BEA AquaLogic® Service Bus Upgrade Guide

Version: 2.6 RP1

Document Date: November 2007

Contents

Upgrade Overview

You can upgrade AquaLogic Service Bus (ALSB) configurations from versions 2.1, 2.5, or 2.6 directly to version 2.6 RP1.

ALSB 2.1 runs on WebLogic Server 9.1. ALSB 2.5 and 2.6+ run on WebLogic Server 9.2+.

In-Place Upgrade

In-place upgrade—the ability to upgrade an existing ALSB installation and corresponding domains within an existing bea_home, such as d:\beaALSB26—is available for upgrades from ALSB 2.6 to 2.6 RP1.

In-place upgrade, however, is not available for upgrades from ALSB 2.1 or 2.5 to 2.6 RP1. Only a *migration* upgrade method is supported in those scenarios. That is, you must install to a new bea_home and create new ALSB 2.6 RP1 domains, then import a configuration that was exported from ALSB 2.1 or 2.5 domains into the newly created 2.6 RP1 domain. In effect, you move the configuration from the 2.1 or 2.5 domain to the new 2.6 RP1 domain(s).

Follow the procedures in the appropriate section:

Upgrading From ALSB 2.6 to 2.6 RP1

or

Upgrading From ALSB 2.1 or 2.5 to 2.6 RP1

- Upgrade Considerations

Considerations for Upgrading WebLogic Server 9.2 MP2 to MP3

If you have already upgraded to ALSB 2.6 RP1 and you want to upgrade WebLogic Server 9.2 from MP2 to MP3, perform the following steps:

1. After upgrading ALSB and your ALSB domains to 2.6 RP1, back up the config.xml files for your 2.6 RP1 domains.
2. Stop your server(s).
3. Upgrade to WebLogic Server 9.2 MP3.
4. In the config.xml file for each ALSB domain, modify the version number of the following libraries to 9.2.3:

   p13n-app-lib

   wlp-light-web-lib

   wlp-framework-common-web-lib

   wlp-framework-struts-1.2-web-lib

   For example, change name element p13n-app-lib#9.2.0@9.2.2 to **p13n-app-lib#9.2.0@9.2.3**.
5. Restart your server(s).

Upgrading From ALSB 2.6 to 2.6 RP1

If you want to upgrade to ALSB 2.6 RP1, you *must* also upgrade your ALSB 2.6 domains to 2.6 RP1.

Upgrading from ALSB 2.6 to 2.6 RP1 involves the following steps:

Step 1: Install ALSB 2.6 RP1

Step 2: Upgrade Your ALSB 2.6 Domains

Note: You can also perform a manual upgrade from ALSB 2.6 to 2.6 RP1, though the more automated upgrade procedure in this section is recommended. If you want to upgrade manually, follow the instructions in Upgrading From ALSB 2.1 or 2.5 to 2.6 RP1 on page 7.

Before you Begin

Before you begin the upgrade process from ALSB 2.6 to 2.6 RP1:

Stop all running ALSB 2.6 servers that will be upgraded.

Back up your ALSB 2.6 installation.

Back up your ALSB 2.6 domains.

Step 1: Install ALSB 2.6 RP1

ALSB 2.6 RP1 provides an in-place installer for upgrading an existing ALSB 2.6 installation. There are two ways to run the upgrade installer:

An executable file obtained from BEA Support (Recommended)

or

BEA’s Smart Update tool

When you install ALSB 2.6 RP1, the installer automatically makes a backup of your ALSB 2.6 installation state so that you can roll back to ALSB 2.6 if necessary. Use the ALSB 2.6 RP1 uninstaller to roll back to a previous product state.

Installing with an Executable File from BEA Support (Recommended)

Contact BEA Support to obtain the ALSB 2.6 RP1 upgrade executable file.

To install ALSB 2.6 RP1 with the executable:

1. Run the executable.
2. In the “Choose BEA Home Directory” window, be sure to select your existing ALSB 2.6 BEA home directory.
3. Accept the remaining defaults.

