Oracle® Fusion Middleware

Release Notes for Oracle Identity Management

14c (14.1.2.1.0)
G10481-04
July 2025

Oracle Fusion Middleware Release Notes for Oracle Identity Management, 14c (14.1.2.1.0)

G10481-04

Primary Author: Oracle Corporation

Contents

4 Oracle Identity Governance

5 Oracle Unified Directory

6 Oracle Internet Directory

Preface

This preface includes the following sections:

Audience

This document is intended for users of Oracle Identity Management 14*c* (14.1.2.1.0).

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.

Conventions

The following text conventions are used in this document:

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

Related Documents

For more information, see the following resources:

- Oracle Fusion Middleware Documentation

This contains documentation for all Oracle Fusion Middleware 14*c* products.

- Oracle Technology Network

  This site contains additional documentation that is not included as part of the documentation libraries.

1
Introduction

Topics

1.1 Latest Release Information

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.

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

1.2 Purpose of this Document

This document contains the release information for Oracle Identity Management 14*c* (14.1.2.1.0). It describes differences between Oracle Identity Management and its documented functionality. Oracle recommends you review its contents before installing, or working with the product.

1.3 System Requirements and Specifications

Oracle Fusion Middleware installation and configuration will not complete successfully unless users meet the hardware and software prerequisite requirements before installation. For more information, see Oracle Fusion Middleware System Requirements and Specifications.

> **Note:**
>
> Fusion Middleware (FMW) is an essential infrastructure component for the IDM product.

1.4 Certification Information

To see versions of platforms and related software for which Oracle Identity Management is certified and supported, go to Oracle Fusion Middleware Supported System Configurations.

1.5 Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support at https://support.oracle.com.

2

What's New in Oracle Identity Management 14c (14.1.2.1.0)

This topic lists the new features for all the products in Oracle Identity Management Release 14*c* (14.1.2.1.0).

Topics

2.1 What's New in Oracle Access Management

Oracle Access Management 14c (14.1.2.1.0) includes the following new features and enhancements:

- **JDK Upgrade**: Oracle Access Management 14c (14.1.2.1.0) is certified for use with JDK 17 and JDK 21, which introduces new features, optimizations, and bug fixes enhancing the overall performance and stability.
- **Deprecating TLSv1.1**: Support for TLSv1.1 and earlier versions has been discontinued. For secure communication in Oracle Access Management, TLSv1.3 is the preferred protocol.
- **Deprecating SIMPLE Mode**: Support for SIMPLE mode communication with access manager has been discontinued.
- **Rules Evaluation**: Rules are now evaluated using GraalVM, replacing Jython. The behavior remains unchanged.
- **Disable Secure Mode**: For new installation, disable the secured mode domain by selecting the **Disable Secure Mode** check-box.

2.2 What's New in Oracle Identity Governance

Oracle Identity Governance (OIG) 14c (14.1.2.1.0) has the following key new features:

- **JDK Upgrade**: Oracle Identity Governance 14c (14.1.2.1.0) is certified for use with JDK 17 and JDK 21, which introduces new features, optimizations, and bug fixes enhancing the overall performance and stability.
- **FMW Upgrade**: OIG 14.1.2.1.0 is based on the latest FMW version 14.1.2.0.0, which has new security updates and performance optimizations.
- **OJET Uptake**: UI Screens based on OJET now use the version 17.1.0 with redwood theme, providing a fresh look to such UI.

- **JCS Uptake**: Cache has been replaced by JCS which has better distributed caching support, and more advanced memory management.
- **Third Party Software Upgrade**: OIG 14.1.2.1.0 uses the latest and most secure version of third party libraries which make the software more secure.
- **IDS Uptake**: Instead of User/Role API, OIG now uses IDS which is better suited for large enterprises and is optimized for high performance authentication.
- **Disable Secure Mode**: For new installation, disable the secured mode domain by selecting the **Disable Secure Mode** check-box.
- **Accessing the New Reconciliation Page**: The reconciliation page UI has been moved from the System Administrator Console to the Self-Service Console, and a new OJET-based interface is now available under **Manage > System Configuration > Reconciliation**.

2.3 What's New in Oracle Unified Directory

Oracle Unified Directory 14*c* (14.1.2.1.0) has the following key features:

- **JDK Upgrade**: Oracle Unified Directory 14c (14.1.2.1.0) is certified for use with JDK 17 and JDK 21, which introduces new features, optimizations, and bug fixes enhancing the overall performance and stability.
- **Berkeley Database Java Edition Upgrade:** Oracle Unified Directory uses Berkeley Database Java Edition for storage and retrieval purposes of OUD. The Berkeley Database Java Edition has been upgraded to version 7.5.18 providing improved functionality and better performance.
- **Deprecating TLS 1.1**: Support for TLS 1.1 and earlier versions has been discontinued. Oracle Unified Directory now requires TLS 1.2 or TLS 1.3 for secure communication.
- **Support for PKCS12 as Default Keystore**: Self-signed certificates are now stored in PKCS12 format by default, providing stronger encryption and improved compatibility. Oracle recommends that you switch the keystore format of the existing security configuration to PKCS12, which is an industry-standard format.
- **Disable Secure Mode**: For new installation, disable the secured mode domain by selecting the **Disable Secure Mode** check-box.

2.4 What's New in Oracle Internet Directory

Oracle Internet Directory 14*c* (14.1.2.1.0) has the following new features:

- **JDK Upgrade**: Oracle Internet Directory 14c (14.1.2.1.0) is certified for use with JDK 17 and JDK 21, which introduces new features, optimizations, and bug fixes enhancing the overall performance and stability.
- **Deprecating TLS 1.1**: Support for TLS 1.1 and earlier versions has been discontinued. Oracle Internet Directory now requires TLS 1.2 or TLS 1.3 for secure communication.
- **Disable Secure Mode**: For new installation, disable the secured mode domain by selecting the **Disable Secure Mode** check-box.

3
Oracle Access Management

Known issues and workarounds for Oracle Access Management include general issues and configuration issues.

Topics

> **Note:**
>
> See What's New in Oracle Access Management for information about new features in this release of Oracle Access Management.

3.1 Access Management Known Issues and Workarounds

This topic describes known issues and workaround for Oracle Access Management. It includes the following topics:

3.1.1 Takes time to propagate a policy or any metadata change

Issue

Set the password policy option to "Disallow previous passwords" and create a new password using the previously used password. The password can still be created.

Workaround

When you perform any change to the policy, it takes time to propagate across the OAM cluster. You should wait for a minimum of 60 seconds or more if the network is slow for the changes to take effect. It is recommended that the changes be made when the OAM servers are offline

3.1.2 User name field in SME UI is case sensitive

Issue

OAM console based session management search is case sensitive.

3.1.3 Exception occurs while using OAM Access Tester Tool

Issue

In OAM Access Tester tool, after entering sever connection details and clicking on **Connect** button, the connection will be established but with the following exception.

