated with the same Cluster Set. Members are associated with the following Cluster Sets: *listOf(ClusterSetName)*.**

Explanation

A disaster recovery choice group can only switch between the resource references of a single Cluster Set.

System action

This disaster recovery policy cannot be activated.

Operator response

Ensure in this disaster recovery policy that the same value is set in the "clusterSetName" attribute of every <Domain> providing a member of this disaster recovery choice group.

EEZP0037E **There are multiple members in the disaster recovery choice group " *DRChoiceGroupName* " that belong to the <Site> with index " *siteIndex* ". Found members *listOf(resRefName at clusterSetName)*.**

Explanation

There is at most one <ResourceReference> allowed for each <Site> in an disaster recovery choice group.

System action

This disaster recovery policy cannot be activated.

Operator response

Remove redundant members located at this <Site> from the disaster recovery choice group in this disaster recovery policy.

EEZP0038E **The member named " *MemberName* " of disaster recovery choice group named " *choiceGroupName* " is not provided by a <Domain> that has a Cluster Set and <Site> specified.**

Explanation

Each member of a disaster recovery choice group has to be associated to a Cluster Set and to a <Site> via its <Domain>.

System action

This disaster recovery policy cannot be activated.

Operator response

Ensure in this disaster recovery policy that the <ChoiceGroup> member is provided by a <Domain> that has the "clusterSetName" attribute set and that has at least one <Node> defined at a <Site>.

EEZP0039E **The member named " *MemberName* " of disaster recovery choice group named " *choiceGroupName* " is not a <ResourceReference>.**

Explanation

Only <ResourceReference> elements are allowed as members of an disaster recovery choice group.

System action

This disaster recovery policy cannot be activated.

Operator response

Ensure in this disaster recovery policy that each member of the disaster recovery choice group is a <ResourceReference>.

EEZP0040E **The preferred member named " *MemberName* " of disaster recovery choice group named " *choiceGroupName* " is not located at <Site> with index "1".**

Explanation

The preferred member of a disaster recovery choice group has to be located at initially primary <Site>.

System action

This disaster recovery policy cannot be activated.

Operator response

Ensure in this disaster recovery policy that the preferred member of this disaster recovery choice group is located at <Site> with index "1".

EEZP0041E **The drml file " *DRMLFileName* " could not be found in the policy pool.**

Explanation

The file does not exist or access rights are not set properly.

System action

The disaster recovery policy cannot be parsed. The automation engine is not able to activate the disaster recovery policy including this drml file and will continue to run with the currently activated policy.

Operator response

Ensure that the specified drml file can be accessed in the policy pool.

EEZP0042E **A SAXException was caught while parsing the policy " *fullQualifiedPolicyPath* " from the policy pool.**

Explanation

The policy is not compliant to the corresponding XML Schema.

System action

The policy cannot be parsed. The automation engine is not able to activate this policy and will continue to run with the currently activated policy.

Operator response

Ensure that the policy is conformant with the XML Schema.

EEZP0043E **Disaster recovery specific attributes like "businessCritical" and "switchableByDROnly" were found in the policy, but the policy is not disaster recovery enabled.**

Explanation

The attributes "businessCritical" and "switchableByDROnly" are only allowed if the policy is disaster recovery enabled.

System action

This policy cannot be activated.

Operator response

Either remove the disaster recovery specific attributes from this policy or add the <DRPolicy> subelement in the <PolicyInformation> specifying the corresponding drml file.

EEZP0044E **The <Domain> named " *domainName* " is stretched across more than two sites. Found <Node> elements with site indices *listOfIndices*.**

Explanation

Spread of domains is restricted to at most two sites.

System action

This disaster recovery policy cannot be activated.

Operator response

Limit the <Node> elements of this <Domain> to at most two <Site> elements in this disaster recovery policy.

EEZP0045E **The <HardwareDevice> of <Node> " *nodeName* " in <Domain> " *domainName* " references a non-existing <Box> / <Slot> pair.**

Explanation

In order to provide <HardwareManagementTasks> for HardwareDevices, the referenced pair of <Box> and <Slot> has to be specified in the disaster recovery policy.

System action

This disaster recovery policy cannot be activated.

Operator response

Add the <Box> and <Slot> specifications with names corresponding to the names referenced in the <HardwareDevice> of the <Node> to this disaster recovery policy.

EEZP0047E **There is no corresponding <ResourceReference> specified for <Site> with index " *siteIndex* " in disaster recovery choice group " *DRChoiceGroupName* ".**

Explanation

This disaster recovery choice group cannot switch to a member at this <Site> and thus cannot be recovered at that <Site>.

System action

This disaster recovery policy cannot be activated.

Operator response

To ensure disaster recovery capability of the <ChoiceGroup> also at this <Site>, specify a proper <ResourceReference> and add it to the group in this disaster recovery policy.

EEZP0050E **The discretionary group named " *GroupName* " contains a business critical member named " *MemberName* ".**

Explanation

Business critical resource references or groups are not allowed as members of discretionary groups.

System action

This disaster recovery policy cannot be activated.

Operator response

In this disaster recovery policy, either remove the "businessCritical" attribute consistently in all of the group's members or set the group "businessCritical".

EEZP0051E **Syntax error in line *lineNumber* column *columnNumber* of policy file " *filePath* ". Original parser exception: *errorMessage***

Explanation

A syntax error occurred while parsing this policy.

System action

This policy cannot be activated.

Operator response

Correct the syntax error in this policy.

EEZP0052E **The number of specified <Site> elements in the disaster recovery policy is not two.**

Explanation

Only setups with exatcly two sites are supported.

System action

This disaster recovery policy cannot be activated.

Operator response

Make sure that there are exactly two <Site> elements in the disaster recovery policy.

EEZP0053E **The <Site> indices are not set as required. Found indices *listOf(siteIndex)*.**

Explanation

The <Site> indices have to be a sequence of increasing numbers starting with "1".

System action

This disaster recovery policy cannot be activated.

Operator response

Set the "index" attributes in the <Site> elements properly in this disaster recovery policy.

EEZP0054E **There is no corresponding <Domain> specified on <Site> with index " *siteIndex* " for the Cluster Set " *clusterSetName* ".**

Explanation

The resources of a Cluster Set cannot be recovered at a <Site> that has no corresponding <Domain> specified supporting a corresponding <ResourceReference>.

System action

This disaster recovery policy cannot be activated.

Operator response

To ensure disaster recovery capability of the Cluster Set in this disaster recovery policy, assign a <Domain> located at the missing <Site> to the Cluster Set by properly setting the "clusterSetName" attribute.

EEZP0055E **Found a " *relationshipName* " <Relationship> with a business critical <Source> named " *sourceName* " and a discretionary <Target> named " *targetName* ".**

Explanation

It is recommended that a business critical resource is not dependent on a discretionary resource.

System action

This disaster recovery policy cannot be activated.

Operator response

Remove the <Relationship> or change the "businessCritical" attribute of either the <Source> or the <Target> in this disaster recovery policy.

EEZP0056E **The business critical group named " *groupName* " has a member named " *memberName* " that is explicitly set to discretionary.**

Explanation

Discretionary members are not allowed in business critical groups.

System action

This disaster recovery policy cannot be activated.

Operator response

Remove the "businessCritical" attribute of either the group from where it was propagated or of its member in this disaster recovery policy.

EEZP0058E **The member named " *memberName* " of the disaster recovery choice group " *choiceGroupName* " participates directly in a Relationship named " *relationshipName* ".**

Explanation

The members of disaster recovery choice groups are not allowed to participate directly in relationships.

System action

This disaster recovery policy cannot be activated.

Operator response

Use the disaster recovery choice group instead of its member to model the relationship in this disaster recovery policy.

EEZP0059E **The member named " *memberName* " of the disaster recovery choice group " *choiceGroupName* " is also member of a group named " *groupName* ".**

Explanation

The members of a disaster recovery choice group are not allowed to be direct members of other groups.

System action

This disaster recovery policy cannot be activated.

Operator response

In this disaster recovery policy, put the disaster recovery choice group instead of its member in the group.

EEZP0060E **The business critical <ResourceReference> " *resourceReferenceName* " is not member of a disaster recovery choice group, but its <Domain> does not cover all sites.**

Explanation

Business critical leaf resources that do not cover all sites, i.e. that are provided by a <Domain> that is not stretched across all sites, have to be placed in disaster recovery choice groups.

System action

This disaster recovery policy cannot be activated.

Operator response

In this disaster recovery policy, put the <ResourceReference> into a proper disaster recovery choice group.

EEZP0061E **The disaster recovery choice group " *choiceGroupName* " with the attribute "switchableByDROnly" is discretionary.**

Explanation

Disaster recovery choice groups have to be business critical.

System action

This disaster recovery policy cannot be activated.

Operator response

Either put the <ChoiceGroup> into a business critical group, specify the disaster recovery choice group explicitly as "businessCritical", or remove the "switchableByDROnly" attribute in this disaster recovery policy.

EEZP0062E **A *exceptionClassName* was caught in rule *ruleClassName* of the policy checker.**

Explanation

The policy check was interrupted by this exception and failed.

System action

This policy contains errors and cannot be activated.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZP0063E **No SNMP agent for: *key of the resource***

Explanation

Mechanism SNMP is specified for a hardware management task though no SNMP agent has been defined for the enclosing box.

System action

The request to activate the policy is rejected.

Operator response

Correct and reactivate your automation policy.

EEZP0064E **Inconsistent hardware management task definition for: *key of the resource***

Explanation

Mechanism SNMP is specified for a hardware management task with a Script element.

System action

The request to activate the policy is rejected.

Operator response

Correct and reactivate your automation policy.

EEZP0065E **Inconsistent hardware management task definition for: *key of the resource***

Explanation

Mechanism Script is specified for a hardware management task though no Script element has been defined for it.

System action

The request to activate the policy is rejected.

Operator response

Correct and reactivate your automation policy.

EEZP0066E **Inconsistent hardware management task definition for: *key of the resource***

Explanation

No timeout is defined for synchroneous execution of the script command.

System action

The request to activate the policy is rejected.

Operator response

Correct and reactivate your automation policy: Either define a timeout for the script command, or specify asynchroneous execution by setting attribute runCommandSync to 0 or 2 in the drml file.

EEZP0067E **The <ResourceReference> " *ResourceReferenceName* " references a fixed resource in <Domain> " *DomainName* " whose hosting <Node> " *NodeName* " is not specified.**

Explanation

Workload on a <Domain> with an incomplete <Node> specification cannot be controlled.

System action

This disaster recovery policy cannot be activated.

Operator response

Add the missing <Node> specification to this drml file.

EEZP0068E **The value " *value* " of the attribute " *attributeName* " in the element <*ElementName*> is not allowed.**

Explanation

This value is reserved.

System action

This disaster recovery policy cannot be activated.

Operator response

Change the value.

EEZP0069E **The name " *name* " is used as domain name and as cluster set name.**

Explanation

Names for domains and cluster sets are used as identifier and must be unique.

System action

This disaster recovery policy cannot be activated.

Operator response

Change the either the domain name or the cluster set name.

EEZP0070E **The specified <*groupForm*> " *groupName* " was found as member of itself.**

Explanation

A group cannot be member of itself.

System action

This policy is not valid.

Operator response

Check that no group is member of itself in this policy.

EEZP0071E **Not able to create an object of type *Object-type*. The name of the tree-node is *node-name*.**

Explanation

There is a problem when building an internal object of the input XML.

System action

The current task ends.

Operator response

Check for related messages.

EEZP0072E **An empty string was found for a mandatory element. This empty string was found in the element <*elementName*> of the parent element <*parentElement*> with name " *name* ".**

Explanation

The empty string value is not supported for this element.

System action

This policy cannot be activated.

Operator response

Add a valid value for this element in this policy.

EEZP0073E **An unsupported character *character* was found in the string " *completeString* ". This string was found in the attribute " *attributeName* " of the element <*element*>.**

Explanation

The character found in the string is not supported.

System action

This policy cannot be activated.

Operator response

Remove the unsupported character from this string in this policy.

EEZP0074E **An empty string was found for a mandatory element. This empty string was found in the element <*elementName*> of the parent element <*parentElement*>.**

Explanation

The empty string value is not supported for this element.

System action

This policy cannot be activated.

Operator response

Add a valid value for this element in this policy.

EEZP0075E **The member " *member name* " has parent groups with different <DesiredState>.**

Explanation

Groups having the same member must have the same <DesiredState>.

System action

This policy cannot be activated.

Operator response

Ensure that all parent groups of this member have the same <DesiredState> specified in the policy.

EEZP0076E **The workloadSetup attribute of the <Domain> element with name " *domain name* " is not allowed for this domain.**

Explanation

The workloadSetup attribute must not be defined in non-stretched domains.

System action

This policy cannot be activated.

Operator response

Remove the workloadSetup attribute of the <Domain> element in the policy.

EEZP0077E **Found <ReplicationReference> elements in the disaster recovery policy.**

Explanation

<ReplicationReference> elements are not supported in disaster recovery enabled policies.

System action

This policy cannot be activated.

Operator response

Either remove the <ReplicationReference> elements from the policy or remove the <DRPolicy> subelement in the <PolicyInformation> specifying the policy as disaster recovery enabled.

EEZP0078E **Found <Resource> elements of class "IBM.ITMResource" in the policy, but integration with IBM Tivoli Monitoring is not enabled in the Universal Automation Adapter configuration.**

Explanation

<Resource> elements of class "IBM.ITMResource" are only supported if the integration with IBM Tivoli Monitoring has been configured and enabled using the configuration utility.

System action

This policy cannot be activated.

Operator response

Use the Universal Automation Adapter configuration task in the configuration utility to enable and configure the integration with IBM Tivoli Monitoring.

