Oracle® Fusion Middleware

Release Notes for Oracle Unified Directory

11*g* Release 2 (11.1.2.2)

E55519-01

January 2015

This document contains the release information for Oracle Unified Directory 11g Release 2 (11.1.2.2). It describes the difference between Oracle Unified Directory (OUD) and its documented functionality.

Oracle recommends you review its contents before installing or working with OUD.

This document is accurate at the time of publication. Oracle will update the Release Notes periodically after the software release. You can access the latest information and additions to these Release Notes on the Oracle Technology Network at:

http://docs.oracle.com/cd/E49437_01/relnotes.111220/e23738/toc.htm

These Release Notes include the following topics:

- Section 1, "System Requirements and Specifications"

- Section 2, "Software Environment Limitations and Recommendations"

- Section 3, "Oracle Unified Directory (OUD) Known Issues and Workarounds"

- Section 4, "Oracle Directory Service Manager (ODSM) Known Issues and Workarounds"

- Section 5, "Documentation Accessibility"

1 System Requirements and Specifications

Before performing any installation, you should read the system requirements and certification documents to ensure that your environment meets the minimum installation requirements for the products you are installing. The following documents are available on Oracle Technology Network (OTN):

- *Oracle Fusion Middleware System Requirements and Specifications for Oracle Identity and Access Management*

  This document contains detailed information related to hardware and software requirements, minimum disk space and memory requirements, and required system libraries, packages, or patches when installing OUD with other Oracle products.

- Oracle Fusion Middleware Supported System Configurations

  http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-certification-100350.html

  This landing page contains links to certification information for all products in Fusion Middleware suite.

- Oracle Unified Directory (OUD) 11gR1 (11.1.2.x) Certification Matrix

  This document contains the most detailed information about supported application servers, supported clients, JDK requirements, and IPv4/IPv6 certifications for installing OUD.   This document is updated when new information becomes available.

  To access this document, on the Oracle Fusion Middleware Supported System Configurations landing page, follow the link to "System Requirements and Supported Platforms for Oracle Unified Directory 11gR1."

ORACLE®

- *Oracle® Fusion Middleware Installation Guide for Oracle Unified Directory 11g Release 2 (11.1.2)*

  Chapter 1, "Before You Install Oracle Unified Directory" contains pre-installation system notes and other information you should review prior to OUD installation.

The following sections describe additional information specific to OUD installation requirements:

- Section 1.1, "Hardware Requirements"

- Section 1.2, "Software Requirements"

- Section 1.3, "Certified Languages"

1.1 Hardware Requirements

As a general guideline, the following hardware is recommended:

Table 1   Recommended Hardware

Hardware Component	Requirement
RAM	**Evaluation purposes:** At least 256 MB of free memory for a small database.
	Production: Minimum of 2 GB.
Local disk space	**Evaluation purposes:** For a small database and sufficient space for log files, your system should have at least 100 MB of free local disk space. Preferably, you should have at least 1 GB of disk space.
	Production: For a typical production deployment with a maximum of 250,000 entries and no binary attributes, such as images, 4 GB of disk space might be sufficient for the database only. You might need an additional 1 GB of disk space for log files. You need to determine disk space for the change log database (DB), which is dependent on the load (updates per second) and on the replication purge delay (that is, the time the server should keep information about internal updates). The change log DB can grow up to 30-40 GB with loads of 1,000 modifications per second.
	When you use global index replication, ensure that you have enough disk space for the replication change logs. By default, the change log stores changes from the last 100 hours. The configuration should be based on the expected size of the service. For example, you would need 150 GB for 5,000 modify/seconds.
	While the directory server can be used with databases and logs installed on NFS-mounted file systems, related files must not be accessed at same time from different systems. Sufficient space should be provided for the database.

For optimal performance, your system must have sufficient RAM memory for the JVM heap and database cache. For more information about setting the JVM heap and database cache, see "Configuring the JVM, Java Options, and Database Cache" in *Oracle Fusion Middleware Installation Guide for Oracle Unified Directory*.

Your system should also have enough disk space to store the generated log files. The server log files can consume up to 1 GB of disk space with default server settings. In replicated environments, the change log database can grow up to 30-40 GB with loads of 1,000 mods/sec. For information about setting the log file size, see "Configuring Log Rotation Policies" in *Oracle Fusion Middleware Administrator's Guide for Oracle Unified Directory*.