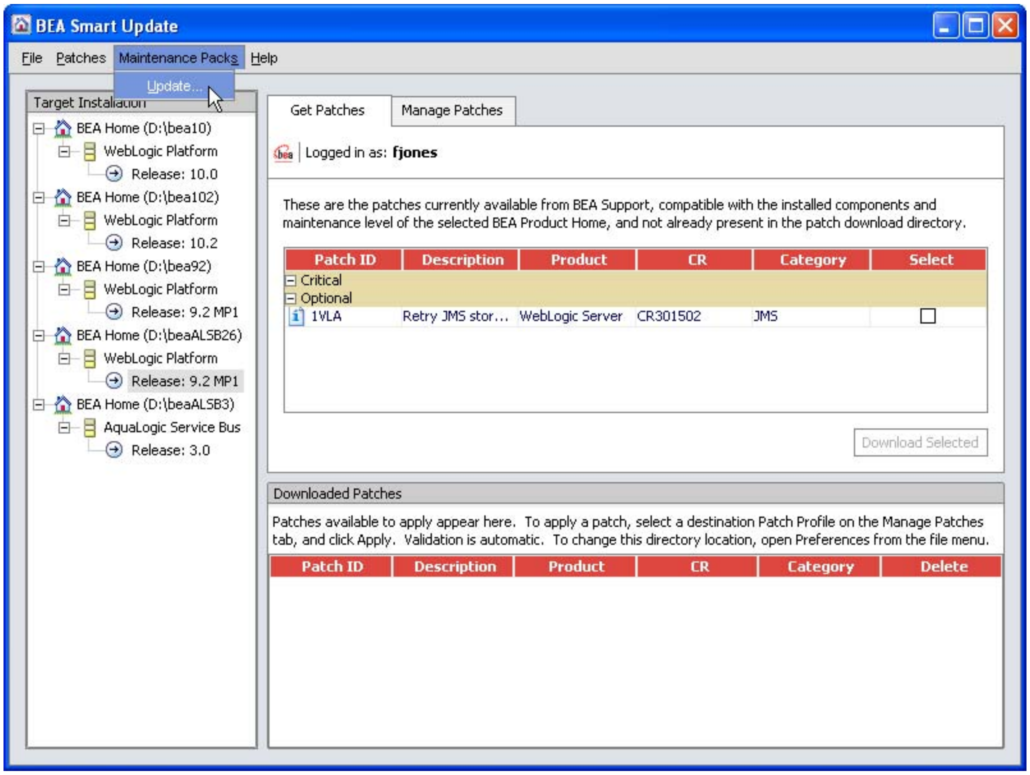
Installing with the Smart Update Tool

As an alternative to the recommended approach of installing with an executable file obtained from BEA support, you can install ALSB 2.6 RP1 using BEA's Smart Update tool. Smart Update automatically detects your installed BEA products and lets you install relevant patches and maintenance packs.

> **Note**: If you upgrade to ALSB 2.6 RP1 using the Smart Update tool, you must also manually apply necessary patches for the release. See the steps in this section for details.

For detailed information on using Smart Update, see "Downloading and Installing Maintenance Packs" in the *Installing Maintenance Updates and Maintenance Packs* guide at http://e-docs.bea.com/common/docs92/smart_update/service.html.

Figure 1 shows the Smart Update tool.



Logged in as: **fjones**

These are the patches currently available from BEA Support, compatible with the installed components and maintenance level of the selected BEA Product Home, and not already present in the patch download directory.

Patch ID	Description	Product	CR	Category	Select
Critical					
Optional					
1VLA	Retry JMS stor...	WebLogic Server	CR301502	JMS	□

Patches available to apply appear here. To apply a patch, select a destination Patch Profile on the Manage Patches tab, and click Apply. Validation is automatic. To change this directory location, open Preferences from the file menu.

Patch ID	Description	Product	CR	Category	Delete

Figure 1: Smart Update tool

To install ALSB 2.6 RP1 with Smart Update:

1. Launch Smart Update and log in with the BEA eSupport login provided with your support agreement.
2. In the Smart Update menu, choose Maintenance Packs > Update, and locate and install ALSB 2.6 RP1.
3. After installing ALSB 2.6 RP1, go to the Get Patches tab.
4. In the Target Installation pane, select the ALSB 2.6 release.

5. Download the following patch set through the Patches > Retrieve Private menu:

Patch identifier	Passcode
Q4MZ	EU9W5J6M

   Patch set Q4MZ automatically downloads the following patches: BZ6J, 7KCW, Z7MC, and JJPY.

6. Go to the Manage Patches tab. Click the Apply button next to patch set Q4MZ. The patches are installed.

Command Line Installation – If you download and install the patch set and patches with the Smart Update command-line feature, be sure to download the patch set and patches into the same download directory.

Step 2: Upgrade Your ALSB 2.6 Domains

You must upgrade your ALSB 2.6 domains after installing ALSB 2.6 RP1.

