Oracle® Fusion Middleware

Checklist for Installing and Deploying Oracle Identity and Access Management

11*g* Release 2 (11.1.2.2.0)

E52892-02

April 2014

This guide contains installation and deployment checklists for Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) components.

Oracle Fusion Middleware Checklist for Installing and Deploying Oracle Identity and Access Management, 11*g* Release 2 (11.1.2.2.0)

E52892-02

Primary Author: Shynitha K S

Contributors: Ashish Gupta, Ashish Kolli, Deepak Ramakrishnan, Gururaj BS, Madhu Martin, Peter LaQuerre, Shishir Kumar, Sylvain Duloutre, Teena George

Contents

Preface

This Preface provides supporting information for the *Oracle Identity and Access Management Deployment Checklists* and includes the following topics:

- Audience
- Documentation Accessibility
- Related Documents
- Conventions

Audience

Oracle Identity and Access Management Deployment Checklists is intended for administrators who are responsible for installing and deploying Oracle Identity and Access Management components.

This document does not cover the procedural information for installing and deploying Oracle Identity Management and Access Management components. For installation and configuration procedures, refer to *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` or visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` if you are hearing impaired.

Related Documents

This section identifies additional documents related to Oracle Identity and Access Management. You can access Oracle documentation online from the Oracle Technology Network (OTN) Web site at the following URL:

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

Refer to the following documents for additional information on each subject:

Oracle Fusion Middleware

- *Oracle Fusion Middleware Administrator's Guide*
- *Oracle Fusion Middleware Security Guide*

High Availability

- *Oracle Fusion Middleware High Availability Guide*

Oracle Fusion Middleware Repository Creation Utility

- *Oracle Fusion Middleware Repository Creation Utility User's Guide*

Oracle Identity Manager

- *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*

Oracle Access Management

- *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*

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.

1 Overview and General Preparation

This chapter includes the following topics:

- Purpose of IAM Deployment Checklists
- General Preparation

1.1 Purpose of IAM Deployment Checklists

Use these checklists as common guidelines for deploying Oracle identity and Access Management (11.1.2.2) in production.

1.2 General Preparation

This chapter contains a general preparation checklist for customers interested in deploying Oracle Identity and Access Management in any of the supported scenarios. Use this checklist as a prerequisite for using scenario-specific checklists, which are included in subsequent chapters of this document.

Table 1–1 General Preparation Checklist

Requirement	Check when Verified
Review the supported operating system, hardware, and JVM described in *Oracle Fusion Middleware Supported System Configurations*.	□
Review the Oracle Identity and Access Management system requirements described in *Oracle Fusion Middleware 11g Release 2 (11.1.2.x) for Oracle Identity and Access management*.	□
Read and understand the installation and deployment process by reading the Oracle Identity and Access Management deployment documentation and the official Oracle Identity and Access Management release notes.	□
Read and understand the new or changed features introduced in this release of Oracle Identity and Access Management by reading product documentation.	□
If you are upgrading from a previous release of Oracle Identity and Access Management, read and understand the supported upgrade starting points and any impact on your current environment.	□

Table 1–1 (Cont.) General Preparation Checklist

Requirement	Check when Verified
Read the official Oracle Identity and Access Management release notes and familiarize with any known issues or limitations in this release.	□

2 Oracle Unified Directory Deployment

This chapter contains a checklist for customers interested in deploying only Oracle Unified Directory.

