Oracle® Fusion Middleware

Verifying Your Oracle Identity and Access Management Environment

11*g* Release 2 (11.1.2.3.0)

E57636-01

April 2015

This guide contains installation and deployment checklists for Oracle Identity and Access Management 11*g* Release 2 (11.1.2.3.0) components.

ORACLE

Oracle Fusion Middleware Verifying Your Oracle Identity and Access Management Environment, 11*g* Release 2 (11.1.2.3.0)

E57636-01

Primary Author: Rekha Kamath

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

Contents

Preface

This preface provides supporting information for *Verifying Your Oracle Identity and Access Management Environment* and includes the following topics:

Audience

Verifying Your Oracle Identity and Access Management Environment 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 and Access Management components. For installation and configuration procedures, refer to the *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

- *Administrator's Guide*
- *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 Administering 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 Introduction

This guide is divided into two parts.

Part I, "Oracle Identity and Access Environment Health Check Utility"

Part I provides information about the Oracle Identity and Access Environment Health Check Utility. This is a tool that can be used to automatically test various configurations, environment setup, tuning information, and so on in an Oracle Identity and Access Management environment. The Oracle Identity and Access Environment Health Check Utility can be executed at any time for verifying the details of your environment. The tool retrieves relevant data from your environment and compares it with an Oracle recommended benchmark value for each of the settings. The tool then generates XML and HTML reports, which provide detailed information for each of the items tested.

Part II, "Manual Checklist"

Part II provides information about the manual checklists for the Oracle Identity and Access Management deployment. These checklists can be used as common guidelines for deploying Oracle Identity and Access Management in production.

Part I

Oracle Identity and Access Environment Health Check Utility

Part I of this guide provides information about the Oracle Identity and Access Environment Health Check Utility. It introduces various directories used by the tool, the xml files and plugins that are used for executing the tool, and includes information about the command used for executing the tool. The second chapter covers information about analyzing the report generated by the Oracle Identity and Access Environment Health Check Utility.

Part I contains the following chapters:

2

Understanding the Oracle Identity and Access Environment Health Check Utility

This chapter provides information about the Oracle Identity and Access Environment Health Check Utility. In addition, it includes information about the directories and plugins used by the utility.

This chapter includes the following sections.

2.1 What is the Oracle Identity and Access Environment Health Check Utility

The Oracle Identity and Access Environment Health Check Utility is used to check the technical aspects of your Oracle Identity and Access Management setup and provides an overall measurement of various settings and configurations of your environment.

For example, it verifies network connectivity between different servers, ensures that database index configuration is consistent across servers, and examines error log files.

If you are using the Oracle Identity and Access Management Life Cycle Management (LCM) tools, then the Oracle Identity and Access Environment Health Check Utility is automatically invoked as part of the pre-installation and post-configuration steps.

Further, after installing and configuring Oracle Identity and Access Management Life Cycle Management tools, the product-specific plugins can be executed at any time to verify the health of the deployment.

If you are manually installing and configuring Oracle Identity and Access Management, then you can execute the Health Check Utility on-demand, at various stages, such as pre-installation, post-installation, pre-upgrade, post-configuration, and so on.

Note:

For more information about executing the Health Check Utility, see the following:

- "Running the Health Check Utility to Verify Basic System Requirements" in the *Deployment Guide for Oracle Identity and Access Management*.
- "Running the Environment Health Check Utility After Configuration" in the *Installation Guide for Oracle Identity and Access Management*.

For more information about the automated deployment method, see "About the Automated Deployment of Oracle Identity and Access Management" in the *Deployment Guide for Oracle Identity and Access Management*.

2.2 About Health Check Utility Directories, Plugins, and Properties File

This section provides information about the following:

- Understanding the Health Check Utility Directory Structure
- Understanding the Health Check Utility XML Files and Plugins
- Understanding the idmhc.properties File of the Health Check Utility

2.2.1 Understanding the Health Check Utility Directory Structure

The Oracle Identity and Access Environment Health Check Utility uses specific directories for executing plugins and for storing log files. Regardless of whether you run the utility from the automated LCM tools or the manual installation procedure, these directories are installed into the *healthcheck* directory inside the Oracle home.

The table below provides information about these directories.

Note: The Oracle home directory is created when you install Oracle Identity and Access Management using the Oracle Identity and Access Management Installer or when you run the Life Cycle Management deployment wizard.

Table 2–1 Environment Health Check Utility Directories

Directory	Description
healthcheck/bin	Contains the execution scripts (idmhc.sh and idmhc.bat) and the idmhc.properties file. For more information about the idmhc.sh and idmhc.bat commands, see Section 2.3, "Executing the Oracle Identity and Access Environment Health Check Utility." For more information about the idmhc.properties file, see Section 2.2.3, "Understanding the idmhc.properties File of the Health Check Utility."

Table 2–1 (Cont.) Environment Health Check Utility Directories

Directory	Description
`healthcheck/config`	Contains the xml files that must be provided as input when running the `idmhc.sh` and `idmhc.bat` commands. For more information about the xml files and the plugins included in these files, see Section 2.2.2, "Understanding the Health Check Utility XML Files and Plugins."
`healthcheck/lib`	Contains relevant jar files.
`current_working_directory``/logs/healthchecker`	Contains log files. If a log directory is not specified when you run the Environment Health Check Utility, log files are stored in the *`current_working_directory`*`/logs/healthchecker` directory by default. For more information, see Section 3.1, "Oracle Identity and Access Environment Health Check Summary Reports."

2.2.2 Understanding the Health Check Utility XML Files and Plugins

This section provides information about all the xml files and the plugins that are used when the Oracle Identity and Access Environment Health Check Utility is executed.

The Oracle Identity and Access Environment Health Check Utility is run, either from the command line or by the automated LCM tools, by executing the `idmhc.sh` command (`idmhc.bat` on Windows).

The xml file that is passed to the Environment Health Check Utility contains the plugins that need to be executed. All relevant xml files reside in the *`ORACLE_HOME`*`/healthcheck/config` directory.

There are xml files for generic tests, such as `PreInstallChecks_mandatory.xml`, `PreInstallChecks_mandatory_manual.xml`, `PreInstallChecks_db.xml`, `PreInstallChecks_optional.xml`, and `PostInstallChecks.xml`. There are also xml files that are product specific, such as `PostInstallChecks_oim.xml`, `PostConfigChecks_oudhost.xml`, and `PostInstallChecks_oam.xml`.

Each xml file contains a set of plugins that are covered in the following sections:

- PreInstallChecks_mandatory.xml
- PreInstallChecks_mandatory_manual.xml
- PreInstallChecks_db.xml
- PreInstallChecks_optional.xml
- PostInstallChecks.xml
- PostInstallChecks_oim.xml (Oracle Identity Manager)
- PostConfigChecks_oudhost.xml (Oracle Unified Directory)
- PostInstallChecks_oam.xml (Oracle Access Manager)

2.2.2.1 PreInstallChecks_mandatory.xml

The `PreInstallChecks_mandatory.xml` file includes several mandatory prerequisite checks that must be executed before installing an Oracle Identity and Access

Management environment. The table below provides information about the plugins included in this xml file.

Table 2–2 PreInstallChecks_mandatory.xml Plugins

Plugin	Description
`FreeMemoryCheck`	Checks whether the host has the recommended free main memory before performing an installation. As part of Oracle Identity and Access Management automated installer integration, the Health Check Utility automatically finds the products that are getting installed on a particular host, calculates the benchmark value for free memory, and then validates it. **Note**: This plugin is applicable only if you are using the Life Cycle Management (LCM) tools for installing Oracle Identity and Access Management.
`KernelParamCheck`	Checks the kernel parameters, such as `shmmax`, `shmall`, maximum file descriptor limit, hard and soft limits of number of files open, hard and soft limits of number of processes, and so on.
`OSCheck`	Checks Operating System, Release, and Operating System architecture of the host, and compares that information against the benchmark value and then validates it.
`FreePortsCheck`	Checks whether the ports are free. The Environment Health Check Utility automatically finds the ports that need to be free on the current host. If you are manually executing the utility, you must update the `PreInstallChecks_mandatory.xml` file with a semicolon-separated list of ports that you want to check in the `invoke` element under `FreePortsCheck`. For example: `<plugin id="FreePortsCheck" description="Check whether ports are free" invoke="`**`7001;7101`**`" plugin.class="oracle.idm.healthcheck.plugins.freeportcheck.FreePortsCheckPlugin" class.path="$HC_LOCATION/lib/idmhcplugins.jar" stoponerror="false"/>` If ports are not provided in this file, the check will be skipped.
`DiskSpaceCheck`	Checks whether the host has the recommended available disk space before performing an installation. The Environment Health Check Utility automatically finds the products that are getting installed on a particular host, calculates the benchmark value for disk space, and then validates it.