1. In a command window, go to the <weblogic_home>/common/bin directory.
2. Execute the following script for each ALSB 2.6 domain:

   upgradeWLPConfigFile.cmd/sh <fully qualified config.xml>

   For example:

   upgradeWLPConfigFile.cmd
   d:\beaALSB26\user_projects\domains\base_domain\config\config.xml
3. Execute the following script for each ALSB 2.6 domain:

   ALSBDomainUtils.cmd/sh upgradeALSBDomain <fully qualified path to domain>

   For example:

   ALSBDomainUtils.cmd upgradeALSBDomain
   d:\beaALSB26\user_projects\domains\base_domain

Your upgrade is complete. Restart your server(s).

Upgrading From ALSB 2.1 or 2.5 to 2.6 RP1

No wizard is provided to facilitate the migration of an ALSB 2.1 or 2.5 domain to an ALSB 2.6 RP1 domain; all steps are manual. To upgrade an ALSB domain to 2.6 RP1, complete the steps described in this section.

Note: You can also upgrade from ALSB 2.6 to 2.6 RP1 using these procedures rather than performing the recommended, more automated upgrade described in Upgrading From ALSB 2.6 to 2.6 RP1 on page 5. If you perform these manual steps to upgrade from ALSB 2.6:

Follow the instructions for ALSB 2.5 where appropriate.

Where differences between ALSB 2.5 and 2.6 appear, consider the ALSB 2.6 information.

Where ALSB 2.5 documentation is referenced, see the relevant ALSB 2.6 documentation, located at http://edocs.bea.com/alsb/docs26/index.html.

Step 1: Export the ALSB 2.1 or 2.5 Configuration

Use the ALSB Console to export the ALSB 2.1 or 2.5 configuration that you want to upgrade. To do so, log on as Administrator, and select **Export Resources** from the **System Administration** panel in the console. For information about exporting ALSB configurations, see the appropriate *Using the AquaLogic Service Bus Console* document:

"Exporting Configuration Data" in System Administration (2.1)

"Exporting Configuration Data" in System Administration (2.5)

You can also export configurations using the AquaLogic Service Bus DeploymentMBean (for 2.1) and the ALSBConfigurationMBean (for 2.5). For information, see the appropriate *AquaLogic Service Bus Deployment Guide*:

Using the ALSB Deployment API (for 2.1)

Using the Deployment APIs (for 2.5)

Note: In most cases, you cannot export WebLogic Server resources, such as the JMS resources , SNMP trap settings, and the Work Manager definitions. You must re-create these objects in the new ALSB domain, as described in Step 6: Recreate Other WebLogic Server Objects.

Step 2: Export the Security Configurations

Use the WebLogic Server Administration Console to export security data from the domain: In the WebLogic Server Administration Console, select **Domain Structure**→**Security Realms**, then choose the security realm. Select **Migration**→**Export** to export the data.

The following table summarizes the security data and the types of security providers in which it is stored.

Security Data	**Security Provider Type**
User accounts	Authentication Provider
Group definitions	Authentication Provider
Role definitions	Role Mapping Provider
User names and passwords in service	Username/Password Credential Mapping

accounts	Provider
PKI credential map entries	PKI Credential Mapping Provider
SAML Relying Parties	SAML Credential Mapping Provider V2
SAML Asserting Parties	SAML Identity Assertion Provider V2
Trusted Certificates (for SSL and WSS)	Certification Path Provider (Certificate Registry)

The set of providers to export is different depending on whether you are upgrading from 2.1 or 2.5 as described in the following sections:

Exporting 2.1 Security Configurations

Exporting 2.5 Security Configurations

Exporting 2.1 Security Configurations

If you created service accounts and added user names and passwords to the service accounts, then your domain includes a username/password credential mapping provider. If your domain includes this provider or a PKI credential mapping provider, you must configure the export process to export credential mapping passwords in clear text (unencrypted). Your new domain will not be able to use passwords that were encrypted by a different domain.

To Export Credential Mapping Data with Unencrypted Passwords

1. Carefully restrict access to the directory and file into which you export credential maps so that unauthorized users cannot read the unencrypted passwords. When you import the credential maps into the new domain, the credential mapping provider encrypts the passwords. After the upgrade is complete, securely dispose of the file with unencrypted passwords.
2. Export data from each security provider individually.

   WebLogic Server allows you to either export all of the security data in a single export operation or to export data from each security provider individually. Do **not** export all of the data in a single export operation. The single export operation does not allow you to export passwords in clear text.
3. While exporting data from the credential mapping providers, do the following to export the passwords for the credentials in clear text: When the WebLogic Server Administration Console displays a page with the **Export Constraints** text box, enter the following: `passwords=cleartext`

For more information, see Migrating Security Data in *Securing WebLogic Server*.