In Access Tester Console:

```
SEVERE: Server reported that incorrect NAP version is being used, while
client attempted to communicate using NAP version 5. See server log for more
information.
```

Stack trace in Server Logs:

```
<Error> <oracle.oam.proxy.oam> <OAM-04020> <Exception encountered while
processing the request message for agent {0} at IP {1} Request message
{2} :oracle.security.am.proxy.oam.requesthandler.OAMProxyException: Partner:
TestWebgate is registered with version 11.0.0.0. Runtime version of agent is
different: 11.* .Agent will not be able to communicate with the server
at
oracle.security.am.proxy.oam.requesthandler.ObAAAServiceServer.getClientAuthen
tInfo(ObAAAServiceServer.java:159)
at
oracle.security.am.proxy.oam.requesthandler.RequestHandler.ObAuthenReqChalleng
eHandler(RequestHandler.java:566)
at
oracle.security.am.proxy.oam.requesthandler.RequestHandler.handleRequest(Reque
stHandler.java:229)
at
oracle.security.am.proxy.oam.requesthandler.RequestHandler.handleMessage(Reque
stHandler.java:180)
at
oracle.security.am.proxy.oam.requesthandler.ControllerMessageBean.getResponseM
essage(ControllerMessageBean.java:94)
at
oracle.security.am.proxy.oam.requesthandler.ControllerMessageBean_eo7ylc_MDOIm
pl.__WL_invoke(Unknown Source)
at
weblogic.ejb.container.internal.MessageDrivenLocalObject.invoke(MessageDrivenL
ocalObject.java:127)
at
oracle.security.am.proxy.oam.requesthandler.ControllerMessageBean_eo7ylc_MDOIm
pl.getResponseMessage(Unknown Source)
at
oracle.security.am.proxy.oam.mina.ObClientToProxyHandler.getResponse(ObClientT
oProxyHandler.java:316)
at
oracle.security.am.proxy.oam.mina.ObClientToProxyHandler.messageReceived(ObCli
entToProxyHandler.java:270)
at
org.apache.mina.common.DefaultIoFilterChain$TailFilter.messageReceived(Default
IoFilterChain.java:743)
at
```

```
org.apache.mina.common.DefaultIoFilterChain.callNextMessageReceived(DefaultIoF
ilterChain.java:405)
at
org.apache.mina.common.DefaultIoFilterChain.access$1200(DefaultIoFilterChain.j
ava:40)
at
org.apache.mina.common.DefaultIoFilterChain$EntryImpl$1.messageReceived(Defaul
tIoFilterChain.java:823)
at org.apache.mina.common.IoFilterEvent.fire(IoFilterEvent.java:54)
at org.apache.mina.common.IoEvent.run(IoEvent.java:62)
at
oracle.security.am.proxy.oam.mina.CommonJWorkImpl.run(CommonJWorkImpl.java:85)
at
weblogic.work.j2ee.J2EEWorkManager$WorkWithListener.run(J2EEWorkManager.java:2
09)
at
weblogic.invocation.ComponentInvocationContextManager._runAs(ComponentInvocati
onContextManager.java:352)
at
weblogic.invocation.ComponentInvocationContextManager.runAs(ComponentInvocatio
nContextManager.java:337)
at
weblogic.work.LivePartitionUtility.doRunWorkUnderContext(LivePartitionUtility.
java:57)
at
weblogic.work.PartitionUtility.runWorkUnderContext(PartitionUtility.java:41)
at
weblogic.work.SelfTuningWorkManagerImpl.runWorkUnderContext(SelfTuningWorkMana
gerImpl.java:644)
at weblogic.work.ExecuteThread.execute(ExecuteThread.java:415)
at weblogic.work.ExecuteThread.run(ExecuteThread.java:355)
>
```

> **Note:**
>
> The above exception will be seen while using Access Tester. Access Tester will try to connect with NAP version 5, then with NAP version 4 and followed by NAP version 3 if the former does not work. But, there is no impact on the functionality.

3.2 Access Management Console Issues

This topic describes Console issues and workaround for Oracle Access Management (Access Manager). It includes the following topic:

- OOB OAM console logout does not work

3.2.1 OOB OAM console logout does not work

Issue

Till R2PS3, IAMSuiteAgent was the OOB agent protecting the OAM console. From 12c PS3 onwards, OAM console can be protected using a webgate agent.

Workaround

Close OAM console instead of logout.

Server side session will not be created when OAM console accesses OOB. As per EDG (Enterprise Development Guide), it is recommended to protect OAM console using a webgate agent.

3.3 Features Not Supported in Access Manager

This section provides a list of features that are not supported in Access Manager releases.

- Features Not Supported in Access Manager 14.1.2.1.0

3.3.1 Features Not Supported in Access Manager 14.1.2.1.0

The following table lists the features that will be unsupported from OAM 14.1.2.1.0.

- Support for SIMPLE mode communication with access manager is no longer available.

4

Oracle Identity Governance

Known issues and workarounds for Oracle Identity Governance include general issues and issues related to multi-language support.

Topics

> **Note:**
>
> See What's New in Oracle Identity Governance for information about new features in this release of Oracle Identity Governance.

4.1 General Issues and Workarounds

This section describes the general issues and workarounds in this release of Oracle Identity Governance.

4.1.1 The Request for Others Option is Available for All Users

Issue

When you click the **Request Access** tile in the **Self Service** tab of Oracle Identity Self Service, the **Request for Others** option should be enabled only for authorized users and managers. However, the **Request for Others** option is enabled for all users irrespective of authorization.

4.1.2 Session Time-out Warning Displayed When Using the Deployment Manager

Issue

When using the new UIs such as Deployment Manager, Resource History, Manage Connector, IT Resource or Application Instance in Identity Console using Oracle JET, a session time-out warning message is displayed although the system is not idle.

Currently, there is no workaround for this issue. Click **OK** on the warning message box and continue.

4.1.3 LDAP Synchronization Not Supported

Issue

LDAP synchronization, or integration between Oracle Identity Governance (OIG) and Oracle Access Manager (OAM) by using the IDMConfigTool is not supported in Oracle Identity Governance 12c (12.1.4.0) onwards.

Oracle Identity Governance 12c (12.2.1.3.1) release onwards, OAM-OIG integration using LDAP Connectors is supported.

Workaround

If you have upgraded from Release 11.1.2.3 to Release 12.2.1.3, then you can continue with LDAP synchronization, as described in Enabling LDAP Synchronization in Oracle Identity Manager in *Integration Guide for Oracle Identity Management Suite* for Release 11.1.2.3.

4.1.4 Logo Not Displayed in Certification Reports

Issue

When you log in to Oracle Identity Self Service and view certification reports,the logo is displayed in the PDF, Excel, and RTF formats of the report. However, the logo is not displayed in the HTML, Excel 2000, and CSV formats of the report.

Similarly, when you log in to Oracle BI Publisher Enterprise and view certification reports, the logo is displayed in the PDF, Excel, and RTF formats of the report. However, the logo is not displayed in the HTML, Excel 2000, and CSV formats of the report.

4.1.5 Pending Request Approval Fails

Issue

In a clustered deployment of Oracle Identity Governance, when a node fail over occurs, clicking **Approve** on the Request Approval page throws an exception, and displays `404 Page Not Found` on the page. The exception is:

```
<Mar 11, 2019 3:03:49,288 AM PDT> <Error> <Cluster> <BEA-003144> <All session
objects should be serializable to replicate. Check the objects in the
session. Failed to replicate a non-serializable object in context /identity.
java.rmi.UnmarshalException: error unmarshalling arguments; nested exception
```

```
is:
java.io.InvalidClassException: filter status: REJECTED
at weblogic.utils.StackTraceDisabled.unknownMethod()
Caused By: java.io.InvalidClassException: filter status: REJECTED
at weblogic.utils.StackTraceDisabled.unknownMethod()
>
<Mar 11, 2019 3:03:49,909 AM PDT> <Warning>
<oracle.adfinternal.view.faces.renderkit.rich.RegionRenderer>
<ADF_FACES-60099> <The region component with id: pt1:_d_reg:region2 has
detected a page fragment with multiple root components. Fragments with more
than one root component may not display correctly in a region and may have a
negative impact on performance. It is recommended that you restructure the
page fragment to have a single root component.>
<Mar 11, 2019 3:03:50,175 AM PDT> <Error> <Cluster> <BEA-003144> <All session
objects should be serializable to replicate. Check the objects in the
session. Failed to replicate a non-serializable object in context /identity.
java.rmi.UnmarshalException: error unmarshalling arguments; nested exception
is:
java.io.InvalidClassException: filter status: REJECTED
at weblogic.utils.StackTraceDisabled.unknownMethod()
Caused By: java.io.InvalidClassException: filter status: REJECTED
at weblogic.utils.StackTraceDisabled.unknownMethod()
```

Workaround

The issue can be resolved by updating the `setDomainEnv.sh` file with the following Java property in each node of the cluster, and then starting the WebLogic server:

```
-Dweblogic.oif.serialFilter=maxdepth=250
```

4.1.6 Duplicate Entries Are Not Allowed in Lookups

Issue

You can add duplicate entries in Lookups by using the Design Console without encountering any errors. But when duplicate entries are added to Lookups by using the Identity System Administration, then the following pop-up error is displayed:

```
JBO-oracle.iam.ui.common.model.lookupcode.lookup.entity.EditLookupsEO_RULE1: Each Lookup
must have a unique key (Lookup Type, Lookup Code).
```

The error is generated because duplicate entries are not allowed in Lookups.