Table 2–1 Oracle Unified Directory Deployment Checklist

Requirement	Check when Verified
Identify and verify the latest Oracle Unified Directory patches and updates. For more information, see “Information Center : Overview Oracle Unified Directory (OUD) (Doc ID 1418884.2)” on My Oracle Support.	□
If you are using an Oracle Linux Enterprise 6 64-bit machine, ensure that you have installed the additional i686 packages before running the Oracle Unified Directory installer. For more information, see “System Requirements and Certification” in the *Oracle Fusion Middleware Installation Guide for Oracle Unified Directory*.	□
Ensure that your system has sufficient RAM memory for JVM heap and database cache. For more information, see “Configuring the JVM heap, Java Options and Database Cache” in the *Oracle Fusion Middleware Installation Guide for Oracle Unified Directory*.	□
Ensure that your system has sufficient disk space to store the generated log files and replication metadata in addition to other data stored in LDAP. **Note:** The server log files can consume up to 1GB of disk space with default server settings. In replicated environments, the change log database can grow up to 30-40 GB with loads of 1,000mods/sec. For information about setting the log file size, see “Configuring Log Rotation Policies” in the *Oracle Fusion Middleware Administrator’s Guide for Oracle Unified Directory*.	□
Ensure that you have tuned the JVM and Oracle Unified Directory to improve scalability and performance. For more information, see “Configuring the JVM Java Options, and Database Cache” in the *Oracle Fusion Middleware Installation Guide for Oracle Unified Directory*.	□

Table 2–1 (Cont.) Oracle Unified Directory Deployment Checklist

Requirement	Check when Verified
On Linux machines, ensure that the maximum file descriptor limit per process is set to `65535`. For more information, see "Software Requirements" in the *Oracle Fusion Middleware Release Notes for Oracle Unified Directory 11g Release 2 (11.1.2.2)*.	□
On Windows machines, verify that the administrator has access rights on the instance path when Oracle Unified Directory is set up to run as a Windows Service. For more information, see "Software Requirements" in the *Oracle Fusion Middleware Release Notes for Oracle Unified Directory 11g Release 2 (11.1.2.2)*.	□
Ensure that appropriate database indexes are configured and initialized to handle specific search pattern, especially for attributes defined in custom user schema.	□
Ensure that every existing Oracle Unified Directory server was started at the time new Oracle Unified Directory server(s) were added to the replication topology.	□
Ensure that full network connectivity is enabled between every Oracle Unified Directory Replication Server. Every Oracle Unified Directory Replication server can connect to each other (firewall ports enabled, DNS resolution, and so on).	□
Verify that every replicated Oracle Unified Directory directory server was properly initialized with same data (same generation ID). For more information about generation ID usage, see "Adding a Directory Server to an Existing Replicated Topology" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Unified Directory*.	□
When initializing a new server with LDIF import, ensure that the LDIF is not older than the replication purge delay (4 days, by default). For more information about replication purge delay, see "Purging Historical Information" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Unified Directory 11g Release 2 (11.1.2)*.	□
If you plan to use binary copy to initialize servers, or restore servers, or to do both, ensure that database index configuration is consistent across Oracle Unified Directory servers. For more information about indexing, see "Indexing Directory Data" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Unified Directory 11g Release 2 (11.1.2)*.	□
Run the dsreplication status tool to verify that the Oracle Unified Directory replication topology is properly initialized. For more information about dsreplication, see "Monitoring a Replicated Topology" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Unified Directory 11g Release 2 (11.1.2)*.	□

Table 2–1 (Cont.) Oracle Unified Directory Deployment Checklist

Requirement	Check when Verified
Examine Oracle Unified Directory error log files, and confirm that no errors are reported. **Note:** For information about logging, see the section, "Monitoring Oracle Unified Directory" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Unified Directory 11g Release 2 (11.1.2)*.	□
Examine the Oracle Unified Directory access logs to identify issues, such as insufficient privileges or unindexed searches. In the access logs, search for the strings: ■ Unindexed ■ Privilege	□

3

Oracle Access Manager Deployment

This chapter contains a checklist for customers interested in deploying Oracle Access manager with LDAP.