Table 2–2 (Cont.) PreInstallChecks_mandatory.xml Plugins

Plugin	Description
HostsCheck	Checks whether the hosts are reachable. The Environment Health Check Utility automatically finds the hosts that need to be pinged. If you are manually executing the utility, you must update the PreInstallChecks_mandatory.xml file with a semicolon-separated list of host names that you want to check in the invoke element under HostsCheck. For example: <plugin id="HostsCheck" description="Check Reachability of hosts" invoke="**host1.example.com;host2.example.com**" plugin.class="oracle.idm.healthcheck.plugins. hostcheck.PingHostsPlugin" class.path="$HC_LOCATION/lib/idmhcplugins.jar" stoponerror="false"/> If the host names are not provided in this file, the check will be skipped.
DBParameterCheck	Validates values of various predefined parameters on Oracle Identity Manager (OIM), Oracle Internet Directory (OID), and Oracle Access Manager (OAM) databases installed on the host. In addition, it verifies character set, Oracle Text, Oracle JVM, and XATRANS View. In addition, details such as hosts, ports, user names, and passwords are automatically obtained by the Environment Health Check Utility.
DBSchemaCheck	Checks whether the host has the required database schema in its database as part of product installation (OIM, OID, or OAM). These properties are automatically obtained by the Environment Health Check Utility.
JDKCheck	Checks whether the host has the recommended Java Virtual Machine version.
PackageInstalledCheck	Checks whether the host has all required packages and patches installed.

Table 2–2 (Cont.) PreInstallChecks_mandatory.xml Plugins

Plugin	Description
PermissionsCheck	Checks whether specific file directories have recommended read, write, and execute permissions. The permission check is done on repo location, idmtop, shared config and lcmdir. If you are manually executing the utility, you must update the PreInstallChecks_mandatory.xml file with a semicolon-separated list of directory paths and permissions that you want to check in the invoke element under PermissionsCheck. Provide the directory paths and permissions in the following format: *directory_path1=permissions_required;directory_path2=permissions_required* Where *permissions_required* is some combination of R (Read), W (Write), and X (Execute) permissions. For example: <plugin id="PermissionsCheck" description="Verifying Path Permissions" invoke="**/scratch/install=RWX;/u01/idmtop=RW**" plugin.class="oracle.idm.healthcheck.plugins.verifyPermissions.PermissionsPlugin" class.path="$HC_LOCATION/lib/idmhcplugins.jar" stoponerror="false"/> If directory paths and permissions are not provided in this file, the check will be skipped.
XClockCheck	Checks whether other user interfaces are displayed in the environments.

2.2.2.2 PreInstallChecks_mandatory_manual.xml

The PreInstallChecks_mandatory_manual.xml file includes several mandatory prerequisite checks that must be manually executed before installing an Oracle Identity and Access Management environment. The table below provides information about the plugins included in this xml file.

Table 2–3 PreInstallChecks_mandatory_manual.xml Plugins

Plugin	Description
OSCheck	Checks Operating System, Release, and Operating System architecture of the host, compares that information against the benchmark value, and then validates it.
JDKCheck	Checks whether the host has the recommended Java Virtual Machine version.
PackageInstalledCheck	Checks whether the host has all required packages and patches installed.
XClockCheck	Checks whether other user interfaces are displayed in the environments.

2.2.2.3 PreInstallChecks_db.xml

The PreInstallChecks_db.xml file includes a prerequisite check that must be manually executed on the Oracle Identity Manager database host before installing an

Oracle Identity and Access Management environment. The table below provides information about the plugin included in this xml file.

Table 2–4 PreInstallChecks_db.xml Plugin

Plugin	Description
DBPatchCheck	Checks whether the mandatory database patches are applied on the database host. For information about any patches that you must apply, see "Downloading and Applying Required Patches" in the *Release Notes for Oracle Identity Management*.

2.2.2.4 PreInstallChecks_optional.xml

The PreInstallChecks_optional.xml file includes generic prerequisite checks that are executed before installing an Oracle Identity and Access Management environment. The table below provides information about the plugins included in this xml file.

Table 2–5 PreInstallChecks_optional.xml Plugins

Plugin	Description
KernelParamCheck	Checks the kernel parameters, such as shmmax, shmall, maximum file descriptor limit, hard and soft limits of number of files open, hard and soft limits of number of processes, and so on.
ProcessorCheck	Checks the processor and the number of cores on the host, and verifies if it meets the recommended values.

2.2.2.5 PostInstallChecks.xml

The PostInstallChecks.xml file includes generic post-installation and post-configuration checks that must be manually executed after setting up an Oracle Identity and Access Management environment. The table below provides information about the plugins included in this xml file.

Table 2–6 PostInstallChecks.xml Plugins

Plugin	Description
IDStoreCheck	Verifies whether the LDAP identity store is up and running, and whether a successful connection can be established to that server.
WLSCheck	Verifies the Oracle WebLogic Server configuration and ordering of authenticators. In addition, it checks if the WLSAdmins group is added to the list of WebLogic Administrators and if the WebLogic Server domain is running in production mode.
IDStoreInLdapCheck	Checks whether the identity store is properly configured for other components, such as Oracle Access Manager and Oracle Identity Manager, to work with this identity store. The Environment Health Check Utility checks if any attribute or properties are missing in the configuration. **Note**: This plugin is applicable only if you used the Life Cycle Management (LCM) tools to install Oracle Identity and Access Management.

Table 2–6 (Cont.) PostInstallChecks.xml Plugins

Plugin	Description
ConsoleUrlCheck	Verifies whether the product console URLs are up, and checks for OIM, OAM, WebLogic, and server consoles. The URLs are automatically formed and checked by the Environment Health Check Utility. **Note**: This plugin is applicable only if you used the Life Cycle Management (LCM) tools to install Oracle Identity and Access Management.
DataSourcesCheck	Verifies if the Data sources configured in WebLogic Server are functioning properly.

2.2.2.6 PostInstallChecks_oim.xml (Oracle Identity Manager)

The PostInstallChecks_oim.xml file includes post-installation checks specific to Oracle Identity Manager that must be manually executed after setting up an Oracle Identity and Access Management environment. The table below provides information about the plugins included in this xml file.

Table 2–7 PostInstallChecks_oim.xml Plugin

Plugin	Description
OIMSOAConfigCheck	Verifies all the SOA configurations, such as ProviderURL, RmiURL, and JpsContextName. Checks the SOA coherence configuration if the environment is clustered. In addition, the plugin checks if SOAAdministrator has SOAAdmin role.
OIMFrontEndURLCheck	Validates OIMFrontEndURL and OIMExternalFrontEndURL from the Discovery MBean against user provided values.
OIMUMSConfigurationCheck	Checks the UserMessagingService configuration, gets all the details of the UMS account, and tries to connect to the account using the password provided for the account.
OIMCertificationCheck	Checks whether the System Property **Identity Auditor Feature set Availability** is set to true. If set to false, the plugin will fail.
OIMUDFIndexCheck	Checks if all the user defined attributes that are searchable have corresponding indexes defined for them. If indexes are not defined, the plugin will fail.
OIMAuthorizationSeedCheck	This plugin verifies that during the installation phase, after the Repository Creation Utility was run to create Oracle Identity Manager and its dependent schemas, the authorization policies or application stripe is seeded correctly using the APM-UI cluster.
OIMCacheConfigCheck	Checks to ensure that the XMLConfig.cacheConfig Clustered MBean property is set to **true**.
OIMCatalogSynchronizationCheck	Checks to ensure that the Catalog is synchronized with base entities (Entitlements, Roles and ApplicationInstances).
OIMJDBCConnectionPoolParamsCheck	Checks recommended values for the JDBC Connection Pool.

Table 2–7 (Cont.) PostInstallChecks_oim.xml Plugin

Plugin	Description
OIMWorkManagerCheck	Checks to ensure that the properties Maximum Threads Constraint for work managers OIMMDBWorkManager and OIMUIWorkManager are set to 6 and 10, respectively.
OIMJMSServerCheck	Checks whether the default values of Message Buffer Size and Messages Maximum properties are set to the recommended values. ■ Message Buffer Size: 200 MB (209715200 bytes) ■ Messages Maximum: -1 or any number not less than 400000.
OIMApplicationConnectivityCheck	Checks whether the service account used for connectivity has rights to perform operations on the target.