4.1.7 Change Indicator for Child Table Modification in a Disconnected Application Instance Not Displayed for Manual Fulfillment Task

In a disconnected application instance, the change indicator for child table modification is not displayed for manual fulfillment task.

4.1.8 Default Session Timeout

Issue

The default session timeout for Identity Self Service and Identity System Administration is set to 10 minutes.

The default session timeout is set by the following entry in the `web.xml` file:

```
<session-config>
        <session-timeout>10</session-timeout>
</session-config>
```

For Identity Self Service: `$FMW_HOME/Oracle_IDM1/server/apps/oracle.iam.console.identity.self-service.ear /oracle.iam.console.identity.self-service.war/WEB-INF/web.xml`

For Identity System Administration: `$FMW_HOME/Oracle_IDM1/server/apps/oracle.iam.console.identity.sysadmin.ear/oracle.iam.console.identity.sysadmin.war/WEB-INF/web.xml`

However, changing the default session timeout value is not supported.

4.2 Configuration Issues and Workarounds

This section describes the configuration issues and workarounds in this release of Oracle Identity Governance.

- OIM-SOA Integration MBean Fails During Domain Configuration
- Error Stack in OIM Managed Server Logs
- Error in OIM Managed Server Logs

4.2.1 OIM-SOA Integration MBean Fails During Domain Configuration

Issue

When you configure the Oracle Identity Governance domain, run the `offlineconfigmanager.sh` script, and start all servers, and then invoke the OIM-SOA integration MBean, the following error is logged in the server logs:

```
<May 6, 2019 12:50:29,701 AM PDT> <Error> <com.oracle.coherence> <BEA-000000>
<2019-05-06 00:50:29.701/217214.494 Oracle Coherence GE 12.2.1.4.0 <Error>
(thread=Cluster, member=3): Received cluster heartbeat from the senior
Member(Id=1, Timestamp=2019-05-03 12:25:22.783, Address=10.248.121.88:25538,
MachineId=42905,
Location=site:example.com,machine:slc16oqj,process:30630,member:AdminServer,
 Role=WeblogicServer) that does not contain this Member(Id=3,
Timestamp=2019-05-03 12:30:58.275, Address=10.248.121.88:14080,
MachineId=42905,
Location=site:example.com,machine:slc16oqj,process:31978,member:oim_server1,
 Role=WeblogicServer); stopping cluster service.>

<May 6, 2019 12:50:29,753 AM PDT> <Warning> <Log Management> <BEA-170011>
<The LogBroadcaster on this server failed to broadcast log messages to the
Administration Server. The Administration Server may not be running. Message
broadcasts to the Administration Server will be disabled.>
```

Workaround

Make sure that date and time on the WebLogic host and database host are in sync. After making sure date and time are in sync, invoke `oimsoaintegrationmbean` again.

4.2.2 Error Stack in OIM Managed Server Logs

The following error stack is shown in OIM managed server logs:

```
Jul 17, 2019 12:35:03,548 AM PDT> <Error>
<oracle.adfinternal.view.page.editor.utils.ReflectionUtility> <WCS-16178>
<Error instantiating class -
oracle.adfdtinternal.view.faces.portlet.PortletDefinitionDTFactory>
<Jul 17, 2019 12:35:03,584 AM PDT> <Warning>
<oracle.adfinternal.view.faces.renderkit.rich.NavigationPaneRenderer>
<BEA-000000> <Warning: There are no items to render for this level>
<Jul 17, 2019 12:35:20,490 AM PDT> <Warning>
<oracle.iam.platform.kernel.impl> <IAM-0089999> <Kernel Information:
```

This is a benign error without any functional impact and can be ignored.

4.2.3 Error in OIM Managed Server Logs

The following error is shown in the OIM managed server logs:

```
"
<Aug 7, 2019 5:04:50,334 AM PDT> <Error> <XELLERATE.APIS> <BEA-000000>
<Class/Method:
tcITResourceInstanceOperationsBean/updateWithCredentialStoreData encounter
some problems: Parameter User Reservation Container not  present in
credential store. pls check for svr_key:1>
returning the ovd url value :
```

This is a benign error without any functional impact and can be ignored.

4.3 Multi-Language Support Issues and Workarounds

This section describes the multi-language support issues and workarounds in this release of Oracle Identity Governance.

- Locale Drop Down Not Translated for My Information and Modify User Pages
- Search Result Message in the Export Configuration Page Not Translated

4.3.1 Locale Drop Down Not Translated for My Information and Modify User Pages

Issue

The Locale list in the My Information page and Modify User page of Identity Self Service are not translated if the browser language is set to any one of the following:

- Arabic (ar)
- Hebrew (he)
- Danish (da)
- Czech (cs)
- Dutch (nl)
- Romanian (ro)
- Slovak (sk)
- Norwegian (no)
- Hungarian (hu)

4.3.2 Search Result Message in the Export Configuration Page Not Translated

Issue

When you perform a default search in the Export Configuration page of the Deployment Manager, the search result message is displayed only in English, and is not translated to other languages.

4.4 Features Not Supported in Oracle Identity Governance 14c (14.1.2.1.0)

The following features are not supported in this release:

Features Unsupported in 14.1.2.1.0	Description
Generic Technology Connector (GTC)	Generic Technology Connector for developing custom connectors is not supported in this release.
Segregation of Duties (SoD) using Oracle Application Access Controls Governor (OAACG)	SoD check with OAACG is not supported. In this release, SoD and audit violations are managed by using the Identity Audit feature of Oracle Identity Governance. See Managing Identity Audit in *Performing Self Service Tasks with Oracle Identity Governance*.

5

Oracle Unified Directory

Known issues and workarounds for Oracle Unified Directory include general issues and known issues related with Oracle Unified Directory, Oracle Unified Directory Services Manager, and related directory components.

Topics

> **Note:**
>
> - See What's New in Oracle Unified Directory for information about new features in this release of Oracle Unified Directory.

5.1 Oracle Unified Directory System Requirements and Specifications

You must read through 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 for your reference:

- Keep the following in mind during OUD installation:

  > **Note:**
  >
  > This applies only to collocated OUD installations and does not apply to standalone OUD 14.1.2.1.0 installations.

  – **Fresh OUD Installation:** Apply the 'Latest IDM 14.1.2.1.0 Stack Patch Bundle (April 2025 or later)' to the OUD 14.1.2.1.0 `ORACLE_HOME` before domain creation. For more information check Stack Patch Bundle (SPB) for Oracle Identity Management Products, Doc ID 2657920.2, at https://support.oracle.com. This applies only to collocated OUD installations and does not apply to standalone OUD 14.1.2.1.0 installations.

  – **Upgrade OUD Installation:**

Apply the "Latest IDM 14.1.2.1.0 Stack Patch Bundle (April 2025 or later)" to the OUD 14.1.2.1.0 `ORACLE_HOME` before performing the reconfiguration step. For more information check SPB for Oracle Identity Management Products, Doc ID 2657920.2, https://support.oracle.com.

Apply the one-off EM patch (search for Bug ID 37476292 at https://support.oracle.com) manually using OPatch to the OUD 14.1.2.1.0 `ORACLE_HOME` before performing the reconfiguration step.