Exporting 2.5 Security Configurations

Starting with the ALSB 2.5 release, both PKI and username/password credentials are stored in both the WebLogic Server realm and in the ALSB configuration repository. Consequently, credentials are exported as part of the configuration JAR that was generated and exported in Step

1 of this procedure. When the JAR is imported into the new 2.6 RP1 domain, the realm data will be populated based on the contents of the JAR file. As a result, when you upgrade from ALSB 2.5, neither PKI Credentials nor username/password credentials should be exported.

Step 3: Install ALSB 2.6 RP1

Install the full ALSB 2.6 RP1 product into a new BEA home directory. Obtain the full installer from the BEA download site or from BEA Support.

For detailed installation instructions, see the *BEA AquaLogic Service Bus 2.6 Installation Guide* at http://edocs.bea.com/alsb/docs26/install/index.html.

Step 4: Create a New ALSB 2.6 RP1 Domain

Create a new ALSB 2.6 RP1 domain using the Domain Configuration Wizard or using the offline configuration tools, as described in:

> Creating a New AquaLogic Service Bus Domain in Creating WebLogic Domains Using the Configuration Wizard
>
> or
>
> "Creating and Extending Domains" in Using Offline Configuration Tools.

Step 5: Configure WebLogic Server Security

In the new domain, configure the WebLogic security framework with SSL and the security providers that you need to support your proxy and business services. See Configuring the WebLogic Security Framework: Main Steps in the *AquaLogic Service Bus Security Guide*.

Note the following security-related information about importing a 2.1 or 2.5 Configuration:

> As of ALSB 2.5, the WebLogic Default Authorization provider and Default Role Mapping provider was deprecated. See Deprecated Security Features in *BEA AquaLogic Service Bus 2.5 Release Notes*.
>
> Instead of configuring these providers in your new domain, BEA recommends that you use the WebLogic XACML Authorization provider and XACML Role Mapping provider. Later in the upgrade process you can import 2.1 or 2.5 policies and role maps into the XACML providers.
>
> If your new domain uses a PKI credential mapping provider, copy the keystores to the new domain and configure the PKI credential mapping provider to use the keystore.
>
> If your 2.1 or 2.5 domain modified the Web Service security configurations named `__SERVICE_BUS_INBOUND_WEB_SERVICE_SECURITY_MBEAN__` or `__SERVICE_BUS_OUTBOUND_WEB_SERVICE_SECURITY_MBEAN__`, make the same modifications in the 2.6 RP1 domain.
>
> For example, if in your 2.1 domain you added the `UseX509ForIdentity` property to the `__SERVICE_BUS_INBOUND_WEB_SERVICE_SECURITY_MBEAN__` configuration (which is required to support inbound authentication with an X.509 token), add the property in the 2.6 RP1 domain. See Use X.509 certificates to establish identity in *The WebLogic Server Administration Console Online Help*.

Step 6: Recreate Other WebLogic Server Objects

In the new ALSB 2.6 RP1 domain, recreate WebLogic Server objects that could not be exported in Step 1: Export the ALSB 2.1 or 2.5 Configuration, including:

JMS resources, such as connection factories, queues, topics, and so on.

Work Manager definitions

SNMP agent and trap destination settings

For more information about configuring WebLogic Server domain resources, see Overview of WebLogic Server System Administration in *Introduction to BEA WebLogic Server and BEA WebLogic Express*.

Add the Tuxedo domain ID as a WebLogic Server user (this is a requirement to invoke a successful request to a Tuxedo service)

Configure WTC Local Access Point and Remote Access Point resources when your configuration includes Tuxedo transport-based services

For information, see Configuring WebLogic Tuxedo Connector for Tuxedo Transport in *Interoperability Solution for Tuxedo*.

Step 7: Import Security Data

Use the WebLogic Server Administration Console to import the security data that you exported in Step 2: Export the Security Configurations into the new ALSB domain. See Import data into a security provider in the *WebLogic Server Administration Console Online Help* at the following URL: http://edocs.bea.com/wls/docs92/ConsoleHelp/taskhelp/security/ImportDataIntoSecurityProviders.html.

Note the following:

Import the security information for each security provider separately.

See Only One Credential Mapping Provider Allowed.

