ORACLE Help Center (//docs.oracle.com/en/) Sign In (http://www.oracle.com/webapps/redirect/signon?nexturl=https://docs.oracle.com/cd/E17904_01/doc.1111/e14770/ha.htm)

Home (../../../../) / Oracle Fusion Middleware Online Documentation Library, 11g Release 1 (11.1.1.4) (../../index.htm) / Release Notes (../../nav/relnotes.htm)

Fusion Middleware Release Notes

()

Categories

- Home (../../index.htm)
- Release Notes (../../nav/relnotes.htm)
- Get Started (../../nav/getstarted.htm)
- Install, patch, and upgrade (../../nav/ipu.htm)
- Develop applications (../../nav/develop.htm)
- Develop Web services (../../nav/webservices.htm)
- Administer the environment (../../nav/manage.htm)
- Secure the environment (../../nav/secure.htm)
- Use the Oracle WebLogic Scripting Tool (WLST) (../../nav/wlst.htm)
- Use third-party application servers (../../nav/thirdparty.htm)
- Access end-user documentation (../../nav/user.htm)
- Licensing (../../nav/cross.htm#licensing)
- References and APIs (../../nav/ref.htm)

() ()

Download

6 Oracle Fusion Middleware High Availability and Enterprise Deployment

This chapter describes issues associated with Oracle Fusion Middleware high availability and enterprise deployment. It includes the following topics:

- Section 6.1, "General Issues and Workarounds"
- Section 6.2, "Configuration Issues and Workarounds"
- Section 6.3, "Testing Abrupt Failures of WebLogic Server When Using File Stores on NFS"
- Section 6.4, "Documentation Errata"

> **Note:**
>
> This chapter contains issues you might encounter while configuring any of the any of the Oracle Fusion Middleware products for high availability or an enterprise deployment.
>
> Be sure to review the product-specific release note chapters elsewhere in this document for any additional issues specific to the products you are using.

() ()

6.1 General Issues and Workarounds

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

- Section 6.1.1, "Logout Does Not Function when Oracle Access Manager 11*g* is Integrated with Oracle Identity Federation 11*g*"
- Section 6.1.2, "Secure Resources in Application Tier"
- Section 6.1.3, "mod_wl Not Supported for OHS Routing to Managed Server Cluster"
- Section 6.1.4, "Only Documented Procedures Supported"
- Section 6.1.5, "SOA Composer Generates Error During Failover"
- Section 6.1.6, "Accessing Web Services Policies Page in Cold Failover Environment"
- Section 6.1.7, "Considerations for Oracle Identity Federation HA in SSL Mode"
- Section 6.1.8, "Online Help Context May be Lost When Failover Occurs in High Availability Environment"
- Section 6.1.9, "ASCRS Cannot be Used to Create a Database Resource for the Oracle Database Console Service on Windows"
- Section 6.1.10, "Changes to Rulesets May Not be Persisted During an Oracle RAC Instance Failover"
- Section 6.1.11, "Manual Retries May be Necessary When Redeploying Tasks During an Oracle RAC Failover"
- Section 6.1.12, "Timeout Settings for SOA Request-Response Operations are Not Propagated in a Node Failure"

- Section 6.1.13, "Scale Out and Scale Up Operations Fail"
- Section 6.1.14, "Harmless SQLIntegrityConstraintViolationException Can be Received in a SOA Cluster"
- Section 6.1.15, "WebLogic Cluster WS-AT Recovery Can Put a Server into a 'Warning' State"
- Section 6.1.16, "Very Intensive Uploads from I/PM to UCM May Require Use of IP-Based Filters in UCM Instead of Hostname-Based Filters"
- Section 6.1.17, "Worklist Application May Throw Exception if Action Dropdown Menu is Used During a Failover"
- Section 6.1.18, "ClassCastExceptions in a SOA Cluster for the SOA Worklist Application"
- Section 6.1.19, "Use srvctl in 11.2 Oracle RAC Databases to Set Up AQ Notification and Server-side TAF"
- Section 6.1.20, "Oracle I/PM Input Files May Not be Processed Correctly During an Oracle RAC Failover"
- Section 6.1.21, "Failover Is Not Seamless When Creating Reports in Oracle BI Publisher"
- Section 6.1.22, "Failed to Load Error Appears in Layout View When Oracle BI Publisher Managed Server is Failed Over"
- Section 6.1.23, "When Scheduling an Oracle BI Publisher Job, a Popup Window Appears After Managed Server Failover"
- Section 6.1.24, "Cannot Save Agent When Oracle Business Intelligence Managed Server Fails Over"
- Section 6.1.25, "Patch 10094106 Required for SSO Configuration in an Enterprise Deployment"
- Section 6.1.26, "Installing Additional Oracle Portal, Forms, Reports, and Discoverer Instances After Upgrading Oracle Single Sign-On 10*g* to Oracle Access Manager 11*g*"
- Section 6.1.26, "Installing Additional Oracle Portal, Forms, Reports, and Discoverer Instances After Upgrading Oracle Single Sign-On 10*g* to Oracle Access Manager 11*g*"

() ()

6.1.1 Logout Does Not Function when Oracle Access Manager 11*g* is Integrated with Oracle Identity Federation 11*g*

Errors occur during logout when Oracle Access Manager is integrated with Oracle Identity Federation. No workaround exists at this time. Please contact Oracle Support to obtain the fix for Bug #9969090 to resolve this issue.

() ()

6.1.2 Secure Resources in Application Tier

It is highly recommended that the application tier in the SOA Enterprise Deployment topology and the WebCenter Enterprise Deployment topology is protected against anonymous RMI connections. To prevent RMI access to the middle tier from outside the subset configured, follow the steps in "Configure connection filtering" in the Oracle WebLogic Server Administration Console Online Help. Execute all of the steps, except as noted in the following:

1. Do not execute the substep for configuring the default connection filter. Execute the substep for configuring a custom connection filter.
2. In the Connection Filter Rules field, add the rules that will allow all protocol access to servers from the middle tier subnet while allowing only http(s) access from outside the subnet, as shown in the following example:

```
nnn.nnn.0.0/nnn.nnn.0.0  * * allow
0.0.0.0/0 * * allow t3 t3s
```

() ()

6.1.3 mod_wl Not Supported for OHS Routing to Managed Server Cluster

Oracle Fusion Middleware supports only `mod_wls_ohs` and does not support `mod_wl` for Oracle HTTP Server routing to a cluster of managed servers.

() ()

6.1.4 Only Documented Procedures Supported

For Oracle Fusion Middleware high availability deployments, Oracle strongly recommends following only the configuration procedures documented in the *Oracle Fusion Middleware High Availability Guide* and the *Oracle Fusion Middleware Enterprise Deployment Guides*.

() ()

6.1.5 SOA Composer Generates Error During Failover

During failover, if you are in a SOA Composer dialog box and the connected server is down, you will receive an error, such as `Target Unreachable, 'messageData' returned null`.

To continue working in the SOA Composer, open a new browser window and navigate to the SOA Composer.

() ()

6.1.6 Accessing Web Services Policies Page in Cold Failover Environment

In a Cold Failover Cluster (CFC) environment, the following exception is displayed when Web Services policies page is accessed in Fusion Middleware Control:

```
Unable to connect to Oracle WSM Policy Manager.
Cannot locate policy manager query/update service. Policy manager service
look up did not find a valid service.
```

To avoid this, implement one the following options:

- Create virtual hostname aliased SSL certificate and add to the key store.
- Add "-Dweblogic.security.SSL.ignoreHostnameVerification=true" to the JAVA_OPTIONS parameter in the startWeblogic.sh or startWeblogic.cmd files

() ()

6.1.7 Considerations for Oracle Identity Federation HA in SSL Mode

In a high availability environment with two (or more) Oracle Identity Federation servers mirroring one another and a load balancer at the front-end, there are two ways to set up SSL:

- Configure SSL on the load balancer, so that the SSL connection is between the user and the load balancer. In that case, the keystore/certificate used by the load balancer has a CN referencing the address of the load balancer.

