Oracle® Fusion Middleware

Infrastructure Release Notes

12*c* (12.1.2)

E40595-01

June 2013

ORACLE®

Oracle Fusion Middleware Infrastructure Release Notes, 12*c* (12.1.2)

E40595-01

Primary Author: Sreetama Ghosh

Contributing Author: Shynitha K S, Rekha Kamath

Contents

1 Install and Configure

2 Patching and Upgrade

3 High Availability

4 Oracle Fusion Middleware Administration

5 Platform Security Services

6 Oracle User Messaging Service

7 Web Services

Preface

This book is about build automation and continuous integration for applications that you develop and deploy to a Fusion Middleware runtime environment. This book describes the new features added in Fusion Middleware 12*c* to make it easier for users to automate application build and test and to adopt continuous integration techniques with Fusion Middleware.

Audience

This document is intended for developers and build managers who are responsible for building applications that will be deployed into a Fusion Middleware runtime environment and who want to automate their build processes or adopt, or both continuous integration techniques in the context of Fusion Middleware.

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 documents in the Oracle Other Product One Release 7.0 documentation set or in the Oracle Other Product Two Release 6.1 documentation set:

- *Oracle Other Product One Release Notes*
- *Oracle Other Product One Configuration Guide*
- *Oracle Other Product Two Getting Started Guide*
- *Oracle Other Product Two Reference Guide*
- *Oracle Other Product Two Tuning and Performance 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 Install and Configure

This chapter describes issues pertaining to Oracle Fusion Middleware product installation and configuration.

The following topics are covered in this chapter:

- Section 1.1, "Issues Pertaining to Product Installation"
- Section 1.2, "Issues Pertaining to Product Configuration"
- Section 1.3, "Issues Pertaining to Product Installation and Configuration Documentation"
- Section 1.4, "Documentation Errata"

1.1 Issues Pertaining to Product Installation

There are no known issues at this time.

1.2 Issues Pertaining to Product Configuration

This section contains the following topics:

- Section 1.2.1, "Oracle Configuration Manager Cannot be Configured From the Product Installer on IBM AIX"
- Section 1.2.2, "Harmless Error Messages When Creating IAU_APPEND and IAU_VIEWER Schemas From the Command Line"

1.2.1 Oracle Configuration Manager Cannot be Configured From the Product Installer on IBM AIX

In 12*c* (12.1.2), Oracle Configuration Manager cannot be configured through the installer on IBM AIX operating systems.

To work around this issue:

1. Start the product installer as documented in the product install guide.
2. On the Specify Security Updates screen, de-select **I wish to receive security updates via My Oracle Support**.
3. Complete the product installation and dismiss the installer.
4. Run the `setupCCR` and `configCCR` scripts in the `*ORACLE_HOME*/oracle_common/ccr` directory to setup and configure Oracle Configuration Manager.

1.2.2 Harmless Error Messages When Creating IAU_APPEND and IAU_VIEWER Schemas From the Command Line

If you are running the Repository Creation Utility (RCU) from the command line and performing the system load and data load phases separately, the `IAU_APPEND` and `IAU_VIEWER` schemas will generate error messages.

These error messages can be safely ignored, and both `IAU_APPEND` and `IAU_VIEWER` schemas will be created.

1.3 Issues Pertaining to Product Installation and Configuration Documentation

This section contains the following topics:

- Section 1.3.1, "Oracle WebLogic Server ZIP Installer Documentation Erroneously Asks for JAVA_VENDOR to be Set"
- Section 1.3.2, "SIP Server Template Incorrectly Displayed During Configuration"
- Section 1.3.3, "Incorrect Step Displayed on the Installation Complete Screen"
- Section 1.3.4, "Incorrect Administration Console URL Format on the Configuration and Reconfiguration Screen"
- Section 1.3.5, "ODI Instance Option Displayed While Running FMW Infrastructure Configuration Wizard"
- Section 1.3.6, "Edit wlst Offline Script"
- Section 1.3.7, "Performance Issues While Configuring Domains with Remote Databases"
- Section 1.3.8, "Error Message Displayed When Incorrect Version of JDK Used for Installation"
- Section 1.3.9, "Deinstallation of the Fusion Middleware Product Does Not Erase All Program Shortcuts"
- Section 1.3.10, "Incorrect Error Message Displayed if JDK not Compatible with Operating System"
- Section 1.3.11, "Prerequisite Checks Fail While installing Oracle Fusion Middleware Products on Some HP Hosts"
- Section 1.3.12, "Errors Displayed During 12c ASCORE Installation"
- Section 1.3.13, "Warning Messages in make.log File"
- Section 1.3.14, "Deinstalling Oracle Fusion Middleware Product Does Not Erase All Program Shortcuts in Windows OS"
- Section 1.3.15, "Register NodeManager as a Windows Service Serving a Standalone OHS Domain"
- Section 1.3.16, "Simple Security Mode Does Not Function with OAM Server"
- Section 1.3.17, "Deinstalling Product Leaves Behind Files That Should Have Been Deleted"

1.3.1 Oracle WebLogic Server ZIP Installer Documentation Erroneously Asks for JAVA_ VENDOR to be Set

The ZIP installer for Oracle WebLogic Server documentation (`README.txt`) states that on Windows operating systems, the `JAVA_VENDOR` environment variable must be set to the JVM that is being used prior to starting the Configuration Wizard.

This is incorrect, as setting the `JAVA_VENDOR` variable is not a requirement. If this variable is not set, the Configuration Wizard will extract the `VM_TYPE` from the environment to point to the correct JDK.

The valid values of `JAVA_VENDOR` are `Oracle` or `Apple`, and the valid values of `VM_TYPE` are `HotSpot` or `Apple`.

1.3.2 SIP Server Template Incorrectly Displayed During Configuration

During configuration, the configuration wizard displays the SIP Server Template incorrectly.

Do not select this template during configuration.

1.3.3 Incorrect Step Displayed on the Installation Complete Screen

Bug # 16928758

On completing a standalone OHS installation, the step 'Start Node Manager and Domain Servers' is displayed as one of the next steps you should take after installation.

This information is incorrect, as there are no domain servers configured during the standalone installation.

1.3.4 Incorrect Administration Console URL Format on the Configuration and Reconfiguration Screen

An incorrect format of the administration console URL is displayed on the summary page of the Fusion Middleware Infrastructure configuration or reconfiguration wizard.

The correct format of the administration console URL is:

```
http://machine_name:port/console
```

1.3.5 ODI Instance Option Displayed While Running FMW Infrastructure Configuration Wizard

When you are creating a system component using the Fusion Middleware Configuration Wizard, ODI is listed as a component type that you can create, even though Oracle Data Integrator is not available in the current Fusion Middleware 12c (12.1.2) release.

Do not select this component type when creating or reconfiguring a domain.

1.3.6 Edit wlst Offline Script

When using a wlst offline script with multiple `updateDomain()` calls, you must add a `readDomain()` call after each `updateDomain()` call.

1.3.7 Performance Issues While Configuring Domains with Remote Databases

If you are creating a new domain with the Fusion Middleware Configuration Wizard, it may take longer to perform certain setup operations. You might notice these longer operation times when performing the following tasks:

- During RCU creation of the IAU schema.
- During domain creation when loading security policies
- During node manager startup when node manager is configured to use the key
- store service

1.3.8 Error Message Displayed When Incorrect Version of JDK Used for Installation

When you attempt to install a Fusion Middleware product on a 64-bit system, using a JDK for a 32-bit system, an error message is displayed before the installation begins.