You can configure Oracle Unified Directory in such a way that it uses substantially less, or more, disk space depending on your application and performance needs. Any setup considerations must determine the amount of memory for the server's database and log files.

On Solaris systems, the operating system should be configured to have at least twice as much virtual memory as JVM heap. To achieve this, you might need to increase the size of the operating system swap space.

1.2 Software Requirements

In addition to the operating system, application server, and JDK requirements described in this document:

http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-certification-100350.html

be sure to resolve the following OS-specific requirements:

- Section 1.2.1, "File Descriptor Requirements (Linux Systems)"
- Section 1.2.2, "Specific Requirements for Installation in Solaris Zones"

1.2.1 File Descriptor Requirements (Linux Systems)

The issue described in this section affects Linux systems only. All other supported platforms are unaffected.

To ensure optimal server performance, the total number of client connections, database files, and log files must not exceed the maximum file descriptor limit on the operating system (`ulimit -n`). By default, the directory server allows an unlimited number of connections but is restricted by the file descriptor limit on the operating system. Linux systems limit the number of file descriptors that any one process may open to 1024 per process.

After the directory server has exceeded the file descriptor limit of 1024 per process, any new process and worker threads will be blocked. For example, if the directory server attempts to open a Oracle Berkeley JE database file when the operating system has exceeded the file descriptor limit, the directory server will no longer be able to open a connection that can lead to a corrupted database exception. Likewise, if you have a directory server that exceeds the file descriptor limit set by the operating system, the directory server can become unresponsive as the LDAP connection handler consumes all of the CPU's processing in attempting to open a new connection.

To fix this condition, set the maximum file descriptor limit to `65535` per process on Linux machines.

To view the maximum file descriptor limit, run the following command:

```
/sbin/sysctl -a | grep file-max
```

If the `file-max` value is lower than `65535`, then perform the following steps:

1. Using any text editor, create or edit the `/etc/sysctl.conf` file, and add or edit lines similar to the following:

   ```
   fs.file-max = 65536
   ```

2. Enter the following command to change the current values of the kernel parameters:

   ```
   /sbin/sysctl -p
   ```

3. Enter the command `/sbin/sysctl -a | grep file-max` to confirm that the values are set correctly.

4. Using any text editor, edit the `/etc/security/limits.conf` file, and add the following lines:

   ```
   soft nofile 1024
   hard nofile 65535
   ```

> **Note:** When you specify the values in the `/etc/sysctl.conf` or `/etc/security/limits.conf` file, they persist when you restart the system.

1.2.2 Specific Requirements for Installation in Solaris Zones

The Oracle Unified Directory software treats global, full local, and sparse zones as an independent physical system. Installing the server in any type of Solaris zone is therefore like installing on an independent system. The software does not share services or file locations with other zones.

1.3 Certified Languages

Oracle Unified Directory 11*g* Release 2 (11.1.2.2) is certified for the following languages:

- Chinese (Simplified)

- Chinese (Traditional)

- French

- German

- Italian

- Japanese

- Korean

- Spanish

- Portuguese (Brazilian)

> **Note:** Certain error messages (specifically, the SEVERE and FATAL messages) are displayed in English only.

2 Software Environment Limitations and Recommendations

The Oracle Unified Directory 11*g* Release 2 (11.1.2.2) software has some limitations that might affect the initial deployment of your directory server. Follow the recommendations for deployments in this section.

Administrators also should appropriately tune the Oracle Unified Directory directory server and its Java Virtual Machine (JVM) to ensure that adequately sized hardware is made available to support heavy write operations. For more information, see "Configuring the JVM, Java Options, and Database Cache" in *Oracle Fusion Middleware Installation Guide for Oracle Unified Directory*.

This section describes the following topics:

- Section 2.1, "Oracle Unified Directory 11g Release 2 (11.1.2.2) Limitations"

- Section 2.2, "Oracle Unified Directory Software Recommendations"

2.1 Oracle Unified Directory 11*g* Release 2 (11.1.2.2) Limitations

This section lists the limitations of Oracle Unified Directory 11*g* Release 2 (11.1.2.2). They are as follows:

- The Oracle Unified Directory directory server provides full LDAP v3 support, except for alias dereferencing, and limited support for LDAPv2.