- Checking the System Requirements for Oracle Unified Directory.

  This document provides information related to hardware and software requirements, minimum disk space and memory requirements, and required system libraries, packages, or patches when installing Oracle Unified Directory 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 14*c* (14.1.2.1.0).
  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 Oracle Unified Directory. This document always contains the latest information for a specific release.

- *Oracle® Fusion Middleware Installing Oracle Unified Directory 14c (14.1.2.1.0)*

  Planning the Oracle Unified Directory Installation contains pre-installation system notes and other information you should review prior to Oracle Unified Directory installation.

The following sections describe additional information specific to Oracle Unified Directory installation requirements:

- Hardware Requirements
- Software Requirements
- Certified Languages

5.1.1 Hardware Requirements

You must bear in mind the minimum hardware requirements for installation that are recommended for this release.

As a general guideline, the following hardware is recommended:

Table 5-1 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.

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, and Database Cache Options for Oracle Unified Directory 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.

5.1.2 Software Requirements

You must bear in mind the software requirements that are to be met before beginning the installation.

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.

You must ensure to resolve the following operating system specific requirements:

- File Descriptor Requirements (Linux Systems)
- Specific Requirements for Installation in Solaris Zones

5.1.2.1 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
   ```

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

5.1.2.2 Specific Requirements for Installation in Solaris Zones

This section describes the specific requirements for installation of Oracle Unified Directory on 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.

5.1.3 Certified Languages

You can find here the list of languages supported, called certified languages.

Oracle Unified Directory 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.

5.2 Software Environment Limitations and Recommendations

This section describes the limitations that might affect the initial deployment of your directory server.

The Oracle Unified Directory 14*c* (14.1.2.1.0) 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. See Configuring the JVM, Java, and Database Cache Options for Oracle Unified Directory in *Oracle Fusion Middleware Installing Oracle Unified Directory*.

This section describes the following topics:

- Software Recommendations

5.2.1 OUD 14c (14.1.2.1.0) Limitations

This section lists the limitations of Oracle Unified Directory 14*c* (14.1.2.1.0). 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. See Viewing the Certification Matrix in *Oracle Fusion Middleware Installing Oracle Unified Directory*.
- 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.

5.2.2 Viewing the Certification Matrix

This section describes the procedure to view 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 14*c* Release (14.1.2.1.0).
3. Click the *xls* link to view the certification matrix and then click the **Interop** tab for the list of supported external directory servers.

5.2.3 Software Recommendations

This section lists the recommendations for using Oracle Unified Directory.

The recommendations that are to be followed are:

- 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. See Configuring the JVM, Java, and Database Cache Options for Oracle Unified Directory 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.
- If you want to perform `isMemberOf` query for complex searches involving static groups, it is advisable to keep group membership and user entry under the same backend.

5.2.4 Deprecation of the Password Notification Change plug-in

Starting with Oracle Unified Directory 12c (12.2.1.4.0), the Password Notification Change plug-in (`oidpwdcn.dll`) is deprecated.

Oracle recommends that you replace this plug-in with the centrally managed users (CMU) feature provided by Oracle Database.

5.3 Oracle Unified Directory (OUD) Known Issues and Workarounds

The following sections describe known issues and limitations with the Oracle Unified Directory 14*c* (14.1.2.1.0) core server at the time of this release.

- (Bug 29964155) Unable to Find the System Component Details in the config.xml File
- PBKDF2WithHmacSHA512–based password storage schemes might fail due to JDK bug
- (Bug 20109035) OUD upgrade fails to set the purging flag in the ds-sync-hist index
- (Bug 19786556) During modification of a large static group, the administrative limit might be exceeded
- (Bug 19767906) ECL changes are delayed by the clock difference between servers in topology
- (Bug 19260923) Using the signal SIGSTOP causes failures
- (Bug 17874888) Removing the data-sync privilege for a user removes all privileges for that user
- (Bug 17797663) Pass-Through Authentication subject to limitations when configured with Kerberos authentication provider.
- (Bug 17689711) Enabling the changelog for a suffix on two servers will unexpectedly enable replication on the suffix
- (Bug 14772631) If an AddOutboundTransformation definition contains a dot, then a search request might fail
- (Bug 14080885) The moveplan interface does not have a field to update the path for keystore pin file
- (Bug 14652478) The runInstaller command fails to check for appropriate OS
- (Bug 14065106) Translation is not supported for some error message and online Help
- (Bug 14055062) If the value for parameter -j,--rootUserPasswordFile is provided as a relative path, commands fail
- (Bug 13996369) The gicadm command does not import a catalog
- (Bug 13965857) If you specify an alternative location for a cloned server instance, the cloned server instance is not completely configured
- (Bug 13954545) The ldapsearch.bat client incorrectly handles a trailing asterisk character
- (Bug 12291860) No SNMP trap is sent if the server is stopped using the stop-ds command with no credentials
- (Bug 12280658) The ModDN operation is not supported if DNs are indexed in the global index catalog (GIC)

- (Bug 12266690) Load balancing routes are deleted without warning
- (Bug 11718654) Error Occurs in Replicated Topology with a Heavy Workload

5.3.1 (Bug 29964155) Unable to Find the System Component Details in the config.xml File

Issue

If you update the node manager properties like username and password, the system component details in the `config.xml` file are deleted. This causes the OUD system component to fail while trying to start/stop the component using `stopComponent.sh`/`startComponent.sh`.

Workaround

Ensure that you do not update the node manager details after creating the system components.

5.3.2 PBKDF2WithHmacSHA512–based password storage schemes might fail due to JDK bug

Issue

If you are using the following password storage schemes that are based on PBKDF2WithHmacSHA512 algorithm, then you might experience unpredictable results. This problem occurs owing to an issue with JDK 8.

- `cn=PBKDF2 HMAC SHA-512,cn=Password Storage Schemes,cn=config`
- `cn=EUS PBKDF2 SHA-512,cn=Password Storage Schemes,cn=config`

If you are using the preceding schemes on a heavily-loaded server, then you might not be able to bind to Oracle Unified Directory.

Workaround

This issue is fixed in JDK 9. This fix has been backported to JDK 8. Oracle recommends that you to apply the JDK patch if you are using the preceding PBKDF2WithHmacSHA512–based password storage schemes in your configuration. For more information about applying this patch, you can contact My Oracle Support.

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

Issue

Bug Number: 20109035

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
```

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

Issue

Bug Number: 19786556

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

Workaround

Increasing the `member-lookthrough-limit` property. See Managing Static Groups With More Than 100,000 Members in *Oracle® Fusion Middleware Administering Oracle Unified Directory*.

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

Issue

Bug Number: 19767906

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.

5.3.6 (Bug 19260923) Using the signal SIGSTOP causes failures

Issue

Bug Number: 19260923

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"`

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

Issue

Bug Number: 17874888

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
```

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

Issue

Bug Number: 17797663

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.

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

Issue

Bug Number: 17689711

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.

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

Issue

Bug Number: 14772631

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.

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

Issue

Bug Number: 14080885

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`.

5.3.12 (Bug 14652478) The runInstaller command fails to check for appropriate OS

Issue

Bug Number: 14652478

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 Checking the System Requirements for Oracle Unified Directory in *Oracle® Fusion Middleware Installing Oracle Unified Directory*

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

Issue

Bug Number: 14065106

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.

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

Issue

Bug Number: 14055062

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
```

5.3.15 (Bug 13996369) The gicadm command does not import a catalog

Issue

Bug Number: 13996369

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

Workaround

Specify an absolute path to import a catalog.