Refer to the *System Requirements and Specifications* document for your product, and download a suitable JDK from the following location, before installing the Fusion Middleware software:

`http://www.oracle.com/technetwork/java/javase/downloads/index.html`

1.3.9 Deinstallation of the Fusion Middleware Product Does Not Erase All Program Shortcuts

Deinstalling a Fusion Middleware product does not erase the shortcuts from the product's home directory.

Manually delete the program shortcuts.

1.3.10 Incorrect Error Message Displayed if JDK not Compatible with Operating System

If you run the installer jar file from a 32-bit JDK7 JVM on a 64-bit machine, the installer displays an incorrect message that the version of the JVM is correct and the version of the operating system on which the software is installed is incorrect.

Refer to the System Requirements and Specifications document for your product, and download a suitable JDK from the following location, before installing the Fusion Middleware software:

`http://www.oracle.com/technetwork/java/javase/downloads/index.html`

1.3.11 Prerequisite Checks Fail While installing Oracle Fusion Middleware Products on Some HP Hosts

While installing Oracle Fusion Middleware products on some HP hosts, the prerequisite check related to CPU speed fails.

While launching the installer, specify the command line option -ignoreSysPrereqs. This lets the installer skip the System Prerequisite Checks and proceed with the installation.

1.3.12 Errors Displayed During 12c ASCORE Installation

While installing Oracle Web Tier 12*c* (12.1.2) on an Oracle Solaris 11 system, the following errors are seen in the console:

```
sh: line 1:usr/sbin/patchadd:not found
```

Ignore these error messages.

1.3.13 Warning Messages in make.log File

While installing 12.1.2 OHS on AIX, warning messages appear in the make.log file in the following location:

```
OHS_HOME/install/make.log
```

Ignore these error messages.

1.3.14 Deinstalling Oracle Fusion Middleware Product Does Not Erase All Program Shortcuts in Windows OS

Deinstalling a Fusion Middleware product from a Windows OS does not erase the shortcuts from the product's home directory.

Manually delete the program shortcuts.

1.3.15 Register NodeManager as a Windows Service Serving a Standalone OHS Domain

To register NodeManager as a Windows Service serving a Standalone OHS domain do the following after you have created the standalone domain:

1. Set the `JAVA_OPTIONS` environment variable so that it points to the standalone OHS domain directory. Enter the following command to set the environment variable:

   ```
   set JAVA_OPTIONS=-Dohs.product.home=C:\work\stand\ohs
   -Dweblogic.RootDirectory=domain_directory
   ```

   For example:

   ```
   Set Java_options=-dohs.product.home=c:\work\stand\ohs
   -dweblogic.rootdirectory=c:\oracle_home\ohs\user_projects\domains\ohs
   ```

2. Navigate to the `domain\bin` directory, and run the following command:

   ```
   installNodeMgrSvc.cmd
   ```

1.3.16 Simple Security Mode Does Not Function with OAM Server

On the AIX Platform, Simple Security Mode is not functioning with OAM Server.

While registering new Webgate Agent for artifacts generation, select **Open** or **Cert Security Mode** in OAM Server Console.

1.3.17 Deinstalling Product Leaves Behind Files That Should Have Been Deleted

The 12.1.2 deinstall does not remove all the files.

To remove all of the Fusion Middleware installed in your Oracle Home, run deinstall for all the products installed, and then delete the entire Oracle Home directory.

1.4 Documentation Errata

This section contains the following topics:

- Section 1.4.1, "Oracle WebLogic Server and Coherence Installation Type Name is Incorrect"
- Section 1.4.2, "Managed Server Names are Incorrect"

1.4.1 Oracle WebLogic Server and Coherence Installation Type Name is Incorrect

In Installing and Configuring Oracle WebLogic Server and Coherence, one of the installation types is incorrectly referred to as the "Complete with Examples" installation type.

The correct name of this installation type is "Complete Installation."

1.4.2 Managed Server Names are Incorrect

In "Starting the Managed Servers" in ***Installing and Configuring the Oracle Fusion Middleware Infrastructure***, there are references to Managed Servers named `adf_server_1` and `adf_server_2`.

The correct names of the Managed Servers are `infra_server_1` and `infra_server_2`.

2

Patching and Upgrade

This chapter describes issues related to the Infrastructure 12.1.2 upgrade.

The following topics are covered in this chapter:

- Issues Pertaining to Product Upgrade
- Issues Pertaining to Product Patching

2.1 Issues Pertaining to Product Upgrade

This section contains the following topics:

- Section 2.1.1, "Upgrade Assistant Script Execution Triggers Error Message on Solaris X64 Platforms"
- Section 2.1.2, "Log Button Does Not Display Logs"
- Section 2.1.3, "Error Message Displayed on Terminal Screen While upgrading OHS 12.1.2 on Solaris.X64"

2.1.1 Upgrade Assistant Script Execution Triggers Error Message on Solaris X64 Platforms

When launching the Upgrade Assistant from a Solaris X64 platform command line, the following error can appear:

```
./ua: [[: not found
```

You can ignore this message. The Upgrade Assistant will continue to launch in GUI mode despite this error.

2.1.2 Log Button Does Not Display Logs

The Log button in the Upgrade Assistant wizard does not display the logs.

Use a text editor outside the Upgrade Assistant to view the logs.

2.1.3 Error Message Displayed on Terminal Screen While upgrading OHS 12.1.2 on Solaris.X64

The following error message is displayed on the terminal screen during Fusion Middleware Upgrade Assistant 12.1.2 `ua` script execution :

```
./ua: [[: not found
./ua: [[: not found
```

Ignore this error message.

2.1.4 JRF Domains Do Not Support JRockit in 12.1.2

In Oracle Fusion Middleware 12.1.2. JRockit is supported only for WebLogic Server client-side applications. JRockit is no longer supported for use with WebLogic Server JRF domains

2.2 Issues Pertaining to Product Patching

This section contains the following topics:

- Error with Library Regeneration During OPatch
- OPatch Does Not Restore Regenerated Libraries Even After User Quits the Patching Process

2.2.1 Error with Library Regeneration During OPatch

The following message is displayed when library regeneration fails during OPatch:

```
Patching component oracle.wls.core.app.server, 12.1.2.0.0...

There is an error with library regeneration, please refer to the log file for
details. OPatch will continue applying the patch.....

OPatch failed with error code 115
```

Due to this error, the patch is not applied to all affected libraries. This leads to an inconsistent state of the environment.

Run OPatch rollback to restore the pre-patch environment.

For more information about how to roll back a patch, see "Using OPatch to Patch Oracle Fusion Middleware" in *Patching with OPatch.*

2.2.2 OPatch Does Not Restore Regenerated Libraries Even After User Quits the Patching Process

When OPatch postscript fails, users choose not to proceed the patching process, and quit. After quitting the patching process, OPatch does not restore regenerated libraries correctly.

Check the OPatch log to determine whether the library regeneration has occurred. If the library regeneration has occurred, then apply the patch again. When the OPatch post script fails again, choose `y` to proceed with the patching process. OPatch will not rollback the patch automatically this time. User needs to roll back OPatch manually to restore the pre-patch environment.