  The communication between the load balancer and the WLS/Oracle Identity Federation can be clear or SSL (and in the latter case, Oracle WebLogic Server can use any keystore/certificates, as long as these are trusted by the load balancer).

- SSL is configured on the Oracle Identity Federation servers, so that the SSL connection is between the user and the Oracle Identity Federation server. In this case, the CN of the keystore/certificate from the Oracle WebLogic Server/Oracle Identity Federation installation needs to reference the address of the load balancer, as the user will connect using the hostname of the load balancer, and the Certificate CN needs to match the load balancer's address.

  In short, the keystore/certificate of the SSL endpoint connected to the user (load balancer or Oracle WebLogic Server/Oracle Identity Federation) needs to have its CN set to the hostname of the load balancer, since it is the address that the user will use to connect to Oracle Identity Federation.

() ()

6.1.8 Online Help Context May be Lost When Failover Occurs in High Availability Environment

In a high availability environment, if you are using online help and a failover occurs on one of the machines in your environment, your context in online help may be lost when the application is failed over.

For example, the online help table of contents may not remember the topic that was selected prior to the failover, or the last online help search results may be lost.

No data is lost, and your next online help request after the failover will be handled properly.

() ()

6.1.9 ASCRS Cannot be Used to Create a Database Resource for the Oracle Database Console Service on Windows

In Patch Set 2 of the Oracle Fusion Middleware 11*g* Release 1 (11.1.1) release, a new feature was added to Application Server Cluster Ready Services (ASCRS) to enable users to create an ASCRS database resource for the Oracle Database Console service. Using ASCRS to create an ASCRS database resource is described in the "Creating an Oracle Database Resource" section of the "Using Cluster Ready Services" chapter in the *Oracle Fusion Middleware High Availability Guide*.

This feature works on UNIX, because the Oracle Database Console can be CFC enabled on UNIX.

However, on Windows, there is no CFC support for the Oracle Database Console service. Therefore, you cannot use

ASCRS to create a database resource for the Oracle Database Console service on Windows.

() ()

6.1.10 Changes to Rulesets May Not be Persisted During an Oracle RAC Instance Failover

When you update rulesets (used in Human Workflow or BPEL) through the Worklist configuration UI or the SOA Composer application during an Oracle RAC instance failover, the new rule metadata may not get persisted to the database. In this case, you will need to perform a manual retry. However, you can continue to use the older version of metadata without any errors.

() ()

6.1.11 Manual Retries May be Necessary When Redeploying Tasks During an Oracle RAC Failover

When redeploying tasks with large number of rules during an Oracle RAC instance failover, a manual retry may be needed by the end user occasionally.

() ()

6.1.12 Timeout Settings for SOA Request-Response Operations are Not Propagated in a Node Failure

In an active-active Oracle SOA cluster, when a node failure occurs, the timeout settings for request-response operations in receive activities are not propagated from one node to the other node or nodes. If a failure occurs in the server that scheduled these activities, they must be rescheduled with the scheduler upon server restart.

() ()

6.1.13 Scale Out and Scale Up Operations Fail

The scale out and scale up operations performed on your environment after re-associating the local file based WLS LDAP store with an external LDAP store will fail. To avoid this failure, follow the steps below before performing a scale up or scale out operation.

1. Edit the **`setDomainEnv.sh`** file located under the *DOMAIN_HOME* **`/bin`** directory and add the "-Dcommon.components.home=${*COMMON_COMPONENTS_HOME*}" and "-Djrf.version=11.1.1" variables to the the file.

2. These variables should be added to the "EXTRA_JAVA_PROPERTIES". For example:

```
EXTRA_JAVA_PROPERTIES="-Ddomain.home=${DOMAIN_HOME}
-Dcommon.components.home=${COMMON_COMPONENTS_HOME} -Djrf.version=11.1.1
       .
       .
       .
```

3. Save the file and proceed with the scale out or scale up operation.

() ()

6.1.14 Harmless SQLIntegrityConstraintViolationException Can be Received in a SOA Cluster

The following SQLIntegrityConstraintViolationException can be received in a SOA cluster:

```
[TopLink Warning]: 2010.04.11 14:26:53.941--UnitOfWork(275924841)--Exception
[TOPLINK-4002] (Oracle TopLink - 11g Release 1 (11.1.1.3.0):
Internal Exception: java.sql.SQLIntegrityConstraintViolationException:
ORA-00001: unique constraint (JYIPS2RC4B49_SOAINFRA.SYS_C0035333) violated
   .
   .
   .
```

This is not a bug. In a cluster environment, when the messages for the same group arrive on both the nodes, one node is bound to experience this exception for the first message. The application is aware of this exception and handles it properly. It does not break any functionality.

This exception can also come on a single node after you restart the server and send the message for the existing group. Again, this exception will be experienced on the very first message.

In summary, this exception is within the application design and does not impact any functionality. It is for this reason that you do not see this exception logged as severe in the soa-diagnostic logs.

Toplink does, however, log it in its server logs.

() ()

6.1.15 WebLogic Cluster WS-AT Recovery Can Put a Server into a 'Warning' State

In certain WebLogic cluster process crash scenarios, WS-AT recovery will result in stuck threads that put the server into a "warning" state. WS-AT data recovery is successful in these cases despite the fact that the logs display "failed state" messages, due to the fact that commit acks are not being processed correctly for this scenario (this issue does not occur when the scenario involves the rollback of the transaction). While the server may continue to function in this "warning" state, the threads will continue to be stuck until the transaction abandonment timeout (which defaults to 24 hours) is reached. The workaround is to restart the server, which removes the stuck threads and "warning" state. A patch for this issue can be obtained from Oracle Support.

() ()

6.1.16 Very Intensive Uploads from I/PM to UCM May Require Use of IP-Based Filters in UCM Instead of Hostname-Based Filters

The "Adding the I/PM Server Listen Addresses to the List of Allowed Hosts in UCM" section in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Enterprise Content Management Suite* (../../doc.1111/e15483/extend_ipm.htm#CMEDG658) and the "Adding the I/PM Server Listen Addresses to the List of Allowed Hosts in UCM" section in the *Oracle Fusion Middleware High Availability Guide* (../../core.1111/e10106/ecm.htm#ASHIA5323) describe how to add hostname-based filters for Oracle I/PM managed server listen addresses to the list of allowed hosts in Oracle UCM.

When using hostname-based filters in Oracle UCM (`config.cfg` file) a high latency/performance impact may be observed in the system for very intensive uploads of documents from Oracle I/PM to Oracle UCM. This is caused by the reverse DNS lookup that is required in Oracle UCM to allow the connections from Oracle I/PM servers. Using hostname-based filters is recommended in preparation for configuring the system for Disaster Protection and to restore to a different host (since the configuration used is IP-agnostic when using hostname-based filters). However if the performance of the uploads needs to be improved, users can use instead IP-based filters. To do this:

1. Edit the file `/u01/app/oracle/admin/`*domainName*`/ucm_cluster/config/config.cfg` and remove or comment out:

```
SocketHostNameSecurityFilter=localhost|localhost.mydomain.com|ecmhost1vhn1|ecmhost2vhn1

AlwaysReverseLookupForHost=Yes
```

2. Add the IP addresses (listen address) of the WLS_IPM1 and WLS_IPM2 managed servers (ECMHOST1VHN1 and ECMHOST2VHN1, respectively) to the SocketHostAddressSecurityFilter parameter list as follows:

```
SocketHostAddressSecurityFilter=127.0.0.1|0:0:0:0:0:0:0:1|X.X.X.X|Y.Y.Y.
```

   where X.X.X.X and Y.Y.Y.Y are the listen addresses of WLS_IPM1 and WLS_IPM2 respectively. Notice that 127.0.0.1 also needs to be added as shown above.