2.2.2.7 PostConfigChecks_oudhost.xml (Oracle Unified Directory)

The PostConfigChecks_oudhost.xml file includes post-configuration checks specific to Oracle Unified Directory that must be manually executed after Oracle Unified Directory has been installed and configured. The table below provides information about the plugins included in this xml file:

Table 2–8 PostConfigChecks_oudhost.xml Plugins

Plugin	Description
OUDLogPlugin	Examines Oracle Unified Directory (OUD) error log files logs/server.out and logs/errors, and confirms that no errors are reported. **Note:** As this plugin is run post-configuration, it will only check the error log files. If the logs have already rotated and created errors.<date> files, those files will not be checked.
OUDIndexPlugin	If OUD is deployed with replication enabled, this plugin ensures that the indexes are consistent on all the OUD replicated servers. **Note:** This check will only trigger warnings (and not failures) as it is acceptable to have inconsistent index definitions across replicated servers. Index inconsistency may cause issues if binary copy is used to initialize or restore servers, but will not harm the server.
ReplicationCheck	If Oracle Unified Directory is deployed with replication enabled, this plugin ensures that all the Oracle Unified Directory replicated servers are reachable and that the replication does not show any issues, such as missing changes or inconsistent number.

2.2.2.8 PostInstallChecks_oam.xml (Oracle Access Manager)

The PostInstallChecks_oam.xml file includes post-installation checks specific to Oracle Access Manager (OAM) that must be manually executed after setting up an Oracle Identity and Access Management environment. The table below provides information about the plugins included in this xml file.

Table 2–9 PostnstallChecks_oam.xml

Plugin	Description
IDMDomainAgentCheckPlugin	Ensures that IDMDomainAgent and/or IAMSuiteAgent is removed from the list of authenticators in the Oracle Access Manager (OAM) domain.
JVMValueCheckPlugin	Checks whether the XMS and XMX values are set to same level.
OamServerClusterCheckPlugin	Checks whether there is a cluster of OAM servers.

2.2.3 Understanding the idmhc.properties File of the Health Check Utility

This section provides information about the idmhc.properties file of the Environment Health Check Utility.

The Environment Health Check Utility uses the idmhc.properties file located in the healthcheck/bin directory to run the plugins listed in the XML files of the utility. The idmhc.properties file contains parameters that define the connectivity of identity store, schemas for various components of the Oracle Identity and Access Management suite, WebLogic Server schemas, Oracle Unified Directory (OUD) checks, and so on.

Example 2–1 displays the contents of the idmhc.properties file. Table 2–10 provides a description of the parameters listed in the idmhc.properties file.

> **Note:** You must provide certain passwords to the Health Check Utility for the utility to run successfully. Passwords can be set in the idmhc.properties file before running the utility. However, it is strongly recommended that you do not specify or store any of your passwords in this file. When executed, the Health Check Utility prompts you to enter values for any required passwords.

Example 2–1 Sample idmhc.properties File

```
# Below parameters are needed for IDStore connectivity plugin
IDSTORE_HOST:
IDSTORE_PORT:
IDSTORE_BINDDN:
# If below SSL port is provided, then SSL connectivity will be validated. Not
mandatory.
IDSTORE_SSL_PORT:
IDSTORE_GROUPSEARCHBASE:
IDSTORE_USERSEARCHBASE:
IDSTORE_SYSTEMIDSEARCHBASE:

#Below parameters are needed for OID Schema Connecitivity
OID_DB_HOST:
OID_DB_PORT:
OID_DB_SERVICE_NAME:
OID_DB_USER:
OID_DB_SYS_USER:
OID_DB_CONNECTION_STRING:
#Format of Connection String - db1^db2 where db1 is host:port@servicename .

#Below parameters are needed for OAM Schema Connecitivity
OAM_DB_HOST:
OAM_DB_PORT:
OAM_DB_SERVICE_NAME:
```

```
OAM_DB_USER:
OAM_DB_SYS_USER:
OAM_DB_CONNECTION_STRING:
#Format of Connection String - db1^db2 where db1 is host:port@servicename .

#Below parameters are needed for OIM Schema Connecitivity
OIM_DB_HOST:
OIM_DB_PORT:
OIM_DB_SERVICE_NAME:
OIM_DB_USER:
OIM_DB_SYS_USER:
OIM_DB_CONNECTION_STRING:
#Format of Connection String - db1^db2 where db1 is host:port@servicename .

#Below parameters are needed for OMSM Schema Connecitivity
OMSM_DB_HOST:
OMSM_DB_PORT:
OMSM_DB_SERVICE_NAME:
OMSM_DB_USER:
OMSM_DB_CONNECTION_STRING:
#Format of Connection String - db1^db2 where db1 is host:port@servicename .

#Below Parameters are needed for OAM Weblogic Server Connectivity
OAM_WLS_ADMINSERVER_HOST:
#Either port or SSL port is mandatory
OAM_WLS_ADMINSERVER_PORT:
OAM_WLS_ADMINSERVER_SSLPORT:
OAM_WLSADMIN_USER:
OAM_WLS_ADMINSERVER_TRUSTSTORE:
OAM_WLS_ADMINSERVER_TRUSTSTORE_PASSPHRASE:


#Below Parameters are needed for OIM Weblogic Server Connectivity
OIM_WLS_ADMINSERVER_HOST:
#Either port or SSL port is mandatory
OIM_WLS_ADMINSERVER_PORT:
OIM_WLS_ADMINSERVER_SSLPORT:
OIM_WLSADMIN_USER:
OIM_WLS_ADMINSERVER_TRUSTSTORE:
OIM_WLS_ADMINSERVER_TRUSTSTORE_PASSPHRASE:

#ORACLE_HOME in a database host. Required to check recommended patches via
PreInstallChecks_dbhost.xml
#eg: /u01/app/aime/product/11.2.0/dbhome_1
ORACLE_HOME:

#Below parameters are needed for OIM Server Connectivity
SOASERVER_HOST:
OIMSERVER_HOST:
OIMSERVER_PORT:
OIMSERVER_SSL_PORT:
OIMADMIN_USERNAME:
SOAADMIN_USERNAME:
OIMSERVER_SERVER_TYPE:
SOASERVER_PORT:
SOASERVER_SSL_PORT:
# Refer to the Enterprise Deployment Guidelines for understanding relevant
details.
OIMSERVER_INTERNALLOADBALANCERURL:
OIMSERVER_EXTERNALLOADBALANCERURL:
```

```
# The home directory for the SOA suite installed on the machine.
# eg:  /u01/app/Oracle/Middleware/Oracle_SOA
SOA_HOME:
TRUST_STORE:
TRUST_STORE_PASSPHRASE:
TRUST_STORE_TYPE:JKS

#Below parameters are needed for OUD checks
OUD_HOST:
OUD_ADMINPORT:
# AdminUID is the uid of the global administrator configured for replication
# Usual value is OUD_ADMINUID: admin
# Leave empty if replication is not configured for this instance (the plugins
# related to replication will be skipped)
OUD_ADMINUID:
# OUD_HOME is the path to OUD installation, for example /app/idm/Oracle_OUD1
# This property is optional. If not specified, it will be set to
# $HC_LOCATION/.. where HC_LOCATION is the path to healthcheck
#OUD_HOME:
# OUD_INSTANCE_HOME is the path to OUD instance, for example /app/idm/asinst_1
OUD_INSTANCE_HOME:

#HTTP proxy server details, to be provided if proxy is configured
HTTP_PROXY_HOST:
HTTP_PROXY_PORT:
HTTP_PROXY_USERNAME:
HTTP_PROXY_PASSWORD

#Enter products installed in the current host in a comma separated manner.Valid
options are OIM,OAM,OMSM,WEB,LDAP
HOST_TYPE:
```

Table 2–10 Parameters Listed in idmhc.properties File

Parameter	Description	Required For
Parameters for LDAP and Oracle Database		
IDSTORE_HOST	Enter the host name of the Identity and Policy Store directory for LDAP connectivity.	IDStoreCheck in PostInstallChecks.xml
IDSTORE_PORT	Enter the port of the Identity and Policy Store directory for LDAP connectivity.	IDStoreCheck in PostInstallChecks.xml
IDSTORE_BINDDN	Enter the Identity and Policy Store directory Bind DN for LDAP authentication.	IDStoreCheck in PostInstallChecks.xml
IDSTORE_PASSWORD	Enter the Identity and Policy Store directory password for LDAP Authentication. This parameter is optional. If not provided, you will be prompted for this password when you run the Health Check Utility.	IdStoreInLdapCheck and IDStoreCheck in PostInstallChecks.xml
IDSTORE_SSL_PORT	Enter the Identity and Policy Store directory SSL mode port for LDAP connectivity. This parameter is optional. The details of this parameter will be validated by the Health Check Utility if provided.	IDStoreCheck and IdStoreInLdapCheck in PostInstallChecks.xml

