IBM

IBM Service Management Unite V1.1.2 - Installation and Configuration Guide

Contents

Chapter 1. IBM Service Management Unite V1.1.2

IBM® Service Management Unite is the customizable Dashboard Application Services Hub (DASH) interface that is available with IBM Service Management Suite for z/OS® V1.3.0 and above.

Service Management Unite provides system programmers, operators, and administrators with a transparent view of system health status and allows for easy problem identification. The console enables operators to see both monitoring and automation exception events together, so they can identify critical problems. Operators can quickly and confidently analyze, isolate and diagnose problems by providing all relevant data in a single location. Service Management Unite also enables operators to interact directly with the system by issuing commands and viewing results without going to a different console.

Note: For the prerequisites of Service Management Unite and the download information, see the Customer Support Portal for IBM® Service Management Suite for z/OS.

The following example illustrates a Service Management Unite user scenario:

1. The operator views both monitoring and automation exception events, sorted by severity on the consolidated event viewer, and customized for her area of support.
2. The event viewer has the events sorted by priority, so the operator selects the top event not acknowledged by another operator.
3. The event pertains to a problem with a resource owned by a WebSphere® Messaging Queue Manager.
4. The operator navigates to the WebSphere Messaging Queue Manager detail page to view key performance metrics, and determines that a specific channel is not running.
5. The operator navigates to the problem isolation page for channel not running. The operator views a list of suggested actions to restore service.
6. The operator issues a command to fix the problem and restore service.

Service Management Unite also provides access to automation functions to start, stop or recycle business applications running on z/OS, even from mobile devices. This flexibility helps system programmers, operators, and administrators by delivering more usable and efficient automation and system and network management capabilities. The integrated operations console can be used by operators to issue commands such as starting and stopping heterogeneous business applications on IBM z Systems and distributed platforms.

Chapter 2. New in this release

This information contains an overview of the major changes to Service Management Unite.

IBM Service Management Unite V1.1.2 provides the following key new features:

- Added z/OS Problem Isolation dashboards to allow you to identify and resolve z/OS-based resource conflicts and delay states.
- Redesigned z/OS dashboard to speed problem identification and resolution.
- Increased integration with System Automation to ensure operators can issue commands to resolve problems without impacting automation policies.
- Enhanced interface to control System Automation scheduling and policies.
- Added Captured Messages dashboard to show you the captured messages for a specific node or resource.
- Added Monitoring History dashboard to show you the monitoring history for a specific monitor resource.
- Added support for end-to-end automation in IBM System Automation for z/OS V4.1.0 for cross-sysplex configurations.

Chapter 3. Overview

IBM Service Management Unite is the customizable dashboard interface that is available with IBM Service Management Suite for z/OS V1.3.0 and above. This documentation guides you through the Service Management Unite installation and configuration process.

Overview of Service Management Unite

IBM Service Management Unite is a customizable service management user interface that provides dashboards to monitor and operate z system environments.

IBM Service Management Unite has two components:

* Service Management Unite Automation. It provides the overall health status of the automation domains and nodes.
* Service Management Unite Performance Management. It helps you monitor and manage z/OS operating systems, networks, and storage subsystems.

They work together to empower the operations staff to analyze and resolve problems more quickly.

IBM Service Management Unite provides the following capabilities:

* Provides a consolidated view of system health status, and thus reduces the time and effort in accelerating problem identification.
* Delivers simplified, efficient automation, and system and network management capabilities, which streamlines operators' workflow.
* Provides an integrated operations console, which can be used to issue commands and resolve problems. It increases the degree of automation and avoids manual and time intensive tasks.
* Provides highly customized dashboard that helps you best suite your needs.
* Supports mobile access, which enables you to check your system anytime and anywhere.

For related information, refer to the following resources:

Table 1. Related documentation for installing and configuring Service Management Unite

Related documentation	Location
IBM Service Management Unite V1.1.2 readme file	Component installation package
IBM Service Management Suite for z/OS Suite License Information CD (LC27-6399-02)	Shipped on CD
IBM Service Management Suite for z/OS Program Directory (GI13-2328-05)	Knowledge Center: Program Directory
Dashboard console online help	Click the question mark icon (?) on the dashboard console toolbar

Service Management Unite architecture

The following diagram depicts the comprehensive IBM Service Management Unite V1.1.2 and related IBM Service Management Suite for z/OS V1.4.2 system architecture.
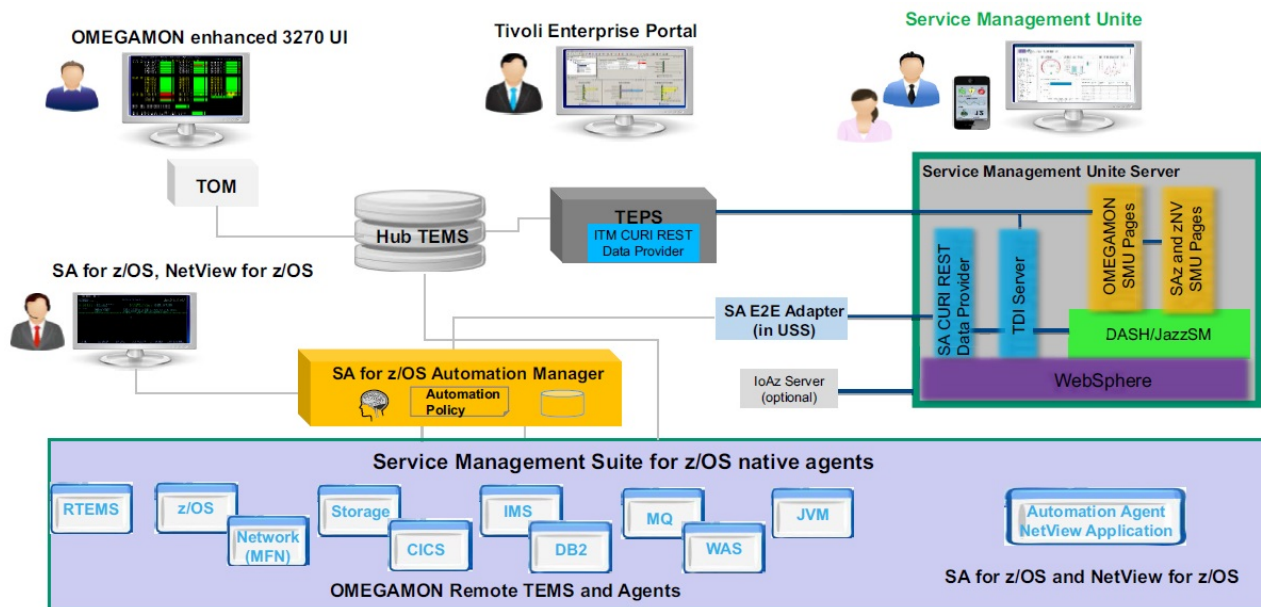
Figure 1. IBM Service Management Unite architecture

License information

Before you install and configure IBM Service Management Unite, you must accept the license agreement.

The IBM Service Management Unite V1.1.2 license is included with the IBM Service Management Suite for z/OS V1.4.2 license. The installation launchpad will prompt you to accept the license agreement.

Chapter 4. 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.

The Service Management Unite Deployment Planning Checklist summarizes the planning and deployment of Service Management Unite and can be used as a reference.

Environment requirements

To successfully install and configure IBM Service Management Unite V1.1.2, your IBM Service Management Suite for z/OS V1.4.2 environment must meet certain requirements.

Your environment must include at least one system running z/OS V1.13 or later, and at least one physical or virtual image of Linux x86-64 or Linux on System z®. Critical prerequisite components for installing and using IBM Service Management Unite include WebSphere Application Server and Jazz™ for Service Management with Dashboard Application Services Hub (DASH). Refer to "Software prerequisites" on page 9 for the complete list of requirements.

Note: Installing multiple Service Management Unite instances on one server is not supported.

IBM Service Management Unite V1.1.2 supports these IBM Service Management Suite for z/OS V1.4.2 components:
- System Automation for z/OS 4.1.0
- System Automation for z/OS 3.5.0 (with APAR OA51668 installed)
- OMEGAMON® Performance Management Suite for z/OS 5.4.1 (which includes IBM Tivoli® Monitoring infrastructure)
- NetView® for z/OS 6.2.1
- Tivoli Asset Discovery for z/OS 8.1
- IBM Operations Analytics - Log Analysis 1.3.1

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 registry to use with IBM Service Management Unite.

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

Supported operating systems

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

The following table lists the operating systems that are supported for IBM Service Management Unite Automation, including the local agentless adapter.

Table 2. Supported operating systems for IBM Service Management Unite

Operating system	IBM System x[1]	IBM System z
SUSE Linux Enterprise Server 11 (64 bit)	X	X
SUSE Linux Enterprise Server 12 (64 bit)[3]	X	X
Red Hat Enterprise Linux 5 (64 bit)[2]	X	X
Red Hat RHEL Linux 6 (64 bit)	X	X
Red Hat RHEL Linux 7 (64 bit)	X	X

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 higher.
- Service Pack levels of the listed Red Hat version or higher.

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 higher are also supported. However, the live migration functionality provided by this hypervisor is not supported.
2. The supported minimum level is Red Hat Enterprise Linux 5.6.
3. 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 higher.

Supported web browsers and mobile OS in DASH

IBM Service Management Unite V1.1.2 is supported using various web browsers and mobile devices

For specific web browser support in Service Management Unite and Dashboard Application Services Hub (DASH), refer to: http://www.ibm.com/support/docview.wss?uid=swg21652158.

Hardware requirements

Before you begin installation and configuration, be sure you have identified and addressed any required hardware prerequisites.

Memory

Make sure you have enough memory available on the server to install IBM Service Management Unite.

The minimum required memory (RAM) is 4 GB or more to install WebSphere Application Server and IBM Service Management Unite on the same server. For

large environments, it is recommended to have a system with 8 GB RAM. If you start to install IBM Service Management Unite, a memory check is automatically processed. If the server provides less than 4 GB operational memory, a warning is displayed.

Disk space

Make sure that enough disk space is available for the installation.

At least 6 GB is required to install IBM Service Management Unite. 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, enter the following commands:

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

The prerequisites scanner prints the expected disk space and other prerequisites.

TCP/IP connectivity

It is required to install several products to run IBM Service Management Unite. Some of these products require TCP/IP connections.

You can install WebSphere Application Server and Service Management Unite Automation on one server or on different servers, depending on your architecture.

Provide TCP/IP connections between the following products and IBM Service Management Unite components:

- WebSphere Application Server and the resource adapters

Software prerequisites

Prerequisite software must be installed in your IBM Service Management Suite for z/OS V1.4.2 environment before you install and configure IBM Service Management Unite V1.1.2. Prerequisite checks are run automatically at various points in the installation process.

Table 3. Software prerequisites for installing and configuring IBM Service Management Unite V1.1.2

Prerequisite / Requirement	Automation / Performance Management	Location
IBM Service Management Suite for z/OS V1.4.2	Both	Shopz: http://www.ibm.com/software/shopzseries/ShopzSeries_public.wss
Jazz for Service Management V1.1.2.1 or V1.1.3 (JazzSM) Note:Dashboard Application Services Hub (DASH) is a prerequisite service included with JazzSM. Make sure that you tick DASH V3.1.2.1 or V3.1.3 when you install JazzSM.	Both	IBM Service Management Unite download page: https://www.ibm.com/marketing/iwm/iwm/web/preLogin.do?source=swg-ibmsms [1]

Table 3. Software prerequisites for installing and configuring IBM Service Management Unite V1.1.2 (continued)

Prerequisite / Requirement		Automation / Performance Management	Location
WebSphere® Application Server V8.5.5.x for Linux Multilingual - OR - WebSphere Application Server V8.5.5.x for Linux on System z® [2] Note:Make sure you also tick WebSphere Application Server SDK V1.7 during your installation, which is included with WebSphere® Application Server V8.5.5.		Both	IBM Service Management Unite download page: https://www.ibm.com/marketing/iwm/iwm/web/preLogin.do?source=swg-ibmsms [1]
Korn shell		Automation	
Tivoli Enterprise Portal Server and IBM Operations Analytics - Log Analysis v1.3.1 integration enabled in PARMGEN		Performance Management	http://www.ibm.com/support/docview.wss?uid=swg21696831
IBM Tivoli Monitoring V6.3.0 Fix Pack 6 (includes IBM Tivoli Monitoring Data Provider)		Performance Management	Fix Pack 6: http://www.ibm.com/support/docview.wss?uid=swg24040390
Tivoli Directory Integrator (TDI) V7.1.1 - Fix Pack 4 or higher		Performance Management	TDI 7.1.1.5 installation package is included with JazzSM V1.1.3
OMEGAMON XE for z/OS and IBM Operations Analytics - Log Analysis V1.3.1 integration PTFs for the following agents	OMEGAMON XE for WebSphere MQ Monitoring	Performance Management	http://www.ibm.com/support/docview.wss?uid=swg1OA46839
	OMEGAMON XE for WebSphere Message Broker Monitoring	Performance Management	http://www.ibm.com/support/docview.wss?uid=swg1OA46840
	OMEGAMON XE for Storage	Performance Management	http://www.ibm.com/support/docview.wss?uid=swg1OA46871

Note:

1. To access the download link, ensure that you already have an IBM ID. If you don't have one, access the following link for registration: https://www.ibm.com/account/us-en/signup/register.html?Target=https://myibm.ibm.com/. You also need the access key, which is supplied with the IBM Service Management Suite for z/OS V1.4.2 on a CD titled "Accessing IBM Service Management Unite".

2. The minimum fixpack level for DASH 3.1.2.1 is WebSphere Application Server V8.5.5.4.

   The minimum fixpack level for DASH 3.1.3 is WebSphere Application Server V8.5.5.9.

Software to access product data

Accessing product data in IBM Service Management Unite V1.1.2 requires installing and configuring the applicable support software.

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

- System Automation for z/OS end-to-end Adapter
- System Automation for Multiplatforms Adapter
- System Automation Application Manager Remote Agentless Adapter

To make product data available to Service Management Unite Performance Management, you must install OMEGAMON z/OS agents for the following product versions, as applicable to your environment:

- IBM Tivoli Composite Management for Application Diagnostics v7.1.03 FP8, or later
- IBM Tivoli OMEGAMON XE for CICS® on z/OS v5.3.0
- IBM Tivoli OMEGAMON XE for DB2® PE and PM on z/OS v5.3.0
- IBM Tivoli OMEGAMON XE for IMS on z/OS v5.3.0
- IBM Tivoli OMEGAMON XE for Messaging for z/OS v5.3.0
- IBM Tivoli OMEGAMON XE on z/OS v5.3.0 with PTF UA80391 Fix Pack, 5.3.0-TIV-KM5-FP0003
- IBM Tivoli OMEGAMON XE on Mainframe Networks v5.3.0
- IBM Operations Analytics - Log Analysis v1.3.2
- IBM Tivoli Netview for z/OS Enterprise Management Agent V6.2.1

Running commands and using canzlog in IBM Service Management Unite V1.1.2 requires NetView for z/OS 6.2.1.

Jazz for Service Management and WebSphere Application Server

Jazz for Service Management and WebSphere Application Server are software prerequisites that you must install before you install Service Management Unite. Before you install or update Jazz for Service Management, refer to the technotes and readme information for Jazz for Service Management. Technotes provide information about late-breaking issues, limitations, and fixes.

The following JazzSM pages are available online resources:

1. Jazz for Service Management Version 1.1.2.1 Readme: http://www.ibm.com/support/docview.wss?uid=swg24040447
2. Jazz for Service Management Version 1.1.3.0 Readme: http://www.ibm.com/support/docview.wss?uid=swg24042190
3. Jazz for Service Management Version 1.1.2.1 Technotes: http://www.ibm.com/support/search.wss?q=jazzsm1121relnotes (Click the **Newest first** link for the most recent posts.)
4. Jazz for Service Management Version 1.1.3.0 Technotes: http://www.ibm.com/support/search.wss?q=jazzsm1130relnotes (Click the Newest first link for the most recent posts.)
5. Jazz for Service Management developerWorks: http://www.ibm.com/developerworks/community/blogs/69ec672c-dd6b-443d-add8-bb9a9a490eba?lang=en

To install Jazz for Service Management and WebSphere Application Server , refer to "Installing Jazz for Service Management and WebSphere Application Server as root" on page 16.

Installation tools

The following installation tools are provided with IBM Service Management Suite for z/OS V1.4.2 for installing and configuring IBM Service Management Unite V1.1.2.

Service Management Unite launchpad

Use the Service Management Unite launchpad as the starting point for installing and configuring Service Management Unite. The launchpad.sh file is located under the directory where the Service Management Unite installation .tar file has been expanded.

The launchpad takes you through verifying your prerequisites and launching the installers for Service Management Unite Automation (InstallAnywhere) and Service Management Unite Performance Management (IBM Installation Manager).

InstallAnywhere

InstallAnywhere is included in Service Management Unite and is invoked from the Service Management Unite launchpad to install and configure Service Management Unite Automation.

Start InstallAnywhere from the Service Management Unite launchpad (launchpad.sh in your product package). From the launchpad, click on **Installing** > **Service Management Unite Automation**. Use InstallAnywhere to install and configure system automation tools.

IBM Installation Manager

IBM Installation Manager is included in Service Management Unite and is invoked from the Service Management Unite launchpad to install and configure Service Management Unite Performance Management.

IBM Installation Manager can be used in a GUI or can be started from the command line in silent mode with installation values supplied from an input file.

- To start IBM Installation Manager in silent mode, see Silent mode installation .
- To use the GUI, start IBM Installation Manager from the Service Management Unite launchpad. From the launchpad, click on **Installing** > **Service Management Unite Performance Management wizard**.

The installation process requires that it runs under a user ID with administrative authority. **root** is the recommended user.

Preinstallation checklist

Use this checklist to organize the required information for installing IBM Service Management Unite V1.1.2.

Compile the following information before you begin the installation process:

__ 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.

__ Verify the location and password for the WebSphere Application Server default root certificate key store and the node default key store.

__ Verify the key store, trust files, and passwords for Tivoli Directory Integrator (TDI) V7.1.1 Fix Pack 4. Also confirm the Tivoli Directory Integrator solution service directory and that the Tivoli Directory Integrator server is enabled as a system service.

__ Verify the installation credentials, server location, and port number for IBM Operations Analytics for z Systems if you use.

___ Verify the IBM Tivoli Monitoring, Tivoli Enterprise Monitoring Server, and Tivoli Enterprise Portal Server locations and the user IDs and passwords for each.

___ Determine the Service Management Unite Automation installation directory, if you don't want to use the default path `opt/IBM/smsz/ing`.

___ Determine the IBM Installation Manager installation directory, if you don't want to use the default path.

___ Determine whether any Tivoli Common Directory setup and whether another product uses it.

___ If remote DB2 is to be used for Service Management Unite Automation, determine the DB2 JDBC driver path, the DB2 instance host name, the DB2 instance port number, the database instance owner name and password.

___ Determine the functional user ID to be used for Service Management Unite Automation internally.

___ Determine the Service Management Unite Automation Administrator user ID.

Chapter 5. Installing and uninstalling

This information provides the following topics to help you install and uninstall Service Management Unite and related software prerequisites.

Installing and uninstalling SMU Automation

Installing Service Management Unite Automation requires meeting the prerequisites, installing the required and optional software, and running the Service Management Unite launchpad and InstallAnywhere.

The following flowchart guides you through the installation process of Service Management Unite Automation. Complete the steps as applicable and skip the steps that you don't need.
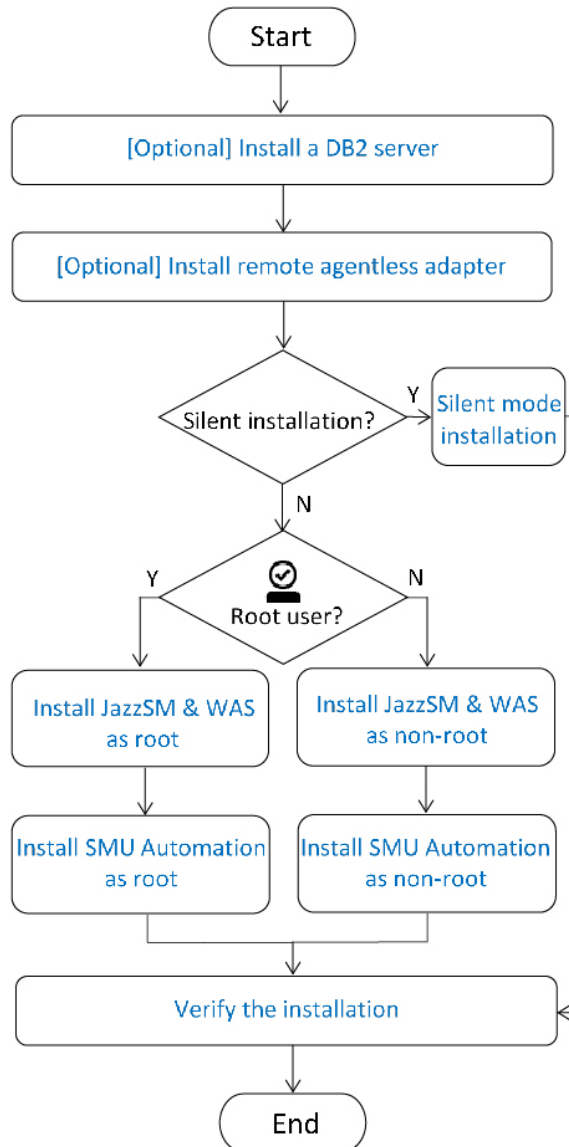
Installing Jazz for Service Management and WebSphere Application Server

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.

Installing Jazz for Service Management and WebSphere Application Server as root

If you haven't installed Jazz for Service Management and WebSphere Application Server on the server, complete the following steps to install software prerequisites using the root authority.

Procedure

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 1.1.0.2 including Installation Manager:
   - AIX: `JAZZ_FOR_SM_1.1.0.2_FOR_AIX_ML.zip` (`CISZ2ML.zip`)
   - Linux: `JAZZ_FOR_SM_1.1.0.2_FOR_LINUX_ML.zip` (`CISZ3ML.zip`)
   - Linux on System z: `JAZZ_FOR_SM_1.1.0.2_LINUX_SYS_Z.zip` (`CISZ4ML.zip`)

   WebSphere Application Server Version 8.5.0.1:
   - AIX: `WAS_V8.5.0.1_FOR_JAZZSM_AIX_ML.zip` (`CIES5ML.zip`)
   - Linux: `WAS_V8.5.0.1_FOR_JAZZSM_LINUX_ML.zip` (`CIES6ML.zip`)
   - Linux on System z: `WAS_V8.5.0.1_FOR_JAZZSM_LINUX_Z_ML.zip` (`CIES7ML.zip`)

3. Install Jazz SM 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 as documented in Middleware software requirements. For more information about JAZZ for Service Management prerequisites, see Hardware and software requirements.

   b. The Installation Manager window opens. Select the following packages to be installed:
      - IBM Installation Manager Version 1.6.1
      - IBM WebSphere Application Server Version 8.5.0.1
      - IBM WebSphere SDK Java Technology Edition Version 7.0.2.0
      - Jazz for Service Management extension for IBM WebSphere 8.5 Version 1.1.0.1
      - IBM Dashboard Application Services Hub Version 3.1.0.2

   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. Important: On the Features window, expand **IBM WebSphere Application Server 8.5.0.1 > IBM WebSphere SDK for Java Technology Edition 6** and select **IBM 32-bit WebSphere SDK for Java**.