EEZP0079E **The element <MonitorAttribute> is specified in an invalid format. It must contain a dot separating the attribute group of an IBM Tivoli Monitoring agent and the name of the attribute within that attribute group that should be used to determine the observed state of the resource. The specified value of the <MonitorAttribute> element is "** ***MonitorAttributeValue*** **" and was found in the parent element <*parentElement*> with name "** ***name*** **".**

Explanation

In order to determine the observed state of the resource, the agent attribute specified in the policy element MonitorAttribute is queried periodically. The attribute is specified in the form <AttributeGroup>.<AttributeName> in the policy element MonitorAttribute. The attribute group and the attribute name within that group must be separated by exactly one dot.

System action

This policy cannot be activated.

Operator response

Modify the value of the MonitorAttribute element in the policy, so that a valid attribute group and attribute name are specified. Then reactivate the policy.

EEZP0080E **The "node" attribute of a resource of class "IBM.ITMResource" is specified in an invalid format. It must contain a valid managed system name as known to the IBM Tivoli Monitoring environment. A valid managed system name contains two or three name components which are separated by colons. The specified value of the "node" attribute is "** ***node value*** **" and was found in the <Resource> element named "** ***resource name*** **".**

Explanation

For resources of class "IBM.ITMResource", the node attribute must contain a valid managed system name corresponding to the Tivoli Monitoring agent that manages the resource. A valid managed system name contains two or three name components which are separated by colons. For example, a valid managed system name is "Apache:host1:KHTP".

System action

This policy cannot be activated.

Operator response

Modify the node attribute value of the Resource element in the policy, so that it contains a valid managed system name. Then reactivate the policy.

EEZP0081E **No <UserName> has been specified for the <IBM.ITMResourceAttributes> element which is named "** ***name*** **" and no generic IBM Tivoli Monitoring user has been configured in the SA Application Manager configuration utility.**

Explanation

You can configure a generic user to log in to the IBM Tivoli Monitoring SOAP server using the SA Application Manager configuration utitlity. This generic user is used if no <UserName> is specified in the <IBM.ITMResourceAttributes> element within the policy. If no generic user is configured, you must specify a <UserName> element in the policy for the

<IBM.ITMResourceAttributes> element. For this Universal Automation Adapter instance no generic user has been configured, and this policy contains <IBM.ITMResourceAttributes> elements that do not contain a <UserName> element.

System action

This policy cannot be activated.

Operator response

Add <UserName> elements to all <IBM.ITMResourceAttributes> elements in the policy, or define a generic IBM Tivoli Monitoring user using the SA Application Manager configuration utility.

EEZP0082E **The availability target of <ServerGroup> "** ***server group name*** **" is not in the valid range of 1 to "** ***member count*** **".**

Explanation

The availability target of a ServerGroup has to be greater than zero and not greater than the member count.

System action

This policy cannot be activated.

Operator response

Adjust the value of the availabilityTarget attribute of the <ServerGroup> element in this policy.

EEZP0083E **The satisfactory target of <ServerGroup> "** ***server group name*** **" is not in the valid range of 1 to "** ***member count*** **".**

Explanation

The availability target of a ServerGroup has to be greater than zero and not greater than the member count.

System action

This policy cannot be activated.

Operator response

Adjust the value of the availabilityTarget attribute of the <ServerGroup> element in this policy.

EEZP0084E **The availability target of <ServerGroup> "** ***server group name*** **" is not in the valid range. The availability target must be equal to or greater than the satisfactory target, which is "** ***satisfactory target*** **".**

Explanation

The availability target of a ServerGroup has to be equal to or greater than the satisfactory target.

System action

This policy cannot be activated.

Operator response

Adjust the values of the availabilityTarget attribute and/or the satisfactoryTarget of the <ServerGroup> element in this policy.

EEZP0085E **The <ResourceReference> "** ***resource reference name*** **" is the source of a relationship and also member of the <ServerGroup> "** ***server group name*** **". Only one of both is allowed.**

Explanation

The members of a <ServerGroup> must not be the source of relationships.

System action

This policy cannot be activated.

Operator response

Either remove all relations starting from the <ResourceReference> or remove the <ResourceReference> from the <ServerGroup>

EEZP0086E **The <ResourceReference> "** ***resource reference name*** **" is the target of a relationship and also member of the <ServerGroup> "** ***server group name*** **". Only one of both is allowed.**

Explanation

The members of a <ServerGroup> must not be the target of relationships.

System action

This policy cannot be activated.

Operator response

Either remove all relations pointing to the <ResourceReference> or remove the <ResourceReference> from the <ServerGroup>

EEZP0087E **The ServerGroup " *server group name* " has more members than the maximum allowed value (" *maximum server group members* ").**

Explanation

The amount of members of a <ServerGroup> is limited.

System action

This policy cannot be activated.

Operator response

Reduce the number of members from the <ServerGroup>

EEZP0088E **The <Relationship> " *relationshipName* " between <Source> " *sourceResourceName* " and <Target> " *targetResourceName* " links two dynamic resource references.**

Explanation

Relationships between two dynamic resource references are not supported.

System action

This policy cannot be activated.

Operator response

Change the relationship to include at most one dynamic resource reference.

EEZP0089E **The <ChoiceGroup> " *choiceGroupName* " contains the dynamic resource reference " *dynamicResourceReferenceName* " in its <Members> list.**

Explanation

Dynamic resource references are not supported as members of choice groups. A dynamic resource reference can be a member of a <ResourceGroup>.

System action

This policy cannot be activated.

Operator response

Remove the dynamic resource reference from the member list of the choice group. Add one or multiple static resources instead. The static resource can be a <ResourceGroup> which contains the dynamic resource reference.

EEZP0090E **The <ServerGroup> " *serverGroupName* " contains the dynamic resource reference " *dynamicResourceReferenceName* " in its <Members> list.**

Explanation

Dynamic resource references are not supported as members of server groups. A dynamic resource reference can be a member of a <ResourceGroup>.

System action

This policy cannot be activated.

Operator response

Remove the dynamic resource reference from the member list of the server group. Add one or multiple static resources instead. The static resource can be a <ResourceGroup> which contains the dynamic resource reference.

EEZP0500W **The specified member " *memberName* " of the <ChoiceGroup> " *choiceGroupName* " was also found as a <Source> or <Target> of a <Relationship>.**

Explanation

The member of a <ChoiceGroup> should not be the <Source> or <Target> of a <Relationship> at the same time.

System action

Application continues.

Operator response

To avoid complexity, delete the <Relationship> or delete this <ChoiceGroup> member in this policy.

EEZP0502W **The two <Relationship> elements with <Type> "StartAfter" and <Type> "StopAfter" were found with the same <Source> " *source* " and <Target> " *target* ".**

Explanation

The two <Relationship> elements with <Type> "StartAfter" and <Type> "StopAfter" should not have the same <Source> and <Target>. With this configuration the <Target> is started before the <Source> and the <Target> is stopped before the <Source>.

System action

Application continues.

Operator response

Verify this behavior. The common usage of "StartAfter" together with "StopAfter" is the following: 1. The <Source> of the "StartAfter" is the <Target> of the "StopAfter". 2. The <Target> of the "StartAfter" is the <Source> of the "StopAfter".

EEZP0503W **The <DesiredState> " *Reference State* " of the <ResourceReference> with name " *Reference Name* " does not match the <DesiredState> " *Group State* " of its parent group with name " *Group Name* ".**

Explanation

The <DesiredState> of the group member will be ignored.

System action

The <DesiredState> of this <ResourceReference> will be set to the <DesiredState> of its parent group. Application continues.

Operator response

To avoid this warning specify the same <DesiredState> for this <ResourceReference> and its parent group.

EEZP0504W **The <DesiredState> " *member group State* " of the group with name " *member group Name* " does not match the <DesiredState> " *hosting group state* " of its parent group with name " *hosting group name* ".**

Explanation

The <DesiredState> of the group member will be ignored.

System action

The <DesiredState> of this group will be set to the <DesiredState> of its parent group. Application continues.

Operator response

To avoid this warning specify the same <DesiredState> for this group and its parent group.

EEZP0505W **The <ChoiceGroup> " *choiceGroupName* " was found as member of the <ChoiceGroup> " *choiceGroupName* ".**

Explanation

The member of a <ChoiceGroup> should not be another <ChoiceGroup>.

System action

Application continues.

Operator response

To avoid complexity, delete the <ChoiceGroup> from the <ChoiceGroup> in this policy.

EEZP0506W **The resource group with name *resourceGroupName* has linked more than 100 resources.**

Explanation

The numbers of resources linked by a resource group is limited to 100.

System action

Application continues.

Operator response

Reduce the number of resources linked by this group.

EEZP0507W **Found a StartAfter relationship with source " *Source Name* " having <DesiredState> "Online" and target " *Target Name* " having <DesiredState> "Offline".**

Explanation

An online request will be propagated along this relationship. Therefore, the <DesiredState> of the target resource will be ignored.

System action

The <DesiredState> of the target resource will be set to "Online". Application continues.

Operator response

To avoid this warning, specify the <DesiredState> "Online" also for the target of this relationship.

EEZP2013I **Setting the <DesiredState> of the top-level resource " *Resource Name* " to "Online", because it is not specified in the policy.**

Explanation

Top-level resources require a default <DesiredState>.

System action

The <DesiredState> for this resource is set to "Online". Application continues.

Operator response

No action required.

Prefix EEZQ

This section contains messages with prefix EEZQ.

EEZQ0001E **Unable to create the URL for " *URL name* ". Exception details: *exceptionDetails***

Explanation

The system failed to build an URL object from the the URL name.

System action

The current task ends.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/.

EEZQ0002E **Unable to connect to the IBM Tivoli Enterprise Monitoring Server (TEMS) at " *connectionName* ". Exception details: *exceptionDetails***

Explanation

The system failed to connect to the TEMS server.

System action

The current task ends.

Operator response

Verify that the target system and the TEMS application are available.

EEZQ0003E **Unable to create an SSL socket factory. Exception details: *exceptionDetails***

Explanation

The system failed to create or to initialize a transport layer security (TLS) context.

System action

The current task ends.

Operator response

Verify that the TLS protocol is available within this Java virtual machine.

EEZQ0004E **Communicating with the IBM Tivoli Enterprise Monitoring Server (TEMS) at " *connectionName* " failed. Exception details: *exceptionDetails***

Explanation

An exception occured while sending or receiving data.

System action

The current task ends.

Operator response

Evaluate the exception details. Retry the operation.

EEZQ0005E **Unable to parse the response that was received from the IBM Tivoli Enterprise Monitoring Server (TEMS) at " *connectionName* ". Exception details: *exceptionDetails***

Explanation

An exception occured while processing the XML data that were received from TEMS.

System action

The current task ends.

Operator response

Evaluate the exception details. Retry the operation.

EEZQ0006E **Did not receive a "Result" object within the response to the remote system command " *commandName* " for target " *targetName* " that was sent to the IBM Tivoli Enterprise Monitoring Server (TEMS). The following data have been returned instead: *returnedData***

Explanation

The TEMS accepted the command but did not return a proper "Result" return code.

System action

The current task ends.

Operator response

Evaluate the command and the returned data. Retry the operation.

EEZQ0007E **A SOAP fault was received as response to request " *requestName* " for target " *targetName* " that was sent to the IBM Tivoli Enterprise Monitoring Server (TEMS). The following SOAP fault data have been returned: *returnedData***

Explanation

The TEMS returned a SOAP fault response to the request.

System action

The current task ends.

Operator response

Evaluate the command and the returned fault data. Retry the operation.

EEZQ0008E **Expected nonempty input but received no input in class: *className*, method: *methodName*, parameter: *parameterName***

Explanation

A parameter with a null or empty value was encountered. This is an indication of a programming error on the client side of the ITM facade.

System action

The method ends without processing the request.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

Prefix EEZR (Universal Automation Adapter)

This section contains messages with prefix EEZR.

EEZR0020E **Resource: *resource* does not exist.**

Explanation

A request was submitted against a resource that does not exist.

System action

The request was not processed.

Operator response

Check whether the resource exists. If it does not exist, the resource was removed. If it exists, re-submit the request.

EEZR0021E **The domain name *domain_policy* specified in the policy file does not match the domain name *domain_configured* configured in the end-to-end automation manager configuration utility.**

Explanation

The policy was not activated, because the domain names do not match.

System action

The policy was not activated.

Operator response

Make sure that the domain name in the policy file matches the configured domain name.

EEZR0036E **The request *request* is not implemented.**

Explanation

The request is currently not supported.

System action

The request was not accepted.

Operator response

Check whether a more recent version of the automation adapter is available that supports the request.

EEZR0038E **The request *request* submitted against resource " *resource* " failed. The remote command returned with return code *return_code*.**

Explanation

The remote command that is defined for the request in the policy failed with a non-zero return code.

System action

The request was not processed successfully.

Operator response

Check the preceding messages to determine why the command failed.

EEZR0039E **It is currently not allowed to submit the request *request* against resource " *resource* ". Reset the resource before you re-submit the request.**

Explanation

It is currently not allowed to submit the request against the resource.

System action

The request was not processed.

Operator response

Reset the resource before you re-submit the request.

EEZR0040E **The authentication for user ID *user* failed. The authentication error message is: *message***

Explanation

The user ID and password could not be authenticated on the system where the Universal Automation Adapter is running for a reason other than credential validation or expiration.

System action

No requests will be accepted for this user ID.

Operator response

Check the authentication error message to determine the reason for the failure.

EEZR0041E **The credential validation for user ID *user* failed. The authentication error message is: *message***

Explanation

The user ID and password validation failed on the system where the Universal Automation Adapter is running.

System action

No requests will be accepted for this user ID.

Operator response

Check the authentication error message to determine the reason for the failure. Make sure that the specified the user ID and password which is configured for the

Universal Automation Adapter domain is correct. Note that those entries are case-sensitive.

EEZR0042E **The login for user ID *user* failed, because the user account expired. The authentication error message is: *message***

Explanation

The user account is expired.

System action

No requests will be accepted for this user ID.

Operator response

Ask the system administrator to reactivate the user account.

EEZR0043E **The login for user ID *user* failed, because the password expired. The authentication error message is: *message***

Explanation

The password is expired.