Table 2–10 (Cont.) Parameters Listed in idmhc.properties File

Parameter	Description	Required For
IDSTORE_ GROUPSEARCHBASE	Enter the Identity and Policy Store directory DN for Group Search Base.	IdStoreInLdapCheck in PostInstallChecks.xml
IDSTORE_ USERSEARCHBASE	Enter the Identity and Policy Store directory DN for User Search Base.	IdStoreInLdapCheck in PostInstallChecks.xml
IDSTORE_ SYSTEMIDSEARCHBASE	Enter the Identity and Policy Store directory DN for *SYSTEMID* Search Base.	IdStoreInLdapCheck in PostInstallChecks.xml
OID_DB_HOST	Enter the host name of the system where the Oracle Internet Directory (OID) database is installed.	DBParameterCheck and DBSchemaCheck in PreInstallChecks_ mandatory.xml
OID_DB_PORT	Enter the port of the OID database machine.	DBParameterCheck and DBSchemaCheck in PreInstallChecks_ mandatory.xml
OID_DB_SERVICE_ NAME	Enter the service name of the OID database.	DBParameterCheck and DBSchemaCheck in PreInstallChecks_ mandatory.xml
OID_DB_USER	Enter the prefix name of the OID database schema.	DBSchemaCheck in PreInstallChecks_ mandatory.xml
OID_DB_PASSWORD	Enter the password of the OID database schema. This parameter is optional. If not provided, you will be prompted for this password when you run the Health Check Utility.	DBSchemaCheck in PreInstallChecks_ mandatory.xml
OID_DB_SYS_USER	Enter the system user name of the OID database.	DBParameterCheck in PreInstallChecks_ mandatory.xml
OID_DB_SYS_ PASSWORD	Enter the system password of the OID database. This parameter is optional. If not provided, you will be prompted for this password when you run the Health Check Utility.	DBParameterCheck in PreInstallChecks_ mandatory.xml
OID_DB_ CONNECTION_ STRING	Enter the connection string for OID RAC database in the following format: db1^db2 where db1 is *host:port@servicename*	DBParameterCheck and DBSchemaCheck in PreInstallChecks_ mandatory.xml
OAM_DB_HOST	Enter host name of the system where the Oracle Access Manager (OAM) database is installed.	DBParameterCheck and DBSchemaCheck in PreInstallChecks_ mandatory.xml
OAM_DB_PORT	Enter the port of the OAM database machine.	DBParameterCheck and DBSchemaCheck in PreInstallChecks_ mandatory.xml

Table 2–10 (Cont.) Parameters Listed in idmhc.properties File

Parameter	Description	Required For
OAM_DB_SERVICE_NAME	Enter the service name of the OAM database.	DBParameterCheck and DBSchemaCheck in PreInstallChecks_mandatory.xml
OAM_DB_USER	Enter the prefix name of the OAM database schema.	DBSchemaCheck in PreInstallChecks_mandatory.xml
OAM_DB_PASSWORD	Enter the password of the OAM database schema. This parameter is optional. If not provided, you will be prompted for this password when you run the Health Check Utility.	DBSchemaCheck in PreInstallChecks_mandatory.xml
OAM_DB_SYS_USER	Enter the system user name of the OAM database.	DBParameterCheck in PreInstallChecks_mandatory.xml
OAM_DB_SYS_PASSWORD	Enter the system password of the OAM database. This parameter is optional. If not provided, you will be prompted for this password when you run the Health Check Utility.	DBParameterCheck in PreInstallChecks_mandatory.xml
OAM_DB_CONNECTION_STRING	Enter the connection string for OAM RAC database in the following format: db1^db2 where db1 is *host*:*port*@*servicename*	DBParameterCheck and DBSchemaCheck in PreInstallChecks_mandatory.xml
OIM_DB_HOST	Enter the host name of the system where the Oracle Identity Manager (OIM) database is installed.	DBParameterCheck and DBSchemaCheck in PreInstallChecks_mandatory.xml PostInstallChecks_oim.xml
OIM_DB_PORT	Enter the port of the OIM database machine.	DBParameterCheck and DBSchemaCheck in PreInstallChecks_mandatory.xml PostInstallChecks_oim.xml
OIM_DB_SERVICE_NAME	Enter the service name of the OIM database.	DBParameterCheck and DBSchemaCheck in PreInstallChecks_mandatory.xml PostInstallChecks_oim.xml
OIM_DB_USER	Enter the prefix name of the OIM database schema.	DBSchemaCheck in PreInstallChecks_mandatory.xml PostInstallChecks_oim.xml
OIM_DB_PASSWORD	Enter the password of the OIM database schema. This parameter is optional. If not provided, you will be prompted for this password when you run the Health Check Utility.	DBSchemaCheck in PreInstallChecks_mandatory.xml PostInstallChecks_oim.xml

Table 2–10 (Cont.) Parameters Listed in idmhc.properties File

Parameter	Description	Required For
OIM_DB_SYS_USER	Enter the system user name of the OIM database.	DBParameterCheck in PreInstallChecks_mandatory.xml
OIM_DB_SYS_PASSWORD	Enter the system password of the OIM database. This parameter is optional. If not provided, you will be prompted for this password when you run the Health Check Utility.	DBParameterCheck in PreInstallChecks_mandatory.xml
OIM_DB_CONNECTION_STRING	Enter the connection string for OIM RAC database in the following format: db1^db2 where db1 is *host:port@servicename*	DBParameterCheck and DBSchemaCheck in PreInstallChecks_mandatory.xml
OMSM_DB_HOST	Enter the host name of the system where the Oracle Mobile Security Manager (OMSM) database is installed.	DBSchemaCheck in PreInstallChecks_mandatory.xml
OMSM_DB_PORT	Enter the port of the OMSM database machine.	DBSchemaCheck in PreInstallChecks_mandatory.xml
OMSM_DB_SERVICE_NAME	Enter the service name of the OMSM database.	DBSchemaCheck in PreInstallChecks_mandatory.xml
OMSM_DB_USER	Enter the prefix name of the OMSM database schema.	DBSchemaCheck in PreInstallChecks_mandatory.xml
OMSM_DB_PASSWORD	Enter the password of the OMSM database schema. This parameter is optional. If not provided, you will be prompted for this password when you run the Health Check Utility.	DBSchemaCheck in PreInstallChecks_mandatory.xml
OMSM_DB_CONNECTION_STRING	Enter the connection string for OMSM RAC database in the following format: db1^db2 where db1 is *host:port@servicename*	DBSchemaCheck in PreInstallChecks_mandatory.xml
Parameters for Oracle Access Manager Oracle WebLogic Server Connectivity		
OAM_WLS_ADMINSERVER_HOST	Enter the host name of the OAM Domain of the Oracle Weblogic Administration Server.	WLSCheck and DataSourcesCheck in PostInstallChecks.xml PostInstallChecks_oam.xml
OAM_WLS_ADMINSERVER_PORT	Enter the OAM Domain port of the Oracle Weblogic Administration Server. This parameter is optional only if you specified a value for the OAM_WLS_ADMINSERVER_SSLPORT property.	WLSCheck and DataSourcesCheck in PostInstallChecks.xml PostInstallChecks_oam.xml