- Oracle Unified Directory when setup for Enterprise User Security is currently validated for proxy for the following directory servers:

  - Sun Java System Directory Server Enterprise Edition 6.3

  - Microsoft Active Directory 2008 R2 and Active Directory 2012

  - Novell eDirectory 8.8

- Oracle Unified Directory 11*g* Release 2

■ The proxy server provides the best search performance when the search queries ask for the specific required attributes (rather than all the attributes) of an entry.

2.2 Oracle Unified Directory Software Recommendations

This section lists the recommendations for using Oracle Unified Directory 11*g* Release 2 (11.1.2.2). They are as follows:

■ The directory server provides better performance when the database files are cached entirely into memory.

■ The default settings of the Oracle Unified Directory directory server are targeted initially at evaluators or developers who are running equipment with a limited amount of resources. For this reason, you should tune the Java virtual machine (JVM) and the directory server itself to improve scalability and performance, particularly for write operations. For more information, see "Configuring the JVM, Java Options, and Database Cache" in *Oracle Fusion Middleware Installation Guide for Oracle Unified Directory*.

■ If you want to import large LDIF files by using the `import-ldif` command, then it is recommended that you use the `--skipDNvalidation` option. However, if you are not certain that the LDIF file is valid, using this option is not advised.

3 Oracle Unified Directory (OUD) Known Issues and Workarounds

The following sections describe known issues and limitations with the Oracle Unified Directory 11*g* Release 2 (11.1.2.2) core server at the time of this release.

3.1 (Bug 17881246) Warning message is displayed: "Macro ACIs are not compatible with OUD servers..."

If you migrate an ODSEE instance to an OUD server using `ds2oud`, the following warning may be displayed: "Macro ACIs are not compatible with OUD servers and should not be used in a mixed environment."

Workaround
Macro ACIs are now compatible, and you can safely ignore this warning.

3.2 (Bug 17874888) Root user containing ds-privilege-name: -data-sync has no privileges.

The `data-sync` privilege has been removed from this release of OUD, and the OUD server no longer recognizes the privilege. For example, if the root user is created as follows:

```
dn: cn=myroot,cn=Root DNs,cn=config
objectClass: inetOrgPerson
objectClass: person
objectClass: top
objectClass: ds-cfg-root-dn-user
objectClass: organizationalPerson
userPassword: admin-password
cn: myroot
sn: myroot
ds-cfg-alternate-bind-dn: cn=myroot
givenName: My Root User
ds-privilege-name: -data-sync
```

then the OUD server does not recognize the privilege, and cannot remove it. Instead, the OUD server removes all privileges for this user.

Workaround

Remove the value `-data-sync` from the `ds-privilege-name` attribute of root users. For example:

```
$ ldapmodify -h localhost -p 4444 --useSSL
dn: cn=myroot,cn=Root DNs,cn=config
changetype:modify
delete:ds-privilege-name
ds-privilege-name: -data-sync
```

3.3 (Bug 17867250) Windows service associated with OUD cannot be launched.

When you setup OUD to run as a Windows Service, and then restart the Windows system, an error message is displayed. The Windows service cannot be launched. This occurs when the administrator does not have access rights on the instance path.

Workaround

Enable the administrator's access rights on the instance path.

3.4 (Bug 17797663) Pass-Through Authentication subject to limitations when configured with Kerberos authentication provider.

When pass-through authentication (PTA) is configured with a Kerberos authentication provider, certain conditions must be met in order for the bind to succeed.

Workaround

Configure PTA to meet the following conditions:

- The user provider must be a local backend.

- The PTA suffix, the user suffix, and the authentication suffix must be the same. The easiest way to configure the suffixes to be the same is to define the PTA suffix, and leave the other suffixes undefined.

3.5 (Bug 17766636) Operational Status field indicates "Unexpected Error."

When using the DSCC to monitor the replication gateway, on the Directory Servers tab, the operational status indicates "Unexpected Error."