System action

No requests will be accepted for this user ID.

Operator response

Ask the system administrator to reset the password.

EEZR0044E **An unexpected error occurred. The error message is: *error-message*.**

Explanation

The automation adapter detected an error that cannot be handled.

System action

The request may not have been processed.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZR0051E **The request *request* was submitted against resource *resource*. The request was ignored, because another request against this resource is already currently being processed.**

Explanation

Only one request at a time can be processed against a resource.

System action

The request was not processed.

Operator response

Wait for the request that is currently being processed to complete. Check the state of the resource to determine whether the request was successful. Otherwise check the log file.

EEZR0060E **Authentication failed when establishing a connection from local node " *localNode* " to remote node " *remoteNode* " with user ID " *userID* " using " *authenticationMode* " authentication for resource " *resource name* ".**

Explanation

The user credentials used are incorrect. The remote operation could not be completed successfully.

System action

The resource status is set to non-recoverable error. The processing is stopped until the resource is reset.

Operator response

Make sure that the user credentials used to perform the remote operation are correctly defined in the configuration utility. In the System Automation operations console reset the resource.

EEZR0061E **A connection from local node " *localNode* " to remote node " *remoteNode* " could not be established for resource " *resource name* ". The original error was: " *excMessage* "**

Explanation

A connection between the local and remote node could not be established. Possible problem reasons are: 1) The hostname specified in the policy file is incorrect. 2) The remote node is not online. 3) A firewall between the local node and the remote node blocks the connection. The command on the remote node could not be executed.

System action

For monitor commands, the attempt to establish the connection is repeated periodically.

Operator response

Make sure that the local as well as the remote node are known host names and that IP connectivity between those two systems is correctly set up. Check whether network problems were reported at the time where the failure occured.

EEZR0062E **The connection from local node "** ***localNode*** **" to remote node "** ***remoteNode*** **" was lost for resource "** ***resource name*** **". The original error was: "** ***excMessage*** **"**

Explanation

An error occurred when attempting to execute a command on a remote node. The connection between the local node and the remote target node was lost during the operation. The operation could not be completed successfully.

System action

For monitor commands, the attempt to establish the connection is repeated periodically.

Operator response

Make sure that IP connectivity between the local node and the remote node is set up correctly. The failure may also occur due to timeouts. Check the original exception message to determine the root cause of the problem.

EEZR0063E **An unexpected I/O Exception occurred when attempting to execute the command "** ***cmdName*** **" on remote node "** ***remoteNode*** **" for resource "** ***resource name*** **". The original error was: "** ***excMessage*** **"**

Explanation

An error occurred when attempting to execute a command on a remote node. Executing the command on the remote target node failed with an unexpected I/O exception. The remote execution could not be completed successfully.

System action

The resource status is set to non-recoverable error. The processing is stopped until the resource is reset.

Operator response

Make sure that the command on the target node is defined correctly and accessible in read and execute mode. Check the original exception message to determine the root cause of the problem.

EEZR0064E **An unexpected file not found exception occurred when attempting to execute the command "** ***cmdName*** **" on remote node "** ***remoteNode*** **" for resource "** ***resource name*** **". The original error was: "** ***excMessage*** **"**

Explanation

An error occurred when attempting to execute a command on a remote node. The execution of the command on the remote target node failed with an unexpected file not found exception. The remote execution could not be completed successfully.

System action

The resource status is set to non-recoverable error. The processing is stopped until the resource is reset.

Operator response

Make sure that the command on the target node is defined correctly and accessible in read and execute mode. Check the original exception message to determine the root cause of the problem.

EEZR0065E **An unexpected timeout occurred while executing the command "** ***cmdName*** **" on remote node "** ***remoteNode*** **" with the timeout** ***timeout*** **seconds for resource "** ***resource name*** **".**

Explanation

An error occurred while executing a command on a remote node. The execution of the command on the remote target node failed with an unexpected timeout. The remote execution could not be completed successfully.

System action

For monitor commands, the attempt to establish the connection is repeated periodically.

Operator response

Make sure that the command on the target node and the timeout value are defined correctly.

EEZR0066E **An unexpected permission denied exception occurred when attempting to execute the command " *cmdName* " on remote node " *remoteNode* " for resource " *resource name* ". The original error was: " *excMessage* "**

Explanation

An error occurred when attempting to execute a command on a remote node. Executing the command on the remote target node failed with an unexpected permission denied exception. The remote execution could not be completed successfully.

System action

The resource status is set to non-recoverable error. The processing is stopped until the resource is reset.

Operator response

Make sure that the command on the target node is defined correctly and accessible in read and execute mode. Check the original exception message to determine the root cause of the problem.

EEZR0071E **An error occurred while storing the policy file " *fileName* " on local node " *localNode* ". The original error was: " *errMessage* "**

Explanation

The policy file could not be stored successfully in the policy pool on the node where the Universal Automation Adapter is located.

System action

No policy file was saved.

Operator response

Check if there is enough disk space on the node where the Universal Automation Adapter is located. Check the original exception message to determine the root cause of the problem.

EEZR0072E **An error occurred while reading the policy file " *fileName* " on local node " *localNode* ". The original error was: " *errMessage* "**

Explanation

The policy file could not be read successfully from the policy pool on the node where the Universal Automation Adapter is located.

System action

No policy file was read.

Operator response

Check if the file exists on the node where the Universal Automation Adapter is located. Check the original exception message to determine the root cause of the problem.

EEZR0073E **The policy could not be activated because the policy file " *policyFile* " could not be found.**

Explanation

The policy file does not exist in the policy pool on the node where the Universal Automation Adapter is located.

System action

The policy is not activated.

Operator response

Verify that the policy file exists in the policy pool.

EEZR0074E **No automation policies are available in the policy pool directory " *directory* " for automation domain " *domain* ".**

Explanation

There are no policy files with the domain name mentioned above in the policy pool directory.

System action

No policies are found.

Operator response

Check if the policy pool contains policy files for the mentioned domain.

EEZR0075E **The policy file " *fileName* " cannot be deleted because the policy is currently active.**

Explanation

The file of the currently active policy cannot be deleted.

System action

The policy file is not deleted.

Operator response

Deactivate the current policy. Then try to delete the policy file again.

EEZR0076E **An error occurred when intialization the remote node access information. The configuration file " *ConfigurationFile* " cannot be opened or has syntax errors.**

Explanation

The adapter requires this configuration file in order to set up connections to other nodes.

System action

Initializing the remote node access information failed.

Operator response

Make sure that the adapter configuration file exists and is correctly configured.

EEZR0077E **No user credentials are configured for the resource " *resource name* ".**

Explanation

A user and password must be defined for the node on which the resource is running or the corresponding SSH private and public keys must be configured.

System action

The remote command is not executed.

Operator response

Locate the resource in the policy. Either define a user and password value for the node that is related to that resource using the configuration utility or configure the SSH private and public keys for that node and user.

EEZR0079E **Unable to activate the policy file " *policyFile* " in the policy pool directory " *policyPool* " using the user ID " *request userid* ".**

Explanation

Either the policy does not comply to the XML syntax or the policy did not pass the policy semantics checks.

System action

The policy cannot be activated. The adapter will continue operation with its currently activated policy.

Operator response

Check error messages logged for this policy before this message. Resolve the error(s) and then activate the policy again.

EEZR0080E **Unable to determine the observed state for resource " *resource name* " because the attribute name " *attribute name* " does not exist in attribute group " *attributeGroup* ". The managed system name of the corresponding IBM Tivoli Monitoring resource is: " *ITM managed system name* ".**

Explanation

In order to determine the observed state of the resource, the agent attribute specified in the policy element MonitorAttribute is queried periodically. The attribute is specified in the form <AttributeGroup>.<AttributeName> in the policy element MonitorAttribute. The AttributeGroup was queried successfully but the specified AttributeName does not exist in the attribute group.

System action

The observed state cannot be determined. The resource is set to a fatal error state. The processing is stopped until the resource is reset.

Operator response

Modify the value of the MonitorAttribute element in the policy, so that a valid attribute group and attribute name are specified. Then reactivate the policy.

EEZR0081E **Unable to determine the observed state for resource " *resource name* ". The query that was sent to the IBM Tivoli Enterprise Monitoring Server (TEMS) in order to retrieve the value for the specified agent attribute " *attribute name* " failed. The managed system name of the corresponding IBM Tivoli**

Monitoring resource is: " *ITM managed system name* ".

Explanation

In order to determine the observed state of the resource, the agent attribute specified in the policy element MonitorAttribute is queried periodically. The attribute is specified in the form <AttributeGroup>.<AttributeName> in the policy element MonitorAttribute. The corresponding SOAP request against the hub monitoring server to retrieve the value of the attribute failed. Check previous messages to determine the reason.

System action

The observed state cannot be determined. The resource is set to a fatal error state. The processing is stopped until the resource is reset.

Operator response

Check the messages to determine the reason why the SOAP request failed.

EEZR0082E **Unable to determine the observed state for resource " *resource name* ". The query that was sent to the IBM Tivoli Enterprise Monitoring Server (TEMS) in order to retrieve the value for the specified agent attribute " *attribute name* " failed. The following attribute filter has been specified: " *attribute filter* ". The managed system name of the corresponding IBM Tivoli Monitoring resource is: " *ITM managed system name* ".**

Explanation

In order to determine the observed state of the resource, the agent attribute specified in the policy element MonitorAttribute is queried periodically. The attribute is specified in the form <AttributeGroup>.<AttributeName> in the policy element MonitorAttribute. In addition there is an attribute filter specified in the policy that limits the data returned by the query. The corresponding SOAP request against the hub monitoring server to retrieve the value of the attribute failed. Check previous messages to determine the reason.

System action

The observed state cannot be determined. The resource is set to a fatal error state. The processing is stopped until the resource is reset.

Operator response

Check the messages to determine the reason why the SOAP request failed.

EEZR0083E **Unable to determine the observed state for resource " *resource name* " because the query to retrieve the specified agent attribute returned multiple results. The query that was sent to the IBM Tivoli Enterprise Monitoring Server (TEMS) in order to retrieve the contents of the specified agent attribute group " *attribute group* " succeeded. However, the result set has multiple rows and an attribute value cannot be determined unambiguously. The following attribute filter has been specified: " *attribute filter* ". The rows returned by the query are: " *query results* " The managed system name of the corresponding IBM Tivoli Monitoring resource is: " *ITM managed system name* ".**

Explanation

In order to determine the observed state of the resource, the agent attribute specified in the policy element MonitorAttribute is queried periodically. The attribute is specified in the form <AttributeGroup>.<AttributeName> in the policy element MonitorAttribute. In addition there is an attribute filter specified in the policy that limits the data returned by the query. The AttributeGroup was queried successfully but the query returned multiple rows. The query must return only one row in order to be able to map an attribute value to an observed state for the resource.

System action

The observed state cannot be determined. The resource is set to a fatal error state. The processing is stopped until the resource is reset.

Operator response

Modify the policy and use the MonitorQueryAttrFilter element to limit the data returned by the query to a maximum of one row. Then reactivate the policy.

EEZR0084E **In order to start or stop resource "** ***resource name*** **", the command "** ***remoteSystemCommand*** **" was issued against "** ***ITM managed system name*** **" but returned with error code "** ***rc*** **".**

Explanation

The policy elements StartCommand and StopCommand specify the command that should be used to start or stop the resource using an IBM Tivoli Monitoring agent. The command has been successfully submitted to the target managed system via the SOAP interface provided by the IBM Tivoli Enterprise Monitoring Server (TEMS). However, the command returned with a non zero return code. The command may have been rejected because the resource is in a state for which the specified command is not valid.

System action

The command has not been executed successfully. The resource is set to a fatal error state. The processing is stopped until the resource is reset.

Operator response

Check the log file of the IBM Tivoli Monitoring agent to determine why the command did not return successfully. Reset the resource before resending the command.

EEZR0085E **Unable to determine the observed state for resource "** ***resource name*** **" because the attribute "** ***attribute name*** **" specified in the MonitorAttribute policy element has an invalid format.**

Explanation

In order to determine the observed state of the resource, the agent attribute specified in the policy element MonitorAttribute is queried periodically. The attribute is specified in the form <AttributeGroup>.<AttributeName> in the policy element MonitorAttribute. The attribute group and the attribute name within that group must be separated by exactly one dot.

System action

The observed state cannot be determined. The resource is set to a fatal error state. The processing is stopped until the resource is reset.

Operator response

Modify the value of the MonitorAttribute element in the policy, so that a valid attribute group and attribute name are specified. Then reactivate the policy.

EEZR0086E **Unable to determine the observed state for resource "** ***resource name*** **" because the IBM Tivoli Monitoring agent is not running. The managed system name of the corresponding IBM Tivoli Monitoring resource is: "** ***ITM managed system name*** **".**

Explanation

In order to determine the observed state of the resource, the agent attribute specified in the policy element MonitorAttribute is queried periodically. The query returned no results because the corresponding IBM Tivoli Monitoring agent was offline.

System action

The observed state cannot be determined. The resource is set to an error state.

Operator response

Start the IBM Tivoli Monitoring agent corresponding to the specified managed system name.

EEZR0087E **Unable to determine the observed state for resource "** ***resource name*** **" because the specified managed system name does not exist. The managed system name of the corresponding IBM Tivoli Monitoring resource is: "** ***ITM managed system name*** **".**

Explanation

In order to determine the observed state of the resource, the agent attribute specified in the policy element MonitorAttribute is queried periodically. The corresponding SOAP request against the hub monitoring server failed because the managed system name of the IBM Tivoli Monitoring resource does not exist. The managed system name is specified in the policy in the node attribute of the Resource element.

System action

The observed state cannot be determined. The resource is set to a fatal error state. The processing is stopped until the resource is reset.

Operator response

Modify the managed system name of the resource in the policy, so that an existing managed system name is specified. Then reactivate the policy.

EEZR0504W **The location of the automation policy pool *location* was not found on node *node*.**

Explanation

When trying to show the list of available policies, the policy pool location was not found on the node where the adapter currently runs.