Table 2–10 (Cont.) Parameters Listed in idmhc.properties File

Parameter	Description	Required For
OAM_WLS_ ADMINSERVER_ SSLPORT	Enter the OAM Domain SSL port of the Oracle WebLogic Server Administration Server. This parameter is optional only if you specified a value for the OAM_WLS_ADMINSERVER_PORT property.	WLSCheck and DataSourcesCheck in PostInstallChecks.xml PostInstallChecks_ oam.xml
OAM_WLSADMIN_ USER	Enter the OAM Domain user name of the Oracle WebLogic Administration Server.	WLSCheck and DataSourcesCheck in PostInstallChecks.xml PostInstallChecks_ oam.xml
OAM_WLSADMIN_ PASSWORD	Enter the OAM Domain password of the Oracle WebLogic Administration Server. This parameter is optional. If not provided, you will be prompted for this password when you run the Health Check Utility.	WLSCheck and DataSourcesCheck in PostInstallChecks.xml PostInstallChecks_ oam.xml
OAM_WLS_ ADMINSERVER_ TRUSTSTORE	Enter the absolute path to the OAM Domain Trust store file of the Oracle WebLogic Administration Server. The details of this parameter must be provided if SSL port is used.	WLSCheck and DataSourcesCheck in PostInstallChecks.xml
OAM_WLS_ ADMINSERVER_ TRUSTSTORE_ PASSPHRASE	Enter the password of the OAM Domain Trust store file of the Oracle WebLogic Administration Server. The details of this parameter must be provided if SSL port is used. This parameter is optional. If not provided, you will be prompted for this password when you run the Health Check Utility.	WLSCheck and DataSourcesCheck in PostInstallChecks.xml
Parameters for Oracle Identity Manager Oracle WebLogic Server Connectivity		
OIM_WLS_ ADMINSERVER_HOST	Enter the host name of the OIM Domain of the Oracle WebLogic Administration Server.	WLSCheck and DataSourcesCheck in PostInstallChecks.xml PostInstallChecks_ oim.xml
OIM_WLS_ ADMINSERVER_PORT	Enter the OIM Domain port of the Oracle Weblogic Administration Server. This parameter is optional only if you specified a value for the OIM_WLS_ADMINSERVER_SSLPORT property.	WLSCheck and DataSourcesCheck in PostInstallChecks.xml PostInstallChecks_ oim.xml
OIM_WLS_ ADMINSERVER_ SSLPORT	Enter the OIM Domain SSL port of the Oracle WebLogic Administration Server. This parameter is optional only if you specified a value for the OIM_WLS_ADMINSERVER_PORT property.	WLSCheck and DataSourcesCheck in PostInstallChecks.xml PostInstallChecks_ oim.xml

Table 2–10 (Cont.) Parameters Listed in idmhc.properties File

Parameter	Description	Required For
OIM_WLSADMIN_USER	Enter the OIM Domain user name of the Oracle WebLogic Administration Server.	WLSCheck and DataSourcesCheck in PostInstallChecks.xml PostInstallChecks_oim.xml
OIM_WLSADMIN_PASSWORD	Enter the OIM Domain password of the Oracle WebLogic Administration Server. This parameter is optional. If not provided, you will be prompted for this password when you run the Health Check Utility.	WLSCheck and DataSourcesCheck in PostInstallChecks.xml PostInstallChecks_oim.xml
OIM_WLS_ADMINSERVER_TRUSTSTORE	Enter the absolute path to the OIM Domain Trust store file of the Oracle WebLogic Administration Server. The details of this parameter must be provided if SSL port is used.	WLSCheck and DataSourcesCheck in PostInstallChecks.xml
OIM_WLS_ADMINSERVER_TRUSTSTORE_PASSPHRASE	Enter the password of the OIM Domain Trust store file of the Oracle WebLogic Administration Server. The details of this parameter must be provided if SSL port is used. This parameter is optional. If not provided, you will be prompted for this password when you run the Health Check Utility.	WLSCheck and DataSourcesCheck in PostInstallChecks.xml
Parameters for HTTP Proxy Server		
HTTP_PROXY_HOST	Enter the host name of the HTTP proxy server.	
HTTP_PROXY_PORT	Enter the port of the HTTP proxy server.	
HTTP_PROXY_USERNAME	Enter the user name of the HTTP proxy server.	
HTTP_PROXY_PASSWORD	Enter the password of the HTTP proxy server. This parameter is optional. If not provided, you will be prompted for this password when you run the Health Check Utility.	
Parameters for Manual Installation Only		
HOST_TYPE	Enter the products installed on the current host. Use commas to separate the products. This parameter is required to perform disk space and memory checks in a manual deployment scenario. For example: OIM,OAM,OMSM,WEB,LDAP	FreeMemoryCheck and DiskSpaceCheck in PreInstallChecks_mandatory.xml
ORACLE_HOME	Enter the absolute path of the Oracle home directory on the database host. This is the Oracle home where the Oracle Identity Manager database is installed. For example, /u01/app/aime/product/11.2.0/dbhome_1. This parameter is required to manually execute PreInstallChecks_dbhost.xml on the database host to check whether the mandatory database patches are applied on the database.	DBPatchCheck in PreInstallChecks_db.xml
Parameters for Oracle Identity Manager		

Table 2–10 (Cont.) Parameters Listed in idmhc.properties File

Parameter	Description	Required For
SOASERVER_HOST	Enter the host name of the Managed Server hosting Oracle SOA.	PostInstallChecks_oim.xml
OIMSERVER_HOST	Enter the host name of the Managed Server hosting Oracle Identity Manager.	PostInstallChecks_oim.xml
OIMSERVER_PORT	Specify the default TCP port that the Managed Server hosting Oracle Identity Manager uses to listen for regular (non-SSL) incoming connections.	PostInstallChecks_oim.xml
OIMSERVER_SSL_PORT	Specify the default TCP port that the Managed Server hosting Oracle Identity Manager uses to listen for SSL connections.	PostInstallChecks_oim.xml
OIMADMIN_USERNAME	Enter the Oracle Identity Manager administrator user name.	PostInstallChecks_oim.xml
OIMADMIN_PASSWORD	Enter the Oracle Identity Manager administrator password. This parameter is optional. If not provided, you will be prompted for this password when you run the Health Check Utility.	PostInstallChecks_oim.xml
SOAADMIN_USERNAME	Enter the SOA administrator user name.	PostInstallChecks_oim.xml
SOAADMIN_PASSWORD	Enter the SOA administrator password. This parameter is optional. If not provided, you will be prompted for this password when you run the Health Check Utility.	PostInstallChecks_oim.xml
OIMSERVER_SERVER_TYPE	Enter `wls` as the Oracle Identity Manager server type. Oracle WebLogic Server is the only server type that is supported for this release.	PostInstallChecks_oim.xml
SOASERVER_PORT	Enter the default TCP port that the Managed Server hosting Oracle SOA uses to listen for regular (non-SSL) incoming connections.	PostInstallChecks_oim.xml
SOASERVER_SSL_PORT	Enter the default TCP port that the Managed Server hosting Oracle SOA uses to listen for SSL connection requests.	PostInstallChecks_oim.xml
OIMSERVER_INTERNALLOADBALANCERURL	Enter the URL used to access the Oracle Identity Manager user interface. You can enter the load-balancer URL or web server URL depending on the application server, or single application server URL. This value is used by Oracle Identity Manager in the notification e-mails as well as the callback URL for SOA calls.	PostInstallChecks_oim.xml
OIMSERVER_EXTERNALLOADBALANCERURL	Enter the details of single-node deployment that do not use Oracle HTTP Server to access Oracle Identity Manager Managed Server. This parameter is optional. For deployments with Single Sign-on (SSO) configured and that use Oracle HTTP Server to access the Oracle Identity Manager Managed Server, provide the SSO URL where the OIM user interface is available.	PostInstallChecks_oim.xml

Table 2–10 (Cont.) Parameters Listed in idmhc.properties File

Parameter	Description	Required For
EMAIL_ACCOUNT_PASSWORD	Enter the password used for mail server configuration using Oracle User Messaging Service. This parameter is optional. If not provided, you will be prompted for this password when you run the Health Check Utility.	PostInstallChecks_oim.xml
SOA_HOME	Specify the absolute directory path where SOA application is installed.	PostInstallChecks_oim.xml
TRUST_STORE	Enter the file name and the absolute path to the Trust Keystore.	PostInstallChecks_oim.xml
TRUST_STORE_PASSPHRASE	Enter the password to the Trust Keystore. This parameter is optional. If not provided, you will be prompted for this password when you run the Health Check Utility.	PostInstallChecks_oim.xml
TRUST_STORE_TYPE	Enter the Trust Keystore type. The commonly used value for this parameter is JKS.	PostInstallChecks_oim.xml
Parameters for Oracle Unified Directory		
OUD_HOST	Specify the host name of the server where Oracle Unified Directory is installed.	PostConfigChecks_oudhost.xml
OUD_ADMINPORT	Enter the Oracle Unified Directory administration connector port.	PostConfigChecks_oudhost.xml
OUD_ADMINUID	Specify the user name of the global administrator for Oracle Unified Directory replication. The default value of this parameter is admin. You can skip this parameter if the replication is not configured on the Oracle Unified Directory instance.	ReplicationCheck in PostConfigChecks_oudhost.xml
OUD_ADMINPASSWORD	Specify the password of the global administrator for Oracle Unified Directory replication. You can skip this parameter if the replication is not configured on the Oracle Unified Directory instance. This parameter is optional. If not provided, you will be prompted for this password when you run the Health Check Utility.	PostConfigChecks_oudhost.xml
OUD_HOME	Enter the path to directory where Oracle Unified Directory is installed. This parameter is optional. For example: /app/idm/Oracle_OUD1.	PostConfigChecks_oudhost.xml
OUD_INSTANCE_HOME	Specify the path to the Oracle Unified Directory instance. For example: /app/idm/asinst_1	PostConfigChecks_oudhost.xml

2.3 Executing the Oracle Identity and Access Environment Health Check Utility

The Oracle Identity and Access Environment Health Check Utility performs validation checks against your Oracle Identity and Access Management setup. The utility gathers

data from your environment, runs a set of health check plugins in an XML file, and generates a report that compares your environment configuration settings with various Oracle recommended configuration settings.