Table 3–1 Oracle Access Manager Deployment Checklist

Requirement	Check when Verified
Ensure that a supported Oracle Database, an Oracle Middleware Home, and an LDAP installation are available.	□
Ensure that Oracle Access Manager, OPSS, and Audit schemas are created using Repository Creation Utility (RCU).	□
Ensure that the WebLogic Domain hosting Oracle Access manager is running in Production mode instead of Development mode.	□
Ensure that Oracle Access Manager ports are not in use in addition to the HTTP/HTTPS ports used by Oracle Access Manager WebLogic Server Cluster, Oracle Access Manager also uses OAP and Coherence Ports (default value 5575, 9095 respectively).	□
Ensure that IDMDomainAgent is removed from the Weblogic Domain running Oracle Access Manager, as the WebGate setup in enterprise deployments handles single sign-on.	□
Ensure that JVM is tuned to make maximum use of machine capacity. Ensure that the XMS and XMX values are set to same level (4-8 GB depending on machine capacity). **Note:** You can update JVM tuning parameters in the `<Domain_HOME>/bin/setDomainEnv` script. After updating the tuning parameters, you must restart Oracle Access Manager servers.	□
Ensure that your LDAP is preconfigured as an Identity Store as described in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.	□

Table 3–1 (Cont.) Oracle Access Manager Deployment Checklist

Requirement	Check when Verified
Ensure that the Identity Store has the required schemas extended. **Note:** The specific schemas are loaded when the ID Store is prepared. They are also present in the `$IAM_ORACLE_HOME/oam/ldap/schema` directory.	□
Ensure that the Identity Store is seeded with the required users, groups, and privileges, based on the input properties passed to the idmConfigTool.	□
Ensure that the idmConfigTool is used to configure Oracle Access Manager. **Note:** When you configure Oracle Access Manager by using the idmConfigTool, Oracle Access Manager is configured to use LDAP, and an Access Manager Webgate agent is created.	□
Ensure that the LDAP Identity Store is configured in the Access Management Suite by using the Oracle Access Manager Administration Console.	□
Ensure that Webgate/Agent communication to Oracle Access Manager servers is in either SIMPLE or CERT mode.	□
Ensure that Oracle HTTP Server is front ending Access Manager Admin Console and has a webgate wired to Access Manager using the WebGate Agent profile created by idmConfigTool.	□
Ensure that the Security Store is configured immediately after configuring Oracle Access Management WebLogic domain. You must do this before starting Oracle Access Manager servers.	□
Ensure that WebLogic Server providers are configured correctly with OUD Authenticator or LDAP Authenticator pointing to the OUD Store or to the LDAP Store, respectively. You must configure WLS providers in the following sequence: ■ OAMIDAsserter ■ OUD Authenticator (or LDAP Authenticator) ■ Default Authenticator ■ Default Identity Asserter	□
Ensure that the WLSAdmins Group is added to the list of WebLogic Administrators. This is the group created when the LDAP Store was prepared.	□
Ensure that Oracle Access Manager's performance is tuned based on the tuning guidelines. For more information, see "Oracle Access Management Performance Tuning" in the *Oracle Fusion Middleware Performance and Tuning Guide*.	□
Ensure that you have configured a custom login and error pages to meet your deployment requirements.	□

Table 3–1 (Cont.) Oracle Access Manager Deployment Checklist

Requirement	Check when Verified
Ensure that Webgate to Oracle Access Manager connectivity parameters are set to proper values: Threshold Timeout: Set to 10 seconds instead of the default value of -1. Max Session Time: Set to the half of firewall timeout between Webgate and the Oracle Access Manager server.	□
Ensure that Oracle Access Manager to LDAP connectivity parameters are set to proper values: Connection Refresh time is set to half of the firewall timeout between Oracle Access Manager and LDAP store. Request time out is set to 2 seconds or higher.	□
Ensure that the Load Balancer is configured to populate the IS_SSL=ssl header if terminating SSL in front of web servers where webgate is installed.	□
Ensure Oracle Access Manager front end URL that is collecting user credentials is configured for SSL.	□
Confirm that Oracle Access Manager-protected applications are not using the IAMSuiteAgent Host Identifier.	□
Confirm that common image file patterns are part of the excluded URL list (*.css, *.gif, *.png).	□
If you have excluded the 'root' patterns, '/*', '/…/*' or '/**' in an Application Domain, ensure that you fully understand the security implications.	□
If you have set 'DenyOnNotProtected' to false in Webgate profile, ensure that you fully understand the security implications.	□
If managing password policy in Oracle Access Manager, ensure that the password policy is more restrictive that the policy used at LDAP level. This will ensure that the Directory/LDAP password never supersedes enforcement at the Oracle Access Management level.	□
Ensure that you have reviewed the amount of Audit data produced for production load and adjusted settings (Low, Medium, High), so that only desired audit data is generated.	□
Ensure that you have an Audit data purge scheduled that is compliant with your data retention policies.	□

4

Oracle Identity Manager Deployment

This chapter contains a checklist for customers interested in deploying Oracle Identity Manager with LDAP.