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

Issue

Bug Number: 13965857

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
```

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

Issue

Bug Number: 13954545

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.

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

Issue

Bug Number: 12291860

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.

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

Issue

Bug Number: 12280658

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.

5.3.20 (Bug 12266690) Load balancing routes are deleted without warning

Issue

Bug Number: 12266690

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.

5.3.21 (Bug 11718654) Error Occurs in Replicated Topology with a Heavy Workload

Issue

Bug Number: 11718654

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. See Tuning the Server Configuration in *Oracle® Fusion Middleware Administering Oracle Unified Directory*.

5.4 Oracle Unified Directory Services Manager (Oracle Unified Directory Services Manager) Known Issues and Workarounds

The following sections describe known issues with Oracle Unified Directory Services Manager at the time of Oracle Unified Directory 14*c* (14.1.2.1.0) release.

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

This section describes the following known issues and workarounds:

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

Issue

Bug Number: 17582404

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.

5.4.2 (Bugs 18789805/18915580/18905879/18884612/18874750) Modification Issues with Join Workflow Element

Issue

Bug Number: 18789805/18915580/18905879/18884612/18874750

The results of modification of certain elements and parameters in JOIN Workflow Element in OUDSM 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.

5.4.3 (Bug 18871434) Join DN attribute does not return in Advanced Search in OUDSM

Issue

Bug Number: 18871434

In OUDSM, 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.

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

Issue

Bug Number: 19028533

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.

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

Issue

Bug Number: 17462792

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.

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

Issue

Bug Number: 17262682

After installing OUD and OUDSM on Windows 2008 R2, when you try to access the OUDSM URL, the message "Starting Oracle Directory Services Manager..." displays, but the OUDSM 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 OUDSM URL in the trusted sites.

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

5.4.7 (Bug 16946878) Alerts not sent as designed

Issue

Bug Number: 16946878

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
```

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

Issue

Bug Number: 16056177

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 the Data Browser tab.

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

Issue

Bug Number: 15928439

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

Workaround

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

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

Issue

Bug Number: 12363352

When you are in the screenreader mode, the Create, Apply, and Cancel buttons in the OUDSM 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.

5.5 Related Oracle Directory Components Known Issues and Workarounds

This section describes the known issues and its workarounds for Oracle Directory Integration Platform and Oracle Identity Directory Services.

Topics

5.5.1 Oracle Directory Integration Platform

Known issues and workarounds for Oracle Directory Integration Platform include general issues and configuration issues.

Topics

5.5.1.1 General Oracle Directory Integration Platform Issues and Workarounds

This section describes general issues and workarounds.

Topics

5.5.1.1.1 Enabling the Domain-Wide Administration Port on Oracle WebLogic Server Prevents use of the DIP Command Line Interface

Issue

Be aware that enabling the domain-wide administration port on any WebLogic server running Directory Integration Platform will prevent you from using the DIP command line interface using a standard administrator account. Entering DIP commands will result in an error similar to the following:

```
User: "weblogic", failed to be authenticated
```

Workaround

Administrators can still use the Enterprise Manager (EM) GUI to configure and manage Oracle Directory Integration Platform.

5.5.1.1.2 LDIF Files That Contain Non-ASCII Characters Will Cause the testProfile Command Option to Fail if the LDIF File has Native Encoding

Issue

When running DIP Tester from a command-line, the `manageSyncProfiles testProfile` command will fail if the `-ldiffile` option is specified and the LDIF file contains non-ASCII characters.

Workaround

Note that LDIF files with UTF-8 encoding are not impacted by this limitation. If an LDIF file containing multibyte characters cannot be saved with UTF-8 encoding, then use the following workaround:

1. From a command-line, add the entry using the `ldapadd` command and include the `-E` option to specify the locale. For the required command syntax, see ldapadd Command Reference in *Oracle Fusion Middleware Reference for Oracle Identity Management*.
2. Get the specific `changeNumber` for the last add operation.
3. Execute the `testProfile` command using the `changeNumber` from the previous step.

   For more information, see the section Running DIP Tester From the WLST Command-Line Interface in *Oracle Fusion Middleware Administering Oracle Directory Integration Platform*.

5.5.1.1.3 Running the testProfile Command with LDIF Files Option Fails in Advance Mode

Issue

When running DIP Tester from a command-line in advance mode, the `manageSyncProfiles testProfile` command will fail if the `-ldiffile` option is specified and may synchronize the wrong operation.

Workaround

To resolve this issue, run the `manageSyncProfile updatechgnum` command. See Running DIP Tester From the WLST Command-Line Interface in the *Oracle Fusion Middleware Administering Oracle Directory Integration Platform*.

5.5.1.1.4 Some Changes May Not Get Synchronized Due to Race Condition in Heavily-Loaded Source Directory

Issued

If the source directory is heavily-loaded, a race condition may occur where database commits cannot keep pace with updates to the `lastchangenumber`. If this race condition occurs, Oracle Directory Integration Platform may not be able to synchronize some of the changes.

> **Note:**
>
> This issue only occurs if you are using Oracle Internet Directory as the back-end directory.

Workaround

To resolve this issue, perform the following steps to enable database commits to keep pace with the `lastchangenumber`:

1. Increase the value of the synchronization profile's Scheduling Interval.
2. Control the number of times the search is performed on the source directory during a synchronization cycle by setting the `searchDeltaSize` parameter in the profile. Oracle suggests starting with a value of 10, then adjusting the value as needed.

5.5.1.1.5 manageSyncProfiles Utility Prompts for Connected Directory Password

Issue

When you run the `manageSyncProfiles` utility to synchronize with a database, the `manageSyncProfiles` register prompts for the connected directory password.

Workaround

Ensure that you specify the connected database password and not the directory password.

5.5.1.1.6 The Oracle Password Filter for Microsoft Active Directory Installation Screens Displays 11*g* Version

There is no impact to functionality and no user action is needed.

5.5.1.1.7 Resource Usage Charts will not be Displayed

The DIP home page does not display the resource usage charts in Oracle Directory Integration Platform 12c (12.2.1.3).

5.5.1.2 Oracle Directory Integration Platform Configuration Issues and Workarounds

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

- Specify the Service Name While Creating Synchronization Profiles
- If Oracle Internet Directory is the Back-End Directory then do not use localhost as Oracle Internet Directory Hostname When Configuring Oracle Directory Integration Platform
- You may Need to Restart the Directory Integration Platform After Running dipConfigurator Against Oracle Unified Directory
- When Configuring a Profile, you may Need to Scroll Past a Section of Whitespace to View Mapping Rules
- Specify the Host Name and Port Number for an Oracle RAC Database

5.5.1.2.1 Specify the Service Name While Creating Synchronization Profiles

When you create the synchronization profile, ensure that you specify the database service name and not the SID.

Examples:

To connect to a database, use the form `host:port:serviceName` for the `odip.profile.condirurl` connection detail property in a directory synchronization profile.

Specify the database service name for **Database Service ID** in the **Create Synchronization Profile** page in Oracle Enterprise Manager Fusion Middleware Control. See Creating Synchronization Profiles in *Oracle Fusion Middleware Administering Oracle Directory Integration Platform*.

5.5.1.2.2 If Oracle Internet Directory is the Back-End Directory then do not use localhost as Oracle Internet Directory Hostname When Configuring Oracle Directory Integration Platform

When configuring Oracle Directory Integration Platform against an existing Oracle Internet Directory using the Configuration Wizard, you must specify the hostname for Oracle Internet Directory using only its fully qualified domain name (such as `myhost.example.com`). Do not use `localhost` as the Oracle Internet Directory hostname even if Oracle Directory Integration Platform and Oracle Internet Directory are collocated on the same host.

If you use `localhost` as the Oracle Internet Directory hostname, you will not be able to start the Oracle WebLogic Managed Server hosting Oracle Directory Integration Platform.

5.5.1.2.3 You may Need to Restart the Directory Integration Platform After Running dipConfigurator Against Oracle Unified Directory

After running dipConfigurator against an Oracle Unified Directory (OUD) endpoint, if you are unable to open the Directory Integration Platform (DIP) UI in Enterprise Manger, stop and start DIP to fix the UI problem.