The `idmhc.sh` execution script (`idmhc.bat` for Windows) is required to run the Environment Health Check Utility and can be found in the `healthcheck/bin` directory.

Note:

Before running the Oracle Identity and Access Environment Health Check Utility,

- Ensure that you have provided the required information about the environment in the `idmhc.properties` file. For more information, see Section 2.2.3, "Understanding the idmhc.properties File of the Health Check Utility."
- Ensure that you have set the `JAVA_HOME` environment variable to the full path of the JDK directory.

The options used for executing this command vary depending on whether you completed a manual installation or an automated installation of Oracle Identity and Access Management.

This section describes the scenarios in which the Environment Health Check Utility can be executed:

- Executing the Oracle Identity and Access Environment Health Check Utility in a Manual Install Setup
- Executing Oracle Identity and Access Environment Health Check Utility in an Automated Install Setup

2.3.1 Executing the Oracle Identity and Access Environment Health Check Utility in a Manual Install Setup

Perform the following steps to manually run the Oracle Identity and Access Environment Health Check Utility:

1. Change directory to the location that contains the executable file:

   On Linux or UNIX:

   ```
   cd ORACLE_HOME/healthcheck/bin
   ```

   On Windows:

   ```
   cd ORACLE_HOME\healthcheck\bin
   ```

2. Execute the Environment Health Check Utility by running the following command:

   On Linux or UNIX:

   ```
   idmhc.sh -manifest location_of_manifest_file -topology location_of_
   topology.xml_file -credconfig location_of_credconfig_folder -group group_
   name(s) [-recover true|false] [-logDir path_to_healthcheck_log_files]
   [-DlogLevel=loglevel]
   ```

   On Windows:

   ```
   idmhc.bat -manifest location_of_manifest_file -topology location_of_
   ```

topology.xml_file -credconfig *location_of_credconfig_folder* -group *group_name(s)* [-recover true|false] [-logDir *path_to_healthcheck_log_files*] [-DlogLevel=*loglevel*]

For example:

idmhc.sh -manifest *ORACLE_HOME*/healthcheck/config/PostInstallChecks.xml -logDir *ORACLE_HOME*/healthcheck/bin/logs/healthchecker -DlogLevel=FINEST

Table 2–11 describes the various parameters you can use when you run the Environment Health Check Utility.

Table 2–11 Parameters for the Environment Health Check Utility Command

Option	Description
-manifest	Enter the location of the plugin manifest file. This parameter is mandatory. It configure the plugins to be executed. The manifest files are located in the healthcheck/config directory.
-topology	Enter the location of the topology.xml file. This parameter is optional. If specified, you do not need to enter values for the parameters in the idmhc.properties file. If you specify this option when running the command and there are values present in the idmhc.properties file, then the Health Check Utility will use the values in idmhc.properties. This option is applicable only if you are manually executing the Environment Health Check Utility in an automated install setup.
-credconfig	Enter the location of the credconfig folder. This parameter is optional. If specified, you do not need to enter values for the parameters in the idmhc.properties file. If you specify this option when running the command and there are values present in the idmhc.properties file, then the Environment Health Check Utility will use the values in idmhc.properties. This option is applicable only if you are manually executing the Environment Health Check Utility in an automated install setup.
-group	Specify the group names as defined in the manifest file. Use commas to separate the values. This parameter is optional.
-recover	Specify either true or false. Specify true to recover from the latest snapshot. The default is false. This parameter is optional.
-logDir	Specify the location where the Environment Health Check Utility will store the log files and reports.This parameter is optional. If not specified, the utility saves the Health Check summary reports in the *Current_working_directory*/logs/healthchecker directory by default.

Table 2–11 (Cont.) Parameters for the Environment Health Check Utility Command

Option	Description
`-DlogLevel`	Specify the level at which messages need to be recorded in the log file. Enter one of the following values: ■ `SEVERE` ■ `WARNING` ■ `INFO` ■ `CONFIG` ■ `FINE` ■ `FINER` ■ `FINEST` This parameter is optional. If not specified, the default is `INFO`.

You can use the options listed in Table 2–12 when executing the command.

Table 2–12 Options for the Environment Health Check Utility Command

Option	Description
`-v`	Print product version and exit the tool.
`-h`	Print help information and exit the tool.

Note: For information on how to manually execute the Health Check Utility in a manual install setup after configuration, see "Running the Environment Health Check Utility After Configuration" in the *Installation Guide for Oracle Identity and Access Management*.

2.3.2 Executing Oracle Identity and Access Environment Health Check Utility in an Automated Install Setup

If you installed Oracle Identity and Access Management using the Life Cycle Management tools, the Oracle Identity and Access Environment Health Check Utility is automatically invoked by the automated installer.

To manually execute the Health Check Utility in an automated install setup, follow the steps listed in Section 2.3.1.

Note: For information on how to manually execute the Health Check Utility before installing the Life Cycle Management (LCM) tools, see "Running the Health Check Utility to Verify Basic System Requirements" in the *Deployment Guide for Oracle Identity and Access Management*.

3

Analyzing Health Check Reports

When you run the Oracle Identity and Access Environment Health Check Utility, it retrieves relevant data from your environment and compares it with an Oracle recommended benchmark value for each of the configuration, tuning, and other settings. This information is then generated as XML and HTML reports. This chapter provides information about these reports. In addition, it provides information about how to analyze these reports.

This chapter includes the following sections:

- Oracle Identity and Access Environment Health Check Summary Reports

3.1 Oracle Identity and Access Environment Health Check Summary Reports

Whenever you run the Oracle Identity and Access Environment Health Check Utility, it generates XML and HTML reports along with all the other information about your environment. If you do not specify a log directory when you run the utility, these reports are placed at *Current_Working_directory*/logs/healthchecker. In addition, a log file is written to the same location.

For more information, see the following topic:

- Health Check Report Samples

3.1.1 Health Check Report Samples

Both the HTML and XML reports provide information about the various tests, plugin IDs, status, and corrective actions. In addition, the reports include information about the time a report was generated, host name, and the total time taken for each test.

For samples of the HTML and XML reports generated by the Health Check Utility, see the following topics:

- Sample of Health Check Report in HTML Format
- Sample of Health Check Report in XML Format