Workaround

1. Stop the replication gateway.

2. Edit the legacy configuration file `<INSTANCE_PATH>/OUD/config/legacy-config.ldif`.

    Find the mapping tree entry corresponding to the suffix that you cannot manage through DSCC because of the "unexpected error." Remove the slash character (\) present in the `cn` value.

    For example, after the modification you should have an entry similar to this:

```
dn: cn=dc=example\,dc=com,cn=mapping tree,cn=gwconfig
objectClass: extensibleobject
objectClass: nsMappingTree
objectClass: top
nsslapd-state: backend
nsslapd-backend: example1
cn: dc=example,dc=com
entryUUID: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
```

3. Restart the replication gateway.

4. Refresh the DSCC page.

3.6 (Bug 17740008) When adding new suffixes to be replicated, EUS suffixes are not displayed as replication options.

When a suffix is configured with the Enterprise User Security (EUS) option, and you want to replicate its contents, some of the internal suffixes required by EUS (and that should also be replicated) are not displayed as replication options.

Workaround

Use the `dsreplication` command, and provide the base DN of the internal suffixes (for example cn=*eussuffix* and `cn=oraclecontext`) explicitly as an argument.

For example, if you want to replicate the suffix CN=*EUSSuffix*, run the following command:

```
dsreplication enable --baseDN CN=EUSSuffix --baseDN cn=OracleContext --baseDN
cn=OracleSchemaVersion
```

3.7 (Bug 17739791) When using `oud-setup`, EUS suffixes are not displayed as replication options.

When using the `oud-setup` command to configure two OUD servers for replication with the Enterprise User Security (EUS) option, EUS suffixes are not displayed as replication options.

Workaround

 Use the `dsreplication` command to configure the servers for replication. See also Section 3.6 above.

3.8 (Bug 17689711) Enabling the changelog for multiple suffixes on the same replication servers may cause unwanted configuration changes.

You may encounter this issue when you have two servers containing two suffixes: one suffix already configured for replication (for example `dc=example,dc=com`), and the other suffix *not* configured for replication (for example `cn=companyname.`) When you enable the changelog for `cn=companyname` in both servers, replication is automatically configured for the `cn=companyname` suffix because the servers themselves have already been defined and configured for replication.

Workaround

 There is currently no workaround for this issue.

3.9 (Bug 17627747) Error message is displayed when a workflow element contains a `remote-ldap-server-bind-password-file` value.

When upgrading from OUD 11g Release 11.1.1.1, if a workflow element contains a `remote-ldap-server-bind-password-file` value, then the following message is displayed:

```
[18/Oct/2013:17:47:28 +0200] category=PROXY_LDAP severity=SEVERE_ERROR
msgID=28573708 msg=File not found:
@ /.../tmp/ds1-888646394-rootpw.
```

The upgrade process will continue regardless of this message.

Workaround

 Once the upgrade is completed, manually set the `remote-ldap-server-bind-password-file` value again.

3.10 (Bug 17588927) After uninstallation, the server is still up and running despite uninstallation tool reporting a successful uninstallion.

Uninstallation is unsuccessful, and the following message is displayed, "Error reading data from server. There is an error with the certificate presented by the server."

Workaround

If after uninstallation of an instance, the instance is still running, kill the relevant process from the system. Check that all files and directories have been removed. If they have not been removed, manually remove them.

3.11 (Bug 17582404) ADF error is displayed in WebLogic Server logs.

When accessing an entry in the data view, the following error message appears in the WebLogic Server logs:

```
<Oct 9, 2013 8:04:17 AM PDT> <Error>
<oracle.adf.controller.internal.binding.TaskFlowRegionInitialConditions>
<ADFC-64007> <ADFc: Task flow binding parameter 'entryObject' of type
'oracle.idm.directoryservices.odsm.model.oid.UserEntry' on binding
'oidDBdetailtaskflow' is not serializable, potential for incorrect
application behavior or data loss.>
```

Workaround

The error does not affect the WebLogic Server functionality. You can safely ignore the message.

3.12 (Bug 17580087) OUD fails to set the purging flag in the `ds-sync-hist` index.

When upgrading from OUD 11g Release 11.1.1.5 or Release 11.1.2.0 to OUD 11g Release 11.1.2.2, the latest release fails to set the purging flag in the `ds-sync-hist` index.

