Oracle® Fusion Middleware

Release Notes for Oracle Identity Management

12c (12.2.1.3)

E96073-05

January 2020

Oracle Fusion Middleware Release Notes for Oracle Identity Management, 12c (12.2.1.3)

E96073-05

Primary Author: Anju Poovaiah

Contributing Authors: Binitha Monnappa, Devanshi Mohan, Sandhya US, Showvik Choudhury, Sudhira Subudhi

Contents

Preface

1 Introduction

2 What's New in Oracle Identity Management 12c (12.2.1.3.0)

3 Oracle Access Management

6 Oracle Internet Directory

Preface

This preface includes the following sections:

Audience

This document is intended for users of Oracle Identity Management 12*c* (12.2.1.3.0).

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 12*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 12*c* (12.2.1.3.0). 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.

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.

For latest update on Oracle Access Manager, see *Oracle Access Manager 12cPS3 released (12.2.1.3.0)* (Doc ID 2296644.1).

For latest update on Oracle Unified Directory, see *Oracle Unified Directory 12c PS3 released (12.2.1.3.0)* (Doc ID 2296668.1).

For latest update on Oracle Internet Directory, see *Oracle Internet Directory 12c PS3 released (12.2.1.3.0)* (Doc ID 2310155.1).

2
What's New in Oracle Identity Management 12*c* (12.2.1.3.0)

This topic lists the new features for all the products in Oracle Identity Management Release 12*c* (12.2.1.3.0).

Topics

2.1 What's New in Oracle Access Management

Oracle Access Management 12c (12.2.1.3) includes the following new features:

- **OAuth MDC**

  Provides support for OAuth in a Multi Data Center environment. This feature supports the following:

  – OAuth Artifacts (such as Identity Domains, Clients, Resources, and so on) created on Data Center1(DC1) are visible and are seamlessly synchronized across data centers.

  – OAuth trust artifacts (such as trust certificates used to sign and issue JWT tokens) are visible across other data centers.

  – An OAuth token generated on DC1 will be validated on other data centers. Runtime will work seamlessly with different DCs.

  – A session created on DC1 associated with a validated token is seamlessly validated by other DCs when the request reaches them.

  – Refresh token generated on DC1 will be valid on DC2. When played against DC2, it is validated and an access token is generated on DC2.

  See Configuring OAuth Services in *Oracle® Fusion Middleware Administering Oracle Access Management*

- **MDC Lifecycle simplification**

  Simplifies the process of setting up and administering OAM Multi-data Center Topologies without using T2P tooling. New REST based APIs introduced for administrative and diagnostic purposes significantly reduce the number of configuration steps performed in the MDC environment. Migration of OAM system configuration and policy artifacts from one Data Center to another is now simplified and done through MDC Admin REST APIs.

See Implementing Multi-data centres in *Oracle® Fusion Middleware Administering Oracle Access Management*

- **OAM Caching Simplification**

  This feature supports the following:

  - OAM 12c supports database-backed server-side session management to synchronize the session state across multiple nodes of an OAM 12c server cluster.

    See Maintaining Access Manager Sessions in *Oracle® Fusion Middleware Administering Oracle Access Management*

  - It implements database-based authentication plugin import, distribution and activation.

    See Custom Plug-ins Actions in *Oracle® Fusion Middleware Administering Oracle Access Management*

  - The configuration and policy is propagated through the configuration and policy store using periodic polling.

    See Policy Interval for System and Policy Configuration in *Oracle® Fusion Middleware Administering Oracle Access Management*

- **TLS1.2 and SHA2**

  OAM 12c supports **TLS1.2** to provide communications security over the internet. All the simple mode certificates that are generated out-of-the-box for WebGate SSL communication are upgraded to **SHA2**.

  See TLS 1.2 support in Oracle Access Management in *Oracle® Fusion Middleware Administering Oracle Access Management*

- **Password policy**

  This feature supports the following:

  - OAM 12c supports multiple password policies for setting up varied levels of password based complexity protection for users belonging to different groups.

    See Multiple Password Policies in *Oracle® Fusion Middleware Administering Oracle Access Management*

  - Forgot Password feature in OAM can be experienced using One Time Pin generation by using password change REST API’s.

    See Setting up the Forgot Password Module in *Oracle® Fusion Middleware Administering Oracle Access Management*

  - Forced Password change can be administered using REST API’s.

    See Forced Password Change Policy in *Oracle® Fusion Middleware Administering Oracle Access Management*

- **OMA**

  - Experience a new enhanced enrollment process for adding your accounts to the OMA app.
  - Use **App Protection** feature to protect your OMA app with a fingerprint identity sensor such as Touch ID for iOS and Fingerprint for Andriod.
  - Windows 10 platform is now supported.

See Configuring the Oracle Mobile Authenticator in *Oracle® Fusion Middleware Administering Oracle Access Management*

- **REST API**

  REST API’s are introduced in 12c for Federation Management, Multi Data Center, OAuth,, Password Management, Multifactor authentication OTP, Password Policy and Session Management. They are documented in REST API’s reference documents.

  See,

  – REST API for Federation Management in Oracle Access Manager

  – REST API for Multi Data Center in Oracle Access Manager

  – REST API for OAuth in Oracle Access Manager

  – REST API for Password Management in Oracle Access Manager

  – REST API for Multifactor Authentication OTP in Oracle Access Manager

  – REST API for Password Policy Management in Oracle Access Manager

  – REST API for Session Management in Oracle Access Manager

- **Simplified Installation Process**

  – The installation process is simplified with reduced number of steps, compared to the earlier releases.

  – Bootstrapping is the process of creating out-of-the-box Oracle Access Management (OAM) artifacts in the OAM store. For example, authentication schemes under policy components. 12*c* (12.2.1.3.0) allows to re-bootstrap individual components if failed. For example, policy, system, federation.

    This makes the installation process easier. In case of failure, individual components can be re-run again, instead of starting over from the beginning.

  – The number of post-configuration steps are reduced in 12*c* (12.2.1.3.0).

2.2 What's New in Oracle Identity Governance

Oracle Identity Governance 12*c* (12.2.1.3.0) has the following key new features:

- Oracle Identity Governance enables you to define your own custom access reviewer for user certifications. See Custom Reviewer for User Certifications in *Performing Self Service Tasks with Oracle Identity Governance*.
- Group or certifier assignments must be claimed by a user to take actions on it and released by the user for other users in the group to view the actions taken. See Claiming and Releasing Group Certifier Assignments in *Performing Self Service Tasks with Oracle Identity Governance*. Group certifier assignments can be defined while creating the certification definitions. See Creating Certification Definitions in *Performing Self Service Tasks with Oracle Identity Governance*.
- New options have been introduced under the Limit the entitlement-assignments to certify for each user option for creating a user certification definition. See Creating a User Certification Definition in *Performing Self Service Tasks with Oracle Identity Governance*.
- New option **Include entitlements provisioned by access policy** has been introduced for creating an entitlement certification definition. See Creating an

Entitlement Certification Definition in *Performing Self Service Tasks with Oracle Identity Governance*.