3.1.1.1 Sample of Health Check Report in HTML Format

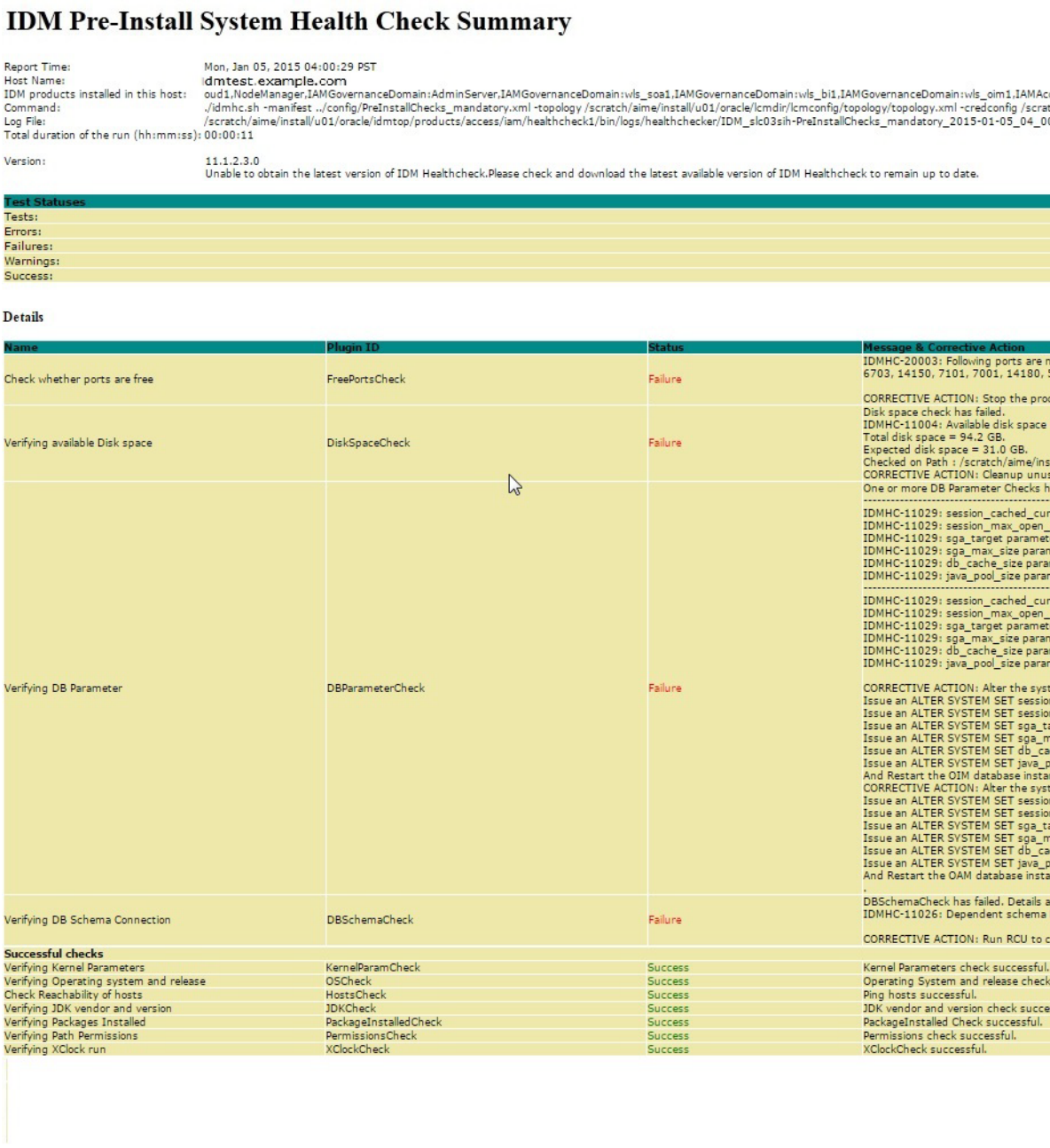
This section contains a sample Health Check report in HTML format. The HTML report includes the following information:

Table 3–1 Health Check HTML Report Information

Details	Description
Name	Name of the test.
Plugin ID	Plugin used for each test. The plugin differs based on your deployment. For more information about the plugins, see Section 2.2.2, "Understanding the Health Check Utility XML Files and Plugins."
Status	Status of each test. It could be Success, Warning, or Failure.
Message and Corrective Action	This column provides more information about each test. In case of Failure or Warning, this column includes information about the corrective steps that need to be taken to fix any issues. **Note**: For detailed information about fixing any issues, check the log file, which is located at *Current_working_directory*/logs/healthchecker by default.
Time	Time taken for each test.

Note: The values shown in the sample report might not be meaningful. The sample report is provided here merely to indicate the information that the report includes and to give you a general idea about the format and structure of the report.

Figure 3–1 Sample of Health Check Report in HTML Format



IDM Pre-Install System Health Check Summary

Report Time:	Mon, Jan 05, 2015 04:00:29 PST
Host Name:	idmtest.example.com
IDM products installed in this host:	oud1,NodeManager,IAMGovernanceDomain:AdminServer,IAMGovernanceDomain:wls_soa1,IAMGovernanceDomain:wls_bi1,IAMGovernanceDomain:wls_oim1,IAMAc
Command:	./idmhc.sh -manifest ../config/PreInstallChecks_mandatory.xml -topology /scratch/aime/install/u01/oracle/lcmdir/lcmconfig/topology/topology.xml -credconfig /scrat
Log File:	/scratch/aime/install/u01/oracle/idmtop/products/access/iam/healthcheck1/bin/logs/healthchecker/IDM_slc03sih-PreInstallChecks_mandatory_2015-01-05_04_0
Total duration of the run (hh:mm:ss):	00:00:11
Version:	11.1.2.3.0 Unable to obtain the latest version of IDM Healthcheck.Please check and download the latest available version of IDM Healthcheck to remain up to date.

Test Statuses	
Tests:	
Errors:	
Failures:	
Warnings:	
Success:	

Details

Name	Plugin ID	Status	Message & Corrective Action
Check whether ports are free	FreePortsCheck	Failure	IDMHC-20003: Following ports are n 6703, 14150, 7101, 7001, 14180, 5 CORRECTIVE ACTION: Stop the proc
Verifying available Disk space	DiskSpaceCheck	Failure	Disk space check has failed. IDMHC-11004: Available disk space Total disk space = 94.2 GB. Expected disk space = 31.0 GB. Checked on Path : /scratch/aime/ins CORRECTIVE ACTION: Cleanup unus
Verifying DB Parameter	DBParameterCheck	Failure	One or more DB Parameter Checks h ---------- IDMHC-11029: session_cached_cur IDMHC-11029: session_max_open_ IDMHC-11029: sga_target paramet IDMHC-11029: sga_max_size paran IDMHC-11029: db_cache_size para IDMHC-11029: java_pool_size paran ---------- IDMHC-11029: session_cached_cur IDMHC-11029: session_max_open_ IDMHC-11029: sga_target paramet IDMHC-11029: sga_max_size paran IDMHC-11029: db_cache_size para IDMHC-11029: java_pool_size paran CORRECTIVE ACTION: Alter the syst Issue an ALTER SYSTEM SET sessio Issue an ALTER SYSTEM SET sessio Issue an ALTER SYSTEM SET sga_ta Issue an ALTER SYSTEM SET sga_m Issue an ALTER SYSTEM SET db_ca Issue an ALTER SYSTEM SET java_p And Restart the OIM database insta CORRECTIVE ACTION: Alter the syst Issue an ALTER SYSTEM SET sessio Issue an ALTER SYSTEM SET sessio Issue an ALTER SYSTEM SET sga_ta Issue an ALTER SYSTEM SET sga_m Issue an ALTER SYSTEM SET db_ca Issue an ALTER SYSTEM SET java_p And Restart the OAM database insta .
Verifying DB Schema Connection	DBSchemaCheck	Failure	DBSchemaCheck has failed. Details a IDMHC-11026: Dependent schema CORRECTIVE ACTION: Run RCU to c
Successful checks			
Verifying Kernel Parameters	KernelParamCheck	Success	Kernel Parameters check successful.
Verifying Operating system and release	OSCheck	Success	Operating System and release check
Check Reachability of hosts	HostsCheck	Success	Ping hosts successful.
Verifying JDK vendor and version	JDKCheck	Success	JDK vendor and version check succe
Verifying Packages Installed	PackageInstalledCheck	Success	PackageInstalled Check successful.
Verifying Path Permissions	PermissionsCheck	Success	Permissions check successful.
Verifying XClock run	XClockCheck	Success	XClockCheck successful.

3.1.1.2 Sample of Health Check Report in XML Format

This section contains a sample Health Check report in XML format.

> **Note:** The values shown in the sample report might not be meaningful. The sample report is provided here merely to indicate the information that the report includes and to give you a general idea about the format and structure of the report.