3. Restart the UCM servers.

() ()

6.1.17 Worklist Application May Throw Exception if Action Dropdown Menu is Used During a Failover 11.10

If you use the Oracle Business Process Management Suite Worklist application **Actions** dropdown menu to take action on a task while a failover is in progress, an exception similar to the following may be thrown:

```
<oracle.adf.view.rich.component.fragment.UIXInclude> <ADF_FACES-10020> <Tear
down of include component context failed due to an unhandled e
xception.
java.util.NoSuchElementException
        at java.util.ArrayDeque.removeFirst(ArrayDeque.java:251)
        at java.util.ArrayDeque.pop(ArrayDeque.java:480)
        at
oracle.adfinternal.view.faces.context.ApplicationContextManagerImpl.popContext
Change(ApplicationContextManagerImpl.java:66)
  .
  .
  .
```

In this case, the approval or rejection of the task does not go through.

To work around this problem, use either of these approaches:

- Instead of using the **Actions** dropdown menu to take action on the task, use the TaskForm to take action.

- Do a refresh after the error message. Then take the action again using the **Actions** dropdown menu.

() ()

6.1.18 ClassCastExceptions in a SOA Cluster for the SOA Worklist Application

ClassCastExceptions may arise in a SOA cluster for the Oracle SOA Worklist application (`java.lang.ClassCastException: oracle.adf.model.dcframe.DataControlFrameImpl` is reported in the logs). As a result, the Worklist application state may not be replicated to other managed servers in the cluster. The Worklist application and the corresponding user sessions will be usable after the exception is thrown, but any failovers to other servers in the cluster will not succeed.

There is no workaround to this problem.

To solve this problem, download the patch for bug 9561444, which solves the problem. Follow these steps:

1. To obtain the patch, log into My Oracle Support (formerly Oracle*MetaLink*) at the following URL:

   `http://support.oracle.com` (http://support.oracle.com)

2. Click the **Patches & Updates** tab.

3. In the **Patch Search** section, enter 9561444 in the **Patch ID or number is** field, and enter your platform in the field after the **and Platform is** field.

4. Click **Search**.

5. On the Patch Search page, click the patch number in the **Patch ID** column. This causes the page content to change to display detailed information about the patch.

6. Click **Download** to download the patch.

() ()

6.1.19 Use srvctl in 11.2 Oracle RAC Databases to Set Up AQ Notification and Server-side TAF

Because of a known issue in 11.2 Oracle RAC databases, it is required to use `srvctl` to set up AQ notification and server-side TAF. Using DBMS_SQL packages will not work as expected.

Here is an example use of `srvctl`:

```
srvctl modify service -d orcl -s orclSVC -e SELECT -m BASIC -w 5 -z 5 -q TRUE
```

In the example:

orcl - Database Name

orclSVC - Service Name used by middleware component

SELECT - Failover type

BASIC - Failover method

5 - Failover delay

5 - Failover retry

TRUE - AQ HA notifications set to TRUE

Please refer to the Oracle 11.2 Oracle database documentation for detailed information about this command usage.

() ()

6.1.20 Oracle I/PM Input Files May Not be Processed Correctly During an Oracle RAC Failover

With Oracle I/PM and Oracle UCM file processing, some files may not get loaded in UCM properly during an Oracle RAC instance failover.

The incoming files to be processed by Oracle I/PM are put into an input folder. Oracle I/PM processes the files in the input folder and then puts them into Oracle UCM, which is backed by an Oracle RAC database. Sometimes when an Oracle RAC instance failure occurs, the retry may not happen correctly, and the incoming files do not get processed. These unprocessed files show up in an error folder. These unprocessed files can manually be put back into the input folder and processed.

() ()

6.1.21 Failover Is Not Seamless When Creating Reports in Oracle BI Publisher

If you create a report in Oracle BI Publisher, and a Managed Server is failed over before the report is saved, the failover might not be seamless. For example, when you attempt to save the report, the system might not be responsive.

If this occurs, click one of the header links, such as **Home** or **Catalog**, to be redirected to the Oracle BI Publisher login page. Then, log in and create and save the report again.

() ()

6.1.22 Failed to Load Error Appears in Layout View When Oracle BI Publisher Managed Server is Failed Over

In the Oracle BI Publisher layout editor, when a Managed Server is failed over, opening or creating a Web-based layout can cause the following error to appear:

```
Failed to load: object_name
Please contact the system administrator.
```

To work around this issue, close the message and click one of the header links, such as **Home** or **Catalog**, to be redirected to the login page.

() ()

6.1.23 When Scheduling an Oracle BI Publisher Job, a Popup Window Appears After Managed Server Failover

When scheduling a job in Oracle BI Publisher, after a Managed Server fails over, a large popup window appears when you click **Submit** that shows the HTML source for the login page.

To work around this issue, close the message window and click one of the header links, such as **Home** or **Catalog**, to be redirected to the login page. You will need to re-create the report job again.

() ()

6.1.24 Cannot Save Agent When Oracle Business Intelligence Managed Server Fails Over

If you create an agent in the Oracle Business Intelligence Web interface, and a Managed Server fails over before you save the agent, an error occurs when you try to save the agent.

To work around this issue, log out, then log back in to Oracle Business Intelligence and create the agent again.

() ()

6.1.25 Patch 10094106 Required for SSO Configuration in an Enterprise Deployment

Before you configure SSO using Oracle Access Manager 11g, as described in the chapter "Configuring Single Sign-on for Administration Consoles" in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*, you must apply Patch 10094106.

If you do not apply this patch, you might get a "404 Not Found" error when you attempt to access a protected application deployed on Oracle WebLogic Server with valid credentials.

() ()

6.1.26 Installing Additional Oracle Portal, Forms, Reports, and Discoverer Instances After Upgrading Oracle Single Sign-On 10*g* to Oracle Access Manager 11*g*

This issue occurs with Oracle Portal, Forms, Reports, and Discoverer 11g environments that have been upgraded from using Oracle Single-Sign On 10*g* to Oracle Access Manager 11*g* for authentication.

When performing subsequent Oracle Portal, Forms, Reports, and Discoverer 11*g* installations against the same environment where the initial Oracle Portal, Forms, Reports, and Discoverer 10*g* installation was upgraded to Oracle Access Manager, there are some requirements that must be met.

- For each subsequent Oracle Portal, Forms, Reports, and Discoverer 11*g* installation, you must maintain the original Oracle Single Sign-On 10*g* instance and keep it actively running--in addition to new Oracle Access Manager 11*g* instance--while the additional Oracle Portal, Forms, Reports, and Discoverer 11*g* installations are performed.

  This is necessary because Oracle Portal, Forms, Reports, and Discoverer 11*g* cannot be installed directly against Oracle Access Manager 11*g*.

- After the subsequent classic installs are completed, the Oracle Single Sign-On 10*g* to Oracle Access Manager 11*g* upgrade procedure must be performed again. For more information, see "Upgrading Your Oracle Single Sign-On Environment (../../upgrade.1111/e10129/upgrade_oam.htm#FUPIM674)" in the *Oracle Fusion Middleware Upgrade Guide for Oracle Identity Management*.

  This procedure upgrades the new Oracle Portal, Forms, Reports, and Discoverer 11*g* instance to Oracle Access Manager 11*g*.

Note that these considerations apply only in an environment with Multiple Oracle Portal, Forms, Reports, and Discoverer 11*g* middle tiers that are installed or added to a your environment after the initial upgrade from Oracle Single Sign-On 10*g* to Oracle Access Manager 11*g*.