System action

No policies for activation are provided.

Operator response

Use the configuration utility to specify the correct 'Policy pool location', which is the directory where the automation policy files are stored for activation.

EEZR0601I **The resource *resource* has already the requested state *requested state*.**

Explanation

The request failed, because the requested resource state and the current resource state are the same.

System action

The request was not processed.

Operator response

No further action is required, because the resource is already in the requested state.

EEZR0602I **The resource " *resource* " can only be reset if the compound state is "Fatal". The compound state of the resource is currently " *compound state* " and the operational state is " *operational state* ".**

Explanation

The reset request was rejected because the resource can only be reset if the compound state is "Fatal". The compound state is "Fatal" if the operational state implies that an operator intervention is required.

System action

The reset request was not processed.

Operator response

No further action is required, because the resource is not in compound state "Fatal".

EEZR0610I **The reset request was submitted against resource " *resource* " by user ID " *userid* " to resolve a non-recoverable error.**

Explanation

A resource in a non-recoverable error state is not monitored until the resource is reset. The user submitted a reset request for the resource to make it eligible for monitoring again.

System action

The reset request was submitted against the resource and monitoring of the resource was started again.

Operator response

Verify that the resource does not show any errors in the System Automation operations console.

EEZR0611I **The request *request* was submitted against resource " *resource* " using remote user ID " *target userid* " and requesting user ID " *request userid* ". Comment: " *comment* "**

Explanation

A user submitted a request to change the resource state.

System action

The request was submitted against the resource on the target node.

Operator response

Verify that the resource changes its state in the System Automation operations console.

EEZR0612I **The policy was activated by user ID " *request userid* " using the policy file " *policyFile* " located in the policy pool directory " *policyPool* ".**

Explanation

A user activated a new policy.

System action

The requested policy is activated. The adapter starts monitoring the resources that are defined in the policy.

Operator response

Verify that the resources defined in the policy are displayed in the System Automation operations console.

EEZR0613I **The policy was deactivated by user ID " *request userid* ". The active policy file was " *policyFile* " located in the policy pool directory " *policyPool* ".**

Explanation

A user deactivated the currently active policy.

System action

The active policy is deactivated. The adapter no longer monitors the resources that are defined in the deactivated policy.

Operator response

Verify that no resources defined in the deactivated policy are displayed in the System Automation operations console.

EEZR0614I **During the adapter startup, a policy was automatically activated using the policy file " *policyFile* " located in the policy pool directory " *policyPool* ".**

Explanation

When the adapter was started, it automatically activated the policy that was previously active.

System action

The requested policy is activated. The adapter starts monitoring the resources that are defined in the policy.

Operator response

Verify that the resources defined in the policy are displayed in the System Automation operations console.

Prefix EEZU

This section contains messages with prefix EEZU.

EEZU0001E **The following RuntimeException occurred: *Exception text***

Explanation

The processing was interrupted by a RuntimeException and cannot complete correctly.

System action

The current task ends.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZU0002E **The following error occurred while writing file *filename* : *Exception text***

Explanation

The processing was interrupted by an error and cannot complete correctly.

System action

The current task ends.

Operator response

Check the error details and retry the operation.

EEZU0003E **The following error occurred while reading file *filename* : *Exception text***

Explanation

The processing was interrupted by an error and cannot complete correctly.

System action

The current task ends.

Operator response

Check the error details and retry the operation.

EEZU0004E **An error has occurred while accessing the automation framework: *Exception text***

Explanation

An error has occurred while accessing the automation framework running on the management server. The requested action could not be processed. Possible causes: 1) The management server is down. 2) The automation framework (Enterprise application EEZEAR) is not started. 3) The are some inconsistencies regarding the level of the operations console and the automation framework.

System action

The requested action is cancelled.

Operator response

Ensure that the management server is up and running. Check that the enterprise application EEZEAR is started. Verify that the levels of the operations console and the automation framework are appropriate. Refer to the 'Related errors' section for more details about the problem. If the problem persists, contact your system administrator.

EEZU0005E **The credential vault service was not found or could not be loaded: *Exception text***

Explanation

The credential vault cannot be accessed because the corresponding service was not found or could not be loaded due to an initialization error.

System action

The current task ends.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZU0006E **The page with the ID *Page UID* could not be found: *Exception text***

Explanation

The application tried to load the page with the specified ID to display the log data. However, the page with this ID could not be found.

System action

The application continues, but the log data cannot be displayed.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZU0007E **The credential vault cannot be accessed: *Exception text***

Explanation

Possible causes: 1) The credential vault is not accessible for technical reasons. 2) The credential vault is not accessible for security reasons.

System action

The current task ends.

Operator response

Evaluate the error details and check if one of the possible causes applies.

EEZU0008E **The credential secret for automation domain *Automation domain name* is not set: *Exception text***

Explanation

A user credential for a certain automation domain was requested but is not set for the user.

System action

The current task ends.

Operator response

Logout and login again.

EEZU0010E **Unable to receive events from the automation framework. The following error occurred while trying to read an event: *Exception text***

Explanation

An error has occurred while trying to access the event path to the management server. The operations console is not able to receive any events and is therefore not able to update the status information for resources if the status changes. Possible causes: 1) The management server is down. 2) The JMS service of the management server is not working properly. 3) The JMS topic used for sending events is not available

System action

Processing continues, but no events can be received.

Operator response

Ensure that the management server is up and running. Check that the JMS service of the management server is setup correctly and that the JMS topic used for sending events is available. If the problem persists, contact your system administrator.

EEZU0011E **Unable to set up the event path between the operations console and the automation framework: *Exception text***

Explanation

The connection to the right JMS service on the management server could not be established. This connection is used to receive events about status changes from connected automation domains. Possible causes: 1) The management server is down. 2) The JMS service of the management server is not working properly. 3) The JMS topic used for sending events is not available

System action

Processing ends.

Operator response

Ensure that the management server is up and running. Check that the JMS service of the management server is setup correctly and that the JMS topic used for sending events is available. If the problem persists, contact your system administrator.

EEZU0012E **An error occurred trying to look up the JMS service on the management server to establish the event path: *Exception text***

Explanation

An error has occurred while trying to access the management server. Possible causes: 1) The management server is down. 2) The JMS service of the management server is not working properly. 3) The JMS topic used for sending events is not available

System action

Processing ends.

Operator response

Ensure that the management server is up and running. Check that the JMS service of the management server is setup correctly and that the JMS topic used for sending events is available. If the problem persists, contact your system administrator.

EEZU0013E **An error has occurred while trying to establish the connection to the automation framework: *Exception text***

Explanation

An error has occurred while connecting to the automation framework running on the management server. Possible causes: 1) The management server is down. 2) The automation framework (Enterprise application EEZEAR) is not started. 3) The are inconsistencies regarding the level of the operations console and the automation framework. 4) You are not authorized to access the automation framework.

System action

Processing ends.

Operator response

Ensure that the management server is up and running. Check that the enterprise application EEZEAR is started. Ensure that you have the right permissions. Also verify that the levels of the operations console and the automation framework are appropriate. Refer to the 'Related errors' section for more details about the problem. If the problem persists, contact your system administrator.

EEZU0015E The log data cannot be displayed because the service to launch a new page was not found or could not be loaded

Explanation

The log data is normally displayed on a new page within the Dashboard Application Services Hub, but the service to launch a new page was not found or could not be loaded due to an initialization error.

System action

The application continues, but the log data cannot be displayed.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/.

EEZU0016E An error occurred trying to look up the automation framework to connect to automation domains: *Exception text*

Explanation

An error has occurred while trying to look up the automation framework's Session Beans that are part of the Enterprise application EEZEAR. Possible causes: 1) The management server is down. 2) The automation framework (Enterprise application EEZEAR) is not started or is not deployed correctly.

System action

Processing ends.

Operator response

Ensure that the management server is up and running. Check that the enterprise application EEZEAR is started. If the problem persists, contact your system administrator.

EEZU0017E There is no log data available for automation domain *Automation domain*

Explanation

No log file exists for the automation domain. The log file is normally located on the node where the automation domain's automation adapter is running, or if it is the end-to-end automation domain, where the end-to-end automation engine is running.

System action

The application continues without displaying log data.

Operator response

Ensure that logging is set up correctly for this automation domain; for example, check the eezjlog.properties file. If the problem persists, contact your system administrator.

EEZU0018E Creating EIF event receiver failed, error message is: *Exception text*

Explanation

The operations console accesses first-level automation domains directly (direct access mode). To be able to receive events from first-level automation domains an Event Integration Facility (EIF) event receiver must be created. Creating the event receiver failed.

System action

The operations console will not receive events.

Operator response

Examine the error message to find the cause of failure.

EEZU0019E The operations console was notified of new domain *new domain* that has the same name as the known domain *known domain*

Explanation

The operations console accesses first-level automation domains directly (direct access mode). It was notified about a new domain that has the same name as a domain that is already known by the operations console. However, the connection information of the of the form 'domainname@ip-address:port' suggest that the new domain automates a different cluster than the known domain. Every domain operated from an operations console must have a unique name.

System action

The domain is not allowed to join and therefore, will not show up in the topology view.

Operator response

Try to determine from the information of new domain where the domain is located. If the new domain automates a different cluster than the known domain, have the name of the new domain changed, and its automation adapter restarted to notify the operations console.

EEZU0020E **The operations console was notified of domain *domain* from adapter *adapter* with version *adapter version* that is lower than the required minimum version *minimum version***

Explanation

The operations console accesses first-level automation domains directly (direct access mode). It was notified about a domain from an adapter with a version that is too low for reliable operation.

System action

The domain is not allowed to join and therefore, will not show up in the topology view.

Operator response

Try to locate the adapter that tried to join the domain and have it upgraded to a version that is equal or higher than the required minimum version. Then have the automation adapter restarted to notify the operations console.

EEZU0021E **The operations console contacted a domain *domain* with adapter *adapter* at version *adapter version* that is lower than the required minimum version *minimum version***

Explanation

The operations console accesses first-level automation domains directly (direct access mode). It contacted a domain from an adapter with a version that is too low for reliable operation.

System action

The operations console must not communicate with the domain which has a too low version and therefore, the domain will remain disabled in the topology view.

Operator response

Try to locate the adapter of the domain and have it upgraded to a version that is equal or higher than the required minimum version. Then have the automation adapter restarted to notify the operations console.

EEZU0022E **The resource with resource name *resource* and resource class *resource class* does not exist on domain *domain***

Explanation

The operations console was launched from another component passing resource context information. The specified resource cannot be found. Reasons can be that the resource does not exist anymore, the corresponding automation adapter is not running, the host name or the event port used by the automation adapter are configured incorrectly or the domain name is mapped to a different name by the automation adapter.

System action

The current task ends. The operations console starts without navigating to the specified resource.

Operator response

Press OK to continue working with the operations console.

EEZU0023E **The domain *domain* does not exist**

Explanation

The operations console was launched from another component passing a domain name as context information. The specified domain cannot be found. Reasons can be that the corresponding automation adapter is not running, the host name or the event port used by the automation adapter are configured incorrectly or the domain name is mapped to a different name by the automation adapter.

System action

The current task ends. The operations console starts without navigating to the specified domain.

Operator response

Press OK to continue working with the operations console.

EEZU0024E **The resource with resource name *resource* and resource class *resource class* located on node *resource node* does not exist on domain *domain***

Explanation

The operations console was launched from another component passing resource context information. The specified resource cannot be found. Reasons can be that the resource does not exist anymore, the corresponding automation adapter is not running, the host name or the event port used by the automation adapter are configured incorrectly or the domain name is mapped to a different name by the automation adapter.

System action

The current task ends. The operations console starts without navigating to the specified resource.

Operator response

Press OK to continue working with the operations console.

EEZU0025E **Unable to contact the automation framework using the specified server name *Server name* and port *Port***

Explanation

Before the connection properties are stored, it is verified that the automation framework can be accessed using the specified server name and port. However, the connection to the automation framework could not be established. Possible causes: 1) You specified incorrect values for server name and port. 2) The automation framework (Enterprise application EEZEAR) is not started. 3) You are not authorized to access the automation framework

System action

The connection properties are not stored.

Operator response

Verify that your entries for server name and port are correct. This is the BOOTSTRAP_ADDRESS configured for the application server to accept Web client requests. Ensure that you have the right permissions. Also check that the enterprise application EEZEAR is started. Refer to the 'Related errors' section for more details about the problem. If the problem persists, contact your system administrator.

EEZU0026E **Unable to launch the page with the name *Page name* . Error details: *Exception text***

Explanation

An internal error occurred while trying to launch a new page in the Dashboard Application Services Hub. This might be related to an installation or setup problem.

System action

The new page is not launched.

Operator response

Verify that your environment is set up correctly, re-start the WebSphere Application Server and try again.

EEZU0027E **Error while writing preference settings to disk. Error details: *Exception text***

Explanation

Some preferences are stored in properties files on the system where the WebSphere Application Server runs. These properties files are located in a product specific directory below the current Application Server profile. An error occurred while trying to write the preferences to disk.

System action

The application continues without storing the preference values.

Operator response

Ensure that the mentioned directory exists and that you have the rights to write into this directory.

EEZU0028E **Node *node* cannot be included, because site *site* is in maintenance mode**

Explanation

Site maintenance was started for the nodes of this site by a disaster recovery manager. This involves excluding this node from automation.

System action

The node is not included.

Operator response

Wait until the site maintenance period is over.

EEZU0029E **The resource reference *resource name* referring to first-level automation domain *firstLevelDomain* does not exist on end-to-end automation domain *e2eDomain***

Explanation

The operations console was launched from another component passing resource context information. The specified resource cannot be found. Reasons can be that the resource does not exist anymore or the end-to-end automation engine is not running.

System action

The current task ends. The operations console starts without navigating to the specified resource.

Operator response

Press OK to continue working with the operations console.

