Oracle® Fusion Middleware

Upgrade Guide for Oracle Service Bus

11*g* Release 1 (11.1.1.7.0)

E15032-05

June 2013

ORACLE®

Oracle Fusion Middleware Upgrade Guide for Oracle Service Bus, 11*g* Release 1 (11.1.1.7.0)

E15032-05

Contents

Preface

This manual is intended for Oracle Service Bus system administrators who are responsible for upgrading Oracle Service Bus to 11*g* Release 1 (11.1.1.7.0). It is assumed that the readers of this manual have knowledge of the following:

- Oracle Service Bus configuration

- Oracle WebLogic administration domain concepts

- The configuration and expected behavior of the system being upgraded

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

For more information, see the following related documentation available in the Oracle Fusion Middleware 11*g* documentation library:

- *Oracle Fusion Middleware Installation Guide for Oracle Service Bus*

- *Oracle Fusion Middleware Concepts and Architecture for Oracle Service Bus*

- *Oracle Fusion Middleware Administrator's Guide for Oracle Service Bus*

- *Oracle Fusion Middleware Developer's Guide for Oracle Service Bus*

- *Oracle Fusion Middleware Deployment Guide for Oracle Service Bus*

- *Oracle Fusion Middleware Upgrade Planning Guide*

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Summary of Upgrade Process

This chapter provides a summary of the Oracle Service Bus upgrade process from 10*g* to 11*g*.

This chapter contains the following sections:

- Getting Started
- Flow Chart for Oracle Service Bus Upgrade Process
- Steps in the Oracle Service Bus Upgrade Process

> **Note:** In-place upgrade is not supported for Oracle Service Bus domains.

1.1 Getting Started

Before you start your upgrade of Oracle Service Bus, review the following:

- Review upgrade concepts in the *Oracle Fusion Middleware Upgrade Planning Guide*
- Upgrade starting points

1.2 Flow Chart for Oracle Service Bus Upgrade Process

Figure 1–1 illustrates the Oracle Service Bus upgrade process. Review this chart to get familiar with the steps you will be required to take, based on your existing environment.

Figure 1–1   Flow Chart of the Oracle Service Bus Upgrade Process
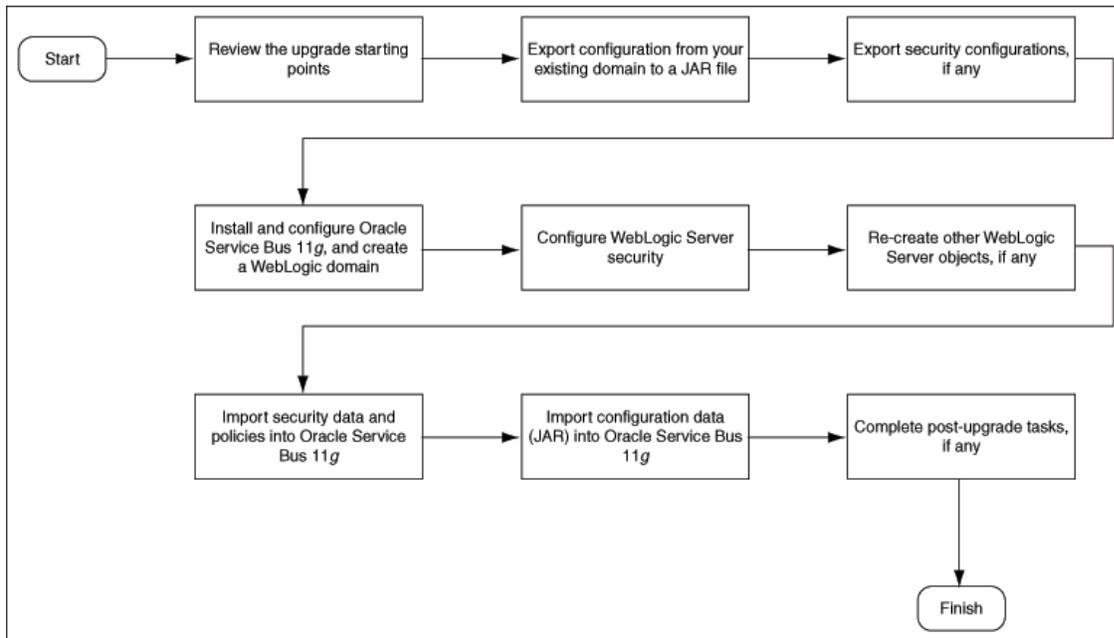
1.3 Steps in the Oracle Service Bus Upgrade Process

Table 1–1 describes each of the steps in the upgrade process flow chart, which is shown in Figure 1–1. The table also provides information on where to get more information on each step in the process.

Table 1–1   Table Describing the Steps in the Oracle Service Bus Upgrade Process for 11g

Step	Description	More Information
Review Upgrade Concepts in the *Oracle Fusion Middleware Upgrade Planning Guide*.	The *Oracle Fusion Middleware Upgrade Planning Guide* provides a high-level overview of how to upgrade your Oracle Fusion Middleware environment. It includes compatibility information and instructions for upgrading any databases that support your middleware components.	*Oracle Fusion Middleware Upgrade Planning Guide*
Understand the upgrade starting points.	Before planning your upgrade, you should be familiar with the supported starting points for an Oracle Service Bus upgrade.	Section 2.2, "Starting Points for Oracle Service Bus Upgrade"
Complete the required prerequisites.	Before you start the upgrade, you should complete the required prerequisites.	Section 2.3, "Prerequisites for Upgrading to Oracle Service Bus 11g Release 1 (11.1.1.7.0)"
Export Oracle Service Bus configuration JAR files.	You must export the configuration JAR files from your existing domain.	Section 2.4, "Task 1: Exporting Configuration from Existing Domain"

Table 1–1   (Cont.) Table Describing the Steps in the Oracle Service Bus Upgrade Process for 11g