()
()

6.1.27 Using the Enterprise Deployment Guide for Oracle Identity Management with 11.1.1.4.0

Chapter 4, "Installing the Software (../../core.1111/e12035/install.htm#IMEDG734)," in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management* describes how to install the Oracle Fusion Middleware software and apply some specific patches to your 11*g* Release 1 (11.1.1.3.0) Oracle Identity Management environment.

If you are planning to implement an Oracle Identity Management enterprise deployment using Oracle Fusion Middleware 11*g* Release (11.1.1.4.0), then note the following as you review the instructions in Chapter 4:

- Before you review Section 4.5, "Installing Oracle Fusion Middleware," note that the process to install Oracle Identity Management 11*g* Release 1 (11.1.1.4.0) is as follows:

  1. Download and install Oracle Identity Management 11*g* Release 1 (11.1.1.2.0), which is a full installer you can use to install a new Oracle Identity Management 11.1.1.2.0 Oracle home inside the Middleware home you created when you installed Oracle WebLogic Server.
  2. Download and install the Oracle Identity Management 11*g* Release 1 (11.1.1.4.0) patch set, which is a patch set installer with updates your 11.1.1.2.0 Oracle home to 11.1.1.4.0.

- The patches listed in Section 4.7, "Patching the Software," are not necessary if you install the 11.1.1.4.0 patch set, except in one scenario. Specifically, if your deployment uses Oracle Identity Manager, the following two procedures are necessary for an 11.1.1.4.0 enterprise deployment. For all other deployment scenarios, these are not required:

  - Section 4.7.7, "Creating the wlfullclient.jar File"
  - Section 4.7.8, "Provisioning the OIM Login Modules Under the WebLogic Server Library Directory"

() ()

6.2 Configuration Issues and Workarounds

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

- Section 6.2.1, "jca.retry.count Doubled in a Clustered Environment"
- Section 6.2.2, "Cluster Time Zones Must Be the Same"
- Section 6.2.3, "Fusion Middleware Control May Display Incorrect Status"
- Section 6.2.4, "Accumulated BPEL Instances Cause Performance Decrease"
- Section 6.2.5, "Extra Message Enqueue when One a Cluster Server is Brought Down and Back Up"
- Section 6.2.6, "Duplicate Unrecoverable Human Workflow Instance Created with Oracle RAC Failover"
- Section 6.2.7, "Configuration Files Missing after Planned Administration Server Node Shutdown or Reboot"
- Section 6.2.8, "No High Availability Support for SOA B2B TCP/IP"
- Section 6.2.9, "WebLogic Administration Server on Machines with Multiple Network Cards"
- Section 6.2.10, "Additional Parameters for SOA and Oracle RAC Data Sources"
- Section 6.2.11, "Message Sequencing and MLLP Not Supported in Oracle B2B HA Environments"

- Section 6.2.12, "Credentials not Propagated for Transport Protocols in B2B"
- Section 6.2.13, "Access Control Exception After Expanding Cluster Against an Extended Domain"
- Section 6.2.14, "Create a Protected Resource for Oracle Identity Navigator"
- Section 6.2.15, "Use Fully-Qualified Hostnames when Configuring Front-end Hosts in High Availability Configurations"
- Section 6.2.16, "Managed Server goes into Suspended Status After RAC Failover"
- Section 6.1.8, "Online Help Context May be Lost When Failover Occurs in High Availability Environment"

() ()

6.2.1 jca.retry.count Doubled in a Clustered Environment

In a clustered environment, each node maintains its own in-memory Hasmap for inbound retry. The `jca.retry.count` property is specified as **3** for the inbound retry feature. However, each node tries three times. As a result, the total retry count becomes 6 if the clustered environment has two nodes.

() ()

6.2.2 Cluster Time Zones Must Be the Same

All the machines in a cluster must be in the same time zone. WAN clusters are not supported by Oracle Fusion Middleware high availability. Even machines in the same time zone may have issues when started by command line. Oracle recommends using Node Manager to start the servers.

() ()

6.2.3 Fusion Middleware Control May Display Incorrect Status

In some instances, Oracle WebLogic Fusion Middleware Control may display the incorrect status of a component immediately after the component has been restarted or failed over.

() ()

6.2.4 Accumulated BPEL Instances Cause Performance Decrease

In a scaled out clustered environment, if a large number of BPEL instances are accumulated in the database, it causes the database's performance to decrease, and the following error is generated: MANY THREADS STUCK FOR 600+ SECONDS.

To avoid this error, remove old BPEL instances from the database.

() ()

6.2.5 Extra Message Enqueue when One a Cluster Server is Brought Down and Back Up

In a non-XA environment, MQSeries Adapters do not guarantee the only once delivery of the messages from inbound adapters to the endpoint in case of local transaction. In this scenario, if an inbound message is published to the endpoint, and before committing the transaction, the SOA server is brought down, inbound message are rolled back and the same message is again dequeued and published to the endpoint. This creates an extra message in outbound queue.

In an XA environment, MQ Messages are actually not lost but held by Queue Manager due to an inconsistent state. To retrieve the held messages, restart the Queue Manager.

() ()

6.2.6 Duplicate Unrecoverable Human Workflow Instance Created with Oracle RAC Failover

As soon as Oracle Human Workflow commits its transaction, the control passes back to BPEL, which almost instantaneously commits its transaction. Between this window, if the Oracle RAC instance goes down, on failover, the message is retried and can cause duplicate tasks. The duplicate task can show up in two ways - either a duplicate task appears in worklistapp, or an unrecoverable BPEL instance is created. This BPEL instance appears in BPEL Recovery. It is not possible to recover this BPEL instance as **consumer**, because this task has already completed.

() ()

6.2.7 Configuration Files Missing after Planned Administration Server Node Shutdown or Reboot

The following information refers to Chapter 10, "Managing the Topology," of the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle SOA Suite*.

When performing a planned stop of the Administration Server's node (rebooting or shutting down the Admin Server's machine), it may occur that the OS NFS service is disabled before the Administration Server itself is stopped. This (depending on the configuration of services at the OS level) can cause the detection of missing files in the Administration Server's domain directory and trigger their deletion in the domain directories in other nodes. This can result in the framework deleting some of the files under `domain_dir/fmwconfig/`. This behavior is typically not observed for unplanned downtimes, such as machine panic, power loss, or machine crash. To avoid this behavior, shutdown the Administration Server before performing reboots or, alternatively, use the appropriate OS configuration to set the order of services in such a way that NFS service is disabled with later precedence than the Administration Server's process. See your OS administration documentation for the corresponding required configuration for the services' order.

() ()

6.2.8 No High Availability Support for SOA B2B TCP/IP

High availability failover support is not available for SOA B2B TCP/IP protocol. This effects primarily deployments using HL7 over MLLP. For inbound communication in a clustered environment, all B2B servers are active and the address exposed for inbound traffic is a load balancer virtual server. Also, in an outage scenario where an active managed server is no longer available, the persistent TCP/IP connection is lost and the client is expected to reestablish the connection.

() ()

6.2.9 WebLogic Administration Server on Machines with Multiple Network Cards

When installing Oracle WebLogic Server on a server with multiple network cards, always specify a Listen Address for the Administration Server. The address used should be the DNS Name/IP Address of the network card you wish to use for Administration Server communication.

To set the Listen Address:

1. In the Oracle WebLogic Server Administration Console, select **Environment**, and then **Servers** from the domain structure menu.
2. Click the Administration Server.
3. Click **Lock and Edit** from the Change Center to allow editing.
4. Enter a Listen Address.
5. Click **Save**.
6. Click **Activate Changes** in the Change Center.