BEA recommends that you import access control policies into the WebLogic XACML Authorization Provider. If you exported data from the WebLogic Default Authorization Provider in your 2.1 or 2.5 domain, when you import into the XACML Authorization Provider make sure that you select `DefaultAtz` from the **Import Format** list.

BEA recommends that you import security role maps into the WebLogic XACML Role Mapping Provider. If you exported data from the WebLogic Default Role Mapper Provider in your 2.1 or 2.5 domain, when you import into the XACML provider make sure you select `DefaultRoles` in the **Import Format** list.

Step 8: Import the ALSB Configuration Data

Import the 2.1 or 2.5 configuration data that you exported in Step 1: Export the ALSB 2.1 or 2.5 Configuration into the new 2.6 RP1 domain

To do so, log on to the ALSB Console as Administrator, and select **Import Resources** from the **System Administration** panel. For information about importing ALSB configurations, see "Importing Configuration Data" in System Administration in *Using the AquaLogic Service Bus Console*.

Note: You cannot import artifacts into a 2.6 RP1 domain if artifacts of the same type and name are already present in the 2.6 RP1 domain. In other words, import the configuration data into a newly created domain, or a domain that contains only projects, folders, or services unrelated to the artifacts you are importing.

2.1 Service Accounts

In the case of 2.1 service accounts, the import process attempts to re-bind each 2.1 service account to the user names and passwords that are in the username/password credential mapping provider. For example, if your 2.1 domain included a service account with the user name of "pat" and password of "patspassword", the import process looks in the username/password credential mapping provider in the 2.6 RP1 domain for "pat" and "patspassword." If the import process does not find the credentials for a service account in the username/password credential mapping provider, you must add credentials to the service account before you can activate the session. You cannot import empty service accounts into ALSB.

For each 2.1 proxy service provider, the import process does the following:

> Searches the PKI credential mapping provider for alias-to-key-pair bindings that match those in the imported proxy service provider. If it finds a match, it enables the proxy service provider to use those key-pair bindings. If it does not find a match, the import process imports the proxy service provider without any key-pair bindings. While it is valid to create a proxy service provider that contains no key-pair bindings, if you want to use the provider to provide credentials, you must use the ALSB Console to add key-pair bindings to the proxy service provider.
>
> Prompts you to remove X.509 certificates that were used only for Web Service Security (WSS) authentication.
>
> In ALSB 2.6 RP1, you cannot create a proxy service provider that supplies an X.509 credential only for WSS authentication. You can create a proxy service provider that supplies X.509 credentials for digital signatures, digital encryption, or SSL client authentication. The proxy service provider uses the X.509 digital-signature credential for those web services that require the certificate for both WSS authentication and digital signature.
>
> If a 2.1 proxy service provider contained a digital-signature credential and an X.509 authentication credential, and if both credentials refer to the same key-pair, the import process does not import the X.509 token authentication credential. You do not need to remove the credential. To confirm that the X.509 token authentication credential will not be imported into the 2.6 RP1 domain, the import process outputs the following message: *Service Provider has been upgraded. The Web Service Security X.509 Token key has been removed. This credential was deprecated in ALSB 2.5. The Digital Signature key will be used instead*.
>
> For information about the security changes in ALSB versions after 2.1, see Transport-Level Access Control Changes in 2.1 or 2.5 to 2.6 RP1 Upgrade Considerations. For additional information about the security changes from ALSB 2.1 to 2.5 described in this section (and applicable to 2.6 RP1), see Security Updates Expand Configuration Options in the ALSB 2.5 *Release Notes*.

Step 9: Complete Any Manual Upgrade Procedures

Some ALSB domain configuration changes are not automated and must be implemented manually. See Upgrade Considerations.

This completes the creation of your new ALSB 2.6 RP1 domain.

Upgrade Considerations

This section describes considerations for upgrading various ALSB configuration artifacts. It describes how ALSB 2.1 and 2.5 differ in behavior from ALSB 2.6+ in specific areas that may impact the configurations you are upgrading. It includes the following topics:

2.1 or 2.5 to 2.6 RP1 Upgrade Considerations

Please read the following upgrade considerations whether you are upgrading from 2.1 or 2.5 configurations to 2.6 RP1:

"Use SSL" Attribute Controls Whether SSL is Used to Access JMS Queues

ALSB JMS services (proxy and business) have a "Use SSL" attribute that controls whether SSL should be used to access the JMS queues. However, in ALSB 2.5 and earlier, JMS business services did not use SSL when reading the outbound responses even if "Use SSL" was specified. This was corrected in ALSB 2.6.