EEZU0030E **You are not authorized to perform the operation *methodName*. The user ID needs to be granted one of the following user roles: *List of required roles***

Explanation

Authorization failed while trying to invoke an operation for which a specific user role is required. The user ID used to log in to the Dashboard Application Services Hub is not granted any of the required user roles.

System action

The requested operation is cancelled.

Operator response

Ensure that the permissions and user roles defined in the WebSphere Application Server are set up correctly. User IDs can be granted specific rights by adding them to one of the predefined user groups. For example add a user ID to the user group EEZAdministratorGroup to assign the user role EEZAdministrator to this user ID. User Management can be performed using the 'Users and Groups' > 'Manage Users' task.

EEZU0031E **The virtual server for node *nodename* could not be found. The requested operation will not be performed**

Explanation

The virtual server for the node could not be found. Neither a shutdown nor a startup operation can be performed against the node.

System action

The requested operation is cancelled.

Operator response

Ensure that the hardware adapter is running and the connection to zEnterprise® HMC is established.

EEZU0032E **The end-to-end automation management server on *hostname* has been stopped**

Explanation

The automation JEE framework has been stopped. Either the enterprise application EEZEAR or the WebSphere Application Server hosting it has been stopped. The operations console cannot communicate with any automation backend without the automation JEE framework.

System action

The operations console will be closed.

Operator response

Ensure that the management server is up and running. Check that the enterprise application EEZEAR is started. Then restart the operations console.

EEZU0033E **Unexpected behavior from end-to-end adapter: *Exception text***

Explanation

The end-to-end adapter answers with an unexpected response. No further processing of the adapter's response is possible.

System action

The response cannot be handled and is rejected. It is not guaranteed that the command was executed.

Operator response

Ensure that the version of the end-to-end adapter matches the requirements and if it is configured properly.

EEZU0034E **Malformed response from end-to-end adapter: *Exception text***

Explanation

The end-to-end adapter response does not match its specification and cannot be parsed. No further processing of the adapter's response is possible.

System action

The response cannot be parsed and is rejected. It is not guaranteed that the command was executed.

Operator response

Ensure that the version of the end-to-end adapter matches the requirements and that it is configured properly.

EEZU0035E **Command execution on end-to-end adapter failed with reason code *reason code*: *Exception text***

Explanation

Execution of a command on the end-to-end adapter failed.

System action

The command is not executed.

Operator response

Check the log of the end-to-end adapter and verify that it is configured properly.

EEZU0036E **Execution of command exits with non-zero return code *return code***

Explanation

The execution of a command with the end-to-end adapter returned a non-zero return code. If the command was executed in parallel on several systems, the execution on the other systems may return with another return code.

System action

The command was executed but is likely to be failed.

Operator response

Analyze the reason of the non-zero return code.

EEZU0037E **INGRCANZ version *version number* from the end-to-end adapter not supported**

Explanation

The version of the INGRCANZ command, coming with the end-to-end adapter, is not supported and its response cannot be handled.

System action

No output from INGRCANZ will be available.

Operator response

Ensure the INGRCANZ version is supported.

EEZU0038E **Unexpected behavior from INGRCANZ: *Exception text***

Explanation

The INGRCANZ command, included in the end-to-end adapter, answers with an unexpected response. No CANZLOG messages can be fetched.

System action

The response cannot be handled and is rejected.

Operator response

Ensure that the version of the end-to-end adapter including the INGRCANZ command matches the requirements and that it is configured properly.

EEZU0039E **Correlation ID of response from INGRCANZ does not match. Expected is *expected corr ID*, received was *received corr ID***

Explanation

The INGRCANZ command, included in the end-to-end adapter, answers with an unexpected correlation ID. Therefore the response does not match its request. No CANZLOG messages are fetched.

System action

The response cannot be handled and is rejected.

Operator response

Ensure that the version of the end-to-end adapter including the INGRCANZ command matches the requirements and that it is configured properly.

EEZU0040E **Collection of system log messages for system *system name* failed: *Exception text***

Explanation

The collection of system log messages failed for a specific system.

System action

The collection failed for various reasons.

Operator response

Analyze the reason of the failure.

EEZU0041E **Collection of system log messages for system *system name* not supported**

Explanation

The collection of system log messages is not supported on the specified system.

System action

No system log messages are collected.

Operator response

Retry on a supported system.

EEZU0042E **No system log messages available for the requested point in time**

Explanation

CANZLOG messages are only kept for a limited period of time. If system log messages are requested for a time in the past, they might not be available anymore.

System action

No system log messages are collected.

Operator response

Retry with a more recent time.

EEZU0044E **Invalid regular expression for filtering of system log messages: *Exception text***

Explanation

The specified regular expression for the filtering of system log messages is invalid.

System action

No system log messages are collected.

Operator response

Retry with a valid regular expression.

EEZU0045E **System or resource *resource name* does not exist**

Explanation

The system log was launched from another component passing resource context information. The specified resource cannot be found. Reasons can be that the resource does not exist anymore, the corresponding automation adapter is not running, the host name or the event port used by the automation adapter are configured incorrectly or the domain name is mapped to a different name by the automation adapter.

System action

No system log messages are collected.

Operator response

Retry with a valid system or resource name.

EEZU0046E **Cannot load system log for resource *resource name* near its last state change**

Explanation

The system log near the resource's last state change cannot be loaded because the specified resource is not a valid resource or does not exist.

System action

No system log messages are collected.

Operator response

Retry with a valid resource name.

EEZU0047E **Cannot execute command on system *system name***

Explanation

The command cannot be executed because the specified resource is not a system node or does not exist. The command execution was launched from another component passing resource context information. The specified resource cannot be found. Reasons can be that the resource does not represent a system, the resource does not exist anymore, the corresponding automation adapter is not running, the host name or the event port used by the automation adapter are configured incorrectly or the domain name is mapped to a different name by the automation adapter.

System action

The command is not executed.

Operator response

Retry with a valid system resource name.

EEZU0048E **Execution of commands on system *system name* not supported**

Explanation

The execution of commands is not supported on the specified system.

System action

The command is not executed.

Operator response

Retry on a supported system.

EEZU0049E **User *user name* not authorized to execute command *command name* on system *system name***

Explanation

End-to-end Adapter security context switch successful. But user is not authorized to execute the command.

System action

The command is not executed.

Operator response

Provide the necessary authorization for the user.

EEZU0050E **Command *command name* does not exist on system *system name***

Explanation

End-to-end Adapter security context switch successful. But the command does not exist.

System action

The command is not executed.

Operator response

None.

EEZU0051E **Operator task *task name* is not defined on *system name***

Explanation

End-to-end Adapter security context switch failed. Operator task is not defined.

System action

The command is not executed.

Operator response

Define the operator task.

EEZU0052E **Empty command**

Explanation

An empty command cannot be executed.

System action

No command is executed.

Operator response

None.

EEZU0053E **Cannot execute command on system with SMFID *system identifier* on Sysplex *sysplex name***

Explanation

The command cannot be executed because the specified resource is not a system node or does not exist. The command execution was launched from another component passing resource context information. The specified resource cannot be found. Reasons can be that the resource does not represent a system, the resource does not exist anymore, the corresponding automation adapter is not running, the host name or the event port used by the automation adapter are configured incorrectly or the domain name is mapped to a different name by the automation adapter.

System action

The command is not executed.

Operator response

Retry with a valid SMFID and Sysplex name.

EEZU0054E **Cannot execute command without context of a domain and/ or system**

Explanation

The command cannot be executed because the context of the domain and/ or system is missing, on which the command should be executed. The command execution was launched from another component without passing resource context information.

System action

The command is not executed.

Operator response

Retry and provide the necessary context by a resource ID or with a SMFID and Sysplex name.

EEZU0055E **Command execution response needs too long. Timeout exceeded**

Explanation

The End-to-end Adapter needs too long to respond for the execution of a command. The request's timeout is exceeded.

System action

It is not clear if the command was executed, partly executed or not executed at all.

Operator response

Analyze the End-to-end adapter and its log files to see why the command execution needs so long of if there is another problem.

EEZU0056E **Unknown misbehavior during execution of *command name* on system *system name***

Explanation

End-to-end Adapter security context switch successful. The command was executed but the response signals a misbehavior which cannot be exactly identified by the end-to-end adapter.

System action

It is not clear if the command was executed, partly executed or not executed at all.

Operator response

Analyze the End-to-end adapter and its log files to see why the response signals a misbehavior.

EEZU0057E **Required parameter *parameter name* is missing**

Explanation

A required parameter was not provided for a data set. Without this parameter, the data set cannot be loaded.

System action

The data set cannot be loaded.

Operator response

Verify why the data set was not provided. E.g. a DASH widget uses the data set without providing the necessary parameter.

EEZU0058E **No page header information available for page *page id***

Explanation

Page header information was requested for a specific page, but no such information is available.

System action

The data set cannot be loaded.

Operator response

Retry and provide a page ID for which page header information is available.

EEZU0059E **Invalid regular expression**

Explanation

The provided regular expression is not valid.

System action

No matching entries can be found.

Operator response

Correct the regular expression. A description of the correct syntax can be found in the Online Help.

EEZU0080E **Captured messages are not supported on *resource name***

Explanation

Captured messages are not supported on the specified resource.

System action

No captured messages can be displayed.

Operator response

Retry with a supported resource.

EEZU0081E **Unexpected response from INGCAPT: *Exception text***

Explanation

The INGCAPT command returns with an unexpected response. Desired action cannot be performed.

System action

The response cannot be handled and is rejected.

Operator response

Analyze the reason of the failure.

EEZU0082E **Invalid arguments provided for INGCAPT: *arguments***

Explanation

The arguments provided for INGCAPT are invalid. Without valid arguments, the captured messages cannot be read.

System action

The captured messages cannot be read.

Operator response

Verify why invalid arguments were provided.

EEZU0083E **INGCAPT routed to wrong (sub)system: *system name***

Explanation

The INGCAPT command returns with an unexpected response, because it was routed to the wrong (sub)system. Desired action cannot be performed.

System action

The response cannot be handled and is rejected.

Operator response

Analyze the reason of the failure.

EEZU0090E **Monitoring history not supported on *resource name***

Explanation

Monitoring history not supported on the specified resource.

System action

No monitoring history messages can be displayed.

Operator response

Retry with a supported resource.

EEZU0091E **Invalid arguments provided for INGCAPT: *arguments***

Explanation

The arguments provided for INGCAPT are invalid. Without valid arguments, the monitoring history messages cannot be read.

System action

The monitoring history messages cannot be read.

Operator response

Verify why invalid arguments were provided.

EEZU0100E **Memory shortage exception**

Explanation

It was detected that there is less than 20 percent of WebSphere heap size still available. To avoid an out of memory situation which could cause the management server not to function anymore, the current task has been interrupted.

System action

The current task ends. The displayed policy may be incomplete.

Operator response

Increase the WebSphere heap size. It is recommended that you close this policy editor session.

EEZU0101E **An unexpected error occured: *situation description***

Explanation

The processing was interrupted because an unexpected error occurred.

System action

Processing ends.

Operator response

Check IBM Electronic Support for additional information - http://www.ibm.com/support/entry/portal/

EEZU0102E Cannot overwrite the currently active policy

Explanation

You selected the policy file which is currently the domain's active policy as target to store your current policy. For an end-to-end automation domain or for a UAA domain, it is not allowed to overwrite the active policy.

System action

The policy is not stored.

Operator response

Store the current policy under a different file name.

EEZU0103E Received empty policy from JEE framework

Explanation

The received policy was empty. This may happen if the user tried to open the currently active policy from a domain which does not have any policy activated.

System action

The policy is not received.

Operator response

Verify that the policy you try to open exists.

EEZU0110E Failed to parse XML response from `INGWHY`: *Exception text*

Explanation

The response to the **`INGWHY`** command is unexpected causing an XML parsing error. No problem isolation information can be fetched.

System action

The response cannot be handled and is rejected.

Operator response

Check IBM Electronic Support for additional information: http://www.ibm.com/support/entry/portal/.

EEZU0603E The resource with resource name *resource* and resource class *resource class* contains an invalid property. Property *property* cannot be empty

Explanation

The property is required.

System action

In order to avoid creating an invalid policy, the policy XML is not changed.

Operator response

Type in some value for the property.

EEZU0604E The resource with resource name *resource* and resource class *resource class* contains an invalid property. For the property *property*, a valid integer value with a maximum allowed value of *maxValue* is expected

Explanation

The input value is above the maximum allowed value.

System action

In order to avoid creating an invalid policy, the policy XML is not changed.

Operator response

Type in a valid value which is below the maximum allowed value.

EEZU0605E The resource with resource name *resource* and resource class *resource class* contains an invalid property. For the property *property*, a valid integer value with a minimum allowed value of *minValue* is expected

Explanation

The input value is below the minimum allowed value.

System action

In order to avoid creating an invalid policy, the policy XML is not changed.

Operator response

Type in a valid value which is above the minimum allowed value.

EEZU0606E **The resource with resource name *resource* and resource class *resource class* contains an invalid property. For the property *property*, a valid integer value with a value between *minValue* and *maxValue* expected**

Explanation

The property value is outside of the allowed range.

System action

In order to avoid creating an invalid policy, the policy XML is not changed.

Operator response

Type in a value which is within the valid range.

EEZU0607E **The resource with resource name *resource* and resource class *resource class* has a non-unique resource name**

Explanation

All resources have to have a unique resource name.

System action

In order to avoid creating an invalid policy, the policy XML is not changed.

Operator response

Choose a unique resource name.

EEZU0608E **Attempt to create multiple references to the resource with resource key *resource key***

Explanation

It is not possible to create multiple resource references referencing the same referenced resource.

System action

In order to avoid creating an invalid policy, the policy XML is not changed.

Operator response

Only create one resource reference per base resource.

EEZU0609E **Failed to parse XML policy file *fileName***

Explanation

The specified file does not contain a parsable XML policy, or it cannot be opened.

System action

The requested operation is aborted.

Operator response

Make sure to specify a valid policy file which is accessible and which contains valid XML data.