5.5.1.2.4 When Configuring a Profile, you may Need to Scroll Past a Section of Whitespace to View Mapping Rules

If you are using Internet Explorer to view the Directory Integration Platform (DIP) UI, you may need to scroll past a large blank space to see the profile mapping rules section. This issue is not known to affect other browsers.

5.5.1.2.5 Specify the Host Name and Port Number for an Oracle RAC Database

Issue

While configuring Oracle Directory Integration Platform for Oracle Internet Directory as the back-end directory, If you only specify the URL for the RAC database in the `dbconfig` file, then the following error messages appear:

```
Error occurred in configuring DataSource.
Error occurred in rolling back DataSource changes.
Error occurred in configuring DataSource.
Error occurred during DIP configuration Step - DataSourceConfigurationStep.
Error occurred in DIP configuration against OID as backend.
```

Workaround

To resolve this issue, specify the `URL`, `DB_HOST` , and `DB_PORT` for the Oracle RAC database in the `dbconfig` file.

5.5.1.3 Provisioning Issues

This section describes provisioning issues.

Topics

- Modification may not Propagate Using Interface Protocol (Inbound) Version 3.0
- Provisioning from Oracle Internet Directory (Back-End Directory) to an Application May Fail

5.5.1.3.1 Modification may not Propagate Using Interface Protocol (Inbound) Version 3.0

Issue

When an inbound provisioning profile with interface protocol version 3.0 is configured with Oracle Internet Directory (Back-End Directory), then modification fails to propagate.

Workaround

See https://support.oracle.com/.

5.5.1.3.2 Provisioning from Oracle Internet Directory (Back-End Directory) to an Application May Fail

Issue

If you delete a provisioning profile for Oracle Internet Directory, and recreate it with same name, then the provisioning from Oracle Internet Directory to an application may fail.

Workaround

To resolve this issue, create a provisioning profile and specify a new name.

For more information on creating a provisioning profile, see About manageProvProfiles Command in *Oracle Fusion Middleware Administering Oracle Directory Integration Platform*.

5.5.2 Oracle Identity Directory Services

Known issues and workarounds for Oracle Identity Directory Services include general issues and known issues related with Identity Directory Services (IDS).

Topics

- Oracle Identity Directory Services Documentation Changes

5.5.2.1 Oracle Identity Directory Services Documentation Changes

Identity Governance Framework introduced some behavioral changes in the 12c (12.2.1.3.0) release. This includes deprecated and desupported features and components.

Deprecated Chapters or Books

By deprecate, we mean that the feature is no longer being enhanced but is still supported for the full life of the 12c (12.2.1.3.0) release. By desupported, we mean that Oracle will no longer fix bugs related to that feature and may remove the code altogether. Where indicated, a deprecated feature may be desupported in a future major release.

From 12c (12.2.1.3.0) release onward, the User and Role API and the ArisID API features have been officially deprecated.

- From 12*c* (12.2.1.3.0) release onward, the following Javadocs were deprecated:
  - *Java API Reference for Identity Governance Framework IDXUserRole*
  - *Java API Reference for Identity Governance Framework UserRole*

  Oracle recommends the use of Identity Directory API. See *Oracle® Fusion Middleware Java API Reference for Identity Directory Services*.
- Deprecation of Using the ArisID API functionality from 12*c* (12.2.1.3.0) onward.

Oracle recommends that you use instead Identity Directory API from Identity Governance Framework and migrate usage to this framework. For information about this migration, see Migrating to Identity Directory API.

6
Oracle Internet Directory

This chapter describes issues associated with Oracle Internet Directory. It includes the following topics:

Topics

6.1 Oracle Internet Directory System Requirements and Specifications

You must read through the system requirements and certification documents to ensure that your environment meets the minimum installation requirements for the products you are installing.

Important Considerations for OID 14.1.2.1.0 Installation:

The following guidelines apply only to the standalone OID 14.1.2.1.0 upgrade installation scenario.

- **Upgrade OID Installation:**
  Apply the one-off UA patch (search for Bug ID 37465410 at https://support.oracle.com) manually using OPatch to the OID 14.1.2.1.0 `ORACLE_HOME` before performing UA READINESS for a standalone OID domain.

The following guidelines apply only to collocated 14.1.2.1.0 OID installations and does not apply to standalone OID 14.1.2.1.0 installations.

- **Fresh OID Installation:**
  - Apply the 'Latest IDM 14.1.2.1.0 Stack Patch Bundle (April 2025 or later)' to the OID 14.1.2.1.0 `ORACLE_HOME` before domain creation. For more information check SPB for Oracle Identity Management Products, Doc ID 2657920.2, at https://support.oracle.com.
- **Upgrade OID Installation:**
  - Apply the 'Latest IDM 14.1.2.1.0 Stack Patch Bundle (April 2025 or later)' to the OID 14.1.2.1.0 `ORACLE_HOME` before performing the reconfiguration step. For more information check SPB for Oracle Identity Management Products, Doc ID 2657920.2, at https://support.oracle.com.
  - Apply the one-off EM patch (search for Bug ID 37476292 at https://support.oracle.com) manually using OPatch to the OID 14.1.2.1.0 `ORACLE_HOME` before performing the reconfiguration step.

6.2 General Oracle Internet Directory Issues and Workarounds

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

6.2.1 (Bug 25875893) ODS Schema details not getting auto-filled using Schemas Option

Issue

When you are upgrading from 11g Release 1(11.1.1.9.0) in the Upgrade Assistant, if you select **All Schemas Used By a Domain** option, the schema details are not auto-populated in ODS Schemas screen.

Workaround

As a workaround, user has to manually provide ODS schema details such as Database Type, string etc.

6.2.2 (Bug 25814730) OID12*c*PS3: Startup fails because low system shared memory on Solaris

Issue

OID server startup fails on Solaris platforms due to low system shared memory.

Workaround

To fix this issue, you need to increase shared memory on Solaris system platform when DB is collocated. If you are installing only OID, then you need 1.5GB shared memory.

For example, as a root user, if you increase `project.max-shm-memory` to 12GB(from 8 GB), the OID instance is brought up.

```
prctl -n project.max-shm-memory -v 12gb -r -i project default
$ prctl -n project.max-shm-memory $$
process: 7423: bash

NAME    PRIVILEGE       VALUE    FLAG   ACTION                       RECIPIENT
project.max-locked-memory
        privileged      12.0GB      -   deny                             -
        system          16.0EB    max   deny                             -
```

6.2.3 (Bug 26564247)PS3 OID: Help link on ODSM URL does not work

Issue

When you login to ODSM and click on **Help**, help pages are not accessible.

Workaround

Though the help is not accessible via ODSM help, we can access the pages through OID document library. See Overview of Oracle Directory Service Manager

6.2.4 (Bug 19898973)Substring Filter Not Supported for Collective Attributes

Issue

Oracle Internet Directory does not provide support for substring filter for collective attributes. For instance, the following substring filter is not supported:

```
tenantguid=*234*
```

Workaround

However, the equality filter for instance, `tenantguid=12345` is supported for collective attributes.

6.2.5 (Bug 14079791) Search on rootDSE `lastchangenumber` Attribute Works For One Attribute At A Time

Issue

If you perform `ldapsearch` on rootDSE to fetch the `lastchangenumber` attribute along with other attributes, then `lastchangenumber` is not retrieved.

For instance, when you run the following command then `lastchangenumber` attribute is not retrieved:

```
ldapsearch -p port -D "cn=orcladmin" -w password -b "" -s base "objectclass=*"
changelog lastchangenumber
```

Workaround

The workaround for this problem is to perform `ldapsearch` on rootDSE only for `lastchangenumber` attribute as follows:

```
ldapsearch -p <port> -h <hostname> -b ' ' -s base '(objectclass=*)' lastchangenumber

lastchangenumber=4714
```

6.2.6 (Bug 17348090) Search with Filter Containing AND Operation of Collective Attributes Not Supported

Issue

When the search filter contains only collective attribute expressions, and an AND (&) operation is performed, then the server does not return expected results.