() ()

6.2.10 Additional Parameters for SOA and Oracle RAC Data Sources

In some deployments of SOA with Oracle RAC, you may need to set additional parameters in addition to the out of the box configuration of the individual data sources in an Oracle RAC configuration. The additional parameters are:

1. Add property `oracle.jdbc.ReadTimeout=300000` (300000 milliseconds) for each data source.

   The actual value of the `ReadTimeout` parameter may differ based on additional considerations.

2. If the network is not reliable, then it is difficult for a client to detect the frequent disconnections when the server is abruptly disconnected. By default, a client running on Linux takes 7200 seconds (2 hours) to sense the abrupt disconnections. This value is equal to the value of the `tcp_keepalive_time` property. To configure the application to detect the disconnections faster, set the value of the `tcp_keepalive_time`, `tcp_keepalive_interval`, and `tcp_keepalive_probes` properties to a lower value at the operating system level.

   > **Note:**
   > Setting a low value for the `tcp_keepalive_interval` property leads to frequent probe packets on the network, which can make the system slower. Therefore, the value of this property should be set appropriately based on system requirements.

For example, set `tcp_keepalive_time=600` at the system running the WebLogic Server managed server.

Also, you must specify the `ENABLE=BROKEN` parameter in the `DESCRIPTION` clause in the connection descriptor. For example:

```
dbc:oracle:thin:@(DESCRIPTION=(enable=broken)(ADDRESS_LIST=(ADDRESS=(PRO
TOCOL=TCP)(HOST=node1-vip.mycompany.com)(PORT=1521)))(CONNECT_DATA=(SERVICE_
NAME=orcl.us.oracle.com)(INSTANCE_NAME=orcl1)))
```

As a result, the data source configuration appears as follows:

```
<url>jdbc:oracle:thin:@(DESCRIPTION=(enable=broken)(ADDRESS_LIST=(ADDRESS=(PRO
TOCOL=TCP)(HOST=node1-vip.us.oracle.com)(PORT=1521)))(CONNECT_DATA=(SERVICE_NAME=orcl.us.oracle.
    <driver-name>oracle.jdbc.xa.client.OracleXADataSource</driver-name>
    <properties>
      <property>
        <name>oracle.jdbc.ReadTimeout</name>
        <value>300000</value>
      </property>
      <property>
        <name>user</name>
        <value>jmsuser</value>
      </property>
      <property>
        <name>oracle.net.CONNECT_TIMEOUT</name>
        <value>10000</value>
      </property>
    </properties>
```

() ()

6.2.11 Message Sequencing and MLLP Not Supported in Oracle B2B HA Environments

Message sequencing and MLLP are not supported in Oracle B2B high availability (HA) environments.

() ()

6.2.12 Credentials not Propagated for Transport Protocols in B2B

The Oracle FMW credential store maintains usernames and passwords that you define for Transport protocols. If you use the default file store for these credentials, changes you make to usernames and passwords do not propagate across nodes. You must use a central LDAP for these credentials to be synchronized across nodes in a cluster, as described in, and required by, the Oracle Fusion Middleware High Availability Guide and Enterprise Deployment Guides.

() ()

6.2.13 Access Control Exception After Expanding Cluster Against an Extended Domain

The Oracle Identity Federation server has been observed to fail due to access control exceptions under the following circumstances:

1. You create a domain with no Identity Management components on **`host1`**.
2. On **`host2`**, you extend that domain in clustered mode, select all Identity Management components, and select **`Create Schema`**.
3. On **`host1`**, you expand the cluster and select all components.

Due to a bug, the file ***`DOMAIN_HOME`*** **`/config/fmwconfig system-jazn-data.xml`** on **`host1`** is overwritten so that the **`<grant>`** element is removed, which causes the access control exceptions when the Oracle Identity Federation server is started.

To restore the **`<grant>`** element, you use the WLST **`grantPermission`** command.

On Linux, enter the following three commands at the bash prompt. Type each command on one line.

When typing the commands, replace ***`ORACLE_COMMON_HOME`*** with the path to the Oracle Common Home folder, located in the Middleware Home. When prompted for information to connect to WebLogic, enter the WLS Administrator Credentials and the location of the WebLogic Administration Server.

```
ORACLE_COMMON_HOME/common/bin/wlst.sh
ORACLE_COMMON_HOME/modules/oracle.jps_11.1.1/common/wlstscripts/grantPermissi
on.py -codeBaseURL
file:\${domain.home}/servers/\${weblogic.Name}/tmp/_WL_user/OIF_11.1.1.2.0/-
-permClass oracle.security.jps.service.credstore.CredentialAccessPermission
-permTarget context=SYSTEM,mapName=OIF,keyName=* -permActions read

ORACLE_COMMON_HOME/common/bin/wlst.sh
ORACLE_COMMON_HOME/modules/oracle.jps_11.1.1/common/wlstscripts/grantPermissi
on.py -codeBaseURL
file:\${domain.home}/servers/\${weblogic.Name}/tmp/_WL_user/OIF_11.1.1.2.0/-
-permClass oracle.security.jps.service.credstore.CredentialAccessPermission
-permTarget credstoressp.credstore -permActions read

ORACLE_COMMON_HOME/common/bin/wlst.sh
ORACLE_COMMON_HOME/modules/oracle.jps_11.1.1/common/wlstscripts/grantPermissi
on.py -codeBaseURL
file:\${domain.home}/servers/\${weblogic.Name}/tmp/_WL_user/OIF_11.1.1.2.0/-
-permClass oracle.security.jps.service.credstore.CredentialAccessPermission
-permTarget credstoressp.credstore.OIF.* -permActions read
```

On Windows, enter the following three commands at the command prompt. Type each command on one line.

When typing the commands, replace ***`ORACLE_COMMON_HOME`*** with the path to the Oracle Common Home folder, located in the Middleware Home. When prompted for information to connect to WebLogic, enter the WLS Administrator Credentials and the location of the WebLogic Administration Server.

```
ORACLE_COMMON_HOME\common\bin\wlst.cmd
ORACLE_COMMON_HOME\modules\oracle.jps_11.1.1\common\wlstscripts\grantPermiss
ion.py -codeBaseURL
file:${domain.home}/servers/\${weblogic.Name}/tmp/_WL_user/OIF_11.1.1.2.0/-
-permClass oracle.security.jps.service.credstore.CredentialAccessPermission
-permTarget context=SYSTEM,mapName=OIF,keyName=* -permActions read

ORACLE_COMMON_HOME\common\bin\wlst.cmd
ORACLE_COMMON_HOME\modules\oracle.jps_11.1.1\common\wlstscripts\grantPermiss
ion.py -codeBaseURL
file:${domain.home}/servers/${weblogic.Name}/tmp/_WL_user/OIF_11.1.1.2.0/-
-permClass oracle.security.jps.service.credstore.CredentialAccessPermission
-permTarget credstoressp.credstore -permActions read

ORACLE_COMMON_HOME\common\bin\wlst.cmd
ORACLE_COMMON_HOME\modules\oracle.jps_11.1.1\common\wlstscripts\grantPermiss
ion.py -codeBaseURL
file:${domain.home}/servers/${weblogic.Name}/tmp/_WL_user/OIF_11.1.1.2.0/-
-permClass oracle.security.jps.service.credstore.CredentialAccessPermission
-permTarget credstoressp.credstore.OIF.* -permActions read
```

() ()

6.2.14 Create a Protected Resource for Oracle Identity Navigator

To create a protected resource for Oracle Identity Navigator, log in to the Oracle Access Manager console at **`http://admin.mycompany.com/oamconsole`** using the **`oamadmin`** account. Then proceed as follows:

1. From the Navigation window expand: **Application Domains** > **IDMDomainAgent**.

2. Click **Resources**.

3. Click **Create** on the tool bar below the **Browse** tab).

   Enter the following information:

   - **Type**: **`http`**
   - **Host Identifier**: **`IDMDomain`**
   - **Resource URL**: **`/oinav`**

4. Click **Apply**.

5. From the Navigation window expand: **Application Domains** > **IDMDomainAgent** >**Authentication Policies**.

6. Click **Protected HigherLevel Policy**.

7. Click **Edit** on the tool bar below the **Browse** tab.

8. In the **Resources** box, click **+**.

9. From the list, select the resource **/oinav**.

10. Click **Apply**.

11. From the Navigation window expand: **Application Domains** > **IDMDomainAgent** >**Authorization Policies**.

12. Click **Protected Resource Policy**.

13. Click **Edit** on the tool bar below the **Browse** tab.

14. In the Resources box, click **+**.

15. From the list, select the resource **/oinav**

16. Click **Apply**.

() ()

6.2.15 Use Fully-Qualified Hostnames when Configuring Front-end Hosts in High Availability Configurations

Oracle recommends using the full name of the host, including the domain name, when configuring front-end hosts in Oracle Fusion Middleware high availability configurations. Use the host's full name instead of using only the host name.