EEZU0610E **Empty policy file name**

Explanation

Policy file name entry field cannot be empty.

System action

The file load operation is not executed.

Operator response

Specify a file name.

EEZU0611E **The resource with resource name *resource* and resource class *resource class* contains an invalid property. Property *property* must be a valid IPv6 address**

Explanation

The property should contain a valid IPv6 address.

System action

In order to avoid creating an invalid policy, the policy XML is not changed.

Operator response

Type in a valid IPv6 address for the property.

EEZU0612E **The policy name or policy file name exists**

Explanation

The policy name and policy file name must be unique in the domain.

System action

The save operation is not executed.

Operator response

Specify a different policy name or policy file name.

EEZU0613E **The resource name exists**

Explanation

The resource name must be unique to the other resources in the domain.

System action

The save operation is not executed.

Operator response

Specify a different resource name.

EEZU0614E **The policy pool cannot be accessed**

Explanation

The processing is interrupted by a parameter error and cannot complete correctly.

System action

The current task ends.

Operator response

Check and make sure the policy pool exists.

EEZU0615E **The automation policy or automation resource cannot be updated: *Exception text***

Explanation

The update processing is interrupted by a parameter error and cannot complete correctly.

System action

The update task ends.

Operator response

Refer to the exception text to correct parameters and try again.

EEZU0616E **The original policy file cannot be loaded**

Explanation

The processing is interrupted by an unexpected error and cannot complete correctly.

System action

The current task ends.

Operator response

Check and make sure the file exists in the policy pool.

EEZU0618E **The automation policy is not valid**

Explanation

The automation policy in the policy pool contains errors or warnings that can’t pass the validity check.

System action

None.

Operator response

View the errors or warnings, and correct the properties of the policy.

EEZU0619E **Required parameter *parameter name* is missing**

Explanation

A required parameter is not provided for a policy. Without this parameter, the policy information cannot be updated.

System action

The policy information cannot be updated.

Operator response

Verify why the parameter is not provided, reload the page and try again later.

EEZU0620E **The resource can not be found**

Explanation

The specified resource doesn't exist.

System action

None.

Operator response

Retry with a resource that exists.

EEZU0700E Zowe™ explorer server cannot be connected with URL *URL name*

Explanation

The explorer server cannot be connected. The server might be offline, or not correctly configured in configuration file `eez.zowe.properties`.

System action

Connection is not established with Zowe explorer server.

Operator response

- Check if the explorer server is online.
- Check the configuration file `eez.zowe.properties` to make sure the explorer server is correctly configured. The default location is `/etc/opt/IBM/smsz/ing/cfg`.

EEZU0701E HTTP request to URL *URL name* failed with status code: *code number*

Explanation

The HTTP request failed to proceed.

System action

The HTTP request to Zowe™ explorer server failed.

Operator response

Check the returned status code and error log for detailed reasons.

EEZU0702E The JSON data returned from Zowe™ explorer server is not expected

Explanation

The data type of the returned JSON data is not expected.

System action

Data is not retrieved from Zowe explorer server.

Operator response

Check the version of Zowe explorer server that is installed and make sure the version is supported by SMU.

EEZU0703E The Zowe™ explorer server cannot be connected with HTTPS

Explanation

The keystore for Zowe explorer server is not correctly configured in SMU, and thus HTTPS connection cannot be established.

System action

Connection is not established with Zowe explorer server.

Operator response

Check configuration file `eez.zowe.properties` and make sure the keystore for Zowe explorer server is correctly configured. The default location is `/etc/opt/IBM/smsz/ing/cfg`.

EEZU0704E The property values are changed by another person

Explanation

Some property values have been changed since you loaded this page.

System action

None.

Operator response

Refresh the page to reload the values.

EEZU0705E The Universal Automation Adapter can not be enabled

Explanation

At least one valid domain name should be provided to enable the Universal Automation Adapter. The domain name is missing or contains unsupported characters.

System action

None.

Operator response

Specify a valid domain name and try again.

EEZU0706E **Can not connect to Zowe™ explorer server**

Explanation

Can not initialize REST Client, some properties of Zowe explorer server are not set.

System action

REST client for Zowe explorer server is not initialized.

Operator response

Check Zowe configuration file `eez.zowe.properties`, make sure all necessary properties are set.

EEZU0707E **Unable to retrieve the attributes for data set *data set name***

Explanation

The data set attributes cannot be retrieved by Zowe™ REST APIs.

System action

None.

Operator response

Contact the system administrator to check if the data set is correctly created with required attributes being all set.

EEZU0708E **The automation system with SMFID *system identifier* on Sysplex *sysplex name* cannot be found**

Explanation

The system can not be found among the systems that are connected via the SA z/OS E2E adapter. The possible causes are:

- The automation domain or the corresponding E2E adapter is not running.
- The event path from the automation domain to Service Management Unite is not established.
- The host name or the event port used by the E2E adapter is configured incorrectly.

System action

The current task ends.

Operator response

Make sure that the automation domain and the E2E adapter are running. Check the adapter log and make sure the E2E adapter is configured for the correct management server IP address and port. If the expected system is displayed in Service Management Unite, compare the SMFID property of the system in the system's Properties dialog and the Sysplex Name property in the automation domain's Properties dialog with the values shown in the error message.

EEZU0709E **The specified file *file name* does not exist**

Explanation

The file you specified does not exist on the SMU server.

System action

None.

Operator response

Verify if the file exists on server and specify the correct the file name and file location.

EEZU0710E **An unexpected error occurred that caused the save action failed**

Explanation

An unexpected internal error occurred when you save the configuration file.

System action

The save operation is not executed.

Operator response

Contact the system administrator to check if the save request is correct, or contact IBM support (https://www.ibm.com/support/home/) for additional support.

EEZU0712E **The specified `widgetType` *widget type* is not supported**

Explanation

The specified value for property **`widgetType`** in `ibm-portal-topology.xml` is not supported.

System action

None.

Operator response

Check the supported value for **`widgetType`** in `EEZUIConstants`.

EEZU0713E The specified host name or IP address *host name* is not valid

Explanation

The host name or IP address specified is not valid.

System action

None.

Operator response

Provide the correct host name or IP address.

EEZU0714E The *component name* server cannot be connected with URL *URL name*

Explanation

The *component name* server cannot be connected. The server might be offline, or not correctly configured in the configuration file *properties file name*.

System action

The connection is not established with the *component name* server.

Operator response

- Check if the *component name* server is online.
- Check the configuration file *properties file name* to make sure the *component name* server is correctly configured. The default location for the configuration file is `/etc/opt/IBM/smsz/ing/cfg`.

EEZU0715E HTTP request to URL *URL name* failed with status code: *code number*, exception name: *exception*, returned message: *returned message*

Explanation

The HTTP request failed to proceed.

System action

The HTTP request to the *component name* server failed.

Operator response

Check the returned status code and error log for detailed reasons.

EEZU0716E The data cannot be loaded

Explanation

UTF-8 is not supported when encoding URL.

System action

None.

Operator response

Contact the system administrator to check your JVM environment on SMU server and make sure that UTF-8 is supported.

EEZU0717E The *component name* server cannot be connected with HTTPS

Explanation

The keystore for *component name* server is not correctly configured in SMU, and thus HTTPS connection cannot be established.

System action

Connection is not established with the *component name* server.

Operator response

Check configuration file *properties file name* and make sure the keystore for *component name* server is correctly configured. The default location for the configuration file is `/etc/opt/IBM/smsz/ing/cfg`.

EEZU0718E The *component name* server cannot be connected because of missing properties

Explanation

The REST client can not be initialized, some properties of the *component name* server are not set.

System action

The REST client is not initialized.

Operator response

Check configuration file *properties file name* and make sure all necessary properties are set. The default location for the configuration file is `/etc/opt/IBM/smsz/ing/cfg`.

EEZU0719E **The operation failed with HTTP status code: *code number*, exception name: *exception*, returned message: *returned message***

Explanation

The HTTP request for the action failed to proceed.

System action

The HTTP request to the *component name* server failed.

Operator response

Check the returned status code and error log for detailed reasons.

EEZU1000E **Resource *resource name* does not exist**

Explanation

The specified resource cannot be found. Reasons can be that the resource does not exist anymore, has been deleted or the corresponding automation adapter is not running.

System action

Desired action cannot be completed.

Operator response

Retry with a valid resource.

EEZU0111E **Missing data in response from `INGWHY`**

Explanation

The response to the **`INGWHY`** command misses required data.

No problem isolation information can be fetched.

System action

The response cannot be handled and is rejected.

Operator response

Check IBM Electronic Support for additional information: http://www.ibm.com/support/entry/portal/.

EEZU0112E **Problem isolation not supported on *resource name***

Explanation

Problem isolation is not supported on the specified resource.

System action

No problem isolation can be performed.

Operator response

Retry with a supported resource.

EEZU1001E **System *system name* does not exist**

Explanation

The specified system cannot be found. Reasons can be that the resource id does not represent a system, the system does not exist anymore, has been deleted or the corresponding automation adapter is not running.

System action

Desired action cannot be completed.

Operator response

Retry with a valid system.

EEZU1002E **Domain *domain name* does not exist**

Explanation

The specified domain cannot be found. Reasons can be that the resource id does not represent a domain, the domain does not exist anymore, has been deleted or the corresponding automation adapter is not running.

System action

Desired action cannot be completed.

Operator response

Retry with a valid domain.

EEZU1003E UTC offset for domain *domain name* not available

Explanation

The UTC offset for the specified domain is not available, because the corresponding automation adapter does not support querying the UTC offset.

System action

Desired action cannot be completed.

Operator response

Ensure the corresponding automation adapter supports querying the UTC offset.

EEZU1004E Operation not supported on *resource name*

Explanation

The desired operation is not supported on the specified resource.

System action

Operation cannot be performed.

Operator response

Retry with a supported resource.

EEZU1100E Invalid time format:*Exception text*

Explanation

The specified time format is invalid.

System action

Desired action cannot be completed.

Operator response

Retry with a valid time format.

EEZU1101E Invalid interval: *Exception text*

Explanation

The specified interval is invalid.

System action

Desired action cannot be completed.

Operator response

Retry with a valid interval.

EEZU0500W The automation domain *domain name* no longer exists

Explanation

You specified an automation domain that no longer exists. Possible reasons are that the automation domain has been deleted in the meantime.

System action

The current task continues.

Operator response

Check if the adapter for the specified domain is running properly. If the domain is deleted in the meantime, remove the corresponding widget from the dashboard.

EEZU0501W The selected resource *resource name* no longer exists

Explanation

You selected a resource that no longer exists. Possible reasons are that the resource has been deleted in the meantime or the automation policy has been changed or deactivated.

System action

The current task continues.

Operator response

If the resource is still displayed, use menu item 'Refresh all' to obtain the currently available resources.

EEZU0502W The selected node *node name* no longer exists

Explanation

You selected a node that no longer exists. Possible reasons are that the node has been deleted in the meantime.

System action

The current task continues.

Operator response

If the node is still displayed, use menu item 'Refresh all' to obtain the currently available nodes.

EEZU0503W The request has been submitted but has not been processed yet

Explanation

A request has been submitted but was not processed by the corresponding automation manager. Reasons for this can be a slow network or an automation manager that is not responding.

System action

The application continues.

Operator response

If the request is not processed soon, send the request again. If the problem persists, check the connections to the automation manager and inspect the log files of the automation manager for problems.

EEZU0504W The order to cancel the operator request has been submitted, but the request is still not canceled yet

Explanation

A cancel request has been submitted but was not processed by the corresponding automation manager. Reasons for this can be a slow network or an automation manager that is not responding.

System action

The application continues.

Operator response

If the request is not processed soon, cancel the request again. If the problem persists, check the connections to the automation manager and inspect the log files of the automation manager for problems.

EEZU0505W The order to change the automation policy has been submitted, but the policy change has not been completely processed yet

Explanation

The order to change the automation policy has been submitted to the corresponding automation manager, but the processing of this change has not finished yet. Reasons for this can be a slow network or an automation manager that is not responding.

System action

The application continues. When the processing of the policy change has been completed the screen will automatically refresh to reflect the change.

Operator response

If the problem persists, check the connections to the automation manager and inspect the log files of the automation manager for problems.

EEZU0506W Domain *Domain name* became unavailable

Explanation

The operations console accesses first-level automation domains directly (direct access mode). A domain that had been contacted successfully before, became unavailable when the operations console tried to perform a request on a first-level automation domain. The automation adapter or the node of the domain may have shut down without being able to notify the operations console.

System action

The request and any further request will not be performed on the domain until it becomes available.

Operator response

If you are using the operations console and the automation domain is still displayed, use menu item 'Refresh all' to obtain the currently available domains. If 'Refresh all' is not available, close and restart the current task to obtain the currently available domains.

EEZU0507W The management server is no longer available

Explanation

The session may be no longer valid (e.g. timed out or logged off).

System action

None

Operator response

Logout and login again. If the problem persists, restart the WebSphere Application Server.

EEZU0508W **The automation resource with resource ID *resource id* no longer exists**

Explanation

You specified an automation resource that no longer exists. Possible reasons are that the automation resource has been deleted in the meantime.

System action

The current task continues.

Operator response

Check if the specified resource still exists in your automation topology. If the resource is deleted in the meantime, remove the corresponding widget from the dashboard.

EEZU0509W **No automation policies are available for domain *domain name***

Explanation

The specified automation domain did not return any policy to display.

System action

The current task ends.

Operator response

Check if the specified domain supports to list policies and has a proper policy pool defined. Check that policies with correctly specified domain name exist in this policy pool.

EEZU0510W **Automation domain *domain name* is not accessible at this moment**

Explanation

The specified automation domain cannot be accessed.

System action

The current task ends.

Operator response

Check if the specified domain is in a state `available` and the communication state is OK.

Check if the Universal Automation Adapter (UAA) is started. Go to SMU server and run the command in terminal: **`eezuaadapter`**.