For more information about how to roll back a patch, see "Using OPatch to Patch Oracle Fusion Middleware" in *Patching with OPatch.*

3
High Availability

This chapter describes the issues related to Oracle Fusion Middleware high availability.

The following topic is covered in this chapter:

- Section 3.1, "Issues Pertaining to File Persistence."

3.1 Issues Pertaining to File Persistence

This section contains the following topic:

- Section 3.1.1, "File Persistence Store is Present When Using OPSS and MDS Data Sources."

3.1.1 File Persistence Store is Present When Using OPSS and MDS Data Sources

An MDS data source has a WebLogic Server file persistence store allocated along with the data source. Because the file persistence store is used only in development mode, you can ignore it for high availability purposes. There is no need to recover the file persistence store in the event of failure.

4

Oracle Fusion Middleware Administration

This chapter describes issues associated with Oracle Fusion Middleware administration. It includes the following topics:

- Section 4.1, "General Issues and Workarounds"
- Section 4.2, "Documentation Errata for the Administering Oracle Fusion Middleware"

4.1 General Issues and Workarounds

This section describes configuration issues and their workarounds. It includes the following topics:

- Section 4.1.1, "Limitations in Moving from Test to Production"
- Section 4.1.2, "SSL Certificate Chain Required on Certain Browsers"

4.1.1 Limitations in Moving from Test to Production

Note the following limitations in moving from test to production:

- When you are moving Oracle Platform Security Services and the data is moving from LDAP to LDAP, the source and target LDAP domain component hierarchy must be same. If it is not, the Oracle Platform Security Services data movement will fail. For example, if the source is hierarchy is configured as `dc=us,dc=com`, the target LDAP must have the same domain component hierarchy.
- On Windows, Node Manager must be shut down before you run the copyConfig script.
- If SSL is disabled on the source, any values for the keystores and certificates are copied to the target environment. To work around this issue, take one of the following steps:
  - Delete the values in the source environment:
    a. In Fusion Middleware Control, for each server, from the WebLogic Server menu, select Administration, then Keystores.
    b. Delete the values for the following:
    ```
    Demo Identity Keystore
    Demo Identity Keystore Type
    Demo Trust Keystore
    Demo Trust Keystore Type
    ```
    c. Click **Save.**

   d. For each server, from the WebLogic Server menu, select Administration, then SSL.

   e. Delete the values for the following:

   ```
   Identity and Trust Locations
   Private Key Location
   Certificate Locatio
   Demo Trust Keystore Type
   ```

  – If the source environment is configured with the keystore service, the target is configured with Demo certificates. After you execute the movement scripts, update the target environment to use actual certificates. See "Managing Keys and Certificates with the Keystore Service" in *Securing Applications with Oracle Platform Security Services*.

  – After you extract the move plan, edit it, substituting dummy values. However, the passphrase values must be a valid file which can contain any text. Later, if you want to enable SSL on the target system, modify the SSL values.

- If the source domain is configured with Custom Identity from a well-known Certificate Authority, the move plan still expects Custom Trust Location and Custom Trust Keystore Password properties. To work around this, you can point to the default trust keystore of the JDK and its password. For example, the default trust keystore of the JDK is located at:

  ```
  JDK_HOME/jre/lib/security/cacerts
  ```

- When you move Oracle HTTP Server, the MatchExpression directive is not moved. To work around this:

  1. After the pasteConfig operation completes, check if any MatchExpression string is present in any of the configuration files in the following directory:

     ```
     DOMAIN_HOME/config/fmwconfig/components/OHS/component_name
     ```

  2. If a MatchExpression string exists in any file, update the values with the target endpoints.

- When you execute pasteConfig and the archive contains Oracle Platform Security Services, the script may return the following errors:

  ```
  oracle.security.audit.util.StrictValidationEventHandler handleEvent
  WARNING: Failed to validate the xml content. Reason: cvc-complex-type.2.4.b:
  The content of element '' is not complete. One of
  '{"http://xmlns.oracle.com/ias/audit/audit-2.0.xsd":source}' is expected..
  Apr 24, 2013 6:28:29 AM
  oracle.security.audit.util.StrictValidationEventHandler handleEvent
  WARNING: Failed to validate the xml content. Reason: cvc-complex-type.2.4.b:
  The content of element '' is not complete. One of
  '{"http://xmlns.oracle.com/ias/audit/audit-2.0.xsd":source}' is expected..
  ```

  You can ignore these errors.

4.1.2 SSL Certificate Chain Required on Certain Browsers

When you configure SSL for Oracle HTTP Server, you may need to import the entire certificate chain (rootCA, Intermediate CAs and so on).

Certain browsers, for example Internet Explorer, require that the entire certificate chain be imported to the browsers for SSL handshake to work. If your certificate was issued by an intermediate CA, you will need to ensure that the complete chain of certificates is available on the browser or the handshake will fail. If an intermediate certificate in the chain expires, it must be renewed along with all the certificates (such as OHS server) in the chain.

4.2 Documentation Errata for the *Administering Oracle Fusion Middleware*

There are no documentation errata at this time.

5 Platform Security Services

This is chapter describes issues associated with Oracle Platform Security Services and Oracle Security Developer Tools. It includes the following topics:

- Section 5.1, "Configuration Issues and Workarounds"
- Section 5.2, "Documentation Errata"

5.1 Configuration Issues and Workarounds

There are no configuration issues to report.

5.2 Documentation Errata

This section contains corrections to documentation errors, in the following sections:

- Section 5.2.1, "Corrections to WSLT Infrastructure Security Commands"

5.2.1 Corrections to WSLT Infrastructure Security Commands

This section describes several corrections to security commands in the book *Infrastructure Security WLST Command Reference* (E29489-01)

- The leading sentence in section 2.1.1.34: "Online command that migrates the policy and credential stores to an LDAP repository." is incorrect; instead, it should be: "Online command that migrates policies, credentials, audit metadata, and keys from an existing OPSS security store to a target OPSS security store."
- The statement in section 2.1.1.40.1: "No restart is needed" can be ignored since the command is offline.
- The leading sentence in section 2.1.1.40.3 is incorrect; it should read "The following invocation rolls over the encryption key."
- The statement in section 2.1.1.41.1: "Modifies the type, user name, password, URL, and port number of a credential in the domain credential store with given map name and key name." is incorrect; instead, it should read "Updates password credentials only."
- Remove the clause "and maximum log directory size" from the description of `getAuditPolicy` in Section 2.1.2.2.1. Also change the first example in Section 2.1.2.2.3 to read:

```
wls:/mydomain/serverConfig> getAuditPolicy()
Location changed to domainRuntime tree. This is a read-only tree with
DomainMBean as the root.
For more help, use help(domainRuntime)
```

```
FilterPreset:All
Max Log File Size:104857600
```

- The discussion of the `setAuditRepository` command, in Section 2.1.2.5.2 Syntax, omits an additional argument named `timezone`. Change the syntax to read as follows:

  ```
  setAuditRepository([switchToDB],[dataSourceName],[interval], [timezone])
  ```

  and in the table of arguments, add the following:

  timezone: timezone in which the audit loader records the timestamps of the audit events. The valid values are "`utc`" and "`local`".