- The Certification Dashboard enables sorting and listing the certifications by the percentage completion of the certifications. See Sorting Certification Search Results in *Performing Self Service Tasks with Oracle Identity Governance*.
- Oracle Identity Governance supports inheriting the access granted via access policies from the parent role to child role. See Evaluating Policies for Role Inheritance in *Performing Self Service Tasks with Oracle Identity Governance*.
- Access Policy can be created and managed from the Manage tab in Identity Self Service. See Managing Access Policies in *Performing Self Service Tasks with Oracle Identity Governance*.
- The application onboarding capability in Identity Self Service allows you to create and manage applications, templates, and instances of applications, and clone applications. See Managing Application Onboarding in *Performing Self Service Tasks with Oracle Identity Governance*.
- In Identity System Administration, the **Import** and **Export** options for incremental migration of deployments by using the Deployment Manager have a new interface and flow. See Migrating Incrementally Using the Deployment Manager in *Administering Oracle Identity Governance*.
- Oracle Identity Governance provides a new real-time certification purging solution. See Using the Real-Time Certification Purge in Oracle Identity Governance in *Administering Oracle Identity Governance*.
- The user interface for defining connectors and upgrading connectors have been enhanced. See Defining a Connector and Wizard Mode Upgrade in Staging Environment in *Administering Oracle Identity Governance*.
- SCIM resources are secured by custom Oracle Web Services Manager (OWSM) policy, custom request headers, and a origin whitelist. See Securing SCIM Resources in *Developing and Customizing Applications for Oracle Identity Governance*.
- Oracle Identity Governance provides a JSON Web Token (JWT) service to simplify the use of Oracle Identity Governance SCIM-REST service. See Using the JSON Web Token (JWT) Service.
- Oracle Identity Governance provides policy sets containing attached OWSM policies on application path that make Restful and SOAP services secure. See Understanding Global Policy Attachments in *Developing and Customizing Applications for Oracle Identity Governance*.
- Multiple sandboxes can be published in bulk and in a specified sequence. See Understanding Sandbox Operations and Publishing Sandboxes in Bulk and Sequence in *Developing and Customizing Applications for Oracle Identity Governance*.
- The installation process is simplified in 12*c* (12.2.1.3.0).
  - Integrated quick installer is introduced in 12*c* (12.2.1.3.0) for Oracle Identity Governance. This can be used to install Oracle Fusion Middleware Infrastructure 12*c* (12.2.1.3.0), Oracle SOA Suite 12*c* (12.2.1.3.0), and Oracle Identity and Access Management 12*c* (12.2.1.3.0) in one go. You do not have to use multiple installers to install the products required for Oracle Identity Governance.

  - Configuration through bootstrapping as part of server startup has been introduced in 12*c* (12.2.1.3.0). Post-configuration steps required in the earlier releases (11*g*) are now done through auto-discovery during bootstrap, both in case of cluster mode and out-of-the box configuration.

2.3 What's New in Oracle Unified Directory

Oracle Unified Directory 12*c* (12.2.1.3.0) has the following key features:

- Improved performance and scalability:
  - The bulk offline import process for large deployments using the `import-ldif` command has been significantly enhanced and simplified.
  - Support for Transparent Network Substrate (TNS) aliases that allow effortless and transparent migration of TNS entries and aliases from Oracle Internet Directory. Oracle Unified Directory TNS aliases are compatible with TNS aliases on Oracle Internet Directory and therefore supported by database tools, such as netmgr.
  - Support for TNS aliases for Oracle Unified Directory deployments with Oracle Enterprise User Security (EUS) configured. See Enabling TNS Alias Support for EUS-enabled Configurations in *Oracle® Fusion Middleware Installing Oracle Unified Directory*.
  - Support to Retrieve Multi-Valued Attributes in the Created Order. See Retrieving Multi-Valued Attributes in the Order of Creation in *Oracle® Fusion Middleware Administering Oracle Unified Directory*.
- Enhanced security through:
  - Password-Based Key Derivation Function 2 Password Storage Schemes. See Password Storage Scheme in *Oracle® Fusion Middleware Administering Oracle Unified Directory*.
- ODSM Rebranding:
  - The Oracle Directory Services Manager (ODSM) interface for Oracle Unified Directory is, now, re-branded as Oracle Unified Directory Services Manager (OUDSM).
- Support for TLS 1.2 Protocols and Cipher Suites:
  - Supported TLS Protocols and Cipher Suites. See Supported TLS Protocols and Cipher Suites by Oracle Unified Directory in *Oracle® Fusion Middleware Administering Oracle Unified Directory*.
  - Support for Overriding System Default Protocols and Cipher Suites for TLS Communication. See Overriding System Default Protocols and Cipher Suites for TLS Communication in *Oracle® Fusion Middleware Administering Oracle Unified Directory*.
  - Support for Governing SSL/TLS Protocol and Cipher Suites. See About the Configurable LDAP Extension Properties Relevant to Security in *Oracle® Fusion Middleware Administering Oracle Unified Directory*.
  - Support for Configuring TLS Protocol Version and Cipher Suites in Connection handler. See Specifying Protocol Version and Cipher suites in a Connection Handler in *Oracle® Fusion Middleware Administering Oracle Unified Directory*.
  - Support for Configuring TLS Protocol Version and Cipher Suites in Crypto Manager for Replication. See Configuring SSL Protocol and Cipher Suites in

    Crypto Manager for Replication in *Oracle® Fusion Middleware Administering Oracle Unified Directory*.
  - Support of RDBMS Extension to Use Secure Connection. See Creating an RDBMS Extension to Use Secure Connection in *Oracle® Fusion Middleware Administering Oracle Unified Directory*.
  - Support for Configuring TLS Protocol Version and Cipher Suites for OUDSM to OUD Communication. See Configuring TLS Protocol and Cipher Suites for OUDSM to OUD Communication in *Oracle® Fusion Middleware Administering Oracle Unified Directory*.
- Support for new log publishers that are configurable via OUDSM:
  - Multiple log publishers are listed and configurable via OUDSM. See Viewing Existing Log Publishers in *Oracle® Fusion Middleware Administering Oracle Unified Directory*.
- Support for WebLogic Scripting Tool provisioning commands:
  - Multiple WLST provisioning commands are supported for configuring a WebLogic domain and for creating and deleting OUD instances. See Support for WLST Provisioning Commands in *Oracle® Fusion Middleware Installing Oracle Unified Directory*.
- Support for the Upgrade OUD Instance script:
  - The script updates the install path of each instance to point to the new Oracle 12*c* Home and also updates the Java properties for each instance. See Upgrading an Existing Oracle Unified Directory Server Instance in *Oracle® Fusion Middleware Installing Oracle Unified Directory*.
- Support for Oracle Fusion Middleware configuration tools:
  - Support for Oracle Fusion Middleware Configuration Wizard to create or extend a WebLogic domain with OUD system component on the admin machine. See Configuring OUD and OUDSM in a Single Domain in *Oracle® Fusion Middleware Installing Oracle Unified Directory*.
  - Support for Oracle Fusion Middleware Repository Creation Utility to create database schemas and load in your database. See Creating Database Schemas for the Infrastructure Domain Using the Repository Creation Utility in *Oracle® Fusion Middleware Installing Oracle Unified Directory*.
  - Support for Oracle Fusion Middleware Reconfiguration Wizard to reconfigure a WebLogic Server domain. See Upgrading OUDSM from 11g to 12c Using the Reconfiguration Wizard in *Oracle® Fusion Middleware Installing Oracle Unified Directory*.
- REST API
  - REST API's are introduced in 12c for Oracle Unified Directory. See Admin REST APIs for Oracle Unified Directory