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

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

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

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

4. Important: Activate the 32-bit version of Java 7 for the WebSphere Application Server profile:

```
<was_root>/bin/managesdk.sh -enableProfile -sdkName 1.7_32 -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.

Results

You are now ready to install System Automation Application Manager using its own installer.

Installing Jazz for Service Management and WebSphere Application Server as non-root

By default, the IBM WebSphere Application Server that hosts IBM Service Management Unite runs as root. However, it can also be installed and run by using a non-root user ID. In that case, Service Management Unite 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`.

[Optional] Planning for the agentless adapter

Decide if you want to install the local or remote agentless adapter.

Installation for the local agentless adapter and remote agentless adapters is performed in different ways. The local agentless adapter is automatically installed together with the IBM Service Management Unite Automation product as described in "Installing SMU Automation" on page 29. You can install remote agentless adapters on systems other than the system where IBM Service Management Unite is installed. Only one instance of the agentless adapter can be installed on any remote node on Linux systems.

For more information, refer to "Tuning the number of domains and resources of agentless adapters" on page 65.

Supported target operating systems
You can install the remote agentless adapter on various Linux operating system versions.

The operating system versions that are supported by the local agentless adapter are identical to the operating systems versions that are supported by IBM Service Management Unite. Refer to "Supported operating systems" on page 7 for the corresponding list.

For a list of operating systems where remote applications that are managed by an agentless adapter may run, see "Supported operating systems for non-clustered nodes managed by the agentless adapter."

Supported operating systems for non-clustered nodes managed by the agentless adapter:

The agentless adapter manages non-clustered nodes on various versions of Windows, AIX, Linux, Solaris, z/OS, and HP-UX operating systems.

Remote applications managed by the agentless adapter via remote protocols such as SSH can be located on one of the following supported operating systems:

Table 4. Supported operating systems

Operating system	IBM System x[1], [2]		Power Systems™[2]	IBM System z[2]	Other platforms[2]
	32 bit	64 bit			
Windows Server 2008	x	x			IA64
Windows Server 2008 R2		x			IA64
Windows 7	x	x			
Windows 8	x	x			
Windows Server 2012		x			
Windows Server 2012 R2		x			
AIX® 6.1	x	x	x		
AIX 7.1	x	x	x		
SLES 11.0	x	x			
Red Hat RHEL Linux 5	x	x	x	x	IA64
Red Hat RHEL Linux 6	x	x	x	x	IA64
Red Hat Desktop 5.0	x	x			
Red Hat Desktop 6.0	x	x			
SOLARIS 10	x	x			SPARC
z/OS V1.13 or later[3]				x	
HP-UX 11i	x	x			PA-RISC, IA64
IBMi 7.1					

Note:

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

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

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

2. Secure communications with targets, using SSH Protocol (SSH version 2), requires the use of:

   - OpenSSH 3.6.1 or higher
   - AIX targets: OpenSSH 4.7
   - z/OS targets: OpenSSH 3.8.1
   - SSH packages from other vendors, or earlier versions, are not supported.

3. 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 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.

Required settings for target machines that host `IBM.RemoteResource` resources

The agentless adapter uses the IBM Remote Execution and Access (RXA) technology to start, stop, and monitor resources on remote nodes. This topic describes the RXA requirements that must be fulfilled by remote nodes that host the resources defined for an agentless adapter domain. These nodes are referred to as target-nodes.

Note: Many RXA operations require access to resources that are not generally accessible by ordinary user accounts. Therefore, for all target platforms, the account names that you use to log onto remote machines must have administrative privileges on each target machine.

Windows targets:

Some IBM Remote Execution and Access (RXA) operations rely on VBScript and Windows Management Instrumentation (WMI) calls to execute scripts on Windows targets.

Windows protocol methods do not work if:
- Windows Scripting Host (WSH) or the WMI service is disabled on the target.
- VBScript is otherwise disabled.

If you intend to access Windows targets using SMB protocol over NetBIOS, which is determined by `setSMBTransportType()` :
- Port 139 or the port specified by `setNetBIOSPort()`, must not be blocked by firewalls or IP security policies.
- **Enable NetBIOS over TCP/IP** must be selected in the Control Panel settings for the machine's network connections properties. To enable NetBIOS over TCP/IP, select: **Control Panel –> Network and Dial-Up Connections –> <some connection> --> Properties –> Internet Protocol (TCP/IP) –> Advanced –> WINS –> Enable NetBIOS over TCP/IP**.

Consult the documentation for your firewall to ensure that these ports are not blocked for inbound requests. To determine if security policies are blocking these ports, select: **Start –>Settings –> Control Panel –> Administrative Tools**.

Depending on whether your policies are stored locally or in Active Directory, the next steps are as follows:
- Locally stored policies: Select **Administrative Tools –> Local Security Policy –> IP Security Policies on Local Computer**.
- Policies stored in Active Directory: Select **Administrative Tools –> Default Domain Security Settings –> IP Security Policies on Active Directory Administrative Tools –> Default Domain Controller Security Settings –> IP Security Policies on Active Directory**

Examine the IP security policies, and edit or remove filters that block the ports listed above. The following list contains the ports reserved for NetBIOS. Ensure that all ports currently used by RXA are not blocked.

```
Port
Number Use
135 NetBIOS Remote procedure call. At this time, RXA does not use this port.
```

```
137 NetBIOS Name service
138 NetBIOS Datagram. At this time, RXA does not use this port.
139 NetBIOS Session (file/print sharing)
445 CIFS (On XP and Win2K)
```

Before you access Inter Process Communications share (IPC$), make sure the server service has been started: Select **Control Panel –> Administrative Tools –> Services –> Server**. RXA requires that **Simple File Sharing** is disabled.

Windows Server 2008

On Windows Server 2008 you might need to disable **User Account Control** if your account is not a domain user account.

The *User Account Control* feature of Windows Server 2008 requires you to run several steps before RXA applications can communicate with Vista targets.

If you have a domain user account, ensure that the local and the target machine are both members of a Windows domain.

If you are a member of a local administrators group and you use a local user account, complete the three steps to be able to run administrative tasks on the target machine:

Step 1.
    Enable the built-in Administrator account and use it to connect. To enable the built-in Administrator account, open the **Windows Control Panel** and select **Administrative Tools –> Local Security Policy –> Security Settings –> Local Policies –> Security Options**. Then double-click **Accounts: Administrator account status** and select **Enable**.

Step 2.
    Disable **User Account Control** if a different Administrator user account is used to connect to the Vista target. To disable **User Account Control**, open the Windows Control Panel and select **Administrative Tools –> Local Security Policy –> Security Settings –> Local Policies –> Security Options**. Then double-click **User Account Control**: Run all administrators in **Admin Approval Mode** and select **Disable**. Reboot your system.

Step 3.
    Disable **User Account Control** when you administer a workstation with a local user account (Security Account Manager user account). Otherwise, you do not connect as a full administrator and are not able to perform administrative tasks. To disable **User Account Control**, run the following tasks:

    1. Select **Start –> Run**, type `regedit` and then press **ENTER**.
    2. Locate and then select the following registry subkey:
       `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`
    3. If the `LocalAccountTokenFilterPolicy` registry entry does not exist, follow these steps:
        a. On the **Edit** menu, point to **New**, and click `DWORD Value`.
        b. Type `LocalAccountTokenFilterPolicy` and press **ENTER**.
        c. Right-click `LocalAccountTokenFilterPolicy` and then select **Modify**.
        d. In the Value data box, type **1** and click **OK**.
        e. Restart your computer.

Alternatively, you can manually modify the registry entry by typing the following on the command line:

```
cmd /c reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system
/v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
```

Windows 7

On Windows 7, the default start-up type for the *Remote Registry* service is manual. The *Remote Registry* service must be running to enable RXA.

To check whether the *Remote Registry* service is enabled and started:

Step 1 Go to **Start –> Run**.

Step 2 Type `services.msc` and press **ENTER**.

Step 3 When the Microsoft Management Console starts, ensure that the service status is started. If not, right-click **Remote Registry** and click **Start**. To avoid problems with the manual start up, set the **Remote Registry** service start-up type to **automatic**.

Complete the following steps if you want to automatically start the service after the server boot:

1. Right-click **Remote Registry** and select **Properties**.
2. In the **Start-up type** option, choose **Automatic**.
3. Click **Apply** and **OK**.

When the system starts, **Remote Registry** starts automatically.

Unix and Linux targets:

IBM Remote Execution and Access (RXA) does not supply SSH code for UNIX machines. Ensure SSH is installed and enabled on any target you want to access using SSH protocol.

OpenSSH 3.7.1 or higher contains security enhancements not available in earlier releases. Remote Execution and Access 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 RXA 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
    ```

In order to use SFTP for file transfers, in addition to calling `SSHProtocol.setUSESFTP(true)`, make sure that the SFTP server is enabled on the target machine. Note that the location of the `sftp-server` is OS dependent. It is typically found in the following locations:

- Solaris: `/usr/lib/ssh/sftp-server`
- Linux: `/usr/libexec/openssh/sftp-server`

- HP-UX: /opt/ssh/libexec/sftp-server
- AIX: /usr/sbin/sftp-server

The sshd_config file contains a line similar to the one below. Make sure the line that enables the sftp-server subsystem is not commented out, and that it points to the OS-specific location of the sftp-server subsystem. For example:

Subsystem sftp /one_of/the_paths/shown_above

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.

Supported versions of IBM Tivoli Monitoring (ITM) used by adapters

You can use the agentless adapter to integrate resources that are monitored by IBM Tivoli Monitoring or by Composite Application Manager. These Tivoli Monitoring managed resources are integrated by using existing Tivoli Monitoring agents. The agentless adapter retrieves monitoring information from Tivoli Monitoring Agents and runs start and stop operations via these agents.

At a minimum, IBM Service Management Unite requires IBM Tivoli Monitoring V6.3.0 fix pack 6.

Note: If you are installing only Service Management Unite Automation, you can use Tivoli Monitoring 6.2 and later.

The following types of Tivoli Monitoring agents can be integrated:
- Application agents (also referred to as non-OS agents) and custom agents
- OS agents

Service Management Unite Automation provides predefined templates for the integration of the following agents:
- Apache Web Server
- WebSphere Application Server
- DB2
- Custom agents that are built with the Tivoli Monitoring Agent Builder
- Linux OS Agent
- UNIX OS Agent

[Optional] Installing and uninstalling the remote agentless adapter

This section introduces how to install and uninstall the remote agentless adapter.

Accessing the installation package

The remote agentless adapter is part of IBM System Automation Application Manager and is available on the IBM software download site of IBM Service Management Unite.

Electronic distribution

There is a separate electronic deliverable for each supported operating system. The following table lists the archives that you need to install the remote agentless adapter.

Table 5. Archive files of the electronic deliverable

Operating system	Archive name	Description
Linux on System x®	SA_AM_ 4.1_RemoteClient_LinSysX.tar	To extract the archive, GNU tar 1.13 or later is required. Use the tar -xf command to extract the files to a temporary directory.
Linux on System z®	SA_AM _4.1_RemoteClient_LinSysZ.tar	To extract the archive, GNU tar 1.13 or later is required. Use the tar -xf command to extract the files to a temporary directory.

After extracting the archive, the directory structure is created.

Table 6. Directory Structure of the Remote Agentless Adapter after extracting

Operating system	Installation wizard file
Linux on System x®	EEZ4101Remote/I386/ALAdapt/setup.bin
Linux on System z	EEZ4101Remote/S390/ALAdapt/setup.bin

Installing the remote agentless adapter

Use the installation wizard to install the remote agentless adapter on Linux systems.

About this task

The installation wizard files are located either on the product DVD of System Automation Application Manager or in the directory of the IBM® Service Management Unite download site that is created as a result of extracting the electronic deliverable archive file for the respective operating system.

Procedure

1. Log on to the system where you want to install the remote agentless adapter with a user ID that has administrator authority. This user ID is typically root.
2. Change to the directory that contains the installation program.
3. Run the following command to launch the installation wizard.

   ./setup.bin
4. The wizard is started, click **OK** to display the Welcome window. The language is detected automatically on your computer, or you can select it on the Welcome window. To launch the installation wizard to generate a response file, use the following command:

   <installation_wizard> -Dpreparesilent=true.The following response file is generated:

   <install_root>\install\install.properties.Click **Next** on the Welcome window to display the license agreement.

5. Select **I accept both the IBM and the non-IBM terms to agree to the license agreement**. Click **Next** to display the installation directory window.
6. The installation directory is displayed, and the default directory can't be changed. Click **Next** to display the Tivoli Common Directory window.
7. If the Tivoli Common Directory is not detected on your system, the default location is displayed and can't be changed if the server is Linux system. On other systems, you can specify a different directory. If a Tivoli Common Directory is detected on your system, you can't change the directory that is displayed. Click **Next** to display the preinstall summary.
8. Review the displayed information, and click **Install** to start the installation process. While the adapter is being installed, a progress window is displayed.
9. When the installation is complete, an installation summary window is displayed, on which you can verify the success of the installation. If problems occur, check the applicable installation log files for more information. Click **Done** to exit the installation wizard.

What to do next

For more information about how to configure the remote agentless adapters, refer to Configuring remote agentless adapters.

Uninstalling the remote agentless adapter

An uninstallation program is provided to remove the adapter that was installed by the installation wizard.

Before you begin

If you want to uninstall the remote agentless adapter, you need the same authorization as described in Installing the remote agentless adapter for an initial installation.

To determine the status of the adapter, run the following command:

`eezaladapter status`

If the adapter is still running, issue the command to stop the adapter before you start the uninstallation process:

`eezaladapter stop`

About this task

During uninstallation, you might be prompted to confirm that specific files are to be deleted. Make sure that the correct files are listed before you confirm the deletion.

Procedure

1. To start the uninstallation program, issue the following command:
   `EEZ_INSTALL_ROOT/uninstall/uninstall`.
2. The uninstallation program is started in the same language as used for the installation. On the Welcome window, click **Next** to display the pre-uninstallation summary.
3. Review the displayed information, and click **Uninstall** to start the uninstallation process.

   The wizard removes the remote agentless adapter from your system without removing the configuration files.

4. When the uninstallation is completed, the uninstallation summary is displayed. If problems occur, check the applicable installation log files for more information. Click **Done** to close the uninstallation wizard.

Installing and uninstalling service for the remote agentless adapter

Installing service means applying corrective service fix packs to release 4.1 of the IBM System Automation Application Manager remote agentless adapter. The service fix packs that you use for updating a remote agentless adapter are referred to as product fix packs.

Before you begin

To install a product fix pack, you need to meet the following requirements:
- Product fix packs are always cumulative.
- Release 4.1 must be installed before any product fix pack can be installed.
- To install a product fix pack, you must have root authority.

Product fix packs and interim fixes are delivered as archives in TAR-format for Linux.

Where to obtain fixes:

The fix packs are available at Tivoli System Automation Application Manager 4.1.0 Support page. The fix packs provide the links to the product related archives.

Archive naming conventions:

The archives to upgrade a remote agentless adapter from version 4.1 have the following syntax:

`4.1.0-TIV-SAAMR-<platform>-FP<fix_pack_number>.<archive_type>`

- `<platform>`: Represents the platform on which the remote agentless adapter is installed.
- `<fix_pack_number>`: Represents the fix pack number.
- `<archive_type>`: Represents the platform-specific file extension of the archive.

Usage instructions for the platform-specific archives:

These are the archives for applying service to the remote agentless adapter.

Table 7. Archives for applying service to remote agentless adapter

Operating system	Archive name	Description
Linux on System x	`4.1.0-TIV-SAAMR-I386-FP<fix_pack_number>.tar`	To extract the archive, GNU tar 1.13 or later is required. Use the `tar -xf` command to extract the files. This is where you find the update installer program after unpacking the product fix pack archive: `EEZ41<mf>Remote/I386/ALAdapt/setup.bin`

Table 7. Archives for applying service to remote agentless adapter (continued)

Operating system	Archive name	Description
Linux on System z	`4.1.0-TIV-SAAMR-S390-FP<fix_pack_number>.tar`	To extract the archive, GNU tar 1.13 or later is required. Use the `tar -xf` command to extract the files. This is where you find the update installer program after unpacking the product fix pack archive: `EEZ41<mf>Remote/S390/ALAdapt/setup.bin`

Procedure

1. To **install** service for the remote agentless adapter, complete the following steps:

   a. Check the release notes to find out which archives are required.

   b. Check the release notes to find out which archives are required.

   c. Download the archives for product fix packs from the System Automation Application Manager support site to a temporary directory.

   d. Extract the product fix pack archive to a temporary directory, and check the release notes for additional or deviating installation instructions.

   e. Change to the directory in which the update wizard program is located and launch the update wizard. The same authorization is required as described in "Installing the remote agentless adapter" on page 24.

   f. Follow the instructions on the wizard panels to install the product fix pack. The steps that you have to perform are the same as described for the initial installation.

2. To **uninstall** service for the remote agentless adapter, complete the following steps:

   If you want to uninstall service, you need to uninstall the complete remote agentless adapter as described in Uninstalling the remote agentless adapter. Then you can reinstall to the level required.

[Optional] Installing a DB2 server

You can either install a DB2 server, or use the embedded Derby database in your Service Management Unite environment.

Installing a DB2 server

You can use the typical installation of a single-partition database environment.

Create a DB2 instance before you install IBM Service Management Unite. Make sure that the DB2 server meets the required version level.

On a 64-bit operating system, the following link must exist in the home directory of the DB2 instance owner:

`/home/<db2 instance name>/sqllib/lib64/libdb2tsa.so`

If this link does not exist, use the following command to create the link:

```
ln -s /home/<db2 instance name>/sqllib/lib64/libdb2tsa.so.1
  /home/<db2 instance name>/sqllib/lib64/libdb2tsa.so
```

Installing the JDBC driver for setting up a remote DB2 database

Depending on which operating system the remote DB2 is installed on, you need the following files:

- DB2 for Linux, or AIX:
  - `db2jcc.jar`
  - `db2jcc_license_cu.jar`: License file for DB2 for Linux, or AIX

  You can find these files in the `<DB2_install_home>/sqllib/java` directory.
- DB2 for z/OS
  - `db2jcc.jar`
  - `db2jcc_license_cisuz.jar`: License file for DB2 for z/OS

  You can find these files in the subdirectory `classes` or `jcc/classes` of the DB2 JDBC installation directory in the HFS.

  Note: The **IBM DB2 driver for JDBC and SQLJ** needs to be installed separately, after you have installed DB2 for z/OS.

You have the following options to install the JDBC driver:
- Create a new folder. Copy the files listed above into this folder. Point the installer to the directory as described in "Starting the SMU Automation installer" on page 31.
- Use the WebSphere JDBC driver: Copy the appropriate `.jar` files into the directory `<was_home>/universalDriver/lib`, if not already available. Point the installer to the directory as described in "Starting the SMU Automation installer" on page 31.
- Use the DB2 runtime client JDBC driver: Point the installer to the directory with the appropriate `.jar` files as described in "Starting the SMU Automation installer" on page 31.

AIX® or Linux: Creating the automation database and the database tables

You need to create the automation database, and also create the automation tables in the database on DB2® server system. If your DB2® server runs on Linux or AIX, perform the following steps.

Procedure

1. Log into the system as root.
2. Copy the shell scripts located in the IBM® Service Management Unite`<EEZ_INSTALL_ROOT>/DDL/Script` directory to your host DB2 system.
3. Run the following shell scripts:

   db2_create_automgr_db.sh \<db_name\> \<instance_owner\> \<instance_pwd\> \<script_directory\>

   db2_create_reporting_tables.sh \<db_name\> \<instance_owner\> \<instance_pwd\> \<script_directory\>

   where
   - `<db_name>` is the desired name of the automation manager database.

     Example: EAUTODB
   - `<instance_owner>` is the instance owner user ID of the DB2 instance.

     Example: db2inst1
   - `<instance_pwd>` is the password of the instance owner user ID.
   - `<script_directory>` is the directory where you copied the DB2 scripts for System Automation to in step 2 (/DDL/Script).
4. Issue the following commands to verify that the remote database is created correctly:

a. Log on as DB2 instance owner.

b. `db2 connect to <db_name>`

c. `db2 list tables for schema eautousr`

d. `db2 disconnect <db_name>`

The output of the `list tables` command displays the following table names:

```
EEZAUTOMATIONACCESS
EEZAUTOMATIONRELATION
EEZCOMMONEVENTS
EEZDOMAINSUBSCRIPTION
EEZNODE
EEZOPERATORDOMAINFILTER
EEZOPERATORDOMAINPREFERENCES
EEZOPERATORHIDDENDOMAIN
EEZPERSISTENTREQUEST
EEZRESOURCESUBSCRIPTION
EEZSAFOSEVENTS
```

z/OS: Creating the automation database and the database tables

If you have a DB2 server system that runs on z/OS, adjust and run the following jobs.

Procedure

1. Adjust and run the following jobs. They are provided in the extracted directory DDL/DB2 of your Service Management Unite Automation installation.

   ATVED100

   This job creates a DB2 table space, tables, and index entries.

   ATVED10C

   This job deletes the objects created by job ATVED100.

   Follow the instructions within the jobs to adjust them to your environment.

   Note:

   a. Make sure that DB2 is active before submitting the jobs.

   b. Before rerunning job ATVED100, run job ATVED10C to cleanup the table space and tables defined by the previous run.

   c. The user ID under which these jobs are submitted must have DB2 SYSADM (system administrator) authority.

2. Issue the following commands to verify that the remote database is created correctly:

   a. Ensure that DB2 is running.

   b. Invoke the DB2 Administration Tool from TSO.

   c. Select the DB2 that is hosting the Service Management Unite Automation tables.

   d. Invoke the DB2 System Catalog function (option **1**).

   e. Navigate to Databases (option **D**).

   f. Select EAUTODB (or whatever name you have chosen) and specify option **T**.

   The tables listed are displayed.

Installing SMU Automation

The following instructions describe how to install Service Management Unite Automation using InstallAnywhere.

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 8. 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`

Non-root installation

To install Service Management Unite Automation using a non-root user, ensure that you've installed Jazz for Service Management and WebSphere Application Server using the same non-root user ID that Service Management Unite Automation uses. For more information, refer to "Installing Jazz for Service Management and WebSphere Application Server as non-root" on page 17.

Before you begin

If you plan to install IBM Service Management Unite Automation and want to use the Agentless 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 Agentless 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 IBM Service Management Unite 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 Service Management Unite using the non-root user ID that you also used for installing the WebSphere Application Server runtime environment.

2. Start the Service Management Unite Automation installer from the command line instead of using the common launchpad. For more information, see Starting the installers. On the command line, specify the **vconfig** parameter as follows:

   - Change to the directory that contains the installation program, for example,
   ```
   SMUAUTO1122X/x86_64/ or SMUAUTO1122Z/s390/
   ```
   - Start the installation by launching the installation wizard using:
   ```
   ./setup.bin -Dvconfig=true
   ```

   Note: The **vconfig** parameter is used to create the `cfg` directory below the installation root directory, for which the user has write-access, instead of using the default directory `/etc/opt/IBM`, for which your non-root user does not have write-access by default.

3. Choose an installation directory for which your non-root user has write-access during the installation, for example, a directory below the user's home directory: `/home/<user>/IBM/smsz/ing`.

   Note: If you install Service Management Unite Automation as non-root user, the shortcut to the command `cfgsmu` is not created. To open `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.

GUI mode installation

You can run a wizard-based graphical installation to install Service Management Unite Automation.

The installation comprises these phases:

1. In the preinstallation phase, you need to specify the installation parameters.
2. The installation phase begins when you click the **Install** button 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 simply starting the installer again.
3. The configuration phase, in which the necessary WebSphere Application Server and database configuration is performed. The configuration step can be canceled at any time.

Starting the SMU Automation installer:

To install Service Management Unite Automation on Linux for System z or Linux for System x, firstly you need to start the installers – InstallAnywhere.

Before you begin

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

Procedure
1. Extract the contents of the `SMUv1.1.2.x-zWebUI-xLinux.tar` file or the `SMUv1.1.2.x-zWebUI-zLinux.tar` file as appropriate into a temporary directory.
2. Either use the common launchpad to launch the Service Management Unite Automation installer or manually start the installer from the command line:
   a. Start the installer through the common launchpad:
      1) Run the launchpad.sh script. This opens a common launchpad from which the IBM Service Management Unite installers can be launched.
      2) From the main launchpad, select **Installing > Service Management Unite Automation wizard** to display a document in the launchpad that contains a link for Service Management Unite Automation. Select this link to start the installer. The installer displays a graphical interface to perform installation and configuration tasks.
   b. Start the installer from the command line:
      1) Change to the directory that contains the installation program: E.g.: `SMUAUTO1122X/x86_64/` or `SMUAUTO1122Z/s390/`
      2) Start the installation by launching the installation wizard using `setup.bin`

Installing SMU Automation via installer:

Complete the following steps to install Service Management Unite Automation. During installation, enter the data you collected. Make sure that you specify all required parameters and that your entries are correct.

Procedure
1. Start the installer either from the command line or the launchpad. To see how to start the installer, refer to "Starting the SMU Automation installer" on page 31.
2. The installation wizard is opened and the "Introduction" window is displayed. On this window, you can see the available installation options: perform an initial installation, resume a canceled or failed installation, or perform an update installation. Read the information on this window and click **Next** to proceed.
3. The Software License Agreement window is displayed. Carefully read the terms of the license agreement.

   To accept the terms of the license agreement, select **I accept the terms** and click **Next**.
4. On the Installation Directory window, specify the directory where you want to install Service Management Unite Automation or accept the default location. Click **Next**.
5. If the installation program detects a Tivoli Common Directory on your system, for example, because a Tivoli product is already installed, the directory must also be used for Service Management Unite Automation. In this case, the Tivoli Common Directory window is not displayed.

If the installation program does not detect a Tivoli Common Directory on your system, accept the default location or specify the directory to which the Tivoli log files are to be written. Click **Next**.

6. On the Database Server window, select the database environment type you are using and click **Next**.

   Which window is displayed next, depends on the type of database environment you selected:

   - **Embedded Derby database ("local"):** Proceed with step 7.
   - **IBM DB2 LUW on different system ("remote"):** Proceed with step 8.
   - **IBM DB2 for z/OS on different system ("remote z/OS"):** Proceed with step 9.

7. The **Derby on local system** window is displayed only if you using an embedded Derby database. Specify the database name or accept the default name and click **Next.** Note that any existing database with the name you specify is dropped automatically without warning. Click **Next** and proceed with step 10.

8. The **IBM DB2 Database on remote system** window is displayed only if you are using a remote DB2 setup.

   a. Specify the database name (see Creating the automation database and the database tables for setting up a remote DB2 database) and click **Next**.

   b. Specify the path to the DB2 JDBC driver or click **Choose** to select the directory (see "Installing the JDBC driver for setting up a remote DB2 database" on page 27 and Creating the automation database and the database tables for setting up a remote DB2 database), and specify the name and password of the database instance owner. Click **Next.**

      Note: InstallAnywhere checks the contents of the defined directory and displays an error message if it does not contain a JDBC driver with a valid license.

   c. In the field **DB2 server host name**, type the fully qualified host name of the system where the DB2 server is installed.

      In the field **DB2 server port**, the port number of the DB2 server must be specified. Enter port number of your DB2 on z/OS database.

      To skip the access test, select the **Skip DB2 access** check box. Click **Next**.

9. The **IBM DB2 Database on remote system on z/OS** window is displayed only if you are using a remote DB2 on z/OS setup.

   a. Enter the location information of the database that runs on z/OS and the schema name of the database. Click **Next**.

   b. Specify the path to the DB2 JDBC driver or click **Choose** to select the directory, and specify the name and password of the database instance owner. Click **Next**.

   c. In the **DB2 server host name** field, type the fully qualified host name of the system where the DB2 server is installed.

      In the **DB2 server port** field, specify the port number of the DB2 server. Enter port number **446**.

10. On the User and Group Administration window, specify whether your WebSphere has administrative access to users and groups.

    Typically, this is the case in setups with federated user repositories where you can manage users and groups via the administrative console. If you click **Yes**, the installer creates users and groups in that repository to use with Service

Management Unite Automation. If you click **No**, the installer does not make any changes to users and groups. Click **No**, if you use a central LDAP user repository and the users and groups exist in this repository. This is the case if you created them manually in the LDAP repository or if a previous Service Management Unite Automation installation created them in the same LDAP repository. For further information, refer to "Configuring an LDAP user registry (optional)" on page 86.

11. The installation directory of WebSphere Application Server is detected on your system and displayed on the WebSphere Application Server window.

    a. Click **Next.**

    b. Specify a WebSphere Application Server administrative account and password and click **Next**.

12. On the **System Automation Functional user ID** window, specify password for the functional user ID eezdmn and password for the automation framework. Do not use cut and paste to enter the password and the password confirmation. Type in the password and the password 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.

    Note: Do not choose the same name for both the System Automation functional user ID and the WebSphere Application Server administrator user ID, as this may lead to problems if you later uninstall IBM Service Management Unite Automation. For example, do not specify wasadmin for both users.

13. On the **System Automation Administration user ID** window, specify the user ID and password of the System Automation administrator. It is recommended to use eezadmin. Click **Next**.

    Note: Do not choose the same name for both the System Automation Administration user ID and the WebSphere Application Server administrator user ID, as this may lead to problems if you uninstall Service Management Unite Automation. For example, do not specify wasadmin for both users.

14. When you have specified all the required information on the installation panels, the Pre-Install Summary window is displayed. The installer checks for disk availability. If the disk space requirements are not met, installation is not possible. Click **Install** to start the installation. The installation can take up to two hours to complete. While the component is being installed and configured, information panels display the progress.

15. When the installation of Service Management Unite Automation is complete, the Installation Complete window is displayed. Click **Done** to close InstallAnywhere. For information about verifying the installation, refer to Verifying the Installation.

Silent mode installation

You can also install Service Management Unite Automation in silent mode if you have the silent input properties.

Before you begin

The silent installation is run by using a previously created silent input properties file. You can generate the `install.properties` input file in two ways:

- Run a wizard-based graphical installation using `setup.bin` with the -Dpreparesilent=true option. When the installation procedure completes, the `install.properties` file is created in the <EEZ_INSTALL_ROOT>/install subdirectory of the product installation path. When an update installation is performed, the file is read to obtain the parameters and values needed for the update process. If this file is not found, the update installation fails.

  If you want to perform a silent installation of Service Management Unite Automation on more than one system, you can take the `install.properties` file which was generated during a graphical installation, and use it on other systems of the same type. You might need to replace system-specific parameters in the file to customize it for the target system.

- You can prepare an `install.properties` file without performing a complete installation on the target system. The first part of the installation procedure gathers all the necessary parameters needed to generate the `install.properties` file. You do this by starting the graphical installer on the target system with the options **-Dpreparesilent=true** and **-Dpropertiesfileonly=true**. With these options, the installation procedure stops before the product files are copied to the product directory. The `install.properties` file is created and stored in directory /tmp.

  If you want the file to be created in a specific path, you can optionally specify **-Dpropertiesfilepath=<fully_qualified_path>**. If the specified path is incorrect, the file is saved in the default temporary directory on the system.

For example, if you want the file to be saved to /var/mydir, use the following command:

```
setup.bin -Dpreparesilent=true -Dpropertiesfileonly=true
-Dpropertiesfilepath=/var/mydir
```

Note: The option -Dpropertiesfilepath=<fully_qualified_path> can be used only if -Dpreparesilent=true and -Dpropertiesfileonly=true are also specified. You can use the `install.properties` file for a silent installation only if the -Dpreparesilent=true option is specified.

Procedure

1. Copy the input properties file `install.properties` to the system on which you want to perform the silent installation.
2. Edit the `install.properties` file and make sure that it contains all your system-specific parameters, such as host names, directories, and so on. Password parameters in the `install.properties` file do not contain any values. You must add the passwords manually to the file, or else the installation fails.
3. To start the installation, enter the following command depending on the platform you use:

   ```
   setup.bin -f <fully_qualified_properties_file_name>
   ```

   If the input file `install.properties` is found, silent installation starts. If the file is not found, the wizard-driven installation starts.

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 the uninstallation program to uninstall Service Management Unite Automation. A graphical uninstallation program is provided to remove the components that are installed.

Before you begin

- During uninstallation, a number of panels are displayed, prompting you to confirm that specific files are to be deleted. Check the files carefully before confirming the deletion.
- If you changed the user repository settings of WebSphere Application Server to an external user repository after the installation of Service Management Unite Automation component, the following change is required:

  Change the variable *EXTERNAL_USER_REP_ACTIVATE* in file `<EEZ_INSTALL_ROOT>/uninstall/installvariables.properties` to false:`EXTERNAL_USER_REP_ACTIVATE=false`.

  This prevents users and groups from being deleted in the WebSphere Application Server in a subsequent uninstallation process.

Procedure

1. Launch the uninstallation program by issueing the following command: `<EEZ_INSTALL_ROOT>/uninstall/uninstall`. This starts the uninstallation wizard.
2. Read the information on Introduction window and click **Next** to proceed.
3. Provide the requested information for the WebSphere administrative user ID and password.
4. The Start Uninstallation window is displayed. Click **Uninstall** to start the uninstallation. Some information panels are displayed while the uninstallation program checks your system for the information needed for the uninstall.
5. When the uninstallation is complete, a summary window is displayed. To exit the uninstallation program, click **Done**.
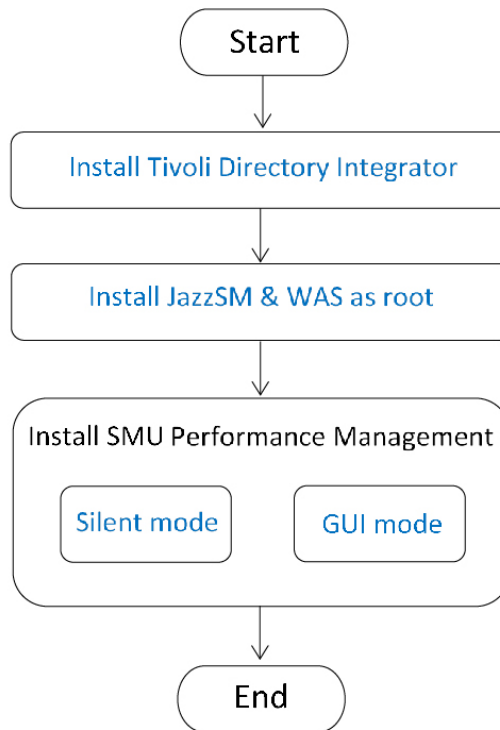
   Note: If problems were encountered during the unconfiguration step, an error window appears before the actual uninstallation step, in which the files are removed from the disk. In such a case, perform the following steps:

   a. On the error window, click **Save installation log files.**
   b. Click **Next** if you want to remove all installed files. Otherwise, click **Cancel** to perform corrective actions and then rerun the uninstallation.

Installing and uninstalling SMU Performance Management

This section introduces how to install and uninstall Service Management Unite Performance Management.

The following flowchart guides you through the installation process of Service Management Unite Performance Management.

Installing Jazz for Service Management and WebSphere Application Server as root

If you haven't installed Jazz for Service Management and WebSphere Application Server on the server, complete the following steps to install software prerequisites using the root authority.

Procedure

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 1.1.0.2 including Installation Manager:
   - AIX: `JAZZ_FOR_SM_1.1.0.2_FOR_AIX_ML.zip` (CISZ2ML.zip)
   - Linux: `JAZZ_FOR_SM_1.1.0.2_FOR_LINUX_ML.zip` (CISZ3ML.zip)
   - Linux on System z: `JAZZ_FOR_SM_1.1.0.2_LINUX_SYS_Z.zip` (CISZ4ML.zip)

   WebSphere Application Server Version 8.5.0.1:
   - AIX: `WAS_V8.5.0.1_FOR_JAZZSM_AIX_ML.zip` (CIES5ML.zip)
   - Linux: `WAS_V8.5.0.1_FOR_JAZZSM_LINUX_ML.zip` (CIES6ML.zip)
   - Linux on System z: `WAS_V8.5.0.1_FOR_JAZZSM_LINUX_Z_ML.zip` (CIES7ML.zip)

3. Install Jazz SM 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 as documented in Middleware software requirements. For more information about JAZZ for Service Management prerequisites, see Hardware and software requirements.

b. The Installation Manager window opens. Select the following packages to be installed:
   - IBM Installation Manager Version 1.6.1
   - IBM WebSphere Application Server Version 8.5.0.1
   - IBM WebSphere SDK Java Technology Edition Version 7.0.2.0
   - Jazz for Service Management extension for IBM WebSphere 8.5 Version 1.1.0.1
   - IBM Dashboard Application Services Hub Version 3.1.0.2

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. Important: On the Features window, expand **IBM WebSphere Application Server 8.5.0.1 > IBM WebSphere SDK for Java Technology Edition 6** and select **IBM 32-bit WebSphere SDK for Java**.

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

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

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

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

4. Important: Activate the 32-bit version of Java 7 for the WebSphere Application Server profile:

```
<was_root>/bin/managesdk.sh -enableProfile -sdkName 1.7_32 -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.

Results

You are now ready to install System Automation Application Manager using its own installer.

Installing Tivoli Directory Integrator server

Service Management Unite uses Tivoli Directory Integrator to integrate and incorporate data into DASH widgets.

Before you install Service Management Unite Performance Management, make sure that you have installed the Tivoli Directory Integrator server. For detailed information about how to install Tivoli Directory Integrator, refer to Installation instructions for IBM Tivoli Directory Integrator.

Note: You can only install one Tivoli Directory Integrator server on the server where Service Management Unite is installed.

Installing SMU Performance Management

The following instructions describe how to install Service Management Unite Performance Management using IBM Installation Manager.

The installation process uses WebSphere Application Server and Tivoli Directory Integrator command line utilities, which require the appropriate servers to be active for the files to be installed. The installation process will start these servers if they are inactive. The installer pages provide input fields that are needed for configuration and successful execution of the command line utilities. The following pages are pre-filled with default or discovered values:

- Tivoli Directory Integrator and Jazz for Service Management installation directories
- WebSphere Application Server server name, administrator ID, and administrator password
- Tivoli Directory Integrator solutions directory
- Parameters needed to run the Tivoli Directory Integrator command utility. These parameters are an SSL key database file location, a truststore file location, and the password for the key database file. The parameters are set to the default values included with Tivoli Directory Integrator. If your installation modified Tivoli Directory Integrator security, you might need to update these parameters.
- IBM Tivoli Monitoring, IBM Operations Analytics - Log Analysis, and System Automation properties that are used by the Tivoli Directory Integrator configuration.
- Parameters are needed for WebSphere Application Server and Tivoli Directory Integrator to exchange digital certificates. These include WebSphere Application Server certificate key store properties, Jazz for Service Management profile values and Tivoli Directory Integrator trust store values. If Tivoli Directory Integrator and WebSphere Application Server are on different systems, and the installation is running on the WebSphere Application Server system, the location of the Tivoli Directory Integrator system, and a user ID and password valid on that system must also be supplied.

GUI mode installation

You can install Service Management Unite Performance Management using GUI mode.

Starting the SMU Performance Management installer:

You can use the launchpad and IBM Installation Manager to install Service Management Unite Performance Management on Linux for System z or Linux for System x.

Before you begin

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

Note: If the Tivoli Directory Integrator server and WebSphere Application Server are installed on different systems, ensure that you meet the following requirements:
- The Service Management Unite Performance Management installation package is available on both systems.
- The Tivoli Directory Integrator system should be active and accessible from the WebSphere Application Server system.

Procedure
1. Extract the contents of the `SMUv1.1.2.x-zWebUI-xLinux.tar` file or the `SMUv1.1.2.x-zWebUI-zLinux.tar` file into a temporary directory.
2. Either use the common launchpad to launch the Service Management Unite Performance Management installer or manually start the installer from the command line:
   a. Start the installer through the common launchpad:
      1) Run the `launchpad.sh` script. This script opens a common launchpad from which the IBM Service Management Unite installer can be started.
      2) From the main launchpad, select **Installing > Service Management Unite Performance Management wizard** to display a document in the launchpad that contains a link for Service Management Unite Performance Management.
      3) Select the **IBM Service Management Unite Performance Management** link to start the installer. The installer displays a graphical interface to perform installation and configuration tasks.
   b. Start the installer from the command line:
      1) Browse to the location that contains the installation program, for example, SMUPRF1122X/im64_linux/ or SMUPRF1122Z/im64_zlinux/ (select the installation location according to your platform).
      2) Run the command to start the installation, for example,
         `./install`
      3) Select **File —>Preferences** and click on **Add repository** after the IBM Installation Manager restarts after installation.
      4) Browse to the location that you extracted the Service Management Unite tar file and navigate to the SMUPRF1122X directory. Select the `diskTag.inf` file within that directory and then click OK to add the repository and click OK to exit the Preferences menu.
      5) Click on the **Install** in IBM Installation Manager to install Service Management Unite.

Installing SMU Performance Management via installer:

Complete the following steps to install Service Management Unite Performance Management.

Procedure
1. Start the installer either from the command line or the launchpad. To see how to start the installer, refer to "Starting the SMU Performance Management installer" on page 41.
2. On the IBM Installation Manager Start page, click **Install** to start your installation.
3. On the Install Packages page, select **IBM Service Management Unite Performance Management version 1.1.2.x**. Click **Next** to continue.
4. IBM Installation Manager checks for the prerequisite packages on your computer. If your computer does not meet the prerequisites check, the **Validation Results** page shows the missing prerequisites. If all prerequisites are met, you are presented with the license agreement page.
5. On the Licenses page, select **I accept the terms in the license agreement** and click **Next**.
6. The shared resources directory location is displayed. Use the default path or you can optionally specify a path in the **Shared Resources Directory** field. The shared resources directory is the directory where installation artifacts are stored so they can be used by one or more product package groups. You can specify the shared resources directory only the first time you install a package. Click **Next**.
7. The package group name and the default installation location are shown. The **Create a new package group** option is selected by default and only this option is supported for the installation of Service Management Unite Performance Management. A package group represents a directory in which packages share resources with other packages in the same group. A package group is assigned a name automatically. Click **Next**.
8. On the Install Packages page, select **IBM Service Management Unite Performance Management 1.1.2.x**. If WebSphere (which supports DASH) and Tivoli Directory Integrator are on different systems, you can select only one of the extensions to install at a time. Click **Next**.
9. On the Features tab, under the DASH Extensions Configuration window, verify the **DASH directory location** and the **WebSphere user id**, **password**, and **Jazz Application server**. Click **Next**.
10. In the TDI Extensions Configuration window, verify the **TDI Install Directory** location, **TDI Solutions Directory** location, and **TDI command parameter** fields. Click **Next**. If Tivoli Directory Integrator is already being used to support a non-Service Management Unite Dashboard Application Services Hub configuration, specify this existing solutions directory. Only one solutions directory should be used for a Tivoli Directory Integrator-Dashboard Application Services Hub connection.
11. In the TDI Solution Properties window, verify the **Solution Properties** fields. Click **Next**. The **Solution Properties** fields can be updated after installation. For details on the properties, see Configuring properties files. Password fields do not have a default; if you are unsure of the values, enter blank spaces, and update the properties after installation.
12. In the SSL certificate exchange window, verify the **Jazz profile node directory** location, **WebSphere keystore password** for the certificate key stores found in the directory, and **Local TDI Fields**. **Note:** The **WebSphere keystore password**

field is initially set to the IBM-supplied default of "WebAS" included with WebSphere Application Server. The **Local TDI Fields** verifies the location, name, and password for a Tivoli Directory Integrator trust store file for Service Management Unite. If WebSphere and Tivoli Directory Integrator are on different systems, you must verify the location and a user ID and password for the Tivoli Directory Integrator system. Additionally, you must verify the Tivoli Directory Integrator installation and solution directory on that system.

13. Click **Next**. Preinstallation summary information is displayed, which includes the target installation location, list of packages, and repository information.

14. Verify the summary information, and click **Install**. The installation starts and a progress bar is displayed. A postinstallation summary page is displayed after installation.

15. Click the **View Log File** link to inspect the Installation Manager log. **Note:** Some warning messages regarding the failure of `tdisrvctl` commands might appear in the log. These messages can be disregarded.

16. Click **Finish**. Click **File > Exit** to exit Installation Manager.

What to do next

If WebSphere Application Server and Tivoli Directory Integrator are on different systems, check the installation manager log after WebSphere Application Server is installed and verify that no errors occur for the `configure_sl.sh` command. The script might have failed due to TCP/IP problems between the two systems. If the script did not run properly, contact IBM support for assistance in manually configuring the SSL connection.

Silent mode installation

You can install Service Management Unite Performance Management 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 Service Management Unite Performance Management 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 three response file templates and a script to install or update to install the performance management component in silent mode:

`silentInstall.xml`
> Use this template when WebSphere and Tivoli Directory Integrator are on the same system.