However, this means that when a such business service (JMS request/response business service with "Use SSL" selected) from ALSB 2.1 or 2.5 is imported into 2.6 RP1, there may be a problem if the outbound response URL corresponds to a non-SSL port. Attempts to use SSL to talk to this non-SSL port will result in an error.

Workaround: The outbound response queue URL must be corrected to use the SSL port. When you import a 2.1 or 2.5 configuration JAR that contains a request/response outbound JMS business service with "Use SSL" specified, a warning is issued in the ALSB Console.

SOAP Services Imported from 2.1 or 2.5 JARs use SOAP 1.1 by Default

ALSB adds support for SOAP 1.2. All of the SOAP services imported from 2.1 or 2.5 JARs use SOAP 1.1 by default.

UDDI Configuration

In 2.6, the UDDI auto Import feature was enhanced to allow the auto synchronization with UDDI registries. Notifications are sent from the UDDI registry to ALSB when a change occurs in the registry for a service to which ALSB is subscribed.

In the case of single node, the notification is sent to the managed server HTTP address. In clustered configurations, the notification is sent to the Admin server HTTP address.

An “Auto Import” flag is added to the registry configuration to indicate whether auto synchronization is enabled for the registry. While importing an ALSB 2.1 or 2.5 JAR file, ALSB disables this flag, thus retaining the old behavior.

Operational Customization

Operational parameters were enhanced in ALSB 2.6. The following table describes the value that ALSB uses for Service Operational Parameters.

Parameter	New in 2.6 or Existing in 2.1 or 2.5	Value set in 2.6+ Configuration
Service State	Existing	As specified in imported JAR
‘Monitoring’ enable/disable	Existing	As specified in imported JAR
‘Monitoring Aggregation Interval’	Existing	As specified in imported JAR If none specified, then default is set to 10 min.
‘Reporting’ enable/disable	New	Enable
‘Tracing’ enable/disable	Existing	As specified in imported JAR
‘Logging’ enable/disable ‘Logging’ severity level	New New	Enable Debug
‘SLA Alerting’ enable/disable ‘SLA Alerting’ severity level	New New	Enable Normal
‘Pipeline Alerting’ enable/disable ‘Pipeline Alerting’ severity level	New New	If Monitoring is Enabled: Enable and Normal If Monitoring is Disabled: Disabled and Normal

Alert Logs, Execution History, and Undo Records Not Exportable

Alert logs, execution history, and undo records in ALSB 2.1 or 2.5 domains cannot be exported to your new ALSB 2.6 RP1 domains.

2.1 to 2.6 RP1 Upgrade Considerations

When upgrading 2.1 configurations to 2.6 RP1, consider the following:

(These issues do not apply when upgrading 2.5 configurations to 2.6 RP1.) .

Some Error Codes Are Not Generated in 2.5 (or later) Versions

In ALSB 2.5 and 2.6+, error codes BEA-382101, BEA-382102, and BEA-382151 are not generated while preparing an inbound response or outbound request.

In ALSB 2.1, these errors were generated for the conditions as described in the following listing:

BEA-382101—invalid content assigned to `$inbound/transport/response`

BEA-382102—invalid content assigned to `$outbound/transport/request`

BEA-382151—invalid service name assigned to `$outbound@name`

In ALSB 2.1, these errors were caught in the binding layer at run time.

In ALSB 2.6+, these errors are caught at design time in the Replace action and result in an error code of BEA-382040, indicating that an Assign action failed.

New Error Codes Require Update

If you use WSS or relied on specific ALSB 2.1 error codes, either on proxy service error-handlers or client-side code, note the following change in ALSB 2.6+.

Whenever WebLogic Server WSS returns a SOAP fault to ALSB, the ALSB message-context has a fault with:

error code: BEA-386201

description: `A web service security fault occurred [<root-wss-error>][<root-wss-fault-string>]` where:

`root-wss-error` is the error-code from the WebLogic Server WSS SOAP fault,

`root-wss-fault-string` is the fault-string from the WebLogic Server WSS SOAP fault.

details: an instance of XML element {http://www.bea.com/wli/sb/errors}WebServiceSecurityFault. This XML element also contains the root-fault error-code, fault-string, and fault-details.

The ALSB default error handler returns the root SOAP fault to the client.

Workaround:

BEA recommends that you update your error-handlers and/or client-side code to deal with the new error codes.

You can also write an error-handler that maps the new error-codes back to the ALSB 2.1 error code. However, this is not a BEA-recommended approach.

