BEA AquaLogic Service Bus ™ Upgrade Guide

Version: 2.6

Document Date: January 2007

Upgrade Overview

You can upgrade AquaLogic Service Bus configurations from versions 2.1 and 2.5 to version 2.6.

AquaLogic Service Bus 2.1 runs on WebLogic Server 9.1. AquaLogic Service Bus 2.5 and 2.6 run on WebLogic Server 9.2.

The upgrade of *in-place* domains is not supported for AquaLogic Service Bus 2.6; only a *migration* upgrade method is supported. That is, you must create a new AquaLogic Service Bus 2.6 domain, then import a configuration that was exported from a 2.1 or a 2.5 domain into the newly created 2.6 domain. In effect, you move the configuration from the 2.1 or 2.5 domain to the new 2.6 domain.

The upgrade to 2.6 domains is supported for both clustered and non-clustered domains.

Migration Upgrade

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

Step 1: Export the AquaLogic Service Bus 2.1 or 2.5 Configuration

Use the AquaLogic Service Bus Console to export the AquaLogic Service Bus 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 AquaLogic Service Bus 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 AquaLogic Service Bus 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 AquaLogic Service Bus 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 accounts	Username/Password Credential Mapping 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 AquaLogic Service Bus 2.5 release, both PKI and username/password credentials are stored in both the WebLogic Server realm and in the AquaLogic Service Bus 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 domain, the realm data will be populated based on the contents of the JAR file. As a result, when you upgrade from AquaLogic Service Bus 2.5, neither PKI Credentials nor username/password credentials should be exported.

Step 3: Install AquaLogic Service Bus 2.6

Install the AquaLogic Service Bus 2.6 software as described in the AquaLogic Service Bus Installation Guide.

Step 4: Create a New AquaLogic Service Bus 2.6 Domain

Create a new AquaLogic Service Bus 2.6 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-realted information about importing a 2.1 or 2.5 Configuration:

- In AquaLogic Service Bus 2.5, the WebLogic Default Authorization provider and Default Role Mapping provider was deprecated. 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 2.1or 2.5

policies and role maps into the XACML providers. See Deprecated Security Features in *BEA AquaLogic Service Bus Release Notes*.

- 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 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 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 AquaLogic Service Bus 2.6 domain, recreate WebLogic Server objects that could not be exported in Step 1 (Step 1: Export the AquaLogic Service Bus 2.1 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 AquaLogic Service Bus 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 AquaLogic Service Bus Configuration Data

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

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

Note: You cannot import artifacts into a 2.6 domain if artifacts of the same type and name are already present in the 2.6 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 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 AquaLogic Service Bus.

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 AquaLogic Service Bus 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 AquaLogic Service Bus 2.6, 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 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 has been deprecated in AquaLogic Service Bus 2.5. The Digital Signature key will be used instead.*

For information about the security changes in AquaLogic Service Bus versions after 2.1, see Transport-Level Access Control Changes in 2.1 to 2.6 Upgrade Considerations. For additional information about the security changes between AquaLogic Service Bus 2.1 and 2.5, see Security Updates Expand Configuration Options in "What's New in AquaLogic Service Bus" in *BEA AquaLogic Service Bus Release Notes.*

Step 9: Complete Any Manual Upgrade Procedures

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

This completes the creation of your new AquaLogic Service Bus 2.6 domain.

Upgrade Considerations

This section describes considerations for upgrading various AquaLogic Service Bus configuration artifacts. It describes how AquaLogic Service Bus 2.1 and 2.5 differ in behavior from AquaLogic Service Bus 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 Upgrade Considerations

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

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

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

However, this means that when a such business service (JMS request/response business service with "Use SSL" selected) from AquaLogic Service Bus 2.1 or 2.5 is imported into 2.6, 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 AquaLogic Service Bus Console.

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

AquaLogic Service Bus 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 has been enhanced to allow the auto synchronization with UDDI registries. Notifications are sent from the UDDI registry to AquaLogic Service Bus when a change occurs in the registry for a service to which AquaLogic Service Bus 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 AquaLogic Service Bus 2.1 or 2.5 JAR file, AquaLogic Service Bus disables this flag, thus retaining the old behavior.