  Example:

  ```
  wls:/mydomain/serverConfig>
  setAuditRepository(switchToDB="true",dataSourceName="jdbc/AuditAppendDataSource
  ",interval="14",timezone="utc")
  ```

- In both examples of setAuditRepository in Section 2.1.2.5.3, change the data source jndi name to `jdbc/AuditAppendDataSource` which is the default audit data source jndi name.
- In Section 2.1.2.9.1 for the createAuditDBView command, change the first sentence to read:

  "This command generates a SQL script that you can use to create a database view to query audit log records of a specified component from the database . "

6 Oracle User Messaging Service

This chapter describes issues associated with Oracle User Messaging Service (UMS).

It includes the following topics:

- Section 6.1, "General Issues and Workarounds"
- Section 6.2, "Configuration Issues and Workarounds"

6.1 General Issues and Workarounds

This section describes general issue and workarounds. It includes the following topics:

- Section 6.1.1, "Extension Driver has Different Target Types for 11g and 12c"
- Section 6.1.2, "Node Manager Fails to Start After Configuring Oracle User Messaging Service and Oracle HTTP Server"
- Section 6.1.3, "UMS Schema Purge Script is Available for Download"
- Section 6.1.4, "Messages Metrics Rendered as Unavailable in the Performance Page for User Messaging Server"
- Section 6.1.5, "User Messaging Service URLs Unavailable After Restart"

6.1.1 Extension Driver has Different Target Types for 11g and 12c

In Oracle Enterprise Manager Fusion Middleware Control 12c, the User Messaging Service Extension driver will be displayed under the User Messaging Service folder, instead of the Application Deployments folder in the left navigation pane. The driver performance data is also available for the extension driver. This is an expected behavior.

6.1.2 Node Manager Fails to Start After Configuring Oracle User Messaging Service and Oracle HTTP Server

In a cluster environment, the node manager may fail to start if you have configured Oracle User Messaging Service (UMS) and Oracle HTTP Server in a domain with Oracle Real Application Clusters (RAC) multi data sources.

Workaround

UMS uses about 100 connections per data source if all UMS drivers are deployed and running. Therefore, in a clustered environment with RAC setup, you may have to increase the maximum number of connections allowed on the database server. Set this value to the sum of maximum number of connections per data source for each WebLogic Server. For example, when Oracle RAC is used with three nodes, that is two

WebLogic Servers with three Oracle RAC data sources, set the maximum number of connections to 600 (2 x 3 x 100).

6.1.3 UMS Schema Purge Script is Available for Download

A UMS schema purge script is available for your download and use. You can access the script and instructions for its use by contacting Oracle Support.

> **Note:** The purge script is available as part of the UMS 12c component for Oracle Database users.

6.1.4 Messages Metrics Rendered as Unavailable in the Performance Page for User Messaging Server

When no metric data is found (for example when no messages have been sent or received after server setup), the Metrics Performance page will display *Unavailable*. This is not a problem with the software, and the Performance reporting is operating properly. As soon as *Send* and *Receive* traffic exists, the Performance page will display results normally.

6.1.5 User Messaging Service URLs Unavailable After Restart

Upon restarting the User Messaging Service server (*usermessagingserver*) from Oracle Enterprise Manager Fusion Middleware Control or through Oracle WebLogic Console, you may get an error: `Error 503--Service Unavailable` when attempting to access any URLs served by the User Messaging Service server, such as the User Preferences UI (*/sdpmessaging/userprefs-ui*) or the various Web Services endpoints. This error occurs intermittently in cases when the Oracle WebLogic Server is heavily loaded (such as with a SOA instance). To work around this issue:

- Restart the User Messaging Service server again (two or more restarts may be required).
- If multiple User Messaging Service server restarts are not sufficient, then restart the entire Oracle WebLogic Server instance.

6.2 Configuration Issues and Workarounds

This section describes configuration issues and their workarounds. It includes the following topics:

- Section 6.2.1, "Pre-seeded Channel for Worklist and Pop-up Drivers Cannot be Removed"
- Section 6.2.2, "Use Correct SSL Trust Store When Configuring Drivers"
- Section 6.2.3, "Worklist Driver Configuration"

6.2.1 Pre-seeded Channel for Worklist and Pop-up Drivers Cannot be Removed

If you deinstall the Worklist or Pop-up driver, the pre-seeded channel for these drivers cannot be removed. The pre-seeded channel will remain available in your preference list.

6.2.2 Use Correct SSL Trust Store When Configuring Drivers

Before configuring any User Messaging Service Driver (such as the Email Driver), to connect to a remote gateway using SSL, ensure that the SSL Trust Store is properly configured as described in "Configure Keystores" in *Oracle WebLogic Server Administration Console Online Help*.

Ensure that the value of the JVM system property (`javax.net.ssl.trustStore`) set in `$DOMAIN_HOME/bin/setDomainEnv.sh` (or Windows equivalent file) points to the correct trust store that you want to use.The Java Standard Trust Store is located at:

`$JAVA_HOME/jre/lib/security/cacerts` or `$BEA_JAVA_HOME/jre/lib/security/cacerts`

With the default out-of-the-box configuration of SSL trust store, that is with the Java Standard Trust Store, the UMS driver will be able to connect to the Oracle Beehive Email Server over SSL. Note that in some installations, for example, when you have SOA installed, the Java Standard Trust Store is replaced by a Demo Trust Store. In such situations, the Trust Store may not contain the valid root certificate needed by Oracle Beehive Email Server. To resolve this issue, follow the instructions for using the correct SSL trust store. Replacing the `DemoTrust` keystore in the `setDomainEnv.sh` file (or Windows equivalent file) with the Java Standard SSL trust store will enable UMS email driver to connect successfully over SSL to the Oracle Beehive Email Server.

6.2.3 Worklist Driver Configuration

While following the Worklist Driver configuration instructions, you may see that *Oracle User Messaging Service for SOA* in the Configuration Wizard is not selected, leading you to think that it is not configured and that you must select and configure it. This is not the case. The basic Oracle User Messaging Service is already configured, along with a few UMS drivers.

Continue to follow the documented instructions, and disregard the fact that the *Oracle User Messaging Service for SOA* option is not selected.

7 Web Services

This chapter describes issues associated with Web services development, security, and administration, including Oracle Web Services Manager.

It includes the following topics:

> **Note:** For WebLogic Web Services, see "Web Services and XML Issues and Workarounds" in the *Oracle Fusion Middleware Release Notes for Oracle WebLogic Server*.

7.1 Using Multibyte User Credentials with wss_http_token_* Policy

In this release, multibyte user credentials are not supported for the `wss_http_token_*` policies. If multibyte user credentials are required, use a different policy, such as `wss_username_token_*` policy. For more information about the available policies, see "Predefined Policies" in *Securing Web Services and Managing Policies with Oracle Web Services Manager*.

7.2 Performing a Bulk Upload of Policies

When performing a bulk import of policies to the MDS repository, if the operation does not succeed initially, retry the operation until the bulk import succeeds.

For the most part, this can occur for an Oracle RAC database when the database is switched during the metadata upload. If there are *n* databases in the Oracle RAC database, then you may need to retry this operation *n* times.

For more information about bulk import of policies, see "Migrating Policies" in the *Administering Web Services*.

7.3 Removing Post-deployment Customizations

When the `connections.xml` file is changed after deployment using the `AdfConnection` MBean, the complete connection is saved as a customization. This means that changes to the connection in a redeployed application are overwritten by the customization.