Workaround

Set the `ds-cfg-purging` flag of the `ds-sync-hist` index to true. Then rebuild the `ds-sync-hist` index:

```
./dsconfig set-local-db-index-prop --element-name userRoot --index-name ds-sync-hist --set
purging:true
```

```
./rebuild-index -b "dc=example,dc=com" -i ds-sync-hist
```

3.13 (Bug 17567689) OUD server fails to reject an add request.

Replication error occurs when the OUD server fails to reject an add request (using the replication repair control) for an entry which contains no `entryuuid`.

Workaround

If an entry which contains no `entryuuid` has been added using the replication repair control, the entry should be deleted and re-added with the proper `entryuuid` (using the repair control for all operations).

3.14 (Bug 17564774) Message "Fatal error during the processing of the DPS" is displayed.

The `dps2oud` command returns the following error message: "Fatal error during the processing of the DPS." This occurs when the configuration contains multiple data-views with the same view-base, and contains no distribution algorithm.

Workaround

Update the Directory Proxy Server configuration file so that each view-base is attached to only one data-view.

3.15 (Bug 16477758) Entry cache might not be correctly updated.

Entry cache might not be correctly updated.

Workaround

Disable the entry cache, running the following command:

```
dsconfig set-entry-cache-prop \
--cache-name FIFO \
--set enabled:false\
--port ADMIN_PORT \
--bindDN cn=Directory\ Manager \
--bindPassword ****** \
--no-prompt
```

3.16 (Bug 16214645) While setting up the Enterprise User Security (EUS) configuration, an error may occur.

When you install an Oracle database version 11.1.6.0 while setting up the Enterprise User Security (EUS) configuration, you might encounter the message "ORA-28030 Server encountered problems accessing LDAP directory service."

Workaround

1. Launch Oracle Wallet Manager, and open the wallet which is by default stored under:

   `$ ORACLE_BASE/admin/<SID>/ wallet`

2. Provide the password for wallet which was given while registering using DBCA.

3. Select the auto-login checkbox from the wallet manager File > Auto-login menu.

4. Save the wallet again to create the `cwallet.sso`.

3.17 (Bug 14772631) If an `AddOutboundTransformation` definition contains a dot, then a search request might fail.

When you configure an `AddOutboundTransformation` with `virtualAttr={%sn%.%cn%@o.com}` where the definition contains a dot, then a search request with a filter on the `virtualAttr` parameter might not work correctly.

For instance, the `sn` and `cn` backend attribute values contain a dot, such as `"sn:sn.light"` and `"cn:cn.light."` Here, a search request with a filter on the `virtualAttr`, for example `"virtualAttr=sn.light.cn.light@o.com"` might not work correctly.

Workaround

There is currently no workaround for this issue.

3.18 (Bug 14768705) Errors occur while configuring the client-attribute value for an `AddOutboundTransformation`.

If you omit the curly brackets {} while configuring the client-attribute value for an `AddOutboundTransformation`, for instance `client-attribute:"cn=%sn%.%cn%"` instead of `"cn={%sn%.%cn%}"` then the `dsconfig` command does not throw any warning. However, the transformation does not work correctly.

Workaround

Be sure to use curly brackets {} while configuring the client-attribute value for `AddOutboundTransformation`.

3.19 (Bug 14768666) When you use the `addoutboundattr` transformation, the `ldapcompare` command might erroneously return `FALSE`.

When you use the `addoutboundattr` transformation, for instance `cn=%sn%` with conflict behavior set to `Merge-real-and-virtual`, then the `ldapcompare` command might erroneously return `FALSE`, because comparison is done only on `sn` values and not on `cn` values.

Workaround

There is currently no workaround for this issue.

3.20 (Bug 17449719) The `start-ds --upgrade` command produces warning message.

After upgrading an OUD instance to 11*g* Release 2 (11.1.2.1), the `start-ds -upgrade` command displays the following message: MILD WARNINGS: MISSING INDEX IN VIRTUALACIS BACKEND.

Workaround

You can safely ignore the message.

3.21 (Bug 14080885) The `moveplan` interface does not have a field to update the path for keystore pin file.

The `moveplan` interface does not have a field to update the path for keystore pin file during the cloning process.