2.4 What's New in Oracle Internet Directory

Oracle Internet Directory 12*c* Release 2 (12.2.1.3.0) has the following key new features:

- Oracle Internet Directory now uses WebLogic Management Framework for basic administrative tasks through a common command line, API and user interface.

See What is the WebLogic Management Framework? in *Understanding Fusion Middleware*.

- Diagnostic log messages are captured in OID server log files that includes database SQL statements and other operational time metrics. From this release, `oiddiag` tool is capable of generating HTML summary reports. See Oracle Internet Directory Debug Logs in *Oracle Fusion Middleware Administering Oracle Internet Directory* and About Oracle Internet Directory Server Diagnostic Command-Line Tool in *Oracle Fusion Middleware Reference for Oracle Identity Management*.
- Replication improvements including additional debug statements for change log processing and retry_cnt updates, range fix for HIQ processing, reversed order of search results for subtree deletes, replication queue stats and replication dn info in `oiddiag` report are added. See Managing and Monitoring Replication in *Oracle Fusion Middleware Administering Oracle Internet Directory*.

  Replication server now supports one-way or two-way authentication SSL mode. See Use of SSL Encryption in Oracle Internet Directory Replication in *Oracle Fusion Middleware Administering Oracle Internet Directory*
- Out-of-box default SSL configuration of OID server instance has the value of `orclcryptoversion` is set to 24. This means, only TLSv1.2 and TLSv1.1 are enabled. See Configuring Secure Sockets Layer (SSL) for other configuration settings in *Oracle Fusion Middleware Administering Oracle Internet Directory*.

  To enable no-auth mode of SSL, anonymous cipher should be configured in Oracle Internet Directory. See Configuring ODSM Connection with SSL Enabled in *Oracle Fusion Middleware Administering Oracle Internet Directory*

2.5 What's New in Oracle Identity Management Integration

Integrate Oracle Identity Governance (OIG) and Oracle Access Manager (OAM) using LDAP Connectors.

- Execute the new automated script, `OIGOAMIntegration.sh` to accomplish OIG-OAM integration in a single step. The script utilizes user-supplied values from property files to perform various configurations. See One-step Procedure for OIG-OAM Integration Using Automated Script in *Integration Guide for Oracle Identity Management Suite*.
- Alternatively, execute individual configuration steps sequentially to accomplish the integration incrementally. This is done by running the new automated script, `OIGOAMIntegration.sh` several times, each time with a different parameter to specify which operation to be performed. See Step-by-step Procedure for OIG-OAM Integration Using Automated Script *Integration Guide for Oracle Identity Management Suite*.

3

Oracle Access Management

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

Topics

- Access Management Known Issues and Workarounds
- Access Management Configuration Issues and Workarounds
- Access Management Console Issues
- Features Not Supported in Access Manager 12.2.1.3.0

> **Note:**
>
> See What's New in Oracle Access Management for information about new features in this release of Oracle Access Management.
>
> Bundle Patch for Oracle Access Management Server and Webgate 12 *c* (12.2.1.3.5) release is available. For more information see,
>
> - Bundle Patch for Oracle Access Management 12c (12.2.1.3.5) Readme
> - Bundle Patch for Oracle Access Management WebGate 12c (12.2.1.3.5) Readme

3.1 Access Management Known Issues and Workarounds

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

- Takes time to propagate a policy or any metadata change
- User name field in SME UI is case sensitive
- Unused References in OAM console
- Deprecated Java Policy
- Test-to-Production Not Supported in OAM
- chghost Tool does not Work with OAM
- Exception occurs while using OAM Access Tester Tool

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 Unused References in OAM console

Issue

Following are the references in OAM console that are unused:

- Access Portal
- OAuth Service
- Allow OAuth Token
- Token Issuance Policies
- Access Portal Service Settings

3.1.4 Deprecated Java Policy

For Upgrade Customers, refer java policy. See TLS1.2 Support in Oracle Access Management

3.1.5 Test-to-Production Not Supported in OAM

Issue

OAM does not support Test-to-Production (T2P) tools in this release.

Workaround

To create one or more cloned data centers follow the steps in the procedure, Adding an Additional Clone Data Center to the Existing Multi-Data Center Setup.

3.1.6 chghost Tool does not Work with OAM

Issue

OAM does not support *chghost* tool in this release.

Workaround

The host:port for primary and secondary servers can be configured using the UI parameters on OAM console.

See Configuring and Managing Registered OAM Agents Using the Console

The webgate profiles and policies on OAM server use the import/export partners or Bulk updates for Webgates.

See

- Import Partners
- Export Partners
- Bulk updates to Webgates

For webgates, you can do either of the following when host and port information is changed:

- Manually edit the host and port information of new OAM server by updating the *ObAccessClient.xml* at target host.
- You can register the Webgate agent with the new Oracle Access Manager by using the Oracle Access Manager Administration Console and replace the old artifacts.

  See Registering an OAM Agent using the console

  Alternatively, you can use the RREG command-line tool to register a new Webgate agent.

  See Locating and Preparing the RREG Tool and Remote Registration Tools, Modes, and Process

> **Note:**
>
> *ObAccessClient.xml* can be found at `webgate_Instance _Dir ($ {Oracle_Home}/user_projects/domains/$(DOMAIN_HOME)/config/fmwconfig/components/OHS/ohs1/webgate/config/ObAccessClient.xml)`