Step	Description	More Information
Export security configuration from Existing Domain.	You must export the security configuration from your existing domain.	Section 2.5, "Task 2: Exporting Security Configurations"
Install and Configure Oracle Service Bus 11*g*.	Install and configure an instance of Oracle Service Bus 11*g* Release 1 (11.1.1). You must start the Administration Server and Managed Servers, after completing the installation and configuration.	Section 2.6, "Task 3: Installing and Configuring the Oracle Service Bus 11g Release 1 (11.1.1.7.0)"
Configure Oracle WebLogic Server security.	In the new 11*g* domain, configure the Oracle WebLogic security framework.	Section 2.7, "Task 4: Configuring Oracle WebLogic Server security"
Re-create Oracle WebLogic Server objects.	In the new Oracle Service Bus domain, re-create the Oracle WebLogic Server objects (JMS resources, such as connection factories, queues, topics, and so on) that could not be exported.	Section 2.8, "Task 5: Re-creating Other Oracle WebLogic Server Objects"
Configure Oracle WebLogic Server security and recreate other Oracle WebLogic Server objects.	You must import the security configuration to the Oracle Service Bus 11*g* domain.	Section 2.9, "Task 6: Importing Security Data and Policies into the Oracle Service Bus 11g Release 1 (11.1.1.7.0)"
Import Oracle Service Bus configuration JAR files.	You must import the JAR files to the Oracle Service Bus 11*g* R1 domain.	Section 2.10, "Task 7: Importing Configuration JAR File into Oracle Service Bus 11g Release 1 (11.1.1.7.0)"
Perform Any Required Post-Upgrade Manual Steps.	The upgrade process automates some of the upgrade procedures, but in many cases, there are additional manual tasks that you might have to perform in some cases.	Section 2.11, "Task 8: Completing Any Required Oracle Service Bus Post-Upgrade Tasks"

2

Upgrading to Oracle Service Bus 11*g* Release 1 (11.1.1.7.0)

This chapter describes how to upgrade AquaLogic Service Bus (2.6 and 3.0) and Oracle Service Bus (10.3.1.0) to Oracle Service Bus 11*g* Release 1 (11.1.1.7.0).

This chapter contains the following sections:

- Upgrade Overview
- Starting Points for Oracle Service Bus Upgrade
- Prerequisites for Upgrading to Oracle Service Bus 11g Release 1 (11.1.1.7.0)
- Task 1: Exporting Configuration from Existing Domain
- Task 2: Exporting Security Configurations
- Task 3: Installing and Configuring the Oracle Service Bus 11g Release 1 (11.1.1.7.0)
- Task 4: Configuring Oracle WebLogic Server security
- Task 5: Re-creating Other Oracle WebLogic Server Objects
- Task 6: Importing Security Data and Policies into the Oracle Service Bus 11g Release 1 (11.1.1.7.0)
- Task 7: Importing Configuration JAR File into Oracle Service Bus 11g Release 1 (11.1.1.7.0)
- Task 8: Completing Any Required Oracle Service Bus Post-Upgrade Tasks
- Verifying Your Upgrade

> **Note:** Before proceeding with the upgrade, you must review the following:
>
> - Upgrade concepts in the *Oracle Fusion Middleware Upgrade Planning Guide*
> - Section 2.2, "Starting Points for Oracle Service Bus Upgrade"

2.1 Upgrade Overview

Direct automated in-place upgrade of AquaLogic Service Bus 2.6, 2.6 RP1, 3.0, Oracle Service Bus 10*g* Release 3 (10.3), and 10*g* Release 3 Maintenance Pack 1 (10.3.1) domain to Oracle Service Bus 11*g* Release 1 (11.1.1.7.0) domains is not supported. The upgrade process includes the following steps:

- Task 1: Exporting Configuration from Existing Domain

- Task 2: Exporting Security Configurations
- Task 3: Installing and Configuring the Oracle Service Bus 11g Release 1 (11.1.1.7.0)
- Task 4: Configuring Oracle WebLogic Server security
- Task 5: Re-creating Other Oracle WebLogic Server Objects
- Task 6: Importing Security Data and Policies into the Oracle Service Bus 11g Release 1 (11.1.1.7.0)
- Task 7: Importing Configuration JAR File into Oracle Service Bus 11g Release 1 (11.1.1.7.0)
- Task 8: Completing Any Required Oracle Service Bus Post-Upgrade Tasks

The upgrade to new Oracle Service Bus domains is supported for both clustered and non-clustered domains.

Before starting the upgrade process, refer to the Prerequisites for Upgrading to Oracle Service Bus 11g Release 1 (11.1.1.7.0) and Upgrade Considerations sections.

Table 2–1 identifies the version of Oracle WebLogic Server on which each version of AquaLogic Service Bus or Oracle Service Bus runs.

Table 2–1   Oracle Service Bus and Oracle WebLogic Server Versions

Service Bus Version	WebLogic Server Version
Oracle Service Bus 11*g* Release 1 (11.1.1.7.0)	10.3.6
Oracle Service Bus 11*g* Release 1 (11.1.1.6.0)	10.3.6
Oracle Service Bus 11*g* Release 1 (11.1.1.5.0)	10. 3.5
Oracle Service Bus 11*g* Release 1 (11.1.1.4.0)	10.3.4
Oracle Service Bus 11*g* Release 1 (11.1.1.3.0)	10.3.3
Oracle Service Bus 10*g* Release 3 Maintenance Pack 1 (10.3.1)	10.3
Oracle Service Bus 10*g* Release 3 (10.3)	10.3
AquaLogic Service Bus 3.0	10.0 MP1
AquaLogic Service Bus RP1	9.2 MP2
AquaLogic Service Bus 2.6	9.2 MP1

2.2 Starting Points for Oracle Service Bus Upgrade

The follows starting points are supported:

- AquaLogic Service Bus 2.6
- AquaLogic Service Bus 2.6 RP1
- AquaLogic Service Bus 3.0
- Oracle Service Bus 10*g* Release 3 (10.3)
- Oracle Service Bus 10*g* Release 3 Maintenance Pack 1 (10.3.1)

> **Note:**   You cannot upgrade `config.jar` file from versions earlier than AquaLogic Service Bus 2.6, to Oracle Service Bus 11*g* Release 1 (11.1.1.7.0).

> **Note:** If you have an existing Oracle Service Bus 11*g* Release 1 (11.1.1.3.0) installation, you must patch Oracle Service Bus 11*g* Release 1 (11.1.1.3.0) to Oracle Service Bus 11*g* Release 1 (11.1.1.7.0) using the Patch Set installer, as specified in the *Oracle Fusion Middleware Patching Guide*.
>
> In addition, complete any post patching procedure, including Domain Migration from 11*g* Release 1 (11.1.1.3.0) to 11*g* Release 1 (11.1.1.7.0). For more information, see the section Post-Migration Configuration for Oracle Fusion Middleware Components in the *Oracle Fusion Middleware Patching Guide*.

2.3 Prerequisites for Upgrading to Oracle Service Bus 11*g* Release 1 (11.1.1.7.0)

This section contains the following:

- Section 2.3.1, "Backing Up Your Environment"
- Section 2.3.2, "Patching Oracle WebLogic Server 10.3.5"
- Section 2.3.3, "Patching Oracle WebLogic Server 10.3.6"

2.3.1 Backing Up Your Environment

Before upgrading to the latest version of Oracle Service Bus, ensure that you back up your *OSB_HOME* or *ALSB_HOME* and your domains (if they reside outside of *OSB_HOME* or *ALSB_HOME*).