Workaround

Use the `dsconfig` command on the cloned instance to update the `key-store-pin-file` value of `JKS Key Manager Provider` while cloning.

3.22 (Bug 14652478) The `runInstaller` command fails to check for appropriate OS.

On Oracle Linux Enterprise 6, the `runInstaller` command may require i686 packages to be present on the system. Although the missing packages are not directly required for OUD to operate properly, they are required during the installation process.

Workaround

Prior to running the `runInstaller` command, install the required i686 packages. See the "Section 1.1 System Requirements and Cerification" in the *Installation Guide for Oracle Unified Directory*.

3.23 (Bug 14065106) Translation is not supported for some error message and online Help.

Oracle Unified Directory does not support translation of both messages and Help for `oudCopyConfig`, `oudExtractMovePlan`, and `oudPasteConfig` commands.

Workaround

There is currently no workaround for this issue.

3.24 (Bug 14055062) If the value for parameter `-j, --rootUserPasswordFile` is provided as a relative path, commands fail.

On Windows system, if the value for parameter `-j, --rootUserPasswordFile` is provided as a relative path, then `oud-setup, oud-proxy-setup,` and `oud-replication-gateway-setup` commands fail.

Workaround

Provide an absolute path for `-j, --rootUserPasswordFile` parameter.

For example:

`-j C:\local\Password.txt`

3.25 (Bug 13996369) The `gicadm` command does not import a catalog.

The `gicadm` command does not import a catalog when you specify a relative path.

Workaround

Specify an absolute path to import a catalog.

3.26 (Bug 13991574) If the entry for a secret key is defined in a remote server, an error message is displayed when importing the symmetric key entry.

When merging two replication gateway topologies, if the entry for a secret key is defined in a remote server, a message similar to this is displayed):

```
[23/Apr/2013 04:05:48 +0200] category=CORE severity=SEVERE_ERROR
msgID=262798
msg=An error occurred in the trust store synchronization thread:
CryptoManager failed to import the symmetric key entry
"ds-cfg-key-id=b11909bc-8a5a-4ac2-a9b6-dabb19d1608d,cn=secret keys,cn=admin
data" because it could not obtain a symmetric key attribute value that can be
decoded by this instance (CryptoManagerSync.java:299
CryptoManagerSync.java:233 CryptoManagerSync.java:263
LocalBackendWorkflowElement.java:521 TaskUtils.java:167
LDAPReplicationDomain.java:4665 LDAPReplicationDomain.java:4612
ReplicationDomain.java:2345 ReplicationDomain.java:819
ListenerThread.java:100)
```

Workaround

You can safely ignore this message. Despite the error severity indicated in the message, there is no impact to functionality.

3.27 (Bug 13965857) If you specify an alternative location for a cloned server instance, the cloned server instance is not completely configured.

The `-tih, -targetInstanceHomeLoc` option of the `oudPasteConfig` command allows you to specify the location of the cloned server instance. If you specify an alternative location, for the cloned server instance, the instance is still created in the default location (*TARGET_ORACLE_HOME/../TARGET_INSTANCE_NAME*) and

no error message is generated. However, the cloned server is configured partially as some custom parameters are not updated in the cloned server instance.

Workaround

To successfully clone the server instance, as the `-tih` parameter is mandatory, you must explicitly provide the default location for the `-tih` parameter as follows:

`-tih TARGET_ORACLE_HOME/../TARGET_INSTANCE_NAME`

3.28 (Bug 13954545) The `ldapsearch.bat` client incorrectly handles a trailing asterisk character.

On a Windows system with a JDK 1.7 (previous to Update 11) JVM instance running, the `ldapsearch.bat` client might not handle the trailing "*" correctly.

Workaround

Download the latest JDK version to leverage the fixes and updates that are added to the Java SE platform.

3.29 (Bug 12329839) Errors occur if the `runInstaller` command is executed on SuSE Linux Enterprise Server 11.

When you run the Oracle Unified Directory installer using the `runInstaller` command on SuSE Linux Enterprise Server 11, the prerequisite checks are not executed and an error is generated.

Workaround

Use the `-ignoreSysPrereqs` flag while running the `runInstaller` command.