`silentInstall_tdi.xml`
> Use this template when WebSphere and Tivoli Directory Integrator are on different systems. This template is used for the silent installation on the Tivoli Directory Integrator system.

silentInstall_DASH.xml

> Use this template when WebSphere and Tivoli Directory Integrator are on different systems. This template is used for the silent installation on the WebSphere system.

Procedure

1. Extract the contents of the SMUv1.1.2.x-zWebUI-xLinux.tar file or the SMUv1.1.2.x-zWebUI-zLinux.tar file into a temporary directory.

2. Browser to directory `SMUPRF1122X` or `SMUPRF1122Z`, where "X" is for Linux for System x and "Z" is for Linux on System z.

3. Browser to the directory `response_files`, and select the response file to edit based on your environment. If you need to edit the response file, create a backup copy.

4. Modify or add values for a number of properties, which are indicated by the "xxxxxxxx" string. In the response file, default values are provided for many properties, but you can edit **data key=** properties if you need to modify values for your environment. See the comments in the file for more details.

   Note: The repository location is the location of the performance management code. By default, this location is the SMUPRF* directory in the installation package. In the response file, replace xxx with the path to the work directory where the installation package is open and yyyyy with the rest of the SMUPRF* directory name. For example, `location=/temp/install/SMUPRF1122Z`.

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. Install the components as applicable.

   - To install both the Tivoli Directory Integrator and Dashboard Application Services Hub components on one server, run the following command in the directory where you extract the installation package.

     `./silentInstall.sh`

     When you start **silentInstall.sh**, the default is to run **silentInstall.xml**.

   - To install only the Tivoli Directory Integrator component, edit the **silentInstall_tdi.xml** and run the following command:

     `./silentInstall.sh TDI`

   - To install only the Dashboard Application Services Hub component, edit the **silentInstall_DASH.xml** and run the following command:

     `./silentInstall.sh DASH`

7. Refer to the `packageinstall.log` file that is created in the same directory as the **silentInstall.sh** if the prerequisite checker fails, or the installation fails. Fix the issues and rerun the **silentInstall.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

A successful installation is noted by a final message beginning with **Installed com.ibm.cmis.webui....**

Uninstalling SMU Performance Management

This section introduces how to uninstall IBM Service Management Unite Performance Management.

Procedure

1. Browse to the directory where IBM Installation Manager locates. The typical directory is: `/opt/IBM/InstallationManager/eclipse`
2. Issue the following command to start the dialogue.

   `./IBMIM`
3. In the IBM Installation Manager dialog, select **Uninstall** to start your uninstallation.
4. In the Uninstall Packages - select packages to uninstall panel, select **IBM Service Management Unite Performance**. Click **Next**.
5. In the Uninstall Packages - Common Configurations - Dash Extensions Configuration panel, verify the fields that are already filled it, enter the password for the **WebSphere user id**. Click **Next**.
6. In the Uninstall Packages - Common Configurations - TDI Extensions Configuration panel, all of the necessary fields should be filled. Click **Next**.

   Note: If the **TDI Keystore Password** has changed since installation, you need to update it.
7. In the Uninstall Packages - Review the summary information panel, verify the package to be uninstalled. Click **Uninstall**.
8. The uninstallation will take several minutes. When the Uninstall Packages - The following package was uninstalled panel is reached, click **Finish** to return to the main IBM Installation Manager dialog.
9. To exit IBM Installation Manager, click **File** > **Exit**.

Chapter 6. Upgrading

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

Upgrading SMU Automation

IBM Service Management Unite recommends installing the latest version of Service Management Unite Automation as it becomes available. The InstallAnywhere installer that is used for Service Management Unite Automation is part of the Service Management Unite package. The installer detects if an initial installation or an update installation needs to be performed.

Procedure

1. Extract the content of the `SMUv1.1.2.x-zWebUI-xLinux.tar` file or the `SMUv1.1.2.x-zWebUI-zLinux.tar` file as appropriate into a temporary directory.
2. Change to the directory that contains the installation program:

   For Linux on System x: `SMUAUTO1122X/x86_64/`

   For Linux on System z: `SMUAUTO1122Z/s390/`
3. Start the installation by launching the installation wizard using `setup.bin`.
4. When the installation wizard is launched successfully, the Welcome panel appears. The installer detects that this is an update installation if a previous version of IBM Service Management Unite is found on the system.
5. Follow the instructions on the installation panels to install the update.

Upgrading SMU Performance Management

IBM Service Management Unite recommends installing the latest version of Service Management Unite Performance Management as it becomes available. You can use the Update Packages wizard in IBM Installation Manager to install updates.

About this task

This procedure describes an update to the default installation where both the DASH and Tivoli Directory Integrator components are installed. If you are updating an installation where only one component is installed, only the pages relevant to the selected feature are shown.

Procedure

1. Start IBM Installation Manager.
2. On the Start page of Installation Manager, click **Update**.
3. In the Update Packages page, select **IBM Service Management Unite Performance Management**.
4. Select desired version, for example, **V1.1.2.2** and click **Next**.
5. On the Licenses page, select **I accept the terms in the license agreement** and click **Next**.

6. On the Features tab, under the Common Configurations > DASH Extensions Configuration window, verify the DASH directory installation location, Jazz application server, and enter the **WebSphere user id**, **password**, and **server name**. Click **Next**.

7. In the TDI Extensions Configuration window, verify the **TDI Install Directory**, **TDI Solutions Directory**, and **TDI command parameter** fields. Click **Next**.

8. In the TDI Solution Properties window, verify the **Solution Properties** fields. Click **Next**.

9. In the SSL certificate exchange window, verify the **Jazz profile node directory** location, **WebSphere keystore password** for the root certificate key store found in the directory, and **Local TDI Fields**. Click **Next**.

   Note: The **WebSphere keystore password** field is initially set to the IBM-supplied default of "WebAS" included with WebSphere Application Server. The **Local TDI Fields** verifies the location, file name, and password for a Tivoli Directory Integrator trust store file for Service Management Unite. If WebSphere and Tivoli Directory Integrator are on different systems, you must verify the location, user ID, and password for the Tivoli Directory Integrator system. Additionally, you must verify the Tivoli Directory Integrator installation and solution directory on that system.

10. On the Summary page, review your choices before installing the updates. Click **Update** to install the updates.

    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.

11. Optional: When the update process completes, a message that confirms the success of the process is displayed near the top of the page. Click **View log file** to open the log file for the current session in a new window. You must close the Installation Log window to continue.

12. Click **Finish** to close Installation Manager.

Chapter 7. Configuring and administrating

This information provides the following topics to help you configure and administrate Service Management Unite after installation.

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 components that you require, complete the configuration tasks to fully prepare your infrastructure environment.

This topic describes the following configuration scenarios:
- How to configure agentless adapters (see Configuring access to agentless adapters (optional)).
- How to configure Service Management Unite Automation and specify credentials for connected automation domains (see "Configuring the SMU Automation host" on page 51).

Note: You must ensure that an X Window is available for displaying the graphical configuration panels. At a minimum, you must use the configuration dialog 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. If an X Window is not available, silent configuration is the only supported method on this system. For more information, see "Starting silent configuration" on page 68.

Starting the SMU Automation configuration dialog

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

For more information about the `cfgsmu` configuration utility, refer to "Configuring SMU Automation with the cfgsmu configuration tool" on page 72.

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.

Configuring the SMU Automation settings

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.
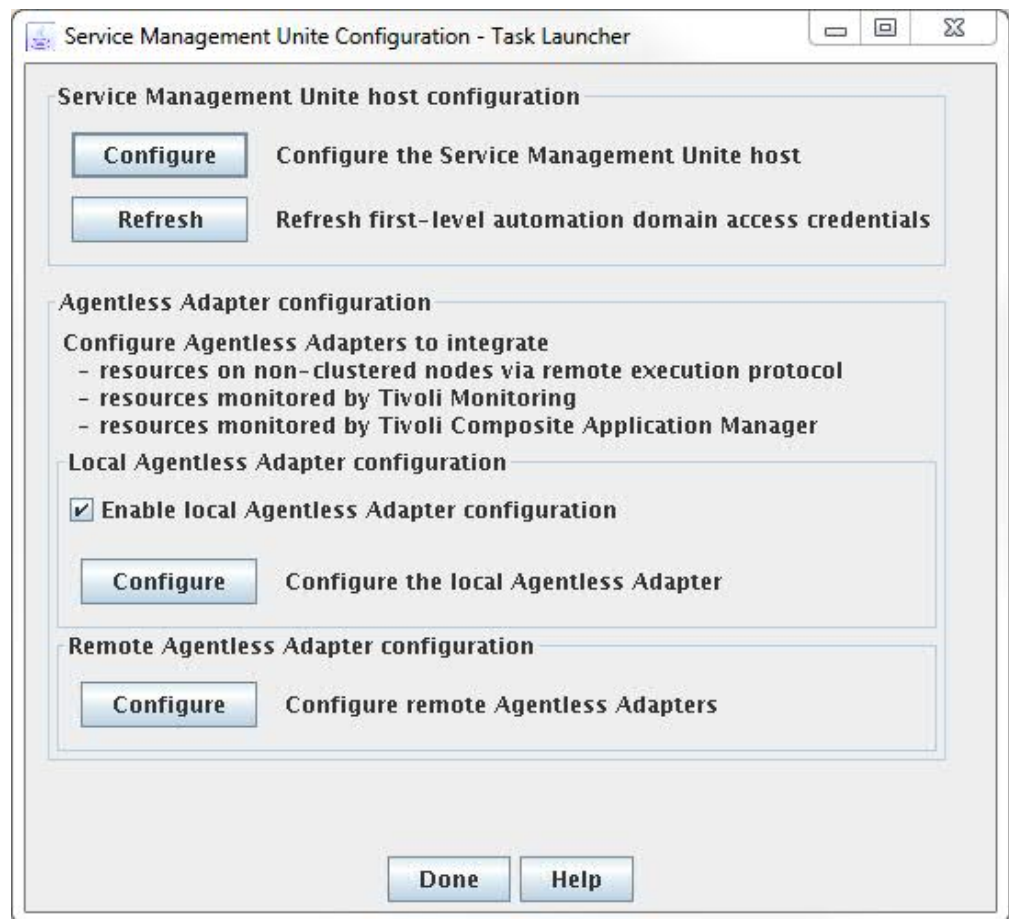
Figure 2. IBM Service Management Unite configuration - main menu

- The **Service Management Unite host configuration** section contains the following controls and fields:

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 "Configuring the SMU Automation host."

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

- The **Agentless Adapter configuration** section contains the following controls and fields:

Enable local agentless adapter configuration
> Select this check box to enable the **Local agentless adapter configuration** with the following effects:
> - The **Configure** button of the **Local Agentless Adapter configuration** is enabled.
> - Configuration files of the local agentless adapter are updated if they are affected by changes that you apply to the Service Management Unite configuration.
>
> The configuration dialog remembers the enable/disable status of the local agentless adapter configuration across multiple invocations.
>
> **Note:** This check box applies only to the local agentless adapter, but not to any remote agentless adapter.

Local agentless adapter Configure button
> Click **Configure** in the **Local Agentless Adapter configuration** section of this tab to open the agentless adapter configuration dialog. For more information, see "Configuring the local agentless adapter" on page 56.

Remote agentless adapter Configure button
> Click **Configure** in the **Remote Agentless Adapter configuration** section of this tab to open the remote agentless adapter configuration dialog. For more information, see "Configuring remote agentless adapters" on page 62.

More detailed information about all configuration tasks is available in the online help. To start the online help, click **Help** in the menu bar of the configuration dialog.

Configuring the SMU Automation host

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.

The following topics describe the Service Management Unite configuration dialog. To open the configuration dialog, process the following steps:

1. Start the configuration dialog (see Starting the Service Management Unite Automation configuration dialog).

2. Click **Configure** on the **Service Management Unite** host button. The common configuration dialog opens.

Post-configuration tasks:

After the configuration properties are edited, the configuration settings can be dynamically activated by clicking the **Refresh** task on the main menu of the **Service Management Unite Configuration - task launcher**. See also "Refreshing the SMU common configuration" on page 53.

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 Generating Keystore and Truststore with SSL public and private keys.

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.

Saving the common configuration: To save your changes to the IBM Service Management Unite common configuration properties files, click **Save** on the configuration dialog. 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.

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.

[Optional] Configuring access to agentless adapters

Use the agentless adapter to access and integrate non-clustered nodes into an automation environment.

Configure either the local agentless adapter or one or multiple remote agentless adapters or a combination of both. Run the `cfgsmu` command and start the configuration task that you want to perform from the task launcher window. For more information, see "Starting the SMU Automation configuration dialog" on page 49.

Configure the local and remote agentless adapters on the system where the Service Management Unite Automation operations console is installed. Enter the `cfgsmu` command to open the configuration utility. After the configuration for one instance of the remote agentless adapter is completed, this configuration must be distributed to the corresponding adapter host.

Figure 3 on page 55 displays how configurations for agentless adapters are maintained.

Post-configuration tasks:

After the configuration properties are edited, the configuration settings can be dynamically activated by clicking the **Refresh** task on the main menu of the Service Management Unite Configuration - task launcher. See also "Refreshing the SMU common configuration" on page 53.

Figure 3. Maintaining configurations for multiple agentless adapters

For more information about how to work with the agentless adapter and develop agentless adapter policies, refer to the following:

- Working with the agentless adapter

- Developing automation policies for the agentless adapter
- Agentless adapter policy XML reference.

Configuring the local agentless adapter:

The Service Management Unite Automation local agentless adapter configuration dialog helps you to configure the local agentless adapter settings.

To open the configuration dialog, click **Configure** in the **Local Agentless Adapter configuration** 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 agentless adapter policy.

Controls and fields on the Adapter tab:

Request port number
> Specify the number of the port on which the agentless adapter listens for requests from the operations console host. The default port is 2005.

Policy pool location
> Specify the qualified path name of the directory that contains the agentless adapter policies. These policies define resources on non-clustered nodes. The resources are managed by the agentless adapter. Click **Browse** to select a directory.

Automation domain list
> The table lists automation domain names. Each domain represents a set of resources on nodes that are not clustered and managed by the agentless 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.

Add, Remove or Rename domains
> To change the list of domains, click the corresponding tasks:
>
> **Add**   Click **Add** to open a dialog. Specify the domain name that you want to add to the list.
>
> **Remove**
>> Select a domain from the list and click **Remove**.
>
> **Rename**
>> Select the domain name that you want to rename and click **Rename**. A dialog opens. Enter the new name.

Click **Advanced**. A dialog opens to specify the adapter runtime behavior:

Adapter stop delay
> Defines the time, in seconds, within which the adapter stop is delayed to allow the adapter to properly deliver the domain leave event. The default value is 5. You can increase the value on slow systems. The value ranges between 3 through 60 seconds.

Remote contact activity interval
> Defines the time after which the automation adapter stops if there is no communication with the operations console host. The default value is 0

seconds which means that the adapter never stops. It continues to run and waits until it is contacted again by the operations console host.

Initial contact retry interval

Defines the time, in minutes, within which the adapter attempts to contact the operations console host until it succeeds or the specified time elapses. The default value is 0, where 0 means the adapter attempts to contact the operations console host indefinitely. The value range is 0 - 1440 minutes.

Enable EIF event caching

Select this check box to activate event caching.

EIF reconnect attempt interval

Defines the time that the adapter waits before it attempts to reestablish the connection to the operations console host after the connection is interrupted. The default value is 30 seconds. The value range is 1 - 3600 seconds.

User Credentials tab:

Use the User Credentials tab to configure credentials of the agentless adapter. These credentials are used to access remote nodes, which host remote resources that are managed by the agentless adapter.

These credentials are not required for IBM Tivoli Monitoring resources that are managed by the agentless adapter. Credentials for IBM Tivoli Monitoring resources are configured on the Tivoli Monitoring tab. For details about how to configure these credentials, see "Tivoli Monitoring tab" on page 58.

Controls and fields on the User Credentials tab:

Configure the user IDs and passwords that the agentless adapter uses to access remote nodes, which host resources that are managed by the agentless adapter.

Generic user ID

Enter a generic user ID to access all non-clustered nodes for which no specific credentials are defined in the list **Credentials for accessing specific non-clustered nodes**. Generic credentials are optional. If you want to remove already configured generic credentials, leave the user ID field empty.

Generic password

Enter your password for the generic user ID. This field is mandatory only if you supplied a generic user ID. Click **Change** to change the password.

Credentials for accessing specific non-clustered nodes

Define user credentials for each non-clustered node for which the generic credentials do not apply. The list shows all currently defined user credentials and their related node names.

Add   Click **Add** to define a new user ID and password to access remote nodes. More than one user credential per node is allowed.

Remove

To remove an entry from the list, select a user ID and click **Remove**.

Modify

To edit the node name, user ID, or password, select an entry from the list and click **Modify**.

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 agentless 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.

Tivoli Monitoring tab:

Use the Tivoli Monitoring tab to configure the integration of Tivoli Monitoring and IBM Tivoli Composite Application Manager (ITCAM) resources by defining settings and credentials to access the Tivoli Monitoring SOAP Server.

Controls and fields on the Monitoring tab:

Enable integration of ITM/ITCAM resources
Select this check box if you want to integrate ITM/ITCAM resources in a policy for a domain that is managed by the local agentless adapter. Selecting this option enables all controls on this tab pane.

Configure settings to access the Tivoli Monitoring SOAP server:

Host name or IP address
Specify the name or the IP address of the host where the hub monitoring server that hosts the SOAP service is running.

SOAP server port number
Specify the service point port number of the SOAP server hosted by the hub monitoring server. The default number for a non-SSL port is 1920. The default number for an SSL port is 3661. You must specify the number of an SSL port if you selected the check box to use Secure Socket Layer (SSL) for communication with the SOAP server.

SOAP alias of hub
Specify the alias name of the hub monitoring server to which a SOAP request is routed. The request is routed to the hub monitoring server, which is on the same system as the SOAP server. In this configuration, you must specify SOAP as the alias. If you want to route the SOAP request to a remote hub, specify the alias name of this remote hub. This alias must be previously defined to the SOAP server in the ITM/ITCAM SOAP server configuration.

Use SSL for communication with the SOAP server
Select this check box if the agentless adapter must use Secure Socket Layer (SSL) for communication with the SOAP server. If you select this option,

you must specify the number of an SSL port in the **SOAP server port number** field. The https protocol is used for communication.

Configure credentials for accessing the Tivoli Monitoring SOAP server:

Define the user credentials for each user ID that is specified for an ITM/ITCAM resource in an agentless adapter policy. You can define the user credentials in the list of specific credentials for accessing the SOAP server. When no user ID for the ITM/ITCAM resources is specified in the policy, the generic user credentials are used.

Generic user ID
> Specify the generic user ID that is used to access the ITM/ITCAM resources for which a user ID was omitted in the agentless adapter policy. If you specified a user ID for all ITM/ITCAM resources in the agentless adapter policies, this field is not used. Generic credentials are optional. If you want to remove already configured generic credentials, leave the user ID field empty.

Generic Password
> Specify the password of the generic user ID. This field is mandatory only if you supplied a generic user ID. Click **Change** to change the password.

Specific credentials for accessing the Tivoli Monitoring SOAP server
> Define each user ID that you specified for an ITM/ITCAM resource in an agentless adapter policy. Use the following tasks:

> **Add** Click **Add** to define a new user ID and password to access the SOAP Server.

> **Remove**
>> To remove an entry from the list, select a user ID and click **Remove**.

> **Modify**
>> To edit the user ID or password, select an entry from the list and click **Modify**.

Note: You can define the SOAP server security setup to accept a user ID with an empty password. For example, if you want to use the agentless adapter in a test environment, you can specify the user ID for the corresponding ITM/ITCAM resource in the agentless adapter policy. It is not required to define the user ID in the list of specific credentials to access the SOAP server. In this case, the agentless adapter attempts to access the ITM/ITCAM resource with the user ID defined in the policy and an empty password.

Security tab:

Use the **Security** tab to configure the settings for user authentication and secure data transport.

You can configure the following settings:

Secure Sockets Layer (SSL) for data transport
> Configure SSL for data transport between the agentless adapter and the operations console.

User authentication
> Configure whether user authentication is enforced on the system where the agentless adapter is running.

User authentication with SSH public and private keys
Configure user authentication between the agentless adapter and remote non-clustered nodes with SSH public and private keys. This authentication method applies only to remote resources, which are accessed by using a remote execution protocol. It does not apply to IBM Tivoli Monitoring resources defined in the agentless adapter policy because for IBM Tivoli Monitoring resources an existing IBM Tivoli Monitoring security infrastructure is reused. The user ID that you specify for a remote resource in an agentless adapter policy is used to authenticate on the remote node where the resource is located. The agentless adapter separately authenticates each user ID that is specified for a remote resource in the agentless adapter policy. The adapter authenticates those users on remote nodes in the following sequence:

1. The user ID that is specified for a remote resource in the agentless adapter automation policy is defined in the **Credentials for accessing specific non-clustered nodes** list on the **User Credentials** tab: The agentless adapter uses the password that is associated with that specific user ID.

2. The user ID that is specified for a remote resource in the agentless adapter automation policy is defined as **Generic user ID for non-clustered nodes** on the **User Credentials** tab: The agentless adapter uses the password that is associated with that generic user ID.

3. For the user ID that is specified for a remote resource in the agentless adapter policy, user authentication is processed by using SSH public and private keys. In this case, check **Enable user authentication with SSH public and private keys** and specify the SSH private key file and passphrase.

Controls and fields on the Security tab:

Configure Secure Sockets Layer for transport:

Enable SSL for data transport between the end-to-end automation host and the agentless adapter
Check this check box to enable the Secure Sockets Layer (SSL) protocol. The following fields are enabled:

Truststore
Enter the fully qualified 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 Generating Keystore and Truststore with SSL public and private keys.

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

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

Note: Passwords must be identical if truststore and keystore are in two different files.

Certificate alias
> Enter the alias name of the certificate that is used by the server. If not specified, the keystore file must contain only one entry, which is the one to be used.

Configure user authentication between the Automation Manager and the agentless adapter with the Pluggable Access Module (PAM).

Enforce user authentication between the end-to-end automation host and the agentless adapter
> Click the check box to enable user authentication with Pluggable Access Module (PAM). If not checked, user authentication is bypassed.

Configure security for the communication between the agentless adapter and remote non-clustered nodes.

Enable user authentication with SSH public and private keys
> Check this check box to use SSH keys for authentication. Use SSH keys for user IDs that have no generic or specific access credentials that are defined on the **User Credentials** tab.

SSH private key file
> Enter the fully qualified name of the SSH 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 agentless adapter is running has read access for this file. Click **Browse** to select a file.

SSH private key file
> Enter the fully qualified name of the SSH 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 agentless adapter is running has read access for this file. Click **Browse** to select a file.

