Oracle® Fusion Middleware

Release Notes for Oracle Unified Directory

11*g* Release 2 (11.1.2.3)

E55519-02

January 2017

This document contains the release information for Oracle Unified Directory 11*g* Release 2 (11.1.2.3). 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 Help Center for OUD 11*g* Release 2 (11.1.2.3) by searching for that release number in the library. You can access the Oracle Help Center at the following website:

`http://docs.oracle.com/en/`

These Release Notes include the following topics:

1 What's New in This Release

The following is a list of new features in the OUD 11*g* Release 2 (11.1.2.3):

- Enhanced security:
  - Password Masking in Audit Log. For more information see, "Masking Attributes in the Audit Log" and "Support for Encryption in Replication Topology"
  - Support for Linux Crypt algorithm. For more information see, "Crypt Algorithm"
  - Password expiration available as a virtual attribute. For more information see, "Configuring Virtual Attributes"

- Simplified deployment through:
  - OUD server metrics displayed in ODSM console. For more information see, "Viewing the Server Metrics"
  - Support for native replication with Sun DSEE 6.3. For more information see, "Exporting User Data from (O)DSEE to OUD"
- Virtual Directory Capabilities:

  Note: To use the virtual directory capabilities described here, you must have a valid `Oracle Directory Service Plus` license.

  - Join between multiple backends. For more information see, "Using Entries from Multiple Directories" and "Configuring a Virtual Directory View of Your Repositories"
  - Database connector. For more information see, "Configuring Access to Identity Data Stored in an RDBMS"
- Further performance and scalability:
  - Support for large static groups. For more information see, "Defining Groups" and "Additional Tuning Recommendations"
  - Reduced memory footprint through entry compaction and selective attribute caching. For more information see, "Configuring Selective Attribute Caching" and, "Saving Database Space Using Tokens for Attribute Values"

2 Supported Interfaces for Directory Virtualization Features

Note: To use the virtual directory capabilities described here, you must have a valid `Oracle Directory Service Plus` license.

Table 1 lists the supported interfaces for virtualization workflow elements in this release:

Note: The Dynamic Tree, and Flat Tree workflow elements are not supported in this release. If you encounter any functions in the interfaces for these workflow elements, do not execute them as they are not supported.

Table 1 Oracle Unified Directory Virtualization Features

Workflow Element	Configure with Command Line	Configure with ODSM	Additional Information
Join	Yes	Yes	See "Configuring a Virtual Directory View of Your Repositories"
HideByFilter	Yes	No	See "Filtering Search Results Using the HideByFilter"

Table 1 (Cont.) Oracle Unified Directory Virtualization Features

Workflow Element	Configure with Command Line	Configure with ODSM	Additional Information
GetRidOfDuplicates	Yes	No	See "Eliminating Duplicate Entries from Search Results Using the GetRidOfDuplicates"
Active Directory Password Update	Yes	No	See "Updating User Passwords Stored in Active Directory"
RDBMS	Yes	No	See "Configuring Access to Identity Data Stored in an RDBMS"
VirtualMemberOf	Yes	No	See, "Adding the memberof User Attribute to person Entries"

3 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. To view the certification matrix:

  1. Access the Oracle Fusion Middleware Supported System Configurations landing page:

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

  2. Scroll down to System Requirements and Supported Platforms for Oracle Identity and Access Management 11*g* Release 2 (11.1.2.3.0).

  3. Click the *xls* link to view the 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 as new information becomes available.

- *Oracle® Fusion Middleware Installing 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 3.1, "Hardware Requirements"
- Section 3.2, "Software Requirements"
- Section 3.3, "Certified Languages"

3.1 Hardware Requirements

As a general guideline, the following hardware is recommended:

Table 2 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.

For optimal performance, your system must have sufficient RAM memory for the JVM heap and database cache. The server also provides ready-to-use tuning. For more information about setting the JVM heap and database cache, see "Configuring the JVM, Java Options, and Database Cache" in *Oracle Fusion Middleware Installing 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 Administering 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 applications and performance needs. Any setup considerations must determine the amount of memory for the server's database and log files.

On Solaris and Linux 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.

3.2 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 operating system specific requirements:

- Section 3.2.1, "File Descriptor Requirements (Linux Systems)"
- Section 3.2.2, "Specific Requirements for Installation in Solaris Zones"

3.2.1 File Descriptor Requirements (Linux Systems)

The recommendation described in this section affects Linux systems only. All other supported platforms are not impacted.