For example, if you run the following commands having collective attributes only, then if you run an AND operation, the server fails to return the desired result.

```
ldapsearch -b 'cn=u1,cn=collandbug' '&(description=coll1 desc)
(description=coll2 desc)' dn
```

Workaround

There is no workaround for this issue.

6.2.7 (Bug 18196425) ODSM Adds Fake Entries to the Chained Container and Displays Duplicate Entries During Export

Issue

In ODSM, when you set up server chaining with Oracle Directory Server Enterprise Edition (ODSEE) as the backend the following issues emerge:

- If you create an entry through ODSM, then ODSM pretends to add the entry to the remote server through chaining. However, the entry does not get added on the remote server, ODSEE.
- If you add the preceding entry directly to the remote backend, and navigate to the parent entry through the Data Explorer tab, and then export to LDIF the same entry, you will see duplicate entries.

Workaround

There is no workaround for this issue.

6.2.8 (Bug 18695967) ODSM Does Not Create Entry of Custom objectclass With Custom Mandatory Field

Issue

On the Schema tab, create a custom attribute and a custom objectclass, and also select custom attribute as indexed. Now, on the Data Browser tab if you create an entry of `objectclass="custom object class"` then it does not allow you to enter the mandatory value in the custom attribute field.

Workaround

There is no workaround for this issue.

6.2.9 (Bug 16964666) Cloned Oracle Internet Directory Instance Fails or Runs Slowly

Issue

In a cloned Oracle Internet Directory environment, undesired host names can cause errors, failures, or performance degradation.

This problem can occur when you clone an Oracle Internet Directory instance and the cloned target instance gets undesired host names from the source instance. Some of these hosts might be outside of a firewall or otherwise inaccessible to the target instance.

The cloned Oracle Internet Directory instance assumes it is in a clustered environment and tries to access the undesired hosts for notifications and other changes. However, the cloned instance cannot access some of the hosts and subsequently fails, returns errors, or runs slowly.

For example, this problem can occur during the following operations for a cloned Oracle Internet Directory target instance:

- Running the `faovmdeploy.sh createTopology` command to create an Oracle Virtual Machine (VM)
- Deploying Enterprise Manager agents in different Oracle Virtual Machines

Workaround

To fix this problem, remove the undesired host names from the cloned Oracle Internet Directory instance, as follows:

1. Set the required environment variables. For example:

```
export ORACLE_INSTANCE=/u01/oid/oid_inst
export ORACLE_HOME=/u01/oid/oid_home
export PATH=$ORACLE_HOME/bin:$ORACLE_INSTANCE/bin:$PATH
export TNS_ADMIN=$ORACLE_INSTANCE/config
```

2. Connect to the Oracle Database and delete the entries with the undesired Oracle Internet Directory host names. For example, in the following queries, substitute the undesired host name for *sourceHostname*:

```
sqlplus ods@oiddb
delete from ods_shm where nodename like '%sourceHostname%';
delete from ods_shm_key where nodename like '%sourceHostname%';
```

```
delete from ods_guardian where nodename like '%sourceHostname%';
delete from ods_process_status where hostname like '%sourceHostname%';
commit;
```

3. Stop and then restart the cloned Oracle Internet Directory component. For example:

```
opmnctl stopproc ias-component=oid1
opmnctl startproc ias-component=oid1
```

4. Find the `cn` entries with the undesired Oracle Internet Directory host names. For example:

```
ldapsearch -h oid_host -p oid_port -D cn=orcladmin -w admin_password -b
"cn=subregistrysubentry" -s sub "objectclass=*" dn
cn=oid1_1_hostName1,cn=osdldapd,cn=subregistrysubentry
cn=oid1_1_hostName2,cn=osdldapd,cn=subregistrysubentry
cn=oid1_1_myhost.example.com,cn=osdldapd,cn=subregistrysubentry
```

5. From the results in the previous step, remove the entries with the undesired host names. For example:

```
ldapdelete h oid_host -p oid_port -D cn=orcladmin -w admin_password
"cn=oid1_1_hostName1,cn=osdldapd,cn=subregistrysubentry"
ldapdelete h oid_host -p oid_port -D cn=orcladmin -w admin_password
"cn=oid1_1_hostName2,cn=osdldapd,cn=subregistrysubentry"
```

6. Verify that the undesired host names are removed. For example:

```
ldapsearch h oid_host -p oid_port -D cn=orcladmin -w admin_password -b
"cn=subregistrysubentry" -s sub "objectclass=*" dn
cn=oid1_1_myhost.example.com,cn=osdldapd,cn=subregistrysubentry
```

> **See Also:**
>
> "Cloning Oracle Fusion Middleware" in the *Oracle Fusion Middleware Administrator's Guide*.

6.2.10 (Bug 16498988) Oracle Internet Directory Fails to Start on Solaris SPARC System Using ISM

Issue

Oracle Internet Directory fails to start on the following Oracle Solaris SPARC system using Intimate Shared Memory (ISM): `5.11 11.1 sun4v sparc sun4v`

Workaround

As a workaround for this problem, set the following values, as shown in the next procedure:

- Set the total amount of operating system physical locked memory allowed (`project.max-locked-memory`) for Oracle Internet Directory to 2 GB or higher so that the value aligns with the supported page sizes. The `pagesize -a` command lists all the supported page sizes on Solaris systems.
- Set the `orclecachemaxsize` attribute to less than the `project.max-locked-memory` and ensure that the value aligns with the OS supported page sizes. For example, set the value to 256 MB.

In the following procedure, it is assumed that the Oracle Internet Directory services are managed by an operating system user named "oracle":

1. Log in to the Solaris SPARC system as the root user.
2. Check the project membership of the OID user.

   If the OID user belongs to the default project:

   a. Create a new project with the value of maximum locked memory set to 2 GB or higher, and associate the OID user with the newly created project. On Solaris 10 and 11, project id 3 represents the default project. For example:

   ```
   # id -p oracle
   uid=2345(oracle) gid=529(dba) projid=3(default)
   # projadd -p 150 -K "project.max-locked-memory=(priv,2G,deny)" oidmaxlkmem
   # usermod -K project=oidmaxlkmem oracle
   ```

   b. Verify that the value for the resource control `project.max-locked-memory` was set to 2 GB, as expected. For example:

   ```
   # su - oracle

   $ id -p oracle
   uid=2345(oracle) gid=529(dba) projid=150(oidmaxlkmem)

   $ prctl -n project.max-locked-memory -i project 150
   project: 150: oidmaxlkmem
   NAME    PRIVILEGE       VALUE    FLAG   ACTION                       RECIPIENT
   project.max-locked-memory
           privileged      2.00GB      -   deny                                 -
           system          16.0EB    max   deny                                 -
   ```

   If the OID user belongs to a non-default project:

   a. Modify the corresponding project to include the `project.max-locked-memory` resource control and set the value to 2 GB or higher. For example:

   ```
   # id -p oracle
   uid=2345(oracle) gid=529(dba) projid=125(oraproj)

   # projmod -a -K "project.max-locked-memory=(priv,2G,deny)" oraproj
   ```

   b. Verify that the value for the resource control `project.max-locked-memory` was set to 2 GB, as expected. For example:

   ```
   # projects -l oraproj
   oraproj
           projid : 125
           comment: ""
           users  : (none)
           groups : (none)
           attribs: project.max-locked-memory=(priv,2147483648,deny)
                    project.max-shm-memory=(priv,34359738368,deny)

   # su - oracle
   $ id -p
   uid=2345(oracle) gid=529(dba) projid=125(oraproj)

   $ prctl -n project.max-locked-memory -i project 125
   project: 125: oraproj
   NAME    PRIVILEGE       VALUE    FLAG   ACTION  RECIPIENT
   project.max-locked-memory
           privileged      2.00GB      -   deny    -
           system          16.0EB    max   deny    -
   ```

3. Set the entry cache maximum size (`orclecachemaxsize` attribute) to a value that is less than the maximum locked memory size allowed by the OS and that aligns with the OS supported page sizes.