Private key passphrase
> Enter the passphrase that you used to generate the SSH private key file with the **ssh-keygen** utility. Click **Change** to change the passphrase. The passphrase is optional because you can omit the passphrase when you use the **ssh-keygen** utility. Click **Change** to remove a passphrase. Leave all entry fields in the dialog empty and select **OK**.

Logger tab:

Use the **Logger** tab to specify settings for logging, tracing and First Failure Data Capture.

Controls and fields on the Logger tab:

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
> Select the **Message logging level**, depending on the severity of messages that you want to be logged.

Trace logging level

Select the **Trace logging level**, depending on the severity of the incidents that you want to be 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.

First failure data capture (FFDC) maximum disk space

Specify the maximum disk space in bytes used by FFDC traces, which are written to the FFDC trace directory. The default space is 10485760 bytes (10 MB).

First failure data capture (FFDC) space exceeded policy

Select one of the options:

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 ID filter mode

Select one of the options:

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.

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 on a new line. Wildcard characters, for example, *E (for all error messages), are allowed.

Saving the local agentless adapter configuration: To save your changes to the IBM Service Management Unite agentless adapter configuration properties files, click **Save** on the configuration dialog. Upon 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.

Configuring remote agentless adapters:

The IBM Service Management Unite remote agentless adapter configuration dialog helps you to configure remote agentless adapter settings.

Use the remote IBM Service Management Unite configuration window to maintain the configurations for one or multiple remote agentless adapter instances.

The list of remote agentless adapter configurations shows one entry for each currently configured remote agentless instance:

Remote Agentless Adapter Host
> The host name of the node where the remote IBM Service Management
> Unite instance is installed.

Configuration Directory
> The configuration directory is always `/etc/opt/IBM/tsamp/eez/rala/cfg`

Configuration complete
> The configuration complete value indicates whether the configuration for
> the corresponding remote IBM Service Management Unite instance is
> completed or not.
> - No: Initial value after you added a configuration.
> - Yes: After you successfully completed the **Configure** task for the adapter
>   instance.
>
> **Note:** You can distribute only completed configurations to the remote host.

Click **Add** to add a configuration for another remote IBM Service Management
Unite instance. A dialog opens to specify the remote node name of the host.

Click **Remove** to remove the selected configuration from the list. All configuration
files related to that configuration are deleted on the system where the
configuration utility runs. If you distributed the configuration already, the
configuration files on the remote host will not be deleted.

Click **Configure** to open the configuration dialog for the selected configuration.
For more information, see "Configuring a remote agentless adapter instance."

Click **Distribute** to distribute the selected configuration. For more information, see
"Distributing a remote agentless adapter configuration" on page 64.

Configuring a remote agentless adapter instance:

The content of the configuration dialog tabs and the semantics of the fields are
mostly the same as described in "Configuring the local agentless adapter" on page
56. Below you can find the description of tabs or fields that are unique for a
remote agentless adapter configuration. To open the configuration dialog, select the
entry that you want to configure and click **Configure** in the remote agentless
adapter configuration window.

Post-configuration tasks

Distribute the remote agentless adapter configuration to the corresponding remote
agentless adapter host. For more information, see "Distributing a remote agentless
adapter configuration" on page 64.

Adapter tab

Refer to "Adapter tab" on page 56 for a description of this tab content and the
semantics of the fields on the tab. One control is added to the Adapter tab for the
remote agentless adapter:

Host name or IP address
> Host name or IP address of the node where the adapter runs. The default
> value is the remote agentless adapter host name that you specified for this
> adapter instance in the remote agentless adapter configuration window. If

you want to change this value, for example to an IP address, make sure that the new value refers to the host where this adapter instance is installed.

User Credentials tab

Refer to "User Credentials tab" on page 57 for a description of this tab content and the semantics of the fields on the tab.

Tivoli Monitoring tab

Refer to "Tivoli Monitoring tab" on page 58 for a description of this tab content and the semantics of the fields on the tab.

Security tab

Refer to "Security tab" on page 59 for a description of this tab content and the semantics of the fields on the tab.

Logger tab

Refer to "Logger tab" on page 61 for a description of this tab content and the semantics of the fields on the tab.

Saving the remote agentless adapter configuration:

To save your changes to the IBM Service Management Unite remote agentless adapter configuration properties files, click **Save** in the configuration dialog. Upon completion, a configuration update status window is displayed, showing which configuration files were updated. If errors occurred during the update, the corresponding error messages are also displayed.

Note: The configuration files are located in a subdirectory of the standard configuration directory. The name of the subdirectory is the remote agentless adapter host name that you specified for this adapter instance in the remote agentless adapter configuration window.

Distributing a remote agentless adapter configuration:

Use the remote agentless adapter configuration distribution dialog to distribute the configuration files for a remote instance to the remote host where that adapter instance is installed.

To open the configuration distribution dialog, select the entry that you want to distribute and click **Distribute** in the remote agentless adapter configuration window. Provide the following input in the **Remote agentless adapter configuration distribution** dialog:

Remote host login user ID and password
>	The credentials that are used to access the remote agentless adapter host. The specified user ID must have write access to the configuration directory.

Recycle remote agentless adapter after configuration distribution
>	Check whether you want the agentless adapter to be stopped and restarted on the remote host after the configuration distribution runs. Then, the remote agentless adapter runs with the changed configuration values. The

remote agentless adapter is recycled only if the distribution of all configuration files is completed successfully and if the adapter is running.

Click **OK** to distribute the configuration. Upon completion, the Configuration distribution status window opens to show the list of configuration files that are distributed. If you selected **Recycle the remote agentless adapter after configuration distribution**, you are informed about the result of the recycle attempt and the status of the adapter on the remote host.

Controlling agentless adapters:

Use the `eezaladapter` command to start, stop, and monitor agentless adapters. To control the local agentless adapter, run the command on the system where the Service Management Unite Automation operations console is installed. To control the remote agentless adapters, run the command on the respective remote host.

Configuring agentless adapters in silent mode:

You can configure agentless adapters in silent mode as an alternative to using the configuration dialogs.

Use the silent mode when:
* configuring the local agentless adapter.
* configuring remote agentless adapters.
* adding, removing, and distributing remote agentless adapter configurations.

Refer to "Configuring SMU Automation in silent mode" on page 66 for a detailed description of the silent mode configuration tasks.

Tuning the number of domains and resources of agentless adapters: The number of resources that can be managed by agentless adapters 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 agentless adapters run. 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 agentless adapters.

Recommendations for the local agentless 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.

Recommendations for one remote agentless adapter instance:
1. Do not define more than 40 domains.
2. Do not include more than 250 resources in each domain.
3. Do not define more than 450 remote resources in total.

For each agentless adapter instance (local and remote), 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
  - agentless 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 9 shows the silent input properties files that are generated if the **-g** or **-gr** option is specified.

Table 9. 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`
Local agentless adapter	`cfgsmu -s -eu -g ⎮ -gr`	`<EEZ_CONFIG_ROOT>/` `silent.eezaladapt.properties`
	`cfgsmu -s -eu -g ⎮ -gr -l` *location*	*location*`/silent.eezaladapt.properties`
Remote agentless adapter	`cfgsmu -s -ru -o` *host* `-g ⎮ -gr`	`<EEZ_CONFIG_ROOT>/` `silent.remotealadapt.properties`
	`cfgsmu -s -ru -o` *host* `-g ⎮ -gr` `-l` *location*	*location*`/` `silent.remotealadapt.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. Log on to the system where IBM Service Management Unite is installed.
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 local agentless adapter:

      cfgsmu -s -eu

   c. Configure the remote agentless adapters:

      cfgsmu -s -ru -o *host* [-ra [-w *configdir*] | -rr | -rd -u *userid* -p *password*]

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 66. 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".

Tasks that do not update configuration files
The output for all tasks to add, remove, or distribute a remote agentless adapter is a corresponding task completion message.

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 operations console host and agentless 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 "Configuring SMU Automation with the cfgsmu configuration tool" on page 72.

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 local agentless adapter. For example, the host and port the agentless 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 local agentless adapter uses to access remote non-clustered nodes. The resources that the agentless 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 local agentless 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 local agentless 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 local agentless adapter.

eez.aladapter.jlog.properties
> The properties in this file determine which information is written to the log and trace files of the local agentless adapter.

eez.aladapter.plugin.properties
> The properties in this file are used to configure settings that are unique for the local agentless adapter: for example, the location of the XML policy pool.

eez.aladapter.plugin.<domain>.properties
> For each local agentless adapter domain, a domain-specific copy of eez.aladapter.plugin.properties is created:

remote_node/**eez.aladapter.properties**
remote_node/**eez.aladapter.dif.properties**
remote_node/**eez.aladapter.ssh.properties**
remote_node/**eez.aladapter.ssl.properties**
remote_node/**eez.aladapter.jaas.properties**
remote_node/**eez.aladapter.plugin.properties**
remote_node/**eez.aladapter.plugin.<domain>.properties**
> These files are stored for each remote agentless adapter instance in a subdirectory for the node on which the remote agentless adapter is installed.

remote_node/**eez.aladapter.jlog.properties**
> The properties in this file determine which information is written to the log and trace files of an instance of the remote agentless adapter.

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 73. 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 30 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.

Property	User-based	Description
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 SMU Automation with the cfgsmu configuration tool

The cfgsmu configuration tool is used to configure Service Management Unite Automation. Use the settings described here to configure your environment.

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 local agentless adapter for non-clustered nodes.

-ru
  Configure a remote agentless adapter for non-clustered nodes.

-o Specify the node name of remote agentless adapter host.

host
  Remote agentless adapter host node.

-ra
  Add a remote agentless adapter configuration.

-rr
  Remove a remote agentless adapter configuration.

-rd
  Distribute a remote agentless adapter configuration.

-u Specify user ID for remote agentless adapter distribution node.

uid
  Remote distribution node user ID.

-p Specify password for remote agentless adapter distribution node.

pwd
  Remote distribution node password.

If none of the options **-ra**, **-rr**, or **-rd** is specified, the remote agentless adapter settings for the specified host are configured.

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.

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 10. 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.
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 agentless adapter to access remote nodes. The user ID is specified for each resource in the agentless 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 agentless 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 an agentless 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 agentless adapter. Depending on what you configured, different authentication methods are used.

#	Description	Location	Configuration	Details
4	Credential for the agentless adapter to access Tivoli Monitoring resources via a hub monitoring server. A user ID can be specified for each resource in the agentless 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 agentless adapter: in the local or remote agentless adapter configuration on the **Monitoring** tab. **Hub TEMS:** • In the configuration of the hub TEMS	This credential is used by an agentless 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 an agentless adapter or by any other automation adapter:

Resources hosted directly by an agentless adapter:

Describes which user credentials are required to operate resources hosted directly by the agentless adapter.

Figure 4. Operating resources directly on single nodes

The numbers in the pictures refer to the numbers of the credentials in "User credentials" on page 74.

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 an agentless adapter. As soon as you select the agentless adapter domain, the operations console prompts for a credential to access the agentless adapter domain (Credential 2).

3. Select the resource that you want to stop, and run a stop command against it. The agentless adapter checks which user ID is specified for the resource in the agentless 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 11. Access roles for IBM Service Management Unite

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 11. Access roles for IBM Service Management Unite (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 11. Access roles for IBM Service Management Unite (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 IBM Service Management Unite 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 12. Role to group assignment

Role	Group name
EEZMonitor	EEZMonitorGroup

Table 12. Role to group assignment (continued)

Role	Group name
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 13. 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 77

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 user credentials to access DB2

This authentication entry is required to allow the application EEZEAR to access the automation database, if a remote DB2 is used. Perform the following steps to modify the default authentication data the automation management server uses to access DB2:

Procedure

1. Log on to the **WebSphere administrative console**. Go to **Security > Secure administration, applications, and infrastructure > Java Authentication and Authorization Service > J2C authentication data**

2. In the table, select the alias `EEZDB2AuthAlias`

3. Change the password or the user ID and the password and click **OK**.

4. From the menu, select **save**.

5. Click **save** to save and activate the new configuration. Do not restart the WebSphere Application Server. For more information, refer to the documentation of the WebSphere Application Server.

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 52.

The automation framework uses the credentials to authenticate to first-level automation domains.

Configuring SMU Performance Management

After a successful installation, you must complete configuration tasks to finish setting up Service Management Unite Performance Management.

Note: If you installed Service Management Unite Performance Management by running a silent installation program, you can skip to Configuring historical data collections.

Configuring properties files

You can modify the properties file values for Service Management Unite Performance Management after installation.

About this task

During installation, you can configure the `DASH_ITMCollector`, `DASH_SA`, and `DASH_IOALA` properties files for Service Management Unite Performance Management using IBM Installation Manager.

After installation, you can configure Tivoli Directory Integrator using the Tivoli Directory Integrator configuration editor. The configuration editor is GUI-based and allows you to edit assembly lines and customize how data is presented in Dashboard Application Services Hub (DASH) V3.1.2.1.

This topic guides you to configure the properties files after installation.

Procedure

1. Go to the solution directory. The default directory is `/opt/IBM/TDI/V7.1.1/DASH_ITMCollector`.

2. Edit the following fields in the `DASH_ITMCollector` properties file.
   - **itm.provider** (location of the Tivoli Enterprise Monitoring Server)

- **itm.url** (location of the Tivoli Enterprise Portal Server)
- **itm.user** (your Tivoli Enterprise Portal Server user ID)
- **itm.password** (your IBM Tivoli Monitoring user password)

3. If you are using the default solution directory, `/opt/IBM/TDI/V7.1.1/DASH_ITMCollector` (SOLDIR), enter the following commands to encrypt the password that is specified in the DASH_ITMCollector properties file.

```
/opt/IBM/TDI/V7.1.1/serverapi/cryptoutils.sh -input /opt/IBM/TDI/V7.1.1/DASH_ITMCollector/DASH_IT
-output /opt/IBM/TDI/V7.1.1/DASH_ITMCollector/DASH_ITMCollector.properties -mode encrypt_props
-keystore /opt/IBM/TDI/V7.1.1/testserver.jks -storepass server -alias server
```

If you are not using the default solution directory, you see the following command where you replace **SOLDIR** with your chosen solution directory:

```
-input SOLDIR/DASH_ITMCollector.properties -output SOLDIR/DASH_ITMCollector.properties
```

The Tivoli Directory Integrator solutions directory **TDI_SOLDIR** defaults to `/opt/IBM/TDI/V7.1.1/DASH_ITMCollector` and the Tivoli Directory Integrator installation directory **TDI_INSTDIR** defaults to `/opt/IBM/TDI/V7.1.1`.

```
TDI_INSTDIR/serverapi/cryptoutils.sh
-input TDI_SOLDIR/DASH_ITMCollector/DASH_ITMCollector.properties
-output TDI_SOLDIR/DASH_ITMCollector/DASH_ITMCollector.properties -mode encrypt_props
-keystore TDI_INSTDIR/testserver.jks -storepass server -alias server
```

You must replace **TDI_SOLDIR** with your chosen Tivoli Directory Integrator solution directory and replace **TDI_INSTDIR** with your chosen Tivoli Directory Integrator installation directory.

4. Edit the following fields in the DASH_SA properties file.
- **sa.user** (a System Automation user ID)
- **sa.password** (password for the System Automation user ID)

5. Edit the following fields in the DASH_IOALA properties file if you are using IBM Operations Analytics - Log Analysis.
- **Server** (host name or IP address of your IBM Operations Analytics for z Systems)
- **Port** (IBM Operations Analytics for z Systems server port)

Integration with IBM Operations Analytics - Log Analysis

To use the IBM Operations Analytics - Log Analysis launch functions, it is recommended to configure single sign-on (SSO) between the WebSphere Application Server server hosting JazzSM and the Liberty Server used by IBM Operations Analytics - Log Analysis.

WebSphere Application Server products include SSO functionality based on IBM's Lightweight Third-Party Authentication (LTPA) technology. When properly configured, these functions support navigation among WebSphere-based applications, passing authentication information as LTPA tokens in HTTP cookies. The user is prompted for authentication credentials only once, and any subsequent authentications are automatically handled in the background using the LTPA tokens included in the associated web requests. If SSO is not set up between the WAS server hosting JazzSM and the Liberty Server that is used by IBM Operations Analytics - Log Analysis, you must sign on to the IBM Operations Analytics - Log Analysis server from a separate browser tab before launching from within the IBM Service Management Unite product. This will create the LTPA tokens and HTTP cookies required by this function.

Configuring historical data collections

To view data collected from OMEGAMON monitoring agents in Service Management Unite Performance Management dashboard, you must create the historical collections.

The following example steps are provided for you to configure each attribute group from which you want to collect historical data. Your user ID must have "Configure History" permission to open the History Collection Configuration window. To create a historical collection, log on to the Tivoli Enterprise Portal first.

Configuring OMEGAMON for z/OS historical data collections

If you have not had historical collection active for the Address Space CPU Utilization attribute table, complete the following steps to create historical collections for OMEGAMON for z/OS.

Procedure

1. On the Tivoli Enterprise Portal client panel, click **History Configuration**.
2. In the left panel, select **OMEGAMON for z/OS** and right-click to select **Create new collection setting**.
3. In the dialog box, enter **Address Space CPU Utilization** in the **Name** field, and select **Address Space CPU Utilization** from the **Attribute Group** list.
4. Click **OK** to open the History Collection Configuration window.
5. Complete the fields in the **Basic** tab:
   - **Collection Interval**: 5 minute
   - **Collection Location**: TEMA
6. In the **Distribution** tab, select the **Managed System (Agent)** check box.
7. From the **Available Managed System Groups** list, select ***MVS_SYSTEM** and move it to the **Start collection on** list.
8. Click **OK**.

Configuring WebSphere Application Server historical data collections

Complete the following steps to create historical collections for WebSphere Application Server.

Procedure

1. Click **History Configuration**.
2. In the left pane, select **ITCAM for WebSphere** and right-click to select **Create new collection setting**.
3. In the dialog box, enter **Application Server Summary** in the **Name** field and select **Application Server** from the **Attribute Group** list.
4. Click **OK** to open the History Collection Configuration window.
5. Complete the fields in the **Basic** tab:
   - **Collection Interval**: 1 minute
   - **Collection Location**: TEMA
6. In the **Distribution** tab, select the **Managed System (Agent)** check box.
7. From the **Available Managed System Groups** list, select ***CAM_WAS_SERVER** and move it to the **Start collection on** list.
8. Click **OK**.

9. Repeat steps 4-8, entering **Garbage Collection** in the **Name** field and select **Garbage Collection Analysis** from the **Attribute Group** list.

10. Repeat steps 4-8, entering **Request Time and Rates** in the **Name** field and select **Request Time and Rates** from the **Attribute Group** list.

11. Repeat steps 4-8, entering **Request Analysis** in the **Name** field and select **Request Analysis** from the **Attribute Group** list.

Configuring and administrating Service Management Unite

Complete the following tasks after installing Service Management Unite Automation and Service Management Unite Performance Management.

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.

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.

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 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 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. 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.

The installer of IBM Service Management Unite 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.

If you reconfigure the user repository after you installed IBM Service Management Unite, 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.

  1. On the configuration page of your LDAP repository in the **Additional Properties** area, click **Federated repositories entity types to LDAP object classes mapping**.

  2. Click **New** to define a new entity type to class mapping.

  3. 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.

  4. Click **Apply** and then **Save**.

  5. 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.

  6. 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**.
	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 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.

This configuration is also required if you install IBM Service Management Unite after you configured an LDAP repository. The installer creates the default users and user groups for you in the LDAP repository.

This configuration is also required if you install IBM Service Management Unite Automation after you configured an LDAP repository. The installer creates the default users and user groups for you in the LDAP repository.

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.

> On the **User and Group Administration** page of the installer click **Yes**. The default users and groups for IBM Service Management Unite are created in your configured LDAP user repository. If you already created the default user groups and users for IBM Service Management Unite 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 and you did not define the default users and groups for IBM Service Management Unite 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."

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, 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 to an LDAP-based configuration:

1. Create users and groups to use with IBM Service Management Unite in the LDAP repository if they do not exist. For more information, see "Creating default users and groups."

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 95.

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 97.

Creating default users and groups:

IBM Service Management Unite requires a set of default users and groups. These users and groups are created during the installation of IBM Service Management Unite.

If you configured a new LDAP user repository after IBM Service Management Unite 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 14. 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 installations, the users and groups must be created only once and can then be used by all IBM Service Management Unite 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."
- 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 95.

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 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 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 installation deletes the default users and groups from the LDAP repository.

Procedure

To adapt the installation variables, apply the following change:

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.

If you configured a new LDAP user repository after IBM Service Management Unite 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 15. 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 16. 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 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 (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 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.

Defining a CURI Data Provider connection

An IBM Tivoli Monitoring CURI Data Provider connection is required to provide monitoring agent data to IBM Service Management Unite.

Each Tivoli Enterprise Monitoring Server has an IBM Tivoli Monitoring CURI Data Provider (ITMcDP) to serve the data.

Attention: To enable the IBM Tivoli Monitoring CURI Data Provider, you must select the **Enable the dashboard data provider** option when configuring the Tivoli Enterprise Portal Server.

1. Start your Tivoli Enterprise Portal interface.
2. Navigate to **Console Settings > Connections**.
3. Under the Server information section, select **HTTP** from the Protocol list.
4. Specify the Tivoli Enterprise Portal Server host name and set the port to 15200.
5. Specify a valid Tivoli Enterprise Portal Server user ID and password, and click **Search**.
6. Select the radio button for the CURI Data Provider connection that is displayed.
7. Under the Connection information section, enter ITMSD in the **Provider ID** field.
8. Select **OK** to complete the CURI Data Provider connection definition.

