ORACLE
Consulting

Infrastructure Administration

Identity Governance Services 1.0.0

Infrastructure Administration

Identity Governance Services 1.0.0

by Sophie Strecke, Dieter Steding, and Sylvert Bernet

Table of Contents

Preface

Audience

This guide is intended for resource administrators and target system integration teams.

Reference Documents

For information about installing and using Oracle Identity and Access Management, visit the following Oracle Help Center page:

- *https://docs.oracle.com/en/middleware/idm/suite/12.2.1.3/index.html*

Confidentiality

The material contained in this documentation represents proprietary, confidential information pertaining to Oracle products and methods.

The audience agrees that the information in this documentation shall not be disclosed outside of Oracle, and shall not be duplicated, used, or disclosed for any purpose other than to evaluate this procedure.

Typographical Conventions

The following table describes the typographic changes that 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.

Symbol Conventions

The following table explains symbols that might be used in this document.

Convention	Meaning
[ ]	Contains optional arguments and command options.
{ | }	Contains a set of choices for a required command option.
${ }	Indicates a variable reference.
-	Joins simultaneous multiple keystrokes.
+	Joins consecutive multiple keystrokes.
>	Indicates menu item selection in a graphical user interface.

About the Service

The service provides an API to generate anonymized identifiers for user accounts. The purpose of these anonymous identifiers is to hide the true identity of a person in external communication, such as the Internet, in order to prevent conclusions about the person.

This guide describes the procedures for deploying and using the service.

This chapter contains the following sections:

Deployment Configurations

The target system must be a Java EE 8 complient application server. The following table lists the verified deployment configurations for the target system.

System	Requirement
Oracle Identity Governance	You can use one of the following releases of Oracle Identity Governance: • Oracle Identity Governance 12c Re PS3 (12.2.1.3.0) • Oracle Identity Governance 12c Re PS4 (12.2.1.4.0)
Java JDK	Google API Gateway Edge

Supported Languages

The deployment the following languages:

- English
- French
- German

<seealso> </seealso>

Features of the Service

This section discusses the following topics:

Roadmap for Deploying and Using the Service

Subsequent sections include the additional information covered by this guide:

Deployment of the Service

The service is deployed on a Java EE 8 complient application server. For a successful provision of the service in such an application server, it must be prepared accordingly in advance.

This chapter describes the procedures for preparing the application server and covers:

This chapter contains the following sections:

Create Domain

The configuration of production domain has been made with production in mind, so there are a number of differences when compared to the default domain which are listed below. Not all of these will be wanted for development environments, but all are good practice for production domains.

Differences in Server Configuration

1. Autodeployment has been disabled.

   Payara Server comes with a deployment scanner. This is a security risk for production, so it is disabled by default in the domain.xml.

2. Dynamic application reloading is disabled.

   For the same reason as above, this is disabled by default in the domain.xml.

3. Dynamic reloading of JSP pages in `default-web.xml` is disabled.

   The `<init-param>` setting reload-interval in the `default-web.xml` has been set to a value of `-1` so that it is disabled.

4. The EJB container `max-pool-size` has been set to `128`.

5. The `max-thread-pool-size` setting for `thread-pool-1` has been increased to `250`.

6. File caching has been enabled for both default HTTP listeners (`http-listener-1` and `http-listener-2`).

7. Isolated classloading has been enabled by default at the server level.

   The property `fish.payara.classloading.delegate` has been set to `false`.

8. A default transaction timeout of 300 seconds has been added for xa and non-xa transactions.

9. Default group-to-role mapping is enabled.

10. The maximum size for the thread pool `http-thread-pool` has been increased from `5` to `50`.

Differences in JVM Options

With the aim of production domain being to target production, the production domain has JVM options specifically configured for usage on JDK 8. Since JDK 7 has reached its end-of-life, it is therefore a security risk to run a JVM lower than version 8 in production. However, production domain can be configured to run on JDK 7 if necessary by editing the JVM options.