When you use Fusion Middleware Control to make changes to an application's `connections.xml` file after deployment, a new `connections.xml` file is created as a customization and stored in the MDS repository. This customization persists for the life of the application. Therefore, if you redeploy the application, the customized `connections.xml` file continues to be applied as a customization on the application.

To allow the redeployed application's `connections.xml` file to be applied without the prior customization (from Fusion Middleware Control), you must explicitly remove the `connections.xml` customizations from the MDS repository.

For example, if you deploy an application with a Web services data control, then use Fusion Middleware Control to attach the `username_token_client_policy`, and subsequently detach the policy. Then, you return to JDeveloper to edit the application and attach the `http_token_client_policy`, and redeploy the application. When you view the application using Fusion Middleware Control, you see that it is not using the `http_token_client_policy` that you attached. That is because it is using the customized connections.xml file that you previously created using Fusion Middleware Control.

If you remove the connections.xml customizations from the MDS repository, the application will use the its own `connections.xml` file.

7.4 Reviewing Localization Limitations

The following information is supported in **English only** in this release of Oracle Enterprise Manager:

- All fields in the policy and assertion template except the `orawsp:displayName` field.
- If using the `?orawsdl` browser address, the `orawsp:description` field.

7.5 Fusion Middleware Control Does Not List Policies When Two Servers Are SSL Enabled (Two-way SSL)

When a Managed Server is Two-way enabled SSL (for example, a SOA server hosting OWSM Policy Manager over Two-way SSL) and the Administration Server hosting Fusion Middleware Control is correctly configured to access the Two-way SSL-enabled Managed Server, Fusion Middleware Control still does not list the OWSM policies.

7.6 Web Service Test Page Cannot Test Input Arguments Bound to SOAP Headers

For Web services that have any input arguments bound to SOAP headers, the Test Web Service page in the Fusion Middleware Control console cannot show the message. Therefore, such operations cannot be tested with the **Test Web Service** page.

For example, if the input for a multi-part WSDL is viewed through Fusion Middleware Control, and one input argument is bound to a SOAP header, the composite instance fails with the following exception because the other part of the message was missing in the input:

```
ORAMED-01203:[No Part]No part exist with name "request1" in source message
```

To resolve such an issue, select XML View for Input Arguments and edit the payload to pass input for both parts of the WSDL.

7.7 Possible Limitation When Using Custom Exactly-one Policies

In some cases, there can be a limitation when using custom Exactly-one policies. For a set of assertions within the exactly-one policy, if a request message satisfies the first assertion, then the first assertion gets executed and a response is sent accordingly. However, this may not be the desired behavior in some cases because the request may be intended for the subsequent assertions.

For example, you may have a client policy that has `Timestamp=ON` and a service exactly-one policy that has a `wss11 username token` with message protection assertions: the first has `Timestamp=OFF`; the second has `Timestamp=ON`. Therefore, the first assertion in the service exactly-one policy is not expecting the Timestamp in the request, yet the second assertion does expect it. In this case, the first assertion gets executed and the response is sent with no Timestamp. However, the client-side processing then fails because it expects the Timestamp that was sent in the request.

This limitation can exist with any cases where a client policy expects a greater number of elements to be signed and a service policy does not.

7.8 Ignore "Services Compatibility" Error for Security Policies Used Between OWSM and WebLogic Server

Fusion Middleware Control may display a false error message when verifying compatibility of service policies. This incompatibility message is shown when using Enterprise Manager to attach an OWSM Security client policy. Upon clicking the **Check Services Compatibility**, a message states that policies are incompatible despite the fact that these might be compatible.

Workaround:

If OWSM policies are attached at the Web service endpoint, use the corresponding client policy. For example, if the service has `wss11_saml_or_username_token_with_message_protection_service_policy`, `wss11_saml_token_with_message_protection_client_policy`, or `wss11_username_token_with_message_protection_client_policy` will work at the client side. If non-WSM policies are attached to the Web Service, see the *Interoperability Solutions Guide for Oracle Web Services Manager* for information about the corresponding client policy and attach it.

7.9 Security Policies Do Not Work on Subscriber Mediator Component

Component Authorization `denyall` policy does not work at subscriber mediator component. Authorization policy works for other normal mediator component cases.

7.10 Policy Table Might Not Show Attached Policies for Some Locales

Select the Web service application in Fusion Middleware Control and navigate to the Web service endpoint. Attach a policy to the endpoint in the Attach/Detach page. Sometimes the Directly Attached Polices table might not display the attached policies for the following locales: `zh-cn`, `zh-tw`, `ja`, `pt-br`, `es`, `fr`, `ko`.

As a workaround, enlarge the columns.

7.11 Usage Tracking Not Enabled for WebLogic Web Service Client

In this release, usage tracking and analysis is not provided for WebLogic Java EE Web service clients.

7.12 Do Not Attach a Permitall and Denyall Policy to the Same Web Service

Although you can attach multiple authorization policies to the same Web service, you should not attach both a `permitall` and `denyall` policy. If you do so, however, the combination validates successfully in this release.

Workaround:

Do not attach a `permitall` and `denyall` policy to the same Web service. For more information about authorization policies, see "Configuring Authorization" in *Securing Web Services and Managing Policies with Oracle Web Services Manager*.

7.13 Scoped Configuration Override Persists for Subsequent References to the Same Policy

When using a scoped configuration override for the server side identity/encryption key (`keystore.enc.csf.key`) with a message protection policy, the override value is stored in the policy. Because the policy is cached, any subsequent references to this policy by other services will contain the override value. Therefore, the results will not be as expected.

An example of this scenario is as follows:

- An Oracle Infrastructure Web service has an attached message protection service policy. Both the service identity (service public encryption key, `keystore.enc.csf.key`) and the service message protection policy are advertised in the service WSDL. If the service encryption key is overwritten, using the global `setWSMPolicyOverride` command for example, then the scoped overwritten value for the `keystore.enc.csf.key` property that was intended for the specific attachment/reference of the initial service may affect other services attachments/references to the same policy.

Workaround

The recommended workaround is to perform a cache refresh when possible. For example, if a policy attachment/reference has a scoped override for the property `keystore.enc.csf.key` and it has been enforced or advertised once, the cached policy contains the override, however the original policy in the repository is not affected. To clear the override you can refresh the cache using methods such as restarting the server, redeploying the application, modifying the policy using Fusion Middleware Control, and so on.

In some scenarios, however, a cache refresh is not feasible. For example, if a service with a policy attachment/reference has a scoped override for the property `keystore.enc.csf.key` and it is enforced before other services that reference the same policy in a flow of execution that does not allow time for a manual cache refresh, then the policy in the cache referenced by the subsequent services contains the configuration override. For example, in an asynchronous service where the same policy is attached to both the asynchronous request and the asynchronous callback client, and only the asynchronous request attachment/reference has the override (the asynchronous callback does not), the asynchronous callback policy enforcement happens after the asynchronous request. In this case, the callback client accesses the policy in the cache that contains the configuration override. Since there is no opportunity to refresh the cache, there is no workaround available.

7.14 Restart Applications to Get an Accurate Policy Usage Count

If a policy that is being referred to by a Web Service is deleted and then re-imported, then its usage count will not be correct and application(s) must be restarted to obtain an accurate usage count.

7.15 Performance Improvements in Web Services Policy Pages

Performance improvements have been made to the Web Services Policy pages in Fusion Middleware Control by removing the unnecessary role query.