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 by default 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 an Oracle Berkeley Java Edition 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
   ```

3.2.2 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.

3.3 Certified Languages

Oracle Unified Directory 11*g* Release 2 (11.1.2.3) 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.

4 Software Environment Limitations and Recommendations

The Oracle Unified Directory 11*g* Release 2 (11.1.2.3) 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 Installing Oracle Unified Directory*.

This section describes the following topics:

4.1 Oracle Unified Directory 11g Release 2 (11.1.2.3) Limitations

This section lists the limitations of Oracle Unified Directory 11*g* Release 2 (11.1.2.3). They are as follows:

- The Oracle Unified Directory directory server provides full LDAP v3 support, except for alias dereferencing, and limited support for LDAPv2.
- For Enterprise User Security, Oracle Unified Directory is validated to store and manage users and groups locally, and also for proxying to other external directory servers. The list of supported external directory servers is documented in the certification matrix. To view the certification matrix:
  1. Access the Oracle Fusion Middleware Supported System Configurations landing page:

     http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-certification-100350.html
  2. Scroll down to System Requirements and Supported Platforms for Oracle Identity and Access Management 11*g* Release 2 (11.1.2.3.0).
  3. Click the *xls* link to view the certification matrix and then click the **Interop** tab for the list of supported external directory servers.
- Oracle Unified Directory Server in proxy mode provides the best search performance when the search queries ask for the specific required attributes (rather than all the attributes) of an entry.

4.2 Oracle Unified Directory Software Recommendations

This section lists the recommendations for using Oracle Unified Directory 11*g* Release 2 (11.1.2.3). 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 Installing 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.

5 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 (11.1.2.3) core server at the time of this release.

5.1 (Bug 20593163) The command `start-ds --upgrade` fails if the server already has a `passwordexpirationtime` virtual attribute

If you upgrade an instance of Oracle Unified Directory from 11g R2 PS1 or 11g R2PS2 to 11g R2PS3 that contains `passwordExpirationTime` virtual attribute (`"cn=Password Expiration Time,cn=Virtual Attributes,cn=config"`), then the `start-ds --upgrade` command might throw the following error message:

```
"Patch from earlier OUD version to current version failed: The entry cn=Password
Expiration Time,cn=Virtual Attributes,cn=config cannot be added because an entry
with that name already exists"
```

This error occurs because the server already contains the `passwordExpirationTime` virtual attribute.

Workaround

Ignore the warning and restart the server.

You can also apply the workaround, which is to remove the password expiration configuration before running the upgrade. For more information, see "Configuring Virtual Attributes Using dsconfig" in *Administering Oracle Unified Directory*.

5.2 (Bug 23215822) Attribute Value Returned Not In Mixed Case If RDN Value

When you upgrade from 11.1.2.2.0 to 11.1.2.3.0, case sensitivity of attribute value might be lost due to the default behavior of the compact-encoding feature in 11.1.2.3.0.

Workaround

You can retain case sensitive values by setting the value of compact-encoding flag to false right before the upgrade. See "Retaining Case Sensitivity in Attributes During Upgrade" in Administering Oracle Unified Directory.

5.3 (Bug 20235234) OUD-Setup, ODSM and manage-suffix are missing some configuration changes to properly integrate with EUS

When manage-suffix is used to integrate a suffix with EUS, the following configuration changes are missing:

- The password storage scheme in the default password policy update
- The password storage scheme in the Import password policy plug-in update
- The cipher suites in the LDAPS connection handlers update

Workaround

'If you have configured a suffix with manage-suffix to integrate with EUS, run the following command-lines to update the password storage scheme configuration and the LDAP connection handler cipher suite configuration:

```
<OUD_INSTANCE_ROOT>/bin/dsconfig set-password-policy-prop \
          --policy-name Default\ Password\ Policy \
          --set allow-pre-encoded-passwords:true \
          --set default-password-storage-scheme:Salted\ SHA-1 \
          --hostname <host name> \
          --port <admin port> \
          --trustAll \
```

```
          --bindDN cn=Directory\ Manager \
          --bindPasswordFile <file containing directory manager password> \
          --no-prompt

<OUD_INSTANCE_ROOT>/bin/dsconfig set-plugin-prop \
          --plugin-name Password\ Policy\ Import \
          --set default-auth-password-storage-scheme:Salted\ SHA-1 \
          --set default-user-password-storage-scheme:Salted\ SHA-1 \
          --hostname <host name> \
          --port <admin port> \
          --trustAll \
          --bindDN cn=Directory\ Manager \
          --bindPasswordFile <file containing directory manager password> \
          --no-prompt
```

The configuration of each of the LDAPS connection handlers must also be updated. If the cipher has not been modified, run the following:

```
<OUD_INSTANCE_ROOT>/bin/dsconfig set-connection-handler-prop \
          --handler-name LDAPS\ Connection\ Handler \
          --add ssl-cipher-suite:jvm \
          --add ssl-cipher-suite:SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA \
          --add ssl-cipher-suite:SSL_DH_anon_EXPORT_WITH_RC4_40_MD5 \
          --add ssl-cipher-suite:SSL_DH_anon_WITH_3DES_EDE_CBC_SHA \
          --add ssl-cipher-suite:SSL_DH_anon_WITH_DES_CBC_SHA \
          --add ssl-cipher-suite:SSL_DH_anon_WITH_RC4_128_MD5 \
          --hostname <host name> \
          --port <admin port> \
          --trustAll \
          --bindDN cn=Directory\ Manager \
          --bindPasswordFile <file containing directory manager password> \
          --no-prompt
```

If you have modified the cipher suite configuration (for example: if you have configured other suites than the one provided by the JVM), run the following instead:

```
<OUD_INSTANCE_ROOT>/bin/dsconfig set-connection-handler-prop \
          --handler-name LDAPS\ Connection\ Handler \
          --add ssl-cipher-suite:SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA \
          --add ssl-cipher-suite:SSL_DH_anon_EXPORT_WITH_RC4_40_MD5 \
          --add ssl-cipher-suite:SSL_DH_anon_WITH_3DES_EDE_CBC_SHA \
          --add ssl-cipher-suite:SSL_DH_anon_WITH_DES_CBC_SHA \
          --add ssl-cipher-suite:SSL_DH_anon_WITH_RC4_128_MD5 \
          --hostname <host name> \
          --port <admin port> \
          --trustAll \
          --bindDN cn=Directory\ Manager \
          --bindPasswordFile <file containing directory manager password> \
          --no-prompt
```

5.4 (Bug 20109035) OUD upgrade fails to set the purging flag in the ds-sync-hist index

When the `ds-sync-hist` flag of the `ds-cfg-purging` is set to false, the OUD upgrade 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
```

5.5 (Bug 19786556) During modification of a large static group, the administrative limit might be exceeded

Misleading additional information occurs when a static large group is modified.

Workaround

Increasing the `member-lookthrough-limit` property. For more information, see "Managing Static Groups With More Than 100,000 Members" in *Administering Oracle Unified Directory*.

5.6 (Bug 19778292) The dsreplication initialize-all command fails

When you run the `dsreplication initialize-all` command, a failure can occur if one of the remote servers to initialize is stopped or is too slow.

Workaround

Rerun the `dsreplication initialize-all` command.

5.7 (Bug 19767906) ECL changes are delayed by the clock difference between servers in topology

Although there are two servers in the replication topology, results are returned from one server only. This error occurs during data transfer between the replication servers.

Workaround

There is currently no workaround for this issue.

5.8 (Bug 19260923) Using the signal SIGSTOP causes failures

When you use the signal SIGSTOP to pause the server, it can disable the backend upon using SIGSCONT to resume server processing. This problem occurs because SIGSTOP is not supported by OUD.

Workaround

Set BDB JE latch timeout to a duration longer than the duration between SIGSTOP and SIGCONT. The following is an example: `dsconfig set-workflow-element-prop --add je-property:je.env.latchTimeout="12 h"`

5.9 (Bug 18837001) The commands dsreplication initialize-all and dsreplication initialize freeze

When initialization is launched in a replicating topology, `dsreplication initialize-all` and `dsreplication initialize` commands, hang after sending a few entries. This occurs during processing.

Workaround

Rerun the commands.

5.10 (Bug 17874888) Removing the data-sync privilege for a user removes all privileges for that user

The data-sync privilege was not an operational privilege and consequently the OUD server does not recognize this 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

All references to this privilege in the OUD server configuration should be removed. 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
```

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

When you set up 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 and in the directories below the instance path (notably on the directory containing the database, by default called 'db').

5.12 (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.

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

When using the Oracle Directory Server Enterprise Edition Console 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.

5.14 (Bug 17689711) Enabling the changelog for a suffix on two servers will unexpectedly enable replication on the suffix

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.

5.15 (Bug 17409345) ldapcompare Does Not Work With RDBMS Virtualization

When comparing attribute values using `ldapcompare`, an error occurs because `ldapcompare` is not supported in this release.

Workaround

There is currently no workaround for this issue because `ldapcompare` is not supported in this release.

5.16 (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.

5.17 (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`.

5.18 (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 Certification" in *Installing Oracle Unified Directory*.

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

The messages and Help for `oudCopyConfig`, `oudExtractMovePlan`, and `oudPasteConfig` command-line tools of Oracle Unified Directory are only available in English.

Workaround

There is currently no workaround for this issue.

5.20 (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
```

5.21 (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.