If you want to revert to your previously installed version of Oracle Service Bus after upgrading to Oracle Service Bus 11*g* Release 1 (11.1.1.7.0), you must restore your Oracle Service Bus environment from backup.

If you want to save customizations you made to the Oracle Service Bus samples, export and save your sample configurations. You must import the configuration after upgrade to restore your customizations.

2.3.2 Patching Oracle WebLogic Server 10.3.5

If you are upgrading to the latest Oracle Service Bus from an environment running Oracle WebLogic Server 10.3.5, you must install two WebLogic Server patches, as described in the "Patches Required for Oracle WebLogic Server 11gR1 (10.3.5)" section in the Oracle Fusion Middleware System Requirements and Specifications document.

2.3.3 Patching Oracle WebLogic Server 10.3.6

If you are upgrading to the latest Oracle Service Bus in an environment running Oracle WebLogic Server 10.3.6, you must install the required WebLogic Server patches as described on the "Known Issues for Oracle SOA Products and Oracle AIA Foundation Pack" page on Oracle Technology Network:

http://www.oracle.com/technetwork/middleware/docs/aiasoarelnotesps6-186 6030.html

2.4 Task 1: Exporting Configuration from Existing Domain

To export your existing domain configuration, complete the following steps:

1. Start the Oracle Service Bus Administration Server for the domain you plan to upgrade to 11*g* Release 1 (11.1.1.7.0).

2. Log in to the Oracle Service Bus Administration Console by using the Administration Server user name and the password.

3. Select **System Administration**, and then **Export Resources**.

   The **Export Resources** page is displayed.

4. Select the projects or resources you want to export.

   - If you selected **Export Projects**, you cannot deselect the check boxes for individual resources.

     a. Expand the project folders. The name, type, last modified time, and references for each resource contained in the project are displayed.

     b. Select the check boxes associated with the projects or resources you want to export.

     c. Clear the check boxes associated with the projects or resources that you do not want to export.

   - If you selected **Export Resources**, select or clear the **Include Dependencies** check box. Use this option to export any other resources that this resource references.

5. Click **Export** to create a JAR file.

2.5 Task 2: Exporting Security Configurations

You can use the Oracle WebLogic Administration Console to export security data from the existing domain. To export security data to a file, complete the following steps:

1. Log in to the Oracle WebLogic Administration Console by using the Administration Server user name and the password.

2. In the left pane, select **Security Realms** under **Domain Structure** and then select the realm whose security data you want to export (for example, **myrealm**).

3. Select the **Migration** tab, and then click the **Export** tab to export the data.

4. In the **Export Directory on Server** field, specify the directory on the Administration Server to which to export the security data.

5. Click **Save**.

   The security data is saved in a file in the location you specified.

Table 2–2 summarizes the security data and types of security providers in which the data is stored.

Table 2–2   Security Data and Providers

Security Data	Security Provider Type
Group definitions	Authentication provider
User accounts	Authentication provider
Role definitions	Role mapping provider
User names and passwords in service accounts	Username and password credential mapping provider
PKI credential map entries	PKI credential mapping provider

Table 2–2   (Cont.) Security Data and Providers

Security Data	Security Provider Type
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)

> **Note:** The set of providers to export is different depending on what version you are upgrading from as described in the following sections.

Exporting AquaLogic Service Bus 2.6, 2.6 RP1, and 3.0 Security Configurations

Starting with the AquaLogic Service Bus 2.5 release, PKI, username and password credentials are stored in the WebLogic Server realm and in the ALSB configuration repository. Consequently, these credentials are exported as part of the configuration JAR that was generated and exported in Task 1: Exporting Configuration from Existing Domain. When the JAR is imported into the new domain, the realm data is populated based on the contents of the JAR file. This means that you do not need to export PKI Credentials or username/password credentials when you upgrade from AquaLogic Service Bus 2.6 and later.

For more information, see the "Migrating Security Data" chapter in the *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

Exporting Proxy Services with Access Control Policies in AquaLogic Service Bus 2.6

The exports from AquaLogic Service Bus 2.6 or earlier releases will not have any access control policies in the exported JAR files. You must first export the security realm which includes access control policies, from the AquaLogic Service Bus 2.6 and 2.6 RP1 domain on Oracle WebLogic Server 9.2 to the new Oracle Service Bus 11*g* Release 1 (11.1.1.7.0) domain on Oracle WebLogic Server 10.3.4.

Then you must export the configuration JAR file with proxy services from the AquaLogic Service Bus 2.6 and 2.6 RP1 domain to the new Oracle Service Bus 11*g* Release 1 (11.1.1.7.0) domain. For more information, see "Export data from a security provider" chapter in the *Oracle Fusion Middleware Oracle WebLogic Server Administration Console Help*.

2.6 Task 3: Installing and Configuring the Oracle Service Bus 11*g* Release 1 (11.1.1.7.0)

To install and configure Oracle Service Bus, refer to the *Oracle Fusion Middleware Installation Guide for Oracle Service Bus*.

> **Note:** After installing and configuring the Oracle Service Bus, ensure that the Administration Server and the Managed Servers are up and running.
>
> If you want to use Oracle Web Services Manager policies with Oracle Service Bus, you must select the Oracle Web Services Manager extension template after selecting one of the Oracle Service Bus domain templates when configuring the Oracle WebLogic domain.

2.7 Task 4: Configuring Oracle WebLogic Server security

In the new 11*g* Release 1 (11.1.1.7.0) domain, configure the Oracle WebLogic security framework with SSL and the security providers required to support your proxy and business services. For more information, see the "Configuring the WebLogic Security Framework: Main Steps" section in the *Oracle Fusion Middleware Developer's Guide for Oracle Service Bus*.

If you are importing configuration, note the following:

- 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 domain has 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 new domain. For example, if in your 2. 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 new domain. For more information, see the "Use X.509 certificates to establish identity" topic in the *Oracle Fusion Middleware Oracle WebLogic Server Administration Console Help*.

2.8 Task 5: Re-creating Other Oracle WebLogic Server Objects

In the new Oracle Service Bus domain, re-create the Oracle WebLogic Server objects that could not be exported in Task 1: Exporting Configuration from Existing Domain, including the following:

- 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 Oracle WebLogic Server domain resources, see the "Overview of WebLogic Server System Administration" chapter in the *Oracle Fusion Middleware Introduction to Oracle WebLogic Server*.

> **Note:** You should configure the domain-scoped SNMP agent in the Oracle WebLogic Server Console. Oracle WebLogic Server 10.x has enhanced SNMP features. For more information about SNMP, see the *Oracle WebLogic SNMP Management Guide*.

Add the Tuxedo domain ID as an Oracle WebLogic Server user (this is a requirement to successful invoke 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 Oracle WebLogic Tuxedo Connector for Tuxedo Transport in *Interoperability Solution for Tuxedo*.