7.16 Incorrect Compatible Client Policies List

When generating client policies from the WSDL, as described in "Generating Client Policies from a WSDL" in *Securing Web Services and Managing Policies With Oracle Web Services Manager*, the `wss_username_token_over_ssl_client_policy` policy is not returned in the list of compatible client policies for a corresponding Web service that has the following policy attached:

```
wss11_saml_or_username_token_with_message_protection_service_policy
```

This client policy does appear in the list of compatible client policies when attaching policies to the same client, as described in "Attaching Policies Directly to Web Service Clients" in *Securing Web Services and Managing Policies With Oracle Web Services Manager*.

7.17 Secure Conversation Element is Seen in Custom ExactlyOne Policies

When creating an ExactlyOne policy using the secure conversation policies, the `secure-conversation` element may be present in the newly created policy. OWSM does not currently support the use of the `secure-conversation` element. The element can be safely ignored. For information on the policies that support secure conversation, see "Which Policies Support WS-SecureConversation?" in *Securing Web Services and Managing Policies with Oracle Web Services Manager*.

7.18 Web Services Reliable Messaging is Not Supported in the Current Release

The WebLogic Server 12*c* (12.1.2) JAX-WS WS-ReliableMessaging implementation is generally not recommended for production purposes and has been disabled by default. The Web services reliable messaging sample application delivered with the WebLogic Server examples server is also disabled by default.

Customers seeking to use JAX-WS WS-ReliableMessaging in WebLogic Server 12*c* (12.1.2) for evaluation purposes, or customers who require use of JAX-WS WS-ReliableMessaging functionality in production, should contact Oracle Customer Support.

`http://www.oracle.com/us/support/index.html`

7.19 Bulk Attachment of Policies is not Supported in the Current Release

Attaching one or more policies to one or more Web services using the bulk attachment feature is not supported in the current release. Please use the Policy Set feature instead.

For more information on Policy Sets, see "Attaching Policies Globally Using Policy Sets Using WLST" and "Schema Reference for Policy Sets" in *Securing Web Services and Managing Policies with Oracle Web Services Manager*.

7.20 Enterprise Manager Returns You to the OWSM Policies Page After Editing a Client Policy

When you generate client policies in Enterprise Manager, the Generate Client Policies page is displayed and the generated policies are shown as Not saved. Once you save the policies, and then edit one of them, you are returned to the OWSM Policies page. This is an error in Enterprise Manager. You should be returned to the Generate Client Policies page.

To edit additional policies, use the search feature in the OWSM Policies page to locate the client policy you wish to edit.

For more information, see "Generating Client Policies from a WSDL" in *Securing Web Services and Managing Policies with Oracle Web Services Manager*.

7.21 KSS and HSM Keystore Configuration Changes Do Not Display

When you save your Keystore Service (KSS) or Hardware Security Module (HSM) configuration changes on the OWSM Domain Configuration page, the changes are implemented but not displayed (that is, the page gives no indication that the changes were made).

For more information on configuring the KSS and HSM keystores on the OWSM Domain Configuration page, see "Configuring OWSM to Use the KSS Keystore" and "Configuring OWSM to Use HSM Keystores" in *Securing Web Services and Managing Policies with Oracle Web Services Manager*.

7.22 JKS Configuration Screen Displays Incorrect Values

If you configure the OWSM keystore for KSS and then attempt to configure the JKS keystore, the **Path** field and the **Key** menus in the JKS configuration screen are populated with the values for the KSS keystore.

Workaround: Clear the Path and Key fields in the JKS configuration screen before configuring the JKS keystore. For information on configuring JKS keystore in OWSM, see "Configuring OWSM to Use the JKS Keystore" in *Securing Web Services and Managing Policies with Oracle Web Services Manager*

7.23 Token Attribute Rule Configuration Does Not Work Correctly in Fusion Middleware Control

In Fusion Middleware Control, the configuration of a token attribute rule for a trusted issuer on the Authentication tab in the Domain Configuration page is not working correctly. As a workaround, use WLST commands to configure the token attribute rule.

Configuring a token attribute rule in Fusion Middleware Control is described in "Configuring Token Attribute Rules for Trusted Issuers Using Fusion Middleware Control" in *Securing Web Services and Managing Policies with Oracle Web Services Manager*. Configuring a token attribute rule using WLST is described in "Configuring SAML Trusted Issuers, DN Lists, and Token Attribute Rules Using WLST" in *Securing Web Services and Managing Policies with Oracle Web Services Manager*.

7.24 Context Root Must Not be Set to "/" When Securing REST Applications

If you want to secure a REST application using OWSM policies, then the context root for the application must be set to some value other than the forward slash ("/").

7.25 Domain Configuration Is Not Supported in Classpath Mode

If the Policy Manager URL is configured as a classpath, then domain-level configuration is not supported. All domain-level configuration information is stored in the OWSM repository, and not the JAR file that is included in the classpath. For information about configuring the Policy Manager URL, see the following sections in *Securing Web Services and Managing Policies with Oracle Web Services Manager*:

- "Configuring the Policy Manager Connection Using Fusion Middleware Control"
- "Configuring the Policy Manager Connection Using WLST"

If you wish to manage domain-level configuration, configure the Policy Manager URL to specify a remote domain or use `auto` mode. Once you have configured the new Policy Manager URL mode, you must restart the server for it to take effect.

7.26 Apply/Revert Buttons Are Not Activated After Editing SAML Trust on Authentication Tab of OWSM Domain Configuration Page

When editing the SAML trusted issuers and DN lists on the Authentication tab of the OWSM Domain Configuration page, as described in "Configuring SAML Trusted Issuers and DN Lists Using FMC" in *Securing Web Services and Managing Policies with Oracle Web Services Manager*, the **Apply** and **Revert** buttons are not activated until you edit another field on the page. If necessary, make "dummy" edits in another field to activate the buttons.

7.27 Query by Example Feature is Not Working

"Using the Query by Example Filter" (for Web Service policies) and "Using the Query by Example Filter" (for assertion templates) in *Securing Web Services and Managing Policies with Oracle Web Services Manager* describe how to search for policies and assertion templates by querying on a specific field. This feature is not working in the current release.

Workaround: To work around this issue, use the advanced search utility as described in "Using Advanced Search" (for Web Service policies) and in "Using Advanced Search" (for assertion templates) in *Securing Web Services and Managing Policies with Oracle Web Services Manager*.

7.28 An NPE Can be Thrown if STS Certificate is Missing from Signed SAML Token

By default, Oracle Security Token Service (OSTS) does not include an STS signing certificate inside the signed SAML token returned from STS. If OWSM encounters a signed token without an STS certificate inside a SAML signature, then it throws a `NullPointerException` (NPE).

Workaround: To work around this problem, ensure that an STS certificate is present in the signed SAML token. For information on configuring a policy for STS, see "Setting

Up Automatic Policy Configuration for STS" in *Securing Web Services and Managing Policies with Oracle Web Services Manager*.

7.29 Avoiding XML Encryption Attacks

In past releases, OWSM sent different fault codes (for example, `FailedAuthentication`, `InvalidSecurityToken`, `FailedCheck`, and so on) for different error cases In the current release, this default behavior has been changed. OWSM now sends the `InvalidSecurity` fault code for all error cases. This has been done to avoid XML encryption attacks. An encryption attack is possible if the service sends different fault codes for different types of errors (for example, `FailedAuthentication`, `InvalidSecurityToken`, `FailedCheck`, and so on).