Table 4–1 Oracle Identity Manager Deployment Checklist

Requirement	Check when Verified
Ensure that a supported Oracle Database, an Oracle Middleware Home, and an LDAP installation are available.	□
During the installation phase, after the Repository Creation Utility was run to create Oracle Identity Manager and its dependent schemas, check if the authorization policies or application stripe is seeded correctly using the APM-UI cluster.	□
Ensure that Oracle Identity Manager and SOA ports are not in use. By default, Oracle Identity Manager Server uses `14000` and SOA Server uses `8001`.	□
Ensure that the database-based OPSS security store configuration is done before running the Oracle Identity Manager configuration wizard.	□

If large pages are supported and enabled in the Operating System, ensure that JVM is configured as follows:
Arguments:
`-XX:+UseLargePages` (for HotSpot JVM)
`-XX:+UseLargePagesForHeap`
`-XX:+ForceLargePagesForHeap` (for JRockit JVM).
In JRockit JVM, if you are enabling large pages, do not use the argument:
`-XX:+UseLargePagesForCode`
	□

Oracle Identity Manager uses ApplicationDB, oimOperationsDB, and oimJMSStoreDS data sources deployed on Oracle Web Logic Server. As a general guideline, ensure that the capacity for these data sources is increased as follows: Initial Capacity=50; Minimum Capacity=50; Max Capacity=150; and Inactive time out=30. For more information about determining appropriate capacity values for your environment, see "Performance Tuning Guidelines and Diagnostics Collection for Oracle Identity Manager (OIM) (Doc ID 1539554.1)" on My Oracle Support.	□

Table 4–1 (Cont.) Oracle Identity Manager Deployment Checklist

Requirement	Check when Verified
Ensure that default values of Message Buffer Size and Messages Maximum properties are changed to the recommended values, 200MB (209715200 bytes) and 400000, respectively.	□
Ensure that the properties Maximum Threads Constraint of work managers OIMMDBWorkManager and OIMUIWorkManager are set to `80` and `20`, respectively.	□
Ensured that database indexes for searchable User Defined Attributes (UDF) exist.	□
Consider SOA JVM memory tuning recommendations described in sections "Tuning JVM Memory Settings for Oracle Identity Manager" and "Changing the Number of Open File Descriptors for UNIX (Optional)" in the *Oracle Fusion Middleware Performance and Tuning Guide*.	□
Ensure that multicasting is supported between cluster Oracle Identity Manager nodes and make sure that ports `45566` and `3121` are open.	□
Ensure that the JMS file store is on a shared storage or file system that is available to all Managed Servers in the Oracle Identity Manager cluster.	□
Ensure that the `XMLConfig.cacheConfig` Clustered MBean property is set to `true`. Use the MBean Browser in Fusion Middleware Control to locate the `XMLConfig.CacheConfig` MBean under **Application Defined MBeans**-->**oracle.iam**-->**XMLConfig.CacheConfig**-->**Cache**-->**Config**-->**oim**-->**<version>**-->**Attributes**-->**Clustered**. You can also follow the Performance Tuning Guidelines and Diagnostics Collection for Oracle Identity Manager (Doc ID 1539554.1) for more cache tuning options.	□
Ensure that the `OimExternalFrontEndURL` (in the discoveryConfig section of `oim-config.xml`) is set to the external LBR URL, such as `https://sso.mycompany.com:443`. Ensure that `OimFrontEndURL` is set to an internal URL, such as `http://idminternal.mycompany.com:80`.	□
Ensure that each Oracle Identity Manager domain has its own unique multicast address and it is not shared with other instances in the same subnet.	□
Ensure that your LDAP is preconfigured as an Identity Store as described in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.	□
Ensure that the Identity Store has the required schemas extended.	□
Ensure that the Identity Store is seeded with the required users, groups, and privileges, based on the input properties passed to the idmConfigTool.	□
Ensure that all of the prerequisites for LDAP Sync configuration, as described in the *Installation Guide for Oracle Identity and Access Management*, are satisfied.	□