3.1.7 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.getClientAut
hentInfo(ObAAAServiceServer.java:159)
at
oracle.security.am.proxy.oam.requesthandler.RequestHandler.ObAuthenReqChall
engeHandler(RequestHandler.java:566)
at
oracle.security.am.proxy.oam.requesthandler.RequestHandler.handleRequest(Re
questHandler.java:229)
at
oracle.security.am.proxy.oam.requesthandler.RequestHandler.handleMessage(Re
questHandler.java:180)
at
oracle.security.am.proxy.oam.requesthandler.ControllerMessageBean.getRespon
seMessage(ControllerMessageBean.java:94)
at
oracle.security.am.proxy.oam.requesthandler.ControllerMessageBean_eo7ylc_MD
OImpl.__WL_invoke(Unknown Source)
at
weblogic.ejb.container.internal.MessageDrivenLocalObject.invoke(MessageDriv
enLocalObject.java:127)
at
oracle.security.am.proxy.oam.requesthandler.ControllerMessageBean_eo7ylc_MD
OImpl.getResponseMessage(Unknown Source)
at
oracle.security.am.proxy.oam.mina.ObClientToProxyHandler.getResponse(ObClie
ntToProxyHandler.java:316)
at
oracle.security.am.proxy.oam.mina.ObClientToProxyHandler.messageReceived(Ob
ClientToProxyHandler.java:270)
at
org.apache.mina.common.DefaultIoFilterChain$TailFilter.messageReceived(Defa
ultIoFilterChain.java:743)
at
org.apache.mina.common.DefaultIoFilterChain.callNextMessageReceived(Default
IoFilterChain.java:405)
at
org.apache.mina.common.DefaultIoFilterChain.access$1200(DefaultIoFilterChai
n.java:40)
at
```

```
org.apache.mina.common.DefaultIoFilterChain$EntryImpl$1.messageReceived(Def
aultIoFilterChain.java:823)
at org.apache.mina.common.IoFilterEvent.fire(IoFilterEvent.java:54)
at org.apache.mina.common.IoEvent.run(IoEvent.java:62)
at
oracle.security.am.proxy.oam.mina.CommonJWorkImpl.run(CommonJWorkImpl.java:
85)
at
weblogic.work.j2ee.J2EEWorkManager$WorkWithListener.run(J2EEWorkManager.jav
a:209)
at
weblogic.invocation.ComponentInvocationContextManager._runAs(ComponentInvoc
ationContextManager.java:352)
at
weblogic.invocation.ComponentInvocationContextManager.runAs(ComponentInvoca
tionContextManager.java:337)
at
weblogic.work.LivePartitionUtility.doRunWorkUnderContext(LivePartitionUtili
ty.java:57)
at
weblogic.work.PartitionUtility.runWorkUnderContext(PartitionUtility.java:
41)
at
weblogic.work.SelfTuningWorkManagerImpl.runWorkUnderContext(SelfTuningWorkM
anagerImpl.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 Configuration Issues and Workarounds

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

- Audit Integration with BI Publisher

3.2.1 Audit Integration with BI Publisher

Issue

BI Publisher is not supported in 12cPS3. Due to which, post upgrade some reports might not work.

BI Publisher will be available post PS3.

3.3 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

3.3.1 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.

3.4 Features Not Supported in Access Manager 12.2.1.3.0

The following table lists the features that will be unsupported from OAM 12.2.1.3.0 and provides the migration path:

Unsupported Features in OAM 12.2.1.3.0	Description	Migration Path
10g OSSO server co-existence	OAM 12c server does not support co-existence with the OSSO servers	Upgrade from OSSO to OAM 11g R2PS3 and then upgrade to OAM 12c.
OpenSSO server co-existence	OAM 12c server does not support co-existence with the OpenSSO server.	Upgrade to OAM 11gR2PS3 and then upgrade to OAM 12c.
OAM 10g server co-existence	OAM 12c server does not support co-existence with OAM 10g server.	Migrate to OAM 12c server.
OpenSSO agents	OpenSSO agents are not supported in the OAM 12c release.	Migrate to supported 12c agents. OAM 11g and 12c WebGates and Accessgates are supported in OAM 12.2.1.3.0
mod_osso	OAM 12c does not support mod OSSO (OSSO Agent Proxy) agents.	Migrate to 12c WebGate agents and upgrade to OAM 12c.
OAM10g WebGate	OAM 12c server does not support OAM 10 WebGates.	Migrate to OAM11g R2PS3 or OAM 12c WebGates Upgrade the server to OAM 12c.

Unsupported Features in OAM 12.2.1.3.0	Description	Migration Path
IDMConfigTool	OAM 12c does not support the following commands and attributes: • `prepareIDStore= FUSION` • `prepareIDStore= OAAM` • `configPolicyStore` • `configOVD` • `disableOVDAccessConfig` • `postProvConfig` • `validate: All options are not supported` • `ovdConfigUpgrade` • `upgradeOIMTo11gWebgate` • `POLICYSTORE_SHARES_IDSTORE` • `SPLIT_DOMAIN`	
IAMSuiteAgent	OAM 12c does not support IAMSuiteAgent. Till R2PS3, IAMSuiteAgent was the OOB agent protecting the OAM console. From 12c PS3 onwards, this is done using default OOB Login page. As per EDG (Enterprise Development Guide), it is recommended to protect OAM console using a webgate agent.	
Oracle Mobile Security Suite (OMSS)	OAM 12c does not support OMSS.	

In 12c, for mobile and social login usecases, we recommend customers to use standard OAuth. We are deprecating proprietary way of achieving these use cases so that the customers can move to a more standards-based approach that would allow better interoperability and facilitate an easier transition to Oracle Identity Cloud Service (IDCS) in the future. The following services are deprecated in 12c:

- Mobile and Social Services
- Mobile OAuth Service
- Security Token Service
- Access Portal Service

4

Oracle Identity Governance

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

Topics

- General Issues and Workarounds
- Multi-Language Support Issues and Workarounds
- Documentation Errata
- Features Not Supported in Oracle Identity Governance 12*c* (12.2.1.3.0)
- Comparison of Oracle Identity Governance Applications Deployed in 11*g* and 12*c*

> **Note:**
>
> - See What's New in Oracle Identity Governance for information about new features in this release of Oracle Identity Governance.
> - Bundle Patch for Oracle Identity Governance 12c (12.2.1.3.5) release is available. For more information see, Bundle Patch for Oracle Identity Governance 12c (12.2.1.3.5) Readme.

4.1 General Issues and Workarounds

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

- The Request for Others Option is Available for All Users
- Session Time-out Warning Displayed When Using the Deployment Manager
- EditFailedException When Releasing Configuration from WebLogic Console
- LDAP Synchronization Not Supported
- Errors for Custom Attribute Values

4.1.1 The Request for Others Option is Available for All Users

Issue

Impacted Releases: 12c (12.2.1.3.0)

Impacted Platforms:

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

Impacted Releases: 12*c* (12.2.1.3.0)

Impacted Platforms:

When using the Deployment Manager, 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 EditFailedException When Releasing Configuration from WebLogic Console

Issue

Impacted Releases: 12*c* (12.2.1.3.0)

Impacted Platforms:

In an Oracle Identity Governance deployment that has been upgraded from an earlier release, when you click **Release Configuration** in Oracle WebLogic Console, the following error is generated:

```
weblogic.management.provider.EditFailedException: Error loading jdbc/oimMDS-jdbc.xml
```

This error does not have any functional impact on the WebLogic configuration.