2.9 Task 6: Importing Security Data and Policies into the Oracle Service Bus 11*g* Release 1 (11.1.1.7.0)

Use the Oracle WebLogic Administration Console to import the security data that you exported in Task 2: Exporting Security Configurations into the new Oracle Service Bus domain. For more information, see the "Import data into a security provider" chapter in the *Oracle Fusion Middleware Oracle WebLogic Server Administration Console Help*.

> **Note:** Import the security information for each security provider separately.

Importing Proxy Services with Access Control Policies in AquaLogic Service Bus 2.6

You must first export the security realm with access control policies in AquaLogic Service Bus 2.6 and 2.6 RP1 domain using Oracle WebLogic Server 9.2 to Oracle Service Bus 11*g* Release 1 (11.1.1.7.0) domain using Oracle WebLogic Server 10.3.4.

Then you must export the configuration jar with the proxy services from the AquaLogic Service Bus 2.6 and 2.6 RP1 domain to Oracle Service Bus 11*g* Release 1 (11.1.1.7.0) domain. For more information, see "Import data into a security provider" chapter in the *Oracle Fusion Middleware Oracle WebLogic Server Administration Console Help*.

2.10 Task 7: Importing Configuration JAR File into Oracle Service Bus 11*g* Release 1 (11.1.1.7.0)

You must import the JAR files that you have previously exported from your old domain to Oracle Service Bus 11*g* Release 1 (11.1.1.7.0) by completing the following steps:

1. Log in to the Oracle Service Bus Console by using the Administration Server user name and the password.

2. Click **Create** to create a new session, or click **Edit** to enter an existing session.

3. Select **System Administration**, and then **Import Resources**.

    The **Import Resources** page is displayed.

4. Select the project or resource JAR file that you exported in Task 1: Exporting Configuration from Existing Domain.

    a. In the **File Name** field, click **Browse** to locate the directory where the JAR file is stored.

    b. Select the JAR file, and then click **Open**.

5. Click **Next**.

    The **Import Resources - Resource JAR File** page is displayed.

6. Select **Include Dependencies** to import the resource JAR file and to ensure that all its associated resources are imported.

7. Select the check boxes associated with the projects or resources you want to import, and clear the check boxes associated with the projects or resources that you do not want to import.

8. Click **Import**.

The Import Summary page is displayed. This page displays a summary of the files imported and their status.

9. Click **Activate** in the **Change Center**. The **Activate Session** page shows the session name, user name, and a description field.

2.11 Task 8: Completing Any Required Oracle Service Bus Post-Upgrade Tasks

Some Oracle Service Bus domain configuration changes are not automated and must be implemented manually. For more information, see Upgrade Considerations.

You cannot upgrade the workspace that was used to develop Oracle Service Bus projects from the previous releases. Therefore, you must upgrade the workspace by performing one of the following steps:

Note: Oracle Service Bus 11*g* Release 1 (11.1.1) uses the Oracle Enterprise Pack for Eclipse (OEPE) Integrated Development Environment (IDE). For more information, see "Interoperability Scenarios and Considerations" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Service Bus*.

- Create a new workspace in Oracle Service Bus 11*g* Release 1 (11.1.1.7.0) using Oracle Enterprise Pack for Eclipse, and then export the config.jar files from the previous releases of workspace.

- Import the exported configuration JAR file into the new workspace using Oracle Enterprise Pack for Eclipse for Oracle Service Bus 11*g* Release 1 (11.1.1.7.0). The import process will automatically upgrade the configuration JAR file. Alternatively, you can import the configuration JAR file into an Oracle Service Bus server on 11*g* Release 1 (11.1.1.7.0) to upgrade the configuration JAR file. Then export the configuration JAR file from server and import it into the workspace using Oracle Enterprise Pack for Eclipse for Oracle Service Bus 11*g* Release 1 (11.1.1.7.0).

Note: When you import any configuration JAR into the 11*g* Release 1 (11.1.1.7.0) IDE, the operational and administrative settings are removed. To retain these settings, first import the configuration JAR file into the console, export and import the file into the 11*g* Release 1 (11.1.1.7.0) IDE, as described above. When you later move configuration from IDE to Console, enable Preserve operational settings, so that operational settings that were imported in the first step are preserved.

2.12 Verifying Your Upgrade

To verify that your upgrade was successful, find the new version number in the lower left corner of the login window when you access the Oracle Service Bus Administration Console, as shown in Figure 2–1.

Figure 2–1   Oracle Service Bus Administration Console
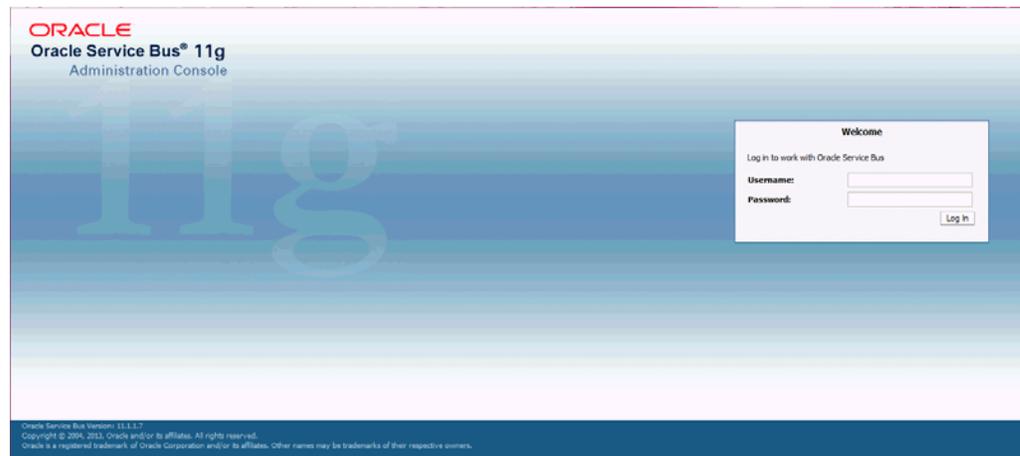
The URL for the Oracle Service Bus Administration Console is:

`http://`*`administration_server_hostname`*`:`*`administration_server_port_number`*`/sbconsole`

3

Upgrade Considerations

This chapter provides considerations for upgrading various Oracle Service Bus configuration artifacts to Oracle Service Bus 11*g* Release 1 (11.1.1.7.0).