Table 4–1 (Cont.) Oracle Identity Manager Deployment Checklist

Requirement	Check when Verified
Verify that the physical LDAP is not used directly with Oracle Identity Manager. **Note:** If you are configuring LDAP-Sync after configuring Oracle Identity Manager or by manually editing IT Resource Directory Server instance, use the LDAP URL corresponding to OVD against the Server URL, or leave it blank. In the latter case you should configure libOVD.	□
Ensure that the `jpsContextName` attribute value is set to oim in SOA and UMS configuration MBeans.	□
If you are deploying Oracle Identity Manager behind a Load Balancer or a Web Server, ensure that you have configured the Oracle Identity Manager front end URL and the SOA SOAP URL with the Load Balancer/WebServer URL.	□
If you are using SSL in the communication between Oracle Identity Manager and SOA, ensure that the URLs are configured to use HTTPS and that the keystores in use contain the appropriate certificates.	□
If SPML calls are not being processed, verify that the client invoking the SPML service is using a compatible Oracle Web Services Manager (Oracle WSM) client and server security policies.	□
If you are going to create custom scheduled tasks or make any changes to the default configuration of Oracle Identity Manager Scheduler, review “Creating Custom Scheduled Tasks” in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.	□
Ensure that the system property Display Certification or Attestation is set to Certification or Both to have certification enabled.	□
Ensure that the log level is set to warning or lower. **Note:** By default, the logging level in Oracle loggers is set to notification. In most cases, this log level is unnecessary and can be changed to warning (TRACE:32) or lower.	□
Ensure that the Catalog synchronized with base entities.	□
Ensure that you have determined the frequency of running the schedule task “Evaluate User Policies”. **Note:** By default, this scheduled task runs every 10 minutes.	□
Ensure that you have reviewed the Usage Recommendation guidelines in the documentation before using Oracle Identity Manager Connectors.	□
Ensure that the service account used for connectivity has rights to perform operations on the target.	□
Ensure that the appropriate firewall ports are open.	□
Ensure that the LDAP replication is configured in Safe-Read mode.	□
Ensure that the LDAP password policies are lenient when compared to Oracle Identity Manager password policies.	□

Table 4–1 (Cont.) Oracle Identity Manager Deployment Checklist

Requirement	Check when Verified
It is recommended that you increase the heap size and permgen memory for production environments and monitor the memory usage pattern. Based on the usage, you can choose to increase or decrease the memory settings. The following are the initial recommended values for the memory-related tuning parameters: ■ JVM Parameter: HotSpot JVM and JRockit JVM ■ Minimum Heap Size (Xms): 4GB ■ Maximum Heap Size (Xmx): 4GB ■ PermSize (-XX:PermSize): 500m (Not applicable for JRockit JVM) ■ PermGen size (-XX:MaxPermSize): 1GB (Not applicable for JRockit JVM)	□
Ensure that the SOA Coherence configuration for the Coherence cluster is done correctly. For more information about updating the SOA Coherence configuration for Coherence cluster, see "Updating the Coherence Configuration for the Coherence Cluster" in the *Oracle Fusion Middleware High Availability Guide*.	□
Ensure that the User Messaging Service (UMS) mail configuration for notifications is done correctly. For more information about using UMS for notifications, see "Using UMS for Notification" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.	□
Verify if the audit level system property `XL.UserProfileAuditDataCollection` is set to the correct audit level. For more information about the supported audit levels, see "Audit Levels" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*. For more information about modifying the value of the system property, see "Managing System Properties" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.	□
To avoid schema password expiration issues, verify that the password expiration policies for the database have been set appropriately. For more information, see "Options To Resolve The Expired OIM Schema Password In Oracle Database 11g (Doc ID 1326142.1)" on My Oracle Support.	□