Workaround

To workaround this issue, open the following DataSource configurations, make any changes, and then save and activate the changes:

- `ApplicationDB`
- `mds-oim`
- `oimJMSStoreDS`
- `oimOperationsDB`
- `soaOIMLookupDB`

4.1.4 LDAP Synchronization Not Supported

Issue

Impacted Releases: 12c (12.2.1.3.0)

LDAP synchronization is not supported in Oracle Identity Governance 12*c* (12.2.1.3.0).

LDAP synchronization works when Oracle Identity Governance is integrated with Oracle Access Management (OAM). But OAM-OIG integration using `IDMConfigTool` is not supported in this release.

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.

> **Note:**
>
> Bundle Patch for Oracle Identity Governance 12c (12.2.1.3.1) release is available and it supports Oracle Identity Governance (OIG) and Oracle Access Manager (OAM) integration using LDAP Connectors. For more information, see What's New in Oracle Identity Management Integration.

4.1.5 Errors for Custom Attribute Values

Issue

If you set the values of some attributes in the User Form in Identity System Administraion and add the attributes to the My Information page in the Identity Self Service by customizing the page, issues are seen for the Pager and Fax attributes on specifying the values of those attributes. For example:

- Set the value of the Mobile attribute as 20 in the User Form of Identity System Administration. In Identity Self Service, add the Mobile attribute to the My Information page by customizing the page. If you provide a value of the Mobile attribute that is greater that 20 (say 25 characters), then an error is displayed when you click **Apply**.
- Set the value of the Pager attribute as 40 in the User Form of Identity System Administration. In Identity Self Service, add the Pager attribute to the My Information page by customizing the page. If you provide a value that is greater than 40 (say 45 chars), then only 40 characters are saved without displaying any error.
- The default value of the Fax attribute is set to 4000.

4.2 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

- Some Strings Not Translated on Application Onboarding Screens

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

Issue

Bug Number: 24903901

Impacted Releases: 12c (12.2.1.3)

Impacted Platforms:

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)

4.2.2 Search Result Message in the Export Configuration Page Not Translated

Issue

Impacted Releases: 12*c* (12.2.1.3.0)

Impacted Platforms:

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.

4.2.3 Some Strings Not Translated on Application Onboarding Screens

Issue

Bug Number: 26525535

Impacted Releases: 12*c* (12.2.1.3.0)

Impacted Platforms:

The following text in the application onboarding pages in Identity Self Service are not translated in German:

- **Connector Package:** The **Connector Package** option in the Basic Information page of the Create Application wizard and the Create Authoritative Application wizard
- **Schema:** The **Schema** page of the Create Application wizard and the Create Authoritative Application wizard
- **Name** and **Connector Name:** The **Name** and **Connector Name** options in the search list of the Applications page
- **Organization:** The **Organization** tab in the Settings page of the Create Application wizard and the Create Authoritative Application wizard
- **Account Name:** The **Account Name** drop down in the Applications page
- **Provisioning Field:** The **Provisioning Field** column name in the Schema tab of the Create Application wizard and the Create Authoritative Application wizard
- **Action Script:** The **Action Script** buttons in the Applications page

4.3 Documentation Errata

This topic contains the following documentation errata for Oracle Identity Governance documentation:

- In *Help Topics for Oracle Identity Governance*, the correct description for the **Combine Repeated Approvals** option in the History table of the Edit Fulfillment Task page should be:

  Click to combine the approvals that have been done repeatedly.

4.4 Features Not Supported in Oracle Identity Governance 12*c* (12.2.1.3.0)

The following features are not supported in this release:

Features Unsupported in 12.2.1.3.0	Description
OMSS integration	Integration of Oracle Identity Governance and Oracle Mobile Security Suite is not supported in this release.
Embedded BI Publisher reports	Embedded BI Publisher is not supported in this release. Standalone BI Publisher can be installed and configured to use Identity Governance reports. See Configuring Reports in *Developing and Customizing Applications for Oracle Identity Governance*.
Post-install configuration GUI	The post-install configuration GUI is not supported in this release.
LCM configuration tool	The LCM configuration tool is not supported in this release.
Remote Manager	The Remote Manager is not available in this release and has been de-supported.

Features Unsupported in 12.2.1.3.0	Description
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*.
Diagnostic Dashboard	The Diagnostic Dashboard (XIMDD) utility is not supported in this release. For some of the tests using the XIMDD utility, you can do the following: • For Oracle Database Prerequisites Check, use the appropriate DB query. • For JMS Messaging Verification, view the state of JMS queues listed in the Enterprise manager Fusion Middleware Control. • For Database Connectivity Check, use the WebLogic Administration Console. • For Java VM System Properties Report, Jprofiler can be with the process ID of the server to extract the JVM parameters.
BAT scripts	BAT scripts, such as uploadNotificationTemplates.bat, comparator_config.bat, OIMMTUpgrade_WS.bat, OIMUpgrade.bat, opamSetup.bat, patch_oimapp.bat, and updateLdapConnectionData.bat, are not supported in this release. In addition, the scripts under *MW_HOME*/server/ldap_config_uti/ are also not supported.

4.5 Comparison of Oracle Identity Governance Applications Deployed in 11*g* and 12*c*

Review the Oracle Identity Governance applications deployed for WebLogic Server in both 11*g* and 12*c*, and their locations.

In 11*g*, there were 20 distinct applications deployed for WebLogic Server, and 11 sub-applications under `oim.ear`.

In 12*c*, there are only 8 main-stream applications available. Rest of the applications are consolidated under `oim.ear`, to optimize the disk space.

Table 4-1 Applications and Libraries Deployed in 11*g* and 12*c*

Oracle Identity Manager Applications and Libraries in 11*g*	Oracle Identity Governance Applications and Libraries in 12*c*
• `metadata.ear` • `oim_xe_metadata.ear` • `oracle.iam.ui.oia-view.war` • `scim-oim-services.war` • `metadata_xe.ear` • `oracle.iam.console.identity.self-service.ear` • `oracle.iam.ui.view.war` • `sodcheck-service.ear` • `Nexaweb.ear` • `oracle.iam.console.identity.sysadmin.ear` • `provisioning-callback.ear` • `spml-dsml.ear` • `oim.ear` • `oracle.iam.ui.custom-dev-starter-pack.war` • `reqsvc.ear` • `spml-xsd.ear` • `oim_ee_metadata.ear` • `oracle.iam.ui.model.ear` • `role-sod.ear` • `TaskDetails.ear`	• `oim.ear` • `oracle.iam.ui.model.ear` • `oracle.iam.console.identity.self-service.ear` • `oracle.iam.ui.oia-view.war` • `oracle.iam.console.identity.sysadmin.ear` • `oracle.iam.ui.view.war` • `oracle.iam.ui.custom-dev-starter-pack.war` • `oimclient.jar`