It includes the following topics:

- Upgrade Considerations for AquaLogic Service Bus 2.6 Users
- AquaLogic Service Bus 3.0 Upgrade Considerations
- Oracle Service Bus 10g Upgrade Considerations
- Changes to Carriage Return Handling in XML in 11g Release 1 (11.1.1.6.0) and Later

3.1 Upgrade Considerations for AquaLogic Service Bus 2.6 Users

Read the following sections if you are using AquaLogic Service Bus 2.6 configurations:

- Integrated Development Environment
- Alert Rules
- Displaying References from Alerts to Alert Destinations
- Details Sent to Alert Destinations
- Import-Export Alert Rule Changes
- Session-Aware Access Control Management of Proxy Services
- Transport SDK and Transport Provider Changes

3.1.1 Integrated Development Environment

Many of the design time features available in the AquaLogic Service Bus Console are available in Oracle Enterprise Pack for Eclipse, which is the Oracle Service Bus integrated development environment (IDE).

If you want to use the IDE instead of the Console, you can import an AquaLogic Service Bus 2.6 configuration JAR directly into the 11*g* Release 1 (11.1.1.7.0) IDE. For information about importing a JAR file into the 11*g* Release 1 (11.1.1.7.0) IDE, see the "Importing Resources" section in the *Oracle Fusion Middleware Administrator's Guide for Oracle Service Bus*.

> **Note:** When you import any configuration JAR into the 11*g* Release 1 (11.1.1.7.0) IDE, the operational and administrative settings are removed. To retain these settings, first import the configuration JAR file into the console, export and import the file into the 11*g* Release 1 (11.1.1.7.0) IDE, as described above. When you later move configuration from IDE to Console, enable Preserve operational settings, so that operational settings that were imported in the first step are preserved.

For information about exporting JAR files, see Task 2: Exporting Security Configurations.

3.1.2 Alert Rules

The Service Level Agreements (SLA) alert rules features in AquaLogic Service Bus 3.0 and later differ slightly from previous releases. These changes do not affect the run-time evaluation or how alerts are issued. However, you may notice the following changes:

- In AquaLogic Service Bus 2.6, alert rule resources were created as separate resources and individually maintained. In Oracle Service Bus 11*g* Release 1 (11.1.1.6.0), alert rules are part of the service definition. Because Alert Rules are part of the service definition and are no longer resources themselves, this affects their display in the References and Referenced By pages in the AquaLogic Service Bus Console. For information about viewing references, see the "View References Page" section in the *Oracle Fusion Middleware Administrator's Guide for Oracle Service Bus*.

- You may notice minor changes in the content of the alerts as related to various destinations. For information about alert destinations, see the "Alert Destinations" section in the *Oracle Fusion Middleware Administrator's Guide for Oracle Service Bus*.

- Starting in AquaLogic Service Bus 3.0, if an alert rule is renamed, then for the alerts issued in the past and under the old name, the console will no longer provide access to the rule definition on the **Alert Summary** and **Extended SLA Alert History** pages.

3.1.3 Displaying References from Alerts to Alert Destinations

In AquaLogic Service Bus 2.6 and earlier versions where you could see distinct entries of alert rules in the AquaLogic Service Bus Console, references to alert destinations through alert rules from proxy and business services are maintained and displayed as a single reference. For example, in a proxy service, if multiple alert rules and multiple pipeline alert actions use the same alert destination, only one entry for the alert destination is displayed in the Referenced By page for that alert destination. For more information, see the "Alert Destinations" section in the *Oracle Fusion Middleware Administrator's Guide for Oracle Service Bus*.

Since Alerts are no longer separate resources in AquaLogic Service Bus 3.0 and later releases, the way references from alerts to alert destinations are displayed is different from AquaLogic Service Bus 3.0 and later releases. Two pages in the Console are affected. First, the **Referenced By** field in the Alert Destination page no longer displays the Alert Rule that is referencing the destination. Instead, the **Reference By** field displays the service that contains the alert. A side effect of this is that if a service has multiple alerts (SLA alerts or pipeline alerts) that reference the same Alert destination, the associated service is listed only once in the **Referenced By** field.

Second, the Alert Rule page no longer contains the Reference information. Instead, the Service Summary page for the associated service contains the Alert Destinations referenced in the **References** field. For more information, see the "Alert Destinations" section in the *Oracle Fusion Middleware Administrator's Guide for Oracle Service Bus*.

3.1.4 Details Sent to Alert Destinations

When an SLA alert is issued to configured destinations, the alert details include a Rule ID as in AquaLogic Service Bus 2.6 and before. However, in AquaLogic Service Bus 3.0 and later releases, the value of the Rule ID is set to a combination of the global name of the parent service and the name of the alert rule. For the SNMP trap, the Rule ID is truncated to 64 characters, as in AquaLogic Service Bus 2.6 and earlier.

3.1.5 Import-Export Alert Rule Changes

Unlike AquaLogic Service Bus 2.6, which merged alerts with any existing alerts during import, AquaLogic Service Bus 3.0 and later releases provides users with preserve-overwrite semantics. This feature allows you to either keep all existing alerts or overwrite them, regardless of whether the alerts have the same name or not.

3.1.6 Session-Aware Access Control Management of Proxy Services

The security realm must be configured before completing the steps described in this section.

The exported JARs from AquaLogic Service Bus 2.6 do not contain any access control policies. Before importing a configuration JAR from AquaLogic Service Bus 2.6 release, Oracle Service Bus 11*g* Release 1 (11.1.1.7.0) uses a pre-import access control policy to perform an in-place upgrade of the JAR to 11*g* Release 1 (11.1.1.7.0). To perform the in-place upgrade, the pre-processor queries all manageable authorization providers for each proxy service and retrieves a list of applicable access control policies. It then inserts those policies into the service definition of the proxy service. This is done on best-effort basis.

A manageable authorization provider is an authorization provider that implements the `PolicyEditorMBean` interface. Such providers expose read-write APIs that allow the Oracle WebLogic Server and the Oracle AquaLogic Service Bus console to add, modify, or delete policies stored in them.

For transport level and default message-level policies, the system queries only those providers that expose the `PolicyEditorMBean` to retrieve any applicable policies, and inserts these policies into the service definition.

For operational message-level policies, the system can query providers that have implemented the `PolicyListerMBean`. For providers that have not implemented the `PolicyListerMBean` interface, the operation-level policies are not retrieved.

After the in-place upgrade finishes, the import process proceeds as if the configuration JAR is of type 11*g* Release 1 (11.1.1.7.0), including the access control policies retrieved from the authorization providers. Table 3–1 explains various combinations of the applicable parameters and the outcome of the import process. Note that the outcome is the result of the import process and does not represent anything done after the configuration is imported.