EEZU0511W **Automation domain *domain name* does not support policy activation with this product**

Explanation

The specified automation domain does not support to list or activate policies through this product.

System action

The current task ends.

Operator response

This product cannot be used to handle policies of this domain.

EEZU0512W **The automation JEE framework (Enterprise application EEZEAR) is not fully initialized yet and refuses to accept requests. Wait until the EEZEAR application is fully initialized, then re-open the dashboard**

Explanation

The automation JEE framework (Enterprise application EEZEAR) is not fully initialized yet. The communication with attached domains is not possible until all components of the EEZEAR application are initialized.

System action

The system waits until the automation JEE framework is initialized before processing requests.

Operator response

Re-open the dashboard.

EEZU0513W **No automation policy resource is available**

Explanation

The policy does not contain any resource to display.

System action

None.

Operator response

Add new resources to the policy.

EEZU0520W The adapter log file of automation domain *domain name* requires operator attention

Explanation

The adapter log file contains errors or warnings which require operator attention.

System action

The current task ends.

Operator response

View the adapter log and look for warning or error messages to be resolved by human interaction.

EEZU0550W Automation domain *domainName* is not accessible at this time

Explanation

The automation domain exists, but it is currently not possible to communicate with it.

System action

You can continue using the policy editor, however it is not possible to use the harvesting functionality against the offline domain or to make use of that domain's policy pool while the domain is offline.

Operator response

If you want to use the harvesting functionality or the policy pool of the offline domain, make sure that the automation domain is running. If it is a first-level automation domain, verify that the automation adapter is running. Retry the operation after the timeout period defined by the environment variable com.ibm.eez.aab.watchdog-interval-seconds. If the problem persists, restart the automation adapter (in case of a first-level automation domain) or the end-to-end automation engine (in case of an end-to-end automation domain). Note that you can save your policy temporarily to local file instead of to the policy pool.

EEZU0601W The policy contains XML comments. XML comments will be removed

Explanation

The policy XML file contains XML comments which are not supported. These XML comments will be lost when the policy is loaded into the policy editor.

System action

The policy editor continues to load the policy file, but XML comments are removed.

Operator response

If editing policy XML files manually, you should not use XML comments. You can use the Description field of resources instead.

EEZU0602W The version of this policy file or of the used connected domain does not match the version of the policy editor. Version of policy file or used domain: *version in policy file* . Version of policy editor: *policy editor version*

Explanation

The version of the policy XML file does not match the version of the policy editor. This may result in incompatibilities. In case you have connected the policy editor to a domain running a different level, it might be impossible to activate the policy generated with this version of the policy editor.

System action

If the version of the policy XML is higher than the version of the policy editor, some elements unknown to this policy editor version may be accidentally removed if saving the policy. If the version of the policy XML is lower than the version of the policy editor and you save it, down-level versions of the corresponding automation product may reject to activate that policy. If you save a policy to a domain with a lower level than the policy editor, that domain might not be able to activate that policy.

Operator response

After saving the policy with this version of the policy editor, please check manually whether any expected component is missing. Use a policy editor with the corresponding version whenever possible.

EEZU0603W While trying to read history data from the automation database, it was detected that no schema name has been specified for the automation database

Explanation

The parameter 'database-schema-name' is missing in the file eez.automation.engine.properties.

System action

The default schema name 'EAUTOUSR' will be used.

Operator response

If you use another schema name than 'EAUTOUSR', ensure that the parameter 'database-schema-name' exists in the file eez.automation.engine.properties.

EEZU1000I **No policy is activated**

Explanation

No resources are displayed because no policy is activated.

System action

None.

Operator response

Activate a policy.

EEZU1001I **No System Log Messages available that match the executed query**

Explanation

The queried System Log does not contain any messages, that match the executed query.

System action

No System Logs can be displayed.

Operator response

None.

EEZU1002I **No response**

Explanation

The executed command returns no response.

System action

None.

Operator response

None.

EEZU1080I **No captured messages available for resource *resource name***

Explanation

There are no captured message available for the specified resource. Either there are no messages captured for this resource yet or message capturing is not configured in the policy.

System action

No captured messages can be displayed.

Operator response

Verify that message capturing is configured for this resource in the policy.

EEZU1090I **No monitoring history messages available for monitor *monitor name***

Explanation

There are no monitoring history message available for the specified monitor. Either there are no history messages captured for this monitor yet or monitoring history is not configured in the policy.

System action

No monitoring history messages can be displayed.

Operator response

Verify that monitoring history is configured for this monitor in the policy.

EEZU2000I **Domain State for domain *domain name* is *domain state***

Explanation

The domain changed its state to the specified value.

System action

The system will handle this change. Resource References to this domain will change their state accordingly.

Operator response

None.

EEZU2001I **Domain *domain name* joined successfully**

Explanation

The domain is now available and ready for being managed.

System action

The system will handle this change. Resource References to this domain will change their state accordingly.

Operator response

None.

EEZU2002I **Domain Communication State for domain *domain name* is *domain communication state***

Explanation

The domain has a new communication state.

System action

The system will handle this change. Resource References to this domain will change their state accordingly.

Operator response

None.

EEZU2003I **Request event for *request type* request has been received from domain *domain name* for resource *resource name***

Explanation

A request has been added on the specified resource.

System action

The system will handle this change.

Operator response

None.

EEZU2004I **Request deleted event has been received from domain *domain name* for resource *resource name***

Explanation

A request has been added on the specified resource.

System action

The system will handle this change.

Operator response

None.

EEZU2005I **Policy changed event has been received from domain *domain name***

Explanation

The policy containing resource, group and relationship definitions has changed for this domain.

System action

The system will handle this change.

Operator response

None.

EEZU2006I **The job with job name *job name* does not run under JES. Therefore, no job information can be displayed.**

Explanation

The JES Explorer displays the job information, such as the output of the job or the JCL, only for the jobs that run under JES. It cannot display the job information for address spaces that don't run under JES, for example, system address spaces that are started before JES comes up.

System action

None.

Operator response

None.

EEZU2000W **Domain *domain name* left**

Explanation

The domain is not available anymore for being managed.

System action

The system will handle this change. Resource References to this domain will change their state accordingly.

Operator response

None.

EEZU2002W **Domain Communication State for domain *domain name* is *domain communication state***

Explanation

The domain has a new communication state.

System action

The system will handle this change. Resource References to this domain will change their state accordingly.

Operator response

None.

EEZU2002E **Domain Communication State for domain *domain name* is *domain communication state***

Explanation

The domain has a new communication state.

System action

The system will handle this change. Resource References to this domain will change their state accordingly.

Operator response

None.

Chapter 11. SMU exploitation and integration with Zowe™

Starting from Service Management Unite (SMU) Version 1.1.5, SMU is integrated with Zowe™ to modernize the automation and monitoring on IBM Z.

Overview

To continue modernizing the automation and monitoring on IBM Z®, SMU Automation is integrated with Zowe to provide more capabilities to facilitate the operation on the mainframe.

What is SMU Automation?

IBM Service Management Unite Automation is the new customizable dashboard interface that is available with IBM Z System Automation V4.1.0 and later. It provides a single point of control for multiple SAplexes to operate in your environment.

For more information about SMU Automation, see Chapter 2, "Overview of Service Management Unite Automation," on page 3.

What is Zowe?

Zowe offers modern interfaces to interact with z/OS and allows you to work with z/OS in a way that is similar to what you experience on cloud platforms today. You can use these interfaces as delivered or through plug-ins and extensions that are created by clients or third-party vendors.

Zowe consists of the following main components:

Zowe Application Framework
A web user interface (UI) that provides a virtual desktop containing a number of apps allowing access to z/OS function. Base Zowe includes apps for traditional access such as a 3270 terminal and a VT Terminal, as well as an editor and explorers for working with JES, MVS Data Sets and Unix System Services.

z/OS services
Provides a range of APIs for the management of z/OS JES jobs and MVS data set services.

API Mediation Layer
Provides a gateway that acts as a reverse proxy for z/OS services, together with a catalog of REST APIs and a dynamic discovery capability. Base Zowe provides core services for working with MVS Data Sets, JES, as well as working with z/OSMF REST APIs. The API Mediation Layer also provides a framework for Single Sign On (SSO).

Zowe CLI
Provides a command-line interface that lets you interact with the mainframe remotely and use common tools such as Integrated Development Environments (IDEs), shell commands, bash scripts, and build tools for mainframe development. It provides a set of utilities and services for application developers that want to become efficient in supporting and building z/OS applications quickly. It provides a core set of commands for working with data sets, USS, JES, as well as issuing TSO and console commands. Some Zowe extensions are powered by Zowe CLI, for example the Visual Studio Code Extension for Zowe.

For more information about Zowe, see Zowe overview.

What is SMU exploitation and integration with Zowe?

Integrated with Zowe, SMU Automation offers extended functions to allow you to interact with z/OS resources, such as managing JES and MVS details in the SMU dashboards. When Zowe is installed and configured to connect with the SMU Automation server, you can interact with mainframe data sets and jobs like modern cloud or desktop platform.

- A Zowe application plug-in (SMU plug-in) is provided to allow you to use SMU Automation directly on Zowe Desktop and leverage free and commercial APIs in Zowe Application Framework.
- A new **JES Explorer** dashboard is provided to allow you to view job content and job output to isolate environmental issues. The **JES Explorer** dashboard can be started from System Automation APL resources.

Why should you use SMU exploitation and integration with Zowe?

- New plug-in on Zowe Desktop

  You can quickly and easily access the SMU plug-in on Zowe Desktop where other common tools are available, which gives you a unified and integrated user experience.
- Improved problem identification

  You can isolate environmental issues by seamlessly navigating into the **JES Explorer** dashboard to view any job information without the need to switch the application or use another terminal.
- Reduced Time-to-Value (TTV)

  New developers or system programmers can quickly get onboard to work on the mainframe.

Prerequisites

Review the following prerequisites to prepare your environment for integrating SMU Automation with Zowe.

Table 34. Prerequisites

Requirements for SMU Automation	**Requirements for Zowe**
SMU Automation V1.1.5, or later. To obtain the installation files, see "Obtaining installation files" on page 17.	• For SMU Automation V1.1.5, Zowe V0.9.4 and V0.9.5 open beta are supported. • For SMU Automation V1.1.6, Zowe V1.0.1, V1.1.0, V1.2.0, V1.3.0, and V1.4.0 are supported. To obtain the installation files, see Obtaining installation files. **Note:** IBM offers some support for the open source software. To review IBM's support policy for open source software, see Third party software and Open Source software in the IBM Software Support Handbook.
• Environment requirements • Hardware requirements • Software prerequisites **Important:** To use the new capabilities offered by SMU integration with Zowe, APAR OA54684 must be installed in IBM Z System Automation.	• System requirements

Installing and Configuring

This section provides roadmap for installing and configuring SMU and Zowe™.

Roadmap for SMU installation and configuration

Review the following installation roadmap and configuration roadmap to deploy your SMU environment.

SMU installation roadmap

Docker	Root	Non-root	Silent
If you have a Docker runtime environment: "Installing Service Management Unite Automation" on page 18	If you install SMU using the root user ID: 1. Install JazzSM and WebSphere Application Server as root. 2. Install SMU Automation as root.	If you install SMU using the non-root user ID: 1. Install JazzSM and WebSphere Application Server as non-root. 2. Install SMU Automation as non-root.	If the Window Manager is not available: 1. Install JazzSM and WebSphere Application Server in silent. 2. Install SMU Automation in silent.

SMU configuration roadmap

Table 35. SMU configuration roadmap

SMU Automation
1. Quick startup of End-to-End Automation Adapter.
2. Configure the SMU Automation host. You can use either the **cfgsmu** or the new web configuration tool to customize your configuration: • "[Use Web Config Tool] Configuring the Universal Automation Adapter" on page 71. • "[Use Web Config Tool] Configuring the Universal Automation Adapter" on page 71.
3. Secure the connection to automation adapters.
4. [Optional] Configure access to the Universal Automation Adapters.

Roadmap for Zowe™ installation and configuration

Review the following installation roadmap and configuration roadmap to deploy your Zowe™ environment.

Zowe installation roadmap

Installing Zowe involves several steps that you must complete in the appropriate sequence. Review the following installation roadmap that presents the task-flow for preparing your environment and installing and configuring Zowe before you begin the installation process.

- Install Zowe on z/OS.
- Install Zowe CLI.

Zowe configuration roadmap

After you install Zowe, you can optionally configure the terminal application plug-ins or modify the Zowe Application Server (zLUX Proxy Server) and ZSS configuration, if needed.

- Configure Zowe Application Framework.
- Configure Zowe CLI.

Integrating

Integrate SMU with Zowe™ to exploit the extended functionality.

Applying a DASH fix pack

You must apply a DASH fix pack after you install Service Management Unite. Otherwise, you will have problems in navigating to the second level SMU dashboards on Zowe™ Desktop.

Procedure

1. Go to IBM Fix Central via https://ibm.biz/Bd23aG.
2. Download fix pack `1.1.3-TIV-JazzSM-multi-FP002`.
3. Follow the steps that are described in `readme.txt` to apply the fix pack.
4. Restart the DASH server.

Installing SMU plug-in in Zowe™

Run script **`installSMUPlugin.sh`** to install SMU plug-in so that you can access SMU console from Zowe™ Desktop.

Before you begin

Make sure the user ID has the authority to access directory *<Zowe_rootDir>* where you installed Zowe, the default location is `/zowe/1.0.1` if you install Zowe version 1.0.1.

Procedure

1. Log in to the server where Zowe is installed.
2. Issue the command to extract the SMU plug-in package `SMU_Zowe_Plugin_v1.0.x.tar` (included in the SMU installation package) to a directory, for example, `smu-plugin`.