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. Ensure that each of the following properties are set to 5 seconds:

   ```
   ActiveMQBroker.timeout=5
   ActiveMQBroker.pollDelay=5
   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, 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**.

Logging on to Service Management Unite

After your environment is installed and configured correctly, log on to Service Management Unite using the web browser and credentials that you defined during the installation. The default DASH login URL is https://*hostname*:16311/ibm/console/logon.jsp.

Displaying the Service Management Unite welcome page

To display the IBM Service Management Unite welcome page when you log in, your WebSphere Application Server user ID must be granted a minimum System Automation group permission of EEZMonitor.

This group permission can be set in the WebSphere Application Server administrative console by going to **Users and Groups > Manage Users**. Search for

the user ID, click its name, and then open the **Groups** tab and add the necessary EEZ group permissions. Additional group permissions, such as `EEZAdministrator`, are required for access to System Automation functions and command execution from pages.

For information on group roles, see "Authorizing users and groups within the Dashboard Application Services Hub" on page 80.

Using the online help

All user, administrative and task information is available in the Service Management Unite dashboard console online help only.

You can access the online help after you have installed Service Management Unite by clicking the ▣ icon (**Help**) on the dashboard navigation toolbar and selecting **InfoCenter**.

To access context help for widgets on the predefined Service Management Unite Automation and Service Management Unite Performance Management dashboards, click the **Help** button in the top right corner of the widget. Information about data that is used in the widget is displayed in the **General** tab. A technical description of the widget is shown in the **Usage** tab.

Chapter 8. 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 and Performance Management. Support information and resources are also included.

Unable to start the launchpad on certain Red Hat and Firefox releases

If the launchpad doesn't start after you run the launchpad.sh from a Terminal Window, it is often caused by the version incompatibility between Mozilla Firefox and the launchpad. The SMU launchpad and the JazzSM launchpad can not launch on Red Hat Linux 6.x or 7.x with Mozilla Firefox 43.0.0 and later.

To resolve this problem, you can start the installers directly to install the products instead of using the launchpad.
* To start the SMU Automation installer manually from the command line, refer to Starting the installers.
* To start the SMU Performance Manager installer manually, refer to Starting the Service Management Unite Performance Management installers.

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 Agentless Adapter, 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 agentless adapter:

Figure 5. Communication flow: Start a resource on a single node

1. An operator submits a start request against a resource configured for an agentless 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 agentless adapter.
5. The agentless adapter remotely executes the start script on the remote node. The scripts and the node are specified in the agentless adapter policy.

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 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 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 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 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 local agentless 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.

See the following technote: http://www.ibm.com/support/docview.wss?uid=swg21659618.

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.

See the following technote: http://www.ibm.com/support/docview.wss?uid=swg21659902.

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 113.

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."

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 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 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 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 17. Reserved return codes for Command Execution

Reserved Return Code	Meaning for IBM Service Management Unite	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 18. 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, 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 19. 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.
DB2	If remote DB2 is used, ensure that the DB2 instance is started. See "WebSphere Application Server cannot connect to DB2" on page 119 for details.
EventHandlerBean	See "EEZBus is not started" on page 117.

Table 19. Sub-components implicated by message EEZJ0030E (continued)

Subcomponent name	Solution
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 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.

Troubleshooting the policy editor

Previously specified domain name not used: If a policy file is loaded from a policy pool and the policy file contains errors, the domain name of the domain hosting the policy pool is automatically used for that policy, regardless of what automation domain was specified before.

Mozilla Firefox browser displays special characters incorrectly: If special characters are incorrectly displayed in the policy editor, select **View > Character Encoding > Auto Detect > Universal** in the browser menu.

Policy editor does not print out the complete policy on some printers: If you have a printer driver installed that prints out only a subset of the policy which fits on the first page instead of printing the policy on multiple pages which can be combined to a poster, proceed as follows:

Generate an image of the policy using policy editor functionality. Open this image in an image editing application. Print the image. Most image editing applications are capable to print out large images on multiple pages.

Policy editor does not display save dialog box: If no Save dialog box appear, use the web browser options to ensure the browser does not block popups.

Troubleshooting the agentless adapter

Agentless adapter does not start: If there is no agentless adapter domain already defined, the Agentless Adapter will not start successfully. Define at least one agentless domain using the configuration utility and retry to start the Agentless Adapter.

Agentless 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 agentless adapter log files:
>   - `msgEEZALAdapter.log`

- eventEEZALAdapter.log and traceFlatEEZALAdapter.log (if the trace logging level is not set to Off)

Default local agentless adapter installation directory
/opt/IBM/smsz/ing/eez/bin

Default remote agentless adapter installation directory
/opt/IBM/tsamp/eez/bin

Agentless adapter fails to connect to the operations console host:

For a local agentless adapter installation check if ports are configured as expected, and TCP sessions are established.

For a remote agentless adapter, perform the same checks as for the local agentless adapter, and make sure the firewall allows connections in both directions.

Check with netstat if TCP sessions are established:
- Whether the agentless adapter listens on the request port (default port is 2001).
- Whether the operations console host listens on the event port (default port is 2002).

For both the local and remote agentless adapter, 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 agentless adapter.
- telnet <agentless adapter address> 2001 from the system running the IBM Service Management Unite installation.

Where <operations console host> is the IP address or fully qualified domain name of the system hosting the IBM Service Management Unite installation. <agentless adapter address> is the IP address or fully qualified domain name of the agentless adapter. If a session setup is not possible using telnet check again that the firewall allows this.

Agentless adapter domain and resource states are not refreshed as expected:

If the states of remote resources that are managed by the agentless adapter do not reflect the actual state of the resources within a reasonable time frame then consider to tune the agentless adapter domain topology. For more information, see "Tuning the number of domains and resources of agentless adapters" on page 65.

Analyzing the states of remote resources:

If the states of remote resources that are managed via the agentless 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 20. 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.
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.

Table 20. 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
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 21. 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.Use this topic for troubleshooting problems you experience when you install IBM Service Management Unite Automation.

Procedures for troubleshooting an installation

If the installation fails, the installation wizard displays an error message.

When an error occurs, immediately archive the installation log files (see "Using the log file collector utility" on page 125). This ensures that the original log files are retained, which is important should you need to contact IBM Support, and you can use the archive for your own troubleshooting activities.

An error occurred in the pre-installation phase
> If an error occurs in the pre-installation phase, that is, before the **Install** button was clicked, click the button **Save installation log files** to collect all installation log files. The zip file will be created at the location specified.

An error occurred in the installation phase
> Typically, errors only occur in the installation phase if insufficient disk space is available.

An error occurred in the configuration phase

Click **Finish** to finish the installation, then change to `<EEZ_INSTALL_ROOT>/install` and run the log file collector utility. The log zip will be created in the same directory. For details see "Using the log file collector utility" on page 125.

Using the Configuration problem analysis dialog

The Configuration problem analysis dialog assists in handling post-installation configuration issues. The Configuration problem analysis dialog is displayed if a post-installation step fails. The dialog is divided into two panels. The first panel displays an introductory explanation and points to the directory that contains the detailed installation log.

The second panel provides information that assists to identify the root cause of the problem on the following tabs:

- The Step details tab shows the step number, the technical step ID, the return code of the step, and the step description.
- The Executed command tab shows details of the executed command.

After you resolved the issue, you can then click **Retry** to re-execute the step.

Click **Retry** to re-execute the most recent step. Click **Exit** to quit the installation. If you restart the installation later, the installation resumes at the step that previously failed.

Installing on machines with system resources at or below the minimum required level can lead to timeouts. Normally, a timeout is not a problem in the configuration phase. A pop-up window is displayed with a detailed explanation of why the timeout occurred. Click **Retry** to rerun the step that had timed out.

Cleaning up from a failed installation

Installation can be canceled at any time. Clean up depending on the installation phase when the installation was canceled or when the installation failed:

- Installation was canceled or failed before the installation was started: no cleanup is necessary
- Installation was canceled or failed during the installation phase: Run the uninstaller to clean up files that were installed on disk.
- Installation was canceled during the configuration phase: Installation can be resumed.

  If the system must be cleaned up again, rerun the installer, and then run the uninstaller to undo all configuration steps and to remove all installed files from disk.
- Installation failed during the configuration phase: Corrective actions might be needed before installation can be resumed.

  To recover the files if the product was uninstalled, but the unconfiguration was not successful and the files are needed to manually run the remaining unconfiguration steps: Run the installer with the option `-Dfilesonly=true` in this case, only the files are installed; no configuration is performed.

  Be sure to undo the configuration changes that were made during the installation before uninstalling. Otherwise, the configuration changes are retained and the scripts to remove them are already uninstalled.

Recovering from a lock out situation during installation:

If the installation fails try to uninstall the product and reinstall again. If the re-installation fails showing a message like "product is already installed at same level", delete the file /var/.com.zerog.registry.xml.

Note: .com.zerog.registry.xml is a hidden file.
Make sure that no other product needs this file. Browse the file and verify whether you have no other entries that point to different products. Otherwise, contact support for further recommendations.

Using the log file collector utility

When an error occurs, use the log file collector utility to collect the log files that were written during the installation. The utility generates an archive that you can use for your own troubleshooting activities and send to IBM Support if you cannot resolve the error.

Perform these steps to run the log file collector utility:

1. Change the directory to <EEZ_INSTALL_ROOT>/install.
2. Issue the command collectinstallerlogs.sh.

   The command can be invoked with the option **-D** to copy all logs (in case Java is not available). The directory tree created can then be packed manually.

   The name of the file that is created by the utility is eezinstallerlogs_<timestamp>.zip.

   On Linux you can invoke the command with the option **tar** to use tar rather than jar for packing.

   The resulting archive has the following directory structure:

   - EEZ_logs
   - cfg: configuration files (for the automation framework, etc.)
   - logs: eezinstall.log, etc.
   - sh: scripts used by installer
   - WAS_logs
   - logs: general WAS server logs
   - <server name>: logs for the selected WebSphere Application Server

Installation Manager 32-bit installation error
Use this procedure to debug a 32-bit installation error when using Installation Manager.

The 32-bit Service Management Unite Performance Management package cannot be installed in JazzSM 64-bit core services. To correct this error use the default value for installing Service Management Unite Performance Management, which is to install as a new package group.

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.

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`.

DB2 access test hangs:

If the attempt to access the database does not return (an indeterminate dialog is shown for a very long time), the test may be hung. The DB2 password may be expired.

To resolve the problem, perform these steps:

1. End the installer. Because **Cancel** is not enabled at this point, end the installer using the `kill` command. If the installer is killed, files in the system temporary directory remain on the system. If desired, you can manually delete the files in the following way:

   Delete the directories `dirs /tmp/<xxxxxx>.tmp` and `/tmp/ install.dir.<xxxxxx>>` (where `<xxxxxx>` is an arbitrary number)
2. Check if the DB2 password is expired.
3. Renew the DB2 password.
4. Restart the installation.

Exceptions appear in file eezinstall.log:

Any NoClassDefFoundError exceptions that appear in the `eezinstall.log` file *before* the file EEZEAR was deployed can be ignored.

Note: In the last step of the install process the intermediate log is copied to the subfolder `install` in the user install directory. This copy omits the messages from the installer finish process (3 or 4 lines). If these lines are required the original install log should be read. This log file can be found in the `tmp` directory with a name of the form: `install.dir.xxxxxxxx`.

Troubleshooting for configuration

Use this topic for troubleshooting problems you experience when you configure IBM Service Management Unite.

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 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 22. 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 23. 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 24. 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 25. 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 26. 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 27. 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 28. 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 29. 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 30. 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 31. 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.

Gathering information for IBM Support

If you cannot resolve an installation problem, send the installation log file archive to IBM support (see "Using the log file collector utility" on page 125).

Troubleshooting SMU Performance Management

Troubleshooting and support information for Service Management Unite Performance Management 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.

Installation Manager 32-bit installation error

Use this procedure to debug a 32-bit installation error when using Installation Manager.

The 32-bit Service Management Unite Performance Management package cannot be installed in JazzSM 64-bit core services. To correct this error use the default value for installing Service Management Unite Performance Management, which is to install as a new package group.

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.

Increasing runtime memory

Tivoli Directory Integrator does not use all available memory so edit the ibmdisrv file to increase runtime memory and avoid out of memory errors. To increase the runtime memory, add the two **-Xms2048M -Xmx4096M** space-separated arguments to the Java invocation command.

Procedure

1. To increase the heap size of Java Virtual Machine, include **-Xms** and **-Xmx** options in the ibmdisrv script file. For example, to set the minimum heap memory size to 2048 bytes and maximum heap memory size to 4096 bytes, modify the script.

   Note: On Linux systems, the file name is ibmdisrv and the file is in the main Tivoli Directory Integrator directory.
2. Find the following line in ibmdisrv:

   ```
   "$TDI_JAVA_PROGRAM" $TDI_MIXEDMODE_FLAG -cp
   "$TDI_HOME_DIR/IDILoader.jar" "$LOG_4J"
   com.ibm.di.loader.ServerLauncher "$@" &
   ```
3. Change the script as shown:

   ```
   "$TDI_JAVA_PROGRAM" $TDI_MIXEDMODE_FLAG -Xms2048m -Xmx4096m -cp
   "$TDI_HOME_DIR/IDILoader.jar" "$LOG_4J"
   com.ibm.di.loader.ServerLauncher "$@" &
   ```

   Note: Do not copy and paste the examples into your ibmdisrv file. Add the two arguments without changing any of the other arguments.

Recycle the Tivoli Directory Integrator server

After you complete the post installation configuration tasks, manually recycle the Tivoli Directory Integrator server by issuing the following commands.

Procedure

1. To stop the Tivoli Directory Integrator server:

   ```
   ps -ef | grep TDI | gawk '!/grep/ {print $2}' | xargs kill -9
   ```

2. To start the Tivoli Directory Integrator server, if you are using the default solution directory:

   ```
   /opt/IBM/TDI/V7.1.1/ibmdisrv -d -s /opt/IBM/TDI/V7.1.1/DASH_ITMCollector
   &> /opt/IBM/TDI/V7.1.1/DASH_ITMCollector/logs/ibmdisrv.log &
   ```

Known problems and solutions

This section contains know problems and solutions of troubleshooting for Service Management Unite Performance Management.

Error installing into non-default package group

Use this procedure to debug an error installing into an existing package group.

Attempting to install the performance management package into an existing Installation Manager package group results in an error. Because performance management requires a unique package group, use the default settings and allow Installation Manager to create a new package group for performance management.

Invalid Configuration Location

Use this procedure to debug an invalid configuration location error.

This error can occur if the user ID that is doing the installation does not match the user ID that installed Installation Manager. A window with Invalid Configuration Location is displayed containing text starting with, "Locking is not possible in the directory *directory_path*." This error is related to file permission bits for `.fileTableLock` files within the configuration directory structure.

To fix this problem, change to the configuration directory within the *directory_path* described in the error, and issue the following commands:

```
chmod -R g+rwx .
chgrp -R groupName config_directory .
```

The *groupName* value is the primary group of the user attempting the 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.

TDISRVCTL installation failure

Use this procedure to debug a failure during Tivoli Directory Integrator installation.

If Tivoli Directory Integrator installation attempts result in a **tdisrvctl** command failure, verify that the Tivoli Directory Integrator server is active and that the security credentials for the command are valid.

The following command returns Tivoli Directory Integrator server status:

```
ps -ef | grep TDI
```

If the server is not active, open a terminal window and issue the following command from the Tivoli Directory Integrator installation directory:

```
ibmdisrv -d
```

If the server is active, the port and security parameters specified for the command on the configuration panel might be incorrect. An efficient method for debugging command problems is to issue a **tdisrvctl** command from the Tivoli Directory Integrator installation directory. For example, run the following command:

```
./bin/tdisrvctl –K serverapi/testadmin/jks –P administrator –T
testserver.jks –op srvinfo
```

The command uses the default TDI security for the –K,-T and –P parameters, which might have changed during your Tivoli Directory Integrator installation.

Unable to discover the installed TDI

Use this procedure to debug a failed Tivoli Directory Integrator prerequisite check when the correct TDI level is installed.

If the prerequisite check for Tivoli Directory Integrator fails but the correct level of Tivoli Directory Integrator is installed, Tivoli Directory Integrator might have been installed by a non-root user. To detect Tivoli Directory Integrator and its installed level, Installation Manager examines the file named .com.zerog.registry.xml. If Tivoli Directory Integrator was not installed by a root user, this file might be located in the home directory of the applicable non-root user. Search for the file and copy it to the /var directory, and then rerun the prerequisite check.

IBM Tivoli Monitoring CURI Data Provider not defined

Use this procedure to debug "no data" errors that occur if the IBM Tivoli Monitoring CURI Data Provider is not defined.

When you configure Service Management Unite, you must define the connection from the Dashboard Application Services Hub to the IBM Tivoli Monitoring CURI Data Provider. If Tivoli Directory Integrator is running, but the IBM Tivoli Monitoring CURI Data Provider connection is not defined, only partial data is available on the details pages. On these pages, some widgets show data, while other widgets display errors with a dataset name included in the error message. The error messages have "@ITMSD" at the end, which indicates the connection is not defined.

To detect if the dashboard data provider is defined, go to **Console Settings > Connections** and look for a connection with an ID of "ITMSD". If one is not listed, define the connection from Dashboard Application Services Hub to the IBM Tivoli Monitoring CURI Data Provider as described in the "Defining a CURI Data Provider connection" on page 98 topic.

IBM Tivoli Monitoring CURI Data Provider not enabled

Use this procedure to debug "no data" errors that occur if the IBM Tivoli Monitoring CURI Data Provider is not enabled.

If the System Health dashboard displays no data, check to see whether the dashboard data provider is enabled. When you configure the Tivoli Enterprise Portal Server, you must enable it to be a dashboard data provider to deliver data to Service Management Unite.

To detect if the dashboard data provider is enabled, in the Service Management Unite dashboard, go to **Console Settings > Connections**. If you correctly entered the server information details during post-installation configuration as described in "Defining a CURI Data Provider connection" on page 98, it is likely that the dashboard data provider was not enabled.

In the `SystemOut.log` file, a message displays saying that it cannot get to the Tivoli Enterprise Portal Server. This statement is an extra indication that the data provider is not enabled.

To enable the dashboard data provider, see the "Verifying the dashboard data provider is enabled" topic in the *IBM Tivoli Monitoring Installation and Setup Guide*.

Secure Sockets Layer connection error

Use this procedure to debug a failure to define the Secure Sockets Layer (SSL) connection between WebSphere Application Server and Tivoli Directory Integrator.

If the System Health page does not display automation events in the Events table, or automation domains in the Health Status widget, the SSL connection between WebSphere Application Server and Tivoli Directory Integrator might not be properly defined.

For the System Health page to display System Automation and OMEGAMON data, there must be an SSL connection established between Tivoli Directory Integrator and WebSphere Application Server. This connection should be defined during the installation process.

Tivoli Directory Integrator errors

Use this procedure to debug "no data" conditions that might occur because of Tivoli Directory Integrator issues.

The performance management component uses Tivoli Directory Integrator to get data. If Tivoli Directory Integrator is not configured correctly, you cannot access the details dashboards for performance management.

To detect a Tivoli Directory Integrator error, go to **Console Settings > Connections**. When the status of the Tivoli Directory Integrator is "No data returned", this indicates a problem between the Tivoli Directory Integrator component that runs inside of WebSphere Application Server and the Tivoli Directory Integrator server.

Try to edit the Tivoli Directory Integrator connection by clicking **OK** and then **Cancel**. If the status of the Tivoli Directory Integrator changes to "Working" in the Connections page, you can skip the rest of this topic. If it does not change to "Working", then continue with the following steps.

To verify that the Tivoli Directory Integrator server is running correctly, you can issue the following command:

`curl http://localhost:1098/rest`.

If the command returns a message that says "couldn't connect to the host", this message indicates that the server has a problem or is not running.

When there are two Tivoli Directory Integrator servers with the same solution directory running, the multiple processes running might cause a "no data" condition. The Tivoli Directory Integrator component that runs on WebSphere

Application Server can handle a single connection. If you are already using Tivoli Directory Integrator with other Jazz for Service Management products, you must use the same solution directory. All Tivoli Directory Integrator solutions or projects must be run in the same solution directory that Service Management Unite uses.

If a performance management workspace or the System Health dashboard displays "No data returned" and the Tivoli Directory Integrator components are running, there might be an issue in the Tivoli Directory Integrator connection. You might also see "Cannot Access Data Provider xxxxxxx@TDI" or "No Items to Display" messages in Dashboard Application Service Hub widgets. On the System Health page, if the System Automation domains or automation events are not displaying, this indicates an issue between Tivoli Directory Integrator and the System Automation data provider.

Note: Anything after the at sign (@) symbol in a data widget refers to the data provider used for the widget.

Tivoli Directory Integrator solution directory (SOLDIR) contains the properties files and logs. The logs subdirectory contains the `ibmdi.log` file where Tivoli Directory Integrator server messages are recorded. Each time an assembly line runs, messages and exceptions are written to the log. An exception typically causes an assembly line to fail and not return data, or return only some data. The last five Tivoli Directory Integrator logs are stored in `ibmdi.log.1` through `ibmdi.log.5`. Each time Tivoli Directory Integrator is restarted, a new log is rewritten.

Welcome page display error
Use this procedure to debug an error in displaying the welcome page.

This error can occur if a user was not granted the System Automation group permission of `EEZMonitor`.

To fix this issue, see "Displaying the Service Management Unite welcome page" on page 101.

Gathering information for IBM Support

If you cannot resolve an installation problem, send the installation log file archive to IBM support (see "Using the log file collector utility" on page 125).

Support for Service Management Unite

To access service and support for IBM Service Management Unite V1.1.2, use the following resources:

Service Management Unite software:
> http://www.ibm.com/software/products/en/service-management-unite

Customer portal:
> http://www.ibm.com/support/docview.wss?uid=swg21962625

Fix Central:
> http://www.ibm.com/support/fixcentral/

Service Engage:
> http://www.ibmserviceengage.com

Service Management Connect for System z:
> http://www.ibm.com/developerworks/servicemanagement/z/index.html

Support Portal:
        https://www.ibm.com/support/entry/portal

Chapter 9. Messages

This section contains messages for Service Management Unite Automation and Performance Management.

Message formats

This section introduces the formats of IBM Service Management Unite messages, including the text formats and description formats.

- Message text formats

  Most messages are preceded by an identifier, as illustrated in Figure 1.
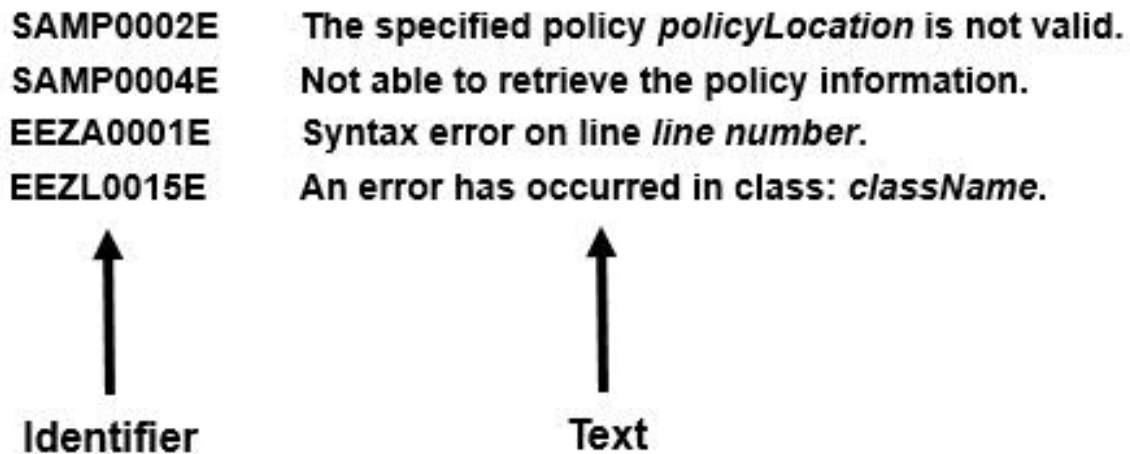
Figure 6. Sample message format

- 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.

Policy editor messages

This reference provides all messages that are generated by the policy editor of System Automation for Multiplatforms.

SAMP0001E An 'IOException' was caught 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 task is ended.

Operator response: Try to resolve the problem described in the exception message and resubmit the command.

SAMP0002E The specified policy *policyLocation* **is not valid.**

Explanation: The policy is not valid. You cannot perform any task with this policy.

System action: The current task ends.

Operator response: Try to make the policy valid by analyzing the error messages following this message. Then resubmit the command.

SAMP0003E 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 that may describe the root cause of the problem.

SAMP0004E Not able to retrieve the policy information.

Explanation: The policy information cannot be retrieved because the policy is not valid.

System action: The current task ends.

Operator response: Try to make the policy valid by analyzing all the error messages.

SAMP0005E Received errors when trying to activate the policy.

Explanation: Policy activation task resulted in errors.

System action: The activation task ends.

Operator response: Analyze the error messages and try to resolve the problem.

SAMP0006E The specified policy file " *policyFile* **" cannot be found.**

Explanation: The policy cannot be loaded from this location.

System action: The current task ends.

Operator response: Verify the policy XML file name and its path.

SAMP0007E Original Parser Exception: *exceptionMessage*

Explanation: An internal problem occurred while parsing this policy.

System action: The task cannot be performed.

Operator response: Verify if the product is installed correctly.

SAMP0008E Received errors when trying to deactivate the current policy.

Explanation: Policy deactivation resulted in errors.

System action: The deactivation task ends.

Operator response: Analyze the error messages and try to resolve the problem.

SAMP0009E Received errors when trying to check the policy.

Explanation: Policy check task resulted in errors.

System action: The check task ends.

Operator response: Analyze the error messages and try to resolve the problem.

SAMP0010E Received errors when trying to save the current policy.

Explanation: Policy save task resulted in errors.

System action: The save task ends.

Operator response: Analyze the error messages and try to resolve the problem.

SAMP0011E The resource with name *resourceName* **and class** *className* **was found as member of multiple groups.**

Explanation: A resource can only be member of one group.

System action: This policy is not valid and cannot be activated.

Operator response: Check that each resource is only member of at most one group element in this policy.

SAMP0012E **The resource with name** *resourceName* **and class** *className* **was found as member of an equivalency and of a group.**

Explanation: A resource cannot be member of a group and of an equivalency.

System action: This policy is not valid and cannot be activated.

Operator response: Check that each resource is only member of either a group or an equivalency.

SAMP0013E **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 is not valid.

Operator response: Check that the group has no duplicate <Members> child elements in this policy.

SAMP0014E **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.

SAMP0015E **The resource group with name** *resourceGroupName* **has a nesting level of more than 50.**

Explanation: The nesting level of a resource group is limited to 50.

System action: This policy is not valid and cannot be activated.

Operator response: Reduce the nesting level of this group and resubmit the command.

SAMP0016E **An 'Exception' was caught 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 task is ended.

Operator response: Try to resolve the problem described in the exception message and resubmit the command.

SAMP0017E **The relationship with the source with name** *sourceName* **and type** *type* **has a target with the same key.**

Explanation: A relationship cannot have the same source and target.

System action: This policy is not valid and cannot be activated.

Operator response: Correct the relationship and resubmit the command.

SAMP0018E **The relationship source with name** *sourceName* **and class** *sourceClass* **is not a resource group nor member of a resource group.**

Explanation: A relationship source must either be a resource group or member of a resource group.

System action: This policy is not valid and cannot be activated.

Operator response: Correct the relationship and resubmit the command.

SAMP0019E **An error occurred in method** *methodName* **of class** *className***. Error details** *details***.**

Explanation: The processing was interrupted by this error and cannot complete.

System action: The task is ended.

Operator response: Try to resolve the problem described in the error details and resubmit the command.

SAMP0020E **The specified <Relationship> with the <Type> "** *relationType* **", the <Source> with the name "** *source* **" and the <Target> with the name "** *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.

SAMP0021E **An 'UTFDataFormatException' was caught 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 task cannot be performed.

Operator response: Ensure the correct data format of

the policy document by only using editors which create UTF-8 conform documents.

SAMP0022E A *<Element>* **can only contain either a** *<subElement1>* **or a** *<subElement2>***.**

Explanation: It is not allowed to specify both kinds of sub-elements for this element.

System action: This policy cannot be activated.

Operator response: Check that at only one of the conflicting sub-elements is specified in this policy.

SAMP0023E A *<Element>* **that contains a** *<subElement1>* **must also contain a** *<subElement2>***.**

Explanation: It is not allowed to specify only one of these sub-elements for this element.

System action: This policy cannot be activated.

Operator response: Check that both sub-elements are specified in this policy.

SAMP0024E A *<Element>* **that contains a** *<subElement1>* **must also contain a** *<subElement2>* **or a** *<subElement3>***.**

Explanation: It is not allowed to specify only one of these sub-elements for this element.

System action: This policy cannot be activated.

Operator response: Check that both sub-elements are specified in this policy.

SAMP0025E The *<Element>* **with the name "** *referenceName* **" refers to a resource that does not exist on the cluster.**

Explanation: Every resource that is referenced within the policy must exist in the cluster.

System action: This policy cannot be activated.

Operator response: Create the resource on the cluster then resubmit the command.

SAMP0026E The node with the name " *nodeName* **" does not exist on the cluster.**

Explanation: Every node that is referred to within the policy must exist in the cluster.

System action: This policy cannot be activated.

Operator response: Correct the value of the node in the policy then resubmit the command.

SAMP0027E The node with the name " *nodeName* **" is not online in the cluster.**

Explanation: Every node that is referred to within a resource attribute must be online in the cluster.

System action: This policy cannot be activated.

Operator response: Correct the value of the node in the policy or make the node online then resubmit the command.

SAMP0028E The value " *domainName* **" of the element** *<elementName>* **does not conform to the real name of the cluster "** *actualDomainName* **".**

Explanation: The name of the cluster specified in the policy must be equal to the real name.

System action: This policy cannot be activated.

Operator response: Correct the value in the policy then resubmit the command.

SAMP0029E The specified element *<element>* **with the name "** *groupName* **" contains a member with a different name "** *memberName* **" .**

Explanation: For this kind of group all <Members> child elements must have the same name as the group itself.

System action: This policy is not valid.

Operator response: Check that the groups name is equal to all <Members> child elements names in this policy.

SAMP0030E The specified element *<element>* **was found more than once.**

Explanation: Only zero or one element of this type is allowed in the policy.

System action: This policy cannot be activated.

Operator response: Check that at most one element of this type is specified in the policy.

SAMP0031E The specified element *<childElement>* **was found more than once as child element of** *<parentElement>***.**

Explanation: Only zero or one element of this type is allowed.

System action: This policy cannot be activated.

Operator response: Check that at most one element of this type is specified in this policy.

SAMP0032E The specified element *<childElement>* **was found more than once as child element of** *<parentElement>* **with the name "** *parentName* **".**

Explanation: Only zero or 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.

SAMP0033E The value " *value* **" of the element** *<allowedNode>* **does not exist as a node, nor is an equivalency with this name defined.**

Explanation: This value must either be a node or the name of an equivalency.

System action: This policy is not valid and cannot be activated.

Operator response: Correct the policy and resubmit the command.

SAMP0034E The element *<element>* **with the name "** *equivalencyName* **" cannot be target of a location relationship.**

Explanation: A location relationship cannot have a target element of that kind.

System action: This policy is not valid and cannot be activated.

Operator response: Correct the relationship and resubmit the command.

SAMP0035E The element *<element>* **with the value "** *elementValue* **" can only be used with a location relationship except the relationship of the type "** *isStartableType* **".**

Explanation: A condition is not allowed for this kind of relationship.

System action: This policy is not valid and cannot be activated.

Operator response: Correct the relationship and resubmit the command.

SAMP0036E The element *<element>* **with the name "** *elementValue* **" has got members that are not from the same resource class.**

Explanation: All members of an equivalency must be from the same resource class.

System action: This policy is not valid and cannot be activated.

Operator response: Correct the equivalency and resubmit the command.

SAMP0037E The connection to the backend failed because the following exception occurred: *exception*

Explanation: An exception occurred when trying to perform an operation on the backend.

System action: The policy cannot be activated.

Operator response: Analyze the exception description and try to correct the problem.

SAMP0038E The element *<tie-breaker>* **with the name "** *name* **" is set to active although at least one other element of this kind is set to active, too.**

Explanation: Only one such element is allowed to be active.

System action: The policy cannot be activated.

Operator response: Ensure there is at most one active element of this kind in the policy and resubmit the command.

SAMP0039E The specified element *<element>* **with the value "** *value* **" of the subelement** *<subelement1>* **cannot contain a subelement** *<subelement2>* **as well.**

Explanation: For this kind of element some subelements are not allowed for certain subelement values.

System action: This policy is not valid.

Operator response: Remove the invalid subelement or change the value of the other subelement and resubmit the command.

SAMP0040E An IOException was caught when trying to write the policy to the file " *filename* **". The exception message was:** *exception-message***.**

Explanation: The file could not be written.

System action: The active task ends.

Operator response: Ensure the directory does exist and there is enough disk space available then resubmit the command.

SAMP0041E Exception occurred when trying to validate the selection string " *selectString* **". Either the selection string is not valid or the connection to the backend failed. Exception message was:** *exception***.**

Explanation: An exception occurred when trying to validate the selection string.

System action: The policy cannot be activated.

Operator response: Ensure the selection string is valid. Analyze the exception description and try to correct the problem.

SAMP0042E **The <*Element*> with the name "** *referenceName* **" has an invalid value for the subelement <*Sub-Element*>.**

Explanation: <ResourceReference> elements may not have one of the following values for their <Class> subelement: IBM.Application, IBM.ServiceIP, IBM.Test .

System action: This policy cannot be activated.

Operator response: Correct the subelement value then resubmit the command.

SAMP0043E **The <*Element*> with the type "** *value* **" is not allowed on a "** *value* **" system.**

Explanation: The processing was interrupted by this error and cannot complete.

System action: This policy cannot be activated.

Operator response: Correct the value then resubmit the command.

SAMP0044E **A <*Element*> must either contain a <*Subelement*> or a <*Subelement*>.**

Explanation: The processing was interrupted by this error and cannot complete.

System action: This policy cannot be activated.

Operator response: Correct the element then resubmit the command.

SAMP0045E **An IOException was caught when trying to read from the included policy file "** *filename* **". The exception message was:** *exception-message***.**

Explanation: The file could not be read.

System action: The active task ends.

Operator response: Ensure the file does exist and the userid used for the command has sufficient access rights then resubmit the command.

SAMP0046E **The syntax of the input policy file "** *filename* **" is invalid. The line in error is:** *invalid line***.**

Explanation: The input policy file contains an invalid line.

System action: The active task ends.

Operator response: Correct the invalid line in the input file then resubmit the command.

SAMP0047E **Variable referenced within line "** *invalid line* **" not found in top-level XML file. Variable is referenced within file: "** *inputfilename* **".**

Explanation: The input policy contains a variable that is not defined in the top-level XML file.

System action: The active task ends.

Operator response: Add the variable to the top-level XML file then resubmit the command.

SAMP0048E **The policy created from the top-level file** *policyLocation* **is not valid. The resulting policy can be found in the temporary file** *temp-filename***.**

Explanation: The resulting policy is not valid. You cannot perform any task with this policy.

System action: The current task ends.

Operator response: Try to make the policy valid by analyzing the error messages following this message. Then resubmit the command.

SAMP0049E **An error occurred in class:** *className* **method:** *methodName***. The resource** *resourceName* **could not be defined. There was no exception, but the define call did not return any object either.**

Explanation: The current process was interrupted by this exception and cannot complete.

System action: The policy activation process stops and will return with this error message.

Operator response: Check if this resource was described properly in the XML policy document and restart the activation.

SAMP0050E **An error occurred in class:** *className* **method:** *methodName***. The resource** *resourceName* **could not be defined. The received exception was** *exception*

Explanation: The process was interrupted by this exception and cannot complete.

System action: The policy activation process stops and will not complete.

Operator response: Check if this resource was described properly in the XML policy document and restart the activation.

SAMP0051E An error occurred in class: *className* **method:** *methodName*. **The resource** *resourceName* **could not be added to the resource group** *groupName*. **The received exception was** *exception*

Explanation: The process was interrupted by this exception and cannot complete.

System action: The policy activation process stops and will not complete.

Operator response: Try to solve the problem described in the exception message and resubmit the command.

SAMP0052E An error occurred in class: *className* **method:** *methodName*. **The resource group** *groupName* **could not be set to the desired state** *state*. **The received exception was** *exception*

Explanation: The process was interrupted by this exception and cannot complete.

System action: The policy activation process stops and will not complete.

Operator response: Try to solve the problem described in the exception message and resubmit the command.

SAMP0053E An error occurred in class: *className* **method:** *methodName*. **The resource** *resourceName* **could not be undefined. The received exception was** *exception*

Explanation: The reason could be that the resource is not Offline or FailedOffline or the resource might have been deleted before by internal commands.

System action: The policy activation or deactivation will continue.

Operator response: Check if the resource still exists. Analyze the exception and try to resubmit the command.

SAMP0054E An error occurred in class: *className* **method:** *methodName*. **The resource** *resourceName* **could not be identified and located. This can be caused by an exception or the resource could not be found. Therefore the resource** *resourceName* **cannot be added to the resource group** *groupName*. **The received exception was** *exception*

Explanation: The process was interrupted by this exception and cannot complete.

System action: The policy activation process stops and will not complete.

Operator response: Try to solve the problem described in the exception message and resubmit the command.

SAMP0055E An error occurred in class: *className* **method:** *methodName*. **The resource group** *groupName* **could not be identified and located. This can be caused by an exception or the resource could not be found. Therefore the resource group** *groupName* **cannot be set to the state** *state*. **The received exception was** *exception*

Explanation: The process was interrupted by this exception and cannot complete.

System action: The policy activation process stops and will not complete.

Operator response: Try to solve the problem described in the exception message and resubmit the command.

SAMP0056E An error occurred in class: *className* **method:** *methodName*. **The resource** *resourceName* **could not be identified and located. This can be caused by an exception or the resource could not be found. Therefore the resource** *resourceName* **cannot be created, because it requires resource** *resourceName*. **The received exception was** *exception*

Explanation: The process was interrupted by this exception and cannot complete.

System action: The policy activation process stops and will not complete.

Operator response: Try to solve the problem described in the exception message and resubmit the command.

SAMP0057E An error occurred in class: *className* **method:** *methodName*. **The resource** *resourceName* **could not be identified and located. This can be caused by an exception or the resource could not be found. Therefore the resource** *resourceName* **cannot be deleted. The received exception was** *exception*

Explanation: The resource might have been deleted before by internal commands.

System action: The current process will continue.

Operator response: Check if the resource still exists. Analyze the exception and try to resubmit the command.

SAMP0058E An error occurred in class: *className* **method:** *methodName*. **The resource** *resourceName* **could not be identified and located. This can be caused by an exception or the resource could not be found. Therefore the resource** *resourceName* **cannot be modified. The**

received exception was *exception*

Explanation: The process was interrupted by this exception and cannot complete.

System action: The current process will continue.

Operator response: Check if the resource still exists. Analyze the exception and try to resubmit the command.

SAMP0059E An error occurred in class: *className* **method:** *methodName*. **The resource** *resourceName* **could not be modified. There was no exception, but the define call did not return any object either.**

Explanation: The current process was interrupted by this exception and cannot complete.

System action: The policy activation process stops and will return with this error message.

Operator response: Check if this resource was described properly in the XML policy.

SAMP0060E An error occurred in class: *className* **method:** *methodName*. **The resource** *resourceName* **could not be modified. The received exception was** *exception*

Explanation: The current process was interrupted by this exception and cannot complete.

System action: The policy activation process stops and will return with this error message.

Operator response: Check if this resource was described properly in the XML policy and restart the activation.

SAMP0061E An error occurred in class: *className* **method:** *methodName*. **The IBM.TieBreaker resource** *resourceName* **could not be identified and located. The received exception was** *exception*

Explanation: The current process was interrupted by this exception and cannot complete.

System action: The policy activation process stops and will return with this error message.

Operator response: Check if this resource was described properly in the XML policy and restart the activation.

SAMP0062E An error occurred in class: *className* **method:** *methodName*. **The active IBM.TieBreaker resource could not be identified and located. Therefore the IBM.TieBreaker resource** *resourceName* **could not be modified or created. The received exception was** *exception*

Explanation: The current process was interrupted by this exception and cannot complete.

System action: The policy activation process stops and will return with this error message.

Operator response: Check if this resource was described properly in the XML policy and restart the activation.

SAMP0063E An error occurred in class: *className* **method:** *methodName*. **The IBM.TieBreaker resource** *resourceName* **could not be set to active. The received exception was** *exception*

Explanation: The current process was interrupted by this exception and cannot complete.

System action: The policy activation process stops and will return with this error message.

Operator response: Check if this resource was described properly in the XML policy and restart the activation.

SAMP0064E An error occurred in class: *className* **method:** *methodName*. **The subscription from consumer** *consumer* **to resource** *resourceName* **has failed. The received exception was** *exception*

Explanation: The current process was interrupted by this exception and cannot complete.

System action: The policy activation process stops and will return with this error message.

Operator response: Check if this resource was described properly in the XML policy and restart the activation.

SAMP0065E The attempt to update the current automation policy failed because errors were detected.

Explanation: The policy update task resulted in errors.

System action: The policy update task ends.

Operator response: Analyze the subsequent error messages and try to resolve the problem.

SAMP0066E The *<element>* **with the name** *elementName* **contains a member that has an invalid value** *className* **for its attribute class.**

Explanation: For this kind of element the value of the class attribute must be equal for all its members.

System action: This policy cannot be activated.

Operator response: Check that all members have the correct value for the class attribute.

SAMP0067E **An error occurred in class:** *className* **method:** *methodName*. **The resource** *resourceName* **could not be removed from the resource group** *groupName*. **The received exception was** *exception*

Explanation: The process was interrupted by this exception and cannot complete.

System action: The policy activation process stops and will not complete.

Operator response: Try to solve the problem described in the exception message and resubmit the command.

SAMP0068E **The specified resource group with the name "** *name* **" contains a member that is a** *<subelement>*. **This is only allowed for resource groups that have a value of "** *value* **" for the subelement** *<subelement1>*.

Explanation: Resource groups that are collocated cannot have concurrent members.

System action: This policy is not valid.

Operator response: Remove the invalid member or change the value of the subelement and resubmit the command.

SAMP0070E **An error occurred in class:** *className* **method:** *methodName*.

Explanation: The current process was interrupted by this exception and cannot complete.

System action: The policy deactivation process stops and will return with this error message.

Operator response: Try to submit the command again.

SAMP0071E **An error occurred in class:** *className* **method:** *methodName*.

Explanation: The current process was interrupted by this exception and cannot complete.

System action: The policy save process stops and will return with this error message.

Operator response: Try to submit the command again.

SAMP0072E **Failed to set information about the activated policy file name:** *fileName*, **the error message is:** *error-message*.