This default behavior can be changed by setting the domain-wide agent property `use.unified.fault.code` to `false`. However, this is not recommended, because it might allow XML encryption attacks. The default value for this property, "`true`", will cause OWSM to send the `InvalidSecurity` fault code for all error cases. For more information on the `use.unified.fault.code` property, see "Configuring Security Policy Enforcement Using WLST" in *Securing Web Services and Managing Policies with Oracle Web Services Manager*.

7.30 Cross-Domain Policy Manager Configuration is Not Supported in this Release

Configuration to a Policy Manager in a remote domain is not supported in this release. Therefore, the procedures to connect to a remote Policy Manager, described in the following topics in *Securing Web Services and Managing Policies with Oracle Web Services Manager*, are not recommended in a production environment:

- Configuring the Connection to a Remote Policy Manager
- Configuring the Policy Manager Connection Using Fusion Middleware Control
- Configuring the Policy Manager Connection Using WLST

7.31 OWSM Introspection Plug-in Fails When Proxy is Configured Incorrectly

OWSM provides an introspection plug-in for Oracle Virtual Assembly Builder, which is a tool for virtualizing installed Oracle components, modifying those components, and then deploying them into an Oracle VM environment. For more information, see "OWSM Introspection Plug-in for Oracle Virtual Assembly Builder" in *Securing Web Services and Managing Policies with Oracle Web Services Manager*.

The OWSM introspection plug-in executes when you introspect a WebLogic domain using the `abctl introspectWLS12` command or Oracle Virtual Assembly Builder Studio (`abstudio.sh`). This introspection may fail in the following conditions:

- When the Administration Server listen address is configured to listen on a particular address that is different than `localhost`.

  Workaround:

  1. Clear the Administration Server listen address in the Administration Console to enable the local address to be in effect, as described in "Configure listen address" in *Oracle WebLogic Server Administration Console Online Help*.
  2. Set the Administration Server listen address to `localhost`.

- When proxy setting is performed during introspection. This introspection may fail when a proxy server is required in your networking environment and no proxy configuration is available to the tool being used to perform the introspection (for example, `abctl` or `abstudio.sh`).

  Workaround:

  If you are introspecting using `abstudio.sh`, you must bypass the proxy setting for `localhost`. Please consult the *Release Notes for Oracle Virtual Assembly Builder* for information about configuring the proxy.

  If you are introspecting with `abctl`, use the standard proxy configuration properties for Java applications. Before issuing the `abctl` command, set the properties in your environment using the `SYSPROPS` environment variable to bypass the proxy setting for `localhost`. For example, use one of the following commands, based on your shell:

  csh: `setenv SYSPROPS '-Dhttp.proxyHost=`*`myProxyHost`*` -Dhttp.proxyPort=`*`NN`*` -Dhttp.nonProxyHosts=localhost|`*`n.n.n.n`*

  sh/bash/ksh: `export SYSPROPS '-Dhttp.proxyHost=`*`myProxyHost`*` -Dhttp.proxyPort=`*`NN`*` -Dhttp.nonProxyHosts=localhost|`*`n.n.n.n`*

  Note: The actual proxy settings will be specific to your environment.

7.32 BadContextToken is Not Handled in Unified Fault Code

This bug impacts the reissue of the secure conversation token (SCT). The SCT is reissued when a `BadContextToken` fault is received at client side. However, due to this bug, the client does not clear its cache and continues to send the same token until the token expires.

This situation can happen when the client has a valid token and the service does not have the same token in the session manager. If service side persistence is not enabled and the server goes down, then it will not have the session IDs then the server resumes. As a result, client requests will fail. Normally, the client-side cache is cleared when the `BadContextToken` fault is received, but due to unified fault code, the client will receive a different fault code.

The workaround is to disable unified fault code. For more information on the `use.unified.fault.code` option, see "Configuring Security Policy Enforcement Using WLST" in *Securing Web Services and Managing Policies with Oracle Web Services Manager*.

7.33 Deprecated Commands for Oracle Infrastructure Web Services

Table 7–1 lists the WLST commands for Oracle Infrastructure Web Services (or clients) that were available in Oracle Fusion Middleware 11*g* release and which have been deprecated in 12*c* (12.1.2). In addition, the table lists the new WLST command equivalent and provides an example of how you can update your code use the new command.

For more information about the WLST commands, see "Web Services Custom WLST Commands" in *WLST Command Reference for Infrastructure Components*.

Table 7–1 Deprecated Commands for Oracle Infrastructure Web Services

Deprecated Command (11g)	Recommended Command (12*c*)	Updating Your Code

`abortRespositorySession`	`abortWSMSession`	11*g* Release (for Repository operations):
		`wls:/jrfServer_domain/serverConfig>` **`abortRepositorySession()`**
		12*c* Release (for both Repository and PolicySubject operations):
		`wls:/jrfServer_domain/serverConfig>` **`abortWSMSession()`**

`attachPolicySet`	`setWSMPolicySetScope`	11*g* Release:
		`wls:/jrfServer_domain/serverConfig>` **`attachPolicySet ('Domain("base_domain")')`**
		12*c* Release:
		`wls:/jrfServer_domain/serverConfig>` **`setWSMPolicySetScope ('Domain("base_domain")')`**

`attachPolicySetPolicy`	`attachWSMPolicy`
	`attachWSMPolicies`
		11*g* Release (for both Repository and PolicySubject operation on policy set):
		`wls:/jrfServer_domain/serverConfig>` **`attachPolicySetPolicy ('oracle/wss_username_token_service_policy')`**
		12*c* Release:
		`wls:/jrfServer_domain/serverConfig>` **`attachWSMPolicy('oracle/wss_username_token_service_policy')`**
		`wls:/wls-domain/serverConfig>`**`attachWSMPolicies(["oracle/wss_username_token_client_policy","oracle/log_policy"])`**

`beginRespositorySession`	`beginWSMSession`	11*g* Release (for Repository operations):
		`wls:/jrfServer_domain/serverConfig>` **`beginRepositorySession()`**
		12*c* Release (for both Repository and PolicySubject operations):
		`wls:/jrfServer_domain/serverConfig>` **`beginWSMSession()`**

`clonePolicySet`	`cloneWSMPolicySet`	11*g* Release:
		`wls:/jrfServer_domain/serverConfig>` **`clonePolicySet ('myNewPolicySet', 'myPolicySet')`**
		12*c* Release:
		`wls:/jrfServer_domain/serverConfig>` **`cloneWSMPolicySet ('myNewPolicySet', 'myPolicySet')`**

Table 7–1 (Cont.) Deprecated Commands for Oracle Infrastructure Web Services

Deprecated Command (11g)	Recommended Command (12*c*)	Updating Your Code

commitRespositorySession	commitWSMSession	11*g* Release (for Repository operations):
		wls:/jrfServer_domain/serverConfig> **commitRepositorySession()**
		12*c* Release (for both Repository and PolicySubject operations):
		wls:/jrfServer_domain/serverConfig> **commitWSMSession()**

createPolicySet	createWSMPolicySet	11*g* Release: wls:/jrfServer_domain/serverConfig> **createPolicySet('myPolicySet', 'ws-service', 'Domain("base_ domain")')** 12*c* Release: wls:/jrfServer_domain/serverConfig> **createWSMPolicySet ('myPolicySet', 'ws-service', 'Domain("base_ domain")')**
deletePolicySet	deleteWSMPolicySet	11*g* Release: wls:/jrfServer_domain/serverConfig> **deletePolicySet('myPolicySet')** 12*c* Release: wls:/jrfServer_domain/serverConfig> **deleteWSMPolicySet ('myPolicySet')**

describeRespositorySession	describeWSMSession	11*g* Release (for Repository operations):
		wls:/jrfServer_domain/serverConfig> **describeRepositorySession()**
		11*g* Release (for PolicySubject operations):
		N/A
		12*c* Release (for both Repository and PolicySubject operations):
		wls:/jrfServer_domain/serverConfig> **describeWSMSession()**