Table 3–1   Applicable Parameters and Import Outcomes

Version of config.jar Being Imported	Proxy	ACLs in Core Repository	Preserve Policies	ACLs in Session Service Definition	Explanation
2.6	New	N/A (No)	N/A (No)	From manageable authorization providers	Upgrades the JAR to 11*g* Release 1 (11.1.1.7.0), which involves pulling all applicable ACLs from all manageable authorization providers. The service definition in session will have ACLs from the configuration JAR directly from the Authorization Providers.
2.6	Exists	No	No	From manageable authorization providers	Upgrades the JAR to 11*g* Release 1 (11.1.1.7.0). The service definition in session has ACLs from the configuration JAR directly from the Authorization Providers.
2.6	Exists	No	No	None	Upgrades the JAR to 11*g* Release 1 (11.1.1.7.0). The service definition in session has no ACLs.
2.6	Exists	Yes	No	From manageable authorization providers	Upgrades the JAR to 11*g* Release 1 (11.1.1.7.0). The service definition in session has ACLs from the configuration JAR directly from the Authorization Providers.
2.6	Exits	Yes	Yes	From the core repository in the config framework	Upgrades the JAR to 11*g* Release 1 (11.1.1.7.0). The service definition in session retains ACLs from the core repository

If an authorization provider does not exist in the target Oracle Service Bus 11*g* Release 1 (11.1.1.7.0) system, the import process ignores the imported ACLs for the authorization provider and displays a warning. In this case, you can discard the session, or undo the import task, and then add the authorization providers to the server and re-import. Alternatively, you can do a dummy update operation of security parameters in the Oracle Service Bus Console, and the system will auto-correct any conflicts that it can on best-effort basis. These changes are atomic and reversible if you discard the session.

For more information about updating the security parameters, see the "Message Level Security Configuration" section in the *Oracle Fusion Middleware Administrator's Guide for Oracle Service Bus*.

3.1.7 Transport SDK and Transport Provider Changes

The following changes may impact the Oracle Service Bus configuration:

- Message Retry Count for Business Service Configuration
- Duplicate URIs for a Business Service are Removed
- Application Errors Retries

- HTTPS Transport Changes

- Transport Configuration in the Design Environment

3.1.7.1 Message Retry Count for Business Service Configuration

In AquaLogic Service Bus 2.6, the message retry count applies to the list of URIs for a business service. In Oracle Service Bus 11*g* Release 1 (11.1.1.7.0), the retry count applies to the individual URL endpoints. The upgrade process maintains the 2.6 behavior as follows:

```
new_retries = N-1 + old_retries*N
```

where `N` is the total number of URIs and `old_retries` is the 2.6 retry count.

For example, suppose that in AquaLogic Service Bus 2.6, you have three URLs configured for the business service and a retry count of one. With the 2.6 retry mechanism all three URLs are tried. Then after the retry delay, all three URLs are retried again. To obtain the same behavior in 3.0 and later releases, the retry count is changed to five, which is obtained by applying the formula: (3 -1) + (1*3) = 5. The net effect is exactly the same: all three URLs are tried once (using two of the five retries), then after the retry delay, the three URLs are tried once more (using the last three of the five retries).

If only a single URL is configured, the old behavior and the new behavior are the same; the retry count does not change during the upgrade.

For more information, see the "Business Services: Creating and Managing" section in the *Oracle Fusion Middleware Administrator's Guide for Oracle Service Bus*.

3.1.7.2 Duplicate URIs for a Business Service are Removed

When importing business services into Oracle Service Bus 11*g* Release 1 (11.1.1.7.0), the import process removes the duplicate URIs in the 2.6 configurations. If the URIs use randomly weighted load balancing algorithms and the weights are set, the weights are adjusted accordingly. For example, if the business service is configured with the following URIs and weights:

- URI_A 1

- URI_B 3

- URI_A 1

When the business service is upgraded into 11*g* Release 1 (11.1.1.7.0), the URI set is modified as follows:

- URI_A 2

- URI_B 3

For Business services configured with other algorithms, the upgrade removes the duplicate URIs and no other changes are made.

For more information about setting the parameters for the load balancing algorithm, see the "Business Services: Creating and Managing" section in the *Oracle Fusion Middleware Administrator's Guide for Oracle Service Bus*.

3.1.7.3 Application Errors Retries

In case of delivery failure when sending outbound requests, Oracle Service Bus allows you to specify whether to retry endpoint URIs for application errors, such as a SOAP

fault. This does not affect retries for communication errors. This new option is available on the Transport Configuration page for business services. For more information, see the "Transport Configuration Page" section in the *Oracle Fusion Middleware Administrator's Guide for Oracle Service Bus*. After the number of retries is exceeded, an error is issued.

To maintain the 2.6 behavior, new tag is added with the default value set to **true**.

```
<xs:element name="retry-application-errors" type="xs:boolean"  minOccurs="0"/>
```

This tag will only be added to the transport end point whose provider configuration has the flag declare-application-errors as true.

3.1.7.4 HTTPS Transport Changes

To simplify switching between HTTP and HTTPS in the AquaLogic Service Bus 3.0 and later releases console, the HTTPS transport configuration has been removed and its functionality has been added to the 3.0 inbound HTTP transport provider. The 11*g* Release 1 (11.1.1.7.0) HTTP Transport Configuration page contains a check box to enable HTTPS.

A new element, `use-https` is added to the schema of the HTTP Transport inbound properties.

```
<xs:element name="use-https" type="xs:boolean" minOccurs="0"/>
```

Any existing HTTPS Transport configurations are upgraded to HTTP transport with this flag set to true.

> **Note:** This functionality is only applicable to HTTP proxy services.

3.1.7.5 Transport Configuration in the Design Environment

In earlier releases, AquaLogic Service Bus transports were configured only through the AquaLogic Service Bus Console. However, starting in ALSB 3.0, the transports can be designed on Eclipse. For more information, see "Developing Oracle Service Bus Transports for Workshop for WebLogic" in the *Oracle Fusion Middleware Transport SDK User Guide for Oracle Service Bus*.

3.2 AquaLogic Service Bus 3.0 Upgrade Considerations

Read the following sections if you are using AquaLogic Service Bus 3.0:

- Upgrading an AquaLogic Service Bus 3.0 Workspace in Oracle Enterprise Pack for Eclipse

- JNDI Service Account Deprecated for Java Message Service Business Service

- Pipeline Action ID Upgrade

- Pipeline Monitoring Level

- Enhanced Validation

3.2.1 Upgrading an AquaLogic Service Bus 3.0 Workspace in Oracle Enterprise Pack for Eclipse

To upgrade an AquaLogic Service Bus 3.0 workspace to Oracle Service Bus Oracle Enterprise Pack for Eclipse, perform the following steps:

> **Note:** After you upgrade the workspace, you can no longer open it in WorkSpace Studio 1.1 for ALSB 3.0.