Explanation: The actual activation of the policy was successful, but saving its name and time failed.

System action: The name of the file of the activated policy and the activation time was not saved.

Operator response: Try to submit the command again.

SAMP0073E **Failed to set information about deactivating a policy. The error message is:** *error-message*.

Explanation: The actual deactivation of the policy was successful, but saving the fact failed.

System action: The fact that the policy was deactivated was not saved.

Operator response: Try to submit the command again.

SAMP0074E **The** *<Element>* **element with the name** *elementName* **must contain a** *<Subelement>* **subelement, because it describes an IPv6 address.**

Explanation: The required subelement is missing. The processing was interrupted by this error and cannot complete.

System action: This policy cannot be activated.

Operator response: Correct the element then resubmit the command.

SAMP0075E **The** *<Element>* **element with the name** *elementName* **contains both a** *<Subelement>* **subelement and a** *<Subelement>* **subelement.**

Explanation: It is not allowed to specify both subelements. The processing was interrupted by this error and cannot complete.

System action: This policy cannot be activated.

Operator response: Correct the element then resubmit the command.

SAMP0076E **The** *<Element>* **element with the name** *elementName* **contains a** *<Subelement>* **subelement that is too large.**

Explanation: The processing was interrupted by this error and cannot complete.

System action: This policy cannot be activated.

Operator response: Correct the element then resubmit the command.

SAMP0077E **The** *<Element>* **element with the name** *elementName* **contains a link local address.**

Explanation: The processing was interrupted by this error and cannot complete.

System action: This policy cannot be activated.

Operator response: Correct the element then resubmit the command.

SAMP0078E **The *\<Element\>* element with the name *elementName* contains a multicast address.**

Explanation: The processing was interrupted by this error and cannot complete.

System action: This policy cannot be activated.

Operator response: Correct the element then resubmit the command.

SAMP0079E **The *\<Element\>* element is not supported with the current Active Version *avn*.**

Explanation: The processing was interrupted by this error and cannot complete.

System action: This policy cannot be activated.

Operator response: Correct the element or update the Active Version then resubmit the command.

SAMP0080E **The activation task was not able to delete all existing resources. The reason for this is shown in the previous messages.**

Explanation: Deletion of existing resources failed. The processing was interrupted by this error and cannot complete.

System action: The activation task ends.

Operator response: If the reason for the failure is that some resource is not Offline respectively Failed Offline then you may retry the command using the force option -f.

SAMP0081E **The deactivation task was not able to delete all existing resources. The reason for this is shown in the previous messages.**

Explanation: Deletion of resources failed. The processing was interrupted by this error and cannot complete.

System action: The deactivation task ends.

Operator response: If the reason for the failure is that some resource is not Offline respectively Failed Offline then you may retry the sampolicy command using the force option -f.

SAMP0082E **The update task was not able to delete all existing resources. The reason for this is shown in the previous messages.**

Explanation: Deletion of existing resources failed. The processing was interrupted by this error and cannot complete.

System action: The update task ends.

Operator response: If the reason for the failure is that some resource is not Offline respectively Failed Offline then you may retry the command using the force option -f.

SAMP0083E **The value *value* of the var element with name *name* is either not valid for the specified type " *type* " or did not pass the extended value check.**

Explanation: The value specified needs to be of the specified type and pass the extended value check.

System action: This policy is not valid and cannot be activated.

Operator response: Correct the value and resubmit the command.

SAMP0084E **The value attribute of the var element with name *name* must not be empty.**

Explanation: The value attribute must not be empty.

System action: This policy is not valid and cannot be activated.

Operator response: Specify a value and resubmit the command.

SAMP0085E **The *attribute* attribute value of the include element that points to file *file* must not be empty.**

Explanation: The attribute value must not be empty.

System action: This policy is not valid and cannot be activated.

Operator response: Specify a value and resubmit the command.

SAMP0086E **At least on of the value attributes of the nested var elements of varoption element with name *name* is not valid for the specified type.**

Explanation: The value specified needs to be of the specified type.

System action: This policy is not valid and cannot be activated.

Operator response: Correct the value and resubmit the command.

SAMP0087E **The *element* attribute value of the var element with name *name* must not be empty.**

Explanation: The attribute value must not be empty.

System action: This policy is not valid and cannot be activated.

Operator response: Specify a value and resubmit the command.

SAMP0088E The dynSelString attribute of the var element with name *name* must not contain only one var name.

Explanation: There must be more than one var name in the dynSelString attribute.

System action: This policy is not valid and cannot be activated.

Operator response: Specify two var names separated by "," and resubmit the command.

SAMP0089E At least one var that is referenced in the dynSelString attribute of the var element with name *name* does not exist.

Explanation: The var elements referenced in the dynSelString attribute must exist for the policy.

System action: This policy is not valid and cannot be activated.

Operator response: Specify two var names separated by "," and resubmit the command.

SAMP0090E The var element referenced in the multi attribute of the include element that points to file *name* does not exist.

Explanation: A var element that is referenced in a multi attribute value must exist for the policy.

System action: This policy is not valid and cannot be activated.

Operator response: Remove the include element or change the value of the multi attribute to an existing var; then resubmit the command.

SAMP0091E Two include elements must not point to the same file: *file*.

Explanation: Two include elements must not point to one and the same xml file.

System action: This policy is not valid and cannot be activated.

Operator response: Remove one include element or change the xml file it points to; then resubmit the command.

SAMP0092E If the enumeration attribute is set to value="choice", the attribute validValues must also be specified and vice versa. The var element with name *name* does contain either only enumeration=choice or validValue.

Explanation: If you set the enumeration attribute to

value="choice", the validValues attribute must also be specified. If you specify the validValue attribute, you must set the enumeration attribute to value="choice".

System action: This policy is not valid and cannot be activated.

Operator response: Either specify both values or remove the specified enumeration=choice/validValues attribute. Resubmit the command.

SAMP0093E At least one of the entries of the validValues attribute value does not match the specified type attribute value and/or the min/max attribute values of the var element with name *name*.

Explanation: All entries of the validValues attribute value must comply with the specified type attribute value and or the min/max attribute values.

System action: This policy is not valid and cannot be activated.

Operator response: Correct the validValues attribute value and resubmit the command.

SAMP0094E At least one var that is referenced in the multi attribute of the include element that points to the xml file *file* does not exist.

Explanation: The var elements referenced in the multi attribute must exist for the policy.

System action: This policy is not valid and cannot be activated.

Operator response: Specify existing var names separated by "," and resubmit the command.

SAMP0095E The value attribute of the varoption element with name *name* must not be empty.

Explanation: The value attribute must not be empty.

System action: This policy is not valid and cannot be activated.

Operator response: Specify either "yes" or "no" and resubmit the command.

SAMP0096E There is no valid license available for the policy you are trying to activate.

Explanation: The policy you are trying to activate requires a separate license that is currently not installed.

System action: This policy cannot be activated without the missing license.

Operator response: Install the license and resubmit the command.

SAMP0097E The value of the max attribute is smaller than the value of the min attribute for the var element with name *name***.**

Explanation: The value of the max attribute must be greater than or equal to the value of the min attribute.

System action: This policy is not valid and cannot be activated.

Operator response: Correct the min and max attribute values and resubmit the command.

SAMP0098E For a var element with attribute enumeration=array, each value must have the same number of sub-values as specified in the var name. The var element with name *name* **does not comply to this rule.**

Explanation: For a var element with attribute enumeration=array, the attribute name contains multiple sub-elements, separated by "||". Like for var elements with attribute enumeration=list, multiple values can be specified, each separated by ",", However, each value must have the same number of sub-values as the attribute name, also separated by "||". Example: The var name is "varOne||varTwo". A valid value entry would be "valueOne_1||valueTwo_1,valueOne_2||valueTwo_2"

System action: This policy is not valid and cannot be activated.

Operator response: Correct the number of sub-values and resubmit the command.

SAMP0099E For an include element with attribute matrix specified, the first var name value of the matrix must point to a var with attribute ref set, the second var name value must point to a var element of enumeration type multilist. The include element that points to the xml file *name* **does not comply to this rule.**

Explanation: The matrix attribute of an include element must contain exactly two values, the first one pointing to a var with attribute ref set, the second value pointing to a var element of enumeration type multilist.

System action: This policy is not valid and cannot be activated.

Operator response: Correct the values of the matrix attribute and resubmit the command.

SAMP0100E For a var element with attribute ref used, the attribute valuePrefix must be set as well. The var element with name *name* **does not comply to this rule.**

Explanation: For a var element that has the attribute

ref set, the valuePrefix attribute must also be set.

System action: This policy is not valid and cannot be activated.

Operator response: Add the valuePrefix attribute.

SAMP0101E For a var element with enumeration multilist, the type attribute must not be boolean. The var element with name *name* **does not comply to this rule.**

Explanation: For a var element that has the attribute enumeration set to multilist, the type attribute must not be set to boolean.

System action: This policy is not valid and cannot be activated.

Operator response: Correct the type attribute.

SAMP0102E The var element with name *name* **has a different number of values than the var elements with the names** *name***. This is not valid.**

Explanation: All var elements that are referenced in a multi attribute of an include element must have the same number of values. All but the first var elements that are referenced in a matrix attribute of an include element must have the same number of values.

System action: This policy is not valid and cannot be activated.

Operator response: Specify the same number of values for each of the var elements.

SAMP0103E Sampolicy template processing was stopped because no policy pool is configured.

Explanation: Sampolicy template processing requires a configured policy pool. If no policy pool is defined, template processing cannot be performed.

System action: This policy cannot be processed.

Operator response: Use the cfgsamadapter configuration utility to configure a policy pool.

SAMP0104E This policy template is not the latest version. This policy cannot be processed using the sampolicy wizard. The current version of this policy is *version***, the minimum version for this policy is** *version***.**

Explanation: A policy with an earlier version than the latest supported needs to be migrated to the latest version using the wizard.

System action: This policy is not valid and cannot be activated.

Operator response: Use the sampolicy wizard migrate option to migrate the current policy to the latest version.

SAMP0105E **Sampolicy template processing was stopped because the configuration file for the policy pool could not be read. The following exception occured:** *exception*

Explanation: Sampolicy template processing requires a configured policy pool. If the configuration file for the policy pool cannot be read, template processing cannot be performed.

System action: This policy cannot be processed.

Operator response: Analyse the message of the exception and ensure that the configuration file exist and is readable.

SAMP0106E **Sampolicy template processing was stopped because the policy pool directory** *dir* **either does not exist or is not writable.**

Explanation: Sampolicy template processing requires a configured policy pool. This directory must exist and be enabled for read and write operations. If the policy pool does not exist or is not enabled for read and write, template processing cannot be performed.

System action: This policy template file cannot be processed.

Operator response: Ensure that the policy pool directory exist and is enabled for read and write.

SAMP0500W **The policy contains no resource group.**

Explanation: The policy is valid, but without a resource group there is no automation active.

System action: Processing continues.

Operator response: Ensure this is what you want to do. Otherwise change the policy to contain at least one resource group and resubmit the command.

SAMP0501W **An 'Exception' was caught in method** *methodName* **of class** *className*. **The received message was** *message*.

Explanation: The processing was interrupted by this exception but it can continue.

System action: Processing continues.

Operator response: Try to resolve the problem described in the exception message.

SAMP0502W **The two <Relationship> elements with <Type> "StartAfter" and <Type> "StopAfter" were found with the same <Source> with the name "** *source* **" and <Target> with the name "** *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".

SAMP0503W **All members of the group with the name "** *groupName* **" should be collocated, because the group is part of a location relationship or of a relationship of the type "** *dependsOnType* **". Set the value of the groups tag** <*memberLocation*> **to "** *collocatedValue* **".**

Explanation: For these kinds of relationships all members of a source or target group should be collocated.

System action: Application continues.

Operator response: Check that all members of this group are collocated in this policy.

SAMP0504W **The specified <Relationship> with <Type> "** *relationType* **" and <Source> with the name "** *Sourcename* **" and <Target> with the name "** *Target* **" was found in a loop.**

Explanation: <Relationship> elements of the same <Type> where one <Relationship> element <Target> is the next <Relationship> element <Source> should not form a loop.

System action: Application continues.

Operator response: Check that the <Relationship> elements are not defined as loop in this policy.

SAMP0505W **A <Relationship> with the <Type> "** *relationType* **" was found that has linked more than 100 resources.**

Explanation: The numbers of resources linked by a relationship is limited to 100.

System action: Application continues.

Operator response: Reduce the number of resources linked by the relationship.

SAMP0506W The specified element *<element>* **with the value "** *value* **" of the subelement** *<subelement1>* **should not contain a subelement** *<subelement2>* **as well. This subelement is ignored.**

Explanation: For this kind of element some subelements are not supported for certain subelement values.

System action: Application continues. Subelement is ignored.

Operator response: Remove the invalid subelement or change the value of the other subelement.

SAMP0507W 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.

SAMP0508W An error occurred in method *methodName* **of class** *className***. Error details** *details***.**

Explanation: The processing was interrupted by this error but it can continue.

System action: Processing continues.

Operator response: Try to resolve the problem described in the error details.

SAMP0509W A non-critical error occurred in method *methodName* **of class** *className* **during activation of a new policy. Error details** *details***.**

Explanation: The processing was interrupted by this error but it can continue.

System action: Activation continues.

Operator response: Try to resolve the problem described in the error details. Try to activate the policy again and check if the error still occurs.

SAMP0510W A non-critical error occurred in method *methodName* **of class** *className* **during deactivation of the current policy. Error details** *details***.**

Explanation: The processing was interrupted by this error but it can continue.

System action: Deactivation continues.

Operator response: Try to resolve the problem described in the error details. Try to deactivate the policy again and check, if the error still occurs.

SAMP0511W A non-critical error occurred in method *methodName* **of class** *className* **during saving of the current policy. Error details** *details***.**

Explanation: The processing was interrupted by this error but it can continue.

System action: Saving process continues.

Operator response: Try to resolve the problem described in the error details. Resubmit the save command and check if the error still occurs.

SAMP0512W The resource group member *name* **is specified with the invalid attribute combination of non-mandatory and "** *value* **".**

Explanation: For this kind of element this combination of attribute values is invalid.

System action: Processing continues.

Operator response: Correct the invalid value and resubmit the command.

SAMP0513W Resource group *groupName* **is still not offline and cannot be removed.**

Explanation: The update/remove task tried to offline the resources that shall be removed. But at least one resource still is online.

System action: The processing was interrupted by this error and cannot complete.

Operator response: Try to resolve the problem described in the error details. Resubmit the update/remove command and check, if the error still occurs.

SAMP0514W The name of the resource *resourceName* **exceeds the allowed length.**

Explanation: A resource was detected in the domain, whose name exceeds the allowed length.

System action: Processing continues.

Operator response: It is recommended to change the resource name to a value that does not exceed the allowed length. Then resubmit the command.

SAMP1001I The specified policy *policyLocation* **is valid.**

Explanation: The policy is valid and can be activated.

System action: Processing continues.

Operator response: No action required.

SAMP1002I   The policy has the following policy information:

Explanation: This is the information for the policy.

System action: Processing continues.

Operator response: No action required.

SAMP1003I   The policy has been activated successfully.

Explanation: The policy is now active in the domain.

System action: Processing continues.

Operator response: No action required.

SAMP1004I   The activation task ends.

Explanation: The policy is not going to be activated because the user did not confirm this action.

System action: Processing ends.

Operator response: No action required.

SAMP1005I   The activation task ends.

Explanation: The automation policy could not be activated.

System action: Processing ends.

Operator response: Try to make the policy valid by analyzing the error messages following this message. Then resubmit the command.

SAMP1007I   The automation policy was deactivated successfully.

Explanation: There is now no policy active in the domain.

System action: Processing continues.

Operator response: No action required.

SAMP1008I   Template processing failed. The active task ends.

Explanation: Template processing failed and therefore the active task cannot complete successfully.

System action: Processing ends.

Operator response: Try to make the template policy valid by analyzing the error messages following this message. Then resubmit the command.

SAMP1009I   The automation policy was updated successfully.

Explanation: The current automation policy was updated with the new policy.

System action: Processing continues.

Operator response: No action required.

SAMP1010I   The update task ends because you did not confirm the action.

Explanation: The current automation policy can only be updated if you confirm the update action.

System action: Processing ends.

Operator response: No action required.

SAMP1011I   The attempt to update the current automation policy failed.

Explanation: The current automation policy could not be updated.

System action: Processing ends.

Operator response: Try to make the policy valid by analyzing the error messages following this message. Then resubmit the command.

EEZ message catalog

This section lists the messages that are generated by subcomponents of the IBM Service Management Unite 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** – Agentless 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.

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 "** *loaclNode* **" 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 "** *loaclNode* **" 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 "** *loaclNode* **" 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 "** *loaclNode* **" 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 "** *loaclNode* **" 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 "** *loaclNode* **" 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.

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).

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.

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. 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).

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.

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.

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.

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*

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.

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.

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 Agentless 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 Agentless 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 Agentless 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 (Agentless 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 Agentless 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 Agentless 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 Agentless 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 timout occurred while executing the command "** *cmdName* **" on remote node "** *remoteNode* **" with the timout** *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 Agentless Adapter is located.

System action: No policy file was saved.

Operator response: Check if there is enough disk space on the node where the Agentless 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 Agentless Adapter is located.

System action: No policy file was read.

Operator response: Check if the file exists on the node where the Agentless 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 Agentless 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 notifed 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 notifed 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 notifed 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 notifed 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 **Invalid time range selection for system log messages.**

Explanation: The specified time range selection for the collection of system log messages is invalid.

System action: No system log messages are collected.

Operator response: Retry with a valid time range selection.

EEZU0043E **Invalid time format for system log messages:** *Exception text*

Explanation: The specified time format for the collection of system log messages is invalid.

System action: No system log messages are collected.

Operator response: Retry with a valid time format.

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: E2E 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: E2E 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: E2E 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 E2E 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 E2E 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: E2E Adapter security context switch successful. The command was executed but the response signals a misbehavior which cannot be exactly identified by the E2E adapter.

System action: It is not clear if the command was executed, partly executed or not executed at all.

Operator response: Analyze the E2E 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.

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/.

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.

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 online and communication state is OK.

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.

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.

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 an agentless 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.

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.

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.

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 online 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.

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.

SMU Performance Management messages

All messages that are generated by Service Management Unite Performance Management 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 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.

KWU0001W Error while running the Prerequisite Scan. The Prerequisite Scan cannot proceed.

Operator response: The scan cannot be run for different reasons: the temporary directory does not have at least 5 MB, or the system registries are corrupted. Analyze the Installation Manager log files to see more details on the error. Check the troubleshooting information for a solution.

KWU0002W You did not install the WebSphere Application Server V 8.5.5.4 or higher. Installation of DASH extensions disabled.

Operator response: Install the WebSphere Application Server at a supported level and rerun the installation.

KWU0003W You did not install Core services in Jazz for Service Management 1.1.2 or higher. Installation of DASH extensions disabled.

Operator response: Install the Core services in Jazz for Service Management and rerun the installation.

KWU0004W You did not install the IBM Dashboard Application Services Hub 3.1.2 or higher. Installation of DASH extensions disabled.

Operator response: Install the IBM Dashboard Application Services Hub 3.1.2 and rerun the installation.

KWU0005W The program cannot verify the system prerequisites.

Operator response: Before proceeding with the installation, verify that your workstation meets all the required prerequisites by reading the IBM Workload Scheduler System Requirements.

KWU0006W You did not install IBM Tivoli Directory Integrator V7.1.1.4 or higher. Installation of TDI extensions disabled.

Operator response: Install TDI at a supported level and rerun the installation.

KWU0007E Internal error encountered in prerequisite checking.

Operator response: Check Installation Manager logs for information on the error.

KWU0101E Missing value for the "{0}" field.

Explanation: The specified input field has been left blank.

Operator response: Supply a value for the missing field.

KWU0102E DASH profile directory not found in JazzSM profile.

Explanation: The properties/.tipinfo properties file was not found in the DASH profile directory.

Operator response: Check the value specified for the DASH directory.

KWU0103E Websphere security credentials invalid.

Explanation: A WSADMIN command failed because of invalid security credentials.

Operator response: Check the Websphere user ID and password.

KWU0104E Unable to connect to WAS server.

Explanation: A WSADMIN command failed because a connection could not be established to a server.

Operator response: Ensure that the WAS server is active.

KWU0105E Specified TDI install directory does not exist.

Explanation: The directory specified as the TDI install directory could not be found.

Operator response: Ensure that the directory location is correct.

KWU0106E Missing or invalid value supplied for TDI server port.

Explanation: The TDI server port field is blank or contains a non-numeric value.

Operator response: Enter the correct port.

KWU0107E The TDI keystore file cannot be found.

Explanation: The TDI keystore file location is blank or invalid.

Operator response: Supply the location of the TDI keystore file.

KWU0108E The TDI truststore file cannot be found.

Explanation: The TDI truststore file location is blank or invalid.

Operator response: Supply the location of the TDI truststore file.

KWU0109E   Unable to connect to the TDI server.

Explanation: The TDI server may not be active or the supplied security credentials are invalid.

Operator response: Check that the TDI server is active and the credentials are valid.

KWU0110E   The specified JazzSM profile node directory is invalid.

Explanation: The JazzSM profile node directory is blank or does not exist.

Operator response: Supply the location of the JazzSM profile node directory.

KWU0111E   The specified TDI trust store directory is invalid.

Explanation: The TDI trust store directory is blank or does not exist.

Operator response: Supply the location of the TDI trust store directory.

Index

J

Java EE framework
  environment variables 113
jazz
  post-installation 101
Jazz for Service Management 40
  installation 16, 38
  installing 11

L

LDAP
  configure 88
  entity types 91
LDAP groups
  authorize 95
LDAP repository
  migrating 93
  security realm 91
LDAP server 89
LDAP user registry
  configuring 86
  federated repository 87
  planning 87
local agentless adapter
  saving 62
log file collector utility 125
log files 130
  automation engine 106
  automation framework 106
log viewer 106
LTPA settings
  LTPA password 101
  LTPA timeout 101

M

messages
  EEZ 152
  EEZ prefix 152
  Performance Management 216
  policy editor 138
  Service Management Unite 103
Messages
  EEZA0001E 152
  EEZA0002E 152
  EEZA0003E 153
  EEZA0004E 153
  EEZA0006E 153
  EEZA0007E 153
  EEZA0008E 153
  EEZA0009E 153
  EEZA0010E 153
  EEZA0011E 153
  EEZA0012E 154
  EEZA0013E 154
  EEZA0014E 154
  EEZA0015E 154
  EEZA0017E 154
  EEZA0022E 154
  EEZA0023E 154
  EEZA0024E 154
  EEZA0025E 154
  EEZA0026E 154
  EEZA0027E 154
  EEZA0028E 155

Messages *(continued)*
  EEZA0029E 155
  EEZA0030E 155
  EEZA0031E 155
  EEZA0032E 155
  EEZA0033E 155
  EEZA0036E 155
  EEZA0037E 155
  EEZA0038E 155
  EEZA0039E 155
  EEZA0040E 156
  EEZA0041E 156
  EEZA0042E 156
  EEZA0043E 156
  EEZA0045E 156
  EEZA0047E 156
  EEZA0051W 156
  EEZA0052E 156
  EEZA0053E 156
  EEZA0055E 157
  EEZA0056I 157
  EEZA0057E 157
  EEZA0058E 157
  EEZA0059E 157
  EEZA0060I 157
  EEZA0061E 157
  EEZA0062I 157
  EEZA0063I 157
  EEZA0064I 158
  EEZA0070E 158
  EEZA0071E 158
  EEZA0100I 158
  EEZA0101I 158
  EEZA0102I 158
  EEZA0103I 158
  EEZA0104I 158
  EEZA0105I 158
  EEZA0111I 158
  EEZA0112I 158
  EEZA0113I 159
  EEZA0114I 159
  EEZA0115I 159
  EEZA0116I 159
  EEZA0117I 159
  EEZA0118I 159
  EEZA9991E 159
  EEZA9992E 159
  EEZC0001I 159
  EEZC0002I 159
  EEZC0003I 160
  EEZC0004I 160
  EEZC0006E 160
  EEZC0007E 160
  EEZC0008E 160
  EEZC0009E 160
  EEZC0010E 161
  EEZC0011E 161
  EEZC0012E 161
  EEZC0013E 161
  EEZC0014E 161
  EEZC0015E 161
  EEZI0001E 162
  EEZI0003E 162
  EEZI0005E 162
  EEZI0012E 162
  EEZI0013E 162
  EEZI0014E 162

Messages *(continued)*
  EEZI0015E 162
  EEZI0016E 162
  EEZI0017E 163
  EEZI0018E 163
  EEZI0019E 163
  EEZI0021E 163
  EEZI0022E 163
  EEZI0023E 163
  EEZI0031E 163
  EEZI0032E 163
  EEZI0041E 164
  EEZI0042E 164
  EEZI0044E 164
  EEZI0046E 164
  EEZI0047E 164
  EEZI0048E 164
  EEZI0049E 164
  EEZI0050E 164
  EEZI0051E 164
  EEZI0052E 165
  EEZI0501W 165
  EEZI0545W 165
  EEZI2001I 165
  EEZI2002I 165
  EEZJ0001E 165
  EEZJ0002E 165
  EEZJ0003E 165
  EEZJ0004E 166
  EEZJ0005E 166
  EEZJ0006E 166
  EEZJ0007E 166
  EEZJ0008E 166
  EEZJ0009E 166
  EEZJ0010E 166
  EEZJ0011E 166
  EEZJ0013E 166
  EEZJ0014E 167
  EEZJ0015E 167
  EEZJ0016E 167
  EEZJ0017E 167
  EEZJ0018E 167
  EEZJ0019E 167
  EEZJ0020E 167
  EEZJ0021E 168
  EEZJ0022E 168
  EEZJ0023E 168
  EEZJ0024E 168
  EEZJ0025E 168
  EEZJ0026E 168
  EEZJ0029E 168
  EEZJ0030E 168
  EEZJ0031E 169
  EEZJ0032E 169
  EEZJ0033E 169
  EEZJ0034E 169
  EEZJ0035E 169
  EEZJ0036E 169
  EEZJ0037E 169
  EEZJ0038E 169
  EEZJ0039E 170
  EEZJ0040E 170
  EEZJ0041E 170
  EEZJ0042E 170
  EEZJ0043E 170
  EEZJ0044E 170
  EEZJ0045E 170