Users in the IntegrationOperator Role Do Not Have Export Privileges

In ALSB 2.1, users in the IntegrationOperator role were allowed to export ALSB configurations; in 2.5 and 2.6+ they are not. The workaround is to reassign such users to a different role.

Only One Credential Mapping Provider Allowed

Only one PKI and one username/password credential mapping provider is allowed in ALSB 2.5 and 2.6+.

In AquaLogic Service 2.5 or 2.6+, you can configure at most one PKI credential mapping provider and at most one username/password credential mapping provider. In AquaLogic 2.1, you can have multiple PKI credential mapping providers and multiple username/password credential mapping providers. Consequently, if you are upgrading from AquaLogic 2.1 to 2.6 RP1 and you created multiple PKI or username/password credential mapping providers in 2.1, you must import all PKI mapping data into a single PKI credential mapping provider and import all username/password mapping data into a single username/password credential mapping provider.

New Alert Summary Field in ALSB 2.6+

In ALSB 2.1 you could not customize the content of the alert summary field when you defined an E-mail action for an SLA alert. All alert summaries (the contents of which populated the E-mail's `Subject` line) contained the text: `AquaLogic Service Bus Alert`. In ALSB 2.5 and 2.6+, a new alert-summary field that you can customize is provided when you configure SLA alerts and pipeline alert actions.

For those SLA alerts that are migrated from 2.1 to 2.6 RP1, ALSB populates the alert summary field with the 2.1 text: `AquaLogic Service Bus Alert`.

After you complete the upgrade, you can change the message in the alert summary field to something more descriptive. For more information about configuring alert actions, see "Alert" under Proxy Service: Actions in *Using the AquaLogic Service Bus Console*. See also “Creating and Alert Rule” in Monitoring in *Using the AquaLogic Service Bus Console*.

2.6 RP1 Alert Destination Resources are Created from 2.1 Alert Rules

A new resource called an Alert Destination was introduced in ALSB 2.5. It is used to capture a list of recipients that can receive alert notifications from ALSB. When an SLA alert rule is upgraded from 2.1 to 2.6 RP1, the alert actions configured in the 2.1 SLA Alert Rule are extracted and used to create an Alert Destination resource. The SLA Alert Rule is then updated to reference this resource.

The Alert Destination created resides in the same project and folder as the service with which the alert rule is associated. The name of the Alert Destination is specified as `Alert Destination - xxxxxx`, where `xxxxxx` is a unique number.

The upgrade process creates an Alert Destination for each unique combination of recipients. In other words, if ten SLA Alert Rules with the same set of recipients were upgraded from 2.1, only one Alert Destination resource is created in the same project and folder as the service that is associated with the first SLA Alert Rule.

For information about Alert Destinations, see Alert Destinations in *Using the AquaLogic Service Bus Console*.

2.6 RP1 Run Time Does Not Generate Missing Headers when Sending Multipart Messages

If an ALSB proxy service receives a multipart message (that is, a message with attachments) where the root part does not have an associated Content-ID MIME header, subsequent multipart messages sent by that proxy service will not have a Content-ID MIME header for the root part. In 2.1, ALSB corrected for the missing headers in client messages by generating the header when sending multipart messages. In 2.6 RP1, the missing header is not automatically generated. Therefore, you must ensure that clients sending multipart messages to ALSB include a Content-ID header and "start" parameter.

The presence of this Content-ID header directly affects the presence of the "start" parameter in the "multipart/related" Content-Type of the multipart message.

While the Content-ID header and "start" parameter are considered optional by MIME standards, some Web Service stacks may require them and may return an error response back to the proxy service if they are absent.

Transport-Level Access Control Changes After ALSB 2.1

In ALSB 2.1, transport-level access control was limited to HTTP and HTTPS proxy services. Access control was enforced by the web-container. The authorization check was done against a weblogic.security.service.URLResource. See

http://e-docs.bea.com/wls/docs91/javadocs/weblogic/security/service/URLResource.html

In 2.5 and later versions, ALSB has a transport-level access control check on entry to all proxy services, regardless of transport. The call to the authorization service is now done in ALSB code, the web-container does not do an authorization check anymore. As a side-effect, the check is now done against a `com.bea.wli.sb.security.ALSBProxyServiceResource`. The default policy on `ALSBProxyServiceResource` grants access to all requests. You can configure a transport-level access control policy on a proxy service in the ALSB console, as described in http://e-docs.bea.com/alsb/docs261/consolehelp/securityconfiguration.html.