   ```
   tar -xof SMU_Zowe_Plugin_v1.0.x.tar
   ```

   Note: After the tar file is extracted, ensure other users in this system also have the read and write access to these files. You can check the access with command **`umask`**. If the value is `0077`, set the value to `0022` and extract the tar kit again:

   ```
   umask 0022
   tar -xof SMU_Zowe_Plugin_v1.0.x.tar
   ```

3. Browse to directory *`<Zowe_rootDir>`*`/scripts` where shell scripts are stored.
4. Issue the following command to stop Zowe services:

   ```
   ./zowe-stop.sh
   ```

5. Browse to the directory where the SMU plug-in files are extracted.

   You can use either of the following ways to install SMU plug-in:

   - Automatic installation:
     a. Issue the following command to install SMU plug-in:

        ```
        ./installSMUPlugin.sh <Zowe_rootDir> <SMU server console URL>
        ```

        Example:

        ```
        ./installSMUPlugin.sh /var/zowe/1.0.1 https://smuserver.com:16311/ibm/console
        ```

   - Manual installation:

a. Browse to the extracted SMU plug-in package, for example, smu-plugin/SMU/web, and open file index.html.

b. Specify value for parameter **SMU_WEB_CONSOLE_URL** and save the changes.

c. Copy file com.ibm.smu.json to Zowe plug-ins directory <*Zowe_rootDir*>/zlux-example-server/deploy/instance/ZLUX/plugins.

d. Copy file com.ibm.smu.json to Zowe plug-ins directory <*Zowe_rootDir*>/zlux-example-server/plugins.

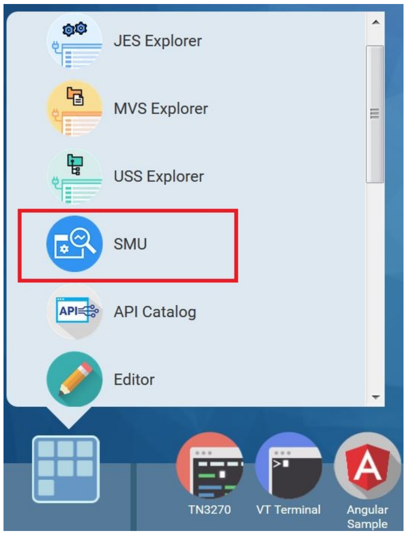
e. Copy folder smu-plugin to directory <*Zowe_rootDir*>.

6. After you successfully installed SMU plug-in, navigate to directory <*Zowe_rootDir*>/scripts and restart Zowe services.

```
./zowe-start.sh
```

Results

SMU plug-in is successfully installed, and you can find the entry icon for SMU plug-in in the toolbox.



Creating a keystore file

To secure the connection to Zowe™ micro-services server, use the Java keytool to import Zowe certificate to the keystore.

Procedure

1. From a supported browser, access Zowe micro-services server via https://<your.server>:<atlasport>.

   Where,

   - *<your.server>* is the host name of the server where Zowe is installed.
   - *<atlasport>* is the API Gateway port, for example, 7554 is the default number.

   The supported browsers are:

   - Google Chrome V54 or later
   - Mozilla Firefox V44 or later
   - Safari V11 or later
   - Microsoft Edge (Windows 10)

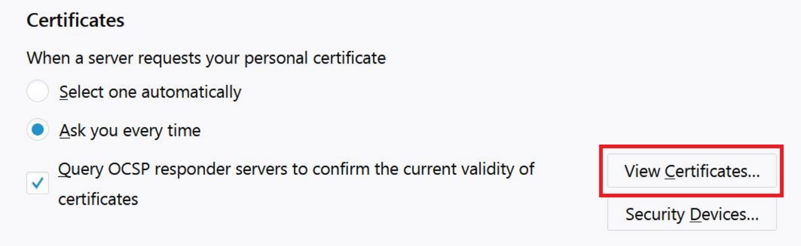
2. If you get a security message about an insecure connection, add exception for the certificate.

   Take Firefox Version 60.2.1 as an example:

a. Click **Advanced** and then click **Add Exception...**.

b. In the task menu, select **Options** → **Privacy & Security**.

c. Click **View Certificates...** to open the Certificate Manager.



Certificates

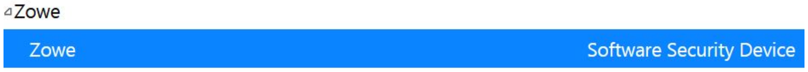
When a server requests your personal certificate

○ Select one automatically

● Ask you every time

☑ Query OCSP responder servers to confirm the current validity of certificates

d. In the certificate list, select the certificate of your Zowe micro-services server.



◿Zowe

Zowe Software Security Device

e. Click **Export...** to save the certificate as X.509 certificate. For example, save it as `zowe.crt`.

3. Issue the following command to create a keystore file and import the exported certificate to the keystore:

   ```
   keytool -import -noprompt -trustcacerts -alias <alias> -file <filename> -keystore <keystore
   name> -storepass <keystore password>
   ```

   Where,

   - *<alias>* is the alias name of the entry. All keystore entries (key and trusted certificate entries) are accessed via unique aliases.
   - *<filename>* is the file name of the exported certificate, for example, `zowe.crt`.
   - *<keystore name>* is the name of the keystore file.
   - *<keystore password>* is the keystore password.

   If you have an existing keystore file, you can use its keystore file name and password to import the certificate.

4. Upload the created keystore file to your SMU server. You can place it anywhere that the SMU server can access it.

   Note: If you use the SMU Docker image, you can use command **`docker cp`** to copy the keystore file into Docker.

What to do next

You need to configure the properties to specify the location of the keystore file, and then restart the SMU service.

Configuring the properties to connect with Zowe™

Use the web configuration tool to configure the properties to establish the connection between Zowe™ and the SMU server.

Procedure

1. In the navigation bar, click **System Configuration** → **Configure Service Management Unite** to start the web configuration tool.
2. Click **Zowe** to switch tab to open the Zowe configuration page.
3. Select **Enable Zowe Dashboards in Service Management Unite**. The properties fields are displayed.

   - Host Information

Default Port Number
The default HTTPS port of Zowe gateway on the z/OS system.

- Click **Add new** to create new host information.

  In the new row, specify the following parameters:

  SysPlex Name
  The name of the Sysplex.

  SMFID
  The SMF ID assigned to the system.

  Host Name
  The host name of the z/OS system where Zowe is installed.

  Port Number
  The HTTPS port number of the Zowe gateway on the z/OS system.

  Operation
  Click **OK** to save the new item. You can click **Cancel** to cancel the changes.

  Enable
  Check it so that you can view the corresponding SysPlex data in the MVS or JES explorer dashboard. Otherwise, the data for the SysPlex cannot be displayed.

- To modify the existing host information, click ✎.
- To delete the credential, click 🗑.

- Security

  Keystore
  The location of the keystore file.

  Specify the absolute path of the keystore file that you created in the last step. When querying Zowe micro-services REST APIs to get job or data set information, the certificate in keystore will be used.

  Keystore password
  The password of the keystore.

  Confirm keystore password
  Identical value as specified in the keystore password field to confirm password correctness.

4. Click **Save** to save all your changes.
5. Restart the DASH server.

   For example, in the *JazzSM_HOME*/`profile/bin` directory, for a server that is named server1, issue the following commands to stop and start the server:

   ```
   ./stopServer.sh server1
   ./startServer.sh server1
   ```

Uninstalling SMU plug-in in Zowe™

Run script **`uninstallSMUPlugin.sh`** to uninstall SMU plug-in in Zowe™.

Before you begin

Make sure the user ID has the authority to access directory *<Zowe_rootDir>* where you installed Zowe, the default location is `/zowe/1.0.1` if you install Zowe version 1.0.1.

Procedure

1. Log in to the server where Zowe is installed.
2. Browse to directory *<Zowe_rootDir>*`/scripts` where shell scripts are stored.

3. Issue the following command to stop Zowe services:

```
./zowe-stop.sh
```

4. Browse to the directory where the SMU plug-in files are extracted.
5. Issue the following command to uninstall SMU plug-in:

```
./uninstallSMUPlugin.sh <Zowe_rootDir>
```

6. After you successfully uninstalled SMU plug-in, navigate to directory `<Zowe_rootDir>/scripts` and restart Zowe services.

```
./zowe-start.sh
```

Results

SMU plug-in is successfully uninstalled.

Note: If you pinned the SMU plug-in to the taskbar on Zowe Desktop, you need to manually delete the pinned icon after the uninstallation.

Scenarios

Scenarios contain step-by-step instructions for doing specific tasks in SMU with Zowe™.

Accessing SMU plug-in on Zowe™ desktop

When Zowe and SMU are correctly configured, you can access SMU plug-in on Zowe™ Desktop.

Procedure

1. From a supported browser, open the Zowe Desktop at `https://myhost:httpsPort`.

   Where:

   - *myHost* is the host name of the server on which you are running the Zowe Application Server.
   - *httpsPort* is the value that is assigned to *node.https.port* in `zluxserver.json`.

     For example, if you run the Zowe Application server on host *myhost* and the value that is assigned to *node.https.port* in `zluxserver.json` is 12345, you would specify `https://myhost:12345/`.

   Important:

   - When you initially open the Zowe Desktop, a security message alerts you that you are attempting to open a site that has an invalid HTTPS certificate. Other applications within the Zowe Desktop like the SMU plug-in might also encounter this message. To prevent this message, add the URLs that you see to your list of trusted sites.

     If you clear the browser cache, you must add the URL to your trusted sites again.
   - When the browser asks you to **Leave Page** (Firefox) or **Leave site** (Chrome),
     - For Firefox, click **Stay on Page**.
     - For Google Chrome, click **Cancel**.

     Otherwise, the page will be redirected.
2. Enter your mainframe credentials in the **Username** and **Password** fields and press **Enter**.

   Upon authentication of your user name and password, the Zowe desktop opens.
3. Click the Start menu ▦ and select the SMU plug-in by clicking 🔍.

   Important: If the page cannot be displayed because of the security issues, add the URL (`https://`*hostname*`:16311/ibm/console/logon.jsp`) that you see to your list of trusted sites.

4. Enter your credentials in the **Username** and **Password** fields and press **Enter**.

   The default username is `eezadmin`.

   Upon authentication, the SMU Welcome page is displayed.

Viewing JES job information

When SMU is integrated with Zowe™, you can view JES job information and output in the **JES Explorer** dashboard.

About this task

You can use Zowe JES Explorer to query JES jobs with filters, and view the related steps, files, and status. SMU is integrated with Zowe JES Explorer so that you can isolate environmental issues by seamlessly navigating into the JES Explorer dashboard to view any job information without the need to switch the application or use another terminal.

Procedure

1. Access the **JES Explorer** dashboard:

   Right-click an SA APL resource, and select **View Job Information**. For example,

   a. In the Navigation bar, click **Administration** → **Explore Automation Domains**.

   b. Right-click an application in the **Resources** widget and select **View Job Information**.

   You can also open Zowe JES Explorer in another tab:

   Right-click a node in automation dashboards and select **Launch JES Explorer**.

   Note: If you are the first time to open this explorer from SMU, a pop dialogue is displayed assisting you in accepting the certificate to avoid security issues.

   a. Click the text with hyperlink **Zowe JES Explorer (*URL*)**. The browser opens a new window.

   b. Accept the certificate and allow the content to be displayed.

      For example, if you use Firefox, click **Advanced** > **Add Exception...** > **Confirm Security Exception**.

   c. In the pop-up window, provide the credentials that you use to access z/OS environment and click **OK**.

   d. Return to the SMU console and click **Close** to close the pop-up information.
2. The **JES Explorer** dashboard is opened.
   - In widget **Job Informaiton**, the job content including the job name and status is displayed.
     - Click ⊞ to show the job instances. For each job instance, click ⊞ to view the job files and job steps.
     - Hover the cursor over a job name, job instance, job file, or job step, you can view the general properties. You can also right-click a row and select **Properties** to view the properties.
   - In widget **Content Viewer**, you can view the detailed job content of a job file that you selected in the **Job Informaiton** widget.

     Important: If you select a job that doesn't run under JES, no job information can be displayed.

     The **JES Explorer** dashboard displays the job information, such as the output of the job or the JCL, only for the jobs that run under JES. It cannot display the job information for address spaces that don't run under JES, for example, system address spaces that are started before JES comes up.
3. In widget **Job Informaiton**, click the job file that you would like to view. You can see the job content is displayed in **Content Viewer**.

Viewing and editing MVS data set information

When SMU is integrated with Zowe™, you can view MVS data set information in the **MVS Explorer** dashboard.

About this task

You can use Zowe MVS Explorer to view and edit data sets and members. SMU is integrated with Zowe MVS Explorer, so that you can view data set attributes such as **blksize**, **LRECL** and others, and view and edit data set member or sequential data set content via the MVS Explorer dashboard.

You can view and edit only with the supported data set type. You cannot see the **View Data Set** option if you select an unsupported type.

Table 36. Supported and unsupported data set type

Supported data set type	**Unsupported data set type**
Partitioned	VSAM
Physical Sequential	VSAM Unmovable
PDS Extended	ISAM
Physical Seq Unmovable	ISAM Unmovable
Partitioned Unmovable	Hierarchical File
	Direct Access
	Direct Access Unmovable
	Extended Seq Unmovable
	Extended Sequential

Note: You need the corresponding authorities to read or write the data set. For example, write access is required to edit the data set content.

Procedure

1. Right-click a node in automation dashboards and select **Launch MVS Dataset Explorer**.

   Zowe JES Explorer is opened in another browser tab.
2. Click the data set or member that you would like to edit, and you can see the content is displayed in the right viewer.
3. Edit the content as needed.
4. Click **SAVE** to save your edits.

   To save the content as a new member, click **SAVE AS...**. In the pop-up window, specify a new member name and click **OK**. The new member is created.

Appendix A. Notices

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The performance data 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.

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

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

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

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

COPYRIGHT LICENSE:

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

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows:
© (your company name) (year).
Portions of this code are derived from IBM Corp. Sample Programs.
© Copyright IBM Corp. _enter the year or years_.

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 "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

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.

Programming Interface Information

This book documents programming interfaces that allow the customer to write programs to obtain the services of IBM System Automation for z/OS.

SC27-8747-00