For example, if myhost is the name of a frontend host in a high availability configuration, set the frontend host URL to the fully-qualified hostname, such as myhost.mycompany.com as DNS or local host name resolution files (for example, /etc/hosts) define.

() ()

6.2.16 Managed Server goes into Suspended Status After RAC Failover

The Managed Server wls_ods(x) can enter a suspended status in the following situations:

- A database connection in the data source is wrong or not complete.

- The host is not a fully-qualified host for the database.

To correct the status of the Managed Server wls_ods(x):

1. Under the data source, verify that the database connection is correct and complete with the domain.

2. Under the data source, verify that the host name for the database is a fully- qualified hostname with the domain.

3. Verify the connection by selecting the Test button.

()
()

6.2.17 Primary/Secondary Configuration Section of the Availability Tab is Not Visible

During the system component scale out process, the Primary/Secondary Configuration section in the Availability tab of the Capacity Management page in Fusion Middleware Control may not be visible in the browser. This issue occurs when you perform the scale out process using Microsoft Internet Explorer version 7.0.5730.11.

To avoid this issue, do not use the browser Microsoft Internet Explorer version 7.0.5730.11 to scale out; use another browser such as Google Chrome.

() ()

6.3 Testing Abrupt Failures of WebLogic Server When Using File Stores on NFS

Oracle strongly recommends verifying the behavior of a server restart after abrupt machine failures when the JMS messages and transaction logs are stored on an NFS mounted directory. Depending on the NFS implementation, different issues can arise post failover/restart. The behavior can be verified by abruptly shutting down the node hosting the Web Logic servers while these are running. If the server is configured for server migration, it should be started automatically in the failover node after the corresponding failover period. If not, a manual restart of the WebLogic Server on the same host (after the node has completely rebooted) can be performed. Specifically, if Oracle WebLogic Server does not restart after abrupt machine failure when JMS messages and transaction logs are stored on NFS mounted directory, the following errors may appear in the server log files:

```
<MMM dd, yyyy hh:mm:ss a z> <Error> <Store> <BEA-280061> <The persistent
store "_WLS_server_soa1" could not be deployed:
weblogic.store.PersistentStoreException: java.io.IOException:
[Store:280021]There was an error while opening the file store file
"_WLS_SERVER_SOA1000000.DAT"
weblogic.store.PersistentStoreException: java.io.IOException:
[Store:280021]There was an error while opening the file store file
"_WLS_SERVER_SOA1000000.DAT"
        at weblogic.store.io.file.Heap.open(Heap.java:168)
        at weblogic.store.io.file.FileStoreIO.open(FileStoreIO.java:88)
...
java.io.IOException: Error from fcntl() for file locking, Resource
temporarily unavailable, errno=11
```

This error is due to the NFS system not releasing the lock on the stores. WebLogic Server maintains locks on files used for storing JMS data and transaction logs to protect from potential data corruption if two instances of the same WebLogic Server are accidentally started. The NFS storage device does not become aware of machine failure in a timely manner; therefore, the locks are not released by the storage device. As a result, after abrupt machine failure, followed by a restart, any subsequent attempt by WebLogic Server to acquire locks on the previously locked files may fail. Refer to your storage vendor documentation for additional information on the locking of files stored in NFS mounted directories on the storage device. If it is not reasonably possible to tune locking behavior in your NFS environment, use one of the following two solutions to unlock the logs and data files.

Use one of the following two solutions to unlock the logs and data files.

() Solution 1

Manually unlock the logs and JMS data files and start the servers by creating a copy of the locked persistence store file and using the copy for subsequent operations. To create a copy of the locked persistence store file, rename the file, and then copy it back to its original name. The following sample steps assume that transaction logs are stored in the **`/shared/tlogs`** directory and JMS data is stored in the **`/shared/jms`** directory.

```
cd /shared/tlogs
mv _WLS_SOA_SERVER1000000.DAT _WLS_SOA_SERVER1000000.DAT.old
cp _WLS_SOA_SERVER1000000.DAT.old _WLS_SOA_SERVER1000000.DAT
cd /shared/jms
mv SOAJMSFILESTORE_AUTO_1000000.DAT SOAJMSFILESTORE_AUTO_1000000.DAT.old
cp SOAJMSFILESTORE_AUTO_1000000.DAT.old SOAJMSFILESTORE_AUTO_1000000.DAT
mv UMSJMSFILESTORE_AUTO_1000000.DAT UMSJMSFILESTORE_AUTO_1000000.DAT.old
cp UMSJMSFILESTORE_AUTO_1000000.DAT.old UMSJMSFILESTORE_AUTO_1000000.DAT
```

With this solution, the WebLogic file locking mechanism continues to provide protection from any accidental data corruption if multiple instances of the same servers were accidently started. However, the servers must be restarted manually after abrupt machine failures. File stores will create multiple consecutively numbered .DAT files when they are used to store large amounts of data. All files may need to be copied and renamed when this occurs.

() Solution 2

You can also use the WebLogic Server Administration Console to disable WebLogic file locking mechanisms for the default file store, a custom file store, a JMS paging file store, and a Diagnostics file store, as described in the following sections.

> **WARNING:**
>
> With this solution, since the WebLogic locking is disabled, automated server restarts and failovers should succeed. Be very cautious, however, when using this option. The WebLogic file locking feature is designed to help prevent severe file corruptions that can occur in undesired concurrency scenarios. If the server using the file store is configured for server migration, always configure the database based leasing option. This enforces additional locking mechanisms using database tables, and prevents automated restart of more than one instance of the same WebLogic Server. Additional procedural precautions must be implemented to avoid any human error and to ensure that one and only one instance of a server is manually started at any give point in time. Similarly, extra precautions must be taken to ensure that no two domains have a store with the same name that references the same directory.

() Disabling File Locking for the Default File Store

Follow these steps to disable file locking for the default file store using the WebLogic Server Administration Console:

1. If necessary, click **Lock & Edit** in the Change Center (upper left corner) of the Administration Console to get an Edit lock for the domain.

2. In the **Domain Structure** tree, expand the **Environment** node and select **Servers**.
3. In the **Summary of Servers** list, select the server you want to modify.
4. Select the **Configuration > Services** tab.
5. Scroll down to the **Default Store** section and click **Advanced**.
6. Scroll down and deselect the **Enable File Locking** check box.
7. Click **Save** to save the changes. If necessary, click **Activate Changes** in the Change Center.
8. **Restart** the server you modified for the changes to take effect.