Operational Customization

Operational parameters have been enhanced in AquaLogic Service Bus 2.6. The following table describes the value that AquaLogic Service Bus 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

2.1 –to– 2.6 Upgrade Considerations

When upgrading 2.1 configurations to 2.6, consider the following:

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

Change in Representation of undo Records

The serialized representation of `undo` records has changed so that `undo` records can be upgraded in 2.5 and beyond. However, as a result of this enhancement, the `undo` feature is unavailable if an upgrade occurs from 2.1 to 2.6. In other words, if you make changes in the 2.1 configuration and then upgrade to 2.6, you cannot (in the new domain) `undo` the changes you made in the 2.1 domain. However, you can still see the execution and the activation history in the AquaLogic Service Bus Console.

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

In AquaLogic Service Bus 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 AquaLogic Service Bus 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 AquaLogic Service Bus 2.1, these errors were caught in the binding layer at run time.

In AquaLogic Service Bus 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 AquaLogic Service Bus 2.1 error codes, either on proxy service error-handlers or client-side code, note the following change in AquaLogic Service Bus 2.6.

Whenever WebLogic Server WSS returns a SOAP fault to AquaLogic Service Bus, the AquaLogic Service Bus 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 AquaLogic Service Bus 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 AquaLogic Service Bus 2.1 error code. However, this is not a BEA-recommended approach.

Users in the IntegrationOperator Role Do Not Have Export Privileges

In AquaLogic Service Bus 2.1, users in the IntegrationOperator role were allowed to export AquaLogic Service Bus 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 AquaLogic Service Bus 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 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.

2.1 SLA Alert Logs are Unavailable in 2.6

In 2.1, SLA alerts were captured in the WebLogic Diagnostics Framework (WLDF) log. Migration to a 2.6 domain removes the contents of the 2.1 log. Consequently, the alerts and their details are not displayed in the new domain's AquaLogic Service Bus Console.

Alerts in the reporting log are removed when you perform an upgrade.

If the 2.1 alerts are issued in E-mail, they continue to be available in the user E-mail accounts after the upgrade. However, if any of those alerts were configured with a JMS action only (that is, with either a JMS queue or JMS topic defined as the JMS destination), you must set up new queues and topics in the 2.6 domain. Consequently, the old JMS actions are lost.

New Alert Summary Field in AquaLogic Service Bus 2.6

In AquaLogic Service Bus 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 AquaLogic Service Bus 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, AquaLogic Service Bus 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 Alert Destination Resources are Created from 2.1 Alert Rules

A new resource called an Alert Destination was introduced in AquaLogic Service Bus 2.5. It is used to capture a list of recipients that can receive alert notifications from AquaLogic Service Bus. When an SLA alert rule is upgraded from 2.1 to 2.6, 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 Run Time Does Not Generate Missing Headers when Sending Multipart Messages

If an AquaLogic Service Bus 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, AquaLogic Service Bus corrected for the missing headers in client messages by generating the header when sending multipart messages. In 2.6, the missing header is not automatically generated. Therefore, you must ensure that clients sending multipart messages to AquaLogic Service Bus 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 AquaLogic Service Bus 2.1

In AquaLogic Service Bus 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, AquaLogic Service Bus 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 AquaLogic Service Bus 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 AquaLogic Service Bus console, as described in http://e-docs.bea.com/alsb/docs26/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 AquaLogic Service Bus 2.1 you could use these policy conditions to secure HTTP/S proxy services, but these policy conditions are not allowed in ALSB 2.5.

- 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 AquaLogic Service Bus 2.5, the web-container passed some URLResource-specific context properties to the security providers. AquaLogic Service Bus 2.6 (and 2.5) passes 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/docs26/consolehelp/securityconfiguration.html

- As mentioned above, for AquaLogic Service Bus versions after 2.5, all proxy service invocations go through an access control check, including colocated optimized calls, calls to local-transport proxies and calls from the AquaLogic Service Bus 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/docs26/relnotes/

- The default policy on ALSBProxyServiceResource is automatically created in new AquaLogic Service Bus domains.

About Access Control Policies during Upgrade

During upgrade of AquaLogic Service Bus 2.1 to 2.6, AquaLogic Service Bus 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, AquaLogic Service Bus 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, AquaLogic Service Bus 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 AquaLogic Service Bus 2.5; t is not supported in AquaLogic Service Bus 2.6. If you are using the EntitleNet provider, you should upgrade to the XACML authorization provider.

During a 2.1 to 2.6 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 AquaLogic Service Bus 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 AquaLogic Service Bus configuration JAR during import. These changes are not atomic. Consider this scenario: a user creates an AquaLogic Service Bus session and imports a 2.1 configuration JAR, which causes some automatic policy updates. If the user now decides to abandon the AquaLogic Service Bus session (by undoing the changes without activating) the policy changes are not rolled back.