1. Start WorkSpace Studio 1.1 in ALSB 3.0 and open the workspace you are upgrading.

2. Close the ALSB perspective and all editors.

3. Close all projects.

4. Close WorkSpace Studio 1.1.

5. Back up your workspace.

6. Start Oracle Enterprise Pack for Eclipse in 11*g* Release 1 (11.1.1.6.0), and open the workspace you are upgrading.

7. Wait for upgrade to start. When you open an AquaLogic Service Bus 3.0 workspace in Oracle Enterprise Pack for Eclipse for Oracle Service Bus 11*g* Release 1 (11.1.1.7.0), it will take a few moments for the upgrade process to start. Do not edit the workspace until the upgrade completes and the confirmation dialog appears.

8. After upgrading projects, open the **Oracle Service Bus** perspective and continue working with the newly upgraded projects and artifacts.

3.2.2 JNDI Service Account Deprecated for Java Message Service Business Service

In Oracle Service Bus 11*g* Release 1 (11.1.1.7.0), the `jndi-service-account` is deprecated. After upgrading to 11*g* Release 1 (11.1.1.7.0), the Oracle Service Bus Java Message Service (JMS) business service uses the `jms-service-account` for both JMS and JNDI purposes.

The following table shows how the Oracle Service Bus JMS business service migrates JNDI and JMS accounts.

Table 3–2   JMS Business Service JMS and JNDI Account Migration

jms-service-account Before Upgrade	jndi-service-account Before Upgrade	jms-service-account After Upgrade
sa-1	sa-1	sa-1
sa-1	sa-2	sa-1
sa-1	—	sa-1
—	sa-2	sa-2

3.2.3 Pipeline Action ID Upgrade

After upgrading to 11*g* Release 1 (11.1.1.7.0), all the actions in a pipeline are assigned a unique ID.

3.2.4 Pipeline Monitoring Level

In 11*g* Release 1 (11.1.1.7.0), proxy services use a new monitoring flag to control the level of statistics collected. The three levels are:

- `Service` - coarse grained statistics.

- `Pipeline` - the same level at which statistics were gathered in AquaLogic Service Bus 3.0.

- `Action` - fine grained statistics.

The upgrade sets the monitoring flag to a value of `Pipeline`.

3.2.5 Enhanced Validation

As of Oracle Service Bus 11*g* Release 1 (11.1.1.7.0), validation rules in the following areas have been made more strict and may result in design time or run time errors:

- Enhanced WSDL and service validation: after upgrading from previous releases to Oracle Service Bus 11*g* Release 1 (11.1.1.7.0), one may get conflict messages, such as:

  - ```
    [OSB Kernel:398022]No corresponding mapping was found in
    the service definition for the WSDL operation:
    OPERATION-NAME
    ```

  - ```
    [OSB Kernel:398034]Two operations expect the same incoming
    message, you must use a selector different than message
    body
    ```

  In this case, update your WSDL or service as the error message indicates.

- Enhanced Split-Join validation: AquaLogic Service Bus 3.0 allowed an insert action in a Split-Join to insert into an uninitialized variable. In Oracle Service Bus 11*g* Release 1 (11.1.1.7.0), such an insert action will fail with the following error:

  ```
  Variable 'VARIABLE-NAME' is being referenced before it has been initialized
  with a value.: Fault
  [{http://docs.oasis-open.org/wsbpel/2.0/process/executable}uninitializedVariabl
  e]
  ```

  If your Split-Join works in AquaLogic Service Bus 3.0 and fails in Oracle Service Bus 11*g* Release 1 (11.1.1.7.0) with the above error, then modify the Split-Join to initialize the variable before insert.

- Enhanced JMS proxy and business service URI validation: prior to Oracle Service Bus 11*g* Release 1 (11.1.1.7.0), you could enter a JMS proxy and business service URI without a host and port. In Oracle Service Bus 11*g* Release 1 (11.1.1.7.0), Oracle Service Bus applies the following validation:

  - For a JMS proxy service URI, you may omit the host and port. Doing so will display a confirmation dialog prior to commit.

  - For a JMS business service URI, you must always specify the host and port.

3.3 Oracle Service Bus 10*g* Upgrade Considerations

You must read the following upgrade considerations if you are using Oracle Service Bus 10*g* Release 3 Maintenance Pack 1 (10.3.1) or Oracle Service Bus 10g Release 3 (10.3):

- Alerts Upgrade

- JCA Endpoint Configuration

- JMS Business Service Configuration

- Global Operational Settings

- UDDI Configuration

3.3.1 Alerts Upgrade

The upgrade will preserve the existing behavior as follows:

- An Alert Log Enabled flag is added to the Alert destinations and the default value is `true`, by default.

- SLA definitions and Pipeline Alert definitions that do not have an alert destination associated with them will be upgraded as follows:

  – A new alert destination is created as part of the upgrade process. It is created under the same project as the service being upgraded, and it will have the name `AlertDestinationForLogging`. This alert destination will have only alert logging turned on. If there are multiple services under the same project that are subject to this upgrade logic, they will share the same alert destination.

  – SLA and pipeline alert definitions with no alert destinations are upgraded, so that they now reference this new alert destination.

3.3.2 JCA Endpoint Configuration

JCA Endpoint configuration will be upgraded to use the new configuration. WSDL with JCA WSIF extensions will be upgraded to Oracle Service Bus 11*g* adapter artifact. For example, JCA file, abstract WSDL, and concrete WSDL will provide the interface to upgrade JCA 10*g* wsdl to WSDL 11*g* and JCA file. Other upgrades will be as follows:

Config JAR Upgrade

JCA upgrader will scan for the imported Oracle Service Bus config.jar file, and then the JCA WSDL (Oracle SOA 10*g* WSDL with WSIF JCA extension) and the JCA services in the config.jar file will be upgraded.

> **Note:** Only JCA WSDL that are associated with JCA services will be upgraded. If JCA WSDL is not used by any JCA service, then it will not be upgraded.

JCA WSDL Upgrade

JCA WSDL in the imported config.jar file will be upgraded. A JCA resource and an abstract WSDL will be generated from the JCA WSDL. A concrete WSDL will be generated from the abstract WSDL and the JCA resource. The concrete WSDL will be generated based on the following rules:

- Target namespace should be the same as the abstract WSDL.

- JCA (concrete) WSDL in 10g with the WSIF JCA binding will be upgraded to a JCA resource containing the JCA binding, abstract WSDL containing the abstract part of the 10g WSDL, and a concrete WSDL containing the soap binding based on portType defined in the abstract WSDL. The JCA service based on the JCA WSDL in 10g will be upgraded to be based on the concrete WSDL containing the soap binding and will also have a reference to the JCA resource.

- The binding section will contain a SOAP 1.1 binding.

- The SOAP 1.1 binding style is document.

- The SOAP 1.1 binding section will contain all operations from the abstract WSDL.