The resulting `config.xml` entry will look like the following:

```
<server>
  <name>examplesServer</name>
  ...
  <default-file-store>
    <synchronous-write-policy>Direct-Write</synchronous-write-policy>
    <io-buffer-size>-1</io-buffer-size>
    <max-file-size>1342177280</max-file-size>
    <block-size>-1</block-size>
    <initial-size>0</initial-size>
    <file-locking-enabled>false</file-locking-enabled>
  </default-file-store>
</server>
```

() Disabling File Locking for a Custom File Store

Follow these steps to disable file locking for a custom file store using the WebLogic Server Administration Console:

1. If necessary, click **Lock & Edit** in the Change Center (upper left corner) of the Administration Console to get an Edit lock for the domain.
2. In the **Domain Structure** tree, expand the **Services** node and select **Persistent Stores**.
3. In the **Summary of Persistent Stores** list, select the custom file store you want to modify.
4. On the **Configuration** tab for the custom file store, click **Advanced** to display advanced store settings.
5. Scroll down to the bottom of the page and deselect the **Enable File Locking** check box.
6. Click **Save** to save the changes. If necessary, click **Activate Changes** in the Change Center.
7. If the custom file store was in use, you must restart the server for the changes to take effect.

The resulting `config.xml` entry will look like the following:

```
<file-store>
  <name>CustomFileStore-0</name>
  <directory>C:\custom-file-store</directory>
  <synchronous-write-policy>Direct-Write</synchronous-write-policy>
  <io-buffer-size>-1</io-buffer-size>
  <max-file-size>1342177280</max-file-size>
  <block-size>-1</block-size>
  <initial-size>0</initial-size>
  <file-locking-enabled>false</file-locking-enabled>
  <target>examplesServer</target>
</file-store>
```

() Disabling File Locking for a JMS Paging File Store

Follow these steps to disable file locking for a JMS paging file store using the WebLogic Server Administration Console:

1. If necessary, click **Lock & Edit** in the Change Center (upper left corner) of the Administration Console to get an Edit lock for the domain.
2. In the **Domain Structure** tree, expand the **Services** node, expand the **Messaging** node, and select **JMS Servers**.
3. In the **Summary of JMS Servers** list, select the JMS server you want to modify.

4. On the **Configuration > General** tab for the JMS Server, scroll down and deselect the **Paging File Locking Enabled** check box.

5. Click **Save** to save the changes. If necessary, click **Activate Changes** in the Change Center.

6. **Restart** the server you modified for the changes to take effect.

The resulting `config.xml` file entry will look like the following:

```
<jms-server>
  <name>examplesJMSServer</name>
  <target>examplesServer</target>
  <persistent-store>exampleJDBCStore</persistent-store>
  ...
  <paging-file-locking-enabled>false</paging-file-locking-enabled>
  ...
</jms-server>
```

() Disabling File Locking for a Diagnostics File Store

Follow these steps to disable file locking for a Diagnostics file store using the WebLogic Server Administration Console:

1. If necessary, click **Lock & Edit** in the Change Center (upper left corner) of the Administration Console to get an Edit lock for the domain.

2. In the **Domain Structure** tree, expand the **Diagnostics** node and select **Archives**.

3. In the **Summary of Diagnostic Archives** list, select the server name of the archive that you want to modify.

4. On the **Settings for [server_name]** page, deselect the **Diagnostic Store File Locking Enabled** check box.

5. Click **Save** to save the changes. If necessary, click **Activate Changes** in the Change Center.

6. **Restart** the server you modified for the changes to take effect.

The resulting `config.xml` file will look like this:

```
  <server>
    <name>examplesServer</name>
    ...
    <server-diagnostic-config>
      <diagnostic-store-dir>data/store/diagnostics</diagnostic-store-dir>
      <diagnostic-store-file-locking-enabled>false</diagnostic-store-file-locking-
enabled>
      <diagnostic-data-archive-type>FileStoreArchive</diagnostic-data-archive-type>
      <data-retirement-enabled>true</data-retirement-enabled>
      <preferred-store-size-limit>100</preferred-store-size-limit>
      <store-size-check-period>1</store-size-check-period>
    </server-diagnostic-config>
  </server>
```

() ()

6.4 Documentation Errata

This section describes documentation errata. It includes the following topics:

- Section 6.4.1, "Documentation Errata for the Fusion Middleware High Availability Guide"
- Section 6.4.2, "Documentation Errata for the Fusion Middleware Enterprise Deployment Guide for Oracle WebCenter"
- Section 6.4.3, "Documentation Errata for the Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management"
- Section 6.4.4, "Documentation Errata for the Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Business Intelligence"
- Section 6.4.5, "Documentation Errata Affecting Multiple Enterprise Deployment Guides"

() ()

6.4.1 Documentation Errata for the Fusion Middleware High Availability Guide

This section contains Documentation Errata for *Oracle Fusion Middleware High Availability Guide*.

It includes the following topic:

- Section 6.4.1.1, "Latest Requirements and Certification Information"

() ()

6.4.1.1 Latest Requirements and Certification Information

Several manuals in the Oracle Fusion Middleware 11g documentation set have information on Oracle Fusion Middleware system requirements, prerequisites, specifications, and certification information.

- The latest information on Oracle Fusion Middleware system requirements, prerequisites, specifications, and certification information can be found in the following documents on Oracle Technology Network:

  `http://www.oracle.com/technology/software/products/ias/files/fusion_certification.html` (http://www

  This document contains information related to hardware and software requirements, minimum disk space and memory requirements, and required system libraries, packages, or patches.

- Oracle Fusion Middleware Certification information at:

  `http://www.oracle.com/technology/software/products/ias/files/fusion_certification.html` (http://www

  This document contains information related to supported installation types, platforms, operating systems, databases, JDKs, and third-party products.

() ()

6.4.2 Documentation Errata for the Fusion Middleware Enterprise Deployment Guide for Oracle WebCenter

This section contains Documentation Errata for *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle WebCenter*.

It includes the following topics:

- Section 6.4.2.1, "Link to Section 8.1.3 is Missing"
- Section 6.4.2.2, "Additional Information for Discussions Forum Mulitcast to Unicast Conversion"
- Section 6.4.2.3, "Additional Discussion Connection Properties Explained in Administration Guide"

() ()

6.4.2.1 Link to Section 8.1.3 is Missing

In Section 8.1, "Configuring the Discussion Forum Connection" of the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle WebCenter*, the link to section 8.1.3, "Creating a Discussions Server Connection for WebCenter From EM" is missing.

() ()

6.4.2.2 Additional Information for Discussions Forum Mulitcast to Unicast Conversion

In section 6.14, "Converting Discussions Forum from Multicast to Unicast" of the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle WebCenter*, the following information is missing from Step 3:

Step 3: Repeat steps 1 and 2 for WLS_Services2, swapping WCHost1 for WCHost2, and WCHost2 for WCHost1 as follows:

```
-Dtangosol.coherence.wka1=WCHost2 -Dtangosol.coherence.wka2=WCHost1
-Dtangosol.coherence.localhost=WCHost2 -Dtangosol.coherence.wka1.port=8089
-Dtangosol.coherence.wka2.port=8089
```

() ()

6.4.2.3 Additional Discussion Connection Properties Explained in Administration Guide

For additional Discussions Server connection properties associated with the procedure in Section 8.1.3 "Creating a Discussions Server Connection for WebCenter From EM" of the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle WebCenter*, refer to section 12.3.1, "Registering Discussions Servers Using Fusion Middleware Control," in the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter*.

() ()

6.4.3 Documentation Errata for the Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management

This section contains Documentation Errata for *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management* (../../core.1111/e12035/toc.htm).

It includes the following topic:

- Section 6.4.3.1, "Errors in Post-Installation Steps for Expanding the Oracle Directory Integration Platform and ODSM Cluster"

() ()

6.4.3.1 Errors in Post-Installation Steps for Expanding the Oracle Directory Integration Platform and ODSM Cluster

The following errors exist in subsections of Section 9.2.2 "Post-Installation Steps."