This change has the following implications:

> A policy is composed of one or more policy conditions, grouped together by boolean operators. Most policy conditions can be used to secure any resources (for example is-user-in-role). However, some policy conditions can only be used to secure resources of a specific type. There are policy conditions which can be applied only to URLResource. These are:
>
> > weblogic.entitlement.rules.HttpRequestAttrIsSet
> >
> > weblogic.entitlement.rules.HttpRequestAttrNumberPredicate
> >
> > weblogic.entitlement.rules.HttpRequestAttrNumberEquals
> >
> > weblogic.entitlement.rules.HttpRequestAttrNumberGreater
> >
> > weblogic.entitlement.rules.HttpRequestAttrNumberLess
> >
> > weblogic.entitlement.rules.HttpRequestAttrStringEquals
>
> In ALSB 2.1 you could use these policy conditions to secure HTTP/S proxy services, but these policy conditions are not allowed in ALSB 2.6 RP1.

The context properties passed to the security framework are also different.

Note: context properties are passed in a weblogic.security.service.ContextHandler instance. For more information, see http://e-docs.bea.com//wls/docs91/javadocs/weblogic/security/service/ContextHandler.html

Prior to ALSB 2.5, the web-container passed some URLResource-specific context properties to the security providers. ALSB 2.5 and 2.6+ pass a different set of context properties. Some of these are described in “Adding Policy Conditions” in Security Configuration at the following URL: http://edocs.bea.com/alsb/docs261/consolehelp/securityconfiguration.html

As mentioned above, for ALSB versions after 2.5, all proxy service invocations go through an access control check, including co-located optimized calls, calls to local-transport proxies and calls from the ALSB test console.

Because URLResource is not used in 2.5 or 2.6+, a proxy service's transport-level access control policy is no longer tied to the endpoint's URI. You can change the proxy service URI and the existing policy will still take effect. However, the policy is now dependent on the proxy service location (project and/or folders) and name. Operations such as resource/project/folder rename, move, clone, delete and undo do not have any effect on an authorization provider's policy database. Be careful when performing these operations to avoid loosing an access control policy or leaving orphan access control policies in the system. See Known Issue for CR222177 in the AquaLogic Service Bus Release Notes at the following URL: http://e-docs.bea.com/alsb/docs261/relnotes/.

The default policy on ALSBProxyServiceResource is automatically created in new ALSB domains.

About Access Control Policies during Upgrade

During upgrade of ALSB 2.1 to 2.6 RP1, ALSB checks to see if the default policy on ALSBProxyServiceResource exists in at least one authorization provider. If this policy does not exist, then it is created. Read access to the policy database is optional—if an authorization provider does not support reads, ALSB displays an alert message:

“*AquaLogic Service Bus could not determine if the default ALSBProxyServiceResource policy is present or not because some authorization providers do not implement PolicyReaderMBean. ALSB could not deploy the policy because neither EntitleNet provider nor XACML provider is present. If the policy is indeed missing, the administrator must create it."*

Similarly, write access to the policy database is optional. If an authorization provider does not provide write access, ALSB displays the following alert message:

"AquaLogic Service Bus has determined the default ALSBProxyServiceResource policy is missing. ALSB could not deploy the policy because neither EntitleNet provider nor XACML provider is present. Access to all ALSB proxy services will be denied. The administrator must create the policy using the provider tools."

Note: The EntitleNet provider was deprecated in ALSB 2.5; it is not supported in ALSB 2.6 RP1. If you are using the EntitleNet provider, you should upgrade to the XACML authorization provider.

During a 2.1 to 2.6 RP1 upgrade, access control policies on HTTP or HTTPS proxy services are also automatically migrated. If there is a policy on the URLResource matching the service URI, the policy is copied over to the corresponding ALSBProxyServiceResource. The original policy (the one on URLResource) is deleted. There is one exception to this: if the original policy used one of the URLResource-specific conditions, the policy cannot be upgraded. In this case ALSB creates a policy for this service, which denies all access to the service and writes the following alert to the log file:

"[POLICY MIGRATION] [proxy service: <service>] [authorization provider: <provider>] The 2.1 policy cannot be migrated because it makes use of policy predicates which are specific to URLResource. A deny-all policy will be bound to the proxy. You must re-configure this policy in the console."

Warning: These automatic changes to the policy database occur while staging an ALSB configuration JAR during import. These changes are not atomic. Consider this scenario: a user creates an ALSB session and imports a 2.1 configuration JAR, which causes some automatic policy updates. If the user now decides to abandon the ALSB session (by undoing the changes without activating) the policy changes are not rolled back.