3.30 (Bug 12291860) No SNMP trap is sent if the server is stopped using the `stop-ds` command with no credentials.

On Windows systems no SNMP trap is sent if the server is stopped by using `stop-ds` with no credentials. The server is, however, stopped correctly.

The SNMP trap is sent if the server is stopped by using `stop-ds -D bindDN -p password`.

Workaround

There is currently no workaround for this issue.

3.31 (Bug 12280658) The ModDN operation is not supported if DNs are indexed in the global index catalog (GIC).

When a distribution is using a GIC, and the GIC indexes the entry DNs, the ModifyDN operation is not supported.

If DNs are not indexed in the global index catalog, the modify DN operation is supported. Otherwise, only the modify RDN operation is supported.

Workaround

Although indexing the DN is recommended for performance reasons, as a workaround in this situation, do not index the DN.

3.32 (Bug 12266690) Load balancing routes are deleted without warning.

If you delete the load balancing workflow element or the load balancing algorithm, the load balancing routes are also deleted without any warning.

Workaround

There is currently no workaround for this issue.

3.33 (Bug 11869296) Cleaning process does not end.

Under heavy and sustained load the database cleaning process does not end.

Workaround

Configure a larger database cache. For more information, see "Tuning the Server Configuration" in *Oracle Fusion Middleware Administrator's Guide for Oracle Unified Directory.*

3.34 (Bug 11812850) Installation fails if path to Java includes a space character.

On Windows system, if the path to your Java installation in the `-jreLoc` option includes a space character, then the installer does not run appropriately and terminates.

Workaround

Provide the path to your Java installation in DOS 8.3 format.

For example:

```
-jreloc C:\Progra~1\Java\jdk1.6.0_21
```

For more information, see "Installing Oracle Unified Directory" in *Oracle Fusion Middleware Installation Guide for Oracle Unified Directory.*

3.35 (Bug 11810392) Non-ASCII characters are displayed base64-encoded.

If DN or attribute values of returned entries contain non-ASCII characters, the DN or values are displayed base64-encoded.

Workaround

There is currently no workaround for this issue.

3.36 (Bug 11718654) Error occurs in replicated topology with a heavy workload.

In a replicated topology, if the server has a heavy workload, then the following error message is recorded in the error log: "The server failed to obtain a read lock on the parent entry `dc=example`, `dc=com` after multiple attempts."

Workaround

Configure a larger database cache. For more information, see "Tuning the Server Configuration" in *Oracle Fusion Middleware Administrator's Guide for Oracle Unified Directory*.

3.37 (Bug 11678445) The `oud-setup` command fails when appropriate file permissions are not set.

When you run the `oud-setup` command and set the `INSTANCE_NAME` variable to a path for which you do not have the appropriate file permissions, the command fails.

Workaround

Set the required file permissions for the path to which `INSTANCE_NAME` variable points.

4 Oracle Directory Service Manager (ODSM) Known Issues and Workarounds

The following sections describe known issues with Oracle Directory Services Manager at the time of Oracle Unified Directory 11*g* Release 2 (11.1.2.2) release.

4.1 (Bug 18196601)

Oracle Unified Directory Resource Center and Online Help do not display properly using Internet Explorer 11.

Workaround

 There is no workaround at this time.

4.2 (Bug 17773298) Certificates are accepted automatically without user verification.

When a connection is made to a server for replication management, and the security certificate returned by the server is not present in the trust-store, the user is not prompted to verify the validity of the certificate.

Workaround

 There is no workaround at this time.

4.3 (Bug 17773238) Cannot configure secure communication using Replication Management graphical interface.

The Replication Management graphical interface does not provide a means to configure a replication server to use secure communication.

Workaround

 Use the `dsreplication` command.

4.4 (Bug 17747692) ODSM EAR Implementation Version is always displayed as 11.1.1.5.0.

In a WebLogic Server deployment of ODSM, the Implementation Version number 11.1.1.5.0 is displayed for the ODSM EAR file (`odsm.ear`) regardless of the actual ODSM 11.1.x.x product version. The Implementation Version number is displayed next to a deployed application in the list of deployments shown in the WebLogic Administration Console.

Workaround

You can safely ignore the Implementation Version number displayed.

4.5 (Bug 17487942) Cannot create a key manager of PKCS type.