Table 7–1 (Cont.) Deprecated Commands for Oracle Infrastructure Web Services

Deprecated Command (11g)	Recommended Command (12*c*)	Updating Your Code
detachPolicySet	detachWSMPolicy detachWSMPolicies	11*g* Release (for both Repository and PolicySubject operation on policy set): wls:/jrfServer_domain/serverConfig> **detachPolicySet ('oracle/wss_username_token_service_policy')** 12*c* Release: wls:/jrfServer_domain/serverConfig> **detachWSMPolicy('oracle/wss_username_token_service_policy')** wls:/wls-domain/serverConfig>**detachWSMPolicies(["oracle/log_policy","oracle/wss_username_token_client_policy"])**
displayPolicySet	displayWSMPolicySet	11*g* Release: wls:/jrfServer_domain/serverConfig> **displayPolicySet('myPolicySet')** 12*c* Release: wls:/jrfServer_domain/serverConfig> **displayWSMPolicySet ('myPolicySet')**
enablePolicySet	enableWSMPolicySet	11*g* Release: wls:/jrfServer_domain/serverConfig> **enablePolicySet(true)** 12*c* Release: wls:/jrfServer_domain/serverConfig> **enableWSMPolicySet(true)**
enablePolicySetPolicy	enableWSMPolicy enableWSMPolicies	11*g* Release: wls:/wls-domain/serverConfig>**enablePolicySetPolicy('/oracle/log_policy',false)** 12*c* Release: wls:/wls-domain/serverConfig>**enableWSMPolicy('/oracle/log_policy',false)** wls:/wls-domain/serverConfig>**enableWSMPolicies(["oracle/log_policy", "oracle/wss_username_token_client_policy"], true)**

Table 7–1 (Cont.) Deprecated Commands for Oracle Infrastructure Web Services

Deprecated Command (11g)	Recommended Command (12*c*)	Updating Your Code

`exportRepository`	`exportWSMRepository`	11*g* Release:
		`wls:/jrfServer_domain/serverConfig>` **`exportRepository ("/tmp/repo.zip")`**
		12*c* Release:
		`wls:/jrfServer_domain/serverConfig>` **`exportWSMRepository ("/tmp/repo.zip")`**

`importRepository`	`importWSMArchive`	11*g* Release (for repository documents):
		`wls:/jrfServer_domain/serverConfig>` **`importRepository ("/tmp/repo.zip")`**
		12*c* Release (for repository documents):
		`wls:/jrfServer_domain/serverConfig>` **`importWSMArchive ("/tmp/repo.zip")`**

`listPolicySets`	`listWSMPolicySets`	11*g* Release:
		`wls:/wls-domain/serverConfig>`**`listPolicySets('sca-reference')`**
		12*c* Release:
		`wls:/wls-domain/serverConfig>`**`listWSMPolicySets('sca-reference')`**

`migrateAttachments`	`migrateWSMAttachments`	11*g* Release:
		`wls:/jrfServer_domain/serverConfig>` **`migrateAttachments()`**
		12*c* Release:
		`wls:/jrfServer_domain/serverConfig>` **`migrateWSMAttachments()`**

`modifyPolicySet`	`selectWSMPolicySet`	11*g* Release:
		`wls:/jrfServer_domain/serverConfig>` **`modifyPolicySet('myPolicySet')`**
		12*c* Release:
		`wls:/jrfServer_domain/serverConfig>` **`selectWSMPolicySet ('myPolicySet')`**

`resetWSMPolicyRepository`	`restWSMRepository`	11*g* Release:
		`wls:/jrfServer_domain/serverConfig>` **`resetWSMPolicyRepository()`**
		12*c* Release:
		`wls:/jrfServer_domain/serverConfig>` **`resetWSMRepository()`**

Table 7–1 (Cont.) Deprecated Commands for Oracle Infrastructure Web Services

Deprecated Command (11g)	Recommended Command (12*c*)	Updating Your Code

`setPolicySetConstraint`	`setWSMPolicySetConstraint`	11*g* Release:
		`wls:/jrfServer_domain/serverConfig>` **`setPolicySetConstraint ('HTTPHeader("VIRTUAL_HOST_TYPE","external")')`**
		12*c* Release:
		`wls:/jrfServer_domain/serverConfig>` **`setWSMPolicySetConstraint ('HTTPHeader("VIRTUAL_HOST_TYPE","external")')`**

`setPolicySetDescription`	`setWSMPolicySetDescription`	11*g* Release:
		`wls:/jrfServer_domain/serverConfig>` **`setPolicySetDescription ('Global policy set for web service endpoint.')`**
		12*c* Release:
		`wls:/jrfServer_domain/serverConfig>` **`setWSMPolicySetDescription ('Global policy set for web service endpoint.')`**

`setWebServicePolicyOverride`	`setWSMPolicyOverride`	11*g* Release:
		`wls:/jrfServer_domain/serverConfig>` **`setWebServicePolicyOverride ('/base_domain/server1/HelloWorld#1_0','j2wbasicPolicy', 'web', '{http://namespace/}WssUsernameService','JRFWssUsernamePort', 'oracle/wss_username_token_service_policy', 'reference.priority', '10')`**
		12*c* Release:
		`wls:/jrfServer_domain/serverConfig>` **`setWSMPolicyOverride ('oracle/wss_username_token_service_policy', 'reference.priority', '10')`**

Table 7–1 (Cont.) Deprecated Commands for Oracle Infrastructure Web Services

Deprecated Command (11g)	Recommended Command (12*c*)	Updating Your Code

`setPolicySetPolicyOverride`	`setWSMPolicyOverride`	11*g* Release (for both Repository and PolicySubject operation on policy set):
		`wls:/jrfServer_domain/serverConfig>` **`setPolicySetPolicyOverride ('oracle/wss_username_token_service_policy', 'reference.priority', '10')`**
		12*c* Release:
		`wls:/jrfServer_domain/serverConfig>` **`setWSMPolicyOverride ('oracle/wss_username_token_service_policy', 'reference.priority', '10')`**

`upgradeWSMPolicyRepository`	`upgradeWSMRepository`	11*g* Release:
		`wls:/jrfServer_domain/serverConfig>` **`upgradeWSMPolicyRepository()`**
		12*c* Release:
		`wls:/jrfServer_domain/serverConfig>` **`upgradeWSMRepository()`**

`validatePolicySet`	`validateWSMPolicySet`	11*g* Release:
		`wls:/jrfServer_domain/serverConfig>` **`validatePolicySet ('myPolicySet')`**
		12*c* Release:
		`wls:/jrfServer_domain/serverConfig>` **`validateWSMPolicySet ('myPolicySet')`**