   For example, using SQL*Plus, set the value to 256 MB:

   ```
   sqlplus ods@oiddb
   update ds_attrstore set attrval='256m'
     where entryid=940 and attrname='orclecachemaxsize';
   commit;
   ```

4. Run the `config.sh` script to configure Oracle Internet Directory.

6.2.11 ODSM Browser Window Becomes Unusable

Issue

Under certain circumstances, after you launch ODSM from Fusion Middleware Control, then select a new ODSM task, the browser window might become unusable. For example, the window might refresh repeatedly, appear as a blank page, fail to accept user input, or display a null pointer error.

Workaround

As a workaround, go to the URL: `http://`*`host`*`:`*`port`*`/odsm`, where *host* and *port* specify the location where ODSM is running, for example, `http://myserver.example.com:7005/odsm`. You can then use the ODSM window to log in to a server.

6.2.12 (Bug 8464130)Turkish Dotted I Character is Not Handled Correctly

Issue

Due to a bug, Oracle Internet Directory cannot handle the upper-case dotted I character in the Turkish character set correctly. This can cause problems in ODSM and in command-line utilities.

Workaround

There is no workaround for this issue.

6.2.13 (Bug 10383377) SQL of OPSS ldapsearch Might Take High CPU%

Issue

The SQL of an OPSS one level `ldapsearch` operation, with filter "`orcljaznprincipal=`*`value`*" and required attributes, might take unreasonably high percentage DB CPU.

Workaround

If this search performance impacts the overall performance of the machine and other processes, you can resolve the issue by performing the following steps in the Oracle Database:

1. Log in to the Oracle Database as user `ODS` and execute the following SQL:

   ```
   BEGIN
   DBMS_STATS.GATHER_TABLE_STATS(OWNNAME=>'ODS',
                                 TABNAME=>'CT_ORCLJAZNPRINCIPAL',
                                 ESTIMATE_PERCENT=>DBMS_STATS.AUTO_SAMPLE_SIZE,
   ```

```
                                        CASCADE=>TRUE);
END;
/
```

2. Flush the shared pool by using the ALTER SYSTEM statement, as described in the *Oracle Database SQL Language Reference*.

6.2.14 Unable to set up OID replication in Oracle Enterprise Manager

Issue

The wizard for setting up replication is no longer available in Oracle Enterprise Manager Fusion Middleware Control 12c Administration menu.

Workaround

You can use the command line tools for setting up LDAP-based replication. See Command-line Tools to Setup and Modify Replication in *Administering Oracle Internet Directory*.

6.2.15 Unable to estimate OID tuning and sizing needs in Oracle Enterprise Manager

Issue

The wizard for estimating sizing and tuning needs is no longer available in Oracle Enterprise Manager Fusion Middleware Control 12c Administration menu.

Workaround

For recommendations on sizing and tuning Oracle Internet Directory, see Tuning and Sizing Oracle Internet Directory in *Administering Oracle Internet Directory*.

6.2.16 Unable to manage wallet for OID in Oracle Enterprise Manager

Issue

The wallet option is no longer available in Oracle Enterprise Manager Fusion Middleware Control 12c Security menu.

Workaround

You can use the orapki tool or the keystore service to create a wallet, see Wallet Management and Keystore Management in *Administering Oracle Fusion Middleware*.

6.2.17 In IBM AIX, OID Schema Load May Fail While Running the RCU Tool

Issue

Impacted Platforms: IBM AIX

After successful installation of Oracle Internet Directory 12c on AIX operating system, the OID schema load using the RCU tool fails with the following error:

```
Error initializing SQLPlusEngine:
java.io.IOException: java.io.IOException: java.io.IOException:
java.io.IOException: java.io.IOException:
java.io.IOException: java.io.IOException: java.io.IOException:
java.io.IOException: java.io.IOException:
```

```
java.io.IOException: java.io.IOException: Error initializing sqlplus.
at
oracle.sysman.assistants.common.dbutil.sqlplus.SQLPlusEngine.setDefaultEngineS
ettings(SQLPlusEngine.java:2144)
at
oracle.sysman.assistants.common.dbutil.sqlplus.SQLPlusEngine.initialize(SQLPlu
sEngine.java:352)
at
oracle.sysman.assistants.rcu.backend.action.SQLPlusAction.perform(SQLPlusActio
n.java:214)
at
oracle.sysman.assistants.rcu.backend.task.AbstractCompTask.execute(AbstractCom
pTask.java:255)
at
oracle.sysman.assistants.rcu.backend.task.ActualTask.run(TaskRunner.java:346)
at java.lang.Thread.run(Thread.java:785)
```

Oracle Internet Directory 12c is bundled with IBM AIX Database client 12.1.0.2.0 version. The issue is related to the IOCP API symbols dependency in IBM AIX Database 12.1.0.2 client library. Enable the IOCP module in the machine where OID server is installed to resolve this issue.

Workaround

On IBM AIX in IBM POWER Systems (64-Bit), enable I/O completion ports (IOCP) before initiating the install process. To enable IOCP ports, set the status of the IOCP port to `Available`.

To check if the IOCP module is enabled, run the `lsdev` command:

```
$ lsdev | grep iocp
```

By default, IOCP is set to `Defined`, and hence not enabled. The following sample output shows the IOCP status is set to `Defined`:

```
iocp0      Defined       I/O Completion Ports
```

To enable IOCP, set the IOCP status to `Available` using the following procedure:

1. Log in as `root` and run the following command:

   ```
   # smitty iocp
   ```

2. Select **Change / Show Characteristics of I/O Completion Ports**.
3. Change the configured state at system restart from `Defined` to `Available`.
4. Run the `lsdev` command to confirm the IOCP status is set to `Available`:

   ```
   $ lsdev | grep iocp
   iocp0      Available       I/O Completion Ports
   ```

5. Perform a system restart to make the changes permanent.

6.3 Oracle Internet Directory Configuration Issues and Workarounds

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

- Warning When Creating a Remote Oracle Internet Directory Instance

6.3.1 Warning When Creating a Remote Oracle Internet Directory Instance

Issue

When you create an Oracle Internet Directory instance targeted to a remote node, on first machine, the following warning is displayed in the Administration Server logs:

```
 <Warning> <Management> <BEA-141296> <Unable  to contact Node Manager on
"oidhost2".
Activation for system component "oid2"  is deferred until "oidhost2" becomes
available.
java.lang.RuntimeException: Node Manager is not available on machine oidhost2
```

Workaround

This warning can be ignored.

6.4 Documentation Errata

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

- Replication Instructions in Tutorial for Identity Management are Incomplete

6.4.1 Replication Instructions in Tutorial for Identity Management are Incomplete

In the *Tutorial for Identity Management*, which is linked from *Getting Started with Oracle Identity Management*, Setting up Oracle Internet Directory Replication, is missing important information.

Specifically, the instructions do not work unless the new consumer node is empty. If the new consumer node has pre-loaded data, then various conflict resolution and invalid attribute name format messages will appear in the replication logs.

For more information, see Rules for Configuring LDAP-Based Replication in the *Oracle Fusion Middleware Administering Oracle Internet Directory*.

7

Oracle Identity Management Integration

Notes for this release include information about supported integrations.

- Oracle Identity Management System Requirements and Specifications

7.1 Oracle Identity Management System Requirements and Specifications

Keep the following point in mind during OIM installation:

- The following one-off the patches must be applied when using fmw_14.1.2.1.0_idm_generic.jar for an OIM installation. These patches should be applied after installation but before creating a domain.
  - 37443542: Search for this Bug ID at https://support.oracle.com.
  - 37512243: Search for this Bug ID at https://support.oracle.com.