Example 3–1 Sample of Health Check Report in XML Format

```
<?xml version="1.0" encoding="UTF-8"?>
<actions report_title="IDM Pre-Install System Health Check Summary" report_
date="Wed, Oct 29, 2014 23:09:45 PDT" elapsed_time="00:00:02" num_total="8" num_
error="0" num_failure="3" num_warning="0" num_success="5" log_
file="../healthchecker/IDM_slc02wkv-PreInstallChecks_mandatory_2014-10-29_11_
09-42PM.log" host_name="idmtest.example.com" products_list="null" cmd_
invoked="./idmhc.sh -manifest ..healthcheck/config/PreInstallChecks_
mandatory.xml">
  <action>
    <name>Verifying Kernel Parameters</name>
    <id>KernelParamCheck</id>
    <status>Failure</status>
    <message>One or more kernel parameters check has failed.

Current kernel.shmmax:1073741824. Minimum kernel.shmmax required:2147483648.
Failure.</message>
    <duration>00:00:00</duration>
  </action>
  <action>
    <name>Verifying Operating system and release</name>
    <id>OSCheck</id>
    <status>Success</status>
    <message>Operating System and release check are successful.</message>
    <duration>00:00:00</duration>
  </action>
  <action>
    <name>Check whether ports are free</name>
    <id>FreePortsCheck</id>
    <status>Success</status>
    <message>Free ports check is successful.</message>
    <duration>00:00:00</duration>
  </action>
  <action>
    <name>Verifying available Disk space</name>
    <id>DiskSpaceCheck</id>
    <status>Success</status>
    <message>Disk space check is successful.</message>
    <duration>00:00:00</duration>
  </action>
  <action>
    <name>Verifying DB Parameter</name>
    <id>DBParameterCheck</id>
    <status>Failure</status>
    <message>One or more DB Parameter Checks have failed. Details are provided
below
---------------------------------------------------------------------
DB Connection details found missing for OIM.
---------------------------------------------------------------------
DB Connection details found missing for OAM.
---------------------------------------------------------------------
DB Connection details found missing for OID.
.</message>
    <duration>00:00:00</duration>
  </action>
  <action>
    <name>Verifying DB Schema Connection</name>
    <id>DBSchemaCheck</id>
    <status>Failure</status>
    <message>DBSchemaCheck has failed. Details are provided below.
```

```
DB Connection details found missing for OID Schema.
DB Connection details found missing for OIM Schema.
DB Connection details found missing for OAM Schema.</message>
    <duration>00:00:00</duration>
  </action>
  <action>
    <name>Verifying JDK vendor and version</name>
    <id>JDKCheck</id>
    <status>Success</status>
    <message>JDK vendor and version check is successful.</message>
    <duration>00:00:00</duration>
  </action>
  <action>
    <name>Verifying Packages Installed</name>
    <id>PackageInstalledCheck</id>
    <status>Success</status>
    <message>Package Installed Check is successful.</message>
    <duration>00:00:00</duration>
  </action>
</actions>
```

Part II

Manual Checklist

It is important to check the sanity and health of your Oracle Identity and Access Management deployment and servers at various stages. Health checks need to be performed in the following scenarios:

- To check the readiness of the server, the necessary prerequisite libraries, packages, operating-system parameter values configured as required by the Oracle Identity and Access Management software.
- To check the sanity of your Oracle Identity and Access Management environment after installation:
  - To verify the connections between various tiers, Identity and Access Management databases, Identity and Access Management LDAP, and so on.
  - To verify the results of the execution of some basic functionality such as, account provisioning in corporate directory, Single Sign-On (SSO) to Out-Of-The-Box consoles, and so on.
  - To check the parameters of your deployment after patching or upgrade of the software.

To help you verify your Oracle Identity and Access Management environment at various stages of its life cycle, a checklist capturing relevant aspects, has been introduced.

The purpose of the manual checklist is to ensure that you do not miss out on any of the important steps while performing a deployment.

In the following chapters, you will find generic checklists, which are useful while deploying Oracle Identity and Access Management in any of the supported scenarios. In addition, there are checklists for specific scenarios, such as deploying Oracle Unified Directory, deploying Oracle Access Manager with a LDAP, and deploying Oracle Identity Manager with a LDAP.

Part II contains the following chapters:

4

Overview and General Preparation

This chapter contains a general preparation checklist for deploying Oracle Identity and Access Management.

It includes the following topics:

- Purpose of Oracle Identity and Access Management Deployment Checklists
- General Preparation

4.1 Purpose of Oracle Identity and Access Management Deployment Checklists

The Oracle Identity and Access Management deployment checklists are common guidelines for deploying Oracle Identity and Access Management 11*g* Release 2 (11.1.2.3.0) in production.

4.2 General Preparation

This chapter contains a general preparation checklist for 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 4–1 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.	☐

Table 4–1 (Cont.) General Preparation Checklist

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

5

Checklist for Deploying Oracle Unified Directory

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

Table 5–1 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 "Checking the System Requirements for Oracle Unified Directory" in *Installing Oracle Unified Directory*.	▫
Ensure that your system has sufficient RAM memory for JVM heap and database cache. For more information, see "Configuring the JVM, Java, and Database Cache Options for Oracle Unified Directory" in *Installing 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 "Support to Configure the Name of Rotated Log Files Using Local Time Stamp" in *Administering 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, and Database Cache Options for Oracle Unified Directory" in *Installing Oracle Unified Directory*.	▫
On Linux machines, ensure that the maximum file descriptor limit per process is set to `65535`. For more information, see "Software Requirements" in the *Release Notes for Oracle Unified Directory*.	▫

Table 5–1 (Cont.) Oracle Unified Directory Deployment Checklist

Requirement	Check when Verified
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 *Release Notes for Oracle Unified Directory*.	▫
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 "Understanding the Oracle Unified Directory Replication Model" in *Administering 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 *Administering Oracle Unified Directory*.	▫
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 *Administering Oracle Unified Directory*.	▫
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 *Administering Oracle Unified Directory*.	▫
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 and ODSEE Replication Status in Deployments Using Replication Gateways" in *Administering Oracle Unified Directory*.	▫
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	▫

6

Checklist for Deploying Oracle Access Manager

This chapter contains a checklist for deploying Oracle Access Manager with LDAP.

Table 6–1 Oracle Access Manager Deployment Checklist

Requirement	Check when Verified
Ensure that a supported Oracle Database, an Oracle Middleware Home, and a 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 `IAMSuiteAgent` 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 the Oracle Access Manager servers.	☐
Ensure that your LDAP is preconfigured as an Identity Store as described in the *Installation Guide for Oracle Identity and Access Management*.	☐
Ensure that the Identity Store has the required schemas extended. **Note:** The specific schemas are loaded when the identity store is prepared. They are also present in the `IAM_HOME/oam/ldap/schema` directory.	☐

Table 6–1 (Cont.) Oracle Access Manager Deployment Checklist

Requirement	Check when Verified
Ensure that the Identity Store is seeded with the required users, groups, and privileges, based on the input properties passed to the `idmConfigTool` command.	☐
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 Oracle Access Manager Webgate agent is created.	☐
Ensure that the LDAP Identity Store is configured in the Oracle 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 the Oracle Access Manager Administration Console and has a webgate wired to Oracle 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 WebLogic Server 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 performance is tuned based on the tuning guidelines. For more information, see "Oracle Access Management Performance Tuning" in the *Performance and Tuning Guide*.	☐
Ensure that you have configured a custom login and error pages to meet your deployment requirements.	☐
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.	☐

Table 6–1 (Cont.) Oracle Access Manager Deployment Checklist

Requirement	Check when Verified
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 the 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.	☐

7

Checklist for Deploying Oracle Identity Manager

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

Table 7–1 Oracle Identity Manager Deployment Checklist

Requirement	Check when Verified
Ensure that a supported Oracle Database, an Oracle Middleware Home, and a 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 Hot Spot JVM)
`-XX:+UseLargePagesForHeap`
`-XX:+ForceLargePagesForHeap` (for JRockit JVM).
In JRockit JVM, if you are enabling large pages, do not use the argument:
`-XX:+UseLargePagesForCode`
	☐

Table 7–1 (Cont.) Oracle Identity Manager Deployment Checklist

Requirement	Check when Verified
Oracle Identity Manager uses ApplicationDB, oimOperationsDB, and oimJMSStoreDS data sources deployed on Oracle WebLogic Server. As a general guideline, ensure that the capacity for these data sources is increased as follows: ■ ApplicationDB: Initial Capacity=50; Minimum Capacity=50; Max Capacity= 50; and Inactive time out seconds=300. ■ oimOperationsDB: Initial Capacity=32: Minimum Capacity=32; Max Capacity=32; and Inactive time out seconds=300. ■ oimJMSStoreDS: Initial Capacity=15; Minimum Capacity=15; Max Capacity=15; and Inactive time out seconds=300 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.	☐
Ensure that default values of Message Buffer Size and Messages Maximum properties are changed to the recommended values: ■ Message Buffer Size: 200 MB (209715200 bytes) ■ Messages Maximum: -1 or any number not less than 400000	☐
Ensure that the properties Maximum Threads Constraint of work managers `OIMMDBWorkManager` and `OIMUIWorkManager` are set to `6` and `10`, 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 *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`.	☐

Table 7–1 (Cont.) Oracle Identity Manager Deployment Checklist

Requirement	Check when Verified
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 *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.	☐
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 Oracle Virtual Directory (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/web server 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 *Administering 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.	☐

Table 7–1 (Cont.) Oracle Identity Manager Deployment Checklist

Requirement	Check when Verified
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.	☐
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 *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 *Administering 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 *Developing and Customizing Applications for Oracle Identity Manager*. For more information about modifying the value of the system property, see "Managing System Properties" in *Administering Oracle Identity Manager*.	☐

Table 7–1 (Cont.) Oracle Identity Manager Deployment Checklist

Requirement	Check when Verified
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.	☐