- The title of Section 9.2.2.1 should be "Copying the DIP Application to wls_ods2."
- All reference to copying to **`IDMHOST2`** should be removed from Section 9.2.2.1. During **`wls_ods2`** startup, the application is automatically propagated to **`IDMHOST2`** .
- Perform the copy only on **`IDMHOST1`** . Copy the ***`MW_HOME`*** **`/admin/IDMDomain/aserver/`** ***`IDMDomain`*** **`/config/fmwconfig/servers/wls_ods1/applications`** directory to the ***`MW_HOME`*** **`/admin/`** ***`IDMDomain`*** **`/aserver/`** ***`IDMDomain`*** **`/config/fmwconfig/servers/wls_ods2`** directory on **`IDMHOST1`** . For example:

  ```
  cp -rp MW_HOME/admin/IDMDomain/aserver/IDMDomain/config/fmwconfig/servers/wls_ods1/application
  ```

- Ignore the following sections, as they are no longer necessary:

  - Section 9.2.2.2, "Setting the Listen Address for the Managed Servers"
  - Section 9.2.2.3, "Starting the Managed Server on IDMHOST1"

() ()

6.4.4 Documentation Errata for the Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Business Intelligence

This section contains documentation errata for *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Business Intelligence*.

It includes the following topics:

Section 6.4.4.1, "Additional Step Must be Performed After Setting the Location of the BI Publisher Configuration Folder"

Section 6.4.4.2, "Corrections to the Setting the Location of the Shared Oracle BI Presentation Catalog Section"

() ()

6.4.4.1 Additional Step Must be Performed After Setting the Location of the BI Publisher Configuration Folder

After restarting Oracle BI Publisher when specifying the location of the configuration folder, as described in Section 6.5.3.1, "Setting the Location of the Shared Oracle BI Publisher Configuration Folder," you must copy the XML configuration file for Oracle BI Publisher from the Managed Server to the Administration Server location. Oracle BI Publisher reads its configuration from the Administration Server central location rather than from the Managed Server's configuration directory when the Managed Servers are restarted.

To do this, on APPHOST1, copy the file xmlp-server-config.xml from:

ORACLE_BASE/admin/*domain_name*/mserver/*domain_name*/config/bipublisher

to:

ORACLE_BASE/admin/*domain_name*/aserver/*domain_name*/config/bipublisher

() ()

6.4.4.2 Corrections to the Setting the Location of the Shared Oracle BI Presentation Catalog Section

The "Setting the Location of the Shared Oracle BI Presentation Catalog" section of the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Business Intelligence* should be replaced by the following section:

Each Presentation Services instance loads the Oracle BI Presentation Catalog from the catalog location specified in Fusion Middleware Control.

Perform the following steps:

1. Copy your existing (locally published) Oracle BI Presentation Catalog to the shared location. An example of a locally published catalog is:

   ```
   ORACLE_INSTANCE/bifoundation/OracleBIPresentationServicesComponent/
   coreapplication_obipsn/catalog/SampleAppLite
   ```

   You must perform this step before designating the **Catalog Location** from Fusion Middleware Control.

   If you plan to use the SampleAppLite catalog mentioned as an example in this section as the shared catalog, make sure to copy it from APPHOST1.

2. Log in to Fusion Middleware Control.

3. Expand the **Business Intelligence** node in the Farm_*domain_name* window.

4. Click **coreapplication**.

5. Click **Deployment**, then click **Repository**.

6. Click **Lock and Edit Configuration**.

7. Specify the **Catalog Location** for the shared Oracle BI Presentation Catalog.

   In a Windows environment, specify a UNC path name.

8. Click **Apply**.

9. Click **Activate Changes**.

() ()

6.4.5 Documentation Errata Affecting Multiple Enterprise Deployment Guides

This section describes documentation errata that affects multiple Enterprise Deployment Guides. Any Enterprise Deployment Guide that have the documentation errata issue discussed in the release notes below should be updated as specified in that release note.

It includes these topics:

- Section 6.4.5.1, "Sections on Configuring Oracle Coherence for SOA Composites Need Fixes"
- Section 6.4.5.2, "Updates are Needed to Steps for Testing Server Migration"
- Section 6.4.5.3, "Steps for Updating Data Sources for Server Migration Need Updates"
- Section 6.4.5.4, "Clarification of the Procedure for Configuring the Analytics Collectors"

() ()

6.4.5.1 Sections on Configuring Oracle Coherence for SOA Composites Need Fixes

Several Enterprise Deployment Guide manuals have a "Configuring Oracle Coherence for Deploying Composites" section that includes a Note like the following:

> **Note:**
>
> The Coherence cluster used for deployment uses port 8088 by default. This port can be changed by specifying the `-Dtangosol.coherence.wka` *n* `.port` startup parameter.

This Note should read as follows:

> **Note:**
>
> The Coherence cluster used for deployment uses port 8088 by default. This port can be changed by specifying a different port (for example, 8089) with the `-Dtangosol.coherence.wka` *n* `.port` and `-Dtangosol.coherence.localport` startup parameters. For example:
> WLS_SOA1 (enter the following into the Arguments field on a single line, without a carriage return):

```
-Dtangosol.coherence.wka1=soahost1vhn1
-Dtangosol.coherence.wka2=soahost2vhn1
-Dtangosol.coherence.localhost=soahost1vhn1
-Dtangosol.coherence.localport=8089
-Dtangosol.coherence.wka1.port=8089
-Dtangosol.coherence.wka2.port=8089
```

WLS_SOA2 (enter the following into the Arguments field on a single line, without a carriage return):

```
-Dtangosol.coherence.wka1=soahost1vhn1
-Dtangosol.coherence.wka2=soahost2vhn1
-Dtangosol.coherence.localhost=soahost2vhn1
-Dtangosol.coherence.localport=8089
-Dtangosol.coherence.wka1.port=8089
-Dtangosol.coherence.wka2.port=8089
```

() ()

6.4.5.2 Updates are Needed to Steps for Testing Server Migration

Several Enterprise Deployment Guide manuals have one or more subsections that describe how to test server migration.

The following Note should appear at the end of every section on testing server migration:

> **Note:**
>
> After a server is migrated, to fail it back to its original node/machine, stop the managed server from the Oracle WebLogic Administration Console and then start it again. The appropriate Node Manager will start the managed server on the machine to which it was originally assigned.

() ()

6.4.5.3 Steps for Updating Data Sources for Server Migration Need Updates

Several Enterprise Deployment Guide manuals have one or more subsections that describe how to update the data sources used for leasing when you configure server migration.

The following text appears in the instructions on how to update data sources for leasing as part of server migration configuration:

Use Supports Global Transactions, One-Phase Commit, and specify a service name for your database

That text should appear as follows:

Data sources do not require support for global transactions. Therefore, do *not* use any type of distributed transaction emulation/participation algorithm for the data source (do not choose the **Supports Global Transactions** option, or the **Logging Last Resource**, **Emulate Two-Phase Commit**, or **One-Phase Commit** options of the **Supports Global Transactions** option), and specify a service name for your database.

() ()

6.4.5.4 Clarification of the Procedure for Configuring the Analytics Collectors

Bug 10384373

Section 6.4.16, "Configuring the Analytics (../../core.1111/e10106/adf.htm#ASHIA5794)" in the *Oracle Fusion Middleware High Availability Guide* contains content that indicates that you must configure an analytic collector cluster. In fact, there is no need to configure the collectors themselves. Instead, the procedure in this section explains how to configure the Oracle WebCenter Spaces servers to communicate with the analytic collectors.

Further, for Oracle Fusion Middleware 11*g* Release 1 (11.1.1.4.0), clustered analytics collectors are not supported for collecting WebCenter events.

❮ (https://docs.oracle.com/cd/E17904_01/index.htm) Page 10 of 72 ❯ (https://docs.oracle.com/cd/E17904_01/doc.1111/e14770/was.htm)