When you try to create a key manager and specify the type as PKCS type, an error message is displayed: "The key store pin must be specified."

Workaround

Use the `dsconf` command.

4.6 (Bug 17462792) Subtabs may not display as designed on Solaris.

When accessing the Directory Service Manager tab or Topology Manager tab using Firefox on a Solaris system, the subtabs may not display as expected.

Workaround

Click the forward arrows (>>) or back arrows (<<) to open a menu, and then navigate among the subtabs.

4.7 (Bug 17422259) Error occurs when creating a new ACI.

On the Security tab, when creating a new ACI, if you navigate away from the Security tab without modifying any field and then return to the Security tab, an error occurs.

Workaround

 Click the Create icon displayed at the left to create the ACI.

4.8 (Bug 17262682) Default browser settings may not allow ODSM URL to be accessible on Windows 2008.

After installing OUD and ODSM on Windows 2008 Release 2, when you try to access the ODSM URL, the message "Starting Oracle Directory Services Manager..." displays, but the ODSM application does not load in the browser as expected. This can occur when you use Microsoft Internet Explorer version 8 or 9 browsers.

Workaround

1. Verify that JavaScript is enabled.

2. Add the ODSM URL in the trusted sites.

   Go to Tools-> Internet Options -> Security -> Trusted sites -> Sites -> Add. Then click Add to add the ODSM URL to a site.

4.9 (Bug 16946878) Alerts not sent as designed.

On the Alert Handler Properties page, the Disabled Alert Type and Enabled Alert Type fields do not work as designed. Regardless of the setting for either field, alerts are never sent as expected.

Workaround

Use `dsconfig set-alert-handler-prop` to add or remove enabled-alert-type or disabled-alert-type values.

Use `dsconfig set-alert-handler-prop set-alert-handler-prop --add enabled-alert-type:`*alert type value* to add enabled-alert-type *alert type value*.

Use `dsconfig set-alert-handler-prop set-alert-handler-prop --remove enabled-alert-type:`*alert type value* to remove enabled-alert-type *alert type value*.

Example:

```
# dsconfig -h slc03roj -p 4444 -D "cn=Directory Manager" -j /tmp/oud -n -X
set-alert-handler-prop --handler-name "SMTP Alert handler name" --remove
enabled-alert-type:org.opends.server.DirectoryServerShutdown
```

4.10 (Bug 16056177) On the Advanced Search page, when you click an entry in the Search Results table, some buttons do not behave as expected.

On the Advanced Search page, when you click an entry in the Search Results table, the **Show Attributes** button does not appear if Optional Attributes is already expanded. However, if you collapse **Optional Attibutes** and then expand, the **Show Attributes** button appears. But, when you click the button the Select Attributes dialog box is blank.

Workaround

To view the entry details, you can select the same entry from Data Browser tab.

4.11 (Bug 15928439) Java NullPointer exception occurs if a changelog entry does not contain a specified objectclass.

When this NullPointer exception is encountered, the contents of that particular changelog entry cannot be accessed from ODSM. You can continue to use ODSM to perform other tasks and access other entries.

Workaround

To access a changelog entry with no objectclasse specified, use a different LDAP client.

4.12 (Bug 12363352) In the screenreader mode, focus for some buttons does not work as expected.

When you are in the screenreader mode, the Create, Apply, and Cancel buttons in the Oracle Directory Services Manager interface do not get focus after modification.

Workaround

Press the Tab key until you get the focus on the required button. Alternatively, you can use the mouse to activate the required button.

4.13 (Bug 11937031) Microsoft Internet Explorer 7 does not render some Web pages of Oracle Directory Services Manager properly.

Microsoft Internet Explorer 7 does not render some Web pages of Oracle Directory Services Manager properly. It does not lead to any loss of functionality, but some Web pages display with unnecessary scroll bars or wrapped field names.

Workaround

Upgrade the browser to Microsoft Internet Explorer 8 or Microsoft Internet Explorer 9. While using Microsoft Internet Explorer 8 or Microsoft Internet Explorer 9, you need to disable the compatibility view mode in the browser. For more information about how to disable the compatibility view mode in the browser, refer to the following Web page: http://support.microsoft.com/kb/956197

5 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.