Table 4-2 Applications and Libraries Under oim.ear in 11*g* and 12*c*

Applications and Libraries Under oim.ear in 11*g*	Applications and Libraries Under oim.ear in 12*c*
• `dataobjects-ejb.jar` • `IdentityAuditCallbackService.war` • `SchedulerService-web.war` • `iam-async-mdb.jar` • `jmx-config-lifecycle.war` • `workflowservice.war` • `callbackResponseService.war` • `iam-consoles-faces.war` • `xlWebApp.war` • `CertificationCallbackService.war` • `iam-ejb.jar`	• `AppAsyncMdb.jar` • `OIGUI.war` • `oimrest.war` • `applicationrest.war` • `provisioning-callback.war` • `callbackResponseService.war` • `reqsvc.war` • `CertificationCallbackService.war` • `rest-oig-service.war` • `dataobjects-ejb.jar` • `role-sod.war` • `FacadeWebApp.war` • `SchedulerService-web.war` • `iam-async-mdb.jar` • `scim-oim-services.war` • `iam-consoles-faces.war` • `sodcheckservice-web.war` • `iam-ejb.jar` • `spml-xsd.war` • `IdentityAuditCallbackService.war` • `tokservice.war` • `jmx-config-lifecycle.war` • `workflowservice.war` • `xlWebApp.war`

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

- Supported Interfaces for Directory Virtualization Features
- System Requirements and Specifications
- Software Environment Limitations and Recommendations
- Oracle Unified Directory (OUD) Known Issues and Workarounds
- Oracle Unified Directory Services Manager (OUDSM) Known Issues and Workarounds
- Related Oracle Directory Components Known Issues and Workarounds

> **Note:**
>
> - See What's New in Oracle Unified Directory for information about new features in this release of Oracle Unified Directory.
> - Bundle Patch for Oracle Unified Directory 12c (12.2.1.3.180829) release is available. For more information see, Bundle Patch for Oracle Unified Directory 12c (12.2.1.3.180829).
> - Bundle Patch for Oracle Unified Directory 12c (12.2.1.3.180626) release is available. For more information see, Bundle Patch for Oracle Unified Directory 12c (12.2.1.3.180626).
> - Bundle Patch for Oracle Unified Directory 12c (12.2.1.3.180322) release is available. For more information see, Bundle Patch for Oracle Unified Directory 12c (12.2.1.3.180322).

5.1 Supported Interfaces for Directory Virtualization Features

This section lists the Interfaces that are supported 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 5-1 Oracle Unified Directory Virtualization Features

Workflow Element	Configure with Command Line	Configure with OUDSM	Additional Information
Join	Yes	Yes	See Configuring a Virtual Directory View of Your Repositories in *Oracle® Fusion Middleware Administering Oracle Unified Directory*.
HideByFilter	Yes	No	See Filtering Search Results Using the HideByFilter in *Oracle® Fusion Middleware Administering Oracle Unified Directory*.
GetRidOfDuplicates	Yes	No	See Eliminating Duplicate Entries from Search Results Using the GetRidOfDuplicates in *Oracle® Fusion Middleware Administering Oracle Unified Directory*.
Active Directory Password Update	Yes	No	See Updating User Passwords Stored in Active Directory in *Oracle® Fusion Middleware Administering Oracle Unified Directory*.

Table 5-1 (Cont.) Oracle Unified Directory Virtualization Features

Workflow Element	Configure with Command Line	Configure with OUDSM	Additional Information
RDBMS	Yes	No	See Configuring Access to Identity Data Stored in an RDBMS in *Oracle® Fusion Middleware Administering Oracle Unified Directory*.
VirtualMemberOf	Yes	No	SeeAdding the memberof User Attribute to person Entries in *Oracle® Fusion Middleware Administering Oracle Unified Directory*.

5.2 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.

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 Installing Oracle Unified Directory 12c (12.2.1.3.0).

  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 12*c* (12.2.1.3.0).
  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 Oracle Unified Directory. This document always contains the latest information for a specific release.

- *Oracle® Fusion Middleware Installing Oracle Unified Directory 12c (12.2.1.3.0)*

  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

5.2.1 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 5-2 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.

5.2.2 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

5.2.2.1 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.

5.2.2.2 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.

5.2.3 Certified Languages

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

Oracle Unified Directory 12*c* (12.2.1.3.0) 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.

5.3 Software Environment Limitations and Recommendations

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

The Oracle Unified Directory 12*c* (12.2.1.3.0) 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 Options, and Database Cache in *Oracle Fusion Middleware Installing Oracle Unified Directory*.

This section describes the following topics:

- OUD 12c (12.2.1.3.0) Limitations
- Viewing the Certification Matrix
- Software Recommendations

5.3.1 OUD 12c (12.2.1.3.0) Limitations

This section lists the limitations of Oracle Unified Directory 12*c* (12.2.1.3.0). 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.

5.3.2 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 12*c* Release 2 (12.2.1.3.0).
3. Click the *xls* link to view the certification matrix and then click the **Interop** tab for the list of supported external directory servers.

5.3.3 Software Recommendations

This section lists the recommendations for using Oracle Unified Directory (12.2.1.3.0).

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 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.

5.4 Oracle Unified Directory (OUD) Known Issues and Workarounds

The following sections describe known issues and limitations with the Oracle Unified Directory 12*c* (12.2.1.3.0) core server at the time of this release.

- PBKDF2WithHmacSHA512–based password storage schemes might fail due to JDK bug
- (Bug 25363559) Disabling the Deprecated File-Based Access, Admin Access, and Error Loggers
- (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 19778292) The dsreplication initialize-all command fails
- (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

5.4.1 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.

5.4.2 (Bug 25363559) Disabling the Deprecated File-Based Access, Admin Access, and Error Loggers

Issue

Bug Number: 25363559

In this release, Oracle Unified Directory provides new set of "Oracle" log publishers, which write diagnostic log files in the Oracle Diagnostic Logging (ODL) format. So, file-based access, admin access and error loggers have been deprecated in favor of the corresponding Oracle access, admin access and error loggers. However, for backward compatibility reasons, they are also enabled by default, along with the corresponding Oracle loggers. So, it is recommended to disable the file-based access, admin access and error loggers.

Workaround

Disable the deprecated file-based loggers (File-Based Access Logger, File-Based Admin Access Logger, and File-Based Error Logger) and rely on the corresponding Oracle loggers.

To disable a log publisher, set its enabled property to false. For example, to disable the File-Based Access Logger, run the following command:

```
$ dsconfig -h localhost -p 4444 -D "cn=Directory Manager" -j pwd-file -X -n \
  set-log-publisher-prop --publisher-name "File-Based Access Logger" \
  --set enabled:false
```

5.4.3 (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
```

5.4.4 (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*.

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

Issue

Bug Number: 19778292

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.

5.4.6 (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.

5.4.7 (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"`

5.4.8 (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
```

5.4.9 (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.

5.4.10 (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.

5.4.11 (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.

5.4.12 (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`.

5.4.13 (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 Section 1.1 System Requirements and Certification in *Oracle® Fusion Middleware Installing Oracle Unified Directory*

5.4.14 (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.

5.4.15 (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
```

5.4.16 (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.

5.4.17 (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
```

5.4.18 (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.