The following JVM options only appear in production domain:

- -server
- -Xmx2g
- -Xms2g
- -XX:+UseG1GC
- -XX:+UseStringDeduplication
- -XX:MaxGCPauseMillis=500
- -XX:MaxMetaspaceSize=2g
- -XX:+IgnoreUnrecognizedVMOptions
- -Djdk.tls.rejectClientInitiatedRenegotiation=true

The following JVM options only appear in the default domain:

- -client
- -Djavax.management.builder.initial=com.sun.enterprise.v3.admin.AppServerMBeanSer
- -Xmx512m
- -XX:NewRatio=2
- -Dcom.sun.enterprise.security.httpsOutboundKeyAlias=s1as
- -Dorg.glassfish.additionalOSGiBundlesToStart=org.apache.felix.shell,org.apache.felix.g
- -Dosgi.shell.telnet.port=6666
- -Dosgi.shell.telnet.maxconn=1
- -Dosgi.shell.telnet.ip=127.0.0.1
- -Dgosh.args=--nointeractive
- -Dfelix.fileinstall.dir=${com.sun.aas.installRoot}/modules/autostart/
- -Dfelix.fileinstall.poll=5000
- -Dfelix.fileinstall.log.level=2
- -Dfelix.fileinstall.bundles.new.start=true
- -Dfelix.fileinstall.bundles.startTransient=true
- -Dfelix.fileinstall.disableConfigSave=false
- -Dcom.ctc.wstx.returnNullForDefaultNamespace=true

The following JVM options appear in both domain and production domain:

- -Xbootclasspath/p:${com.sun.aas.installRoot}/lib/grizzly-npn-bootstrap.jar

- -Djava.awt.headless=true
- -Djdk.corba.allowOutputStreamSubclass=true
- -Djavax.xml.accessExternalSchema=all
- -XX:+UnlockDiagnosticVMOptions
- -Djava.security.policy=${com.sun.aas.instanceRoot}/config/server.policy
- -Djava.security.auth.login.config=${com.sun.aas.instanceRoot}/config/login.conf
- -Djavax.net.ssl.keyStore=${com.sun.aas.instanceRoot}/config/keystore.jks
- -Djavax.net.ssl.trustStore=${com.sun.aas.instanceRoot}/config/cacerts.jks
- -Djdbc.drivers=org.apache.derby.jdbc.ClientDriver
- -DANTLR_USE_DIRECT_CLASS_LOADING=true
- -Dcom.sun.enterprise.config.config_environment_factory_class=com.sun.enterprise.cor
- -Djdk.tls.rejectClientInitiatedRenegotiation=true
- -Dorg.jboss.weld.serialization.beanIdentifierIndexOptimization=false
- -Dorg.jboss.weld.serialization.beanIdentifierIndexOptimization=false
- -Dorg.glassfish.grizzly.DEFAULT_MEMORY_MANAGER=org.glassfish.grizzly.memory.

Support for the `java.endorsed.dirs` and `java.ext.dirs` options are removed from version 5.192 onwards (these were deprecated since 5.191). The concept of endorsed and ext directories are no longer supported with Java 9+.

The service is deployed in a sce

Optional Package

The service relies on the Java optional package mechanism.

Optional packages are packages of Java classes and associated native code that application developers can use to extend the functionality of the core platform.

To ensure the Java optional package mechanism, copy the JAR files into the *domain-dir*`/lib` directory, or use the `asadmin add-library` command with the `--type ext` option, then restart the server. For more information about the `asadmin add-library` command, see the *GlassFish Server Open Source Edition Reference Manual*.

Following packages needs to be copied:

Package	Directory
ocs-hst-core.jar	<domain-home>/lib
ocs-hst-jps.jar	<domain-home>/lib
ocs-hst-json.jar	<domain-home>/lib

Package	Directory
ocs-hst-rest.jar	<domain-home>/lib
ocs-iad-saml.jar	<domain-home>/lib
ocs-igd-scim.jar	<domain-home>/lib