5.22 (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
```

5.23 (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.

5.24 (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.

5.25 (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.

5.26 (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.

5.27 (Bug 11869296) Cleaning process does not end

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

Workaround

Configure a larger database cache. For more information, see "Tuning the Server Configuration" in *Oracle Fusion Middleware Administering Oracle Unified Directory.*

5.28 (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\jdk1.7
```

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

5.29 (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 Administering Oracle Unified Directory*.

6 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 (OUD) 11*g* Release 2 (11.1.2.3) release.

> **Note:** If Oracle Unified Directory has recently been updated, you might encounter a problem when you try to invoke ODSM. During an Oracle Unified Directory update operation, ODSM is also updated, and the ODSM URL can change. This problem usually occurs if you used your browser to invoke the earlier version of ODSM.
>
> Therefore, to invoke the updated version of ODSM, first clear your browser's cache and cookies.

6.1 (Bug 20113230) When replication is disabled a problem occurs

When ODSM is used to disable replication in a server by first disabling the replicated suffix and then the replication server, `dsreplication` enable fails when an attempt is made to add a new server to that topology.

Workaround

Disable the replication on the server by running following `dsreplication` command-line tool:

```
$ bin/dsreplication disable --disableAll
```

6.2 (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.

6.3 (Bug 18325609) LDAP error code 21

The error, LDAP: "error code 21- an attempt to modify an ACI attribute type in the entry dc-example, dc-com failed...." occurs when the creation of a new ACI in OUD with ODSM fails.

Workaround

In the text editor view, change the ACI bind rule Boolean operator value from "null" to "AND".

6.4 (Bug 18658519) Paging results in ODSM are not consistent

When using the Advanced Search paging in ODSM with the page results set to 5, the results remain the same when paging. When the results per page is set to 4, the problem does not occur.

Workaround

Do not set the page results to 5.

6.5 (Bugs 18789805/18915580/18905879/18884612/18874750) Modification Issues with JOIN Workflow Element

The results of modification of certain elements and parameters in JOIN Workflow Element in ODSM are not saved.

The list of parameters that are not saved are:

- "Attribute Storage", "Attribute Retrieval" for both Primary and Secondary Participant
- join suffix value
- join condition
- bind priority in the Participant Relations
- LDAP operations

Workaround

Use dsconfig to do the modification.

6.6 (Bug 18871434) Join DN attribute does not return in Advanced Search in ODSM

In ODSM, query using advanced search does not return the Join DN attribute. Using ldapsearch, the search returns the join dn attribute.

Workaround

Use ldapsearch to get the Join DN attribute.

6.7 (Bug 19028533) Adv Search: Issue with Search in pick attributes table

On the Advanced Search Page, the search operation on the Attribute picker window for the "Fetched Attributes" and "Sort Results On" sections, returns error: "An unresolvable error has occurred. Contact your administrator for more information."

Workaround

Manually select the attribute by scrolling down the Select Attribute table.

6.8 (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.

6.9 (Bug 17262682) Default browser settings may not allow ODSM URL to be accessible on Windows 2008 R2

After installing OUD and ODSM on Windows 2008 R2, 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.

6.10 (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 --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
```

6.11 (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.

6.12 (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.

6.13 (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.

7 Documentation Errata

This section contains the following documentation errata for The Oracle Fusion Middleware Configuration Reference for Oracle Unified Directory.

7.1 (Bug 20511374) Free Disk Space Log Retention Policy page refers to Java 6

In the Free Disk Space Log Retention Policy page, it states "This policy is only available on Java 6." The correct statement is: "This policy is only available with Java 7." Other references to Java 6 in this guide should also refer to Java 7.

For the specific versions of Java 7 supported by Oracle Unified Directory, check the certification matrix in Section 3, "System Requirements and Specifications."

8 General Issues and Workarounds

This section describes general issues and workarounds.

8.1 Java Runtime Environment Has SSLv3 Disabled By Default

Starting with JDK 8u31, JDK 7u75, and JDK 6u91, the Java Runtime Environment has SSLv3 disabled by default. For more information about this change, see http://www.oracle.com/technetwork/java/javase/documentation/cve-2014-3566-2342133.html

If you apply any of these Java updates, then any attempt to connect to Oracle Unified Directory with SSLv3 will fail.

Workaround

To solve this issue, configure the client LDAP application to use a different protocol. You may need to check whether any fixes are available that enable your client LDAP application to use a different protocol.

9 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 that have purchased support 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.

Oracle® Fusion Middleware Release Notes for Oracle Unified Directory, 11*g* Release 2 (11.1.2.3)
E55519-02