5.4.19 (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.

5.4.20 (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.

5.4.21 (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.

5.4.22 (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*.

5.5 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 12*c* (12.2.1.3.0) 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:

- (Bug 17582404) ADF error is displayed in WebLogic Server logs.
- (Bugs 18789805/18915580/18905879/18884612/18874750) Modification Issues with Join Workflow Element
- (Bug 18871434) Join DN attribute does not return in Advanced Search in OUDSM
- (Bug 19028533) Adv Search: Issue with Search in pick attributes table
- (Bug 17462792) Subtabs may not display as designed on Solaris

- (Bug 17262682) Default browser settings may not allow OUDSM URL to be accessible on Windows 2008 R2(Bug 17462792) Subtabs may not display as designed on Solaris
- (Bug 16946878) Alerts not sent as designed
- (Bug 16056177) On the Advanced Search page, when you click an entry in the Search Results table, some buttons do not behave as expected
- (Bug 15928439) Java NullPointer exception occurs if a changelog entry does not contain a specified objectclass
- (Bug 12363352) In the screenreader mode, focus for some buttons does not work as expected

5.5.1 (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.

5.5.2 (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.

5.5.3 (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.

5.5.4 (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.

5.5.5 (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.

5.5.6 (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.

5.5.7 (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
```

5.5.8 (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.

5.5.9 (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.

5.5.10 (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.

5.6 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 Governance Framework.

Topics

- Oracle Directory Integration Platform
- Oracle Identity Governance Framework

5.6.1 Oracle Directory Integration Platform

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

Topics

- General Oracle Directory Integration Platform Issues and Workarounds
- Oracle Directory Integration Platform Configuration Issues and Workarounds

- Provisioning Issues

5.6.1.1 General Oracle Directory Integration Platform Issues and Workarounds

This section describes general issues and workarounds.

Topics

- Enabling the Domain-Wide Administration Port on Oracle WebLogic Server Prevents use of the DIP Command Line Interface
- LDIF Files That Contain Non-ASCII Characters Will Cause the testProfile Command Option to Fail if the LDIF File has Native Encoding
- Running the testProfile Command with LDIF Files Option Fails in Advance Mode
- Some Changes May Not Get Synchronized Due to Race Condition in Heavily-Loaded Source Director
- manageSyncProfiles Utility Prompts for Connected Directory Password
- The Oracle Password Filter for Microsoft Active Directory Installation Screens Displays 11g Version
- Resource Usage Charts will not be Displayed

5.6.1.1.1 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.

5.6.1.1.2 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*.

5.6.1.1.3 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*.

5.6.1.1.4 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.

5.6.1.1.5 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.

5.6.1.1.6 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.

5.6.1.1.7 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).

5.6.1.2 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

5.6.1.2.1 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*.

5.6.1.2.2 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.

5.6.1.2.3 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.

5.6.1.2.4 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.

5.6.1.2.5 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.

5.6.1.3 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

5.6.1.3.1 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/.

5.6.1.3.2 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*.

5.6.2 Oracle Identity Governance Framework

Known issues and workarounds for Oracle Identity Governance Framework include general issues and known issues related with Identity Governance Framework and Library Oracle Virtual Directory (LibOVD).

Topics

- LibOVD Known Issues and Workarounds
- Oracle Identity Governance Framework Documentation Changes

5.6.2.1 LibOVD Known Issues and Workarounds

Known issues related with LibOVD for release 12*c* (12.2.1.3.0).

Topics

- libovdconfig.bat script Does Not Support a Space in File Path
- Users with Same Name in Multiple Identity Stores

5.6.2.1.1 libovdconfig.bat script Does Not Support a Space in File Path

Issue

On the Microsoft Windows platform, the `libovdconfig.bat` script does not work if the path to your Java installation in the `-jreLoc` option includes a space character. For example, `C:\Program Files\Java\jdk1.7.0_21`.

Workaround

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

For example:

```
-jreloc C:\Progra~1\Java\jdk1.7.0_21
```

5.6.2.1.2 Users with Same Name in Multiple Identity Stores

Issue

If a user name is present in more than one LDAP repository and the `virtualize` property is set to use LibOVD, then the data in only one of those repositories is returned when you query that user name with the Identity Directory API.

Workaround

Currently, there is no workaround for this issue.

5.6.2.2 Oracle Identity Governance Framework Documentation Changes

Identity Governance Framework introduces 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 12*c* (12.2.1.3.0) release onward, the following Javadocs are 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 *Java API Reference for Identity Governance Framework Identity Directory*.
- Deprecation of Using the ArisID API functionality from 12*c* (12.2.1.3.0) onward.

6

Oracle Internet Directory

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

Topics

- General Oracle Internet Directory Issues and Workarounds
- Oracle Internet Directory Configuration Issues and Workarounds
- Documentation Errata

> **Note:**
>
> - Bundle Patch for Oracle internet Directory 12*c* (12.2.1.3.180315) release is available. For more information see, Bundle Patch for Oracle Internet Directory 12*c* (12.2.1.3.180315).

6.1 General Oracle Internet Directory Issues and Workarounds

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

- (Bug 25875893) ODS Schema details not getting auto-filled using Schemas Option
- (Bug 25814730) OID12cPS3: Startup fails because low system shared memory on Solaris
- (Bug 26564247) PS3 OID: Help link on ODSM URL does not work
- (Bug 19898973)Substring Filter Not Supported for Collective Attributes
- (Bug 14079791) Search on rootDSE `lastchangenumber` Attribute Works For One Attribute At A Time
- (Bug 17348090) Search with Filter Containing AND Operation of Collective Attributes Not Supported
- (Bug 17435510) Oracle Database Requires Patch to Fix Purge Job Problems
- (Bug 18695967) ODSM Does Not Create Entry of Custom objectclass With Custom Mandatory Field
- (Bug 18196425) ODSM Adds Fake Entries to the Chained Container and Displays Duplicate Entries During Export
- (Bug 19521548) Oracle Internet Directory Upgrade from 10.1.4.3 to 11.1.1.9.0 Fails During Configuration on AIX

- (Bug 12833947) ODSM Problems in Internet Explorer 7
- (Bug 16964666) Cloned Oracle Internet Directory Instance Fails or Runs Slowly
- (Bug 16498988) Oracle Internet Directory Fails to Start on Solaris SPARC System Using ISM
- ODSM Browser Window Becomes Unusable
- (Bug 9050432) Bulkmodify Might Generate Errors
- (Bug 8464130)Turkish Dotted I Character is Not Handled Correctly
- (Bug 10383377) SQL of OPSS ldapsearch Might Take High CPU%
- Unable to set up OID replication in Oracle Enterprise Manager
- Unable to estimate OID tuning and sizing needs in Oracle Enterprise Manager
- Unable to manage wallet for OID in Oracle Enterprise Manager

6.1.1 (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.

6.1.2 (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                                 -
```

6.1.3 (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

6.1.4 (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.