- For each binding operation, a SOAP 1.1 operation element will be generated with soapAction attribute set to the operation name.

- For each binding operation's input and output element, there will be a SOAP 1.1 body element generated with attribute use set to literal.

- To support specific AQ use case that has header message defined in abstract WSDL, a SOAP header element will be generated for the operation's input binding section. The assumption is that AQ abstract WSDL will contain a WSDL message name "Header_msg" and the message contains a single part named "Header".

- A service section will be created with a port for the generated binding The generated port will contain a SOAP 1.1 address element with location attribute set to:

```
jca://<adapter_connection_factory_jndi>
```

> **Note:** If a non-jca (e.g. http, jms etc.) service type proxy/business service in Oracle Service Bus 10*g* is based on a WSDL that has jca binding, and if the same WSDL is not used by a jca service type proxy/business service, then the WSDL will not be upgraded and hence there will be a conflict on import. You must manually fix the WSDL to have a non-jca binding such as soap binding to over come the conflict.

Example 3–1   JCA Concrete WSDL

```
<?xml version="1.0"?>
<definitions name="db-inbound-concrete"
      targetNamespace="http://xmlns.oracle.com/pcbpel/adapter/db/db_inbound/"
      xmlns:tns="http://xmlns.oracle.com/pcbpel/adapter/db/db_inbound/"
      xmlns="http://schemas.xmlsoap.org/wsdl/"
      xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
  <import namespace="http://xmlns.abc.com/pcbpel/adapter/db/db_inbound/"
         location="inbound.wsdl"/>
  <binding name="db-inbound_binding" type="tns:db-inbound_ptt">
    <soap:binding style="document"
                  transport="http://www.abc.com/wli/sb/transports/jca"/>
    <operation name="receive">
      <soap:operation soapAction="receive"/>
<input name="receive">
  <soap:body use="literal"/>
</input>
      </operation>
  </binding>

  <service name="db-inbound">
    <port name="db-inbound_pt" binding="tns:db-inbound_binding">
      <soap:address location="jca://eis/DB/OSBJCADBConnection"/>
    </port>
  </service>
</definitions>
```

The existing JCA WSDL in the config jar will be updated with the concrete WSDL.

JCA Service Upgrade

Each JCA Service in the config jar will be updated with a change in JCA transport specific configuration. A reference to the generated JCA resource will be added to the

JCA transport specific configuration section. All other properties defined in the endpoint configuration will remain the same. The JCA service will still contain the same dependency on the same WSDL and binding, although the content of the WSDL is updated to contain the generated concrete WSDL.

TopLink Mapping File Content

TopLink Mapping file content will be extracted from the endpoint configuration. An XML resource will be created the toplink mapping file content extracted from endpoint configuration will be stored as the content for the XML resource. The name of the XML resource will be the toplink mapping file name specified in activation/interaction spec property in endpoint configuration without the ".xml" file extension.

A dependency on the generated toplink mapping file XML resource will be generated in the JCA file resource for this JCA service.

AQ Adapter WSDL with Header Upgrade

Prior to SOA 11*g*, the Header element definition in AQ adapter WSDL is defined with the namespace that is the same as the target namespace of WSDL itself. In SOA 11*g*, AQ adapter has changed the target namespace for the Header element in WSDL. The new namespace is a fixed namespace as the following:

`http://xmlns.oracle.com/pcbpel/adapter/aq/headers/payloadheaders/`

OSB JCA transport upgrader will automatically modify the target namespace for the Header element in AQ adapter WSDL to match the new fixed target namespace listed above.

Manual Upgrade

The JCA adapters headers used in 10*g* is now available in the `NormalizedMessage` properties. The NormalizedMessage header properties is used in 11*g*, when AQ adapter needs to have payload header. If payload header is required, then queue header and payload header will be transmitted through NormalizedMessage headers

Due to the change in header support, you must upgrade some Oracle Service Bus 10g configuration manually. Specifically, if the pipeline is accessing message header types that are not present in 11*g*, the configuration will have to be upgrade to access the header through Transport Header.

3.3.3 JMS Business Service Configuration

JMS business services using the request/response pattern (both MessageID as well as CorrelationID based correlation) will be upgraded to use the new configuration. The existing `Is response required` flag is enhanced with the `Response Queues` property option. You can specify `None`, `One per Request URI`, or `One for all Request URIs` as the value for the `Response Queues` property option. The following table shows how the existing values are upgraded.

Table 3–3   JMS Business Service Configuration

Is Response Required	Response Queues
True	One for all Request URIs
False	None

When the `Is Response Required` value is set to `true`, then the same value is used in Oracle Service Bus 11*g*, and the `Response Queues` option is set as `One` for all `Request URIs`.

When the `Is Response Required` value is set to true in the pre upgrade services then the `Response Queues` option is set as One for all `One for all Request URIs` with new configuration Response-URI for each target. In a standalone domain, this target will be a single server. The existing connection-factory and the response JNDI names are merged with the new ResponseURI configuration. The ResponseURI format is created with the available host/port information from the first service URI from business service and appended with the connection-factory and the response queue JNDI name. The host/port information is always retrieved from first service URI. The first service URI also contains a connection-factory, which is retrieved if the configured connection-factory for response is empty.

The format of Response URI is as follows:
`'jms://<ip>:<port>,<ip>:<port>/<connection-factory-jndi-name>/<response-queue-jndi-name>'`

3.3.4 Global Operational Settings

When you import a Global Operational Settings resource that does not contain result-caching element, then a new result-caching element is added with the default value `true`.

3.3.5 UDDI Configuration

UDDI related elements have been moved from the `ServiceEntry` element in `Services.xsd` to a new element `uddiConfiguration`. This element is used for business services that are imported from UDDI.

After the upgrade, during synchronization if the WSDL exist with the old name, then this name will be used. However if the WSDL does not exist then a new wsdl will be created with the new naming conventions.

The service key as well as the service name for the service will now be stored as part of the `uddiConfiguration` element.

3.4 Changes to Carriage Return Handling in XML in 11g Release 1 (11.1.1.6.0) and Later

An update was made to Apache XMLBeans, which corrects handling of carriage return characters in an XML document. The update was made because XMLBeans did not properly escape carriage return characters (`\r`). If the document contained ``, it was correctly unescaped to `\r` when parsed into XMLBeans; however, `\r` was not escaped when it was streamed out. This resulted in an invalid XML document because `\r` is invalid in XML. After the fix to XMLBeans, `\r` is correctly escaped to ``.

If you upgrade to version 11*g* Release 1 (11.1.1.6.0) or later, and currently have a workaround for the above issue in place, you need to modify how return characters are handled. For example, if the workaround was to escape `` a second time to `&#13;` in order for it to be streamed back out as ``, you need to remove the second escape to avoid validation errors.