6.1.5 (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
```

6.1.6 (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.

6.1.7 (Bug 17435510) Oracle Database Requires Patch to Fix Purge Job Problems

Issue

Some versions of Oracle Database, such as 10.1.0.5.0rec.jul10, 10.2.0.4.5.psu, 10.2.0.5.1psu, 11.1.0.7.4psu, and 11.2.0.1.2psu require a patch to fix Oracle Internet Directory purge job problems.

Without the patch, a purge jobs operation does not function properly, and these symptoms can occur:

- Oracle Internet Directory change logs do not get purged, and the purge log shows ORA-23421 errors.
- Executing change log purge jobs with `orclpurgenow` set to 1 hangs.

Workaround

If you are experiencing the preceding purge job problems with any of the listed Oracle Database versions, then apply the latest Patch Set Update (PSU) for your Oracle Database that fixes RDBMS bug 9294838. If so, apply the RDBMS patch for your database. You can apply the patch after you have installed Oracle Internet Directory.

6.1.8 (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.

6.1.9 (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.

6.1.10 (Bug 19521548) Oracle Internet Directory Upgrade from 10.1.4.3 to 11.1.1.9.0 Fails During Configuration on AIX

Issue

This issue occurs when you upgrade Oracle Internet Directory from 10.1.4.3 to 11.1.1.9.0 on AIX. The upgrade fails during configuration with the following error:

```
javax.net.ssl.SSLException: Received fatal alert: illegal_parameter
```

Workaround

The workaround for this issue is to add the java option to disable ECDH ciphers while configuring Oracle Internet Directory 11.1.1.9.0, as shown in the following example:

```
ORACLE_HOME/config.sh -Doracle.ldap.odi.sslsocketfactory.disable-ecc=true
```

6.1.11 (Bug 12833947) ODSM Problems in Internet Explorer 7

Issue

The ODSM interface might not appear as described in Internet Explorer 7.

For example, the **Logout** link might not be displayed.

Workaround

If this causes problems, upgrade to Internet Explorer 8 or 9 or use a different browser.

6.1.12 (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*.

6.1.13 (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.

6.1.14 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.

6.1.15 (Bug 9050432) Bulkmodify Might Generate Errors

Issue

If Oracle Internet Directory is using Oracle Database 11*g* Release 1 (11.1.0.7.0), you might see `ORA-600` errors while performing `bulkmodify` operations.

Workaround

To correct this problem, apply the fixes for Bug 7019313 and Bug 7614692 to the Oracle Database.

6.1.16 (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.

6.1.17 (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*.

6.1.18 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*.

6.1.19 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*.

6.1.20 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 Oracle Internet Directory Configuration Issues and Workarounds

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

- Accept TLS Protocol for SSL support

6.2.1 Accept TLS Protocol for SSL support

Issue

While configuring Oracle Internet Directory in SSL mode, if SSLv3 is disabled and you try to enable the TLS mode only, then the Oracle Internet Directory configuration hangs. This happens when `orclsslciphersuite` attribute is populated with unsupported cipher suites.

Workaround

The workaround is to remove the unsupported cipher suite from the `orclsslciphersuite` attribute. For more information about the supported cipher suite list, see "Supported Cipher Suites" in Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory.

In addition, you must completely disable SSLv3 and TLS 1.0, and enable TLS for configuring Oracle Internet Directory in SSL mode. For enabling only TLS (and disabling SSLv3), you need to modify the value of `orclcryptoversion` attribute to `24`. This value refers to TLS 1.1 and TLS 1.2. For more information, see "Supported Protocol Versions" in *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

Run the `ldapmodify` command to update the value of `orclcryptoversion` to `24` as follows:

```
ldapmodify -D "cn=orcladmin" -q -p portNum -h hostname -f ldifFile
```

Here `ldifFile` contains:

```
dn: cn=oid1,cn=osdldapd,cn=subconfigsubentry
changetype: modify
replace: orclcryptoversion
orclcryptoversion: 24
```

6.2.2 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.

6.3 Documentation Errata

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

- Replication Instructions in Tutorial for Identity Management are Incomplete

6.3.1 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.

Features Supported in Release 12.2.1.3.0

Oracle Identity Management supports the following integration in this release:

- Oracle Access Management 12c and Oracle Identity Governance 12c using LDAP Connectors
- Oracle Access Management 12c and Oracle Adaptive Access Manager 11g R2PS3

Features Not Supported in Release 12.2.1.3.1

Oracle Identity Management doesn’t support the following integrations features in this release:

- For all directory types (OUD, OID, and AD) the following reconciliations are not supported:
  - User delete full and incremental reconciliation.
  - Reconciliation of deleted roles that have user members or child roles.
- For Active Directory type, Role hierarchy full and incremental reconciliation is not supported.
- If LDAP directory is used as a target in customer's setup, you cannot use it for OAM-OIG integration. It is not supported out-of-box and must be handled as one-off.

This chapter contains the following topic:

- Oracle Identity Management Integration Issues and Workarounds

\

7.1 Oracle Identity Management Integration Issues and Workarounds

Use OIG as a primary source for managing Users and Roles.

Perform deletion of users, or role related changes such as memberships and hierarchy in OIG and not directly against the directory.

The following are the known limitations for the OIG-OAM integration:

- If you are cloning the **SSOTrusted-for-SSOTarget** application to reconcile against another LDAP target (not the LDAP used for SSO integration) for trusted reconcile with OIG, make sure that the name of the cloned application does not contain the following keywords:

  - `SSOTrusted`
  - `OID Trusted App`
  - `AD Authoritative`

  If these keywords are used in the cloned application name, the trusted reconcile will reconcile the users to OIG, but will not synchronize those users to SSO LDAP.

- For all directory types, the version number in the LDAP connector templates must match the version number of the downloaded connector bundle. It requires directly editing the template XML files. For example, If OUD is your directory type, update the XMLs under `$ORACLE_HOME/idm/server/ssointg/connector/oud/` directly to change the connector version from `11.1.1.7.0` to `12.2.1.3.0`.
- Group names must be unique in target LDAP for SSO-integrated setup.
- Orchestration-Provisioning Compensation will not be performed by any of the LDAP account, role, user membership, and role hierarchy post process handlers.

Account Self-Locking Issues

In an Oracle Identity Governance-Oracle Access Manager Integration environment, connection sockets in IDS pool times out and does not reset as expected. Oracle Access Manager does not lock User after five invalid login attempts. Apply the libOVD patch as follows:

Before applying the patches to Oracle software in your Oracle Fusion Middleware environment, ensure that you have and unzipped it.

1. Download the latest libOVD patch, `p26401006_122130_Generic.zip` and unzip it to the desired location.
2. Set the environmental variables.

   ```
   export ORALCE_HOME=/scratch/work/access
   ```

3. Stop the OAM domain.
4. Apply libOVD patch through `opatch apply` command.
5. Restart the OAM domain.

See Patching Your Environment Using OPatch in *Oracle Fusion Middleware Patching with OPatch*.